Orange et CNAM Bretagne, Cybersécurité SEC101, eduf@ction
Notes de cours éditées le 11 novembre 2019

Détecter : de la surveillance à l'évènement de sécurité

Eric DUPUIS[1,2]*

Résumé
Ce document donne les fondamentaux de la gestion de la menace et de sa détection.
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse compilé en un document unique.
Ce document ne constitue pas à lui seul le référentiel du cours. Ce sont des notes de synthèse mises à disposition comme support pédagogique.

Mots clefs
Évènements, attaques, détection, SIEM, SOC

[1] *Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France*
[2] *RSSI Orange Cyberdefense*
***email** : eric.dupuis@cnam.fr – eric.dupuis@orange.com

Veiller sur les menaces nécessite de veiller sur deux choses :

— Les menaces génériques, ou ciblant un domaine particulier (Santé, Industrie, Banque ...) que l'on trouve généralement en utilisant des technologies de "threat Intelligence" permettant

— Les menaces ciblées, dont les indices d'émergence peuvent être détecter en analysant la menace ou en recherchant des indices de compromissions quand ces menaces sont actives dans le périmètre de l'entreprise.

et ceci de deux manières :

— Surveillance de l'écosystème de la menace (IOC, DarkWeb, Threat Intelligence...)

— Recherche de compromission, ou d'infection (Threat Hunting, ...)

Ce sont des sujets que nous aborderons dans le processus de gestion de la menace.

0.0.1 Surveillance de la compromission

Un des domaine de la surveillance est donc celui de la compromission. C'est à dire la surveillance dans le fameux Darkweb de l'emergence de données volées, "perdues" par une entreprise ou par un particulier.

0.0.2 Surveillance du ciblage

La surveillance du ciblage, que les anglo-saxons appelle le TARGETTING est aussi un élément d'anticipation. En effet, ces éléments sont souvent les premiers signaux d'un préparation d'un évènement "cyber" qui pourrait toucher l'entreprise.

On y trouve l'émergence de la collecte d'information sur une cible donnée. La mise en oeuvre dans les code malveillant de targetting d'IP spécifique, etc...

Il y a deux types d'outils pour ce se faire :

— La surveillance classique du web de type "cyberveille", qui permet de découvrir des éléments appartenant à l'entreprise compromis (soient les données, soient des informations permettant de déduire que l'entreprise a été compromise).

— L'analyse en temps réel des codes malveillants qui peut permettre en regardant de manière détaillée l'évolution du code pour comprendre et connaitre les modalités des attaques et les nouvelles cibles.

0.0.3 Que faire des ces informations

Disposer des fragilités de l'entreprise, et connaitre les scénarios potentiels permets d'évaluer un niveau de risque.

1. La gestion de la menace

Gérer la menace comporte deux domaines d'activités :

— La veille, au sens renseignement sur la menace (Threat Intelligence)

— La détection d'attaque, ou de menaces potentielles au sein de l'environnement (Threat Detection)

2. Détecter

"Détecter oui, mais détecter quoi et pourquoi" est la phrase maitresse de la première étape de réflexion autour de la gestion de la détection d'incident de

sécurité. La première question a se poser est qu'est ce qu'un incident de sécurité pour l'entreprise. Si il est vrai qu'il existe un certain nombre de menace "standard" que l'on considère très rapidement comme un incident, le déploiement d'outil de gestion d'incident de sécurité ne serait être limite qu'à cette usage standard.

Il y a de nombreuses manières de détecter des tentatives d'attaques dans un système. Les IPS/IDS (Intrusion Prevention System / Intrusion Detection System), Firewall réseaux et firewall applicatif. Toutefois l'imagination des attaquants est suffisamment grande, pour que des attaques complexes ne puisse être détecté par ces seuls outils et produits de sécurité protégeant les flux informationnels.

Nous pouvons en effet considérer par exemple que la détection d'un rançonlogiciel dans l'entreprise est un bien un incident complexe, qu'un IPS/IDS ne détectera pas, qui va par ailleurs nécessiter une alerte et une remédiation rapide si ce n'est immédiate. Toutefois une fuite d'information sur un système métier par des mécanismes discrets sera souvent étudié spécifiquement. Globalement le déploiement d'une fonction d'alerte va nécessiter la définition des "menaces" redoutés par l'entreprise. Ces dernières sont généralement issus des analyses de risque. En effet, il est important au delà des menaces dits standards de revenir au source du déploiement de fonction de sécurité qui sont de gérer et couvrir les risques.

