INF813-CISSP-08-PA

0:02
Non, récemment il est parti. En fait je je l'ai lancé. Je pense que j'avais un souci de connexion donc on ne l'avait pas pris. C'est juste ça, c'est bon. OK, donc on va parler de des enquêtes, donc les différents types d'enquêtes qui existent, on a les enquêtes administratives.

0:31
Quand on a souvent des enjeux juridiques ou on veut savoir plusieurs un événement qui s'est passé, il y a plusieurs types d'enquêtes qu'on veut mener. Donc il y a Parmi ces enquêtes, on a une enquête administrative qu'on peut mener. Donc ce sont des enquêtes qui peuvent être internes, qui sont menées juste dans le but opérationnel ou disciplinaire. On peut avoir des enquêtes criminelles ou pénales qui visent à prouver qu'un crime a été commis. Donc on peut avoir des enquêtes civiles juste pour résoudre des litiges entre parties, entre des parties. Donc c'est pas.

1:00
Dans l'ordre criminel, donc on va pas peut être vous condamner pour ça. Donc généralement les les enquêtes civiles, vous avez eu un litige avec quelqu'un, vous avez fait affaire avec avec quelqu'un et puis ça s'est pas bien déroulé, donc on vous pouvez aller au niveau civil. Ensuite on peut avoir des enquêtes conformité, donc c'est pour vérifier la conformité à une norme, donc par exemple PCA et DSS. Donc si admettons on est, on veut être conforme à PCA et DSSP.

1:25
On peut venir faire une enquête ? Bon on va appeler ça un audit pour vérifier. Est ce que on est correct avec la norme ? Et puis est ce que on peut avoir la certification ? Les attestations qui prouvent qu'on a le PCADSS dans la sphère informatique. On peut mener des enquêtes en informatique donc on pourra peut être regarder tout ce qui est média, donc examiner tout ce qui est média physique. Donc on a les supports, les ordinateurs qu'on peut regarder.

1:52
Peut faire l'analyse des logiciels donc on pourra trouver des traces malicieuses et l'identité de l'auteur. On peut faire des analyses réseau donc on va regarder le réseau des journaux afin d'identifier et puis connaître la cause. On peut faire des enquêtes sur tout ce qui est matériel périphérique intégré donc des analyses de matériel et périphériques donc peut être clavier sourit pour voir si on est capable de trouver des empreintes là-dessus on a.

2:21
Un processus à faire quand on fait des enquêtes informatiques, on appelle généralement le Electronic Discovery, donc on va, on passe généralement par ces étapes là, les, les, les 9, les 9 étapes qu'on va faire. La première c'est la gouvernance. Donc j'ai laissé les thèmes en anglais, les thèmes en français qui ressemblent plus à des thèmes anglais je pense. J'ai pas changé parce qu'en réalité le le CSSP vous allez lui passer en anglais.

2:45
Donc autant que faire ce que si j'ai l'équivalent du thème en anglais. C'est vrai qu'on fait le cours en français, mais je mets le thème en anglais pour que vous vous retrouviez quand vous allez faire vos vos tests avec des documents en anglais. Donc gouvernance et guargernance il n'y a pas grande différence donc je le remercie. Donc lui ça sera à ce niveau-là. On va organiser l'information dès les

départs pour qu'elle soit facile à retrouver en cas de litige. Et 2e ça sera l'identification, on va repérer les fichiers ou.

3:14
Les systèmes qui contiennent l'information pertinente, dès qu'on pense qu'il y a, on va, on va faire un procès. Ensuite il y a la préservation qui est protéger les données contre toute notification ou suppression. Donc quand on a les données qu'on va utiliser pour des preuves, on fait tout pour les préserver. Il faut peut être fermer le support en en juste en lecture pour ne pas qu'on puisse écrire la chose. Il y a quelque chose à suivre, il faut le faire.

3:39
Ensuite on a la cueillette qu'on appelle collection aussi, qui peut, qui permet de rassembler les données concernant concernées. Dans un emplacement central, on a le traitement ou le processing qui permet de nettoyer les données pour éliminer les informations manifestement inutiles. Donc souvent on a des doublons ou des lots qui sont pas pertinents, donc on va les enlever. Ensuite on a la review review qui est le le review pour examiner ce qui reste.

4:05
Pour voir ce qui est pertinent et retirer ce qui est confidentiel. Donc des fois on peut avoir dans les éléments qu'on a des échanges de courriels avec peut être l'avocat ou en interne au niveau de l'entreprise on veut pas que les gens aient ces informations donc on pourrait enlever ces informations là. Ensuite on a l'analyse ou l'analyse qui permet d'inspecter faire des inspections plus poussées sur le contenu, le contexte. Donc ça peut inclure des corrélations, des mots clés, des chronologies.

4:35
Ensuite on a la production qui est formater les données pour pouvoir les transmettre à la partie adverse, donc les fichiers PDF, le format juridique. Ensuite on a la présentation des résultats qui est montré les les données au tribunal, au témoin ou aux jurés dans une forme claire et intelligible. On a la chaîne de costody qui est chain of custody, qui est une chaîne.

5:03
Qui qui est un processus sur le projet de documentation qui permet de garantir l'intégrité, l'authenticité de la, des, des, des preuves. Donc avec la chaîne des qu'on se dit on va la chaîne de de possession, on va essayer d'avoir le journal des preuves, donc notamment qui va inclure les les attributs suivants, les caractéristiques suivants, les personnes impliquées, la destruction de la preuve, le lieu, la date, l'heure et la découverte de la découverte de la de la preuve.

5:32
Ensuite, on va avoir des méthodes, des méthodes qui ont été utilisées pour la découverte, le stockage et puis comment ça a été préservé et puis le transport. Ensuite, on aura le suivi de la prise d'identification à la description. On a maintenant les types de preuves. Ça, c'est des éléments qui sautent beaucoup quand on fait les tests de CSSPI, c'est des éléments qui faut chercher à comprendre les différents types de preuves.

6:03
Parce que on peut tourner la question dans tous les sens. Mais une fois que vous comprenez le le concept, ça sera plus facile pour vous de répondre aux questions. Donc les différents types de preuves qu'on a, on a la preuve qu'on appelle réelle qui est physique. Et puis qui est Real trop souvent dans certains documents que vous allez avoir object évidence.

6:22
Qui ? Qui peut être l'ordinateur qui est saisi, le clavier avec empreinte ou tout autre élément physique qu'on peut saisir ? Donc on va eux, on va les appeler Real object evidence ou en français Real ou physique. Donc on a la 2e preuve qui est la preuve documentaire, donc documentary evidence qui va obéir à 2 rôles, 2 règles donc la première règle qui est le best evidence Hall qui est appelé la meilleure preuve donc c'est à dire que on considère avec cette règle là.

6:53
Le document qui est fiable, c'est le document original. Donc si vous voulez prouver, admettons que vous avez un passeport, Ben venez avec le passeport original, la photocopie ça va pas nous servir à grand chose. On peut montrer la photocopie vraiment quand on a pas le document original, mais c'est le document original qui est préféré. Donc ça c'est la première règle fournie des tous les documentaires. La 2e règle c'est le parole du Dance rôle.

7:17
Qui est la règle de la preuve intersecte c'est vrai que parole en en français ça veut dire parole, mais ça c'est pas c'est pas c'est c'est dans toujours dans le cadre documentaire. Donc ça veut dire que le document écrit est présumé contenu tous les termes de l'accord et prime sur tous les tout accord verbal antérieur ou parallèle. Donc ça veut dire quoi ? Ça veut dire que si entre vous ou dans un contexte d'affaires vous avez écrit un document.

7:43
Pour vous engager, tout ce que vous allez dire oralement verbalement n'a plus n'a plus de sens, c'est qu'on va considérer le document écrit qui va faire foi. Donc ça sera pareil dans au au tribunal si et si quand on parle de preuve c'est plus, on vous voyez plus dans l'aspect qu'on va aller devant un un juge ou au tribunal. Donc on essaie de donner les formations comme si on était dans un cours de droit. Donc que ça soit dans le cadre informatique ou pas, ces thèmes là sont valables également.

8:15
Autre chose, autre type de preuve, c'est le témoignage. Donc c'est Simon evidence, donc ça peut être un témoignage verbal ou écrit, donc quelqu'un peut venir témoigner, il peut venir à la Cour ou il peut venir au tribunal témoigner directement dit ce qu'il a vu ou par écrit il va témoigner. Mais on veut que le témoignage soit direct, donc on veut pas de ouï-dire ou de de 2nde main. C'est à dire ?

8:40
Toi, tu n'étais pas sur le lieu où tu n'as pas vu, mais tu as entendu les gens dire que donc on revient. Tu reviens dire que toi tu l'as tu. Tu tu viens te porter comme un témoin alors que tu n'étais pas là sur les lieux. T'es pas un témoin direct. Donc en anglais, généralement vous allez voir RC dans les documents, plus les les documents de CSSP. Ensuite un autre qui rentre dans le témoignage.

9:08
C'est le témoignage d'experts. Donc on peut avoir des des experts qui peuvent venir témoigner, qui peuvent venir témoigner, dire oui selon moi mon expérience tel aspect on peut pas peut être on peut pas avoir fait une attaque de phishing sans envoyer un courriel parce que c'est pas possible qu'on ait on on ait eu l'attaque de fiches sans courriel dont on a forcément le courriel qui est quelque part qu'il faut trouver donc.

9:32

Le l'expert va venir nous donner plus d'informations par rapport à son expertise. Donc ce sont des témoignages qui sont souvent qui sont acceptés aussi. L'autre type de preuve, c'est la preuve démonstrative. Donc c'est on va plus prendre des éléments visuels, des schémas, des diagrammes donc qui sont utilisés pour illustrer ou appuyer un témoignage. Donc très souvent ça constitue pas une preuve, mais ça peut rendre le témoignage plus compréhensif.

9:59
Et puis il est souvent accepté par le jury si ça ne force pas l'interprétation. Donc voici les 4 types de preuves qu'on peut avoir avec leurs spécificités. Donc c'est bon, c'est important de maîtriser tout ce qui est baisse, évidence, rôle, parole, évidence, rôle, savoir c'est quoi le Rci ? Connaître les 4 types de de preuve pour que lors de votre test, vous puissiez vous en sortir. C'est bon, on continue.

10:29
Ok, on continue. Oui OK oui gilas s'il vous plaît Monsieur. Ma question c'était de savoir c'est quoi le le lien où pouvez vous établir un parallélisme entre votre cours, le cours que vous donnez cette soirée là et le projet, ça clique, le, le projet d'enquête, ça dans le cadre, ça clique.

10:57
Il y a un procès qui doit qui il y a, il y a un projet là qui qui qui est en train de fouiller ou de de mener des enquêtes par rapport à ce qui s'est passé. Ouais à la 5 est ce que qu'est ce qu'on peut retenir de points communs ou comprendre faire un parallélisme concernant votre cours et ce projet là tu parles de ce que du slide qu'on vient d'expliquer là hein, c'est bien ça hein ? Ouais ouais Ah OK dans le dans le cadre de votre cours en général voilà.

11:26
OK Ben ça ça va être vraiment long mais moi je je veux juste parler de l'enquête sinon si c'est le le le cours ça va être vraiment long, on on va rentrer dans tous les détails. Puis bon y a peut être des paramètres que moi je maîtrise pas mais je vais juste parler par exemple de l'enquête donc juste l'enquête j'ai vu que ils ont sorti le le taux horaire par exemple des consultants ils ont dit que y a des les consultants sont passés je crois de 80 ou 85$ à 300,00$ de l'heure en moins de je sais pas un an ou 2 ans.

11:52
Donc ça, s'ils le disent-ils ont seulement vu une preuve quelque part. Et ça peut être une preuve peut être documentée quelque part, soit un un rapport ou quelque chose de décrit. Donc ça pourrait être dans ce contexte-là, ça pourrait être un témoignage. Peut être que et quelqu'un peut être qui était qui passait le contrat, ou ils ont trouvé un document écrit quelque part, ou ça peut être un une preuve documentaire qu'ils auraient vu quelque part maintenant. Sinon globalement le projet.

12:23
Ça clique, je connais pas tout. Le contexte c'est que j'ai des amis qui qui qui travaillent, qui m'en avaient parlé. Mais j'ai pas tout le contexte du projet donc je veux pas m'aventurer de peur de raconter des choses que je ne sais pas. Mais si c'est dans le cadre de des enquêtes, c'est ce que je peux. Je peux dire. OK, on a parlé tantôt des différentes preuves qu'on peut avoir.

12:52
Mais il y a des preuves qui sont admissibles et les preuves qui sont admissibles doivent correspondre doivent respecter 3 conditions de base. Donc la première c'est que la preuve doit être pertinente pour État bien fait. Donc on vient, on veut dire que quelqu'un comme l'exemple que je donnais on dit on

veut dire que sur le projet s'applique dont parlait gires les consultants étaient payés de 80$ à à 390$ en moins de 01h00 en moins de un an ou 2 ans. Mais il faut avoir.

13:20
Une preuve qui en parle donc on va pas aller prendre une preuve d'un autre projet qui n'a rien à voir et puis venir prouver. Donc il faut que le le la preuve soit pertinente pour le cas qu'on est en train d'investiguer. 2e chose, le fait en question doit être matériel, c'est à dire avoir un lien direct avec l'affaire donc ça rentre un peu dans la même chose donc on va prendre une preuve qui rentre en lien direct avec le cas ça qui donne en train de parler. 3e, la preuve doit être légale donc c'est à dire obtenue selon la loi, donc je prends un cas.

13:49
Si admettons qu'on avait un rapport ou le un contrat des des consultants ou un contrat de la compagnie qui donne des consultants et dans lequel on avait le taux horaire, la preuve est légale si ça a été obtenu de la bonne façon. Mais si ils ont piraté le système de la compagnie pour trouver la preuve n'est pas recevable. C'est vrai que ça, ça nous donne l'info, mais la preuve n'est pas recevable. Donc une preuve elle doit être obtenue de façon légale.

14:17
D'abord, donc ça ce sont les conditions pour que les preuves soient valables. On a donné les différents types, on a donné les conditions, lesquelles les preuves sont valables. Donc pour avoir les preuves, qu'est ce qu'il ne faut pas faire pour ? On a parlé tantôt les différentes preuves qui sont acceptées, les conditions d'acceptation des preuves. Maintenant qu'est ce qu'on ne fait pas donc pour les systèmes d'exploitation donc ?

14:42
On ne modifie pas la date heure des fichiers. Donc si si jamais admettons on veut vous on veut enquêter sur des éléments que vous avez mis en base dans une base de données ou peut être dans le système d'exploitation. Vous avez enregistré un fichier, vous pouvez changer l'heure du de du système d'exploitation et là ça va plus refléter la réalité. Donc quand en cas d'enquête on veut pas que ça soit fait, on change pas l'heure, on va, on arrête pas les processus.

15:12
Même si il y a un virus là-dessus, on arrête pas les processus, on les laisse Asus, on arrête pas les systèmes, on peut contenir les systèmes pour ne pas qu'il y ait de la propagation. On arrête pas les systèmes jusqu'à ce que il y ait un expert qui vienne capturer l'image. Sinon à un moment donné oui on peut arrêter. Ensuite on installe pas les correctifs pour bruer les enquêtes. Donc admettons on a il y avait une une vulnérabilité sur le réseau, c'est la vulnérabilité que les acteurs ont utilisé.

15:41
Lors d'une enquête on va pas venir corriger la vulnérabilité. Puis qui dit que la vulnérabilité n'existait pas ? Donc on laisse Aziz, on ne touche à rien, on va pas exécuter des programmes qui sont pas de confiance. C'est vrai que pour collecter tout ce qui est forensic, à un moment donné on va installer des logiciels mais ça sera juste sur la la recommandation de la compagnie qui est chargée, faire le forensic, écrire par-dessus les preuves potentielles en effectuant l'installation des logiciels. Donc ça on ne fait pas.

16:11
Sur toujours, qu'est ce qu'on peut faire avec des systèmes opérationnels ? Donc on peut copier les

médias originaux pour des fins d'analyses, on peut recueillir des preuves et maintenir la chaîne de possession, donc on n'a pas eu les constituants. On peut tout documenter, puis utiliser des exécutables de confiance provenant des kits de réponse aux incidents pour recueillir les données volatiles, donc dont je parlais tantôt. On a des kits qu'on utilise en cas de réponse aux incidents, donc.

16:36
On peut les on peut les installer sous recommandation de la de la compagnie qui est venue faire la la réponse aux incidents et qui va faire le forensic, donc qu'est ce qu'on va rechercher ? Donc on a des matériels non autorisés a été rattaché au réseau, ça on va les chercher. On va chercher des signes d'accès non autorisés à partir des contrôles d'accès physiques. Donc est ce que quelqu'un est rentré sur le site ?

17:03
Dans dans nos locaux sans carte d'accès ou même s'il avait qu'un avec des cartes d'accès, est ce qu'il était autorisé à rentrer dans certaines salles, on va voir est ce qu'il y avait des outils de piratage qui étaient là, des processus non autorisés ou des applications qui sont en cours d'exécution. On va voir est ce qu'il y a des manquements ou absents des journaux d'événements parce qu'il arrive que lors de certaines attaques on va effacer certains journaux d'événements pour ne pas avoir des traces.

17:29
On va les événements des journaux, des IDS, on veut les, on veut les garder. Est ce que y avait des y avait des visites sur des sites adultes, est ce que y avait des logiciels piratés ? Est ce que y avait des courriels violents qui violaient des politiques de l'entreprise ? Donc admettons que on transfère des des renseignements personnels à des personnes ou à une boîte personnelle, donc ça on va regarder tous ces aspects. Est ce que y avait des numéros, des cartes de crédit, des données des clients, tout ça ?

17:56
On va regarder aussi. Est ce qu'il y avait des connexions inhabituelles, des échecs, des outils de sécurité, des succès inhabituels, des outils de sécurité, des échecs dans les tentatives de connexion, des activités en dehors des heures normales de travail, des élévations ou changements de dans les droits des utilisateurs, et puis la perte d'intégrité des fichiers systèmes. Donc on a les outils qui sont capables de nous donner ces informations là. Ensuite l'authentification des éléments.

18:23
Donc, principalement à l'aide d'une fonction de hachage, on peut retrouver ça, les enquêteurs qui peuvent travailler sur des copies judiciaires, la copie des des copies de sécurité. Et puis on pourrait dépliquer d'une façon dupliquer les informations d'une façon qu'il soit acceptable à à la Cour ou pour les enquêtes. On pourrait vérifier aussi les équipements, donc les téléphones, les tablettes, les ordinateurs, tout ça, que ça soit personnel ou pas.

18:51
On pourrait regarder quel est le téléphone intelligent, les smartphones, analyser les vidéos puis les captures de changes qui ont été faites. On pourrait regarder tout ce qui est USP des mémoires Flash et cetera sur le réseau. On pourra surveiller le réseau, regarder des des sniffers qu'on avait sur le réseau et chercher des comportements ou activités suspects. Essayer de ne pas alerter les pirates informatiques qui sont actifs sur notre réseau. Si on a des ony pot, on pourrait les mettre. On va en parler après.

19:21
Est ce que c'est bon à ce niveau ? Il y a un changement, vous parlez d'un vous partez d'un enseignant à l'autre. C'est vrai que je peux être plus rapide ou moins rapide ou ne pas être dans ces détails si vous avez besoin d'éclaircissement si vous trouvez que le débit il est là ou très rapide, laissez-moi savoir s'il vous plaît. O k les activités de journalisation.

19:50
Oui, Émile en premier lieu, moi je trouve le débit correct, ça va, mais si on revient par rapport aux enquêtes, là j'essaie de voir parce que là c'est sûr qu'on réponse aux incidents, faut agir le plus vite possible, puis il faut faire le confinement et l'éradication. Cependant, c'est quel équilibre que je peux avoir entre ?

20:15
Les affaires d'enquête là tu dis OK, on laisse les les choses le plus assez possible, puis il faut faire le confinement, puis l'éradication c'est quoi ? Tu peux conseiller comme équilibre-là dedans ? OK en fait ça arrive que souvent dans certaines éradications on peut. Attends je je vais, je vais retourner.

20:44
Sur le système d'exploitation quoi ne pas faire donc la date on est d'accord, arrêter le processus ça si le processus est en démarrage c'est pas grave, si on on arrête on pourrait redémarrer arrêter le système. C'est là que ça arrive parce que souvent il y a des mémoires qui peuvent être dans la, dans la rame des mémoires, dans la mémoire volatile et lors de redémarrage on pourrait les perdre. Donc très souvent ce qu'on fait dans le confinement, on essaie de vraiment isoler la machine.

21:12
Il y a plusieurs techniques au niveau de des outils pour isoler la machine pour ne pas qu'il y ait de la propagation, mais on ne l'était pas la machine. En réalité, on peut vraiment faire en sorte que au niveau de la communication réseau, qu'ils ne puissent pas communiquer avec les autres qui propagent pas, mais sur la machine sur laquelle il y a l'infection, on pourrait juste la garder jusqu'à ce que on ait l'équipe de réponse aux incidents qui eux vont venir capturer la preuve avant qu'on puisse chat dans le le système.

21:42
Donc moi je dirais à quel moment on l'arrête ou pas, mais c'est vraiment se fier à l'équipe de réponse aux incidents. Qu'est ce qui est prévu ? Qu'est ce qui est prévu dans le playbook au niveau de l'entreprise en cas de ce type d'incident là ? Allô Émile ? Oui oui je t'écoute, je t'écoute, c'est ça Ben je je tu vas aborder la réponse aux incidents tantôt je j'ai mis jeté un peu là-dessus. Ouais non c'est bon.

22:12
C'est bon mais c'est c'est vraiment là. Dans le plan de réponse aux incidents, on on définit souvent tous ces playbooks là qu'est ce qu'on fait si on a un malware ? Ben on va. Dès qu'on arrête pas le système, on fait pas ceci. On il y a des actions qui sont décrites dépendamment de de votre plan. Et quand on dit de ne pas arrêter, c'est ne pas arrêter jusqu'à ce que ceux qui sont censés faire la réponse aux incidents viennent capturer l'image en fait de de l'appareil.

22:40
Pour des fins d'enquêtes ? Donc c'est après ça qu'on pourra redémarrer. Mais sinon si admettons que on a des virus avant en tout cas de d'isoler qu'on sent que il est lui même capable de détruire toutes

les preuves. Je pense qu'on peut prendre des actions. Peut être de de chat donne, mais ça va dépendre vraiment de soit votre playbook ou bien de votre SPO qui est défini au niveau de la réponse aux incidents, de de l'incidence spécifique. Oui c'est cool.

23:13
Oui, merci Abdellah. Je voulais rebondir un peu sur la question rapidement. Un peu de de mon collègue Émile en fait sur ce point. Des fois ce qui arrive dans la dans le monde réel, disons dans certaines compagnies, c'est juste que, mettons, que on prenne un exemple banal, il y a un serveur de production qui est comme infecté.

23:32
Et et disons que comme tu viens de le dire, il faut l'isoler de telle sorte que on appelle l'équipe de des des réponses aux incidents qui vient faire une capture pour pouvoir comme investiguer plus tard. Et puis après remettre pouf quoi. Mais ce qui arrive souvent, on fait auquel les enjeux auxquels on fait souvent fait on fait face. C'est souvent le la haute direction qui souvent met un tout petit peu la pression pour que. Mettons, si certains comme je viens de dire certains serveurs de production.

24:02
Faut que ça reparte parce que le temps que le l'équipe de réponse aux incidents arrive, investit, fasse l'image. Ben il y a un temps qui s'écoule fait que c'est C'est pourquoi je dis je je comprends comme tu viens de le dire. Des fois c'est il faut être défini par l'entreprise mais des fois c'est sur le papier c'est bien, mais dans dans le dans les faits réels, des fois c'est on est pris par entre 2 feux quoi fait que c'est ?

24:30
Oui ce que tu dis je je je comprends. Mais on peut prendre souvent des VM, on peut prendre des VM qui comportent tous les éléments qui se trouvent sur la machine en question et puis repartir l'autre machine, ça c'est une chose qu'on peut faire. Mais souvent on a des sites de de relève aussi qui sont là, on a des sites de relève qui sont là, on va le voir tantôt, on a des stratégies au niveau des sites de relève, on peut décider que vu que on a notre site un qui est attaqué, on a un on a un ransomware qui est là-bas tout ça.

24:59
Et qu'on peut pas. Ben on peut basculer sur le site 2 et le site un. On a le temps de faire le recouvrement, donc ça c'est des choses qu'on peut, c'est c'est des stratégies qu'on là on pourrait être défini au niveau de l'organisation en cas de de plan de de relève, mais dans le cas spécifique en tout cas il y a si c'est une petite organisation qui a pas tout, Ben c'est de faire la capture déjà de la VM de la machine comme ça ça constitue une preuve. Et puis Ben on peut repartir la.

25:28
La preuve pour qu'on puisse travailler, mais comme vous l'avez vu, vous l'avez vu, il y a eu beaucoup d'incidents au Québec. Ici, je vous parle de rappelle par exemple le cas de Promutuel, ça prend plusieurs jours avant qu'on relève tous les systèmes. C'est pas, c'est pas pour rien, c'est pas que les admins, ils peuvent pas écraser les systèmes et puis les lancer. Ils ont souvent des images qui sont là, mais si ça prend plusieurs jours, c'est tout ça en fait qui fait que souvent on n'a pas le choix, il faut attendre. C'est vrai que on perd de l'argent, mais souvent il y a.

25:58
Il y a des réalités qui font que on peut pas tout de suite remettre le système en marche pour pour

faire partie quoi ? Ok sur la surveillance Ben la surveillance Ben on récupère généralement les logs. Oui Nasser.

26:24
Oui, Bonsoir tout le monde juste pour continuer dans le le même sens que mon collègue Brest. Au niveau de des enquêtes aussi. Là ça dépend de l'ordonnance qui a été émis par le Tribunal. Par exemple, s'il y a des enquêtes criminelles à ce moment-là, même l'entreprise n'a pas le choix là que de suivre ce que l'ordonnance des tribunal a mentionné. Parce que c'est des cas par exemple.

26:46
Qui touche la pornographie juvénile où ça dépend ? Le le cas où l'attaque aussi là c'est que c'est des attaques à plus haut niveau, par exemple des APT que par exemple qui touchent le CE qu'on appelle le secret industriel ou des secteurs stratégiques aussi là malheureusement l'entreprise doit se soumettre à à cette ordonnance. De ce que j'ai compris peut être y aura certaines choses que je connais pas encore là mais y a certaines choses, on est obligé de suivre ces ces procédures là. Merci.

27:16
Merci de de de toutes les façons au niveau de l'organisation en tout cas celle qui ont un certain niveau de maturité, c'est des plans en fait on c'est c'est des plans qui sont définis déjà, donc on appelle ça des plans de réponse aux incidents qui sont définis. Qu'est ce qu'on fait si jamais on a un incident ? Ça il y a le plan, il est défini, la communication, tout ce qui rentre dans la chaîne est ce que le côté légal tout ça.

27:42
On a ça généralement écrit quelque part et puis en cas d'incident, on sait comment intervenir. C'est vrai, dans le fait de l'action, on est embrouillé. Puis comme ce que Brice disait, on veut répartir mais il y a la réalité qui est là, on peut pas répartir parce que il y a des préalables à faire, un peu comme tu le dis là il y a des préalables, on peut pas répartir comme ça, donc il faut se donner le temps. Et puis C'est pourquoi on prône plus d'avoir des sites de relève, on va en parler tantôt quand on veut avoir en tout cas une bonne sécurité.

28:10
On a un plan de continuité, on a des sites de relève. Au cas où le premier site n'est pas bon, Ben on peut basculer sur l'autre site le temps que on puisse faire toutes les activités nécessaires dans le site qui a été infecté. C'est bon pour les la journalisation et la surveillance. C'est simple, on a nos différents logs, on va donner les.

28:31
Pour les les éléments sur les logs, on a nos différentes logs qui sont générées par les systèmes, par les applications, par les proxys, par tout ce qui est routeurs, tout ça et on les regroupe quelque part. Donc ça peut être dans un syslog tout ça. Et puis les syslogs peut les forwarder dans dans un outil qu'on appelle généralement CM Security information manager qui lui va faire toute la corrélation. Donc je vais montrer les éléments qu'on est capable de de de voir les fonctionnalités du CM.

29:02
On fait l'échantillonnage des événements qu'on reçoit, donc on va recevoir tous les logs et en fonction des logs, les logs en fonction des use cases, ça va créer des événements et des événements. Ça peut être positif comme peut être juste un changement qui est normal ou négatif. Là ça rentre

dans le cadre d'un incident, là ça va entraîner en fonction des SEA, ça va entraîner un très short qui va alerter donc on va établir.

29:27
En fonction des use kees, à quel moment on déclenche un événement et à quel moment ça va déclencher des réponses. Donc au niveau de des équipes qui vont faire la surveillance, Ben on va définir le niveau de priorité et en fonction des niveaux de priorité Ben on va définir l'escalade à faire. Est ce que pour tel événement qui a des priorités cadre qui est pas très sévère, est ce que on a l'air du juste l'équipe support qui vont intervenir support niveau un et lorsqu'on on on monte en termes de priorité ? Ben.

29:56
Ça peut être la cellule de crise qui va rentrer en alerte pour prendre les décisions nécessaires. Au niveau de la journalisation surveillance, on regarde beaucoup tout ce qui est trafic sortant, donc le U Grace Monitoring. On regarde aussi le tout ce qui est U Grèce mais le U Grèce c'est plus pour voir. Est ce que on a des fuites de données ? On a des infiltrations au niveau du réseau donc au niveau de la surveillance sont vraiment des éléments qu'on regarde. On regarde aussi des fois tout ce qui est comportement anormal des utilisateurs.

30:24
Un utilisateur par exemple qui est qui a l'habitude de se connecter à Montréal, s'il se connecte un matin peut être au Vietnam et qu'il n'avait pas signalé. Ça doit être des des news qui peuvent soulever des des alertes. Donc ça c'est des ce sont des fonctionnalités classiques de de ICN. Donc je parlais de logs collections donc qui vont collecter les logs ? Ils vont analyser les logs vont faire la corrélation avec avec les Logs donc.

30:54
Il y a les logs applicatives, les logs systèmes, les logs réseaux, donc ils sont capables de faire les corrélations pour voir. Oui j'ai Emmanuel qui est connecté sur sa machine, il est allé sur tel réseau, il a il a, il a utilisé tel serveur. Ben tel serveur est censé communiquer avec l'autre, est ce que on n'est pas dans un cas d'attaque ? Donc le Siam est capable de faire ces corrélations là et puis ressortir de l'information, ressortir des alertes.

31:18
Ensuite on a le log forensic, donc tout ce qui est log qui peuvent être intéressantes pour l'investigation, on peut l'avoir. Tout ce qui est a été compliance en termes de conformité peut ressortir des rapports qui nous aident à la conformité, les tout ce qui est log applicatif. Puis il est capable de regarder tout ce qui est activité humaine, activité des utilisateurs, les actions des utilisateurs sur certaines applications.

31:45
Ensuite tout ce qui est object Access mon auditing donc on pourrait regarder les accès peut être à à la BD, les accès acheter un fichier. Ensuite ils font de l'alertage comme je l'ai je l'ai mentionné, on peut regarder les activités des utilisateurs, ils font du dashboarding, ils peuvent avoir des dashboard, des reporting. Des fois l'INTÉGRITY Monitoring voir l'intégrité avec des fichiers qu'on a.

32:10
Des systèmes donc. Donc il va regarder tout ce qui est log au niveau des systèmes puis des tout ce qui est object Access Auditing qui est répété 2 fois. Ça c'est des exemples des types de logs courants

qu'on retrouve. Donc on va retrouver sur vraiment les logs de sécurité donc des tout ce qui est accès au fichier Imprimante donc lui permet de détecter tout ce qui est violation et accès non autorisé.

32:35
Donc on a les systèmes log qui sont les les les événements système démarrage, arrêt arrêt puis des services. Donc on peut voir si peut être il y a un d'achapotage pour manipulation du système. On a tout ce qui est application log donc des événements définis par les développeurs donc tracer des actions dans une application. Donc on a tout ce qui est pare-feu firewall log.

32:57
Donc trafic bloqué ou autorisé. Donc on a tout ce qui est proxy, le log proxy des sites visités, durée de validation, tentatives interdites. On a tout ce qui est change log donc historique des demandes, des modifications et leur mise en œuvre. Donc on pourrait avoir d'autres logs mais ça c'est ceux qui sont couramment utilisés. Est ce que au niveau de la JOURNALISATION c'est bon ? C'est correct.

33:31
Je peux juste ajouter un petit un petit commentaire de plus par rapport au 7.2. Oui aujourd'hui je me suis mis à lire le document d'une liste 800- 92 si je me souviens bien par rapport au Log Management. Puis une affaire qui me puis ça c'est vraiment un commentaire bon pour tout le monde.

33:57
Dans la révision un de 2023 il est stipulé que Sim n'est pas fait de collecter des logs juste pour collecter des logs. On a quand même des on a quand même certains prérequis conformité ou au niveau de la menace mais dans la planification des logs. Puis pour ça que j'adore ta ta slide 31.

34:25
C'est parce que il y a des entreprises qui collectent des logs juste pour collecter des logs, puis qui font pas nécessairement de planification puis de d'avoir des use case puis ça c'est une puis c'est une question que qui était au dernier dascon aussi ?

34:49
C'est c'est quoi qu'on doit privilégier ? C'est c'est plus des cas des des cas de menaces, des des plus forts. Ben je comprends aussi qu'on a des qu'on a des conformités réglementaires à faire là. Mais c'est au niveau de la priorisation des logs, c'est qu'est ce qu'on fait ? Ouais OK.

35:11
Rapidement pour les le CM. Bon oui il y en a qui veut implanter le CM juste pour checker la conformité parce que dans leur ils sont dans des business où on exige d'avoir des CM donc ils vont avoir un CM mais qui est pas configuré. Donc comme tu l'as dit que ça soit un CM n'importe quel outil de sécurité si tu l'as que tu l'as pas configuré c'est comme si tu n'avais rien. Donc tu peux avoir les bons outils que ça soit les NDR, les Dr.

35:37
Les les le next Gen Firewall tout tout. Tu peux avoir tout ce que tu veux mais si t'as pas bien configuré tu n'as rien, tu tu es vraiment en en cas d'audit tu peux checker que tu l'as mais c'est pas bien configuré. Donc ça c'est de façon générale tous les outils de sécurité pour les use case on va voir le maître attaque tantôt, c'est vraiment mapper les les use case sur les techniques des attaquants.

36:02
Donc on va regarder dans notre secteur d'affaires les types de systèmes qu'on a, quels sont les types d'attaques auxquels on est exposés qui sont fréquents. Donc on pourrait-on pourrait ressortir cette technique là parce que le le maître attaque, on va revenir là-dessus. Je veux pas passer trop de temps mais on peut regarder les différentes techniques et puis on va cocher des techniques qui sont puritaires chez nous, qui sont.

36:26
Qui dans dans notre secteur d'activité ? Et puis salon les systèmes qu'on a. Et là très vite on va faire en sorte d'avoir ces use kes là. Donc ça ça, ça pourrait être des des choses qu'on peut travailler là-dessus pour améliorer régulièrement. C'est au jour au jour un, on n'aura pas tous les use que c'est clair là, mais le ciel est est censé évoluer.

36:44
Donc sur le temps donc après aussi des activités, des tests d'intrusion. Si si dans l'entreprise y a des Blue TEAM, des Red TEAM. Donc en fonction des écarts qui seront détectés sur des cas d'utilisation qui seront pas vus parce qu'il peut y avoir des attaques ou le CN ne verra rien, il va pas sortir des alertes. Donc ça veut dire que c'est des cas de chatons qui seront pas là. Donc on va venir mapper ces cas ces techniques là sur des cas d'utilisation du maître Attack. Et puis améliorer la performance du ciel c'est bon.

37:14
Merci OK on est maintenant dans la gestion de la configuration en fait le le le le CSSP c'est plus des des concepts de de comprendre comment la sécurité fonctionne. C'est c'est indépendant de la technologie donc on va pas dire ici comment telle technologie j'ai la gestion de la configuration, on va dire comment la gestion de la configuration doit se faire après.

37:43
Les outils vont gérer de leur façon, Microsoft va gérer sa façon mais ils vont toujours être proche de ce qui en ce qu'on est en train d'être de de que ici parce que eux aussi se basent sur ces ces éléments là pour des pour faire leurs outils. Parce que si c'est loin de ces outils là, de de ces recommandations là, ils vont être très loin de ce qui se fait dans le monde de l'entreprise. Donc ça c'est plus les grands concepts, comment est ce qu'on fait la chose ? Donc c'est mieux de comprendre. Une fois que vous comprenez, peu importe l'outil qu'on va vous présenter, vous saurez les éléments clés qu'on a besoin.

38:12
Donc tantôt on a parlé du CM, il y a plusieurs CM sur le marché, on a du sentinelle, on a du curada, on a du splink peu importe ce qu'on va vous dire comme CM c'est les mêmes fonctionnalités qu'ils que ces CM là auront, donc c'est les fonctionnalités clés que ces CM là auront. Après ça va dépendre de qu'est ce que l'équipe technique maîtrise et ou ou dépendamment de quel fournisseur est moins cher on va faire le choix. Mais en gros les fonctionnalités clés que j'ai montrées là il faut qu'on les retrouve dans ces CM là.

38:41
Donc et puis des fois les CM aussi, même les fabricants les font évoluer. Donc très souvent on n'a pas toutes les fonctionnalités au départ mais avec le roadmap du fabricant on arrive à voir tous les éléments, donc dans la la gestion de la configuration. Donc c'est simple, ce qu'on fait avec la gestion de la configuration c'est qu'on veut. On veut déployer nos systèmes dans un État cohérent et sécurisé.

39:09
Donc on on veut également que là cette sécurité là, que cet État là reste tout au long du cycle de vie. Donc en gros qu'est ce que ça veut dire ? J'ai mon téléphone, j'ai mon téléphone, j'ai fait des des paramétrages, j'ai j'ai mis le son à un certain niveau, la luminosité à un certain niveau, je veux que cette configuration là reste. Donc très souvent quand vous donnez le téléphone à votre enfant, Ben il change la config donc ça pour ne pas qu'il change. Vous faites une bonne gestion de configuration.

39:36
Mais la gestion de configuration que nous on fait généralement de façon standarde et on va reprendre avec l'enfant et puis on va remettre à la configuration qu'on avait en entreprise, on peut pas se permettre ça. Donc on fait tout pour que le système qu'on aura Ben qu'il y ait la configuration et que la configuration se retrouve dans tous nos systèmes. Donc c'est c'est vraiment ça le principe de la gestion de la configuration. Donc on veut s'arranger que la configuration initiale qu'on a le bizline qu'on va configurer va se retrouver sur l'ensemble de nos systèmes.

40:01
Donc ça va nous permettre en termes de cas d'utilisation, de faire des déploiements rapides et cohérents sur les postes de travail. Donc en cas de compromission, Ben c'est de revenir à l'État. L'état initial remise à l'état d'un système compromis. Donc puisque on a la configuration, on connaît tous les éléments de configuration qu'on a, les images qu'on a généralement, donc on est capable de les faire revenir à la configuration standard qu'on avait.

40:28
Donc pour faire la gestion de la configuration, Ben on crée une configuration des références qu'on on appelle le design. Donc on on a une image de Windows, Windows 11 qu'on veut mettre sur les machines de l'organisation. Mais on va prendre la machine, on va on, on va prendre un système Windows, on va lui donner les services utiles, on va enlever les services qu'on utilise pas, on va mettre les applications qu'on veut là-dessus, les IDR, tout ce qu'on veut, tout ce qu'on ne veut pas, on met toutes les configurations qu'on veut.

40:55
On va les définir et ça devient notre design de référence et cette design de référence qu'on va utiliser sur l'ensemble de nos systèmes dans notre environnement. Donc on va utiliser l'image pour déployer la configuration. Donc on installateur dans ce cas ici à droite, ce qu'on fait c'est que on on va définir un design en un. Ensuite on va créer une image de référence sur le serveur et l'image sera réutilisée sur l'ensemble des systèmes qui sont déployés dans l'image qui est là.

41:21
Ensuite, on fait tout pour maintenir et suivre la configuration des références. Donc des fois on peut faire une configuration d'un système, mais après la configuration d'un d'un système, le système peut changer de configuration. Donc il faut que on ait un outil qui est capable de nous dire Ben cette configuration là c'est. Il y a eu un écart par rapport à la configuration de base qui avait été définie. Donc très souvent ça peut nous permettre de détecter des incidents au niveau d'un, d'un, d'un, d'un système.

41:49
Que on a la configuration de base admettons, on on a fermé certains ports sur la machine et on se rend compte que il y a des ports qui sont ouverts. Ces ports là c'était pas censé être ouvert, donc tout

de suite ça peut déclencher des des incidents. Et ça c'est quand vraiment on fait le monitoring de de de la configuration de base qu'on est capable de savoir que on a cet écart là. Donc le processus de gestion de la configuration.

42:17
Donc dans la la première chose on fait l'identification de la configuration, donc on appelle configuration identification. Donc les administrateurs de les administrateurs ils vont documenter la configuration actuelle des systèmes et des logiciels dans toute l'organisation. Donc comme j'ai parlé le cas de de Windows Phone, ça c'est ça, ça sera les les postes de travail, mais on aura aussi la configuration des serveurs Windows, on pourrait avoir les la configuration des Linux, donc il faut avoir toutes ces configurations là documentées.

42:44
Comme ça on sait que pour tel système, voici telle configuration qu'on mettra là-dessus. Ensuite il y a le contrôle de la configuration qu'on appelle configuration contrôle. Donc toutes les modifications, que ça soit les mises à jour, les âges ou les retraits, ça doit respecter la politique de gestion du changement et la gestion de configuration. Donc on va définir une gestion de changement qu'on va parler, dont on va parler après dans le document si on veut faire des modifications. Donc on a admettons, on, on a notre baseline qui est là.

43:14
Et dans notre baseline, on fermait, on acceptait le port 81 jour, on se rend compte que Ben c'est dangereux d'ouvrir le port 80. On va fermer le port 80 mais on se lève pas pour appliquer, il faut quand même que ça suive la procédure ou les politiques qui sont définies pour la gestion de changement ou la gestion de configuration au niveau de l'organisation. Ensuite, on a le suivi de l'état de la configuration donc qui s'appelle qu'on appelle configuration status et canting.

43:44
Ce sont des des procédures formelles sont mises en place pour enregistrer toutes les modifications autorisées. Donc si on a fait des modifications, Ben on veut le te retrouver quelque part. Il faut que ça soit documenté. Ensuite on a le l'audit de la configuration qu'elle est, qu'elle configurer configuration, purification, un audit dans les documents, vous allez voir configuration et audit simplement, donc on va faire des audits périodiques.

44:07
Pour vérifier la conformité et détecter les écarts. Donc on veut s'assurer que la réalité des systèmes en production correspondent bien à ce qui est documenté et que il y a pas des modifications là-dessus. Donc c'est l'exemple que je donnais. Si on a un système et que il y a un écart là-dessus par rapport à la configuration de base, Ben ça doit soulever des des interrogations pour nous amener à voir qu'est ce qui est fait là-dessus.

44:30
Donc ça c'est une image pour vraiment montrer ce que je parle, ce dont tu parlais tantôt. Donc on va commencer par tout ce qui est planning, management et planning. Donc on a tout ce qui est programme, support, formation. Et on commence maintenant par la configuration, l'identification de la configuration. Ensuite on a la configuration Control, on a configuration status and cutting, et ensuite on a la configuration verification and audit.

44:55

Donc ça c'est un exemple. Une image qui explique bien les relations entre les différentes étapes de processus de gestion de la configuration, fondement des opérations de de sécurité. Donc dans la plupart des documents de sécurité, vous allez voir ces thèmes là.

45:17
Donc besoin de savoir qui est limite ou non. Donc ça veut dire que l'accès à l'information n'est autorisé que si l'utilisateur en a besoin pour accomplir une tâche spécifique. Donc on ne donne pas les accès parce que c'est mon ami à quelqu'un qui n'en a pas besoin. Donc ton ami peut être dans l'entreprise, c'est toi qui donne les accès, mais tu lui donnes pas plus d'accès dont il a besoin, tu lui donnes juste ce dont il a besoin. Ça peut être ton patron, ton manager, ou bien ça peut être le CIO.

45:42
Si il n'a pas besoin des accès, il n'est pas administrateur, il n'a pas besoin d'avoir des des accès admin sur les serveurs, il n'en a, il n'en a rien à faire, il c'est rien ce qu'on fait sur les serveurs même s'il est informaticien, mais c'est pas lui qui opère donc on lui donne pas les accès d'admin sur les serveurs. Ensuite on a le moindre privilège donc on va souvent le le moindre privilège associé au besoin de savoir mais c'est différent.

46:05
Donc le moindre privilège. Donc on va donner juste à l'utilisateur, ou bien souvent au processus, uniquement les permissions nécessaires pour exécuter ces fonctions sans privilège excessif. Donc ce dont tu as, ce dont tu as réellement besoin, on va te donner. Donc ça peut rejoindre un peu le besoin de savoir, mais il y a des nuances entre les 2 principes. Ensuite on a la séparation des tâches ou des responsabilités qui est séparation de disent. Donc le principe ça, ça dit que une même personne ne doit pas exercer des fonctions critiques incompatibles.

46:35
Comme par exemple initier ou approuver une transaction. Donc si au niveau de l'entreprise je suis la personne qui est capable d'émettre la une facture et la personne qui paye, Ben je peux faire faire une fraude facilement. Donc c'est ça. Donc on fait en sorte que une même personne n'ait pas lui même le pouvoir de d'initier ou des des fonctions critiques qui lui permettent de faire des transactions à la à la société générale en en France.

47:04
Donc ça c'est un principe de sécurité qu'il faut mettre en place, surtout dans dans souvent des projets, des projets de déploiement de solutions, soit des des solutions de finances. Il faut vraiment au niveau de la ligne d'affaire qu'ils définissent toutes les règles de séparation des tâches et ça doit être quelque chose sur lesquelles on est pointé là-dessus en matière de sécurité. Ensuite, on a la gestion des comptes privilégiés qu'on appelle généralement le PAM, qui est la mise en œuvre de politiques strictes pour contrôler l'usage des comptes à eau privilégiés.

47:33
Donc les comptes d'admin routes, la journalisation, la surveillance, la rotation des accès. Donc on a, c'est vraiment des des outils qui nous permettent de faire le le pas. Ensuite, on a la rotation des postes OK drop rotation qui est une partie qui consiste à déplacer périodiquement des employés d'un poste à un autre pour limiter les risques de fraude, pour garantir les continuités opérationnelles. Il y a des employés qui font jamais en vacances, qui sont tout le temps-là.

48:01

Qui sont dans certains postes où ils sont capables de de toujours faire les la fraude ou ce qu'ils ce qu'ils font de malicieux. Mais si on fait souvent la rotation, Ben il y a des gens qui sont capables d'aller voir qu'est ce qui se fait de l'autre côté ? Et puis capable, on sera capable de de détecter certaines actions malicieuses. Ensuite on a un autre un autre conseil qui est l'accord de niveau de service qui est le SLD.

48:26
Donc c'est un contrat formel entre un fournisseur de services et un client définissant des niveaux attendus de service, donc en terme de disponibilité et de temps de réponse avec des mesures précises. Donc généralement avec le cm le le MDR Detection respons finalement comme on l'appelle, il y a des entreprises qui n'ont pas les équipes des sécurités nécessaires pour avoir une équipe socle dédiée. Donc souvent ils font affaire avec des soccer, des services.

48:54
Avec avec ces types de contrats Là Ben on va avec ces ces types de fournisseurs, Ben on va définir des SLI pour dire nous on veut que vous soyez disponible 24 7 en termes de délai de réponse, que la réponse soit rapide, que vous soyez en que que dès dès que y a des alertes là que vous soyez relatif réactif là-dessus en delà de en en termes de minutes. Donc ce serait des des éléments qu'on pourrait définir dans le contrat.

49:28
Ensuite, l'un des fondements, c'est l'un des éléments qu'on va expliquer, c'est le le malt Attack. Je vais parler rapidement du du malt Attack avec la question de de Émile. Le malt Attack, c'est c'est une base de de connaissances, donc qui est accessible à tout le monde. Donc lui, il va définir les tactiques, les techniques, les procédures qui sont utilisées par les par les attaquants donc.

49:55
On on va décrire tout ce que les attaquants font pour attaquer, pour attaquer une entreprise. Donc comme c'est décrit ainsi, Ben ça sera plus facile pour nous de savoir, de connaître leurs techniques et ensuite pouvoir se défendre. Donc si on sait comment ils nous attaquent, Ben on saura comment décrire, comment aller se protéger si on connaît une attaque et on peut tout de suite avoir les défenses pour se protéger.

50:21
Donc elle va se baser sur l'observation réelle des Minas, donc s'est mis à jour régulièrement. Donc va se concentrer sur les acteurs des Minas, leur comportement et puis les outils qu'ils utilisent. Donc c'est animé par une Communauté. Et puis elle sera décrit des des outils des principaux attaques à présenter, les malware, les outils qui sont utilisés. Il est utilisé sous forme matricielle pour faciliter la lecture, donc il a les éléments clés comme les le TTTP.

50:48
Donc la tactique ce sont des objectifs stratégiques des attaquants. Donc vous allez voir la reconnaissance, persistance, escalade des privilèges, escalation des données. Ensuite les techniques ce sont des méthodes spécifiques qui vont être utilisées, donc ça va permettre de détecter. Puis atelier, atelier détecter et atelier par l'équipe bleue, donc l'équipe qui va qui est censée faire la défense de l'organisation et puis réaliser pour l'équipe rouge. Donc le l'équipe rouge va utiliser cette technique là pour attaquer. Donc c'est vraiment ces techniques que les attaquants utilisent donc.

51:17

Si on fait un rateam, donc l'équipe rouge va utiliser cette technique là pour attaquer ensuite la procédure. Ce sont des actions concrètes réalisées par les attaquants pour mettre en œuvre les techniques, donc ça c'est un exemple. Donc on a la, on a les tactiques qui sont là, on a les différentes techniques qui sont là et puis à l'intérieur on va avoir des sous techniques et puis des procédures. Donc ça c'est un exemple de la matrice. Est ce que vous avez tous le lien du maître attaque si quelqu'un là vous pouvez le mettre dans la dans le chat pour le bénéfice de tout le monde.

51:48
Ensuite ça c'est des exemples de techniques. Et puis la description de ces techniques là, des tactiques. Donc un exemple de tactique unish all Access. Donc on peut passer par le phishing sous technique super phishing. Donc en terme de qu'est ce qu'on fait ? Ben on va utiliser des courriels.

52:08
Qui qui ? Qui contient un miel malicieux. Donc on peut utiliser aussi des courriels, qui va, qui sera dans un contexte de piratage écologique, jouer sur la majorité de la personne ou on va avoir un lien qui contient un code malicieux. Donc ça c'est un exemple de tactiques techniques et puis de procédures qui sont utilisées par les attaquants. Merci beaucoup zefri.

52:35
On n'a pas le temps sinon j'allais parcourir tous les aspects du maitre Attack et pour vous montrer peut être le hightag explorer mais on n'a pas le temps. On a beaucoup de slides à parcourir mais vous pouvez vous amuser avec le lien que j'ai fini envoyé. Il y a beaucoup de ressources, il y a beaucoup d'éléments pour votre culture en cybersécurité, c'est c'est très important. Quand je disais tantôt à Émile Émile, on on regarde beaucoup ces techniques là pour améliorer les use case au niveau du.

53:04
Au niveau du CN, donc ça c'est un cas de phishing. Mais même dans le cas du phishing, y aura des techniques et puis des des mitigations. Surtout qu'on aura aussi pour améliorer nos détections au niveau de de tout ce qui est phishing. Donc on va peut être travailler sur tout ce qui est filtrage de courriels, sur tout ce qui est outils au niveau de emailing pour améliorer notre détection puis améliorer tout ce qui est.

53:32
Système d'attaque, système de protection de coréen. Donc ça c'est le cas de de la zonage. On a d'autres techniques comme peut être les insustrations de données, le, le mouvement latéral, tout ce qui est reconnaissance et ces reconnaissances là.

53:48
On on on peut connaître les techniques et les techniques là vont correspondre. Les techniques de mitra attaque peuvent nous permettre au niveau de des use case, mettre en place des use case au niveau des CM pour savoir si on est en train de de nous scanner, si quelqu'un essaie de nous envoyer de l'amsonage ou si on est en train de faire un mouvement latéral. Bref, toutes les techniques du Mile Trattack, on peut les transformer en use case dans un outil de de CM et puis pouvoir déclencher des alertes.

54:18
C'est bon donc ça c'est un exemple dont on parlait tantôt. Ensuite on a un autre outil qu'on appelle la la chaîne de de de Killechen donc lui il va replanter les différentes étapes nécessaires pour la

recherche du d'une menace. Donc c'est c'est le synonyme, c'est chaîne cybercriminel donc vous allez voir dans certains documents, kille Chen, CV, quille chain, cyber Atta chain.

54:45
Donc l'idée est de connaître comment est ce qu'on nous attaque pour pouvoir se défendre. Donc si on sait comment on nous attaque, on peut mieux se défendre. Donc ça c'est le cyberculture, ça a été développé par Locken marchand. Merci beaucoup Emine Locken marchand qui lui a développé les différentes étapes. Donc on a, on commence par la reconnaissance, donc autant dans le milt attaque, on a la différentes étapes, on a les différentes étapes, les différentes tactiques. Ici on a les grandes étapes qu'on a.

55:15
Pour mener une attaque, donc on a la reconnaissance, donc on va chercher les e-mails on il y a la reconisation, c'est qu'on va préparer tout ce qui est exploit avec un pack d'or qu'on va mettre dans un on va livrer à travers un pays l'autre. On peut envoyer un courriel ou le déposer dans une clé USB, on peut faire l'exploitation, on peut faire l'installation sur un malware, on peut faire en sorte qu'ils communiquent avec un système de commande contrôle. Et puis dès qu'on atteint notre objectif, Ben on peut fermer tout ce qui est.

55:44
Tout ce qui est case pour nous retrouver c'est bon. Merci beaucoup Émile pour le Difend le Difend donc on a le Mike attaque et puis on a le difend attaque qui lui parle de tous les éléments défensifs qu'on peut utiliser pour se protéger. Donc il lui il est complémentaire au au Mike attaque le 7.5.

56:13
Appliquer la protection des ressources. Donc on va au au niveau de le le principe au niveau des des ressources qu'on a. Ben tous les systèmes que tous les outils qu'on a, on doit les sécuriser. Que ça soit les systèmes, les données, les supports physiques ou numériques, que ça soit les distures, les clés USB et autres. Si on les utilise bien sûr, on doit les sécuriser tout au long de leur site de vie.

56:44
Donc du déploiement jusqu'à la destruction. Donc tant que on a un actif dans notre environnement, Ben on se doit de le sécuriser. C'est vrai que dépendamment du niveau de criticité, il y a des mesures de sécurité appropriées qu'on va mettre, mais on doit les sécuriser tous. Donc des techniques de protection, on va déjà faire le marquage, donc on va faire le souvent le labeling selon le niveau de sensibilité. Donc que ça soit confidentiel, public ou secret.

57:13
On va faire le stockage de la civage de façon sécurisée, donc on va faire le chiffrement en tout ce qui est transport, tout ce qui est en transit. Ben on on va faire la communication. Si on tant qu'on a des communications, on va faire en sorte que ça soit des communications qui sont chiffrées. Et après si on n'utilise plus le média, que ça soit les dictures, les types qu'on utilise, les Blu Ray et autres les bandes magnétiques, Ben si on les utilise plus, Ben il faut les détruire de de la façon la plus sécuritaire.

57:43
Et dépendamment des médias, je pense que vous avez une section sur les médias. La destruction des médias, Ben on le détruira en fonction du type de média en question pour ne pas avoir les informations confidentielles sur le média. On est maintenant à la gestion des incidents.

58:07
Donc la gestion des incidents, les incidents, c'est quoi ? C'est que on a souvent une tentative d'intelligence sur le réseau. Donc il y a quelqu'un qui cherche à ancrer sur notre réseau. On a souvent des tentatives de déni des services, donc DDOS. On a souvent des logiciels malicieux qui sont là dans notre qui vont être dans notre réseau. On a souvent des accès non autorisés aux données, donc on a un système ou une base de données où on a, on a des renseignements personnels quelque part dans l'entreprise.

58:36
Et on a fait des accès. Mais on voit que il y a des personnes qui n'ont pas l'accès et qui ont accédé à l'information et ou bien on peut avoir une violation aux politiques de sécurité de l'organisation. Donc ça c'est c'est un incident. Donc si on respecte pas les politiques de l'organisation, c'est un incident de sécurité. Donc admettons que on définit, on dit dans l'entreprise que on fait des campagnes de sensibilisation.

59:01
Et que vous êtes sensé faire un cours, une formation par an si vous ne faites pas la formation. Mais si, si, c'est un cas de force majeure, oui, mais si vous décidez de ne faire pas faire la formation, c'est comme si vous c'est c'est vu, un peu comme si vous n'avez pas respecté la politique de l'organisation. Donc ça c'est un cas. 2e cas, on dit que on n'utilise pas des ordinateurs professionnels à des cas à des cas d'usage personnel, mais si vous le faites, c'est un manquement.

59:30
On dit aussi dans l'organisation, mais on n'ouvre pas des stockages infonuagiques en ligne comme Dropbox et autres. Si vous l'ouvrez, c'est un cas de violation aux politiques. Souvent, si c'est possible techniquement, l'organisation va le bloquer. Mais s'il ne le bloque pas, que vous le faites, Ben c'est une violation à la sécurité. Un cas qui est beaucoup visible dans les organisations. On a tout ce qui est intelligence artificielle et générative.

59:55
On dit que on n'autorise pas lier à génération en entreprise. Donc si y a une directive ou un encadrement qui sort dans ce contexte, si vous le respectez pas, c'est vu comme un incident. C'est bon. C'est vrai que y a pas de piratage tout ça, mais si vous ne recevez pas une politique, c'est comme si c'est c'est un incident et on doit le traiter avec le la, le processus de gestion des incidents.

1:00:21
C'est c'est vrai que lui il n'est pas, il n'est pas critique. Comme si on nous avait on avait une attaque des DDOS ou une intelligence réseau, mais ça reste que c'est un incident qu'on doit traiter les différentes étapes, la gestion des incidents. Ben on a la détection RESPONSE mitigation, Reporting, recovery re médiation et puis les ondeleurs et puis après on reprend si jamais on a un nouveau incident.

1:00:46
Donc pour la détection, Ben on a les différentes techniques de détection, donc on a tout ce qui est IDS, oui Émile, qui sont même des tables de préparation est où ? Parce que faut que tu prépares quand même tes playbacks puis tout ça non ça c'est ça doit être dans le plan de réponse aux incidents, mais ici c'est plus quand l'incident survient, qu'est ce qu'on fait ? Ah OK, merci de votre précision.

1:01:14
Merci OK donc on a la les techniques de détection, on a les IDS antivirus, on a aujourd'hui des IDR, des NDR, plein d'autres éléments, on a la corrélation et audit de journaux, on a les rapports d'incidents par utilisateur, donc on va valider. Est ce que la menace est réelle ? Donc est ce que effectivement on est devant un cas qui a été un cas avéré ? Est ce que c'est pas un faux positif ?

1:01:43
Donc oui, si c'est un cas d'incident, si c'est un cas de si c'est un incident, Ben on va commencer à réagir. Si c'est un incident majeur, Ben on va faire intervenir l'équipe de réponse aux incidents. Et si c'est un incident mineur, Ben on va suivre le les, le processus qui est établi. Et puis on va essayer de d'aller très rapidement pour essayer de faire les autres actions mitigations puis répondre aux incidents.

1:02:09
En cas d'incident majeur, un peu les questions qu'on avait posées, est ce qu'on arrête le système ou pas ? Ben on va définir selon les playbooks qu'on a, est ce qu'est ce qu'on fait si on a un incident de ce type et on va suivre ce qu'on a défini dans notre playbook en cas de d'incident selon la définition.

1:02:34
Ensuite à la mitigation. Donc c'est l'État qu'on tente de continuer où endiguer la menace. Donc l'ordinateur est affecté, on peut faire la déconnexion réseau, on peut essayer de faire l'isolement pour ne pas propager à la question est ce qu'on éteint l'ordinateur ? Mais ça va dépendre de qu'est ce qu'on on a défini dans le plus gros ? Qu'est ce que la réponse aux incidents à donner si ?

1:02:57
On n'a pas trop le choix qu'on fait avant de fermer. Ben si on peut prendre une image à chaud, sinon on a la possibilité de prendre une image à chaud avec des systèmes comme via le mail ou autre. Mais on va le faire pour au moins garder l'État à chaud du système. Ensuite pour le reporting, est ce qu'on le on veut communiquer en interne ? Très souvent quand il y a des incidents, c'est pas tout le monde qui est au courant. C'est vraiment une cellule spécifique qui est informée.

1:03:27
Après, l'externe est ce qu'on parle avec l'externe. Généralement dans les organisations, on définit la personne qui doit communiquer en cas d'incident. C'est pas parce que toi tu es le responsable en sécurité que dès qu'il y a un incident tu vas tu vas sortir dans les journaux pour expliquer t'as pas t'es si t'es pas désigné pour ça dans l'Organisation, Ben tu parles à personne. Et c'est pareil pour tout le monde, toutes les personnes qui sont en sécurité et qui sont dans la cellule de crise. Personne n'a le droit de parler, de dire qu'est ce qui s'est passé ?

1:03:55
On laisse la relation publique le gérer. Ça reste des informations confidentielles dans l'organisation. Quand on parle aux partenaires, il y a des personnes désignées pour parler aux partenaires. De toutes les façons, c'est des éléments qui sont définis très souvent dans le plan de dans le plan de réponse aux incidents. Les partenaires d'affaires, c'est pas nous qui communiquons avec eux. Il y a des personnes qui sont habilités pour communiquer les autorités pour les poursuites criminelles, on va laisser le légal gérer ça. Donc en gros, en cas d'incident.

1:04:23

On n'est pas censés bavarder, on n'est pas bavard, on laisse les personnes désignées qui peuvent parler, c'est eux qui vont expliquer. Nous, même si on sait tout, on est tenu par le secret, on signe un dire pour ne pas divulguer les informations confidentielles, mais on n'a rien à divulguer. Ça reste dans votre tête, c'est pas même à à la maison, on n'en parle pas, c'est dire jusqu'à quel niveau on en sécurité, on garde l'information et puis.

1:04:51
Si c'est ça, c'est la personne qui est censée communiquer, qui communique l'information, qui que la personne doit communiquer, c'est tout pour le recovery. Ben quand on finit on fait le reporting, Ben on va. On va aller continuer l'enquête, puis on va revenir à l'État fonctionnel, de confiance. Donc là où le système était, on va y mettre les bonnes images, on va faire appel à notre.

1:05:18
Gestion de la configuration pour mettre la bonne image sur les applications, sur le le système en question, la remédiation. Ben on va tenter de colmater l'adresse de façon adéquate. Donc on va analyser les causes fondamentales, que ce soit en informatique ou dans tout hein. Pour régler un problème de façon définitive, il faut regarder la cause profonde. Quand tu regardes la cause profonde, Ben si, dès que tu trouves la cause profonde.

1:05:44
Il y a plusieurs techniques pour trouver la cause profonde. Souvent on parle de de d'avoir les 5, pourquoi d'ici les les cinquièmes, pourquoi on va quand même retrouver la vraie cause ? Donc quand on applique ça, Ben on va régler notre problème de façon définitive. Donc pour le l'autre cause, Ben on va appliquer les correctifs, la configuration des bases. Si on avait des comptes administrateurs qui n'étaient pas protégés, Ben on va essayer de les protéger ensuite pour le le choix de l'heure, Ben.

1:06:12
Très souvent, on oublie quand on a un incident qu'on a colmaté, on a corrigé tout. On oublie alors que c'est c'est l'étape qui est vraiment importante, où on doit s'asseoir et puis dire qu'est ce qui s'est passé, qu'est ce que par où ça a débuté, qu'est ce qu'on on doit arrêter et puis qu'est ce qu'on doit continuer de faire, qu'est ce que globalement, qu'est ce qu'on fait pour s'améliorer ? Donc ça, si je fais une référence à.

1:06:41
À la roue de Deming. Donc ça ça sera vraiment dans le dans l'amélioration. Donc on va vraiment se poser les vraies questions, puis qu'est ce qu'on on change dans notre façon de fonctionner ? Qu'est ce qu'on doit continuer à faire pour que ce type d'incident là n'arrive pas ? Ou si ça arrive que très tôt on arrive à le à l'arrêter avant que ça nous cause du tort. Mesures de détection et de prévention.

1:07:14
Et pour les mesures de de prévention ? Ben rapidement pour les pages on va appliquer systématiquement les pages sur nos systèmes quand on a le Microsoft. Donc par exemple on va faire des pages tool Day dès que le système sort l'application Store. Donc c'est une mal façon pour nous de c'est une prévention pour l'organisation. Autre chose, ne pas laisser des services systèmes ou des protocoles inutiles actifs. Donc ça c'est le c'est le la le cours 101 du harding.

1:07:41
Les systèmes ensuite, faut installer tout ce qui est IDSIPS sur les réseaux, donc devant les infrastructures critiques, au minimum, si on n'a pas les moyens de couvrir tout, on a aujourd'hui des

solutions qu'on appelle des NDR, qui qui sont l'équivalent des IDR, mais pour les réseaux, et ensuite faut avoir des logiciels déployés partout et mis à jour, donc IDRIDR qu'on peut avoir sur low and point.

1:08:08
Ensuite faut mettre en place, avoir des de l'isolation réseau, donc avoir des coupes, que avoir des proxy protégés, avoir la gestion des configurations dont on a parlé, maîtriser tout ce qu'on va mettre sur nos systèmes, avoir une un processus de configuration pour ne pas que le système change à chaque fois de de paramètres. Donc dès qu'on aura défini notre configuration Ben on va le suivre. Ensuite faut mettre en place des listes des listes noires donc wrestling wrestling et blacklisting.

1:08:37
La liste blanche c'est on autorise uniquement ce qui est explicitement permis, donc les programmes autorisés. Donc dans l'organisation on peut dire Ben nous on accepte que le logiciel qu'on a autorisé l'idée avec les listes blanches, Ben tout ce qu'il tout ce qu'on n'a pas accepté, Ben on on le, on le rejette avec la liste noire, on bloque tout ce qui est interdit. Donc ça veut dire que tu dois connaître en amont tout ce qui est interdit. Donc ça veut dire que ce que tu ne connais pas, c'est quoi ne sera pas sur ta liste noire sera permis.

1:09:05
Donc très souvent, dépendamment de ce qu'on fait il y a, il y aura des projets ou des activités où on va privilégier la liste noire à la liste blanche et vice versa. Donc ça va dépendre. Si on est capable de faire un inventaire global de des programmes qu'on utilise dans l'Organisation, Ben on va pour la liste blanche. Mais si on n'est pas capable de savoir qu'est ce qu'on va utiliser globalement et qu'on veut pas arrêter l'utilisation par les par, on veut pas bloquer la production de nos utilisateurs.

1:09:34
Mais on va aller avec la liste noire fonctionner. Un exemple tant encore avec les Gena I mais on peut dire au niveau de l'Organisation, Ben on maîtrise pas CHA GPT donc on va bloquer cha GPT, on va bloquer tous les EI connus, mais les EI qu'on ne connaît pas, Ben on va pas les bloquer donc on sera dans une liste noire. Mais par contre on peut dire qu'on va faire une liste blanche donc on va autoriser tout ce qui est gena I qu'on connaît maintenant on dira tous tous les autres que nous on ne connaît pas, tu les bloques tout.

1:10:03
Donc ça va dépendre de ce qu'on veut dans l'organisation. Donc peu importe, dépendamment de de notre choix, on va aller vers des listes blanches ou des listes noires. Ensuite, on peut pour toujours se pour se pour se protéger au niveau de l'Organisation, Ben on peut aller vers des services de sécurité des tiers. Donc tantôt, j'ai parlé des des soccer, des services qu'on on organise. On utilise beaucoup au niveau des entreprises, des des services, des provider, des MSS PI.

1:10:34
Pour la gestion souvent des des, des, des pare feux, souvent on n'a pas l'expertise interne donc on peut faire affaire avec des compagnies qui vont gérer tous nos outils de sécurité ou souvent la réponse aux incidents. On peut avoir des compagnies qui vont nous aider à faire la subveillance de 4 7 si on n'a pas l'expertise, des fois il y a des expertises spécialisées qu'on n'a pas donc on peut aller les chercher. Donc ça permet aussi de réduire des coûts internes parce que mettre en place un CM.

1:11:02

Dans une organisation de petite taille, avec toute l'équipe que ça demande, ça devient coûteux pour une entreprise. Donc des fois ils vont externaliser ces services. Là ensuite on peut faire de l'isolation par par Carsat, le Centre boxing, donc on va admettons. Si on a un programme, on veut tester, on a un logiciel malveillant, on veut s'assurer qu'il est bon et on va le mettre dans un centre boxing, le tester, s'assurer qu'il est bon avant de l'autoriser. Mais des fois, on nous demande d'autoriser certains outils dans l'organisation.

1:11:32
Mais on ne sait pas qu'est ce que l'outil fait, comment est ce qu'il fonctionne ? Ben on peut le tester dans notre outil de sandboxing pour nous assurer que il est exempt de vulnérabilité ou exempt de d'éléments malicieux. Ensuite, on a tout ce qui est intelligence artificielle aujourd'hui qui vient améliorer la sécurité. Donc tout ce qui est outil d'intelligence artificielle, c'est souvent intégré dans les cm. C'est ce qui fait que souvent les nos cm sont beaucoup intelligents.

1:12:01
On a souvent des IDR qui ont aussi l'intelligence artificielle, des moteurs d'intelligence artificielle. On a des services, souvent des trucs intelligents, qui travaillent aussi avec les outils. DI ensuite, faut pouvoir bien sûr avec les des outils qu'on aura à notre disposition des IDR et autres, pouvoir détecter les activités anormales sur un réseau, donc identifier des différentes tentatives, des types de réponses, que ça soit actif ou passives.

1:12:33
Avec les outils de NDR, très souvent, et lui, il va essayer de faire une corrélation des trafics, regarder ce qui se fait dans le réseau et puis soulever souvent des alertes ou des éléments de comportements anormaux. Admettons que vous êtes dans votre réseau, vous n'avez jamais communiqué avec une adresse IP et du coup on voit que y a un gros volume de données qui est en train d'être transféré vers cette adresse IP. Là Ben le NDR pourrait bloquer.

1:13:02
Je cette ce transfert là dès qu'il il il détecte que y a un transfert qui est qui est en train d'être fait. Donc il peut arrêter tout de suite le transfert parce que il voit que y a une transaction qui s'est fait sur une adresse qui est pas qui est inhabituelle ou bien il voit un mouvement latéral sur des serveurs, il voit que y a une trafic et il peut le bloquer s'il est bien configuré. Bien sûr on part sur la base que c'est bien configuré.

1:13:30
Ensuite on a des outils de détection qu'on peut utiliser, donc qu'on va appeler onypot, des pots de miel qui nous servent de défense active qui consiste à tirer sur des ressources, des serveurs, des programmes service, des attaquants afin de les identifier. Donc souvent si c'est mal configuré, Ben on peut utiliser ça aussi pour rentrer dans votre réseau aussi. Donc si vous ne maîtrisez, si l'organisation ne maîtrise pas, c'est pas la peine de mettre des des onypots.

1:13:57
Pour ne pas s'exposer, pour ne pas s'exposer. Parce que si tu mets des onypot, que tu es accessible de l'extérieur et que t'as pas bien fait la configuration. Mais à travers le onypot on peut rentrer dans ton réseau. Ensuite on a aussi des ony net qui sont des réseaux, des réseaux leurs qui a le même principe que des onypot et ensemble de plusieurs pots de miel sur un même réseau. Donc on peut avoir des onypot des différents onypot qu'on va mettre sur les réseaux pour attirer et puis savoir quels sont les types d'attaquants qu'on aura ou bien quelles sont les techniques qui sont utilisées pour se protéger.

1:14:27
Je répète, si vous n'avez pas la maturité nécessaire pour mettre des ony pot, ne les mettez pas, n'allez pas provoquer les gens, c'est bon. OK Ezaïa a mis les sorts oui le dans le CM oui on pourrait avoir aussi les les on peut. Oui, on pourrait intégrer aussi les les sorts dans les outils pour la prévention, pour la la réponse aux incidents, oui.

1:14:56
Au doux oui. Si au fait, je ne vois même pas l'importance de mettre en place le Reni post parce que tu mets ça en place, c'est pour encore attirer l'attention au fait des des attaquants. Donc je ne vois même pas l'importance. Au fait, il dit que si on ne m'inquiète pas. Bon, je ne vois pas au fait dans quel minuscule. Au fait, il est important de mettre en place un reni post.

1:15:24
Bon, ça oui oui, ça, ça dépend vraiment de la la maturité de l'organisation. Si vous avez mis en place des systèmes de détection robuste et que vous vous dites OK, nous on a mis tout en place. Mais en même temps, si jamais quelqu'un arrive à à traverser certaines de notre système de défense périmétrique qui vient dans notre réseau, Ben on veut faire en sorte que, en termes de reconnaissance, qu'il aille vers un système.

1:15:50
Qui est qui est vers notre onipot donc généralement l'attaquant il va aller vers la chose la plus facile. Donc quand il va trouver les onipot Ben il va aller dans les onipot et dans les Onipot il va se dire oui j'ai eu le serveur mais là ça permet à au système de de détection de savoir tout de suite que il y a eu un cas qui est arrivé. C'est vrai que le c'est un système qui qui avait pas d'importance en réalité parce que c'est c'est onipot.

1:16:17
Et là vous allez améliorer les outils de défense par rapport à ça. Donc oui les je connais des entreprises qui ont des on epot qui ont et ils ont leur ils ont cette ils ils voient cette pertinence là pour améliorer leurs outils de défense. Je vois que c'est voilà c'est bon. J'ai eu ma réponse en fait c'est l'amélioration des outils de défense. Ouais c'est ça, c'est pour apprendre le technique que tu ne fais pas les attaquants pour pouvoir ouais c'est ça c'est ça.

1:16:46
Merci c'est ça. Parce que en réalité si l'attaquant rentre et que on le détecte pas, parce que oui on on peut ne pas détecter, on peut ne pas détecter pour plusieurs raisons, soit on n'a pas le use case défini parce que ça arrive, donc l'attaquant peut rentrer dans notre système. Donc il y a aucune organisation qui peut dire Moi je suis sécuritaire à 100%, aucune organisation. Pourquoi on parle de la notion de défense en profondeur ? Donc il peut arriver que qu'il rentre, mais s'il rentre.

1:17:16
Si le vente il y aura, on peut l'amener quelque part pour savoir que on n'a pas le use case en question. Et puis on va mettre le use case pour que prochainement on puisse les détecter continue. Donc oui, il y a il y en a qui ont parlé du sort. Oui, le sort généralement dans les systèmes de défense, dans les dans les sorts, on a souvent aussi des des sorts qu'on on ajoute très souvent au ciel.

1:17:44
Donc qui va faire l'encastration de tout ce qui est réponse ou les réponses automatisées,

dépendamment des boucles des plis qu'on aura défini ? Généralement, vous prenez combien de minutes de pause quand vous faites votre cours ? 15 Min OK moi j'aime pas trop 15 Min c'est trop long, on va, on va réduire, on va prendre 10 Min, on va prendre 10 min de pause.

1:18:19
À 20h00 et puis on va revenir à à 20h00. 10O K 15 Min, c'est trop long OK ? Gestion des correctifs et des vulnérabilités, OK. Donc on commence par la fameuse station de Saint Zoo. L'art de la guerre, qui connaît son ennemi comme il se connaît en sans combat, ne sera point défait. Qui se connaît ?

1:18:48
Mais ne connaît pas, l'ennemi sera victorieux une fois sur 2. Que dire de ceux qui ne connaissent pas plus que leurs ennemis ? Isariste STOP m'étonner au niveau OK c'est bon. Donc l'art de la guerre c'est ça. Donc on dit faut connaître, faut connaître ton ennemi, connaître ton ennemi. Si tu connais ton ennemi, c'est sûr que tu vas gagner tes combats.

1:19:14
Donc ton ennemi on a parlé pour connaître l'ennemi, on a tout ce qui aimerait être attaque. On a vu tantôt, on a vu le cyber cul chain, on a aussi les vulnérabilités qu'on va voir tantôt. Donc notre attaquant il va toujours utiliser les vulnérabilités pour venir nous attaquer. Donc on nous on va essayer d'aller corriger ces vulnérabilités là avant que lui il les découvre. Donc on va continuer ça après la pause donc on se retrouve.

1:19:44
À 20h10 tantôt.

1:29:23
Allô ? Vous êtes là ? Ok ? Continue. Donc on la gestion des correctifs et des vulnérabilités. Donc en réalité c'est avoir un environnement qui est exempt de vulnérabilité.

1:29:48
Les correctifs, les correctifs, c'est on les on généralement on les déploie ou sont développés à la suite de découverte de d'une vulnérabilité, ou que le fabricant se rend compte que le système ne fonctionne pas d'une certaine façon et que il va peut être le corriger avant que les uns le les, les les autres, les attaquants sachent ou les chercheurs voient la vulnérabilité ou la faille.

1:30:15
Et très souvent, quand les autres le voient avant eux, on appelle ça souvent des héros DI mais on en parle pas. On reste vraiment à haut niveau. Ici, on a très souvent de nombreuses vulnérabilités, souvent qu'on on découvre. Donc l'idée c'est d'être capable d'examiner les systèmes pour découvrir les vulnérabilités connues et proposer les recommandations.

1:30:43
Donc pour pouvoir faire la gestion de vulnérabilité, Ben on passe déjà dans un premier temps par le balayage des vulnérabilités. On permet, ça permet de savoir quels sont les types de vulnérabilités qu'on a. Donc on pourrait avoir des mauvaises configurations, des passwords qui qui des passwords qui sont laissés dans les systèmes.

1:31:06

Pourra effectuer savoir quels sont les réseaux qu'on a des services non autorisés. Donc avec le balayage, on n'est pas capable de de voir ça. Les les systèmes qui ont des vulnérabilités. Ensuite, on pourra utiliser des outils spécialisés au niveau des applications web, des bases de données pour détecter les vulnérabilités. Donc on a les outils comme des Suse open base, n'expose, rap, CV et autres qu'on peut utiliser pour faire le balayage des vulnérabilités.

1:31:36
Ensuite, quand on a les vulnérabilités, on détecte dans l'environnement les vulnérabilités qu'on a, on fait l'évaluation des risques. Donc c'est pas parce que on découvre des vulnérabilités que tout de suite on se met à les corriger. Parce que en réalité, pour les corriger, ça prend beaucoup d'efforts, ça prend souvent des gens, ça prend beaucoup beaucoup de choses. Donc on fait l'évaluation des risques donc ça va permettre de mettre ou non en place des le correctif. Donc est ce que déjà c'est possible de mettre le correctif en place ? Parce que souvent on a des systèmes déjuets.

1:32:05
Sur lesquels on peut pas mettre de correctifs donc on pourra rien mettre. Est ce que ça demande qu'on ait des privilèges ? Est ce que ça demande qu'on élève des privilèges pour exploiter la vulnérabilité ? Est ce que c'est facile d'exploiter la vulnérabilité ? Quels sont les efforts pour mettre le collectif ? On pourrait regarder quelle est la criticité de l'actif. Bref, on pourra faire certaines évaluations avant de de décider de qu'est ce qu'on fait sur la vulnérabilité en question.

1:32:36
Ensuite pour le déploiement de du correctif Ben on va regarder, on va regarder l'intégrité du correctif est ce qu'il redémarre tout ? Est ce que il y a eu des tests là dessus ? Est ce que certains tests sont faits avec des scripts ? Est ce qu'on a un plan de retour en arrière ?

1:32:54
Très souvent quand on applique les correctifs on on il faut les tester d'abord. Donc si on a les environnements on va commencer peut être par les environnements dev, les tester, s'assurer que tout est bon. Et bien sûr on a toujours un plan de retour en arrière si jamais le collectif ne fonctionne pas correctement et si c'est bon, on l'accepte. Puis on peut le rendre à tout l'âge. Donc on va faire le déploiement, on on va faire des sauvegardes avant l'application de la production, avant l'application en prod.

1:33:22
Si jamais ça demande qu'on modifie le code, Ben on va modifier le code. On va valider que le déploiement est effectué sur des équipements qui sont nécessaires et puis on va documenter le changement, mais souvent très souvent l'application. Si, si, ça demande en tout cas un grand correctif, ça va passer généralement par une demande de changement. Elle va suivre le processus de changement pour que ça soit documenté.

1:33:51
Le choix des outils donc on peut décider d'avoir des solutions achetées. Ben je connais moins de personnes qui ont des solutions développées à l'interne aujourd'hui dans la gestion des Vulnérabilités, quoi que ça peut exister. Donc on va prendre en compte le les plateformes qu'on a, l'expertise interne et puis voir est ce que le système il est capable d'être automatisé puis jusqu'à quel niveau il est automatisé ? Est ce que utiliser l'argent ou il n'utilise pas d'argent ? Est ce que.

1:34:20

On le contrôle en temps réel ou bien il il délivre son système selon lui, son son bon vouloir en termes d'outils à date en tout cas. Je sais que dans le temps il y avait des nerus autres qu'on on achetait, mais bon, ça restait que c'était pas développé en interne. Et puis pour faire du Dashboard, les entreprises développaient avec Power BI des dashboards quand Nexus n'avaient pas un certain niveau de maturité, mais aujourd'hui ils ont des dashboards qui sont intégrés.

1:34:49
En tout cas, je connais moins d'entreprises qui développent eux-mêmes leurs outils achetés, leurs leurs outils de de scan, de vulnérabilité. À moins que on parte sur du open source. Et puis quand on essaie de de l'adapter à ce qu'on veut. Mais aller un développement à 0 à partir de 0, là c'est vraiment rare. Processus de gestion de changement donc on on a parlé tantôt de gestion de configuration, ça va avec la gestion de changement.

1:35:18
On a suivi en fait le la numérotation de de CSSPI. Sinon moi j'aurais mis les 2 l'un à côté de l'autre groupe. Oui Monsieur Fofana, petite question, je voulais savoir pour si vous avez une idée en termes de statistiques, les outils de test de pénétration ou les outils comme les CM ce genre d'outils là est ce que vous avez une idée des proportions ?

1:35:47
En termes d'outils open source et d'outils propriétaires que le monde professionnel utilise parce que les gens utilisent plus des outils open source ou c'est plutôt que des outils propriétaires, les les les ce que je vais te dire, les les les entreprises généralement vont utiliser ce qui est propriétaire. Pourquoi ? Même si c'est open source, ça sera un open source qui a vraiment un support là derrière. Donc en termes de proportion.

1:36:15
J'ai pas les chiffres exacts et puis ça va dépendre des solutions. Mais les outils propriétaires sont généralement au-dessus dans la plupart en tout cas des statistiques récentes que j'ai vu. Les outils propriétaires sont au-dessus pour plusieurs raisons, les entreprises veulent pas ********** elles veulent se concentrer sur leur cœur de métier.

1:36:35
En plus ils veulent avoir du support quand ils ont des problèmes. Donc une entreprise comme Microsoft ou Oracle on sait que IBM on sait que l'entreprise est là. Si j'ai un problème ils ont un support ils vont m'aider. Mais si je prends une solution open source c'est une communauté. Ben je m'adresse à qui ? Et plus souvent j'ai pas l'expertise en interne donc quand j'ai pas l'expertise ça devient compliqué. Un autre exemple, je vais parler par exemple de off 0.

1:37:02
Off 0, et puis il y a des solutions open source qui s'appellent glu par exemple, qui va faire du SSO, tout ça, mais le glu il il va te revenir moins cher en termes de licence mais en termes de support si ton équipe technique est limitée, Ben il s'arrête là alors que l'autre tu as du sport, tu as toute la documentation qui est derrière donc c'est vrai que tu payes mais tu as tout ce qu'il faut. Et puis ton l'équipe technique va se concentrer sur autre chose et puis en entreprise.

1:37:31
Bon ils vont pas désigner sur les moyens pour le choix des solutions en fait. Donc si c'est la solution propriétaire qui fait le travail on ira. Des fois la solution open source peut faire le travail mais la

solution open source ça veut pas dire forcément que c'est gratuit hein. Donc des fois le licencing et puis le tout le développement qu'on va avoir derrière ça peut devenir plus coûteux en fait. Mais pour reprendre faire court, moi c'est plus propriétaire. Les solutions propriétaire sont beaucoup utilisées.

1:38:01
Mais si vous vous voulez utiliser une solution, c'est que vous êtes-vous êtes dans le cas dans le contexte académique ou vous voulez pour votre curiosité personnelle, utilisez un outil. Des fois il y a des il y a des fournisseurs qui vont vous donner des triols et puis après des triols.

1:38:21
Si c'est pas utilisé pour beaucoup de cas vous pouvez utiliser ces solutions là pour vous même votre connaissance améliorée. Donc déjà des exemples d'outils comme des services de sécurité de notation tout ça que vous pouvez avoir ou bien des solutions des services par exemple qui vont faire la DRC que vous pouvez avoir mais sinon utiliser des outils open source va vous faire monter en compétence rapidement. Je prends un exemple.

1:38:49
Open vase par exemple, si je n'ai pas de tinabol mais si j'ai open vase je peux l'utiliser, ça va me me m'aider à à comprendre les stands de vulnérabilité, comment ça se passe ? Ben c'est les c'est les mêmes, ça sera le même fonctionnement que tinabol. Donc tout de suite ça me dit ce qu'on fait autre chose, j'ai j'oublie son nom là je pense c'est alien, Volt ou autre qui est open source qui est que je peux utiliser quand je ne peux pas avoir du sentinelle.

1:39:14
Ou je peux pas avoir du plan qui qui coûte cher donc je vais prendre ça. Et puis travailler par exemple par avec des waf par exemple, des Waf ça ça peut coûter cher. Mais si vous voulez tester ou ou c'est une organisation qui a pas trop les moyens, vous pouvez utiliser par exemple du mode Security avec du Waf pour vous protéger. Donc bref, on a dans le monde open source, moi je dirais le monde open source aide beaucoup à faire avancer l'informatique.

1:39:42
Mais à partir du moment où on rentre dans la business, ils vont plus aller vers du de du propriétaire quoi que souvent même les propriétaires là ils utilisent souvent des moteurs open source. Oui on continue Nacer, t'avais une question, non non je j'ai pas de question, c'est juste quand vous parlez mode sécurité, j'ai dit c'est ça aussi donc Ah OKOKOK c'est ça ? Donc il y a il y a beaucoup de de solutions qui sont là. Moi je vais vous donner un exemple, Linux par exemple.

1:40:09
Quand tu utilises Linux, tu vas savoir beaucoup de choses sur l'informatique que quand tu utilises Windows parce que Windows c'est propriétaire, on veut pas que les gens s'emmerdent, ils sont en entreprise, on veut qu'ils cliquent, ils déposent. Mais quand tu utilises Linux tu vas savoir comment l'ordinateur fonctionne plus rapidement que quand tu utilises Windows. Donc c'est juste un exemple. Mais puis il y a il y a plein d'autres choses, tu as beaucoup de solutions.

1:40:34
En utilisant du open source, tu en tu en apprends plus que si tu utilises de du propriétaire. Oui Ahmed, oui Bonjour Abdullah, je pense juste pour une petite nuance, il y a une différence entre du open source et du Free. Oui j'en ai parlé tantôt, j'ai dit tout, c'est pas c'est pas tout ce qui est open source

qui est gratuit, c'est ça c'est ça. Donc il y a du open source qui est très bien supporté par des fournisseurs qui donnent beaucoup, beaucoup de supports par rapport à ça, OK ?

1:41:04
D'accord OK merci, merci OK donc Bruce est bon pour oui, excellent. Excellent Monsieur Monsieur Fofana. En fait disons l'approche de ma question était plus je sais que les outils par exemple qui rendent des services, les entreprises vont plus ou moins partir sur.

1:41:29
Des solutions propriétaires ? Mais je me dis si je veux faire par exemple un test de pénétration, c'est pas potentiellement quelque chose qui rentre en ligne de compte en termes de production. Donc OKOKOK ces ces genres d'outils là qui ne sont pas des outils qui qui créent la production, qui qui rentrent dans le réseau en tant que tel, mais des outils de supervision, des outils de de, des tests de pénétration, des tests de vulnérabilité.

1:41:54
Peut être que ces outils là, le seul élément éventuellement que les gens n'auront pas, c'est la formation. Moi personnellement je suis pas forcément encore très expérimenté côté sécurité sur ces aspects-là. Donc je me demandais mais la ma ma question, j'ai eu la réponse à ma question, à savoir que si je m'entraîne, même si j'ai des outils open source, ça peut tout de même donner aussi avec un point de vue sur ces gens d'approche là OK.

1:42:21
Ibrahim a la main levée, peut être que il va donner plus d'additifs avant que je revienne là-dessus Ibrahim vas y t'as la main levée Ibrahim est ce que c'est pour donner une question ou donner un additif à ce que Brou a dit ? Apparemment il nous a laissé. Donc oui oui dans le contexte des des pentest, oui on utilise beaucoup du open source. Surtout kali Kali est beaucoup utilisé pour les tests.

1:42:48
Mais en même temps il y a burp burp qui est beaucoup utilisé aussi, qui lui est propriétaire. Je je pense open source mais il est pas gratuit. Voilà pour ne pas me tromper je sais que ils ont une édition Community et puis ils ont une audition propriétaire qui est beaucoup utilisée. Mais sinon après beaucoup d'outils d'open test c'est vraiment des open source qui sont utilisés. Si si on on est dans le contexte du du des des tests d'intelligence. Maintenant de plus en plus on on commence à avoir des outils qu'on appelle des basses bridge Attack, simulation.

1:43:16
Qui sont naturellement des services qu'on va acheter, qui vont venir essayer de de simuler des attaques au niveau de l'entreprise. Bon ça c'est clair que tu vas pas aller prendre quelque chose d'un plein de choses pour l'intégrer dans ton réseau mais globalement les outils de de pentest en tout cas la plupart là c'est du open source. Je sais que les gens utilisent beaucoup burber peut beaucoup utiliser mais lui c'est c'est pas gratuit. Il y a une exposition Community mais qui est vraiment limitée. Super super merci Monsieur, oui merci.

1:43:48
Mais bon mais mais en même temps comme je l'ai dit là, toutes tous les outils qu'on utilise en entreprise, là très souvent ils sont basés sur du sur du open source hein. Quand vous voyez un système pour faire beaucoup de recherche et de développement dans les entreprises qui le font, ils

vont partir sur du open source, ils vont prendre du open source, ils vont travailler là-dessus et après bon ça devient leur solution, ils vont-ils vont le vendre après.

1:44:11
Donc dans le cadre dans le cadre de l'apprentissage, moi je vous conseille, allez dans du open source, vous allez en en savoir plus que celui du que celui du du propriétaire, le propriétaire. C'est bon parce que ça vous permet d'aller vite quand vous êtes en entreprise, vous scannez, vous avez les infos, mais le open source vous allez savoir plus de choses. Oui Mathurin, oui Mathurin, t'avais ta main levée, c'est sur Newton, je t'entends pas.

1:44:45
Ouais, je voulais juste ajouter qu'en fait du open source, généralement comme son nom l'indique, c'est du OPEN. En fait quand c'est propriétaire, souvent c'est limité, souvent en fait on veut tester des choses, on veut tester des choses qui qui ne sont pas dans le cadre de la limite. En fait quand on fait des pentexs, on a par exemple je peux prendre par exemple quand c'est propriétaire par exemple, c'est déjà défini, c'est à dire Vous allez faire ci, vous allez faire ça, vous allez tester des ports. Alors quand c'est du open on peut faire soi-même ses combinaisons.

1:45:15
Donc ça ça ouvre beaucoup plus le champ lorsque c'est des open en fait. Et ça ce que je voulais ajouter. Merci pour ton additif. On continue processus de gestion de du changement, donc à quel moment on fait par exemple un changement ? Donc on va documenter des changements quand par exemple on a des nouveaux, des nouveaux matériels.

1:45:47
Quand on a une nouvelle application qu'on va, on veut mettre dans notre environnement, quand par exemple on a différentes configurations, on va faire le changement de configuration et autre, on veut changer de règle, de pare-feu et autre. Mais bref, tout ce qu'on veut faire dans notre environnement, Ben on passe par un changement. Donc quand on veut faire, on veut changer quelque chose. Tu vois, là c'est ça. Seulement on veut changer quelque chose, on passe par la gestion du changement.

1:46:15
On a le on a le correctif politique, procédure standard. Bon la politique c'est pas forcément la le même fonctionnement mais c'est clair que quand on écrit une politique ou une procédure mais on on va l'approuver, on va montrer aux parties prenantes qui sont OK et puis après ça rentre en ça rentre en vigueur dans dans le cadre des politiques. C'est pas rentré en production mais c'est rentré en ça va rentrer en vigueur.

1:46:40
Donc ça rentre en vigueur. Là on on abroge les autres directives ou politiques en lien avec ça, donc on prend le nouveau. Mais c'est pareil, on c'est c'est tout ce gestion de changement qu'on on va faire. Le but c'est d'assurer qu'un changement est maîtrisé. Je veux faire la différence entre gestion de on a, on a la gestion de changement dans le contexte organisationnel et puis la gestion du changement du côté informatique.

1:47:10
La gestion des changements côté organisationnel, des fois on on veut introduire un nouveau système dans l'organisation dans le cadre d'un projet et puis on va vous parler gestion des changements et dans la gestion des changements c'est plus le changement de comportement humain. Donc il y a

toute une équipe qui va travailler. Comment est ce que vous allez accepter ? Faire l'adoption du du produit ? Donc ça c'est la gestion de la demande. Je vais pas dans le contexte informatique. Haïti c'est vraiment calqué sur les processus Haïti.

1:47:37
Donc dans la gestion des changements, Ben on veut s'assurer qu'un changement est maîtrisé, donc les administrateurs sont informés qu'il y aura du changement. Les effets du changement, on réduit les les effets négatifs et on est capable de faire un retour en arrière si le changement cause des problèmes. Donc c'est c'est, c'est vraiment, c'est vraiment formalisé. Je veux déployer un un système, un docker, un un conteneur quelque part dans mon Azure, mais je vais passer par un processus de gestion des changements puisque ça s'intègre dans mon environnement.

1:48:05
Et étant donné que j'ai ma procédure de gestion de changement que j'ai je je définis, j'explique que j'ai testé, ça fonctionne, j'ai ma procédure de retour en arrière, que là si ça marche pas, Ben je floche le le système je je reviens à 0. Donc tout ça on documente et là on on est, on est quand même sans bon, pas sans danger, mais le on réduit le risque qu'il y ait des un mauvais fonctionnement.

1:48:34
Les étapes de la gestion du changement ? Ben on fait la demande du changement, donc on veut par exemple rajouter un système, donc on va faire la demande. On veut ajouter un système de scan de vulnérabilité. On veut augmenter la portée sur certaines applications parce que on peut avoir nos applications externes sur lesquelles peut être on veut, on veut faire des scans.

1:48:56
Des fois si on ne sait pas puisque le scan il va envoyer des requêtes donc ça peut être vu comme des attaques. Donc il faut faire une demande de changement pour pouvoir intégrer cette porte ce système là de périmètre là dans notre scan. Ensuite on a un comité de de changement qui approuve la demande, donc on a sûrement des comités qui peuvent approuver des changements urgents, des changements standards et autres. Ensuite on a, on va documenter le changement.

1:49:21
On va préparer un plan de retour en arrière comme je parlais, on va tester le changement, on va mettre en place le changement et puis on va faire le rapport et enregistrer le changement. Donc on ne fait pas dans dans une organisation, on ne change pas, on on, on n'échange pas les choses comme ça, on change avec une un processus bien défini. Donc si comme je je, je je quand quand j'ai fait le cours de IT, il y a quelqu'un qui me disait.

1:49:48
Si tu gères ta maison selon les bonnes pratiques, Ben tu auras moins de problèmes. Donc si admettons que à la maison on gère, on fait la gestion du changement, genre on veut mettre une nouvelle, on veut changer la télévision à la maison, Ben on va, on va informer les personnes de la maison, on a un petit comité avec Madame, avec les enfants, on approuve et c'est vrai qu'on va pas, on documente pas tout, mais si jamais la télévision qui vient à la maison va créer des problèmes, Ben on est capable de l'échanger et puis mettre l'ancien.

1:50:18
Bon le test, Ben généralement on va le tester chez le chez le chez le vendeur et puis à la maison si on l'a testé pendant un moment, s'il marche pas, Ben on va le retourner et puis bon, on va mettre en

place des changements et puis dès à présent le le téléviseur sera comme un outil qui sera dans notre dans notre CMDB je pense. C'est le thème qu'on j'ai, j'ai pas, je l'ai pas ici, mais ça va être dans nos inventaires en fait, comme l'outil qu'on a dans notre environnement.

1:50:47
Donc c'est pareil ce qu'on fait en entreprise, on peut l'appliquer au niveau dans notre vie quotidienne, dans notre vie quotidienne, pour s'améliorer. Parce que ça, ce sont des pratiques qui ont été éprouvées, qui ont un moment donné. Les gens se sont dit, mais si on ne fonctionne pas de cette façon, il y aura trop de dégâts en matière informatique. Donc on va avoir la gestion de la configuration, on va avoir la gestion du changement, on va avoir la gestion des incidents, on va avoir la gestion des problèmes, donc.

1:51:13
Tout ça la sécurité va récupérer et c'est ces éléments là que vous êtes en train de voir à travers le cours ici. Donc même gestion des incidents, c'est pas quelque chose qui a été inventé par la CSSPI, c'est ça existe dans le fonctionnement, dans la gestion des du TI, des TI, donc on va récupérer en termes de sécurité, qu'est ce qu'on est capable de faire ? Et puis on on adopte donc tous les termes là si ceux qui ont fait du IT vous allez retrouver les différentes termes, gestion du changement, gestion de configuration, gestion des incidents et autres.

1:51:45
Continue donc dans notre inventaire. Quand on fait le la gestion de changement dans l'inventaire, Ben on va identifier, documenter les éléments comme matériel, logiciel à configuration. On va identifier les écarts dans les configurations. Donc généralement on a la configuration de base dont on a parlé, donc s'il y a des écarts, Ben on va le savoir. On va avoir un inventaire détaillé, donc l'intégrité du système, le recouvrement possible, les correctifs s'ils sont appliqués ou pas.

