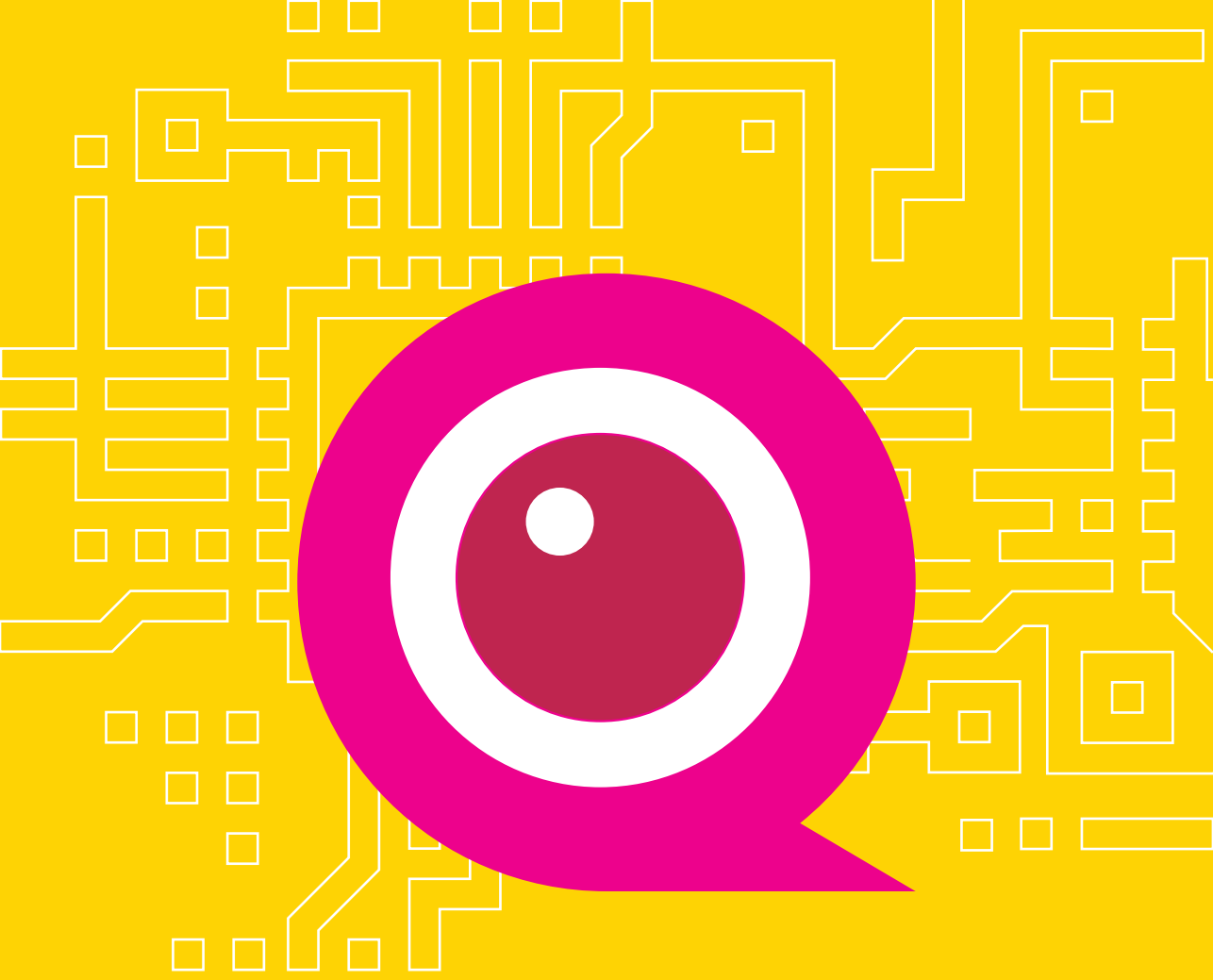


CYBERSÉCURITÉ &INNOVATIONS

EDITION 2018

Le regard des Assises et de l'EPITA

lesassises de la sécurité et des systèmes d'information

EPITA ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

UN PARTENARIAT SOUS LE SIGNE DE L'EXCELLENCE

Evénement business devenu la référence dans le domaine de la cybersécurité, **les Assises de la Sécurité se veulent aussi le reflet de l'innovation d'un secteur en constante évolution.** Depuis longtemps, nous souhaitions mettre davantage en valeur toute cette richesse portée par nos partenaires et par nos visiteurs. D'autant que d'année en année, la qualité des contenus proposés aux Assises n'a cessé de croître. C'est pourquoi, nous avons décidé de nouer **un partenariat avec l'EPITA, l'école des ingénieurs en intelligence informatique, et plus particulièrement sa Majeure SRS (Système, Réseau et Sécurité) qui forme les futurs professionnels de la cybersécurité.** Placé sous le signe de l'excellence, ce partenariat a pour objectif de réaliser un ouvrage mettant en avant les solutions technologiques vues par les étudiants d'aujourd'hui mais qui demain auront peut-être l'opportunité de venir aux Assises en tant que RSSI ou partenaire.

Ce livret couvre une partie de l'innovation et des solutions présentées aux Assises, et ne se veut pas exhaustif. L'offre est si riche, le champ qu'embrasse la cyber devient tellement vaste qu'il a fallu faire des choix, en coordination avec les enseignants de l'EPITA. C'est ce travail, que nous avons le plaisir de vous présenter.
Ne doutons pas qu'il est le premier d'une longue série.

Florence Puybareau

Directrice de la Communication et des Contenus, DG Consultants

UN PARTENARIAT UNIQUE POUR UNE VISION DE PROSPECTIVE

L'école d'ingénieur EPITA a toujours participé aux Assises, en particulier à travers ses nombreux anciens. C'est avec une grande fierté cette année que l'école contribue directement à ce rendez-vous incontournable de la cybersécurité en France.
Grâce à nos futurs ingénieurs, en dernière année dans la majeure Système, Réseau et Sécurité, et à travers un partenariat exceptionnel avec l'organisation des Assises, nous avons l'honneur et le plaisir de vous présenter cet ouvrage visant à éclairer de manière synthétique quelques tendances et innovations, agrémentées d'interviews prises par nos étudiants pendant les Assises.
Nous tenons à remercier tous les partenaires et les participants des Assises qui ont partagé avec nos étudiants leurs conseils et expériences, ou qui ont tout simplement donné un peu de leur temps. L'une des forces des Assises est cet espace unique d'échange et nous espérons que ces quelques pages produites par ces yeux neufs, y contribueront.

Nos futurs ingénieurs du numérique auront le difficile devoir de l'innovation permanente et le fantastique pouvoir d'imaginer une société nouvelle et meilleure, dans un contexte géopolitique complexe, au sein d'économies imprédictibles et face à l'émergence de nouvelles menaces.

Ce fût une formidable opportunité et un excellent défi que l'école saura relever à nouveau avec la prochaine génération.

Joël Courtois
Directeur de l'EPITA

CHIFFRES CLÉS DES ASSISES 2018

2 900
PARTICIPANTS

6 880
RENDEZ-VOUS ONE TO ONE

165
ATELIERS ET CONFÉRENCES

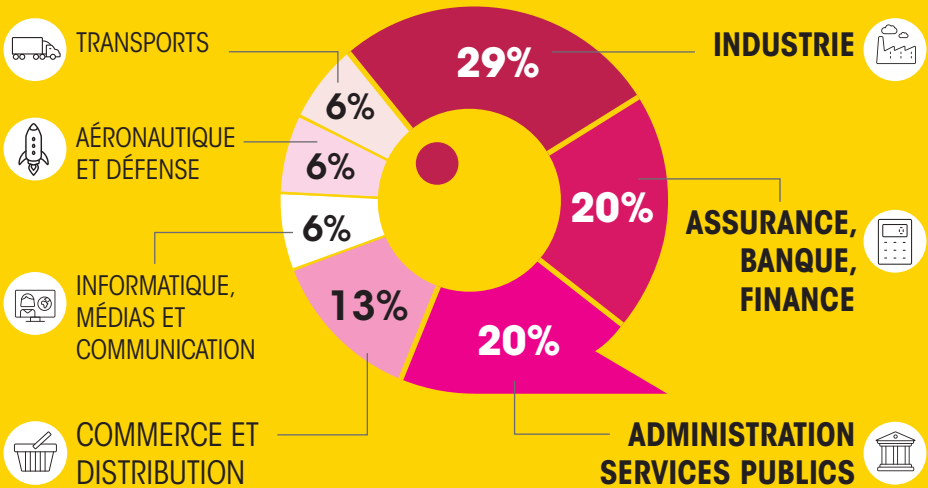
1 310 **RSSI et DSI** REPRÉSENTANT 686 SOCIÉTÉS

