

Sécurité des Réseaux

Chapitre I : Introduction Générale

Mouhcine BOUAYAD
Licence SID

Module

- Module sur la sécurité informatique / Architecture Intranet & Internet
- Notes :
 - 50% exposé sur un thème qui ne sera pas abordé durant le cours (présentation orale et écrite)
 - 50% partiel
 - QCM - 2H partiel (23 Novembre 2020)

GAME VS PIRATAGE

- Module destiné à la protection, pas à l'attaque. Mais si cela vous amuse :
- Certains organismes "anodins" sont sous la protection de la DGSI ou pire...
- Quand vous réussissez à pirater un organisme c'est parce que :
 - Il ne fait pas de sécurité
 - Il a une bonne sécurité, mais avec une faille => Analyse de journaux
 - Vous avez piraté un Honeypot (pot de miel). Bravo vous êtes sous microscope
- Accord international G8-24
 - Gel de situation de police à police,
 - Régularisation judiciaire par la suite.

DURA LEX SED LEX

➤ **Accès et maintien :**

- Pénal : Art 323-1 : 30 000€, 2 ans de prison
- si en plus altération : 45 000 €, 3 ans de prison
- si en plus STAD (Système de traitement automatisé de données) de l'état : 75 000 €, 5 ans de prison

➤ **Entrave au système d'information :**

- Pénal : Art 323-2 : 75 000 €, 5 ans de prison.
- si en plus STAD de l'état : 100 000 €, 7 ans de prison

➤ **Possession d'outils de piratage :**

- Pénal : peines identiques aux infractions "possibles".

DURA LEX SED LEX

« Pas vu, pas pris »
« Vu : Niqué »



Le danger est partout !

Le risque ZERO n'existe pas !

<https://www.usine-digitale.fr/article/apple-se-serait-fait-derober-90-go-de-fichiers-lors-d-un-piratage-par-un-adolescent-de-16-ans.N731379>

Apple se fait dérober 90 Go de fichiers lors d'un piratage par un adolescent de 16 ans

VU AILLEURS Un jeune australien de 16 ans est parvenu à infiltrer le réseau informatique d'Apple pendant près d'un an. L'adolescent comparait cette semaine devant le tribunal pour enfants.

FLORIANE LECLERC

PUBLIÉ LE 17 AOÛT 2018 À 17H45

APPLE, CYBERSÉCURITÉ, AUSTRALIE



Scénario 1 : Extorsion d'une PME

- Romain, un employé du service des finances d'une grande entreprise publique, reçoit un courriel de son PDG avec un fichier PDF joint. Le PDF concerne les résultats du troisième trimestre de la société. **Romain ouvre la pièce jointe.**
- Le même scénario se déroule dans toute l'organisation alors que des dizaines d'autres employés sont amenés à cliquer sur la pièce jointe. Lorsque le fichier PDF s'ouvre, un ransomware est installé sur les ordinateurs des employés et commence le processus de collecte et de cryptage des données de l'entreprise.
- Le but des attaquants est le gain financier, car ils détiennent les données de la société à des fins de rançon jusqu'à ce qu'ils soient payés.



Scénario 2 : Extorsion d'une PME

● Lien vidéo :

<https://www.youtube.com/watch?v=4gR562GW7TI>

Scénario 3 : Des nations ciblées

- Certains des logiciels malveillants d'aujourd'hui sont si complexes et coûteux à créer que les experts en sécurité estiment que **seul un État ou un groupe de nations** pourrait avoir les capacités nécessaires pour le créer. De tels logiciels malveillants peuvent cibler l'infrastructure vulnérable d'un pays, comme **le système d'eau ou le réseau électrique**.
- C'était le but du ver **Stuxnet**, qui infectait des clés USB. Ces lecteurs étaient transportés par cinq fournisseurs de composants iraniens, avec l'intention d'infiltrer les installations nucléaires supportées par les fournisseurs.
- Stuxnet a été conçu pour infiltrer les systèmes d'exploitation **Windows** puis cibler les logiciels **Step 7**. **Step 7** a été développée par **Siemens** pour ses automates programmables. Stuxnet recherchait un modèle spécifique des automates Siemens qui contrôlent les centrifugeuses dans les installations nucléaires. Le ver a été transmis des clés USB infectées aux automates programmables et a **finalement endommagé plusieurs de ces centrifugeuses**.

Scénario 2 : Des nations ciblées

- Lien #1 vidéo :

<https://www.youtube.com/watch?v=rjHSKUyKQyw>

- Lien #2 :

<http://www.zerodaysfilm.com/>



Les acteurs malveillants



Qui sont les acteurs malveillants ?

- Les acteurs malveillants incluent les amateurs, les hacktivistes, les groupes criminels organisés, les groupes parrainés par un État, les groupes terroristes...
- Les acteurs malveillants sont des individus ou un groupe d'individus qui effectuent des cyberattaques contre un autre individu ou une autre organisation.
- Les cyberattaques sont des actes intentionnels et malveillants destinés à avoir un impact négatif sur une autre personne ou organisation.



Les amateurs

- Les amateurs, également connus sous le nom de script kiddies, ont peu ou pas de compétences.
- Ils utilisent souvent des outils existants ou des instructions trouvées sur Internet pour lancer des attaques.
- Certains sont simplement curieux, tandis que d'autres tentent de démontrer leurs compétences en causant des dommages.
- Même s'ils utilisent des outils de base, les résultats peuvent toujours être dévastateurs.

Et si on ne sait pas faire ☺ ?????

15

DDOS SERVICE

DDOSSERVICE.COM

PROTECT

Login Chat

1. Login the chat as a guest.
2. Tell us your target.
3. We will test attack your target for 10 mins.
4. We will set the price.
5. After you decide to deal with us, you will choice your payment method and pay us.
6. After we receive payment we will start DDOS.