1:52:13
Ensuite on a l'inventeur de tout ce qui est matériel, tout ce qui est proche de travail, serveur, équipement, télécommunication. Puis on va parler des services. Après on a qu'est ce qui est nécessaire si c'est un remplacement, une destruction ou un contrôle qu'on veut faire là-dessus pour le matériel, on peut avoir tous ces éléments là dans notre configuration database comme le manufacturier, l'adresse Mac, le numéro de série, le système d'exploitation, l'endroit, le bios, l'adresse, l'étiquette, les codes barres.

1:52:43
Le nom du logiciel, le serveur, quand ? Quand c'est un logiciel, la clé d'activation, le type de logiciel, nombre de licences, licence, expiration et puis les licences qui sont portables. Donc on doit avoir toutes les informations là dans notre système qui nous permet de de gérer les inventaires. Pour la gestion du matériel, Ben on va faire le marquage numéro, code, barres, RFDRFID la gestion du site de vie.

1:53:08
Le nettoyage des dispositifs avant de s'en départir. Donc si jamais on a un support, que ça soit une machine ou un un support de de données. Mais avant de le donner ou ou de se débarrasser de ça, Ben il faut le nettoyer correctement ou le détruire correctement. Pour la gestion des licences, Ben on va chercher un outil qui va nous permettre de gérer les licences parce que souvent c'est fastidieux quand on a un gros pack. Et puis on a beaucoup de de logiciels à gérer, donc.

1:53:34
Très souvent ou les entreprises vont se faire aider des outils comme des applications Portefolio management, définir ce qu'ils doivent gérer et autres. On a aussi des actifs virtuels qu'on a comme des machines virtuelles, des conteneurs. Exemple, des dockers, des VDI, des Virtual Desktop Management test of Infrastructures. Ensuite, on pourra avoir des Software defined Network, des dessins, des virtuels Storage aérial qu'on va avoir.

1:54:05
Des les SDN c'est si vous voulez, ce sont des réseaux qui sont gérés en forme logiciel donc ça ça sera si vous voulez des contrôleurs qui vont nous permettre de faire peut être des la segmentation, protéger des IP et PA donc des SDN vont nous permettre de ça serait un peu comme des pas vraiment des points d'accès mais des des des points qui qui sont pas en termes matériels mais en termes logiciels.

1:54:32
Et ensuite tout ce qui est actif Infonuagique, Ben on doit les les identifier tous nos SAS, tous nos passes et tous nos IAS, on doit les connaître. Mathurin, t'as ta main levée, est ce que c'est une ancienne main ou c'est une nouvelle main ? Désolé, c'est une ancienne main. OK OK donc la stratégie de de récupération des données donc on a quand on veut avoir accès peut être à.

1:55:06
À un site web ou à une page au niveau de l'organisation. Mais on a on va partir de l'accès Internet. On a très souvent un autre balanceur qui est devant nos web serveurs qui permet de balancer la charge. Par exemple si un un serveur qui est occupé, Ben il va aller vers un 2e serveur ou un 3e serveur. Ensuite on pourra avoir un firewall. Après ça c'est un waff qui est là, on pourra avoir un firewall ici.

1:55:35
Qui lui également va avoir le balancement entre des bases de données. Mais à l'intérieur des bases de données, on a des disques dus qui sont là, qui eux vont utiliser les raids, les raids dont on va parler tantôt. Donc les disques dus, il y a une façon de les disposer pour assurer une bonne performance et une bonne tolérance au disque. Donc derrière des des bases de données, on a des disques qui sont là, les disques.

1:56:00
Très souvent les disques que vous voyez, on les a derrière les bases de données et derrière tout le stockage qu'on a dans l'informatique. Donc on va voir maintenant le raid c'est quoi ? Quels sont les différents niveaux de raid ? Et puis quels sont les différents noms qui sont là derrière ? Et puis quels sont ceux qui sont le plus utilisés ? Donc le raid c'est le Redondent and Area of Independent dis.

1:56:26
Donc c'est une méthode de gestion des stockages qui combine plusieurs disques durs pour améliorer les performances et ou offrir la tolérance aux pannes. Donc comme vous le savez, vous avez-vous même votre ordinateur sur votre ordinateur, vous avez un disque dur qui est là, donc le disque dur s'il tombe, Ben c'est fini hein. Vous n'avez plus vos données donc C'est pourquoi on vous demande de sauvegarder les données sur d'autres supports. Je, moi je parle du point de vue personnel.

1:56:52
Mais en entreprise on peut pas se permettre de perdre la donnée et puis dire on a perdu les

informations parce que notre disque est gâté ou bien notre disque est tombé en panne. Donc il y a toute une stratégie qu'on met en place pour avoir plusieurs disques durs pour recliquer les informations, pour que si jamais on a une panne sur un disque on peut le remplacer pour récupérer les informations et pour que on puisse être sûr d'avoir toujours l'information. Donc. Et si je prends du point de vue personnel ?

1:57:18
Généralement, rares sont les personnes parmi nous qui n'a pas encore perdu des données d'individus. En tout cas moi j'en ai perdu, j'avais sauvegardé des données quelques pages, je les ai perdues mais dans le contexte d'entreprise on peut pas tolérer que tu perdes des informations. Si je prends une banque comme RBCRBC peut pas dire tu as fait une transaction tel jour, on l'a perdu parce qu'on a un 18 qui est tombé en panne donc c'est pas c'est même pas pensable. Nous on n'est même pas, on pense même pas à ça. Donc ce qu'on met en place c'est le raid généralement qu'on met en place.

1:57:47
Pour s'assurer que on a les bains de performances. Et puis on a la tolérance. Donc on a le raid 0 qui est là, il y a plusieurs niveaux, donc on a le 0123456 et puis on saute à raid 10. Donc maintenant chaque raid a ses spécificités et a ses méthodes. Et Parmi ces raids, ceux qui sont ceux sur lesquels j'ai les astérisques sont les plus utilisés. Donc le raid 0 Ben il permet, c'est on appelle ça le stripping wireward quality.

1:58:14
Il permet de faire la répartition des données entre les tissus et lui n'a pas de redondance. Le raid un, Ben lui il fait le mirroring mais n'a pas de parité donc il il copie exactement les données sur 2 10 ou plus. Le RAID 2 lui il utilise des codes de correction d'erreur au niveau du BIT il est pas trop utilisé, il est pas utilisé dans le passé. Ensuite le raid 3 on a les entrelentements avec parité au niveau octet.

1:58:41
Donc donc on a le raid 4, le raid 4 qui est l'entre lancement avec des parités au niveau bloc donc qui est similaire au RAID 3 avec des blocs. Le RAID 5 est l'entre lancement avec des des parités réparties donc donc c'est un bon compromis entre la performance et la redondance des capacités. Donc on a une parité sur tous les disques et on a le raid 6 6 qui est l'emplacement avec double parité. Donc qui est l'extension du RAID 5 avec double parité.

1:59:10
On a le raid 10 qui est qui fait du mirroring qui est le mélange du RAID un et le RAID 0 donc il combine le raid un et le RAID 0 donc pour une bonne performance. Donc comme je l'ai dit le RAID 0, le raid 5610 sont les plus utilisés. Le raid un lui il fait le le miroir et le un le le 10 c'est comme le un plus le 0 donc il combine le 0 et puis le un.

1:59:41
Donc exemple de de de raid un, donc le raid un, comme vous le voyez on aura le 0, le 0 on a le peut être on a, on a l'information a un on a le 10A un a 3A 5A 7A 2. Donc on aura dans le RAID 0, on aura les éléments comme ça répartis comme ça dans le même raid 0.

2:00:07
On aura une même réplication quand on fait le raid un, donc on prend le raid 0, on prend le raid donc on aura le RAID 0 un pour le raid un on aura une réplication. Donc comme vous voyez le raid un on parle de de mirroring donc on va prendre le un il a son son équivalent de l'autre côté le RAID le a 3 il

a son équivalent, pareil pour l'autre il a son équivalent donc ça ça va faire le raid un +0 donc ça va faire le raid 10 c'est bon.

2:00:40
Dans le cadre de du CSSP, c'est vraiment maîtriser, c'est quel type c'est, c'est vraiment connaître les raids, comprendre leur définition, comment ils fonctionnent, qui sont ceux qui sont utilisés. Dans le cas pratique, vraiment, il faut voyez un 10, comment on le fait, mais j'en ai pas. C'est vraiment se limiter à à l'exemple qui est là, comment ça se fait pour essayer de d'imaginer en terme de.

2:01:04
De 10. Comment on fait le remplacement ? Puis comment est ce que on arrive à combiner les différents types de raids, les stratégies de réplication. Donc pour la reprise de confiance, Ben on va procurer l'assurance que suite à une panne, un système, mais aussi sécuritaire qu'il était avant le désastre. Donc, comme je je donnais l'exemple de RBC, on nous en tant que utilisateurs.

2:01:35
On va pas comprendre que on ait perdu des informations sur une de nos transactions, surtout quand on a fait un dépôt. On va pas accepter ça. Donc il faut que eux ils ils aient des systèmes qui sont qui sont capables de même s'il y a un désastre là revenir à l'État où ils étaient et être toujours sécuritaires. Quand je donne l'exemple de RBC. Mais c'est pareil hein pour nos entreprises où on a les informations souvent des clients.

2:02:00
Donc il requiert une copie sécuritaire et fiable du système. Il se produit lorsque le système n'est plus stable ou sécuritaire. On peut avoir une reprise manuelle, donc aucun mécanisme de gestion des défaillances dans ce cas-là ou on peut avoir une reprise automatisée donc capacité pour au moins un type de désastre automatisée mais sans perte induit. Donc certains objets seront protégés donc on peut avoir aussi des reprises fonctionnelles.

2:02:27
Ou des reprises font juste reprendre des fonctions essentielles ou des fonctions critiques de l'organisation. La récupération des systèmes après panne, donc on voit la la, le redémarrage du système en mode mono utilisateur ou console de récupération, la récupération des systèmes de fichiers actifs lors des échecs. La récupération des fichiers manquants ou endommagés, la récupération caractéristique de sécurité tels que les étiquettes de sécurité des fichiers.

2:02:57
Généralement, les, les labels sur les fichiers, les les métadonnées sur les fichiers, la vérification des fichiers critiques pour la sécurité, tels que les fichiers tels que les fichiers de mots de passe, les fichiers de mots de passe système, mais et TC généralement, dans les systèmes d'Inix pour le redémarrage, le redémarrage d'un système doit toujours afficher une fenêtre d'authentification, donc de façon générale, Logunk strict.

2:03:25
Et le redémarrage, il vient après un arrêt fiable par un administrateur par exemple n'importe n'importe quand lorsque le système s'arrête de lui même lorsqu'il celui-ci détecte, détecte qu'il n'est plus fiable. Pour les centres de secours, on a également prend en compte des centres de secours, des services d'abonnement. Donc aujourd'hui on a beaucoup de systèmes qu'on appelle des design services.

2:03:52
Très souvent, c'est des systèmes qui nous permettent de de faire des recouvrements de nos systèmes plus rapidement. On pourra. On a plusieurs types de sites pour les recouvrements, donc on a des hors sites, donc on pourra avoir des systèmes miroirs, donc actifs, donc des systèmes qui se répliquent automatiquement.

2:04:15
On pourrait avoir aussi des systèmes de ces cours équipés, donc c'est des systèmes où on a tous nos serveurs que on a dans. Dans l'exemple où on avait parlé d'un incident au début du cours, j'avais parlé d'un incident où on pouvait il y a, il y a je pense. C'est Émile qui avait posé la question, si jamais non, c'est Brice plutôt qui a dit des fois quand on a des attaques, souvent les.

2:04:43
La business veut qu'on on restaure le système rapidement. Donc je disais que si on a un autre site et que dans ce sur ce site là on a les informations, on est capable de relever le site. On peut le relever le temps que on reste pour le premier site. Donc ici dans la stratégie de récupération, Ben on peut avoir des hors sites. Donc on peut avoir un site où on a des sites actifs donc c'est des c'est un site où les informations sont de part et d'autre républiques et répliquées.

2:05:10
De part et d'autre donc la même information qu'on a dans le site B on a dans le site a sur le site a comme on peut avoir des sites qui sont équipés, on appelle des autres sites. Donc c'est un site où on a l'ensemble de nos machines, on a tout ce qu'on a dans l'autre site mais sauf que on l'a pas activé donc il est là, on est correct dès que on est prêt, il suffit juste de lancer tout est prêt ou on peut avoir un site, on des wames site des sites intermédiaires, c'est des sites où on a quelques appareils.

2:05:38
Mais on n'a pas tout l'ensemble de nos éléments donc c'est lui. Il aura besoin de plus de serveurs ou plus de d'applications pour que il soit fonctionnel parce qu'il n'est pas tout de suite fonctionnel. Et on aura des sites DC pour blanc Call, site où c'est un site où vraiment on a minimalement les éléments. Mais pour le mettre en place ça va prendre plus de jours que peut être un site, un hors site. Ensuite on peut avoir des accords réciproques ou on peut avoir d'autres options, des centres de traitement comme des data centers.

2:06:08
La question pourquoi est ce que on choisirait un site par rapport à un autre ? Je vais en parler tantôt, ça prend le budget, ça prend plein d'autres d'autres aspects pour un site miroir. Donc la reprise lui, il est instantané parce que le site est toujours fonctionnel et le site est toujours en fonction. Donc si on met les données dans le site A Ben on a les données.

2:06:30
Les les mêmes données dans le site B Donc je prends dans le cadre de des sauvegardes des données. Donc j'ai une entreprise, j'ai, j'ai, je traite des données, j'ai des bases de données, j'ai des sauvegardes de mes données, donc que ça soit mes bases de données, mes serveurs, tout ça, j'essaie de les sauvegarder quelque part, j'essaie de les sauvegarder quelque part, donc pour les sauvegarder, Ben je peux les mettre sur un site qui est actif, actif de telle sorte que.

2:06:56

Si jamais en cas de de ransomware j'ai ma sauvegarde qui est attaquée sur mon premier site mais l'autre site j'ai les mêmes données qui sont là-bas que je peux récupérer rapidement maintenant la question est ce que la réplication va pas copier les mêmes ransomware ?

2:07:12
Non parce que des on a des systèmes aujourd'hui qui sont capables de détecter des menaces et qui sont capables de bloquer certains menaces. On a plusieurs comme volts vimbacables des solutions vraiment éprouvées qui qui vont pas copier systématiquement des logiciels malveillants d'un site à l'autre. Ensuite on a les sites de secours qui sont équipés. J'ai parlé de hot sites donc lui c'est quelques heures donc il contient tous les équipements nécessaires donc dès qu'on est prêt on l'active.

2:07:41
On n'a pas besoin d'attendre plusieurs instants pour l'activer donc comme vous le comprenez. Donc ça veut dire que si j'ai un hot site, les mêmes équipements que j'ai dans mon site principal, Ben je dois l'avoir de l'autre côté. Donc c'est que mes équipements je les achète 2 fois donc ça demande un plus gros investissement. Ensuite on a les One sites donc lui le recrutement prend plusieurs jours donc il contient déjà des équipements de base mais pas des données donc on a les données ailleurs donc quand on a besoin pour faire.

2:08:10
La récupération, mais on va, ça va prendre plusieurs jours parce que on n'a pas toutes les données, on n'a pas tous nos serveurs qui sont en place. Ensuite le site de secours cold site, mais lui il va prendre plusieurs jours, donc il contient juste l'électricité, les emplacements physiques mais pas d'équipement. Donc c'est un coût qui est très bas. Donc ça va dépendre de qu'est ce que on a au niveau de l'entreprise comme budget pour notre stratégie de récupération.

2:08:38
Est ce que on comprend tous c'est quoi quand on parle de récupération ? C'est quoi ? Parce que quand on a un incident et dans les après l'incident on a on avait parlé des différentes étapes, on veut récupérer. Donc l'incident peut concerner tout un site complet mais si tout notre site complet est est est attaqué ou toutes les les informations sont chiffrées par un ransomware.

2:09:05
Ben ça va arrêter notre opération, mais si on a un site de récupération Ben on pourra le récupérer rapidement et puis continuer nos opérations. Mercière désolé, c'est une erreur, pardon désolé j'avais beaucoup de mails légers, je vous voyais pas désolé c'est court, oui oui désolé il y a pas de problème en fait je voulais revenir, tu as tu as dit quelque chose qui m'a interpellé, je voulais savoir quand tu as dit tantôt, tout à l'heure que.

2:09:35
Il faut faire disons des les réplications. Et puis tu avais pris l'exemple, mettons de Vimba Cap et que ça ne avec l'intelligence ça ne permet pas de répliquer. Je peux dire des cochonneries en griffes comme ça. Ma question est de savoir est ce que ça ne joue pas sur l'intégrité de la Réplication ?

2:09:54
Parce que des fois on peut avoir comme des faux positifs, mais le le l'intelligence va se dire Non Ben je fais pas ça pourtant c'est important. Je veux dire est ce que ça joue pas quelque chose comme ça ? Oui c'est possible, il peut avoir des des faux positifs mais c'est dans le Fain twinning qu'on arrive à

annuler ces éléments là. OKOK oui je dis moi je je j'ai pas dit que non, il y a jamais de faux positifs, oui il peut avoir de faux positifs. OK oui zéphirin.

2:10:24
Oui, Bonsoir au fond la, moi j'étais j'ai depuis le début du cours, j'essaie de faire le fil conducteur en lien avec le forensic du début versus là où on est rendu actuellement. Là je comprends que les éléments qui ont été précités dans dans le cours ont avaient pour objectif justement de voir un peu les bonnes pratiques, mais ce qui est l'importance de chaque de chaque composant, de telle sorte que quand on arrive dans un site de de relève par exemple, on est attaqué.

2:10:53
Mais de l'autre côté le système attaqué a été comme isolé est en en on va dire en en recherche là où c'est à dire en investigation. Et là on est au moment où nous parlons en ce moment on est en train de de restaurer ou bien de de de repartir, de faire un plein de relève pour justement avoir une continuité d'affaire. Est ce que je suis bien le cours en ce de ce point de vue là ?

2:11:17
Oui tu suis le cours maintenant est ce que dans la pratique c'est le cheminement correct ? Ça peut être le cas ou non. Sinon oui dans le cours c'est ça. Maintenant, s'il y a une attaque, on avait montré les les différents schémas de de processus de gestion d'incidents. S'il y a une attaque, on fait tout pour garder la preuve comme on a dit la les pour les preuves touristiques.

2:11:44
On va faire la récupération tout en faisant tout en gardant en fait les preuves pour la pour le forensic, ça c'est pour vraiment permettre qu'on roule l'opération, mais en même temps qu'on est en train de rouler l'opération. Les enquêtes peuvent continuer jusqu'à trouver qu'est ce qui s'est passé ? Parce que attention, n'oublie pas qu'on a une attaque. On a très souvent une cybération qui doit nous rembourser, mais elle veut savoir que ce qui s'est passé. Donc oui, on aura le forensic.

2:12:09
Maintenant dans l'ordre est ce que on finira de tout récupérer et on va continuer la forêt les les investigations oui ça se peut et très souvent c'est le cas. Les forêts s'ils peuvent aller prendre plus de temps c'est ça ? Je sais pas si ça répond à ta question, oui oui oui. Et donc pour aller plus loin, je comprends que ce sont les assureurs qui vont décider de c'est à dire après avoir recueilli toute la preuve nécessaire vont décider de nous libérer le site qui est en train de se faire investiguer.

2:12:41
Est ce que non pas forcément pas forcément dès que on a collecté les preuves, généralement quand il y a des incidents, très souvent quand quand il y a une cyber assurance hein le le la cyber assurance exige souvent ces brutch coach hein. Et puis toute son équipe ils ils ils exigent quelques entreprises qui sont censées intervenir en cas de cyber accident, cyber incident. Donc très souvent ces entreprises ou ces personnes là sont dans votre plan de gestion des incidents.

2:13:06
Donc quand il y a un problème, c'est eux qui vont intervenir, ils les cyberassurances, leur font confiance, donc eux dans le cas du forum ainsi qu'ils vont tout récupérer. Donc quand ils vont récupérer leurs preuves et que ils nous donnent le Go, ils vous donnent le Go pour répartir vos systèmes, vous répartez vos systèmes, ils vont continuer à faire leur enquête donc c'est pas forcément les cyberassurance qui va donner le ça sera si si vous voulez les partenaires que la cyber argent aura

mandaté. Dès qu'ils vous donnent le Go, vous répartez vos systèmes, vous n'allez pas attendre parce que.

2:13:33
Admettons que on est dans un site hors site, on est on est sur un site, un un autre site ou un site qui est qui a qui a tous les équipements. Ben là puisque l'autre site n'est pas bon, on est sur un site, c'est court là, donc si jamais on a un incident là-bas on est mort. Donc le site c'est court, c'est vraiment c'est comme ton piné secours de ta voiture, tu vas le mettre pour te dépanner mais tu vas pas rouler avec ça, tu vas te dépanner et puis tu vas réparer ton ton autre roue pour que si pour pour le pour remplacer.

2:14:02
Pour mettre le secours à sa place et puis garder le la ta ta vraie roue. Donc dès que ces partenaires là donnent le OK Ben on est on est capable de faire la récupération rapidement. Oui parce que moi je posais la question parce que nous on a des plans d'action justement dans ces plans d'action là oui on est mal pris. On appelle l'assureur d'une part, mais d'autre part on appelle notre consultant en cybersécurité qui va justement nous appuyer.

2:14:28
Dans la démarche et parallèlement, on doit continuer à passer à travers les étapes, c'est à dire arriver jusque au plan de relève pour la continuité des affaires. En attendant, parallèlement de l'autre côté, Ben les investigations sont en train de se faire. Nous les consultons et là en train de nous accompagner dans la reprise des affaires et aussi dans la recherche parce que on ne sait pas avec qui est ce que l'assureur arrive.

2:14:51
Et donc moi, moi dans mon cas, on a le gouvernement qui intervient et à ce moment-là c'est c'est lui qui devient le chef d'or. Qu'est ce qu'on pourrait écouter ? Moi j'interviens et tout doit être fait en fonction de mes procédures internes. Moi OK, c'est bon à ce qui se dit en ce moment, OK c'est bon. Merci pour ton additif de toutes les façons.

2:15:14
Que ça soit au gouvernement. Bon, parce que s'il peut avoir le cas d'une entreprise qui est dans un groupe hein, qui a cette procédure, qui dit nous on veut tel partenaire qui va intervenir en cas d'incident, Ben vous les avez dans votre plan. Si c'était la garde du gouvernement qui définit, vous avez ça le cyberassureur si il définit le partenaire avec qui on fait affaire. Donc en cas d'incidents, on les appelle, ils vont intervenir, eux, ils vont collecter la preuve, puis il y aura un partenaire. Soit ça peut être notre équipe de réponse des incidents, on va faire la récupération, commencer nos activités.

2:15:44
Mais avant ça on aurait sauvegardé tout ce qui est élément pour le forensic. Ouais Émile, oui merci beaucoup. Je sais pas si moi je sais qu'il était 55 mais j'aurais une question vraiment simple par rapport aux technologies, rate là vraiment ou des 5 que tu as marqué le raid 0 plus un ?

2:16:04
Versus le RAID 1.1+0 admettons, j'ai un disque qui brise un raid 0 plus un, on remplace le disque, ça récupère de ça récupère de l'autre, mais le raid un +0 là je vois c'est tout. OK non je viens, je viens de le voir, c'est tout strippé puis OK j'avais juste mal lu encore qu'un disque qui brise Ben l'autre qui prend l'air. Ouais c'est ça. Et puis on le remplace rapidement.

2:16:32
C'est comme le le le c'est pas parce que le secours est là que on est on est confortable hein. Dès que ça brise on on le remplace et qu'on soit on soit correct. Là j'avais juste mal lu les les c'est beau. Merci OKOK donc on avait parlé des différents sites donc on avait site à site blanc, site intermédiaire.

2:16:57
On a on peut avec la Géo Géodiversité donc plusieurs centres de traitement, donc distribution de traitement dans plusieurs centres, création d'une architecture de sérieux propice à la redondance pour l'Info Nuagique bon ça peut être une option qui est de plus en plus utilisée. On on transfère la gestion de la GÉO résonance des infrastructures. Donc si on est dans du des de l'Info Nuagique, Ben on a on initialement quand on a notre data Center. Bon, on parle issue d'une infonuagique, quoi que.

2:17:24
Même dans les fonds nuagiques, on va aller vers des solutions aussi multicloud, parce que on veut pas avoir de dépendance juste sur un fournisseur. Donc on a dû on est dans Azure, mais si on peut être sur AWS ou Google Aussi, Ben on va essayer avoir une stratégie multicloud au cas où Azure même c'est Azure. Parce que si Azure même a des problèmes, Ben on est capable d'aller sur du AWS, donc peut avoir plusieurs stratégies comme ça au niveau de l'organisation. Ouais au doux.

2:17:53
Oui en fait oui j'ai juste une petite question là c'est pour savoir la différence entre le One site et puis le code site en terme de du nombre de jours OK et pour la récupération on voit que pour le pour le web site par exemple je vois plusieurs jours et pour le 2nd qui est code site je vois jusqu'à 30 jours OK donc j'aimerais savoir est ce que pour.

2:18:19
One ça va être là là où nous sommes en train de parler de plusieurs jours, est ce que c'est on peut dire inférieur à 30 jours ? Ou bien c'est pas exactement parce que ça non non non on peut-on peut-on peut pas donner la date exacte c'est qu'on on peut pas donner le nombre de jours. Exemple on donne une prévision en fait l'idée c'est de dire que lui il prend moins de jours que le col site, donc on dit jusqu'à 30 jours, voilà on on on on donne 30 jours parce que on se dit que c'est ce qui est acceptable parce que si ton opération.

2:18:49
Dépasse 30 jours il se peut que peut être tu déposes les les la clé donc c'est juste un exemple qu'on a donné mais il y a des récupérations qui peuvent être encore plus longues donc c'est juste à titre de grandeur qu'on donne. Mais on n'a pas on peut pas dire exactement le nombre de jours. Ça va dépendre aussi de beaucoup de paramètres comme je je je je pense. Je présume que dans les autres que vous avez vu les RTO, les RPO et autres, est ce que vous avez vu ça dans dans le cours de dans les autres cours ?

2:19:17
Parce qu'on a fait ça, oui RTO voilà donc oui ça va, voilà exactement donc récupération exactement dans le plan de récupération, les RTO, les RTO que vous allez définir là va venir jouer sur le type de sites dont vous avez besoin. Donc si on vous dit non, on veut récupérer rapidement en termes de secondes ou en termes de Ben Voilà combien ça coûte en dollars, si on dit OK, on est prêt à payer, Ben vous allez tout faire pour avoir un site qui va avec. Donc dépendamment de votre budget, vous allez prendre un warm site ou un outside ou un Call site dépendamment de.

2:19:47
De qu'est ce que vous avez défini dans un business continuity plan ? Les RTE et puis les RPIO donc c'est ça qui va traduire. Qu'est ce que vous choisissez comme type de site ? D'accord, c'est bon, c'est c'est comme voilà, c'est comme un exemple hein, c'est comme toi, tu as un chalet et dans ton chalet tu as une maison, tu as ta maison, tu tu tu viens à Montréal et puis tu as un chalet et tu payes les mêmes factures de Hydro. Tout, tout, tout, tout ça va dépendre de tes moyens.

2:20:16
Si tu as les moyens d'avoir le Chalet, entretenir tant mieux, mais si t'as pas les moyens, Ben tu vas juste avoir une maison et plus souvent prendre souvent des Airbnb quand tu voyages ou louer juste le le chalet. Donc c'est c'est le même concept en fait. Sauf que en entreprise, Ben on est obligé de de de standardiser. Et puis d'après une de mes connaissances, c'est juste que on ajoute plus des euros, c'est c'est la même chose comme à la maison, mais on ajoute plus des euros quand on est en entreprise.

2:20:46
C'est ça. Donc c'est beau. On a dans le tout sur la stratégie, on peut avoir des accords de réciprocité, donc 2 entreprises dans le dans le cadre de desa ou autres pas une option qui a une obligation légale. On peut avoir des ententes verbales avec des partenaires, donc quelques points à traiter. C'est que la disponibilité, l'assistance, l'interopérabilité, le conflit d'intérêts, la gestion des changements qu'il faut qu'il faut voir dans ces cas de.

2:21:16
Stratégie de récupération, autre option pour un centre de traitement, donc on peut avoir des centres de traitement mobile. On peut avoir également des matériels de remplacement interne ou externe où on peut avoir des bâtiments aussi préfabriqués. Il arrive dans le cas peut être de des compagnies comme Bell, il peut avoir des des centres mobiles. Admettons que le système.

2:21:41
Système de télécommunication, peut être ne marche pas dans une dans une zone, donc on peut avoir un système mobile qui peut venir peut être fournir le service des télécommunications, tout comme il peut avoir des endroits où on n'a pas de l'eau, mais ça c'est pas dans le cadre informatique. C'est dans le cas des endroits où il y a des crises, peut avoir des centres où on n'a pas de l'eau, donc peut avoir des camions mobiles qui passent pour les services. Donc ça c'est tous des stratégies qu'on peut avoir aussi dans le monde informatique, c'est bon.

2:22:12
Processus de reprise après sinistre, donc on a le sinistre, donc après le sinistre on veut faire la récupération, on peut faire, on veut faire la reprise après sinistre. Donc le but principal c'est de prévoir, prévenir ou limiter les blessures aux personnes. Donc retenez toujours dans le cas de la sécurité.

2:22:36
Quand il y a une crise, on sauve les vies humaines. D'abord ce sont les plus chères, on essaie de voler les on, on cherche à sauver les vies humaines avant de sauver les serveurs et puis les logiciels. Bon pas que les le l'avant de servir les les serveurs et les données. Faut prévenir ou limiter les pertes aux actifs. Quand on finit de sauver les gens, Ben il faut préserver aussi les actifs là donc c'est ça, prévenir, restaurer, limiter les pertes des fonctions.

2:23:03

Vital de l'entreprise. Donc si il y a des éléments qu'on qui sont critiques pour nous en entreprise, Ben il faut tout faire pour les sauver. Donc on va répondre donc avec des instructions simples et compréhensives. Donc selon la nature du désastre, on va répondre selon la nature du désastre. Le personnel, Ben on va avoir une liste de personnes à contacter en cas de sinistre.

2:23:29
Donc pour l'utilisation, pour la communication, Ben on a une liste, un check list qu'on va avoir pour voir. Est ce que on a communiqué de façon suffisante pour l'évaluation ? On a les triages, on va établir les impacts pour la restauration, Ben on va utiliser les sauvegardes un peu. On pense tout à l'heure à la stratégie de la la stratégie dont on avait parlé, stratégie de restauration, la restauration, ça va avec des sauvegardes.

2:23:55
Ensuite, toujours pour la récupération des données, Ben on a les copies de sécurité des gouttes électroniques. La récupération des codes sources peut avoir pour les copies de sécurité site ou hors site. Ben on va avoir une identification transfert et puis avoir un transfert contrôlé, avoir un stockage sécurisé, connaître la durée de rétention et puis les données systèmes et des copies de sécurité.

2:24:22
Pour la sauvegarde Backup, Ben on va identifier les données à sauvegarder parce que une sauvegarde pas, on va pas tout sauvegarder. Finalement il y a des données qu'on veut sauvegarder, il y en a qu'on veut pas sauvegarder, on va installer ou configurer des agents de sauvegarde, on va faire une sauvegarde fréquente voulue selon la critique et la variabilité. On va valider l'intégrité des sauvegardes, un peu la question de de Brice, tantôt de de ces coûts.

2:24:49
On va transférer les données en lieu sûr, on va archiver sécuritairement selon la durée de rétention et puis les copies. On va détruire les sauvegardes lorsqu'elles ne sont plus nécessaires parce que il faut gérer aussi l'espace de stockage qu'on a au niveau de si on est dans le dans de l'Info Nuagique, Ben on a des espaces de stockage qu'on paye en fonction de notre consommation dans les services sauvegardes dont on n'utilise plus, Ben faut s'en débarrasser.

2:25:20
On va parler maintenant des différents types de sauvegarde, donc on a la sauvegarde qui est complète, donc ça c'est facile à comprendre. J'ai lundi, mardi, mercredi, jeudi, vendredi, samedi, dimanche. Donc je fais ma sauvegarde le dimanche, je fais ma sauvegarde le lundi, je fais ma sauvegarde mardi tout ce que j'ai fait lundi, dimanche, là je prends tout, je les mets dans lundi.

2:25:46
Lundi, je récupère tout ce que j'ai, je mets mardi, mardi, tout ce que j'ai, je mets mercredi, mercredi ainsi de suite, dimanche j'ai toute ma sauvegarde complète, je reprends, je je reprends mon exercice, ça la sauvegarde complète comme ça c'est simple, c'est c'est facile à comprendre. Ensuite on a la sauvegarde incrémentale, la sauvegarde incrémentale, qu'est ce qu'elle fait ? Elle copie uniquement les fichiers modifiés depuis la dernière sauvegarde complète.

2:26:16
Ou incrémental donc j'ai fait ma dernière sauvegarde complète, j'avais vu la dernière sauvegarde le dimanche, j'ai fait ma dernière sauvegarde du dimanche, je suis au lundi, je vais juste prendre les fichiers du lundi qui ont changé, qui ont été modifiés si y a pas des fichiers qui ont été modifiés

puisque j'ai ma sauvegarde complète qui a été faite. Donc ça veut dire que mes données du dimanche sont bonnes. Mardi je fais pareil, je vais juste prendre les fichiers du mardi qui ont été modifiés.

2:26:43
Et j'ajoute sur ce que j'avais déjà lundi, là-dessus je fais, je reprends l'exercice mardi pareil si mardi il y a eu des des fichiers qui ont changé, je vais reprendre les fichiers du mardi qui vont revenir le mercredi. Pareil je continue jusqu'à la fin et à la fin je vais juste avoir les fichiers que j'ai modifiés, les fichiers qui ont été modifiés depuis la dernière sauvegarde.

2:27:13
Donc si j'ai fait des j'ai fait des modifications, si j'ai pas fait des modifications, je les prends pas en compte. Mais si j'ai fait des modifications, si j'ai fait des modifications sur des figés, je les prends en compte. Mais il va toujours prendre la la dernière sauvegarde incrémentale ou la dernière sauvegarde complète. Donc comme vous le voyez chaque fois, il va rajouter les nouvelles sauvegardes qu'on a. Donc ça c'est la sauvegarde incrémentale. La sauvegarde différentielle, elle, elle copie les fichiers modifiés depuis la dernière sauvegarde complète, peu importe les sauvegardes différentielles précédentes.

2:27:44
Donc elle, elle va regarder le dimanche. J'avais fait une sauvegarde complète le lundi, je prends juste les fichiers qui ont été sauvegardés, les les fichiers qui ont été modifiés le mardi, je prends ceux qui ont été modifiés lundi, mardi je le prends pareil, je continue l'exercice. Donc la différence entre le la sauvegarde incrémentale et la sauvegarde différentielle, c'est que l'incrémental.

2:28:08
Lui il va prendre les fichiers modifiés qui ont été modifiés depuis la dernière sauvegarde complète ou incrémentale. Elle elle elle prend juste différence, elle elle prend juste c'est quoi a modifié depuis la dernière sauvegarde complète tu vois ? Oui en fait moi ma question c'était pour la complète je vois pas de différence vraiment entre l'INCRÉMENTALE et le complet, c'est c'est la même chose.

2:28:38
Comme si je dirais c'est un peu la même chose non c'est pas la même chose la complète elle peu importe qu'elle soit modifiée ou pas, elle elle copie tout, c'est à dire le le le je suis au dimanche, le lundi, le lundi il va recopier, il va prendre toute la sauvegarde que j'ai, il va tout copier, que j'ai modifié ou pas, il fait toute la copie donc ça va faire augmenter la bande passante. Admettons que je fasse une copie à distance, donc il va non seulement utiliser mon trafic internet.

2:29:07
Il va aller utiliser plus d'espace puisque il va copier tout ce que j'ai. J'avais déjà fait une sauvegarde de toute la la la sauvegarde complète. Lui il va les reprendre tous, il va tous les copier lundi, il prend tout ce qui a été fait lundi, les nouveaux qui se sont rajoutés, tout ce qui a été modifié, tout ce qui n'a pas été modifié, il recopie tout ça. C'est ce que la sauvegarde complète fait. La sauvegarde incrémentale, elle prend en compte juste puisqu'elle a déjà fait une sauvegarde complète, il y a déjà une sauvegarde complète, elle va prendre juste les données qui ont été modifiées.

2:29:36
Et puis la dernière sauvegarde incrémentale ou complète, c'est ça la différence entre les 2. Donc en termes d'utilisation de bande passante, l'incrémental va en utiliser moins que la sauvegarde complète. OK oui merci, je comprends mieux. Donc c'est l'incrémental va être un peu plus rapide que la foule,

mais la différentielle va être plus rapide que l'incrémental. Ouais aussi OK, je comprends bien, c'est bon OK ?

2:30:08
C'est bon ? Est ce qu'il y a d'autres questions ça il y a beaucoup oui. Est ce que vous pouvez s'il vous plaît répéter la différentielle, la différentielle ? En fait elle fait la copie des fichiers modifiés depuis la dernière sauvegarde complète. Donc peu importe les sauvegardes différentielles, elle elle regarde pas les différences différentielles comme dans l'incrémental donc elle va prendre dès qu'on fait une sauvegarde complète le dimanche.

2:30:34
Jusqu'à la au prochain dimanche au dimanche prochain, elle va juste prendre les fichiers qui ont été modifiés. C'est ces fichiers modifiés qu'elle va envoyer puisque il y a on a déjà une sauvegarde complète, c'est bon mais ce que je vois, même incrémental, il fait juste la copie de la dernière sauvegarde. Non elle fait pas la dernière de la elle fait la copie de ce qui a été modifié. Oui lors de la dernière.

2:31:03
Sauvegarde complète ou incrémentale, oui, alors que elle la elle elle regarde pas la différentielle, elle ce qu'elle fait chaque jour elle regarde pas ça, elle regarde, elle compare par rapport à la la la sauvegarde complète jusqu'à la prochaine sauvegarde complète. Qu'est ce qu'il y a à modifier ? C'est ce qu'elle envoie donc à chaque fois il va copier le les modifications, ça c'est le différentiel qui fait ça, lui il prend juste les fichiers modifiés depuis la dernière sauvegarde complète, OK.

2:31:33
Merci ouais Brian, oui ça pour ça, ça veut dire que dans le fond, la la plus rapide alors c'est l'incrémental, C'est ça ? Non, la plus rapide c'est la, ça sera la différentielle. Ah mais la différentielle en fait. Dans quel sens ? Pourquoi ? Parce que.

2:31:58
La différence entre l'incrémental et la différentiel, c'est c'est justement le fait que l'incremental se se se charge de de gérant. En fait, l'ensemble des fichiers qui ont simplement été modifiés depuis la dernière sauvegarde incrémentale ou bien différentielle. Donc admettons, non, non, non, non incrémental est complexe, ou bien.

2:32:22
Complète en fait. Oui, donc admettons. Par exemple, pour la sauvegarde incrémentale, si si je fais ma sauvegarde le dimanche dans le lundi, ça va récupérer seulement les fichiers modifiés. Les les fichiers modifiés en fait depuis dimanche, le mardi ça va récupérer les fichiers modifiés en fait et mais qui n'ont pas été.

2:32:50
Le en fait ça va récupérer les fichiers modifiés par rapport à lundi donc en fait c'est c'est c'est comme si le lundi on récupérait simplement les fichiers modifiés par rapport à dimanche et maintenant le mardi on récupère les fichiers qui ont été modifiés en ce jour et qui sont oui oui oui c'est vrai tu as tu as, tu as raison c'est vrai c'est vrai l'incrémentale oui elle elle est rapide, oui et maintenant la différentielle.

2:33:17

Va se recharger simplement de si si on fait la sauvegarde le dimanche, la sauvegarde complète le le dimanche. Le lundi ça récupère naturellement les fichiers qui ont été modifiés, mais le mardi ça va récupérer les fichiers du mardi et ceux du lundi. Ouais tu as raison c'est ça.

2:33:39
C'est le oui c'est vrai. Tu as raison la l'incrémental je je fais une une une nouvelle l'incrémental elle est plus rapide mais en termes de restauration elle est plus longue par rapport à la différentielle et la différentielle, elle elle est plus rapide en fait en termes de restauration. Mais des fois s'il y a pas un gros écart entre les données incrémentales ça revient. Ça revient souvent à la même chose puisque la dernière lui il prend toujours par rapport à la dernière sauvegarde complète et l'autre.

2:34:08
Incrémental prend la dernière sauvegarde complète ou la dernière sauvegarde incrémentale, donc dépendamment de notre fréquence de sauvegarde, les 2 peuvent aller pareil, mais la différentielle elle elle est plus rapide en termes de de récupération. OK c'est bon, est ce que il y a d'autres questions ? On va aller vite, il me reste pas assez de temps.

2:34:38
Vous avez un quizz ? Après c'est ça hein ? OK donc pour les bases de données, pour tout ce qui est base de données, Ben on a la voûte électronique sauvegarde on peut faire les sauvegardes par lot ou on peut envoyer tous les fichiers modifiés pour la finalisation Remote journaling donc on peut faire en temps réel les journaux de transaction sur les DB, les transferts à différence des fichiers, le delta qui est pas transféré.

2:35:05
On peut faire le miroir des bases de données, c'est à dire faire en sorte que la même base de données on le retrouve de part et d'autre pour la reprise. Comme vous le voyez, plus on a un site de réplication qui est synchrone, plus ça coûte cher et moins on met moins de temps pour la récupération. À la question de tantôt on doit-on doit, plus on va.

2:35:34
Avoir un site qui est plus synchrone donc le site est synchrone, on a les autres sites et autres donc on a une bonne disponibilité, on a une bonne disponibilité en temps en continu donc la récupération va être plus rapide donc ça sera en termes de minutes. Et moins on est, moins on a. On a un site qui qui est moins asynchrone mais qui est moins synchrone. Autant pour moi donc qui ?

2:36:03
Qui n'est pas en temps réel. Donc on va mettre plus de temps pour le recouvrement, c'est ce qui est tout à fait normal. Et plus on est, on est synchrone, plus c'est cher. Donc parce que on aura dédoublé tous nos éléments continue. Test plan de reprise après sinistre donc les tests de reprise après sinistre bon, on a parlé tantôt de reprise après sinistre.

2:36:32
Mais en réalité, tout ça est préparé. Donc puisque on on sait que on peut avoir souvent des incidents qui peuvent rendre notre site non fonctionnel ou qui peut rendre notre entreprise non fonctionnelle. Donc on a prévu des stratégies, des de récupération qu'on avait. On a un plan de reprise après sinistre, mais le plan de récupération après sinistre, il faut à un moment donné le tester.

2:37:02

Dans un scénario ou peut être si on a un vrai sinistre, on peut le tester très souvent. Les tests souvent sont pas bien faits je reconnais, mais il y a quand même des stratégies qu'il faut utiliser et il y a des des des différents types de tests qu'on peut utiliser et dépendamment du type de test, Ben ça peut nous dire si notre plan tient ou notre plan ne tient pas. Donc dépendamment de l'efficacité ou de la rigueur du test, ça peut nous donner une idée sur.

2:37:31
Nos tests sur la l'efficacité de nos tests donc le premier type de test c'est la vérification de la liste, donc on appelle check list sur Youtube, donc qu'est ce qu'on fait ? Ça c'est c'est sur papier qu'on teste, donc on a un plan de relève, on a la distribution du plan et vérification par les gestionnaires, donc c'est juste un papier, on dit OK, nous on a dit Quand on aura un sinistre, voici par quoi on commence, voilà, on va commencer par régler les services, on va relever.

2:38:00
Les les les bases de données, on va rélever telle aspect, telle telle telle application et en autre donc ça on aura les check lists qu'on va tester, c'est déjà bon, c'est déjà un bon, un bon début. Si on fait déjà les les vérifications de la liste check list review c'est déjà bon ou bien on fait les validations manuelles donc on appelle structure workflow. Donc ça sera des tables top qu'on va faire. Donc on va faire la révision du plan en groupe, on va prendre les différents acteurs, on va faire des jeux de rôle, des scénarios, des réactions, mais c'est sur papier toujours.

2:38:29
Donc on va dire OK en cas d'attaque, toi tu es, tu es l'expert en communication. Le journaliste interroge, qu'est ce que tu vas dire ? Va parler OK toi tu es le respect en cybersécurité qu'est ce que tu fais ? Donc on va partager les scénarios et voir, est ce que les gens réagissent bien ? S'ils réagissent pas bien on va s'améliorer mais ça c'est pas encore le test pratique. On a ensuite la simulation qui est réalisée avec des équipes et des services du test, donc un simulé dans un environnement.

2:38:58
Au site de relève donc le scénario et puis réaction des liquides. Donc là en ce moment on commence à rentrer dans un test réel, on va aller simuler réellement si notre site ne fonctionne pas, mais on va pas arrêter le site, on va juste aller tester. Ensuite on va faire la simulation parallèle, donc dans la simulation parallèle on va réaliser avec les équipements et les services de production, donc les services en production fonctionnent au site de relais, donc on va faire en sorte que on a nos systèmes qui fonctionnent de part et d'autre, donc que ça soit dans notre premier sur notre premier site.

2:39:27
Ou sur le site de relève. Ensuite on a le test complet dans l'interruption qui est le full full interruption test donc qu'est ce qu'on va faire ? Tous les services sont fermés, tous les systèmes de production fonctionnant aussi souvent fonctionné aussi sur le site de relève donc on va vraiment tester en cas réels si on a un destas est ce que notre site de secours est un bon site de secours ? C'est comme tu as ton piné secours et puis ton piné secours, il est dégonflé, tu l'as jamais testé donc.

2:39:52
Faut souvent regarder ton pinus eko pour voir est ce qu'il est gonflé donc c'est c'est un peu ça le même concept donc on va regarder est ce que le pinus secours est gonflé donc on va souvent tester le site, est ce que le site le le site des relèves est fonctionnel très souvent. Moi je vois beaucoup de tests tests parallèles ou les ou les simulations, les simulations ou les simulations parallèles, mais bon

rarement des il y a souvent des tests complets d'interruptions, mais on va le faire souvent sur certains systèmes.

2:40:22
Pas arrêter, pas prendre tout le je veux dire tout l'environnement au complet. Donc il y a plusieurs stratégies que les gens vont utiliser donc c'est la meilleure façon d'utiliser le le plan est ce que le plan fonctionne ? Donc plus de risques sur les systèmes de production donc de jamais débuter par ce type de test. Donc il faut vraiment arriver à un certain niveau de maturité avant d'arrêter tout ça avant avant de d'arriver à ce full interruption de tests.

2:40:52
La limite des tests c'est que aucun test n'est comme la réalité. Donc comme j'ai donné l'exemple tantôt de du pneu secours, oui tu peux regarder ton pneu secours, ça t'a l'air gonflé, mais quand tu auras besoin quand tu vas le regarder tu vas voir qu'il n'est pas gonflé. Donc aucun test n'est comme la réalité. Donc les exercices d'évacuation en cas de feu, oui il y a l'alarme qui sonne les gens en cours, mais il y a des personnes qui savent que c'est pas c'est un test, c'est pas un vrai.

2:41:20
Il y a pas d'incendie réellement, donc souvent les tests aussi coûtent cher. Donc si vous faites une full interruption, Ben ça va coûter beaucoup plus cher. Mais minimalement il faut quand même. Même si c'est du check list review, il faut quand même arriver à un à un moment de tester votre plan de votre plan de d'hier pour vous assurer en cas de d'incident ou en cas de désastre que vous êtes capable de. Vous avez quand même quelque chose en place qui fonctionne ensuite les éléments auxquels on doit faire attention. Donc pas d'intégration des plans à la gestion du changement.

2:41:50
Donc des fois on n'intègre pas le plan. La gestion des changements, c'est un plan qui est qui est fait indifféremment de d'une gestion des changements. Donc on aura des changements aux infrastructures et à l'environnement, des logiciels, matériels, applications et des personnes. Ensuite la discussion de nouvelles versions. Toutes les anciennes copies doivent être détruites. Donc si on a des nouvelles versions, il faut donner la la nouvelle version du plan.

2:42:20
Au moins 3 copies de plan doivent être existées, donc pour annotation en cas d'urgence sur les sites et puis avoir un plan hors site. Ensuite, on doit avoir un plan imprimé parce que, à un moment donné, si on l'a dans l'ordinateur, tout peut être bloqué. Ensuite, il faut avoir les informations sensibles basées sur le besoin de savoir et avoir la connaissance de tout le plan.

2:42:47
Exercice de continuité d'activité. Donc on a parlé de plan de de désastre tantôt. Donc si on a le deer, le disaster Recovery, on maintenant on va parler des exercices de continuité des activités. La continuité des activités elle elle va un peu au-delà de de plan de désastre qui peut être peut concerner juste les les équipements.

2:43:13
Mais le plan de continuité c'est toute la stratégie sur les activités qu'on a, est ce que les activités qu'on qu'on mène sont, qu'est ce qu'on doit relever en premier, par quoi, par quel service on doit commencer, quels sont les éléments clés qu'on doit utiliser ? Donc ça le plan de continuité va définir tout ça et avec l'exercice de plan de continuité on pourra savoir ces différents éléments là, donc quels

sont les déclencheurs d'un plan de continuité ? Donc autant on a un plan de désastre, on a un plan de continuité également, donc ça peut être des changements de personnel.

2:43:43
Ça peut être le changement de processus métier. On va voir. Est ce que notre plan de continuité fonctionne ? Changement technologique, changement dans les priorités commerciales, les règlements, s'il y a une nouvelle loi et autres, les résultats d'incidents passés, les recommandations d'audit, les résultats des tests et exercices. Donc un plan de continuité peut prendre en compte le tout ce que on a vu comme désastre et tout ce qu'on a vu comme stratégie de restauration. Donc dans un plan de continuité on va voir ces différents éléments là.

2:44:13
Des fois vous allez avoir un plan de désastre qui est différent d'un plan de continuité. Mais le plan de continuité à un moment donné va faire appel au plan de désastre suite on a la gérer la sécurité et puis les problèmes de sécurité, de sécurité on va, on vous laisse quelques minutes. Ben la sécurité Ben on va s'assurer de contrôler le le périmètre interne.

2:44:40
Donc nos stationnements, nos bâtiments, les accès, il y aura des zones auxquelles on n'accède pas les les, les locaux, les armoires doivent être bien hermétiquement fermés et que quelques personnes doivent avoir accès. Les zones, tout le monde ne doit pas accès. Accéder partout nos salles serveurs, ça sera juste les admins ou des personnes qui sont censées accéder, qui doivent accéder. Et puis pour la sécurité physique, tout le monde doit être comme des des gardiens.

2:45:07
Donc, si vous constatez dans votre entreprise des déplacements inhabituels, Ben vous devez signaler à l'équipe de sécurité. Il peut arriver souvent que des personnes peut être qu'ils font le nettoyage puisqu'ils nettoient. Souvent dans certaines salles, ils accèdent aux salles, mais c'est souvent s'assurer qu'ils ne dépassent pas un certain nombre de temps parce que on sait pas ça peut être quelqu'un qui veut vous pirater, qui s'est transformé en nettoyeur de votre salle. Donc il faut être en alerte. Et puis tout le monde en entreprise.

2:45:37
Doivent être vigilants sur ces aspects-là les problèmes de sûreté. Donc tantôt je disais les employés sont les cibles les plus faciles en déplacement, donc s'il y a un enjeu, Ben c'est les employés. D'abord. Des données sensibles, éviter de conserver sur les dispositifs des utilisateurs, il faut toujours les chiffrer des logiciels malveillants et surveillances dont on peut avoir des pilatages physiques. On peut se protéger en utilisant des appareils temporaires.

2:46:04
Des fois le Wifi gratuit c'est à éviter si vous partez dans les bibliothèques éviter et le café autant que faire ce que peut utiliser le wifi public parce que souvent c'est pas trop sécurisé. Les VPN pour les accès à distance on recommande toujours de les avoir. Ensuite on recommande de faire la sensibilisation donc les utilisateurs seront toujours les plus grands, le plus grand risque de l'organisation donc comme je l'ai je l'avais dit en cas de danger.

2:46:33
Ben c'est les utilisateurs qu'on protège le premier. Ensuite, la mise en place d'un programme efficace de sensibilisation. Donc on va, on fait la sensibilisation à la sécurité, pas juste pour l'aspect de d'un

mot de passe ou de l'utilisation des actifs. Mais aussi on fait les la sensibilisation aussi pour la sécurité physique également.

2:46:56
Donc on va donner des principes, des principes, des des principes directeurs pour protéger l'organisation, pour que les utilisateurs soient informés et s'assurer que les employés soient au courant des pratiques de sécurité lors de leurs déplacements, que ça soit les voyages ou qu'ils soient dans des cybercafés, c'est tout pour aujourd'hui. Est ce que vous avez des questions ? Est ce que vous avez des suggestions ? C'était le premier cours, je sais pas.

2:47:24
Trop à quoi vous étiez habitué avec Dominique ? Donc est ce qu'il y a des suggestions pour l'amélioration pour le prochain cours ? Le prochain cours ça sera donné par David Sami mais après on se retrouve pour la suite des cours sur la communication réseaux et autres. Est ce qu'il y a des suggestions ? Questions plaintes ça va c'était correct OKOK, oui c'était bien OK.

2:47:54
C'est bon c'est bon d'accord. Donc oui j'ai oui c'est une question à propos de la configuration des disques. Aussi la notion de KVM configurer avec KVM est ce que c'est une bonne pratique ou bien non KVM je sais pas hein c'est quoi. J'ai dit KVM c'est de de configurer le disque en utilisant le configuration.

2:48:23
Par KVM, les les KVM c'est qu'est ce qui c'est ? Qu'est ce qui permet à mettons de mettre sur une même boîte la gestion ce d'ordinateur ou de savoir puis t'as juste à appuyer sur un piton pour modifier c'est comme un sélecteur là OK puis t'as puis t'as des KVM qui qui se vendent.

2:48:44
Ben comme moi par exemple j'ai une j'ai une KVM mais genre juste matériel mais t'as certaine KVM que t'as des configurations logicielles là non mais il y en a, il y en a un carnet Virtual machine aussi qui est sur Linux aussi, c'est des KVM aussi. Ah.

2:49:01
On appelle ça que la virtualisation servait drive des affaires comme ça oui KVM c'est la virtualisation c'est comme VM ouais mais c'est une solution. OK j'avais l'ancienne OKOKOK je te parce que des des petites machines c'est lecteur physique, on appelle ça aussi des KVMOK je connaissais pas. Non non c'est vous, vous venez de m'apprendre quelque chose mais merci hayette est ce que tu n'es pas mieux de lecture hayette s'exprimer ?

2:49:29
Qu'est ce qu'elle veut ? Oui vas y ouais sur le KVM oui vas y vas, y va, y vas y le KVM c'est la façon de configurer un disque dur, par exemple si on utilise des Red c'est la façon de répliquer les données, le système, les KVM, ça veut dire désolé la machine complètement en dans un système virtuel c'est de créer un disque isolé par rapport à l'autre, mais est ce qu'on récupère de dans ce cas là ? Est ce qu'on récupère les données quand il y a des pertes ou bien ?

2:49:59
Est ce qu'il y a une manière de je ne sais pas ? OK, Tu tu parles de une machine virtuelle qui est sur un un support physique ? Si comme par exemple si je donne l'exemple d'open source comme xane un

serveur xane c'est si on on peut par exemple configurer le serveur pour la création des machines virtuelles en utilisant par exemple une configuration avec le KVM au lieu de Red.

2:50:30
C'est ça le le le raid là c'est vraiment au niveau physique hein, au niveau des disques durs, est ce que le KVM dont toi tu parles là c'est sur la couche application ? Non c'est la couche disque aussi, c'est la couche c'est la couche disque OKOK je je connaissais pas, je vais je vais regarder et puis peut être la séance prochaine je je vais faire mes recherches et puis te revenir d'accord merci t'inquiète t'as je suis autant dépassé de toi là.

2:50:58
C'est ça je je vais faire mes recherches et puis on revient, on finit pas d'apprendre hein. Le monde informatique est tellement vaste que tu découvres des choses tous les jours. Oui vas y Lucien. Oui juste une petite question là sur la page 78OK la dernière ligne.

2:51:18
On a parlé de la connaissance de tout le plan entre parenthèses restreint. Est ce que c'est pour dire que on doit garder secret au fait le plan de reprise là qu'on a mis en place ? Oui oui plan de reprise, oui c'est secret, c'est secret dans l'organisation, oui c'est c'est bon, dans la classification peut être on pourrait le mettre interne, ça va dépendre mais c'est pas tout le monde d'abord qui a accès à ça dans l'organisation ?

2:51:46
Parce que ce que tout le monde sait en fait, c'est si tu veux, c'est votre stratégie, comment vous remettez les choses. Donc s'il y a quelqu'un, même dans l'organisation, qui est contre vous, il sait comment il sait votre stratégie. Donc c'est pas des documents. C'est vrai que quand on travaille là-dessus, il y a beaucoup de brouillons qui circulent entre des personnes, mais une fois qu'on a la version approuvée, ça c'est pas visible, on le donne pas à n'importe qui, d'accord ?

2:52:13
Maintenant de ça, euh oui c'est bon c'est bon euh tu disais au début ou bien avec un moment-là qu'on a un cuivre à faire, euh donc euh je voulais comprendre ce que c'est pour parler, on fait le cuivre ou bien ? Non le quiz c'est pareil hein, je pense que vous avez 5 ou 7 5 jours, je sais pas trop. En tout cas on m'a dit que vous avez 5 jours pour faire le quiz après chaque cours. Je crois que vous avez des quiz mais vous avez 5 jours pour faire, j'ai pas le nombre de jours, j'ai pas regardé.

2:52:42
Le Moodle Exam mais je sais que vous avez un quiz. Après oui oui effectivement, on fait souvent des questions, c'est 5 jours, c'est ça ? Vous avez 5 jours pour faire le quiz, donc vous avez tout le temps pour réviser. Et puis dès que vous êtes prêt, vous allez faire votre quiz. Mais à date, ça se passe bien hein ? Vos quiz c'est bon, ça se passe bien, OKOK.

2:53:07
C'est bon c'est bon de toutes les façons, mais j'espère que vous tous vous voulez passer votre CISSP réellement hein. Après le cours vous allez vous préparer pour passer votre CSSP Monsieur j'ai une question, oui y a est ce que si l'on veut de passer le le les certificats CSSP comme par exemple on n'a pas expérience de travail, est ce que vous vous me conseillez de le faire après ?

2:53:36

Après avoir une expérience de travail ou bien même si maintenant on pourra le passer c'est bon. C'est vrai que quand t'as pas l'expérience quand on dit expérience ça ça dépend aussi hein. Quand t'as pas toute l'expérience des 5 ans d'expérience avec le Bachelor ou le master je pense que tu peux gagner un an ou 2 ans donc après après il va te rester peut être 3 ans d'expérience pratique en sécurité pour valider mais.

2:54:04
Oui c'est 5 ans, mais tu as des Rivers de un an, 2 ans, Dépendamment de tu as une maîtrise ou un Bachelor, mais quoi que à la fin quoi ça Allô, il y a quelqu'un qui qui qui parle, t'as des 90 aussi crédits qui viennent avec le Bachelor aussi que tu peux le faire comme tu viens de dire Ouais c'est ça donc donc il va te rester peut être 2 ans ou 3 ans donc si tu as 2 ans en toi tu as 3 ans ou 4 ans en sécurité. Moi je te conseille va faire ton CSSP.

2:54:33
Maintenant si tu n'as pas fait, si tu n'as pas d'expérience, il y a quand même tu peux passer le CSSP mais ils vont te donner. J'ai j'ai pas le nom de la certification, ils vont te donner mais tu n'auras pas le CSSP. C'est vrai qu'on le on le passe plus au Québec ici il faut aller peut être en Ontario, mais pour moi quelqu'un qui passe le CSSP qui a l'examen, si moi je dois embaucher quelqu'un, moi je le prends parce que je me dis qu'il comprend c'est quoi la sécurité déjà il connaît le concept, je n'ai pas à lui expliquer.

2:55:03
En tout cas il y a des choses que j'ai pas à lui expliquer, il comprend c'est quoi la sécurité ? Donc tu dès que tu as ça ça te permet. Après quand tu vas valider tes expériences tu pourras avoir maintenant si tu veux rentrer dans le domaine est ce que c'est le CSSP ? Parce que le CSSP c'est plus côté leadership aussi de la sécurité. Donc tout ce qu'on a vu qu'est ce que c'est vraiment discuter au niveau de de ceux qui gèrent la stratégie de la sécurité au niveau tactique donc c'est pas au niveau opérationnel.

2:55:30
Donc est ce que toi tu veux rentrer dans le domaine sous ? Tu veux juste rentrer en gouvernance sans expérience est ce que c'est possible ou tu rentres en sécurité opérationnelle pour commencer ? Moi je dis tu as plus de chance de commencer en opérationnel qu'en gouvernance donc va chercher des éléments d'autres certifications. Si tu fais le CSS c'est bon Ben va chercher d'autres certifications qui te permettent de commencer en opérationnel et puis après un an 2 ans tu pourras balancer en gouvernance.

2:56:00
Je crois que il y en a qui commencent aussi directement en gouvernance hein. Il peut commencer en junior, en analyse, en en conformité et puis évoluer aussi. Mais si tu as l'expérience, si tu as déjà 3 4 ans, 3 2 ans, 3 ans en sécurité, moi je te dirais va faire ton CSSP faut même pas réfléchir 2 fois merci merci beaucoup. Est ce qu'il y a d'autres questions ?

2:56:28
Est ce que il y a d'autres questions ? Est ce que la plupart d'entre vous vous êtes travailleur étudiant à temps plein ? Est ce que parmi vous il y a beaucoup qui sont étudiants ? On on est travailleur mais pas pas peut être spécifiquement en sécurité OKOKOK mais la plupart des concepts là sont des concepts d'entreprise dans le monde informatique on comprend la question c'est est ce que les expériences qui sont pas ciblées spécifiquement à à une fonction de sécurité ?

2:56:55
Mais qu'on on comprend quand même pas mal de choses, que ces gens-là sont aussi éligibles pour aller passer l'examen, c'est ça ? Ouais ouais en fait il y a plusieurs domaines je crois. Il y a 8 domaines en CSSP et souvent on va te demander, est ce que tu as eu de l'expérience dans des domaines ? Donc peut être ton type de poste peut ne pas être sécurité mais si tu as travaillé dans les domaines, par exemple ceux qui font du développement d'applications, il y a un domaine qui s'appelle le SDLC. Donc si tu appliques la sécurité ça peut être tu peux aller chercher des expériences avec ça.

2:57:25
Donc on va combiner certains domaines, peut être la, la gouvernance, la sécurité opérationnelle. Il y a des gens qui sont dans l'administration système mais qui font beaucoup de sécurité, donc eux ça sera facile pour eux après d'aller chercher ces expériences là pour valider. Donc si tu es dans un domaine que ton titre n'est pas forcément sécurité, ça veut pas dire que t'es pas éligible. Faut vraiment regarder les conditions.

2:57:49
Pour pouvoir valider en fait le après avoir eu l'examen bien sûr pour valider l'obtention de la certification c'est bon OK s'il y a plus de questions je vais vous laisser merci beaucoup. Et puis bonne soirée à vous. Bonne soirée, merci bonne soirée.

INF813-Séance09-20250611-PA01

0:03
Non pour l'instant il y a rien eu, je suis juste connecté, je me suis pas présenté, j'ai rien fait, j'ai juste partager mon écran. Ok c'est bon est ce que tout le monde voit l'écran de de David ? Oui on voit le module 3. Oui c'est bon ouais moi je vois. Oui OK donc parfait. Aujourd'hui séance 9, on va parler de cryptographie.

0:26
Donc on ça sera fait par David David Samit, il va se présenter tantôt, il va donner plus d'informations sur lui. En fait, c'est quelqu'un qui travaille dans la cryptographie depuis longtemps. Et puis on s'est dit que ça allait être une une meilleure personne pour parler des cryptographies, l'historique et puis les les détails sur la cryptographie, ça va nous permettre, vous et moi, d'en apprendre davantage sur la crypto. David, vas y, il va, il va utiliser toutes les les 3 h donc.

0:55
On aura, on aura un ou 10 min de pause comme d'habitude. OK, donc avant tout faut rendre à César ce qui appartient à César. Donc merci Dominique Brodeur de m'avoir proposé cette intervention et puis merci à tout le monde boudoulaye qui m'ont proposé ça. Les slides ne sont pas 100% à moi, ils viennent de Monsieur tardif et de Mihaye qui les avait fait avant moi. Je les ai juste modifié, mis à ma sauce.

1:23
Mais je n'en revendique pas la paternité donc c'est pour ça que je dis légèrement adapté par mes soins si vous voulez me contacter. Après si vous avez des questions vous avez mon email. David. Samy at gmail.com n'hésitez pas. Vous pouvez aussi me demander sur LinkedIn si vous voulez pas m'envoyer d'e mail ou quoi ? J'ai pas une empreinte très large sur le web à dessein. C'est pas que je sais pas utiliser les réseaux sociaux c'est juste que j'en veux pas.

1:47
Donc Email je vous conseille quand même de mettre crochet Sherbrooke crochet au début de votre titre parce que sinon ça va passer dans le grand nombre d'emails que je vous vois pas passer et vous allez être frustré que je vous ai proposé 2 et que ça c'est jamais arrivé et vraiment vous avez besoin qu'on se rencontre en présentiel ? Je travaille pour des jardins au complexe des jardins. Je m'occupe de leur cryptographie architecte entre entre le projet et le le domaine.

2:17
Et donc un soir ou un 12h00, c'est avec plaisir. Si vous avez des questions, on peut se rencontrer de visu, prendre un café et discuter de cryptographie. Voilà, Ceci dit, maintenant c'est un cours. Normalement, j'ai commencé à l'enseigner il y a. J'ai commencé à enseigner ça en 98, donc ça fait plus de 25 ans.

2:42
Petit mot d'humour, l'astrophysique expliquée de manière simple et à droite, la crypto expliquée de manière simple. C'est un cours sur lequel on pourrait faire sans mentir 35 à 40 h de cours et ce serait encore assez dense aujourd'hui, on a 3 h, donc vous imaginez que comme l'enseignement MIT, on vous dit, c'est l'équivalent d'essayer de boire à la sortie de la pompe à incendie. Il y a un petit peu de pression et ça va arracher.

3:08
Il y a un programme au niveau de CSSP, c'est pas moi qui l'ai établi, il va falloir qu'on couvre tout donc en avant. Alors maintenant oui, je, je suis Français, vous l'entendez sans doute à mon accent, personne n'est parfait. Qu'est ce que je connais à la crypto ? Je suis tombé dedans en 1992. Étude de technicien d'ingénieur double compétence électronique informatique, master en microélectronique, master en algorithmie et cryptographie.

3:33
J'ai fait ma thèse de doctorat sur les canaux latéraux, c'est à dire comment Piquer Hinkley, un système qui fait de la crypto. Tous les coups sont permis. Je l'ai jamais défendue, mais elle était classée, enfin je l'ai jamais défendue publiquement, je l'ai défendue en privé, elle a été classée parmi les 4 meilleurs au monde à l'époque y a 20, ouais, plus plus de 20 ans de ça et qu'est ce que j'ai fait comme parcours industriel industrie ? J'ai travaillé dans de la petite boîte, j'ai travaillé dans de la start-up, la dernière a été vendue à Apple, on était ici à.

4:03
À Montréal, elle était vendue à Apple pour 120000000 de dollars. J'étais responsable de la sécurité. C'est ce qui a permis à Apple de faire TAP to pay, c'est à dire lire de la carte sans contact sur un téléphone. Je suis passé chez Intel en tant qu'architect hardware, je suis passé chez Microsoft en tant que architect Software mais dans le cloud, donc double compétence. Et puis j'ai fait d'autres boîtes de fortune, 500 broadcom very Phone, enfin bon.

4:33
J'ai j'ai travaillé en France, Belgique, Angleterre, États-Unis, Australie et Canada donc j'ai un petit peu fait le tour du monde et j'ai travaillé dans des petites et des grandes boîtes. Donc si vous voulez qu'on parle de maths, on peut le faire. Je suis le genre de personne qui peut prendre le stylo et on peut faire des maths pendant 4 h si vous voulez. Mais je pense pas que c'est ce qui va vous amuser ici. Donc allons y. On est sur un domaine qui va être quand même assez intense. Le chemin le plus court c'est pas forcément la ligne droite.

5:02
Pas sur une boule, pas sur terre. Donc ici c'est du XKCD, le Laptop est chiffré et on pourrait monter 111 cluster d'un 1000000 de dollars pour le casser. Ah non c'est du RSA 4096 on peut rien faire. Bon Ben pourquoi on fout pas des drogues aux mecs et on achète une clé à 5,00$? On lui fout des grands coups sur la tête, il va nous donner le password ?

5:26
Très réaliste, très réaliste, on va pas parler ici, on va je suis pas Member de dépôt donc je m'y connais pas en clé. Par contre on va parler de cluster du 1000000 de dollars et comment attaquer de l'autre côté, ça veut pas dire que je vais essayer quand même de rester réaliste dans un certain nombre de choses. Ça veut quand même pas dire que de temps en temps si vraiment vous voulez l'atteler c'est pas mieux de pour se reposer sur l'erreur humaine ou simplement l'atteler en grand coup de clé à molette et 5$ mais.

5:55
Je suis pas là pour vous apprendre à être des brigands, je suis là pour vous montrer comment on fait de la Crypto, donc on va rester dans la partie de gauche d'accord plan de séance, on va parler de solutions cryptographiques forcément, de cycles de vie, de clés d'algorithmes, de méthodes de

cryptographie, de non répudiation. Donc une signature, qu'est ce que c'est, qu'est ce que c'est que le les fonctions de HH quels sont les prérequis de la signature ? Qu'est ce que c'est qu'une infrastructure avec les publiques, une PKI en anglais, quelles sont les bonnes pratiques de gestion ?

6:24
Pour les signatures et les certificats donc on va couvrir ce qui est pardon ce qui est requis pour votre CSISSP. On va parler d'attaques donc des attaques par force brute et pourquoi c'est limité. Des attaques ça a été chiffré uniquement c'est à dire le cas le plus connu c'est les gens qui ont juste écouté le résultat de ce qui est passé sur le canal d'accord. Donc ils ont obtenu juste les chiffrés d'attaques texte entre les reconnues.

6:50
Bah si je peux avoir le texte En clair avant le chiffrement et le texte chiffré, qu'est ce que je peux faire ? Un exemple, c'est les Allemands qui chiffraient les bulletins météo pendant la 2e Guerre mondiale. Bah c'est pas si malin que ça parce que il suffit de lever le nez. Et puis la météo elle est au-dessus de nous hein. On la voit donc le bulletin météo on a quand même une bonne idée de ce qui s'y passe et donc dans ce cas-là on a quand même une très bonne idée de l'entrée avant la crypto et de la sortie.

7:15
De la même manière, si vous terminez tout le temps par highlitler et que on vous envoie un porte mine poser des mines dans un port, on s'attend à ce que le commandant de port envoie avec sa machine de chiffrement un message en disant, Attention machin nanana mine. Donc y a déjà des mots qu'on connaît, il va pas dire canari ou lavabo, il va parler de mine le gars, et donc ça peut aider d'avoir des attaques. Un texte En clair connu.

7:39
L'analyse de fréquences alors ça je vous l'expliquais tout à l'heure. C'est la répartition des fréquences dans les langues et en fait les lettres ne sont pas probables donc ça permet de faire des attaques. Texte chiffré choisi Ben j'ai accès au texte En clair et je peux choisir un chiffré de manière.

8:04
Allô, on va la chiffrer et puis on va changer. Oui Allô David, on t'a perdu 10 secondes, on m'a perdu 10 secondes. Texte chiffré choisi, texte chiffré choisi je disais c'est, on va choisir des textes chiffrés, mais on aura accès aux textes En clair, d'accord, et on va pouvoir essayer de regarder de ce fait là ce qu'on peut attaquer la cryptanalyse différentielle, cette fois-ci, c'est que pour un même algorithme.

8:31
On va rentrer quelque chose, obtenir sa sortie, donc un texte En clair, obtenir un texte chiffré et on va regarder ce qui se passe. Si le texte en entrée a un tout petit changement, quel est l'effet sur la sortie ? S'il y a un tout petit changement cryptanalyse linéaire, alors je vous parlerai tout à l'heure des boîtes S et on parlera des probabilités en sortie de boîte S et comment on arrive à retrouver la clé. Alors après tout ça, c'est gentil, c'est des attaques mathématiques, ce sont des attaques où.

9:00
On va vous dire ça casse si on a, si jamais on a des questions, on peut les poser ? Oui oui oui, si vous avez des questions, vous m'interrompez. Si par contre je vois que votre question je vais la traiter plus tard, je vous le dirai. Au pire, si elle est vraiment trop latérale, on la traitera au moment de la pause. Moi je prendrai pas de pause, je répondrai aux questions s'il y en a et.

9:23
Oui n'hésitez pas à m'interrompre poser des questions comme je vous dis, c'est pas mon premier cours. Donc j'ai réagencé le cours dans un sens où je vais essayer de de vous retirer de la tête les les les cas les plus classiques. Mais oui bien évidemment, c'est tellement dense que vous aurez des questions donc.

9:46
On peut avoir des attaques qui sont des attaques mathématiques sur lesquelles il vous faut des milliards de milliards de puissance, 60 textes chiffrés, textes En clair, coupe machin. Mais il faut aussi avoir des attaques sur l'implémentation parce qu'à un moment il faut que ça tourne. Faut que ce soit dans une puce, faut que ce soit dans une boîte. Est ce que si je regarde la température, est ce que si je regarde la consommation, est ce que si je regarde le rayonnement est ce que si je regarde le temps utilisé je peux réussir à vous piquer la clé ? Et puis si je peux pas avec tout ça, est ce que je peux secouer le système ?

10:15
De manière à ce qu'il y ait une fuite de manière à ce qu'il fasse une erreur, de manière à ce que au final il me donne un résultat faux mais qu'en utilisant des structures mathématiques derrière j'arrive à extraire pâte les vous avez également des attaques par rejet. Est ce que je peux prendre un truc qui est passé chiffré il y a quelques temps ? Le remettre au milieu ? Est ce que ça passe ? Est ce que je peux faire des maths et utiliser des structures algébriques pour essayer de casser le système ?

10:40
Attaque analytique, est ce qu'y a des failles structurelles dans votre algo puis les statistiques, est ce que vos générateurs aléatoires sont bons ? Est ce que vous avez un poids de hamming ? Le poids de hamming, c'est le nombre de un dans un mot qui est équilibré, est ce que vous avez à peu près autant de un que de 0 ? Est ce qu'y a des biais ? Voilà ça c'est le genre d'attaques dont on va parler aujourd'hui, alors on parlera également d'injection de fautes, pourquoi c'est très efficace, de séquences de l'attaque de l'homme au milieu, Man in the middle en anglais donc comment chaque côté se fait abuser ?

11:10
Comment parfois ? Ben c'est pas nécessaire de choper par exemple le mot de passe, le HC alors on verra ce que c'est que le h mais le h le condensat ou le die just du mot de passe qui sont la même chose en français ou en anglais suffit pour faire des mauvais coups ou suffisait pour faire des mauvais coups. Chez Microsoft on parlera un petit peu de kerberos, mais je pense que on aura pas trop le temps d'en parler tellement on a d'autres choses à faire. Et puis on parlera un petit peu de rançongiciel, cette idée qu'a eu moty Young, très grand cryptographe.

11:39
Qui a dit Ben un jour vous allez voir, on a maintenant tellement de vitesse en crypto que il y a des gens qui vont faire des faire des virus, ils vont faire des trucs qui vont chiffrer vos contenus de données, vous allez pas le voir parce que Ben ils vous laisseront passer. Tout est chiffré. C'est comme si quelqu'un venait et mettait une une barrière autour de chez vous, puis un beau jour ils ferment la barrière, vous voulez rentrer, vous voulez sortir, vous devez payer. Maintenant ça s'appelle un PH.

12:03
Mais là c'est pareil, vous avez accès à vous donner jusqu'à ce qu'ils vous disent Ben en fait vous vous

êtes pas rendu compte, mais on les a chiffrés maintenant. Ben si vous voulez vous me devez de l'argent quoi. Alors j'aimerais qu'on discute probabilité et quantité parce que probabilité quantité également qu'on discute après de puissance de calcul et de puissance de 2 de taille. Donc est ce qu'il existe un d à une face parce que.

12:30
Est ce que forcément une surface à 2 côtés ou est ce qu'il y a un truc qui a un seul côté ? Est ce que ça existe ? Bah c'est le ruban de mobius ruban de Mobius il a qu'un seul côté donc c'est le vous irez voir sur en ligne un ruban de mobius c'est prenez le ruban, vous le vous le tordez de bas en haut et vous le reconnectez sur lui même, ça a qu'un seul côté, donc là de toute manière si vous le lancez 100% vous tombez du bon côté.

13:00
La pièce c'est on commence à dire probabilité que j'ai des jumeaux, Ben c'est une chance sur 250 en moyenne vous allez me dire Ouais mais bon 250 c'est pas beaucoup donc quelle est la probabilité que vous trouviez le bon cheveu sur ma tête ? Oui, on parlera cryptoposquantique à la fin. Le bon cheveu sur ma tête c'est une chance sur l'ordre de 10000. Mourir foudroyé c'est une chance sur 1000000. Gagner le premier rang du loto, c'est une chance sur 13000000.

13:29
Être mangé par un requin et décédé, c'est une chance sur 264000000. Alors vous me dites oui mais si par exemple je prenais une cellule dans le corps humain ? Ben là on est sur du 3,7 10 puissance 13, on est sur des dizaines de milliers de milliards de cellules dans le corps. D'accord, vous avez dû passer en en j'allais dire au lycée comment on appelle ça High School.

13:58
Et on vous parle du nombre d'Avogadro 60210, puissance 23, la Mole en chimie, Ben la Mole, pour vous donner une idée, c'est à peu près du même niveau que de dire j'ai une goutte d'eau cherche à trouver l'atome dedans. D'accord, si maintenant on parlait des on parlait du nombre d'atomes dans le corps humain, je dis atome et pas cellule. On est à 10 puissance 27, Ben énumérer 10, puissance 20 27.

14:26
Pour que vous ayez une idée, c'est à peu près ce que les Américains sont capables de faire avec la NSA qui est l'agence de renseignement qui est encore plus grosse que la CIA. Leur puissance de frappe, elle est à peu près à 10 puissance 27. Je vous montrerai tout à l'heure pourquoi alors 10 puissance 50 par exemple, c'est l'entropie d'un trou noir, on joue le parc kelvin, 10 puissance 100 c'est le Gogol, donc 111 avec 100 0 derrière et 10 puissance 104 c'est l'entropie de l'univers. D'accord, donc ça c'est pour vous donner une idée, donc gagner.

14:55
Au premier rang, le loto en étant foudroyé en même mettant qu'on est mangé par un requin et qu'on a les jumeaux en crypto c'est commun ce genre de probabilité. Pourquoi ? Parce qu'elle est pas si énorme que ça si vous voulez quand vous avez des machines qui calculent très très vite on on va tout essayer. Donc parlons un petit peu de puissance de 2 de puissance 10 c'est le kilo.

15:21
Ouais c'est le Gogol 10 puissance 100 c'est le Gogol c'est d'où ? C'est de là que Google prend son nom hein Google ils se sont dit Oh indexer tout le web machin ça va être énorme, ça va demander à un gogol c'est de là que Google vient donc bah je vous quoi que je vous dise Je vous invite moi je vais

pas le faire là parce que mon écran est partagé mais en ligne vérifiez ce que je dis hein donc 2 puissance 10 c'est le kilo, à l'époque c'était alors stockage c'était de la puce ouais.

15:46
De puissance 20 c'est le méga donc là vous avez un gars qui qui qui qui tenait à l'époque un un disque dur IBM pour main frame c'était du méga giga. Ben c'est ce que vous avez aujourd'hui sur votre disque dur. Alors que vous ayez 10, 20, 30, 40 ou 100 giga tant que vous n'avez pas des milliers qu'on n'est pas passés au tera. Pour moi c'est pareil hein. C'est l'ordre de grandeur tera, mais c'est pareil. Vous avez encore ça sur de la carte micro SD, sur du disque et ainsi de suite.

16:14
Alors derrière ils sont dans mes notes, je les connais plus par cœur mais derrière vous avez alors kilomega Giga Terra PETA Hexa ça doit être du yotazeta je pense. Allez voir. Alors depuis 156 donc il y a un algorithme qui s'appelle DESS que je vais vous présenter tout à l'heure depuis 156 et une recherche exhaustive sur la taille de la clé. Ben c'est.

16:43
Aujourd'hui, quelques minutes de calcul. Quelques dizaines de minutes de calcul avec quelques dizaines de milliers de dollars sur votre bureau. 2 puissance 60, c'est ce qui a été fait. C'était 10000PC au CERN quand on a calculé le poids du du boson de Higgs, y en avait 3 en moyenne qui tombaient en panne tous les jours. Machin, na, na, na. Donc c'est des trucs qui sont encore atteignables par des grosses entités. Mais depuis 162 par exemple, on considère que c'est.

17:12
La quantité de hachage par 2nde qui est faite pour Bitcoin au niveau mondial. Je vous ai mis la courbe en dessous pour que vous ayez une idée de comment ça évoluer. 2 puissance 80 à 2 puissance 90 on pense que c'est la puissance de la NSA s'ils mettent toutes leurs machines sur la table. Pourquoi je sais que personne a fait du bruit de force à 2 puissance 128 ? Parce que je suis allé ouvrir Maps et que la Hollande est pas encore sous l'eau. Si on l'avait fait, on aurait dégagé tellement de chaleur que à priori on aurait fait fendre des pôles.

17:40
Et que le premier pays qui aurait disparu serait la Hollande. Vous allez me dire ça explique peut être du réchauffement climatique, y a peut être un un clown dans un coin qui est en train de faire du bruit de force mais on l'aurait su depuis 160. C'est ce qu'il faut pour énumérer shawwan qui est un algorithme de hachage qui aujourd'hui est considéré comme cassé. Pourquoi depuis 160 160 ? Pardon parce que c'est le double de 80 et vous verrez tout à l'heure une attaque qu'on appelle le paradoxe des anniversaires. Qui vous dit que on va prendre de l'ordre de la racine carrée ?

18:10
Eh Ben la racine carrée de 2 puissance 160 c'est 2 puissance 80 et et donc de ce cas-là on s'assure que les Américains sont pas capables de le casser. Vous allez me dire, Ouais mais attendez-vous êtes gentils. Nous, université de Sherbrooke, on va se faire une sphère de Dyson, on va construire un ordinateur dans l'espace à la température moyenne de l'espace, donc 3,3° kelvin, on va aller prendre la quantité d'énergie la plus petite qu'on connaisse. Donc une fois la constante de boltzman, on va faire un truc pour passer d'un BIT à l'autre.

18:40
On va utiliser boltzmann. D'accord, on va aller chercher un code Grey de manière à ce qu'on change

qu'un bit entre 2 choses continues. Enfin 2 choses consécutives, voilà et on prend toute l'énergie du soleil pendant 20 ans et advienne que pour un Ben. Moi je vous dis, pour savoir combien de bits vous changez de ça, il faut prendre le log de cette valeur divisé par le log de 2 et le log il a une belle propriété, c'est qu'à l'infini il croit pas très vite. En fait il croit plus lentement qu'à peu près n'importe quel polynôme.

19:10
Et donc vous aurez 192 bits de bruteforce. Alors vous avez tué toute vie sur terre hein ? Vous avez pris du soleil pour vous pendant 20 ans, mais 192 bits vous allez me dire, Ouais mais vous savez, après Sherbrooke j'irai faire une autre prestigieuse université, et là je prendrai une supernova. Super, mais là ça fait 219 bits. Alors faut se rappeler par exemple que AES c'est 256 bits en bruteforce hein. D'accord donc il y a pas de possibilité de bruteforce, si on peut vous raconter ce qu'on veut sur le nombre du GPU machin.

19:38
Juste en termes d'énergie il y a pas assez, je parle pas de temps, je parle pas de vitesse. Non non juste énergie ça passera pas. Nombre d'atomes dans l'univers 10 puissance 81 c'est à dire 2 puissance 270 et vous allez voir qu'on va jouer avec des nombres aujourd'hui qui sont très largement au-dessus de ça. Donc même si vous aviez trouvé la manière de ****** dans un atome une information et je passe sur les problèmes de bus de réseau de ça passerait pas.

20:06
D'accord, donc c'est ce dont on va parler. Alors parlons un petit peu de puissance machine pour montrer à quel point elles sont limitées si vous allez chercher sur le le top 500 front tire département of énergie. Alors qui sont les gros consommateurs de puissance de machine ? Ben un, les États département de l'énergie c'est en gros eux ceux qui sont en charge de l'arme nucléaire. Donc ça veut dire également simulation, simulation nucléaire qui est énormément consommatrice, la météo.

20:34
C'est à dire que les équations de Navier Stokes, ça demande également beaucoup de calculs. Et puis Ben les services secrets crypto cassages. Donc là on est sur des trucs qui ont du GPU et qui ont des processeurs, c'est pas des asics, c'est pas des puces dédiées. On est sur l'ordre de de l'ordre de 8,6 1000000 de cœurs CPU et GPU combinés, c'est fait de l'ordre d'un hexaflop. C'est pas des choses qui sont très rapides. Par exemple, pensez pas que vous pourriez faire de la crypto avec ça en vous disant Ouais je pourrais faire du du du du.

21:04
Non, ça contribuerait à 1,4% du Mining global mondial. C'est pas fait pour, c'est pas designé pour Ouais, c'est l'équivalent de prendre une formule un pour aller faire les courses. Vous y allez très vite mais il faudra faire plein, plein plein de aller retour parce que Ben il y a pas de coffre. Donc 8000009 1000000 de cœurs pour aura encore département de l'énergie Eagle qui est le 3e 2000000 de cœurs qui lui est sur Azure 561 petaflops.

21:32
Faut quand même se rappeler que Microsoft considère qu'à tout moment ils ont de l'ordre de 10000000 de cœurs inutilisés donc ils ont en gros un super calculateur distribué non utilisé des questions jusque là pas de questions. N'ayant pas mes notes, je vous prie de m'excuser. J'ai oublié de faire quelque chose que je voulais faire très tôt et je vais vous demander s'il vous plaît tous ceux qui

sont nés. On va faire un petit exercice dont j'aurai besoin plus tard, mais j'en ai besoin maintenant en fait, qu'on le fasse maintenant.

22:01
Tous ceux qui sont nés en janvier vous m'écrivez dans le chat janvier et puis votre date donc il y a quelqu'un qui va le faire pour moi. Moi je suis né le 25 donc vous mettez janvier 25, il y en a un qui met janvier 25 et puis tous ceux qui sont nés en janvier alors si vous voulez pas révéler votre date je demande pas l'année hein, je demande juste le mois janvier et le le la date derrière. Si vous voulez pas mettre le vôtre mettez celui de votre copine, votre frère, votre sœur, votre père, votre mère. Je m'en fous, il me faut une date donc mettons.

22:31
Tous ceux qui ont qui sont là en janvier, on fait ça pendant une minute, puis on va faire tous ceux qui sont nés en février, d'accord, encore une minute, puis tous ceux qui sont nés en mars, puis tous ceux qui sont nés en avril, vous avez compris, je vais aller jusqu'à décembre. Pourquoi ? Parce que je vais vous montrer qu'on va rapidement avoir des collisions. Bon, on utilisera ça plus tard. Donc Deep crack, alors Deep crack, ça veut dire la raie des fesses en anglais. Je vous prie de m'excuser pour la vulgarité, mais c'est comme ça que ça a été nommé.

23:01
C'est une boîte qui avait construit en 1998 pour 250000$ avec l'E FF Electronic Mountear Foundation un une machine pour casser du des et casser du des en brute force en 9 jours. Bon la première fois qu'ils l'ont mis en marche, ça a bousillé la climatisation dans le building parce que ça dégageait trop de chaleur. Mais ça vous donne une idée, y a 20 ans de ça, pas pas de +27 ans de ça, donc casser du 256 bits en enfin pardon Oh là là ont cassé du 56 bits.

23:29
On cachait du 56 bits, pas du 256, du 56 bits en de l'ordre de une semaine +2 jours. Alors à côté vous avez Copacabana, Copacabana c'est cette fois-ci ce que je vous disais là vous allez faire du 56 bits sur votre bureau, c'est de l'ordre de 50000$, c'est 2006, c'est des spartan. Et puis Ben derrière vous avez aujourd'hui les gars qui font du du, du, du, du mining, du du minage. On verra tout à l'heure ce que c'est, on pourra en parler à la pause si vous voulez.

23:57
Calculer des h le calcul des h comme des cochons, on est à 50 hexa h par 2nde sur le le le plus gros marathon digital holding ce qui est le le plus gros hacheur en en bitcoin, c'est de l'ordre de 50 hexa H donc on n'est pas en giga. On n'est pas en milliards, on n'est pas en Terra, en milliers de milliards, on n'est pas en.

24:24
Là on est en examen, c'est à dire 1000000 de milliards. Donc ceci vous montre une idée de à quel point, pour avoir toutes les machines que vous voulez, vous êtes quand même limités en puissance. Donc l'attaque par force brute, l'attaquant attaque et essaye. Tout était possible d'un texte chiffré jusqu'à se trouver la traduction intelligible du texte. En clair, en moyenne, vous allez parcourir la moitié puisque il y a une chance sur 2 que ce soit dans la moitié du haut, la moitié du A en moyenne, vous allez placer à la moitié.

24:51
On parle de BFMIBFMI bruteforce massive. Ignorance d'accord, donc c'est la méthode bourrin. Un

cheval des chevals on va droit dans le mur alors c'est si vous êtes proche du truc, c'est mignon pour aller chercher ce qu'il faut mais faudra pas me raconter à la fin du cours. Ouais mais vous voyez votre truc en 256 bits ? Si je prends tous les GPU de la terre je dis a non, il y aura pas assez d'énergie d'accord ?

25:17
Alors, solution cryptographique, chiffrer, ça veut dire quoi ? Ça veut dire rendre un message incompréhensible, mais on va utiliser un secret, on va utiliser une clé de chiffre, de, de, de, de chiffrement ou de déchiffrement. Déchiffrer Ben c'est partir du message chiffré et utiliser la clé pour retourner au clair, décrypter. Cette fois-ci c'est quand on n'aura pas la clé. Là on veut essayer de on est l'attaquant cette fois-ci dans les 2 autres cas, on est à priori l'utilisateur.

25:48
Et on essaie de revenir au message En clair à partir du message chiffré des questions. Oui Monsieur, Bonjour, une petite question s'il vous plaît, c'est juste pour ne pas être bête là quand vous parlez du manque d'énergie pour par exemple casser un un cryptage de l'ordre de 256, c'est de quelle énergie énergie électrique le le l'alimentation c'est je peux, c'est ce que j'ai dit ici.

26:13
J'ai j'ai, j'ai dit, vous prenez toute l'énergie du soleil pendant 20 ans en construisant une machine qui prendrait pour changer chaque bit une fois la constante de boltzmann. Vous faites 192 bits. Vous êtes ici là énergie du énergie du soleil. Pendant 20 ans elle vous a permis de bouger un compteur de 192 bits. Juste compter hein ? Ouais, si vous avez pris l'énergie d'une supernova, vous avez fait 219 bits. Donc là on est pas en train de parler de ce qui sort de la prise de courant.

26:42
On s'est mis dans l'univers à la température moyenne machin nanana et même en étant utilisé les quantités d'énergie les plus petites connues, on n'a pas assez d'énergie pour tout faire. Je suis pas je suis pas en train de parler de kilowattheure et de machin. Je suis non non non non. Je suis dans un mode d'un ordinateur qui serait le plus efficace en physique de trucs qu'on ne s'est même pas approché de loin. On consomme trop d'énergie.

27:12
Ça a du sens ou c'est c'est ? J'ai répondu à votre question ou pas ? Non c'est cool, merci, parfait alors on continue stéganographie donc stéganographie c'est pas de la Crypto, c'est une technique qui consiste à dissimuler un message, on désire le transmettre de manière confidentielle mais on va pas le chiffrer, on va le cacher. Ce qui est différent on va le cacher au milieu d'un ensemble de données d'apparence anodine, de manière à ce que ça devienne imperceptible. D'accord donc vous avez des exemples, vous pourrez aller regarder.

27:41
De l'ordre invisible par exemple, c'est de la Téléanographie, mais au passé, y avait un des Romains qui voulaient détruire Carthage, y avait des Grecs qui, voyant que y avait une attaque qui se préparait, y a un gars qui a pris un de ses esclaves, qui a simplement fait raser la tête de l'esclave, qui a tatoué un message sur la tête de l'esclave, qui a laissé repousser les cheveux et qui a dit tu vas de l'autre côté.

28:07
À tel endroit, et quand tu arrives, tu leur dis qu'ils te rasent la tête. Bon, les mecs ont rasé la tête, ils ont lu le message, ils se sont préparés, ils ont pu gagner la bataille. Puisqu'on parlait ici de préparation

de navire, on parlait de de plusieurs mois de préparation, c'est de la STÉGANOGRAPHIE, il y a pas de crypto là-dedans, d'accord, une des manières de faire, c'est d'inclure du texte dans une image. Alors comment on fait ? On fait simplement que l'œil voit très bien dans le vert et beaucoup, beaucoup moins bien dans le bleu.

28:36
C'est pour ça que je vous mets une diversion verte par exemple. Mais qu'est ce qu'on va faire ? On va aller chercher sur du RGB sur le byte de l'octet bleu on va dire Ouais, le BIT de points faibles, allez on dégage, on met à la place l'information qu'on veut, quelle différence entre ce bleu là et le bleu juste à côté ? Personne n'y verra rien. Donc par exemple ici vous allez voir une fleur, d'accord, mais si on regarde de l'autre, si si, si on retire et qu'on garde que les bit de points faibles.

29:05
Oui dans le bleu, mais on trouve ceci et et et ça va prendre 8 octets pour cacher un octet, puisque dans chaque octet on ne peut cacher qu'un seul bit, c'est c'est c'est un bit à la fois tous les 8. Oui mais fondamentalement au bout de 10 octets on aura caché 10 bits. D'accord ? Et donc vous pouvez vous en sortir et cacher de l'information qui va devenir.

29:35
Accessible d'accord, à quiconque connaît le secret. Ça veut pas dire qu'elle a été cryptée, ça veut dire qu'elle a été cachée au milieu de la foule, cachée ici, entre autres au milieu des pixels. Mais par exemple un truc récent c'est comment Elon Musk se débrouiller pour savoir d'où étaient les fuites ? Et il envoie un email ? Bah il envoie le même Email à plusieurs personnes mais il a pas la même position de virgule ou les mêmes espaces.

30:05
L'information est la même. Par contre si vous avez pas modifié la position des virgules et des espaces et que vous avez futé un journaliste, lui il a encore les originaux et donc il saura qui était la source, qui était le traître, c'était ganographie question, pas de question super. La Cryptologie, c'est la somme de 2 choses, c'est la somme de la cryptographie et de la cryptanalyse. Cryptographie, c'est l'art de construire cryptanalyse, c'est l'art d'attaquer. D'accord donc.

30:31
On va créer des systèmes de chiffrement symétrique ou asymétrique. Symétrique, c'est Alice et Bob, on parle de A et B Alice et Bob partagent la même clé ou asymétrique où ils auront. Il y aura plus que 2 clés. D'accord, mais cryptanalyse en casse. Cryptographie, on construit cryptologie, c'est l'ensemble des 2. Ici, on va parler de cryptographie.

30:56
Un petit peu de cryptanalyse donc de cryptologie, mais beaucoup de cryptographie. Par contre on va très peu discuter de stéganographie un autre sujet, c'est moins intéressant puis que rien. Si vous voulez faire de la STÉGANO, je vous conseille que ce que vous cachez, ça m'intéresse à être chiffré avant. Alors l'histoire alors moi j'ai une approche depuis le temps que j'enseigne ça qui est de dire je pense que si les gens comprennent ce qui s'est passé avant, d'où ça vient, alors les choses.

31:25
Prennent +2 sens à leurs yeux, donc il faut raconter l'histoire. Oui, vous voyez en dessous, vous avez quelques dates, 3000 avant Jésus Christ, 3000, c'est le premier acte cryptographique. C'est ce qui nous

sépare de la préhistoire. Comment on passe de la préhistoire à l'histoire ? C'est l'invention de l'écriture. Ben si vous savez pas lire l'écriture c'est un code, donc l'acte qui fait passer l'humanité.

31:51
Alors c'est pas le premier janvier moins 3000 hein, c'est aux alentours de l'acte qui fait passer l'humanité dans de la préhistoire à l'histoire. C'est un acte cryptographique, c'est l'invention de l'écriture. Moi alors 476 je le je le connaissais pas par cœur hein, mais je j'ai une fille qui qui passait un exam sur les Romains, je l'ai fait bosser la semaine dernière. 476, c'est.

32:18
La séparation des 2 empires romains, romains d'occident, romains d'Orient et c'est la fin de l'empire Romain d'Occident. C'est donc la fin de l'Antiquité, le début du Moyen Âge. 1492, c'est le début de l'ère moderne, c'est Christophe Colomb, l'Amérique. 1789, déclaration des droits de l'homme et du citoyen, c'est la phase contemporaine et 2024 c'est la mise en place d'algorithmes post quantiques. Alors discutons un peu maintenant d'histoire.

32:44
Ben si vous Regardez les 7 merveilles du monde machin il n'en reste qu'une qui est la pyramide déguisée. Donc on est de l'ordre de moins 2000. Mais à ce moment-là il y a des scribes, déjà des gens qui étaient en charge de l'écriture, tout le monde savait pas lire et écrire qui modifiaient des livres de livres par exemple pour cacher des recettes de vernis. Que tout le monde puisse pas les comprendre, c'est une forme de chiffrement. Vous avez également, 2000 ans plus tard ou à peu près 1950 ans plus tard, l'ordre de grandeur.

33:15
Des chiffres comme les chiffres de César. Alors on dit César, pas forcément Jules César au sens les empereurs romains. Décalage de 3 dans l'alphabet si vous lisez la guerre des Gaules, machin, vous allez me dire mais décalage de 3 dans l'alphabet, faut quand même pas être très malin. Oui mais à l'époque tout le monde sait pas lire. Et puis quand César vous demande de porter un message, je pense que votre but est quand même de le porter et pas de d'essayer de vous retourner contre lui.

33:38
C'est avant tout déjà de de de résister au gars qui a envie de vous mettre un lève entre les 2 épaules. Donc vous avez autre chose à faire que de la cryptanalyse. Il va rien se passer à peu près jusqu'au Moyen Âge, jusqu'au 16e siècle où enfin il va rien se passer. Non entre les 2 va y avoir high kindi, on va en parler tout à l'heure mais je je je garde pour un slide, il va y avoir de la cryptanalyse, des manières de casser, mais la grosse invention cryptographique va venir au 16e siècle avec le chiffre de visionnaire, on en parlera tout à l'heure.

