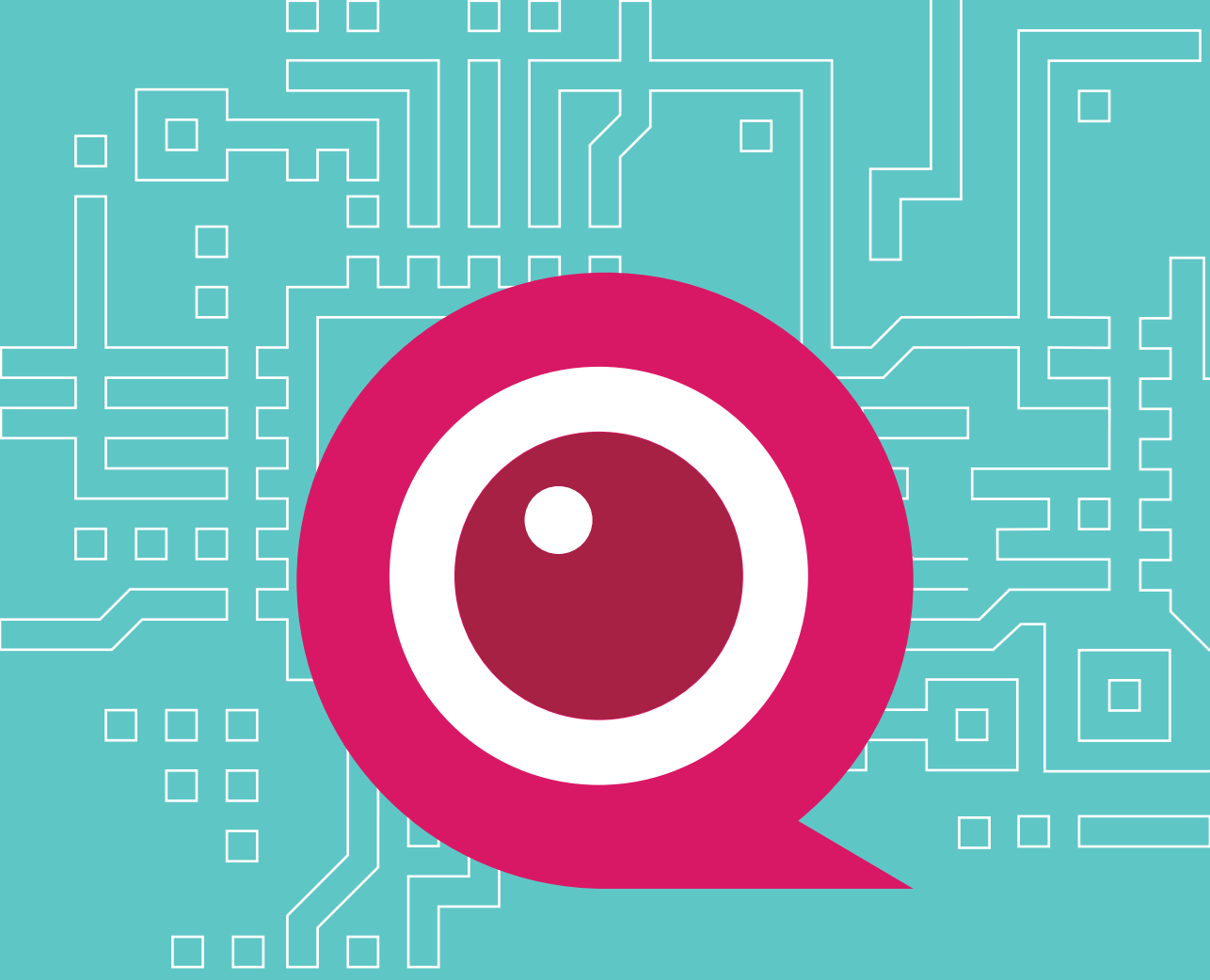


CYBERSÉCURITÉ &INNOVATIONS

ÉDITION 2019

Le regard des Assises et de l'EPITA

LES ASSISES

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

2E ÉDITION

READY FOR IT!

25 > 27 MAI 2020

MONACO

LE RENDEZ-VOUS
DE LA CONVERGENCE DES TECHNOLOGIES

Cloud **Data** **Cyber**

LES ASSISES 2 EPITA

DG CONSULTANTS

COMEXPOSIUM

CHIFFRES CLÉS DES ASSISES 2019

3 100
PARTICIPANTS

7 300
RENDEZ-VOUS ONE TO ONE

171
ATELIERS ET CONFÉRENCES

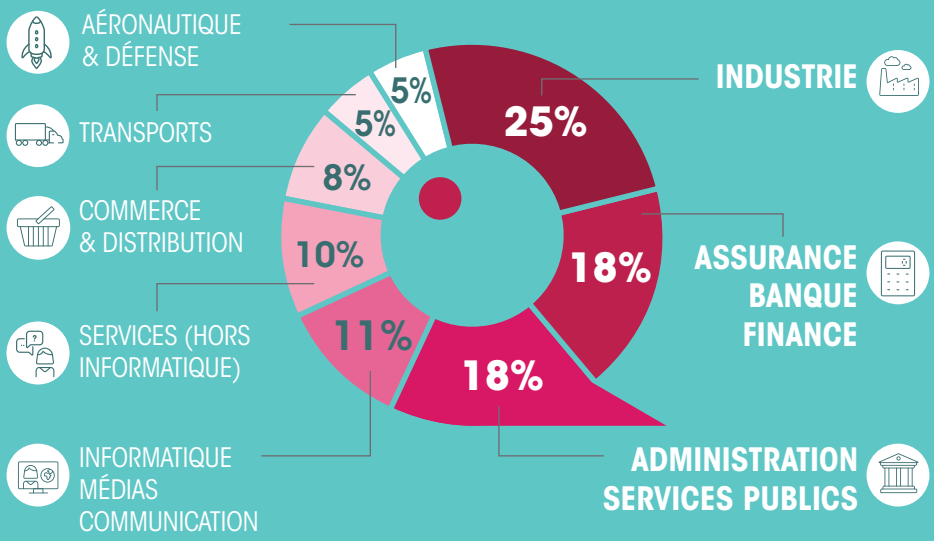
1 330 **RSSI & DSI**
REPRÉSENTANTS
686 SOCIÉTÉS

+41% **DE NOUVEAUX INVITÉS**

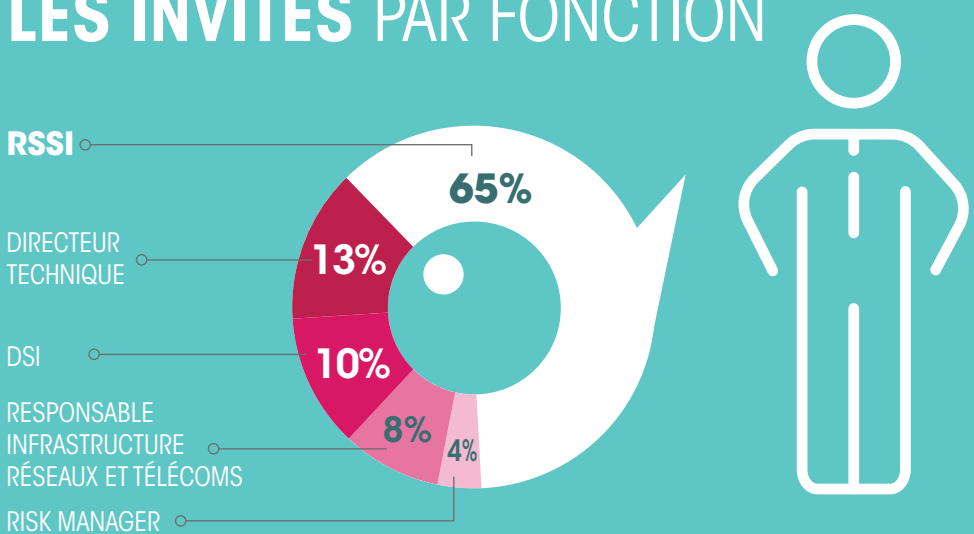
163 **PARTENAIRES**

54 **JOURNALISTES & BLOGUEURS**

LES INVITÉS PAR SECTEUR



LES INVITÉS PAR FONCTION



Pour réussir, le RSSI doit être dynamique, communicant et transversal

Gérard Leymarie,
CISO et DPO du Groupe Elior

CISO et DPO du Groupe Elior, Gérard Leymarie a remporté le Prix Spécial du Jury du Grand Prix des RSSI 2019. C'est également un ancien élève de l'EPITA. Il revient sur son parcours et la fonction de RSSI.

VOUS ÊTES DIPLÔMÉ DE L'EPITA (promotion 1999). POURQUOI À L'ÉPOQUE AVOIR CHOISI CETTE ÉCOLE D'INGÉNIEUR ?

Je cherchais une formation très opérationnelle et très pragmatique qui soit aussi bien orientée sur la technique que sur la partie magistrale. L'EPITA répondait à ses attentes avec ses méthodes *(avec la fameuse piscine reprise depuis par d'autres écoles, ndlr)*, le fait de travailler en mode projet et en équipe. C'était peu courant dans les écoles d'ingénieur. L'EPITA fut vraiment pionnière dans ce domaine.

ET COMMENT ÊTES-VOUS ARRIVÉ DANS LE SECTEUR DE LA SSI ?

C'était un sujet qui m'intéressait déjà quand j'étais à l'EPITA. J'avais pris une spécialisation télécoms et réseaux dans laquelle il y avait de la sécurité. Et d'une façon générale, nous avions une bonne sensibilisation à cette problématique, à travers une approche originale, très pratique. Après un an dans une SSII, j'ai rejoint le groupe Accor comme Responsable sécurité infrastructure où j'ai eu l'occasion de travailler avec Serge Saghroune. À l'époque, nous n'étions que deux pour nous occuper de la sécurité informatique d'un groupe international (ils sont aujourd'hui une trentaine). Nous avons tout fait. Ce fut une excellente formation. J'ai appris à parler au Comex, aux utilisateurs, tout en restant en contact avec la partie technique. Pour moi, c'est essentiel. Durant toute ma carrière, je n'ai jamais voulu décrocher de la technique car je veux comprendre les problématiques technologiques.