En premier lieu, il convient de chercher à détecter les menaces non couvertes par les mesures de sécurité, les fameuses menaces résiduelles.

Dans l'environnement de l'entreprise, les scénarios complexes issus de l'analyse de risques lors de l'étude des évènements redoutés vont donner les évènements corrélés à détecter. On y trouvera l'application concrète des arbres d'attaques popularisé par une des plus célèbre cyber expert Bruce Schneier (1) qui est présentée de manière un peu plus détaillée dans le chapitre Arbre d'attaques

3. Alerter

3.0.1 Arbre d'attaques

Les arbres d'attaques sont une représentation des scénarios d'attaques. La racine représente le but final de l'attaque, les différents noeuds sont les buts intermédiaires et les feuilles les actions élémentaires à effectuer. Ces actions seront valuées au potentiel d'attaque des critères communs. On distingue trois types de nœuds :

Nœud disjonctif OR : OU logique. Cela signifie que pour que le nœud soit réalisé, il faut qu'au moins un de ses fils soit réalisé. Nœud conjonctif AND : ET logique. Pour sa réalisation, il faut que l'ensemble de ses fils soit réalisé. Nœud conjonctif séquentiel SAND : Pour sa réalisation, il faut que l'ensemble de ses fils soit réalisé

dans un ordre séquentiel c'est-à-dire les fils sont effectués les uns après les autres dans l'ordre indiqué. En fonction de ces noeuds les valeurs des feuilles seront remontées pour obtenir le potentiel d'attaque de la racine.

Vers ADTool http ://satoss.uni.lu/members/piotr/adtool/ ADTool est un logiciel qui permet la création, l'édition et l'affichage de ces arbres. Il permet de valuer les feuilles et faire remonter les valeurs à la racine selon différents algorithmes

4. Log Management

5. surveiller les fuites

6. Gestion de la menace

Nous avons évoqué dans le chapitre sur l'anticipation, la veille sur la menace. Opérer la détection d'attaques ou de menaces dormante dans l'environnement de l'entreprise nécessite une connaissance précise des mécanismes d'exécution oui d'opération de ces menaces. La connaissance de ces mécanismes d'action, de protection, de déploiement, de réplication, de survivabilité, de déplacement des codes malveillants par exemple est la base de leur détection. Il es en de même sur les scénario mixant des actions sur les réseaux ou sur les systèmes informatiques ou numériques. Ces connaissances sont généralement structurés dans des base de connaissances dont les sources sont gratuites ou payantes.

6.1 Cibles de menaces

6.2 Sources de menaces

Nous parlerons ici de sources de menaces comme les indicateurs permettant d'identifier l'origine technique d'une menace. Cela peut être une adresse mail, un serveur/service de mail , une adresse IP de provenance d'un code malveillant, d'une attaque, ou d'un comportement anormal.

On peut citer par exemple Une adresse mail connue pour envoyer un code malveillant. le blacklistage d'adresse IP ou de d'adresse de serveur Mail pour Spam

En face, il des attaquants qui bien entendue vont changer leur position pour émettre ou attaquer d'ailleurs, ou avec une autre forme (furtivité)

Les sources de menace dans l'environnement internet

6.3 Data Lake

6.4 Threats Huntings

La chasse à la menaces dormantes ou aux compromissions mais aussi le maintien du contact entre la défense et les attaquants.

La chasse aux menaces est une tactique permettant de connaître avec plus d'accuité l'environnement de la menance et donc le degré de risque de cyberattaques auquel est soumise une entreprise.

La terminologie threat hunting regroupe plusieurs type de d'action et la définition de n'est pas totalement stabilisée. Globalement on y trouve deux grande classes de threat hunting

Celle travaillant autour de l'environnent, de la surface d'attaque et qui oriente ses actions sur des méthodes de "recherches" permettant de débusquer des menances latentes ou des menaces dormantes et les reveiller et de les suivre de les comprendres et Pour établir le contact avec l'attaquant.