34:08
Et puis la crypto, chaque fois que vous Regardez la crypto, l'armée est pas loin derrière ce qui fait rentrer les États-Unis dans la Première Guerre mondiale. C'est ce qu'on appelle Le Télégramme de Zimmermann, télégramme échangé entre envoyé par les Allemands mexicains qui leur promettaient des terres s'ils attaquaient des États-Unis et qui disaient au Japon, faites en d'eux mêmes alors que officiellement tout le monde était notre façon de parler. Ben les Anglais ont attrapé ces télégrammes non déchiffrés et non montré aux Américains qui sont rentrés en guerre.

34:37
2e guerre mondiale, elle a été gagnée par les Occidentaux, façon de parler et par les alliés parce que

une des raisons c'est que les chiffres allemands, les chiffres allemands et Lima avaient été cassés par Alan Turing. On en parlera tout à l'heure dans les années 70. Dans les années 70, vous avez quelques algo cruciaux qui sont apparus en symétrique ou en asymétrique, comme RSA, et donc vous avez une furie d'activité. Une activité très très importante depuis.

35:08
Et depuis enfin 20e siècle, fin du 20e siècle, 70 jusqu'à maintenant. Et puis là maintenant, on est en train d'attendre l'arrivée des ordinateurs quantiques et donc on se prépare avec des algorithmes qui sont post quantiques, qui vont résister aux algorithmes quantiques. C'est pour ça que j'ai écrit en dessous que à partir de 1000 975009 75, vous allez voir apparaître le premier standard de chiffrement qui va respecter les principes de kirchhoff. On va parler de kirchhoff dans quelques instants et vous aurez le des.

35:34
Qui va paraître en 75 en 77RSA les courbes elliptiques en 85AES en 2001, donc vous voyez que y a de l'activité, il s'est rien passé à peu près entre 2000 et et moins 50 et là en quelques années, boum boum boum Boum boum ça tape très très fort. Des questions, pas de questions. Ah on est maintenant en août, super donc continuez. Ben il reste septembre, octobre, novembre, décembre. Allez y balancez vos anniversaires.

36:04
Solution cryptographique. Alors kirchhoff nous dit quoi ? Vous avez un bouquin qui s'appelle que je vous mets à la fin dans les slides, qui s'appelle cryptographie appliquée de Bru Schneider qui est très intéressant, je vous recommande de le lire, c'est un petit peu large mais bouquin technique très intéressant. Il commence son bouquin en disant, Si vous cachez, vous vous construisez un coffre et vous le cachez dans New York et vous demandez à quelqu'un, ouvrez ce coffre, c'est de la Stéganographie. Ouais, c'est pas de.

36:33
Il y a rien de de cryptographique là-dedans. Si par contre vous prenez le coffre, vous mettez la clé dans votre poche et vous dites au gars je réponds à toutes tes questions, comment je l'ai construit son architecture ? Je vais faire des coffres avec toi qui sont à l'identique, t'auras tout sur le secret de la clé et malgré ça tu pourras pas l'ouvrir. Alors on est en crypto. Le fait de cacher un coffre dans New York c'est de la stegano le fait de dire à quelqu'un je n'ai aucun secret pour toi sauf ma clé, c'est de la Crypto le principe de kirchhoff alors j'ai toujours ma petite blague qui dit.

37:04
Kirchhoff et pas Smirnov. Pour les alcooliques, Smirnov c'est autre chose nous dit que le cryptosystème doit être sécurisé même si l'attaquant connait tous les détails de conception du système. La seule chose qu'il ne peut pas connaître c'est la clé est le on va considérer que le système a été vu espionné donc autant tout donné quasiment comme de l'Open source et considérer que malgré ça vous pouvez pas l'attaquer. D'accord, si vous faites de la sécurité à travers l'obscurité ça se passera mal de manière générale.

37:33
Alors vous avez ici un besoin dans puis des temps immémoriaux de protéger de l'information. On a dit l'invention de l'écriture, cette première aire cryptographique. On a parlé des scripts, mais vous avez ici l'algorithme AD bash qui est un truc que vous trouvez dans les chez les Hébreux, mais a donne ZB

donne y si vous partez du en haut, C'est a donne ZB donne YC donne X, mais Regardez l'autre colonne en bas, Regardez ici c'est la même chose, Z donne a.

38:02
Y donne BC donne X donc en fait la 2e colonne on n'en a pas besoin, celle-ci suffit si vous la faites dans les 2 sens et en fait la somme, Ben elle vaut toujours 26 si vous faites la somme des 2. Ouais enfin ou la différence vous êtes sur une constante, c'est à dire que le A et le Z sont ensemble, le B et le y le C et le X oui et puis forcément au milieu vous allez avoir le M et le n qui sont voisins.

38:30
D'accord, ça veut dire quoi ? Ça veut dire que si vous vous cryptez Sherbrooke mais là des vous allez voir que les 2E donnent 2V et les 2O donnent 2L. Donc si on regarde ça on se dit bah je sais pas ce que c'est mais le s se répète pas I et I se répète. Bah oui c'est nos RR d'accord, LL c'est notre OO et VV c'est notre EE.

38:57
Gardez ça en tête parce que dans quelques instants on va parler de cryptanalyse fréquentielle. Alors dans à peu près n'importe quel pays de de temps immémoriaux, la question c'est à quelle famille tu appartiens. On sait toujours qui est la mère, mais ce qui est intéressant c'est la la, la descendance dans les sociétés patriarcales. Alors le Phone en allemand, le 2 en français, le Ben En arabe, c'est c'est c'est relié à une famille. Mais si vous commencez à mettre cette.

39:26
Ce truc là dans les noms des gens, bah ces lettres là elles vont apparaître plus fréquemment. Donc en fait c'est juste un exemple. Mais c'est vrai de manière générale la répartition des lettres n'est pas uniforme. En me donnant Gonzalez, vous avez beaucoup plus de e, de t, de a que de X, de Q ou de Z en fait la meilleure manière de voir c'est ce que je vous ai mis ici, les points du Scrabble, Regardez la distribution des points, puis vous vous rendez compte que bah distribution là de points ici.

39:54
Alors le h il est pas mal placé parce qu'il vaut 4 points alors que il y a il y a encore des un à côté. D'accord c'est peut être pas la meilleure valeur, mais pour tout le reste ça avance quand même de manière assez linéaire. 121313144243345810. Alors c'est sûr que si vous mettez whisky avec un W, un h un k un y sur un mot compte triple, allez prendre votre douche hein. La partie est pliée mais les fréquences.

40:25
Ne sont pas uniformes. Ce qui veut dire que si vous remplacez toujours la même lettre par la même valeur, Ben ces fréquences on va les retrouver dans le texte chiffré. Et si je vois beaucoup de trucs qui apparaissent en anglais, je me dirais Ben a priori ce sera peut être plus des EDT ou des a que des x, des Q ou des Z Ben ceux-ci ça a été découvert par Al Kindi. D'accord Al le même al que Al Djebra ou Al Qaïda ?

40:51
C'est l'analyse fréquentielle. Alors c'était des moines initialement qui s'en étaient rendu compte parce que il copiait des textes secrets, des textes religieux à la main. Monsieur Rank Xerox était pas encore passé par là avec sa photocopieuse. Et puis il se sont rendu compte qu'il y avait des lettres qui copiaient beaucoup plus que d'autres. Alors ce que je vous raconte ici, vous pouvez appliquer une

lettre et vous pouvez l'appliquer à un 10 g, un couple de lettres ou un trigramme 3 lettres, ça va encore être vrai.

41:17
Donc ça veut dire quoi ? Ça veut dire que par exemple le double l qu'on a vu ici dans le chiffré, dans le double O en anglais ou le double M en français, c'est des trucs qui vont réapparaître. Par contre le ZK si vous parlez de tchèque peut être, mais en français pas beaucoup, en anglais pas beaucoup non plus. Vous voyez. Donc vous avez un biais statistique qui se retrouve dans le chiffré.

41:45
Et en analysant le biais 7 XI dans le chiffré, vous pouvez remonter au clair, est ce que c'est clair pour tout le monde ? Oui non des questions o K on continue, oui allez y je vois des mains qui se lèvent, allez y posez vos questions. Question, c'est moi tu avais levé la main ? Vas y non, c'était une erreur, excusez-moi, pardon donc.

42:15
Ceci est vrai pour toutes les langues. Alors attention, on va pas commencer à aller parler de trucs qui s'écrivent de manière. Moi j'ai une question, s'il vous plaît, je vous en prie, allez y quand même des vous savez il y a des caractères un peu spéciaux, accent @et autres. Est ce que ça rentre en jeu dans ça ? Parce que parce qu'on se base sur les 26 lettres de l'alphabet où on prend en compte des ça change rien, ça change rien que vous ayez un document technique très technique ou maintenant des trucs avec Internet machin.

42:44
Ben au pire c'est quand même un biais statistique parce que une adresse Email sans @moi j'attends de la voir donc. Et en plus on s'attend à on s'attend à ce qu'elle soit pas en premier et qu'elle soit pas en dernier non plus de la meilleure manière que si c'est une adresse Email il y aura sans doute un point quelque part. Mais je parle ici, je parle ici de on va dire des lettres classiques mais c'est le c'est le concept de manière générale. Mais l'accent machin ne change rien.

43:14
Au contraire, ça va même vous permettre d'identifier si vous commencez à avoir des trémas sur des A ou des trucs comme ça. Vous êtes sans doute plus sur des langues nordiques que sur du méditerranéen. D'accord ? Donc vous vous rendez compte que en espérant tout en espagnol, en portugais, en italien, en français machin, c'est quand même le E qui est le plus fréquent, puis le A, puis le I, puis le n, puis le o alors si vous êtes à la haut de la fortune ou aux mots fléchés, ça vous permet de tricher puisque vous risquez de.

43:42
Trouver des trucs qui sont très présents, d'accord Ben mots fléchés. Vous avez intérêt typiquement ou les mots emmêlés, vous avez intérêt à prendre cette fois-ci l'opposé, prendre des trucs qui apparaissent très apparemment et trouver les quelques instants de cette lettre dans la grille. Et Regardez autour, vous allez tomber sur votre mot. Oui, si vous prenez les lettres qui apparaissent le plus, vous allez avoir un élément de recherche qui est moins d'être optimal.

44:10
Alors 420 avant Jésus Christ, les spartiates par exemple utilisaient la cital, donc cette fois-ci on écrit sur un ruban, on met le ruban autour d'un bout de bois, d'un cône ou quoi que ce soit, on écrit à l'horizontal, on déroule, on envoie le morceau de cuir, le papier, ce que vous voulez, et de l'autre côté,

il faut que les gars fassent la même chose sur le même ruban, prennent le même ruban sur le même morceau de bois pour réussir à j'ai bien dit.

44:36
Cône ou morceau de bois ? Mais on n'est pas sur, on n'est pas sur des trucs de 13 M de large, donc en terme de brut de force, tester toutes les possibilités, ça va finir par se trouver. Vous voyez ce que je veux dire ? On va faire quelques essais, c'est quelques heures à la main, on va le c'est plus un retardateur qu'autre chose, c'est pas la, c'est pas le système absolu. Alors je vous ai dit, 50 ans avant notre ère Jules César, mais au sens les Césars, les empereurs ont une un décalage de 3 positions dans l'alphabet.

45:04
Alors ça veut dire Ouais mais vous allez me dire mais qu'est ce qui se passe pour le z ? Parce que le Z décalé de 3, Ben on travaille au module O 26, c'est à dire que le Z il va devenir le C pardon non, il va devenir le B puisque le le a devient le c d'accord donc en fait au lieu d'avoir une ligne, Ben maintenant vous avez un cercle ou un tor, vous refermez le alphabet sur lui même et puis vous vous déplacez en penchant ou dans l'autre. On parle ici de chiffrement par substitution, c'est semblable à.

45:34
Bâche donc par exemple le le mot logique donne ce mot là, d'accord. Et pour ceux qui sont assez âgés, comme moi j'ai la cinquantaine. Mais quand j'étais jeune ingénieur dans les années 95, j'étais encore sur les bords de l'école Netscape qui avait, quand on voulait insulter quelqu'un en ligne, y avait le rot 13. Donc vous appuyez sur rot 13. Dans les News groupes, vous écrivez votre cochonnerie, puis vous remettez rot 13 derrière. Si le mec veut aller le lire, il fait rot 13. Ben Rot 13A. Un avantage, c'est que c'est la moitié de 26.

46:01
Le chiffrement et le déchiffrement c'est la même opération, il y a pas besoin de se mettre d'accord sur la clé, c'est la même pour tout le monde, il faut décaler 13 et il y a qu'une seule opération à coder, pas 2. D'accord ? Alors vous allez me dire oui mais si maintenant je suis attaquable avec un système où en mesurant les biais statistiques et la présence de mes lettres on arrive à deviner ce qu'il y a dans le texte chiffré ? Pourquoi je me débrouille pour que.

46:32
Pourquoi est ce que je me débrouille pas pour que une lettre en puisse en donner plusieurs ? Le E la première fois Ben il donne J mais là s'il continue à donner J sur un système monoalphabétique, j'ai qu'un seul alphabet de remplacement. Par contre si j'avais un système polyalphabétique d'accord, Ben le la la même lettre donnerait pas toujours la même chose, mon a un coup il donnerait U par exemple, un coup il donnerait M Ben ça c'est l'idée de Blaise de Vigenère. Donc vous voyez, on est passé du à peu près Jésus.

47:01
Au Moyen Âge, c'est Blaise de Vijenner qui nous dit ça, et c'est en 1586 qui a cette idée qu'en fait baptistel l'avait déjà eu avant lui en 1553 et on a des traces d'un gars qui avait fait la même chose au 13e siècle. En fait ça va être cassé par kavinski en 108006033100 ans plus tard et on se rend compte que babbage, donc Babette, si on vous dit quelque chose, c'est quoi Monsieur Babège ?

47:35
Personne. Bon, la, l'inventaire de la machine, c'est ça, c'est ça. C'est ça la machine. La machine qui fait

un des premiers automates. Un Monsieur qui avait démontré par exemple que c'était pas intéressant de se prendre la tête à calculer des prix de timbres. Il valait mieux avoir un prix de timbre unique et qui soit pas lié à la distance. Et donc il commence à créer un automate mécanique, un calculateur, une grande machine.

48:01
Ce qui a jamais marché parce qu'il y avait des problèmes de mécanique, de tolérance mécanique. Mais l'architecture était bonne. Et Ben la personne qui a écrit le premier Manuel sur ce, la première premier programmeur de cette machine, c'était une femme, ada lovelace, qui avait écrit un un Manuel extrêmement précis, développé ainsi de suite et d'où le langage ada porte porte le nom. C'est en en hommage à Ada Lovelace donc, qui était la fille en fait du du bras droit de bahage.

48:30
Donc vous avez par exemple notre ami Vigener qui avait fait ça un petit peu avant sur des textes en en hébreu. Je vous ai mis le le, le document, donc vous allez avoir un système polyalphabétique, c'est à dire que vous allez dire j'adore écouter la musique, la radio toute la journée. Le l'athlé c'est musique, donc vous écrivez musique, musique, musique, musique, musique, musique. On rentre un j un M et ici on va aller regarder d'accord la lettre. En clair, le J.

49:01
Colonne du J, le M PAM, ça doit me donner. Qu'est ce qu'ils me disent ici un V ? Ouais, on obtient la lettre V, c'est ça ? On obtient la lettre V ici, d'accord. Donc si vous Regardez la 2e lettre qui a un A, vous rentrez un a, vous allez chercher au niveau du U, ça vous donne un U.

49:30
D'accord donc le A il donne un U par contre le prochain a qui va venir, comme il sera pas en face du U le A il va être en face du M, il nous donnera autre chose, le a en face du M il me donnera un M d'accord donc maintenant il y a plus de cryptanalyse fréquentielle directement. Par contre il va y avoir des patterns. Si j'arrive à déterminer que j'ai des lettres qui se répètent tous les X, je vais pouvoir déterminer ici, j'aurai une répétition tous les 7.

49:57
Matteley, c'est musique, MUSIQUE, 7 lettres et sur des textes assez longs, je me rends compte que tous les 7 sur un paterne, Ah Ben maintenant je vais essayer de trouver des mots de 7. Alors déjà si c'est des mots du dictionnaire, vous êtes mal barré. Parce que comme musique, parce que Ben le dictionnaire, tout le monde l'a et c'est des trucs qu'on peut brut forcer. Donc si vraiment vous voulez être très fort, il va falloir prendre des mots aléatoires et il va falloir que vous essayez d'éviter les patterns.

50:27
Alors, solution cryptographique ? Il existe en fait en crypto une porte logique, on parlera des booléens tout à l'heure, on va déjà rentrer dans les booléens, ici qui est le xor ? Alors le xor c'est une fonction qui est magnifique parce que elle permet c'est l'un ou l'autre, mais pas les 2. Vous mettez les 2 à 0, ça vous dit non ? Vous mettez les 2 à un, ça vous dit non ? Par contre vous en mettez un seul à un, ça vous dit oui, ça vous donne un un, donc l'un ou l'autre, mais sûrement pas les 2.

50:56
D'accord, mais ça veut dire quoi ? Ça veut dire que 2 choses qui sont identiques donnent 1000 Xor 0 ça vous donne 0 mais un xor un ça vous donne aussi 0. Donc si vous utilisez cette porte pour chiffrer

et le xor et la porte pour des raisons que j'ai pas le temps d'expliquer de base du chiffrement, mais méfiez-vous parce que si vous faites par exemple message xor clé et vous reprenez le même message, xor une autre clé. Ben moi j'ai juste à xorer.

51:26
Les sorties entre elles, les messages vont sauter. Message de message va me donner genre message va me donner 0 il va me rester clé exhorte clé de la même manière si vous avez pris clé exorte clé prime. De la même manière si vous avez pris la même clé avec 2 messages différents, les clés vont s'annuler entre elles. Va me rester les différences entre les messages. Donc dans ces cas-là vous voulez que la clé ne soit pas réutilisée si vous utilisez juste un xor ? D'accord sauf falloir révéler les différences.

51:55
Et il faut qu'elle soit vraiment aléatoire. Si votre livre est pas aléatoire, vous allez avoir des problèmes. En fait, vous voyez, on parle ici du seul chiffrement qui est incassable, qu'on appelle le chiffrement de vernam ou le masque jetable. D'accord, c'est un chiffrement où ? Mais pour éviter le Pattern d'Athlé doit être aussi longue que le message, elle doit être complètement aléatoire.

52:24
Pour éviter les attaques du dictionnaire, le machin et puis pour éviter les répétitions, les les, les trucs de xor et ainsi de suite, on doit l'utiliser qu'une seule fois. Donc si vous avez un message où vous faites des xor, votre clé est aléatoire ou sinon comme étage utilisé une fois une seule moi je vous signe vous êtes incassable. Par contre si vous voulez livrer, vous voulez échanger avec quelqu'un, un vous avez intérêt à rester synchro parce que si vous vous désynchronisez c'est foutu et 2 Ben si vous voulez échanger 10 gigas de données, il faut échanger 10 gigas de clé.

52:58
La question que j'ai dans ce cas-là c'est Ben pourquoi au lieu d'échanger la télé vous allez pas échanger de message ? Alors attention ce message est utilisé par les ce ce ce genre de choses est utilisé par les espions, particulièrement les Russes, le NKVD dans la 2e Guerre mondiale qui est un petit peu le KGB. Mais l'extérieur utilisait ça les Américains.

53:23
Avec un projet qui s'appelle Venona ont espionné toutes les communications. Je parle des années de la guerre. En 2e guerre mondiale, toutes les communications qui rentraient et qui sortaient de l'ambassade russe et les Russes ont eu des problèmes puisque leurs générateurs aléatoires ont été détruits et ils ont commencé à réutiliser les clés. les Américains ont utilisé le billet statistique que je vous ai donné. En 42 c'était 1,8%, en 43 ils ont chopé 4000000 des messages. En 44 c'était 19 49% des messages.

53:51
Et en 45 1,5% quand vous leur en parlez, ils vous disent ouais non c'était pas très successfull hein. C'est quand même juste un un de l'ordre de un pour 100. Oui en 42 et en 45. En 44 vous étiez quand même à 50% des messages, 49%. Cette technique, elle est utilisée pour chiffrer le téléphone rouge. Téléphone rouge qui était la ligne entre Moscou et Washington pour éviter de se ****** des bombes sur la physique sur le visage.

54:10
Ben téléphone rouge, téléphone rouge, là c'est facile hein, il suffit de prendre des hélico avec des

Rambo pour d'un côté délivrer des des les les les messages, enfin des clés. Pareil dans l'autre sens, et on est bon d'accord, mais vous vous rendez compte que les seuls chiffres qui sont incassables, c'est en fait un chiffre qui est inutilisable dans la pratique. Alors on va parler un petit peu de la machine uniquement, donc cette ce ce ce ce ce chiffre de vernam.

54:41
Il a paré un homme américain, il a paré. Alors je vais demander à quelqu'un s'il vous plaît, je sais pas, il me faut un volontaire, est ce qu'il y a quelqu'un qui est qui est volontaire pour faire un petit travail sur ce qu'on a mis dans le chat, y a quelqu'un qui est volontaire, personne. Alors les dames d'abord parmi les dames, est ce qu'il y a quelqu'un qui est volontaire ? Ah y a quelqu'un qui est volontaire, je sais pas qui c'est.

55:11
Bon Monsieur, qui a levé la main ou la dame qui a levé la main ? S'il vous plaît, prenez dans le chat, vous Regardez en janvier s'il y a 2 personnes qui ont le même anniversaire et vous me dites vous mettez janvier. Combien y a de personnes qui ont le même anniversaire parce qu'il y en a 2 qui sont nés le 25, 2 qui sont nés le premier, 3 qui sont nés le 13. Quel est le nombre de collisions ? Pareil en février, pareil en mars, pareil en avril jusqu'à décembre. Moi ma théorie c'est qu'on va avoir des collisions, je sais pas s'il y a l'ordre de 80% dans la salle.

55:38
Y a 4 personnes dans la salle, c'est très très très élevé. Je vous montrerai tout à l'heure pourquoi à partir du moment où il y a 23 personnes dans une salle, on a 50% de chances que 2 personnes aient le même anniversaire. Et donc quels sont les effets sur pardon ma prof j'ai pas vu j'ai j'ai j'ai loupé le truc, je sais pas qui c'est quoi avait écrit ma prof, quelque chose qui commençait à voir le message et puis ça a disparu si vous voulez le reposter. Quelqu'un avait posté derrière, donc.

56:09
Ça a des effets en cryptographie, le fait que des choses tirées au hasard vont finir par avoir des collisions, qui c'est quoi a la main levée ? Question, pas de question. Donc il y en a un qui prend le le truc et qui détermine le nombre de collisions pour tous les mois, ça devrait normalement faire très très mal. Donc on va parler d'enigma le chiffre de vernam on est à la fin du 19e siècle, donc les années 1800 et les bananes.

56:37
Et on est sur de l'électromécanique, c'est à dire qu'on va commencer à utiliser du relais, faire passer du courant pour créer des champs magnétiques pour déplacer les choses. Mais y a pas de transistor. Le transistor viendra beaucoup plus tard, dans les années 50 ou 60. Et donc.

56:54
Électromécanique, on va essayer de faire des machines qui vont être électromécaniques, qui vont bouger comme ça, ça va donc faire du clic, clic, ça va faire du bruit. D'où la notion de de bombe dont on va parler dans quelques instants. Machine électromécanique, et Ben on se rend compte que vernham ne marche pas super bien, mais est ce qu'on pourrait quand même pas utiliser des machines ? Utiliser une automatisation pour chiffrer. Et donc en 1919, il y a coach.

57:23
Mais c'est en fait comme d'habitude plusieurs personnes hein. C'est Van Hegel, Cherbius, Pringler qui ont travaillé sur des machines de chiffrement et qui vont lâcher cette machine qui va être utilisée

pendant les Allemands, avec les Allemands pendant la 2e Guerre mondiale et Nigma, c'est une machine qui avait l'ordre de 10000000 de milliards de possibilités, ce qui revient à peu près 53 bits. D'accord, elle est utilisée alors en interne, vous avez des rotors d'accord, donc on peut vous presser une touche sur le clavier, Vous voyez ici le clavier, ici vous avez des des, des loupiot.

57:52
Ça rentre, ça traverse des rotors. Donc les rotors, au bout d'un certain temps, quand lui il a fait un tour complet, le 2e change d'un cran, quand lui a fait un tour complet change d'un cran. Donc le secret, c'est la position des rotors. OK, ici vous avez les rotors, la position des rotors, vous appuyez sur a, ça traverse les rotors, ça fait 1/2 tour au bout, ça repart dans l'autre sens, ça vous donne un g, vous réappuyez sur a, ça fait un autre chemin, ça vous donne un C parce que le retard droit a avancé de une position.

58:18
Ceci, si vous avez vu le film, est ce que vous avez vu le film The imitation Game d'Alan Turing avec Alan Turing et quelque chose à quelqu'un imitation Game il y a quelques années au cinéma ? Oui non, personne va au cinéma. Ouais Ben Turing était t'as parlé un petit peu de turing, turing et le cerveau qui a permis de casser l'énigme.

58:48
Non, je vais. Je vais vous parler de turing quelques instants parce que c'est aujourd'hui, si vous recevez un prix Nobel, l'équivalent d'un prix Nobel en informatique, vous avez un prix turing turing conçu en Inde. Hors de question que la mère couche en Inde. Elle rentre en Angleterre pour accoucher. Elle repart auprès de son mari turing et, élevé par sa grand-mère turing, tombe amoureux d'un, d'un, d'un, d'un camarade d'école au lycée qui va mourir d'une.

59:19
D'une oui, comment ça s'appelle ? Ah les trucs au niveau des poumons tuberculeusement. Et ce gars était brillant. Je je fréquente des pour Christopher et c'est un gamin qui découvre. À 12 ans, il développe l'arc développement limité de l'arc tangente, il détonne sa prof de maths et ainsi de suite, il fait sa thèse.

59:45
Il fait sa thèse, il va créer les fameuses machines de turing, on en parlera dans quelques instants avec Alonzo Church et ainsi de suite. Puis il est déjà approché par les services secrets anglais, puis il va aller aux États-Unis, l'Institut des des des études avancées à Princeton. La guerre éclate, il est ramené en Angleterre et les différences des Allemands qui ont utilisé leurs ingénieurs comme shirakanon. Les Anglais sont un peu plus malins et on va demander à turing de casser énigme.

1:00:09
Turing va travailler à bletch les parcs, il va construire ce qui va être l'équivalent du premier ordinateur, mettre en application et tous ses travaux de thèse. Ben c'est ce que Benedic Cumberbatch joue là avec une machine qui s'appelle colosus. Et en fait turing est gay. Un jour, il va se faire cambrioler par le copain ou l'ami d'un de ses petits copains. Il va au, il va au commissariat pour déclarer ça, il dit.

1:00:37
Boyfriend à la place de Guefriend pas, et là le je vais pouvoir casser de l'universitaire parce que la guerre est finie, turing et universitaire, tout ce qu'il avait fait classifier au plus haut niveau, et ainsi de suite. Au final, il passe devant le juge, on lui donne 2 choix, castration chimique ou la prison, il prend

la castration chimique, il a des effets de gynéco, masqual les seins qui poussent, machin libido est toujours là.

1:01:04
Et turing était fasciné à l'époque par Walt Disney, Walt Disney, les premiers films, le dessin animé de Walt Disney, Blanche Neige. Et donc qu'est ce que turing fait ? Il prend une pomme, il la trompe dans le signalur et il la mord, il en décède. Et c'est par exemple, ils ont toujours dit que c'était pas le cas. Mais vous avez une petite société qui s'appelle Apple qui a commencé avec.

1:01:29
J'ai commencé à vendre des machines qui ne sont rien d'autre que des machines de turing. On va parler de la machine de turing dans quelques instants et qui a pour logo une pomme croquée avec le drapeau homosexuel. Au début, ils ont toujours dit non, on n'avait rien à voir dans l'histoire. Oui, à part que la pomme que turing a mangée, c'était une pomme qui s'appelait une Macintosh, comme par hasard. Donc machine de turing, qu'est ce que c'est ? C'est une bande.

1:01:55
Infini, vous prenez une comme une pellicule photo, une bande infinie avec des cellules, et puis vous mettez une tête de lecture qui peut se déplacer à droite ou à gauche. D'accord, vous coupez la bande à un endroit en disant, ceci est ma cellule numéro un, elle est peut être infinie à droite, mais vous y résumez plus loin que la gauche et la bande va se déplacer de cellule en cellule et à chaque fois elle va tomber sur un caractère à l'intérieur. En fonction du caractère, la tête de lecture va faire quelque chose, retourner au début.

1:02:22
Inverser les 2 cellules suivantes et ainsi de suite. Ben en fait la bande elle représente quoi ? Elle représente votre ordinateur. Les lettres représentent le jeu d'instruction en assembleur et les cellules représentent la mémoire qui est infinie. Si vous arrivez à avoir un algorithme ou quand on rajoute des entrées, on n'a pas une mémoire qui évolue de manière exponentielle en explosant si c'est encore une une augmentation contrôlée ou si le nombre de déplacements de la tête est encore contrôlé.

1:02:50
Alors vous êtes en mémoire et en temps polynomial. Sinon, vous êtes non polynomiale. P égale p une des grandes questions de l'informatique. Je reviens à Crypto avant que turing fasse ses travaux.

1:03:03
Les Polonais avaient mis la main sur enigma. Marianne Reyjouski avait construit ces fameuses bombes, ces trucs électrométaniques qui faisaient TIC, TIC, TIC. Donc on pensait que c'était de la bombe. C'est lui qui a fait qui a posé les bases des travaux d'analyse exhaustive que Turing a repris derrière. Vous avez ici la technique utilisée par Turing dans Colosus. Je vous envoie, c'est juste à côté de.

1:03:30
De chez Red Bull, c'est à côté de Bletchlepar, c'est à côté de Milton Keynes, alors on continue les solutions cryptographiques. Par exemple si on a un chiffrement polyalphabétique, donc une lettre qui devient plusieurs, on peut utiliser par exemple 1£ comme clé et là si vous voulez on n'aura plus de Pattern comme à l'avis génère. Donc si vous prenez Harry Potter première page, enfin premier bouquin page 34, ligne 18, caractère 32 et ainsi de suite, ça va être plus difficile de vous tracer, d'accord ? Vous avez également le councilman sypher, c'est à dire cette fois-ci c'est de la Stegano, pas de la Crypto.

1:04:00
Où là vous allez dire par exemple, je prends la première lettre de tous mes mots, Bonjour, il serait important d'écrire à notre curé pour son moustiquaire machin de Nana. Ben là, si on prend un sur 3, on fait le mot sécurité. Très bonne manière par exemple de créer des pass Word. Vous prenez des poèmes que vous connaissez-vous prenez la première lettre du premier mot, 2e du 2e, 3e du 3e et ainsi de suite, ou par exemple, PI la 3e lettre du premier, première lettre du 2e, 4e lettre du suivant, et ainsi de suite. Et vous créez des mots de passe. Tout le monde connaît PI.

1:04:29
Le poème vous le connaissez par cœur, si vous perdez le mot de passe vous savez le retrouver, d'accord ? Alors texte En clair ça s'appelle plain texte ou clear Tex, ça n'a subit aucune transformation texte chiffré, c'est ça ? If in texte, ça a subi une transformation, la clé, on a dit que c'était un grand nombre de bits et ça devait être aléatoire, assez grand pour que rappelez-vous les premiers slides, on ne puisse pas parcourir en bruit de force, on ne puisse pas attaquer, alors forcément ça dépend du temps, ce qui était vrai en 1900.

1:04:56
45 ici, enfin les années 40, 53 bits pour enigma, aujourd'hui 53 bits. Je vous ai dit ici, à ce niveau-là, 53 bits, vous faites tourner ça ? Copacabana fait tourner 56 bits en 20 Min sur votre bureau, mais on n'est plus dans les années 40, la guerre elle a été gagnée et donc aujourd'hui la question ne se pose plus. D'accord, c'est ce qui établit la force du cryptosystème, si vous avez une clé de 8 bits, vous avez 2 puissance 8, alors mettez pas des clés de 8 bits, parce que 8 bits ça s'attaque à la main hein, on est bien d'accord, c'est une.

1:05:26
Bonne raison pour se rappeler de ne pas faire vos algorithmes de crypto vous même. Ça prend 20 ans pour devenir cryptographe et moi même qui fait de la crypto depuis bien longtemps, je m'amuserai pas à faire des algo. Pourquoi ? Parce que en crypto tout est public et il faut que vous ayez déjà fait un certain nombre, que vous vous soyez déjà fait casser parce que vous avez peut être eu une idée géniale. Mais y a quelqu'un de l'autre côté de la planète qui connaît un truc en maths que vous connaissez pas et qui fait tout tomber. Donc vous prenez un algo, vous le soumettez à la Communauté.

1:05:50
Si vraiment tout le monde se casse les dents dessus après quelques années, on commencera à s'y intéresser. Mais réinventer la roue, non ? Sur alors vous avez ici des questions, des questions, questions, une fois 2*3 fois adjugé, vendu, OK, donc solution cryptographique, vous avez ici quelques algorithmes de chiffrement, alors on parle de description du procès, décryptage, principe de karshoff, tout est public. Par exemple, ici, vous allez avoir le des, le des qui commence par.

1:06:20
Une permutation initiale et ceci ici on va en parler dans quelques instants s'appelle la ronde de Festelle la ronde de Festelle qui est répétée 16 fois puisque là vous avez 3 petits points de k un à K 16 Donc vous allez avoir une clé qui va. On a des ce que je comprends, on a des collisions super, on s'y attendait donc on va avoir mais ça m'étonne. On n'a pas une collision sur le 25 janvier. Il me semble qu'il y a quelqu'un qui a le même anniversaire que moi. Bon c'est pas grave.

1:06:48

Vous allez avoir une clé qui va rentrer, qui va en donner des sous clés de K un à k 16. La clé K un va rentrer au niveau de la première ronde clé K 2 et ainsi de suite. Et au final comme vous avez une permutation initiale, vous avez une permutation inversée à la fin. Donc ce qui va se passer c'est que vous vous rendez compte que la partie droite ici rentre et devient la partie gauche, donc 64 bits à rentrer. Boum ils 32 de droite et tout de suite ils 32 de gauche. Par contre ceux de gauche ils vont être xore.

1:07:18
Avec quelque chose ici qui est une fonction F fonction F qui est fonction de la sous clé ronde, les 32 bits de droite. Et ça va venir donner ici le résultat d'entrée du xor avec les 32 bits de gauche, et ça va devenir la partie droite qu'on va donc retrouver directement en dessous et ainsi de suite. Et la partie gauche sera abîmée. Donc à chaque fois vous abîmez la moitié de votre clé, la moitié de votre texte.

1:07:48
Moitié droite ou gauche et une sur 2 alors ceci c'est le des des qui est un des premiers algos dans les années 70, enfin le premier même qui a été fait avec les principes de kirchhoff, on va parler de son histoire tout à l'heure, le 2e. Alors ici on manipule des boulets hein, on manipule des bits, on est sur du 0 et du un, le 2e C'est RSARSA, ici on est en théorie des nombres, on est sur des maths, alors théorie des nombres pour être très clair.

1:08:17
C'est pas la la question c'est pas est ce que les nombres existent ? C'est une théorie ou pas ? C'est un domaine des mathématiques qui est sans doute considéré comme le domaine le plus pur, le domaine le plus propre, celui où il y avait pas d'application militaire. C'est à dire que si vous me parlez de probabilité, si vous me parlez d'ensemble, si vous me parlez d'Équations différentielles, je vous donnerai pour chacune l'application militaire.

1:08:48
Je vous parlerai de virus, de bactéries de décollage, de fusée ou de roquette et ainsi de suite. Et chaque truc a une application militaire. Pendant des années la théorie des noms n'en avait pas, c'était le domaine vierge, un toucher y avait pas de MAT et puis là ça arrive et tout d'un coup la factorisation des composites j'ai bien dit des composites la facturation des premiers parce qu'en premier ça se décompose en un fois lui même la factorisation des composites va devenir.

1:09:14
Un problème central de la cryptographie. Et là tout d'un coup, tout le monde veut en être. C'est la le la bulle de l'an 2000. Mais dans les années 70, si vous êtes un matheux que vous travaillez en factorisation, là il y a du travail tout d'un coup. D'accord, on va travailler, on va traverser RSA dans quelques instants. Puis de l'autre côté vous avez, pour montrer des diversités, un autre algorithme qui s'appelle poufish qui lui a été soumis comme candidat à.

1:09:42
L'a ES, c'était un des candidats AES vous aviez too fish, mars serpent rendall, mars serpent, too fish rendal et comment s'appelle le dernier verset 6 et au final c'est rendall qui a gagné. Donc description de l'algo, tout est connu, tout est expliqué, il y a pas de Secret, alors on va parler de qu'est ce que c'est qu'une signature, une signature ? D'où vient la notion de signature ? La notion de signature digitale ?

1:10:09

On va vous expliquer ce que c'est, mais d'où ça vient ? Initialement ? Ça vient de Monsieur Kennedy qui dit à la NSA, vous allez enfin ouais, vous allez me créer un truc ou quelqu'un peut donner un ordre, tout le monde peut le vérifier, mais personne ne peut contrefaire l'ordre, d'accord, mais un ordre de quoi ? Un ordre de tir nucléaire par exemple, ouvrez le feu, un ordre présidentiel.

1:10:40
Ben on veut que tout le monde puisse vérifier l'ordre du président l'exécuter, mais on ne veut pas que l'ordre puisse être contrefait. C'est un besoin de signature et à vrai dire le besoin de signature initial. Alors à l'époque, on n'a pas d'algorithme de la charge, on n'a pas de système. On parlera de la charge tout à l'heure qui va nous permettre de prendre une information, la condenser, d'écraser dans un.

1:11:08
Truc qui sera a priori unique. Donc c'est pas comme ça qu'on va faire des signatures. Les premières signatures vont être construites par une une technique de redondance. On va on coder la même information 2 fois mais au final on va réussir à avoir des h. Aujourd'hui les h sont CHA 256 CHA 3 qui s'appelle chaque et ainsi de suite. Et donc une signature c'est quoi ? On prend un message, on le h et on va appliquer ce qu'on va appeler une clé privée au h.

1:11:38
On a pas parlé de h on a pas parlé de vie privée ça arrive mais j'explique juste que signature c'est 2 actions alors un algorithme il doit être résistant à la cryptanalyse oui s'il vous plaît est ce que vous pouvez répéter s'il vous plaît le la dernière slide et c'est coupé chez moi je sais pas ce que c'est que mon Ah couper je vous écoute. Est ce que vous avez entendu une dernière chose, le dernier, le dernier slide dernier la précédente.

1:12:08
Le slide d'avant celui-là le slide d'avant oui non c'est c'est pas celui-là le prochain, le prochain oui signature le mail alors qu'est ce que c'est que vous avez entendu là dessus ? Parce que j'ai parlé de Kennedy, vous avez entendu ça ? Oui vous m'avez, vous avez expliqué comme quoi la signature numérique c'est de à propos de 2 actions. Ah oui c'est ça, c'est 2 actions, on prend ce qu'on veut signer, on va le hacher.

1:12:37
On va, on va, on va faire un Ah, on va tenir un condensa ou un die just et sur ce die Just on va appliquer une clé privée. Alors je vous ai pas encore expliqué ce que c'est qu'une clé privée ça arrive mais signature numérique digitale 2 actions. Premièrement on h de on applique la clé privée d'accord des exemples de fonction de h c'est sh 256 ou Sha 3 Sha ça veut dire Secure H algorithm on y arrive, c'est juste pour.

1:13:05
Vous donner une introduction signature numérique, c'est 2 actions, mais on y arrive, on va, on va étudier ça. Qualité de l'algorithme, c'est un problème qui doit résister ? Un algorithme, ça doit résister à la cryptanalyse, c'est à dire aux maths, c'est étudié mathématiquement, tous les coûts sont permis, il faut que les calculs soient complexes, il faut que ça explose, il faut que vous ayez des.

1:13:27
Ça requiert des capacités de stockage qui sont façon de parler plus grandes que le nombre de BIT dans l'univers. Il faut qu'en ayant tous les super calculateurs dont on a parlé au début, vous puissiez pas passer ainsi de suite. Il faut qu'à priori y ait pas de faiblesse de porte dérobée. Il faut que ce soit

simple et rapide. Si on connaît la télé difficile, si on la connaît pas. En gros c'est les contraintes d'un algorithme de cryptographie. Des questions OK, un cryptogramme ?

1:13:58
Rectogramme, c'est ce qui a été chiffré mais il y a pas de structure particulière à priori c'est aléatoire. Si on réutilise la même clé et qu'on a une toute petite variation du texte en entrée, ça doit être très différent. Mais pense ça doit pas être comporté de manière linéaire en sortie par rapport à l'entrée ce serait très très mauvais. Puis ça doit pas être non plus beaucoup beaucoup plus, beaucoup beaucoup plus long que le texte. En clair si je rentre 5 kilos et que j'obtiens 5 mégas en sortie c'est pas bon.

1:14:24
Votre lait, elles doivent être bien gérées, elles doivent être a priori aléatoires, et Ben elles vont poser des problèmes puisque comme elles sont aléatoires, y a tout un tas de systèmes d'optimisation de ci, des ça dans les implémentations qui risquent de se planter puisque y a rien de plus difficile à à travailler que l'aléatoire. On est bien d'accord que les techniques de compression, les ci, les ça sont l'aléatoire, ça marche pas terrible hein ? Ben si vos laits sont aléatoires, elles vont poser des problèmes.

1:14:53
Mais c'est requis, c'est requis. Alors il y a 2 grands styles d'algorithmes, le premier c'est les substitutions, c'est à dire qu'on va remplacer un symbole en un autre en fonction d'une clé. D'accord, donc vous voyez, halo donne PJJK. Alors ça veut dire quoi ? Ça veut dire que le LL il donne le JJ ? Mais là aussi je regarde en disant Ouais mais ce truc là il est pas linéaire parce que Regardez J et k C'est 2 lettres qui se suivent, d'accord, mais l et o C'est pas 2 lettres qui se suivent dans l'alphabet.

1:15:23
Donc ici j'ai une substitution, j'ai pas juste un petit décalage. Les choses sont devenues n'importe quelle lettre est devenue n'importe quelle lettre, alors vous pouvez le faire sur un bit, vous pouvez le faire sur un caractère, vous pouvez le faire sur un groupe de mots ainsi de suite. Mais on va avoir principalement 2 actions, la transposition ou la permutation et la et et de l'autre côté la substitution, donc substitution elle va amener des non linéarités on peut remplacer tout partout transposition ou permutation, c'est les décalages.

1:15:52
On garde les mêmes lettres, on les met dans un autre angle. D'accord, oui, j'écoute. En fait ma question, c'est se base se se trouve au niveau de de l'aléatoire, en fait, parce que le fait de dire que c'est aléatoire, on récupère quand même la valeur de quelque part, mais sauf que la probabilité, la probabilité d'obtenir cette valeur est faible. Si je me trompe pas. Maintenant la question c'est à partir de quelle probabilité on considère qu'on est dans l'aléatoire ?

1:16:19
À partir duquel on considère qu'on ne l'est plus. D'accord ? Alors c'est la la la question en anglais, orland is a piece of strings twas the lance from the middle to the end. Quelle est la longueur d'une corde ? 2 fois la longueur du milieu à la fin. Donc il existe des tests, il existe des tests, des tests aléatoires si on veut regarder le fixe.

1:16:44
Le Nist, le nist a des tests de de tête 800 points 22 un et ainsi de suite qui vont avoir des requis pour la crypto. D'accord ? Alors il y a, si on fait des tests il y a, on va essayer de regarder des marches

aléatoires, on va essayer de regarder des compressibilités, on va essayer de regarder des patterns, de regarder des spectres, de regarder tout un tas de trucs et de décider si c'est ou si c'est pas. Donc en gros.

1:17:12
Le quand est ce que il faut se remettre au on peut aller voir une liste directement ce que une liste écrit je dis 800.22 est ce que quelqu'un peut vérifier si sur Google que je peux le faire sur mon téléphone ici liste 800.22A ça doit être un truc sur l'a LR de tête ou alors je suis déjà gâteux mais c'est possible. La journée fut longue. 800.22A nist ça doit être de l'a LR Row homeless testing voilà donc c'est la réponse, elle est là.

1:17:40
Il y a des valeurs, il y a des valeurs qui vous disent si vous avez tant de répétitions ça passe pas machin. Maintenant le vrai problème il est pas là le vrai problème il est que von Neumann nous disait quiconque veut générer de l'aléa sur une machine à État Fini est en état de pécher. C'est à dire que si vous êtes sur un truc qui est a priori déterministe pour un État donné, donnez-moi l'État pour vous donner votre transition. Je sais où est ce que vous allez aller, Ben il y aura pas d'aléa donc vous allez avoir des générateurs pseudo aléatoires pseudo PSEUDO.

1:18:11
Mais si je connais cette information, je vais vous attraper. Donc comment on fait de la génération aléatoire sur sur un PC ? Ben on va aller chercher si on fait pas attention à se rattraper. Déjà elle a Netscape en disant Oh je prends le numéro du PID de mon process, patati patata. Il y a pas assez d'entropie, il y a pas assez de variation. Au final c'est équivalent à allez 40 bits et 40 Bits c'est quelques milliards, on peut tester toutes les valeurs.

1:18:35
C'est à peu près le je vais vous le dire autrement, vous avez déjà dû voir des gens dans la rue qui vous disent Je vous donne 100$ si je peux deviner si je devine pas votre âge à plus ou moins 5 ans, Bah écoutez je suis désolé pour ces dames ou ces Messieurs, mais il y a déjà tout un tas de paramètres physiologiques qui vous permettent de deviner la de quelqu'un. D'accord ? Les rides, la couleur, les cheveux, la taille, le style, ça le poids et avec plus ou moins 5 ans ça donne une marge de 10 ans. Généralement les 100$ ils les gagnent des gars, enfin ils les gardent.

1:19:04
Très peu de gens gagnent mais c'est la, c'est c'est à peu près la même chose ici. Ouais, il faut vraiment être exceptionnel à 75 ans pour ressembler à à quelqu'un de 40. C'est à peu près la même chose ici. C'est à dire que au niveau aléatoire, si vous allez pas chercher quelque chose sur des bits de points faibles, par exemple au niveau d'un micro ou sur l'attention aux bornes d'une diode dans un processeur en utilisant des effets de température ou simplement par exemple, vous allez aller chercher comme chez untel.

1:19:35
Vous rentrez des cochonneries dans l'a s vous chiffrez la sortie aléatoire mais si vous essayez de faire votre propre générateur dans votre coin, passez-moi les l'expression ça risque de vous ***** au visage. Donc oui il y a des tests, ils sont connus, nist 800.22A est ce que j'ai répondu à la question parfait donc rappelons-nous substitution ça peut être mon linéaire transposition ou permutation alors substitution.

1:20:03
On est remplacé par des lettres ou des symboles, ça crée de la confusion, ça crée de la non hérité, ça permet de diffuser l'information et y a une relation entre l'ATHLÉ et le cryptogramme, et elle peut être complexe, transposition ou permutation. Mais cette fois-ci ça revient à dire je vais prendre les choses, je vais mettre dans l'autre ordre, mais ça revient à une factorielle un fois 2*3*4 jusqu'à n qui est l'exemple classique du calcul pour les programmeurs sur la fonction récursive type, ça permet de diffuser les statistiques, alors attention.

1:20:33
Dans certains cas, on en parlera tout à l'heure. Il faut éviter de créer des structures de groupes en mathématiques parce que alors vous avez toujours des groupes. Je suis gentil de dire qu'il faut éviter des structures, mais il faut éviter de faire des trucs qui soient trop évidents parce que vous allez vous faire attraper. Alors vous avez peut être un jeu de 52 cartes, mais y a que 52 factorielles de de mettre ces cartes dans un certain ordre. 52 factorielles c'est peut être énorme mais le nombre il est limité, d'accord ?

1:20:59
Substitution simple, elle est facile à casser par la fréquence d'origine, par le calcul fréquentiel. Je vous ai dit, la contre-mesure va être d'avoir plusieurs substituts pour une lettre. C'est ce que les algorithmes complexes ont essayé de faire de manière efficace. Alors en cryptographie, vous allez avoir la cryptographie symétrique. Alors chiffrement de flux à 5 à un dans les GSM qui a eu quelques problèmes et RC 4 que je vous conseille pas du tout même s'il est très simple.

1:21:29
Chiffrement par bloc cette fois-ci alors chiffrement de flux et je vais vous montrer après mais c'est bit par BIT si vous avez besoin de 127 bits on vous en donne 127, vous en voulez 12, on vous en donne 12, vous en voulez 33, on vous en donne 33. Chiffrement par bloc AES vous dit Ben moi je chiffre tant de bits en entrée, c'est pas négociable, je fais pas 17 ou 24 vous voyez, moi je prends des entrées de 128 bits tout fiches pareil, donc là c'est des blocs mais en symétrique.

1:21:54
Tout ce qui est symétrique ici, Alice et Bob partagent la même clé. À partir du moment où on va pas partager la même clé et qu'on va être du côté asymétrique, vous allez reposer sur des techniques de maths comme des techniques de factorisation, non composite pour RSA, des techniques de Lobe discret, logarithme discret, où cette fois-ci vous allez changer la représentation. Par exemple pour aller dans les courbes elliptiques ou pour aller sur l'algorithme delgaman. Voici en gros les grandes lignes de la cryptographie.

1:22:20
Alors en photographie, vous avez un grand Monsieur, l'inventeur, le père, l'homme qui a inventé la théorie de l'information qui s'appelle Claude Shannon, c'est celui qui va amener l'algèbre bouléenne. Il a pas inventé l'algèbre de bulle. Monsieur bulle a inventé l'algèbre de bulle, lui a commencé à l'utiliser le MAT avec du vrai question. Alors je je, je vous en prie de poser une autre question parce que j'arrive pas à la lire ma question c'était lorsqu'on lorsqu'on on regarde si on prend l'exemple d'un réseau, non.

1:22:49
Une application comme WhatsApp, on dit chiffrement de bout en bout les chiffrements que les chiffrements qui sont utilisés ce sont les chiffrements par par bloc, par flux ou bien parce qu'on sait

que c'est les messages qu'on envoie sur WhatsApp, les messages sont plus ou moins longs les uns les autres, est ce qu'on fait du chiffrement par bloc, est ce que c'est par flux ou est ce que c'est du chiffrement ? Comment on dit ça ? Alors on reparle de cette question, vous la gardez, on en reparle complètement à la fin OK mais mais gardez la elle est très importante, elle est mais on en est encore au début.

1:23:16
Je vais essayer d'aller, je vais essayer d'aller vite mais on en reparle à la fin. Mais gardez la s'il vous plaît. Donc il amène la Jep bouleyenne c'est le père de la cryptographie moderne, c'est un des pères de l'intelligence artificielle. Il dit qu'un message chiffré doit apporter de la confusion et de diffusion et des systèmes à clé privée. Enfin clé secrète, pardon, on a écrit privé mais ça devrait être secrète, je vais le corriger ici, je peux pas le corriger mais rayez que les privés ici mettez que les secrets doivent.

1:23:45
Utiliser des clés d'une longueur au moins égale à celle du message chiffré. Donc il est en train de vous dire si votre clé est plus petite, vous êtes dans une position où j'ai pas envie d'être, faut qu'elle soit au moins égale, peut être plus longue, mais en dessous vous êtes mal. Pourquoi ? Parce qu'il va y avoir des patterns. C'est ce qu'on a dit tout à l'heure avec vigenère diffusion. C'est la modification d'une lettre d'Hitler qui doit modifier l'ensemble du message chiffré. On ne peut pas laisser le message chiffré morceau par morceau, ça tape sur l'ensemble.

1:24:10
La confusion c'est qu'il y a pas de relation mathématique algébrique simple entre le message clair et le message chiffré. Donc tous nos amis César, décalage de 3 machin, c'est là que ça s'arrête là maintenant on rentre dans le sérieux, d'accord ? Alors les solutions cryptographiques. Alors en symétrique vous avez une clé qui est partagée entre analyse et Bob et c'est la même pour chiffrer et déchiffrer. Alors si vous avez par exemple 8 personnes personnes une 2345678.

1:24:39
Ben le Monsieur en rouge, il a besoin de générer une 234567 clés. D'accord, donc les 8 personnes on en a généré 7, on en a généré n moins une. Mais c'est vrai pour ce Monsieur, c'est vrai pour ce Monsieur, c'est vrai pour ce monsieur. Ben d'ailleurs je vous l'ai représenté ici et ça on va le faire n fois donc n fois n moins une mais lui ?

1:25:07
Et lui qui sont représentés ici par ce ruban là ou ce ruban là, Ben ils ont la même clé puisque c'est la même clé dans les 2 sens. Faut donc diviser l'ensemble par 2, donc on est sur n fois n moins un sur 2 pour ceux qui adorent les mathématiques, gauss et ainsi de suite, on se dit si ça avait été n plus un, ce qui est quand même pas loin de la somme, la somme des n premiers entiers. Attendez, j'arrive, je vais voir votre question. Après Ben on est quand même sur une évolution en n carré.

1:25:37
C'est à dire que s'il y avait 50 personnes 50*49 ça fait 1225 clés. J'évolue, comme le carré du nombre de personnes, ça va vite augmenter ce truc là. Donc la distribution des clés un est sensible parce que quiconque met la main dessus le jeu s'arrête. Les exemples d'algorithmes s'appellent des triple, des AES, les clés de cession TLSSL machin ou les clés qu'on trouve dans IP 5. Donc j'ai intérêt à faire attention comment je distribue. Mais plus j'ai de joueurs, j'ai le carré du nombre de clés.

1:26:06

J'écoute votre question, Allô ? Il y a quelqu'un qui a mis une question dans le chat, je reviens pas tout à coup, je veux juste une information comme vous comptiez modifier le test, j'ai dit que vous ne pouvez pas le modifier parce que vous êtes en mode présentation moi de diaporama oui oui oui non c'est c'est pas grave je vais modifier je vais charger sur moodle après continuez voilà c'est ça vous modifiera après c'est pas que c'est faux hein, c'est juste que pour être précis je préfère parler de clé secrète que de clé privée. Je je je je ne dis pas que c'est faux, je veux juste être précis.

1:26:42
Cryptographie symétrique, donc, on parle toujours d'Alice et Bob Alice et Bob partagent une clé, on parle ici de l'algorithme ES triple DS, ainsi de suite, il y a un texte En clair, il y a une clé, on obtient un chiffré, ça c'est fait chez Alice, le texte chiffré arrive chez Bob, Bob prend sa clé et les chiffres, donc on doit avoir la même clé des 2 côtés, on doit l'avoir échangée de manière sécurisée parce que quiconque d'autre, s'il y a un 3e larron dans l'histoire, un C comme Charlie.

1:27:10
Yves Dropper, comme Estelle, ils ont tous des noms qui sont prédéterminés en Crypto d pour Dane et ainsi de suite on verra tout à l'heure Peggy et Victor. Ben si ils ont la même clé, je s'arrête hein, ils sont dans la communication, y a plus besoin la même crypto elle est cassée donc on doit distribuer de manière sécurisée. On doit conserver de manière sécurisée mais là-dedans y a pas d'authentification, y a pas de signature.

1:27:38
Alice pourrait se faire passer pour Bob. Bob fait passer pour Alice principalement. On utilise ça pour faire pour assurer la confidentialité d'une donnée. Je vous écoute. Quelqu'un a levé la main oui Bonsoir ce matin. Oui oui en fait je voulais juste revenir sur la slide où vous parliez des différents algorithmes de chiffrement.

1:28:02
Oui au niveau asymétrique je sais que depuis quelques temps aussi on parle beaucoup de du de la courbe elliptique. Est ce que à date elle reste encore la plus ? Je veux dire Sécur est ce qu'elle a été dépassée ? Où est ce que la courbe elliptique aujourd'hui ? la NSA depuis les 10 dernières années sur les courbes du nist a envoyé un message en disant arrêtez d'utiliser les courbes elliptiques, je vous recommande d'en utiliser que 3 qui sont sur des premiers.

1:28:32
Alors le premier P il doit faire 521 bits, 256 bits, 384 ou 256, tout le reste. Ils ont dit arrêter de les utiliser, pourquoi ? Parce qu'on pense raisonnablement qu'ils ont su les attaquer et les casser. Je pourrais même vous donner le nom de la personne qui l'a fait, mais je vais pas le faire ici, il suffit juste que vous sachiez que c'est deprecated et que ça a été cassé et on pense que le gouvernement chinois a fait la même chose, donc les problématiques étaient utilisées parce que je vais vous montrer tout à l'heure. Elles prennent beaucoup moins de place que une clé RSA.

1:29:01
Y a beaucoup beaucoup moins, de l'ordre de 10 fois moins mais aujourd'hui. Alors oui elles sont. Il y a quand même encore tout un tas de gens qui continuent à l'utiliser, mais c'est pas ce qui est recommandé par la NSA. Est ce que j'ai répondu à votre question, Allô ? Attention hein, vous allez trouver de la courbe en dehors de la NSA. Ce que vous allez trouver au cœur de Bitcoin, vos portefeuilles Bitcoin machin c'est de la courbe elliptique hein.

1:29:30
OK c'est bon, merci beaucoup. Alors David il est-il est 20 h, on va prendre la pause de de 10 Min et puis on va continuer après OK, ça marche, tu permets ? Oui oui oui, je t'en prie, POUM Poum Ben il est 08h02 à ma montre. Moi je reste là pour répondre à des questions, quoi que ce soit sur la première moitié si vous avez besoin.

1:29:55
Et puis bah dans 10 Min exactement on repart parce que c'est assez intense le contenu qui nous reste. On a fait 40 transparents sur une centaine donc on est dans les temps mais on peut pas trainer c'est ça ? Donc on revient à 20h00, 20h11, C'est ça ? Est ce qu'il y a des questions ?

1:30:47
Oui je vois accéléré, il y a pas de problème, je suis-je suis dans les temps, je suis pas inquiet, l'historique prend toujours entière, les mecs l'ont imprimé, on n'était pas sous forme électronique, ils ont pris le truc, ils sont passés devant les douaniers au Canada, PAM, PAM, PAM, c'est sous forme papier, ils sont allés de l'autre côté, ils ont fait une OCR reconnaissance de caractère et hop il y avait un fork, il y avait un PGP version internationale, donc aujourd'hui.

1:31:09
Il faut être très clair dans les algorithmes que vous avez par exemple chez la NSA suite A et B Suite a c'est des algorithmes militaires. Si vous êtes pas militaire vous allez pas en connaître. Y a des techniques qu'on connaît même pas. Suite B c'est la version des trucs pour les civils, courbe editique, RSA machin. Aujourd'hui il est gars, il sait même plus l'interdire ce genre de choses parce que c'est partout.

1:31:34
C'est partout, c'est dans votre téléphone, c'est dans votre carte bancaire, c'est dans votre frigo, c'est dans votre bagnole. Si vous saviez le nombre de fois où vous touchez de la Crypto dans une journée, vous auriez peur. Un adulte de nos jours je crois, pense en psychologie 800 fois au sexe dans la journée, vous faites plus de 800 fois de la crypto sans vous en rendre compte, donc essayez d'interdire, on va pas s'en sortir, il vaut mieux avoir une idée de ce qui se passe que d'essayer d'interdire. Alors maintenant ça veut pas dire qu'il y a pas des.

1:32:01
Des limitations à l'exportation ? Vous avez vasnar VAASENAR qui sont des accords non contraignants, mais la cryptographie est considérée comme une arme de guerre. Donc au même titre que vous pouvez pas exporter un chasseur, un réacteur nucléaire ou quoi, il y a des trucs en crypto et si elle de surveillance vous pouvez pas exporter mais c'est pas parce que vous allez faire du RSA de l'autre côté de la frontière que qui que ce soit va vous embêter. J'ai répondu à votre question, oui merci beaucoup.

1:32:31
Autre question, oui ma question qui était en attente, à savoir les applications à à les stades WhatsApp, Facebook et autres. Quand tu parles chiffrement de bout en bout, c'est c'est quel type de chiffrement que c'est ? Est ce que c'est par bloc ? Alors généralement ça va être un échange au niveau asymétrique, chacun aura une clé, on va pas voir derrière du symétrique pour aller à fond la caisse que ça va beaucoup plus vite.

1:33:01
Dans certains cas, on aura du chiffrement de flux, on va avoir des protocoles compliqués, on va avoir des protocoles qui vont empêcher des techniques de de rejet, on va avoir des protocoles qui vont empêcher ce qu'on appelle des attaques boomerang, des techniques de clic et ainsi de suite. Celui que vous pouvez regarder si vous si vraiment vous voulez vous renseigner là-dessus, signale l'application signal si chère à Monsieur Exet et ses copains, le protocole est complètement détaillé.

1:33:25
Vous pouvez complètement trouver les algorithmes puisque vraiment on voulait un jour qu'on s'asseye quelque part, qu'on en discute à votre disposition. C'est un ensemble mais c'est principalement de l'hybride. Autre question, vous avez dit l'application signal signal SIGNAL ? Oui oui signal signal vous avez pas vu le CE qui est arrivé au ministère ministre de la défense de de Donald Trump qui avait balancé du signal sur son plan d'attaque, il a utilisé signal comme pour communiquer son plan d'attaque sur l'outil y a quelques semaines. Ça dit rien à personne ça ?

1:33:57
Oui, il est vraiment drôle, c'est c'est ça fait, c'est celui-là, l'algorithme de signal il est-il est connu, il est documenté, c'est derrière. Initialement je crois que c'est marlin. Ah ***** comment il s'appelle marlin, Spike Motin, Spike, Ouais c'est c'est vraiment comme ça le gars qui a fait ça. Autre question, je vous écoute.

1:34:25
Moi j'ai une je pense que y a un peu de questions, il est 45 déjà moi j'en ai, moi j'en ai une pour vous, est ce que est ce que vous pouvez me mettre en un truc dans le chat en en en juste pas pas besoin d'un paragraphe ce que vous auriez ce que vous auriez aimé changer dans ce cours. C'est pas la première fois que je le fais, ça fait 30 quasiment 30 ans que je le fais, mais si vous pouvez me dire.

1:34:51
Je suis essayé de m'améliorer en permanence. Si alors je comprends bien. J'avais que 02h30 02h30, ça va aller vite, ça va dépoter. Mais s'il y avait quoi que ce soit, plus de moins de ci, plus de ça, ce serait bien. Merci je vous répète, vous avez mon email. David. Sami at gmail.com si vous voulez qu'on s'assey un jour autour d'un café, qu'on en discute du côté de Desjardins, j'y serai pas avant.

1:35:19
Mi-juillet mais à votre disposition. Bonne soirée à vous. Merci de votre attention et au plaisir de se croiser dans ce monde IT. Merci bonne soirée, merci. Bonne fin de soirée. Au revoir.

INF813-Séance09-20250611-PA02

0:02
Tu me dis quand c'est fait, oui oui c'est bon, c'est c'est fait bon. Donc en symétrique on va être plus rapide que la symétrique puisqu'on est sur des opérations bouléennes, c'est des 0ED un ça se déplace très vite, on va être robuste, la transmission des clés est sensible et le nombre de clés augmente comme le carré du nombre de participants. Ça amène la confidentialité mais il y a pas de manière de vérifier l'intégrité, il y a pas de manière d'authentifier la source.

0:25
Les algorithmes s'appellent triple des AESIDEA to fiche RC 5RC 6, ceux qui aujourd'hui sont considérés non sécurisés des ou RC 4 d'accord, alors on va prendre le chiffrement. J'utilise généralement le des pour expliquer. Je vais vous amener jusqu'à la symétrique, c'est sans doute le transparent le plus important, ce monsieur qui s'appelle Horsefestyle. Si vous Regardez cette partie là de droite, cette partie de la de gauche, Pardon, c'est le schéma de droite, mais la partie de gauche, C'est ce que je vous ai dit, la partie droite.

0:55
Qui passe à gauche, la partie gauche elle va d'abord elle venir rentrer dans un xor ici qui va être quoi ? La partie droite a subi une expansion, elle passe de 32 à 48 bits, elle prend un xor d'une soutenée, elle est ensuite refermée à 32 bits, elle est permutée et elle passe par le xor. En fait cette partie là c'est ça ici, donc elle a sous clé.

1:21
48 bits l'extension de 32 à 48 donc y a des bits qui vont se répéter et on va passer par les s box. Les s box c'est des boîtes s comme substitution des boîtes de substitution des boîtes de non linéarité qui vont prendre c'est des tables. Vous rentrez une valeur de 6 bits, ça vous donne une valeur de 4. Ce qui va se passer c'est que quand le des va être créé la NSA veut un des à 40 bits et facetelle et ses copains chez IBM puisque ça vient de chez IBM sont sur du 128.

1:52
Ça négocie, ça négocie 80 machin on se met d'accord sur 64 64. Je vous ai dit la taille de clé peut pas être plus petite que le message, donc 64 au niveau de la clé. Ah Ben oui mais en fait la NSA leur dit Ouais Mais vous voyez en fait chez BM votre représentation octal tous les 7 bits, y a un bit qui se répète machin si ce bit répété a été intercepté ça ferait mal. Donc vous me le virez donc 64-8 Ben 56 Bits.

2:17
En fait ce qui va se passer c'est que quand le design est fait chez IBM et qu'il l'a envoyé à la NSA puisque le la NSA a posé un premier appel d'offre qui a été répondu vide, il savait que alors seistol avait fait ce truc là qui s'appelait Demon DEMON d'où le nom du des initial, Lucifer Cifer un jeu de mots. Ils vont dire OK super, donnez-nous le design, on réduit les tailles machin mais quand le design part à la NSA ?

2:45
Il revient avec des boîtes s complètement différentes, ces boîtes de substitution qui sont vraiment des boîtes qui ne devraient contenir que des non linéarités pourquoi la NSA les a modifié ? On ne sait pas. Les NSA refuse de dire et donc il y a une personne qui est un jeune stagiaire qui est là qui s'appelle

Monsieur Merkel. Monsieur Merkel va se poser des questions en se disant mais Ralph Merkel qu'est ce qui se passerait si la NSA avait mis une bague d'or ? Qu'est ce qui se passerait s'il y avait 2 clés ?

3:14
Eh Ben il va commencer à réfléchir à un à des algorithmes avec 2 clés. Et Monsieur Merkel vient d'ouvrir la porte des chiffres asymétriques. D'accord. Donc le des aujourd'hui il est considéré c'est 16 rondes de fait comme insécure vous avez un truc qui est le double des bon double des c'est si vous aviez juste K un et k 2. Le problème de ça c'est que en allant dans ce sens-là.

3:36
Vous allez obtenir en armes de probabilité un certain nombre de sorties, mais vous pouvez aussi repartir dans le de la sortie vers l'entrée et Regardez s'il y a pas 2 trucs qui se joignent quelque part. Donc vous avez 56 bits ici à attaquer, 56 bits à ici à attaquer. Et si vous faites en double DS en double DS, en fait vous avez que 56 bits à attaquer après 16 rondes. Pardon j'ai, je vous écoute. C'est quoi la moitié NR sur commentaire question ?

4:06
C'est quoi le message dans le chat ? Allô ? Bon c'est pas j'ai pas le temps donc donc le 16 bits en en en en double des vous avez 56 bits à attaquer alors qu'en triple des ce qu'on appelle the meeting meet in the Middle.

4:27
J'attaque par l'avant et j'attaque par l'arrière et j'essaie de réconcilier les équations au milieu, ça va pas marcher. Par contre ici ce qu'il va falloir éviter c'est une structure de groupe. Il va falloir éviter que des puisse être l'équivalent de l'addition chez vous. Si je fais X +2+3+5, j'aurais pu faire X +10 directement. Le +2+3+5 c'est +10 parce que j'ai une structure de groupe. Donc si je peux faire de 2 des un seul des ou de 3 des un seul des, Ben ça ça reviendrait à un des et là j'aurais plus.

4:53
3*56 bits, j'aurai 56 bits de clé. Bah en fait on a montré que c'était pas le cas des n'est pas en groupe, d'accord ? Alors ici je vais vous parler une 2nde des canaux latéraux cachés qui était mon sujet de thèse. Si par exemple vous venez regarder la consommation de certains trucs qui font du des, vous Retrouvez IP les 16 rondes IP moins un la permutation puis si vous allez zoomer, vous voyez qu'en consommation vous pouvez voir passer des bits. Donc ceci est un problème. Les implémentations cryptographiques, si on fait pas attention, sont soumises à.

5:20
D'accord des attaques bon des est remplacé par les années 2000, chiffrement asymétrique AES où cette fois-ci on va avoir un nombre de ronds qui va être qui va dépendre de la clé. On va avoir une expansion de clé comme dans le des on va générer des sous clés, on rentre 128 bits d'accord et on va avoir une clé à 100208042012 ou 256 qui va définir la taille ici de nombre de ronds 10, 12 ou 14 d'accord.

5:47
En fait, qu'est ce qui se passe dans une ronde ? Vous avez ad runky subbytes Shift Row Mix Collomb, puis ad runky de la suivante, d'accord, enfin ad runky de la précédente Subbyte Shift Row Mix Collomb AD runky ça se traduit par quoi ? Ça se traduit par le fait que selon le fait que vous mettez un AD runky ou début à la fin, vous chiffrez ou vous déchiffrez d'accord, mais la ronde c'est toujours

subbyte shifro mix, colum ad runky ce qui marche très bien, ça va vous permettre par exemple chez Untel.

6:15
D'avoir des instructions qui vous peuvent permettre de calculer directement la ronde d'a ES d'accord ? Alors la substitution de byte, elle est ici le chiffre o il est là le mix colum et le Ham rounkey. En gros le s pardon l'a ES est principalement linéaire, vous avez une seule de ces opérations qui est massivement non linéaire mais pas se méfier. L'inconvénient à la limite, c'est que quand vous faites du chiffrement symétrique, vous dépendez du fait de pouvoir échanger via un canal sécurisé et de confiance. La clé secrète.

6:42
C'est là-dessus qu'à toute la sécurité du système. Si le système se prendre cette clé secrète, ça se dégrade, c'est fini, ça s'arrête, d'accord ? Donc si l'échange est mal fait, c'est terminé. Si on veut échanger avec plusieurs utilisateurs, faudra donc diffuser la clé à chacun de ces utilisateurs, ce qui augmente les chances de vol, d'interception, de compromission clé et ainsi de suite. Bon, y a 2 types d'algorithmes de chiffres symétriques, chiffrement par bloc dont je viens de vous parler ou le streamsipher chiffrement par flux, mais qu'est ce qu'il va passer pour le flux ?

7:12
On va avoir pour le bloc, on a dit on coupe à 641281042012 la taille du bloc, on chiffre tout, si on a moins on va mettre du rembourrage, on va chiffrer, on déchiffre, on retire le rembourrage, oui, sinon Ben on va voir un générateur aléatoire, on va alimenter un xor ici et BIT par BIT, mais si vous en passez 17, nous on vous en fourni 17, si vous en passez 23 on vous en passe 23, si vous voulez 25 on vous donne 25, c'est bit pas bit, ça va être plus rapide que le bloc, ça va être principalement utilisé chez les militaires, par contre faut rester synchrone.

7:41
Si à un moment on se décale, le jeu s'arrête de l'autre côté, le gars il pourra pas déchiffrer. D'accord ? Alors quand vous utilisez ces trucs là vous avez ce qu'on appelle des modes de chiffrement, le CB. Alors ça c'est des questions classiques du CISSP. Vous allez avoir l'e CB, l'Electronic, hotbook, le cipher, blockchaining, le cipher, freedback, l'amput feedback, le compteur, le GCM.

8:02
Ça fait un bon mode training avec XTS, on va en parler de tous, vous voyez qu'ils sont tous normalisés phips SP 838SP 838D 38E et ainsi de suite. Alors imaginons que je chiffre le pingouin, thux d'accord donc chaque pixel, bah chaque pixel c'est RGB, c'est un nombre de bits machin, mais excusez-moi si on utilise la même clé, Bah sur thux là j'ai plein de pixels qui se ressemblent quand même, le noir va rester du noir et donc ce que vous voyez ici c'est de chiffrer.

8:31
Mais moi je reconnais tux, hein ? Je suis désolé, je vous l'avez peut être chiffré, mais en gros, pour moi, vous avez changé les couleurs ici, puisque les pixels sont chiffrés indépendamment, la même valeur donne toujours la même valeur. Donc oui, ça peut être fait en parallèle, mais tout ce qui est répétitif réapparaît et 2 blocs identiques ont le même cryptogramme. Donc en fait, excusez-moi, mais je pourrais même venir modifier cette image. Et quand vous avez déchiffré, on va retomber sur ce qu'on veut.

9:00

Si je veux dessiner une petite croix ici ou quoi que ce soit, je la ferai réapparaître dans l'entrée. D'accord donc le problème que il y a peu d'informations, enfin s'il y a peu d'informations c'est utilisable mais il faut pas que ce soit sensible, faut pas que ce soit répétitif, sinon vous êtes foutu, d'accord donc pour empêcher ça et obtenir ce genre de chose, mais qu'est ce qu'on va faire ? Parce que vous voyez, j'ai pris le truc, je l'ai coupé, j'ai chiffré, j'ai chiffré, j'ai chiffré, ça m'a donné les morceaux. Mes 2 morceaux qui étaient identiques ont donné la même chose pour éviter ce genre de choses.

9:29
Je vais prendre la sortie du premier du premier, je vais venir faire un xor sur l'entrée du 2e, je vais chaîner mes trucs, cipher bloc, chiffrement de bloc, chaîner Ah bah oui maintenant mon xor ici va venir ***** si ces 2 là sont identiques, là maintenant j'ai plus la même chose qui rentre. Par contre c'est pas parallélisable lui je peux pas le calculer tant avant d'inculquer l'aiguille. Et puis pour casser le début ici il va me falloir un vecteur d'initialisation, va me falloir un truc qui commence ici, d'accord ?

9:57
Si j'ai une erreur, elle va passer de bloc en bloc. Où est ce qu'on utilise ça les courriels ? Chiffrement de fichier, transmission de données, mais chiffrement de fichier si c'est dans certains cas, c'est quand même pas le plus intéressant parce que on va prendre par exemple du compteur qui va être plus efficace. Le vecteur d'initialisation, il a pas à être secret, donc il peut être transmis, mais il faut faire attention à sa réutilisation. Elle peut vous coûter très cher parce que c'est un xor et il doit être unique et aléatoire. Donc on va parler de ce qu'on appelle ici un Nonce.

10:27
Pas le le le le le diplomate du Vatican number use ones on nonces d'accord, et donc on va l'utiliser pour une session, puis ensuite on va en trouver un autre. Donc le mode compteur c'est quoi ? Mais cette fois-ci c'est qu'on va avoir un compteur, donc ce qu'on va chiffrer c'est un compteur la clé on obtient la sortie et le truc qu'on veut chiffrer on vient juste sur un zor avec la sortie d'accord, donc ça par contre ça peut être fait en parallèle, c'est simple, ça peut être de taille variable.

10:55
Bah par contre vos compteurs si on commence à les connaître vous allez être mal. Puis l'intégrité elle est pas maintenue ici, donc ça c'est utilisé pour du streaming, pour du stockage c'est utilisé dans TLS, vous avez un autre qui s'appelle le cypher, feedback feedback pardon cette fois-ci c'est la combinaison de CBC et CTR d'accord, donc vous allez essayer de Démuler un chiffrement de flux d'accord pour des blocs de petites unités, donc vous avez toujours.

11:23
L'étage précédent qui revient comme un IV initialisation vecteur. C'est simple, si le déchiffrement est différent du chiffrement un peu sur AES, la limitation de la propagation des erreurs Ben elle est due à la synchronisation et c'est versatile sur la taille en fonction de la taille de bloc. Par contre ça propage des erreurs, c'est sensible à la cryptanalyse en texte En clair connu et c'est utilisé dans des terminaux communication classique et ainsi de suite. D'accord donc vous chiffrez vecteur d'initialisation.

11:52
Vous prenez votre entrée, vous venez de zorer avec la sortie, ça vous fait ça ? Et puis on repart chez le suivant et on recommence et on recommence et on recommence. Bon vous allez voir pour Wikipédia, pour déchiffrer pour chacun de ces modes là, mais c'est relativement simple, dans chaque cas vous

avez l'o FB qui est là, un peu de feedback, alors cette fois-ci c'est similaire. Oui j'ai une question, s'il vous plaît je vous en prie, vas y oui ma question sera concerne Laurent bourrage.

12:14
En fait oui, lorsqu'on si, si, on en a le cas de chiffrement par bloc, on on suppose que prenons le cas où le message ne suffit pas sans le bloc de 128, c'est à dire qu'il faut faire un rembourrage, les valeurs qu'on choisit, ou bien les données qu'on utilise pour rembourrer ou bien pour compléter le bloc que ça appelle 128. Ouais, ce sont des données standards, ce sont des standards. Oui, on va mettre par exemple 01000, on va marquer du rembourrage.

12:39
Et on va généralement donner un bloc en plus pour dire parce que maintenant vous allez me dire Ouais mais vous êtes mignon avec votre 01000, mais si c'est exactement ce que je veux chiffrer exact, Eh comment je fais ? Eh Ben on va rajouter un bloc en plus pour dire en présence de rembourrage ou pas. Ah OK, donc il y a un bloc qui signifie c'est un rembourrage en gros ouais, c'est ce qu'on fait, OK d'accord. Donc autre question, pardon, non OK, j'avance output feedback, c'est CBDR ou CFB.

13:09
Sauf que cette fois-ci c'est la clé chiffrée qui va être le vecteur en initialisation. La propagation des horaires est limitée parce que vous avez une synchronisation, c'est versatile sur la taille de bloc, ça propage des erreurs. Malheureusement c'est plus sensible encore que la Cryptanalyse en à à texte connu c'est bien si vous avez de la communication Bruitée ou du chiffrement de fichier d'accord, alors vous avez le GCM, le Gallois Quantum mod.

13:38
Cette fois-ci, vous allez avoir un calcul d'intégrité, c'est efficace, c'est parallélisable sur les Processeurs untel, ça marche avec une instruction. À l'époque que j'avais, j'étais l'ingénieur qui l'avait vérifié, c'est le PC mule QDQ. C'est complexe, ça a besoin d'une génération, de nouvelles clés, d'une rotation, d'une dérivation. Après une certaine quantité de données, vous allez avoir besoin de compteurs et de nonces.

14:05
Par contre ça tourne partout, la 5GLIP SEC, le LTE, le TLS, le Wifi 5, le Wifi 6, la messagerie, les transactions de stockage. Vous avez du GCM partout de nos jours ? D'accord ? Parce que la multiplication dans le corps de galois là celle-là ça veut dire quoi ? Ça veut dire que c'est une multiplication booléenne sur laquelle vous avez pas de retenue vous propager, pas les retenues. Donc en gros ici là vous avez des multiplications sur le corps de galois, ici vous avez des xor.

14:33
Et ici vous avez un h qui vient pour une sous clé, c'est très bien. Si vous voulez avoir de l'authentification, alors le XTS, cette fois-ci vous allez séparer la clé en 2 morceaux. Donc c'est résistant contre la manipulation, c'est rapide. Par contre c'est un peu plus complexe, l'implémentation est difficile, ça marche bien pour du stockage ou du système de fichiers.

14:57
D'accord, ça c'est des modes, je vous laisse aller regarder mais vous avez que ça peut s'utiliser de différentes manières. Donc si on regarde le des, on a dit que c'était des blocs de 64 bits, une clé de 56, il y a 16 passes. Et puis je vous ai donné quelques modes d'opération ici, ça a été approuvé par le le Nice en 1977, il a été remplacé en 2001 par l'a ES. Je vous ai présenté l'a ES et je vous ai dit.

15:19
Mais pour le des, la clé est trop courte. Je vous ai j'ai commencé le cours en disant voici ce qu'on peut casser par Copacabana sur son bureau, 50000$ en quelques heures ou EFF 9 jours de travail. Je vous ai expliqué pourquoi le double des est sensible aux attaques meet in the middle, vous attaquez par chaque bout et vous vous Retrouvez au milieu avec des problèmes de 56 bits. Et pourquoi si vous faites du triple des c'est pas le cas parce que vous pouvez pas vous retrouver au milieu de l'algorithme des il faut se retrouver entre 2 algorithmes et vous avez 3*16 rondes.

15:49
Alors l'a ES, il s'appelait initialement Rendall RIJNDAEL, il a été développé par John Damon et Vincent Reimann. On a parlé des autres finalistes, vous pouvez aller jeter un coup d'œil, mars RC 6 serpent tout fiche. Qui étaient les autres candidats pour la finalisation du groupe AES dans un futur rapproché ? On n'est pas trop inquiet les algorithmes post quantiques, enfin les pardon les ordinateurs quantiques pour l'a ES parce que.

16:14
L'algorithme, l'ordinateur quantique, il fera en gros une réduction de la taille de clé par 2. Donc comme vous avez de l'a ES en 256, ça reviendra à de l'a ES à peu près 128, ce qu'on appelle l'algorithme de grover. Maintenant vous l'avez partout, vous l'avez dans les firewall, dans winzip, dans bitlocker, donc du Wifi de l'a ES, il est partout aujourd'hui, c'est le nouveau des depuis 20 ans, ça tourne partout ce truc là. Alors vous avez des algorithmes comme IDEA qui était breveté bloc de 64 bits.

16:43
128 bits 8 passes. Je vous laisse aller regarder la description, vous le trouverez dans des trucs comme pgp par exemple vous avez blowfish qui a maintenant été remplacé par toofish qui a été fait par Bruce Neyer, David Wagner. Et puis je me rappelle plus du dernier auteur, y a pas de brevet, y a pas de licence, ça marche très bien. Tofish successeur de Bluefish, Finaliste de l'a ES 100208210056 ou 25010020892256 bits.

17:11
Quand même complexe au niveau du design, c'est un petit peu une machine à gaz quand même hein. Alors vous avez RC 4RC 4, ça veut dire run scod ou Rivers siffer le 4e du nom 1987 c'est un chiffrement par flux, longueur varie de 4 à 2048 bits. La robustesse est en doute à cause de systèmes où en interne on peut obtenir des États. Ça a été fortement utilisé dans les premiers wifi sur le web.

17:38
Algorithme simple efficace quelques lignes de code je le considère pas comme sécure, je pense qu'il est cassé aujourd'hui RC 5 un autre algorithme RC 6 pareil c'est le truc où vous pouvez aller regarder maintenant par vous même si vous voulez. Alors ici vous avez des tailles, vous voyez que on est en général sur des tailles de blocs de 64 jusqu'à 128. RC 5 peut prendre du 32 mais c'est une exception et puis des tailles de clé.

18:06
Et comme on a dit hein, Blowfish faut se méfier parce que blowfish peut prendre du 32. Et je l'ai bien dit, il faudrait pas que la clé également soit plus petite que le message DESS aussi 56 mais la clé est plus petite que le message. Je vais expliquer pourquoi alors c'est 5 de 0 à 2040. Bon faut faire

attention Skip Jack, algorithme américain très intéressant parce que la dernière ronde a été rajoutée pour.

18:31
En fait, ce qui Jack est beaucoup plus efficace si vous retirez la dernière ronde, la dernière ronde a été rajoutée de manière à abîmer l'algorithme à dessin. D'accord, alors certaines primitives cryptographiques. Il y a on a 10 2 types de chiffrement, chiffrement qui utilisent des modes différents, chiffrement par blocs qui découpent et chiffrement par flux. Mais vous avez également les macs messages Authentication authentification code qui ressemblent aux fonctions de h, donc ils sont combinés pour former des suites cryptographiques.

19:00
Ça permet d'avoir plusieurs choses, plusieurs propriétés en même temps, chiffrement plus fonction de la charge qui va nous permettre de vérifier l'intégrité. On va parler des fonctions, la charge de quelques instants et chiffrement ça amène la confidentialité. Donc si vous utilisez ça avec une partie un chiffre asymétrique, on arrive dans les chiffres asymétriques. Ben vous allez pouvoir échanger votre clé puis utiliser la partie symétrique pour sécuriser la connexion. On est donc sur un modèle hybride.

19:25
C'est le cas typiquement TLSSH machin, échange de clés sur l'asymétrique, puis derrière le symétrique pour aller plus vite, cryptographie asymétrique, je vous ai dit, on va avoir 2 clés cette fois-ci, chaque clé va être faite pour annuler l'autre. D'accord donc c'est un couple de clés, vous en avez une que vous allez donner à tout le monde qui va être votre clé publique et une que vous allez garder pour vous qui doit être votre clé privée. La publique doit être diffusée, la privée doit rester chez vous. Des questions jusque là pas de questions, OK.

19:54
Donc on va utiliser des mathématiques qui vont être une fonction à sens unique, c'est à dire que le calcul est facile à faire dans un sens, puis il est quasi impossible à faire dans l'autre sens. Vous allez me dire donnez-moi un exemple, Ben générer 2 nombres premiers très grands, on parlera de comment on fait ça après multipliez les entre eux, donnez-moi le résultat de sortie. Ben si vous connaissez les premiers c'est facile de leur donner un résultat de sortie. Si je vous donne le résultat de sortie que je vous dis trouvez moi les premiers. C'est un problème difficile, on ne sait pas le faire de manière efficace aujourd'hui.

20:21
Je vais me dire Oh bah attendez-vous êtes gonflés parce que 77 c'est 7*11 je lui dis Ouais 77 C'est 2 chiffres, moi je parle du nombre de 1024 bits, c'est à dire quelques centaines de chiffres. Ben on ne sait pas faire d'accord ? Donc ça va devenir quasi impossible à partir de la clé publique de retrouver la clé privée puisque on ne sait pas faire. C'est là où l'ordinateur quantique va faire très mal parce que lui y a des algorithmes qui lui permettent de faire et ça va nous permettre de dire Bah si j'utilise ma clé publique.

20:50
Moi je peux rien en faire de ma publique, je suis juste à donner aux gens. Et ces gens ils vont faire quoi ? Ils vont soit l'utiliser pour fermer des messages et me la renvoyer pour que j'utilise ma privée pour ouvrir donc du chiffrement. Soit je vais utiliser ma privée sur quelque chose et il va falloir que les gens utilisent ma publi pour l'ouvrir. Ça s'appelle une signature et c'est quelque chose. C'est le die Just

le condensat dont on parlait tout à l'heure. Donc on va faire soit de la confidentialité en chiffrement soit de l'intégrité sur signature donc.

21:20
On a une paire de clés public privé, on a une fonction mathématique qui l'un à l'autre, multiplication, factorisation, ou alors par exemple exponentielle et logarithme. Et on va parler de confidentialité, d'intégrité, d'authentification et de non répudiation, puisque si vous êtes le seul à avoir la clé privée, Ben il y a que vous qui avez pu faire cette opération. Donc RSA est développée en 1978 par 77, ça dépend par Rivest, Shamir et Adleman. Ça leur a valu un prix turing, l'équivalent d'un prix Nobel en informatique. C'est basé sur les difficultés de la Factorisation, c'est à dire Factoriser le produit.

21:49
De grands nombres premiers. J'ai bien dit le produit de grands nombres premiers c'est à dire en composite et pas un grand nombre premier un grand nombre premier factorisé c'est un par lui même donc vous allez prendre 2 nombres premiers PIQ vous allez multiplier ça va être votre clé publique OK c'est couramment utilisé pour faire de l'échange de clé de la signature numérique RSAYA plus de clés RSA au monde qu'il n'y a d'humain vous même sur vous aujourd'hui entre votre iPhone, votre monde, votre voiture machin, vous en avez déjà touché quelques dizaines.

22:16
Et puis ne serait-ce que cette communication qui est en HTPS. Alors parlons un petit peu d'inversion modulaire, si a est l'inverse de BB à l'inverse de a, Ben ça veut dire que un fois B vaut un d'accord. Donc on vous a raconté tout un tas de trucs au à l'école, le plus le moins le fois le diviser donc le plus le moins c'est l'addition de l'opposé, le fois c'est un certain nombre de plus et le diviser c'est l'inverse. Mais un opérateur dont on a le lieu de vous parler c'est le modulo, le Modulo c'est le reste de la division entière quand je retire un nombre d'un autre.

22:44
Autant de fois que possible, qu'est ce qui reste ? Quel est le reste de la division entière ? Je vais me poser la question ici, je cherche des nombres A et B qui va être égal à un donc a et l'inverse de BB, l'inverse de a module o 7, mais ça veut dire quoi ? Qui vaut un module o 7 c'est 7 plus un et 7 un certain nombre de fois, donc 0*7 plus un ça fait un une fois 7 plus un ça fait 8, 2*7 plus un ça fait 15, 3*7 plus un ça fait 22 et ainsi de suite. Donc je vais me poser des questions en disant un fois un Ben ça fait un.

23:14
2*4 et ça fait 8. Si je retire 7, ça fait un 3*5, ça fait 15-14, ça fait un 4*2 8. Mais si je l'avais déjà calculé 5*3 15, je l'avais déjà calculé. 6*6 36-35 5*7 35, ça fait un solution. Les 7 c'est pas plus capable puisque je travaille au 7.

23:38
Donc 123456 module au 6 module au 7 j'ai 6 solutions en fait je pourrais généraliser au premier et dire module au p premier j'ai p moins un nombre sur un inverse, le 0 n'en a pas. Mais qu'est ce qui va se passer ? C'est que ici vous allez avoir la clé publique, ici vous avez une clé privée et chacune va venir annuler l'autre. Il suffit de travailler avec des exposants et ceci va venir nous faire un un dans l'exposant donc vous.

24:06
Prenez des nombres, vous passez par des algorithmes millerabin sur l'obstraction et ainsi de suite qui

vont vous permettre de tester la primalité. J'ai pas dit de factoriser c'est pas pareil que c'est la priorité, c'est pas factoriser déterminer des nombres premiers et vous allez prendre un nombre e qui va être votre clé publique et calculer l'inverse de E modulo P moins un fois Q moins ce qu'on appelle modulo l'indicatrice de l'air. Ceci va vous donner votre nombre d alors ici c'est l'algorithme e cli, le Cli d étendu et ainsi de suite l'inversion modulaire. Vous avez votre clé privé.

24:36
Ben la publique et la privée s'annulent puisque prendre un message, un texto clair P le mettre à la puissance e clé publique. Quiconque fait ça et vous l'envoie, vous vous le mettrez à la puissance D des fois e valent un puisque ça a été construit comme ça, e l'inverse de DD, l'inverse de E et si vous vous Retrouvez avec Phi de n dans l'exposant P à la puissance de Phi de n, Ben vous Obtenez P.

25:04
C'est le théorème de la grange, ceci est RSA, faisons le ici, on va prendre des valeurs, donc on va dire que E c'est le public 2D, c'est la clé privée d'accord, et on va mettre des valeurs p vaut 41Q vaut 43 alors si c'est juste un exemple hein, dans la réalité ces trucs là font des dizaines de des centaines de BITS, le produit va de 1763P moins un fois Q moins un c'est 1680E.

25:32
Oui, il doit être premier. Avec ce nombre là on va prendre 143 et on va calculer l'inverse, modulo 1680 algorithmes euclide étendu on va avoir pour 143 un nombre d qu'on va calculer qui va être à 47. Ah oui 47*143 ça fait 6721, ce qui vaut un modulo 1680. Alors on est prêt, on ANE et D.

25:59
Ceci est un test, on convertit chacun en ascii, on prend le message à la puissance de D si on fait une signature E si on fait 11111 chiffrement modulo 1763, on envoie de l'autre côté message à la puissance e d'accord, et alors ? Notez bien que si vous voyez-vous passer des messages et que vous connaissez pas le D ici, il y a pas besoin de factoriser M, ça s'appelle un problème de logarithme discret. Si vous arrivez à.

26:29
Qui a la même classe de complexité que que RSA. Vous arrivez à répéter le système, donc clé de cryptage, déchiffrement, et vous avez le chiffré de l'autre côté. D'accord, donc les solutions cryptographiques. Si Bob prend la clé, pardon, si Bob prend, veut dire Hello à Alice, il prend la clé publique d'Alice, il chiffre, il envoie et Alice va déchiffrer avec cette clé privée. Si Alice veut faire quelque chose, elle dit je prends, je mets ma clé privée, j'envoie.

26:58
Et n'importe qui qui a la publique peut vérifier mais là ce qu'on va faire ici c'est pas je veux payer 500$. Ce qu'on va faire rentrer c'est le résultat d'une fonction de h c'est ça qui va donner une signature. Vous gardez votre clé privée pour vous, votre clé publique vous devez la mettre à un endroit où les gens peuvent la reconnaître. Le problème c'est que si vous avez pas d'autorité suprême, si vous avez pas quelqu'un qui dit oui, ça c'est la clé publique, Ben Moi demain je m'appelle Barack Obama et puis le jour d'après je m'appellerai Donald Trump, il suffit juste de mettre le nom en face et puis tout le monde pensera écrire à ces personnes là.

27:28
Donc il va falloir qu'il y ait une autorité, quelque chose qui est reconnu par tout le monde. De la même manière que votre passeport est reconnu par tous les pays qui reconnaissent le pays dont vous venez

pour dire Ah bah oui, cette personne elle vient bien de ce pays, elle a un passeport qui a été donné par le ministère de l'Intérieur. De cette là je sais qui j'ai à faire. D'accord. Donc vous avez des garanties d'intégrité et de non réputation, puisque si la clé privée n'a pas été compromise on est bon. Alors là l'avantage c'est que puisque vous avez une clé.

27:56
Par entité cette fois-ci on va croître de manière linéaire. Si vous avez 1400 personnes, vous avez 1400 clés. On a de la confidentialité, du chiffrement, de l'intégrité, de la non répudiation par le fait qu'on puisse pas abuser l'athlé de l'authentification. Par contre c'est de l'ordre de 10 à 100 fois plus lent parce qu'on fait des maths et des modulos par rapport au Boolé un au 0 et notre un et nos xor. C'est inapproprié pour les larges volumes de données.

28:19
Et puis si on travaille au modulo 2048 Bits et qu'on voulait travailler avec 20 Bits, Ben le résultat il fait encore 2048 bits. Donc le test chiffré peut être considérablement plus long que le texte. En clair on retombe sur les problèmes de padding. Attention ces problèmes de rembourrage et de padding, si vous les faites mal vous vous faites compromettre. Les exemples sont, RSA, la cryptographie, parcours elliptique ou d'efi elle même. Alors voici un canal latéral caché. Encore mon sujet de thèse, vous avez ici un chiffrement RSA.

28:46
Pour à cause d'un algorithme qu'on appelle Square and Multiply mètre au carré si ça vaut 0 ou mètre au carré, puis multiplié par la valeur si ça vaut un Ben si vous Regardez bien cette durée là par rapport à celle-là elle est plus petite donc je vais chercher les plus petites. Les marqueurs en rouge, rouge, rouge, rouge.

29:11
Partout ailleurs, je mets du vert et quand je tombe sur un Vert rouge, ça veut dire que je manipule un un dans ma clé privée. Quand je tombe sur un 0, ça veut juste un vert non suivi d'un rouge, ça veut dire que j'avais un 0. Donc ici j'ai rouge vert, ça veut dire un un vert vert vert 0 0 rouge vert un un rouge vert un un rouge vert un un allocilloscope je vous donne votre clé privée. Voici une faille d'implémentation question.

29:40
Pas de question super, vous m'entendez au moins ? Ou je vous ai déjà ? Ouais je vous ai mettre XC il y a plus personne qui bouge. Bon on a l'injection de fautes. Si par exemple vous prenez super super moi aussi moi aussi. Par exemple le laser, vous focalisez le laser à travers un microscope et vous mettez ici votre implémentation cryptographique, Ben vous allez vous retrouver avec des Photons Photons qui vont venir taper votre séium.

30:08
C'est le cas si vous allez dire Raspberry PI et que vous preniez des photos. Il y a pas mal de gens qui sont Ah je comprends pas, je prends une photo au Flash et Boum mon truc est reset. Ben oui parce qu'on a donné de l'énergie à la puce et puis qu'elle sait pas quoi en faire et donc on active le reset. Et bien ici vous donnez de l'énergie à des transistors. Il va bien falloir qu'ils fassent quelque chose avec et ils vont faire des trucs qui sont pas documentés, qui dépendent tellement de facteurs qu'on peut pas machin. Par contre ça donne un résultat qu'il faut et ce résultat qu'il faut comme derrière il y a de grosses structures mathématiques.

30:34
Mais dans certains cas on va vous compromettre ligo dans certains cas par exemple AES si la faute elle est bien placée c'est un coup et je vous donne la clé des ça peut être quelques dizaines voire quelques cinquantaines ou centaines de coups, mais ça peut être littéralement l'exemple que je prends ici de l'attaque par faute c'est un jour sans fin. Vous vous rappelez le jour de la marmotte ? Le mec qui se réveille tous les jours et qui revient le même jour. Moi je prends l'exemple de vouloir tirer sur Air Force One.

30:59
D'accord, le mec qui prend son flic sniper va se mettre à l'aéroport, va arriver à port One et POUM qui tire, il se fait arrêter par les flics pas cher nanana et le lendemain il se relève dans son lit et recommence. Vous allez me dire, ça a pas de sens mais ça a pas de sens. Sauf que on s'est rendu compte sur un force One il y a quelques années qu'il y avait un petit endroit de l'avion qui était pas blindé, petit Orion qui pas petit endroit qui était pas grand chose, c'était la salle de chirurgie.

31:19
Tu veux me dire qu'est ce qu'on s'en fout ? Ben dans les salles de chirurgie y a des bouteilles d'oxygène et si on met une balle dans une bouteille d'oxygène dans un avion ça fait boum et là y a plus d'avion, donc petit endroit qui quand même il aurait fallu se méfier, il aurait fallu le tester et pouvoir balancer plein de balles sur l'avion encore et encore. Donc c'est une balle qui descend en 747 militarisée mais là c'est la même chose, si vous arrivez à faire des reset, à automatiser, à tester, tester, tester, il suffit que ça pète une fois et là bye bye la machine de chiffrement.

31:49
Bon donc cryptographie asymétrique, Alice et Bob ont un problème de distribution de clé, il faut que Bob donne la clé à Alice. Alice va chiffrer avec la clé de Bob, y a que lui qui a la rouge qui permettra d'ouvrir la jaune, d'accord y a pas d'autre possibilité. Alors la signature c'est quoi ? Ben c'est cette fois-ci la clé privée d'Alice qui va être utilisée, donc elle va donner sa publique à Bob. D'accord, elle va prendre une donnée, elle va la hacher, elle va.