38% **DE NOUVEAUX INVITÉS**

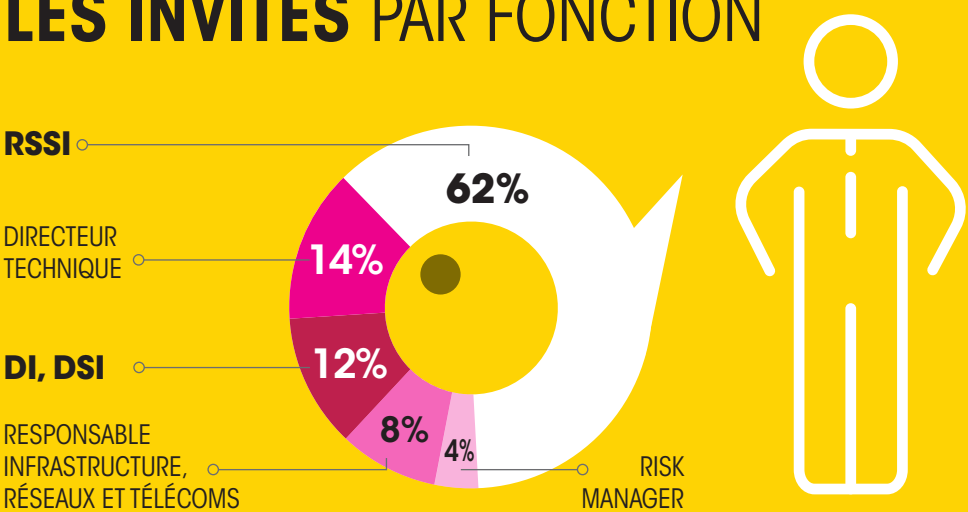
160 **PARTENAIRES**

50 **JOURNALISTES & BLOGUEURS**

LES INVITÉS PAR SECTEUR



LES INVITÉS PAR FONCTION



Emmanuel Germain, *Directeur général adjoint de l'ANSSI*

En travaillant aujourd'hui dans la cybersécurité, on peut avoir un rôle de pionnier

EN CYBERSÉCURITÉ, POURQUOI EST-IL IMPORTANT D'INNOVER ?

Innover en cybersécurité signifie s'adapter car tout change très rapidement. L'innovation revêt différents moyens, différentes méthodes comme la simulation des modèles numériques. A ce titre, l'exemple de Singapour qui crée une smart city est très intéressant car dans ce type de projet, il est nécessaire d'être « Secure by Design », c'est-à-dire penser et implémenter des dispositifs de sécurité d'une solution dès le début de sa conception. Demain, il n'y aura plus d'objets numériques sans sécurité.

COMMENT FAIRE POUR POUVOIR AFFRONTER LES ATTAQUANTS ?

Tout d'abord, il est primordial de prendre conscience des enjeux. Les attaques du printemps 2017, Wannacry en mai et NotPetya en juin, nous ont appris que nous sommes tous des cibles potentielles. Pour y remédier, les dirigeants doivent s'emparer du sujet et intégrer le risque cyber au même titre que les autres risques identifiés par les organisations. Dans un premier temps, un état des lieux de ses systèmes d'information doit être réalisé, pour pouvoir ensuite mettre en œuvre des actions concrètes et développer sa résilience. L'entraînement à la gestion de crise cyber, la formation et la sensibilisation des collaborateurs sont également des leviers déterminants. Concernant l'Etat et les Opérateurs d'importance Vitale (OIV), la protection face aux attaquants passe également par la réglementation.

QUEL EST LE RÔLE DE L'ANSSI EN TERMES D'INNOVATION ?

Il est multiple. Nous possédons 7 laboratoires de recherche (défense des réseaux, cryptographie, ...) avec des chercheurs dont certains sont reconnus pour leur compétence au niveau international. Ils interviennent régulièrement dans des conférences scientifiques pour présenter leurs travaux. Quelques-uns travaillent par exemple sur le chiffrement post-quantique. Nous sommes aussi présents dans divers groupes de travail pour avancer en matière d'innovation dans de multiples secteurs.

QUELLES SONT LES RAISONS POUR ALLER TRAVAILLER DANS LE SECTEUR DE LA CYBERSÉCURITÉ ?

La première motivation ? Il n'y a pas de chômage, c'est un secteur en pleine croissance ! Mais surtout il y a presque tout à faire. Le cyberespace est pour l'instant loin d'être entièrement sécurisé. Dans ce domaine on peut réellement avoir un rôle pionnier.

POURQUOI AVEZ-VOUS SOUHAITÉ INTÉGRER L'ANSSI ?

Je suis à l'ANSSI depuis 2 ans et auparavant, j'ai travaillé dans l'armée. En venant, à l'ANSSI, j'ai été intéressé par la dimension opérationnelle du poste. Aujourd'hui, j'apprécie particulièrement de pouvoir contribuer, avec des équipes exceptionnelles, aux progrès et à l'innovation réalisés par l'Agence.

Conférence d'ouverture,
Guillaume Poupard

Anticipons
pour ne plus subir

Lors de la conférence d'ouverture des Assises, Guillaume Poupard, le Directeur général de l'ANSSI a mis l'accent sur la nécessité pour les entreprises de savoir se défendre face à des attaques de plus en plus sophistiquées. Pour se faire, il préconise d'axer les efforts sur l'anticipation et la détection.

L'anticipation est particulièrement difficile à mettre en place car elle demande un effort collectif: il faut sensibiliser voire former la quasi-totalité de l'entreprise, de la direction aux différents métiers, sans oublier les prestataires qui sont parfois ciblés pour pouvoir toucher leurs clients. Afin d'accompagner cette démarche, l'ANSSI a annoncé la publication avec le soutien du club EBIOS, de la méthode EBIOS RISK MANAGER, une méthode d'analyse et de gestion des risques standardisée mettant en exergue les risques cyber encourus. L'ANSSI a aussi créé un référentiel (PAMS) afin de garantir un certain niveau de sécurité pour les prestataires. La réponse de l'ANSSI au problème d'anticipation collective est donc d'instaurer des systèmes de qualification avec différents niveaux de sécurité afin de créer un ensemble d'acteurs de confiance formés aux bonnes pratiques de sécurité et capables de réagir rapidement.

L'anticipation vise à renforcer l'efficacité et la réactivité de la détection. C'est pourquoi l'ANSSI en complément de la qualification des prestataires de détection d'incidents de sécurité (PDIS), souhaite développer et qualifier deux sondes afin de mieux détecter des attaques de plus en plus discrètes avec les industriels Gatewatcher et Thalès.

Pour conclure, la sécurisation du monde numérique doit passer par une chaîne de confiance. Celle-ci doit inclure chaque acteur, à tous les niveaux, même à l'international. Ce n'est pas encore le cas, mais la mise en place du Cybersecurity Act ayant pour but de développer un système collectif de protection dans l'ensemble de l'Union Européenne, représente déjà une avancée. L'ANSSI continue dans ce sens en s'impliquant dans l'open source et en apportant des solutions même aux petites entreprises.

Keynote par Mikko Hypponen,
Chief Research Officer de F-Secure

Du cyber-sabotage à la cyber-guerre

Stuxnet, ce malware qui a visé des centrales iraniennes d'enrichissement d'uranium en 2010 a marqué un tournant dans l'histoire de la cybersécurité. Pour Mikko Hypponen, directeur de la recherche chez F-Secure, on peut en effet parler d'un avant et d'un après Stuxnet qu'il qualifie de « première arme numérique largement médiatisée ». Cet acte de sabotage a mis en lumière certaines caractéristiques des armes cyber : elles sont effectives, peu coûteuses et il est difficile d'en découvrir l'origine. Mais s'il apparaît que Stuxnet avait une cible précise et a bénéficié du soutien de certains états, il ne peut être considéré comme un acte de cyber-guerre. A la différence de NotPetya qui s'inscrit dans le conflit entre la Russie et l'Ukraine avant de se propager au reste du monde. Selon Mikko Hypponen, le fait que des entreprises internationales aient été touchées par ce genre d'attaque dont elles n'étaient pas la cible peut être considéré comme un dommage collatéral, mais aussi comme la volonté de faire passer un message. Dans ce contexte, les pratiques de défense doivent s'adapter aux évolutions de la menace. Ainsi, à la sécurité périmétrique doit s'ajouter la capacité de détection et de réaction, car dorénavant, il faut admettre la vulnérabilité du système informatique.