* Ddos level : prolexic/nexusguard servers 1

* 攻击范围 黄色网,赌钱网,私服,骗子网,国外网.

contact us: ddosservice@ymail.com
call us : +60177174768
sms : +60177174768

www.ddosservice.com

没有帖子。

主页

订阅: 帖子 (Atom)

source *http://www.ddosservice.com*



Hacktivists

- **Les hacktivistes sont des hackers qui protestent contre diverses idées politiques et sociales.**
- **Les hacktivistes protestent publiquement contre les organisations ou les gouvernements**
 - en publiant des articles et des vidéos,
 - en diffusant des informations sensibles
 - et en perturbant les services Web avec un trafic illégitime dans les attaques par déni de service distribué (DDoS).

Hacked By Moroccan Kingdom

قوات الردع المغربية

Je ne suis pas Charlie /Je ne suis pas terroriste /Je suis musulman et fier de l'être.

Ce que fait charlie n'est pas la liberté d'expression..

Ca s'appelle le terrorisme intellectuel.

Un peu de respect pour les autres religions.

STOP



Payback is a bitch, isn't it?



Operation: Payback

(Subsidiary: Operation Tunisia)

AN OPEN LETTER TO THE GOVERNMENT OF TUNISIA

Greetings from Anonymous.

We have been watching your treatment of your own citizens, and we are both greatly saddened and enraged at your behavior. You have unilaterally declared war on free speech, democracy, and even your own people. Your citizens rally in the streets to demand accountability and their own rights, which you have wrongfully presumed it was in your purview to take from them.

We will use this brief span of attention we've captured to deliver a clear and present message which we hope shall never be forgot. Remember, remember, that the tighter you squeeze the more your citizens shall rebel against your rule. Like a fistful of sand in the palm of your grip, the more you squeeze your citizens the more that they will flow right out of your hand. The more you censor your own citizens the more they shall know about you and what you are doing.

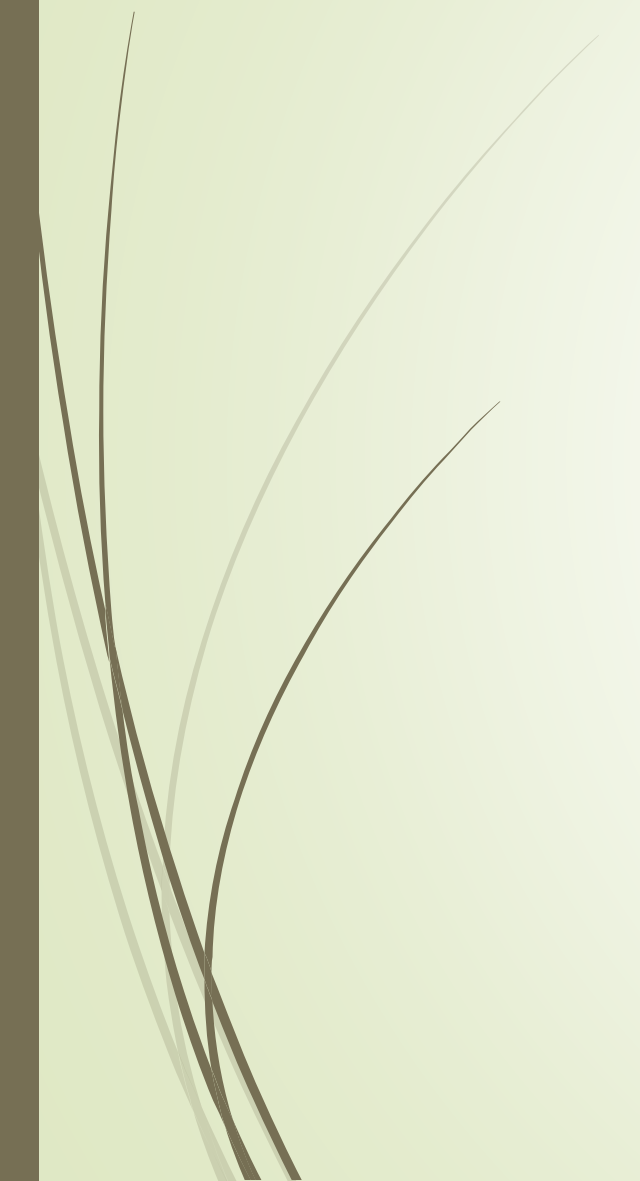

A time for truth has come. A time for people to express themselves freely and to be heard from anywhere in the world. The Tunisian government wants to control the present with falsehoods and misinformation in order to impose a course for the future by keeping the truth hidden from its citizens. We will not remain silent while this happens. Anonymous has heard the cry for freedom from the Tunisian people. Anonymous is willing to help the Tunisian people in this fight against oppression.

This is a warning to the Tunisian Government: violation of the freedom of speech and information of its citizens will not be tolerated. Cyber Attacks will persist until the Tunisian Government respects all Tunisian citizens right to Free Speech and Information and ceases the censoring of the internet.

It's in the hands of the Tunisian government to stop this situation. Free the net and attacks will cease. Continue your oppression and this will just be the beginning.

We are Anonymous.
We are the angry avatar of free speech.
We are the immune system of democracy.
We do not forgive censorship.
We do not forget free speech.
Expect us - always.

Le site internet du
premier ministre
tunisien hacké



Pourquoi ? Les motivations



L'argent

- Une grande partie de l'activité de piratage qui menace constamment la sécurité des réseaux est motivée par un gain financier.
- Les cybercriminels veulent avoir accès aux comptes bancaires, aux données personnelles et à tout ce qu'ils peuvent utiliser pour être monnayer



L'espionnage industriel

- Au cours des dernières années, de nombreux États ont piraté d'autres pays, ou ont interféré avec leurs politiques internes.
- Ces États sont également intéressés par l'utilisation du cyberspace pour l'espionnage industriel.
 - Le vol de propriété intellectuelle peut donner à un pays un avantage important dans le commerce international.
- La défense contre le cyber espionnage et la cyberguerre parrainés par l'État continuera d'être une priorité pour les professionnels de la cybersécurité.