32:20
Faire une signature, c'est à dire qu'elle va appliquer cette clé privée au h d'accord et elle envoie la donnée et la signature. Elle lui dit Ben écoute, voici ce que je veux te donner, voici comment je l'ai signé quand toi tu vas le recevoir mais qu'est ce que tu vas faire ? Tu vas faire le h tu vas prendre la signature, tu vas annuler ma clé privée avec ma clé publique et tu vas trouver quoi ? Mais un h ce h là en fait normalement.

32:48
Et si ces 2 haches là sont identiques, ça veut dire quoi ? Ça veut dire que cette donnée elle a pas changé par rapport à la signature ? Donc en fait je te prouve que la donnée que t'as c'est bien la bonne puisque il y a que moi Alice qui pouvait faire cette opération que tu as contrée avec ma clé publique qui était une opération de clé privée. C'est une signature. Est ce que tout le monde a compris ? Il est nécessaire de pouvoir.

33:21
Distribuer et échanger des clés en toute confiance. Si les clés sont pas distribuées sécuritairement il sera impossible de de confiance. Encore faut faire attention à ce qu'on appelle l'attaque de l'homme au milieu ou Man in the middle, parce que cette fois-ci y a un attaquant qui va se présenter à Alice

comme Bob et à Bob comme Alice. D'accord et lui il va être au milieu à tout écouter, intercepter les clés, intercepter les messages et faire les 400 coups. D'accord donc le pirate cette fois-ci Alice pense parler à Bob, elle parle au pirate, Bob pense parler à Alice, il parle et le gars il est au milieu, il intercepte tout.

33:53
Est ce que c'est clair pour tout le monde ? Alice elle pense pas ça, elle parle à Bob Bob Bob pourra parler à Alice Ben oui, puisque il y a personne qui peut dire à Alice ceci est bien avec le public de Bob, il y a personne qui peut dire à Bob ceci est bien la clé publique d'Alice Ben pour ceci, pour contrer ceci, on va avoir besoin d'une autorité au-dessus qui dit je reconnais ton identité, toi Bob je reconnais ton identité à Alice, prenez utilisez le tous car ceci il va être le public de Bob, prenez utilisez la, il va être le public d'Alice et pour ça il faut une autorité.

34:20
On vient donc maintenant de créer un certificat, la clé publique. Il va falloir que l'autorité dise c'est bien la bonne, maintenir l'intégrité de la clé publique de Bob, maintenir la République d'Alice. L'autorité va utiliser sa propre clé privée et faire des signatures. Nous venons de créer un certificat, vous voyez ? Comme quoi c'est pas si compliqué que ça la crypto. Donc plusieurs mécanismes pourraient changer de manière sécuritaire, d'accord ?

34:50
Ben on va utiliser des mécanismes tels que Diffie Allemagne, j'y arrive dans quelques instants où El Gamal qui sont des fonctions mathématiques qui permettent de faire des échanges de manière sécurisée, où on va faire confiance à 1/3 avec des processus. C'est ce que je viens d'expliquer, une PKI, une infrastructure avec les publics. Donc dans ce cas il va falloir une système de gestion de clé de matériel de rôle, des procédures, passer des audits, respecter des normes et des standards qui garantissent l'authenticité et l'intégrité des clés d'accord. Alors un échange de clés d'efi elle même cette fois ci ?

35:19
Au lieu de faire de la factorisation sur n, on va faire du logarithme discret, on va. Alice et Bob vont se mettre d'accord sur G un générateur et Alice va, vous entendez pas, vous m'entendez ou pas ? Oui c'est bon je vous, moi je vous entends d'accord, oui oui donc dfi helman. Alice et Bob vont se mettre d'accord sur G et sur p un générateur, on va calculer g module op et Alice va calculer.

35:48
Une clé X calculée G à la puissance X module OP Bob va calculer YG à la puissance y module OP et c'est ce qu'ils vont échanger. Et comme quand on voit passer ce résultat, on n'est pas capable d'aller chercher le X ou pas capable d'aller chercher le y Ben celui qui reçoit g à la puissance y il balance son x au milieu, Celui qui ressent celui qui reçoit g à la puissance X il balance son y et on est bon. Donc c'est comme si on avait des peintures en commun et des peintures secrètes. On a un transport public, on fait la somme des peintures, on échange.

36:18
D'accord, et ce qu'on reçoit de l'autre, on refout sa peinture secrète dedans. Si vous Regardez ce qui est passé ici, jaune, vert qui ont donné un bleu avec le rouge, ça donne un marron puisqu'on a croisé jaune rouge qui a donné un orange, mais avec le bleu, ça donne un marron. Donc vous avez toujours ici jaune, rouge, vert, jaune, vert.

36:47
Rouge par contre de cette peinture là vous êtes incapables de savoir ce qu'avait donné l'entrée. Donc on se met d'accord sur un secret en commun, chacun de son côté sans le diffuser publiquement. On va générer un secret personnel et on va l'envoyer de l'autre côté. On va faire un mix et on va remettre son secret à l'intérieur. L'attaquant est incapable de savoir ici avec le jaune qu'il a vu passer, le bleu et le orange et quelles étaient les couleurs à l'intérieur.

37:17
Les solutions cryptographiques ? Ben il faut faire attention à la gestion des clés. Est ce qu'elle est partagée ou pas ? Est ce que il y a une clé publique et est ce que de l'autre côté il y a une clé privée ? L'échange de clé est ce que on le fait avec un mécanisme en dehors d'une bande ? Ou est ce qu'on utilise des clés publiques avec des certificats pour reconnaître que d'accord, les algorithmes et leur vitesse est ce qu'on est sur du public, pardon de la symétrie ou du symétrique ? Est ce qu'on est sur de la théorie des nombres ou des des booléens ?

37:45
Est ce qu'on chiffre des fichiers, est ce qu'on chiffre des des des des entités énormes ? Comment se fait notre distribution de clés ? Est ce qu'on a besoin de signatures digitales et quel est le service qu'on fournit ? Est ce qu'on fournit juste de la confidentialité, du chiffrement ou de l'intégrité de l'Entification voire de la non réputation ? D'accord donc bah le meilleur des 2 mondes c'est quoi ? C'est quand on va commencer par de l'asymétrique en disant mais voici ma clé publique, donne moi la tienne machin.

38:14
Et une fois qu'on va avoir fait ça, maintenant on a un canal sécurisé qui est lent mais dans lequel on va se mettre d'accord sur une clé ES une clé de cession. Donc l'échange il se fait en public. Et puis une fois qu'on a créé le CAL sécurisé, Ben on se met d'accord sur un nombre on va dire le canal est sécurisé et puis après on est on dépote en AES. En gros ceci est le principe de TLS ou dessm. D'accord, c'est le petit s du RHTTP alors ?

38:41
Des solutions cryptographiques mais les niveaux de sécurité le la quantité de bits qu'on devrait brut forcer en puissance de 2 de 80 à 256 aujourd'hui on est sur du 80 parce que je vous ai dit la NSA, si la NSA c'est PT 80 90 Bits, Ben il y a pas besoin d'aller beaucoup plus au-dessus au-dessus de ça, c'est pour ça qu'on fait des trucs à 80 donc par exemple du triple des et puis vous avez des tailles de qui sont équivalentes, c'est à dire qu'en RSA.

39:10
Du 1024 des nombres 2024 avec des premiers de 512 bits Ah, c'est équivalent à du 80 bits du 2048, c'est du 112 bits en puissance de 2, du 15000 bits, c'est 256, d'accord, en logarithme c'est un peu plus petit, c'est 160 jusqu'à 512. Alors après, y a plusieurs logarithmes, hein, Logarithme discret, courbe elliptique. C'est vrai que je vous dis la courbe elliptique, vous vous rendez bien compte que.

39:39
Elle est plus petite en taille 16211526385112 quand RSA fait 1024, 1003, 1007, 1000 et 15000. Beaucoup plus petit. D'accord vos algorithmes de h bon vous allez utiliser SHA chat du chat 2 du chat 3. Vous êtes bons. Des questions donc, en fonction du temps auquel vous voulez résister.

40:11
Jusqu'où vous voulez tenir, vous allez chercher l'un ou l'autre, alors vous avez keelens qui est tenu par un copain qui vous permet de d'aller voir ça. Alors ici c'est pour vous donner une idée des débits. En fait ça peut être bien pire que ça, mais vous vous rendez compte que on passe de mégabits 500 à 200 à 041601 et 2. C'est pour montrer les vitesses. Vous vous rendez compte que 502 cents c'est de l'a ES et puis là c'est de la clé publique en 2000 et puis en 15000 c'est encore pire.

40:41
D'accord, donc ça montre bien que RSA plus là le truc est grand, plus c'est lent, alors que AES ça dépote hein. Alors en asymétrique, en confidentialité, un message est chiffré avec la clé publique et il est déchiffré avec la privée. Ça, c'est qu'on envoie quelque chose à quelqu'un en utilisant cette clé publique. Quand on veut prouver l'origine, on va chiffrer avec la privée et ce sera déchiffré avec la publique, ce qui revient à dire une signature.

41:11
Puisqu'il y a personne d'autre que celui qui avait la privée qui a pu faire le coup. Si on veut faire de notre incidentialité et de la confidentialité, on va chiffrer avec la clé privée de l'émetteur, puis avec la clé publique du destinataire. D'accord donc je vais mettre une signature dans un chiffrement de manière à ce que personne d'autre ne puisse la voir. Alors un algorithme de d'Iffy elman, c'est ce que je vous disais tout à l'heure.

41:39
On se met d'accord sur un g, un générateur et un p d'accord, Alice a une valeur a, Bob a une valeur B et c'est g 2A mode PG 2B mode p on échange et on vient chacun mettre son truc à l'intérieur. Son petit secret à l'intérieur, c'est une distribution de clés, c'est ce qu'on appelle un IKEKE pour qui Exchange c'est basé sur.

42:08
La sécurité alors si vous travaillez module OPQ, c'est basé sur de la factorisation, mais dans tous les cas c'est basé sur du logarithme discret. C'est sensible le pack Man in the middle, parce que si quelqu'un vient ici au milieu, et c'est passé pour Bob à Alice, Alice pour Bob, Ben lui, il va déchiffrer. Mais il y a aucune authentication authentification qui est requise à la transmission des clés. Donc l'étage et le gamal, c'est autre chose, c'est le modèle de Diffie Hellman. Il y a des échanges de clés du chiffrement, c'est dans le domaine public.

42:35
Ça double la longueur du message, J'ai pas le temps de le couvrir ici, vous pouvez aller le voir par vous même, ça fait partie des choses ou si vous avez des questions vous me contactez. On en discute. Faut juste savoir que ça existe. C'est beaucoup des courbes elliptiques, alors cette fois-ci vous avez des courbes de la forme y égal X cube Plus AX plus B d'accord, et cette fois-ci vous allez avoir des propriétés, vous prenez un nombre p un nombre Q vous faites la.

43:05
Ligne qui passe par les 2, vous allez chercher le symétrique de l'autre côté, c'est p plus Q d'accord. Alors dans les propositifs, vous avez un nombre à l'infini, un nombre à l'infini qui va vous permettre de faire des projections. Vous pouvez aussi dans certains cas venir chercher des tangentes, la tangente ici en p pour venir calculer 2P et ainsi de suite, voir où est ce que ça coupe. C'est similaire à RSA, autant

je peux expliquer RSA très rapidement, même le padding machin na na na à quelqu'un qui a fait un un niveau cégep en.

43:35
Une semaine qui sera capable de le coder proprement autant si je veux vous expliquer les courbes dialectiques, si vous avez pas une licence en mathématiques, je m'approcherais pas. C'est horrible dans la la finesse du raisonnement et ainsi de suite, c'est ça peut être très très très compliqué. On parle de descentes infinies, de descentes de Vale descente de ferma, on parle de trucs, c'est c'est c'est des maths qui tâchent, donc ça permet de faire la signature numérique du chiffrement, de la distribution des clés.

44:03
C'est plus efficace que RSA ou DSA qui est l'algorithme de signature. C'est très présent dans les systèmes embarqués dans l'équipement sans fil parce que les clés sont plus petites, alors la longueur de la clé permet de déterminer la force du cryptage. Pour un système donné pour une même longueur, tous les systèmes sont pas équivalents. On vient de le dire, RSA 1024 c'est pas DSA 1024 et si vous voulez la même force c'est combiotique en 160. D'accord ? Alors qu'est ce que c'est qu'une fonction de h ? On en parle depuis un certain temps.

44:31
C'est quelque chose qui va apprendre à montrer une taille arbitraire et qui va avoir une sortie de taille fixe. Donc si on intercepte le message et l'empreinte, on peut altérer le message et recalculer l'empreinte. D'accord donc Fox à travers notre fonction de Eh nous donne ceci, The Red Fox jump over the Blue Dogs ça nous donne ceci, the Red Fox jump ou her. On va changer le V, ça change tout, on change l'ordre EV ça change encore tout.

45:01
On retire le V, ça change encore tout, donc il suffit que vous changiez un bit, ça change tout. En gros comment c'était construit ? Initialement on prenait un block Safer qu'on faisait tourner sur lui même plusieurs fois, ce qu'on appelle le modèle de Merkel Dan garde avec des constantes bien initialisées patati patata. Et ça donnait ceci, d'accord, fonction de h alors comment marche la fonction de h ? Ben je vous ai montré, prenez une entrée, vous avez une sortie, alors ici c'est MD 5 par exemple, MD 5 et aujourd'hui.

45:30
C'est une fonction à sens unique. C'est une fonction qui est facile à calculer dans un sens, mais qui est quasi impossible à recalculer dans l'autre le h, le condensa ou le die just. C'est une taille fixe, c'est en fonction de l'algorithme utilisé des questions. Alors on peut essayer de créer un fichier pour obtenir un h spécifique équivalent à un autre h et d'avoir ce qu'on appelle une collision, c'est à dire 2 entités différentes qui vont donner le même h. C'est de me dire oui mais.

45:59
Forcément qu'il y a 2 entités qui vont donner le MH. Vous êtes marrant vous parce que vous me parlez de trucs qui ont sorti ont par exemple 160 bits. Oui d'accord mais rappelez-vous que je vous ai montré que tout à l'heure 160 vous pouviez pas tester toutes les possibilités. C'est c'est pas possible, il y a pas assez d'énergie dans l'univers, vous avez déjà bouffé le soleil pendant 20 ans. Donc soit il va falloir faire des maths et des maths qui tachent et utiliser des ordinateurs puissants pendant longtemps alors j'ai une petite blague là-dessus, c'est que quand j'enseignais l'informatique, l'électronique à Epita, une école d'ingénieur française.

46:28
Et je faisais ma thèse, je disais toujours aux étudiants, si un jour vous pétez chat un, je prends votre photo, je la mets au-dessus de mon lit et je prierai devant vous tous les jours. J'ai un de mes étudiants qui est devenu directeur chez Google qui s'appelle Ellie Bernstein et c'est lui justement qui a abîmé chat un et donc j'ai dû appeler Ellie en lui disant écoute Ellie, tu te rappelles quand je te disais que j'ai pas envie de mettre ta photo ? J'ai pas envie de prier au-dessus de devant toi tous les jours. Il m'a dit non non mais on s'est compris, je je te relâche de ta promesse. Ce que je voulais dire c'est par là, c'est que la probabilité est très faible, c'est d'arriver, il faut juste faire attention.

46:58
Oui, on sait que ça va arriver, mais dès qu'on voit des fonctions de h qui vont dans le sens 2, on dit il y a un problème et on arrête. D'accord, il y a pas besoin de clé là-dedans. Ça permet par contre de vérifier l'intégrité d'une donnée. Si vous l'avez changée, vous avez bien vu que le h change en sortie. 5 propriétés essentielles, c'est déterministe, ça produit toujours la même empreinte, ça se calcule rapidement, c'est impossible de générer un message pour d'empreinte données.

47:27
Et il y a un effet d'avalanche, une petite modification en entrée, boum, il y a un gros impact en sortie, impossible de trouver 2 messages différents ayant la même valeur d'empreinte a priori c'est la notion de collision. Vous avez MD encore fait par Ron Rivost le R de RSA, elles sont plus considérées comme sécuritaires M 2 2MD 4MD 5MD 6 lui tient encore. Vous avez des trucs comme avale qui sont des blogs de 1024 bits ou RIP MD sur du 160 alors vous allez me dire.

47:53
Vous parliez de chat tout à l'heure, oui c'est curage algorithm qui a été développé par la NSA, c'est le flip 180 flip 160, il est plus sécuritaire, merci Eli chat 22124256384512 bits y a pas de problème chat 3 qui est basé sur la primitive qui est de chaque qui lui n'est plus le modèle de Merkel tannegaard c'est plus un modèle de je lance un block Safer, c'est un modèle d'éponge j'ai pas le temps de je vous dis hein, c'est un cours qui pourrait prendre 40 h, j'ai pas le temps d'expliquer mais on a changé de technologie, ça marche très bien.

48:23
Alors une collision c'est quoi ? C'est quand 2 entrées différentes donnent le même résultat de sortie bien évidemment, puisque on a dit on a 512 bits en entrée par exemple et 256 bits en sortie. Alors moi je je vous donne un exemple de collision, imaginez que vous ayez une photo en noir et blanc, d'accord, un carré en noir et blanc et c'est juste des bits à 0 et un d'accord, vous le prenez-vous calculez le xort de du coin en haut à gauche et du coin en haut à droite.

48:50
Et pareil en dessous, en dessous, en dessous, en dessous et votre carré, il va diminuer de taille de 2, il va, il va se couper en 2, il va devenir un rectangle et on recommence, on refait le zone et ainsi de suite, et à force de jouer à ce jeu là, vous allez tomber sur un bit, donc la moitié du monde tombe sur le 0 et la moitié du monde tombe sur le un. Bien évidemment là les collisions elles sont énormes, mais si vous étiez arrêté à un petit carré en dessous de la forme d'un QR code, ça commencera à ressembler à une fonction de hache, vous me suivez ? Alors mauvaise, parce que oui, on peut, vous pourrez anticiper patati, patata, mais.

49:17

Il faudrait juste que ce soit un peu plus complexe que le Dior, mais la fonction d'Eh ça ressemblerait à ça. D'accord ? Le problème c'est lorsque c'est contrôlable lorsqu'on peut contrôler les collisions. Alors avec ça on va faire des macs messages authentification code qui utilisent des empreintes et cette fois-ci des clés secrètes qu'on va partager. Alors il y a plusieurs types de Mac, les h, Mac, les CBC, Mac, les C, Mac. On va avoir le l'envoyeur qui envoyer un message, une clé qui passe par le message. Le message passe par le Mac, la grogne de Mac et il envoie son message et son Mac.

49:47
Le gars de l'autre côté reçoit le message A la même clé, il refait la même chose, il repasse le message, il obtient un Mac, il y a juste à comparer les 2, si ce sont les 2, Ben c'est que il y a personne qui a modifié le message. Alors une signature numérique, elle garantit l'intégrité d'un message, elle l'authentifie l'auteur du message, elle différencie de la signature écrite numérisée, signature numérique, c'est pas je prends un papier, je signe et je le scanne par la photocopieuse, c'est j'utilise des maths, du RSA et du reste pour aller chercher les structures mathématiques, c'est de la cryptographie asymétrique.

50:18
D'accord, donc on va passer par le h, le condensa, l'empreinte comme vous voulez, c'est ce qui donne la même chose. On applique la clé privée dessus et on a une signature qui va être vérifiée par la clé publique de l'autre côté en utilisant la donnée des questions. Vous me paraissez bien silencieux, ça va pas assez vite ? Vous voulez qu'on accélère ? Ah, je suis sûr que ça va vous réveiller ça.

50:47
Non, ça va assez vite. Bon, d'accord, solution cryptographique, donc digital signature standard, le DSS, qui est le standard absolu, façon de parler de la signature avec DSA normalisé, vous allez le trouver. DSA, c'est digital signature algorithm, c'est une variante du système delgamal, génération des clés, distribution des clés, signature et vérification, c'est en gros standard de signature numérique. Attention, ça requiert des nombres aléatoires si vous le réutilisez.

51:14
C'est comme Sony avec sa playstation, faire la boulette, abus sur le firmware, abus signature, merci, bye bye. Faut faire attention à sa génération aléatoire, surtout si on s'appelle Sony. Alors les solutions cryptographiques Ben en hachage vous permettaient de vérifier l'intégrité. En maths, vous pouvez vérifier l'intégrité et l'authentification. Avec dss, vous pouvez faire l'intégrité, l'authentification, la non répudiation, d'accord.

51:42
Par contre c'est une solution asymétrique, le Mac est symétrique et le hachage est juste un algorithme. Alors vous avez des exemples ici RSA permet de faire du chiffrement, de la signature et de la distribution de clés, pareil pour les cours elliptiques Difi, El mal ne fait que de la distribution de clés, El gamal comme RSA et ECCF fait les 3DSA ne fait que de la signature, le problème du sac à dos il est cassé, on l'oublie. Et puis Death, triple Death, bluefish IDEARC 4 machin, ça ne fait que du chiffrement d'accord et par contre.

52:12
Et la famille des MD ? La famille de chat machin, ça ne fait que du HH d'accord, il faut bien comprendre ces concepts là. Qu'est ce que c'est qu'une infrastructure à clé publique ? C'est quand on a une infrastructure et la clé publique repose essentiellement sur l'authenticité des clés publiques. Ces

clés n'ont pas forcément besoin d'être transmises de manière confidentielle, mais elles doivent être transmises de manière à vérifier leur authenticité. Oui les sources sont pas réfutables.

52:42
Donc les sujets peuvent avoir confiance dans les sources puisqu'on a une autorité suprême au-dessus. Donc une infrastructure a été publique ou PKI. C'est pour la gestion des clés. C'est une infrastructure qui regroupe l'ensemble des équipements physiques, les HSM, les PC, les machins, les logiciels, mais également les procédures humaines, les CP, les CPS. Donc c'est à dire les, les, les, les standards pour générer des certificats ainsi de suite pour la génération de clés. Alors le but d'une infrastructure.

53:09
De ce type, c'est d'avoir une chaîne de confiance de bout en bout pour différentes opérations cryptographiques, le chiffrement, la signature, l'authentification, la dérivation, parfois même de clés sans compromission, en utilisant des mécanismes de signature et de validation. Toute la confiance repose sur l'implémentation sur les technologies utilisées de son opérationnalisation. Je vais pas trahir de secrets, mais par exemple chez Desjardins. Et je pense que Dominique Brodeur a déjà vu quand il y était.

53:37
La salle dans laquelle on fait tourner nos ce truc là vaut 6000000 de dollars et c'est une cage de faraday blindée au 2e étage où il faut double badge pour rentrer. On fait pas tourner ces trucs là sur un coin de table. Et si vous êtes David Sami avec ses petites antennes en bas dans un camion, Ben vous avez 0 possibilité d'interception puisqu'on est dans une cage de faraday, on ne rigole pas avec ces choses là, pas quand on a quelques centaines de milliers à protéger, donc toute la confiance.

54:07
L'infrastructure repose sur une question des technologies utilisées, de son opérationnalisation et ça doit répondre à plusieurs normes standards. C'est pas défini sur un cost IT, sur un point de table dans un resto, il y a des normes, il y a des bonnes pratiques, il y a une industrie, il y a le nist, il y a l'anssi, il y a l'ISO, il y en a d'autres, et ensuite les normes ça ne s'invente pas. Alors à quoi ça sert ? Bah il y a une confidentialité qui est assurée par le chiffrement, ça permet de rendre des données inintelligibles à un attaquant. Si vous avez pas la clé, vous êtes dehors.

54:32
L'intégrité ça permet de s'assurer que l'information n'a pas été modifiée. Alors confidentialité c'est c intégrité c'est I et le A c'est l'authentification, ça permet l'identification de l'origine de l'information, le fameux CIA. Alors il y a des gens qui vous disent ouais mais a en fait c'est invalability, est ce que c'est disponible machin ? Comme disait le prophète, ça se discute, mais il y en a qui vous disent confidentialité, intégrité, authentification, et puis le n pour la non répudiation, si vous n'êtes pas l'émetteur que vous n'avez pas la clé privée, vous ne pouvez pas nier être à l'origine de messages de la même manière que votre banque vous dira.

55:01
S'il y a eu un retrait avec votre carte bancaire et que le PIN a été tapé, mais c'est vous. Si c'est la signature, oui, ça peut être quelqu'un d'autre, c'est facile à contrefaire. Par contre, le PIN, vous êtes censé être le seul ou la seule à le connaître. Les solutions cryptographiques dans une icp ? Ben on va avoir un certificat numérique, on va avoir une autorité de certification, on va avoir une génération et une destruction de certificat, une révocation. Ce certificat a été valable, il ne l'est plus aujourd'hui et donc une gestion de clé donc.

55:30
Vous allez avoir une sera une autorité de certification qui va émettre et recevoir, conserver du certificat. D'accord, vous allez avoir une RA, une autorité d'enregistrement, c'est lui qui vérifie les papiers, vous c'est bien, vous vous allez nous le montrer, c'est lui le notaire quoi d'accord, si lui il dit que c'est OK, il envoie la demande et si le certificat est émis donc vous faites la demande auprès de la RA qui valide, qui dit au CA c'est bon, vous recevez votre certificat, Ben il va vous permettre.

56:00
De vous identifier puisque maintenant on saura que Ben si le certificat de Monsieur vous Ben oui on va vérifier Monsieur vous ça a été émis par le CA. Ah Ben non c'est bon le CA on connaît, y a pas de problème d'accord, et donc quand on vérifie comment on fait, est ce qu'on vient perturber la CA ? Ben non, on a une autorité de validation, d'accord qu'y a une CRL Certificate Revocation List, on va la demander, le certificat il est encore valide ? Oui bon c'est bon Monsieur vous, oui mais on est bon alors.

56:29
D'accord, puis au CSP ça va même un un protocole pour demander de la signature sur du certificat, mais il est-il est en train de tomber en désuétude. Alors on continue, que du bonheur, on en est au slide 118. Je pense que vous allez bien dormir ce soir, on continue 119 le survol des composants d'une infrastructure avec les publics. On a dit l'autorité de certification, c'est le tiers de confiance qui permet d'authentifier les correspondants, donc ça va être délivrer des certificats.

56:58
Ça veut dire un certificat, c'est une identité numérique hein, et ça met c'est la base de l'identité numérique, ça met à la disposition les moyens pour vérifier la validité des certificats qu'elle a fournis. On va donner des noms Open trust en trust sektigo par exemple sont des générateurs des des autorités de certification, ça génère du certificat. Vous allez avoir une sous autorité parce que vous allez dire Ouais mais bon, l'autorité, moi. HSM, moi. HSM, c'est un serveur sous stéroïde qui fait pour résister à plus d'une soixantaine d'attaques dans le genre de celles que je vous ai montrées ?

57:29
Et on va dire, Ben oui mais je voudrais pas mettre ma racine sur le web, me faire exploser machin, donc je vais mettre une sous autorité, d'accord ? Par exemple, Microsoft appuie sur open trust la Registration Authority, celui qui vérifie vos papiers, c'est lui qui accepte la demande de certificat et qui fait la, qui authentifie le demandeur. SCCMMDM ce que vous voulez. La validation Authority, c'est la partie tierce qui offre un service qui assure la validité du certificat.

57:57
Donc la CRL qui vous dit CE certificat est révoqué ou pas et le online certificat de status protocole ? le CSP, le HSM, c'est le gros PC sous stéroïde avec des cartes crypto à l'intérieur ? Si vous l'ouvrez tout saute, c'est pas fait pour être chahuté, si vous le déplacez, qu'il est actif, tout saute, c'est vraiment du truc qui est fait pour calculer et qu'on lui foute la paix. Si vous jouez avec, il est programmé pour tout faire sauter en termes de clé. Quand je dis tout faire sauter c'est on efface les clés hein, y a pas d'explosion dans les data centers je vous rassure mais la.

58:26
Informatique, physique de la voûte, d'accord, c'est l'outil de gestion des clés privées, alors ça demande 111 crypto offisseur des des gardiens il en faut au moins 2. Alors on peut donner des noms,

Thales, Gemalto, Safelet, Luna, les pays chiites de Thales, les atalas, les futuristes, tout ça c'est des HSA. Et puis l'abonné, et c'est la personne ou l'infra ou l'entité qui dit Ben Moi j'ai besoin d'un certificat qu'il reçoit.

58:56
Voilà, c'est vous, c'est moi, c'est Dominique Brodeur. C'est des postes corporatifs, c'est des appareils, c'est des caméras, c'est des serveurs qui doivent interagir avec des machines ou des gens et être dans une infrastructure et faire valider qu'ils appartiennent, par exemple, à une société. Des questions. Autre question, OK, l'autorité de certification, Ben, elle est au cœur de la PKI.

59:23
D'accord, c'est elle qui maintient la cohérence du système et qui enregistre les certificats, qui est responsable de l'émission, de la maintenance et de la révocation des certificats sous son autorité. Si vous lui piquez cette clé privée, le jeu s'arrête. Allez voir ce qui est arrivé à Komodo COMODO au passé, vous allez comprendre. Ça revient à matérialiser le certificat quand vous avez une certification avec une chaîne de confiance. Si vous prenez votre passeport et la chaîne de confiance, elle remonte jusqu'au ministère.

59:53
Jusqu'au pays qui l'a émis. D'accord, passeport, c'est une pièce d'identité fiable, il y a un processus, c'est pas donné au hasard. L'autorité racine, c'est le le gouvernement du Canada, la sous AC, c'est le ministère de l'immigration, les citoyennetés, le Comptoir des passeports, c'est votre RA, votre VA, c'est les documents que vous avez prouvés pour fournir l'exemple, que c'était bien vous, un passeport d'avant, un acte de naissance ainsi de suite.

1:00:19
Le requérant, Ben, c'est le citoyen canadien. Et puis les utilisateurs de tout ça, ça va être les douanes, les compagnies aériennes, n'importe qui qui va vérifier votre passeport. Alors en termes de solution cryptographique, il faut s'assurer que le certificat est bien valide. Le certificat, ça a une date de début, une date de fin. Ça, ce qu'on appelle une, c'est lié à une CRL. Si l'autorité a été compromis, si le certificat a été invoqué, si si, si on vous dit Ben non, celui-là il est plus bon, alors vous avez intérêt normalement à aller vérifier auprès des autorités des CRL avant de commencer à triturer des certificats.

1:00:50
Ça peut être fait en temps réel, alors on va révoquer quand ça a été compromis, quand ça a été mal généré, quand l'information a changé, quand il y a un algorithme qui est devenu obsolète, si on a perdu le certificat, ce genre de chose. Donc vous faites une demande de certificat, vous allez sous une autorité de certification, donc on en avait là. L'autorité racine vous délivre, ça vous revient et vous allez pouvoir l'utiliser pour passer des frontières, d'accord ?

1:01:17
Mais dans une infrastructure à des publics, c'est la même chose. Vous avez une racine avec des HSM derrière qui ont les clés privées qui sont là pour protéger d'accord, la sous AC est capable d'interagir avec ces trucs là, d'accord ? Et puis votre Registration Authority, elle va prendre vos requêtes, elle va faire une demande de certificat d'accord. Et vous quand vous recevez, vous allez vous faire identifier auprès d'une autorité de validation qui également est là.

1:01:47

Alors une infrastructure à la clé publique, principalement les certificats, c'est ce qu'on appelle des X 509. On doit être au niveau de la version 3C maintenant je pense un certificat c'est un numéro de série, c'est un algorithme de signature, c'est un nom d'émetteur, c'est une période de validité, ça a une donc date de début, date de fin d'expiration. Donc ça veut dire que Ben le temps a besoin d'être sécurisé parce que si vous me laissez-moi contrôler le temps.

1:02:13
On va se retrouver en 1900 hein ? Tous les certificats vont être valides de toute façon de parler, donc si votre temps il est pas sécurisé, le jeu va s'arrêter très vite. C'est un nom de sujet et une clé publique d'accord ? Donc selon la version un, 2 ou 3, si vous identifiez l'identificateur le sujet, les extensions et ainsi de suite, vous êtes en XS 109V un V 2V 3 d'accord et vous avez la signature de l'autorité ici avec de l'extension derrière. Donc vous avez une CP, une certificat de police.

1:02:39
Ce qu'on doit faire c'est comment on fait pour respecter la CP, ça c'est le côté opérationnel. Vous avez les standards généraux de l'industrie de national Institut of standard, le List américain qui donne les standards fips, et ainsi de suite que j'ai nommé tout à l'heure fips, c'est Federal Information processing standard. D'accord, c'est la gestion documentaire du chiffrement. Et puis après vous avez l'i ETF Engineering Task Force, les RFC 36 47RFC c'est request for comment.

1:03:02
Les règles d'implantation des technologies ainsi de suite dans les RFC vous n'avez y a pas que de la crypto, y a de tout hein, vous avez les mêmes qui sont des blagues, vous en avez même comme par exemple y en a un qui est c'est non, je sais plus comment 11 47 11 32 qui est qui est une blague qui est comment faire alors y en a qui sont comment faire de de l'i p sur de l'ethernet comment faire ci à travers ça et l'autre c'est comment faire de l'i p à travers des pigeons, comment utiliser des pigeons voyageurs pour faire passer des protocoles IP, la gestion des certificats donc leur rollement va falloir trouver son identité.

1:03:33
La CA va vous créer le certificat, le signer et vous allez l'utiliser pour valider votre identité. En fait, c'est valider la signature du CRA qui va valider votre clé publique. C'est un document qui est remis par la CA qui garantit son anticité par signature qui associe une clé publique à son propriétaire. Je vous ai déjà parlé de ce qu'il y avait à l'intérieur. Alors un certificat c'est quand vous allez chercher HTTPS là ? L'université de Sherbrooke, Ouais.

1:04:01
On vous dit Ben la connexion elle est sécurisée, super l'h, TTPS et on clique dessus, montrez moi le certificat. Ah Ben voilà il vous dit University Sherbrooke c'est septigo, celui-là c'est user trust et il vous dit Québec organisation privée, où est ce que c'est fait machin na na na, vous avez un numéro de sujet, un numéro de série, un pays d'enregistrement, vous avez un nom d'émetteur qui c'est quoi l'a fait ? Ah Ben ça c'est septigo. Alors vous pouvez aller voir par exemple aller voir le site HTTP :

1:04:30
CRT. SH qui lui va vous donner l'ensemble des certificats pour un nom de domaine donné. Il va aller faire le tour de tous les autorités. C'est c'est que Thibault qui fait ça et vous dire mais tel gain, ouais telle entité. Allez, voici tout ce qu'il a, c'est assez intéressant, ça va vous plaire. CRT. SH il y a pas de W devant hein CRT. SH donc nom de l'émetteur PI pas avant telle date, pas après telle date d'accord.

1:04:55
L'information sur la réalité publique, on fait du RSA en 2048 l'a t publique e vaut 65037. Le module n vaut ceci la signature pour le HSA 3 256. D'accord toutes les informations sont là, est ce que c'est clair pour tout le monde, nom de l'émetteur, nom du sujet ? Tout est là, qui c'est quoi a émis, quelles sont les autorités qui a émises qui c'est quoi est entre vous et l'autorité ?

1:05:25
Alors attention, vous pourriez aussi auto signer votre propre certificat. C'est pas c'est fait dans certains cas mais c'est pas c'est pas une bonne pratique parce que comme je vous dis, si vous vous auto signez, moi je m'appelle Donald Trump aujourd'hui, puis demain je serai Barack Obama, alors que si je passe par une autorité, je resterai de l'avis de cellules. Vous pouvez avoir un CA intermédiaire d'accord ? Et puis au final nous avons un client final. Donc ici on avait 7 tigo avec RSA pour une.

1:05:52
Après avoir Secure Server et au-dessus c'était user trust. Donc vous pouvez avoir des chaînes de délégation dans un modèle de confiance hiérarchique. D'accord a fait confiance à B qui fait confiance à C et ainsi de suite. Donc dans la gestion des clés, Ben il va falloir maintenir cette pk. Il va falloir avoir des clés de longueur suffisante en stockage, une transmission des clés de manière sécuritaire. Il va falloir avoir un bon générateur aléatoire des durées de vie.

1:06:18
Qui manipulent des informations sensibles sur les temps qui vont bien oui et puis des exercices de recouvrement, c'est à dire l'escroc ESCROW en cas d'urgence. Alors oui Ben écoutez, ma clé publique elle a sauté, ma clé privée elle a sauté aussi, est ce que vous pouvez pas me les régénérer ? Est ce que je peux pas avoir des clés par avance ? D'accord et puis il faut une destruction sécuritaire parce que si au final vous allez mettre une question, j'arrive une 2nde, je finis ma phrase et je je lis votre question, Enfin vous allez me la reposer si au au final Vous allez mettre votre PC à la poubelle une fois que vous avez fini.

1:06:48
Ben y a des gens qui savent faire du reverse Engineering qui vont vous retrouver votre clé. Donc quand vous allez détruire tout ça, c'est pas juste je fous à la poubelle, c'est pas non plus je broie. Parce que quand on est sur des transistors et des petits trucs qui font quelques dizaines de nanomètres, on a intérêt à chauffer très fort, passer dans des champs magnétiques, détruire proprement machin et pas juste. J'ai balancé le disque dur à la poubelle, je réécoute la question, excusez-moi, Allô Monsieur qui a posé quelque chose dans le chat ?

1:07:18
Oui Bonsoir, moi je je j'ai juste une petite question, mais quand même, on peut avoir une autorité certificat local avec des serveurs et des infrastructures bien blindés bien sûr, puis d'avoir des serrures et des essais intermédiaires, puis de signer nos propres certificats et nos partenaires aussi. C'est juste ça non ? Absolument. Ce que ce que je dis par là c'est que en tant peut être pas été assez clair, vous pouvez faire des trucs en.

1:07:45
Dans votre propriété chez vous, vous pouvez faire à peu près ce que vous voulez. Vous vous comprenez ce que je veux dire à l'interface entre votre propriété et la route ? Ouais ça se discute. Par contre dans l'espace public vous pouvez pas faire ce que vous voulez, on est bien d'accord ? Donc

c'est la même chose ici, c'est la même chose ici, que vous fassiez des trucs derrière chez vous, il y a pas de problème à l'interface des 2, ça se discute dehors, vous avez intérêt à vous en tenir a donc vous pourriez avoir une politique pour chez vous.

1:08:13
Vous alignez sur la politique de dehors et avoir une politique d'interface entre les 2. Je dis juste que si vous allez à l'extérieur et que vous commencez à dire moi j'ai du self sign, vous allez faire rire beaucoup de monde. D'accord ? Si en interne vous avez du self sign, vous êtes pas différent de beaucoup de monde. Y a beaucoup de gens qui font ça. Par contre en extérieur ça passe pas. Oui donc oui vous avez tout à fait raison, mais maintenant la question c'est c'est quoi la cible, moi et mon nombril en intérieur ?

1:08:44
Ou des communications avec d'autres entités étatiques, gouvernementales ou des grandes boîtes à l'extérieur ? Faut savoir de quoi on parle. Ouais, juste un peu le commentaire chez soi, parce que on a des partenaires avec qui on travaille, puis on leur signe aussi le le certificat pour pour qu'ils puissent se connecter à notre réseau, à se connecter à nos infrastructures pour les utiliser. C'est juste pour ça. OK merci. Donc un dernier concept.

1:09:10
Que j'ai rajouté à ce cours par rapport au Slide qu'il y avait, c'est la preuve sans apport de connaissance, la preuve la divulgation nulle ce que l'on appelle du du du ZK 0 Knowledge. Donc imaginez que vous avez Peggy qui est le prouveur et Victor qui est le vérifieur et vous avez une caverne ici vous avez une porte, d'accord ? Et le prouveur dit, Moi je connais le secret de la porte. Peggy connaît le secret de la porte, donc elle disparaît dans la caverne, passe en haut ou en bas et elle vient se mettre à la porte.

1:09:37
Victor vient à l'entrée et lui dit, Eh Peggy, j'aimerais que tu réapparaisses en haut. Ah Ben lui il sait pas si Peggy était du bon côté de la porte. Si Peggy l'était pas, elle est obligée de passer la porte et de l'ouvrir, on est d'accord ? Par contre si Peggy avait été de l'autre côté et qu'il disait en haut, elle avait juste à faire demi-tour. Donc Victor avait une chance sur 2 de coincer Peggy. Par contre s'il avait recommencé ceci un grand nombre de fois mais une chanson 2 une chanson de une chanson sur 2.

1:10:06
Si on le fait 1000 fois, c'est déjà une chance sur 1024. Si on le fait 10 fois, pardon, c'est une chance sur 1024. Si on le fait de l'ordre de 300 fois, c'est à peu près une chance de trouver l'atome que j'ai choisi dans l'univers. Ceci peut être fait avec des structures mathématiques, vous avez des algorithmes Fiat, shamir, et ainsi de suite qui vont vous permettre de faire ça. Et donc au final, quelqu'un pourrait être convaincu d'une information sans jamais.

1:10:35
Avoir vu comment passer la porte, imaginez que j'ai une grille de sous le cou que j'ai résolue elle, on pensait qu'elle était impossible. Je l'ai résolue. Ben vous pouvez me dire, Je veux voir que et sur des petits ensembles de 9 carrés, moi je peux vous sortir les les cellules qui ont été découpées et vous montrer qu'il y a pas de doublon machin. On peut le faire à plusieurs endroits, pas l'intégralité de la grille, mais à plusieurs endroits, on peut le répéter tous les jours.

1:11:02

Et fondamentalement vous n'allez pas apprendre puisque vous savez pas en plus que moi je suis positionné ma grille comment je l'ai tourné ? Vous n'allez pas apprendre comment ma grille est faite mais au final vous serez assez convaincu pour dire Bah ouais je l'ai quand même assez challengé, il y a pas de doublon. La grille il a dû la résoudre de la même manière. Si vous étiez daltonien, si moi je suis daltonien et que vous vous l'êtes pas d'accord et que je suis pas capable de séparer le rouge du vert et je peux prendre les boules, les mettre dans mon dos, pour moi elles sont identiques.

1:11:30
Par contre je vous savais pas si j'ai changé les boules entre ma main gauche et ma main droite et à chaque fois que je vous en montre une vous me donnez la couleur. Il y a que moi qui sait ce que j'ai changé et si à un moment vous me donnez la mauvaise couleur, je me dis Bah tu es aussi daltonien que moi mon pauvre hein, tu me racontes des bêtises. Donc ici ces protocoles permettent de convaincre quelque chose, de de convaincre quelqu'un de quelque chose sans jamais lui donner la preuve absolue. Est ce que vous m'avez suivi en fait dès qu'on sait faire de la signature ?

1:11:57
Il y a un théorème mon crypto qui vous dit que on sait faire du 0 knowledge alors les attaques on a parlé d'attaques analytiques, d'implémentation statistiques, force brute, fréquence tech chiffrée uniquement tech que tu choisis, tech chiffrée meet in the middle birthday Attack. On n'a pas encore parlé du birthday, on va en parler passe de h et ranchon logis. Donc l'attaque analytique cette fois-ci c'est l'algo on va regarder en tant que tel de manière analytique l'algo qu'est ce qu'on peut faire ? On va faire.

1:12:27
On va regarder la structure, on va regarder s'il y a des problèmes d'architecture. Qu'est ce qui se passe la tête d'implémentation ? Je vous ai montré quelques-unes, c'est une faiblesse dans l'implémentation, je vous ai montré sur du temps, je vous ai montré sur du de la consommation. La telle statistique c'est la capacité par exemple à produire de bons nombres aléatoires, mais pas juste que ça, ça peut être un un système qui fait qu'on a plus 111 biais vers le un que vers le 0, on a des patterns qui apparaissent. Ce genre de choses d'accord la tête par bruit de force que je vous ai montré.

1:12:54
Ça a un succès si on a le temps, l'énergie et le stockage, et rapidement ça peut s'arrêter d'accord ? Par contre il y a des attaques plus intelligentes, par exemple quand on fait des h d'accord, si vous arrivez pas à faire ce qu'on a à à rajouter ce qu'on appelle des solt dans les Hash, Ben on va pouvoir faire des dictionnaires, c'est à dire un mot de passe. Prenez votre mot de passe, vous le hachez, c'est ce que vous stockez dans votre base de mots de passe. Ouais d'accord, mais comme il y a toujours des idiots qui vont aller prendre le dictionnaire, moi je peux déjà chier le dictionnaire par avance et comparer avec le résultat.

1:13:24
Vous allez me dire Bah Ouais c'est vrai il a pas raison mais comment je fais ça ? Mais derrière tu veux rajouter un nombre aléatoire sur quelques dizaines de bits de manière à ce que maintenant toto Ben c'est plus toto qui se code en un seul haché il va donner 65000 hachés toto tout d'un coup il faut votre dictionnaire, il devient 65000 fois plus grand et là j'ai que 16 bits si j'en mets 30 c'est 4 milliards. Et là en en stockage je viens de vous, je viens de vous contourner.

1:13:51
Quand il y a pas ce h, on peut faire ce qu'on appelle des rainmotables. J'ai pas le temps d'expliquer

mais rainbotables sur Windows ça vous permettait de choper les passwords en 30 secondes, c'est un compromis temps de mémoire, c'est très très très efficace, ça marchait très bien sur les HSM, c'est des Trucs, vous pouvez les acheter en ligne, vous irez voir par vous même l'analyse de fréquence on en a parlé, utilisait texte chiffré, contrer le nombre d'occurrences de chaque caractère, l'analyse texte En clair connu Ben on a accès au texte En clair et le texte chiffré.

1:14:20
Ouais c'est très efficace, l'algorithme est faible hein, c'est César, c'est 3 lettres ainsi de suite, le non cypher texte, mais c'est de déchiffrer une partie du texte chiffré. D'accord donc c'est quand on connaît juste le texte chiffré, le chosen plan texte. Bah c'est l'attaque de météo que vous disiez tout à l'heure. Quand on commence à demi des ports on regardait au-dessus en disant alors les gars ils sont pas très malins parce qu'ils transmettent des trucs chiffrés et que moi je peux voir En clair, donc ça me donne déjà des idées de corrélation.

1:14:44
Meeting the Middle, mais je vous ai dit, on part d'un début de l'algorithme, on part de la fin de l'algorithme, on essaie de faire des systèmes d'équations et de se rencontrer au milieu, mais sur du des sur du double DESS, c'est mortel. Par exemple, Man in the Middle, Ben je vous ai expliqué, c'est l'attaquant qui se met entre les 2, qui fait penser à croire, qui fait penser à Alice qu'il est Bob, qui fait penser à Bob qu'il est à Alice, il intercepte les communications, c'est très efficace si on a des trucs qui sont auto signés par exemple, on va parler du paradoxe des anniversaires, mais c'est là où on va aller regarder ce que.

1:15:16
Je disais tout à l'heure, c'est que je vais arrêter de partager l'écran une 2nde. Est ce que il y a quelqu'un qui peut, est ce qu'on peut aller regarder le chat ? Qu'est ce que ça a donné en terme de qu'est ce que ça a donné en terme de 2 occurrences, le premier janvier on en a 2, le 20 août on en a 2, 25 avril on en a 2. Vous voyez, on a des collisions, on a tout un tas de gens.

1:15:45
Oui alors ça c'est dû à quoi je repartage mon écran. Donc là on a de la collision chez nous, on vient de nous voir, je repartage mon écran. Pourquoi ? Parce que si vous voulez que 2 personnes au moins le même anniversaire, Ben on va calculer la probabilité que un moins. Tout le monde a un anniversaire différent, mais sur le premier on en 3 65, sur le 2e en 3 64 et ainsi de suite. Donc il est sûr que si on avait 3 66 personnes dans la salle, sachant qu'on est en 3 65, forcément il y a une collision.

1:16:14
3 65, c'est le pire cas, d'accord. 3 66 c'est ça tombe. Par contre le problème c'est quoi ? C'est comme tout à l'heure. Comme je vous avais dit, le gars qui veut communiquer avec les 8 autres, bah il a fait 7 clés et le gars d'à côté, il a aussi fait 7 clés, mais là il faut que personne ne se touche. Et donc ce n carré qu'on avait tout à l'heure dans la distribution, on l'a ici aussi parce qu'il faut que personne ait le même anniversaire et donc on va être de l'ordre de racine carrée de n.

1:16:43
Ce qui veut dire que si on considère que 365 c'est 400, mais on va être de l'ordre de 20, racine carrée de 400 c'est 20 et sur une classe de 30 élèves, 8% de probabilité que quelqu'un soit né à une date donnée, 70% de probabilité si on est né à la même date, je sais pas combien on est dans la salle aujourd'hui, mais collision. Imaginons qu'on soit 80, quasiment 100% de chance qu'on ait des collisions. On est très proche, on est à 95% et plus.

1:17:12
Des 20YA de la collision. Quand vous êtes à 40, 45 personnes, 90% de chances de Collision, Ben ça veut dire quoi ? Ça veut dire que si vous faites pas attention et que vous prenez des messages hachés au hasard, si les nombres, la quantité de bits en sortie est trop petite, vous allez avoir des collisions. Il va falloir avoir des trucs qui soient au-delà de ce qu'on est capable de calculer et donc si les meilleurs peuvent calculer 80 à 90 bits on va aller chercher 2*80 le double, c'est à dire le.

1:17:41
La racine carrée c'est le demi, l'inverse de ça, c'est le double pour aller chercher du 160 bits, ceci explique pourquoi on est allé chercher 160 bits, d'accord, alors on continue les étapes cryptographiques, le replay. Alors cette fois-ci c'est efficace, il y a pas de mécanisme de protection temporelle, on demande une authentification avec des informations pertinentes, et si le temps de vie de la session est pas contrôlé ou s'il y a pas de monstre, Bye bye. Alors les sides Channel. Alors on en a parlé tout à l'heure, consommation Power.

1:18:10
Sonde électrique électromagnétique, c'était moi et ma thèse. C'est moi qui ai poussé ça, l'analyse de trafic, l'introduction d'erreurs volontaires. Je vous ai montré, je vais vous montrer que le bout attaque ça, ça en a une autre. Vous avez la Joconde en mémoire et puis on va venir geler la mémoire. Problème d'implémentation, on va venir geler la mémoire. Et ce sont les chocs électroniques qui font que une puce a des valeurs qui changent en interne quand on retire Power.

1:18:37
Il y a des valeurs qui changent en interne. Pourquoi avec la température, la température c'est quoi ? C'est des chocs de particules, des chocs électroniques. Donc si je viens refroidir mon système et j'aurai de moins en moins de chocs et donc je prends ma puce, je la gèle, je la change de support, je vais la lire ailleurs et je retrouve. Et au fur et à mesure, plus vous êtes descendu en température, plus elle se maintient longtemps, plus vous voyez votre chonde qui s'abîme, qui s'abîme, qui s'abîme. Même là, si vous me montrez de loin, je commence à vous dire ça.

1:19:03
Ouais peut être je sais pas, on dirait Mona Lisa. Bon là on voit plus grand chose, mais ça peut durer un certain temps. Mais si ça c'est votre clé, Ben il baille la clé hein. Donc passe le h c'est la même idée, c'est qu'au lieu de passer le mot de passe, un attaquant pouvait s'authentifier en utilisant le h qui avait été passé, le h qui avait été obtenu auparavant, et dans ntlm, dans LM, dans kerberos, c'était une faille d'implémentation.

1:19:32
Au niveau du protocole d'authentification où la charge du mot de passe reste statique d'une session à l'autre, quel que soit le mot de passe, s'il est pas si, si, s'il est pas on va dire avec un solt avec 1111 Salage propre, vous allez avoir des problèmes en somewhere. Je vous ai parlé de Moutinho tout à l'heure, on clique des fichiers, on bloque l'ordinateur, on vole les données, puis on dit Ben vous voulez un retour à la normale ? Vous payez alors zabrine de poste quand on va avoir des qubits en nombre.

1:20:01
En en bonne quantité, on va avoir une capacité à appliquer l'algorithme de shore. L'algorithme de shore permet de factoriser l'algorithme de grover permet de factoriser ou attaquer le bloc discret l'algorithme de grover permet de trouver des collisions dans des bases de données et donc il y a un

certain nombre d'algorithmes qui ont été choisis parce qu'ils résistent à ça. Qui les algorithmes classiques RSAECC tout ça, ça va partir à la poubelle, il va falloir doubler la taille des symétriques ou alors accepter d'en perdre 50% de la taille.

1:20:28
Et ces algorithmes en fait, en cryptographie post quantique, on a la menace quantique. Alors ça veut dire qu'en 2028 on est censé avoir changé les systèmes de signature de HSM. la Maison Blanche et ses ses copains ont dit en 2030, je veux que vous arrêtiez RSA en 2035, j'en veux plus en circulation. Du point de vue d'une entité, c'est demain hein, c'est pas très très long, c'est c'est c'est c'est ça va être un pour 100 du budget IT sur les 10 prochaines années.

1:20:57
C'est la grande truc qui arrive en cryptographie dans les années à venir. Donc RSA, courbe, elliptique, c'est basé sur une résolution mathématique avec des problèmes tels que la focalisation des entiers, des grands composites ou le log discret. Bah grover et Short vont faire sauter ça. Ce sont des algorithmes qui tournent sur des systèmes quantiques, des des ordinateurs quantiques. Ils sont infiniment plus rapides que ce qu'on a aujourd'hui.

1:21:24
Et donc cette cryptographie là elle est cassée. On va devoir aller chercher d'autres algorithmes. Des problèmes de vecteurs courts dans des réseaux euclidiens, c'est des problèmes qui datent de 96, du décodage de codes linéaires aléatoires, de l'inversion de polynômes multivariés, de la navigation dans des isogénies et des courbes elliptiques super singulières, ou de l'inversion de fonctions de la charge. Le prix à payer, c'est une perte d'efficacité. Et d'être les plus larges, beaucoup plus larges, ça peut être 15000 bits.

1:21:53
Il y a plusieurs propositions qui ont été faites, qui n'ont touristiquement la sécurité d'un problème non polynominal c'est pas encore 100% prouvé, ça ne se rassemble pas, mais la procédure c'est on teste et puis parfois il y en a qui sont morts, il y en a qui avaient été à 2 doigts d'être qualifiés, de rentrer en finale et puis ils sont morts. Il s'avère vulnérable. Il y en a qui ont tenu 5 ou 30 Min sur un PC vis-à-vis d'attaques, donc c'est pas quelque chose qui est encore très très très mature dans la réalité.

1:22:21
Donc la crypto pour quoi faire ? Mais de la confidentialité, de l'intégrité, de l'authentification. La confidentialité c'est du chiffrement, l'intégrité c'est de la validation du fait que ça n'a pas été modifié et l'authentification c'est de la signature disponibilité invalability bah oui c'est parfois le dernier a les primitives cryptographiques. Bah il y a des fonctions de HMD, 5 cassé cha un cassé cha 2 cha 3 invalide.

1:22:44
Des algorithmes de chiffrement symétrique AES triple des des des modes de chiffrement GCMCBC, des modes de chiffrement par flux CTROFB, des algorithmes de chiffrement RSA, des algorithmes de signature DSA sur les courbes elliptiques DSA tout court RSA avec des clés privées de génération de clés asymétriques RSA ou ECDSA, puis des algorithmes d'échange de clés comme dit Fillel Ben robustesse des clés. Ben je vous ai donné les bits ici, je vous ai dit au niveau quantique.

1:23:14
Le jour où ça arrive, la symétrique saute en gros, le symétrique descend de taille, et les haches

subissent également une perte entre les algorithmes de shor et les algorithmes de grover. Conclusion, la cryptographie est basée sur des primitifs simples et éprouvés. Faut pas faire ses propres primitifs, faut même pas essayer de faire ses propres implémentations. Vous allez vous casser la figure, valider ce que vous utilisez, valider la surdité de l'algorithme, éviter les mauvaises utilisations.

1:23:41
Ayez une bonne chaîne de confiance, si vous voulez approfondir, allez voir les bouquins, cryptographie symétrique qui PKIICSC, vous avez la référence, moi j'ai utilisé que j'ai là avec moi. Vous avez également histoire des codes secrets, le livre de Simon Singh, je vous recommande de lire, ça se lit un week-end, c'est très agréable. Crypto appliqué de Bru Schneider l'histoire alors ça c'est le truc qu'il faut lire, si vous avez un été hein, c'est code Breakers de David Khan, si vous voulez vous distraire, vous allez voir le film les experts.

1:24:10
De Robert Redford, 1992 où P égal NP le voyageur de commerce. En 2002, j'aurai pas le temps de toucher les protocoles. Il est déjà 09h35, je prends vos questions et je vous remercie pour votre attention. Question, oui.

1:24:36
Si je me souviens bien, les HSM, c'est pour gérer et clé privée ? Donc j'essaie juste de me souvenir. Tu à mettons, tu crées un certificat avec un certificat RSM, et après ça tu mets tu mets toutes dans ton HSM, c'est j'essaie juste de de revoir le HSM, c'est en PC sous stéroïde avec une carte pour faire de la crypto, ça peut faire de la crypto symétrique, ça peut faire de la crypto asymétrique, ça peut protéger de la clé privée.

1:25:06
Ça peut faire de la dérivation de clés, ça peut faire à peu près n'importe quoi ou on ne veut pas qu'à travers des ex lytes, à travers des side channels, des canal hétéro cachés, des fautes ou quoi que ce soit, on puisse piquer la clé privée. La clé privée, c'est le Saint Graal, si pas de clé privée, Bye bye. Le HSM est là pour la protéger donc la HSM, faire ce qu'on lui demande de faire, c'est une machine à dépoter de la crypto, point voilà, alors le le on va généralement.

1:25:36
Essayer par exemple de mettre une clé de wrap, une clé qui va permettre de chiffrer d'autres clés, une KEK qui un clicking key. Et puis on va aller faire tout un tas de trucs avec. Et puis on va garder la la cake dans le HSM. Si y a un besoin, on a besoin de tout, on éteint tout et on redemande à la HSM de nous la donner. C'est un des exemples d'utilisation. On peut faire de tout dès qu'on a un système où on fait de la crypto, que ce soit Xbox, que ce soit.

1:26:06
Des certificats que ce soit du paiement, on a des h. SM, j'ai répondu à votre question, non peut être pas oui oui oui oui oui. C'était des exemples de HSA. J'attends de voir s'il y a d'autres personnes qui ont des questions, sinon j'aurais une autre question. Thalis, Thales, Thales, Thales, les HSM.

1:26:31
Oui, dans les interac, c'est des pay Shield Pay Shield 10000. Moi j'avais qualifié en tant que j'étais dans un labo, j'ai qualifié le pay Shield 9000. Maintenant ils en sont 10000. Oui, c'est interac. Autre question, y en a pas. Je vais y aller avec la mienne.

1:27:00
Ouais caber, c'est quand est ce qu'on devrait penser commencer à les implanter dans les entreprises ? Alors la première chose à faire c'est généralement, vous avez des providers, vous avez des gens qui vous vendent des HSM, vous avez des gens qui vous vendent des solutions machin, c'est eux qui implémentent, c'est pas vous qui allez allez taper ça dans open SSL. Maintenant la première chose à faire c'est un inventaire, savoir quels algorithmes vous utilisez et où. Parce que.

1:27:30
Si vous alors bien évidemment il y a il y a. On a une idée d'où est le cœur de la crypto, mais la crypto elle est partout, des caméras aux ascenseurs en passant par des systèmes d'accès partout. Donc si vous avez pas une idée de ce qui se passe, ça va mal se passer le jour où ça pète. Moi je dis l'inventaire, les gens sont dessus en ce moment. Maintenant je vais être honnête avec vous, c'est un un faux départ de 100 M. C'est un départ de 100 M façon l'utilisateur quoi.

1:27:58
Qu'est ce que je veux dire par là ? La course va prendre mieux on le sait. Par contre les gars ils sont pas dans les starting block, ils sont sur voilà encore en train de manger des nuggets. Par contre il y a un programme retransmis à la télé et on sait que telle date 2028, 2032, 1035 CE sera fini. Même Microsoft dit Ouais bon Ouais si ça pète on ira chercher des des clés plus grosses quoi. Si il pète du 2044 2048 on mettra du 4096.

1:28:26
Pas forcément d'accord avec ça. Enfin je comprends pourquoi ils le font parce que c'est vrai que un déjà c'est peut être pas demain mais on peut discuter de moi. Je dis que l'inventaire c'est maintenant et en 2030 il faut que ce soit fait. Ça dépend de la taille de votre boîte. Si c'est 3 peut aller dans une start-up ce sera peut être rapide si c'est 50000 personnes. Oups.

1:28:57
Un peu ouais, autre question qui que ce soit, oui amza vas y vas y allez y prenez vos poser vos questions, peut être qu'ils l'ont mieux, est ce que vous m'entendez ? Oui Madame, oui OK Bonsoir ma question c'est concernant les algorithmes des cartographies, bah il y a des règles d'exportation entre les pays. Concernant ces je je voulais savoir.

1:29:31
Quel quel algorithme est restreint d'exportation ? Et que ce soit le l'algorithme lui même ou bien si la la la machine qui supporte le HGM par exemple. Alors je vais vous raconter une blague amusante, moi, quand j'ai commencé à faire de la Crypto en France, la possession de de bouquin de crypto, de d'algorithme de crypto était considérée comme une détention d'arme de guerre de 3e catégorie. Même titre que masque à gaz ou qu'une mitraillette.

1:30:01
Ça s'est beaucoup allégé avec l'arrivée d'Internet. Je vais vous donner un exemple, il y a un gars qui a qui s'appelait Phil Zimmermann qui a fait un algorithme, un un logiciel qui s'appelait PGP qui a démocratisé la crypto. Au niveau de l'E Mail machin ça a beaucoup embêté les Américains et ils avaient des règles qui étaient pas d'exportation de crypto. Alors il y a forcément un mexicain plus malin que les autres qui a lu la règle et qui lui s'est fait tatouer sur le bras un code Pearl, un code Pearl, c'était très petit de génération de clé RSA donc quand il s'est fait attraper.

1:30:30
A l'intérieur du pays qui ont voulu l'exporter à la Donald Trump, il a fait hop hop hop hop là il y a marqué que vous pouvez pas m'exporter, donc si vous m'exportez, vous violez vos propres règles. Il a fallu passer une loi en urgence sur pas d'exportation sous forme électronique, donc tout d'un coup on pouvait exporter le Mexique, Ben pas d'exportation sous forme électronique. Qu'est ce que les hackers ont fait ? PGP le fameux logiciel qui voulait pas sortir, les mecs l'ont imprimé, on n'était pas sous forme électronique.

1:30:55
Ils ont pris le truc, ils sont passés devant des douaniers au Canada, PAM, PAM, PAM, c'est sous forme papier, ils sont allés de l'autre côté, ils ont fait une OCR reconnaissance de caractères et hop il y avait un fork, il y avait un PGP version international. Donc aujourd'hui il faut être très clair dans les algorithmes. Vous avez par exemple chez la NSA suite a et suite B suite a c'est des algorithmes militaires. Si vous êtes pas militaire vous avez pas à en connaître. Il y a des techniques qu'on connaît même pas.

1:31:21
Suite B, c'est la version des trucs pour les civils, courbe, elliptique, RSA, machin. Aujourd'hui il est gars, il s'est même plus d'interdire ce genre de chose parce que c'est partout, c'est partout, c'est dans votre téléphone, c'est dans votre carte bancaire, c'est dans votre frigo, c'est dans votre bagnole. Si vous saviez le nombre de fois où vous touchez de la Crypto dans une journée, vous auriez peur.

1:31:43
Un adulte de nos jours je crois pense en psychologie 800 fois au sexe dans la journée. Vous faites plus de 800 fois de la crypto sans vous en rendre compte. Donc essayez d'interdire, on va pas s'en sortir. Il vaut mieux avoir une idée de ce qui se passe que d'essayer d'interdire. Alors maintenant ça veut pas dire qu'il y a pas des des limitations à l'exportation. Vous avez vasnar VAASENAR qui sont des accords non contraignants, mais la cryptographie est considérée comme une arme de guerre.

1:32:11
Donc au même titre que vous pouvez pas exporter un chasseur, un réacteur nucléaire ou quoi ? Il y a des trucs en crypto et des fichiers de surveillance. Vous pouvez pas exporter mais c'est pas parce que vous allez faire du RSA de l'autre côté de la frontière que qui que ce soit va vous embêter. J'ai répondu à votre question oui merci beaucoup autre question et ma question qui était en attente à savoir.

1:32:38
Les applications à l'instant de WhatsApp, Facebook et autres. Quand tu parles au chiffrement de bout en bout, c'est c'est quel type de chiffrement que c'est ? Est ce que c'est par bloc ? Alors généralement ça va être un échange au niveau asymétrique, chacun aura une clé, on va voir derrière du symétrique pour aller à fond la caisse que ça va beaucoup plus vite.

1:33:01
Dans certains cas, on aura du chiffrement de flux, mais avoir des protocoles compliqués. On va avoir des protocoles qui vont empêcher des techniques de de rejet, on va avoir des protocoles qui vont empêcher ce qu'on appelle des attaques boomerang, des techniques de clic et ainsi de suite. Celui que vous pouvez regarder si vous, si vraiment vous voulez vous renseigner là-dessus, signale

l'application signal si chère à Monsieur Exet et ses copains, le protocole est complètement détaillé, vous.

1:33:26
Vous allez complètement trouver les algorithmes si vraiment on voulait un jour qu'on s'asseye quelque part, qu'on discute à votre disposition, c'est un ensemble mais c'est principalement de l'hybride. Autre question, vous avez dit l'application signal signal SIGNAL ? Oui oui signal signal. Vous avez pas vu le CE qui est arrivé au ministère ministre de la défense de de Donald Trump qui avait balancé du signal sur son plan d'attaque. Il a utilisé le signal comme pour communiquer sur le plan d'attaque sur l'outil il y a quelques semaines. Ça dit rien à personne ça ?

1:33:57
Oui vraiment drôle, c'est c'est ça fait, c'est celui-là, l'algorithme de signal il est-il est connu, il est documenté, c'est derrière. Initialement, je crois que c'est marlin. Ah ***** comment il s'appelle marlin, Spike Motin, Spike, Ouais c'est c'est vraiment comme ça le gars qui a fait ça. Autre question, je vous écoute.

1:34:25
Moi j'ai une bonne question, je pense que y a un peu de question, il est 45 déjà moi j'en ai, moi j'en ai une pour vous, est ce que est ce que vous pouvez me mettre en un truc dans le chat en en en juste pas pas besoin d'un paragraphe ce que vous auriez ce que vous auriez aimé changer dans ce cours. C'est pas la première fois que je le fais, ça fait 30 quasiment 30 ans que je le fais, mais si vous pouvez me dire.

1:34:51
Je suis essayé de m'améliorer en permanence. Si alors je comprends bien. J'avais que 02h30 02h30, ça va aller vite, ça va dépoter. Mais s'il y avait quoi que ce soit, plus de moins de ci, plus de ça, ce serait bien. Merci je vous répète, vous avez mon email. David. Samy at gmail.com si vous voulez qu'on s'assey un jour autour d'un café, qu'on en discute du côté de Desjardins, j'y serai pas avant.

1:35:19
Mi-juillet mais à votre disposition. Bonne soirée à vous. Merci de votre attention et au plaisir de se croiser dans ce monde IT. Merci beaucoup dame, merci. Bonne fin de soirée, au revoir.

INF813-Séance10-20250618_PA01

0:02
Voir le module 3B architecture et système. On a 110 slides donc il va aller un peu vite. Si il y a des slides, que je passe vite, que vous ne comprenez pas, n'hésitez pas à m'arrêter. Je vais revenir là-dessus pour expliquer autant que faire se peut je pense à la fin du cours. Il y a le quiz qui est ouvert également pour une semaine comme d'habitude.

0:27
Demain on va faire également la un autre cours sur la communication réseau, ça également je pense. On va le diviser en 2 parce que c'est c'est beaucoup, c'est 120 slides donc on va diviser en 2, on on va faire une cours demain et puis l'autre on va, on va le faire la semaine prochaine et vous allez faire le quiz après la fin, puis on fera la révision de on, on fera les on donnera les détails sur les examens et puis si possible quelques révisions.

0:57
Hasard ? Allô ? Oui salut. En fait je voulais savoir pour le quiz de ce soir, il vient inclure ce qui a été vu la la semaine passée dans ouais non, pas au cours de la cryptographie, puis pas celui-là c'est ça c'est ça. Donc ça sera le 3 mars qu'on avait cryptographie, plus ce cours là.

1:19
Puis est ce est ce qu'il y aura comme en fait 2 fois plus de questions, 2 fois plus de temps, c'est c'est comment que ça se passe ? Non c'est pareil, c'est le même nombre de questions, même nombre de temps, même temps. OK maintenant je je connais pas les questions hein j'avoue donc oui Marc France oui Bonsoir excuse moi moi je voulais juste me rassurer.

1:45
J'ai vraiment bien compris, est ce que la première partie sera dans le la première partie c'est à dire la première partie de la partie de de de quoi l'examen de section ? Est ce que nous allons vous faire prendre en compte cette partie pour l'examen final ? OK tu veux savoir est ce que est ce que oui tu veux savoir est ce que l'examen final, l'examen final va prendre en compte juste la partie que vous avez vu avec moi, c'est ce que tu demandes ?

2:15
Oui c'est ça je sais pas. Écris moi la question je vais je vais demander, est ce que c'est tous les cours que nous avons vu depuis le début jusqu'à la fin ? Je je sais pas parce que j'ai pas vu les questions. OK Ben je je vais me renseigner je sais pas je me pose la question parce que si je si je me souviens.

2:40
L'enseignant, c'était comment ? Je l'ai comme oui oui Dominique avait dit à moins que je peut être que je confonds. Il avait dit la partie de l'examen c'est serait la partie la 2e partie où parce que il s'arrêtait juste à la à la partie de la l'examen mi session et la partie après lui ce serait-ce serait la partie pour l'examen final. Moi je voulais juste me rassurer.

3:03
C'est ça je je vais confirmer avec lui les les banques de questions sont déjà là, c'est pas moi qui les ai composées. Donc oui je sais pas si ça prend en compte juste la partie que moi j'ai vu ou la partie que lui il a fait, mais je sais que généralement le cours était est toujours donné par 2 personnes donc ils

ont dû faire la la segmentation comme ça. Mais je vais confirmer avec lui c'est bon merci OK c'est bon on on peut commencer.

3:35
Ok parfait donc architecture et système plan de la séance. On va voir aujourd'hui le 3 un, rechercher, mettre en mettre en œuvre et gérer le processus d'ingénierie en utilisant des principes de conception sécurisés. Donc on va voir la modélisation des menaces, donc le truc modeling ?

3:54
Comme vous le savez dans si elle s'expire on on voit les notions, on rentre pas trop en profondeur, on explique les concepts. Plus important c'est de comprendre qu'est ce que chaque concept fait mais on rentre pas en profondeur. Par exemple la modélisation des menaces on va pas le pratiquer, on va juste expliquer. Pareil pour les tous les autres éléments que vous voyez depuis le début du cours, mais c'est de comprendre parce que si vous faites la sécurité faut comprendre la plupart en tout cas avoir une bonne notion sur la plupart des concepts puis savoir ce genre d'application.

4:23
Ensuite, on va parler du monde privilège. De plus, privilège, défense en profondeur, valeur par défaut, seeker default échouez en toute sécurité, fait le Shaker Shakerling séparation des tâches, rester simple, type et simple. Le principe de 0 trust à confidentialité dès la conception privacy by design, faites confiance, mais vérifiez responsabilité partagée.

4:53
En 3 2, on va voir comprendre les concepts fondamentaux des modèles de sécurité. Donc le biba, Bella, puda, Bella, Padoula autant pour moi. Ensuite on 3 3, sélectionner les contrôles en fonction des exigences de sécurité du système. 3 cartes, comprendre les capacités de sécurité des systèmes d'information.

5:17
On va parler de la protection des mémoires, le TPM, le, le chiffrement et le déchiffrement. Tant pour moi je vais corriger ça. Il va 3.5, évaluer et atténuer les vulnérabilités, les architectures des conceptions et les éléments, donc les systèmes basés sur les clients, les systèmes basés sur les serveurs, les systèmes de base de données, système cryptographique, système de contrôle industriel, les systèmes basés sur l'info nuagique, les systèmes distribués.

5:47
Internet des objets, micro services, les conteneurisations, censeur de serveur d'air, système embarqué, système de calcul haute performance, système informatique de périphérie qu'on appelle du normal Edge, système Virtualisé. Ensuite, en 3 8, on va appliquer les principes de sécurité à la conception des sites et des installations, donc tout ce qui est sécurité physique.

6:11
3 9 concevoir les contrôles de sécurité du site et des installations. Donc on va parler des amois de câblage des installations de distribution intermédiaire, salle du serveur, centre de données, installation, stockage multimédia et stockage des des preuves ? Ensuite, on va parler de la sécurité des zones restreintes et le travail des services publics de chauffage, ventilation et climatisation qu'on appelle généralement h back en anglais.

6:40

Les problèmes environnementaux, prévention, détection et suppression des incendies, alimentation, redondance. C'est court également. Donc on commence par le 3. Un principe de conception sécurisée. Donc la première c'est la modélisation des menaces strip modeling dont vous avez entendu parler de ça. Et généralement, dans la sécurisation des systèmes, on parle beaucoup de modélisation des menaces ou de ceux qui travaillent, ceux qui.

7:10
Travaille vilement avec des personnes qui sont dans des Soc, donc c'est un processus d'identification des menaces potentielles sur les sur les systèmes, donc applications ou processus avant qu'elles ne se produisent. Donc le toute modeling c'est quoi ? C'est que on veut concevoir un nouveau système. On veut peut être intégrer un nouveau système dans notre environnement, donc on va faire la modélisation des menaces, donc on va essayer de voir comment est ce que les attaquants peuvent nous attaquer, peuvent attaquer le CE système là, quels sont.

7:40
Les points d'entrée, quels sont les points de sortie qu'ils peuvent utiliser pour faire ressortir de l'information ou pour entrer dans le système ? Donc on va prendre un système quelconque, ça peut être ça peut être soit un un système réseau qu'on veut mettre en place comme un système système d'information simple, un SAS. Tout ça quand quand on veut mettre excusez-moi je pense que je reçois un message.

8:12
OKOK donc parfait. Je continue donc on on peut être avoir un système SAS qu'on veut déployer, mais on s'entend, si on a un système SAS comme Microsoft Dynamics ou Salesforce qu'on veut déployer dans l'Organisation, Ben ça va prendre des intégrations. Et puis on va très souvent faire passer des données donc.

8:35
Dans un tel projet, on va revoir l'ensemble des minaces qu'on peut avoir. Et puis dès qu'on a les menaces, Ben on essaie de mettre les contrôles en place pour atténuer, donc ça vient réduire un peu la surface d'attaque de de notre application ou de notre système. Donc donc les grandes étapes c'est que généralement on va, on définit le périmètre de l'analyse, donc on va comprendre c'est quoi notre système, le diagramme de flux des données, les points de sortie des données. On va identifier les différentes menaces et vulnérabilités de nos systèmes, donc on utilise des.

9:05
Des méthodes de modélisation qu'on va voir tantôt on va ensuite on va définir les comptes mesures et les mesures d'atténuation. Donc dès que on on sait le système qu'on va utiliser, on connaît la portée, on connaît les menaces, on connaît les vulnérabilités, et bien on va mettre les comptes mesures en place pour atténuer et ensuite on on pourra évaluer, voir l'ensemble de notre travail si effectivement on arrive à à corriger ou à contrôler l'ensemble des menaces qu'on a identifiées. Donc c'est en gros ça le.

9:34
La modélisation des menaces, les méthodes qu'on utilise pour la modélisation des menaces. La première méthode c'est stride, généralement qu'on utilise Ben c'est une méthode qui a été faite par par Microsoft, donc la documentation est disponible en ligne. Si vous faites Microsoft vous aviez des outils même de modélisation que vous pouvez avoir donc à stride on s'entend c'est s pour spoofing usurpation tempore une falsification aire répudiation non vérification de l'origine et l'intégrité.

10:04
Informations disclosure pour le I donc divulgation d'informations denial of services qui pour donner des services et élévation de privilèges pour pour l'élévation de des privilèges, élévation d'un privilège donc le soit qu'est ce qu'on fait avec le soit ? Donc les acronymes qu'on voit, ça sera les différents types d'attaques que un un attaquant peut faire sur un système.

10:29
Donc on va regarder ces différents éléments et on va voir à notre niveau quels sont les contrôles qu'on a. Donc est ce qu'on a un contrôle contre le spoofing et on va évaluer l'ensemble des contrôles qu'on a si on n'en a pas et on va en mettre. On va regarder dans la falsification. Est ce que dans notre système avec notre base de données est ce que quelqu'un peut falsifier ? De quoi si l'action peut falsifier ?

10:48
Devra faire en sorte de mettre un contrôle en place contre là falsification au niveau de la RÉFUGIATION est ce que quand quelqu'un fait une action, la personne après peut dénier, peut nous dire que c'est pas elle ? Est ce qu'on fait du Login, est ce que on fait des on est capable de faire de la surveillance ? Donc ça si on le fait pas, Ben ça fait partie des des ménages à traiter. Ensuite on va voir l'information disclosure, tout ce qui est divulgation d'informations, quels sont les points de sortie des données ? Donc on pourra avoir peut être des IPI.

11:17
L'ensemble des exports d'informations qu'on peut avoir, donc on va tout faire pour contrôler ces éléments là pour ne pas qu'on puisse faire sortir de l'information. Et puis le le déni de de service c'est que on peut envoyer plusieurs requêtes à notre système dans le but de le planter. Donc on va voir en termes de disponibilité qu'est ce qu'on fait ? Et puis élévation de privilège est ce que on a, on applique des principes comme les principes de moins de privilège qu'on va avoir. Et puis est ce que on est capable de contrôler l'élévation du privilège dans le système donc.

11:45
On va regarder l'acronyme et on va mettre le contrôle en place associé à ces différentes menaces là. Donc ça c'est un. En tout cas stride est beaucoup populaire. Ensuite on a le lune qui est restant, qui qui est populaire avec la la vulgarisation des encadrements sur la protection, sur la confidentialité, la vie privée. Autre que ça soit GD Pierre ou la loi 25 au Québec ici.

12:09
Donc on a un acronyme qu'on appelle Lindon, qui lui c'est Link identified pour identification non reputation detecting data disclosure on Warren S de la méconnaissance et de la non non-conformité. Donc ça c'est le même principe. Donc on met les acronymes, on voit qu'est ce qu'on a comme contrôle, est ce que cette menace ça s'applique à nous ? Et puis si on n'a pas le contrôle, Ben on va aller chercher le contrôle. Donc comme vous le voyez dans Linden, il y en a un qui vont s'entrecouper avec le stride.

12:37
On a pasta, on a vas, on a les squares qui sont également des méthodes de modélisation dominace. C'est bon, on continue. On a un autre concept qu'on appelle le moins de privilège privilège. Donc ça s'applique à différentes couches d'applications d'abstractions dans dans un système. Donc le principe

c'est c'est que on veut s'assurer que chaque sujet doit pouvoir accéder uniquement aux informations et ressources nécessaires à sa finalité.

13:04
Donc on veut pas par exemple que un stagiaire de la paye voire un stagiaire de la paye. Il peut voir les salaires bien sûr des des salaires auxquels il a, il a le droit, mais il peut ne pas modifier, il va pas lui donner le droit de modification, il va juste avoir le privilège dont il a besoin. Tout comme peut être un agent au marketing qui prend un centre d'appel. Ben il n'a pas besoin de voir le numéro de NAS des des clients donc on va lui cacher ça, on va.

13:29
Faire en sorte qu'il voit juste les informations marketing dont il a besoin, donc c'est ça le le moindre privilège. Ensuite on a la défense en profondeur qui est similaire à la défense en profondeur militaire, donc c'est des défenses multicouches donc et ces défenses là seront comme redondants en cas d'échec de l'autre. Donc qu'est ce qu'on fait ? On commence d'abord par tout ce qui est politique, procédure et puis sensibilisation. Donc déjà on on informe l'ensemble des.

13:58
Des employés sur ce qu'on ne doit pas faire. Ensuite on a la protection physique qu'on va avoir. Après on va mettre tout ce qui est gardien, tout ce qui est mantrap, tout ce qui est caméra de surveillance. Et puis ensuite quand on finit ça, on va avoir notre réseau, on va sécuriser notre réseau, l'ordinateur même, on va le sécuriser les applications, on va mettre la sécurité et puis le device on va faire en sorte que on puisse pas le voler même si on le vole. On va avoir des stratégies en arrière pour pouvoir W Iper le système.

14:26
Donc pour waiter les données qui sont sur le le le mobile. Donc ça c'est ça la défense en en profondeur parce que en sécurité on sait que on on peut toujours un un contrôle de sécurité peut toujours failli mais si tu en as plusieurs à un moment donné l'attaquant peut se décourager. Donc c'est ça on continue allemand on a un autre qui s'appelle valeur par défaut sécurisé donc c'est que par by default c'est que c'est que Default donc.

14:56
On veut s'assurer que par défaut le système sera configuré d'une façon sécuritaire. Donc qu'est ce qu'on veut éviter les mauvaises configurations dès l'installation. Donc quand on a un système, on veut s'assurer que quand on va sur le système, les éléments basiques, Ben on a déjà la sécurité qui est déjà appliquée sur le système. Donc c'est comme un compte est inactif jusqu'à changement de mot de passe temporaire obligatoire, donc on va.

15:22
Créer, si on crée un nouveau compte, on va faire en sorte que le compte il reste inactif jusqu'à ce qu'on change le le mot de passe temporaire, donc on s'assure que on aura la sécurité par défaut là-dessus. Ensuite, on a un autre principe où concept qui est fail secureley, échouer en toute sécurité. Donc lors d'une erreur, toujours revenir à un État stable et sécuritaire. Donc on a un système, par exemple, on a, on a, on a une porte, donc on a une porte.

15:51
On s'est dit que dès que la serrure ne marche pas, on veut que la serrure bloque quand même. Donc ça c'est c'est que dès que la série commence à déconner, on veut pas qu'elle qu'il l'ouvre. La on veut

que la porte soit condamnée. C'est vrai que c'est pas un bon exemple dans le cas d'une porte, mais c'est un peu ça le concept. Donc on a un système, dès que on a on fait une authentification, dès que l'authentification échoue, Ben le système bloque sans qu'on puisse avoir accès. On va pas se dire donc comme quelqu'un a échoué a tenté l'authentification plusieurs fois.

16:21
Et que l'authentification ne marche pas, Ben on va lui donner l'accès. Quand l'authentification échoue, Ben par défaut on le bloque, il va aller trouver un autre moyen. C'est comme quand on conçoit les systèmes, on va donner un temps, on va donner un certain nombre de tentatives pour mettre les mots de passe. Donc on va dire on va donner 5 tentatives. Donc quand les 5 tentatives ne fonctionnent pas, on bloque le système.

16:43
Et puis on demande de d'appeler le centre d'appel pour que on débloque et et là la personne va s'authentifier tout ça. Donc c'est un peu le même principe, donc par défaut en sécurité, quand quand le système échoue, Ben on bloque, on bloque par défaut. Ensuite un autre concept c'est récupérer en confiance, donc trust recovery, donc on a le le redémarrage d'urgence qui est immergence et System, donc lui il va se produire.

17:11
Il va se produire après une erreur système imprévue, donc il va tenir compte de l'État inconvénient de données corrompues. Ensuite on a l'autre élément qui est redémarrage à froid qui est le cold stats qui se produit après une erreur irrécupérable. Intervention humaine, souvent l'intervention humaine est requise donc c'est c'est un peu l'exemple de quand on a Windows 11 donc un Windows 11 pour le redémarrage plus d'urgence. Donc dès que quelque chose ne va pas, Ben il va proposer le le mode sans échec.

17:40
Pour pour nous permettre de de passer là-dessus. Et puis bon souvent il peut montrer le le Blow of Death pour que pour nous dire que le système ne fonctionne pas. Et puis bon ça va ça va redémarrer ou si on veut faire le redémarrage à fois ça ça sera à nous même de de faire la les la manipulation nécessaire pour faire le redémarrage tranquillement. Ou bien si on veut restaurer l'image système, exécuter le diagnostic.

18:07
Ensuite, on a la séparation des tâches, c'est relation of down, ça permet de prévenir des fraudes et des erreurs, donc il permet de diffuser les tâches et les privilèges associés pour un processus parmi plusieurs utilisateurs. Donc par exemple, on veut que pour faire sortir de l'argent ou faire un chèque, on veut 2 signatures. Ou bien pour un développeur, Ben on veut que le développeur quand il met un avant de déployer un code, Ben on veut qu'il y ait une revue de code pour valider Or.

18:35
Par exemple pour faire une transaction d'argent, Ben on veut. On veut pas que la personne qui émette la transaction soit l'approbateur. Donc on veut séparer les différents rôles pour ne pas qu'il y ait des abus ou de la fraude. Donc rester simple donc qui pic simple diminue, diminue le risque de mauvaise manipulation ou de configuration généralement quand un système est simple.

19:02
Quand on rend le système moins complexe, Ben on a la possibilité de voir les différentes menaces, un

peu quand on a parlé de Quant aux modélisations des menaces, quand c'est simple ou bien quand la configuration est simple, Ben on peut voir tout de suite où on a l'erreur, où est ce qu'on peut avoir les menaces et puis on va. On peut faire une bonne modélisation mais quand le système est complexe, faut juste être complexe à devient compliqué. Même souvent pour des personnes qui sont en sécurité, ils arrivent même pas à comprendre le système, donc ils vont donner des recommandations basiques.

19:30
Donc on recommande toujours en sécurité de rendre toujours les choses simples, d'avoir un système simple pour qu'on puisse faire des des bonnes analyses et des bonnes recommandations là-dessus quand on déploie généralement un système, tout ce qui est faux produit que vous avez pas. Vous avez parlé du hard de nuit tout ça. Donc tout ce qui est système service non utilisé, Ben on enlève, on garde vraiment le le système simple.

19:58
Le dépourvu de tous les éléments inutiles. Le principe, le principe du du Zoro presse donc le le Zoro presse c'est c'est une approche, un modèle de sécurité qui valide systématiquement les accès identité donc identification autorisation et qui protège la circulation des données d'une organisation. Donc ça peut comprendre un problème. Et puis tout ce qui est infonuagique.

20:27
Donc on a la disparition du permettre de de sécurité, donc on se dit qu'on a confiance en rien, donc on se protège pour tout. Donc on se dit que tout système peut être compromis. Donc il va régler une partie de la menace interne. C'est à dire que même un employé en interne qui a des accès, qui a des accès légitimes, peut à un moment donné retourner se retourner contre l'organisation.

20:51
Donc avec le 0 trust on fait en sorte que oui, il a l'accès légitime, mais à un moment donné on veut s'assurer que c'est bien lui et que il a légitimement accès à l'information. Bref, même si il a accès à l'information, si il n'a pas il n'a, il n'a pas besoin de certains types d'informations. Ben on va pas lui donner accès en faire ces types d'informations là. Ensuite on va faire en sorte que tout ce qui circule est chiffré également.

21:22
Donc ça peut être un exemple de on peut avoir un un utilisateur qui lui va s'authentifier régulièrement de temps en temps, même si il s'authentifie avec un un appareil qu'on reconnaît à un moment donné on va faire expirer le token et puis on va lui demander de de s'authentifier. Donc on peut même les IPI en interne. Des fois dans des systèmes d'organisation on peut dire comme le IPI interne, donc on a pas besoin de.

21:46
De Token ? Non, on n'a pas besoin de tokens partout ou bien des fois des communications internes on va dire. Comme c'est une communication interne, on n'a pas besoin de que ça soit chiffré. Si le système à date est le système est désuet au point où on ne peut pas chiffrer. Bon, il faut travailler à réparer cette dette technologique là pour que ça soit chiffré par défaut, on va chiffrer toutes les communications même si elles sont en interne.

22:15
On continue toujours avec le 0 Trade donc ça va nécessiter une source unique et forte, une identité forte donc une authentification d'utilisateurs et d'appareils une utilisation du contexte de localisation

conformité d'appareils ce qui est demandé, savoir également les derniers accès, avoir aussi des politiques de gestion d'accès pour accéder à une application ou des données, surveillance de l'ensemble des appareils et des utilisateurs.

22:40
On a un autre concept qui est faites confiance, mais vérifiez donc qui est une phrase fétiche du du du de l'ancien président américain Ronald Reagan. Donc il est utilisé lors de s'il a utilisé lors de ces discussions surtout avec des représentants de l'Union soviétique. Donc ça c'est le mot russe qui signifie faites confiance, mais vérifiez donc. Il se base également un peu sur le principe du du.

23:07
En gros toujours dans le zero trust donc comme on l'a dit, on aura un sujet, on aura un sujet qui toujours cherche à à accéder à une ressource ou 111 objet comme vous l'avez vu dans la gestion des donc le sujet va demander mais quand il fait la demande. Mais on va faire le contrôle et le contrôle peut s'appuyer sur tous les outils qu'on a, que ça soit le sort, la surveillance, les IDM.

23:34
Ensuite on va vérifier avec les politiques qu'on a et on pourra lui donner accès si bien sûr il a accès. Mais on s'arrête pas là, on va toujours vérifier que il est la personne qui doit avoir accès. J'ai des questions dans le chat, je vois pas systématiquement les questions hein. Felshaker open oui on a fait open aussi mais nous on prend le filshaker généralement dans un contexte applique ?

24:05
Ok la la question de de Jean-Marie, dans quel contexte s'applique les 2 cas ? Sécurité physique, sécurité applicative. Oui, le le fail c'est que on peut l'appliquer dans les 2 cas. Attends, je vais, je vais retourner dans le dans les diapositives.

24:29
On peut l'appliquer dans les 2 cas, système, application, système, sécurité physique également. J'ai pas d'exemple en tête mais OK dans dans la sécurité physique par exemple, on peut faire en sorte que si ta carte de ta ta smartcard qui te permet d'authentifier, si ça ne marche pas, Ben on bloque la porte la porte par exemple de la salle serveur. Si ta carte ne marche pas ou le système d'authentification ne marche pas, Ben tu n'auras pas accès. Donc on peut l'accepter. On peut utiliser le fil chez que.

24:56
Le fait, l'Open c'est vraiment des systèmes moins critiques, comme l'exemple de la porte que je donnais. Admettons que on a, on a la cuisine donc on a la cuisine au bureau, on peut utiliser le fait l'Open là-dessus, donc quand ça marche pas on va laisser la porte ouverte dans le cadre de la sécurité physique dans un système. Vraiment si c'est des données qui sont pas vraiment des des des des informations publiques, là on pourra aller peut être vers des systèmes felopen.

25:25
Mais des systèmes critiques où on a besoin de protéger, Ben on va aller toujours vers du Fail socker. Autre question, est ce que l'attaquant peut changer des tokens d'exception ? Oui, il y a des techniques qui existent pour ça. Comment concilier la sécurité applicative et performance sans compromettre l'expérience ? Ça, c'est des sujets de, de, de, de réflexion ou des sujets de recherche. Moi je pense qu'il faut une collaboration avec l'équipe avec.

25:55

La ligne d'affaire, donc généralement discuter avec la ligne d'affaire, le Product Owner pour pouvoir mettre la sécurité et puis leur permettre d'avoir la performance en conduit donc dans généralement dans le déploiement ou la conception des systèmes. Ben en fait par on fait appel à toutes ces équipes là. Donc tu as le Product Owner, tu as l'analyse d'affaires, tu as l'archipel de solutions, tu as la ligne d'affaires aussi, puis avec l'analyse d'affaires, tout ça qu'ils vont apporter, puis tu as la sécurité qui est là donc on va dire OK ça nous.

26:25
Nous on veut tel aspect tel je. Je prends un exemple, un exemple concret, on a un système de d'authentification de nos clients sur une plate forme et puis on dit dans nos exigences, nous on veut un mot de passe de 15 caractères donc la ligne d'affaire va dire non. 15 caractères c'est trop pour mes clients, ils ils vont pas souvenir et puis ils vont pas vouloir revenir se connecter donc on va retrouver un compromis pour dire OK.

26:49
Combien de caractères tu veux ? L'absence peut dire on veut 8, non 8 c'est trop petit donc on va aller à 10, mais si on va à 10 on veut que tu mettes le MFA. Donc souvent c'est des compromis comme ça qu'on va avoir pour non seulement sécuriser le système mais en même temps permettre à la ligne d'affaire de fonctionner parce qu'en fin de compte c'est eux qui font rentrer de l'argent en sport. La sécurité en elle même c'est vrai, on peut calculer les le Le Roy après.

27:14
Mais la sécurité ne fait pas rentrer directement l'argent, à part si c'est une compagnie qui a contre cœur d'unité la sécurité. Donc c'est la ligne d'affaire qui fait rentrer. Donc on va toujours s'aligner sur eux. Mais on va faire en sorte qu'on ait toujours nos, nos, nos principes de sécurité, qu'on mette en place, quitte à souvent laisser en termes de négociation, laisser certains aspects et puis récupérer d'autres.

27:40
Autre question, les mécanismes freinent ils les performances ? Bah on n'est même pas et constitue un levier indispensable pour garantir. Bon c'est un peu la la même chose que je donnais les contrôles compensatoires. Bon ça ça les contrôles compensatoires c'est quand les les contrôles principaux ne fonctionnent pas donc on pourra mettre les contrôles compensatoires pour pour venir compenser.

28:07
Les mesures de sécurité applicative ne freinent pas, donc on va mettre on va, il y a la performance du système, on va mettre les mesures de sécurité, on va surveiller la performance des systèmes, il y a des outils, tout ça comme Die Hard race on va, on va surveiller la performance des systèmes. Si c'est causé par un outil de sécurité, Ben on va s'asseoir et puis on va voir si on peut faire des exclusions. Mais par défaut, les outils de sécurité ne ne freinent pas si c'est pris en compte.

28:34
Dès la conception et pendant la phase dans le projet, c'est les outils de sécurité ne vont pas freiner. Puis oui, il y a des comme l'exemple que j'ai donné. Oui, il y a des situations qui peuvent décourager. Après les clients, on peut discuter et puis trouver un compromis pour que pour ne pas que ça, ça empêche le système de rouler. C'est bon, on continue.

29:01
Parfait donc on était sur la conception, la confidentialité de la conception. Donc privacy by design

donc pour les développeurs. Donc généralement que ça soit Security by design ou privacy by design on fait en sorte de d'impliquer les développeurs des les développeurs je dirais même pas juste les développeurs le devcops.

29:23
Dans le projet tout au long du projet pour s'assurer que on intègre la sécurité dans toutes les parties du projet. Parce que si on intègre pas la sécurité dès le début, après ça ça devient très coûteux quand le système en production doit mettre la sécurité. Il y a des études qui montrent que c'est c'est vraiment pas une échelle vraiment exponentielle. Mettre la sécurité dès le départ versus mettre la sécurité à la fin.

29:45
Donc on sait que les systèmes sont pas parfaits, donc on va mettre la sécurité. Puis si jamais à la longue du projet on se rend compte qu'il y a des éléments qui ne fonctionnent pas, Ben on va le corriger puis l'améliorer. On a également la responsabilité partagée, donc très souvent vous le voyez dans la responsabilité partagée au niveau du cloud, dans la le share responsability entre le customer et le le fournisseur.

30:13
Mais c'est pas juste dans le cloud, c'est dans tout tout ce qui est sécurité, donc on tient. Chacun est responsable des pratiques de sécurité, donc dans dans l'organisation quand on te donne un ordinateur on te dit de d'utiliser un mot de passe fort. Ben c'est ta responsabilité d'utiliser un mot de passe fort. On te dit de pas utiliser certains c'est c'est de ne pas utiliser à ne pas aller sur certains sites ou ne pas utiliser ton ordinateur à des pour des activités personnelles mais.

30:38
Personne ne viendra te contrôler, mais c'est ta responsabilité de respecter tout ça. Ta ta responsabilité de d'aider l'organisation à améliorer sa sécurité parce que tu es en quand même le le la première ligne pour la défense de de l'organisation. Ensuite, chacun doit agir dans le respect des règles de sécurité, y compris la divulgation responsable des vulnérabilités, donc.

31:02
D'abord, on doit tout faire pour respecter les les politiques, les, les directives. Que ça soit la la directive sur l'utilisation acceptable des actifs informationnels, les les directives de sécurité opérationnelle, les directives de directive de gestion des risques, il y en a. Il y en a plein dans l'organisation. On doit les respecter. Une fois que c'est publié par la haute direction, Ben on doit les respecter.

31:28
Quand on voit des vulnérabilités ou quand on voit des activités non anormales sur notre ordinateur, Ben c'est de notre devoir de les signaler. Si on voit une utilisation inappropriée de d'un ordinateur, on doit le signaler. On voit quelqu'un qui est en train de roder dans l'organisation, qui n'est pas un employé connu, Ben on le signale donc c'est c'est c'est beau comme on fait, on raconte des choses mais en sécurité on joue pas avec ça. Donc quand vous voyez quelque chose qui est pas correct, Ben il faut le signaler.

31:57
C'est de votre stabilité, puis vous aider l'organisation à améliorer on est gars. On demande également de signaler tous les messages d'hameçonnage. Donc ce signalement permet non seulement à votre fournisseur e-mail d'approfondir, d'améliorer sa sa, sa détection de courriels malicieux, mais aussi à

votre organisation de se connaître souvent certains patterns et puis voir que certaines personnes comprennent bien.

32:24
Tous les cours de sensibilisation qu'on fait puis sont capables de détecter des courriels malicieux. Donc ça c'est une façon de contribuer puis d'aider l'organisation à améliorer sa posture de sécurité. Modèle de sécurité donc 3 2, donc on a des systèmes ouverts, donc qui vont utiliser des standards reconnus de l'industrie, donc qui vont faciliter les différentes intégrations. Interfaces. Les interfaces sont publiques et connues, donc on a tout ce qui est système open source qu'on connaît.

32:54
Ensuite on a les systèmes fermés comme les les Apple et autres. Donc vous avez iOS versus Android, Android il est ouvert et iOS il est-il est fermé. Généralement les systèmes fermés on a affaire à des standards propriétaires qui s'intègrent facilement avec nombre, nombre, nombre limité de fournisseurs car l'interface est inconnue donc menaces génériques ne sont pas toujours efficaces. Donc c'est un peu ça l'avantage de ces systèmes là.

33:22
Mais en même temps ça veut pas dire que les systèmes ouverts sont pas sécurisés. On a le trust Compet Computing Biz qui est base informatique sécurisée. Donc c'est un peu un concept concept de la base de confiance des éléments d'un système, un système informatique. Donc on a un élément qui prenne en charge la sécurité du système, donc on a le périmètre de sécurité qui est là.

33:50
Qui qui est considéré comme périmètre de conscience ? Donc on a un autre périmètre qui est sur lequel on ne se focus pas parce que ça fait pas partie de notre système. Et on a le moniteur de référence qui est référence, Monitor, qui va intercéder toutes les demandes d'accès. Donc c'est par là qu'on va faire les entrées, on va vérifier les autorisations. Donc ça c'est si vous voulez un une conceptualisation d'un d'un système. Donc on va donner plus de détails. Le périmètre de sécurité.