Mikko Hypponen a également abordé la problématique des objets connectés, toujours plus intelligents mais aussi toujours plus vulnérables du fait de leur connexion internet et de leur architecture similaire à un ordinateur. Ce qui l'amène à conclure que tout système, aussi sécurisé soit-il, sera vulnérable tant que le maillon le plus faible de la chaîne, l'humain, ne sera pas renforcé.

Keynote par Marc van Zadelhoff,
General Manager IBM Security

3 axes
majeurs pour la cybersécurité : intelligence, rapidité et partage de connaissance

L'évolution de la cybermenace oblige les entreprises à s'adapter. En effet, les attaquants étant désormais des organisations professionnelles, chaque faille peut avoir des conséquences extrêmement graves. Dans ce nouveau contexte, IBM concentre ses investissements autour de trois axes majeurs.
Le premier vise à utiliser l'Intelligence artificielle pour rendre les individus plus intelligents, les aider à mieux traiter les données. Ainsi IBM a recours à Watson en tant qu'assistance au SOC. Cette technologie permet à des cyber-analystes d'avoir des données de qualité sur un sujet précis (malware, …) et de traiter des alertes de sécurité plus efficacement. Avec Watson, on passe de 10 alertes traitées par jour à plus de 30.
Le second axe s'appuie sur la rapidité. Pour cela, la pratique est importante. IBM a donc créé des "cyber range" servant à entraîner les équipes de SOC à affronter des crises. Un premier cyber range expérimental a été lancé, et d'autres vont ouvrir à travers le monde.

Enfin, la cybersécurité est aussi une affaire de partage de connaissance. Dans cette perspective, IBM propose X-force Exchange, une solution d'accès aux renseignements sur les menaces externes. Le but est de partager les informations et les résultats collectés.

Intelligence artificielle et cybersécurité : Une arme à double tranchant

L'intelligence artificielle est désormais au coeur du marché de la cybersécurité. De nombreuses entreprises rencontrées lors des Assises développent des outils se basant sur les techniques d'apprentissage automatique telles que le machine learning et le deep learning. Les champs d'applications vont de la détection de comportements anormaux en fonction des flux applicatifs et des logs système à la création de graphes mathématiques afin de détecter les variantes de malwares, sans oublier les systèmes de remédiation autonome. Ce sont des technologies à forte valeur ajoutée qui permettent d'aider les équipes de cybersécurité qui ne peuvent pas vérifier un à un tous les logs/actions sur des réseaux comportant souvent plusieurs centaines ou milliers de postes et utilisateurs, sans parler des datacenters ou des serveurs qui génèrent des trafics très importants.

Cependant, comme cela a été expliqué lors de l'atelier de **Radware** "La réalité artificielle de la cyberdéfense", l'apprentissage automatique est à double tranchant : les attaquants aussi peuvent l'utiliser. Ils entraînent des modèles à détecter leurs malwares avec du deep learning, puis font d'autres modèles offensifs pour apprendre à se cacher des modèles de détection. Ils répètent ensuite cette procédure jusqu'à ce que le malware puisse se cacher de tous les antivirus, même ceux avec des systèmes utilisant de l'intelligence artificielle. Les pirates utilisent aussi ces technologies pour automatiser le spear phishing à partir de documents, mails ou contacts trouvés sur internet. Grâce au ***Natural Language Processing (NLP)***, cette intelligence artificielle peut chercher un contenu ciblé sur internet afin d'apprendre à connaître une personne. *Une comparaison IA et humain a été faite pour du spear phishing sur Twitter : l'humain a contaminé 50 victimes en 2 heures en envoyant 200 tweets, avec 8 heures de recherche préalable . L'IA en 2 heures et sans recherche préalable , a envoyé 800 tweets et fait 275 victimes…*

Keynote par Nico Fischbach, *CTO Forcepoint*

La protection adaptative aux risques : le futur de la cybersécurité ?

Bien souvent, les utilisateurs sont considérés comme des problèmes et non comme des atouts de la sécurité des entreprises. Les politiques de sécurité, ressenties comme des contraintes, ne facilitent pas les partenariats entre DSI et RSSI. Et pourtant, la part de l'humain est centrale dans la sécurité des organisations. La protection adaptative se propose de couvrir l'intersection entre utilisateurs et données afin de réduire les frictions et d'augmenter la confiance. Nécessitant un certain niveau de maturité, cette nouvelle approche, est divisée en quatre étapes. La mise en place d'une politique sur les données privées, impliquant les employés, permet de réduire le fossé entre le ressenti et la réalité juridique. Les politiques de risques, conçues de façon générique permettent un entrainement du système et donne une plus grande liberté aux utilisateurs. Un déploiement contrôlé est réalisé afin de déterminer la façon dont le système est perçu. Enfin, la protection adaptative peut être déployée à grande échelle.

Rencontre avec Coralie Héritier, *CEO d'IDnomic*

QUELQUES MOTS SUR IDNOMIC ?

IDnomic intervient dans l'identité citoyenne notamment dans le cadre de l'émission des passeports biométriques : elle fournit des solutions allant de la sécurisation des fichiers biométriques à la vérification des documents d'identités aux postes de contrôle. Nous gérons la création, la gestion du cycle de vie et le support de certificats électroniques, qui sont des identifiants numériques forts, et qui, associées avec d'autres facteurs d'authentifications (doubles, voire triples) permettent de garantir une sécurisation des accès aux systèmes d'informations de plus en plus faciles et avec un nouveau de sécurité très élevé. IDnomic assure aussi la sécurité des IOT, en utilisant la même technologie, la PKI, qui s'impose de plus en plus comme une technologie transverse et assez universelle.

COMMENT PEUT-ON AUJOURD'HUI RÉSISTER FACE AUX GAFAM ?

Il n'y a probablement pas de futur GAFAM en France. Nous luttons difficilement à eux car si nous avons de très bons ingénieurs et une expertise reconnue, nous ne sommes pas suffisamment bons en marketing. Tenter de résister dans l'absolu est sans doute utopique et n'est pas la solution. Il faut plutôt éviter de dépendre totalement d'eux et proposer des alternatives. C'est ce que fait Hexatrust en regroupant les sociétés qui apportent une technologie de pointe en France et propose des solutions de cybersécurité qui peuvent s'interfacer et rendre plus sure l'utilisation de leurs services. Le but est donc d'apporter une complémentarité plutôt que de lutter contre eux.

AVEZ-VOUS UN MESSAGE À FAIRE PASSER AUX FEMMES QUI TRAVAILLENT OU VEULENT TRAVAILLER DANS LA CYBERSÉCURITÉ ?

La mixité progresse dans tous les domaines et c'est une bonne chose. Cela permet d'avoir une ouverture d'esprit plus grande et de partager des points de vue différents. Cependant en informatique elles représentent encore une petite minorité, a fortiori dans la cybersécurité. Les femmes de la cybersécurité doivent à mon sens avoir un rôle d'ambassadrices. Elles doivent montrer que c'est possible. La promotion des femmes dans l'informatique doit être faite au plus tôt, et les formations doivent être facilitées, dans les cursus scolaires et d'études supérieures, mais aussi dans le cadre de la formation continue.

Un Techlab au cœur du forum

Cette année, les Assises ont innové avec le Techlab réalisé en partenariat avec la société Newlode. Arnaud Cassagne, directeur des Opérations de Newlode explique l'objectif de ce nouveau dispositif : « Alors que pendant longtemps, les éditeurs de solutions de SSI ont été très centrés sur leurs technologies, nous voyons se développer de plus en plus la notion d'écosystème. Car la nécessité de travailler ensemble devient indispensable pour garantir un meilleur niveau de sécurité. C'est ce que nous avons voulu montrer au public des Assises avec six de nos partenaires ».
Deux démonstrations étaient proposées durant toute la durée des Assises. La première réunissait, autour de Newlode, Palo Alto Networks, F5 Networks et ServiceNow. Elle traitait de « l'automatisation de la protection d'une infrastructure cloud ». La seconde réalisée avec SentinelOne, Proofpoint et Splunk avait pour thème « Threat Hunting, détection et rémédiation automatique ».