Et un autres plus active ou proactive dont l'objectif est de rester, conserver le contact avec l'attaquant lors d'une reaction à une alerte.

6.4.1 Etablir le contact

Quand on parle d'établir contact, nous parlons d'aller au contact au sens martial du terme. c'est dire en direct de suivre, caractériser ka sources de la menace et jouer avec elle.

La méthode de "hunter" consiste en premier à dresser un portrait global de la surface d'attaque, tout en identifiant les attaquants potentiels, leurs motifs et leurs façons de faire. Plus précisément, le « threat hunting » consiste en une analyse détaillée de :

— La position de de l'entreprise, notoriété, popularité sur internet, en analysant en particulier les médias traditionnels et les médias sociaux ;

— l'environnement économique de l'entreprise dont ses fournisseurs, ses clients, ses partenaires, ses employés ;

— le corpus technologiques et physique de l'entreprise, dont les architectures techniques et les mécanismes informatique avec l'environnement économique ainsi l'environnement sécuritaire de ses relations.

Sur la base de cette analyse globale, des SPOF (Sigle Point Of Failure) peuvent être trouvés.

grace à la visualisation globale des lien il sera possible comprendre où, comment, pourquoi et potentiellement par qui (hactivistes, anciens employés, fournisseurs, etc.) la prochaine attaque pourrait être perpétrée. Les « threat hunters

», ne sont pas simplement en attente de répondre aux alertes du système de défense, ils cherchent activement des menaces dans leurs propres réseaux afin de prévenir ou de minimiser les dommages. Cette méthode s'avère l'une des plus proactives.

7. SIEM

7.1 un peu d'histoire

Au dela du fait que SIEM est aussi un prénom vient de l'hébreu shim'ôn, "qui est exaucé". le SIEM est aujourd'hui l'aboutissement d'un veux trés anciens des responsable sécurité qui supervise depuis bien des decenies des systèmes de contrôle périmétriques : Corréler tous les évènements arrivants sur l'ensemble de ces équipements.

ce genre d'outillage est passer par différentes étapes de maturation avec des SIM et SEM en effin des SIEM

Bien qu'outillant des processus très similaires mais distincts, les trois acronymes SEM, SIM et SIEM ont tendance à être confus ou à causer de la confusion chez ceux qui sont relativement peu familiarisés avec les processus de sécurité.

La similitude entre la gestion des événements de sécurité ou SEM et la gestion des informations de sécurité ou SIM est au cœur du problème.

Ces deux types de collecte d'informations concernent la collecte d'informations de journal de sécurité ou d'autres données similaires en vue d'un stockage à long terme, ou l'analyse de l'environnement de sécurité d'un réseau.

La principale différence est que,

— dans la gestion des informations de sécurité (SIM) , la technologie consiste à collecter des informations à partir des journaux d'équipement de sécurité, qui peut consister en différents types de données. Gloablement on peut dire qu'un SIM est immement important pour des équipes de superviusion de la sécurité périmitrique. d'une part pour la traçabilité et le reporting de sécurité.

— technologies spécialement conçues pour rechercher des authentifications suspectes, des ouvertures de session sur un compte ou des accès de gestion de haut niveau à des heures précises du jour ou de la nuit.

L'acronyme SIEM ou «gestion des informations de sécurité» fait référence à des technologies combinant à la fois la gestion des informations de sécurité et la gestion des événements de sécurité. Comme ils sont déjà très similaires, le terme générique plus large peut être utile pour décrire les outils et les ressources de

sécurité modernes. Là encore, il est essentiel de différencier la surveillance des événements de la surveillance des informations générales. Un autre moyen essentiel de distinguer ces deux méthodes consiste à considérer la gestion des informations de sécurité comme une sorte de processus à long terme ou plus large, dans lequel des ensembles de données plus diversifiés peuvent être analysés de manière plus méthodique. En revanche, la gestion des événements de sécurité examine à nouveau les types d'événements utilisateur pouvant constituer des signaux d'alerte ou indiquer aux administrateurs des informations spécifiques sur l'activité du réseau.

C'est souvent l'usage d'un SIEM dans une ambiguïté de gestion long terme de la sécurité en tant que propriété d'un système d'une part, et la gestion court terme de l'urgence d'une attente à la sécurité qui pose problème dans les projets et dans les opérations.