Quel est le degré de sécurité de l'Internet des objets?

- L'Internet des objets (IoT) est tout autour de nous et se développe rapidement.
 - Nous commençons tout juste à récolter les bénéfices de l'IoT.
 - De nouvelles façons d'utiliser les objets connectés sont développées quotidiennement. L'IoT aide les individus à connecter les choses pour améliorer leur qualité de vie.
 - Par exemple, de nombreuses personnes utilisent désormais des appareils portables connectés pour suivre leurs activités de fitness.
- Quelle est la sécurité de ces appareils?
 - Par exemple, qui a écrit le firmware?
 - Le programmeur a-t-il prêté attention aux failles de sécurité?
 - Votre thermostat domestique connecté est-il vulnérable aux attaques?
 - Qu'en est-il de votre enregistreur vidéo numérique (DVR)?
 - Si des vulnérabilités de sécurité sont détectées, le microprogramme du périphérique peut-il être corrigé pour éliminer cette vulnérabilité?

Quel est le degré de sécurité de l'Internet des objets?

- De nombreux appareils sur Internet ne sont pas mis à jour avec le dernier micrologiciel. Certains appareils plus anciens n'étaient même pas développés pour être mis à jour avec des correctifs. Ces deux situations créent des opportunités pour les acteurs de la menace et les risques de sécurité pour les propriétaires de ces appareils.
- En octobre 2016, une attaque DDoS contre le fournisseur de noms de domaine Dyn a mis à mal de nombreux sites Web populaires. L'attaque provenait d'un grand nombre de webcams, de DVR, de routeurs et d'autres périphériques IoT compromis par des logiciels malveillants. Ces appareils formaient un «botnet» contrôlé par des pirates informatiques. Ce botnet a été utilisé pour créer une énorme attaque DDoS qui a désactivé les services Internet essentiels. Dyn a posté un blog pour expliquer l'attaque et sa réaction.

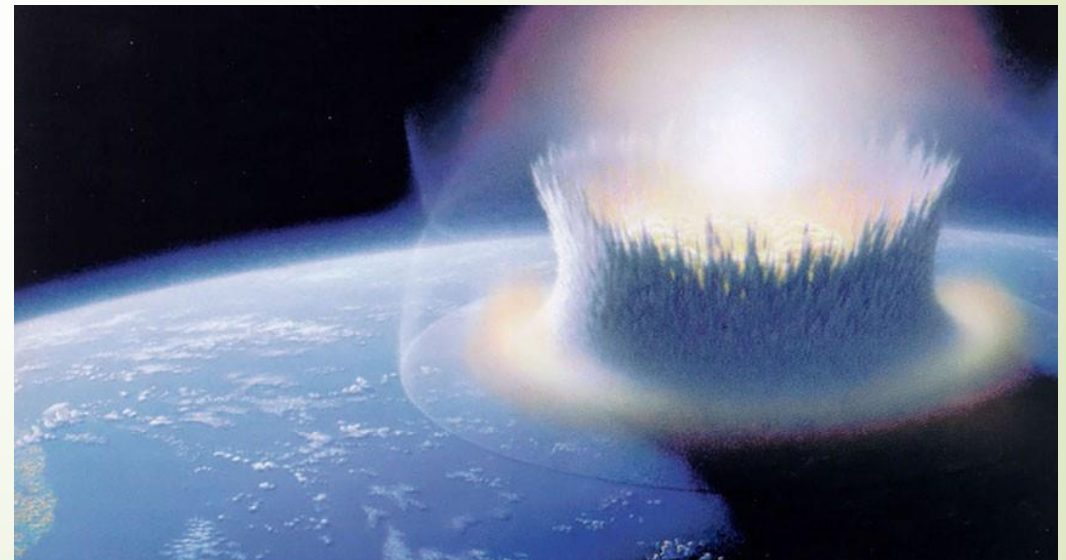


Quel est le degré de sécurité de l'Internet des objets?

Lien vidéo :

<https://www.youtube.com/watch?v=Phm0RmyJt9Y>

L'impact !



PII & PHI

- L'impact économique des cyberattaques est difficile à déterminer avec précision; toutefois, selon un article paru dans Forbes, on estime que les **entreprises perdent 400 milliards** de dollars par an pour les cyberattaques.

– Lien vers article de Forbes:
<https://www.forbes.com/sites/stevenmorgan/2015/11/24/ibms-ceo-onhackers-cyber-crime-is-the-greatestthreat-to-every-company-in-theworld/#5f385e8573f0>

85,235 views | Nov 24, 2015, 06:46am

IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'



Steve Morgan Contributor 
I write about the business of cybersecurity.



NEW YORK, NY - NOVEMBER 03: Chairman, President and CEO of IBM Ginni Rometty participates in a panel discussion at the New York Times 2015 DealBook Conference at the Whitney Museum of American Art on November 3, 2015 in New York City. (Photo by Neilson Barnard/Getty Images for New York Times)

The British insurance company Lloyd's estimates that cyber attacks cost businesses as much as \$400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business. Some vendor and media forecasts put the cybercrime figure as high as \$500 billion and more.

PII & PHI

Les ***Personally identifiable information* (PII)** sont des informations pouvant être utilisées pour identifier **de manière unique un individu**.

Les exemples de PII incluent:

- Prénom & Nom
- Numéro de sécurité sociale
- Date de naissance
- Numéros de carte de crédit
- Numéros de compte bancaire
- Document d'identification délivré par le gouvernement
- Adresse (rue, email, numéros de téléphone)

● L'un des objectifs les plus lucratifs des cybercriminels consiste à obtenir des listes de PII qui peuvent ensuite **être vendues sur le Dark Web**. Le Dark Web est accessible uniquement avec un logiciel spécial (Tor) et est utilisé par les cybercriminels pour protéger leurs activités.