APRÈS L'ENTREPRISE PRIVÉE, VOUS AVEZ PASSÉ HUIT ANS À L'ANSSI. POURQUOI CE PASSAGE DANS LE PUBLIC ?

Par appétence et aussi pour la dimension patriotique du poste *(Gérard Leymarie est Commandant de réserve d'active au sein de la Gendarmerie Nationale, ndlr)*. J'ai pensé que je verrais un aspect métier que je ne connaitrais pas ailleurs. Et ce fut le cas. Ces huit années m'ont permis de travailler avec tous les milieux (les entreprises, les politiques, les administrations) et cela m'a également apporté de nouvelles compétences notamment sur la réglementation et la conformité. Aujourd'hui, quand il faut monter un dossier d'homologation NIS par exemple, je sais faire. Grâce à cette expérience à l'ANSSI, j'ai vraiment pu acquérir un profil multicarte.

EN 2018, VOUS REJOIGNEZ LE GROUPE ELIOR EN TANT QUE CISO ET DPO : DES NOUVEAUX CHALLENGES ?

Oui. Il y avait une énorme marge de progression mais j'ai l'opportunité de restructurer la sécurité au niveau international. Dans le futur, je voudrais m'inscrire dans les propos de Guillaume Poupard aux Assises, « back to basic » et « ne faites plus peur ». Ancrer les fondamentaux, faire respecter les règles d'hygiène informatique, faire que la sécurité soit dans l'ADN de tous les collaborateurs. Il est indispensable que les basiques (patch management, firewall, antivirus) soient intégrés dans tous les projets. Et cela aussi bien chez nos développeurs et architectes qui travaillent sur les applications «On premise» que pour les projets Cloud.

QUE PENSEZ-VOUS DE LA FONCTION DE RSSI AUJOURD'HUI ?

Le métier du RSSI reste lié au profil du RSSI. C'est vous qui façonnez votre poste. Et si vous en avez la volonté, vous pouvez lui donner une grande dimension. J'ai construit ma place et j'ai aussi beaucoup communiqué (c'est essentiel). Par exemple, pour la protection des données, le RSSI peut devenir le « key driver ». Aujourd'hui, chez Elior, nous faisons la différence lors des appels d'offre parce que nous avons été différenciants sur notre politique de traitement des données personnelles et nous l'affichons sur notre site.

EST-CE UN MÉTIER D'AVENIR ?

Absolument. La sécurité prend une place de plus en plus importante dans les projets et le RSSI a un rôle important à jouer dans l'entreprise et dans la DSI. Pour ma part, j'ai une vision opérationnelle de la stratégie donnée par le DSI et de sa mise en œuvre sur le terrain. Mais pour réussir, le RSSI doit être dynamique, communicant et transversal.

Conférence d'ouverture,
Guillaume Poupard,
Directeur Général de l'ANSSI

Vers une cybersécurité positive

Ouvrant la 19ème édition des Assises de la Sécurité, Guillaume Poupard, le Directeur Général de l'ANSSI s'est d'abord voulu très solennel : *« nous ne sommes pas dans une situation de guerre mais nous n'en sommes pas très loin ».* Des propos forts, portés par plusieurs constats : d'une part des entreprises qui, face à la fréquence des cyberattaques ont le sentiment d'être devenues des victimes de guerre. Et puis des États, de plus en plus agressifs, qui n'hésitent pas à recourir au « cybermonde » pour menacer voir attaquer. Dans ce contexte, le DG de l'ANSSI a insisté sur un point essentiel : s'il convient d'être vigilant et de prendre en compte ces questions de sécurité numérique, en revanche, il faut arrêter de faire peur. Certes, il y a un vrai manque d'hygiène informatique de la part de la population mais la terreur ne fonctionne plus.

La solution se trouve d'abord dans la sensibilisation. Et dans la recherche de solutions adaptées à la transformation digitale et aux besoins des entreprises. Pour ce faire, « la France a des atouts » : elle a construit des bases solides et son modèle qui fait coopérer différentes entités privées et publiques est l'un des plus efficaces au monde. Néanmoins, dans la course technologique actuelle, il convient de renforcer ce socle en investissant dans l'innovation.

Parmi les pistes explorées pour répondre à ce besoin d'évolution, Guillaume Poupard a annoncé la création d'un Campus Cyber qui réunira acteurs publics et privés, chercheurs et startups, avec pour objectif une stimulation commune afin de travailler sur des sujets essentiels comme l'intelligence artificielle. Un autre axe suivi par l'ANSSI est l'Open Source, car « la sécurité par l'obscurité n'est pas une voie pérenne ». Actuellement, l'Agence développe deux projets Open Source : OpenCTI *(voir encadré)* sur la Threat Intelligence et DFIR ORC une « boite à outils » constituée par les auditeurs de l'ANSSI à partir des réponses à incident accumulées pendant 10 ans. *Comme le rappelle le Directeur Général, « la détection est le plus gros point faible dans le domaine de la cyber et son amélioration est prioritaire » avant de conclure son message par l'espoir que ces projets, ces évolutions que l'ANSSI et tout l'écosystème porte, nous conduisent vers une « cybersécurité positive ».*

Samuel Hassine, *chef du bureau analyse de la menace à l'ANSSI,* présente le projet OpenCTI

« La genèse d'OpenCTI est relativement simple. Depuis plusieurs années, l'ANSSI a déployé la plateforme MISP (Malware Information Sharing Platform) et des analystes sont chargés de lui fournir des indicateurs de compromission. Cependant, il n'existait pas d'outil comparable pour référencer tous les éléments de la partie pratique opérationnelle comme les tactiques mises en œuvre par les attaquants, les campagnes d'attaques, la victimologie, les grands acteurs et les attributions, jusqu'alors, le référencement de ces différents éléments se faisait à la main par l'analyste dans les pages du wiki, dans des fichiers Excel ou dans des rapports conséquents en PDF.

Il y avait donc besoin de disposer d'un outil pour générer de la donnée structurée pouvant être mise à disposition sur une plateforme consultable par chacun. L'objectif est d'avoir une plateforme accessible à l'ensemble des métiers de la sous-direction des opérations pour la partie réponse à incident et le SOC. C'est un complément à l'infrastructure MISP.

Le produit a été rendu Open Source le 28 juin 2019. Nous travaillons avec le CERT de l'Union Européenne afin de faire évoluer la plateforme également en fonction de leurs besoins. D'autres acteurs, dont des entreprises privées rejoindront peut-être à terme le projet, mais il s'agit d'un produit développé à l'ANSSI pour l'ANSSI qui gardera par conséquent, plus de poids dans les prises de décisions ».

Rajiv Ramaswami,
Chief Operating Officer

Keynote VMware

Il est temps de passer à la sécurité intrinsèque

« Une once de prévention vaut une livre de remède. » C'est en ces termes que Rajiv Ramaswami, Chief Operating Officer Products and Cloud Services de VMware a introduit sa keynote. Cette citation qui provient d'un article écrit par Benjamin Franklin en 1735 évoquait la lutte contre le feu. Mais il est tout à fait réaliste de faire une analogie entre celle-ci et la cybersécurité car le principe reste le même : pour le feu, ce sont les personnes et les équipements qu'il faut protéger ; pour la cybersécurité, ce sont les applications et les données. En poursuivant l'analogie, on comprend que l'anticipation d'un événement redouté est la clé pour éviter que cet événement se produise.

Le problème de la cybersécurité est d'être très réactive et aussi fortement cloisonnée. Les environnements IT actuels sont en effet composés de différentes technologies et applications interconnectées, apportant chacune son ensemble d'outils et de politiques de sécurité. Un défaut de configuration peut donc créer une faille susceptible de compromettre l'écosystème global. Pour Rajiv Ramaswami, il est indispensable de changer de paradigme : passer à un modèle de sécurité intégrée, devenir proactif et enfin basculer d'un modèle en silo à un modèle plus harmonisé.

Mais la mise en place d'une sécurité intrinsèque ne consiste pas en l'ajout de bouts de sécurité sur chaque élément du SI. Elle doit devenir partie intégrante de l'infrastructure. Pour le COO de VMware cela passe par la sécurisation de plusieurs éléments : le workloads, le réseau, l'endpoint et l'identité des utilisateurs. Les méthodes de défense étant différentes pour chaque élément.

Ainsi pour les workloads, la virtualisation va permettre de garantir une meilleure flexibilité et une plus grande isolation des postes de travail et des applications. Concernant la sécurisation du réseau, il est commun de voir des protections "Nord-sud" protégeant l'infrastructure de l'extérieur. Mais une approche différente, la protection "Est-ouest", permet un cloisonnement des applications afin d'éviter la propagation d'une attaque en suivant le principe du moindre privilège. Enfin, concernant la sécurité des endpoints utilisateurs, il faut vérifier trois points : le niveau de confiance du périphérique, l'identité de l'utilisateur et les droits d'accès aux applications.

En conclusion de ses propos, Rajiv Ramaswami, insiste sur le fait que pour avoir une infrastructure sécurisée, il est indispensable que les différentes équipes de sécurité communiquent entre elles.

Keynote Atos

Quelle stratégie pour une Europe de la cybersécurité souveraine et puissante ?

En 2018, l'Union Européenne (UE) lançait le programme Digital Europe. L'objectif de ce programme - pour lequel l'UE s'est engagée à investir 9,2 milliards d'euros entre 2021 et 2027 - est le développement d'une Europe digitale forte ainsi qu'une industrie digitale capable d'assurer une certaine autonomie et souveraineté européenne.

Des réglementations ont déjà vu le jour dans ce sens, comme le RGPD, la directive NIS ou le Cybersecurity Act. Ces contraintes réglementaires sont nécessaires pour accompagner la politique industrielle et apporter de nouveaux services de confiance aux utilisateurs. Mais elles sont complexes à mettre en place. Il faut en effet gérer à la fois l'alignement européen sur la question et les intérêts stratégiques des différents pays.

Pour Coralie Héritier, Directrice Générale d'IDnomic, et Alexis Caurette, Vice-président d'Atos Cybersecurity Products, la montée de l'Europe en matière de cybersécurité possède une deuxième facette : celle d'une action stratégique dans un contexte de guerre économique. Cette guerre économique se constate aujourd'hui à travers l'augmentation et la montée en intensité des attaques cyber sur les entreprises comme sur les organismes publics.