Cette « première » a demandé aux différents intervenants une forte préparation, le but étant de bien faire comprendre l'apport de chaque brique technologique mais aussi l'intérêt de les intégrer pour une efficacité maximum : « Le TechLab a été un vrai succès car les participants aux démo ont pu saisir l'importance de l'écosystème. Nous avons aussi apporté des réponses à l'une de leurs principales préoccupations du moment : le manque de compétences. Quant à nous partenaires, qui sommes parfois concurrents, nous avons montré notre capacité à œuvrer ensemble pour élever le niveau de sécurité de nos clients » précise Arnaud Cassagne.

Keynote par Mike DeCesare, *CEO et Président de Forescout*

« La visibilité complète sur l'ensemble des terminaux connectés au réseau de l'entreprise représente le prochain enjeu en matière de sécurité »

Rencontre avec Benjamin Delpy,

Responsable du Centre de Recherche & Développement en Sécurité de la Banque de France et créateur de mimikatz, outil de pentest pour Windows.

DES REGRETS DE SAVOIR QUE VOTRE OUTIL EST UTILISÉ DE FAÇON OFFENSIVE DANS LE MONDE ?

La première fois que mimikatz a été utilisé publiquement fut durant l'affaire Diginotar.* Avec le recul, si l'on trouve une faiblesse il faut de la visibilité pour faire changer les choses. Windows a notamment changé sa stratégie "grâce" à une exposition de mimikatz, y compris auprès de ses plus gros clients . L'utilisation de mimikatz n'est pas le réel problème : cela fait remonter des problèmes sous-jacents sur les SI car le fait de pouvoir « exécuter » un exécutable sur un poste prouve un problème plus grand.

PENSEZ-VOUS QUE VOUS RECODEREZ MIMIKATZ DANS UN LANGAGE DE HAUT NIVEAU TEL QUE C# ? (Et profiter au passage de refaire une vraie documentation)

Il n'y a pas de vraie documentation mais il y a un wiki qui est maintenant en anglais. Pour comprendre un système Windows il faut se mettre au même niveau, le C est donc préférable pour les moteurs d'authentification … même si cela force à vivre dangereusement avec l'utilisation de pointeurs !

DANS QUELLE MESURE PEUT-ON PUBLIER UNE CYBERARME OPEN-SOURCE EN FRANCE ? LA LÉGISLATION EST-ELLE DIFFÉRENTE ENTRE LES OUTILS DE POST-EXPLOITATION ET DE HACKING ?

En France ce n'est pas très clair. Même le reverse de binaires n'est pas clair au niveau de la loi. Publier sur une exploitation peut être problématique. Mais dans le cas de mimikatz, il s'agit de post-exploitation. Nous ne profitons pas de failles mais juste de l'architecture Windows.

Credential Guard, **l'outil de sécurité par virtualisation**

La virtualisation est aujourd'hui au cœur de la cybersécurité. Microsoft apporte une nouvelle fonctionnalité avec Credential Guard. Introduit par Windows 10, Credential Guard utilise la virtualisation pour permettre notamment de protéger les identifiants de domaine, et ainsi empêcher les pirates de s'emparer des réseaux de l'entreprise. Avant l'apparition de ce concept, lorsque des pirates informatiques compromettaient le système d'exploitation, ils pouvaient accéder aux condensats utilisés pour chiffrer les informations d'identification de l'utilisateur, disponibles sans protection dans la mémoire **RAM.** Le principe de Credential Guard est fondé sur la sécurité par virtualisation : les identifiants sont stockés dans un conteneur Hyper-V, qui n'est pas directement accessible par le système d'exploitation. Ainsi, même si les pirates viennent à compromettre le système, ils ne peuvent accéder aux condensats et donc il leur est impossible de pénétrer les ordinateurs du réseau.

**Diginotar était une autorité racine de certification. En 2011, elle a été victime d'une attaque ce qui eut pour conséquence la compromission de tous les certificats émis jusqu'alors, car il était alors impossible de déterminer les certificats légitimes des illégitimes.*

INFRASTRUCTURE &RÉSEAUX

La sécurité des infrastructures réseau est un sujet très large. Pour ce livre blanc, il a été choisi de faire un zoom sur le SD-WAN.

Après la "cloudification" du stockage, la nouvelle tendance est à l'exportation dans le cloud des infrastructures réseaux. C'est pour cela que nous avons choisi dans cette partie Réseau et Infrastructure le SD-WAN (Software-Defined Wide Area Network). Il s'agit de la troisième génération de réseau, après IPsec (Internet Protocol Security) et MPLS (Multi Protocol Label Switching). Cette avancée technologique permet de créer ou de faire évoluer un réseau d'entreprise à travers le monde entier en toute simplicité, avec ses établissements distants, ses partenaires, des cloud providers, en utilisant n'importe quel fournisseur d'accès à Internet et n'importe quelle technologie, filaires ou sans fil.

Le SD-WAN est une technologie conçue pour :

> Utiliser un ensemble de liens hétérogènes

> Disposer d'une classification de flux applicative

> Router les flux par application

> Intégrer l'interconnexion avec les environnements Cloud

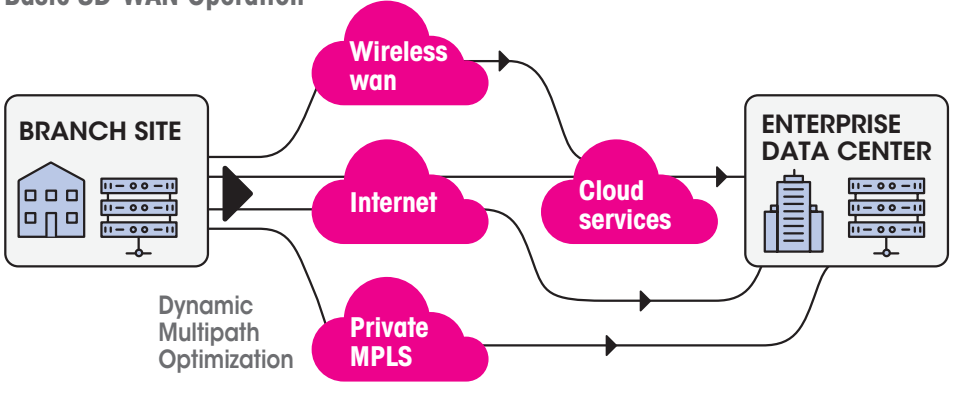
> Permettre un contrôle et un déploiement centralisés.

Le principal critère d'adoption du SD-WAN dans les réseaux d'entreprise est le gain économique résultant du remplacement d'un lien MPLS par un lien internet. Un des atouts majeurs du SD-WAN est sa simplicité de déploiement. Il apporte une couche d'abstraction et permet d'optimiser le trafic d'applications multiples qui tendent de plus en plus vers le Cloud. Le SD-WAN permet également de simplifier le management et l'opérabilité du WAN par un mécanisme d'identification et de priorisation (intelligente et dynamique) des flux.

Cependant, lorsqu'une équipe informatique envisage de déployer une technologie SD-WAN, il est nécessaire qu'elle ait conscience des défis et limites, en termes de cybersécurité, liés à une telle approche. Le SD-WAN doit être sécurisé et permettre le transfert rapide des données des utilisateurs, ainsi que la connectivité aux applications sur de longues distances en toute sérénité.

Une grande partie des implémentations de SD-WAN permet de chiffrer le trafic site-à-site à l'aide de l'IPsec, une norme de protection des données en transit. Parce que la plupart des solutions SD-WAN intègrent l'IPsec, on a souvent tendance à penser que les SD-WAN sont intrinsèquement sécurisés. Cependant IPsec protège les données en transit sur le réseau mais il ne peut rien face à aux intrusions et aux malwares sur le trafic direct d'un réseau distant vers le cloud.