● Les **données personnelles volées peuvent être utilisées pour créer de faux comptes**, tels que des cartes de crédit et des prêts à court terme.

PII & PHI

Un sous-ensemble de PII est les **Protected Health Information (PHI)**.

- La communauté médicale crée et conserve des dossiers médicaux électroniques (DME) contenant des renseignements personnels sur la santé.
- Aux États-Unis, le traitement des renseignements personnels sur la santé est régi par la loi **Health Insurance Portability and Accountability Act (HIPAA)**.
- La réglementation équivalente dans l'Union européenne s'appelle **la protection des données**.
- La plupart des piratages sur des entreprises et des organisations signalées dans les nouvelles impliquaient des PII ou des PHI volés.
- En seulement trois mois en 2016, les attaques suivantes ont eu lieu:
 - En mars 2016, une violation de données chez un fournisseur de soins de santé a révélé les informations personnelles de 2,2 millions de patients.
 - En avril 2016, un ordinateur portable et des lecteurs portables ont été volés à une agence gouvernementale qui contenait des informations personnelles pour 5 millions de personnes.
 - En mai 2016, une violation de données dans une société de paie a révélé les informations sur la paie, les taxes et les avantages sociaux de plus de 600 000 entreprises.

Perte des avantages concurrentiels

- Les entreprises sont de plus en plus préoccupées par l'espionnage des entreprises dans le cyberspace.
- La perte de confiance qui découle de l'impossibilité de protéger les données personnelles de ses clients constitue une autre préoccupation majeure.
- **La perte d'avantage concurrentiel peut provenir de cette perte de confiance plutôt que celle d'une autre société ou d'un autre pays qui vole des secrets commerciaux.**

La sécurité nationale

- Ce ne sont pas seulement les entreprises qui se font pirater.
 - En février 2016, un pirate informatique a publié les informations personnelles de 20 000 employés du US Federal Bureau of Investigation (FBI) et de 9 000 employés du Département américain de la sécurité intérieure (Department of Homeland Security (DHS)).
 - Le pirate était apparemment motivé par des considérations politiques.

La sécurité nationale

- Le ver Stuxnet a été spécifiquement conçu pour entraver les progrès de l'Iran dans l'enrichissement de l'uranium qui pourrait être utilisé dans une arme nucléaire.
- Stuxnet est un excellent exemple d'attaque de réseau motivée par des préoccupations de sécurité nationale. La cyberguerre est une possibilité sérieuse.
- Les pirates informatiques soutenus par l'État peuvent provoquer des perturbations et la destruction de services et de ressources vitaux au sein d'une nation ennemie.
- Internet est devenu essentiel en tant que support pour les activités commerciales et financières.
- La perturbation de ces activités peut dévaster l'économie d'un pays.
- Les contrôleurs, similaires à ceux attaqués par Stuxnet, sont également utilisés pour contrôler le débit d'eau aux barrages et la commutation de l'électricité sur le réseau électrique.
- Les attaques contre de tels contrôleurs peuvent avoir des conséquences désastreuses.



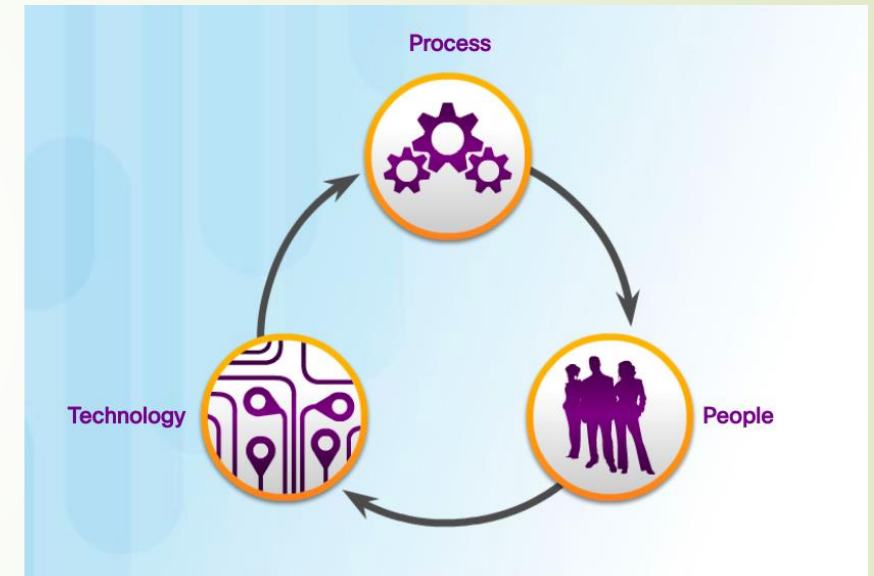
Les soldats dans la guerre contre la cybercriminalité

Le Security Operations Center (SOC)

La défense contre les menaces d'aujourd'hui exige une approche formalisée, structurée et disciplinée, exécutée par des professionnels des centres des opérations de sécurité ou SOC.

- Les SOC fournissent une large gamme de services, allant de la surveillance et de la gestion aux solutions complètes de menaces et de sécurité hébergées, qui peuvent être personnalisées pour répondre aux besoins des clients.
- Les SOC peuvent être entièrement internes, détenues et exploitées par une entreprise, ou des éléments d'un SOC peuvent être sous-traités à des fournisseurs de sécurité

● Les principaux éléments d'un SOC, illustrés dans la figure, sont les personnes, les processus et la technologie.