La cyberprotection d'une entreprise est principalement basée sur les outils de protection périmétriques que ceux ci soit des équipements physiques ou qu'ils soient dans le cloud : systèmes de détection d'intrusion (IDS), scanners de vulnérabilités, antivirus ainsi que systèmes de gestion et corrélation d'événements sécurité (SIEM). Lorsqu'il s'agit de superviser un système informatique à grande échelle réparti sur plusieurs sites, il devient vite très difficile de corréler et analyser toutes les sources d'information disponibles en temps réel afin de détecter les anomalies et les incidents suffisamment vite pour réagir efficacement. Cette complexité est due à la quantité d'information générée, au manque d'interopérabilité entre les outils ainsi qu'à leurs lacunes en matière de visualisation.

la premiere fonction d'un SIEM est déjà de corréler les événements provenant des composants de sécurité. la deuxième fonction de corréler des événement de comportement du SI troisième fonction de corréler avec des événements externes au SI sur la base de capteurs externes (threats intelligence de type renseignement)

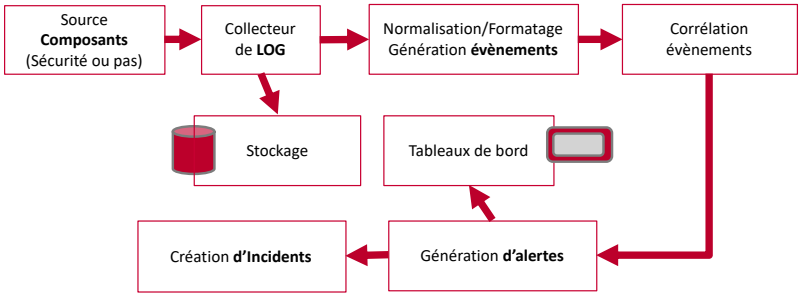

FIGURE 1. architecture d'un SIEM

7.1.1 Analyse d'impact

Un autre problème majeur dans l'usage d'un SIEM est que l'action de comprendre l'impact réel d'une vulnérabilité ou d'une alerte IDS est généralement dévolue à un analyste cybersécurité humain, qui doit lui- même faire le lien entre toutes les informations techniques et sa connaissance de tous les services ou processus liés aux incidents de sécurité détectés sur les composants concernées (serveurs, PC, smartphone, IOT,...) .

Le projet DRA est une étude complémentaire de CIAP qui vise à fournir une analyse de risque en temps réel, afin de déterminer automatiquement l'impact réel dû à la situation sécurité globale du système et du réseau. Pour cela une nouvelle méthodologie innovante a été développée en combinant un générateur automatique d'arbres d'attaque (attack trees/graphs) et un moteur d'analyse de risque « traditionnel » similaire à EBIOS.

Les systèmes de gestion des informations et événements de sécurité (SIEM) font régulièrement l'objet de critiques acerbes. Complexité, besoins importants en ressources de conseil externes. . . de nombreuses entreprises ont été déçues par leur expérience du SIEM pour l'implémentation de la supervision de la sécurité.

Mais la technologie n'est plus, désormais, la raison pour laquelle des entreprises peinent à réussir leurs implémentations de SIEM. Les principales plateformes de SIEM ont reçu de véritables transplantations cérébrales, se transformant en entrepôts de données taillés sur mesure pour fournir les performances et l'élasticité requises. Les connecteurs système et les aggrégateurs de logs, autrefois complexes et peu fiables, sont aujourd'hui efficaces, rendant la collecte de données relativement simple.

Mais il y a une limite au SIEM, comme à toute technologie s'appuyant sur des règles : le SIEM doit savoir ce qu'il doit chercher. Aucun boîtier SIEM ne pourra identifier automatiquement, comme par magie, une attaque tirant profit d'une méthode ou d'une vulnérabilité inédite.

Le SIEM joue un rôle important dans la détection d'attaques. Mais pour qu'il puisse détecter les attaques connues et inconnues, l'entreprise qui le déploie doit construire des ensembles de règles qui lui permettront d'identifier des conditions d'attaques et des indicateurs spécifiques à son environnement. Et le tout de manière cohérente. Comment donc construire ces règles ?