Architecture d'un réseau SD-Wan */ Source : Juniper Networks*



Atelier Fortinet Retour d'Expérience SD-WAN

Pendant les Assises, Fortinet a animé un atelier de retours d'expérience de sa solution SD-WAN. La première partie était consacrée à la raison des choix d'un SD-WAN qui s'est fait parce que « le MPLS, devient de plus en plus complexe, difficilement configurable, et onéreux ». Par ailleurs, le SD-WAN permet une meilleure indépendance vis-à-vis des opérateurs et par la même occasion accélère les temps de déploiement.

Une autre raison mise en avant par les utilisateurs, c'est la possibilité de SD-WAN de maîtriser et potentiellement centraliser les différents flux venant de différents sites. De plus, il devient plus facile de respecter les recommandations de la PCI-DSS avec une meilleure segmentation par rapport à l'utilisation de routeurs MPLS. Le SD-WAN a également grandement amélioré la réactivité et l'exploitation de services proposés sur différents appareils connectés, tout en maintenant un haut niveau de sécurité et de performance.

Néanmoins, l'adoption d'une telle technologie n'est pas forcément aisée. Elle requiert de la part des équipes techniques une bonne connaissance du réseau et des applications.

La révolution 5G, un casse-tête en terme de sécurité

La **5G**, le nouveau standard de communication mobile, est une évolution majeure qui va apporter de l'intelligence dans les équipements réseau mais qui sera aussi vulnérable à des utilisations malveillantes. Lors de la conférence d'ouverture des Assises, Guillaume Poupard a rappelé que l'ANSSI travaille avec les équipementiers et valide chaque nouvel équipement avant son déploiement sur le territoire français afin de s'assurer d'un niveau minimum de sécurité. De l'autre côté, les utilisateurs sont aussi un maillon essentiel pour garantir cette sécurité dans les réseaux, en particulier pour la 5G. Grâce au débit qu'elle propose et à sa latence très faible, la 5G a été conçue pour répondre à bon nombre de besoins et notamment le contrôle de véhicules autonome (drone/voiture/…) ou bien la télé-chirurgie. Cette 5G se doit donc d'être irréprochable du point de vue de la sécurité en raison des services qui vont reposer sur elle. C'est une nécessité cruciale qui mettra sans aucun doute des vies en jeux dans le futur.

Rencontre avec Cyril Haziza,

CISO (Chief Information Security Officer) chez Axa

QUELLE EST VOTRE APPROCHE VIS À VIS DE LA CLOUDIFICATION DES INFRASTRUCTURES ?

En préambule, il me semble important de rappeler que les usages du Cloud sont très différents selon les modèles retenus. Je pense qu'il n'y a pas assez de distinction faite entre le cloud public et le cloud privé, en interne on distingue plutôt le IaaS, le PaaS et le Saas que l'on distribue entre les plateformes. En tant que responsable sécurité, je ne suis pas en charge de la stratégie d'adoption du cloud mais plutôt de sa sécurisation sous toutes ses formes. On constate que l'adoption de technologies de Cloud public implique une modification des méthodes projets et des technologies sous-jacentes. C'est notamment cela qui fixe la cadence de l'adoption du Devops. On doit s'adapter avec de nouvelles méthodologies comme le SSDLC, des outils de compliance, IAST, SAST et DAST dédiés .

CE NOUVEL ENVIRONNEMENT A DONC DES CONSÉQUENCES EN TERMES DE COMPÉTENCES ?

Absolument. Nos ingénieurs doivent également suivre des formations dédiées pour adapter l'identification des risques et les mesures de sécurité associées. Ce dernier point n'est pas à sous-estimer, le besoin de montée en compétences des personnes nécessite un temps d'adaptation, on a encore besoin de plus d'ingénieurs sécurité formés sur les technologies de Cloud public, là où le Cloud privé présente moins d'écart de compétences.

QUELLE EST L'ATTAQUE CYBER QUI VOUS A LE PLUS MARQUÉ ?

Mis à part les grandes attaques de ces dernières années comme Sutxnet et les ripostes qui ont suivi ou les attaques menées par APT28 et certains groupes de hackers célèbres, une attaque qui m'a bien marqué date de 2010. La Chine avait détourné une partie du trafic internet mondial pendant 18 min sans que rien (côté infrastructure chinoise) ne s'écroule. On ne pensait pas cela possible. Aujourd'hui, personne ne sait encore ce qui a été fait de ces données. L'opérateur China Telecom aurait ainsi malencontreusement annoncé des routes internet prioritaires via ses serveurs, pendant ces 18 minutes, pour acheminer le trafic de nombreux sites. Concernant les données, plusieurs sites du gouvernement et de l'armée des Etats-Unis étaient visés. Des données hautement sensibles auraient ainsi été visibles.

CLOUD &SÉCURITÉ

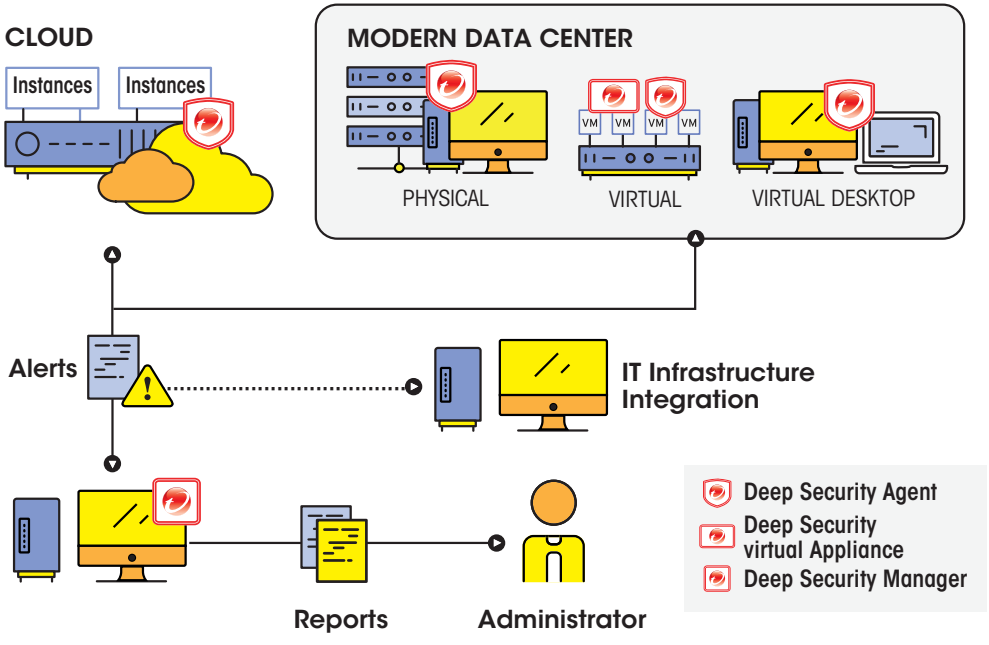
Cloud & Sécurité : la délicate équation

L'une des conséquences de l'émergence du numérique est d'avoir à disponibilité, une quantité gigantesque d'informations en temps réel depuis les différents terminaux et notamment depuis les smartphones. Cela grâce au Cloud, terme qui recouvre l'ensemble des solutions de stockage et de manipulation de données à distance comme le montre le schéma ci-dessous.

Cependant l'utilisation du cloud n'est pas sans risques. En effet, l'accès des données à distance peut permettre à un attaquant d'intercepter les flux via des attaques de type Man In The Middle et d'y chercher des failles afin de compromettre la confidentialité, l'intégrité et la disponibilité des données. Ces attaques peuvent prendre différentes formes parmi lesquelles : **les dénis de service,** où un attaquant va lancer énormément de requêtes grâce à un réseau de botnets jusqu'à ce que le service ne puisse plus fonctionner ; **les services virtualisés,** mal isolés sur une machine permettant d'accéder aux données par ricochet ; **les API non sécurisées** ou contenant des erreurs de code qui peuvent être exploitées pour exécuter du code à distance; **des mots de passe cassés** en raison de la fragilité dans la gestion d'accès des identifiants... Il est donc primordial de suivre un certain nombre de bonnes pratiques et de respecter les normes, dans le cas du Cloud il s'agit des normes ISO 27017 et 27018.

L'infrastructure Cloud et les besoins de sécurité

/ Source : Trend Micro Deep Security



Cloud Public

Comment préserver la souveraineté de nos SI ?