Enfin, le troisième aspect de ce besoin de constituer une Europe de la sécurité est géopolitique. L'exploitation de lois extraterritoriales comme le Cloud Act est un sujet critique car il permet au gouvernement américain d'exploiter ainsi l'hégémonie digitale développée sur son territoire comme levier sur l'Europe. Pour les deux intervenants, il est donc urgent de reprendre le contrôle de la donnée en Europe.

Si la difficulté est d'équilibrer la souveraineté numérique de chaque pays et l'autonomie stratégique européenne, il est toutefois possible de tirer parti de la diversité européenne en coordonnant les savoir-faire des différents États membres et en se dotant d'une capacité de lobbying suffisamment puissante.

Quant au financement, il convient de réfléchir à la manière de mieux accompagner les sociétés à l'international et de pousser au développement de pépites technologiques européennes. *Une solution pourrait être la disposition d'un budget cybersécurité en Europe, à l'image des budgets qui existent déjà en matière d'innovation.*

Alexis Caurette, *Vice-président d'Atos* et Coralie Héritier, *Directrice Générale d'IDnomic*

Keynote Proofpoint

Ryan Kalember
Cybersecurity Strategist

Pourquoi les cybercriminels en savent plus que vous sur vos employés ?

Lors de sa keynote, Ryan Kalember, Vice-Président Exécutif et expert cybersécurité chez Proofpoint a souhaité démontrer qu'aujourd'hui les cyberattaques s'appuient davantage sur le leurre des victimes que sur l'exploitation technique des vulnérabilités. Et, bien que 93% des brèches soient des attaques ciblant spécifiquement des personnes (et 96% de ces attaques se faisant via un email), le budget accordé à la sécurisation des courriels ne représente que 8% du budget total contre 62% accordés à la sécurisation du réseau. Mieux comprendre la cible humaine est donc crucial pour contrer les menaces. Cela passe avant tout par l'identification des "VAP" (Very Attacked People) qui ont des accès privilégiés comme les CEO, CFO, Country Manager… Une fois repérées, ces cibles doivent être soumises à des contraintes de sécurité particulières : vérification antivirale plus approfondie des emails ; authentifications à plusieurs facteurs obligatoires ; participations à des sessions de sensibilisation spécifiques en fonction des vulnérabilités qu'elles peuvent générer… Ryan Kalember conclut en expliquant que la sécurité centrée sur l'Homme est une fantastique opportunité pour les équipes de sécurité de s'engager davantage auprès du business.

Keynote McAfee

Candace Worley
Chief Technical Strategist

Le dilemme de l'automatisation

De nos jours, l'automatisation est encore peu utilisée dans le domaine de la sécurité pour des tâches complexes. C'est le constat que Candace Worley, responsable technique et stratégie et vice-présidente chez McAfee, a dressé lors de sa keynote des Assises. Elle souligne que les organisations automatisent les petites tâches comme celles de la vérification, mais restent encore sceptiques quant à l'automatisation à grande échelle impliquant un contrôle plus important des ressources. L'absence d'une supervision humaine fait craindre les conséquences d'une erreur. Mais face à l'explosion du crime cyber, à l'augmentation des données de surveillance, au manque d'experts cyber, les entreprises doivent impérativement changer de paradigme. L'automatisation à plus grande échelle et pour des tâches plus complexes devient indispensable. Ainsi associer un expert pour traiter les résultats des systèmes automatisés de traitement de données (à base d'IA) permet de prendre des décisions stratégiques tout en offrant la possibilité de vérifier les résultats du traitement des données.

Focus sur le Startup Corner

Le Startup Corner fait partie des innovations lancées pendant les Assises 2019. Des jeunes sociétés représentatives du dynamisme du secteur de la cybersécurité ont eu l'occasion de présenter leur solution technologique lors d'un elevator pitch dédié. ZOOM sur 5 d'entre elles.

Avec plus de dix ans d'expérience dans le domaine de la cybersécurité, les experts de chez **Harfanglab** ont présenté aux Assises leur logiciel EDR (Endpoint Detection and Response). Une solution ouverte, capable de s'interconnecter avec des outils de threat intelligence, des sandbox et une sonde qualifiée. La solution a été conçue afin d'être capable de dialoguer avec des SIEM ou des SOAR. Cette plateforme unique permet une détection plus sure, une investigation poussée pour réduire le temps de qualification des alertes et donne la possibilité de remédier instantanément à la menace sur l'ensemble du parc infecté.

Reachfive propose une solution SAAS de gestion de l'identité client qui répond au besoin des utilisateurs finaux de décliner toute ou partie de leur identité afin d' accéder à des services. Les utilisateurs peuvent se connecter sans mot de passe via des technologies biométriques, du SSO ou des authentifications multifacteurs. Cette fédération des identités permet de prouver une identité ou de s'assurer de celle-ci. Une des utilisations possibles est de réunir l'ensemble des consentements pour le RGPD.

CybelAngel propose une solution de détection des fuites d'informations qui permet de scanner toutes les couches d'internet (clear web, Github, Pastebin, Twitter) à la recherche de potentielles fuites de données. La solution est également capable de faire des recherches sur le deep et le dark web (à travers les forums), sur les espaces de stockage dans le cloud, sur les bases de données et sur les objets connectés. Chaque fuite est dotée d'un score permettant de déterminer la gravité des données ayant fuitées. CybelAngel propose également un outil d'aide à la remédiation

Weakspot développe une solution SAAS permettant de cartographier l'exposition externe d'une entreprise du point de vue d'un attaquant et ainsi de compléter la vision du RSSI . Une fois ces expositions détectées, des contrôles sont réalisés selon la problématique du client : application de la PSSI ou vérification des dernières vulnérabilités. Pour lancer l'analyse, la solution peut travailler à partir d'une adresse mail, d'une adresse IP ou d'un nom de domaine.

La plateforme de **Tehtris** a pour objectif de couvrir les différents pans de la cybersécurité en entreprise (gouvernance, détection, protection et réaction). Il s'agit d'une interface unifiée qui s'appuie sur une base de données d'alertes de sécurité et sur des connaissances des bases de CTI utilisant des mécanismes d'apprentissage évolués. Cette interface permet de suivre des alertes entre les acteurs via des outils de ticketing mais également de chasser les anomalies et d'y remédier. La startup met à disposition six environnements : un SIEM orienté dans la détection, un EPP (Endpoint Protection Platform) antivirus, un EDR avancé mêlant l'euristique, le sandboxing et l'IA, une protection des terminaux mobiles, des HoneyPot et la mise en place de sondes anti-infection.

Le Startup Corner accueillait également les sociétés Digitemis, Allentis et Seclab

Moabi, Prix de l'Innovation 2019

Vainqueur du Prix de l'Innovation des Assises 2019, Moabi, propose une plateforme SaaS qui effectue des audits de sécurité de logiciel automatisés.

Cette plateforme issue de plus de huit ans de réflexion et de deux ans de développement a été créée à la suite de cette constatation : « Il y a un manque de tests d'intrusion réalisés sur le software, les dépendances aux bibliothèques extérieures sont rarement analysées. L'analyse du code source est insuffisante et ne couvre pas les cas nombreux ou le code n'est pas disponible. De plus, le pentest et les red teams arrivent généralement trop tard dans la conception du produit et ne prennent qu'une image partielle et partiale à un temps fixe, ne testant ainsi pas toutes les vulnérabilités présentes sur un système complexe » explique Nicolas Massaviol, Co-fondateur de Moabi.

Moabi fournit une solution SaaS permettant une analyse sécurité des binaires pour tous les logiciels, avec leurs dépendances. La mesure de la cybersécurité passe par 5 critères clefs :

> Le « **Legacy** » mesure la dette technique relative aux technologies ou à l'architecture.

> Le « **Hardening** » évalue l'activation des fonctions de défense en profondeur des compilateurs.

> La « **Cryptographie** » vérifie la force des algorithmes de chiffrement.

> Les « **Vulnerabilities** » présente les vulnérabilités déjà existantes à travers les CVE, ainsi que les Odays grâce au moteur de Moabi pour l'exécution symbolique et l'analyse de teintes.

> La « **Compliance** » intégre les normes de sécurité de code (Posix, MSSDLC, CE99…).

L'analyse et le test des binaires permet de cartographier (mapping) les forces et faiblesses sécurité d'un logiciel ou un firmware complet. Cette cartographie permet également d'identifier les différences entre 2 versions d'un même logiciel pour augmenter progressivement son niveau de sécurité.

En plus de ces 5 métriques, résumées par un meta-indicateur présentant le niveau globale de sécurité « la surface de défense » Moabi évalue également :

> La **criticité d'un binaire** au sein du logiciel, selon ses accès privilégiés (root/administrateur etc...), pour identifier les binaires à corriger en priorité si leur surface de défense est trop faible

> Une « **obfuscation** » délibérée de code, qui témoigne soit de la présence d'une protection de propriété intellectuelle, soit d'un malware.

Ce produit n'a pas vocation à détecter les backdoors. Aucune alerte ne sera remontée sauf si elles sont mal implémentées. À la suite de cette analyse, deux rapports différents seront générés :

> **Un rapport graphique au travers des 5 métriques** pour piloter la sécurité logicielle par des indicateurs stables et cohérents,

> **Un rapport d'identification des écarts** avec l'état de l'art de la cybersécurité et les nouvelles vulnérabilités détectées, avec des propositions de correction et d'amélioration.

Un prix très convoité

Créé en 2006, le Prix de l'Innovation des Assises de la Sécurité récompense chaque année des solutions innovantes sélectionnées par un jury d'experts de la cybersécurité. Accélérateur de notoriété et de business, le Prix de l'Innovation offre au lauréat une visibilité exceptionnelle auprès de la communauté des Assises. Ce prix s'inscrit dans la vocation des Assises de soutenir le développement de jeunes entreprises du secteur.