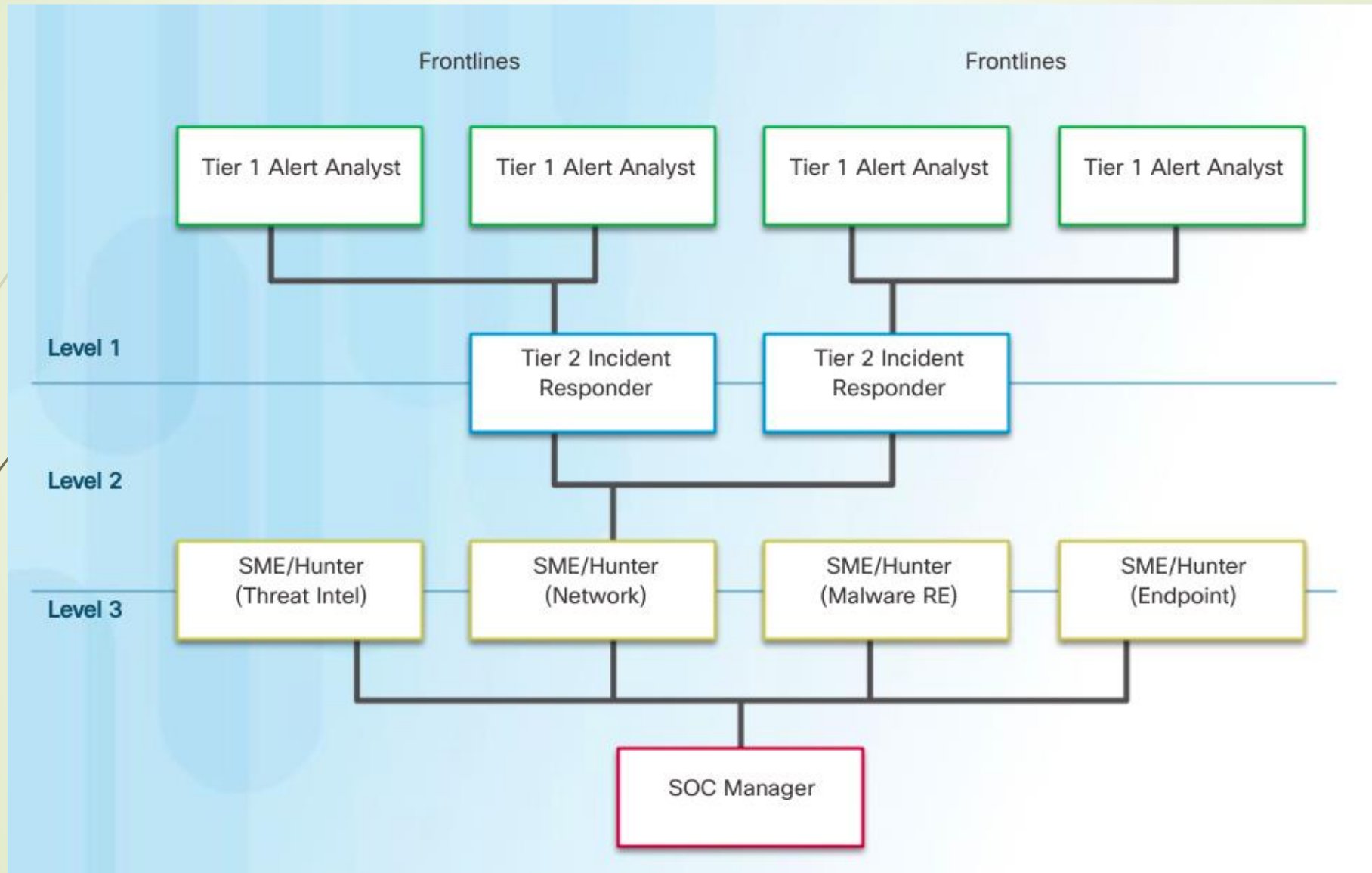


Les profils dans un SOC

Le *SANS Institute* (www.sans.org) classe les rôles des personnes dans un SOC en quatre profils:

- **Tier 1 Alert Analyst/Analyste d'alertes de niveau 1** - Ces professionnels surveillent les alertes entrantes, vérifient qu'un véritable incident s'est produit et transfèrent les tickets vers le niveau 2, si nécessaire.
- **Tier 2 Incident Responder** - Ces professionnels sont chargés d'enquêter en profondeur sur les incidents et de recommander des mesures correctives.
- **Tier 3 Subject Matter Expert (SME)/Hunter** - Ces professionnels possèdent des compétences de niveau expert en matière de réseau et en reverse engineering de logiciels malveillants. Ils sont des experts pour suivre les processus du logiciel malveillant afin de déterminer son impact et comment il peut être supprimé. Ils sont également très impliqués dans la recherche de menaces potentielles et dans la mise en œuvre d'outils de détection de menaces.
- **SOC Manager** - Ce professionnel gère toutes les ressources du SOC et sert de point de contact pour l'organisation ou le client.