Cette table-ronde animée par Alexandre Fernandez -Toro, et avec l'intervention de Cyril Elsen et Raphael Marichez avait pour objectif de présenter les leviers concrets dont disposent les RSSI pour préserver la souveraineté des SI dans un environnement de Cloud public.
En préambule, il a été rappelé que lorsqu'un client utilise un service de cloud public, il n'a pas la main sur les conditions d'utilisation des données. Afin de savoir ce qu'il faut mettre sur un Cloud public ou ce qu'il convient de garder en interne, il est donc nécessaire de faire une analyse de risques et de délimiter un périmètre de confiance sur des critères de sensibilité de la donnée. Pour assurer la sécurité des données il faut appliquer les règles d'hygiène telles qu'elles sont décrites dans la norme ISO 27017 et se référer également à la norme ISO 27001 pour la mise en place d'un système de management de la sécurité.

Le Cloud Computing, sous toutes ses formes (privé, public ou hybride) implique d'importants enjeux économiques pour les entreprises. En sous-traitant la gestion de leurs données et des infrastructures, les entreprises réalisent une réduction des coûts de maintenance, de licences, d'énergie et d'équipements et peuvent mieux rationaliser leurs dépenses. Le Cloud permet au client de se concentrer sur son cœur de métier et sur la définition de son besoin fonctionnel : il n'a plus à se préoccuper des problématiques de conception, d'installation, de maintenance et d'administration. Néanmoins, le Cloud comporte des risques juridiques, techniques et opérationnels dus à la perte de contrôle du client sur le traitement de ses propres données. La répartition des responsabilités n'est en aucun cas triviale. C'est au client d'exiger un certain niveau de sécurité ou d'expertise de la part de ses fournisseurs de Cloud via notamment les audits et le respect des normes ISO.

Au cœur du forum

Le place prise par le cloud dans les entreprises se traduit également aux Assises où étaient présents de nombreux acteurs et solutions s'appuyant sur ce type de service. Deux solutions ont été retenues dans cette partie.

Un grand nombre d'entreprises à travers le monde utilise **Microsoft Azure,** la solution de cloud public de Microsoft. Comme ses concurrents, l'éditeur américain est confronté aux interrogations de ses clients sur la **sécurité de la plateforme, la transparence, l'intégrité des données, le respect de la vie privée et la conformité**.

La plateforme Azure propose des fonctionnalités intégrées et des solutions de sécurisation des applications et services. Elles sont organisées en six zones fonctionnelles : opérations, applications, stockage, mise en réseau, calcul et identité. Chacune de ces solutions met à disposition divers outils interconnectables, avec une documentation détaillée, permettant une gestion des plusieurs notions liées à la sécurité - **prévention, détection, correction de vulnérabilités des applications web, règles de sécurité réseau, chiffrement des communications/comptes de stockage, etc**...

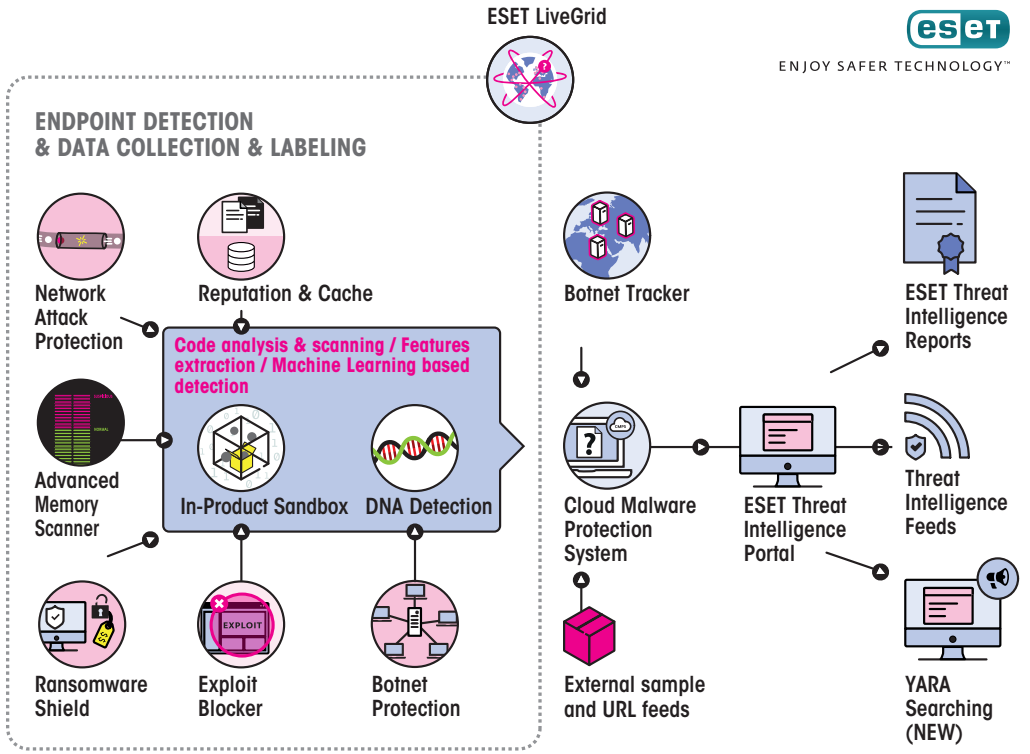
Co-fondée par Luc Delsalle (ancien élève de l'EPITA) et Emmanuel Gras, la startup Alsid (Prix de l'Innovation en 2017) propose une solution de surveillance en temps réel des annuaires Active Directory. L'Active directory d'une entreprise est une cible de choix pour tout pirate puisqu'un AD compromis est souvent synonyme d'accès privilégié au SI de l'entreprise. Pour aider les entreprises à mieux sécuriser leur AD, Alsid propose une solution qui analyse en continu le niveau de sécurité des infrastructures Active Directory (AD) afin de détecter les signaux faibles à l'origine d'une attaque.

Dans sa dernière version, **Alsid permet de détecter et d'isoler en temps réel une attaque ciblée sur l'infrastructure** offrant ainsi la capacité aux équipes d'un SOC d'initier des mesures de réponse sur incident dans les meilleurs délais. Le déploiement de l'offre a été simplifiée : elle est proposée en mode SaaS, sans client à installer localement, sans sonde réseau à positionner et surtout sans compte administrateur à demander sur l'annuaire. Enfin la solution d'Alsid dispose de connecteurs vers plusieurs SIEM du marché (QRadar d'IBM, RSA Security Analytics et via Syslog), afin d'alimenter un éventuel SOC.

Le prochain objectif de Luc Delsalle et d'Emmanuel Gras est de "déployer la solution pour Azure AD c'est à dire appliquer la même chose au cloud qui est une thématique adjacente à l'AD."

PRÉVENTION &FORENSIC

Détection pour des menaces ciblées / *Source : ESET*



Prévention & Forensic

"On assiste aujourd'hui à une rupture opérationnelle et stratégique des menaces. Hier, les attaquants allaient jusqu'à mener des opérations de sabotage comme avec Stuxnet. Puis on a observé une volonté de briser la confiance des citoyens envers leur état (cyberattaque touchant les élections aux États-Unis). Aujourd'hui, nous voyons des acteurs qui exploitent des modes opératoires traditionnellement criminels pour mener des attaques de sabotage d'envergure nationale (NotPetya)."

Maxime Cartan,
Co-fondateur & Président de Citalid
(Prix de l'Innovation 2018)

Comme le dit Maxime Cartan, la cybercriminalité évolue, les attaques se complexifient et visent désormais des acteurs essentiels tels que les OIV afin d'avoir un impact maximum. Les groupes de hackers à l'origines de ces grosses attaques, les APT, peuvent être composés de plusieurs centaines voire milliers de personnes expertes dans leurs domaines. Elles utilisent donc des procédés très élaborés permettant de rester furtivement dans le SI de leur cible pendant en moyenne 200 jours et parfois même pendant plusieurs années. Face à de tels groupes et dans un contexte économique et sociétal marqué par un manque d'ingénieurs en cybersécurité, les organisations, l'État et ses alliés doivent s'unir pour se défendre. C'est effectivement la tendance actuelle - comme l'a exprimé Guillaume Poupard, le Directeur général de l'ANSSI lors de la conférence d'ouverture des Assises de la sécurité - avec l'établissement de normes et de standards. Pour répondre à ces standards, les entreprises doivent toutefois élaborer leur défense en s'appuyant sur les nombreux outils du marché proposés, aussi bien par les grands acteurs que par des startups innovantes. Ces outils sont orientés sur la prévention et souvent mis au point grâce à une étude forensic des menaces.