Techlab

la coopération technologique au service de la cybersécurité

Après le succès de la première édition du Techlab en 2018, Newlode a organisé de nouveau cette année, un espace de démonstration multi-solutions avec six de ses partenaires[1]. Le thème majeur des sessions, qui se sont succédées pendant les trois jours des Assises était ***«Think like a SOC ».*** Ainsi SentinelOne, ProofPoint et Splunk ont montré comment en collaborant de manière efficace, il était possible de réagir contre du **phishing ciblé** de la façon la plus automatisée possible.

- **ProofPoint** permet d'émettre un score de risque via la mise en évidence des éléments à risques. Il est aussi possible, dans le cas d'une attaque, d'obtenir une visualisation de la ligne directrice de celle-ci ainsi que d'émettre des notifications aux points vulnérables. Tous ces éléments peuvent être récapitulés dans un rapport généré automatiquement.
- **SentinelOne** rend possible la recherche par IOC (Indicateur de compromission) et ainsi de les cartographier. Il permet aussi en l'associant avec le Framework MITRE ATT&CK d'établir une possible séquence d'attaque ou la décomposition de celle-ci. De plus, il est également compatible avec des EDRs.
- **Splunk** permet, via l'utilisation de playbook, une orchestration et une automatisation des fonctions de détection ou de remédiation. Ces actions peuvent être lancées de façon automatique ou déclenchées par un email.

Dans l'ensemble, un rapport est ensuite généré, celui-ci est passé à un analyste SOC qui, à travers ces technologies, va constater la présence ou non de traces d'attaque sur le système. L'objectif est donc de libérer les analystes SOC des tâches automatisables et de les aider à se consacrer sur des tâches requérant une expertise humaine.

[1] *Les autres partenaires du Techlab étaient CrowdStrike, Forescout et Tenable*

Trois questions à Loïs Samain,

RSSI adjoint d'EDF Renouvelables

LOÏS, QUELQUES MOTS SUR VOTRE PARCOURS ?

J'ai 31 ans. Je suis diplômé de l'EPITA 2012, spécialisation SRS (Systèmes, Réseaux et Sécurité). Actuellement, je suis RSSI adjoint du groupe EDF Renouvelables, la filiale des énergies renouvelables d'EDF. J'ai eu plusieurs expériences professionnelles qui m'ont permis de connaitre le secteur de la SSI avant d'arriver à ce poste. J'ai d'abord eu l'occasion de faire des stages durant mes études chez EADS Defence & Security (aujourd'hui Airbus) et HSC, une société de conseil en SSI. Puis, pour mon premier poste, je suis parti travailler pour l'entreprise Bull Amesys (aujourd'hui Atos). Après quelques missions au sein du département PKI et Monétique de Bull, je suis devenu Correspondant Sécurité à l'ANTS (Agence Nationale des Titres Sécurisés) pendant quelques années. Puis, j'ai été contacté pour devenir RSSI d'une ESN, Davidson Consulting et y construire toute la sécurité de l'entreprise. Enfin, il y a un peu plus de deux ans et demi, j'ai rejoint EDF Renouvelables pour m'occuper de la cybersécurité du SI tertiaire et industriel de l'entreprise et ses filiales, dans un secteur passionnant en plein développement : les énergies renouvelables.

À VOIR VOTRE EXPÉRIENCE, ON NE DEVIENT PAS RSSI EN SORTANT DE L'ÉCOLE ?

Non, et même si c'était une volonté de ma part de le devenir un jour quand j'étais à l'EPITA, on ne devient pas RSSI en sortant de l'école. Pour parvenir à ce poste, il faut avant tout prendre le temps d'apprendre et de comprendre les différentes composantes de la cybersécurité. Ça se fait étape par étape. Un RSSI est un chef d'orchestre qui a besoin de comprendre les différents domaines composant sa partition et on ne devient compétent qu'à la suite d'expériences professionnelles (et personnelles). Et puis il y a surtout les compétences humaines à se forger, les soft-skills, dont on parle trop peu mais qui sont, à mon sens, essentiels dans notre métier : la communication envers les différentes parties prenantes de l'entreprise (métiers, fonctions transverses, COMEX), la gestion du stress, l'empathie, la résolution de problèmes, la rédaction, la négociation, la flexibilité, etc. Tout cela s'acquiert avec l'expérience (et durant toute la carrière) et nous sont inconnus en sortie d'école.

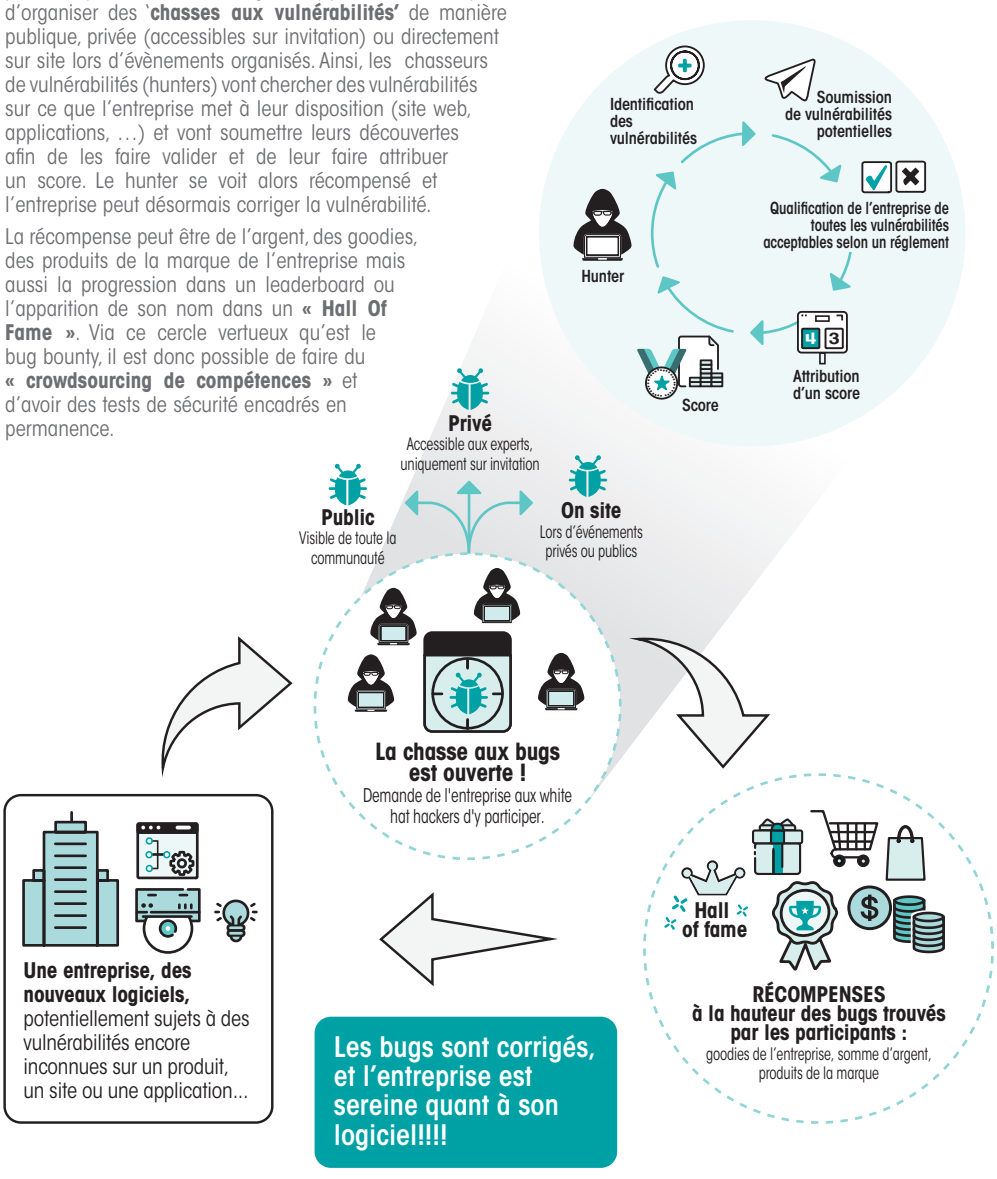
VOUS AVEZ D'AUTRES ACTIVITÉS LIÉES À LA CYBERSÉCURITÉ ?

Absolument. J'ai co-fondé il y a sept ans un podcast « Le Comptoir Sécu » où nous parlons chaque semaine de cybersécurité avec une communauté de passionnés (plus de 3500 écoutes par épisode, 1600 inscrits sur notre Discord). De temps à autre, j'interviens aussi sur NoLimitSecu, un autre podcast sur la cybersécurité. Je suis aussi membre du CESIN, qui est une association fédérant des RSSI et représentants de plus de 500 entreprises et administrations. Cette dernière permet d'échanger régulièrement avec mes pairs sur les différentes questions et problématiques que je rencontre dans mon travail de tous les jours. L'entraide est essentielle dans notre métier et nous avons la chance d'avoir une communauté soudée. Enfin, j'ai la chance depuis 3 ans d'être membre du comité éditorial des Assises de la Sécurité et jury de son prix de l'Innovation *(Voir p.12)*, me permettant de rencontrer et d'échanger avec des startups passionnantes.

Bug Bounty : une mécanique bénéfique pour tous

La menace ne cessant jamais de progresser, la recherche de vulnérabilités pour prévenir des futures intrusions reste donc un point des plus sensibles. Le Bug Bounty permet aux entreprises d'organiser des '**chasses aux vulnérabilités'** de manière publique, privée (accessibles sur invitation) ou directement sur site lors d'évènements organisés. Ainsi, les chasseurs de vulnérabilités (hunters) vont chercher des vulnérabilités sur ce que l'entreprise met à leur disposition (site web, applications, …) et vont soumettre leurs découvertes afin de les faire valider et de leur faire attribuer un score. Le hunter se voit alors récompensé et l'entreprise peut désormais corriger la vulnérabilité.

La récompense peut être de l'argent, des goodies, des produits de la marque de l'entreprise mais aussi la progression dans un leaderboard ou l'apparition de son nom dans un **« Hall Of Fame »**. Via ce cercle vertueux qu'est le bug bounty, il est donc possible de faire du **« crowdsourcing de compétences »** et d'avoir des tests de sécurité encadrés en permanence.



CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Au coeur du Forum

Cybermalveillance.gouv.fr : un succès prometteur

Deux ans après sa création, **le dispositif national d'assistance aux victimes d'actes de cybermalveillance** a trouvé sa place dans l'écosystème français de la cybersécurité. Dylan Cordeiro, Laurent Marchaud et Alexandre Zhan reviennent sur ce succès qui commence à s'exporter.

PENSEZ-VOUS QUE L'EXISTENCE DE CETTE PLATEFORME SOIT BIEN CONNUE DU GRAND PUBLIC ?

Le dispositif lancé en octobre 2017 est récent et s'adresse à l'ensemble de la population française : citoyens, entreprises et collectivités en complément de l'ANSSI qui supporte les OIV et OSE. Dans un premier temps, nous avons choisi de nous faire connaître dans l'écosystème de la communauté cyber afin d'acquérir une certaine légitimité et pour que celle-ci devienne un relais de nos messages. Puis, grâce à diverses actions de communication nous nous faisons connaître d'un nombre toujours plus important de personnes.

QUELLE EST L'AUDIENCE DE VOTRE DISPOSITIF DEPUIS SA CRÉATION, ET QUELS SONT LES RETOURS DES UTILISATEURS ?

Le service d'aide aux victimes permet de distinguer les particuliers des entreprises et donc de connaitre le profil des personnes qui recherchent de l'assistance chez nous.

Aujourd'hui, nous assistons environ 85% de particuliers, 12% d'entreprises et 3% de collectivités. Nous voyons également une évolution du nombre d'entités que nous avons pu aider puisque nous sommes passés de 28 855 parcours victimes sur l'année 2018 à plus de 70 000 depuis le premier janvier 2019. Nous pouvons donc considérer que de plus de plus de nos concitoyens nous connaissent.

QUELS SONT VOS OBJECTIFS FUTURS ET LES ÉVOLUTIONS PROCHAINES APPORTÉES À LA PLATEFORME ?

Nous allons d'ici peu lancer la V2 du site. Nous discutons d'ailleurs sérieusement avec les représentants d'un autre pays pour pouvoir leur fournir notre plateforme, sur le modèle du logiciel libre, afin qu'il puisse reproduire le service. Si un jour, ils développent une fonctionnalité à laquelle nous n'avions pas pensé et qui est intéressante, nous pourrons peut-être l'implémenter de notre côté et améliorer ainsi notre site. Et si par la suite nous passons à deux, trois, quatre pays nous pourrons créer une vraie communauté. En parallèle, l'objectif final est bien évidemment que des citoyens et des PME nous connaissent. Nous souhaitons également élever le niveau de sécurité des prestataires. Aujourd'hui, nous avons 1600 prestataires qui sont en capacité d'aider les gens. Parallèlement les entreprises sont de plus en plus nombreuses à exiger certains niveaux de compétence en sécurité et en informatique de leurs prestataires. Nous sommes sur un label qui sera différent des PASSI PDRIS et PRIS de l'ANSSI. Il sera plus abordable et adapté à notre public et sera lancé dans le courant de l'année 2020.

THREAT INTELLIGENCE

Threat Intelligence

Face à l'augmentation des menaces, la complexification des attaques et aux impacts grandissants de la cyber malveillance, les matériels de sécurité nécessitent d'être constamment au fait du contexte dans lequel ils évoluent.

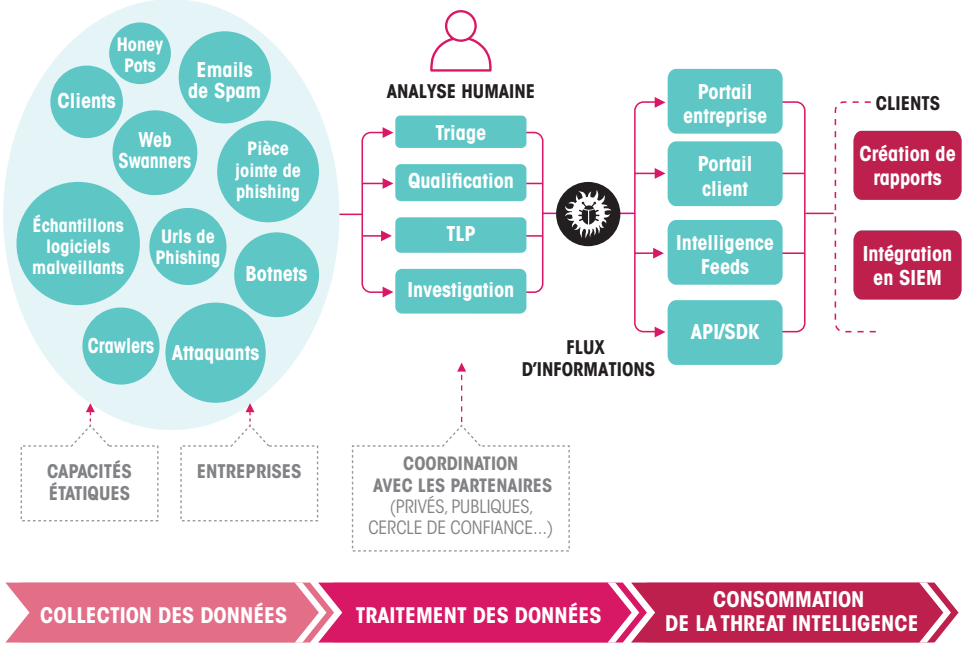
Le renseignement sur la cyber menace, ou threat intelligence, permet ainsi de disséminer de l'information à l'ensemble des éléments de la chaîne de défense afin de pouvoir détecter et traiter les menaces anciennes et nouvelles en fonction de leur comportement.

Pour faire prendre conscience du contexte de sécurité dans lequel évolue un équipement de sécurité, on utilise des ***IOCs*** (Indicators of Compromise) et des ***TTPs*** (Tactics, Techniques and Procedures). L'un permet de détecter, les IOCs mettant en exergue des menaces connues ; l'autre permet de caractériser, les TTPs décrivant la façon dont des acteurs malveillants orchestrent leurs attaques.

Les éléments disséminés peuvent être des informations purement techniques (à destination de proxy, SIEM, ...) mais peuvent être aussi de l'information plus contextuelle (géopolitique, économique, ...) à destination d'analystes traitant un incident de sécurité. Avec la threat intelligence il est possible d'apporter une vision de tout ce qui est connue afin de donner une capacité de décision beaucoup plus efficace.

Ainsi, par la création d'éléments de détection et de caractérisation et via leur dissémination aux équipements pouvant les accepter et aux bons acteurs, la threat intelligence devient un domaine inévitable de la lutte défensive et un enjeu majeur dans la sécurisation des systèmes d'information modernes.

Le monde de la threat intelligence et sa dynamique



Rencontre avec Cyrille Badeau,

VP Europe de ThreatQuotient

COMMENT DÉFINIR VOTRE SOLUTION THREATQ ?

ThreatQ est une solution logicielle qui a pour but d'opérationnaliser le renseignement dans une chaîne de défense cyber. Cette solution capte du renseignement extérieur et intérieur (souvent le plus important) et priorise, dans cet ensemble de renseignement, ce qui doit être diffusé (ou disséminé) à la chaîne de défense pour être consommé, que cette dernière soit représentée par des outils, par des analyses ou par des décideurs. Une plateforme de type ThreatQ c'est exactement l'équivalent d'un service de renseignement pour une défense nationale.

C'EST-À-DIRE ?

La plateforme ThreatQ reprend la notion de « fiche » (utilisée dans le monde du renseignement classique) pour interagir avec les différents organes en présélectionnant des marqueurs d'attaques potentiellement liés à des menaces d'intérêt et en les disséminant auprès du SIEM pour surveillance. A l'instant où l'un de ces marqueurs est détecté, il est remonté à la plateforme (ce qui s'appelle du SIGHTING) pour que son niveau de priorité soit modifié. Le renseignement sur une menace générique devient alors un renseignement contextuel à notre organisation (car il a été constaté par la surveillance) - il est devenu prioritaire.

QUELLES SONT LES TECHNOLOGIES UTILISÉES PAR THREATQ ? ON SUPPOSE MISP ?

On utilise bien évidemment MISP comme source de notre plateforme et comme outil de partage vers la communauté. Mais il y a deux mondes dans les acteurs du renseignement. Le premier, celui pour lequel ThreatQ est pensé, est le monde de l'opérationnalisation du renseignement. Nos clients sont des consommateurs de renseignement, qui ont besoin d'un practice qui permet de capter du renseignement, de le prioriser, de le croiser avec du renseignement interne et de le disséminer. Le deuxième monde est celui des créateurs de renseignement. C'est un métier rare et très différent.

QUEL EST LE NIVEAU DE MATURITÉ DE LA THREAT INTELLIGENCE DANS LES ENTREPRISES FRANÇAISES ?

Il y a une énorme progression ces dernières années notamment sous la pression des régulations. Cela a d'abord touché les organismes d'intérêt vitaux (OIV) car des méthodes de mise en œuvre de la détection et de la réponse leur sont imposées par des processus normés. On parle de certification par l'agence de type PDIS pour la détection et de type PRIS pour la réponse. Ces processus nécessitent de manipuler et de consommer du renseignement. C'est clairement suite à la LPM (2013) qu'il y a eu un vrai démarrage sur le sujet en France. Néanmoins la photo n'est pas totalement satisfaisante. En effet, un service de renseignement a pour but de disséminer de l'information à l'ensemble des éléments de la chaine de défense. *Malheureusement, trop souvent, nous sommes appelés pour démarrer un projet de Threat Intelligence au sein d'un SOC et seulement au sein d'un SOC. Pourtant, le CERT, le CSIRT, l'équipe de MCS, l'équipe de Patch Management, les SECOPS, l'équipe End Point, l'analyse de Risque… sont autant de départements qui pourraient énormément bénéficier du renseignement et venir l'alimenter si celui-ci était pensé pour servir l'ensemble de la chaine*

Atelier
Kaspersky

À la poursuite du « billion dollars hacking group »

En 2018, la justice américaine annonce l'arrestation de plusieurs membres de FIN7 appelé également «The billion dollars hacking group».