Tout collecter

Sans disposer de suffisamment de données collectées, le SIEM n'a pas grand chose à analyser. Mais la première étape est de collecter les bonnes données. Et celles-ci sont notamment les logs des équipements réseau, de sécurité et des serveurs. Ces données sont nombreuses et faciles à obtenir. Ensuite, il faut s'intéresser

aux logs de l'infrastructure applicative (bases de données, applications). Les experts du SIEM ajoutent à cela les données remontées par de nombreuses autres sources, comme celles des systèmes de gestion des identités et des accès, les flux réseau, les résultats des scans de vulnérabilités et les données de configurations.

Avec les SIEM, plus il y a de données collectées, mieux c'est. Si possible, autant tout collecter. S'il est nécessaire de définir des priorités, alors mieux vaut se concentrer sur les actifs technologiques critiques, à commencer par les équipements installés dans les environnements sensibles et ceux manipulant des données soumises à régulation, ou encore ceux touchant à la propriété intellectuelle.

Construire les règles

Construire une règle pour SIEM est un processus itératif. Cela signifie qu'il est relativement lent et qu'il doit être affiné, précisé au fil du temps. De nombreuses personnes sont atteintes de la « paralysie de l'analyste » en début de processus, parce qu'il existe des millions de règles pouvant être définies. Ainsi, Securosis conseille de se concentrer sur les menaces les plus pressentes pour déterminer les règles à définir en premier.

Dans le cadre du processus de modélisation, il convient de commencer par un actif important. Pour cela, il faut adopter le point de vue de l'attaquant et chercher ce que l'on pourrait vouloir voler.

Modéliser la menace. Il faut se mettre à la place de l'attaquant et imaginer comment entrer et voler les données. C'est la modélisation de l'attaque, avec énumération de chaque vecteur avec le SIEM. Et il convient de ne pas oublier l'exfiltration car sa modélisation offre une opportunité supplémentaire de détecter l'attaque avant que les données ne se soient envolées. Dans ce processus, il s'agit d'adopter des attentes réalistes car le modèle d'attaque ne peut pas par essence être parfait ni complet. Mais il convient toutefois d'engager le processus de modélisation. Et il n'y a pas de mauvais point de départ.

Affiner les règles. Il convient ensuite de lancer l'attaque contre le SI, telle que modélisée. Les outils pour cela ne manque pas. C'est l'occasion de suivre ce que fait le SIEM. Déclenche-t-il les bonnes alertes ? Au bon moment ? L'alerte fournit-elle suffisamment d'informations pour assister les personnes chargées de la réaction ? Si l'alerte n'est pas adéquate, il convient de revoir le modèle et d'ajuster les règles.

Optimiser les seuils. Avec le temps, il deviendra de plus en plus clair que certaines alertes surviennent trop souvent, et d'autres pas assez. Dès lors, il convient d'ajuster finement les seuils de déclenchement. C'est toujours une question d'équilibre... un équilibre délicat.

Laver, rincer, recommencer. Une fois l'ensemble initial de règles pour ce mo-

dèle d'attaque spécifique implémenté et optimisé, il convient de passer au vecteur d'attaque suivant, et ainsi de suite, en répétant le processus en modélisant chaque menace.

Ce processus ne s'arrête jamais. Il y a constamment de nouvelles attaques à modéliser et de nouveaux indicateurs à surveiller. Il est toujours important de suivre les informations de sécurité pour savoir quelles attaques sont en vogue. Les rapports tels que celui de Mandiant sur le groupe APT1 intègrent désormais des indicateurs clairs que chaque organisation peut surveiller avec son SIEM. Armé de ces renseignements sur les menaces et d'un environnement de collecte de données complet, il n'y a plus d'excuse : il est temps de commencer à chercher les attaques avancées qui continuent d'émerger.

Mais avec le temps, il sera nécessaire d'ajouter de nouveaux types de données au SIEM, ce qui impliquera de revoir toutes les règles. Par exemple, le trafic réseau, s'il est capturé et transmis au SIEM, fournira quantité de nouvelles informations à étudier. Mais comment ce regard sur le trafic réseau sera-t-il susceptible d'affecter la manière dont certaines attaques sont traitées ? Quelles autres règles faudrait-il ajouter pour détecter l'attaque plus vite ? Ce ne sont pas des questions triviales : il convient de revoir les règles du SIEM chaque fois qu'est ajoutée une nouvelle source de données (ou retirer, le cas échéant) ; cela peut faire la différence sur la rapidité avec laquelle une attaque est détectée… si elle l'est.