Atelier Kaspersky Olympic Destroyer, l'enquête

Olympic Destroyer est un logiciel malveillant qui a frappé les organisateurs, les fournisseurs et les partenaires des Jeux Olympiques d'hiver de PyeongChang en Corée du Sud en février 2018 à travers différentes actions de cybersabotage propres semble-t-il à la Corée du Nord. Bien avant l'acte de sabotage, des courriels d'hameçonnage, déposant des implants PowerShell Empire, ont été envoyés à différentes entités associées aux Jeux Olympiques. Lors de l'analyse post-mortem, les chercheurs de Kaspersky Lab ont pu découvrir que la compromission initiale avait été réalisée à l'aide d'un accès RDP d'un prestataire sud-coréen. Aucune Odays n'a été utilisé. Les attaquants ont utilisé les outils Metasploit, TeamViewer, PowerShell Empire, ainsi que d'autres outils pour la latéralisation dans le réseau compromis et sécuriser leurs accès. Pendant son passage, le malware a volé des mots de passe sauvegardés sur les ordinateurs infectés, les a gardés dans son système pour les utiliser et continuer sa propagation. Olympic Destroyer a utilisé PSExec de Windows et déposé un programme de destruction «destroyer component». La protection contre cette attaque passe par de la défense en profondeur, les mises à jour, la journalisation, la désactivation des macros provenant d'Internet et de certains script powershell. L'attaque serait attribuée en fait au groupe de pirates informatiques russes Sofacy (aussi appelé APT28 ou Fancy Bear) en réaction au bannissement des Jeux d'une partie de la fédération russe pour dopage.

Rencontre avec Benoit Grunemwald,

Directeur des opérations d'ESET

POURQUOI LA THREAT INTELLIGENCE COMME SUJET DES ASSISES ?

Les menaces évoluent et leurs nombres augmentent sans arrêt depuis ces dernières années. Les outils d'infections et post-exploitations évoluent eux aussi sans arrêt, c'est pourquoi nous jugeons que la Threat Intelligence est indispensable dans une bonne analyse de risque afin de prendre en comptes les outils utilisés par ces menaces sur le moment présent. Ces outils permettront de détecter une intrusion, récolter des informations pendant cette intrusion et permettra par la suite de prédire une attaque similaire aux précédentes en déterminant les "Tools, Tactics, and Procedures".

COMMENT SE PASSE LE PARTAGE D'IOC RÉCOLTÉS PAR VOS AGENTS DÉPLOYÉS ?

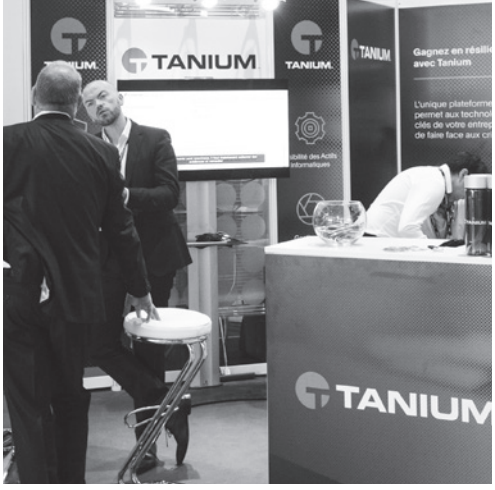
C'est une histoire d'hommes. Il y a des coopérations avec les forces de l'ordre et de la cybersécurité pour des obligations de sécurité "nationale" ou de protection d'infrastructures sensibles, mais aussi avec les entreprises de confiance ou partenaires.

QUE PENSEZ-VOUS DES INITIATIVES TELLES QUE THREATCONNECT OU IBM XFORCE, QUI PERMETTENT DE PARTAGER DES IOCS GRATUITEMENT ?

En partageant des IOCs ont espere qu'elles soient diffusées plus rapidement afin de contrer les menaces. Par contre, diffusion ne veut pas dire intégration. Si des IOCs sont diffusées mais ne sont pas intégrées dans les équipements de detection, cela n'est suivi d'aucun effet. Théoriquement, cela rend la tâche plus difficile aux attaquants. Mais le fait que ces IOCs soient publiques les rend aussi accessibles par les attaquants, qui peuvent surveiller si leurs actions malveillantes sont découvertes.

QUE PENSEZ-VOUS DE L'IA DANS CE DOMAINE, ET EN UTILISEZ-VOUS CHEZ ESET ?

Miser uniquement sur l'Intelligence Artificielle sans former l'humain est dangereux. L'Intelligence Artificielle est une arme, mais une arme à double tranchant. Si on n'inclut pas l'humain dans son pilotage, ou sa création, il ne s'agit que d'un outil parmi de nombreux autres. Lorsque le marketing parle d'IA, nous sommes dans l'imaginaire collectif, avec l'IA qui pilote le monde, mais ce n'est pas encore le cas aujourd'hui. ESET utilise de l'IA depuis 1998, plus précisément des réseaux de neurones récurrents ainsi qu'un groupe de six algorithmes de classification.



Au cœur du forum

Au delà de la détection de malwares, il y a d'autres problématiques à prendre en compte. Par exemple le **shadow IT** qui désigne des solutions mises en oeuvre sans l'approbation de la DSI et qui peut représenter jusqu'à 20% des actifs informatiques de l'entreprise. Ces équipements sont souvent peu maintenus et insuffisamment sécurisés, ce qui peut en faire des cibles de choix pour les pirates.

Pour y remédier, **Tanium** propose sa solution de type endpoint permettant d'avoir une vue en temps réel sur l'intégralité du parc. L'architecture est basée sur un agent déployé à un endroit tactique sur le SI, qui se redéploie sur chaque machine disponible jusqu'à couvrir tout le parc. L'un des points forts de la solution est que les endpoints renvoient les données en "temps constant" (moins de 15 secondes) quel que soit la taille du SI.

La plateforme permet aussi d'envoyer des commandes pour récupérer des infos de tous les endpoints simultanément comme le nombre de machines allumées, utilisateurs connectés, bande passante, CPU, etc…

La société **Darktrace** propose une solution, l'**Entreprise Immune System** qui analyse les flux réseaux grâce à une sonde physique, ressemblant à un serveur, placée dans le cœur du réseau. Elle permet la surveillance de flux au sein du SI, afin de trouver des anomalies et éviter qu'une attaque se propage. **On peut ainsi surveiller les flux de partages de fichiers comme SMB (Server Message Block), le trafic internet, et même l'ajout de clefs USB,** lorsqu'elles sont branchées sur des systèmes Windows qui envoient par défaut une requête au réseau. Il est possible de récupérer des métadonnées à différents niveau, ce qui pourra donner des indices lorsqu'un poste est compromis. Les alertes envoyées sont classées selon 3 métriques : le nombre de machines connectées, le volume de données et les échecs de connexion. Aujourd'hui les technologies ne permettent pas encore d'avoir un système autonome à 100%. Avec le volume de données croissant utilisées, un opérateur a besoin qu'on lui contextualise les informations pour être efficace.

L'objectif est de simplifier la prise de décision en mettant à la disposition de l'opérateur les informations les plus pertinentes.

Et pour finir…

« Pénurie des ressources humaines, le défi »

Sébastien Bombal, *Conseiller ComCyber, Ministère des Armées*

Face à cet univers numérique en pleine expansion, le vivier de ressources humaines disponibles, en France comme à l'international, ne permet plus de couvrir tous les besoins en cybersécurité. Le numérique, et encore plus spécifiquement la cybersécurité, est un domaine d'une complexité exponentiellement croissante, pour lequel la formation des spécialistes est longue, nécessite la mise en pratique, une actualisation et une remise en question permanente.

Les ressources humaines sont le facteur clé pour sécuriser les organisations et accompagner la transformation numérique. Le recrutement de spécialistes, la formation à tous les niveaux, le maintien en compétences ou encore la valorisation ont été des difficultés largement partagées entre les participants lors des Assises de la Sécurité. Véritable défi pour les organisations, cette situation implique de se réinventer en matière de gestion des ressources humaines.