Ces attaquants connus également sous le nom de Carbanak était un groupe organisé visant les banques, les suites d'hôtels ou les chaînes de restaurants depuis 2015. À la suite de cette arrestation, la communauté a pensé à tort que les campagnes d'attaques s'étaient arrêtées.

En 2018-2019, plusieurs alertes analysées par Kaspersky possédaient les mêmes TTPS que FIN7, ce qui les pousse à croire que le groupe aurait en fait survécu aux arrestations de 2018.

Le mode opératoire de FIN7 consiste en plusieurs étapes :

> Reconnaissance de la cible avec du spearphishing remarquablement sophistiqué. L'instauration de véritables conversations, via de nombreux emails, jouant parfois avec les émotions des victimes (peur, stress, anxiété), et un envoi des pièces jointes malveillantes au bon moment permet une efficacité redoutable.

> Deux types de documents peuvent être envoyés à la victime. Le premier est un document Word exploitant la fonctionnalité includePicture pour obtenir des informations sur l'ordinateur de la victime.

Le second est un document Word utilisant les macros afin d'exécuter un implant Griffon permettant de faire de la reconnaissance et de la cartographie des postes de travail.

Par la suite, l'implant télécharge plusieurs modules :

> Un module de reconnaissance

> Un téléchargeur de meterpreter : Tinymet

> Un module de capture d'écran

> Un système de persistance

Ensuite, l'attaquant essaye de se latéraliser dans le réseau afin de trouver les ressources critiques et les exfiltrer pour en faire de la revente et du blanchiment.

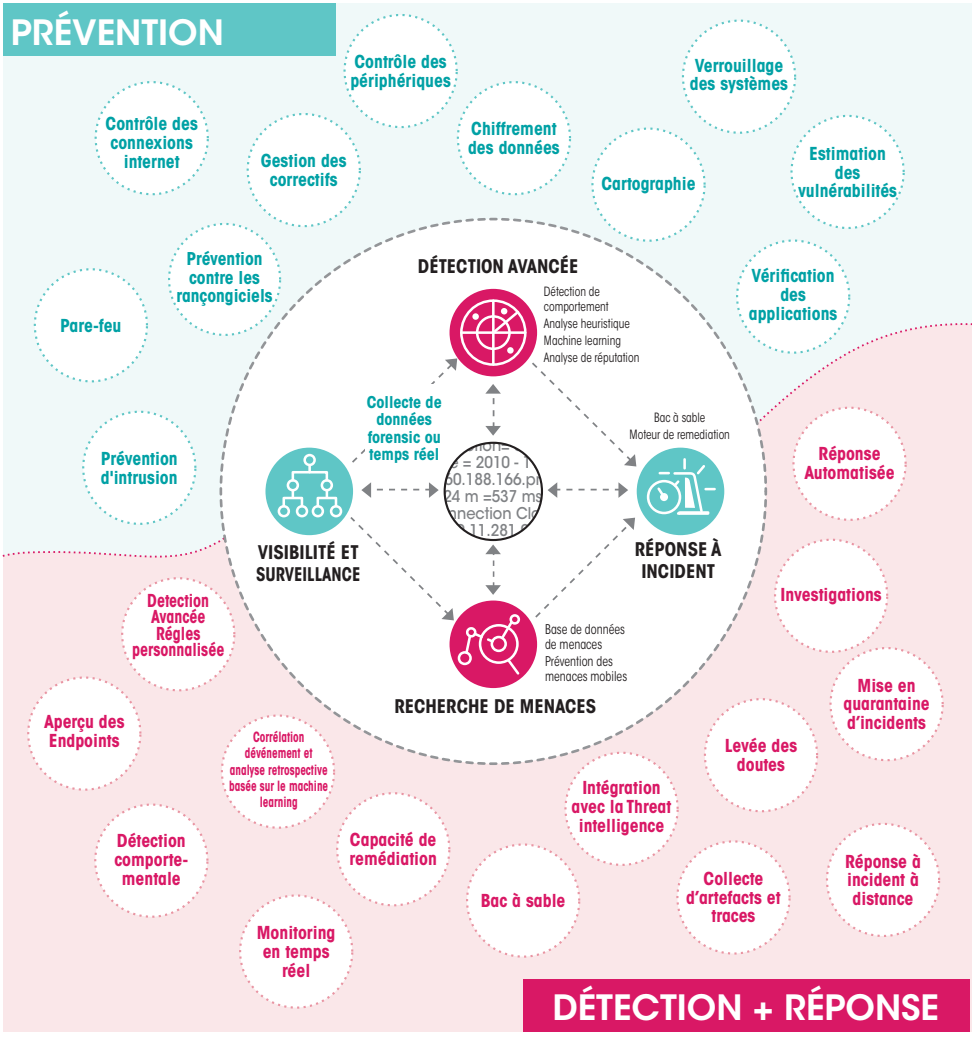
Le but principal de FIN7 est de voler les éléments financiers de l'entreprise (les cartes de crédit ou données financières).

FIN7 a fait une erreur qui a permis à Kaspersky de remonter une piste. Afin de tromper les analystes FIN7 a créé une fausse redirection HTTP 302 vers divers services Google sur leurs serveurs C2s (Command and Control).

Cette erreur a permis de trouver un site étranger d'une fausse entreprise de sécurité. Cette société semble avoir servi à FIN7 pour recruter et employer différents professionnels tels que des développeurs, des pentesters ou des traducteurs, ceux-ci croyant la société légitime.

DÉTECTION & RÉPONSE À INCIDENT

Les EDR, des outils puissants en pleine expansion



« Le temps moyen entre l'entrée et la détection est de plusieurs mois, mais nous avons vu des cas où cela remontait à 3 ans. »

La clef de voûte de la lutte informatique défensive repose sur la détection des incidents de sécurité. Celle-ci est en effet un point crucial puisqu'elle va déterminer la gravité d'impact d'une attaque dans le système d'information. Effectivement, plus le temps de détection sera long, plus un attaquant aura la possibilité de s'installer dans le système d'information cible. La détection est donc un enjeu majeur à ne pas négliger, même si trop souvent il s'agit d'un maillon sous-estimé dans la sécurité des entreprises. La durée moyenne de détection d'activités malveillantes est de 101 jours. La détection se fait notamment au travers d'un SOC (Security Operations Center) ou Centre Opérationnel de Sécurité, qui va regrouper de multiples outils contribuant à la détection.

Lorsqu'un incident de sécurité est détecté, le SOC relaye cet incident aux équipes en charge de la réponse à incidents, qui constituent un CSIRT (Computer Emergency Security Incident Response Team). Dans ce cas-là, le plan de réponse aux incidents, préparé en amont, est mis à exécution.

Néanmoins, comme le dit Cyril Voisin, Chief Security Advisor, Microsoft EMEA, « Aujourd'hui, avec des attaques gérées par des IA, le temps de réaction des humains est cent fois trop court. Un des moyens de le contrer est de l'aborder par une réponse automatisée à la détection d'une intrusion. Cela consiste à appliquer une forme de "playbook" pour investiguer (activités d'une IP, du compte compromis, de d'autres points de latéralisation possibles...). *Cependant, peu de gens vont plus loin en automatisant complètement la réponse, en bloquant des comptes ou en isolant des postes et la remédiation ».*

Atelier Carbon Black

Spécialiste de l'EDR, Carbon Black a présenté lors des Assises, l'activité de sa « Threat Analysis Unit ». Celle-ci a trois missions :

- **comprendre une attaque et la cible de celle-ci ;**
- **détecter et prévenir l'attaque ;**
- **développer des nouvelles techniques de détection.**

« De plus en plus, nous remarquons l'utilisation par les attaquants des LOLBins, soit les binaires "living off the land". Ces derniers sont des fichiers certifiés et signés, présents sur les systèmes d'exploitation par défaut **»** explique Andrew Costis Threat Researcher chez Carbon Black. L'avantage de l'utilisation des LOLBins pour les acteurs malveillants étant que cela génère peu d'IOCs. De plus, les LOLBins sont présents partout et en grand nombre sur les systèmes. Ils sont de plus en plus utilisés et sont un gain de temps considérable pour des attaquants.

Les attaquants exploitent donc les outils et utilitaires natifs et légitimes déjà présents sur le système. Cela leur permet de ne pas être détectés et d'être attractifs pour des APTs. Et même de cacher du code malveillant. Ainsi, différents cas ont été recensés, dont l'utilisation de RegAsm.exe, une calculatrice sur téléphone mobile. Les attaquants sont parvenus à remplacer le contenu de RegASM.exe par celui de l'exécutable malveillant porté par le malware.

Malheureusement, il est difficile de durcir les systèmes pour empêcher ce type d'attaque, ces outils étant nécessaires, pour la plupart, au bon fonctionnement du système d'exploitation (ex: Powershell). Le moindre mal, si on ne peut pas les supprimer est donc de les monitorer.

Rencontre avec David Grout,

CTO et Directeur technique pour l'Europe du Sud de Fireeye

QUELQUES MOTS SUR LES ACTIVITÉS DE FIREEYE ?

Nous avons trois grandes activités. La première est purement technologique. Nous vendons des technologies de protection, d'investigation et de forensics. La deuxième se manifeste à travers la marque Mandiant, des services de réponse à incident. Nous intervenons uniquement pour des attaques de haut niveau technique de type APT par exemple et très peu sur le commodity malware. La troisième activité est basée sur le renseignement avec environ 150 analystes répartis dans 30 pays et 18 langues couvertes en natif.

LES ENTREPRISES COMMENCENT-ELLES AUSSI À SE DOTER D'UN SERVICE DE THREAT INTELLIGENCE ?

Jusqu'en 2016/2017, à part dans les secteurs financiers et gouvernementaux, le niveau de maturité des entreprises en termes de cybersécurité était bas. Très peu de clients avaient des SOCs. Le changement radical est venu avec NotPetya. Le fait que cette attaque ait coûté énormément aux entreprises touchées à créer un besoin de sécurité et des budgets ont été alloués pour cet unique objectif. Dans le cas de la threat intelligence, cela nécessite des équipes d'experts que possèdent peu d'entreprises. Parmi les entreprises du SBF120, seules un tiers d'entre elles environ sont capables de faire de la threat intelligence de manière efficace et mature. Certaines essayent ce service mais ne se rendent pas compte qu'elles ne sont pas prêtes à cela. La structure organisationnelle à mettre en place est également très importante au-delà du service en lui-même

QUELLE EST VOTRE UTILISATION DE L'IA ?