34:18
Lui, il a, c'est une limite qui le sépare du du TBC, du reste du du monde, du le reste des de l'environnement. Donc il va s'assurer que l'ensemble des échanges seront contrôlés par le référence Monitor. Donc le référence Monitor, c'est comme lui permet l'entrée et sortie, donc le TCB, lui, il va renforcer l'obligation de créer des canaux sécuritaires, donc le TCB, il peut être, il peut comprendre le noyau l'ouest de la machine.

34:46
Les services de contrôle d'accès, les systèmes de fichiers, les composants matériels protégés. Donc c'est si vous voulez, c'est un système, c'est un système qu'on appelle le TBC. Ensuite le reference Monitor, donc lui il va gérer les contrôles d'accès des sujets aux objets par procédure stricte. Donc quand vous avez fait la gestion des identités, on vous a dit toujours dans un système informatique, vous voyez comme le modèle, on a un sujet.

35:13
Qui peut être un utilisateur qui va accéder à un objet qui peut être un fichier ou un système ? Donc c'est toujours comme ça. Donc le reference Monitor dans un système c'est lui qui va gérer ces ces accès là, qui va gérer ces acteurs là. Donc il va maitriner la sécurité selon 3 propriétés donc toujours

actif. Donc toutes les requêtes vont passer par le noyau du système donc on a le nom modifiable donc impossible de désactiver le contrôle centre village. Donc on va faire en sorte que dans un système.

35:40
On ne peut pas désactiver certains contrôles sans privilège. C'est comme des fois dans un système, quand on veut enlever certains processus de, on va nous demander de nous mettre en mot d'administrateur pour le gérer. Donc ça c'est ces concepts là qui permettent de mettre ça en place. Ensuite, vérifiables donc les règles de sécurité sont explicites, les décisions sont loguées, donc tout ce qu'on va faire dedans dans un système, Ben on veut le loguer.

36:08
Donc les méthodes qui sont utilisées pour déterminer les attributs d'un sujet. Donc on peut avoir un jeton qui est l'information d'identification du sujet. On peut avoir également la capacité, donc la capacité, c'est le droit du sujet sur l'objet donné, donc un jeton qui vient ou un utilisateur qui vient. Ben on sait quels sont les droits qu'il a. Ensuite on a l'étiquette qui est le niveau de sensibilité ou le niveau de classification de de de l'objet en question qu'on veut utiliser.

36:40
On a plusieurs modèles de nos systèmes, donc on a les modèles machine à État Fini, ça en fait on. On est en train de parler de l'architecture des systèmes. Donc peut être que vous ne travaillez pas dans le domaine de l'architecture des systèmes, mais c'est important de comprendre comme ça dès que vous avez un système, quand on vous parle de de de d'un système quelconque, on peut être dans les organisations où on fait de la conception, ça va vous permettre de de comprendre.

37:06
Dans le contexte du cours on va passer tous les éléments pour que vous compreniez demain vous êtes en en face d'un système ou même dans un déploiement ou dans une acquisition d'une solution avec des intégrations. Ça va vous permettre de comprendre les principes de sécurité qui sont derrière. Donc je reviens là-dessus. On a un modèle à modèle machine à État Fini donc State machine modèle donc c'est un État potentiel contenu connu sécuritaire. Donc j'avais parlé de Secure by Default.

37:33
Donc c'est un peu le même concept. Donc on a un État potentiel d'un système ensuite qui est qui est sécuritaire, on a l'initialisation l'initialisation vers l'état initial qui est sécuritaire. Donc si on veut revenir à l'état initial, Ben on s'assurera que le système il est sécuritaire. Et après chaque action, le modèle s'assure que le système effectue des transitions uniquement entre les États jugés sécuritaires.

37:58
C'est bon. Donc c'est si je veux donner un exemple. Donc, on a un système bancaire qui refuse toute transaction qui violerait une règle qui qui ne qui ne qui ne respecte pas un État sûr. Donc, si admettons, on se dit, pour que tu fasses la transaction, il faut que tu arrives à mettre ton code pin, entrer ta carte et que on t'authentifie correctement. Ben si tu mets ta carte, que.

38:24
Tu n'as pas trouvé le bon code que le système ne devrait pas pouvoir te donner l'accès ? Donc c'est c'est un peu un exemple d'un un modèle machine à État Fini. Donc on a le modèle de flux d'information, donc une formation de flux de modèle qui dérive de modèle à État Fini. Donc lui il prévient que les flux d'informations non sécuritaires entre différents niveaux des systèmes.

38:52
Donc si on a un flux d'informations non sécuritaires, Ben lui, il va tout faire pour prévenir ça. Donc avec ces modèles, on va s'assurer que on n'est pas capable d'aller lire des informations qu'on n'a pas droit. Donc les modèles Bell n'a pas doula et biba, on va les voir tantôt. Donc on va formaliser les règles de d'écriture de lecture pour ne pas que quelqu'un puisse avoir des informations auxquelles il n'a pas droit. Donc par exemple, quelqu'un qui a un niveau top secret.

39:20
Étiquette top secrète, il devrait pas pouvoir lire des non. Quelqu'un qui a un niveau secret il doit pas pouvoir lire un fichier qui a un niveau top secret. Donc c'est comme ça on on on s'assure de l'intégrité en fait des éléments et on s'assure que dans les flux d'informations les on on n'a pas une fuite d'informations ou un accès non autorisé ou une modification non autorisée d'un système quelconque.

39:50
C'est bon, on a un autre modèle qui s'appelle modèle de la non de la non Inter non interférence qui va dériver du modèle de flux d'informations. Donc on prend le modèle de flux d'informations, il va, il va en achetant des éléments on va retrouver un autre modèle. Donc si les entrées sont de niveau de sensibilité faible alors les sorties seront toujours des sensibilités faibles. Donc c'est un exemple là si on a un Guess.

40:18
Qui ne m'a aucun dans son système. Il ne peut pas modifier un Guess. Il a il rentre avec ses informations de Guess mais il ne pourra avoir que ses informations de de Guess. Il va pas avoir un information d'un admin sur un fichier quelconque. Un utilisateur de niveau bas ne verra jamais ce qu'un utilisateur de niveau élevé peut voir donc l'action de a donc sécurité élevée vers un objet de B.

40:45
Qui a un sécurité bas ne devrait pas affecter l'état du système de B et être vu par des sujets de ces sécurités bas. Donc c'est un peu l'exemple que je donnais. Donc un utilisateur Guess mais il peut pas, il peut pas voir les éléments que un admin est censé voir c'est bon. Ensuite on a le modèle de protection, le tech Grant également.

41:17
Donc il permet d'évaluer la sécurité de machines suivant certaines règles. Donc on peut avoir des évolutions probables et puis des incohérences. On a dans le modèle, on représente à travers des nœuds, donc on a un nœud qui est un sujet. Comme je l'ai dit, ça peut être une personne, un processus ou un objet également qui peut être un fichier. Donc on peut avoir X qui est un utilisateur et Z qui est un fichier, et les arêtes qui sont des droits qu'on a donc.

41:47
Dans les droits d'attribution qu'on appelle de Grant le, le sujet peut donner à un sujet ou un objet un droit qu'il possède. Donc le Grant c'est que le le X qui est là, il peut donner un droit, s'il a le le le droit de Grant, il pourra donner ce droit là à y pour que y puisse faire des actions sur le fichier Z ou soit on peut avoir un droit d'acquisition qui est le TIC, donc le TIC c'est le sujet peut prendre les droits d'un autre.

42:16
Sujet donc dans le cadre ici donc on AXX qui est X de X vers YXA un droit de tique sur YYA le droit

d'écriture et lecture sur un fichier Z donc X peut prendre ce droit de d'écriture. Le droit de lecture de ce fichier là il peut le lire, c'est bon, c'est c'est souvent à première vue ce modèle là il est-il n'est pas très bien compris.

42:44
Mais vous pouvez le le repasser après vous allez comprendre c'est pas c'est pas très compliqué, je reviens là-dessus, on a 2 systèmes donc on a on a un utilisateur X et on a un utilisateur y ici donc l'utilisateur y il peut accorder le droit, il peut-il a le il a le g là le Grant ici il a le droit de Grant, il peut donner le droit de Grant à y donc lui il peut donner le droit, il peut peut être si je prends dans le cas de l'argent, il peut donner de l'argent à quelqu'un donc.

43:14
Qu'est ce qu'il fait ? Il va prendre son droit de Grant là et donner le droit à le droit de lecture à y pour que y puisse lire le fichier. C'est bon mais attention, il peut arriver que on puisse utiliser les 2 éléments et ça peut entraîner des propagations. Donc c'est que X non seulement il peut avoir le droit de de, il peut avoir le droit de Grant, mais y aussi peut avoir le droit de t donc sans que X le donne il pourra avoir le le droit de prendre le.

43:43
Le le prendre les droits que XA sur un fichier donné. Donc faut faire attention quand on fait souvent les droits d'accès à qui est ce qu'on donne accès et puis est ce que les accès sont pas souvent transférables et qui est capable d'aller se prendre des droits ou qui est capable de se de de se donner des droits ou donner des droits à d'autres personnes, c'est bon ? Est ce qu'il y a des questions ? Oui Émile.

44:09
Oui, si je récapitule, j'essaie de faire aussi un lien. dans Windows vous avez certains droits de répertoire de fichier, on a le take ownership, donc quand on prend un take ownership donc on on prend-on on se met comme propriétaire des droits du fichier. Donc ton texte est ce que ça serait faire à ça ? Puis le Ground c'est à mettons un système back, donc un utilisateur.

44:41
Donne accorde des accès à un autre utilisateur pour lire un fichier. Oui c'est en plus ça le le le cas de take de Windows. Oui si ça te permet de d'avoir le droit, ça permet à l'utilisateur d'avoir un 3 de ondeship oui il peut avoir ce ce donc c'est un peu le modèle en fait c'est le système qu'on voit se base sur ces ces modèles là. Donc la plupart des modèles qu'on est en train de voir, tous les systèmes qu'on voit.

45:08
Se base sur ça donc peut être que peut être que moi j'ai pas l'exemple concret mais c'est sûr que en regardant tu vas peut être te rappeler que j'ai vu ce système à quelque part. Maintenant le droit de grande ça on le voit hein, c'est un admin qui va donner accès à quelqu'un donc l'admin lui il a le droit de lecture il peut-il a le droit de lecture droit de il peut te donner n'importe quel droit à quelqu'un. Donc si tu restes même dans ton cas de Windows dans Windows sur un fichier de données tu peux aller donner des droits à certains utilisateurs donc ça ça sera le le droit de Grant.

45:38
Là-dessus maintenant là où il faut vraiment regarder, c'est que on peut avoir des des systèmes ou des applications ou bien des processus qui peuvent avoir ces droits là. Donc c'est de faire en sorte que

c'est comme quand on donne un compte de un compte à haut privilège à à un à un compte de service. Donc des fois, souvent il y a certains qui confondent un compte de service. C'est pas un compte à haut privilège. Un compte de service c'est pas par défaut un compte à haut privilège.

46:04
Il peut avoir des petits villages élevés pour les services qu'ils font, mais si tu tu tu tu donnes des petits villages élevés à un compte de service. Ben un attaquant est capable de récupérer le compte de service et plus les les les droits, les les droits de ce compte de service là. Et puis faire des attaques parce que le le compte de service en question intervient sur plusieurs machines. Et puis il a quand même des accès donc en comprenant ces genres de modèles là.

46:31
Tu vas facilement comprendre comment est ce que les attaques s'opèrent ou bien comment est ce que on peut rendre un système plus sécuritaire. Donc c'est plus des concepts mais qui sont vraiment utilisés dans la plupart des systèmes qu'on utilise. Donc merci Émile pour ton ton temps, ça permet de de vraiment mettre l'image là-dessus. Oui une dernière question c'est juste pour me rappeler puis savoir si j'ai bien suivi tes systèmes finis ton premier modèle de système fini fini à l'État fini donc.

47:00
Si j'ai bien compris un exemple de ça, c'est comme le guichet automatique, Tu vérifies, puis après ça, aussitôt que tu es vérifié, t'as toute passé là tu fais ton tu peux faire ta transaction, c'est bien ce cas-là j'ai compris. Puis as tu d'autres exemples de système fini ? J'ai comprendre le concept là.

47:25
OK j'ai j'ai pas tout, mais je peux te prendre un un exemple peut être de de d'actuellement là de on est en ligne, on est sur teams pendant toute notre cour, là on le système doit être sécuritaire, c'est à dire que on doit s'assurer que c'est les bonnes personnes qui sont là. La communication vidéo, pas de de d'interférence dans la communication, pas par exemple de de bruit dans les images donc.

47:54
Le système fini, c'est que le système soit sécuritaire à tout moment. Ça, c'est un exemple de de la communication dans les transactions en ligne dans le e-commerce. Ben on veut s'assurer que tout soit sécuritaire jusqu'à la fin de la transaction. Donc que ça soit au niveau de la sélection de tes produits, le mettre dans le cadre le paiement avec ta carte de crédit sur toute la chaîne, souvent c'est même pas le le fournisseur.

48:21
Le e-commerce, le site des e-commerce qui gère le paiement et des fois c'est une autre application qui gère le paiement. Donc on s'assure que de hein, Voilà comme Paypal, comme voilà Paypal et puis tu as tu as d'autres fournisseurs, c'est ça ? Donc c'est c'est des différentes intégrations. Donc on veut s'assurer que sur toute la chaîne on est sûr que tout est sécuritaire sur toute la tout, tout, tout, toute la sur toute la transaction.

48:49
Donc c'est c'est un peu le le concept. Donc si toi tu tu es dans une entreprise qui veut faire du e-commerce, Ben vous allez voir l'architecture. Vous allez d'abord mettre en place vos produits dans la boutique en ligne et vous allez chercher un fournisseur de paiement en ligne qui est PCADSS et vous devez faire l'intégration. Mais dans l'intégration, assurez-vous que vous IPI là soin sécuritaire qui fait

l'authentification correctement et que au niveau du fournisseur, vous allez faire tous les 2 diligent, s'assurer que lui aussi il est sécuritaire et tout ça.

49:18
C'est bon ça m'éclaircit, merci, c'est beau, merci beaucoup. On continue le modèle de protection, c'est bon ensuite.

49:34
On a le modèle de Bell, la padoula qui est apparu en 19109006010, donc il dérive du modèle de machine à État Fini comme on le disait, avec plusieurs niveaux de sécurité pour les sujets, les objets. Donc il va plus prendre en charge la confidentialité. L'autre qu'on va avoir va prendre en charge l'intégrité. Donc il présume que tout est géré par le modèle, donc aucune considération pour les canaux auxiliaires. Ben il est très efficace lorsque combiné avec d'autres modèles. Donc généralement on va combiner le bel, la padoula au biba.

50:02
Pour être plus efficace donc il a 3 propriétés de confidentialité donc la propriété simple de sécurité donc le sujet ne peut lire un niveau de sécurité supérieur ce qui est évident. Moi on dit que je suis un utilisateur, j'ai accès j'ai je suis pas par exemple administrateur système donc j'ai pas accès à la salle Servette donc quand je rentre avec mon ticket dans.

50:31
Je rentre avec ma carte en entreprise, Ben je peux passer dans les endroits publics mais je peux pas rentrer dans la salle dans la salle machine parce que je peux pas lire un niveau de sécurité supérieur tout comme j'ai j'ai dans la racine. Par exemple dans dans l'exemple de SharePoint, un exemple concret, SharePoint ou un système de fichiers. J'ai plusieurs dossiers, j'ai un dossier par an donc j'ai j'ai un fichier qui se trouve j'ai j'ai un fichier a ?

51:00
Qui se trouve dans un dossier parent P et dans le dossier parent P ? J'ai encore un autre dossier dans lequel j'ai des fichiers, mais je peux donner juste accès dans SharePoint. C'est c'est vraiment visible dans SharePoint. Je peux donner accès à mon fichier a mais je donne pas accès au dossier de telle sorte que la personne qui a accès au fichier, il ne voit pas les autres dossiers qui sont dans mon répertoire de parents qui m'ont, qui sont dans mon répertoire de travail.

51:28
Ni aux parents, aux fichiers parents, au répertoire affiché par an parce que ils ne je leur ai pas donné le droit de lire ce qui est au-dessus, est ce que c'est bon ? C'est l'exemple dans dans SharePoint. Ensuite on a la propriété étoile qui est star Security property. Le sujet ne peut écrire, donc ça ce n'est pas la lecture, c'est l'écriture sur un objet de sensibilité moins élevé. Donc la propriété is forte si limitée au même niveau. Donc on va faire en sorte que quelqu'un.

51:54
Qui est avec la la propriété star Security, il peut pas écrire sur un objet de sécurité moins élevé. Donc comme vous le voyez ici on a le why APP il est-il est-il est autorisé, le why down il est bloqué, donc ici le Read APP il est bloqué mais le rhy down il est-il est autorisé. Ensuite on a propriété de sécurité discrétionnaire dont Discretional Security Properties qui est l'utilisation des matrices d'accès pour le compteur d'accès discrétionnaire donc.

52:23
On peut avoir une matrice d'accès pour donner des accès à qui, à aux personnes qu'on veut. Est ce que c'est bon ? Est ce qu'on comprend un peu le le concept ? Donc comme je l'ai dit, c'est c'est des concepts qu'on va utiliser pour appliquer la sécurité dans notre quotidien. Donc c'est sûr que on va pas vous dire que c'est le modèle de de Bella, pas doula qu'on utilise, mais vous allez remarquer que mais.

52:49
Il m'a donné accès au fichier mais je vois pas le dossier. Vous allez remarquer que d'autres personnes voient le dossier mais c'est juste que ces personnes là ont plus de droits que vous donc ils ils voient le dossier que vous ne voyez pas. C'est bon on continue. On a le modèle biba qui est 1977 donc il est basé sur le Finistère, modèle modèle qu'on en avait vu, donc il y a beaucoup qui vont se baser sur ce modèle, donc lui va prendre en charge l'intégrité. Donc on avait parlé de.

53:16
De tout ce qui était confidentialité dans le la puda et lui il va parler d'intégrité donc il va éviter des modifications par des sujets non autorisés, ce qui est évident, t'es pas autorisé, tu peux pas modifier le fichier. Il évite des modifications non autorisées par sujet autorisé, protège, protège la cohérence interne et externe des des objets. Donc il est très efficace lorsque combiné avec d'autres modèles c'est bon.

53:44
Avec toujours le biba, on va tenter d'éviter l'inférence. Donc des morceaux d'information recueillis permettent de recueillir de l'information sensible. Je sais que la flotte militaire est un ravitaillement dans l'information de niveau bas, je sais que le cadran ont été réglés pour 04h00 par les marins. Je peux déduire qu'un départ est prédit vers 04h00. Donc ça, ça, ça pourrait être de l'information sensible.

54:14
Toujours au niveau de de biba donc, on a 2 propriétés, donc la propriété un qui est la propriété simple d'intégrité donc simple integrity properties. Le sujet ne peut lire un objet de sensibilité inférieure. Propriété étoile d'intégrité START Interbuty properties un sujet ne peut écrire tu es un objet d'une sensibilité supérieure donc il va éviter de diminuer la qualité de l'information. Donc je reprends.

54:41
Pour le le simple integrity properties le sujet ne peut lire un objet de sensibilité inférieure, donc si l'objet si c'est de sensibilité inférieure, il peut pas lire. Donc pour le le simple integrity property un sujet ne peut écrire sur un objet d'une sensibilité supérieure, ce qui est évident. Donc c'est à peu près le même concept que le la puda. Donc ici quand on on va combiner les 2, le biba, moodle et puis le bel, la puda.

55:10
Ben ça va faire en sorte que la personne va juste rester au même niveau. Donc le Bell lapouda, lui, il a la confidentialité et le Bell Bell lapadula, c'est la confidentialité. Le Biba c'est l'intégrité. Donc tu seras pas tu pourras pas WhatsApp si tu es dans le biba ici et ici, tu pourras pas WhatsApp quand tu es dans le Bell lapouda. Donc ça va faire en sorte que la personne va rester avec son même niveau.

55:34

Donc puisque il ne peut pas ni lire ni écrit, car à son propre niveau. Donc c'est comme l'exemple de de fichier de de fichier SharePoint que j'ai donné, mais l'accès que vous avez-vous allez pouvoir lire les informations du du, du du fichier dans lequel vous êtes. Si bien sûr, on vous donne le droit d'écriture aussi. Est ce qu'on peut vous enlever le droit d'écriture ? Donc vous allez rester à votre niveau quand on va coupler les modèles. Donc très généralement.

56:00
Aujourd'hui on va coupler généralement ces 2 modèles là dans nos différents systèmes. C'est transparent pour nous parce que nous on va nous montrer comment est ce que on donne les droits d'accès c'est tout. Mais faut savoir l'origine c'est quoi et puis c'est à quelle fin. On arrive à à avoir ces éléments là. On continue avec d'autres modèles donc on a d'autres modèles qui sont les modèles de carte 800987.

56:25
Donc pour les pour, généralement pour les activités commerciales, les transactions construites sont des patrons définis. Donc on a un client, on a les, on a un portail et puis qui va accéder à la base de données. Donc il va prôner l'intégrité par la séparation des tâches. Au niveau des transactions et implémentations, donc on a parlé tantôt de séparation des tâches comme principe pour éviter leur fraude, on a accès aux données se fait à partir de des interfaces, on a un mécanisme indépendant de validation de l'intégrité qui doit exister.

56:52
Donc le c'est le mot. C'est un modèle qui est beaucoup axé sur l'intégrité transactionnelle, donc on veut s'assurer que les règles métier sont respectées. Donc comme on l'a dit, là on va empêcher les différentes fraudes à travers le à travers la séparation des tâches. Ensuite on a le l'autre modèle qui s'appelle le Grower et Nash qui qui s'appelle généralement le Chinese Wall, la mur de Chine qui.

57:19
Lui prévient des conflits d'intérêts sur l'accès aux données, donc il le fait de façon automatique. Donc il est beaucoup utilisé dans l'aspect légal, les compagnies de d'avocats et autres. Et puis dans tout ce qui est investissements. Donc on veut protéger l'information confidentielle, donc on veut faire en sorte que par exemple, quelqu'un qui qui travaille dans un dossier donné.

57:43
Qui puis va ils puisse pas avoir accès à un autre dossier ? Donc souvent pour s'en sortir on appelle ce modèle là généralement le modèle Coca Cola. Donc on veut juste dire que un consultant qui accède au modèle de Coca Cola il ne pourra jamais accéder à Pepsi sur ce même système. Donc pour que vous compreniez donc ce modèle on dans le jargon on va dire Coca Cola modèle pour que pour te dire si tu accèdes à Coca Cola, Ben Tu n'accèdes pas à Pepsi. Donc c'est pareil. Si tu accès à un système d'une banque a, Ben tu n'auras pas accès au système B.

58:14
Ensuite on a d'autres modèles comme de de Google Messenger model qui lui va beaucoup travailler sur l'intégrité. Donc il va empêcher qu'un utilisateur non autorisé influence l'État ou les actions du système. Donc on a les 100 vers Land model qui est l'intégralité qui base basée également sur l'intégrité. Il maintient la cohérente logique des données dans un système c'est bon.

58:45
On a le modèle de Ground in benning qui contrôle la création et la suppression sujet et objet. Vous

allez voir que on vous appliquez ça d'une certaine façon. Donc on a 8 règles. Donc la première règle c'est que on peut créer de façon sécurité un objet. Comme on crée un utilisateur, on peut créer un un objet, un fichier qu'on peut mettre dans un système.

59:10
Ensuite on peut créer de façon sécurité un sujet, donc un un objet c'est c'est un fichier, un sujet c'est un utilisateur, donc on peut créer un un utilisateur. Donc quand un utilisateur est vient nouvellement dans une entreprise, Ben on crée l'utilisateur, donc ça les les règles c'est une règle de gram d'inim qu'on va utiliser, donc on on va créer l'utilisateur. Si on veut utiliser un fichier, on veut un Word qu'on va partager entre nous, Ben on va venir créer le fichier, donc ça c'est une règle de.

59:40
Gramme qu'on va utiliser. Ensuite on peut supprimer de façon sécurité un objet, donc on peut supprimer un fichier comme on peut supprimer un utilisateur qu'on a créé attribution secrétaire de droit de lecture. Donc on peut donner des droits de lecture à un fichier à un à à un utilisateur donné. Comme on peut supprimer aussi, on peut supprimer ce droit là également.

1:00:06
On peut attribuer de façon sécuritaire du droit d'attribution, donc on peut permettre à quelqu'un de lui pouvoir donner des droits d'attribution donc et des droits de grand. On peut lui permettre également de pouvoir transférer des droits d'accès comme le grand qu'on avait. Il peut transférer des des différents droits. Donc vous savez, vu, c'est c'est des modèles qu'on va utiliser avec des différents dans notre activité, dans nos opérations quotidiennes.

1:00:33
C'est bon ? Est ce que il y a des questions ? Je vois pas toutes les mains levées mais selon quel contexte la la question de hayette, selon quel contexte ? Non, actuellement je pense, dans la plupart de nos systèmes, les contextes, les les, les modèles là sont souvent imbriqués, comme quand je parle de biba par exemple. Bell, la buda c'est souvent des modèles qui sont souvent imbriqués et nous.

1:01:01
Qu'est ce qu'on fait dans les systèmes qu'on utilise ? Ben très souvent on va voir comment est ce que on donne les droits d'accès et on applique ici. Moi je dirais peut être dans la conception des des systèmes tu vas voir est ce que tu veux plus travailler sur l'intégrité ou la confidentialité. Donc dépendamment tu vas prendre le modèle qui va avec. Mais de façon générale dans notre pratique même de sécurité, on sait que.

1:01:26
On donne pas les droits d'accès peut être à quelqu'un. On donne pas des droits d'accès élevés à quelqu'un qui n'en a pas besoin dans le moindre privilège. On va pas faire en sorte que quelqu'un qui n'a pas un privilège, un certain privilège, puisse lire les documents plus confidentiels. Donc on va essayer de respecter ces modèles, mais aujourd'hui la plupart, on n'a pas directement affaire à ces modèles. Comme tu le vois dans tes systèmes, tu vas jamais voir Bell, la buda ou biba quelque part.

1:01:56
Donc, mais il faut comprendre comment est ce que d'où tout tout c'est venu et puis comment comment ça ça se déroule à l'intérieur des des systèmes. On continue donc on a le contrôle selon les exigences de sécurité, donc on a la certification. Donc la certification c'est le processus d'évaluation

technique. Donc comme vous êtes en train de faire le CS le coup de CSSP donc vous allez aller peut être chercher la certification.

1:02:26
Mais pour avoir la certification, Ben on va s'assurer que vous maîtrisez bien tous les concepts de, de, de CSSP que vous répondez-vous avez compris les concepts, on va vous mettre dans plusieurs scénarios pour s'assurer que vous comprenez. On va vous reposer les questions d'une certaine façon. Donc quand vous passez le processus, vous réussissez l'examen. OK, c'est beau, vous avez reçu l'examen, donc vous avez validé tout ce qui est tout ce qu'on pouvait tester sur vous. Ah donc Allô Allô.

1:02:56
OK, c'était une erreur. OK, on continue donc. Donc quand vous avez passé l'examen, Ben ce sont les les critères qu'on aura défini pour que vous puissiez avoir la certification pour que vous puissiez passer par le processus. Ensuite, on pourrait évaluer la conformité de chaque partie. Donc on dans votre situation, on va évaluer, mais dans un système, on va s'assurer que le système est conforme. On va regarder les différents parties, matériels, logiciels, réseaux.

1:03:23
Ensuite on va déterminer le niveau global de sécurité du système selon l'environnement ou son contexte d'utilisation. Donc ça c'est ça sera la certification au niveau système. Mais pour que vous compreniez au niveau personnel, si vous faites-vous voulez faire une certification quelconque professionnelle, Ben il y a les critères qui sont là. Donc on va venir tester les critères pour voir. Est ce que vous répondez aux critères ? Est ce que vous comprenez ?

1:03:50
La matière, vous comprenez le concept ? Puis bon on va vous évaluer et puis si c'est correct on va dire que c'est bon. Vous avez donc ça c'est la certification, donc très souvent la certification Ben on on va vous évaluer ça avec un testeur ou un auditeur qui va venir tester l'environnement généralement. Ensuite on a l'accréditation, donc l'accréditation c'est le processus administratif et décisionnel qui suit la la certification. Donc oui pour un système on est dans le cadre d'un système hein, donc d'un système.

1:04:20
On peut, les auditeurs peuvent venir, ils vont évaluer le système, ils vont dire que le système respecte les comptes, les les critères pour que on puisse lui donner la certification. Maintenant l'accréditeur lui, ça sera le processus décisionnel pour attribuer, donc il va suivre la certification.

1:04:36
Sera validé par l'autorité d'approbation désignée. Généralement ça peut être le le chef de sécurité dans l'entreprise hein ? Donc on va, ça sera la personne telle qui peut approuver les risques, accepter que ce que vous avez donné comme recommandation, Ben on les respecte, donc ils peuvent que le système satisfaire aux exigences des sécurités de l'organisation. Ensuite il peut être émise par une tierce partie, donc ça peut être la sécurité contrôle a ce sort dans le le cadre par exemple de d'un système.

1:05:07
Une certification, par exemple ISO je vais prendre par exemple ISO, ISO 9001 ou ISO 21001. Donc une entreprise peut se faire auditer, donc dans le processus de certification, donc l'entreprise peut se faire

auditer. Et quand l'entreprise se fait auditer, Ben c'est un certificateur tiers, soit bureau véritage SGSDSI qui eux vont venir faire l'audit, qui vont vous donner, qui vont dire que vous respectez les critères.

1:05:34
Pour avoir la certification ISO 9001 ou ISO 27001, eux ils vous donnent la certification parce que ils ont déjà reçu une accréditation, donc ils ont déjà reçu une accréditation, soit de l'organisme qui est capable de d'accréditation au niveau du Canada par exemple qui peut être le SCC, donc ça peut être le le standard console.

1:05:55
Du Canada Conseil console du Canada qui lui va accréditer certaines organisations à pouvoir vous délivrer une certification. Donc au niveau peut être de l'Europe, on pourrait avoir le cofrac et autre. Donc c'est un peu l'exemple pour que vous voyez la différence entre l'accréditation et la certification. Est ce qu'il y a des questions ? Questions ? Pas de questions ?

1:06:25
Je suis tannant, mais je veux juste bien comprendre. Notons par exemple, une entreprise qui est Fire High mansion veut auditil une compagnie pour, mettons, faire du PCIDSS, mettons. Je prends un exemple comme ça. Donc le PCIDSS, ça c'est la certification.

1:06:50
Puis l'accréditation, c'est à, mettons qu'on a donné, mettons à Mansion fireye l'accréditation pour venir nous auditer, parce que c'est ça que j'aime bien, oui, c'est oui, oui c'est ça, c'est ça, tu as bien compris, c'est ça maintenant, c'est bien sûr que Mendion et autres eux aussi ils ont fait leur certification hein, ils ont déjà fait leur certification. On s'assure que eux avant d'aller certifier les gens pour dire qu'ils sont bons, Ben eux ils vont.

1:07:18
Passer par le processus Google de la certification et ils pourront demander à être accrédités. Donc ils sont accrédités comme entreprises qui sont capables de délivrer en fait la la certification. Ah c'est bon ? Je comprends mieux la nuance. Merci. OK c'est beau mais très souvent dans notre contexte on est juste beaucoup certification, on se certifie, mais l'accréditation ça sera une organisation qui elle va.

1:07:45
Nous en tout cas, après l'évaluation, on va nous donner une accréditation pour dire qu'on a le droit de faire ceci. Maintenant c'est bon, c'est bon. Allô ? Oui oui Nacer, Bonjour à tout le monde. C'est juste toujours au niveau de l'accréditation que que un petit peu peut être. J'ai mal compris les choses.

1:08:14
C'est à dire l'accréditation voit vient toute vraiment à la fin que soit la certification faite, l'évaluation par une tierce partie soit faite aussi et vient par la suite à la validation par l'autorité par exemple d'approbation. À ce moment-là, l'accréditation doit être approuvée pour que l'entreprise puisse utiliser un tel ou un tel système. C'est ça ?

1:08:40
Résume un peu, oui oui, oui, oui, oui, oui, oui oui. Un petit résumé que j'ai fait là c'est à dire on va voir la certification, l'évaluation, la validation par le par, l'Autorité et l'accréditation à la fin, puis par la suite, ça c'est c'est sûr, le système sera mis en production. C'est ça, c'est beau. OK, c'est en fait dans le

système de production, on va beaucoup les voir des fois, quand vous Regardez les autos, vous allez voir par exemple.

1:09:07
Je sais pas dans dans dans une dans une voiture vous allez voir des des composants, peut être de d'autres fournisseurs et puis vous allez voir qu'ils ont des accréditations là-dessus. Donc c'est sûr que ils sont passés, peut être par ces projets, ils sont passés par ces processus, ils sont accrédités donc les gens se disent c'est des systèmes fiables donc on pourra les utiliser, les intégrer dans dans nos systèmes c'est bon on continue juste dernière question, c'est à dire une fois il est accrédité le système, le premier système est accrédité.

1:09:36
Et s'il y a un petit changement dans le on dirait le même système, mais s'il y a un petit changement, je dois refaire tout le processus, c'est ça ? Oui oui, même même un petit changement, ça doit être un peu contrôlé. Bon on va on va voir tout à l'heure les modèles de commande culturia tout à l'heure là même même même je on parle même pas d'accréditation hein. Quand tu fais un audit, même dans ton organisation, tu donnes une portée, un périmètre.

1:10:06
Donc si le périmètre change, ce n'est plus le même Audi, donc on va s'en tenir à l'audit que tu as eu à faire. Donc c'est pareil pour ces systèmes qui qui vont être utilisés dans beaucoup de d'autres choses. Non ça ça serait facile que Ben tu vas juste donner la partie où tu es bon et puis l'autre n'est pas bon et puis après tu viens l'ajouter ça ça c'est c'est pas bon. Ouais ouais c'est le cas de PCAIDSS, là c'est à chaque fois qu'il y a un petit changement, il faut se.

1:10:33
Voilà c'est comme ça quand il y a, quand il y a un petit changement, mais PCADSS ils sont pas. Ça dépend du volume de transactions que vous avez ici. Le volume de transactions n'est pas très élevé, on on ça on peut juste avec un un cephaset mentionner. On peut se limiter à ça quand le volume n'est pas trop élevé, mais c'est quand le volume est élevé que là il faut vraiment un QSC pour venir faire l'audit. Ils sont quand même flexés sur certains aspects, ça va dépendre du volume de la transaction, c'est bon.

1:11:05
Oui merci ok donc là on a des des éléments qui qui nous permettent de faire des contrôles. Donc on a on a parlé tantôt de la certification de de la crédisation. Maintenant on va dire comment est ce que on contrôle, quels sont les critères qu'on utilise pour contrôler ?

1:11:20
Donc initialement on avait ces critères là que le TC SEC, le Trust Computer System Evaluation Cultural qui lui généralement on les appelle des orange book ou plus Rainbow Series, donc beaucoup de couleurs. Donc il y a le lien ici que vous pouvez trouver. Plusieurs livres ont défini en fait les critères qu'on utilise pour faire l'évaluation des systèmes. Donc c'est un modèle américain qui est beaucoup basé sur la confidentialité.

1:11:47
Ensuite on a le high sect qui est une formule champ Technology Security evalution, donc lui il permet de d'évaluer également les systèmes. Donc c'est le modèle européen est construit sur les fondations du TC SEC, donc il va faire la séparation entre les fonctionnalités et le niveau d'assurance. Donc on a

on va voir est ce qu'on a les fonctionnalités et puis quel est le niveau d'assurance qu'on a pour chacun de ces éléments là. Ensuite on a le CTC PEC qui est le Canadian Trust Controller.

1:12:15
Product Evalution Cutorium qui est l'équivalent canadien qui fusionne un peu l'approche TC SEC et le IT sec. Ensuite on a le Command Cutorium qui qui en partenariat avec le Canada, États-Unis et Europe afin de remplacer, unifier les tous les les anciens que j'ai cités, ils ont mis en place le ISO 15408 qui va évaluer de façon impassable à la sécurité des systèmes et leur conformité au niveau reiki.

1:12:45
Donc lui il va donner le niveau d'assurance qu'on a. Donc le lien en dessous ici va définir l'ensemble des critères qu'on utilise, le Command criterior qu'on va utiliser pour un système donné. Donc c'est vraiment beaucoup le lien en dessous là le Command Cultura Portal. Donc on peut l'utiliser pour voir l'ensemble des critères qu'on utilise.

1:13:09
Mais ça c'est le niveau d'assurance, donc le niveau d'assurance. On a le EAL un qui est qui veut dire testé, confidentiel, testé, fonctionnel e le niveau 2 qui est testé structurellement, le niveau 3, testé et vérifié méthodiquement, le niveau 4 qui est conçu, testé et vérifié méthodiquement. Le niveau 5 est conçu de façon semi formelle et testée et le niveau 6 qui est conception vérifié de façon semi formelle et système testé.

1:13:38
Le niveau 7 qui est conception vérifiée de façon formelle et systèmes testés. Donc ça c'est le tableau de correspondance. Donc le E un va correspondre de IT sec américain et le TC SEC européen. Donc ça c'est le tableau correspondant. Donc le EAL va correspondre au E 0 et le D de l'autre côté, donc ainsi du site. Donc on fait le tableau. Donc le plus important c'est de comprendre les différents niveaux d'assurance.

1:14:08
Le niveau d'assurance c'est un peu comme on a dans le CCMI les niveaux de maturité, donc c'est un peu ça. C'est un peu le niveau d'assurance qu'on a sur un système. Donc si on dit qu'un système a été testé niveau AEAL un donc on a juste testé qu'il est fonctionnel, mais il n'est pas plus rigoureux que par exemple le Eh 3 qui lui est moins rigoureux que le EAL 7, c'est bon, on continue.

1:14:38
On continue juste les questions, est ce qu'on va faire tous les tests ici ou vraiment c'est en fonction du besoin ? Les tests fonctionnent fonctionnellement, tester structurellement, tester, vérifier méthodiquement. Est ce qu'on doit respecter tous ces ces tests ? Non ça dépend, non non, c'est le niveau d'assurance que tu veux sur ton système que tu vas encore appliquer.

1:15:04
Voilà donc j'ai j'ai par exemple donné j'ai j'ai donné un exemple, peut être pour pour que tu comprennes pour pour juste une image. Tu vois par exemple les les véhicules autonomes qu'on a. On a commencé les tests au niveau de je pense San San Francisco, donc tu as des voitures qui des taxis qui sont commandées, qui ont pas des chauffeurs. Donc on est à la phase test.

1:15:31
C'est vrai que eux ils vont passer à à certains niveaux, je sais pas à quel niveau de maturité ils vont

passer déjà, mais dans nous notre contexte on pourrait dire Bon OK c'est que actuellement comme on n'est pas trop sûr on se dit que peut être c'est il a un niveau d'assurance à un certain niveau peut être E 2EEAL 2EAL 3 donc on peut dire qu'il a un certain niveau de d'assurance donc c'est c'est un exemple donc on veut pas le l'étendre à tout le monde. C'est comme un peu la la Tesla.

1:15:58
Les niveaux par exemple d'autonomie ou bien de de self driving à des niveaux de maturité. Donc aujourd'hui ils sont pas arrivés à un certain niveau où on peut dire à un à un conducteur de juste laisser le self driving parce que ils n'ont pas un certain niveau de maturité. Donc pour revenir à notre cours c'est juste des des niveaux qu'on va utiliser pour notre système. Donc si on est au niveau 3 mais on s'attend pas à un à un niveau peut être élevé par rapport à ce quand on est au niveau 7.

1:16:26
Mais on va pas atteindre le plus grand niveau de maturité avant de mettre le le truc en production, sinon ça va tuer l'innovation. Donc à un moment donné on s'est dit OK, si on l'a testé, qu'il est fonctionnel, on peut commencer à produire et puis on va s'améliorer au fur et à mesure. Donc c'est le cas de tous les systèmes qu'on voit et progressivement ils montent à un niveau de maturité. Et puis à un moment donné on a un produit fini. Demain on aura des des illicos qu'il faudra nous des drones qui voudront nous prendre à la maison, nous transporter au bureau sans conducteur.

1:16:55
Bon je pense ça se fait déjà en Asie mais c'est c'est un peu ça. OK on continue donc capacité de sécurité donc capacité de sécurité des systèmes en 3 4 donc dans le système d'un composant d'un ordinateur. Bon comme vous le savez hein, on a un processeur.

1:17:22
On a les mémoires, mémoires volatiles, RAM, mémoire non volatiles, le rhum, le I prob, mémoire Flash, on a la mémoire virtuelle qui est le swap, le swap, généralement c'est une partie du disque qu'on met à côté pour venir compenser la mémoire RAM quand elle est pleine. Donc le soir, ceux ceux qui ont utilisé les systèmes, je sais pas si ça existe encore, mais en tout cas les systèmes Lumix dans le temps, quand on on faisait l'installation, on mettait chaque fois une mémoire, une mémoire, soit par côté pour.

1:17:52
Pour pouvoir pallier, pour pouvoir aider la la mémoire quand elle était ça existe toujours, ça existe toujours mais est ce qu'on le manipule on le on le définit manuellement encore parce qu'il y a longtemps que j'ai pas installé. Oui on le définit, on le définit manuellement. D'ailleurs en ce moment sur une date 8 il y a une forme de bug nous on vit cet enjeu là en ce moment il y a une forme de bug. J'ai des applications qui utilisent la swap alors que la RAM n'est pas.

1:18:19
C'est pas forcément saturé mais dans leur leur déroulement ils vont-ils vont les solliciter obligatoirement OKOKOK donc des fois ils ne libèrent pas. Donc des fois vous êtes amené à à juger si vous avez le bon, le bon, la bonne capacité de soi pour pas. Donc OK toujours quelque chose qui est très très pertinent. OK merci beaucoup dans Windows ça existe toujours hein ? OK non Windows c'est Windows c'est transparent. Ouais ce qu'on appelle Windows c'est.

1:18:47
Ou quelque chose comme ça j'ai oublié le nom mais ça existe. Ouais Ouais Windows c'est transparent

ouais Émile ouais en effet c'est le page file là, puis le hacker file s'en sert un petit peu un genre de soi, mais moi quand tu fermes l'ordi là ouais c'est beau. Merci pour vos contributions. Ensuite on a les stockages, tout ce qui est HDDSDD clé USBCDDVD, on a les micro logiciels, les framework.

1:19:16
On a les périphéries, claviers, souris, écrans, tout ce que vous voyez, les systèmes d'exploitation Windows, Mac OS, Linux et autres. Ensuite on a l'anneau, l'anneau pour représenter notre système et puis dire quels sont les éléments qui se retrouvent au niveau de chaque système. Donc et on va implémenter les niveaux de sécurité à chaque niveau. Donc plus on est vers le centre.

1:19:43
Plus on a des privilèges qu'on va mettre, plus on va mettre de de de privilèges et puis on on devrait pouvoir mettre plus de sécurité. Usuellement selon le mode 2 utilisateur pour l'application 3, privilège privilégié pour les systèmes d'exploitation. Donc c'est quoi exactement ? On a on a le ring 0 qui est le curlner, donc c'est le noyau de la machine. Ensuite au niveau de du ring un Ben on a tout ce qui est composant du OS.

1:20:12
Au au niveau du ring 2, on a tout ce qui est driver les protocoles et au niveau 3 on a les programmes, on a les applications. Donc comme je l'ai dit, plus on va au niveau des euros, on a besoin de privilèges plus élevés. Les utilisateurs eux, c'est le niveau 3 qu'ils vont voir généralement. Nous c'est le niveau 3 qu'on voit au niveau du processeur, au au niveau de de l'o S Kernel. Là c'est pas trop notre problème. Nous on veut cliquer, avancer, utiliser notre application.

1:20:40
Donc avec ces types de noyaux, là ça permet de ça, ça permet de faire l'isolation et la protection du noyau. Donc quand on voit les différentes couches, ça permet de de faire l'isolation et la protection du du noyau. Donc sur un système c'est comme ça que c'est on a, on a le OS, on a le OS, le noyau, on a tout ce qui est composant qui tourne dans le driver et puis on a les applications qui tournent au-dessus.

1:21:10
Dans un processus, dans un processus processus, il y a plusieurs façons de fonctionner. Donc un processus on va se dire c'est un programme qui est en cours d'exécution, donc très souvent dans vos machines quand vous allez faire contrôle je sais pas pour, pour pour rentrer, pour voir le processus des machines, vous allez voir que il y a des processus qui sont en runing tout ça. Et très souvent quand on a une application qui bug, on rentre là sous Windows et puis on va kill le processus.

1:21:38
Que ça fonctionne pas sous Linux on va faire des commandes pour aller les enlever. Donc pour dire que toutes les activités qui se passent sur notre machine sont gérées par des processus. Maintenant ces processus là ont des États, vous voyez ont des États, donc au départ ils ont des États prêts ou créer étude donc ils sont créés et puis ils sont prêts à à être exécutés. Ensuite ils ont des États en attente qui ont souvent bloqués donc donc ça peut être en attente.

1:22:08
D'une ressource spécifique. Donc il va attendre, soit il va attendre dans la mémoire, soit la la RAM, ou bien il va aller dans le swap ici pour aller attendre. Donc comme disait P file ou swap SP, donc après le waiting, Ben il va aller en exécution donc il va aller, il va le rouler et c'est là que on va voir l'application.

Donc il peut rouler en mode utilisateur au niveau de l'anneau 3, comme il peut rouler en mode privilégié au niveau de l'anneau 0 juste au niveau du kernel.

1:22:37
Et après avoir fait tout ça à un moment donné peut être il peut être bloqué aussi hein, il peut être bloqué et puis et puis il peut être bloqué au niveau aller si la mémoire est occupée, Ben il va aller au niveau du choix. Ensuite il va arriver à un niveau où il est terminé, où il est stoppé, donc l'exécution est finie, il peut être exécuté, il peut être stoppé par lui même ou par un autre processus généralement, donc c'est comme ça que fonctionne.

1:23:03
Tout tout ce qu'on voit sur la machine des processus en anglais et ces processus ont différents États. Donc au niveau des processeurs on a des codes d'authentification, de codes d'authentification, de pointeurs qu'on a, qu'on on va appeler le pack pointeurs authentification de code. Donc ils vont ajouter ajout d'une signature qui est au graphie à une adresse mémoire qu'on va appeler pointeur.

1:23:27
Où ils vont détecter toute manipulation ou falsification du du pointeur. Donc on fait référence au pointeur d'authentification ou au RMV 8 3 donc généralement qui sont utilisés au niveau de des AIOS ou Mac OS dans système, on a aussi la protection de l'espace exécutable qu'on va appeler souvent le pack WXO et le DEP. Donc lui, qu'est ce qu'il fait ? Il va.

1:23:54
Il va masquer masquer la les plages de mémoire, poètes en lecture ou écriture en exécution, en mode utilisateur privilégié. Donc qu'est ce que lui fait ? Il va juste protéger l'espace exécutable qui désigne une technique de sécurité de mémoire qui empêche que un espace mémoire puisse être utilisé à la qu'il puisse être à la fois exécutée et écrite.

1:24:18
Donc il n'est pas granulaire, ne protège pas contre les manipulations des piles. Donc il y a des types de d'attaques qu'on appelle le Routeur oriental programming, donc il va pas protéger contre ça. Donc en gros c'est ça la protection de l'espace, c'est ça ? C'est que on veut pas que un espace mémoire soit à la fois écrite et exécuté, mais en cas d'attaque les attaquants arrivent à le manipuler, donc on peut mettre des codes malicieux.

1:24:48
Ensuite on a la distribution d'espaces discussion aléatoire de l'espace d'adressage qui est le HCR address Space layout randomisation. C'est un positionnement aléatoire par processus, donc de mémoire d'exécution mémoire des données. Donc on a le pinsta qui est l'appel à des fonctions méthodes, procédures où on a le Task qui est l'espace mémoire dynamique géré par l'application, où on a nos librairies qu'on a souvent le libre Lib C ou Kendall Tand D point DL.

1:25:17
Ces points et non virgule. Ensuite on a le le trust Platform Moodle qui est le TPM donc il va assurer l'intégrité de la plateforme donc par signe de confiance de UFIUFI. Donc on a le chiffrement du disque au niveau des chiffrements de disques. Les clés plus authentification d'amorçage, on a la protection par mot de passe pour l'accès à des clés. Et puis on a 5 formes de de TPM qu'on peut avoir.

1:25:46

Donc on a le plus matériel, micro système, hyperviseur et logiciel pour le chiffrement déchiffrement, donc selon la forme de la donnée. Donc on peut se baser sur le HSM, le add we Security moodle qui est la gestion des clés cryptographiques, donc souvent pour les exigences de PCA et DSS pour les financiers, quand on veut faire utiliser les terminaux de paiement. Donc on va utiliser d'avoir le HSM là-dessus.

1:26:22
Attenir la vulnérabilité, on est à la page 61. Attenir la vulnérabilité architecture donc avant, est ce que il y a des questions OKOK, c'est bon, c'est ça ? Armani, c'est ça contrôle all sup, c'est ça pour voir les les processus, c'est bon. Attenir la vulnérabilité architecture.

1:26:56
Ben la statue des systèmes. On a plusieurs types de systèmes qu'on a, donc on on a des systèmes de contrôle industriels qu'on appelle des ICS, donc c'est des noms génériques qu'on a. Mais vous allez retrouver des des modèles, des types qu'on appelle des squadas, ou bien des PLC ou bien des des des DCDCR disponibilité de contrôle système qu'on a des fois donc.

1:27:17
Les les ICI c'est quoi ? C'est que Réseautique Réseautique en mode série, donc souvent ils sont pas sécuritaires et puis ils sont isolés. Donc c'est des anciens systèmes qu'on on utilisait parfois et des fois on puisque c'est des systèmes industriels, des fois on veut les connecter au RP donc il vient augmenter la surface d'attaque. Donc on on a notre usine qui produit donc on veut gérer toutes les tout l'inventaire, savoir quel type de produit on a.

1:27:47
Et puis faire en sorte que ça soit visible sur notre site web pour que éventuellement nos clients puissent passer la commande. Donc on intègre au RP. On peut aussi voir l'aspect finance tout ça. Donc ça ça entraîne des de d'autres points d'attaque. Ce sont des équipements qui sont souvent plus de 20 ans, souvent sans possibilité de mise à jour. Donc on a des systèmes souvent Legacy dans des entreprises où toute la je vais dire.

1:28:16
Toute la technologie est basée là-dessus je suis trouvée toute toute l'activité métier est basée là-dessus mais on peut pas changer le système donc on continue avec le système c'est vieux, on peut pas faire grand chose donc très souvent on va voir comment est ce qu'on peut l'isoler. On peut avoir un impact organisationnel important là-dessus au niveau des ICS. Donc très souvent on utilise l'architecture pure dure pour protéger comme j'ai parlé de tantôt de segmentation.

1:28:44
Donc ce sont des infrastructures. Ils sont utilisés généralement dans les infrastructures essentielles comme les l'eau, énergie Télécom. Très souvent c'est on utilise ces systèmes là. Ensuite un autre type de système qu'on a c'est l'internet des objets industriels, IIOT, Industrial, internet, off things qui lui c'est un peu l'évolution des ICS, nouvelle architecture. Donc là on va voir les les devices, des capteurs, des actionnaires, des machines intelligentes.

1:29:13
On a des Edge, donc tu as des gateway, des concentrateurs de données. On a des forts qui sont des minis serveurs industriels, donc des des systèmes squadas améliorés, des squadas c'est c'est des c'est

dans la famille de AICS, donc les ICS c'est le groupe des Squadas. Et puis d'autres éléments comme les PCS dont je j'avais parlé, les DCS dont je rappelle les PLC et les DCS. Ensuite on a le cloud.

1:29:37
Donc les on pourra avoir les tableaux de bord IA avec la maintenance préventive, donc c'est un peu le schéma qui est là. Donc on on a les devices qui sont là, les senseurs qui sont là, qui vont récupérer les les informations. On a le Edge qui sont là, les get oui on va passer par l'internet, le mini serveur industriel et ensuite avec le cloud des on est capable d'avoir de l'information prédictive qu'on peut donner aux utilisateurs ou à aux décideurs.

1:30:05
Ensuite on a l'internet des objets donc on fait la différence entre les 2. L'internet des objets simple, c'est vraiment ce qu'est utilisé grand public. Donc vous avez votre capteur de thermostat à la Maison pour ça ça va être du high out, mais l'autre ça sera plus industriel. Quoique des fois les 2 se vont se merger. Donc souvent c'est c'est pas trop sécurisé, c'est mal configuré ou c'est pas mis à jour des fois, donc c'est une facile d'exploitation.

1:30:30
Maintenu sur des réseaux indépendants. Donc ça peut être la cafetière, caméra Sonnet, thermostat. Donc aujourd'hui on a plein de IOT chez nous à la maison, la machine à laver plein, plein le la poêle, tout ça. On a aujourd'hui le wi fi dessus et puis c'est connecté à Internet. Ensuite comme élément système à prendre en compte, on a les appareils mobiles qu'on a beaucoup, qu'on utilise beaucoup dans notre, dans les entreprises.

1:31:00
Il est 20 h, on va prendre une pause de de 10 Min et puis on va venir continuer. Après on revient à 20h10.

1:31:59
Monsieur, vous nous partagez votre conversation, pourrez vous peut être arrêter s'il vous plaît ?

1:39:57
Allô, c'est bon, on est là, on peut continuer. Nasser, Nasser, tu es là, oui, oui, je suis là, Annette, tu es là, Émile également, oui je suis là, puis en même temps j'ai une question pour non c'est c'est bon, vas y ça.

1:40:25
Ça permet de de donner plus d'explications. J'aimerais revenir sur ton concept de Edge computing et de **** Computing, est ce que c'est cette ces concepts là c'est uniquement utilisés dans le cadre de l'internet des objets industriels ? Le Fog oui mais le Edge non. Le fog peut être mais le le Edge le le Edge non, le Edge il est utilisé dans.

1:40:55
Les réseaux de façon générale même le fog je peux confirmer mais comme je vois que c'est vraiment industriel mais je peux confirmer mais je sais que le Edge lui tout ce qui est commutateur dans un réseau général. On va tu vas parler de Edge généralement les routes Edge et les les les périphériques Edge dans le concept de réseau de façon générale. OK donc c'est bon OK charmant en informatique là on réinvente pas la roue hein.

1:41:25
On tribale les anciens concepts, on continue, on continue même quand il y a un nouveau concept. Quand tu regardes dans le fond ça, ça reprend certains anciens modèles et puis on continue avec donc on revient là-dessus. Donc parmi les les éléments qu'on peut avoir dans notre environnement au niveau de des des systèmes, donc on a les appareils mobiles qui sont aujourd'hui de plus en plus utilisés dans les entreprises, on a tous des téléphones portables.

1:41:53
On a tous des ordinateurs portables et souvent les téléphones portables qu'on a, c'est des notre téléphone. Dépendamment de la du cas, ça peut nous appartenir comme ça peut appartenir à l'organisation. Donc. Et dans ça il y a des contextes d'utilisation. Donc avec les appareils mobiles, Ben on vient avec des un outil qu'on qui permet de de gérer les devices qu'on appelle le mobile Device management.

1:42:18
Donc le MDM donc il permet de de chiffrer les mémoires, l'effacement ou verrouillage à distance. Il peut permettre de de mettre des politiques là-dessus pour sauver l'écran, la segmentation des stockages. Donc si on a les données d'entreprise pour les données personnelles, on est capable de de faire la segmentation et puis il peut contrôler les applications qu'on a sur le système, donc ça c'est les mobile device qu'on a. Bon je vais pas parler de l'aspect administratif, il faut avoir une politique de.

1:42:47
L'utilisation des appareils mobiles dans l'organisation donc ça on n'en parle pas. On va juste parler des différents modèles qu'on peut avoir avec les l'utilisation des téléphones. Donc le premier ça sera le cobot qu'on appelle Company on business only donc ça veut dire quoi ? C'est que on a avec le le Cobot donc l'appareil est fourni par l'entreprise et le contrôle de l'appareil c'est pour juste à usage de usage professionnel donc.

1:43:17
L'entreprise va donner un appareil, vous n'avez pas le droit de de mettre vos applications personnelles là-dessus. Vous devez pas passer vos appareils personnels, vos appels personnels. Donc c'est justement dans le cas de l'utilisation entreprise. Donc on appelle ça généralement des cobots. On a le le byody qui est le bring your on device qui est lui est c'est le thème populaire, ce que les autres cobots, Copé, Coy sont pas très souvent utilisés.

1:43:43
Donc on a le biody qui est le bring your Home device qui veut dire que Ben on a nous même notre appareil donc on apporte notre appareil et on va bénéficier des ressources de l'entreprise. Donc ça permet la réduction des coûts. Et puis bon la flexibilité aussi au niveau des employés. Donc j'ai mon appareil personnel, je peux partir avec mon appareil.

1:44:05
Et puis je suis enregistré sur le portail de. Je suis enregistré dans le MDM de l'entreprise et je vais recevoir un portail d'entreprise et le portail d'entreprise. Je vais installer les applications de l'entreprise. Je vais installer les les, les, les applications de telle sorte que je puisse avoir accès au Outlook teams de l'entreprise sans avoir un appareil propre de l'entreprise. Ensuite on a le COP Corp qui est le corporate and personal inable donc.

1:44:34
L'entreprise peut te donner un appareil et puis te permettre quelques usages personnels. Donc lui dire OK, je te donne ton le téléphone où je te donne l'ordinateur, mais tu peux utiliser des appareils jusqu'à tu peux utiliser pour des affaires personnelles d'une façon raisonnable. Généralement, c'est ce qui est écrit dans les directives sur l'utilisation acceptable des actifs informationnels.

1:44:58
C'est à dire que on on veut pas te dire de ne pas utiliser, de ne pas ouvrir ton compte de Desjardins sur ton appareil, mais en même temps, on veut que tu tu tu prennes soin comme un bon père de famille. Voilà donc c'est vraiment la l'équilibre en fait entre fais tes activités professionnelles. Certes tu peux faire des activités personnelles mais n'abuse pas. Voilà donc c'est généralement c'est le mode qu'on qu'on on voit généralement beaucoup avec le téléphone, les surtout avec les ordinateurs.

1:45:26
Donc on n'interdit pas. On te dit pas de ne pas utiliser les affaires personnelles, tu peux l'utiliser mais fais attention. Donc on a les CCUID qui est le chose your own device. Donc l'employé l'appareil peut être pour la compagnie mais c'est l'utilisateur qui l'utilisateur. Il va choisir parmi la liste à prouver des appareils qui sont compatibles dans l'organisation.

1:45:51
Donc si je prends le cas par exemple des c'est pas dans notre contexte. Bon je vais prendre UI je prends c'est UI qui est qui a été interdit dans le réseau au niveau du Canada hein si mon mes souvenirs sont bons. Donc au niveau du fédéral par exemple, Ben tu pourras pas utiliser un appareil UI parce que ça fait pas partie de la liste des appareils approuvés. Donc tu vas utiliser des appareils. Tu vas utiliser peut être Samsung Apple des appareils qui sont généralement.

1:46:19
À prouver que tu pourras utiliser c'est bon mais tout ça le le le chose your Or device pourquoi des devices ? Certains devices à prouver ? Moi j'ai fait un petit exercice de essayer de d'appliquer les correctifs sur les appareils mobiles dans le monde iOS. T'as pas de problème, tu as un iOS c'est correct c'est la même chose sur des appareils.

1:46:48
Mais dans le monde Android, chaque marque a son propre Android donc il y a le noyau d'android. Mais tu as Samsung, tu as son Android, tu as Motorola qui a son Android, tu as Google, tu as son Android, tu as plein bon Google je pense que eux ils prennent le natif mais ça devient complexe. Donc plus vous avez des appareils, différents types d'appareils dans l'organisation, ça devient compliqué de faire la mise à jour de les OS tout ça.

1:47:14
Donc si vous voulez mettre une stratégie pour peut être bloquer les OOS à des versions acceptantes ça devient compliqué. Donc si avoir vous avez une possibilité de vraiment restreindre le choix des appareils à juste à certains fabricants ça va faciliter le travail. Mais je m'imagine moi dans mon contexte et pas plus de 1000 employés. Mais je m'imagine des organisations qui ont 10050 1000 employés. Ça va devenir compliqué. Donc on peut si c'est l'entreprise qui donne des appareils.

1:47:43
Mais elle peut choisir certains modèles pour que les mises à jour soient plus faciles après. Ensuite

après les appareils mobiles on a l'info Nuagique donc l'info nuagique on va pas rentrer dans d'autres détails, plein d'aspects que vous savez déjà. Donc on a des des modèles de le modèle de déploiement donc on a le le public qui est accessible tous par Internet donc.

1:48:10
Ça les AWS, les Microsoft, le Microsoft Azure, Google cloud. Donc c'est du cloud public. On a le privé qui est directement sur le réseau des entreprises, donc isolé de l'internet. Donc on a les openstack, les banques ou institutions financières. On a le cloud communautaire qui est partagé par plusieurs organisations ayant les intérêts ou obligations communes. Donc on va avoir cloud santé Canada, éducation, secteur public et on a le hybride qui est selon le type de besoin de données dans le système adepte.

1:48:39
Il est souvent combiné avec le cloud public et le cloud privé. Ensuite on a le modèle de service, le modèle de service, on a le SaaS qui est Software ad services, donc c'est juste l'applicatif qu'on a. Donc c'est M 365, Google Doc, Salesforce et autres Dynamics, toutes les solutions SaaS qu'on utilise aujourd'hui. Chat, GPT tout ça.

1:49:06
Ensuite on a le Task qui est qui lui va avoir OS, intégration des bases de données. Donc on a on peut retrouver dans Google cloud, AWS, Azure et autres donc plateforme de services. On a pas mal de ces solutions là donc on a pas mal de de cloud APP Engine et autres. On a le AIS qui lui infrastructure services qui lui.

1:49:33
On peut avoir tout ce qui est stockage serveur, les outils, donc c'est le plus complet, donc on AAWECS Elastic Computer cloud comme exemple les facteurs de risque.

INF813-Séance10-20250618_PA02

0:01
Ou on dirait peut être l'identité en interne. Donc à un moment donné on peut évoluer donc ça peut amener son lot de risques. On a souvent des rétracteurs au niveau fournisseurs, clients, on a souvent des enjeux de robustesse, transparence et puis visibilité. Des fois un autre système des systèmes basés sur serveur. Donc on a selon oaps on a des top TEN oaps qu'on a.

0:29
Des Vulnérabilités comme les Éjections SQLXML Javascript. Donc on peut injecter des codes imprévus. On a des XML qui peuvent être exploitables, donc abuser des échanges en messages. On a le coach sidè scripting qui est injecté du code, du contenu, du code pour diriger des pages, et on a le code sight request aujourd'hui, qui est l'exploitation de la session active d'un utilisateur pour effectuer une action à son insu.

0:54
Donc depuis un CTS, donc on a plusieurs types d'attaques qu'on peut avoir avec le waps soft TEN, vous en avez plusieurs. On a aussi la falsification des données data DD, donc c'est des petits changements aléatoires aux données, donc principalement qui peut être fait par des menaces internes, donc des mécanismes de vérification d'intégrité. On a des exemples qu'on appelle de salami attaque, donc ce qu'on peut faire, on peut changer de petites valeurs.

1:23
De petites valeurs sur des données financières. Donc qu'est ce que je fais ? Ben je suis-je peux, je peux m'en transférer 1,00$ sur un compte à chaque fois. Ben le le titulaire du compte il le saura pas parce que c'est 1$, donc je peux on peut changer les petites valeurs, faire des petites transactions, on ne saura pas. Donc les mécanismes de séparation des tâches sont inefficaces donc contre ce type d'attaque, donc comme je l'avais dit dans l'exemple précédent, donc on peut faire en sorte que.

1:53
La personne qui demande la transaction soit pas la personne qui approuve la transaction. Donc pour contrer ces genres d'attaques, là on a nos systèmes de gestion des bases de données. Donc avec nos systèmes de gestion des bases de données, on a plusieurs aspects qu'on peut avoir comme l'agrégation. Donc l'agrégation c'est la combinaison d'enregistrements de fait valeur pour construire des informations intéressantes. Donc ça, ça c'est des types d'attaques qu'on pourrait avoir. Donc qu'est ce qu'on fait ? C'est que on a on on peut dire.

2:22
On a une analyse qui peut consulter séparément des affectations des militaires, donc il peut connaître leurs heures et leurs mouvements pour en déduire l'emplacement d'une base, d'une base secrète. Donc ça c'est c'est un petit exemple où je peux par exemple prendre le salaire de une personne ou bien le le le taux horaire d'une personne. On m'a donné le taux horaire, le nombre d'heures, il a travaillé. Je peux ressortir les informations progressivement. Il peut constituer.

2:51
L'information qui va elle devenir sensible. Donc souvent c'est contrôlé par par les DBA, ce genre de ce ce genre d'attaque là. Ensuite, on a un autre élément qui s'appelle l'Inférence, dont l'inférence, c'est l'analyse d'informations non classifiées pour déduire l'information classifiée. Donc un employé connaît

la masse salariale totale et la date d'embauche sans avoir accès au salaire déduit le salaire de chacun en calculant la variation.

3:19
De la masse salariale. Bon, qu'est ce que il peut faire, c'est que il sait ça dans ce cas, l'inférence, c'est que celui qui envoie les salaires ou celui qui traite les salaires, mais il avait la masse salariale totale globale, il sait qu'il y a une nouvelle embauche, il peut faire la soustraction et puis voir. Bon c'est pas tout à fait vrai parce que il peut avoir des augmentations de salaires en temps où il y a des gens qui peuvent faire des over time, mais c'est juste des exemples que vous comprenez en termes d'inférence, qu'est ce qu'on est capable de ?

3:50
De fait, ensuite on a la collecte des données, donc la détection des menaces. Et pour établir des des modèles, on a l'entreposage des données qui lui permet colliger beaucoup de données, de toute provenance, donc permet des des mécanismes, donc analyse des données. On peut trouver des tendances pour récupérer des informations au niveau des de nos BD ensuite.

4:18
On va parler maintenant des micro services, est ce que on a des on a des questions ? OK parfait l'agrégation, l'inférence, ce sont des questions qui sautent beaucoup dans le CSSP donc faut comprendre le les, les différents thèmes. La différence entre les 2 c'est c'est important. Micro services, avant de continuer, on est à 75, il nous reste environ 20 slides. Une petite question.

4:53
Je vais revenir. Est ce que Oh est ce que l'enregistrement continue ? OK oui je le vois de mon côté. Oui OK c'est bon parce que je vois qu'il me il me dit que l'enregistrement s'est arrêté alors que je l'avais pas arrêté. J'avais juste arrêté le partage. Mais bon on va on sera obligé de d'avoir 2 vidéos.

5:26
Ok je vais vous poser une question, est ce que c'est vrai que ça va revenir pendant la révision ? Est ce que pour beaucoup d'entre vous vous faites ce cours là pour réellement passer le cssp ou pour juste valider votre diplôme ? Dans mon cas je pense que c'est l'examen au mois de juillet, c'est déjà planifié.

5:54
Est ce que j'ai ? J'ai d'autres exemples OK donc j'ai les 2OK OK moi aussi là c'est bon planifié pour le mois d'août là donc en même temps Ben ça j'ai terminé la maîtrise fait que c'est comme un peu consolidation là. Puis en même temps Ben je pense que c'est un bon, c'est un bon à tout à voir. OK c'est bon c'était juste par curiosité parce que ça.

6:23
Après c'est c'est des préparations différentes si on veut juste valider le cours ou bien on veut faire le CSSP. C'est beau je pense à la session. Après on on va en parler à l'autre session de demain, on va faire le réseau et puis l'autre session, on va faire la révision. On pourra revenir sur certains aspects pour ceux qui veulent réellement faire le CSSP. Puis Émile a déjà bouclé pour juillet, donc Émile.

6:46
C'est sûr que il faut travailler. C'est le c'est quelle date juillet tu as ? Tu as quelle date mi-juillet mi-juillet à Ottawa ? OKOK donc tu as encore 20 jours ? Ben ça dépend si tu si tu mets, tu te donnes 2 h

chaque soir, je pense que tu peux généralement généralement je me donne 1 h 01h30 par soir de d'étude là.

7:09
OK, je sais qu'il y a des graduellement, des questions, une couple de choses OKOK, c'est beau. OK, je reste dit que l'université a imposé oui. Bon, moi je dirais que c'est c'est bien, si c'est imposé, c'est bon ça, ça va vraiment vous aider. Moi j'avoue que avant d'avoir étudié le CSSP, je faisais, je travaillais en sécurité, c'est vrai, mais.

7:38
Avant d'étudier le CSSPI quand après que j'ai étudié j'étais plus la même personne donc j'ai compris beaucoup de choses. Et puis bon c'est vrai que le le cours c'est beaucoup de slides, mais il y a beaucoup d'informations, ça fait que après vous allez comprendre la sécurité même c'est quoi exactement ? Et puis quel que soit le sujet vous allez être capable de de comprendre et puis vous prononcer là-dessus. Oui zéphirin, oui je sais juste pour faire un pause sur ce que tu dis à bout c'est.

8:07
C'est vraiment une déformation qui qui se vit en temps réel. Et en plus de ça, c'est une très belle consolidation. Pour ce qui est de la formation de la de maîtrise, c'est comme si c'était un fil conducteur en fait par rapport à ce qui s'est pris antérieurement dans les autres courses, c'est c'est c'est beaucoup de déjà vu, mais d'une autre façon, d'une d'une façon un peu plus de de point de vue gouvernance ou encore direction-là dans ce sens-là.

8:37
C'est beau merci zévirin achète avait levé la main. J'avais vu quelqu'un qui avait levé la main. OK oui achète a yet a yet désolé vas y je voulais juste dire comme quoi juste un commentaire c'est un comment dire. Un bon initiative d'avoir secours pour notre programme.

9:06
Ouais Ouais Ouais c'est ça vous, vous avez la chance d'avoir ça au programme. Nous à notre époque quand je faisais ma maîtrise, on n'avait pas ce type de cours. C'est vrai qu'on avait des cours qui reprenaient le siza mais c'était pas un cours de préparation au Siza donc c'était le le module était calqué sur le siza mais c'était pas un cours de préparation comme vous l'avez. Donc moi je pense que c'est une c'est c'est une chance. Et puis je vous encourage à aller sur faire votre CSSP.

9:33
Je je vous encourage ça. Ça vrai que c'est la préparation est vraiment dure après ces cours là ça vous prend encore de faire plusieurs tests pour être prêt, mais allez y faire oui et vite. Puis mon expérience personnelle, quand j'ai acheté le l'examen CSSP, j'ai pris le piece of mind donc je vais avoir droit à un retak. Donc quand je vais faire l'examen je vais faire ça.

10:02
C'est sûr que je vais le porter à la première la première fois, mais au moins avec le Peas of mind, un petit peu plus cher que juste un passage. Au moins t'as un retail en cas d'échec fait que ça te libère un peu plus. Par contre c'est un peu cher aussi là en terme canadien.

10:23
Mais par contre je pense que ça vaut la peine là honnêtement t'inquiète pas, le CSSP c'est c'est l'un des meilleurs investissements, c'est plus rentable que la que le Bitcoin. Donc c'est pas vraiment.

Quand j'ai vu le tour j'ai fait Oh OK, je m'inscrire à ce cours là, puis même moi au niveau de mon travail de tous les jours.

10:43
Je m'en rends compte moi même j'en. Je commence à employer des termes du CSSP mais sur le contrôle j'apprends un petit peu. C'est quoi les les les outils ICS ? Puis je suis en train même de changer mon mon discours OKOK c'est bon c'est bon en tout cas pour moi hein, je vous le dis franchement.

11:07
Initialement, le cours n'était pas donné aux étudiants réguliers, je pense. C'était un cours qui était fait, qui était donné à des entreprises qui envoyaient leurs employés. En tout cas, tout ce que Richard m'a dit, C'est que c'est c'est à partir de cette session là qu'ils l'ont mis au programme et moi je j'ai quand quand il m'a dit J'ai dit mais c'est c'est très bien ça. C'est vraiment une chance que vous avez, en tout cas de de mon point de vue, c'est vraiment une chance. Prenez le cours au sérieux.

11:36
Et puis pour ceux qui n'avaient pas planifié faire allez y fait c'est pas grave c'est 700$ US, planifiez ça au moins d'ici la fin de 2025, passez l'examen si vous l'avez pas eu, c'est pas grave, vous saurez les domaines dans lesquels vous n'avez pas performé et puis vous allez travailler, vous allez repasser votre examen après donc vous allez voir l'examen vous même, vous allez voir la différence un peu dans votre carrière. Ah oui, près des voyages. Bon c'est pas grave, c'est Ottawa n'est pas loin donc.

12:03
Ottawa c'est à 2 sort de Montréal Hein ? Ouais c'est pas c'est pas loin OK OK et puis et puis et puis vous avez votre coût moins cher je pense pour les bon pour ceux qui sont canadiens ou résidents permanents, là le coût n'est pas cher. Peut être pour les étudiants internationaux oui mais un coût de CSSP ça coûte très cher sur la plate forme de IC score.

12:29
Bon, c'était juste pour vous partager un peu mon expérience, vous encourager à à passer à l'action. Allez y faire votre examen pour ceux qui ne l'ont pas encore planifié, allez y faire votre examen sur ce oui, on peut le faire au stage, on peut le faire partout.

12:50
Mais vous savez hein, c'est pas en français hein, il y a pas de français, c'est soit en anglais, en chinois ou mais ça demande aussi une une expérience en cyber hein, on peut pas y aller ? Non ça ça peut pas être plus de 2 ans je crois. Non ça ça ça c'est 5 ans, ça c'est pour valider, c'est pour valider les le CSSP. Mais même si t'as pas validé le CSSP je pense il y a une certification, j'ai pas le nom.

13:17
Qu'on te donne si tu as l'examen et que t'as pas l'expérience. Et puis après quand tu vas avoir l'expérience tu vas compléter et l'associé AISC c'est ça. Puis tu peux accumuler d'expérience. Par contre tu peux faire maintenant un CCSP ou un SSDP si je me souviens bien là. Ouais puis puis même chez AISC il y a une certification de base de CI. Si si si. Ouais justement ils ont une grosse promotion.

13:45
Tu peux faire le le cours du CC puis l'examen à dans cette période ci c'est gratuit, c'est gratuit, c'est juste que faut que tu fasses ton déplacement, c'est 4 modules traits de base, puis tu peux déjà avec ça

ta porte d'entrée mettons pour être pour avoir accès aux ressources de la ISC et de penser à être associé à à ISC, puis après ça.

14:12
Prendre des années d'expérience autre chose aussi, ils prennent en considération certains les autres certifications comme par exemple le CEH. Le CEH, ça compte pour un an. Tu as fait un bac, ça compte pour niveau d'expérience. Là tu peux accumuler ton expérience, travailler avec ton expérience professionnelle dans les domaines du CBK.

14:32
Mais tu peux rajouter aussi des des des certifications qui te donnent des années d'expérience à une multitude de moyens pour accumuler ton 5 ans. Là exactement, c'est comme ça. Comme Émile l'a dit, c'est pareil pour le CSSP, le CICM, puis le 6 ans. 5 ans oui, mais c'est pas 5 ans. Exact que si tu as un bac, une maîtrise ça compte. Un certain point bien sûr dans le domaine hein.

15:01
Et puis comme il a dit là c'est ça il y a Ibrahim qui demande, est ce que avec le VPN peut-on le faire ? L'examen du CSP se fait jamais en ligne ? Les examens du Isaca oui même pendant la COVID on faisait pas ça en ligne. C'est c'est l'un des examens les plus sérieux je vous le dis, moi j'ai j'ai fait le CSSCSMCSSP c'est pas pareil, c'est même pas le même contrôle.

15:26
Oh Ah OK, tu parles du CCCCC ? Oui le CC je sais pas, mais je sais que le CSSP c'est pas le CC. Je sais c'est quand même nouveau, c'est nouveau entrée, je sais pas le CC, je sais pas où ça se fait, mais je sais que le CSSP ça se fait jamais en ligne. Si on le fait en ligne, nous on va se plaindre, c'est c'est tout chez prométrique, le CCCSSP puis tout ça c'est prométrique à l'extérieur du Québec.

15:53
OK Jonathan, vas y et puis on va terminer, on va accélérer puis terminer. Vas y oui je voulais juste mentionner un mot au début tu sais-je pensais ça prenait tu sais comme juste de l'expérience en cybersécurité, puis tu sais des fois on fait des je sais pas, tu sais des on peut être développeur, on peut être gestionnaire au niveau de l'infrastructure puis.

16:13
C'est ça en lisant les au niveau de du CSSP là il y a beaucoup d'expériences qui vont rentrer en ligne de compte. Puis même si t'as pas le titre cybersécurité sur ton CV mais tu sais on en fait directement tous souvent un peu là fait que c'est parce que c'est intéressant de regarder, parce que des fois comme le Développeur Ben ça compte aussi là-dedans ou donc c'est c'est c'est c'est. Je trouve que c'est vraiment bon de le voir là.

16:36
Y a y a plusieurs domaines, un peu ce qu'on est en train de voir ta tête tantôt, là c'est c'est vraiment l'infrastructure qu'on est en train de voir. On parle de micro services, on parle de différents types de serveurs, donc si tu travailles dans l'infrastructure, Ben tu es. Ça fait partie des domaines que on couvre le CSSP tu fais, tu es dans le développement, ça fait partie des domaines que couvre le CSSP, donc ça devrait te permettre de pouvoir avoir une validation des de certains domaines. Je pense que ils prennent 2 domaines dans lesquels tu travailles et puis en plus de ce qu'il a dit.

17:05

Tu peux aller chercher tes 3 ans, tes tes 5 ans facilement, mais c'était ça, on continue micro services sécuritaires en tenant compte de de gestion de la configuration d'une application de micro services. Donc on fait en sorte que les secrets, les clés EPI soient externalisées donc pas dans le code en dur, donc si vous voyez les clés EPI dans le code de vos développeurs, c'est pas bon. Demandez lui dans les villes.

17:34
Ensuite, avec le micro Services, Ben on va faire la découverte de services par une liste d'instances disponibles par les domaines de micro services, le des charges comme le lot balanci, on va avoir des passerelles API et des API Gateway pour les Façages proxy et sécurité. Donc les micro services seront responsables de la définition et de la mise en œuvre des politiques de sécurité.

18:00
On aura la journalisation centralisée pour des plutorts pour l'ensemble des services qu'on a. On va avoir des mesures centralisées pour évaluer la, la performance, la santé, la performance de nos systèmes. On va avoir le traçage disponible pour suivre le cheminement des messages, avoir la résilience et tolérance aux pannes pour contourner les pannes, mise à l'échelle automatique et auto réparation, puis déploiement progressif et progressive robuste de de nos services.

18:30
On a également la gestion des travaux déconnectés des demandes des utilisateurs, donc on a une architecture asynchrone. On veut que les les requêtes des utilisateurs en temps réel soient indépendantes des autres demandes. Ensuite on peut avoir les applications singletons centralisées, donc elles sont souvent appelées design par par thème. Donc on veut que une seule instance d'un objet existe dans toute l'application et existe globalement. Donc ça c'est un peu un exemple de.

18:58
De l'architecture qu'on peut qu'on va retrouver au niveau des micro services, les conteneurs, les conteneurs. On a très souvent des machines virtuelles et on a des conteneurs. Les machines virtuelles, comme vous le voyez, on a la machine hôte, la machine physique, on a les hyperviseurs, on a le système d'exploitation des librairies et les applications. Donc les conteneurs, c'est ça. Et au niveau des non, les machines virtuelles, c'est ça.

19:27
Et au niveau des conteneurs, comme vous le voyez, on a la machine haute, on a le système d'exploitation, on a un moteur de conteneur. Et puis on peut avoir des applications, soit des librairies partagées et par application. Donc il est par rapport à aux machines virtuelles qui sont souvent autonomes ou orientées administrateurs. Eux, ils sont beaucoup orientés développeurs, ils sont légers.

19:52
Donc si je prends le quart d'un d'un conteneur, si je veux admettons une machine, un serveur de base de données POSTGRE SQL, Ben je vais et que je veux rouler juste mon application spécifique. J'ai pas besoin des autres services. Ben je vais aller prendre un conteneur spécifique pour ça. Donc il va aller venir avec toutes les librairies possibles pour ne pas que j'ai à télécharger plusieurs librairies pour pouvoir faire mon travail. Donc ça va me faire gagner en temps. Je prends mon mon conteneur, je l'installe et puis je suis-je suis déjà prêt.

20:22
Donc thème d'architecture, Ben on a le le serveur de le. Parmi les conteneurs les plus utilisés, on a les

dockers. Donc pour avoir un service de dockers, des API qui pourront communiquer des dockers clés, on a le réseau qui peut interfacer d'autres conteneurs, des images et puis des volumes de données qu'on pourrait avoir. Ça c'est c'est l'exemple de l'architecture.

20:47
Donc ça c'est une image un peu qui structure au niveau des dockers qui étaient, puis au niveau des dockers. Donc on a les Dead Tools, des maquettes, plus des différents conteneurs qu'on peut avoir, des OS qui sont en dessous des différents systèmes qu'on peut avoir également. Donc on a du VEVA qui peuvent être sur des machines, des os. On peut avoir des OS de de conteneurs donc, et des différents conteneurs qu'on peut avoir au-dessus, on peut avoir des des applications.

21:17
Là-dessus. Donc ça c'est un peu une image qui montre l'architecture qu'on pourrait avoir au niveau de des conteneurs, des Serverless computing, donc des des des des 100 serveurs comme on le dit en français. Donc on a les l'infonuagique qui évite la planification, donc on veut souvent avoir des des applications sans se casser la tête avec tout ce qui est configuration gestion.

21:47
Maintenance, exploitation des conteneurs, des VM ou des serveurs physiques. Donc on veut que les OSLDOS soient pris en charge par le fournisseur parce que on veut pas. On veut se concentrer sur notre déploiement, on veut se concentrer sur l'application qu'on est en train de développer. La surface d'attente peut être plus grande qu'à plus de composants dans l'application et les solutions de sécurité qui sont souvent pas forcément utiles pour le client.

22:14
Mais ça reste quand même que ça a ses avantages. Le fait que j'ai pas à gérer tout ce qui est configuration mais Toujours est-il que il faut avoir le bon fournisseur qui est là derrière les systèmes embarqués. Donc on a les architectures logicielles qui sont souvent inconnues pour les systèmes embarqués. Donc ça peut être des terminaux, des régulateurs de vitesse adaptée. Tout ce qui est véhicule électrique autonome également qu'on a.

22:40
Donc on recommande toujours de d'isoler lorsque c'est possible des systèmes embarqués, des systèmes qu'on a de façon générale des des des systèmes de l'entreprise. On a les systèmes de calculs haute performance high performance computing, donc ils peuvent effectuer un très grand nombre de calculs complexes et voluminés à haute vitesse. Je signale que ça c'est différent de c'est différent de de l'informatique quantique, c'est pas la même chose ça, c'est vraiment des systèmes qui peuvent faire des hauts calculs.

23:11
Donc il peut faire plusieurs traitements en parallèle. Et puis il y a des processus spécialisés donc on l'utilise vraiment dans la météo, dans l'i a donc il utilise vraiment le flop comme mesure de mesure pour voir la puissance en fait du du calculateur. Ensuite à la question de une île, on a des systèmes informatiques de périphérie qu'on appelle des Edge. Donc comme je disais ça rentre généralement dans les réseaux traditionnels donc.

23:38
Ils vont faire des traitements au plus proche de la source, donc ils vont réduire la latence et réagir en temps réel. Donc tout ce qui est Edge c'est tout ce qui est ici les commutateurs des machines qui sont

vraiment proches. On fait en sorte que au lieu que on aille dessus du cloud ou faire des machines distants. Mais on veut avoir notre petit système à côté qui fait du cashing qui peut faire du brief ring pour pouvoir nous donner l'information rapidement pour réduire les temps de latence. Donc tout ça ça rentre un peu dans l'approche Edge.

24:09
Ou l'informatique de périphérie, système virtualisé donc comme des des machines virtuelles. Donc on a les mêmes machines, les mêmes machines physiques qu'on a montrées tantôt l'exemple avec les les conteneurs. Donc on peut virtualiser les systèmes d'exploitation, le réseau, le stockage serveur, le bureau de travail, les applications et autres. Donc pour les serveurs vous vous avez on a VMware et 6.

24:39
Le stockage, on a des San Visualisés pour le réseau, on a des SDN qu'on peut avoir pour tout ce qui est système d'implantation. Ben on a les les V Linux sur du Windows, on a tous les bureaux, on a les VDI de de Citlx et puis les applications, et on a, on a tout ce qui est conteneurs, les dockers et autres qu'on peut avoir aussi.

25:02
Les préoccupations c'est les mêmes, un peu les mêmes préoccupations que les systèmes physiques hein. Puis en ajoutant la syphèse d'attaque des machines virtuelles, donc on a des enjeux de mise à jour, configuration et puis durcissement sur ces machines virtuelles. Là on a d'autres concepts qu'on a toujours qu'on appelle canal caché ou Cover Channel. Donc lui il va associer au flux de l'information communication. Il va s'associer au flux d'informations quand on fait la communication.

25:32
Donc il va. Il est causé par de mauvaises implémentations de contrôle d'accès ou de partage de ressources. Donc il y en a 2 types, le canal caché de stockage, donc covert Story Channel qui est écrit, du moins j'ai perdu la lumière, donc qui est écrit à un endroit inusité sur le X ou en mémoire.

25:58
Ensuite on a le canal caché par le timing Cover Time Channel qui est inséré dans les dans les silences de communication. Donc des fois quand on fait des communications, il peut avoir un délai pour envoyer des des messages. Et là ce type de de de d'informations peut s'insérer Parmi ces ces silences là, on a tout type de.

26:24
De d'attaques qu'on pourrait avoir le top two qu'on appelle time objet time to use donc c'est l'attaque de séquence d'actions causant une condition de concurrence, donc race condition. Donc il peut se produire, il peut se produire partage d'objets en plus il peut pendant le partage d'objets entre plusieurs processus. Donc comment ça se fait ? C'est que l'objet est modifié entre le moment où il est vérifié où on le check et celui où il est utilisé. Donc.

26:53
On a vérifié un objet, on s'est dit qu'il était bon et avant qu'on vient l'utiliser, on se rend compte que il a été, il a été modifié. Donc les contre-mesures, Ben on va mettre les verrous de logiciels ou de processus pour prévenir les top to.

27:16
On a des bacs d'or, donc des portes dissimulées, donc des bacs d'or. Qu'est ce qui arrive ? C'est que

des fois des développeurs eux-mêmes, quand ils sont en train de de développer des systèmes où ils sont en train de de de soit des faits de certaines corrections, ils peuvent mettre des bacs d'or qui eux leur permettent d'entrer dans le système et contourner toutes les mesures qui sont là. Mais le problème c'est que à la fin, ils oublient.

27:45
Que eux-mêmes ils ont mis des bacs d'or. Et puis ça va devenir des vulnérabilités dans le système. Donc les contre-mesures, c'est faire la revue de compte l'assurance qualité, mettre en place des systèmes, des HIDS, faire le chiffrement des fichiers sur les disques, audits d'accès aux fichiers, disques pour prévenir les bacs d'or, principe de sécurité des sites et installation.

28:20
Principe de sécurité, installation. Donc l'idée c'est de protéger contre les désastres naturels qui sont causés par les humains, qui sont causés par les humains ou par d'autres aspects comme les, les pannes et autres. excusez-moi donc pour les désastres naturels.

28:45
En fait les les menaces on en a de plusieurs donc c'est pas juste les les attaquants naturels qu'on connaît. Donc on a des désastres naturels qui sont peuvent être des fumées, des feux, des inondations, des tremblements de terre, des éruptions volcaniques, des tempêtes, des tornades et des ouragans. Donc je pense il y a 2 ans il y avait des un ouragan qui avait dévasté des installations de de etième aux États-Unis, l'entreprise de Télécope. Donc ça ça.

29:14
Leur avait amené à, je pense à revoir certains plans en interne d'abord, on a aussi des menaces humaines, donc là c'est généralement ce qu'on Crète. Nous c'est vraiment en cybersécurité. On s'est dit bon, quelqu'un de façon intentionnelle ou accidentelle va nous attaquer, donc ça peut être des erreurs, ça peut être je sais pas intentionnel ou ça peut être intentionnel. Sabotage, vandalises, explosions, émanations toxiques, vol, greffe.

29:44
Qui peut dévaster d'autres sites où nous poser des des soucis où on peut avoir des pannes techniques, électricité, climatisation, alimentation en eau, gaz vapeur, équipements, serveurs, hauteur des fois pour attaquer une organisation. Souvent si on a accès à leur système de h VAC. Si on veut faire du mal à une organisation, on connaît leur centre de données. On peut avoir accès alors leur système de h VAC.

30:12
Et dans la salle, c'est vrai, il faut juste mettre la chaleur au lieu de mettre la climatisation tu vas bousiller l'ensemble de leur serveur. Donc c'est une façon d'attaquer ou un autre exemple si je vais attaquer un État, une ville, mais je fais en sorte de prendre le système de distribution d'eau et c'est juste dès que tu augmentes le bah le le nombre de la quantité de chlore et tu vas faire beaucoup de dégâts.

30:38
Donc ils sont autant d'éléments qu'on peut utiliser pour faire des attaques sans être forcément passer par des rançon way. Donc il y a plusieurs façons, soit de faire du mal à une organisation ou à un État. Mais bon, très souvent les les attaquants ils sont quand même éthiques à certains égards, ils refusent,

ils attaquent pas souvent les hôpitaux quoi que. Donc souvent il y a des ils sont attaqués, mais quand ils font des ransomware, ils sont prêts à donner l'appli des fois.

31:07
Ça reste que on est encore humain là-dedans. Mais bon des fois ils retrouvent pas la clé. Donc la l'idée c'est de faire en sorte de ne pas se faire attaquer ou de ne pas de se protéger tout le temps pour ne pas qu'on vous attaque ou quand on vous attaque, vous êtes capable de de vous relever ou vous protéger. On continue.

31:31
Donc on retient que je l'avais dit la semaine dernière, l'employé est ce qui est le plus important et passe avant tout toutes les mesures. Ça c'est en cybersécurité, mais dans d'autres aspects, c'est pas forcément le cas. Des fois on bombarde des la population, tout ça dans dans dans certains domaines. Mais en cybersécurité, quand il y a un désastre, nous on pense aux humains d'abord, on évacue les employés avant de penser au système.

32:01
Accès physique, donc toujours on vient dans l'accès physique, on toujours ce sont des éléments qui vont nous permettre de de nous protéger. Tantôt on a parlé des différences, des sages tout ça. Donc on va parler de qu'est ce qu'on fait maintenant, qu'est ce qu'on fait maintenant pour se protéger ? Donc pour l'accès physique, Ben on va mettre en place la défense en profondeur, la défense en profondeur, c'est pas juste numérique mais même physique on va mettre la défense en profondeur.

32:30
Donc ce qui est périmètre externe, on va mettre les coutures, l'éclairage, les barrières, caméras extérieures, périmètre intermédiaire, on va mettre les contrôles des véhicules gardiens, les SAS d'entrée qu'on appelle généralement des mandrappes, les zones internes, les bases de biométrie, gardiennage 24 7 zones critiques, authentification renforcée d'autres facteurs et autres.

32:54
Pour le choix du site, au centre de données, au Bureau, Ben on va s'assurer qu'on est dans un endroit qui est visible. Voilà, on va pas aller chez cacher dans une forêt où c'est compliqué qu'on on ait accès ou que la logistique n'est ne sera ne sera pas aisée. Donc on va regarder le trafic est sol haut, on va regarder la criminalité. C'est clair que on va pas aller mettre notre centre de données dans un endroit où la criminalité est élevée.

33:20
On va chercher, est ce que on a de la stabilité ? On va regarder la configuration du terrain, est ce que c'est une zone inondable, sismique, une zone industrielle ou chimique ? Donc on va regarder tous ces aspects-là avant de de choisir en fait notre notre site. Ensuite côté contrôle d'accès donc on va regarder le secteur, les véhicules, les personnels, les visiteurs, les clôtures, l'éclairage et les différents détecteurs qu'on a.

33:47
Infrastructures, on va avoir la climatisation, de l'alimentation, l'eau, électricité, gaz et puis les pompiers qui sont pas très loin. Donc ce sont les éléments qui vont rentrer en ligne de compte dans le choix de notre site. Et donc pour faire la sécurité aussi il faut trouver des faut te mettre dans des conditions favorables aussi il faut aller te mettre en danger soi-même. Donc faut minimalement être dans un environnement qui te permet de pratiquer ta sécurité.

34:20
On continue donc on va mettre les contrôles en place. Mais les contrôles vont prendre en compte 4 modèles, toujours dans la stratégie de la sécurité physique. Donc on aura ces 4 modèles là qu'on a lediteur, le dîner, le deeptech et le dealay. Donc l'éditeur c'est quoi ? C'est décourager. Donc on veut faire en sorte.

34:40
De mettre en place des contrôles pour décourager la personne qui veut faire du sabotage ou qui veut nous attaquer. Donc c'est des clôtures, des barrières, des gardes, des avertissements, des barbelés. On va faire en sorte que ça puisse se décourager, toujours dans notre logique de défense en profondeur. Si l'éditeur ne marche pas, on va faire le deny, donc on va faire en sorte qu'on on le refuse systématiquement. Donc une voûte, une pose, une porte ou un torniquet.

35:08
Ça, ça ne fonctionne pas. On va faire le détect, on va s'assurer que on est capable de détecter les mouvements, les fumées quand on a une salle serveur, les CCTV closed circuit télévision pour s'assurer que on a, on est capable de détecter des mouvements, détecter des passages, enregistrer des vidéos et ensuite ça, ça marche pas. On va retarder, on a des verrous, on a des câbles là-dessus, donc ce sont les éléments qu'on utilise pour.

35:36
La sécurité physique, des stratégies qu'on utilise pour la sécurité physique. On continue ensuite pour dans le détail des des des différentes les 4 stratégies qu'on a l'éditeur qui est le décourager. Ben les barrières peuvent être naturelles, donc rivières, forêts, falaises pour fabriquer des murs, clôtures et puis des portes.

36:02
Et dans notre contexte de sécurité, là bon moi je je n'encroche pas quelqu'un d'aller s'installer en forêt clôture pour la faut avoir des clôtures que efficace à plus de 6 pieds donc 1m80 ou avoir des guides des nuits extérieurs efficace à plus de 7 pieds dont 2m10 pour le dinail refusé. Donc on va juste prendre des personnes autorisées donc on va utiliser comme vous le voyez ces cartes là.

36:32
Les cartes bandes magnétiques donc qui est sensible à l'effacement et clonage et et qui est sensible à l'effacement. Il est clonable, il est clonable le NFC newer fired communication donc lui la sécurité est toute tourne autour de la le numéro de série. Si on arrive à récupérer le numéro de service, Ben en effet le numéro de série on est fait la carte intelligence Smartcart Ben lui elle elle a une puce cryptographique qui est intégrée.

37:01
Où on peut utiliser le PIN donc il faut se rappeler du code où on a la biométrie, on va regarder l'empreinte virus, la reconnaissance faciale. Donc ça c'est un exemple un peu de comment est ce qu'on peut assurer la sécurité ? Peut être la la dame elle est à l'intérieur, elle a sa sa carte, elle va peut être utiliser son finger, utiliser le son, le finger point pour rentrer et ça c'est le mantripe, le mantrap.

37:35
Play display 2 est là, donc tant que LL est là, lui il ne pourra pas, il ne pourra pas rentrer. Et on a des équipements tels qu'ils sont là pour des censeurs de personnes qui peuvent compter le nombre de

personnes qui sont là. Donc ce sont autant d'outils qu'on peut avoir pour assurer la sécurité que si c'est dans la zone où on peut avoir une seule personne, Ben on pourra avoir des capteurs qui sont capables de nous dire le nombre de personnes qu'on a. Puis on a une seule personne à la fois, donc dépendamment de la criticité ou de.

38:05
La sensibilité de l'environnement. Mais il y a des mesures adéquates qui aussi ont leur coût hein, qu'on peut mettre dans notre environnement pour la sécurité physique. Pour le détecte, on a le le détecter, donc on peut avoir des capteurs infrarouges, donc on a les variations de température, des capteurs à micro-ondes, des réflexions de corps, des mesures de distance.

38:30
On a des câbles finalement électromagnétiques, donc pour les coupures ou vibrations, donc peut faire des surveillances de clôture et puis des quand il y a des passages sensibles, on a des capteurs acoustiques pour le son, donc quand il y a des briques de des briques de vitre ou de verre on pourrait détecter ça. On a la reconnaissance d'image, donc reconnaissance d'humain ou de mouvements. Donc avec ça on pourra on doit pouvoir déclencher l'alarme.

39:00
Ensuite on a le dealer qui est le retardé donc on a des cadres de sécurité. Donc on a présence humaine qui sont efficaces pour décourager et faciliter certaines validations telles que les cartes d'identité, les feux, les alarmes, les situations d'urgence. On a des contrôles efficaces des visiteurs donc on va tenir un registre de visiteurs, s'assurer que tous les visiteurs qui rentrent, on sait qui rentre. On est capable pour un audit, voir qui sont ceux qui sont rentrés.

39:27
Qu'est ce qu'ils ont fait tout ça ? Puis ça peut nous permettre de nous améliorer en cas d'incident. Donc tout ça, ça peut nous permettre de d'avoir un suivi et puis améliorer notre posture de sécurité totalement. Après les 4 Stratégies, Ben on a des éléments qu'on peut toujours avoir pour notre sécurité. Donc ça c'est un cabinet de de câblage qu'on appelle le Warren Proset.

39:55
Donc faut pas avoir des éléments en fait de mettre les les éléments en vrac, faut vraiment les organiser. Donc faut ensuite gérer les accès. Donc les bio, les cartes magnétiques, les CCTCCTV. Donc faut pas avoir des du matériel inflammable.

40:16
Donc faut avoir des contrôles, un contrôle dans faut faire un contrôle d'accès et enregistrement. Puis souvent ça on l'oublie dans les plans de continuité qu'on dont on avait parlé dans précédent cours. Ensuite, pour toujours notre sécurité. Ben on a les différentes installations qu'on a. Faut aussi faire attention à ça. On a les installations de stockage, multimédia et stockage des crues, donc surveillées par caméra.

40:45
On va s'assurer qu'ils soient protégés contre les vols, donc confort à moi avec COU pour la sécurité des zones restreintes de travail et de travail. Donc on va mettre les les caméras de surveillance et puis on va adopter le principe de bureau prof ou clean dex par ici. Donc ça consiste à ne pas avoir des informations sensibles, visibles ou oubliées sur le Bureau ou rendre visibles à à ceux qui ne devraient pas avoir. C'est ça le principe de bureau propre.