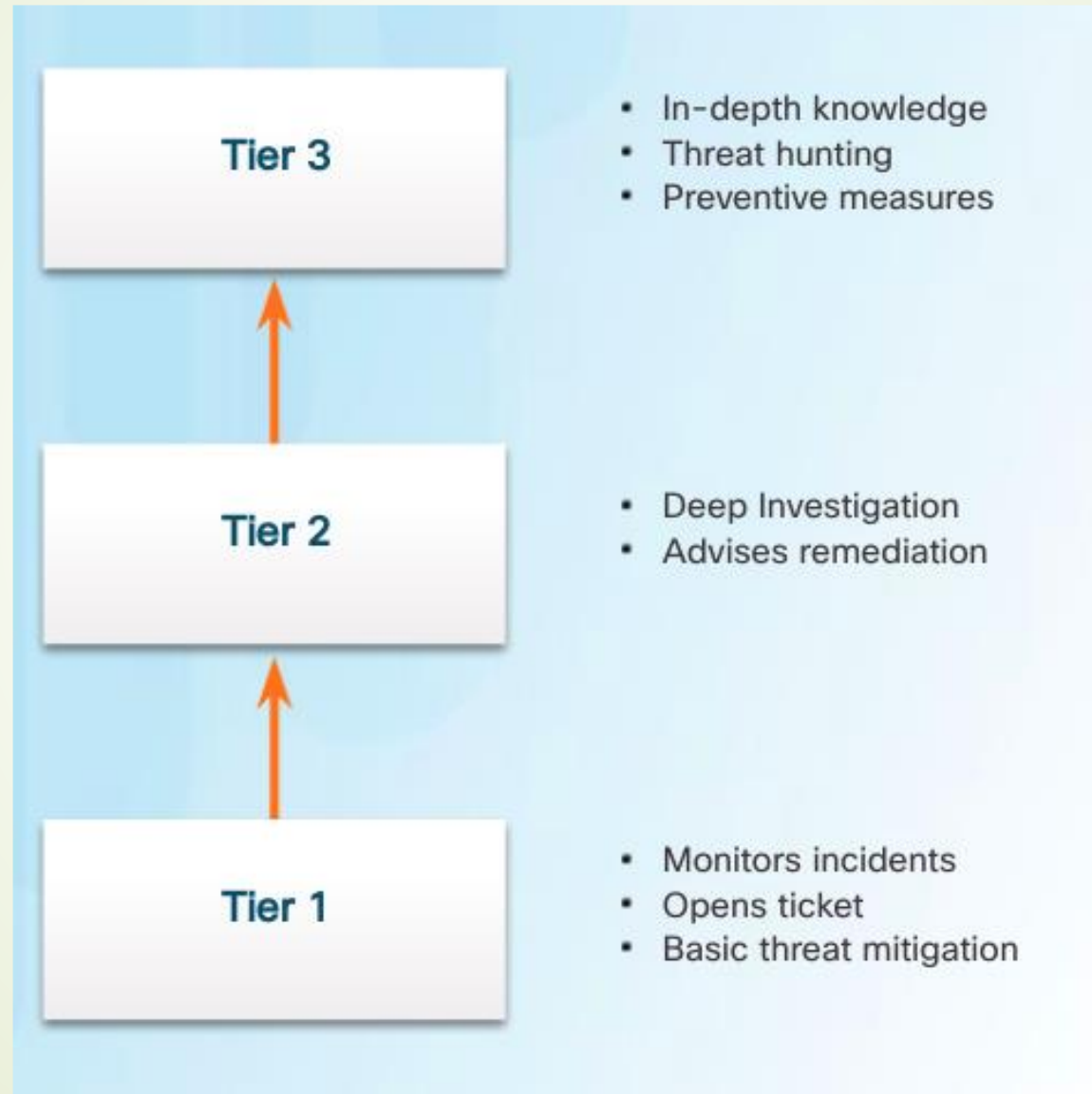
Les profils dans un SOC



Les processus dans un SOC

- L'analyste de niveau 1 commence sa journée par **la surveillance des files d'attente d'alerte de sécurité.**
 - Un système de tickets est fréquemment utilisé pour permettre aux analystes de sélectionner des alertes à partir d'une file d'attente.
- Étant donné que le logiciel qui génère des alertes peut déclencher de fausses alarmes, l'un des travaux de l'analyste de niveau 1 peut **consister à vérifier qu'une alerte représente un véritable incident de sécurité.**
- Lorsque la vérification est établie, **l'incident peut être transmis aux enquêteurs ou à d'autres membres du personnel de sécurité** pour qu'il soit donné suite ou résolu en tant que fausse alerte.
- **Si un ticket ne peut pas être résolu,** l'analyste de niveau 1 transmettra le ticket **à un analyste de niveau 2 pour une investigation et une correction plus approfondies.**
- **Si l'analyste de niveau 2 ne peut pas résoudre le ticket,** il le transmettra **à un analyste de niveau 3** disposant de connaissances approfondies et de compétences de recherche de menaces.