Nous utilisons principalement le machine learning. D'abord en interne. Nous récupérons de la data en télémétrie qui va vers un datalake (VirusTotal par exemple). Nous créons des moteurs de machine learning à partir de ces données. Nous nous en servons pour faire de la clusterisation de campagne. En externe, nous implémentons des algorithmes de machine learning pour des tâches particulières et bien définies notamment dans la protection. La question à se poser avec le machine learning est celle de sa valeur ajoutée et l'endroit où cela est utile

QUELS SONT LES CHALLENGES AUXQUELS FIREEYE DOIT FAIRE FACE AUJOURD'HUI ?

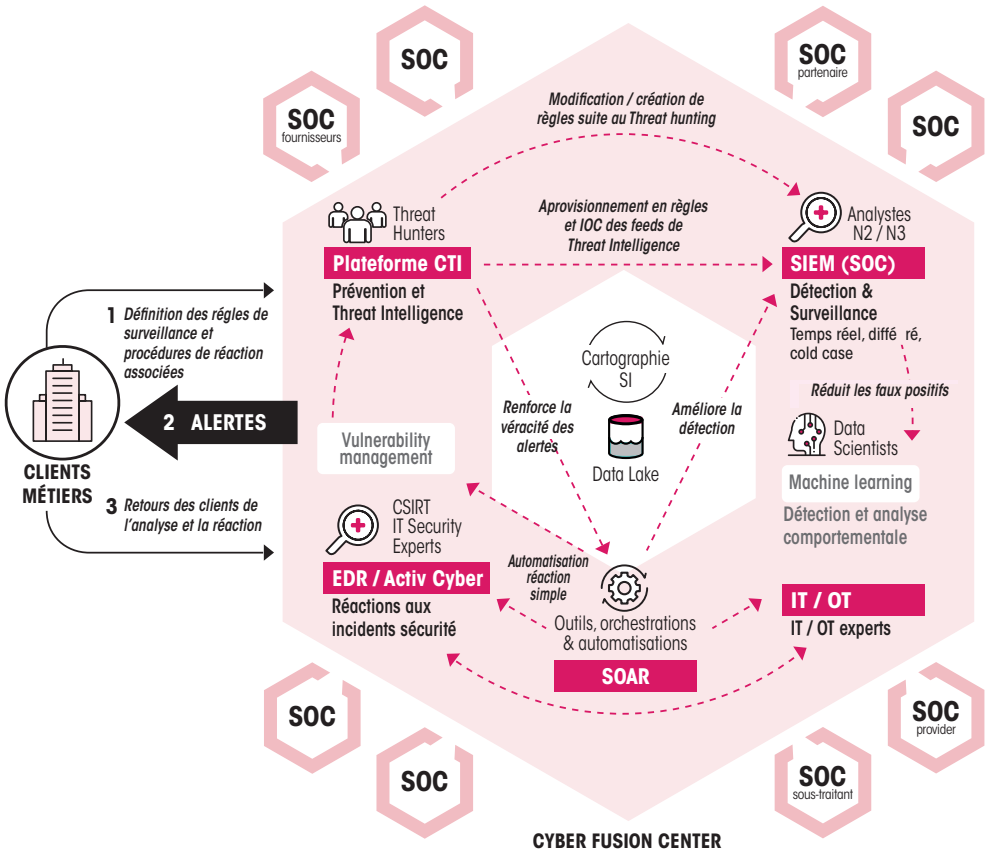
Les grands challenges sont les nouveaux supports (cloud et conteneur). Comment assurer la sécurité ou l'investigation dans un environnement conteneurisé ? Comment appliquer nos méthodes et notre technologie sur ces nouveaux environnements ? Il y a aussi un problème de visibilité dans le cloud, notamment pour les logs. C'est un défi majeur également pour les mois et années à venir.

ACTUELLEMENT, QUELLES SONT LES PLUS GRANDES MENACES CYBER?

La grande peur des entreprises, ce qui leur importe par-dessus tout est de perdre du business. Les points d'entrées les plus courants sont le **phishing, la fraude au président et le webshell**. Ce dont on parle moins souvent, ce sont **les insiders** (personnes licenciées, personnes mécontentes, espionnage…). Mais pour moi, les menaces les plus grandes sont **les impacts géopolitiques et géostratégiques** au niveau cyber.

TENDANCES TECHNOLOGIQUES

Évolution des SOC, vers un «fusion center» ?



« Aujourd'hui, dans les produits de protection, le **Machine Learning** capte environ 60-70% des malwares.»

Machine Learning, Zero trust, EDR, multi-cloud, IoT, 5G, souveraineté des données, et bien d'autres termes étaient parmi les grandes préoccupations des acteurs de la cybersécurité durant cette année 2019. Et certains forgent les tendances d'aujourd'hui et surtout de demain.

Ainsi, **le Machine Learning** est devenu un incontournable de la cybersécurité innovante. Utilisé, entre autres, pour l'analyse comportementale, le Machine Learning permet aux équipes du SOC de faire baisser la charge de travail mais aussi de détecter des signaux faibles de manière automatique et sans assistance humaine. C'est sur ce principe que des sociétés comme Darktrace mais aussi Symantec, Kaspersky et bien d'autres, développent certains de leurs systèmes de détection. Dans le cas de Symantec, l'application du Machine Learning leur a permis de développer un BOT analyste dans un SOC, soit un analyste de premier niveau non-humain.

Le concept du **Fusion Center** vient apporter une part de la solution à ces problématiques. Le Fusion Center propose en effet la fusion du SOC et du CSIRT dans le but de couvrir la détection, la réponse, le threat hunting et l'intelligence sur les menaces tout en réduisant la charge de travail des équipes sécurité. Au coeur de ce concept, les SOAR (Security Ochestration Automation and Response) commencent à prendre une place prépondérante dans la vie du SOC et du CSIRT. On y retrouve ces outils d'automatisation et d'orchestration, couplés au Machine Learning et à la threat intelligence, qui apportent un soutien plus que nécessaire face aux menaces actuelles et futures.

Le zero-trust fait également partie de ces grandes tendances souvent abordées lors des Assises 2019. Laurent Heslault, Directeur des stratégies de sécurité, Symantec EMEA en explique la raison : « De plus en plus de personnes se tournent vers le « zero-trust » qui est une philosophie, plus qu'une technique. Avec « Zero-trust », tout est considéré comme hostile. Il n'y a plus vraiment d'intérieur et d'extérieur. **On inverse le paradigme « je me connecte et je me logue », en « je me logue, et on me connecte »**. Tout se passe sur la couche 7 (couche application) du modèle OSI, ce qui est très intéressant d'un point de vue sécurité. » L'approche zero-trust se positionne comme le successeur du modèle château fort, aujourd'hui caduque face à des problématiques comme le BYOD (Bring your Own Device).

Atelier
Airbus

La sécurisation de l'IoT industriel

La sécurisation de l'IoT industriel devient un réel enjeu de sécurité pour les entreprises concernées. Ces technologies sont intimement liées au système d'information et leur présence dans le secteur sera conséquente dans un futur proche.

Cette omniprésence de l'IOT en entreprise engendre une augmentation de la surface d'attaques, donc un risque sécuritaire accru. Ils peuvent être eux-mêmes une cible comme en 2017, lorsqu'un attaquant a visé les sirènes d'alarme de la ville de Dallas qui ont sonné pendant une heure. Ils peuvent également servir de vecteur d'attaque à l'instar de l'extorsion des données d'un casino à travers un thermomètre connecté. Enfin les IOTs peuvent être considérés comme armes ainsi que l'a démontré le botnet MIRAI.

Il est alors nécessaire de faire une sécurisation de la chaîne d'information de bout en bout. Cette sécurisation, via du chiffrement de type AES, peut se faire au niveau des capteurs grâce à la construction de signatures basées sur des variables d'environnements. Une application de gestion des objets permet par la suite de déchiffrer les données.

Les avantages de cette solution sont :

- une réduction des coûts grâce à l'utilisation d'un réseau lpwan et non un réseau IOT privé;
- l'amélioration du tracking;
- la possibilité de proposer un large catalogue d'appareils.

Cependant, cette solution doit encore se soumettre à des tests d'intrusions à la fin du POC. De plus, une réduction de la durée de vie des batteries des IOT a été observée lors de l'utilisation de cette solution.

5G : une technologie qui fait débat

La 5G a animé toute l'année 2019. Entre débats publics, technologiques et politiques, elle cristallise l'espace des télécommunications. Retour sur cette révolution annoncée dont les problématiques ont été abordées lors d'une table-ronde des Assises 2019.

ÉVOLUTION OU RÉVOLUTION

La **5G** est incontestablement une révolution et même plusieurs révolutions en une. Révolution technique avant tout car à partir de maintenant, le débit va être accru grâce aux ondes millimétriques et il va être possible d'émettre et de recevoir très rapidement des données sur les antennes grâce à des canaux full-duplex et de manière plus perfectionnée qu'avec la 4G. À titre d'exemple, la géolocalisation devient donc de l'ultra-géolocalisaton. C'est aussi une révolution d'usage, la 5G s'adressant d'abord au monde du business plutôt qu'à celui des particuliers. Avec des conséquences dans la façon dont sont déployés le cloud et les réseaux locaux en entreprise. Par ailleurs, la 5G est également une rupture pour les services de sécurité, en matière d'interception, d'écoute et de localisation.