41:15
Ensuite, on a les services publics, les hvags, donc il faut protéger également, comme je vais donner l'exemple, tout ce qui est hvags. Ben si on a accès à votre hvags au niveau de votre data Center sans avoir accès, on peut faire du sabotage juste en augmentant la température. Mais on a aussi des problèmes environnementaux dont il faut prendre, dont il faut tenir compte.

41:42
On a des inondations qui sont des des flaudes, donc il faut avoir des pompes, des détecteurs d'humidité reliés au système d'alarme. Donc dès que on a un peu d'humidité, on doit pouvoir détecter pour qu'on puisse voir la cause. On a les interférences qu'on appelle électro électromagnétiques, interférences. Donc on peut filtrer les lignes d'alimentation électrique parce que souvent on peut avoir des perturbations électriques qui peuvent affecter des équipements sensibles. On a des interférences, RFRFRFI, Radiofréquency, interférences.

42:13
Des cages de faraday qui peuvent bloquer les les champs, les champs magnétiques. On a l'électricité statique donc peut être causée par l'humidité, donc il faut-il faut avoir l'humidité à l'électrique statique, c'est pas forcément causé par l'humidité mais l'humidité. Les tapis d'ignoration, les bracelets de fichage nous permettent un peu de de contrer en fait l'électricité statique ou.

42:41
De pas faire en sorte qu'ils causent des torts, du tort pour nos salles de serveurs ou centres de données. Ben il faut héberger des des des quelques recommandations pour héberger des systèmes par des êtres humains dans les data centers, c'est pas fait. Pour que les hommes y vivent des centres de l'édifice, il faut toujours mettre la centre de données dans le centre de l'édifice, non ? Adossé à un mur extérieur donc.

43:11
Parce que si c'est une autre entreprise, on est, on est contigué à une autre entreprise vers on pourrait rentrer dans notre salle serveur sans qu'on le sache. On a notre système Alpha, ça on en a parlé. Système de prévention d'incendie gaz. O faut avoir de la luminosité dirigée les cages de faraday, comme ce sont des cages pour nous protéger contre les champs magnétiques, des planchers surélevés, avoir des onduleurs, des IPS et des générateurs.

43:40
Bon je continue, est ce qu'il y a la question ? Oui c'est juste au niveau de la cage faraday, pourquoi vraiment besoin dans une salle de serveur ? Ça je j'ai pas vraiment compris. Là si on parle par exemple de trop statique c'est des tapis pour le bracelet on pourra faire ça mais une cage faraday c'est en en général pour. Par exemple je sais qu'on y voit des cages faraday ou des sacs faraday.

44:10
C'est au niveau de la police. Eux ils utilisent ces ces choses là pour mettre par exemple un un cellulaire qui est en cours d'exécution pour éviter que ce soit effacé à distance, on le met dans un sac ou cache farad pour faire des tests ou afin d'éviter que ce soit formaté à distance ou quelque chose comme ça mais la cache farady pour dans l'autre cas je sais pas, je pose la tu tu tu cherches le le cas d'utilisation, pourquoi est ce qu'on utilise le cage farady ? Mais pour moi en tout cas ça fait partie des éléments pour.

44:40
Les problèmes environnementaux excusez-moi, je voulais les problèmes environnementaux ici donc si peut être dans notre salle serveur on a affaire à certaines interférences donc ça pourrait être utile. Peut être je sais pas quel type d'appareil on a. J'ai pas encore vu un telle une telle expérience réelle mais je pense ça fait partie des recommandations, c'est que c'est utilisé à certains endroits mais on pourra faire quelques peut être des recherches pour voir dans quel contexte il est utilisé dans.

45:09
Dans un sens de donner, mais j'ai pas un exemple palpable pour toi et parce que mais tu tu tu tu pourras checker et puis nous revenir. En tout cas au niveau de la police, je sais qu'ils ont-ils ont des caches à rader par exemple, qui ont des verres à part à l'extérieur pour éviter tout de suite, et cetera pour. Alors ils peuvent utiliser cette cache valader pour ouvrir un ordinateur, voir ce que t'es à l'intérieur, sans, sans, sans l'arrêter, puis faire leurs enquêtes, et cetera.

45:36
Pour pour un serveur je sais pas, OK j'ai pas vu, j'ai pas vu, c'est ça ce que me je vois pas le moi de mon côté de mon côté hein, je je vois pas l'utilité de mettre une salle de serveur dans une cage tu non non tu vois pas l'utilité, tu vois pas l'utilité d'avoir une cage de faraday, j'ai pas OK c'est le bon mot mais c'est ça je vois pas l'utilité comme.

46:01
OK je peux est ce que je peux intervenir là dessus ? Oui oui vas y vas y sur mon merveilleux téléphone j'ai fait une petite recherche d'autres cache faire AD sans le serveur. D'ailleurs le premier choix c'est bunkerkit donc c'est une cache faire AD pour la protection des attaques électromagnétiques. Donc justement cette compagnie là.

46:22
Off des une protection de data Center à cause des des protections électromagnétiques, puis t'en as t'en t'en as 4 une là. Donc c'est c'est surtout pour la protection contre les GMC là OK, merci Émile. Et puis il y a, il y a Marielle qui disait que les talkie walkie ont des interférences avec des équipements bio, biomédicales par exemple.

46:50
C'est ça. Mais bon on pourrait avec l'exemple d'Émile et puis Marie on pourrait faire d'autres recherches et puis dire dans quel contexte ils utilisent. Mais oui si c'est pas important on l'utilise pas. Mais si ça si on a besoin c'est ça fait partie des options, c'est bon. Merci pour ta ta question, on a la phase oui.

47:18
Ça veut dire quoi luminosité dirigée en fait ? LL luminosité dirigée en fait si quelqu'un vient dans la salle, tu vois par exemple souvent les les scènes quand on fait les concerts on dirige la luminosité vers l'acteur ou le chanteur. Un truc comme ça c'est c'est c'est un peu ça parce que par rapport au mouvement on va la luminosité peut être pourrait suivre pour voir la personne qui est là en fait.

47:47
OK, c'est pas un média de sécurité ou ça c'est mais ça fait quoi exactement dans dans le mais quand on quand on quand on fait la bon, OK admettons, OK ça fait quoi, mais en fait faut pas voir la salle de

serveur. Une petite truc hein, je parle de centre de données salle serveur, faut pas voir salle de serveur, juste 10 m². Non voilà, il faut voir les centres de données qui qui sont vraiment gigantesques, là OK.

48:15
Ouais sinon si si c'est une salle serveur. Oui, on peut se poser des questions, on fait quoi avec calfaday ? Ou bien ? Mais on parle vraiment de centre de serveur qui peut être à plusieurs pieds carrés, plusieurs superficies. O KOK classification des centres de données. Donc pour les dates à 05h00, on va les classifier à plusieurs niveaux, donc le tiers un.

48:43
C'est des infrastructures de base donc on a la capacité basique, on a des IPS, des classifications de de génératrices, donc c'est vraiment basique. Climatisation génératrice qu'on a le TS 2, on a une redondance partielle donc c'est le TS un plus la redondance. Donc on a des génératrices UPS, climatisation, pompes, donc on en a doublé sur les les différents systèmes.

49:08
Le tiers 3 c'est la maintenance sans interruption donc c'est nos tiers 2 plus entretien sans panne de l'alimentation électrique et climatisation et on a le tiers 4 qui est la tolérance. J'ai j'ai un E que j'ai oublié la tolérance aux pannes. Tiers 3 tolérance aux c'est tiers 3 plus tolérance aux pannes. Donc lui il est vraiment utilisé pour des environnements qui sont beaucoup plus critiques.

49:38
Un instant ok, parfait. On continue, ça va ? Est ce qu'on a des questions ou c'est bon ? Ok ?

50:04
Éclairage avec des minuteurs, détecteurs de mouvements contrôlés à distance, toujours allumés ou au besoin, éclairage d'urgence fluorescent économique, tout ce qui est économique, efficace, sauf à l'extérieur. Donc on a des mercules qui sont qui ont des durées de vie étendues faute luminosité, on a les textines qui sont des poils lumineux, on a des diodes électroluminescence, des lettres donc qui sont économiques, compactes et lumineux. Donc ce sont les en termes d'éclairage qu'on a.

50:33
Le claused circuit, on a la surveillance à à circuit fermé, on a l'évaluation rapide de la menace après détection, on a les moyens de découragement, on conserve les traces d'événements. Donc ici c'est des on appelle ça des PTZ donc panoramiques donc que ils peuvent faire des mouvements en haut, ils peuvent faire des mouvements verticaux.

50:57
Comme il peut faire des mouvements horizontaux donc les les types inclinés où il peut zoomer, rapprocher l'optique où numérique. C'est pourquoi on appelle le PTZ. On a des IDS physiques aussi qu'on peut avoir donc peuvent détecter les intrusions physiques donc des des gardes de sécurité, des détecteurs de mouvements, déplacements de masse. On a des caméras sensibles aux mouvements donc qui peut combiner vidéo plus, analyse du changement de de pixels.

51:26
On a des capteurs acoustiques, les sons qui sont en normaux, on a des bris de verre ou vitres, fréquences sonores du verre brisé, on a des capteurs de poids donc changement de charge. On a des capteurs de vibration également, les triangles de feu, le triangle de feu. Donc on on a plusieurs types de feux qu'on peut avoir, donc on va associer ça au comment est ce qu'on peut contrôler ces feux là ?

51:54
Donc l'eau peut contrôler les feux qui sont gérés par la chaleur, donc l'énergie. Donc genre en soi on a un point inflammable, donc avec l'eau on peut contrôler ça. Les poudres peuvent pour les combustibles, donc papier, bois, plastique, carburant. Donc eux il faut pas mettre de l'eau parce que tu vas juste faire que augmenter. Donc ici ça ça sera en appel, des combustibles ça sera des des fioles, ici des poudres.

52:24
Donc qui peuvent aussi créer aussi des des réactions chimiques quand même des pots de oui on les utilise, mais on peut créer des réactions chimiques, on a des halons, des sauts, des acides, des CO 2 qui sont des utilisés pour des comburants, donc le feu qui est créé par les objets, l'oxygène qui alimente la la réaction. Donc on va tout de suite voir la classification. Puis on a les extracteurs en mousse aussi qui sont utilisés tant pour les comburants et la chaleur, donc pour tout ce qui est est créé.

52:55
Par l'énergie, le ITC et le le tout ce qui est oxygène, le CO 2 ici, donc souvent les extincteurs en mousse peuvent intervenir. Dans ça, je vais vous montrer tantôt la classification, mais avant, voici les 4 étapes d'un incendie, donc quand l'incendie commence, on a le stage un, le niveau un, donc démarrage au départ il y a pas de fumée, donc on a l'accumulation de chaleur. Incendie est en incubation.

53:23
2 on a la fumée qui est visible et puis 3 on a les flammes visibles à l'œil nu et puis 4 on a les chaleurs intenses et proparations de l'incendie ici. Donc avec le temps la température monte. Et puis on tantôt on avait montré les différents éléments qu'on contrôle, donc voici comment ils sont classifiés. Donc aux États-Unis, on AABCD.

53:47
Donc les types de combustibles au niveau a le combustible solide, bois, papier, donc ce sont les les méthodes de contrôle, c'est l'eau, le soda acide, liquide ou en poudre pour les types de combustibles liquides, essence, gras, huile. Donc on a le CO 2, on a le FM 200, donc c'est de type B On a pour le type de combustible classe C électrique, donc on a le toujours le CO 2, le FM 200.

54:14
On a le type de métal, lithium, magnésium, potassium. Donc c'est le poudre qui peut gérer ça comme méthode de contrôle. On continue. Chaque organisation doit avoir un plan d'évacuation d'urgence du personnel. Donc si vous partez dans votre organisation, vous allez voir votre plan d'évacuation. Vous allez voir les endroits où vous devez vous rassembler. Généralement, il y a un plan qui dit où se trouve le point de sortie dans chaque immeuble.

54:45
Le personnel doit être informé des moyens de surveillance, des surveillances mises en place, donc on on doit dire aux aux employés quelles sont les mesures de surveillance, puis la loi 25 nous oblige. De plus, l'organisation doit s'assurer que les informations personnelles de ses employés, prises par le biais des moyens de surveillance ou non, sont adéquatement protégés. J'ai entendu une histoire comme quoi il y a, il y avait.

55:10
Au niveau de d'une entreprise qui faisait la surveillance et puis l'affaire allait en cours et après on disait que c'était on avait. Il n'avait pas pris le consentement des employés, donc ils devaient enlever le le système qui qui faisait la surveillance. Donc si vous faites une surveillance, que les employés sont pas au courant, mais ils peuvent porter plainte et puis bon, vous allez enlever votre surveillance, bien que ça fasse la sécurité.

55:35
Ça peut passer, donc faut toujours prendre. Faut que les gens soient informés, que y a des caméras de surveillance, que ça crée, ça prend leurs images, leur vidéo. Et puis bon, ils doivent être au courant alimentation électrique, donc il faut avoir de la redondance. Donc plusieurs fournisseurs d'entrées des panneaux électriques et alimentation. Parce que si on ne fait pas la redondance, Ben on pourrait avoir le système qui peut être défaillant.

56:05
Où on peut avoir à un moment donné la fourniture d'électricité normale de hydro qui peut ne pas fonctionner. L'alimentation doit être continue. Donc oui on a la redondance, mais en même temps on a d'autres outils comme les IPS qu'on peut mettre les démarrages. Le démarrage doit être instantané donc, mais opération de courte durée. Donc vous savez les générateurs IPS c'est pas pour durée.

56:31
Il peut filtrer l'alimentation sous tension donc avec les surtensions. Donc ça c'est pas juste pour l'entreprise, même à la maison. C'est important d'avoir ces UPSA pour protéger nos appareils donc on peut avoir aussi des des générateurs, des génératrices. Donc le démarrage peut être lent. Opération de longue durée donc besoin de carburant et d'essence gaz pour l'alimentation électrique.

56:57
C'est bon donc pour approfondir, voici pour regarder les principes principes for Security modals, design and capabilities du livre des CSSP Security Security, venerability Trade and contremagers physical Security recrement. C'était tout pour aujourd'hui. Est ce que vous avez des questions, des plaintes et autres ?

57:26
Une petite question du Ah oui vas y oui par rapport aux salles de serveurs là c'est sûr qu'au niveau de sécurité faut privilégier la vie humaine et d'une salle de saveurs qui prend en feu ou contrôlant un feu d'une salle de serveurs, quel des systèmes pourrais tu recommander ?

57:52
À utiliser pour éteindre les feux d'une salle de serveur tout en prenant en compte la vie humaine. Je sais pas si j'avais vu, j'avais mis dedans. OK Ben moi, pour le système que je recommanderais, ça va généralement ça, c'est c'est ce qu'on dit de façon générale, qui ce qu'on fait.

58:24
Mais dans le salle de non, les questions des des questions de CSSP, c'est pas comme ça. Pour les salles de serveur je dirais très souvent, on a des systèmes qui intègrent souvent ces méthodes de contrôle là et qui peuvent s'activer automatiquement dépendamment du type de feu. Donc je peux pas recommander un type de de protection, mais je sais que il y a des systèmes peut être qui peuvent déclencher de l'eau.

58:51
Dès qu'ils détectent le type de feu ou qu'ils peuvent avoir des gaz automatiques qui peuvent mettre des des cas des des CO 2 directement sans peut être intervention humaine. Donc très souvent c'est des c'est des éléments comme ça qu'on a dans les salles de serveur des des des data Center pour la protection. Oui penta panda. Je savais pas que tu étais là hein.

59:21
Et ça va bien, ça va, je vais bien. Et toi ? Merci oui ça va mais Monsieur pour la plupart du temps, pour la plupart du temps on dit que le CO 2 est nocif pour l'homme, donc du coup ça peut se déclencher par INFO passe par une par INFO Alerte et tout. Et les gens qui sont à l'instant ne seront pas que le euh censés déclencher.

59:44
Et ils pourront le respirer. Donc la plupart du temps on demande d'après les dernières recommandations que j'ai lu, ils recommandent d'utiliser le les poudres donc c'est ouais donc c'est c'est plus c'est plus digeste pour l'homme que que le cerveau. Oui OKOK peut être que je sais pas si les méthodes de classification ont été mis à jour. En tout cas récemment quand j'ai regardé le dernier document, là j'ai pas vu de mise à jour-là dessus.

1:00:11
Mais je vais regarder si CSSPA mis ça un jour, je vais, je vais vous faire, je vais vous tenir au courant. Oui j'ai fait rien. Oui je vais récidiver sur cette question parce que je ne sais plus trop si c'était lors d'un crise ou d'un examen que j'avais vu passer. C'est d'un point de vue du du CSSSP, on sait que c'est l'homme qu'il faut privilégier, mais quand il s'agit des accès sensibles où on a.

1:00:38
Juste milieu à faire entre l'homme et la donnée sensible. Comment faire ? Quelle est la la juste mesure à avoir ? Parce que je pense que c'était comme la porte se fermait parce que il fallait.

1:00:52
Prioriser la donnée ? Mais là on perdait la personne parce que il y a il y avait plus d'oxygène dans dans la bâtisse ou qu'il y avait un feu ou encore il fallait laisser la porte ouverte, c'est à dire quand il y a un déclenchement d'incendie, la porte s'ouvrait quand même pour laisser passer l'être humain. Mais en ce moment-là c'est une comme on va dire une faille ou bien une ouverture. Alors c'est quoi la posture du CISS speed ? En sachant que c'est toujours l'homme la priorité, c'est l'homme la priorité.

1:01:21
Maintenant si tu parles du CSSP, c'est l'homme, la pureté. Maintenant dans la pratique, vas y vas y c'était. Si j'avais eu cette question là, j'aurais répondu l'homme, parce que j'aurais balbutié quand même, j'aurais j'aurais pris la non, mais ne ne ne ne balbutie pas, c'est l'homme, la pureté. Maintenant, qu'est ce qui va ça, qu'est ce qui va arriver en en dans la pratique, dans la pratique ?

1:01:47
C'est que si c'est une donnée sensible, il y a il y a 1111 bras dans le film Là qui va vouloir aller sauver la donnée ? Peut être qu'on va pas contrôler mais qui va ressortir peut être héros s'il arrive à sauver la donnée. Mais pour ceux qui sont responsables de l'évacuation des personnes, c'est les personnes d'abord qu'il faut sauver, C'est pourquoi c'est les personnes qu'il faut sauver. Mais c'est sûr que dans le lot il y a un qui va aller chercher chercher à sauver des des informations sensibles. Mais anyway.

1:02:17
On va pas les les informations sensibles, si vous avez bien fait votre plan, tout ce qui est restauration, sauvegardes et autres. C'est pas parce que la data Center prend feu que vous allez mettre la vie de quelqu'un en danger. C'est censé être répliqué ailleurs et puis on vous demande de répliquer à 3 endroits souvent différents. Voilà. Donc on va pas aller courir pour dire je vais aller prendre tel discours, je vais aller prendre tel code secret. C'est c'est censé être ailleurs en fait. Donc on sauve les vies humaines d'abord.

1:02:46
Et puis c'est ça en tout cas CSSP, là il y a il y a des il y a un masseur dans lequel tu te mets, un masseur de manager, un menseur de quelqu'un qui sauve la vie, et puis c'est comme ça tu réponds, mais en réalité dans la vraie vie c'est c'est ce qu'on fait maintenant, je parle pas dans le cas de quand on est en guerre hein. Non ça je ne maîtrise pas, j'ai jamais fait, j'ai jamais été militaire, mais je parle en termes de sécurité, c'est la vie humaine. Parfait Nasser.

1:03:12
T'as répondu déjà à la question ? Parce que moi aussi je dirais plus la vie humaine. Et puis on va c'est à dire éteindre le feu avec les moyens sans sans atteinte à la vie humaine. Parce que on a déjà des backup ailleurs, là on va pas avoir un data Center sans avoir un backup, on va pas les mettre tous dans le même bas comme on dit. Là ils vont être ailleurs à que la place où on a d'autres data Center parce que l'autre il va être dans une autre zone géographique éloignée.

1:03:39
Alors le risque, que ce soit sur les 2 ou 3, c'est un petit peu minimisé et en général aussi, physiquement on fait des des cloisonnements entre les salles. Alors si ça prend dans la salle une, ça prend pas dans la salle 2 en général, c'est c'est un petit peu ça que je voulais dire. Merci. Il y a esaïe qui dit, il y a quelqu'un qui a qui pourrait toujours aller récupérer les backup, ou bien piresable, mais les backup, c'est pas forcément physique hein.

1:04:07
Les backout ça peut être dans le cloud et puis on conseille de ne pas de mettre dans ces 3 supports différents. Donc si tu as gardé tes blackout dans des titres dans un endroit, c'est vous n'avez pas fait votre un bon plan de de dire donc c'est pas c'est c'est pas dans un endroit, c'est aussi c'est c'est pas forcément physique, c'est souvent dans le cloud aussi tout ça.

1:04:32
Et ça peut être des données top secrets où on peut pas les répliquer à ce moment-là il y a que la la personne qui A la clé secrète qui a accès. Non c'est pas une seule personne qui A la clé secrète aussi. Et si la personne meurt on prend. Non, on prend toujours en compte aussi que on est, on a un cycle de vie, on peut partir du jour au lendemain donc non on va pas, on va pas faire en sorte que une seule personne elle.

1:04:58
La clé secrète il y a il y a aussi une autre personne, souvent c'est 2 personnes mais dans dans dans dans dans dans certains cas c'est pas juste 2 personnes qui ont juste la clé. On peut donner la moitié des clés à des personnes, la moitié de part et d'autre pour que on puisse constituer la clé mais on va pas donner à une personne seule c'est bon en réalité la la la vie humaine au-delà de tout hein, elle est plus précieuse que tout.

1:05:28
Donc on va pas, on va pas, peu importe les types de données hein, on va pas privilégier les les données aux hommes donc les données sont censées être répliquées ailleurs. On peut récupérer. Puis bon si on n'a pas la donnée c'est pas la fin du monde, c'est bon vous allez avoir 4 Min s'il y a pas de questions. Merci à vous et bonne soirée bye.

1:05:56
Merci, bonne soirée, bonne soirée, merci bye à demain. Bonne soirée. Allez, bonne soirée.

INF813-Séance-11-Module-4a

0:01
On va voir le module 4A, ce qui est la première partie du module 4 la semaine. La séance prochaine on va voir le module 4B. La suite en fait du cours parce que ça allait nous faire trop de slides, puis bon on allait aller trop vite puis passer certaines explications.

0:25
Donc ça sera divisé en 2. La semaine prochaine, on va voir la 2e partie et on va voir les différents aspects de l'examen. Et puis si possible si vous avez des questions sur certains ou certaines parties du cours avant de commencer. Il y a eu un petit changement par rapport à ce qu'on avait vu hier. Hier, on avait parlé de combustible, donc il y a ça a suscité beaucoup d'interrogations.

0:54
Donc j'ai regardé dans le document de du CSSP édition 10 2024, c'est quoi s'est ajouté au niveau des liquides, c'est le afm. C'est la mousse afm qui a ajouté, on a toujours les CO 2 qui sont là, on a toujours le allant ou l'équivalent, qui peut être le FM 200. Et puis on a la classe K qui s'est ajoutée, qui est matière grasse de cuisson, mélange alcalin, et cetera, acétate, citrate, carbonate de sodium.

1:22
Donc j'ai mis la slide à jour. J'ai mis le le PowerPoint à jour également dans moodle. Donc si vous partez dans moodle, c'est cette version que vous allez trouver. C'est ça pour être à jour par rapport à aux éléments de combustible et les méthodes de contrôle, c'est bon ? OK, Cela étant, on commence le cours d'aujourd'hui.

1:55
Donc aujourd'hui, on va voir le cap. Un, évaluer et mettre en œuvre des principes de conception sécurisés dans les architectures des réseaux. On va parler du modèle osi et TCP IP, on va parler de l'ipv 4 Ipv 6 ipsec un instant je avec mon écran c'est ça ?

2:18
On va parler également des protocoles sécurisés, l'implication des protocoles multicouches, des protocoles convergents comme Five Channel, ouver, Internet également, on va parler de a 6HSI, Voice, spy, micro segmentation, SDNVX, LAN, SD, One sans fil, l'high fi, wifi, Ziggy satellite, 4G, 5G, réseau de distribution de contenus.

2:49
N'hésitez pas à me poser des questions, je ne vous vois pas. Donc si vous avez de quoi vous pouvez peut être lever la main comme ça je pourrais le voir et puis intervenir. Mais bon on peut continuer. Ok ? Je présume que la plupart d'entre vous avez déjà fait des cours de réseaux donc il y a des concepts qui sont quand même familiers.

3:17
On va juste faire juste une révision générale pour revenir sur certains aspects parce que ils sont couverts dans le body of nowley de du Cssp. Donc c'est important de les connaître et puis de savoir comment est ce que on les utilise, on les utilise en pratique. Et puis pouvoir aussi renforcer ce que vous avez appris durant vos anciennes, vos, vos anciennes années et puis peut être se retenant votre parcours de maîtrise.

3:47
Donc le modèle Osi Ben c'est un modèle qui est standardisé sur les communications réseaux, les communications au niveau de du réseau du Network. Donc le modèle osi est fait avec cette couche, donc qui part de du physique, la couche physique, la couche est donnée, la couche réseau, la couche transport, la couche session, la couche présentation, la couche application et on a le TCPIP.

4:14
Qui est lui ? C'est le un modèle à 4 couches, donc on arrive à faire un mapping facilement entre le TCPIP et le modèle Easy. Donc au niveau de la couche TCPIP qui est beaucoup utilisée, qui est utilisée au niveau de l'internet. Donc la couche Link est mappée avec le data Link et puis physique, le Network c'est internet, le transport ne change pas la couche applications va englober applications, présentations sexuelle au niveau de du modèle Easy.

4:44
La pratique le Network Interface au niveau du TCPIP c'est que on va prendre en compte tout ce qui est Ethernet, open ring et puis d'autres protocoles de communication avec une communication physique pour tout ce qui est Network Liar Ben c'est le IP qu'on va utiliser ou tout ce qui est transport Lear. On va parler du TCPIP et puis du IDP. Donc ces protocoles là on va en parler.

5:10
Et puis tout ce qui est application meilleure la couche application. Ben on a le HTTP qu'on utilise généralement quand on fait des navigations sur le net, on a le FTP qui nous permet de de faire le transfert des fichiers. On a le telenet qui permet de faire des communications entre des machines, on a le SMTP qui nous permet de de faire de la messagerie et le DNS qui fait la résolution de nom. Donc on va revenir sur certains certains protocoles qu'on voit ici dans les autres slides.

5:45
Donc au niveau de la de la couche réseau donc on a une correspondance avec les 2 couches un et 2 du modèle aussi donc qui est aussi nommée interface Réseau Network Interfiz et puis accès réseau donc on a le Network Access également. Donc à ce niveau ça c'est la communication au niveau bits qu'on aura. Donc on va utiliser toutes les les les canaux de communication, que ça soit le fidèle, le Wifi.

6:09
Tout ce que vous pouvez imaginer Bluetooth tout ça, ça ça sera au niveau au niveau net, au niveau je dirais au au niveau première couche physique au au niveau de couche Link. Ensuite on a le IP qui est la 2e couche au niveau du TCPIP donc lui il va. Il se situe au niveau 3 du modèle osy donc il permet le le routage à travers un réseau IP.

6:37
Donc on a le IP qui est le protocole de routage ISMP le protocole de diagnostic, on a l'a MP qui a le protocole de résolution des adresses Mac, on va en parler tantôt. Donc au niveau réseau on va parler de des classes d'adresse. Oui oui Bonsoir Monsieur, je voulais savoir pour le Network Enterface dans le cas où on a des on a, on a le même concept dans un dans les dans les dans le cloud. Est ce qu'on considère aussi que c'est au niveau ?

7:06
Donc là c'est virtuel, est ce qu'on on on devrait le considérer comme au niveau un et 2 ou comment ça

fonctionnerait au niveau du oui on le considère au niveau même dans le cloud on le considère au niveau un 2 également OKOK parfait. C'est vrai qu'on c'est vrai qu'on ne le voit pas, mais dans le cloud on on gère, ça c'est c'est abstrait mais cette notion souvent quand on est dans du IAIS mais bon quand on est dans du past on ne le voit pas mais du IAS tu vas voir que tout l'aspect réseau il est géré, on ne on ne le voit pas comme j'ai dit abstrait mais il faut en tenir compte.

7:36
OK merci les classes, les classes d'ADRESSAGES IPIPV 4 généralement avant avant 1993, avant 1993, pour les classes d'adresses IPV 4 on utilisait. Pour les adressages IPV 4 on utilisait les classes donc on avec les classes on avait ABCDE donc.

8:06
Pour ceux qui avaient fait le réseau très longtemps en organisant une en fonction des classes et les classes avaient des masques d'adresses bien précis. Donc au niveau de la classe A, Ben on partait de de un à 126 et puis on avait du juste 8. Qui était le masque de de réseau au niveau de la classe B ? Ben on avait 128 à 191, on avait 2.

8:30
Sly 16 donc on avait 2 octets qui étaient pour la classe Réseau Network host autant pour moi donc on avait la classe C, lui qui partait de 192 à 223 et lui qui avait un octet pour les le réseau pour le Lost et puis les 3 autres octets, les 3 premiers octets qui étaient pour le qui étaient pour le Network pour identifier le Network.

8:57
Le D 200204210039 le E 242 155. Donc qu'est ce qui arrive ? C'est que avec ce modèle on a remarqué que y avait beaucoup de gaspillage d'adresse puisque on était c'était rigide, il fallait se limiter à certaines classes. Donc on a la classe A les on doit utiliser 8 Octets, Ben on se limite à là si on utilise une un adressage pour un réseau spécifique, Ben on peut avoir des gaspillages. Donc. Mais on était rigide, on se limitait à ça.

9:23
Après, il y a eu de l'évolution, on va en parler tantôt. Qu'est ce qui est à remplacer les places dans ces 5 classes d'adresses ? Là donc pour un réseau privé. Donc on avait on a ces différentes plages, là qu'on a les plages réseau pour le privé. On n'utilise pas n'importe quelle adresse pour notre réseau privé en interne.

9:50
Pour notre réseau privé, en interne, soit on utilise le 10 0 0 jusqu'à 10 10.2 100505210055, on n'utilise pas les 205 255 et puis le dernier 255, on va s'arrêter à 254. Mais c'est cette plage qu'on va adresser à utiliser quand on veut faire un réseau local. Si après le 10 on peut utiliser le 100721001600, jusqu'au 172 31, on peut utiliser le 104201210068 ou les 104201210068.

10:18
Si vous vous si vous êtes actuellement sur votre machine, votre réseau Wifi à la maison et vous allez sur CNTV pour faire un IP Config, vous allez voir que votre adresse c'est soit un 10 ou 172 ou 192. Ça peut pas aller au-delà de ça parce que les autres ce sont des adresses qui seront routables sur Internet. Donc ça ce sont les adresses qui sont désignées pour constituer un réseau local. Donc toutes les machines qui sont dans votre réseau local vont utiliser une de ces adresses là.

10:46
Et avec ces adresses là, le nombre d'adresses qu'on peut avoir avec les 10, c'est qu'on peut avoir plus de 16000000. Et avec le les 172, on peut avoir plus de 1000000. Et avec le les 192, on peut avoir jusqu'à 65 machines qu'on peut configurer 65 adresses possibles, 65536 adresses possibles qu'on peut avoir. Donc ça veut dire quoi ? Que si j'utilise le 180121006080 dans mon réseau ?

11:15
Avec cette plage, selon l'adressage de sous réseau que je vais que je peux, je peux aller jusqu'à 165 mais les masques qu'on a vus tantôt ici si peut être j'utilise un masque de 124, ça va juste vous limiter à 254 machines que je pourrais avoir, je peux pas utiliser le 0, je peux pas utiliser le 255 puisqu'on je peux avoir jusqu'à 253 ou 254 marchés adresse possible.

11:40
Après, je peux jouer avec le masque de sous réseau pour augmenter mon le nombre de machines que je peux avoir dans un réseau spécifique. On a des adresses qui sont qui sont privées, automatiques, qui ne sont comme des adresses qui sont allouées, qui sont directement allouées sur certains appareils donc comme le 100609215400. Donc ça c'est une une adresse, une adresse qui est réservée, qu'on n'utilise pas pour notre réseau.

12:09
Et on a un protocole qu'on appelle Dynamic host configuration de DACP qui lui dans notre réseau interne, quand on configure notre routeur Wifi, Ben c'est lui qui donne l'adresse IP aux machines qui se connectent au réseau automatiquement sans que nous on attribue l'adresse. Donc c'est pas ce que vous devez retenir, c'est que l'adressage d'un réseau de d'une machine dans le réseau n'est pas systématique. C'est ce protocole là qui permet de faire en sorte que.

12:39
Une fois que vous ajoutez quelqu'un dans votre réseau wifi mais automatiquement la personne a une adresse IP et que la personne peut naviguer non seulement dans votre réseau interne mais aussi dans votre réseau sur Internet aussi parce que si votre routeur permet de lui donner Internet, Ben il aura Internet. Donc c'est ce protocole qui permet de lui allouer de lui donner une adresse mais aussi de donner un certain bail. C'est à dire que il va pas avoir l'adresse tout le temps, il va lui donner l'adresse et puis peut être sur un certain nombre de temps.

13:08
Et après il va retirer l'adresse. Et puis à un moment donné, il va, il va redonner l'adresse. C'est à une autre personne. Tout à l'heure, on parlait des des classes d'adresses, donc les classes d'adresses ont été remplacées par le CIDR qu'on appelle class less Inter domain routine donc.

13:30
C'est la notation qui permet de remplacer les classes d'adresses qu'on avait et ce que je vous ai présenté tantôt. Donc au lieu de se de se calquer sur les masses d'adresses habituelles qu'on avait, c'est à dire que on avait soit du Slash 8 pour la classe A, slash 16 pour la classe B et Slash 24 pour la les classes C mais on va pas se limiter à ça pour ne pas avoir de gaspillage d'adresses comme je l'ai dit tantôt.

13:55
Donc on va être plus flexible. C'est à dire que même dans une adresse dans une classe d'adresse qui

était initialement a Ben je peux faire du slash 24 si je veux pour des classes d'adresses qui étaient initialement peut être B je au lieu de me limiter au slash Slash 16 que j'avais, Ben je peux faire du slash 8 ou du slash 24 dépendamment de ce que je veux ou je peux faire même du Slash 26 Slash 30 peu importe ce que je veux pour que je puisse.

14:22
En fonction de mon besoin d'adresse pour mon réseau, je puisse dimensionner l'adresse à ce niveau-là et ça évitait d'avoir en fait des gaspillages d'adresse. Donc comme vous pouvez le voir dans le tableau qui est là, donc si on a un format qui est ABCABCD Slash 32, Ben on peut juste avoir une seule adresse sur les 256 qu'on a. Donc initialement c'était.

14:47
Dans une classe, si on pourra avoir juste un sur 250 sites, donc on va continuer. Quand on va faire slash 31, il va nous donner le nombre de machines qu'on peut, le nombre de d'adresses qu'on est capable d'avoir ici, la correspondance de nombre d'adresses qu'on est capable d'avoir selon le masque de sous réseau qu'on pourrait se définir. Donc là c'est plus flexible, on on s'arrête plus plus à 8 16 32. On va définir ce qu'on veut pour avoir le nombre de machines qu'on souhaite avoir dans un réseau spécifique. Et là on a le masque des sous réseaux qui va avec.

15:17
Pour l'adressage pour le le format d'adresse qu'on aura défini ensuite on a on a l'adresse qu'on appelle l'adresse doop back donc qui est l'adresse de le la machine locale. Donc si vous faites par exemple sur votre machine, vous faites tout de suite vous cherchez à connaître l'adresse du du local Post, Ben il va vous donner 107 00001. Donc le 100120700001 c'est l'adresse de votre machine.

15:43
Avant que peut être le routeur lui donne une adresse spécifique. Donc même si le routeur lui a donné une adresse ça reste que quand vous tapez le 120 700 la machine sait que c'est d'elle qu'il s'agit. Donc des fois dans le temps ça pouvait être parfait pour faire peut être des petits tests. Quand vous avez un petit un petit serveur sur votre machine vous pouvez directement au lieu de chercher l'adresse.

16:05
Au lieu de chercher l'adresse de de la machine, Ben avec le 127 vous savez tout de suite que c'est votre machine et puis vous pouvez lui associer le service en question. J'ai vu passer un message, je sais pas si quelqu'un a une question. OK c'est correct, c'est beau, ça va, ça va jusqu'à maintenant pour les adresses IP, ça va OK ?

16:39
Le Network adresse translation. Donc qu'est ce que le NAT fait comme vous le voyez le NAT qu'est ce qu'il fait ? Ben il va cacher le réseau privé et permet de communiquer avec Internet. Donc si on veut sortir avec une adresse on a une adresse dans notre réseau interne. 100801216081 .11 .2.

17:01
1.100 Slash 24 donc j'ai mes différentes adresses donc quand je vais ressortir Ben je viens avec la le NAT et le NAT va donner une adresse qui va me permettre d'aller communiquer tranquillement sur internet et de l'extérieur on n'est pas capable de d'identifier par exemple ma machine. Savoir que c'est cette machine qui a fait la requête parce que la NAT va va gérer tout ça là. Et puis après quand tu as une requête retour Ben il saura, il saura quelle était la source de la requête et puis va l'attribuer.

17:32
Donc on a 3 types, on a le na statique, donc le statique c'est la liaison un en un avec une assignation prédéterminée, avec plusieurs adresses publiques de sortie. Donc on a une adresse interne qu'on a maintenant va nous donner une adresse publique et nous donner une adresse publique spécifique. On va faire notre requête, après on revient, on on a. La retraite est retournée à notre source qui avait qui avait émis la requête.

17:56
On a le dynamique donc c'est un une liaison de un à un donc selon le premier arrivé premier servi avec plusieurs adresses publiques et sorties. Donc on a le 3e qui est le port adress translation donc une adresse publique de sortie. Donc on va gérer au niveau de des ports. Maintenant on va parler tantôt des différents ports qu'on peut avoir. On a parlé du IPV 4, des classes d'adresses, de les classes d'adresses et du CIDR. On va parler maintenant de de l'i PV 6 donc le IPV 6.

18:31
On s'est rendu compte à un moment donné que le IPV 4 allait être insuffisant avec le nombre de machines qu'on est en train d'avoir dans le monde. Généralement, je dans nos maisons, on n'a pas moins de 5 à 10 appareils qui sont connectés simultanément. Si je prends en compte l'imprimante, les ordinateurs, les téléphones, la machine à laver, tout, tout ce qu'on a à la maison qui communique avec Internet, le téléviseur.

18:57
Très souvent dans les foyers on n'a pas moins de 5 appareils, donc 10 appareils. Donc imaginez pour chaque maison on a 10 appareils donc à un moment donné les adresses vont pas suffi donc il y a eu le IPV 6 qui lui va venir pallier le manque d'adresses IPV 4. Donc il est de 32 bits à 128, il part de 32 bits à 128 donc il permet de faire le QOS sur la qualité des services et l'auto configuration également. Mais Google ?

19:26
Dit qu'il reçoit jusqu'à 28% des trafics IPV 4 dans le monde. Donc comment est ce que l'i PV 4 est fait ? Et puis comment est ce que l'i PV si c'est fait donc IPV 4 ? Comme vous le voyez lui il est fait en forme de bits donc on a 172 donc chaque chaque lettre avant le point c'est c'est un octet donc 8 bits.

19:50
Donc le 172 est converti en BIT. Ici le 16 est également converti en BIT, le 254 le un il est converti en BIT, donc les 2 font 32 bits. Avec le IPV 4, Ben on est en hexadécimal donc en hexadécimal comme on l'a dit tantôt, ici on on perd dessus du 32 ou du 128 bits, donc en hexadécimal. Vous avez sûrement vu ces genres de chiffres. Le principe c'est que quand on prend la notation, Ben on va enlever les zéros.

20:17
Donc ce qu'on a ici, on va enlever les les zéros. Donc quand on a les zéros, on va les enlever, on va mettre les les : à leur place. Et souvent quand on a un 0 avant, on enlève le 0. Dans le cas ici on a bon dans cet exemple là ils l'ont pas enlevé, c'est pas grave. Mais généralement dans la notation, quand les zéros avant on les enlève parce qu'on s'est dit que ils n'ont pas de représentation réellement, c'est comme quand dans le.

20:43
Dans la base 10, quand on a 0 un Ben c'est un. Donc ici les grades décimales on a tous les zéros qui

sont derrière, on les enlève et on obtient cette adresse qui est là. Et c'est vraiment sur vos machines également. Si vous faites IP for Config, vous allez voir l'adresse IP 6 Ipv 6 associée à votre adresse. C'est bon on continue ?

21:17
Est ce qu'il y a des questions ? Oui Émile, oui une question d'accord. Mes questions embêtantes as tu des des classes d'adresse IPV 6 ? Parce que là il me semble, je reconnais c'est une adresse une adresse IPV 6 globale mais je je pense pas qu'il y ait eu des classes spécifiques parce que déjà dans le IPV 4 comme je l'ai je l'ai expliqué on avait initialement les classes.

21:45
On a vu que c'était trop compliqué donc on est venu avec le CIDR, mais IPV 6 je sais pas si je pense pas j'en ai pas entendu parler OK donc peut être que pendant qu'on est en train de faire pour certaines pourraient faire les recherches pour voir s'il existe des classes IPV 6 mais j'en ai pas entendu parler OK merci ouais mais même le IPV 4 oublie les classes, pense plutôt comment est ce que avec le masque de sous réseau oui avec le masque de sous réseau comment est ce que tu peux faire ton réseau ?

22:14
En prenant si c'était c'est un réseau interne, c'est un réseau local, Ben tu vas prendre une place d'adresse soit le 1972 ou 992 mais les classes Tu tu les oublies. Amadou, juste pour confirmer. Je me rappelle plus, est ce que avec ipv 6 on a aussi la notion de les adresses publiques et privées comme pour Ipv 4 Ipv 4 par exemple 172 et les adresses 10 c'est des adresses internes qui sont privées.

22:43
Je sais pas, je sais pas Émile, mais on peut-on peut vous pouvez vérifier hein je je vous demande pendant que si je sais pas vérifier en même temps comme ça on apprend nous tous en même temps. Oui Aurélie Aurélie ma question ma question c'est de savoir Aurélien, Ouais vas y oui pourquoi ? Malgré le fait que je pense qu'i PVIPV 4 devait être expiré depuis d'après ce que rapportait, je pense que.

23:11
Il y en a depuis 2000, je crois que c'est 2000, 22021 ou 2022. Pourquoi depuis que ça a expiré on utilise toujours PV 6, pourquoi PVC peine à prendre ? Pourquoi PPV 6 n'a pas remplacé l'i PV 4, mais pourquoi sa peine à prendre de l'ampleur aujourd'hui ? Pourquoi la plupart des serveurs tourne toujours sur IPV 4 et tout et tout et tout bon moi je de de ma petite connaissance fait que c'est pas la la réalité, je pense que déjà on hérite en fait de l'héritage du IPV 4 qu'on a avec la communication.

23:40
Donc peut être que il y a peut être des enjeux d'implémentation à grande échelle du IPV 6 mais ça s'en vient maintenant est ce que on va faire un changement brutal ? Je sais pas mais je sais que quand sur une adresse de machine tu as le IPV 4 et tu as ton IPV 6 qui est associé ? Et généralement dans les projets informatiques on recommande toujours de tourner avec des 2 systèmes pendant que.

24:08
L'autre système est en est en en fonctionnement donc on va pas du jour au lendemain les changer, on pourra rouler les 2 et à un moment donné peut être on pourra switcher. Nasser tu as mis un message, qu'est ce que ? Qu'est ce que ça veut dire ? Nasser tu as mis un lien juste au niveau de des PV 6 privés et publics.

24:33
Je suis pas sûr à 100%, j'ai pas eu vraiment tout à comme information mais je crois qu'on a 2 une adresse IP privée 6 et publique en général le Global Unicast de mémoire aussi, là ça commence par chiffres et le local ça commence par FC quelque chose comme ça mais j'ai pas toute l'information, je crois que le je l'ai déjà lu dans ce sur ce site là mais ça reste à à confirmer là.

25:02
Parfait si vous avez l'information, n'hésitez pas à mettre on va apprendre nous tous. Oui Lucien oui merci c'est juste pour apporter une précision par rapport à l'i PV 6. Là effectivement il y a des correspondances locales en fait il y A quelle correspondance privée au fait ? adresse IP privée OK du coup IPV 6 C'est ça là qui est en fait un local Link OK ?

25:31
Et puis il y a le une classe locale là qui est au fait de l'adresse IPV 6 je crois donc et qui est l'adresse IP publique donc il y a vraiment une correspondance locale et publique au fait ? Donc IPV 6 d'accord c'est ça, pour sortir on utilise les glaces globales là qui commencent par des chiffres et comme il a dit et ça peut commencer par 200 et n'importe quoi. Par contre pour le local, pour le réseau privé, c'est un il y a des.

26:00
Ça commence par des lettres au fait ? OK donc c'est ça FCFDOOK, merci. Merci pour votre contribution continue Internet contrôle Management Protocol, le ICMP donc c'est un message de contrôle d'erreur donc entre les équipements et réseau. Donc il peut être utilisé pour les attaques, donc les attaques Dead OS dos des DOS amplifiés des manding de Middle.

26:37
Des Ping of the Death puis des messages qui sont souvent très longs donc on a différents types de codes qu'on peut avoir. Donc avec le Icmp donc le code 0 il est dit que on a écho ou pas, donc ça veut dire que la c'est la réponse à un Ping. Le 3 ça veut dire que la destination n'est pas atteignable. Le 5 ça veut dire le redirect ça veut dire que c'est on redirige le paquet vers une autre passerelle.

27:01
Le 5, le 6 plutôt Eco request donc ça veut dire que la requête Ping est là pour tester la connectivité et le 9 le routeur appreteizement, le 10 routeur sur le station et le 11 Time Exedy donc ça veut dire que le TTLA expiré. Donc ça c'est les différentes côtes qu'on peut trouver avec le ICMP.

27:27
Pour les attaques par déni de service, donc les tenues de service, l'impact c'est rendre un service indisponible. Donc quand on va faire le DOS sur un une machine et à un moment donné le service ne sera pas disponible. Donc on a le dos qui a qui est fait par une seule source et on a le DOS qui est le dynamique qui est le dynamique dos qui est fait par plusieurs sources.

27:59
Donc qu'est ce qui arrive ? C'est que on a un attaquant qui peut prendre une machine et avec la machine, Ben il va peut être procéder. Il y a une compromission de la machine, il va procéder aux attaques et on a souvent des amplificateurs qui vont en fonction du protocole qui vont les amplifier. On en parle tantôt, les différents amplificateurs. Et puis selon le protocole, quels sont les facteurs d'amplification qu'on peut avoir pour les attaques ?

28:29
Pour un synopsis d'attaque TDOS. Donc comment est ce qu'on procède ? C'est que on prend les détecteurs, les réflecteurs, donc on va détecter les serveurs complices, donc les serveurs qu'on peut utiliser pour aller faire les attaques. Donc l'attaquant qu'est ce qu'il va faire ?

28:45
Il va regarder sur internet quels sont les services qui sont mal configurés, donc des DNS ouverts, des services NTP, des l daps qui sont capables de répondre à une requête sans authentification. Donc des fois on peut juste utiliser vos serveurs, pas pour vous attaquer vous même mais pour vous permettre d'aller faire des attaques. Donc je crois il y a un DOS qui avait été fait en.

29:09
J'ai plus l'année mais qui avait utilisé des caméras de surveillance pour rendre dans les grands services je sais pas de Google et puis Microsoft tout ça j'ai pas j'ai plus l'année en tête mais c'est sûr que c'est des machines victimes qui ont été utilisées ou des machines souvent des machines complices qui ont été utilisées. C'est pas eux peut être que qui ont décidé d'utiliser leurs appareils mais étant donné que il y avait des mauvaises conférences là-dessus. Mais les attaquants les utilisent pour aller procéder faire son attaque ensuite.

29:39
Quand on finit de détecter les les réflecteurs, Ben on va créer le vecteur d'attaque. Donc l'attaquant, il va forger des paquets avec. Il va forger les paquets avec une adresse IP usurpée pour envoyer des requêtes au réflecteur. Le Réflecteur, c'est une machine de serveur complice. Ensuite, il va consolider le vecteur d'attaque, donc il va coordonner plusieurs réflecteurs pour amplifier la charge, souvent à l'aide des botnets.

30:03
Et il va attaquer. Donc tous les réflecteurs envoient leur réponse massive à la cible victime qui est submergée sans avoir rien demandé. Donc si on veut faire un DDOS sur le serveur d'une entreprise, Ben on va passer par ces étapes là pour faire le DOS. Donc on va trouver des serveurs complices voir des services qui sont mal contribués. Comment est ce qu'on peut les exploiter ? On va créer des vecteurs d'attaque, on va consolider, rassembler tous ces éléments là et puis le contrôler via un botnet.

30:33
Et puis lancer tout est toute l'attaque là-dessus. Donc ça c'est les protocoles et puis les amplificateurs qu'on peut avoir. Donc un facteur d'amplificateur d'un protocole ça veut dire que on est on va prendre la taille de la requête. Donc ça veut dire que la machine initiale qui va faire l'attaque, qui va peut être donner de l'ordre, qui va faire la requête, on va prendre la taille de la requête.

31:01
Et on va multiplier par les facteurs d'amplification pour donner la taille de la réponse. Donc la taille de la réponse sera la taille qui va aller vers la machine victime. Donc pour selon le protocole on va donner le la taille d'amplification. Donc si il y a un DLS qui est mal configuré, Ben ça peut aller de 28 à 54 le un NTP lui le facteur d'amplification est plus élevé donc il peut aller jusqu'à à 556. Le plus grand ça sera un Minecraft qui part de 10000 jusqu'à 51000 donc qu'est ce que ça veut dire donc ?

31:31

Ça veut dire que il suffit juste d'avoir ces protocoles là et si j'envoie une requête, une taille d'une requête, il va le multiplier. Donc si c'était peut être la machine de l'attaquant qui faisait l'attaque, qui était capable de d'envoyer peut être la taille ? Prenons un donc il va demander plusieurs types de ces machines là pour envoyer ces requêtes de un. Mais au lieu que on cherche plusieurs machines, Ben on va prendre une machine.

31:59
Aller chercher des serveurs qu'on puisse chercher surtout des protocoles qui ont des amplificateurs plus élevés et puis on va mener l'attaque. Donc l'exemple ici un NTP Ben il va faire 10 fois un DNS. Donc si j'ai eu un serveur NTP qui est mal configuré, un seul serveur NTP ça fait 10 serveurs DNS mal configurés donc l'attaquant peut être va privilégier ce genre de serveurs là et puis faire cette attaque avec donc.

32:24
Des fois c'est pas tant le nombre de d'appareils qui interviennent dans le DOS, mais c'est surtout les protocoles qui ont été utilisés, en tenant compte bien sûr du facteur d'amplification. Classification des attaques DOSDO les attaques DOS, j'ai oublié un s, ici on a les flow multiplication, donc on a les types d'attaques smurf on frangle dont on va parler.

32:52
On a des pay Load magnification avec des TCP, donc on a les signes a, on a les RST, on a les PHS, on a avec UDP on ADNSNTP. Et puis les autres types d'attaque qu'on peut faire avec les DDOS donc ça c'est une classification des DOS. Je vais corriger mon s là après ça c'est le compte mesure qu'on peut avoir.

33:18
Oui on a les DDOS qu'on peut avoir mais en même temps on a des contre-mesures qu'on doit pouvoir mettre en place. Donc on a en terme de classification dans les deployments donc on peut mettre des refacto n des victimes n vous avez le lien en bas, c'est une recherche scientifique pour approfondir les différents éléments on a le scanning donc entière IPD 4 segments scan, on a le defait qui est le onypot qui peut entraîner.

33:46
Comme on avait dit la dernière fois, avoir un entraîner l'attaquant et puis pouvoir savoir qu'est ce qu'il veut faire et puis pouvoir se défendre avec eux parce que j'ai des questions. On demande si le profil utilise le protocole qui n'est pas ça non ? Peut être que la liste n'est pas exhaustive hein.

34:10
Ça, c'est selon l'étude qu'on avait, on a, on a sorti donc sûrement il y a d'autres protocoles qui qui ne sont pas là. Donc si il y a des protocoles connus avec des attaques connues, c'est sûr que un moment donné on va mesurer le protocole, le facteur d'amplification. excusez-moi, on me demande de me connecter à nouveau un instant sur le teams.

34:38

35:47
OK désolé, il y avait le challenge MFA, le système essayait de me identifier à à nouveau. Donc est ce que vous m'entendez ? Est ce que vous m'entendez ? Oui oui OK oui oui oui OK c'est bon on continue

donc on continue les attaques DDOS on en a plusieurs donc on a les insigne float, donc lui il consiste à il envoie des paquets jusqu'à ce que la pile soit remplie.

36:16
Donc il va envoyer plusieurs paquets. Voici l'attaquant ici il va envoyer plusieurs paquets jusqu'à ce que la victime soit vraiment à terre. Donc la technique d'atténuation Ben les pare-feu les équipements réseaux mis à jour la surveillance réseau dont IPIPS. On a une autre attaque qui est le smurf qui est l'envoie des paquets ICM donc on a vu tantôt le protocole ICMP avec IP source modifier.

36:42
Donc les réponses vont directement à la victime. Donc on a l'attaquant qui va envoyer des paquets ICMP. On a le frangol qui est la même technique que le ICMP, mais lui il va utiliser le port 7 et 19 pour mener l'attaque. On a une autre attaque qu'on appelle ping.

37:06
Qui est lui ? Il est efficace lorsque est lancé en grand nombre par des zombies par exemple. Donc généralement c'est le cas typique qu'on voit avec les le scénario qu'on avait parlé tantôt. Donc la technique d'incinération c'est de bloquer les ICMP. On a lepping of diff qui est un paquet de XMP +64, donc qui le la cause un débordement de tampon donc il va faire du du baff Over Flow sur le système.

37:35
Après les attaques DOS, on va parler maintenant de la résolution des adresses, le AIP, adresse, résolution, protocole. Donc qu'est ce que ça fait ? C'est que il résout l'adresse IP en adresse Mac. Donc sur nos différentes machines, toutes nos machines qu'on a, que ça soit nos téléphones, nos ordinateurs, la machine à laver, le la télé, le téléviseur. Ils viennent avec une adresse du fabricant qu'on appelle l'adresse Mac donc.

38:05
Quand on est sur le réseau, Ben le réseau quand il il va donner l'adresse, il va tout au long. On a vu le DACP. Le DACP va attribuer une adresse adresse IP à une machine. Donc quand il va attribuer une adresse IP à la machine, le ARP elle qu'est ce qu'elle fait ? C'est que lui, qu'est ce que autant pour moi c'est un protocole. Il va associer l'adresse IP qui a été donnée par le Routeur à l'adresse Mac de la de l'appareil.

38:36
Qui qui est venu avec la fabrication ? Donc on aura maintenant une association entre l'adresse IP et l'adresse Mac, de telle sorte que si on envoyer un message à une machine depuis le routeur, il sait que c'est associé à telle adresse Mac. Donc il envoie le message à l'adresse Mac en question, c'est bon. Donc l'adresse Mac c'est 48 bits. Les 24 premiers vont identifier le manufacturé, le 24 dernier le numéro de série, c'est bon.

39:05
C'est bon ? Est ce qu'il y a des questions pour l'adresse Mac ? OK parfait donc tout ce qu'on utilise sur l'ordinateur sur sur Internet, s'il y a une il y a une technologie, on va trouver un moyen d'attaquer ça. Donc avec l'a RP comme dont on vient de parler, Ben on a différents types d'attaque qu'on peut avoir. On a dans le ARP poisonnier qu'on appelle ARP spofing.

39:31

Donc qu'est ce que l'attaque va faire ? C'est que il va lier le IP comme je l'ai dit l'adresse IP qu'on a à la mauvaise adresse Mac. Donc comme j'avais dit le routeur qu'est ce que lui fait ? Il sait que j'ai une machine a, j'ai une adresse IP, une adresse IPA donc j'associe les 2, les les les 2 les 2 adresses donc de telle sorte que quand je reçois un message je vais l'envoyer à l'adresse à la machine A.

40:00
Donc le ART spoofing ou poisoning. Qu'est ce qu'il va faire ? Ben il va changer l'adresse Mac de telle sorte que il vient repositionner l'adresse IP à une autre adresse Mac qui a été changée, de telle sorte que si on envoie le message au lieu que ça aille à la machine, la machine titulaire, Ben ça va aller à la machine malicieuse donc, comme vous le voyez ici en bas.

40:24
On a le routeur donc là le LAN il sert c'est quelle adresse ? Donc quand on va il va recevoir le message, Ben il va lui donner avec le poisoning les quand on va envoyer vu que le Mac a été changé avec qui est associé à la mauvaise qui est associée à l'adresse IP à une l'adresse IP originale donc là il va changer l'adresse donc quand on va recevoir le message au lieu que le message aille à la machine.

40:50
La machine source mais ça va aller à la machine de la machine malicieuse, est ce que l'adresse a été changée ? Donc très souvent on le fait avec des outils comme stapi de de Python qui va forger les paquets ARP malicieux. Donc on peut faire 2 types de requêtes, donc se demander c'est quoi whoaze avec l'adresse IP et puis is had avec l'adresse IP qui est associée à l'adresse Mac.

41:18
C'est bon donc on a il y a plusieurs techniques hein pour résoudre c'est ça ? Donc on peut avoir des des caches ARP statiques pour ne pas qu'on puisse changer. On peut avoir l'adressage, on peut avoir aussi la la segmentation réseau donc il y a quand même des stratégies qu'on peut mettre en place pour bloquer tout ça. On a maintenant on va parler maintenant du protocole ipsec.

41:45
Le Ipsec, c'est un cas de protocole associé qui est qui va sécuriser la couche 3. La couche réseau donc peut peut protéger un ou plusieurs flux de données donc il permet la confidentialité, l'intégrité de l'authentification de l'origine et protection contre les, les rejets, les replay. Il est utilisé pour les réseaux privés virtuels, les VPN.

42:14
Donc les composants du hypsec c'est qu'on on a une enquête qu'on appelle en tête en tête d'authentification, le AAH authentification Header qui lui va définir va définir les procédures, le format de parquet pour l'authentification des parties impliquées et des techniques de génération des clés. Donc il va s'assurer de l'intégrité et protection contre les relais ainsi que l'intégrité.

42:39
Un autre composant c'est un capsulation charge sécurisé, donc le ASP qui est un capsulation Security payload qui lui va se charger de séductionnement des messages, qui fait également l'authentification et l'intégrité. On a un autre composant qui s'appelle Association Association de sécurité, le SA Security association qui est le paramètre de sécurité pour une communication unidirectionnelle.

43:07
On a le l'échange de clés clés, l'échange de clés sur Internet, le ITE Internet KE Exchange qui est le

protocole de négociation cryptographique qui établit, gère les SA. Et puis la clé des générations est fait à l'aide de la GODYN Diffie elle même le mode, le mode de fonctionnement de l'i P SEC. Il en a 2 modes. On a le mode transport, donc lui c'est la communication entre 2 hôtes.

43:36
Il va chiffrer jusque la charge utile de l'i P. On va le voir tantôt et il il va toujours avec l'adresse IP réelle donc on va le voir tantôt avec les différentes images. Le mot tunnel lui c'est pour les VPN entre réseaux donc get way, get entre les différents différents gateway donc on a plusieurs machines c'est pas du des postes à out ou poste à poste donc lui il va chiffrer tout le paquet IP donc il va ajouter une nouvelle en tête.

44:06
Et puis il va donner une nouvelle adresse IP qui va, qui sera, qui va identifier le tunnel façon concrète sur les les, les les les les paquets. Comment est ce que ça se passe ? Donc comme je disais tantôt avec le le Ah authentification header Ah transport mode, on a le IP qui est là, on a le Ah header qui est là, on a le TCP et puis on a le PI low, donc comme on l'a dit dans le mail transport.

44:36
Dans le mode transport, il va juste authentifier le TCP et le payload uniquement, donc le IP il va continuer avec le IP, le Ah header, le Ah header, le IP original. Il va continuer avec le IP original, le IP de la machine il va continuer avec avec le le tunnel mode qu'on a vu tantôt, ça change.

45:01
Qu'est ce qu'on fait ? C'est que le IP qui est là il revient ici, le TCP vient là, le IP l'autre vient là. Donc quand on associe les 2, le AHI 2 vient après et on va lui mettre un nouveau IPIP du tunnel IP, l'adresse IP du tunnel qui va continuer avec. Donc là cette fois-ci il va pas juste authentifier juste le pay l'autre il va authentifier même l'adresse IP, il va identifier toute la charge un peu ce qu'on expliquait tantôt dans la slide précédente.

45:31
Ça c'est au niveau du Ah transport authentification header. On a le ESP également fonctionne de la de la même façon, donc comme vous le voyez avec le transport mode du poste à poste. Donc on a le IP, on a le ESP header, on a le TCP, on a le payload, on a le le, le header serment, le trailer et on a le ESP authentification qui va partir.

46:00
Comme vous le voyez avec le transport mode, on a le TCPPI l'autre qui lui il est-il est chiffré, on va authentifier tout ça et quand on passe au tunnel mode on a le header c'est le, c'est la, c'est le même fonctionnement, le IP repasse de l'autre côté et puis le ESP repasse de l'autre côté. On a le IP original de la machine qui est là, on va lui donner une un autre IP et l'en tête va revenir après et tout ça.

46:28
La charge pitule tout est tout sera chiffré, c'est bon c'est abstrait je je vois que c'est abstrait mais c'est c'est comprenez juste le le principe. Comment est ce que ça fonctionne avec les différents paquets pour que vous soyez pas pour qu'on on se pose pas nous-mêmes des questions, comment l'ordinateur arrive à ça ou bien comment le routeur arrive à savoir que c'est telle machine qui a envoyé le message ?

46:55

Ben ils passent par des paquets parce que les paquets savent à quelle adresse et à quelle adresse. On a envoyé le message, quel était l'entête qui était avec, est ce qu'il est authentifié, tout ça. Donc avec ça il sait exactement à quel appareil il doit retourner le message, à quelle haute ou source il doit retourner le message. C'est bon on continue, on a le canal d'échange de clé dont on a parlé tantôt, donc on a les Internet Security Association p Management Protocol.

47:24
Qui lui est utilisé par le le Ike dont on a parlé pour l'échange des codes pour le Security Association, Association de sécurité. Donc on a une entente formelle entre 2 entités, des règles de sécurité et il va maintenir le tutelle en utilisant le Ah, le Ah dont on a parlé. Le ESP comme on l'a dit, lui va s'assurer du chiffrement. Il fait aussi l'authentification et puis l'intégrité.

47:53
Le chiffrement des liaisons encryption, donc ici c'est chiffré, déchiffrer chaque point de routage du réseau jusqu'à son arrivée à sa destination finale, donc tout est crypté. Slash chiffré sur le lien donc permet aux informations de routage d'être utilisées. On a un outil de chiffrement qu'on va appeler le chiffrement de bout en bout, donc l'information utiles sont chiffrées, cryptées.

48:21
L'en tête et les informations de routage sont En clair. Donc vous voyez la différence quand on parle de chiffrement de bout en bout. Généralement quand on on prend nos nos messageries WhatsApp ou Messenger, des fois on voit un dentution, un tout, un dentution, donc c'est ça. Donc c'est l'information utile qui est vraiment chiffrée. Les autres éléments ne sont pas chiffrés alors que le chiffrement des liaisons, tout est chiffré, tout est chiffré sur le lien, c'est bon.

48:52
Ça, c'était la couche réseau. On passe maintenant à la couche transport, la couche 4 du modèle osi, donc dans la couche transport. Dans la couche transport, on a la couche 4, on a le TCP qui est full duplex et il garantit les services.

49:19
Et le IDP lui, c'est juste, c'est plex et aucune assurance, aucune garantie de liaison. Les ports de connexion au niveau de des différents ports, on a 65536 ports qui sont disponibles, on a du 0 à à 1024, 0 à 1023, donc les premiers 1024 qui sont réservés. Donc juste pour les services qui sont connus.

49:48
Du HTTPHTTPHTTPS 443 du SMTP 2024 à 4951 Ben c'est des ports qui sont affectés à des applications spécifiques comme on a le cas de Microsoft de de MySQL. Le temps pour moi le 30 306 c'est MySQL et le 54 32 c'est postgre SQL.

50:17
Donc sur une machine spécifique, si vous lancez une requête pour voir les ports et que vous voyez du 36 0 30 306 ou 54 0 32, ça veut dire que on a une base de données sur cette machine là du 5952 à 65 535, Ben ce sont des ports dynamiques ou privés ou souvent éphémères.

50:44
Donc l'exemple par exemple de l'exemple de du 80 80 qui peut être l'alternative au port 80HTTP donc dans le temps des fois avec Skype ceux qui ont utilisé Skype, Skype, des fois il utilisait je crois le port

80. Donc quand tu utilises une machine avec qui avait besoin d'un serveur web donc ça faisait un conflit. Donc des fois il fallait aller changer l'adresse, l'adresse du serveur web en question.

51:13
Pour qu'ils puissent écouter sur le port 84 20, pour ne pas, pour ne pas rendre le service de Skype indisponible ou pour ne pas empêcher que le serveur web fonctionne. Pour empêcher que le pour faire marcher le serveur FTPSFTV. Non désolé le 84 20 c'est pas un bon exemple. Désolé c'est pas un bon exemple ça, ça doit aller dans le le 1024 5950 et désolé le 84 20 C'est pas un bon exemple.

51:47
J'avais vu 81 autre 0. C'est pas le bon exemple pour le HTTP mais on a le 65000 piles qui sont souvent utilisés pour les p to p les communications p to p quand je vais changer c'est une grosse erreur ça. 38.

52:26
OK, c'est bon, continue toujours dans le la couche transport. Donc on a parlé tantôt du TCP, le TCP, voici la structure de l'antenne TCP, donc on a la source qui est sur 16 bits, la destination également qui est sur 16 bits, on a séquence number qui est sur 32 bits.

52:57
Aknowledge Men Lember qui est sur j'ai pas le nombre de bits ici de accned Man on a le data offset, le reserve, le Flag, le data observe 4 Bits, Reserve qui est sur 4 bits, Flag qui est sur 8 bits, on a le Windows 16 qui est sur 16 bits, le checksum qui est sur 16 bits, le agent point qui est sur 16 bits et puis variable option Ben.

53:26
Le data Data variable j'ai pas le le nombre de bits donc voici un peu une structure d'entête de TCPP un peu de la même façon qu'on a vu avec le les IP, tantôt les paquets IP qu'on a vu, tantôt avec les flags, on a le CWR qui est c'est quoi ? Tu as une question ?

53:52
Non non non c'est pas une question. Je disais c'était 32 bits pour la management je pense selon le schéma OK parfait donc les flags dont on parlait tantôt. Donc on peut avoir le CWR Flag qui est la réduction de la fenêtre de congestion. Donc pour le moment lui il est-il est vraiment rare pour la le sujet pour la congestion c'est rare.

54:17
Le ECW, le ECE, la notification des congestions également pour la gestion des trafics qui est aussi rare, on a le URG qui est urgent, donc pour les données urgentes on a le ACK qui est le acknowledment à l'acquiescement. Pour la synchronisation des ouvertures et des fermetures des sessions on a le PSH qui est le push données à expédier immédiatement.

54:42
On a le RST qui est le reset qui est l'annulation immédiate de la session en cours. On a le SIM qui est la synchronisation, la demande de synchronisation pour une session avec des nouveaux numéros de séquence. On a le film qui est la fin demande de fermeture de session, le TCPIP.

55:10
Pour le TCP, on a le Sim pour établir la connexion avec le TCP, mais on va utiliser des liaisons à 2 sens,

donc tout en check. Donc sur une machine donnée, on a souvent l'état initial qui est là, on a l'état initial qui est là, qui est souvent à clause d'ici.

55:33
Donc le client quand il veut demander l'ouverture de d'une section Ben il va envoyer un segment signe au serveur donc le serveur lui il va le recevoir avec le le signe ici il va retourner un signe hack au retour pour dire que oui j'ai vu ta demande de connexion. Je suis pas contre ta demande de connexion j'accepte et le client.

56:03
Lui, il va envoyer un autre segment à pour dire OK, j'acquiesce la réception de ton, de ton acceptation et la connexion est établie. Donc si je fais un parallèle entre nous les humains, c'est c'est ça, parce que je veux parler avec quelqu'un, je le vois, je le salue, je lui dis Bonjour, il répond, c'est comme s'il acquiesçait, il ouvre la connexion et puis on peut-on peut commencer à échanger, c'est un peu la la même chose.

56:31
C'est bon ? Est ce que il y a des questions avec ça avec le sin sin hack ? Bonjour tout le monde. Oui Monsieur j'ai une question juste juste pour que être sûr est ce que c'est 2 Waze ou bien 3 ? Je pense que c'est 3 moi je peux.

56:57
OK oui 3 True ways en tchèque OK je vais je confirme, je vais confirmer dans le document que j'avais vu qui me parlait de 2 oui dans certains documents je vois True en tchèque il y a des documents où je vois True en tchèque mais oui ton ton ton True tiens je vais, je confirme et puis à la pause je vais confirmer et puis je te rejoins, merci.

57:38
On a des types d'attaques qu'on peut avoir également, donc qu'on appelle l'attaque Land local, Ohia Network, Jingle. Donc ça dépasse des paquets TCP sin avec adresse IP et port TCP de la victime qui sont pareils que ceux de la source. Donc on va vous créer un dinail sur une machine elle même, mais on va faire en sorte que elle envoie la requête avec la même adresse IP.

58:05
La même adresse IP, source, adresse IP destination et sur le même port un signe là-dessus. Donc c'est sûr que la machine va planter donc il va continuer à envoyer la requête. Et puis à un moment donné la machine va planter. La victime se répand à elle même de façon constante, donc le système peut devenir instable. Donc la technique à atténuation c'est le pare-feu. Donc on va faire en sorte que au niveau du pare-feu que une adresse source ne puisse pas envoyer une requête à elle même.

58:40
Après le TCPIP, on va parler maintenant du du IDP, donc le user data Gram Protocol IDP donc lui la structure c'est pareil, on a le porso 16 bits, port destination 16 bits, longueur 16 bits, somme de contrôle et checksum 16 bits. Et puis on a la longueur des données.

59:02
Donc le IDP il transmet des datagrammes sans connexion donc lui il ne garantit pas très souvent le retour. On a le numéro de port dont j'ai parlé qui est associé, on a il est orienté sur la transaction, il n'a aucune garantie de livraison donc il envoie, on sait pas s'il a reçu ou pas. Contrairement au TCP, il est

surtout pour le protocole en temps réel. Donc le cas d'utilisation c'est les DNS pour la résolution de nom des DACP pour l'attribution des IP automatique.

59:32
Les streams, streaming, vidéo, audio, flux média peut avoir avec le I 2P. Après la couche transport on vient à la couche application donc la couche application Ben c'est le protocole sont les protocoles adjudicatifs liés à des ports précis pour l'écoute par serveur. Donc le cas ici le 20 ça sera le file transfert Protocol, le 21 également file transfert Protocol.

1:00:01
Le 22, ça sera ce que le SSH, le 23, Intel net, le 25, c'est SMTP, le 53 c'est DNS, le 80, c'est HTTP, le 110, c'est le POP 3, le 119, c'est le MNTP, le 123, c'est le MTP, le 144, c'est le imap, le 161 c'est le SMMTP pour pouvoir gérer les réseaux, le 194, c'est le IRC pour le le chat dans le temps.

1:00:31
Le 4 4 c'est HTTP Secure donc on a plein plein plein de protocoles donc on a plein plein, plein plein de de ports pour les applications donc les les ports. En fait si on on on considère que une maison, une maison c'est c'est une adresse IP. Les fenêtres ce sont comme ou les portes ce sont comme des ports. Donc on peut avoir plusieurs portes ou plusieurs fenêtres dans une maison.

1:00:56
Donc sur un serveur ou une machine, on peut avoir plusieurs applications qui roulent, mais pour identifier les applications, c'est les ports qu'on va utiliser, donc c'est ce que vous voyez. Donc sur une machine, si on a le serveur on ASM, on a le SMTP, là on a le FFTP, Ben il va utiliser l'adresse de la machine. La machine en question admettons que la machine fait 5921006016080 .1.

1:01:25
L'adresse de l'adresse de le le port va prendre le 100801608012 points 21, donc tout de suite on sait que si on va vers le 1802008010100 68,01€ 21, on est en train de s'adresser au FTP. Si on utilise le 25, on est en train de de s'adresser au C vers SMTP qui est là. Si on est en train de d'utiliser le 80, on est en train de s'adresser au.

1:01:54
Serveur web qui est sur la machine c'est bon c'est bon la notion de de port. Donc comme on est sur la couche application, quand on a parlé des différents ports, on va parler maintenant des services qu'on peut avoir. Un des services qu'on a c'est le DNS qu'on a, donc il lui qu'est ce qu'il fait aujourd'hui ? Si on arrive à naviguer facilement sur Internet c'est grâce au DNS.

1:02:27
Donc ça allait être vraiment difficile pour nous tous de retenir les les, les numéros de chaque site. Déjà, c'est difficile pour nous de retenir le le numéro de nos proches. Donc on ça allait être difficile pour nous de retenir les numéros, les numéros des des différents sites web qu'on a qu'on utilise. Donc la résolution des noms vient aider. Donc je sais tout de suite quand je fais usherbrooke.com, c'est plus facile de retenir que de retenir un numéro et après on a le FQDC non ?

1:02:57
Je j'ai la full calify domain, j'ai fait une erreur ici, c'est le n désolé c'était la fatigue, il y a un n au lieu de C ici je vais changer ça tantôt, c'est le FQDN donc full le calify Domain même ici. Donc lui c'est le nom

complet de la de la machine, pas l'adresse. Donc la structure du DNS c'est comment ? C'est que ici dans le point ici on a le root qui est là.

1:03:23
Ensuite on a les points com.org, on est 2 donc qui sont appelés le top level domain sont des 2 de pays, donc on a les points CA ou des génériques comme des points org qu'on a des points 2 des points CA qu'on a. Ensuite on a les 2nd 2nd level Domain, donc les noms de domaine enregistrés où on peut aussi dire sous domaine de org. Donc on a Wikipédia, on AFSS, on a université de Sherbrooke qu'on a.

1:03:51
Et on a les sous abdomen quand ce sont les sous domaines où les les noms de domaine en en 2 et on a le FQDN qui est le deux.wikipedia.org. Donc le FQDN ça va être 2 wikipedia.org. Donc quand vous voyez une adresse, une Sherbrooke ou service usherbrooke.com, ça c'est le FQDN. Donc vous pouvez tout de suite retrouver quel est le top level domaine.

1:04:21
Quel est le sous 2nde liver domaines ? Et puis quel est le sab, domaine le sab, domaine qu'on a sur un service donné. Donc très souvent pour les bonnes pratiques, il est recommandé d'avoir des sous domaines pour différents services pour que admettons, s'il y a un nom qui est affecté, Ben on peut réutiliser les les autres types de noms, les autres noms de domaines. OK on continue.

1:04:54
Donc ça c'était la description dont je parlais tantôt. C'est vrai que dans la représentation ici c'est comme un mobile, mais c'est pas un mobile. C'est vous voyez ça comme un serveur. Donc on veut faire des requêtes, on a une machine, on fait la requête, on tape Google, google.cagoogle.ca fait la résolution.

1:05:16
Le faire la résolution de du nom de l'adresse Google de google.ca et l'adresse IP publique va sur Internet rechercher l'information et me retourner l'information. Donc le DNS c'est comme ça que ça fonctionne. De façon générale, on va parler maintenant des attaques sur les serveurs DNS les attaques TNS qu'on peut avoir.

1:05:44
Excusez-moi, je sais pas ce que j'ai, je suis régulièrement challengé par mon mon MFA. Un instant je vais régler, je suis challengé à nouveau ma connexion.

1:07:21
Allô, je suis revenu. Y a quelqu'un qui a mis un message dans le chat, on va répondre débar AA mis un message sur tout ce qu'on peut avoir débar est ce que.

1:07:52
Tu peux le partager ton image c'est c'est très bien hein ? J'ai j'avais pas vu, c'est c'est c'est vraiment bien fait qui regroupe vraiment tout ce qu'on peut avoir PCPIPCP tu tu peux commenter un peu du bas. Allô Allô.

1:08:29

Est ce que vous m'entendez ? Moi je vous entends, OK, Gebard est là gebard, tu as mis une très bonne image et puis tu as disparu. On a besoin de ta contribution, OK ?

1:08:50
Ben c'est c'est c'est c'est ça résume un peu ce qu'on est en train de voir. On a le modèle os ici, donc la couche physique c'est vrai que c'est pas exhaustive mais c'est c'est quand même bon. On a le data Link, on a live puis dont on a parlé, on a le P to P, le P to p sleeve, l 2L 2TP, on a le Network IPICMPIGMP, le RIB, le OSPF, le ipsec.

1:09:19
C'est vrai qu'on ne voit pas tout IPR, le RIP et le OSPF, on va pas le voir, on a la couche transport ici, TCPUDPSSLTLS, on va voir tout, on va pas parler du SPX, on a la couche section, on n'en a pas parlé, tout ce qui est NFS, net, bios, SQLRPCSMP, on a la couche présentation, on n'en a pas parlé, ascii et autres, le 12h00, le MPN, le J, peg, non.

1:09:45
La couche 7, oui, on est en train de parler de la couche 7, le FTP le TRTP oui le le document il est quand même. C'est un bon miles Maps qui résume pas mal beaucoup d'éléments au niveau du One SDLCHDILCN spip, le tunneling ?

1:10:15
C'est bon, c'est un bon document qui récap plus ou moins les éléments qu'on va voir. Merci pour le partage. Je vais regarder dans mes documents. C'est bon on continue avec notre cours. Juste des questions.

1:10:39
Au niveau de SS 7, là est ce que c'est toujours vulnérable ou pas ? Parce que je au niveau de quoi le SS 7 vulnérabilité SS 7 sur le téléphone mobile, oui oui oui oui il est toujours vulnérable. Il y a rien qui a été le SS 7. Le SS 7 tu sais dans le temps c'était vulnérable, est ce que c'était SS 7 ? Je me rappelle que il y avait une vulnérabilité mais je sais pas si ça a été résolu.

1:11:08
Signaling System Seven je je dans dans le dans le temps quand j'en avais entendu parler c'était vulnérable mais on continuait à l'utiliser à date je sais pas je je travaillais pas trop en Télécom donc je sais pas si vous avez pouvez faire une recherche rapide pour voir est ce que on l'utilise toujours ça ça va nous aider. OK merci on continue.

1:11:39
Donc les attaques DNS donc on a le rôle DNS serveur donc il peut être complexe mais qui est qu'on est un serveur DNS à proximité du sujet ? Donc il peut intercepter les requêtes DNS et répond avant le serveur autoritaire ou dédié en respectant le QR IID donc son fonctionnement l'attaquant il peut installer contrôler un serveur DNS dans le réseau à proximité.

1:12:04
Il peut écouter ou intercepter les requêtes DNS et il répond plus vite que le serveur. Ce serveur autoritaire donc c'est ça. Si tu veux te jouer un rôle, faut être plus rapide que le propriétaire donc comme ça tu pourras récupérer rapidement l'information. Une autre attaque c'est le DNS cash poisoning le DNS cash poisoning donc l'attaque en question c'est le serveur DNS, il modifie la configuration donc il va donner de fausses informations.

1:12:37
Il va utiliser des forces information jameetta c'est autre chose. Poser la question dameetta a été remplacé a remplacé le radus mais pas le SS 7. Mais on pourra on pourra vérifier en fait des recherches pour voir si le SS 7A été remplacé. Mais je sais que dame te remplace le le radus.

1:12:58
Ensuite on a la corruption de configuration IP, donc en DHCP ou autre par un logiciel malveillant. Une autre attaque c'est proxy falsification, donc sur le fureteur lui même le le navigateur web. Donc on peut exploiter les failles dans le navigateur. On peut permettre un contrôle ou redirection du du trafic donc on va.

1:13:25
Tout faire pour avoir un proxy sur la machine et puis le falsifier. Retourner les riquets de la machine quelque part d'autre. Ensuite on a le domaine I jenking ou Field qui permet de changer l'information d'enregistrement sans le consentement du propriétaire, donc lui. Il peut se faire soit par le vol d'identifiants, le XRF intersection de cession ou attaquant attaquant d'identité responsable de l'enregistrement.

1:13:57
Une autre attaque, c'est la perte de domaine. Ce qui arrive c'est que des fois les gens oublient de renouveler leur domaine, leur nom de domaine chez le registrat, donc ils vont perdre le domaine. Ils vont perdre leur leur nom de domaine. Il y a pas beaucoup de recours mais souvent les registrats, ils vont offrir des périodes de grâce. Tout ça ça va dépendre des registrats.

1:14:22
Donc imaginez que un jour Google perd son nom du domaine. C'est ça serait un scandale Google quand tu tapesgoogle.com mais ça n'appartient plus à Google, quelqu'un d'autre l'a racheté donc vous voyez qu'est ce que ça peut créer donc au niveau de l'entreprise, si vous gérez le DNS votre entreprise, faites en sorte que le renouvellement puisse être automatique. Et puis soyez vigilant sur les dates pour ne pas perdre votre nom de domaine. Parce que si vous devez communiquer après avec vos clients ou.

1:14:50
Vos différents prospects pour leur dire j'ai changé d'adresse, j'ai changé d'adresse e-mail parce que votre domaine n'existe plus, c'est pas c'est pas souvent très intéressant une autre attaque ? Ben c'est l'explication par DNS ça c'est une attaque très souvent qui échappe souvent au DLP traditionnel. Donc les attaquants qu'est ce qu'ils vont faire ?

1:15:23
Ils savent que bon les entreprises qui ont des DLP qui sont en place c'est difficile de faire sortir l'information confidentielle donc qu'est ce qu'ils vont faire ? Comme on peut faire les requêtes et que les requêtes DNS sont pas ne sont pas parties de la portée du DLP normal. Donc je peux faire sortir des informations débris d'informations à travers les requêtes DNS.

1:15:47
Donc je vais faire une première requête DNS. Je vais mettre par exemple l'adresse, le mot de passe avec la requête ça va partir et le serveur de l'attaquant va récupérer l'information. Je vais après mettre une 2e information, donc à la fin il va récupérer les informations, il va aller reconstituer l'information.

Donc oui, si vous avez des DLP dans vos organisations et que ça ne prend pas le DNS, vous pouvez bloquer tout.

1:16:16
Mais il y a toujours un risque qu'on puisse exfiltrer la donnée si vous ne bloquez pas l'exfiltration DNS. Donc il y a plusieurs techniques qu'on peut utiliser pour l'explication. Il y a des outils comme qu'on peut utiliser. Je sais pas si preview arrive à à complémenter ça mais je pense pas qu'ils ont cette puissance. Je sais pas si quelqu'un a l'expérience avec le blocage de l'utilisation DNSDNS avec perview de Microsoft mais ce que je sais.

1:16:45
On utilise des outils comme Cisco ambula pour arriver à à contourner ou arriver à bloquer ces ces genres de d'exfiltration des données. C'est bon ? O K on continue toujours pour ça en en termes de on peut avoir aussi tout ce qui est filtrage de domaine, tout ce qui est surveillant DNS et puis pouvoir faire des des inspections aussi.

1:17:14
Ça peut aider pour l'exfiltration de et empêcher les explications des des DNS. On a d'autres techniques encore qui pour pour sécuriser les DNS qu'on appelle DNS par HTTPS. Donc c'est on va faire la résolution de noms via le protocole D le protocole HTTPS au lieu de passer par le DNS standard.

1:17:40
Ça aide la configuration, l'intégrité, puis ça peut empêcher les écoutes clandestines. Il peut améliorer également les performances. Donc on a un cas ici, au lieu d'avoir le DNS standard sans protection, on peut avoir la protection en ayant du DNS SEC ou du DNS. Des DDNS over HTTPS. C'est c'est 2 techniques je pense. Il y a une 3e technique qui permet également de d'avoir des DNS sécurisés.

1:18:09
Mais juste avec cette technique là, comme vous le voyez avec la requête si j'ai un DNS sécurisé, Ben la requête DNS est chiffrée. On peut avoir du HTTPS chiffré mais ne pas avoir du DNS chiffré c'est différent parce que le la requête DNS vient avant de communiquer avec le site en question. Donc on a le DNS qui est ici, on fait la communication puisqu'on passe par le HTTPS, Ben on est sécurisé. Voici un cas ici où.

1:18:39
On va pas passer par le DHCP, ou on va pas passer par le HTTPDNSHTTPS, on va faire la communication et un autre un attaquant peut être là Man in indol récupérer l'information. Il y a beaucoup de de DNS, des entreprises qui ne sont pas sécurisées parce que qui n'utilisent pas du DNS SEC. Donc si vous avez des des solutions qui sont capables de faire de un peu une reconnaissance, là je vois que.

1:19:08
Il y a beaucoup d'entreprises donc les DNS sont pas sécurisés. Il ne s'agit pas du DNSA, il ne s'agit pas du DNS Over HTP ou du DNS Over TNS. Donc ce sont les différentes techniques qu'on existe pour sécuriser du du DACPDNS. Autant pour moi je sais même pas pourquoi didi je dis DACP régulièrement, on finit avec le DHCP, le le DNS, on arrive sur des protocoles sécurisés.

1:19:39

Le Kerberos, le Kerberos, c'est un protocole qui permet la mise en place de l'authentification unique SSO, donc il est basé sur les notions de chiffrement hybride. Il est basé sur le modèle client serveur tiers. Je pense que vous l'avez vu pendant le cours de Dominique. Il utilise un serveur KDCI qui comprend le authentification serveur et puis le ticket granting Server.

1:20:11
On a le SSH également, qu'on a vu tantôt au niveau de la couche 7, on a le chiffrement de bout en bout avec le SSH, donc qui permet là Allô, c'est juste au niveau de ticket garantie serveur. Parce que si on parle de Golden ticket ou c'est quoi exact, c'est le TGSE, on sait que on a, on a le le Golden ticket pour.

1:20:39
Pour les communications, mais c'était quoi ? Exact ? Je suis un petit peu perdu. Allô, il y a quelqu'un qui qui est en train de parler, mais je te laisse faire des explications. Avant, on a le on a le KDC, on a le TGS, on a le Ah, on a le TGS, on a ce que tu.

1:21:08
Le l'autre élément, non, le TGA c'est différent de ce dont tu parles là si tu veux-je vais, je vais revenir après là-dessus, si on a un bout de temps je vais revenir avec le le kervirus après pour t'expliquer les différents éléments OKOK si si tu si vous me permettez le l'odeur discale c'est vraiment une attaque, un affaire, là au pire tu pourras me, au pire tu pourras me recontacter par après. Tu sais comment me contacter là fait que je je vais te montrer les affaires de la vraie vie.

1:21:38
Ok, on en parle tantôt, je vais, je vais te revenir là-dessus. OK, j'ai pris note, on a le SSH. Le SSH, qui est le chiffrement de bout en bout, permet des tunnels, donc.

1:22:08
Donc le SSA chiffrement. Donc quand on a des communications non chiffrées, Ben on peut l'utiliser pour venir renforcer la le chiffrement. Au niveau de nos communications on a un protocole qu'on appelle signal, ça c'est pas l'application signal lui même. Le protocole s'appelle signal qui fait également des chiffrements bout en bout pour les voir vidéo et texte. Donc il est utilisé pour signal comme application WhatsApp, Messenger et autres.

1:22:34
On a un autre protocole qui s'appelle Secure RPC, donc Remote procédure école sécurisé, donc il fait des appels distants d'une fonction mais avec authentification, parfois avec des chiffrements. On a notre SSL qui est déconseillé. Développé par Nescape, peu importe le la version elle est déconseillée. On a une évolution vers le TLS, l'évolution.

1:23:02
On est on a abandonné le le SSL pour le TLS et les versions recommandées du TLS, c'est le 1.2 et le 1.3, donc il va, il supporte le chiffrement de UDP et puis du Spip pour l'avoir, la voix CIP, la connexion TLS. Donc on avait parlé de signe AD hack ici on va aller plus loin en intégrant les chiffrements au niveau du client et puis du serveur.

1:23:38
Ici quand on a le le acnowledge qu'on a le le signe a qu'on avait dit on avait le acnowledge ou le client, les 2 pouvaient communiquer. Donc le client il va envoyer un un message au serveur, donc il va

lui donner la version de TLS dont il a besoin. Le station ID parce qu'il est déjà connecté, il va le donner au client et le client au niveau du serveur lui va répondre.

1:24:01
Il va donner la la la session ID et puis il va donner le chiffrement avec la version TLS qui va aller avec si ils utilisent un certificat Ben certificat avec le I 509 pour l'authentification et le serveur Hello sera terminé il va revenir le message. Il va avoir maintenant le pre master Keytchange calculer la clé secrète pour leur échange. Ce sera le début de chiffrement et puis dès qu'ils finissent le chiffrement.

1:24:28
Il envoie le message au niveau de du serveur qui lui va également faire le message, chiffrer, retourner le message. C'est comme ça se passe au niveau des séquences de communication. Donc après le signe, là il y a la communication au niveau de de du serveur et du client.

1:24:52
On a le protocole MTLS qui est le mutual TLS qui est l'équivalent client qui est le l'équivalent client authentique TLS. Donc le client lui va fournir son propre X 509 au serveur qu'il pourra valider. Donc entre les 2 il y a une communication, c'est pas juste un côté qui va chiffrer les 2, ils vont chiffrer de part et d'autre.

1:25:15
Donc il est utilisé pour le partage d'informations sensibles. Donc la communication étant chiffrée entre le serveur et mutuellement les les les les : vont chiffrer sont capables de chiffrer l'information. Donc il est utilisé dans vraiment des cas où on a besoin de d'information, de de protéger l'information sensible comme en finance, en santé et autres sur les micro services également.

1:25:46
Toujours dans les protocoles donc on a le challenge Handscape authentification Protocol, donc lui il va chiffrer les noms et mots de passe. Donc l'authentification est fait de façon continue, il protège contre les relais dans les relais ce sont des des challenges qui sont utilisés, donc à chaque fois que il va faire une communication, il va envoyer un challenge.

1:26:11
Il va envoyer un challenge unique et sur certains protocoles, les challenges a souvent été repris, donc lui il protège contre ça. On ne peut pas reprendre le le challenge en question. Les challenges sont les valeurs aléatoires qu'on peut envoyer pour la communication. Ensuite on a le password Authentication Protocol, le pape qui est un standard pour le point au point Protocol, donc lui le nom et le mot de passe sont En clair.

1:26:40
Donc il est moins sécuritaire que le le chap. On a le extensible authentification Protocol, le PAP. Donc lui c'est un cadre qui qui soutient les mécanismes d'authentification tels que les jetons, les facteurs biométriques et les cadres intelligents. Ensuite on a le PAP qui est le protect extensible authentification Protocol, qui est le EAP avec du TLS nom un EAP plus un EAP plus sécurisé.

1:27:18
On a les protocoles multicouches, la sécurité au niveau des protocoles multicouches. Donc lui qu'est ce qu'ils font ? C'est qu'ils vont interagir avec plusieurs couches du modèle. Aussi, comme vous l'avez vu, les différents modèles cette couche eux, ils peuvent utiliser 2 couches, 2 couches ou 3 couches, soit

la couche transport application et le même protocole utilisé partout. Donc quand on avait montré le schéma.

1:27:45
Ça veut dire que chaque couche avec ces protocoles, mais il y a souvent des certains. Il y a souvent certains protocoles qui peuvent agir sur plusieurs couches. Donc c'est le cas par exemple de du protocole DNP 3 qui est utilisé pour les systèmes ICS. Donc lui il va intervenir sur la couche un 2 et la couche 7 donc c'est vraiment utilisé pour les commandes du Squada et puis de la télémétrie industrielle. Donc juste dit que il y a des protocoles multicouches qui existent.

1:28:13
L'avantage c'est que des larges gammes de protocoles au niveau des couches supérieures, le chiffrement, il est incorporé à différentes couches. Et puis la flexibilité et la résilience du réseau. Là sur cette, la flexibilité et la résidence du réseau. Inconvénient, les canaux auxiliaires sont autorisés. Le fil peut être souvent contourné. Il y a une limite de segments imposés qui peuvent être dépassés.

1:28:40
Donc c'est sûr que si on utilise le même protocole sur différentes couches, à un moment donné il peut y avoir, si vous voulez je dirais, des interférences entre les différentes couches. Il est 20 h, on va revenir à 15, on a un peu de temps aujourd'hui, on va revenir à à 20h15 pour continuer.

1:29:52
Émile, merci pour ton lien de rien, puis j'allais rajouter des Silver puis Diamond ticket aussi.

1:31:49
Je sais pas si c'est moi seul, mais je n'entends plus rien. On a la pause. Oh d'accord, désolé.

1:44:49
Allô ? Est ce que vous êtes là ? Ok, on va continuer. Émile, Merci beaucoup pour tes recherches. Je pense à répondre à la question du Golden ticket. Merci Silver ticket Diamond ticket. Merci beaucoup.

1:45:20
Je vais dormir moins bête ce soir OK, on continue pour le True and Shake. La question de hayette c'est bien ça ? Hayette Allô Hayette est là, oui oui je suis là, voilà c'est ça. Oui tu as tu as raison, c'est le True and Shake, c'est ça ? Je sais pas.

1:45:50
Parce que on avait c'était écrit to way établissement de connexion quand je je reviens sur la Slide le 41 OK en fait c'était to way je pense. Comme c'était écrit sur établissement d'une liaison à 200, je sais pas ce qui s'est passé mais il y a un 2 qui s'est retrouvé là.

1:46:16
Le two way n'est n'est pas vraiment utilisé, c'est le two ways. Et puis des fois on parle du four ways parfois, mais dans le cadre de de du Body of Model du Cssp c'est vraiment le le Two ways. Merci pour ta vigilance. On continue.

1:46:54
Donc on était là sur le fibre Channel, on avait le fibre Channel, c'est un protocole pour interconnecter

des systèmes de stockage donc tout ce qui est San sur les réseaux des sur les réseaux NAS jusqu'à 128 gigabits sur l'infrastructure fibre optique et cuve et on a le fibre Channel Over Ethernet.

1:47:22
Qui lui transporte des des trames du fibre Channel sur un réseau Ethernet. Donc c'est moins de de débit par rapport au fibre Channel classique. On a aussi le Internet Small Computer System Interface qui est une norme de stockage réseau basée sur une IP alternative. Donc elle est peu coûteuse par rapport au fibre Channel qu'on vient de voir.

1:47:52
Elle permet aussi le stockage, la transmission et récupération des fichiers indépendants de l'emplacement via des connexions de la wan ou Internet. On a le MPLS qui est le multi multi protocole label Switching.

1:48:12
Ils dirigent des données sur un réseau en fonction de d'étiquettes, de chemins, cours plutôt que d'adresses réseaux plus longues. Il y a d'autres réseaux de qu'on va pas voir comme le RIP et autres. Ils gèrent le ils, ils gèrent les larges gammes de protocole par Capturation donc mettez un ATM from Lee sonnette digital Subscriber.

1:48:41
On a le SDN Software define networking réseau défini par le logiciel, donc lui il sépare la couche infrastructure matérielle de la couche logicielle, donc la gestion des transmissions ou autres. Il permet une indépendance face au fournisseur, la conception et gestion centralisée du réseau. Il va vers la virtualisation du réseau également on a le VX LAN qui est le Virtual extensible LAN.

1:49:08
Donc c'est une technologie de virtualisation de réseau en captulation de type V LAN. Pour tout ce qui est internet au niveau 3, on a des datagram niveau 4 avec le port 47 89, donc il permet jusqu'à 16000000 de réseaux. Logique qu'on peut avoir avec le Virtual extensible LAN. On a les St One également qui sont les Software defend networking in One.

1:49:35
Donc ce sont des concepts de SD One étendus à un One, donc qui va simplifier la gestion et opération d'un One. Il va découpler le matériel de la couche de contrôle qui permet d'optimiser le réseau en réalisant des économies. Il va remplacer puis il complimente le MPLS qu'on vient de voir dans ton trou.

1:50:06
Oui emy, oui j'aimerais revenir au SDM, c'est une notion que je maîtrise un peu moins. Puis j'essaie d'en faire des parallèles. Je veux juste voir. SDM, est ce que c'est l'équivalent comme un serveur enginex en docker ? Donc il y a toutes les.

1:50:32
Toutes les logiciels à l'intérieur de lui même c'est tu ça un SDN ? Ou c'est vraiment une frontière ou une abstraction par rapport à du logiciel ou du matériel ? Je je veux juste essayer de faire le parallèle puis avoir quelques exemples. Moi je dirais que c'est une abstraction des des outils réseaux.

1:50:55
Donc c'est que à travers un logiciel on pourra peut être simuler un switch. En tout cas des équipements réseau qu'on utilise traditionnellement comme mettons des dans Azure ou dans le cloud, on peut mettre du fortunette dans le cloud ou checkpoint dans le cloud. C'est c'est ce genre d'émulation là qu'on fait. Oui oui c'est ça, c'est c'est comme ça que moi je le je le vois, c'est à dire ?

1:51:24
On a de la même façon que tu expliquais les conteneurs et autres si on passe sur le réseau, Ben lui au lieu d'avoir les éléments physiques, Ben on a une virtualisation du réseau qui est là. Donc tous les équipements traditionnels du réseau que tu vois, Ben on va le voir en aspect logiciel plutôt qu'en aspect matériel. OK quand mettons des vignettes ou des.

1:51:50
À des Virtual net ou à des OKOK c'est bon ? J'ai vu à noce n'importe quoi peut être pour. Pour ajouter un peu à ce que vous dites, l'une des manières qu'on peut le comprendre, c'est bon je sais pas s'il y a des gens qui ont déjà fait du réseau intelligent sur la partie mobile par exemple, c'est le fait que le.

1:52:17
Le réseau intelligent est une plateforme plutôt informatique, plus intelligente, donc là où est ce qu'on peut déployer, plus de stratégies. Et puis ils ont des points de contrôle sur les réseaux, les réseaux physiques, donc les réseaux, le Network. Donc quand l'appel arrive, on est capable d'interroger, donc via un protocole spécifique, d'interroger dans le cas du mobile, non pas du SS 7.

1:52:44
D'interroger en fait les plateformes informatiques, de jouer tout un piles de scénarios dont on peut vraiment. Comme c'est un environnement informatique, on peut imaginer tellement de scénarios. Et puis en fin de compte le routage de l'appel. L'ordre est donné par la décision qui sera prise par ce système là. Donc à l'avenir les les routeurs ou les les équipements vont être comme des boîtiers qui vont avoir peut être un petit logiciel.