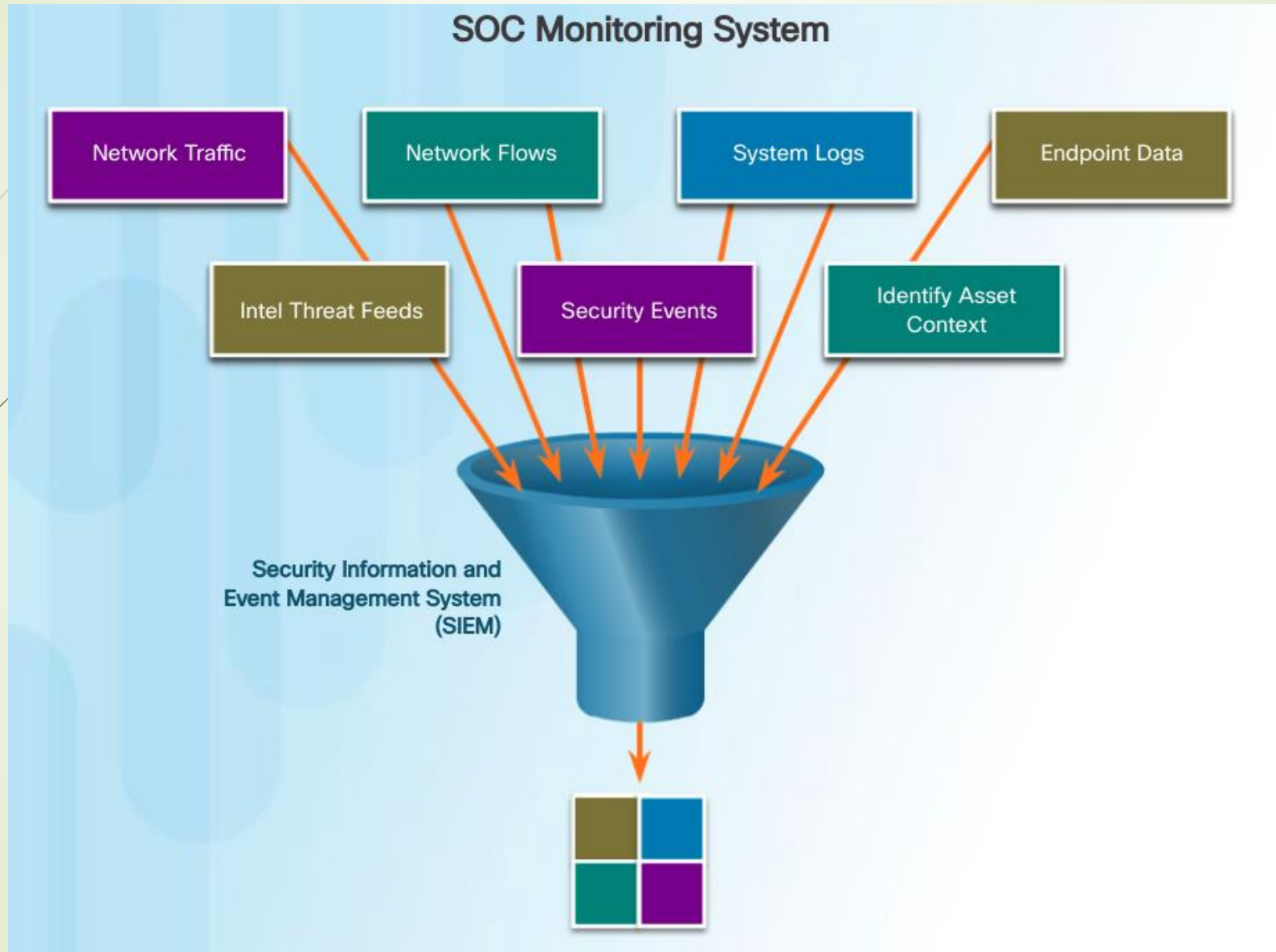
Les processus dans un SOC



Les technologies dans un SOC

- Un SOC a besoin d'un système de gestion des informations et des événements de sécurité (***SIEM ou security information and event management***). Ce système combine des données provenant de plusieurs technologies.
- Les systèmes SIEM sont utilisés pour **collecter et filtrer les données, détecter, analyser et classer les menaces**, et **gérer les ressources** pour mettre en œuvre des **mesures préventives et faire face aux menaces futures**.
- Les technologies SOC comprennent un ou plusieurs des éléments suivants :
 - Collecte, corrélation et analyse des événements
 - Contrôle de sécurité
 - Gestion des journaux
 - Évaluation de la vulnérabilité
 - Suivi des vulnérabilités

Les technologies dans un SOC



Sécurité vs. Disponibilité

- Les réseaux d'entreprise **doivent être opérationnels à tout moment.**
- Chaque entreprise **a une tolérance limitée pour les temps d'arrêt du réseau.** Cette tolérance repose généralement sur une **comparaison du coût du temps d'arrêt par rapport au coût de la protection contre les temps d'arrêt.**
 - Par exemple, dans une petite entreprise de vente au détail avec un seul site géographique, il peut être acceptable d'avoir un routeur comme point de défaillance unique (*single point of failure*).
 - Toutefois, si une grande partie des ventes de cette entreprise provient d'acheteurs en ligne, le propriétaire peut décider de fournir un niveau de redondance pour s'assurer qu'une connexion est toujours disponible.
- **Le temps de disponibilité préféré est souvent mesuré en nombre de minutes d'arrêt par an.**
 - Par exemple, un temps de disponibilité de «cinq neuf» signifie que le réseau est en hausse de 99,999% du temps pour une durée maximale de 5 minutes par an.
 - "Quatre neuf" serait un temps d'arrêt de 53 minutes par an.
- Il y a toujours un **compromis** entre **une sécurité forte** et **un fonctionnement efficace des entreprises.**

Sécurité vs. Disponibilité

Average Downtime Per Year

Availability %	Downtime
99.8%	17.52 hours
99.9% (" three nines")	8.76 hours
99.99% (" four nines")	52.56 minutes
99.999% (" five nines")	5.256 minutes
99.9999% (" six nines")	31.5 seconds
99.99999% (" seven nines")	3.15 seconds