FEUILLETON DE L'ANNÉE

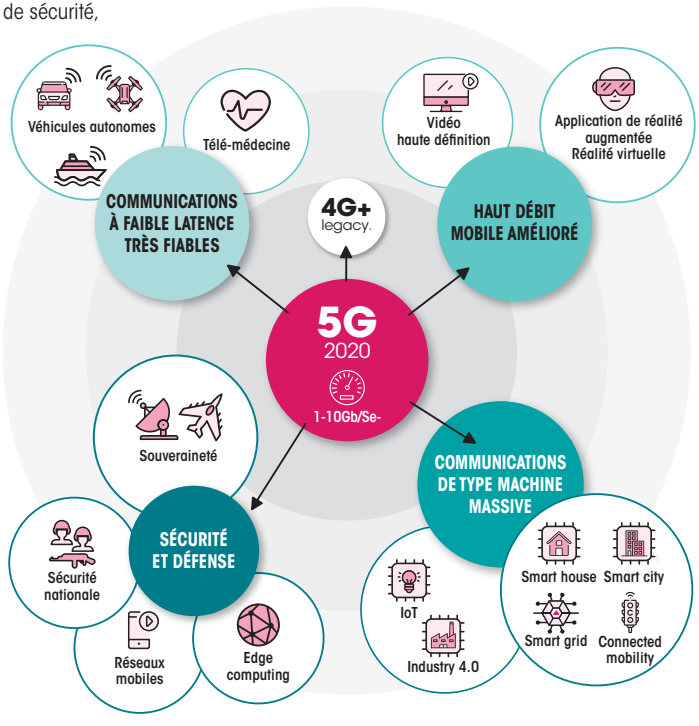
Si la 5G a fait autant parler d'elle cette année, c'est aussi parce qu'elle est un sujet géopolitique majeur opposant notamment l'administration du président américain Donald Trump et la Chine via l'entreprise Huawei. L'escalade qui a eu lieu durant tout le printemps, amenant à des sanctions des États-Unis sur Huawei, est le cœur d'une guerre commerciale sur la technologie de la 5G. La montée en puissance de l'entreprise chinoise dans le monde des télécoms (smartphone, câbles sous-marins, serveurs, cœurs de réseau, etc.) inquiète sur de potentiels risques de prééminence technologique. En effet, le développement de la 5G fait partie intégrante du plan d'investissement « Made in China 2025 » promu par le président Xi Jinping, et le continent européen ne devrait pas être épargné par cette compétition entre les deux superpuissances.

QUE SIGNIFIE LA 5G EN TERMES DE CYBERSÉCURITÉ ?

Pour le RSSI d'une entreprise, la 5G va impliquer des modifications, ouvrant encore plus les systèmes d'information, jusqu'au edge computing. Les migrations vers le cloud s'accélérant significativement, une multitude de nouveaux actifs à gérer va apparaître tandis que progressivement les réseaux distants et locaux vont se transformer en réseaux 5G. La 5G pose aussi de nouveaux défis en termes de sécurisation et de souveraineté notamment pour les Opérateurs d'Importance Vitale (OIV) et les Opérateurs de Service Essentiel (OSE) qui vont devoir s'interroger sur la provenance des équipements et sur leur utilisation dans la protection de leur patrimoine informationnel.

LE FUTUR DE LA 5G : LA 6G

La 5G est encore à peine déployée que l'on parle déjà de sa future évolution : la 6G. Les comités de spécification ont commencé à travailler dessus : là où pour la 5G il y aura du Gb/s en termes de débit, la 6G devrait se décliner en Tb/s. *Si la 5G annonce la fin des réseaux locaux, la 6G promet la suppression complète de tous réseaux d'entreprises au profit de réseaux entièrement managés. La révolution est loin d'être terminée…*



Le mot de la fin…

Sébastien Bombal, *Conseiller ComCyber, Ministère des Armées*

2019 reste dans la continuité d'une numérisation croissante et exponentielle qui transforme en profondeur notre Société. Si elle est source d'opportunité, les attaques et les risques se multiplient et se complexifient avec une tendance sans fin.

Cette année a démontré une nouvelle fois, le panel de risques à prendre en compte depuis la géopolitique du domaine et son impact sur l'économie et le questionnement sur l'ambition en matière de souveraineté, en passant par les risques de manipulation de l'information et les cyberattaques toujours plus ciblées. Ces dernières mettent même à l'épreuve la résilience des victimes, parfois définitivement. La cybercriminalité n'est pas en reste, et l'explosion du phénomène « rançongiciels » en est l'illustration. Elle se confond de plus en plus avec les cyberattaques étatiques.

Les tendances présentées dans ce livret, et recueillies par les étudiants d'EPITA, montrent à quel point à la cybersécurité de bout en bout reste aussi un challenge, même avec une approche « zero trust ». Les attaques indirectes, ciblant un élément de l'écosystème d'une victime, pour l'atteindre ensuite, sont une réalité qu'on ne peut plus ignorer. La sécurisation de l'écosystème, de l'administration ou de l'entreprise étendue, parfois appelée « supply chain », illustre le besoin permanent de penser et d'agir, comme la nature du système à défendre, en réseau.

Il n'y a pas de cybersécurité sans partenariats et échanges avec toutes les parties prenantes. Cette édition des Assises a été encore une fois, un de ces moment-clé d'échange et de convivialité, riche en partage d'expériences.

Je tiens à remercier toute l'équipe des assises, et particulièrement Florence Puybareau, ainsi que les étudiants de l'EPITA, qui ont permis la réalisation de cette nouvelle édition du livret.

Remerciements

Ce livre blanc a été conçu avec la promotion 2020 Systèmes, Réseaux et Sécurité de l'EPITA sous la direction de Sébastien Bombal (Nicolas Balagny-Carbuccia, Hicham Benrabia, Valentine Bernard, Florian Chatelus, Dylan Cordeiro, Tancrede Erulin, Adrien Goetz, Victoria Guehennec, Navid Hamidi Vadagani, Laura Hanot, Laurent Marchaud, Trung Nguyen, Alexis Pain, Antoine Pierdet, Lucas Rangeard, Nicolas Ribeyrolle, Tristan Ruter Naon, Antoine Suel, David Terrine, Vincent Trinh, Marko Vicentijevic, Alexandre Zhan).

Avec une mention spéciale pour Doette Bleton, Arthur Vuagniaux et Mathieu Ghirlanda. Nous remercions les intervenants qui ont contribué à l'enrichissement de ce livre blanc : Gérard Leymarie, Samuel Hassine, Loïs Samain, Cyrille Badeau, Cyril Voisin , Luc Delsalle, David Grout, Laurent Heslault, Dylan Cordeiro, Laurent Marchaud Alexandre Zhan , Nicolas Massaviol.

LES ASSISES

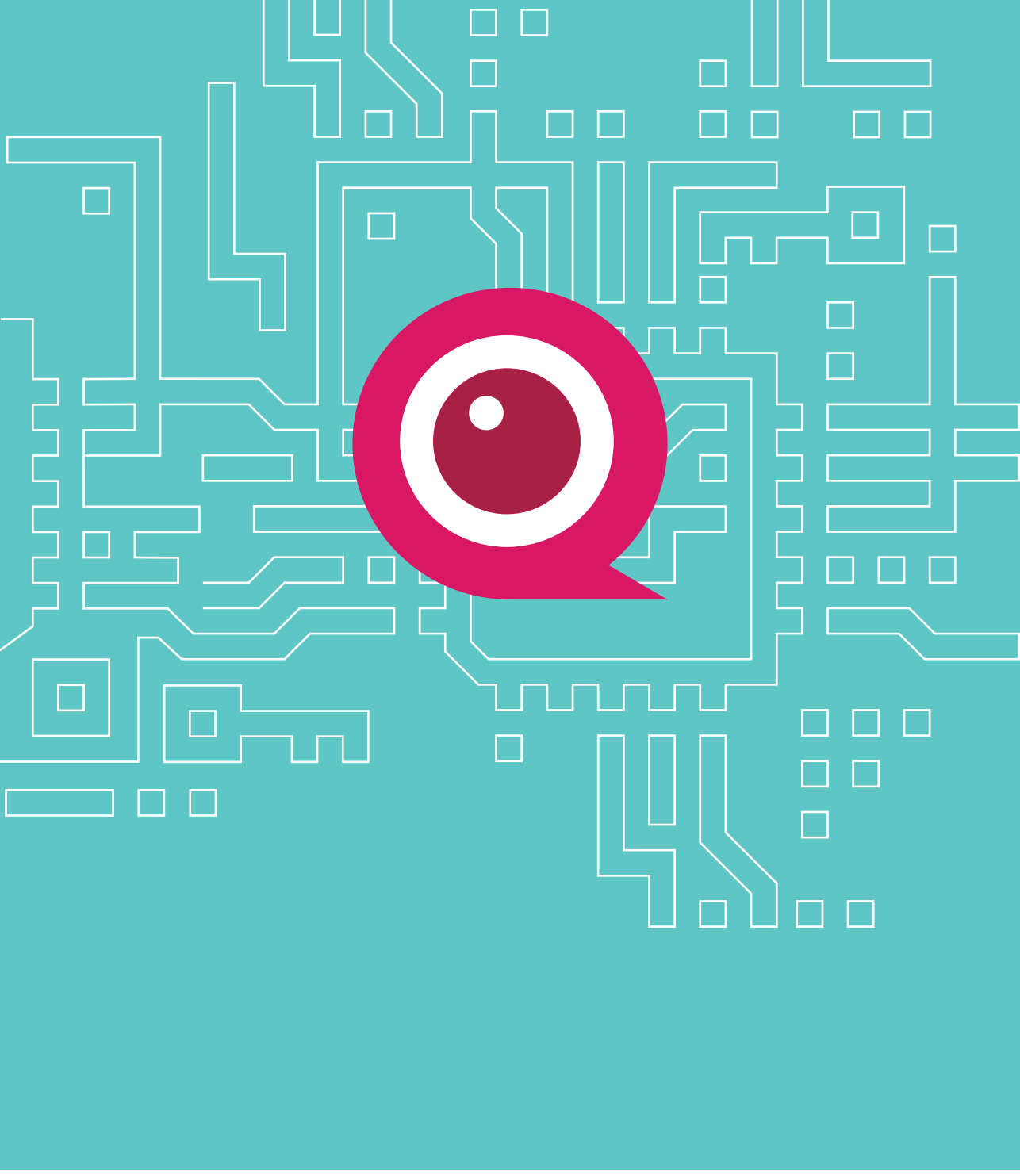
14.10.20 → → 17.10.20

/MONACO ///

→ lesassisesdelacybersecurite.com

DG CONSULTANTS

COMEXPOSIUM



DG CONSULTANTS @Les_Assises @Les_Assises #AssisesSI COMEXPOSIUM

www.lesassisesdelasecurite.com