1:53:09
Qui permet de discuter avec le routeur, le routeur ou le firewall qui est distant. Et puis via ce protocole là l'ordre est donné de laisser passer le trafic, de ne pas le laisser passer de le router dans telle direction ou pas. En gros c'est c'est potentiellement comme ça que ça va être, c'est bon. Merci pour ton additif, est ce que il y a quelqu'un d'autre qui a un point additif à acheter des barres ? Oui oui oui tu te rachètes hein, je t'ai, je t'ai, je t'ai appelé tantôt, t'étais pas là.

1:53:39
Ouais désolé vas y je ouais je vais rajouter quelque chose par rapport à au SDN si on veut faire un parallèle avec la vraie vie. Je sais pas si vous connaissez le produit miraki de Cisco, on va gérer les points d'accès par exemple sur un contrôleur central. L'objectif c'est de séparer le data plane du et du et le contrôle plane qui est nativement dans les outils.

1:54:09
Standards sont gérés dans le même équipement si on prend la suite ou la la, la, le routeur ou le le point d'accès, mais on va séparer le contrôle plane du data plane en en centralisant la gestion sur un contrôleur central. Peu importe, mais il y en a beaucoup de solutions. Mais je fais le parallèle avec la vraie vie. C'est miraqui fortunate ils ont-ils ont ça aussi les Paulo alto, les autres constructions, mais.

1:54:34
C'est vraiment de séparer la la couche gestion des équipements sur un contrôleur central. OK c'est bon merci ça, ça permet de de mieux. Merci la voix sur IP, mais c'est ce qu'on est en train de faire là la, c'est un mécanisme de tunnelage transport transporte la voix et les données de vidéoconférence.

1:55:11
On a les options commerciales et open source. Un exemple, c'est teams qu'on a. Il peut utiliser du matériel téléphonique standard ou plus générique. Donc on a des différents protocoles comme le Real Time Transport Protocol pour le transport audio, vidéo. Et puis on a le site session initiation protocole pour établir, gérer et terminer les appels. Voici P.

1:55:42
On a le Bluetooth qu'on utilise tous la plupart en tout cas, c'est un protocole sans fil de proximité, donc on peut contrôler, faire communiquer notre souris sans fil, notre souris avec notre ordinateur, le clavier l'écouteur tout ça. On peut prendre le Bluetooth, communiquer aussi avec la montre intelligente, avec la voiture. Tout ça donc.

1:56:10
C'est un protocole qui n'a pas une grande portée, vraiment utilisé à proximité. Donc la sécurité c'est un nip qu'on donne qui est qui a un chiffrement faible qui ne peut pas être considéré comme sécuritaire. Il ne peut pas être laissé en mode découverte. Donc on vous conseille pas de laisser votre appareil en mode découverte et n'importe qui peut retrouver votre appareil.

1:56:39
On a le Blue Jacking, qui qui est un exemple d'attaque, donc il peut faire pousser, pousser un message. Plus de contrôle de l'appareil. Il n'est plus présent dans les versions récentes, donc avec les les versions récentes du Bluetooth on peut plus faire du Blue Jacking. Les versions restantes du Bluetooth qui protègent contre le Blue Jacking pour les classes de Bluetooth, Ben on a.

1:57:05
Les la les puissances qui sont là. Et puis on a les types de ranch qui sont là, donc il y en a un qui peut aller jusqu'à 100 M, il y en a un qui s'arrête jusqu'à 0 50 demi mètres. En fait on a les le zip qui est basé sur le du IE donc personal Arian Network donc qui a une portée d'environ 10 M comme le Bluetooth donc il a une clé de de 128 bits.

1:57:37
Il est partagé par centre de confiance. Il conserve la clé réseau, fournit une sécurité point à point l'appareil. Les appareils n'acceptent que des communications provenant d'une clé fournie par le centre de confiance. Est ce que parmi vous, il y en a qui ont déjà utilisé le Zig B peut nous partager son expérience. Est ce que quelqu'un a déjà utilisé le le Zig B Moi je l'ai, je l'ai jamais utilisé. Est ce que il y en a parmi vous qui l'ont utilisé ?

1:58:12
OK continue. Il y a isaïe qui dit que c'est beaucoup dans le IOT, donc en tout cas moi je l'ai jamais utilisé. Ensuite on a les radiofréquence identification donc de RFDRFID, donc ce sont des champs magnétiques. On en a vu quand on faisait la sécurité physique hier, donc on a des champs électromagnétiques pour identifier et suivre automatiquement les étiquettes attachées aux objets.

1:58:41
Donc on a les étiquettes transformation, transport, transpondeur, radio, minuscule. On a les émetteurs récepteurs actifs, on a des transporteurs d'impulsion, d'interrogation, donc étiquettes, donc ils respectent la norme ISO 14 443. On a souvent des étiquettes là-dessus comme vous voyez la piste ici, on a l'antenne qui est à l'intérieur ici.

1:59:09
On a l'antenne qui est là, on a des puces qui sont intégrées dans les lecteurs, dans les, dans les cartes, on a les metteur, les puces électroniques, surtout dans le rfd. Les puces électroniques contiennent un identifiant et éventuellement des données complémentaires, donc qui sont utilisées dans les passeports et puis souvent pour les inventaires.

1:59:38
L'enjeu de sécurité, Ben on a la violation de la pluie privée quand on arrive à récupérer, puis on peut reconstituer certains éléments. Les puces se répondent toujours aux requêtes, donc mes les informations stockées sont limitées car souvent associées à une base de données. Il peut y avoir un protocole, des clés, peut avoir des inférences possibles. le NFC donc lui c'est l'univers fuel communication, donc il est c'est un RFD.

2:00:10
RFID à très courte portée, dont 10 cm, c'est l'extension du 14 446, donc l'utilisation des cartes de paiement, des titres de transport, des clés sans contact en jeu de sécurité. Il est insécure mis à part la proximité mon Enemy middle ou écoute de communication mise à jour des des dispositifs.

2:00:37
On m'avait expliqué le type d'attaque que les gens faisaient, c'est à dire quand vous voyez des pays pas sur les les cartes de crédit il y a, il y a souvent des protections qu'on peut mettre contre les contre, les les le NNFC. Donc souvent les attaquants, qu'est ce qu'ils faisaient ? Ils avaient des terminaux pour les paiements, donc ils passent souvent vers les les sacs à main des personnes.

2:01:05
Et les terminaux récupèrent automatiquement le le paiement. Donc souvent il y a certains types d'attaque qui étaient menés. Et puis bon, très souvent c'était dans les lieux publics. Je sais pas si vous en avez entendu parler de ces types d'attaques là avec les les terminaux de paiement, est ce que est ce que il y en a un qui ont qui ont déjà vu cette expérience là ou malgré tout ?

2:01:35
Oui j'ai juste j'ai juste entendu parler mais je l'ai pas vécu. Mais aussi moi j'ai j'ai quand même remarqué avec certains amis qui activent leur carte là sur leur téléphone ils font des paiements, ils se retrouvent à avoir des retraits sur leur compte sans avoir sûrement. Ils passent par des des genres de trucs là donc.

2:01:58
Moi c'est pour ça, j'ajoute jamais ma mes mes cartes pour nous payer directement sur les pointes au sel. Là donc c'est c'est des choses qu'ils peuvent activer et si toi t'as la carte est activée, ça le prend en charge. Oui mais tu tu peux faire, il y a des protecteurs NFSNNFC que tu peux mais tu t'es tu, tu peux mettre tes cartes dedans pour ne pas qu'on puisse les les faire passer sur un terminal de paiement. Ton bien sûr.

2:02:28
Il y a des protecteurs qui existent pour ça. Oui, mais souvent maintenant les gens on les met par exemple sur le téléphone, là genre on dans la pochette entre le téléphone et la couverture, donc on se rend pas compte en fait. OK c'est vrai c'est ça, mais chose Jonathan, oui moi je voulais juste rajouter.

2:02:50
Justement là ma, ma, ma conjointe, l'année passée elle avait voyagé et quand qu'on est à l'étranger puis qu'on utilise, tu sais, mettons notre notre cellulaire pour payer, il y a plus de chance que la carte elle soit bloquée que si on prend notre carte physiquement et qu'on la rentre dans la machine. Donc j'imagine, il doit y avoir des calculs de risques donc j'imagine pour eux il y a plus de risques d'avoir de la fraude là quand que c'est un paiement, là tu sais avec le RFID là donc OK.

2:03:18
Donc en tout cas si vous voyagez puis vous voulez pas vous faire bloquer la carte, Ben utilisez la la carte physiquement c'est c'est beaucoup, c'est mieux de c'est ça là avec le chip Là t'as t'as moins de chance de faire barrer la carte OK mais bon merci beaucoup Nasser tu as mis sac faraday, est ce que ça existe ? C'est réellement ou c'est un joke ? Oui oui c'est des petites pochettes faraday pour éviter que ce.

2:03:42
Les gens retirent ton sur ton portefeuille sans que tu saches parce que ce qu'ils font en général c'est il prend un terminal de vente puis TPV, puis ils mettent un montant puis ils passent devant toi 10,00$ 20$ sont partis en fumée alors c'est au plus là. Mais maintenant avec avec l'augmentation des limites c'est je crois que y a certains cartes de crédit peux tu peux aller jusqu'à 300$ alors 300$ c'est beaucoup d'argent là. Alors tu peux mettre ta ta carte dans un sac faraday.

2:04:12
Puis une pochette phare AD aussi, ce qu'on appelle pochette phare. AD, ça va, ça va protéger pour les téléphones, j'ai aucune idée, OK c'est bon, merci Marc Vince, oui vas y je t'ai pas entendu, ça fait ça fait 2 séances que t'avais pas parlé hein. Allô ? Oui oui, je disais que ça, ça faisait.

2:04:38
Oui la parole à toi. J'ai dit que ça faisait 2 séances que tu n'avais pas parlé donc tu tu tu tu peux doubler le temps que tu voulais utiliser. Aujourd'hui prends tout le temps qui reste dans le papier aluminium donc ça OK les les les ondes électromagnétiques OK donc ça ça marche également hein. Oui je sais jamais, OK ça marche, mais il y a un type de de papier d'aluminium qu'il faut utiliser. Les policiers l'utilisent déjà.

2:05:06
Il y a un type de papier, c'est pas tous les types de papier d'aluminium que je peux utiliser parce qu'il y a un pesseur ou une norme qu'il faut utiliser. Je me rappelle pas bien OK mais ouais c'est c'est vrai OK c'est beau merci. Ah je j'appris beaucoup de choses aujourd'hui, merci. On continue donc on continue toujours avec les communications donc on a le lify.

2:05:37
Comme un peu le Wifi qu'on connaît. Donc c'est une technologie de communication sans fil qui utilise la lumière émise par les lampes à LED pour transmettre des données. Donc il est similaire au Wifi,

donc il fait 100 gigabits par 2nde, donc il est utilisé dans des zones sensibles. Au RFI, on a maintenant le Wifi, qu'on connaît les fréquences.

2:06:05
Qui sont les plus utilisées ? C'est 2.45 Giga 5 Giga hertz donc il peut utiliser le le CSC ma CA ce sont des protocoles je pense. Pour contre les collisions d'informations peuvent contrôler éviter les collisions, les techniques de gestion des fréquences. On a 2 techniques qu'on peut utiliser je pense, il y en a 3 et on évoque juste les 2.

2:06:34
Il y a le direct séquence Sprint Spectrum. On va donner plus de détails dans le prochain Slide, donc lui c'est le code séquences pour repartir des données. On a le octogonal Fréquenti dirigeant Multiplex donc qui lui il va découper en plusieurs supporteuses octogonales les informations.

2:06:57
On a le Sprint Spectrum, donc le Sprint Spectrum, lui, c'est l'étalement des fréquences du signal transmis. Donc comme vous le voyez ici, on a le signal qui est sur une petite, une petite bande ici qui est épais mais qui va prendre plus de puissance. Et là on a un signal qui va prendre moins de, qui va prendre moins de puissance mais qui va s'étaler sur de la fréquence.

2:07:25
On diminue le risque d'interférence avec d'autres signaux, donc accès multi d'une même bande de fréquence par plusieurs utilisateurs. Il est équivalent d'une communication parallèle, donc la communication identifiée par son code ou sa fréquence de saut. Donc très souvent les cas d'utilisation, on a souvent des radios, les radios FMAM qu'on peut utiliser des fois bon pour les bandes courtes bandes larges, on a.

2:07:52
On a parlé du, du, du, du Wifi et du Bluetooth et autres qui peuvent utiliser tout ce qui est DSS spectre DSS qu'on peut utiliser, qu'on a vu tantôt là le DSS. Donc il utilise l'ensemble des fréquences disponibles simultanément, donc l'augmentation de la base disponible, disponible, disponible. Il est utilisé pour le CDMA, le DG, le 802 11G, le GPS qu'on utilise tout le temps.

2:08:25
On a le OFDM qui est la répartition en fréquence protogonale dont on avait parlé. Donc son cas d'utilisation c'est le LTE, le réseau téléphone, le 802 11AGNAC, on a le 8 mars, on a le 5G également. Donc ça c'est les standards qui lieu, les années d'adoption qui sont là, les fréquences qui sont utilisées.

2:08:54
Le maximum de de données et puis le le ranch qu'on peut avoir. Donc plus vous remarquerez que plus on a des données, un volume de données maximum qu'on peut faire partie la la portée si vous voulez la portée n'est pas très élevée. Bah la portée, la portée ou non. Autant pour moi ce que je suis en train de dire, je suis en train de rencontrer des.

2:09:22
Des choses incohérentes y a pas de j'ai, j'ai y a pas de cohérence entre ça parce que le 505 cents pieds il est moins que aidez moi avec les pieds, les mètres je je m'en sors pas trop, mais je sais que 1000 pieds il est moins que 1000 M, il est plus élevé que 1000 M, c'est ça hein ? Et 1000 ? Et j'étais en train

d'essayer de faire quelqu'une dans ma tête là, 1000 pieds, 1000 pieds je pense, un pied, un pied c'est douce, un pied.

2:09:53
Ouais puis un pouce 2.5 cm OK donc c'est ça, j'aurais dû convertir ça en en mètres. Mais bon en gros ça ça donne une idée un peu de de l'année d'adoption, les fréquences, les les Max et range puis les les données qui peuvent être transmises par les différents standards de IE.

2:10:19
Donc on a les différentes versions de Wifi qui sont la Wifi 6 qui lui prend le 800 de 11 à X en 2000 venu en 2019. Donc on a 10 gigabits par 2nde donc la vitesse est plus élevée donc il fait jusqu'à 1000 pieds. On continue, on a le SSID qu'on connaît.

2:10:39
Tous qui permet d'identifier un réseau sans fil. Donc quand vous on a un réseau sans fil, généralement on met le nom qu'on veut, on peut mettre attention ne pas hacker. Donc c'est le nom de notre réseau Wifi. Quand vous mettez ça, généralement on on va vous hacker hein ? Donc ne ne vous jouez pas les dangereux quand vous mettez les noms de vos SSID, il permet de différencier les réseaux.

2:11:03
Puis ne pas garder des SSID par défaut du manufacturier il peut être visible ou non visible. Attention c'est pas parce que c'est pas visible qu'on peut pas on peut pas voir. Donc avec d'autres appareils poussés on peut voir, on peut voir le signal, on peut voir votre SSID, on a. On va parler maintenant des clés qu'on peut utiliser au niveau de de Wifi. On avait le web qui était là.

2:11:32
Qui lui utilisait le RSC 4 qui est obsolète maintenant. Plus de 64 bits, plus de chiffrement, 44 Bleus, plus les vecteurs d'initiation. Il était facile facile de retrouver la clé en en analysant le le IV 5, il transmet En clair 24 bits, pas assez long. En communiquant, l'attaquant génère à la demande des IV.

2:11:58
La clé unique est partagée. La clé unique est partagée, pas de vérification des séquences les vulnérables aux attaques passives éco depuis actives injection. Donc je présume que personne n'a son protocole qui est de son suffrement qui est issu du web actuellement parce que c'est pas sécuritaire. Après on passe à du web qui lui est venu corriger les faiblesses du web.

2:12:26
Avec le 802 11I, on est passé à au 8 au web 2 donc lui il utilise un TKIP donc qui est vulnérable aux attaques back Trent, donc il avait une clé de 64 ou 128 bits pour l'accès initial. Puis chaque paquet utilise des clés de 128 donc il était basé sur RS 4 qui lui est obsolète, donc il a été déprécié par le web 2 donc.

2:12:54
On laisse le web 2, on laisse, on laisse le WAP 2, le WPA. On laisse également le WAP. On a le WPA 2 qui implémente les exigences obligatoires de 802 11I. Il utilise le CCMP basé sur du AES. Le CCMP, c'est le counter mode du CBC Mag Protocol, donc le counter mode cipher block chain message.

2:13:24

Il a une taille de 168 et puis 256 bits. Donc on on va sur quelque chose qui est quand même sécuritaire. On a le WPA 3 qui utilise le CCMP du WAP 2 et puis du jeu du A et S 128 quand on est en mode CCMP et puis et puis du jeu du 256 quand on est en mode GCM.

2:13:48
Qui est le galois compte Motte, donc on avait le CCM qu'on a dont on a donné la définition, tantôt merci, tantôt le GM, lui c'est le galois comté Motte, tantôt on parlait de quand on parlait je crois. Il y a il y a quelqu'un qui parlait de de SSS 7 et puis il avait parlé du diamèter.

2:14:15
Le diamèteur, lui, il authentifie l'utilisateur ou des dispositifs, donc il va utiliser un serveur d'authentification et il va capitaliser l'infrastructure en place et une évolution du radius. Donc comment ça se passe ? Donc ici on a un supplicant, on a le supplicant ici que qui lui vient d'utilisateur qui va chercher à communiquer.

2:14:43
À travers le E pôle, donc avec le E pôle il va aller au niveau de l'AUTHENTIFICATEUR, il va envoyer la requête l'authentificateur, il va relier cette requête sans traiter. Il va à travers le le Diamateur donc le diamateur lui il va encapsuler le message EAP dans.

2:15:09
Dans le diable, au niveau du serveur d'authentification donc il va exécuter la logique de vérification de mots départ des certificats et autres, donc il va retourner le message, accepte s'il accepte que il soit authentifié, si c'est bien l'utilisateur ou le supply plain ici qui est authentifié, qui a demandé l'authentification, donc dès qu'il est authentifié il va donner le accepte, accepte pour que la communication puisse se faire et au niveau du droit il pourra communiquer si.

2:15:37
C'est une personne qui a pas le droit de faire la connexion, Ben il va lui donner un rejet pour ne pas qu'il puisse être connecté, donc il pourra pas faire l'opération au niveau du droit. Donc c'est le même principe généralement d'authentification, on va passer par le serveur qui authentifie, on fait la communication, on envoie nos identifiants, nos paramètres de connexion, il il nous vérifie. Sachez qu'on est la bonne personne, qu'on a le droit de.

2:16:05
D'aller vers le système ou la ressource qu'on veut utiliser. Et là en ce moment on aura accès. Mais si on n'a pas, on n'a pas les accès nécessaires ou on n'est pas la personne qui doit être qui doit avoir l'authentification, Ben on sera rejeté du système. Donc c'est le même principe que tous les systèmes d'authentification, les attaques qu'on peut avoir au niveau du Wifi. Donc on a le World Driving qui lui.

2:16:33
Il va rechercher activement le signal réseau sans fil avec des outils qu'on peut avoir. On on peut se promener dans le quartier, voir tous les Wifi actifs qu'on a. On a le on a le clair City qu'on va qui va nous permettre de marquer les zones avec des signaux. Donc signalement public, donc quelqu'un passe dans le quartier. Il a remarqué tous les Wifi qu'on peut pirater.

2:17:01
Donc il va mettre un signal pour que facilement on on puisse le trouver. Et souvent ça peut être un code entre ces ces personnes là, entre les les malfaiteurs. Nasser, oui, juste pour le dire, mais là je je

viens de trouver pourquoi il est utilisé dans les téléphones cellulaires. C'est juste pour la communication LTE des données, et cetera. C'est pas ce que je pensais avant là.

2:17:28
C'est je veux partager de le l'article F 5 qui parlait de ça. Merci mais est ce que la personne qui avait posé la question sur le SS 7 est ce qu'il a trouvé la solution ? C'est moi oui c'est moi qui a posé la question, j'ai trouvé la réponse mais mais est ce que le SS 7 il est encore utilisé ou pas ? Ouais il est toujours utilisé. Ouais mais c'est pas tous les protocoles, je j'ai pas fini encore là mais mais c'est pas tous les les les les compagnies de cellulaire qui l'utilisent.

2:17:57
Mais c'est toujours dans certains pays déjà c'est toujours utilisé je crois, même au Canada c'est toujours utilisé, mais le seul que je crois qui qui veut se qui veut débarquer de ça c'est quoi c'est Rogers pour l'instant, mais j'ai pas toutes les informations malheureusement, j'ai pas tout en fait c'est le le changement, c'est pas aussi facile que ça, ça demande beaucoup de les gens préfèrent gérer le risque de tout changer. Ouais Brou vas y.

2:18:27
Maurice, ce que je voulais dire, on on t'entend mal hein, on t'entend pas très bien, on on t'entend pas bien. Allô ? Oui, est ce qu'on m'entend ? Oui oui, on t'entend mieux maintenant, ça va. Je disais en fait que le le SS 7, c'est un peu un protocole analogique sur la partie mobile, avec les réseaux, les réseaux intelligents, les réseaux de facturation.

2:18:53
Et en fait son remplaçant devrait être le diameters qui est plus en fait IP. Donc il y a certainement il y a il y a il y a d'autres protocoles qui sont en train de venir avec la de de l'i MS et de et de et de la 5G. Donc il y a des nouveaux, des nouveaux protocoles en cours mais. Mais le SS 7 l'est carrément analogique. Et puis comme les les collègues sont en train de le dire, là c'est des protocoles.

2:19:21
Probablement en cours de de décommissionnement dans les années à venir, c'est ça ? Merci pour ta contribution. Toi tu es notre expert Telecom, tu nous donnes beaucoup de d'informations Telecom. Merci. Donc je parlais, on parlait des des différentes attaques, on avait parlé de White Raving graffiti, on a des attaques par régie donc c'est la réalisation de de paquets capturés.

2:19:45
Donc pour l'authentification pour, dès que on a un paquet, on essaie de le réjecter pour mettre le système en confiance. On a les attaques un instant, on a les attaques V 5V, 5 attaques qui permet la reconstitution de la clé via la répétition. Donc la valeur c'est une valeur qui est le 5, là c'est la une valeur qui est ajoutée au chiffrement. Donc il était utilisé pour le web généralement.

2:20:16
On a des points d'accès indésirables les rogues donc qu'est ce qu'on peut faire. On peut mettre des points d'accès pour juste tromper les gens ou amener les gens à à aller utiliser les ces réseaux là pour pour essayer de prendre la communication qu'ils font. C'est comme dans un dans une bibliothèque. Bon ça ça ça va être un peu comme le.

2:20:45
Le SSA le le jumeau maléfique là eventuin. Mais pour le le point d'accès indésirable, si un attaquant

veut récupérer des informations de d'une personne, Ben il va peut être mettre un réseau wifi gratuit. Et puis quand les gens se connectent vont se dire Ben il y a un réseau wifi qui est gratuit, les gens vont utiliser alors que lui puisque la communication Ben il peut ne pas être chiffré donc.

2:21:10
Il est capable de récupérer beaucoup de communication qui se passe dans le réseau sur le sur le réseau en question. Il pourra mettre des systèmes comme des wareshats, d'autres outils pour écouter la communication et puis récupérer des informations. Ensuite on a une autre type d'attaque qui est le Evil twins qui est un jumeau magnifique donc qu'est ce qu'on fait ? On peut forcer la connexion à celui par le Clona du SSID ou du ABCID donc qu'est ce qu'on fait j'ai.

2:21:40
Je je suis dans une bibliothèque où je suis dans une entreprise. J'ai besoin, je vais les attaquer. Ben je vais cloner le SSID et amener les utilisateurs à aller vers ce SSID là. Donc puisque je maîtrise je je maîtrise les paramètres où je peux accéder en fait à ce routeur ou au flux de communication. Ben je peux récupérer ce que je veux avec ces communications là.

2:22:08
On est arrivé maintenant sur les satellites. Ben les satellites ils permettent la la connexion internet, ils contiennent beaucoup de latence, donc temps aller retour c'est des hautes fréquences direction, c'est des hautes fréquences qu'on utilise. Donc l'exemple par exemple du du STARLINK. On a beaucoup de satellites, environ 3271 je crois dans le projet, on veut aller jusqu'à 7500.

2:22:36
Le temps de l'attente c'est 60 millisecondes à 35 millisecondes par basse orbite. Pas parce que les c'est pas sur des des méhos, c'est vraiment sur des léos, des orbites qui sont pas très loin. Donc on est sur du 500 à 2002 1000 km. Donc stalink devrait être mondial mais un peu accessible partout.

2:23:02
Est ce qu'il y a des questions ou certains veulent nous parler du projet ? Vous en savez plus sur les les satellites, vous vous pouvez nous en dire plus ? Oui tu avais la main levée, est ce que c'est une ancienne main ou c'est une nouvelle main ? Oh désolé c'est une ancienne main. OK parfait continue les cellulaires.

2:23:32
Donc le cellulaire c'est la réutilisation des mêmes fréquences dans des zones donc qu'on appelle cellules. Donc ça a été initialement quand les réseaux de téléphonie mobile sont arrivés, Ben on les a appelés des réseaux cellulaires, qu'on qu'on on tient le nom en fait de ça, de ce concept là. Donc vous allez voir ici, les pylônes sont dans des sont à certaines zones, ils vont couvrir cette, ils sont placés à certains endroits, ils vont couvrir certaines zones qu'on va appeler des cellules.

2:24:00
Et il y aura des relais entre les différentes cellules. Donc on a la cellule qui est là, on a le la pylône qui est là ou l'antenne qui est là qui couvre une cellule. Et là où elle s'arrête, Ben il y a une autre antenne qui va récupérer jusqu'à couvrir une ville, un pays et puis courir tout un tout un continent. J'espère que c'est pas le seul réseau cellulaire qui couvre, mais c'est un peu le principe de cellules grandissantes.

2:24:27

Donc on on a plusieurs classifications dont on a les micro sels qui peuvent aller à 2 km et plus, on a des micro sels qui font 200 M, on a des femto sels qui font 100 M et puis on a des ato sels qui eux font environ un à 4 km. Mais à tout CEL ça peut vraiment être dans des avions ou des trains où on peut avoir ce genre de réseaux là. Et puis peut être le micro sels peut être dans la campagne ou dans dans une ville.

2:24:57
Donc comme vous voyez les différentes technologies ici. Donc au départ on a commencé avec du NMT, donc avec qui faisait du NG le GSM qui a commencé à faire du DG. C'est là que il y a eu la vulgarisation de des de la téléphonie cellulaire. On a eu d'autres protocoles qui s'appellent idem le TDMA, le CDMA qui étaient toujours du du DG et on a lu après le HS.

2:25:26
CSD du 2.5 le GPRS du 2.5 à l'époque, avec les GPRS, je pense que il y a il y a plein qui peuvent témoigner que quand on a commencé à avoir les communications vidéo et puis aujourd'hui ce qu'on voit c'est c'est vraiment hallucinant, c'est que à l'époque, quand tu envoyais des données, ça prenait tellement de temps. Maintenant pratiquement on on fait tout en temps réel sur notre téléphone. Tout ça donc.

2:25:56
Et ça en moins de peut être 20 ans. On a on a vu toutes ces évolutions là donc c'est vraiment hallucinant tout ce qu'on voit avec la technologie. Ensuite on a évolué. On est arrivé dans du 3G avec du WCDMA, du Edge, du 3G, du Deg, du EMTS avec du 3G, du HSSASPDA avec du 3.5.

2:26:21
On est arrivé avec du 4G du 8 mars, on a du LTE, beaucoup je pense au Canada ici et on est on tend vers la 5G maintenant, du 4G, génération 4G, 4GINT Advanced Standard qu'on on vers ça, qu'on est en train de de tendre la 5G elle c'est grande diversité d'antennes bidigationnelles, c'est une nouvelle bande de fréquence, 6 giga hertz, 26 giga hertz ?

2:26:52
Convergence wifi et cellulaire donc on a des accès multi non orthogonal qui sont des non a soutiens réseau défini par logiciel dont RDSTN. On a des hauts débits, des faibles attentes, des résiliences des c'est des IOT Ready donc qui sont vraiment designés pour l'utilisation des IOT. C'est vrai on a des enjeux de sécurité qui sont là qui sont pas très connus pour le moment parce que pas vulgarisés.

2:27:20
C'est sûr que chaque nouvelle technologie vient avec ses risques de sécurité au niveau de de la 5G. Le Networks Racing, comment est ce que il est structuré la la 5G au niveau de on a l'infrastructure layer qui lui va regrouper tout ce qui est base physique, communication, traitement de données et autres. Donc on a la radio Access Network, on a le transport Network, on a le Core Network, donc ça c'est l'infrastructure d'ailleurs.

2:27:55
On a le Network fonction layer, donc on a le Network fonction qui lui est la logique du fonctionnement. Donc il aura des fonctions logicielles comme la gestion des sessions, les QOS, le pare-feu, l'authentification, les DNS, tout ça. Et on a le le Network operation qui lui va faire la surveillance, la gestion, la location des ressources, les réseaux, les bandes passants, la priorité et autres. On a le service layer qui lui va fournir les services.

2:28:23
Donc on pourra avoir les Virtual mobilier pour État, donc tout ce qui est opérateur de mobile, la téléphonie classique, mais aussi avec la 5G. On va à un certain niveau. Donc on pourra avoir des fournisseurs spécialisés de Turn Party qui pourront qui pourront être des fournisseurs de santé au niveau de des domaines de la santé, industrie, des Smart City qu'on pourrait avoir et on a.

2:28:49
Un autre composant qui est le dans le Network Controller Network Side Controller qui lui comme le dit C'est l'orchestrateur donc il va attribuer, il configurer, il surveille les ressources, les questions, les questions des additifs. Moi je je je. Je voulais juste ajouter que les réseaux Walmart et CDM Max c'est des réseaux mobiles pour le fixe OK ?

2:29:20
C'est des oui c'est de la radio pour le fixe, la partie OK pour le téléphone fixe c'est ça hein ? Pour le pour le réseau fixe exactement. OK c'est bon, merci j'ai des questions. Jonathan, OK la la carte des satellites starling que tu partages avec nous, c'est ça ?

2:29:54
Oui d'exact là c'est dans le fond, ça montre la la quantité de satellites, là je pense qu'on c'est ça, il y a d'autres choix, là on peut voir d'autres sortes de satellites là, mais le premier là comme là on peut voir les c'est les starling que ça monte à à l'écran là donc c'est impressionnant là de voir c'est là qu'on pense que ça, ça fait peut être un peu de pollution hein dans dans l'espace OK je pense qu'on est ce qu'on peut agrandir.

2:30:28
Tu tu dis que les staling sont des quelles couleurs ? Allô, je crois que c'est tous les points là qu'on voit à l'écran. Les Blancs c'est c'est tous des des starling, là OK. Puis si on clique en haut, mettons là tu sais globalstar ou GPS, Ben là on va voir, toutes les points vont changer pour.

2:30:47
Les autres satellites là voir les les les satellites on peut voir que les comme là le GPS on peut voir qu'ils sont beaucoup plus distants. Aussi on peut voir que starling sont en moyenne à 500 km de la terre, fait qu'on voit qu'ils sont beaucoup plus proches. OK Wow OK Ouais.

2:31:16
Je sais pas, je sais pas si j'ai bien compris le collègue qui est passé juste avant le Monsieur qui a présenté les réseaux statiques, il a dit les les réseaux c'est il a dit CDM Max c'est quoi ? C'est pourquoi il dit c'est c'est pour les réseaux, c'est pour les téléphones fixes en fait c'est pas pour le oui c'est ce qu'il a dit Moïse c'est ça hein ? C'est ce que tu as dit à Moïse n'est n'est pas là.

2:31:44
Mais parce que moi j'ai peut être je peux me tromper mais je sais que vas y vas y oui wimax c'est c'est une technologie de de transmission de données sans fil mais dont dont la distance est est très grande, c'est c'est 2 rayons, peut être de 4 des antennes ça peut, ça peut pulvériser à 80 km. Maintenant la réception d'un signal Wimax se fait à partir d'un dispositif ou bien d'un routeur Wimax qui va récupérer le signal qui va transmettre en wifi. Et bien que c'est une technologie pour les téléphones sans fil, ça je savais pas que ça existait déjà, mais parce que ce que c'est.

2:32:14
C'est que c'est 8 Max, c'est les antennes qui arrosent sur un rayon de couverture assez grand c'est 80 km et plus donc après ensuite maintenant il y a une antenne, il y a une un routeur 8 Max qui récupère le signal qui distribue, donc c'est juste 8 Max Hein la la différence d'ailleurs font beaucoup la différence entre 8 Max et 8 faits au niveau de la portée du signal et la zone de couverture. Dire que c'est un c'est pour les téléphones sans fil ça je savais pas. Ouais puis si je peux rajouter moi dans le temps.

2:32:42
Et quelles années de ça ? Je Bell offrait des Routeurs Wimax quand j'allais dans la bibliothèque et ça ne me tentait pas d'aller me brancher sur des réseaux sans fil de bibliothèque uhum et que le téléphone était genre encore à 2.5G, j'apportais mon routeur wimax avec moi et que je connectais directement à mon ordinateur, puis j'avais mon sans fil sans principal réseau de la bibliothèque.

2:33:06
Exactement parce que le les antennes de couverture sont assez grands donc ils ont besoin d'être exactement. Je pense que c'est pas c'est pas adapté. Je pense pas que ce soit adapté pour les téléphones fixes non je pense pas juste juste juste pour ça, mais c'est c'est un cas d'utilisation que seulement Moïse avait donné. Et toi tu donnes un autre cas d'utilisation ? Merci on continue. Connexion fixe, antenne fixe, connexion mobile similaire OK.

2:33:36
Oui à mamie, oui en fait j'ai partagé, j'ai partagé ici justement fixe mais également le Walmart en mobile. Les 2 formules existent, OK donc dans le chat donc une une une image qui explique un peu cela, OK, donc on discute sur un chiffre 9 selon la position des gens, l'autre me dit que c'est 6, l'autre dit que c'est c'est 9, c'est bon, tout le monde a raison, personne n'a tort, OK ?

2:34:07
Ok on continue, je pense que on a, on a fini les slides hein. Donc le dernier c'est le réseau de distribution de contenu. Donc on a un service qui est déployé dans des centres de données afin de fournir une faible attente, des performances élevées et haute disponibilité de contenu hébergé.

2:34:30
Donc il fait comme un load balancing géographique, donc on a des des fournisseurs comme quad, fleurs, acami et BitTorrent. C'est le le dernier slide que j'avais parce que je me disais que on en avait trop, mais apparemment il nous reste encore 25 Min. Soit je je désactive mes autres slides en avance jusqu'à ce qu'ils soient l'heure ou bien.

2:34:58
Je vous laisse le reste du temps s'il y a pas de questions. Et puis on va se retrouver la semaine prochaine donc qu'est ce que moi moi je voterai pour l'option 2 ? Je pense que la journée a été assez longue comme ça, donc on peut aller se reposer si vous permettez non mais s'il y a pas de questions on a je vais vous donner les 25 Min. Est ce qu'il y a des questions ? Est ce qu'il y a des questions ?

2:35:26
Pour ce la le cours de de réseau il nous reste encore une trentaine de slides à terminer je crois un 30 ou 40 slides à terminer et pour la prochaine session on va terminer ce cours. On va revenir sur les

principes de l'examen CSSPI, comment est ce que vous devez faire, comment de vous ? Comment est ce que vous devez vous préparer ? Oui pour l'examen final, OK l'examen final.

2:35:56
C'est le 9 non ? L'examen final c'est je pense c'est la semaine d'après que la semaine après le 25 c'est le 2 juillet. Je crois qu'il y avait un temps qui a été déplacé la dernière fois que c'est ça, puis que qu'est ce qui a, qu'est ce qui a été déplacé je pense c'était le 9 juillet il me semble. Ouais, l'examen c'était le non. L'examen c'est le 2 juillet.

2:36:26
En tout cas ce que moi j'ai c'est le 2 juillet. Qu'est qu'est ce que vous aviez discuté avec Dominique ? Il y avait un décalage, on est en en en cours là parce que il y avait le le cours CEH et le cours CSSP, puis il y avait un décalage, puis je crois que c'est le 9 juillet, OK, l'examen final le 9 juillet, moi c'est que OK, moi ce que j'ai dans mon dans mon calendrier.

2:36:53
Il me reste en réalité si si vous voulez après le cours d'aujourd'hui 19 aujourd'hui il me reste un cours off. Je sais même pas pourquoi le tout ne ressort pas un instant. Ok, il y a un cours, il y a une une séance de révision de mémoire. Alors enfin ce qui va donner le 9 juillet.

2:37:19
De de de ce que j'ai compris des profs, là OK, le l'examen c'est le 9 juillet, c'est ça ? Ouais OK donc moi j'avais une planification différente, c'était le 2 juillet que j'avais ici, parce que là j'ai posé la question, pas hier parce qu'hier je je de mémoire, tu parlais comme l'examen le 2 juillet, puis je voulais marquer. OK, mais c'est Dominique qui nous a dit de c'est le 9.

2:37:46
OKOK c'est pas grave, il me reste en réalité 1/2 cours de sécurité réseau, le 4B sur que le reste. Et puis on va reparler des des éléments de l'examen. Non la prochaine session du 25, on termine le cours de sur le réseau, on revient sur les recommandations pour l'examen et puis si vous voulez dans la la le 2 on pourra faire peut être une une révision.

2:38:15
C'était pour moi c'était l'examen. Mais si c'est pas l'examen on pourra faire une révision. Et puis le 9 où vous allez faire votre examen c'est bon c'est bon, correct le 9 non ? Je vois dans le moodle. Je vois dans le moodle que c'est le 9.

2:38:41
Mais moi j'avais une planification, j'avais une première planification que j'avais reçue. C'était le le le 2. Mais c'est pas grave. Dès que on ça a été décalé sans, ça a été décalé, sans que on mette notre planification à jour sûrement. Je pense que je pense que le prof je pense de mémoire a dit que le 2, mais ça devrait être normalement une séance où tu allais comme nous entraîner pour nous préparer un peu à à l'examen du CSSP.

2:39:09
Pour montrer à peu près comment est ce que il faut se préparer en fait. Et puis on allait avoir un échange avec toi pour avoir un peu plus d'idées. C'est pour ça qu'il a mis comme révision préparation de l'examen mais je pense c'est examen CSSP c'est ça justement c'est ça que moi je comptais faire le

25. Ah OK mais voilà c'est ça dans ma planification puisque le en réalité le le cours le cours il finit le le cours. Il me reste juste 30 ou 40 slides pour terminer le cours.

2:39:39
Et il y a il y a une autre, il y a une autre, il y a un autre PowerPoint pour parler de l'examen. Comment se préparer après quand vous allez avoir la certification ? Maintenant oui, je peux préparer de quoi pour faire une révision et puis parler de l'examen de de façon générale aussi hein, comme les 2, on a le temps. Et puis faire une révision aussi pour l'examen, d'abord votre examen à vous hein, l'examen que vous allez faire pour la fin de session et puis l'examen aussi de du CSSP.

2:40:09
C'est bon, parfait c'est bon. Ouais ouais c'est bon OKOK donc Monsieur je oui Monsieur, est ce que est ce que toujours c'est confirmé l'examen final c'est juste pour la partie que tu tu viens de oui oui oui oui désolé je j'avais ça en tête de vous le dire, ça ça devait être la première phrase du cours mais.

2:40:31
Désolé oui Dominique m'a confirmé que c'est juste la partie que la partie que j'ai j'ai j'ai eu à faire, c'est donc la première. La première partie va comprendre ce que lui il a fait sera juste la première partie, l'examen sera et puis moi ma partie ça sera l'examen final, c'est bon ? Ben de toute façon je vais réviser les questions d'examen et puis je vais voir.

2:41:01
Si vous Retrouvez des questions de de la partie de Dominique, laissez-moi savoir. On sait jamais parce que des fois les on a des banques de questions et puis on révise. Souvent il y a des questions qui peuvent échapper parce que c'est des questions souvent aléatoires. Donc si vous voyez des questions de de la partie de Dominique, laissez-moi savoir c'est bon. Ben je vous laisse le reste des minutes. Bonne soirée à vous.

2:41:29
Ouais pour l'examen c'est sur moodle comme d'habitude ou est ce que c'est fracture ou c'est comment l'intra ? Comment vous l'avez fait ? C'était sur moodle, c'était sur moodle. Ouais oui ça sera sur moodle OK parfait OK l'examen, l'examen intra on vous n'avez pas encore eu la correction hein ? Ouais on a eu la correction, on a eu notre aujourd'hui.

2:41:58
Aujourd'hui depuis je parle depuis quelques jours ouais quelques jours, est ce que est ce que tout le monde l'a reçu ? Moi je l'ai reçu j'ai j'ai vu peut être lundi ouais OK Ouais Ben en tout cas une semaine ouais la moyenne était bonne, en tout cas la moyenne était très bonne donc souvent quand la moyenne est trop bonne c'est bon mais en même temps c'est pas bon parce que le le a plus on est plus exigeant pour les a plus quand la moyenne est trop bonne ouais c'est ça ouais.

2:42:25
Si si tout le monde a 90% celui qui aura 99 il aura le a plus mais si tout le monde a tourne autour de 81 80 peut avoir un a plus. C'est bizarre mais c'est comme ça oui. Est ce que y avait une autre question ésaïe ésaïe peut m'aider à réviser les questions de l'examen monsieur Monsieur Foufana moi je je voulais poser une question concernant les le.

2:42:54
Le le les documents qu'on a fait à 2 l'examen, l'exercice qu'on a fait à 2 en équipe de 2 personnes vous

avez fait des exercices en équipe de 2 personnes. Oui pas dans ce cours là dans plutôt dans l'autre cours que vous avez donné, sécurité des applications OK sécurité des applications oui oui Ah 804OK vas y oui je me demandais c'est est ce que c'est vous êtes en train de corriger ou ?

2:43:20
On doit s'attendre à un peu plus de temps pour non ? Un peu un peu plus de temps c'est souvent ça, ça prend du temps pour la correction de pour finir toutes les corrections pour ce type-là on est en train de voir même peut être on va pour les prochaines sessions, on va peut être changer le mode d'évaluation mais voilà ça va prendre 111 délai un un délai avant que vous ayez vos notes. Vous avez déjà eu la note pour le oaps et puis l'intra donc ouais.

2:43:50
Pour l'examen final c'est plus rapide, c'est le le travail de recherche qui prend du temps mais vous allez avoir vos notes. Généralement c'est un cours où la moyenne est très haute donc c'est on a souvent des problèmes de riches avec ce cours là. Donc souvent 111, 90% peut avoir un B 111 A moins ou un B plus. Oui amani.

2:44:13
Oui pour le cuis en cours oui oui donc ça c'est le lundi, le QI c'est le 25 c'est le 25 c'est c'est pareil hein je pense c'est 10 questions pour 15 Min d'accord c'est le c'est le 25 ça ça sera lancé le 25 si peut être j'avais bon si j'avais prévu de faire tout le cours aujourd'hui, j'allais le déplacer mais ça vaut pas la peine de le déplacer, on va.

2:44:39
Tranquillement faire ça le 25 et puis vous allez avoir du 25 jusqu'au 30 pour le faire et après vous allez faire votre examen le 9 juillet tranquillement c'est bon mais il semblait qu'il y avait un Q qui était ouvert là donc j'ai reçu un message. Ouais le QI non c'est le QI 3 c'est pas c'est le 3 qui est ouvert, c'est le 3 qui est ouvert et qui finit jusqu'au 23.

2:45:04
Voilà c'est ça. Donc lui c'est comme une question déjà donc c'est pas ouvert à 15 Min OK d'accord Ouais c'est le même 15 ouais puis +3 il y a quand je l'ai fait il y avait 12 questions au lieu de 10 je me posais OK Tabarouette sont un petit peu plus intelligents cette fois-ci là Ah je je sais pas bon je vais pas aller rentrer dans les paramètres mais sinon je peux voir les banques mais bon on après on va voir ça je vais je vais je vais arrêter mon partage tu dis +3.

2:45:33
Tu avais combien de questions moi moi hier quand j'ai fait j'avais 12 questions, t'avais 12 questions ? Ouais oui c'est c'est ça, je vois 12 questions c'est ça ? Tu as commencé plutôt en 12 questions, c'est quoi ont fait plus tard en 10 questions c'est c'est 12 c'est 12 questions, 15 Min c'est beaucoup. Ah oui oui oui je vois, mais le le Q 4 c'est 10 questions avec 10 questions, le temps ça passe vite je pense, c'est c'est beaucoup.

2:46:03
Est ce que les 2 questions supplémentaires sont des bonus ? C'est énorme là, parce que des fois, des fois, on n'arrive même pas à réfléchir à la réponse. Comment on répond oui mais on est coincé dans le temps-là des fois on répond parce que le temps il est-il est fini, c'est bon. On répond directement sans réfléchir, OK.

2:46:32
Ben en fait les les c'est ça fait si c'est 15 Min par question, une question fait une minute et demie pour le CSSP, c'est pratiquement la même moyenne hein, tu n'as pas quand tu fais les examens soit CSSPCISN t'as pas beaucoup de temps pour pour réfléchir je pense. Ça c'est c'est pas une manière de évaluer par exemple quoi ça c'est si on regarde le temps et.

2:47:01
Réfléchir pour répondre je pense c'est 2 2 choses qui sont contradictoires parce que évaluer quelque chose c'est de donner le temps de réfléchir pour répondre c'est pas de regarder le temps. Qu'est ce qu'il termine ? J'ai pas répondu, il y a encore des questions que j'ai pas encore répondu. C'est énorme je pense. C'est.

2:47:25
C'est oui, oui c'est, c'est discutable. Il y a des évaluations qu'on qu'on qu'on on, on regarde le temps pour départager aussi. Si tu regardes les certifications, les certifications, il y a un temps. Et puis généralement t'as pas plus de 10 Min pour une question. Tu as tu as autour de une minute, une minute 30 pour une question, donc faut Allô.

2:47:50
Allô désolé je disais 2 Min c'est c'est vraiment rare puis c'est c'est ouais c'est ça c'est c'est c'est ça. Donc si tu es dans un cours de préparation des CSSP que tu as un quizz, Ben on te met dans les mêmes conditions donc c'est ça. Puis puis si je pourrais enregistrer l'application de learning zap puis recommandé dans le cord Learning zap et on utilise la même page quand que je me fais une série de questions.

2:48:20
J'utilise le mettons à 10 questions et il donne 15 Min, puis ça ça se met dans le même pace ça c'est avec ça, c'est avec le onzap l'application qui est qui est recommandée par le four fait que mettons puis un 25 questions c'est 37 Min puis tout ça fait ça essaye de tu viens qu'à t'habituer à à cette page là c'est ça ? Sinon ayette je je comprends ce que tu dis.

2:48:49
Mais c'est ça, il faut limiter le temps, sinon on va donner un temps infini à tout le monde. Et puis tout le monde va avoir 100%, c'est pas ça qu'on veut non plus. On veut évaluer sur le temps comment. Voici dans le dans l'examen, les quiz généralement pour les certifications, voici ce qu'on se dit, on se dit que tu as eu le temps de bosser, tu as eu le temps de maîtriser les concepts et quand on te pose la question.

2:49:14
Tout de suite en quand ? Dès que tu finis de lire la question, on te donne 3 une minute pour lire la question, comprendre la question et puis répondre rapidement. Donc c'est ce que c'est ce qu'on s'est dit. Donc au préalable tu as déjà bossé, tu as déjà évalué, si on te donne beaucoup de temps, Ben tu vas tout trouver donc c'est ça, désolé mais c'est c'est comme ça que ça se passe, c'est avec les les toutes les certifications c'est il y a un temps limite pour ça. Oui Lucien.

2:49:41
Oui je veux revenir sur le puisse me dire quoi ? Est ce que c'est d'autres questions ou bien c'est dit que ça ça doit être est ce que c'est quoi ? Moi je vois que c'est 12 questions. J'ai vu quand je regarde dans

les paramètres c'est 12 questions, 12 en 15 Min c'est ça ? Il y a 12 en 15 Min, il y a 12 en 15 Min mais le 4 le 4 c'est 10 questions en 15 Min.

2:50:08
Je sais pas pourquoi c'est c'est 12. J'avoue c'est pas moi qui ai qui ai fait l'examen mais je peux je peux ça, je peux me renseigner mais c'est pas bien grave que ça soit 12 ou 10, là ça change pas grand chose. De toutes les façons on va vous non ça change pas grand chose parce que de toutes les façons, peu importe les moyennes que vous allez avoir, on va toujours regarder la moyenne du groupe. Donc si vous vous avez fait 12 questions, ça pose pas de problème, on vous évalue sur les mêmes bases.

2:50:35
C'est pas la question évaluée par rapport au groupe, mais quoi ça ayette je je dis comme quoi c'est dévalué. On t'évalue par rapport au groupe, c'est pas question. Par exemple moi je regarde par par rapport à moi. OK OK je est ce que tu peux me clarifier ta question, qu'est ce que tu veux ? Tu veux Allô Hayette OK.

2:51:04
Elle semble ne pas être là mais bon bref c'est c'est c'est ça, c'est comme ça, on évalue même le CSSP aussi, là on te compare au groupe Hein, c'est c'est il y a. Il y a là derrière qui va t'envoyer des questions difficiles que les gens n'ont pas trouvées. Souvent ils vont t'envoyer des questions faciles que les gens ont trouvées, donc on va toujours te comparer par rapport aux autres. Je veux pas dans le monde là on te on compare toujours, on se compare toujours aux autres.

2:51:28
Donc on peut pas définir nous même nos propres règles. Puis puis si je peux rajouter c'est SSP te si je me souviens bien t'as des questions genre qui sont pas comptabilisées ? Je pense que oui c'est un vrai c'est ça je crois. C'est une 15 comptabilisée, mais ça mais tout dépendant selon l'i a tout dépendant ce que ce que tu réponds lui là il essaie de.

2:51:48
D'évaluer ton pourcentage de réussite de l'examen. Puis il peut te rendre, puis s'il est pas certain, il peut te rallonger le nombre de questions hein. De 125 un petit peu plus jusqu'à temps qu'il puisse être sûr. OK d'après moi, d'après ce que je vois, OK tu passes ou tu passes pas, là c'est ça c'est beau.

2:52:11
Merci beaucoup Emile, merci beaucoup Moïse, merci hayette, merci Djeba Moustapha Marie Maria tour merci. Bonne soirée à vous et à la semaine prochaine Bye Bye bye merci, bonne soirée bye.

INF813-Séance-12-Module-4b

0:02
C'est bon ? Est ce que vous voyez mon écran ? Oui oui oui parfait. On y va donc la séance. La séance dernière on n'avait pas terminé tout ce qui était réseau donc on va le terminer aujourd'hui. On verra le 4.2 composants du réseau sécurisé donc.

0:31
Tout ce qui est matériel, alimentation redondante, les médias de transmission, les contrôles d'accès réseau, la sécurité des terminaux. Ensuite, on va voir 143 mettre en œuvre des canaux de communication sécurisés conformément à la conception. Donc tout ce qui est voir collaboration multimédia, accès à distance, données de communication, réseaux mutualisés, connectivité tierce.

1:00
C'est pour les composants de réseau, on a le Cap Coaxial, donc c'est un câble que généralement ceux qui ont les les anciennes télévisions, ceux qui ont utilisé les anciennes télévisions utilisaient ça, et ceux qui ont généralement les le helix de Vidéotron l'ont également. Donc le câble il est comme ça, le a c'est la gaine externe, le B on a un blindage là-dessus.

1:30
Le C on a un diélique et le D on a un conducteur. En termes d'utilisation en Réseautique, Ben on utilise le le fil net qui est le 10 base 2 et on utilise le filtre net qui est le 10 base 5. 10 base 10 ça veut dire 10 mégabits par 2nde et le 2 c'est 2*100 M donc ça fait 2 10 mégabits et 200 M, mais en réalité c'est 185 M que ça prend.

1:59
Et pour les 10 bases, 5 c'est 10 mégabits et 5 500 500 M donc 5*100 M donc 500 M de longueur. En termes d'utilisation également, on l'utilise pour les les câbles sous-marins, transport de données à longue portée. On l'utilise également pour pour le signal vidéo également. Donc voici l'exemple de du câble coaxal de l'entrée du câble coaxial. Ici ça c'est la borne elix de Vidéotron.

2:27
Tantôt, je parlais du HFC, la fibre jusqu'au voisinage, donc ça, ça sera le signal dont je parlais. Tantôt le signal vidéo. Le HFC qui est là, je crois, c'est le réseau de de. C'est une observation de vidéotron, donc à droite, c'est la borne et l'x fille derrière. Ici, en 5, on a l'entrée.

2:54
Je pense que c'est en 3 hein. En 3 on a l'entrée du Cap Coaxia, donc la plupart d'entre vous vous aviez un exemple de Cap Coaxia, vous avez excusez-moi, s'il vous plaît, excusez-moi, j'ai une question, oui vous pouvez revenir à la diapositive précédente s'il vous plaît. Ouais OK, ici peut être je sais pas si je me trompe, vous avez mis là 10 base 2 et 10 base 5, vous avez dit 10 mégabits sur 200 M et 500 M et puis vous dites qu'on peut utiliser ça dans les transports sous-marins.

3:22
Les sous-marins à longue portée, il va falloir faire les racolages je sais pas si j'ai bien compris cette partie parce que non, je dis hein, vas y vas y parce que vous avez dit On peut les utiliser comme câbles sous-marins et vous avez dit transport de données sur de longue portée. Or ça veut dire que si on prend les 10 base 5 ou les 10 base 2, c'est 200 M ou à 185 M en longueur réelle fait en sorte qu'il va falloir beaucoup faire les jointures. Là c'est oui, c'est des segments.

3:49
Oui ce que tu dis c'est c'est c'est une réalité. Je pense pas que à date il est beaucoup utilisé. On utilise beaucoup la fibre optique pour les câbles sous-marins mais ça reste quand même que c'est un câble d'utilisation en fait. Et les 10 bases quand on met 10 base 2 et 10 base 5 c'est vraiment la longueur d'un segment. OK d'accord parce que si on l'utilise en en transport sous-marin ça doit-on doit vraiment vraiment faire des ça, ça doit être très long. Oui je suis d'accord avec toi, merci.

4:22
Donc comme je disais l'abonne de Vidéotron, vous allez voir, vous avez un câble quatial à la maison, ça vous donne une idée de de quoi on parle. Ensuite on a la le fil qu'on appelle le fil avec pain torsadé Twist pair. Donc on a 2 fils conducteurs qui sont enroulés, il y en a 2 sans blindage donc ça c'est le ETP. Une short Twist pair.

4:48
Et on a avec blindage qui est le Shell Dead Trispair. Généralement on va retrouver un code F qui a qui veut dire le Ford c'est c'est le blindage par feuille d'aluminium. Donc souvent on a des des câbles comme vous pouvez le voir au niveau de la droite, ici les catégorisations. Donc on a le level un level 2. Et puis on a catégorie 3UTP on a catégorie 4, catégorie 5 on a catégorie 5 et catégorie 5E on commence à avoir des F donc le F c'est plus pour dire que c'est fold.

5:17
Et des fois on a souvent catégoristique, on a souvent des huches qui sont devant des FTP donc ça va dépendre de la catégorie de du film. Et là plus on a on a de l'aluminium là-dessus, plus c'est résistant au bruit.

5:37
Et au niveau de la de la nomenclature, quand on dès qu'on arrive dans les paires torsadées, on voit plus les comme on l'avait dans les câbles coaxials. Généralement c'est le t qui est à la fin pour tout ce qui est pertes torsadées donc on va voir c'est un GBT ou 100 base t donc généralement on va retrouver cette donc ce qui est devant, généralement ça donne la vitesse et l'autre généralement ça donnait la la la longueur maximale sur.

6:06
Une dimension sur une distance, sur un segment spécifique. Ensuite on a la fibre optique, donc la fibre optique, la structure. On a le cœur qui fait 10 micros, 10 µm. On a la gaine qui est là, qui elle permet de la réflexion interne, de la lumière. Donc la la, le cœur c'est plus en verre plastique et puis va transmettre la donnée via la lumière.

6:31
La protection qui va assurer la la durabilité physique. Donc lui il va aller jusqu'à 230 µm donc il fait de grands débits, donc un un pétabyte par 2nde en laboratoire qui avait été testé par les Japonais en 2013. Mais à date on est autour de en termes de longueur 2000 km jusqu'à 170 térabytes par 2nde.

6:57
Il y a peut être des documentations, vous allez voir peut être des vitesses différentes. Des fois il y a des documentations, ils vont mettre que ça fait plus de 2 giga au-delà de de 2 gigabits par 2nde mais à date jusqu'en 2000 je crois. En 2020 ou 2022 on était autour de 172 térabits télabits par 2nde et le CE

qui est en haut c'est vraiment un test en labo donc je pense pas qu'en pratique on l'est vraiment utilisé mais ça reste quand même ça reste le le support le plus rapide à date.

7:32
En termes de transmission, Ben on a les sonnets qui sont là, donc le le Synchronous Optical Network. On a la correspondance avec le Sonnet Frame, le SDH level, la PI laude qu'on a puisque la vitesse. Et puis on a le line width ici en termes de long métrage, en termes de débit brut, qui inclut le pays load et le ici le pays load, c'est juste le pays load simple.

7:59
La vitesse réelle transportée et ça c'est la vitesse réelle avec la charge. Donc comme vous le voyez ici en kilobit le payload lui, il est plus faible que le Land Read qui lui va comporter non seulement le payload avec tout ce qui est bruit à côté. Donc ça ce sont les correspondances de des différentes catégories, Sonnet level, Sonnet Frame et SDH level au niveau de la transmission avec la la fibre optique.

8:29
Les différents types de signaux, Ben on a les signaux numériques, donc impulsion électrique. Donc ayant 2 États, on a le haut, on a le bas, donc on a un 0 comme vous le voyez ici. Digital signal, les signaux analogiques, on a l'information sous forme de onde qui est en bas, là est ce que vous voyez ma mon curseur où on voit le curseur ?

8:51
OK c'est bon donc là au niveau analogique donc on a en forme d'onde donc il est beaucoup les cas d'utilisation. Il est beaucoup utilisé un système téléphonique analogique traditionnel. Et puis pour tout ce qui est radio FMAM, on a les transmissions asynchrones, donc chaque transmission avec une séquence de bits de début et de fin pour la synchronisation. Donc il synchronise l'émetteur et le récepteur à chaque message.

9:18
Donc on a comme exemple les RS 232, les fameux ports VGA qu'on a et on a le USB un ou le IS 2. Le ISB 1.1 et le ISB 2.0. Désolé je pense j'ai souvent des problèmes avec mes mes points qui deviennent des virgules. Après je vais je vais corriger ça après la pause donc c'est 1.1.

9:47
On a la transmission synchrone Ben les données sont transmises en flux continu donc on a l'horloge de synchronisation qui est partagée. Donc les dans les cas les cas d'utilisation on a internet on a la voix sur UP en temps réel c'est bon s'il y a des questions ça va je vois pas souvent vos mains, je gère avec 2 appareils donc continue.

10:25
Un instant on a les bandes de base baseband qui est le canal. Le canal prend la largeur de la bande passante qui est disponible, donc c'est un seul signal à la fois que comme on l'a ici et on a la large bande qui est le broadband, donc plusieurs canaux ayant leur propre largeur de de bande passante.

11:10
Je je j'aurais une question Ben simpliste, je suis en train d'essayer de faire des liens. Pardon c'est je coupe un peu vas y donc si je comprends bien dans le cadre coalition quand on parle 10 base telle

affaire donc ça se réfère à la bande de base donc un 10 base 2 10 base 5 ça se réfère à la base comme les les câbles RJ 45 c'est c'est tu ça ça fait tu référence à ça.

11:40
Quand qu'on parle de base, non je je ne saurais que les dire quand les les disent. Ici le le 10 base je pense que parce que je sais que drop band c'est matton, DSL quelque chose du genre, ça c'est du drobin connection.

12:08
Uhum. Je me souvenais alors, mais j'essaie juste de me refaire des liens. Non j'ai pas, j'ai pas l'info, je vais, je vais peut être te faire mes recherches uhum puis te revenir après OK ou un ami qui fait de des recherches sur le web. OK, on a les différentes topologies, donc on a les topologies, la, la topologie anneau qui est ring, donc là on a une boucle simple.

12:35
Donc la boucle qui a qui va fonctionner en dans le sens aiguë des montes d'une montre. Donc on aura les différents. Un message va circuler d'un ordinateur à l'autre en suivant le sens des aiguilles d'une montre en cas de collision, comme vous le voyez, Ben si on a la première machine qui a une collision, Ben ça va s'arrêter puisque c'est dans un seul sens. Bon, si c'est dans un sens, on ne peut pas aller de l'autre côté, donc il y a une faible résilience par rapport à à la boucle double, donc la boucle double.

13:05
Mais on a la le sens, le sens des équipes du monde, et on a le sens Trigonométrique. Donc là si on a le premier qui est là qui a un problème, Ben on peut aller vers un autre sens pour faire transférer le message. Donc il est généralement utilisé dans les réseaux FFDDI et sonnet. Pour le réseau bûche, on a le type linéaire et arbre, donc c'est vrai que c'est ici l'arbre, ici le linéaire comme vous le voyez.

13:34
On a les différents nœuds qui sont là, donc dans les nœuds sont sur un cadre, les nœuds sont sur un cadre principal, donc chaque nœud va écouter le trafic sur le bus. Donc à date pour les raisons modernes on utilise plus ces genres de topologie. Là c'est pareil pour le le Truie, donc les on a 2 bus, on en a 2 linéaires et truie donc on utilise toujours.

14:03
Dans l'ethernet avec une autre Cap no cap Coaxial 10 bases, 10 base 2 et 10 base 5, on a la typologie étoile, donc c'est la typologie qui est utilisée dans les réseaux, beaucoup utilisée dans les réseaux modernes, donc on a chaque nœud connecté à un point central, un commutateur généralement, donc le réseau Ethernet c'est le réseau éternel domestique ou entreprise. Donc dans nos réseaux on a généralement d'étoiles qu'on a.

14:32
Ensuite, on a les réseaux maillés, généralement à la maison, on n'a pas le réseau maillés parce que ça coûte cher. Donc chaque nœud doit être directement relié à un autre nœud, donc il y a une fiabilité qui est élevée et puis on a une pleine de redondance. Désolé pour la coquille, j'ai, il y a un e accent aigu qui est encore là. C'est pour généralement les réseaux critiques. Elles sont des données militaires One intersight et redondantes.

15:07
Pour notre réseau LAN, on a l'ethernet avec le IEE 802.3, donc on a la les topologies bus coaxial qu'on

peut utiliser étoiles avec les pertes torsadées et le point à point avec les fibres optiques on a les token ring, le IE 802.5, topologie logique, anneau et physique étoilé. Donc la communication s'est fait via un jeton qui circule.

15:31
Dont un seul appareil pouvait parler à la fois. Donc avec le ring qu'on avait montré, on a le FDDI que le Fiber disseverted dans la interface, donc le passage d'un jeton avec la fibre optique sur un réseau pas très étendu. On a une forte résilience. Donc il a été remplacé par le face Ethernet de 100 mégabits par 2nde et le Giga Ethernet de un Gigabit par 2nde.

16:02
On s'en vient maintenant dans les réseaux, les les appareils qu'on utilise dans le réseau. Donc on a le commutateur, le hub qui était utilisé généralement dans le passé, ça a beaucoup été remplacé par les switch. Le hub, il reforme le signal électrique, donc les pertes d'intensité ou bien des messages du du signal qui est déformé. Il agit sur la couche un couche physique.

16:28
Donc on a les domaines de collisions et de diffusions unique. Donc on a le Cara science multiple Access with collision detection. Puis détecter les différentes collections, les collisions. Il peut s'interconnecter pour augmenter la capacité de des des ports. Donc si on a moins de ports on peut interconnecter les hubs pour avoir plus de ports. Parce que si on a besoin de plus de de n points dans notre réseau.

16:56
On a le fameux modem qui est modulor modulator de Modulator. Il va transformer un signal numérique pour le transmettre sur le canal de communication souvent analogique. Aujourd'hui, les avec les routeurs de nouvelle génération, on a généralement les modems intégrés. Donc avant, quand on faisait de l'internet, on avait souvent l'appareil modem qui était à côté. On avait un autre équipement qui qui servait de de routeur.

17:25
Donc on avait très souvent ces 2 appareils à la maison. Mais de plus en plus les routeurs modernes intègrent les 2, ils intègrent généralement les les modems. Donc on ne voit pas très souvent dans nos réseaux modernes des modems. On a le pont, les bridges, ils vont interconnecter des réseaux du même protocole. Donc il va agir généralement sur la couche 2. Donc le pont lui il a un herbe, il a un herbe de l'autre côté donc il va interconnecter les 2 réseaux.

17:57
Donc il divise les domaines de collisions, le commutateur, il est un peu comme le hub, à la différence que lui, il est un peu plus intelligent. Donc il va régner les appareils entre eux. Donc si on a 2 réseaux star, il pourra les relier entre les 2.

18:16
Il va agir sur la couche 2 optionnellement, souvent sur la couche 3, donc souvent avec des des switch multiliers des switch vraiment Cisco qui vont souvent agir sur la couche 3. Ces switch ont des tables d'Adressages Mac, adressent des liaisons donc qui font une correspondance entre le Mac et le entre l'adresse Mac et l'adresse IP.

18:43

Autoroute, ils ont une autoroute interne pour le transfert rapide des données qui peuvent séparer des domaines de collision. Il a une haute performance parce que plusieurs peut avoir plusieurs communications simultanées. En termes de fonctions avancées. Avec ces gens de switch, on peut faire du vlan. Donc le V LAN permet de créer des domaines de broadcast indépendants, donc il peut isoler logiquement des communications entre plusieurs services.

19:11
Donc on peut faire un sous réseau pour le un, un vlan, un V LAN, autant pour moi pas sous réseau. Un V LAN, un réseau virtuel pour le RHDF les finances donc peut renforcer la sécurité puis réduire la charge de du réseau. Donc comme vous le voyez ici, premier étage, 2e étage, on peut avoir des machines qui sont sur différentes étages, mais ils peuvent être dans un même réseau virtuel.

19:39
Où souvent, on peut avoir même des des réseaux, des appareils qui sont physiquement connectés sur un même commutateur, mais ils peuvent appartenir à différents réseaux. C'est bon, c'est juste virtuel, c'est ça n'a rien à voir avec leur connexion physique. Autre fonctionnalité ?

20:04
On a on peut faire du Power over Ethernet donc c'est la technologie va permettre d'alimenter les clients. Un appareil réseau donc caméra IP, téléphone X téléphone, voiture IP, point d'accès Wifi via le même câble Ethernet donc il peut nous permettre de faire le les ACL et HS Control List donc peut nous dire qui peut accéder à quoi donc à travers les ports levés là également.

20:30
Il peut faire du 802 un point X donc peut permettre d'authentifier qu'il se connecte au réseau. Il peut faire aussi du penac. On va voir tantôt le NAC. Qu'est ce que le NAC fait donc avec des switch, certains switch qui ont des fonctionnalités avancées, on peut faire des activités au niveau de la couche des activités de la couche 3. On a nos routeurs donc le routeur réagit au niveau de la couche 3 aussi.

20:58
Donc il prend en charge le routage entre réseaux, donc lui il est capable de dire où est ce que les paquets doivent partir. Donc on en a 2 types, on a du routage statique où on va définir les tables, on va définir les tables, on va dire tel réseau tu passes par tel gateway, tu joins tel réseau où on peut avoir du routage dynamique avec de l'apprentissage des routes dynamiques, des routes de façon automatique en utilisant l'un de ces protocoles là. Donc soit on peut utiliser le protocole RIP.

21:28
Qui est le routing Information Protocol, qui un protocole de distance qui va calculer le vecteur de distance, donc il va calculer, il va regarder le chemin en fonction du nombre de sauts qu'il lui doit faire, et on a le OSPF qui est le open shorters par First qui va calculer le chemin le plus court basé sur la vitesse, le coût et puis la bande passante, et on a le BGPI qui est le boarder Gateway Protocol.

21:54
Il va utiliser pour le routage entre fournisseur d'accès Internet donc des des packs bonne internet, un autre équipement. C'est le NAC qu'on peut retrouver pour dans notre réseau pour faire la sécurité. Donc le NAC, qu'est ce que lui fait ? Il lie l'identité à l'accès des ressources réseau, donc il va contrôler l'accès en fonction des règles strictes. Donc je peux avoir mon réseau, je peux avoir mon NAC et puis j'ai dit à mon NAC, mais.

22:20
Tel type d'appareil tu les acceptes, tel type d'appareil tu les acceptes pas selon telles conditions. Donc en plus de de on peut faire du 801 point X donc une forme de base. En plus d'être autorisé à utiliser le port 802 point X, le dispositif et l'utilisateur doivent remplir un ensemble de conditions pour accéder au réseau. Donc je peux vérifier une machine qui est pas sur qui a pas son antivirus à jour va pas peut être accéder à mon réseau. Il y a plusieurs conditions que je peux mettre, des politiques de sécurité que je peux mettre pour.

22:50
Mon réseau pour l'accès à mon réseau donc il permet de réduire les vulnérabilités 0D également. On a maintenant les pare feux donc on a les pare feux sans État stetless firewall donc ce sont les firewall de première génération donc toujours sur la couche 3 donc ça va filtrer selon la source, destination et le port donc ne traitent pas l'état d'exception donc C'est pourquoi on l'appelle Stetless.

23:20
Donc les règles, on a les ACR, les policiers, les rouges, les fluteurs qu'on peut appliquer là-dessus. Il est rapide et simple, pas efficace contre des attaques avancées. On a le parfait applicatif application firewall. Lui, il valide les requêtes, donc il peut aller jusqu'à la recette. On peut agir sur tout ce qui est HTTPFTP, puis isoler le réseau à travers un proxy.

23:50
Donc comme vous le voyez ici, je peux avoir une requête, une requête, un utilisateur et lui à travers sa requête on passe par le le firewall, on atteint une machine. Non ? Autant pour moi on a le worksation qui lui va faire la requête passe par le firewall Internet, il va atteindre le serveur. Il revient avec le message puis le message est donné au workstation.

24:16
Et le pare-feu applicatif pourrait agir là-dessus. Donc généralement en termes de proxy on a le pare-feu à État stateful Fire firewall. Donc il va se baser sur l'état des sessions. Donc ouverture, échange, fermeture des sessions. Donc nos fameux sin ARK autres qu'on a vu la dernière fois. Donc ne laisse pas passer un paquet inattendu. Donc il peut opérer sur plusieurs couches 3, 4 et 5.

24:49
On a le pare-feu circuit Circle level get oui donc lui il inspecte les connexions au niveau de la couche 4 TCP TCP udp donc il vérifie chaque ouverture de session par rapport à une table de connexion autorisée. Les règles sur les. Il applique les règles sur les adresses sports heures de la journée, le protocole utilisé utilisateur en question.

25:14
Une fois autorisé, aucune autre vérification par exemple au niveau des paquets n'est effectuée donc et on a les pare-feu de Next Gen Firewall. Bon ils ont mis prochaine génération mais c'est nouvelle génération, c'est la génération actuelle Next Gen Firewall. Mais bon c'est ce qu'on est en train d'utiliser, c'est pas la prochaine génération, c'est la génération actuelle.

25:39
On a des coupes multifonctionnelles. Donc en plus des fonctionnalités standard des d'un firewall, les next Firewall peuvent intégrer des systèmes de prévention d'intrusion, des IPS, des inspections TLS donc, qui peuvent nous permettre de déchiffrer puis inspecter le trafic HTTPS. Généralement les

firewall statiques, les firewall standard n'arrivent pas à faire l'inspection TLS, donc si on veut faire passer par exemple des des informations.

26:09
Peut être on veut faire du DLP et que on ne fait pas de l'inspection TLS. Il y a des informations qu'on pourrait faire sortir par le HTTPS qu'on ne on ne verra rien dedans. Donc pour pousser loin notre gestion des risques en termes de fuites de données, Ben il faut être capable de pouvoir faire une inspection TLS. On a le filtrage d'u RL également qu'on peut qu'on peut avoir sur ces routeurs là la gestion également de la bande passante, tout ce qui est gestion de la du QOS là-dessus.

26:37
Peuvent limiter théoriser le trafic par rapport à l'application et puis les utilisateurs. Ensuite tu peux avoir également des fonctionnalités d'antivirus. On arrive maintenant sur l'architecture. J'ai une question s'il vous plaît j'ai une question. Ouais je me pose la question sur les firewall, en fait l'ordre d'exécution des règles sur les firewall, les séquentielles ou bien est ce que.

27:06
On prend en compte peut être la logique je je prends un exemple, imaginez-vous avez plusieurs règles sur le firewall, Premièrement vous vous interdisez un sous réseau, peut être une adresse IP, non vous interdisez un sous réseau, ensuite en bas la 2e, mais vous autorisez là une adresse IP du sous réseau, comment ça se comporte ? Est ce que l'ordre séquentiel ? Ou bien on fait une analyse le le pare-feu fait une analyse globale pour pouvoir résoudre est ce qu'il y a des parfums qui traitent ça, il y en a, est ce qu'il y a d'autres qui font pas simple ça la question.

27:35
Il y a, il y a des bon je je réponds de ce que je sais. Et puis il y a s'il y a quelqu'un qui a une qui a qui a, qui travaille plus dans le réseau, qui peut nous répondre, on va aller là-dessus. Moi je vais réagir. Je je te donne la réponse en fonction de comment généralement les systèmes l'algorithme fonctionnent. Si tu as une règle qui te dit on dinaille, Ben il va dinail jusqu'à ce que il ait une règle qui le qu'il accepte.

28:05
Maintenant on a des firewall de nouvelles générations maintenant qui sont plus intelligents, qui peuvent te analyser le trafic et puis te dire à un moment donné qu'il y a de l'incohérence dans tes règles, c'est bon. Donc c'est c'est pareil comme les règles de transport qu'on a souvent sur Exchange, il y a Jean Roger qui a enlevé la main. Je vais terminer. On a des règles de transport qu'on a souvent sur.

28:36
Exchange dans la règle des transports tu peux dire quand on admettons on on reçoit un courriel et puis je veux juste que dans le courriel on puisse mettre juste des messages de de notification pour certains types d'utilisateurs. Donc je peux mettre le message mais si dans notre un autre règle je leur demande d'enlever, il se peut que il enlève le message que j'ai eu à envoyer le la première règle que j'ai eu à mettre.

29:04
Jean Roger vas y oui Bonsoir Monsieur, Bonsoir tout le monde c'est un peu c'est pas une question en fait, c'est pour essayer ajouter un peu une réponse à qu'est ce que vous avez donné tantôt pour aider notre camarade là oui vas y à cette question, oui dans les parfums en fait je comment ça fonctionne ?

C'est la première règle qui est rencontrée qui est appliquée et dès que c'est appliqué le le le script ne va pas continuer en fait. Et s'il s'arrête oui et déjà quand il y a, quand il y a un.

29:29
Dans le cas qui l'expliquait tantôt, s'il y a un règle par exemple qui ouvre un qui ouvre une seule règle et qui en baille, dinaille généralement n'est pas fait un modem comme les hasa ou ou bien les News, je laisse comme les les palois de tout ça. Fire moderne aujourd'hui, qu'est ce qu'ils font ? Ils vont te signaler qu'il y a un conflit, qu'il y a un conflit d'intérêt, que tu as 2 règles qui sont comme, qui sont comme jumelées. Il y a les outils en entreprise comme tofin qu'on n'utilise jamais pour.

29:54
Pour optimiser pour faire le client des des règles, ça te permet de mettre des règles qui sont comme les les, les redondances, ça te permet de de de de déceler les redondances dans tes configurations au niveau de des règles. C'est un peu comme ça que ça fonctionne. Merci pour ton additif, merci sans régime est ce que je peux compléter peut être ? Oui vas y pourra peut être m'expliquer étant donné que ils par cela ils vont filtrer le trafic. Une fois qu'ils rencontrent la première règle il s'arrête.

30:27
Maintenant, si, parce que j'ose imaginer que ce que je comprends c'est parfois, on a plusieurs règles qu'on va appliquer sur un paquet, pas seulement les règles de de d'adresse IP. Où ça vient, on a la première règle, ensuite on a la 2e. Je prends un exemple, on dit si tu as de tels réseaux.

30:43
OK Tu tu on on te permet alors ensuite peut être après c'est vérifier si tu as un chiffrement TLS, 1.3 ou je sais pas 1.2 ou SSL et tout et tout et tout. Dans ce cas-là c'est plusieurs règles, mais si il teste juste la première s'arrête comment il fait pour tester la 2e ? Ou bien on parle là de blocs de règles qu'il doit tester, ou bien on peut définir les blocs de règles qu'il doit tester. C'est en fait ça, c'est pour ça que je pose la question, OK ?

31:06
Je j'ai à moins dans ces règles, tu as une source, tu as une destination et tu as des services. C'est en fait 3 conditions, ce sont les 3 conditions de base pour les pour des règles en fait après maintenant les chiffrements ou bien des des des bypass, tout ça là c'est ça peut venir en ajout sur les règles là, mais vraiment le le la règle la condition ce n'est pas nette. Pour avoir une règle ce pare-feu, il te faut une source, une destination et un service d'accord.

31:32
Émile, Ouais, je peux rajouter quoi ? Comme par exemple c'est fortgate ou sur les les, les checkpoints. Ce que tu veux c'est c'est c'est souvent il y a plusieurs blagues comme par exemple l'inspection HTTPS via TLS, c'est vraiment une blague différente. Qui s'occupe de ça ? T'as c'est ça, t'as ta Blade parfum, qui s'occupe qui va selon tes règles.

31:59
Mais inspection HTTPS, c'est vraiment un antivirus. L'i PS, c'est vraiment un d'autres blague qui vient de se compléter. Mais quand qu'on parle pare-feu c'est vraiment gestion de règle un après l'autre fait que mettons il arrive un virus ou en traite, émulation ou en traite inspection mettons t'as quand même tes règles de pare-feu avec tes seenlines puis tout ça ce que tu veux.

32:24

Mais aussi l'autre blague, vérifie, Ah c'est un virus je je le fais tu pendre ? Ah OK c'est vraiment un virus. OK je te bloque la communication même à faire avec des IPS, j'essaye de faire un SQL adjection puis il reconnaît la signature de SQL adjection, il se fait bloquer le le pare-feu et il est à côté. Mais c'est vraiment ta ta Blade IPS qui vient me bloquer fait que c'est c'est pas mal complémentaire là en gros là.

32:55
Je vais devenir complexe de temps en temps mais voilà merci merci Aurélien ta question Jean Roger 1000 merci pour l'éclaircissement les différentes architectures de parfums donc on a le bastion host donc lui c'est un système durci donc configuré pour faire face aux attaques donc on va retirer des services inutiles donc c'est souvent la règle pour tout ce qui est endurcissement.

33:29
Donc il va être généralement dans une DMZ. Donc ça dans le schéma on vous voyez le un VPS c'est c'est juste un un schéma, c'est le un Virtual private cloud, donc c'est un réseau qui est isolé à l'intérieur d'un cloud biblique, donc on a le bastion qui est à l'intérieur. Donc ça c'est un exemple d'architecture qu'on pourra avoir, le bastion os, un autre exemple d'architecture, un autre une autre architecture qu'on peut avoir, c'est l'architecture parfait dual home.

33:57
Donc il a 2 interfaces comme vous le voyez. Donc il va avoir une première ligne de défense entre 2 réseaux. Donc on a un réseau internet et on a un réseau interne donc le le dial Home Post et il sera au milieu des 2 réseaux. Donc là c'est une architecture qu'on peut avoir. Une autre architecture c'est l'architecture parfait screen host donc on a le parfait qui est branché sur un routeur qui filtre.

34:27
Donc on. Les paquets restants sont inspectés par le pare-feu, les paquets restants sont inspectés par le pare-feu. C'est bon est ce que il y a des questions ? On continue, on a un autre, une autre architecture architecture parfait screen sabnet. Donc ça va permettre la création d'une zone démilitarisée.

34:53
Donc on a un screen, on a le réseau interne, on a un firewall, on a la DMZ screen sabenet, ici on a le firewall, on a un screening device, donc généralement les screening devices peut-il y a des opérateurs, je prends Cisco qui peuvent avoir des ces types d'appareils là je sais pas si vous avez d'autres exemples, les sysco ICR par exemple, qui peut permettre de faire le ICL et tout le fortugais dont parlait et 1000 peuvent être utilisés comme des screening devices.

35:26
Ensuite on a l'architecture de sécurité réseau en couche, donc ça c'est au niveau de du CSST. On insiste beaucoup sur cette architecture là, donc on a la première architecture, donc l'architecture en couche on a le la première architecture qui est le single tiers, donc lui il est simple, donc on a un routeur, on a le parfait, puis on a le réseau privé. Donc lui il est simple, c'est single tiers donc il est simple à mettre en place, coût moins élevé.

35:56
Ensuite on a le tout tiers One, donc le tout tiers One ça veut dire 2 couches. Donc on aura la couche, on aura le private Network et puis on aura la DMZ. Donc ça fait nos 2 couches, on a notre firewall, on a notre routeur et puis on a Internet, donc ça c'est tout. Tiers un, on a le tout tiers 2.

36:20

Qui lui ? Il a 2 couches donc on a la DNZ, on a le réseau privé mais on a un firewall qui est là, on a un firewall de plus dans le two TS 2 dans le tweet, TS dans le tweet TS One, on a 3 parties dont on a la DMZ, on a la transaction Sabnet, on a le private Network mais dans le un comme vous le voyez on a la DNZ qui est entre le Firewall qui est entre les les 2 firewall.

36:50
Ensuite on a le twitch S 2 qui lui on a 2 firewall au lieu d'avoir 3, on a 2 firewall 2 d'avoir 3. Et la DMZ ressemble un peu à la DMZ du Two ches One, donc souvent ça peut tromper, mais pour maîtriser, pour mieux comprendre, retenez que two ches 2 c'est juste 2 parties dans le réseau, donc on a privé et puis on ADMZ. Donc ça c'est le two ches.

37:18
Le premier on a un DSL qui est séparé, l'autre les DMZ. Le DMZ communique avec un 2e routeur, donc le TS 2 à 2 routeurs mais par contre le TS 2 lui il a juste 2 routeurs et le TS un il y a 3 routeurs donc c'est juste retenez ça pour ne pas vous tromper dans vos questions. C'est bon ? Est ce qu'il y a des questions à ce niveau ou c'est c'est correct ? Ouais j'en aurais une, oui vas y.

37:48
J'essaie juste de me refaire une représentation mentale des architectures applicatives 3/3 comme par exemple t'as un serveur Web, t'as un backend, puis t'as tes bases de données, donc si je comprends bien, une architecture 3/3 applicative comme ça ça ressemblerait peut être plus mettons à three T Airlines, ça je comprends là.

38:17
Tu as ta DMZ, tu as un sabwet, tu as un sabnet qui est là et derrière tu auras tes bases de données, les Privates Network tu auras tes bases de données là derrière donc tu as tu auras plusieurs couches. Est ce que j'ai une question dans le groupe Jean-Marie Jean-Marie vas y le tout cherche 2 excusez.

38:49
Le le le non le three tiers 2 j'ai 2 routeurs mais le Three TS un j'ai 3 j'ai non c'est un routeur, autant pour moi je je passe c'est des firewall, autant pour moi c'est des firewall. Dans dans dans le Three TS 2 j'ai 2 firewall mais dans le Three TS un j'ai 3 firewall.

39:11
Désolé dans dans tous les cas on a un seul routeur, c'était c'était un lapsus, on a tous les cas, on a un seul, on a un seul routeur, c'est bon tu vois ? OK donc c'est sûr que oui vas y une question au niveau des des routeurs, pourquoi nous avons 3 routeurs ici dans ce cas-là est ce que parce qu'on a une coche par exemple pour le tiers un on va parler de présentation il y a.

39:39
Partie Applicative, une partie de données, c'est pour ça qu'on a 3 routeurs, non non non pas forcément, non, c'est pas des routeurs, ce sont des firewall hein. Tu parles de tu parles de Twitter un hein, c'est ça hein ? Ouais c'est ça je ouais, j'arrive pas vraiment à à voir pourquoi. Non c'est pas c'est pas forcément des présentations la DNZ bon ça peut être nos serveurs web, serveurs de messagerie et autres et transaction ça peut être un réseau.

40:07
Qui a nos actifs mais qui sont peut être moins critiques peut être que les ceux qui sont dans le Private Network. Donc on pourrait avoir peut être dans le private Network nos actifs qui sont plus nos les

joyaux de la couronne, nos bases de données et autres derrière un autre firewall de telle sorte que avant en tout cas d'arriver là tu as plusieurs firewall qui peuvent qui servent à protéger encore le le le réseau c'est pas par rapport à la segmentation là.

40:36
Oui, ça permet aussi de faire la segmentation. OK, puisque oui ça permet de faire la. OK, oui ça rentre les 2, mais la segmentation avec un V, là on peut faire la segmentation puisque là comme on a vu, on appelle, on a vu le V, là on peut faire la segmentation. On peut renforcer la segmentation aussi avec ces firewall là, puis mettre encore d'autres règles spécifiques comme la la question de Aurélien qui parlait des règles.

40:59
On peut faire des règles pour dire à ce niveau du firewall un le premier firewall, DMZ. Bon on a la DMZ donc c'est sûr que tu vas autoriser beaucoup de trafics qui vont venir. Mais après le premier, le premier, le 2e firewall qui va venir, Ben tu vas réduire en fait le le tu vas mettre de différentes règles qui sont qui seront plus strictes que le l'autre firewall et l'autre firewall. Tu vas mettre des règles encore pour qui sont plus strictes que le 2e firewall c'est bon ?

41:29
Merci oui Allô Monsieur oui Allô oui oui si si vous permettez ce slide là oui je voudrais peut être ajouter ce ce au besoin là quelques explications de cas où on peut avoir 3 firewalls Ben du du type Twitter One par exemple.

41:51
Des des cas où on peut l'avoir oui mais je voulais donner des quelques explications, oui OK vas y vas, y vas y vas y oui par exemple en entreprise, quand voilà on a une déconnexion internet, généralement s'il vient sur le le premier firewall, là celui qui est exactement connecté au routeur, ça va gérer les connexions internet sur les connexions distantes, les, les, les, les SSVPN tout ça seront déployés sur sur le premier firewall c'est généralement il sera dédié sur ce firewall, le 2e firewall ça va être.

42:20
Il sera géré un peu la DMZ et aussi des services qui accès à qui ont accès à l'extérieur comme par exemple le les solutions à comme par exemple le, le, le DNS ou ou d'autres services comme le. Ça protège également les voûtes, les voûtes de mots de passe, ça protège également les 6 looks. C'était vraiment les l'environnement serveur.

42:42
Le le 3e va plutôt gérer les communications est-ouest, donc tout ce qui a des communications dans à l'internat, l'entreprise par exemple de de Vélan à l'autre, ça va faire plus de segmentation pour gérer la segmentation puisqu'en faisant la segmentation au niveau des farwest on a plus une une facilité de contrôler qu'est ce qui passe, qu'est ce qui est autorisé ou pas. Donc c'est dans dans un cas comme ça qu'on peut avoir 3 farewell. Bon bien sûr qu'à l'entreprise y a des cas qu'on peut faire des des visualisations pour gérer tout ça. Je comprends que ça c'est.

43:12
Plus logique vraiment pour être toutes les choses. Donc c'est un peu un exemple type qu'on peut utiliser 3 fois. Merci, merci beaucoup Jean Roger, merci pour ton explication, ça permet de mieux comprendre c'est bon est ce que c'est bon avec l'architecture de sécurité ? Oui oui Bonjour tout le monde d'un point de vue CSCISSP là.

43:41
Étant donné qu'actuellement on vit le le phénomène que avec les nouvelles générations de de pare-feu on peut combiner le tout c'est à dire le trafic nord-sud, est-ouest dans le même tant compte tenu de la de la robustesse que peut avoir un pare-feu. Quelles sont les recommandations par rapport à ces architectures là ? Quelle est quelle est la plus préconisée par par le CACAISSP ? Le Cass va pas descendre dans ces détails là.

44:10
Ils vont présenter les différentes architectures pour la sécurité. Mais comme le disait Jean Roger ils vont parler d'aspect logique. Qu'est ce qu'il faut avoir maintenant ? Est ce que toi tu veux tout l'avoir dans un seul firewall le CSCSSP va pas rentrer dans ça dans ces détails là.

44:29
OK, maintenant si on parle par exemple des éléments de redondance points de point de vue de pare-feu, toujours est ce que on prend, c'est à dire on prend l'approche. Par exemple, si je prends le le le Thoot tierto là est ce que je devais faire de la redondance de la même façon d'un point de vue architectural ou je devais toujours concevoir mes mes, mes projets, mes projections en fonction de mon architecture tel quel.

44:55
Ta question c'est je je veux dire par là, chaque fois que je dois aller en redondance, je dois toujours considérer la même infrastructure, les mêmes les mêmes niveaux de couche que j'ai. Par exemple, si je dois choisir une architecture comme le tout tir tool hein, est ce que je peux le rendre redondant de tous les points de vue ? Donc routeur, firewall, firewall ou c'est toujours en tenant compte de certaines considérations spécifiques ? C'est les 2.

45:20
Initialement bon c'est on a, on a un principe qu'on avait dit hein, c'est de rendre les choses simples. Donc si tu as la même architecture, c'est plus facile pour toi même. Mais si tu as certaines spécificités qui veulent toi t'amener à ne pas avoir les mêmes, si tu veux là les les mêmes architectures de sécurité que tu as des spécificités. Oui mais idéalement, tant que c'est simple de part et d'autre, c'est plus facile en fait.

45:47
Ouais OK, un petit mot pour différent ? Tout dépend exactement quand tu parles de l'ordonnance exactement qu'est ce qui est critique ? Est ce que tu veux certainement faire relever toute l'organisation ? Ça veut dire que tu dois certainement reproduire un point ou alors c'est certaines applications que tu veux certainement avoir en redonnance. De là, dépendamment du budget que tu peux faire, mettons du 1.1 ou alors tu peux faire du un pour plusieurs donc ça veut dire que t'es pas obligé d'avoir sur le site de relève toute la même machinerie.

46:17
Que tu as sur le site de production, ça ça dépend encore des organisations et qu'est ce qu'on veut protéger et quel est le niveau du SLD ? Donc on peut le faire pour une pour certaines applications si on veut ça c'est des des actes qu'on voit assez souvent tout à fait d'accord, mais je je vais toujours d'un point de vue de ce qu'on prépare comme examen non ?

46:39

Voilà pourquoi je pose la question pour avoir justement les approches quand la question arrive, est ce qu'il faut qu'on considère les éléments, les éléments de de réponse de Jean-Marie par exemple, ou on doit avoir comme une un guide là bien spécifique ? Non ? Le le guide là spécifique, c'est de garder les principes comme redondance dans ta tête, garder la chose simple, un peu comme comme je l'ai dit, à moins ce qu'on te dise de façon spécifique, il y a un enjeu de budget, mais dans le CSSP.

47:05
Le on va vraiment te parler du budget quand on va calculer les risques, les aro ou AE, mais à ce niveau-là ils vont juste te dire pour tes sites de relève quel type de sites tu veux avoir mais on va pas rentrer dans la spécificité. Si tu as 2 firewall est ce que tu choisis une architecture tout tiers ou non ? Ils vont pas rentrer dans ces dans ces détails là, on va supposer que tu auras les mêmes architectures de part et d'autre.

47:31
Maintenant comme Jean-Marie le disait, S'il y a une spécificité qui fait que Ben en termes de coûts ou certains aspects qui font que tu veux pas avoir les 2 acteurs, tu il y a rien qui te l'impose en fait. Mais on rentre pas dans ces genres de détails là dans le contexte même de de l'examen parfait. Merci. Maintenant dans la pratique c'est autre chose. On continue.

48:01
Donc on a également la sécurité au niveau des dispositifs des endpoints, donc les endpoints on on parle de des ordinateurs, téléphones, tablettes ça donc la première protection. Nos fameux antivirus donc comme on le sait fonctionnent avec les signatures, donc ces séquences inconnaissables, mais les malware polymorphiques peuvent contourner les signatures. Donc on a l'héristique qui est basée sur des règles.

48:27
Des comportements typiques. Il est un peu différent de tout ce qu'est machine learning, mais il regarde quand même des comportements piques basés sur certains règles. On a nos EDR qui analysent des comportements avec des machines learning. Souvent des EDR plus poussés intègrent tout ce qui est analyse de comportements basé sur les signatures et l'iristique, les EDS, les EDR plus avancées. On a des coupe feuilles hautes qu'on peut avoir.

48:57
On a les HIDS ou HIPS, des host Days, IPS et IDS et on sur nos postes de travail on peut avoir des politiques d'authentifications fortes, notamment les MFA ou les authentifications biométriques qu'on peut avoir sur nos appareils. Donc on vient de finir le 4.2. Le 4.3 ce sont les canaux de communication sécurisés, donc on a la fameuse voix sur IP.

49:24
Et le problème de la voix sur IP, c'est que on a un l'habitant appelant peut être falsifié. Donc on a le vice mishing et on a le spip qui est le spam over internet téléphonie. Donc ça généralement c'est quand à un moment donné on on vous appelait. Et puis dès que vous décrochez la personne, la personne dirait un bon bon où la personne coupe. Il y a. C'était beaucoup fréquent je pense. Il y a un an, 2 ans environ, on avait beaucoup ça sur nos différents téléphones.

49:53
On a également comme problème le système de gestion d'appel et de téléphone peuvent être vulnérables. On a les attaques Man de Middle pour usurper la gestion des appels ou téléphones. On a

la falsification de l'authentification 802 un point X on ne peut également écouter les communications voix sur P en décodant le trafic, sauf s'il est Chypre. Donc ça c'est les enjeux qu'on a au niveau de la voix sur P.

50:18
Ça reste quand même que on utilise beaucoup cette technologie là. D'ailleurs, c'est avec ça qu'on est en train de faire notre cours actuellement. On a également un autre élément pour la communication, donc la collaboration multimédia. On a tout ce qui est courriel, donc les options de sécurité qu'on a. On a le diking qui lui va valider le domaine et l'intégrité du message. On a le SPF qui lui protège contre le spam et l'usurpation en validant l'adresse extérieure donc.

50:47
On peut autoriser des domaines ou des IP spécifiques pour communiquer, pour envoyer des messages à notre nom, on a le Dima, qui est le domaine base message Authentication Report Email Conformance. Lui il va, il renforce le SPF et le tekim et puis il va fournir des instructions sur le traitement des échecs. On a beaucoup d'outils sur Internet hein, qui nous permettent de de voir pour un domaine spécifique si ces règles sont appliquées. Donc dans votre compagnie, vous avez.

51:15
Le Talk Book, je je pense le ID Talk Book qu'on peut avoir regarder rapidement si les configurations sont pas là, s'il faut prendre des actions pour corriger surtout l'aspect SPF. Ensuite on a le s même qui est le seeker multiple pose Internet Mail extension qui lui va chiffrer le contenu du courriel, donc la signature numérique pour prouver l'identité et de l'identité de l'expéditeur. Ensuite on a tout ce qui est messagerie instantanée qu'on utilise.

51:45
Donc on utilise les protocoles sécurisés, une petite coquille. Donc on utilise les protocoles sécurisés comme signal protocole XMPT avec TLS. Donc ça c'est c'est au niveau de la communication multimédia. Ensuite on a les réseaux privés VPN, donc pour la connectivité privée sur un autre réseau.

52:19
Donc qui permettent le chiffrement. Donc on a un site, on peut joindre un autre site ? Ben on va utiliser le VPN pour interconnecter nos différents sites. Donc ça c'est la taxonomie des VPN. Donc on a Power un Priv VPN Network provider provision VPN. Donc on a le site site, on a le layer One.

52:45
Le GMPLS, on a le layer tour, on a le layer three, au niveau du layer 2 on a le point to point, on a le multi points, on a le Virtual private lan services, on a le IPI only Land services on ALTP 2V 3 on a le l 2 transport based ensuite à droite, ici on a les customer provisions, on a le Remote Access Volontari Turner.

53:14
On a le side to side ipsec, le grill, le IP in IP. Au niveau toujours du Remote Access, on a le compost éternel, L 2F, le P two p, le l 2TPV 2UV 3 on a le **** TM on a le 2 TM V 2, on a le ipisec, le SSL et le TLS.

53:40
On a également toujours dans notre taxonomie, on a les IP SEC, on a le Grey, on a les IP in IP ce à considérer, on a le pointe au point. Le Tenailing Protocol, donc lui va à capsuler le trafic p to p dans

les paquets IP via le grue. Donc c'est un protocole qui est obsolète. le P to p, on l'a vu tantôt au niveau de la taxonomie.

54:07
On a le layer tour, le forwarding qui lui redirige une connexion plutôt vers un serveur distant qui est encore obsolète, qui est aussi obsolète, et on a le layer tour turning Protocol, le l 2TP qui a une fusion du PPT plus du L 2F qu'on a vu tantôt. Enfin on a le Quantum key distribution, donc c'est une méthode de, une méthode cryptographique qui permet à 2 parties de partager une play secrète.

54:37
Donc il va utiliser la mécanique quantique, donc polarisation des photons dont sont les particules de lumière, comme on l'avait vu dans le coup de cryptographie. C'est le même concept, on a un chiffré, le texte est chiffré, il est déchiffré, il est déchiffré et puis après on a le texte brut. Donc la différence, c'est que lui, il va utiliser la polarisation des des photons pour la communication.

55:04
C'était tout pour cette partie là est ce que il y a des questions ? Oui juste une question au niveau de l 2TP la slide avant s'il te plaît. Puis ici on a dit que c'est la bon. L 2TP c'est la fusion des 2 mais on parle pas de chiffrement aussi hein, il y a aucun, il y a le chiffrement il y a le tu parles du LD.

55:30
L 2TP il y a pas de chiffrement non il y a pas de chiffrement, on ajoute du ipsec là-dessus. OKOK c'est ça ce que j'ai compris aussi là OK on ajoute du ipsec, je pense que attends je vais peut être mettre ajout du on le voit juste on le voit pas dans la slide, non il y a pas de chiffrement natif, il n'a pas de chiffrement natif, je vais le mettre pour que ça reste.

56:07
C'est bon c'est bon ? Ouais ouais c'est ça, merci. OK Ben on a fini la première partie, il y a la 2e partie pour l'examen pour l'examen du CSSP qu'on va voir tantôt Maria tour vas y oui oui ma question c'est c'est par rapport au.