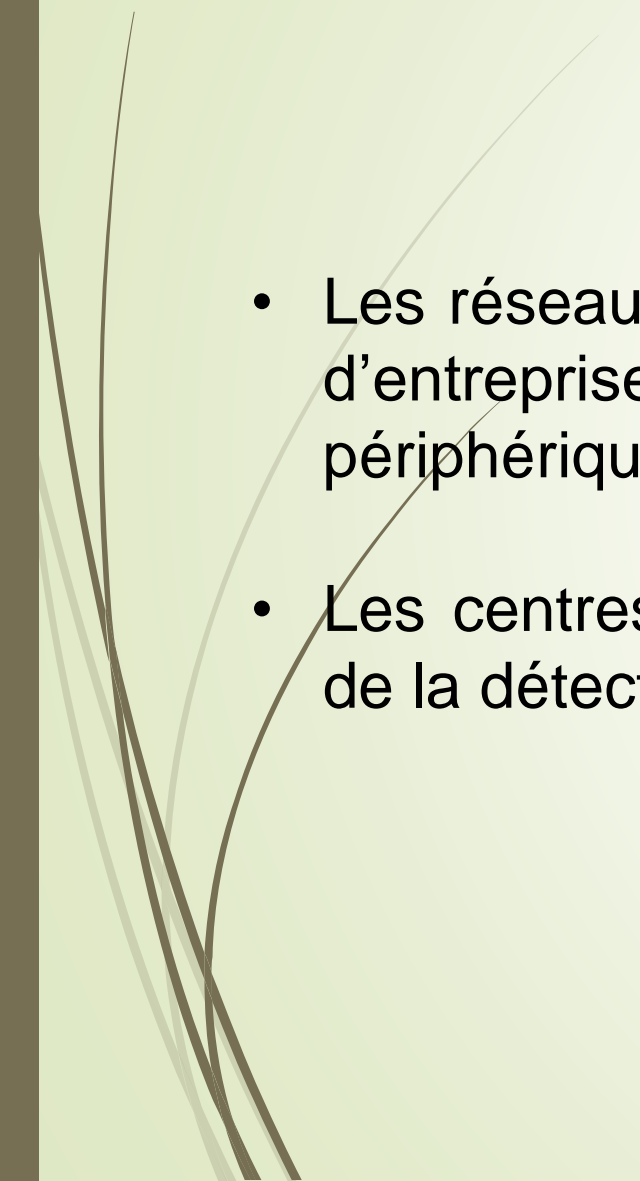


Conclusion

- Des personnes, des entreprises et même des pays peuvent tous être victimes de cyberattaques.
- Différents types d'attaquants, y compris des amateurs qui s'attaquent pour le plaisir et le prestige, des hacktivistes qui tentent de faire avancer une cause politique et des pirates professionnels qui attaquent à des fins lucratives.
- Les pays peuvent attaquer d'autres pays pour obtenir un avantage économique en cas de vol de propriété intellectuelle ou pour endommager ou détruire les actifs d'un autre pays.



Conclusion


- Les réseaux vulnérables aux attaques ne sont pas uniquement des réseaux d'entreprise de PC et de serveurs, mais également des milliers de périphériques sur l'Internet des objets.
 - Les centres d'opérations de sécurité (SOC) sont chargés de la prévention, de la détection et de la réponse à la cybercriminalité.
- 



The END



EXPOSES

- **Par groupe de 3**
 - **Sujet tiré au sort par mes soins**
 - **Noté sur 20**
 - **Compte pour 50% note de partiel**
 - **Rapport à rendre (pdf)**
 - **A présenter sous PPT (max 20min.) pour le 9 novembre**
- 

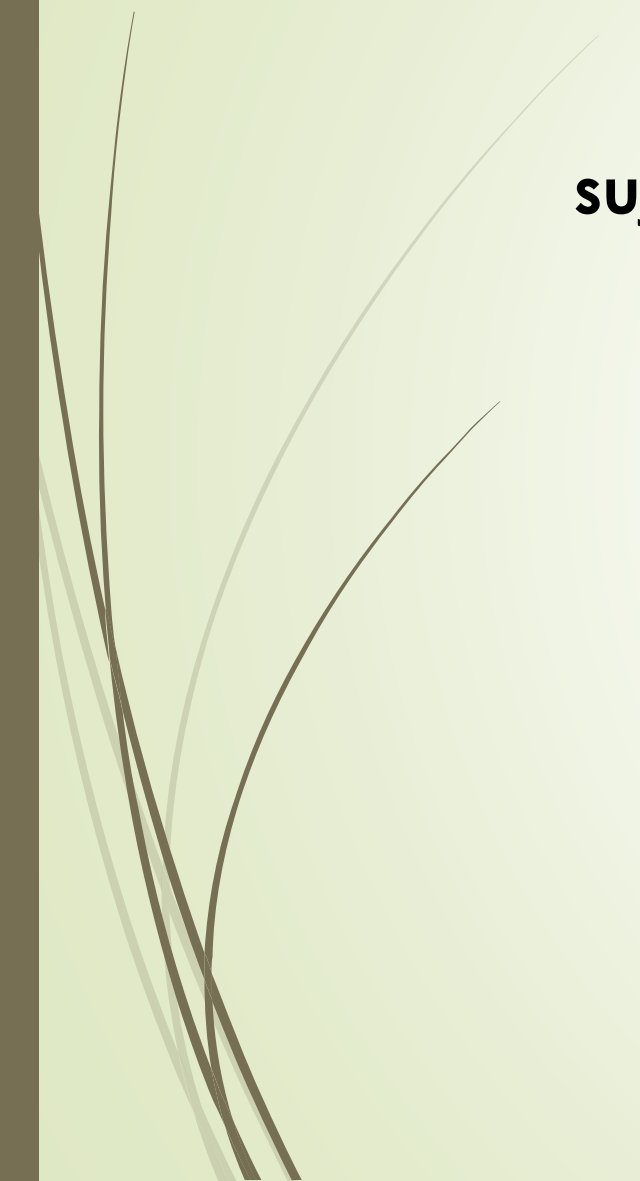


sujet 1: Modèles d'intervention en cas d'incident: la chaîne cybercriminelle

- 2.1- Les étapes de la chaîne cybercriminelle
- 2.2- Reconnaissance (tactique de l'adversaire et défense du SOC)
- 2.3- Militarisation (tactique de l'adversaire et défenses du SOC)
- 2.4- Livraison (tactique de l'adversaire et défenses du SOC)
- 2.5- Exploitation (tactique de l'adversaire et défense du SOC)
- 2.6- Installation (tactique de l'adversaire et défenses du SOC)
- 2.7- Commandement et contrôle (tactique de l'adversaire et défenses du SOC)
- 2.8- Actions sur les objectifs (tactique de l'adversaire et défense du SOC)



sujet 2 : Investigations numériques

- 4.1- Le processus d'investigation numérique
 - 4.2- Types de preuves
 - 4.3- Ordonnance de collecte de preuves
 - 4.4- Chaîne de contrôle
 - 4.5- Intégrité et conservation des données
 - 4.6- Attribution d'attaque
- 



sujet 3 : L'intelligence artificielle



sujet 4 : Le Big Data



sujet 5 : Qu'est-ce que La Blockchain?



sujet 6 : Les crypto monnaies