Le plus important aspect de ce processus est la cohérence. Le SIEM n'est pas une technologie du type « installe et oublie ». Il requiert du temps, de l'attention, et d'être alimenté, tout au long de sa vie opérationnelle.

7.2 quelques défits des SIEM

La problématique globale des SIEM est de corréler de l'événement, la question de fond est la collecte de ses évènements. La collecte de LOG est la principale sources d'événements, toutefois, toute les sources d'événements sont susceptible d'enrichir la corrélation, en particulier les vulnérabilités, les IOC, les infos de end-point en gros corrler des inforamtions d'opératione et de renseignements. Cette notion de FUSION de capteurs cher au militaire est un premier pas et nécessite en parrallele aussi de l'information econimoqie, poltiques ou sociale de l'entreprise. Car ces événements peuvent "matcher" avec des attaques complexes.

7.3 l'intelligence artificiel

Le traitement de masse permet

Mais l'important est que l'IA (ex : vectra) puisse explicquer ses propositions et décisions.

8. quelques SIEM

On peut ciert ainssi quelques SIEM non pas pour en faire un publicité particuliers mais simplement pour donner quelques indications sur la provenance ...

9. L'integration dans la gestion des incidents ITIL

10. Le SOC

Les SOC est au coeur du système de Veille Alerte et réponse. C'est la tour de contrôle de l'espace Cyber.

11. le SOC de demain

On peut par ailleurs s'interroger sur le fait qu'un tel système peut et doit opérer d'autres missions que les missions de sécurité pures. Si la supervision des réseaux a été longtemps au outils au services des techniciens, la supervision de l'environnement digital c'est à dire l'environnement informationnel de l'entreprise est un axe fondamental. Le SOC Security Operation Center peut devenir Cyber Operational Center opérant le suivi des risques digitaux au sens large, incluant les réseaux sociaux et leur cohorte de fausse informations et d'information pouvant être des indicateurs de crise à venir pour l'entreprise.

11.1 Evaluation d'un SOC

L'efficacité d'un SOC

https ://www.globalsecuritymag.fr/SOC-comment-en-mesurer-l,20151005,56416.html

Integration du threats hunting dans les SOC. Par exemple suivre la création de nom de domaine récent pour regarder les noms utiliser dans des requêtes.

11.2 Les outils connexes d'un SOC

au dela des SIEM, il semble important d'ajouter à l'outillage dun SOC un ensemble de système permettant de mesurer et d'évaluer l'impact des attaques. Echelle de RICHTER d'une attaque.

https ://observatoire-fic.com/prendre-la-mesure-des-cyberattaques-peut-on-definir-une-echelle-de-richter-dans-le-cyber/

Références

(1) Bruce SCHNEIER. « Attack trees ». In : *Dr. Dobb's journal* 24.12 (1999), pages 21-29 (cf. page 3).

12. Contributions

12.1 Comment contribuer

Les notes et les présentations sont réalisées sous LaTeX.

Vous pouvez contribuer au projet des notes de cours CNAM SEC101 (CYBERDEF101). Les contributions peuvent se faire sous deux formes :

— Corriger, amender, améliorer les notes publiées. Chaque semestre et année des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.

— Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de votre expertise dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace : (edufaction/CYBERDEF) [1] . Le fichier Tex/Contribute/Contribs.tex contient la liste des personnes ayant contribué à ces notes.
Le guide de contribution est disponible sur le GITHUB. Vous pouvez consulter le document **SEC101-C0-Contrib.doc.pdf** pour les détails de contributions.

12.2 Les contributeurs/auteurs du cours

Les auteurs des contributions sont :

12.2.1 Années 2019

— **François REGIS** (Orange) : CyberHunting

12.2.2 Années 2018

— **Julia HEINZ** (Tyvazoo.com) : ISO dans la gouvernance de la cybersécurité

1. https://github.com/edufaction/CYBERDEF

Table des matières

Table des figures