56:34
Au chemin où on avait les firewall plus le routeur, le tiers là oui uhum donc ici par exemple parce que quand même en entreprise, disons qu'on a souvent 2 entrées internet et tout. Donc comment la connexion va se passer sur le routeur en fait c'est que ils vont on va, on va les brancher les 2 sur le même routeur ou Comment ça va fonctionner.

57:06
Les 2 accès internet, très très très souvent. Ce que je vois, chacun va tomber sur son, sur son routeur. En fait, c'est pour assurer la redondance hein. Donc chacun va tomber sur son routeur et puis on va rédiger à un moment donné le trafic vers les les routeurs, les, les firewalls.

57:25
Donc si on a une communication, par exemple de Bell, ça va venir Bell, on a souvent tellus donc on va le la communication va tomber sur son routeur. J'avais la main levée. Ouais vas y vas y donc si je comprends bien sur sur les rails du firewall dans ce cas-là il il y a juste des services à disons à désactiver et puis balancer sur l'autre, c'est ça ?

57:54
Ça généralement on s'assure que on a les les mêmes règles sur les 2 firewall mais est ce que est ce qu'ils le font et tout ? Parce que moi d'être là lorsque je veux toucher le firewall je sais que oui c'est juste ça que je vois mais en arrière je sais pas. Est ce que ça prend en charge vraiment les 2 en même temps ? En fait tu demandes si le firewall prend en charge les 2 routeurs qui viennent ? Oui c'est ça tes 2 entrées en fait.

58:23
Ok, est ce que quelqu'un a un additif ? Oui vas y ouais oui généralement ce qui se passe c'est que il y a des des routeurs qui ont plusieurs entrées. La plupart ont des ont plusieurs entrées et vous pouvez agréger toutes les 2 connexions sur le même routeur. Même les routeurs logiciels comme PPF 5, on peut mettre 2 ou 3 4 de réseau sur votre l'ordinateur et il va engranger les 2 connexions entrantes et.

58:52
Suivant que et ça va agréger les 2 bandes passantes et faire de l'eau de balancing. Et lorsqu'il y a une connexion qui qui qui ne marche pas, quand les 2 connexions marchent ils agrègent les 2 bandes passantes pour en faire une banque, une bande passante commune. Mais lorsque une connexion est défaillante, c'est la seule connexion qui marche qui est qui est qui est fonctionnelle quoi. Donc ça fait également de follower pour engranger selon les circonstances les 2 bandes passantes ou by bypasser une bande passante qui ne marche pas.

59:21
Donc dans ton, dans ton, dans ton, dans ton scénario, il y a ce Roux seul routeur. Là il y a pas de redondance pour le routeur. Oui, il y a des redondances, c'est à dire que les 2 connexions viennent sur des des ports wan différents. Et si les 2 connexions marchent, le routeur a la capacité d'engranger les 2 bandes passantes, supposant que vous avez un mégabit de part et d'autre, les la bande passante entrante sera 2 mégabits lorsque les 2 les les 2 connexions marchent.

59:49
Mais une fois qu'une connexion bon en Afrique on le fait souvent parce que ce n'est pas stable. Mais lorsque il y a une connexion qui tombe en panne, la seule connexion qui marche peut servir un peu de connexion pour toute la liaison quoi. Pendant que l'autre est en maintenance. Non ? Moi je parlais du seul routeur qui gère tout donc je me dis le seul routeur dans dans ton schéma tu as un seul routeur qui gère un seul routeur ? Si ce routeur là tombe qu'est ce qu'on fait hein ?

1:00:19
Si si ça tombe c'est que c'est que c'est que c'est que c'est en panne. Maintenant si vous voulez vous pouvez également faire, vous pouvez mettre 2 routeurs ensemble et les les mettre dans l'autre balancier aussi. Allez vous le faire, ça c'est fait. Jean-Marie Jean Roger vas y Merci beaucoup pour ton intervention, merci.

1:00:42
Ouais déjà c'était pour c'était possible que avoir 2 connexions internet et un seul routeur c'est inutile, ça sert rien dans le le le mon avis là ça c'est vraiment rien parce que ça ça n'évite pas le 5 2. Offert à moins que je sais pas. Donc pour moi c'est pas un scénario très très conseillé et mais si je crois bien l'autre camad elle voulait savoir également si tu as 2 routeurs, 2 connexions internet et comment le FAR fait pour choisir où est ce qu'il va envoyer le trafic ? Ça a été un peu ça sa question, je sais pas si je trouve.

1:01:10
Qu'on puisse la question un peu trop loin ou bien si elle peut repréciser, oui, la question est un peu liée à ça et c'est qu'est ce qui va être ton primo ? En fait est ce que tu vas prendre un réseau ? Primo, et et si par exemple celui-là est d'un tu tombes sur l'autre en fait quelque quelque chose du genre en fait, d'accord, d'accord. Ben oui, en entreprise il y a plusieurs mécanismes qui peuvent permettre de de gérer ça, tu peux faire le la balance, il s'appelle les premiers Trump à l'un après sur l'autre ou bien mais tu peux faire la la QOS pour.

1:01:40
Définir quel type de trafic utiliser telle bande passante, par exemple dans des entreprises où la voie a une importance, des réunions sont vraiment très très important, où ça, où il priorise, certaines communications voient à passer sur un lien principal.

1:01:56
Le, le, la data et tous les autres peuvent passer sur un lien clairement redondant et l'autre lien est utilisé comme follover de l'au de l'autre. Tu comprends un peu, c'est un peu comme ça que ça fait. Et sinon aussi y a des protocoles de de routage là ou bien avec les distances administratives ou bien avec les routes par défaut, tu peux choisir par défaut où ton trafic passe, sinon c'est s'il est disponible, ça passe par le 2nd. La redondance de cette façon là ? Il y a plusieurs mécanismes pour faire ça.

1:02:23
Merci OK merci Christian. Oui salut c'est juste pour ajouter un peu de de sucre dans dans la pâte là en fait il faut savoir que c'est pas concevable hein. Sucre avec pâte. Bon c'est juste qu'il faut-il faut juste savoir que.

1:02:48
Un routeur, lui, il vient généralement, il vient vide de configuration. Donc c'est à toi maintenant comme ça de définir comment tu veux qu'il fonctionne, dépendamment de la structure de sécurité que tu as dans ton entreprise ou alors de ce que tu veux qu'il fasse. Donc comme ça tu peux, lorsque tu as 2 connexions qui entrent, tu peux les agréger. Avoir 2 One, ça veut dire que tu as One un sur ton port un et One 2 sur ton port 2. Les 2 connexions arrivent maintenant. Y a des des mécanismes comme du du St One.

1:03:18
Quand tu vas activer ça sur ton routeur, les les pare-feu généralement micro fortunette et ils intègrent très bien ce ce principe là c'est que il va comme ça regarder le poids. La, il va avoir des métriques comme la latence, le chemin le plus sur le chemin le plus rapide pour atteindre la destination en fonction des métriques qu'il va observer sur les bandes passantes, sur les connexions entrantes. Il va comme ça choisir quel chemin qu'il va emprunter pour.

1:03:46
Envoyer ton envoyer ta donnée ou ton ton si tu vas accéder à une application. Si tu vas aller sur Internet en fonction des métriques, il va comme ça lui même choisir le chemin qu'il va emprunter. À côté de ça aussi, on peut couper généralement ça avec ce qu'on appelle la haute disponibilité. Ça veut dire quand on joint comme ça un autre routeur fortunette configure de la même façon qui va faire en sorte que si l'un tombe en panne, l'autre va prendre le relais. Mais la technologie toujours du SD One ?

1:04:17
Il va toujours prendre en charge la différence entre le s 2 bande et l'autre balance. Si parce que l'autre balance c'est aussi une technologie qui permet aussi de gérer 2 bandes passantes qu'il y a entre comme les collègues l'ont si bien dit, puis comme ça jumeler les bandes passantes. Tu as une condition de un méga et l'autre de 500 qui le sait pas trop. Un jumelle peut te donner un tunnel plus grand, ça c'est une fonctionnalité de l'autre balancing, mais l'autre balance il peut aussi faire en sorte que.

1:04:40
Il ne jumelle pas les connexions mais il fait un peu comme du SD One. Il va choisir le chemin le plus rapide, le plus sûr pour atteindre sa destination en fonction des métriques. Et tu vois dans le routeur c'est c'est les les. Les notions sont un peu semblent abstraites et compliquées, mais une fois que tu es dans l'équipement, ça se parle tout seul parce que c'est des technologies qui sont dans intérêts dans les dans les routeurs et tu actives juste des cases. Et puis ça se met en place particulièrement toute seule.

1:05:04
Au-delà de ça aussi tu peux compliquer, tu fais tes routes statiques toi même tu définis tes chemins en fonction du OK mon paquet pour toute l'application passe par tel Internet moi si je veux atteindre mon V là ça passe par tel par tel truc donc tu définis comme ça tes trucs c'est un peu ça en fait. Merci Christian. Les chemins dont il parlait on a parlé tantôt des protocoles là pour faire des chemins, les OSPF et le RIP c'est ce sont ces protocoles là qui sont utilisés mais comme il a dit.

1:05:30
Dans le routeur c'est juste la configuration et puis les protocoles là vont se mettre en marche mais nous pour nous c'est important de comprendre comment est ce que le protocole fonctionne après dans le routeur une fois que tu actives la fonctionnalité Ben il va le faire seul. Merci beaucoup pour vos interventions, j'ai fait un vas y oui j'ai c'est pour apporter juste une mise en en situation d'un cas existant comme Abdoulaye le disait tout à l'heure pour le garder simple dans notre infrastructure, Ben c'est tout. Tout est redondant dans le sens que.

1:06:00
C'est 2 Bâtisses, 2 commutateurs, 2 routeurs, 2 têtes ainsi de suite et donc la technologie SDON, elle est utilisée comme l'a mentionné Christian tout à l'heure. Et à part ça, pour ce qui est des des protocoles, ils sont gérés par le par le pare-feu étant donné que c'est un de de nouvelles générations et ça fait que.

1:06:21
Quand la connexion Internet arrive, elle est tranquée dans de de de chaque côté des des commutateurs de tête qui envoient justement la le le le on va dire le trafic vers vers le le pare-feu. Et donc étant donné que on l'a connecté comme ça, il faut non pas seulement les mettre dans l'ordre dans un troc, mais il faut aussi les croiser de telle sorte que dès que tu déconnectes une paire ou un câble, mais le trafic est tout de suite redirigé vers l'autre.

1:06:50
Et en considérant les éléments de poids comme le disait Christian, mais c'est toujours. Mais nous dans notre cas, on a utilisé le BGP. Mais c'est ça fait quasiment la même affaire quand un temps tout de suite l'autre détecte par l'attente de quelques millisecondes Milli bits et puis il retourne tout de suite

le trafic vers le 2nd qui continue à fonctionner. Je sais pas si ça répond de façon globale là à la question de de Marie Atoul, non c'est bon vous avez il en ai beaucoup Abdoul.

1:07:20
Abdoul aminou, alors merci. Alors ce que j'aimerais ajouter c'est que aujourd'hui, avec la technologie SDN par exemple chez Forty Gates, ce que j'ai vu faire c'est que quelque soit le nombre de connexion internet, on peut les gérer à travers le pare-feu. D'accord, toutes ces connexions, elles vont arriver sur le pare-feu et à travers la technologie SD One aujourd'hui chez Forty Gate.

1:07:46
D'accord, ça me permet de gérer les connexions et même de spécifier les services en fonction des connexions. Je je donne un exemple, j'ai par exemple une connexion sale et j'ai des j'ai certains services. Je vais dire je peux dire Ouais je peux critique c'est ça ? Alors je peux décider de dire alors ?

1:08:10
Pour ce service critique là je prends peut être ça peut être peut être Office 365 ou bien bon ça dépend. Alors je peux lui spécifier à travers mes règles SD One clairement que toi tu ne passeras que par la connexion X et donc je peux également le dire.

1:08:34
Je prends un autre service, je lui dis tu passes par ici ou bien tu utilises les 2 connexions à à à un instant donné. Donc ça veut dire que dans le SD One, ce que moi j'ai vu faire chez Portugais en fait je peux gérer mes services comme je veux, quel que soit le nombre de connexions que j'ai. Mon pare-feu est assez intelligent pour me permettre de les gérer et de mutualiser les flux afin que je puisse garantir quand même.

1:09:03
Un certain je vais dire fluidité, une certaine fluidité à à mes utilisateurs sur mon réseau vous voyez. Donc c'est je ne sais pas ce qu'il en est chez les autres mais par contre chez Forty Gate moi j'ai bien vu la technologie SD One c'est encore à travers.

1:09:28
Ce protocole, on gère bien les connexions internet, quel que soit le nombre de connexions internet. C'est ce que j'ai voulu juste ajouter. Merci d'accord, Merci beaucoup pour vos contributions, les différents fournisseurs, Ben ils font tout pour généralement avoir les mêmes fonctionnalités, donc c'est c'est sûr que tu vas retrouver ça chez Palo Alto, chez Checkpoint, à un moment donné, c'est beau, on continue. Ben on avait fini avec ça, c'était.

1:09:58
Passer sur les recommandations pour l'examen. Ben on va aller à la pause. On va aller à la pause et puis on va revenir à 19h55 pour faire la 2e partie. 20 h, OK OK, on se retrouve à 20h00 pour terminer.

1:28:38
Oui Allô, vous êtes là. Bonjour, OK, c'est bon Émile Émile, OK c'est ça. À ta question de de dit base, tu avais demandé, est ce que c'était de la bande de base ? Oui effectivement, c'est bien la bande de base. Ouais, on va continuer.

1:29:10

Pour la préparation à l'examen cssp donc voilà 2e partie, on va juste donner les conseils, comment est ce qu'on prépare l'examen et puis comment est ce que l'examen se déroule après qu'on a eu l'examen ? Qu'est ce qui se passe après ? Bon, on a je crois une trentaine de slides, donc ça va aller vite. La séance prochaine on va faire une révision de.

1:29:37
De la plupart des éléments qu'on aura vus ici. Et puis Ben l'autre séance ça sera l'examen final, pardon la demande le la séance pour si c'est pour quand quoi ça la la prochaine séance ce serait pour quand puisqu'on a dit que on a retenu que l'examen c'est le 9 ou bien c'est oui attends je regarde, oui c'est le 9, oui le le mercredi, le mercredi 2 juillet on a une séance OK et puis l'examen c'est le.

1:30:08
Je vois que dans mon calendrier j'ai un cours le 9 et puis j'ai un cours le 10. Est ce que vous avez ça ? Vous avez un cours le 10 ? Oui seulement pareil dans le calendrier OK c'est ça ? Bah l'examen c'est le 9 non oui l'examen c'est le 9 OK de toute façon on n'a plus rien à et on n'a plus de de séances à faire encore donc.

1:30:36
OK mais bon si vous si vous êtes dispo je suis dispo on peut venir le 10 juste pour janvier ? On continue Monsieur oui Bonsoir Monsieur, est ce que cette partie est, est ce que cette partie est incluse dans le quiz, la préparation de l'examen, le quiz, le quiz 4 oui ce qu'on a vu aujourd'hui, oui c'est c'est inclus dans le quiz 4 ce qu'on a vu celui-là non pour préparer l'examen je.

1:31:06
Je pense pas, non lui n'est pas, il n'est pas prévu, mais le cours qu'on vient de voir oui est prévu dans le et puis ça commence je pense. Aujourd'hui d'accord, mais pour l'examen elle n'est pas inclus. Non l'examen pour l'examen final c'est tout ce qu'on a vu ensemble. OK c'est bon, d'accord OK, mais y a la préparation c'est pour vous même les les techniques pour vous c'est pour.

1:31:33
Y a pas de question pour ça. Oui oui tu avais la main. Oui oui j'ai j'ai la oui Monsieur Fofana, Bonsoir. En fait ma question c'était d'avoir cette précision là sur l'examen lorsqu'on est en mode révision de ce qu'on a vu ensemble ? Ou bien c'est plutôt l'ensemble du coup CISSP qu'on a vu depuis l'autre professeur ?

1:32:00
Moi c'est pour voir l'ensemble de des cours. On a si tu veux des des petits résumés de CSSP qu'est ce qu'on va revoir ensemble ? Non non je parle de l'examen va porter sur non l'examen ça sera juste ce qu'on a vu. Mais la révision de moi je parle c'est vraiment il y a des petits, il y a des petits aides mémoire pour la préparation de l'examen, c'est c'est ça qu'on va voir ensemble.

1:32:29
C'est bon ça marche. Merci oui Jean Jean Roger, Oui Monsieur j'avais une question concernant l'examen, l'examen final, là est ce que ça sera dans le type examen socième c'est c'est c'est ISP ou bien c'est juste comme examen de de session en fait ? T'as vu l'examen ? Ça sera comme l'examen intra OK ?

1:33:00
Oui Amani, oui c'est pour savoir. Est ce que tous les slides que nous avons vu aujourd'hui sont

actuellement disponibles dans le moodle ? Je crois pas avoir vu ça non ce que on a vu le premier cours, oui celui-là est non je vais le mettre après d'accord OK ce site l'a pas vu ça que tu es passé avant moi j'avais pas encore fini d'accord OK d'accord parce que je l'avais pas vu, d'accord merci OK oui Nadine.

1:33:30
Oui ma question pour la semaine prochaine pour le 2, est ce qu'on aura des préparations à la à la certification ou un cours ? Non c'est pas un cours, c'est juste une révision des aides mémoires qu'on utilise généralement pour préparer l'examen. Ok parfait mais en fait c'est pas c'est pas c'est pas votre examen que vous avez le 9, c'est l'examen du CSSP. Maintenant c'est clair que il y aura des éléments qu'on a vu ensemble qui peut vous aider à à préparer votre examen aussi du 9.

1:33:59
Ok donc pour mais l'examen d'une l'examen du 9, c'est seulement ce qu'on a vu ensemble, ce qu'on a vu, la 2e partie jusqu'à aujourd'hui. Ouais, donc ce que moi j'ai fait, ce que David a fait. Et puis les autres séances que j'ai eu à faire, toutes les séances que nous on a fait, sauf celui de Dominique, celui de Dominique, on considère que c'était le bloc un, ça c'est le bloc 2, ça, ça sera. Les questions de l'examen final seront juste sur le bloc 2.

1:34:29
Oui merci. Une question, est ce qu'on peut passer l'examen CSP à tout moment où il faut un délai après le 9 juillet ? Non, l'examen du CSSP tu peux le faire quand tu veux, ça n'a rien à voir avec ton examen. Ton examen de l'université tu peux le payer quand tu te payes le 749 pièces US puis tu ouais tu peux le tu peux le faire quand tu veux, c'est ça c'est bon.

1:34:58
Mais faut pas aller gaspiller ton argent hein. Si t'es pas prêt ou prendre le Peace of mind pour avoir un replay, OK on commence OK donc on va parler du CSSP, C'est petite intro du CSSP, comment s'inscrit pour l'examen ? Et puis la préparation, moi je dirais.

1:35:25
Et en 6 mois, il y a il y en a qui prennent un an souvent pour préparer. Ça dépend du rythme de chacun, de comment est ce que chacun planifie et puis ses les autres activités, la préparation jour avant et puis le jour, le jour de l'examen. Et puis la suite, qu'est ce qu'on fait après quand on a le CS SP Ben le CSSP Certify Information System Security Professionnal.

1:35:53
Ben, certification internationale offerte par IC Square, connue mondialement. En tout cas si vous avez le CSSP on on va plus reconnaître le CSSP peut être que vos diplômes à l'université. Je parle du monde du monde entier de façon générale. C'est sûr que dans le domaine de la sécurité, là où vous voulez travailler, il y aura des gens qui qui connaîtront le CSSP donc.

1:36:18
Ça, ça parle plus vite souvent que le diplôme universitaire, souvent quand l'université n'est pas connue. Ben la la certification et une agricultation de anti ISO 17 24. Le CSSPA est équivalent au niveau 7, donc un master en cybersécurité de regretted qualification framework au Royaume-Uni au UK.

1:36:46

Pour leur système de reconnaissance des diplômes étrangers. Donc ça veut dire quoi ? Si vous avez votre CSSP, si vous êtes à au Royaume-Uni, vous on considère que vous avez le master en cybersécurité, donc toutes les formations. Si vous voulez faire un PHD juste avec votre CSSP, vous pouvez aller faire votre PHD même si vous n'aviez pas fait un master, vous n'aviez pas eu un master sans point de difform dans une université.

1:37:13
Ensuite, public cible, Ben professionnel en cybersécurité, les ciseaux, architectes en sécurité, analyse en sécurité, consultant. Je connais des personnes qui étaient avocats, qui ont fait leur CSSP, qui sont CSSP aujourd'hui avec tout ce qui est protection des renseignements personnels, c'est sûr que on aura des personnes qui font juste la conformité, qui vont qui font aussi leur CSSP, donc on ferme pas la porte.

1:37:43
Tant que la sécurité vous intéresse, vous pouvez aller chercher votre certification expédite. Oui oui j'ai, j'ai une petite question, hein, qui ? Nous, nous qui venons d'un système purement francophone à des niveaux de responsabilité donné, on se trouve confronté à un problème. Le problème le suivant, c'est que lorsque vous évoluez, vous êtes dans la technique pure dès le début. Mais quand vous avancez au fur et à mesure que vous atteignez peut être le rôle de ciseaux.

1:38:13
Vous faites beaucoup plus de temps à gérer des équipes qui travaillent avec vous. Donc vous, vous n'êtes plus dans l'opérationnel, vous n'êtes plutôt dans la technique, mais vous êtes dans le leadership, dans le management, dans la gestion peut être des acquisitions ou beaucoup de choses. Vous comprenez si bien que ce rôle dédié à une certaine technicité vous échappe de plus en plus. Mais là, quand on vous dit que Ben écoute ce le fait d'avoir la certification qui n'est qu'un qui n'est qu'un pas.

1:38:42
Ne serait-ce que minime de votre activité en tant que ciso remplace peu ? Remplacer par exemple un diplôme universitaire où on vous apprend déjà beaucoup de choses, la rédaction par exemple des rapports, la rédaction des d'un certain nombre de documents administratifs. Comment gérer les ressources humaines qui ont pris le qui ont pris le pas sur la technicité pure dont relève un peu cette certification CSP ? Moi je me pose la question de savoir.

1:39:12
Mais est ce que ce que ce qui est valable vous avez dit que ça a pris la place dans un certain nombre de pays ? Est ce que c'est valable dans le monde professionnel dans lequel nous sommes ici ? Je sais pas si ma question a été perçue. Merci. Oui je comprends, j'ai essayé de répondre bon c'est pas dans tous les pays, c'est déjà assez au Royaume-Uni. Mais moi quand je regarde le CSSPI, c'est vrai que la formation du CSSP c'est pas une formation classique d'un master en cybersécurité on s'entend.

1:39:42
Ici on va pas te demander de faire des devoirs, quoi qu'on peut le faire hein, on va pas te demander de faire des devoirs tout ça. On vient, on explique les concerts, on fait les quiz, on s'entraîne, on s'en va faire. Mais si vous avez bien regardé tout ce qui est CSSP depuis le cours que Dominique a donné, le CSSP c'est plus managériale en fait. Donc même dans les questions, je vais en parler même dans les questions du CSSP, c'est pas trop la technique, c'est vrai.

1:40:10

On est souvent issu des milieux techniques, on a soit des développeurs gars du réseau et puis après on vient faire le CSSP. Mais le CSSP c'est pour t'amener à être à un niveau de manager gestionnaire de la cybersécurité. Donc c'est pour te donner en fait ce mindset là de gestionnaire. Donc toutes les questions de CSSP ça va tourner autour de la stratégie, la gouvernance. Donc je tu tu vas le voir, je je vais en parler. Donc si quand tu réponds à une question de CSSC que tu es trop technique, tu vas échouer ton examen.

1:40:40
Donc oui, tu ne fais pas de RH, tu ne fais pas tout ce qui est classique comme dans un master. Mais eux ils se disent selon le Body of no les du CSSP, ce que le CSSP apporte, on peut le mettre au même niveau qu'un master sans cybersécurité. Je pense que c'est ce raisonnement qu'ils ont fait, mais de façon quand je regarde le CSSP et le le CSSB qui est un peu.

1:41:06
L'équivalent en termes de gestionnaire de de certification des gestionnaires. Ça t'amène cette vue business de ton métier de cybersécurité, c'est bon ? Oui Amadou, oui Monsieur, j'aurais une question. Je voulais savoir qu'est ce que vous dites des des gens qui disent et même le prof au début du cours, il avait dit que même si on prend le cours ici, même si on prend des cours en ligne et qu'on on étudie le CSPCSSP.

1:41:35
Il faudrait attendre quelques années de pratique avant de prendre l'examen. Quel quel est votre avis là-dessus vous d'après vous ? Est ce que vous pensez que en prenant ce courtier des cours en ligne qui sont donnés on ne on serait prêt disons dans 6 mois ou il faudrait attendre d'avoir énormément de Ben énormément au moins une bonne ?

1:41:53
Au moins une bonne expérience en cybersécurité avant de prendre l'examen parce que le CEH ça se fait mais le CSSP apparemment il faudrait avoir je je je pense que le le contexte dans lequel Dominique a dit c'est peut être pour la validation de ton CSSP parce que ça va te demander d'avoir 5 ans d'expérience professionnelle. Je pense que c'est dans ce contexte-là qu'il a dit mais pour le CSSP si tu fais le CSSP que tu n'as pas les 5 ans d'expérience.

1:42:22
On te donne une certification, j'ai pas le nom en tête mais on te donne une certification pour dire que tu as validé l'examen et là si tu continues de rester dans le domaine Ben quand tu si tu peux valider tu peux prouver à IC Square que toi tu as eu tes 5 ans d'expérience. En réalité c'est 4 ans plus une année universitaire. Si tu tu as le Bachelor et autre tu tu as tes 4 ans, tu leur envoies des un message, ils vont valider puis ils vont te donner ton CSSP. Donc moi je dirais si vous.

1:42:52
Et faire le cours, ne rester dans la logique. C'est vrai que avec ce cours là vous allez peut être réviser le document de CSSP. Je vous encourage à le réviser, à faire les tests et puis allez y faire votre examen si vous le prenez même si vous n'avez pas l'expérience. Au moins vous avez ça. Moi je moi je vais avoir moi dans un un recrutement. Je vais prendre quelqu'un qui a déjà eu son examen de CSSP, quelqu'un qui n'a pas eu.

1:43:18
Parce que je je sais que lui on va se comprendre, il il connaît, s'il a eu l'examen, il il il sait de quoi il

parle. Ouais voilà donc voilà c'est ça, je pense que c'est c'était dans le contexte de validation du CSP. Est ce que Dominique l'a dit ? Oui effectivement OK merci, est ce que merci d'ajouter des petites choses ? Oui vas y vas y Émile vas y j'avais j'avais mentionné aussi dans un cours précédent.

1:43:44
Au niveau du TSSP, puis même chez AISIS quoi, il y a souvent des des talks qui font là-dessus, ce qui ce qu'ils peuvent recommander. Puis c'est une des questions qui reviennent souvent. Déjà tu peux t'inscrire que tu peux faire un examen. Toi de base t'as le si si c'est cyber Security, c'est un des certifications de base, mais le but c'est que tu deviennes mettons associé si t'as pas nécessairement ces années d'expérience.

1:44:14
Tu peux devenir associate of ISC. Déjà de base aussi des formations universitaires, ça, ça compte en termes d'année d'expérience, il y a aussi des certifications comme le CEH. Le CEH compte pour un an comme par exemple.

1:44:35
À WS ça peut compter aussi comme expérience. Donc tu peux t'accumuler de l'expérience en termes de certification mais aussi au niveau de tes expériences professionnelles tant que tu fais minimum 222 modules. Bien d'expérience dans 2 dans 2 sphères sur 8 c'est ça 2 sphères sur 8.

1:45:02
Ça compte aussi comme expérience. Comme doula il le mentionnait. Il y a des avocats qui faisaient ça parce que il y avait de l'expérience, il y avait des expériences genre gouvernance droit, puis tout ça comme un un pan testeur ou quelqu'un qui fait du réseau, ou quelqu'un qui a fait de la gestion des accès. Et évidemment t'as 3, t'as 3 domaines là fait que t'as plus comme ils disent dans les talks là.

1:45:27
T'as plusieurs méthodes pour accumuler tes années d'expérience, mais après ça, tu peux contacter quelqu'un que son CSSP. Tu jases un peu, prends un café à Montréal, peu importe d'un d'un café, t'expliques ton expérience, tout ça, ça se fait bien. Puis tu demandes ton order semaine, mais comme je te le dis, faut pas nécessairement avoir crainte de tout ça, c'est on se jette dans le vide, puis tout ça, puis on se prépare.

1:45:54
Et tu mets t'as différentes méthodes pour avoir tes années d'expérience ? Fait que ça vaut la peine. Inscris toi chez AISC Square, là il y a plusieurs talks que là-dessus t'as le AISC Square Summit que qui a eu récemment. Il y a d'autres talks qui arrivent bientôt fait que si t'es intéressé, puis en même temps t'es en t'inscrivant chez AISC Square, tu peux devenir avoir le badge.

1:46:23
De se candidate candidate au CSSP. Il dure à peu près un an, c'est ça uhum mais mais déjà d'abord tu peux même faire de CC qui est vraiment de base, qui manque quasiment pas d'expérience, puis c'est vraiment pas mal plus facile que CSSP. Puis t'aurais déjà une porte d'entrée.

1:46:46
C'est ça le le avant. On pouvait pas s'inscrire sur le site de IC Square comme ça hein. Maintenant ils ont facilité donc surtout avec le la certification, le site si dont parlait Émile. Maintenant on peut s'inscrire, il y a beaucoup de ressources là-bas qui vont vous permettre de de vous former donc ça

vaut la peine pour juste votre formation continue d'être là-bas puis pardon de d'occuper ta même. Ouais vas y vas chapitre.

1:47:15
Comme par exemple au Canada, il y a le chapitre de Toronto, il y a des gens membres de Toronto, de des gens outre-Atlantique, comme des chapitres d'Algérie. Tout ça, c'est c'est plein de membres de la Communauté qui sont, qui ont déjà le CSSP, qui peuvent s'entraider. Puis c'est vraiment une une idée d'entraide qu'il y a de derrière ça, puis même.

1:47:40
Ah je savais pas qu'il y avait le chapitre de Montréal. Ouais ouais, il y avait le chapitre de Montréal. Ouais mais te mais c'est vraiment mais t'as vraiment différents différentes ressources. Puis même dans dans certains cours du CSSP t'as même l'aspect communautaire. Tu peux si t'as des questions par rapport aux questions du CSSP, tu peux demander à la Communauté là je pense c'est un des services qui offre chez AIS 6 quoi pour aider les gens à se certifier là.

1:48:10
Bon merci beaucoup Émile Hayette, je pense que t'avais la main levée, tu l'as baissée. Est ce que Émile a répondu à ta question Si Watch vas y oui Bonjour Bonjour Monsieur Bonjour tu attends un instant ayette va ayette va parler ayette vas YOK d'accord merci. Je voulais juste savoir si vous.

1:48:35
Si on on a par exemple le certificat CSSP, ça veut dire on va viser des postes des gestionnaires de de haut niveau par exemple. C'est ça ? Non, c'est pas tous ceux qui ont, c'est c'est ceux qui sont gestionnaires. Voilà il y a il y a des gens qui sont peut être en réseau qui vont juste aller faire le CSSE pour comprendre le langage des gens qui sont en sécurité.

1:48:59
Il y a des gens qui sont représentants, par exemple des fournisseurs comme Fortinette, checkpoint, autres qui vont aller faire leur CSSP. Mais c'est pas tous ceux qui font CSSP qui deviennent gestionnaires. Mais quand t'as le le CSSP, tu as en fait tu es prêt. Tu as les atouts pour être un gestionnaire. Maintenant est ce que tout le monde peut être gestionnaire avec le CSSP ? Le CSSP à lui seul peut pas te permettre de d'être gestionnaire parce que ça prend d'autres compétences.

1:49:27
Mais ça te permet dans la sécurité d'être au niveau stratégie. Donc tout ce qui est juste tu vas pas rester juste côté opérationnel. La sécurité tu vas peut être faire niveau stratégie, faire les programmes de sécurité en tout cas un peu plus à haut niveau plutôt que quelqu'un peut être qui était juste dans l'aspect technique de la sécurité. D'accord merci.

1:49:53
Oui moi ma question c'était par rapport au au training qu'on a sur le site du CISAISI Square. Ouais donc là je me disais est ce que si je veux faire le l'examen est ce que je dois m'inscrire au cours aussi ? Genre c'est recommandé de non le le non ? Je pense que je pense que ce cours là je pense qu'il est suffisant ce que je te recommande.

1:50:21
J'ai, je vais vous recommander des applications ou des des des ressources que vous allez prendre dans dans ce que je vais présenter, tu vas prendre ça, il y a des flashcards, tu vas repasser. Peut être qu'il y a

des conseils qu'on a expliqué, peut être que on n'a pas bien expliqué, ça peut arriver qu'on n'est pas bien expliqué ou que on a expliqué mais tu n'as pas compris donc avec des Flashcards tu vas comprendre, tu vas faire tes tes tests, tu vas tu vas t'améliorer et puis il y a le official guard aussi de de.

1:50:51
Que que de IC Square. Moi je vous recommande de les de le prendre et puis regarder chapitre par chapitre de repasser les différents éléments qu'on a vu. Donc le fait d'avoir faire le coup, vous avez déjà vu la plupart des éléments mais pour renforcer, prenez le le guide ou regarder ça c'est un Deuxièmement, je vais vous donner ce qu'on va avoir la semaine prochaine. Un ensemble de ressources qui ont résumé certains concepts qui vont vous aider à à facilement comprendre les concepts.

1:51:20
Après ça fais juste des des questions pour te préparer parce qu'avec les questions c'est des mises en 4 pratiques des scénarios d'entreprise que tu vas voir dans les questions donc ça va te permettre de mieux comprendre les différents éléments que tu as vu au cours. Et après ça moi je je pense pas que tu aies besoin d'aller faire un autre cours encore. OK super merci OK oui expedit vas y oui merci c'est juste pour une petite précis.

1:51:50
Donc on pourrait avoir de vous des l'ensemble des questions sur lesquelles on pourrait s'exercer. Non moi je, moi je n'ai pas de banque de questions, moi je vais vous recommander où est ce que tu peux avoir des banques de questions pour t'exercer ? OK je je vais te donner les outils qu'il te faut, tout ce que moi je peux faire. J'ai des ressources gens qui qui résument un peu le cours, ça on on va vous partager ça.

1:52:17
Et ça ça peut t'aider dans la préparation c'est comme un aide mémoire, ça va t'aider dans la dans la préparation mais j'ai pas de banque de questions les banques de questions tu pourras peut être te faire une souscription ou acheter l'application mobile pour te préparer c'est bon ? Oui c'est bon correct merci. OK oui ayette Monsieur est ce qu'on aura toujours accès aux aux cours ?

1:52:40
Après la la fin de de la session parce que je je sais pas jusqu'à quel je pense tant que tu es étudiant, tu as accès au moodle hein je pense tant que tu as tu es étudiant, tu as accès au moodle au pire bon tu as tu auras ton onedrive auquel tu auras accès, donc tu pourras mettre tes cours là-bas étudiant une fois étudiant pour la vie hein. Quand tu as quand tu as étudié à l'université de Sherbrooke, tu vas toujours avoir ton courriel.

1:53:10
Mais à un moment donné, ils vont te couper les accès comme gatner je pense. En tout cas, tu n'auras pas toutes les applications en fait, mais tu auras toujours ton courriel de l'université de Sherbrooke donc tu peux garder tes cours là-bas. C'est bon OK, on continue ? Ben il y aura les questions. Au fur et à mesure qu'on va, on va, on va continuer.

1:53:42
Parfait donc ça ce sont les 8 domaines de sécurité du CSSP le premier, le premier domaine c'est

sécurité et gestion des risques, donc sécurité enerisk management. Donc souvent des gens qui vont faire conformité Ben ils pourront remplir ce domaine là donc.

1:53:59
Ici c'est plus les questions, on on est, on parle pas forcément des technologies mais on va parler de comment on a obtenu les risques, comment on traite la la gestion des risques, la gouvernance, la sécurité, la conformité juridique réglementaire. Donc quelqu'un qui est avocat, déjà il peut remplir le premier domaine, ensuite on a le 2e qui est sécurité des actifs AC Security, donc tout ce qui est sauvegarde des actifs c'est primordial.

1:54:26
Le domaine va se concentrer sur la classification, la propriété, le contrôle des actifs, donc en comprenant comment on protège les informations, traiter les informations sensibles et gérer la conversation des la conservation des données ensuite. 3 architecture et ingénierie, c'est c'est ce qu'on a vu ensemble, ça compte pour 13% les les 2 premiers respectivement pour 16 et 10%. Donc ce domaine est le schéma directeur des systèmes sécurisés.

1:54:54
Donc de la cryptographie au principe de conception sécurisée, ce domaine couvre les aspects techniques de la cybersécurité. La maîtrise de ce domaine vous permet de construire et de maintenir des architectures de sécurité robustes. Ensuite 4 on a communication et sécurité réseau donc qui compte 13%. Donc le domaine englobe tout ce qui est architecture réseau, des méthodes de transmission, des protocoles sécurisés. Un peu ce qu'on a vu la séance dernière et cette séance. Ensuite on a la gestion des identités et accès qui compte 13%.

1:55:24
Les contrôles d'accès sont des gardiens de la sécurité. Ce domaine aborde tous les concepts des IIM, des méthodes d'authentification et des mécanismes d'autorisation. On a le sys qui est évaluation et test de sécurité, donc c'est ici. On va regarder tout ce qui est gestion des vulnérabilités, tout ce qui est test de pénétration, les audits de sécurité ou autres. En fait on va faire sécurité des opérations, donc une tout ce qui est surveillance proactive, réaction rapide.

1:55:51
Donc ça va comprendre les opérations de sécurité, la gestion des des des incidents, la reprise après des incidents et le 8 c'est la sécurité dans le développement des logiciels. Donc ici c'est tout ce qui est va traiter la sécurité dans le processus de développement sécurisé des logiciels, y compris la pratique du codage sécurisé, les tests d'intégration et des contrôles sécurité pour avoir la le CSSP si vous passez le CSSP.

1:56:20
Vous devez prouver que vous avez l'expérience dans 2 dans 2 des 8 domaines pour pouvoir valider si vous en avez plus que 2. C'est bon. Donc en gros, ça, ça veut dire que si vous travaillez en conformité ou en juridique ou les ou réglementaire, vous avez déjà un domaine. Si en plus de ça, vous gérez tout ce qui est protection de l'information, les données sensibles, la classification, vous avez votre 2 domaines.

1:56:44
Si vous travaillez peut être dans la classification et que vous faites les les scans de vulnérabilité, vous travaillez dans la gestion des vulnérabilités. Vous travaillez avec les équipes qui font des audits de

sécurité. Ben vous êtes le site, là vous le complétez. Si vous travaillez juste dans la gestion des identités, c'est pas parce que vous êtes dans un votre type de poste s'appelle analyste en sécurité. C'est si c'est pas parce que votre liste s'appelle pas analyste en sécurité que vous faites pas de la sécurité. Vous pouvez être juste administrateur réseau.

1:57:12
Mais en tant que administrateur réseau, vous pouvez travailler dans tout ce qui est communication réseau et puis dans tout ce qui est architecture. Donc ça vous ça vous permet de valider en fait ces ces 2 domaines. Là j'avais une main qui était levée. Oui c'est bon Monsieur, je voulais savoir et comment on fait pour choisir les domaines ? Est ce que ils nous ils nous demandent lorsqu'on veut prendre l'examen de choisir ? Non on vous demande pas, non non non non non, tu fais ton examen.

1:57:40
Quand tu finis ton examen, tu vas venir faire ton prouver que tu as validé les 2 demandes. Tu vas renseigner un formulaire et c'est dans ce formulaire que toi selon ton expérience, tu vas mettre que tel domaine j'ai de l'expérience, tel domaine, j'ai de l'expérience et la personne qui va faire ton endersment là va confirmer que c'est c'est vrai que il te connaît. Vous avez tu as effectivement fait les les les tu as effectivement l'expérience.

1:58:05
Mais après c'est il peut faire aussi un il peut faire aussi un audit hein, il peut faire un audit pour s'assurer que ce que tu dis est vrai. D'accord, ça c'est pour la validation, après que tu aies passé l'examen, tu le réussis. Oui ça c'est après que tu aies passé l'examen. OK parfait merci exactement c'est bon on continue, est ce qu'il y a d'autres questions ?

1:58:25
Et moi j'avais une question par rapport là l'endosmètre là ouais c'est quoi qui va faire l'endosmètre ? C'est c'est une de tes connaissances qui a le CSSP Ah c'est ça la personne doit avoir un CISSP ouais ouais la personne doit avoir un CSSPOKOK merci ouais bon moi je t'ai eu au cours donc je te connais un peu mais si tu as eu ton CSSP c'est pas un problème tu viens me voir OK ? Super merci.

1:58:56
On continue donc l'inscription Ben on va sur le des personnes bio, on va sur la procédure, c'est pas compliqué, mais on fait pas d'examen au Québec à cause du projet de loi 96, donc la loi 14, donc les examens doivent être uniquement en français. Donc le type d'examen qu'on fait qui est le le 4, on le fait pas en français, c'est en anglais, donc ça aussi c'est c'est une autre chose.

1:59:28
Les examens généralement sont le type d'examen qu'on fait. Le 4 c'est en anglais donc on le fait pas en français, donc C'est pourquoi on le fait pas au Québec. Donc les options que vous avez qui sont en en 02h00 de Montréal, donc on a Ottawa et puis on a burlington aux États-Unis. Le coût de l'examen c'est 749,00$ US environ 130,00$ au taux 12 du jour 130$ canadiens.

1:59:58
1030 c'est 1400 1400OK et ça Ça te permet combien d'essais ? C'est te doit un retak là OK 2 c'est 2 essais puis il y a une auto motion à l'heure actuelle de 50 pièces de 50$ US de rabais sur le OK mais c'est c'est bon c'est c'est une option au moins.

2:00:23

Je t'ai dit je je vais la première fois, si j'ai échoué je reviens je vais faire comme ça je vais pas payer les les 1000$ oui m'avance Bonsoir Maxence, Ouais Salut je suis pas certain d'avoir bien compris pour l'examen de CISST, on a combien de de de possibilités de faire l'examen si jamais on échoue la première fois ?

2:00:48
Tu as plusieurs possibilités mais ils ont on va en parler les politiques tu peux le faire 4 fois maximum dans une période de 12 mois mais on va en parler tantôt. OK merci mais si tu es YAY en a qui le font plusieurs fois mais bon si c'est quelque chose que tu veux vraiment avoir je pense que après 2e tentative 3e tentative C'est ça devrait être bon. Et puis bon y en a qui l'ont à la première tentative aussi hein donc OK ça Jonathan.

2:01:18
Moi je voulais juste rajouter un élément là en tout cas ce que ce que j'ai lu le Piece of mind il est juste valide une fois là la première fois qu'on qu'on achète l'examen, là la seule chose c'est si on fait l'examen puis on l'échoue puis après ça j'aimerais ça en avoir 2 chances. Je pense qu'on peut pas là donc.

2:01:39
C'est en tout cas-là moi je je pense pour être sûr d'être. Tu sais-je vais prendre tout de suite le le Peace of Nine là. Mais ouais, c'est ce que j'ai pris moi aussi j'ai pris le Peace of Night en même temps ça te donne comme une assurance supplémentaire de OK, je l'ai échoué, parfait. Au pire j'aurais fait une passé une fin de semaine à Toronto pour ma 2e chance. Fait que ça, ça te donne un certain niveau de confiance, de confidence.

2:02:06
Puis c'est comme si c'était, c'est comme si tu transférais un peu ton risque ce coup ci. Mais bon vous pouvez prendre si tu veux pas prendre le Peace of mind, tu peux juste prendre un examen et puis bosser dur pour aller le valider. Oui Maxence, Ben et puis Émile, qu'est ce qu'on paye ainsi plus pour avoir la possibilité de faire l'examen ?

2:02:33
Le Peace of my est 998 si je me souviens bien. Cependant je pense que y ont y ont présentement le rabais sur un temps limité de 50$ US. Je pense que c'est 948 là mais ça te donne comme 2 2 chances là c'est bon OK c'est ça ? Est ce que excuse moi une dernière question sur ce Peace for my là, est ce que vous avez un délai entre la première et la 2e tentative ? Oui.

2:03:03
Oui, 30 jours, OK merci c'est bon, c'est bon bon la préparation ? Ben on est en plein dans la préparation, je dirais un à 6 mois, c'est ça peut prendre un an dépendamment de de vos activités et votre charge de travail. Ce que vous devez retenir, c'est que la certification CSSP est réputée pour couvrir.

2:03:33
Un très large contenu sans jamais le créger en profondeur. Comme vous l'avez remarqué, il y a des concepts, on reste vraiment à haut niveau, on on descend pas trop, c'est comme la station qui est en dessous et my wide betolli et inch Deep. Donc on est large mais on on est juste une pouce, un pouce de profondeur, on va pas en profondeur donc c'est fait pour que on puisse comprendre.

2:04:01
Tout ce qui tourne dans notre environnement, notre environnement de sécurité comprend pouvoir parler avec les experts de différents domaines sans forcément être expert et puis être capable d'amener toute la sécurité dans ces éléments là. Donc c'est c'est c'est vraiment ça le concept. Et puis pas juste la sécurité sur l'aspect opérationnel mais plus l'aspect gouvernance. Comment est ce que on va mettre en place la stratégie, les processus sans forcément juste à à résoudre le problème ponctuel ?

2:04:31
Oui on peut résoudre le problème ponctuelle mais on veut résoudre le problème sur le long terme. Donc c'est plus ces mindsets là que on on vous apporte. Oui désolé oui oui merci. Ma question va ma question concerne les certifications intermédiaires, est ce que est ce est ce que vous nous conseillerez de prendre des certifications ?

2:05:00
Des éducations fondamentales comme Contia Security plus ou contia en euro plus avant de se lancer dans le CS le CSSP. Ou alors on peut se lancer directement dans le CSSP sans sans cette sans cette fixation intermédiaire. Ça dépend de ton parcours tu vois, ça dépend de ton parcours. Moi quelqu'un qui est juste aux études, qui travaille pas, qui veut rentrer dans le domaine de la sécurité, oui je peux lui dire va faire comme tu as.

2:05:31
Comme tu as plus plus pour montrer que tu as les rudiments, va faire ton C et h tout ça. Mais si tu te réveilles déjà en en en TI, que tu fais déjà les 2 domaines ou que tu fais déjà un domaine, moi je te dirais cherche à compléter l'autre. Va prépare toi pour faire ton CSSP. C'est parce que c'est pas le même niveau de reconnaissance dans les entreprises, c'est c'est pas le même regard tu sais un comme tu as plus et puis.

2:05:57
Un CSSP c'est pas pareil, tu vois que il y a trop d'exigences pour l'avoir même si tu as l'examen il faut attendre 5 ans. Partout où la barrière d'entrée est est est est complexe, ça veut dire que il y a moins de gens qu'on prend, donc quand il y a moins de gens qu'on prend c'est plus intéressant. Donc si la barrière d'entrée est faible il y a beaucoup de gens qui vont l'avoir donc faut aller faire des choses que c'est vrai que je je j'avoue. Un le CSSP c'est pas un examen qui est facile.

2:06:24
Vous allez, vous avez fait le cours, vous allez lire le document du CSSP. Quand vous allez commencer les tests, vous allez vous poser la question, est ce que c'est ? J'ai effectivement fait le cours ou bien j'ai effectivement lu les documents si vous avez effectivement lu mais pour pour comprendre les questions, faut comprendre le ministère dans lequel on fait les questions pour pouvoir répondre. Et puis quand tu vas faire le parcours du CSSP, quand tu vas avoir ta certification, tu seras fier d'avoir eu ta certification et ceux qui ont fait le parcours du CSSP.

2:06:51
Quand quelqu'un l'a, c'est c'est eux qui sont dans les entreprises, c'est eux qui sont des des recruteurs. Donc si tu as le CSSP, quelqu'un a fait le CSSP il il il connaît son parcours, il connaît ton parcours donc il sera plus à l'aise de t'avoir comme collaborateur que quelqu'un qui a contient plus. Donc moi je dirais si tu tu es déjà en en, tu travailles déjà pour aller faire ton CSSP laisse les contia c'est bon.

2:07:19
Allô ? OK c'est oui c'est correct, c'est correct, merci c'est bon. OK, de toutes les façons là en entreprise, faut chercher à être proche de la haute direction, faut toujours chercher à être à à côté de la haute direction, donc partout on va parler de business. Tout ça cherche à aller vers là-bas mais n'abandonne pas la technique, faut comprendre la technique, mais il faut toujours intégrer tout ce qui est business dans dans ce que tu fais, même si tu es un gars en pays.

2:07:47
À la fin, il faut comprendre tous les aspects de gouvernance. On dit on continue. Donc pour la préparation, Ben quand pour l'heure approche, je dirais un mois, un à 6 mois de notre date d'examen, Ben il faut réviser. Se donner un un à 02h00 de séance par jour, ça peut se faire hein facilement c'est il faut vous donner quelques nombres de pages à relire.

2:08:16
Donc ça peut être les séances qu'on qu'on est en train de voir ensemble. Ça peut être des ressources comme le guide qui est là ou il y a un autre document que je recommande qui est out to fanclaught et manager pour essayer essayer de faire exemple. Donc ça c'est de bonnes ressources que vous pourrez utiliser pour vous préparer et Bill et si je peux rajouter pour le vivre là.

2:08:38
Je me donne à peu près une à 02h00 par jour de d'écoute, de révision que tu veux. Enfin c'est très très très très très vrai. Là ouais, c'est, c'est rigoureux. Émile, étant donné que ton temps d'examen est proche, tu es, tu, tu restes. Bon je sais pas, après tu pourras m'écrire si t'es pas loin de moi.

2:09:00
Je vais te passer ce livre là, je l'ai out of funk like a manager pour que tu t'écris pas. Ouais Ouais Ben écoute moi j'étais à Québec là fait que Oh Oh c'est loin mais mais ton ton examen c'est quand c'est pour quand c'est 15 juillet à Ottawa ? OK écris moi peut être que j'ai prévu être à Québec avant ça je je vais peut être te donner le le livre écris moi après en privé on va ? Ouais OK parfait OK.

2:09:30
On continue pour toujours se préparer. Il y a les banques de questions, donc on a une banque avec le le stade du guide qui vient avec des banques de questions. Vous allez vous préparer ça, ça va de 1000 à 2000 questions. Mais attention, c'est pas parce que vous préparez les banques banques de questions que vous allez trouver exactement les mêmes questions à votre examen. Les banques de questions vous préparent à avoir.

2:09:57
Un peu l'esprit, le tas d'esprit de l'examen, mais c'est pas évident. En tout cas j'ai pas encore vu quelqu'un qui m'a dit qu'il a retrouvé ses les questions des banques de questions dans l'examen c'est c'est vraiment différent. Mais en faisant des examens, en faisant les les examens d'avec les banques de questions, ça vous pouvez pas, ça peut pas votre mindset ? Donc vous pouvez prendre celui de, de, du, du Guide officiel, donc ça vous aide.

2:10:21
Et dans votre préparation, arrangez vous à ce que dans tous les domaines vous ne soyez pas en dessous de 80% ? C'est que pour voir si vous êtes prêt, assurez-vous que pour toutes les questions, tous les domaines, vous vous êtes-vous êtes capable de trouver 80% des questions.

2:10:41
Vous allez revoir les chapitres. Si les notes sont en dessous de 80%, ça veut dire que il y a des éléments que vous n'avez pas compris. Des fois vous pouvez comprendre le chapitre mais souvent c'est la question qui est compliquée que vous n'arrivez pas à comprendre. Donc ça faut pouvoir marquer ces questions-là et puis les réviser. Puis à un moment donné, Ben c'est de de comprendre le concept, mémoriser le concept de la question pour que vous puissiez répondre au cas où vous tombez sur une question pareille. Des fois il y a des questions de CSSP, c'est.

2:11:11
Tu, tu, tu c'est c'est compliqué parfois de te dire j'ai compris la logique de la question et puis prochainement si on me pose je vais je vais trouver. Il y aura forcément une ou 2 questions comme ça qui qui vont vous fatiguer mais la plupart les 80% sont atteignables si vous travaillez beaucoup. Donc les ressources comme je l'ai dit le 6 Stadi Guy qui est là, il y a besoin que pour pouvoir avoir besoin exhib je pense que il y a des amis qui l'ont mis et moi ma meilleure application c'est learn.

2:11:39
Learn zap je pense que j'ai j'ai mis l'in zap au lieu de l'in zap. La meilleure application que moi j'ai utilisée c'est learn zap. Pourquoi ? Pourquoi ? J'aime beaucoup l'application d'abord elle est mobile donc j'ai pas besoin d'avoir à chaque fois 1£ avec moi pour faire la révision et tu peux te donner un certain temps, tu le revis de quand tu es disponible.

2:12:09
Quand tu es disponible, tu peux te donner un bout de temps chaque jour, chaque jour 30 Min tu tu places, tu passes tes flashcards et puis tu fais un examen de 30 Min. Tu tu habitues ton cerveau à à faire des examens et puis à à pouvoir les faire en en en à respecter les 01h01 2 c'est la question un peu que je donnais à ayette. Elle demandait pourquoi est ce que les les questions des quiz ça fait 10 questions et le temps était petit.

2:12:38
Mais c'est c'est c'est ça les questions de du CSSP c'est une minute 20, c'est 11,21 ,2 Min par question donc c'est encore plus petit même que les examens, le quiz. Voilà mais c'est clair que il y aura des questions qui seront plus faciles, donc vous allez gagner en temps. Mais la moyenne c'est ça 1.2 par question.

2:13:00
Donc ça je recommande cette application. En tout cas elle est j'ai. J'avais utilisé plusieurs applications mais elle je trouve que elle est beaucoup plus. Il y a beaucoup plus de fonctionnalités pour surtout suivre les vos performances dans les différents domaines. Et puis au fur et à mesure que vous faites l'examen, il est capable de vous dire quel est votre niveau de le niveau de confiance qu'il vous donne pour que vous puissiez passer l'examen. Donc en tout cas j'ai trouvé que c'est une très belle application hein.

2:13:30
Non il y a rien, il y a rien de gratuit à ce niveau-là, on te parle de CSSP donc il y a pas il y a rien de gratuit, c'est payant. La seule chose qui est gratuit pour l'instant c'est le CC que t'as la formation gratuite plus tellement gratuit il faut que tu te déplaces mais le learning zap c'est ça. J'utilise puis j'ai pris un abonnement 6 mois, là c'est ça, tu peux prendre 6 mois tu tu peux, ça va ça ça va dépendre de ton.

2:13:59
Ta préparation, si tu veux, tu peux prendre un an, puis te donner le temps. Si, si. Par exemple, tu as planifié ton ton examen pour un an. Mais tu peux faire comme 1000, prendre 6 mois et puis tu peux faire une extension après. Mais en tout cas, planifier ça dans les 6 prochains mois. Si vous voulez les faire comme ça, ça vous met un peu de pression pour vous préparer. Et puis commencer à à pratiquer, c'est bon.

2:14:24
Et il y a d'autres applications. J'ai, il y a d'autres applications mobiles, mais la meilleure c'était le donc c'est pas la peine de de vous parler des autres applications. Bon un jour avant, Ben un jour avant on se panne pas comme Émile Émile le 14. Ce que tu fais c'est pas le temps d'étudier, donc le 14.

2:14:48
Pas la peine d'étudier de même temps de de de toute manière faut que je parte de Québec à Ottawa de toute manière c'est ça. Donc tu te détends de cuisto. Le sommeil est primordial pour préparer le le cerveau. Et puis je te recommande, je sais pas, tu as déjà bouclé ton heure mais tu peux prendre 10 h pour te donner le temps d'arriver ou pour ne pas être stressé. Donc tu peux au lieu de prendre peut être 9 h, tu pourrais prendre 10 h 11 h comme ça.

2:15:17
Ensuite le jour e bon, c'est le jour J mais on met le jour E pour examen. Tu arrives aussi sur le site un peu plus tôt, 30 Min en avance, les pièces d'identité avec photo non inspirées. Donc il y a les formulaires que tu vas signer, plus de photos, plus d'emprunts, tout ça on s'assure que c'est toi avant de te donner accès à la salle.

2:15:44
Les effets personnels seront laissés dans un casier fermé à clé que vous conservez. Vous devez vous devez démontrer que vous n'avez rien sur vous, donc on va vous palper pour vous assurer que vous n'avez rien. On a l'examen adaptatif qui est le computerize adaptif testing, l'examen adatif. Généralement, c'est ce qu'on va pas, c'est ce qu'on passe. Donc c'est la raison pour laquelle Émile va aller à Ottawa.

2:16:11
Parce que ce cet examen n'est pas disponible en français. Donc c'est un examen qui dure 3 h. Avant, en 2022, c'était 3 h en en 2000, après, ils ont changé 2022, ils se sont passés à 04h00 jusqu'en avril. Le 14 avril 2024, ils sont repassés maintenant à 03h00 parce que ils avaient besoin de.

2:16:38
De tester certaines des questions des banques de questions qu'ils avaient-ils voulaient étoffer ça et puis ils voulaient faire des études, des analyses, tout ça. Donc ils étaient passés à à 04h00 avec plus de questions. Donc au lieu de 100 questions, ils étaient passés à à 125 questions. Donc l'examen c'est entre 100, c'est 100 à 150 questions sur l'ordinateur. Pourquoi 100 à 150 questions ? C'est que.

2:17:06
Vous allez faire les premières 100 questions et le système va analyser si ils trouvent que c'est confortable, que vous avez répondu aux questions que on peut vous donner ou ou mériter d'avoir le CSSP Ben ils vont pas continuer. S'il n'est pas confortable, Ben il va ajouter des questions jusqu'à 150 questions. Donc il se peut que certains n'arrivent même pas à 100 questions. Ils valident leurs

examens ou bien qu'ils n'arrivent pas à 100 questions et qu'ils arrêtent leurs examens parce que on se rend compte que.

2:17:36
Il a tellement échoué aux questions que il peut même pas avoir l'examen même si on continue à 150 questions. Donc si votre examen s'arrête à 100 questions, soit vous avez bien fait ou vous n'avez pas bien fait, mais des fois ça peut continuer à 100 0,01$ 203 jusqu'à 150. Il faut que le système à un moment donné soit confortable sur votre pratique. La complexité des questions varie en fonction des résultats donc, d'où le nom adaptif.

2:18:04
Donc on ne panique pas si les questions deviennent très difficiles, donc c'est bon signe quand les questions deviennent difficiles, que on vous a envoyé des questions faciles et vous avez répondu en même temps, ne vous réjouissez pas trop si les questions sont très faciles, voilà, si les questions sont faciles, vous répondez, concentrez-vous. Chaque question doit être traitée, tu dois tout faire pour répondre bien à chaque question. C'est ça le nombre de questions, c'est valable, variable selon la performance.

2:18:32
Le pointage d'une question varie selon sa difficulté, donc personne ne sait combien. Quel est le poids d'une question ? Personne ne sait parmi les les 100 questions. Parmi les 150 questions, il y a 25 questions qui ne comptent pas, mais on peut pas les distinguer et il y a 75 questions qui sont notées. Donc il y a des questions, il y a des questions qui sont juste là pour tester, pour voir qui sont. C'est des questions qui sont un peu en QE pour voir si elles vont devenir des questions d'examen après.

2:19:01
Donc ces 25 questions on peut pas les distinguer des des des autres questions ? Donc vous aurez un 25 questions qui vont tourner là et ces 5 75 questions qui seront notées. Donc on a un résultat minimal de 700 sur 1000 mais quand tu as l'examen on sait pas combien de points tu as. C'est pas comme le CSA ou le CSM ou.

2:19:26
On te donne le nombre de points que tu as eu CISSP on te dira pas combien tu as eu, on te dit tu as eu l'examen ou t'as pas eu l'examen et tu sais pas combien de points tu as eu. C'est ça les règles d'arrêts ? Il y a 3 règles d'arrêts qu'on peut avoir donc on a les confidences intervalle, roules donc il va, il s'arrête dès que le résultat est clair à 95%. Donc comme je l'ai dit on va de 100 à 150 questions. Donc si il se rend compte que.

2:19:56
À un moment donné, avec les 100 questions ou 110 questions, il se rend compte que Ben j'ai plus besoin de continuer avec toi. Tu as trouvé toutes les questions comme ça sera le cas de Émile ? Ben il va s'arrêter et puis il te dit va voir ton va va voir le surveillant. Mais si il se rend compte que Ben tu as répondu aux questions, tu as toi de toutes les façons.

2:20:20
On est sûr que tu vas pas avoir l'examen donc mais il continue plus il va s'arrêter. Donc ça c'est la la règle de confidentialité. Ensuite on a le la règle de maximum 9 rôles qui est arrêt à 150 questions. Donc si vous faites jusqu'à 150 questions, Ben c'est fini, c'est fini, s'arrête et puis on va évaluer si vous avez eu ou pas. Ouais et ensuite on a l'arrête de de run of time rôle.

2:20:46
J'ai échec si le candidat n'a pas répondu à 75 questions notées ou si la performance est insuffisante sur les dernières. Donc il peut arriver que le temps soit fini et qu'on n'ait pas répondu aux questions. Ça arrive hein ? Parce que au début on peut traîner sur certaines questions pour être sûr qu'on réponde bien aux questions. Donc ça peut arriver que on manque de temps. Donc voici les 3, les les 3 d'arrêt donc si votre examen s'arrête avant les 150 questions.

2:21:16
Soit c'est correct, vous avez trouvé, vous, vous avez l'examen ou sinon c'est c'était tellement poche que on a arrêté. Ça s'arrête à 150 questions, mais ça peut s'arrêter avant les 150 questions.

2:21:37
Il y a un maître qui dit, tu es évalué mais t'as aucune idée comment ? Ben tu es évalué en fonction des domaines. C'est quand tu échoues, tu sais où tu n'as pas fonctionné, mais quand tu quand tu réussis, on te dit pas où tu as réussi. Ça veut dire que quand tu réussis, ça veut dire que tu as validé tous les domaines, les 8 domaines. Mais si tu échoues, on va te dire les domaines où tu as échoué. Donc en même temps on a un autre examen linéaire aussi en anglais qui lui va durer 6 h, mais généralement on le passe pas.

2:22:05
Ça c'est 225 questions et le c'est le même, le résultat 700. Et puis le pointage d'une question varie selon sa difficulté comme l'autre Marie et tout. Oui ma question est que est ce qu'on doit valider tous ces domaines là ? Parce que nos domaines de compétences ne couvrent pas quand même les 8 domaines OS.

2:22:28
Que quand même quand on a la note qu'il faut c'est suffisant ou chaque domaine doit être validé. En fait chaque chaque domaine doit être validé. C'est clair que tous les gens qui font CSSP ils travaillent pas dans tous les domaines de la sécurité. Moi je travaille pas dans tous les domaines de la sécurité, je travaille dans certains domaines, il y en a que je je fais, il y en a que je faisais, que je fais plus. Donc je pense pas que tout le monde travaille dans tous les domaines donc mais il faut comprendre tout ce que tu as vu dans le cours.

2:22:56
Ce qui se trouve dans les dans les guides, faut comprendre c'est quoi les concepts. Si on te pose la question, tu es capable de répondre, c'est ce qu'on attend de toi et pour chaque domaine tu dois au moins avoir la moyenne correcte. Je vais te montrer comment il note, mais pour chaque domaine, si tu n'as pas tu n'es pas, n'as pas le professionnel si tu risques de ne pas valider en fait la la question. Mais bon, tu ne sauras pas. C'est quand tu vas finir l'examen que tu sauras que t'as pas validé certains domaines.

2:23:29
Zephyrène demande comment gérer son temps pendant pendant l'examen pour gérer le temps pendant l'examen. Moi je pense que d'abord faut pas trop se faire confiance et puis faut pas parfois un estime de soi aussi qui est très faible au point de passer 3 3 Min ou 4 Min sur une question.

2:23:50
Tu as une moyenne de une minute 20 par question, donc tu t'arrêtes à ça. Tu lis la question, il y a des

questions qui sont longues, donc tu prends le temps de lire rapidement. Tu vas répondre. Je vais donner tantôt les astuces, comment est ce que on va ? On repère certains mots clés, certains éléments dans les examens, mais tu tu as le temps devant toi et ne dépasse pas une minute 20 par question si tu as regardé la question.

2:24:14
Tu as lu la question, tu as les réponses et les QCM donc tu regardes ce qui est le plus proche de la réalité et puis bon tu tu le valides mais faut pas dépasser 3 Min une question sinon tu vas manquer du temps et puis ton examen va s'arrêter esaïe donc on a le résultat, échec ou succès tout de suite ? Oui on a le résultat tout de suite à la fin de l'examen mais on te donne pas ta certification, ils vont valider ça quelques jours après après les analyses bien sûr la logique des questions.

2:24:43
Donc pour le CSSP, contrairement à d'autres certifications comme le CSM, le Cisa, il y a pas de possibilité de revenir aux questions déjà répondues. C'est comme sur Moodle Moodle, vous pouvez revenir aux questions que vous avez déjà répondu ou marqué des questions. Ça se fait avec CSMH Isaca mais IC Square non sur CSSP non on ne quand tu as validé une question c'est fini, tu reviens plus là-dessus.

2:25:12
Donc prenez ça en compte, faut bien lire la question avant de choisir, on peut procéder par élimination, plusieurs réponses peuvent souvent sembler correctes, donc des fois tu regardes, toutes les réponses sont vraies, mais qu'est ce que je prends ? Donc ça, je vais vous donner les mots clés qu'on regarde pour vraiment choisir, penser toujours gouvernance, gouvernance, stratégie comme un manager et pas trop technique. Donc si on te demande.

2:25:41
On a un firewall qui a un problème, on a des règles de firewall qui fonctionnent pas. Qu'est ce que tu proposes ? Un on demande au technicien de régler la règle de firewall, un peu comme la question que un de vos collègues a posée, on a mis les règles de firewall, on a mis un dîner, un ami Access, qu'est ce qu'on fait ? Et la première chose aura dit OK, tu demandes au technicien d'arranger la règle. 2e chose on va te dire.

2:26:09
Ben on va effacer les règles 3e chose, on va revoir le processus qui a fait qu'on met les règles en place et on va mettre un processus pour la mise à jour des règles pour ne plus que les règles. On on on, on est des erreurs, des règles. Ça c'est la question qui tend plus vers la stratégie, qui va faire en sorte qu'on aura plus jamais de problème sur les règles. Donc ça c'est la meilleure question dans le concept CSSP, c'est pas la réponse de on va dire au technicien de réparer ça, c'est pas la bonne réponse. La bonne réponse c'est.

2:26:39
On va arranger le processus de telle sorte que on n'ait plus des problèmes de règles qu'on met de façon désordonnée. Donc c'est c'est un peu ça le maintien de l'examen, garder le rythme de une minute, une minute 20, une une minute 20 par question et puis rechercher les mots clés. Je vais vous montrer tantôt les mots clés, est ce que vous avez ?

2:27:02
Je m'excuse au bout de Live, ça veut dire qu'il faut faut avoir un chronomètre ou comment ça se fait.

Non il y a il y a il y a un horloge sur le sur votre écran, OK vous avez tout, il y a l'horloge, il y a le calculateur là-dessus il y a tout. OK parfait ouais il y a Ibrahim qui dit si je valide 7 et qu'il y a un domaine, oui c'est un échec, mais c'est ce qui fait que le le taux de réussite du CSSP est vraiment bas. On n'a pas de statistique sur le taux de réussite.

2:27:31
Il y en a qui parlent de 30% mais il y a pas de de statistiques. Mais le taux d'échec est vraiment bas. Le le taux de réussite est vraiment bas. C'est parce que ils sont-ils sont vraiment exigeants sur l'examen. OK les mots clés, Ben les mots clés. Vous allez retrouver des mots clés comme ça comme best first must likely list, short mast not ou inspect primary maximum anchor granty.

2:27:59
Donc qu'est ce que ça implique quand on dit baisse la solution la plus complète, managériale et stratégique, c'est ce qu'on attend de toi. Donc vous choisissez l'option qui soutient l'organisation à long terme ? Un peu l'exemple que je donnais c'est plus. On veut fixer le processus pour ne plus que ça arrive. Donc oui, si le technicien rit pas, ça va régler le problème, mais on veut plus que ça revienne encore, donc proposer des solutions qui vont faire en sorte que ça va plus revenir.

2:28:23
Le fait c'est l'action immédiate à prendre dans un incident ou un processus. Donc pensez confinement sécurité immédiate avant communication ou analyse moi cela crée le scénario ou la réponse avec la plus forte probabilité d'occurrence ou d'efficacité. appuyez-vous sur les bonnes pratiques et la logique du risque. Le liste c'est le moins efficace ou moins propriétaire parmi les choix. Attention, toutes les réponses peuvent être valides. Chercher la moins utile should ce qui est recommandé.

2:28:53
Mais pas obligatoire, donc pensez aux bonnes pratiques et aux règles impératives. Le masque, c'est ce qui est obligatoire, souvent juridique ou contractuel. Briser les obligations légales ou contractuelles, le note ou expert négation, inverser votre logique habituelle lisez très attentivement, souvent cause de mauvaise lecture. Premart Lean c'est objectif principal, c'est quoi vient en premier penser à la mission, à l'objectif central du rôle ou du contrôle.

2:29:22
Maximum ou minimum, ce qui atteint une valeur extrême temps portée efficacité, donc prêter attention aux mesures quantitatives et contextuelles, et le dernier en jeu garanti, demande un contrôle fort, fiable et systématique. Donc choisissez des mécanismes avec preuve, suivi ou audit. C'est bon pour le résultat. Donc on a fait l'examen, on a tenu compte de, on a géré notre temps.

2:29:51
On a regardé les les mots clés et tout ça. Maintenant on a fini, on attend nos notes donc la note immédiate la note vient immédiatement après avoir terminé. Donc il y a pas de note numérique hein, c'est seulement on vous dit si vous avez un pass ou un fil. En cas d'échec le candidat reçoit un feedback par domaine. Donc niveau billot, newer et Ball Professionsy donc le bilan professeur veut dire.

2:30:17
Que vous êtes sous le seuil de compétences sur le c'est pas domaine. Donc les 8 domaines on va vous dire à chaque niveau c'était correct ou pas mais si vous prenez le Piece of Mans vous saurez lesquels. Les domaines vous n'avez pas performé, vous allez aller plus travailler sur ces domaines là pour venir

passer votre examen. Après généralement ceux qui sont et bah ou préférence ainsi ça veut dire que vraiment c'est vous n'êtes pas mal là-dedans. Donc les autres qui sont billo ou neer.

2:30:43
Mais vous travaillez là-dessus pour arriver au niveau de compétences demandées. Si il y a des anomalies qui sont détectées Ben ils vont faire des analyses psychométriques. Donc le résultat pourrait être dans 4 à 6 semaines après. Mais généralement on a le résultat après après l'examen oui.

2:31:12
Maxence, quand tu dis quand tu parles de anomalie détecté, il s'agit de quoi exactement ? Ben si il se rend compte que peut être pendant l'examen, tu as regardé quelque chose ? Je sais pas, tu sais, tu as une défaillance de surveillance, tu as fait des choses que eux ils ont détecté, ils peuvent ne pas être sûrs. Voilà si si je fais quelque chose. Ouais OK mais il faut être correct là, faut faire ton examen, tout ce qu'on te dit de ne pas apporter n'apporte pas.

2:31:41
Tu vas aller dans les toilettes, tu vas dans les toilettes, tu reviens tranquillement, je pense que tu n'as même pas droit à une bouteille d'eau donc si tu as soif, tu sors, tu vas tu. Mais il faut faire rapidement puisque le temps passe. Donc OK c'est bon. Ouais la politique de reprise donc en cas d'échec on peut refaire selon cette politique là. Donc la première reprise c'est après ou 30, 30 jours ? Oui je reste.

2:32:08
C'est bon, moi je voudrais juste savoir, c'est le poste auquel on utilise pour passer l'examen, c'est ton propre ordinateur ou bien ils ont des non jamais ils ont des ordinateurs, OK des des ordinateurs, genre lorsque vous vous connectez, vous n'avez même pas le Bureau qui s'affiche, rien du tout, tout est bloqué, c'est à dire pour ne pas permettre qu'on puisse aller dans autre chose que ouais c'est ça. Non en fait ce sera juste l'interface du CSSP dans lequel tu as tout, tu as ton horloge, tu as ton en fait tout ce que tu as besoin tu l'auras sur l'interface.

2:32:37
Tu peux rien faire d'autre sur la machine, tu ne fais que faire tes lire tes questions, répondre à tes questions, c'est tout, c'est bon. Donc la première reprise c'est après 30 jours. Donc si vous avez le piece of main après 30 jours c'est bon. 2e reprise après 60 jours, 3e reprise est la suivante après 90 jours mais on a juste 4 tentatives maximum par an sur une période de 12 mois.

2:33:07
Oui expédite oui oui en fait la question c'est quand vous dites 30 jours c'est 30 jours strictement ou 30 juin ? Enfin au moins 30 juin après c'est 30 jours après la date de l'examen, après 30 jours d'examen strictement 30 jours. Si vous quand tu dis strictement non non on te dit pas non, on te dit pas de revenir dans 30 jours, on te dit 30 jours au moins alors non non non, ce qu'on veut te dire, on te, on t'oblige pas toi de revenir dans les 30 jours.

2:33:37
Mais si toi tu veux reprends, tu peux pas reprendre le lendemain, tu vas reprendre 30 jours après, c'est ce qu'on te dit, mais on te dit pas si tu échoues, il faut revenir 30 jours après. Dès que vous parlez, c'est comme si c'était strictement 30 jours, c'est à dire que vous avez le thème, que enfin que moi j'aurais compris c'est 30 jours au minimum. Vous attendez 30 jours au minimum avant de recomposer ? Oui oui mais c'est ça avant de revenir faire l'examen, c'est ça ?

2:34:03
Tu fais nos 30 jours, vous entendez au minimum 30 jours, vous pouvez faire même une année après c'est à votre voilà ça voilà ça sont voilà c'est minimum 30 jours avant 30 jours. Mais quand vous dites 30 jours c'est comme vous êtes fixé à 30 jours obligatoirement. Ouais il s'appelle ça le countdown pour te permettre de l'utiliser fait c'est pour ça qu'ils disent C'est pas la première reprise.

2:34:24
Mettons moi admettons que j'échoue le 15, donc je pourrais pas leur prendre pas avant le ma 2e tentative, pas avant la mi-août, donc à partir du 15 à partir du 15 août. Là je peux replanifier ma ma ma première reprise c'est somma. Tu l'as compris ? Merci c'est bon ? Oui c'est bon.

2:34:51
C'est ça, c'est ça, c'est c'est sinon quelqu'un qui va avoir l'examen, tu peux planifier le jour un comme Émile, il s'en va là, il planifie le 15 et puis il planifie le 16. Il se dit, Bon, c'est pas grave, si j'ai j'ai fini, je le sais-je passe. De toute façon, je reviens à Québec avec mon CSSP, mais c'est pas comme ça. Si tu as échoué, ils se disent que t'es t'es pas prêt là va t'apprêter, tu as 30 jours pour t'apprêter pour revenir, mais si tu ne veux plus faire, tu fais plus ça c'est.

2:35:21
Et selon ce que selon ta volonté, oui moi ici oui Monsieur Vauvana Petite petite question c'est est ce que les les 700$ qu'on paye c'est compris dans les 4 reprises ? Non, c'est une seule reprise, à chaque reprise tu payes Oh my God. C'est pourquoi Émile a parlé, Émile a il y a le lean, le truc, le Peace of mend qui te donne une reprise, tu fais l'examen et puis tu as une reprise.

2:35:49
Si c'était 700$ pour les 4, là ça allait être trop facile. Tu Allais avoir trop de 100DGCSSV. Ouais puis puis ça en prenant le Peace of mind comme on a appris dans le cours, c'est que on transfère le risque. Donc on paye un petit peu plus cher, on se paye une petite assurance donc on se transfère le risque et on a un petit peu plus de de confidence. Là c'est ça ? OK mais non c'est pas non, c'est pas pour les 4 examens, c'est pour un seul examen.

2:36:18
L'ensap oui l'ensap est sur iPhone. Moi j'ai un je l'ai utilisé sur mon iPhone faut faut bien regarder, va va faut bien regarder. Je sais pas si ton Apple est sur le Canada mais tu pourras regarder je on l'a sur Apple oui on Android oui c'est beau parfait.

2:36:47
On continue la suite. Bon on a eu l'examen, c'est bon qu'est ce qu'on fait après ? Mais après on on accepte le code d'éthique de IC Square. Je vais peut être vous montrer le code d'éthique rapidement. Non ça c'est pas le code d'éthique. OK je vais vous le montrer après.

2:37:18
Donc il faut accepter le code d'éthique. Tu vas faire endosser votre demande par une personne CSSP. Sinon on peut demander à IC Square si vous n'en avez pas. Donc minimum de 5 ans d'expérience professionnelle requise dans 2 des 8 domaines ou 4 années plus un diplôme ou un Weaver, c'est à dire une dérogation. Donc comme Émile le disait, un CIH, un CIA, un CSM.

2:37:46

Ou un baccalauréat ou une maîtrise va venir compenser une année. Et puis les 4 années, on va vous demander d'avoir l'expérience pour les certifications comme CISM 6AE je pense. Ils vont jusqu'à 2 ans de dérogations. Ensuite, vous aurez 9 mois pour faire parvenir votre demande de certification CSSP après la date de passage d'examen. Je pense que généralement, quand les gens ont l'examen, ils font ça rapidement.

2:38:13
Il y a des bonnes chances que oui ouais c'est ça c'est ça. Maintenant quand vous avez l'examen c'est pas fini. Chaque année vous payez 125$ US pour maintenir votre certification, les frais annuels donc ça vous permet d'avoir accès à toute la plate forme, avoir accès à des formations continues.

2:38:39
Pour la Real certification, chaque 3 ans tu vas faire la Real certification mais ça veut pas dire que tu vas repasser l'examen, on te demande juste de d'avoir 126PE donc continue. Continuons, professionnal Education, sur un site de 3 ans, donc un minimum de 20CPE par année ou ciblés plutôt à 40CPE par an. Donc ça veut dire quoi en fait ? C'est ce qui fait la force séchant de certification, là ça veut dire que si tu as la certification.

2:39:06
Ton recruteur est sûr que toi tu te formes, tu prends des cours ou tu donnes des cours ou tu fais tu suis des conférences, peu whatever. Tu fais des activités en cybersécurité au moins 20 h par année et 100 20 h en 3 ans. C'est sûr que tu vas mieux maîtriser la cybersécurité que quelqu'un qui ne le fait pas. Je je dis pas que tu seras expert partout, mais quelqu'un qui qui travaille dans le domaine en plus.

2:39:36
Il va faire des formations continues. Il fait au moins 20 h par par année ou 40 h par an dépendamment des des des situations. C'est sûr que il en saura mieux que quelqu'un qui lui n'a pas cette obligation. Donc ces certifications là l'un des avantages ça t'amène, toi qui est détenteur de chaque fois te former d'être à jour. Donc c'est l'un des avantages en fait de ces gens de certification là et ici.

2:40:04
Tu n'arrives pas à faire tes 120CPE Ben on va t'arracher ta certification. C'est tellement dur d'avoir ces certifications, c'est coûteux donc tu vas pas même tu vas pas prendre la chance de de les perdre en fait oui enseigner en cybercontre comme expérience oui C'est pourquoi nous autres on enseigne c'est c'est pour avoir tes CP donc quand tu enseignes en fait tu apprends. Donc quand je viens ici je on peut pas le cours. Et puis vous vous me dites beaucoup de choses.

2:40:34
Qui font que qui qui font que j'évolue. Moi aussi. Donc enseigner, faire des séminaires ça compte comme c'est peu. Donc si vous voulez faire des séminaires, laissez-moi savoir. J'ai beaucoup de de demandes, vous allez faire des séminaires et ça va vous compter comme c'est peu et en même temps aussi, on reçoit vraiment beaucoup de courriels de la part de la ISC. Ah Ben cette petite formation de plote, elle donne un CPE.

2:40:57
Ou si jamais vous voulez passer une semaine de formation à Las Vegas, oublie 16 pour odef COM je pense que ça doit bien compter. Oui ça compte, ça compte. Et puis en plus quand tu as plusieurs certifications comme moi dans ma situation je le 6ACSMCSSPIA 6O des fois un seul CP peut compter pour tout tant que c'est dans le domaine de la sécurité. Donc si peut être je donne ce cours là.

2:41:26
Mais ça va compter pour moi, pour le ça va compter un CPE pour moi pour le nombre de cours que je fais. Donc je peux l'utiliser tant pour le CSSP que pour les cisa que pour les CSM. Donc j'ai pas besoin de multiplier les cours en fait. Donc c'est juste faire un plan de vous devez faire en sorte de de partager la connaissance que vous avez parce que ça fait partie. Il faut faire évoluer le le domaine de la cybersécurité, ça fait partie du du code d'éthique, donc aller faire des séminaires.

2:41:53
Suivre des cours. En tout cas si vous faites tout, vous avez votre certification, on a besoin de vous pour former la nouvelle génération avec ce que vous avez comme connaissance. Donc c'est bon. Et puis comme je disais un document quand vous avez le CSSP, c'est pas la fin hein, c'est le début. Donc déjà avec le CSESP on on vous voit comme un expert donc vous n'avez pas droit à l'erreur.

2:42:20
Vous n'avez pas droit à l'erreur, vous devez quand vous. Quand on vous parle d'un nouveau concept ou un nouveau domaine de la cybersécurité ou un nouvel domaine de la DTI, vous devez chercher à comprendre, vous former dedans parce que vous êtes censé maîtriser en fait et tout ce qui touche à la cybersécurité vous devez avoir. Vous devez comprendre. Vous devez pouvoir avoir de de bonnes notions là-dessus. C'est vrai, on vous demande pas d'être expert partout.

2:42:49
Mais vous devez être être capable de comprendre les concepts, expliquer les différents éléments, comprendre la taxonomie généralement, et puis être à même de d'orienter les différentes personnes ou les parties prenantes sur un projet. Est ce que les CPE on perd ? Est ce que 100 oui si tu ne si tu ne valides pas comme je l'ai dit, tu dois faire 100 20 h sur 3 ans donc minimum de 20h00 par année.

2:43:19
Donc après tes 3 ans tu dois pouvoir faire 100 20 h de CPU. Si tu l'as pas fait tu vas perdre ta certification. Mais je pense pas que ouais ça se fait bien là honnêtement alors j'ai un autre certification puis ça ça s'accumule bien là. Ouais ouais c'est ça. Oui le coût de maîtrise compte combien pour le CPE ? Je sais pas ça dépend, c'est par nombre d'heures donc si c'est un coût de 45 h.

2:43:45
Ben tu pourras aller prouver que tu as fait 45 h, ça va passer pour ça mais ça doit être un cours. Je vais je vais montrer les les différentes instructions. Soit c'est un cours c'est de niveau a au niveau B ça peut être lié à la sécurité ou ça peut être lié à un domaine des pays, donc ça va dépendre de quel cours tu fais. Mais oui si tu as si tu as à à à maîtrise, ça sera facile pour toi de d'avoir tes CPE, mais si tu as fini tes études.

2:44:09
Mais c'est pas parce que tu as fini tes études que tu te formes plus. Il y a comme Émile le disait sur le site de IC Square, il y a tellement de formations qui sont disponibles et il y en a beaucoup qui sont gratuites aussi. Donc tu pourras regarder toutes ces différents cours qui vont peut être te parler de stratégie, qui vont te parler de IAM, des spécialisations dans certains domaines, de la sécurité donc. Bref, il y a tellement de ressources pour pour pouvoir faire tes CPE. Si tu ne fais pas les CPE, c'est que tu tiens pas ta certification.

2:44:39

Mais je pense pas que quelqu'un va aller faire le CSSP puis l'abandonner après. Je peux peut être dire après avoir dépensé 1400 pièces tu veux l'avoir ? C'est ça ? Maxence, oui vas y oui. Est ce que en dehors de est ce que en dehors d'effectuer les séminaires et faire d'autres formations pour mettre à jour sa certification, il y a d'autres moyens qui vont qui peuvent nous permettre de de les mettre à jour ?

2:45:09
Oui, on on va le voir tout à l'heure là. Donc il y a 2 catégories de CPE, donc il y a le groupe a donc c'est les activités de développement directement liées au domaine de la sécurité. Et il y a le groupe B qui est qui sont les activités qui sont à l'extérieur du domaine de la sécurité mais qui permettent un développement des compétences transversales. Donc j'ai parlé de suivre une formation ou un cours à l'université conférence et de l'industrie offre une formation en sécurité.

2:45:36
Suivent toi même des des formations en ligne en lien avec la sécurité que tu peux. Tu peux tu peux prouver donc c'est généralement il y a, il y en a d'autres. J'ai j'ai le il y a le document qui spécifie mais en gros ce sont ces éléments là qu'on prend pour pour justifier qu'on a fait des CPU o K merci c'est bon.

2:46:00
Non et l'expérience compte pas dans le CPE. Mais par contre si dans ton expérience de travail ton entreprise t'a envoyé faire une formation sur fortunette, oui ça compte mais ton expérience de travail compte pas. Et là c'est bon. Si tu fais oui, si tu étudies pour avoir une autre certification, oui ça compte. Admettons. Tu as eu ton CSSP ?

2:46:28
Et puis tu as étudié pour aller avoir ton CSM. La formation que tu as faite dans le CSM compte ou si tu fais ton C et h la formation que tu fais pour le C et h compte c'est bon. Si tu fais une formation en intelligence artificielle, ça compte, c'est bon il y a il y a tellement de formations et puis bon c'est pour nous même notre bien si tu tu te formes, Ben c'est c'est sûr que tu vas être plus compétent que ceux qui se forment pas. Donc si tu as la certification, c'est le début.

2:46:56
Mais toi même tu auras la, tu auras la pression d'aller te former. Toi à un moment donné tu vas être un expert dans ton domaine les ce que comme on les ajoute, Ben on a la plateforme de IC Square, on vient, on on met la date de début, date de fin on on va choisir la catégorie. Donc soit si c'est dans l'éducation donc soit on a suivi un cours de IC Square.

2:47:21
Où on a participé à un élément de du P 2U des cours, où on a fait un magazine, un 1£ blanc, où on a fait un séminaire, on a fait une étude, on a étudié à l'université, on a suivi des conférences dans le domaine FORTUNETTE et autres. Souvent les conférences, les actes fest et autres, ça passe hein ? Tu peux prendre pour faire des CPE ? Voilà, ça marche, tu peux utiliser tout ça.

2:47:49
Une formulation de sécurité association Chapter Meeting. Par exemple, si tu es dans le chapitre ICS de de Montréal, que tu participes au meeting, ça compte. Si tu es dans isaaca que tu participes, ça compte également le le Online webinaire, les podcasts, les, les outils, les ressources en ligne, parce

que eux, ils ont des webinaires qui sont intégrés à leur plateforme. Donc quand tu suis ça passe ou quand tu vas sur l'implantation d'un vendeur, fortunaire, checkpoint et autres.

2:48:17
Tu peux les mettre comme CPE ? Question de même, est ce que au niveau je sais qu'ils le font au niveau d'ici comme ça ? Mais participer mettons comme du des bêta tests ou aider à la au développement des de la certification, ça ça doit compter aussi. Oui ça compte, c'est ça qui est en haut là Prochainal Development Institute. Ah OKOK oui Monsieur Isa Tu tu est ce que tu peux aider à composer des examens aussi ?

2:48:46
Donc tout ça ça ça te donne des sais plus quand tu fais ça te donne un ou 2 en tout cas c'est c'est c'est on peut aller les chercher un peu facilement. Ibrahim demande, si on fait des cours en cybersécurité sur Youtube, peut-on les considérer ? Oui mais tu vas les considérer une seule fois et que tu tu fais le cours, que le cours est pertinent. C'est comme si tu avais donné un cours là donc tu vas peut être parce que il faut on va te demander les preuves hein donc tu vas donner la preuve de ta chaîne Youtube pour pour mettre.

2:49:18
Donc ici avec la avec le la catégorie Ben tu vas dire exactement qu'est ce que tu as fait boat service exemple, Development, la question de de Émile Government, private public sector, partition, Security standard, préparation, présentation, lecture, training.

2:49:40
Préparation, webinaire préparation, Proporing New and upteting Exit in queening, séminar Or classroomatreal, safe and seeker online présentation, saving as subject, Motor disputed Or panel discussion. Donc vous avez vu, il y a plein plein de choses qui vous permettent de d'aller faire votre CPE.

2:50:02
Ensuite, sur le volet Development, Ben Chapter Formation Management, donc si vous êtes dans un conseil d'administration de votre chapitre, ça compte aussi, non ? Sécurité Education, classe matériale, non sécurité industrie confluence, ça peut compter non ? Sécurité organisation proportion for non sécurity, présentation unique work experience.

2:50:30
Ça je sais pas si c'est ça, ça c'est pas l'expérience en tout cas en général. Là si c'est une expérience spécifique qui peut compter oui mais pas votre travail de tous les jours. Après tu vas mettre les détails, le titre, le la personne, le la compagnie qui a fourni le training, le nombre de crédit parce que ça va se compter en nombre de temps. Tu vas faire un petit résumé et puis tu vas mettre la preuve. Donc si tu assistes à une conférence tu vas mettre la preuve du ticket.

2:51:00
Si tu as fait un cours Ben tu vas venir soit mettre que donner les informations qui qui prouvent que tu as fait le cours. C'est évident que tu vas pas venir charger tous tes cours mais tu vas me prouver que tu as tu as donné des cours, donner une évidence qui montre que tu as effectivement fait le cours ou la formation. Ensuite tu vas venir dire dans quel domaine tu l'as fait ? Est ce que si c'est un domaine de la sécurité est ce que.

2:51:28
C'est quel domaine de du CSSP tu vas le faire ou si c'est du groupe B qui n'est qui est pas forcément lien à la sécurité mais qui est transversale, donc les domaines de TI et après le tableau de bord tu vas suivre ici. Lui il avait 45 sur 120 et la première année il avait pratiquement fait 45 donc il doit tout faire pour faire au moins 20 20 les autres années pour rester dans ses 120 s'il a dépassé ses corrects hein mais on te dit minimum 120.

2:51:58
Ok, c'était tout. Si le guide officiel qu'on peut prendre pour approfondir, je cherchais le le code éthique.

2:52:28
Si vous avez des questions, n'hésitez pas. OK, le code d'éthique, c'est ça. Protect Society, the Command Good ne sera Republic Trust and Confidence and Infrastructure Act honorabil onesly, juslee, responsabily and legaly dirigeant and competent service to principal Advanced and protect the profession.

2:52:55
Donc ça on met tout ce qui est formation, tout ce qui est en tout cas tout ce que tu peux faire pour faire avancer la cybersécurité. Donc ça vous allez le signer et puis vous allez vous engager à à le faire. Donc c'était c'était tout. Est ce que vous avez des questions ? Des questions ? Jonathan.

2:53:26
Y a pas de question Ibrahim Ibrahim Ibrahim Arouna, est ce que tu es là ? Oui t'as pas de question. Allô oui Ah désolé, j'étais j'étais déplacé. Certainement un moment où vous avez.

2:53:49
Vous voulez que vous poser la question si j'ai des questions ? Non non non non, j'ai pas de question, je demande juste si tu as des questions. Ah OK non non Ben je suis vraiment, c'est correct, c'est c'est correct en fait. Le CSSP, j'avais fait une pour partager un peu mon expérience. J'avais j'avais fait une tentative qui qui n'avait pas fonctionné il y a il y a comme 4 5 ans comme ça.

2:54:13
OK Ben depuis lors j'ai j'ai laissé tomber mais je crois que maintenant c'est la belle occasion de de ça je serai, je serai sur ton dos, faut faut le faire avant la fin de l'année. Ouais je je l'espère vraiment mais je sais que ça demande beaucoup de préparation donc ouais c'est c'est pas c'est pas évident là il faut vraiment s'asseoir et à prendre longtemps là ouais c'est ça on a oui besalem Monsieur Ouais.

2:54:43
Ma ma question c'est de savoir un informaticien ou un bon un développeur d'applications ? Un développeur d'applications qui se lance dans la cybersécurité parfois devrait par quoi devrait-il commencer pour ne pas se par exemple quel peut être son que peut être le cursus quand le le Q 6 c'est quoi ? Quand tu parles de Q, tu parles de cette application ?

2:55:09
Non par exemple oui en en plus parce que le c'est clair que la maîtrise la médecine n'est pas suffisante, il va, il va falloir renforcer la maîtrise oui par quel peut être son cheminement ? Pour quelle

certification ? Peux tu commencer avant nous avant de se lancer avant d'attaquer les grosses certifications comme OK bon moi.

2:55:33
Moi j'ai été développeur tu vois peut être que je suis l'exemple typique. J'ai je suis développeur et puis je suis venu en sécurité donc mais comme je je faisais le gasti et le gasti était calqué sur le siza. Donc j'ai fait mon siza, j'ai fait le siza mais j'avais pas l'expérience requise donc je suis allé travailler. Après 2 ans je suis venu valider et puis j'ai eu mon siza. Moi j'ai commencé par analyste en sécurité sécurité opérationnelle, essayer de comprendre tout ce qu'on fait dans un socle.

2:56:04
Les vulnérabilités, la gestion des Vulnérabilités, tout et progressivement. Étant donné que j'étais développeur, je suis allé vers l'accompagnement projet des équipes de développement. Donc progressivement j'ai j'accompagne de plus en plus des équipes de de développement, tout ce qui est sécurité, sécurité des applications. Je travaille plus dans dans ces aspects-là, puis aspect de aspect gouvernance. Donc moi je te dirais.

2:56:34
Dans un premier temps ils vont pas peut être te mettre dans une équipe de de de développement et puis ça sera pas dans ton intérêt. C'est plus commence analyste commence un peu en pas analyse si tu as eu un socle va dans un socle mais n'abandonne pas ton côté développeur parce que après c'est ce que tu vas utiliser pour accompagner des équipes projets dans le développement ou l'acquisition des logiciels ou la gestion des risques. OK maintenant.

2:57:01
Ton point de vue ça vient de commencer par par être analyste ? Non pas forcément. Tu peux être analyste en cybersécurité, c'est pas juste dans un socle, ça va dépendre de la compagnie, mais commence analyste en sécurité, dépendamment de où on va te mettre, tu vas apprendre en bas et puis après tu vas apporter ton colis côté développement. Puis soit tu vas être plus dans le volet gestion des risques, accompagnement des équipes d'affaires, architecture, sécurité et autres.

2:57:31
Ok merci Monsieur. Ouais mais si en termes de certification il y a le CCLP qui est la certification pour les la le développement sécuritaire qui est fait par le IC score aussi CCSLP ça cette certification là tu vois mon écran ? Allô, est ce que tu vois mon écran ? Oui.

2:57:59
Voilà ça ça c'est la certification qui est qui est faite par IC Square pour ceux qui veulent approfondir le développement des logiciels sécurisés. C'est vrai qu'ils sont développeurs et puis qui veulent rester dedans. Mais à mon humble avis va faire ton CSSP parce que il y a des parties du CSSP qui couvrent ça déjà. Donc va faire ton CSSP tu pourras. En tout cas ça va te donner plus de d'opportunités que ça.

2:58:29
Est ce que il y a d'autres questions ? Est ce que il y a il y a d'autres questions ? Il y a pas de question oui expédite oui en fait la question que le collègue posait tout à l'heure, je ne sais pas. Moi j'avais compris ça autrement. C'est à dire que il dit comme le CSP permet d'avoir d'être au niveau de la stratégie, c'est à dire au niveau des décideurs, il se demandait en fait est ce qu'il faut au début commencer ?

2:59:01
Par comment l'opérationnel ou grandir aller vers la la stratégie à ou bien l'inverse ? Ce qui a plus ce qui a plus facile c'est de commencer par l'opérationnel parce que l'opérationnel il y a beaucoup de gens. On a besoin de beaucoup plus de gens mais tu craches pas sur le morceau si on te prend comme analyste gouvernance ou analyse conformité.

2:59:31
Oui, mais parce que dans ce cas, lorsque vous commencez peut être par l'opérationnel, vous grandissez. C'est comme si c'est quand vous êtes au niveau de la responsabilité, vous êtes au niveau des décideurs que vous faites de CISP et là vous n'aurez plus beaucoup de trucs à faire valoir au niveau de la de votre CPE puisque vous êtes-vous allez être maintenant quelque part. Non, vous allez faire un suivi, vous n'allez plus dans non c'est c'est pas parce que tu es au niveau des décideurs que tu regardes pas la technique hein.

3:00:00
En fait au niveau des décideurs tu vas plus être niveau stratégique de la sécurité, mais quand on dit niveau stratégie de la sécurité, là tu vas faire le programme de sécurité mais dans le programme de sécurité, là on va parler des firewall, on va parler des EDR. Tu es toujours dans la technique en fait. Sauf que tu vas mettre en place des stratégies de gestion des vulnérabilités. Mais c'est pas toi qui va lancer le scan de vulnérabilité, c'est pas toi. Peut être qui va aller chaque fois aller au socle pour dire il y a un incident de niveau 4.

3:00:27
Mais c'est toi qui définis tout ça en fait. Donc tu comprends la technique parce que si tu comprends pas la technique tu peux pas faire la stratégie. Maintenant est ce que quelqu'un qui est junior on va l'amener faire la stratégie ? Ça c'est autre chose. Je je pense pas que étant junior on va t'amener faire la stratégie. Ce que je vois tous ceux qui sont juniors ils rentrent souvent dans des équipes d'analystes en en conformité ou analystes gouvernance ou il y a des entreprises qui l'appellent d'une autre façon. Il va un peu commencer la gouvernance.

3:00:56
Rédaction de documents peut être il va suivre un peu la stratégie avec le directeur ou le ciseau, il va apprendre mais en réalité quand on dit stratégie ça veut pas dire que tu ne touches pas à la technique mais t'es pas dans tu n'es pas dans le Hand zone en fait t'es pas dans le Hand zone, c'est c'est pas toi qu'on appelle. Quand il y a un incident en fait c'est c'est c'était pas au premier niveau en fait d'intervention.

3:01:21
Voilà et puis même le CSSP après tu peux aller en architecture de sécurité tout ça, donc c'est pas que tu ne fais pas du tout de de de technique. Non c'est pas ça, merci c'est beau OK le temps est passé, merci beaucoup, puis bonne soirée, merci bonne soirée Monsieur.

3:01:49
Merci, bonne soirée.