Toutefois, il ne sera pas possible de compenser la cadence des évolutions et des innovations technologiques par une augmentation de ressources humaines proportionnelle. Cette logique conduirait inévitablement à augmenter le décalage entre les moyens de sécurisation globale et la surface attaquable à défendre. D'autres réflexions capacitaires doivent être menées, visant souvent à une forme de mécanisation des actions de cybersécurité à travers des technologies d'automatisation et d'orchestration. Cette mécanisation pose déjà de nombreux challenges en matière d'interopérabilités technologiques et organisationnelles, ainsi que de nouveaux risques. Véritable rupture pour les années à venir, ces projets contribueront à limiter le recours à des ressources humaines et à des expertises rares, pour anticiper, détecter et réagir, même aux attaques les plus élaborées.

En attendant, la guerre des cyber talents est déclarée.

Ce livre blanc a été conçu avec la promotion 2019 Système, Réseau et Sécurité de l'EPITA sous la direction de Sébastien Bombal (Aymane Barka, Hamza Boughemza, Briquet Antoine, Romain Champault, Maxime Chouquet, Lucas Dessert, Maxence Duchet, Ilyass Elomri , Guillaume Esposito, Nathan Faedda, Baptiste Fortin, Florian Garret, Mathieu Ghosn, Corentin Giroud Argoud, Francois Granier, Jonathan Guihard, Ron Hassan, Matthieu Haulin, Quentin Lauzeille, Marc Legendre, Yohann Leon, Martin Leydier, David Marshall, Rogelio Mendoza, Luc Ozanne, Thibaut Passilly, Alessandro Pisu, Charles Prevot, Guillaume Rebut, Harish Segar, Fabien Tessier).

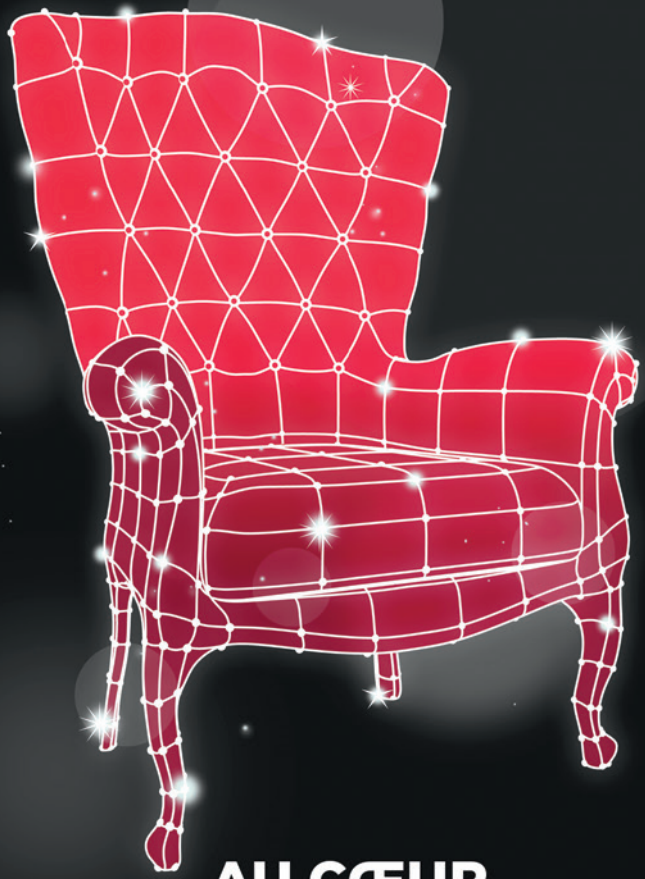
Remerciements

Avec une mention spéciale pour Marc-Antoine Faillon, Agathe Hinsberger et Aurélien Sudul.

Nous remercions particulièrement pour leur temps et leur disponibilité : Emmanuel Germain, Benjamin Delpy, Coralie Héritier, Gérome Billois, Cyril Haziza, Dagobert Lévy, Lois Samain, Luc Delsalle, Maxime Cartan, Benoit Grunemwald, Arnaud Cassagne, Mathilde Imbert, Margaux Tawil, Julien Fistre.

lesassises

de la sécurité et des systèmes d'information



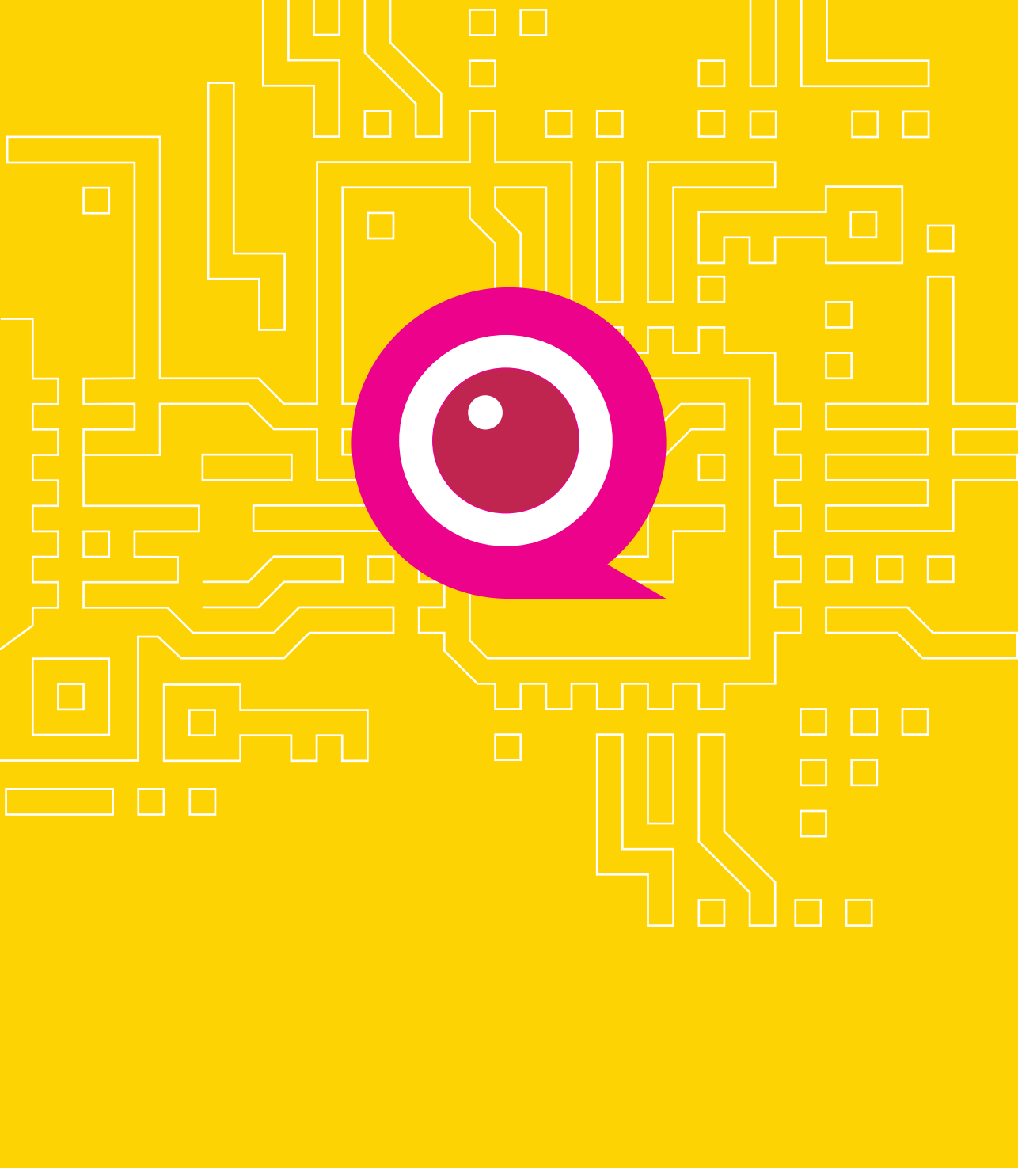
AU CŒUR DE LA COMMUNAUTÉ CYBER

9 › 12 OCTOBRE 2019 MONACO

COMEXPOSIUM

lesassisesdelasecurite.com @Les_Assises #AssisesSI

DC consultants



@Les_Assises #AssisesSI

www.lesassisesdelasecurite.com

DC consultants

COMEXPOSIUM