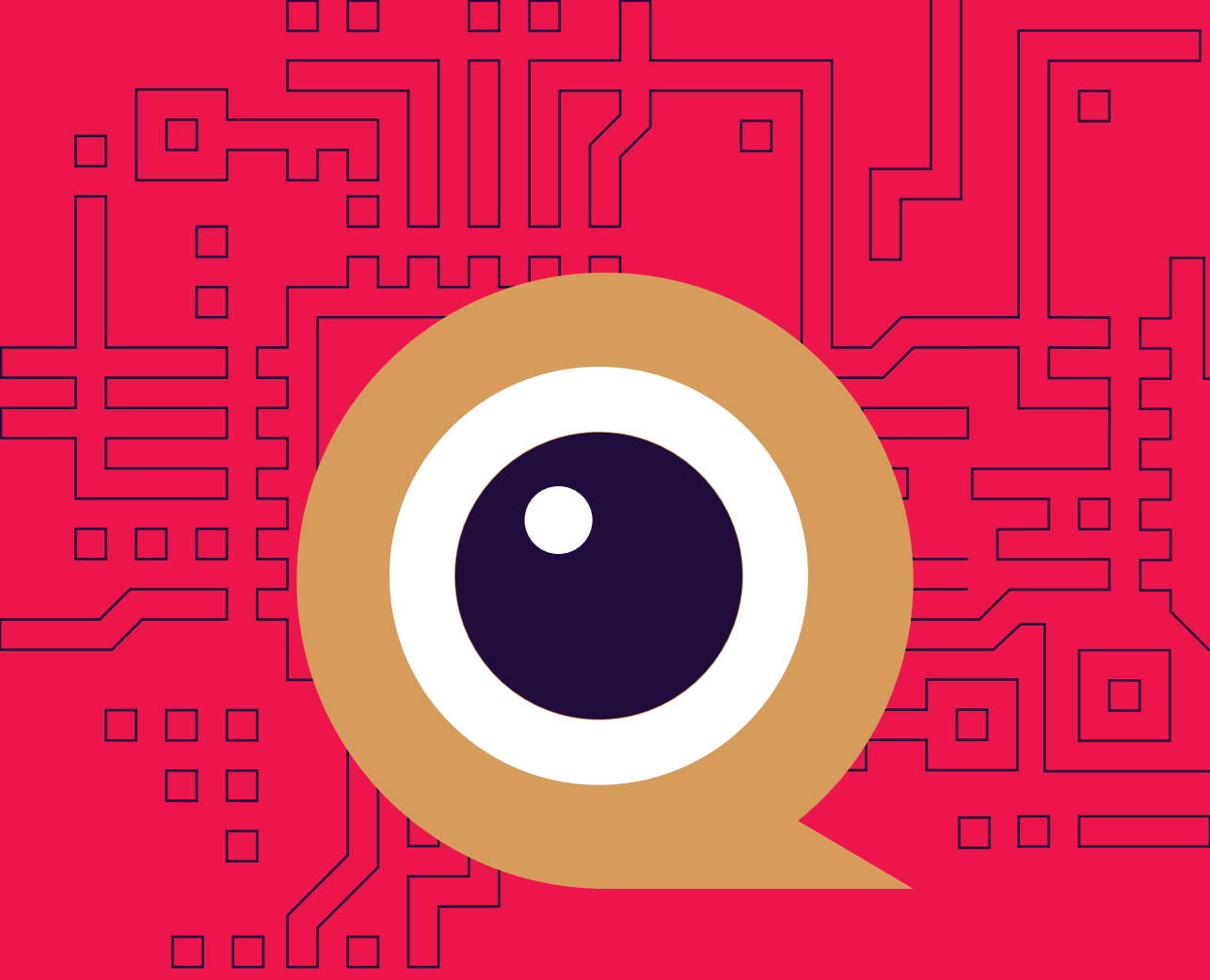


CYBERSÉCURITÉ & INNOVATIONS

/ ÉDITION 2020 ///

Le regard des Assises et de l'EPITA

LES ASSISES

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

LE BILAN EN CHIFFRES 04 - 05

LES TEMPS FORTS DES ASSISES 06 - 14

Trois questions à Olivier Ligneul 06
Conférence d'ouverture par Guillaume Poupard 07
Keynotes Tanium et Microsoft 08
Keynote Crowdstrike - Focus sur le Startup Corner 09
Olvid - Prix de l'Innovation 2020 10
Trois questions à Buster.AI 11
Bilan 2020 : une vague de ransomwares sans précédent 13
Portrait du RSSI en 2021 14

LE COVID ET SES CONSÉQUENCES SUR LA SSI... 15 - 18

Table-ronde Cesin : COVID 19 – La réponse Cyber 17
Atelier Datadome - Atelier Orange 18

SOUVERAINETÉ... 19 - 22

Table ronde - Le Cybermonde, un enjeu géopolitique 21
Table ronde - Bâtir et promouvoir une souveraineté nationale et européenne 22

TENDANCES... 23 - 29

Atelier Cybereason 24
Table ronde - Zero Trust 25
Zero Trust, Cryptographie et IA en première ligne 26
Least Privilege Access - Just in Time Access (JIT)t 27

→ CHIFFRES CLÉS DES ASSISES 2020

1 750
PARTICIPANTS

6 000
RENDEZ-VOUS ONE TO ONE

140
ATELIERS ET CONFÉRENCES

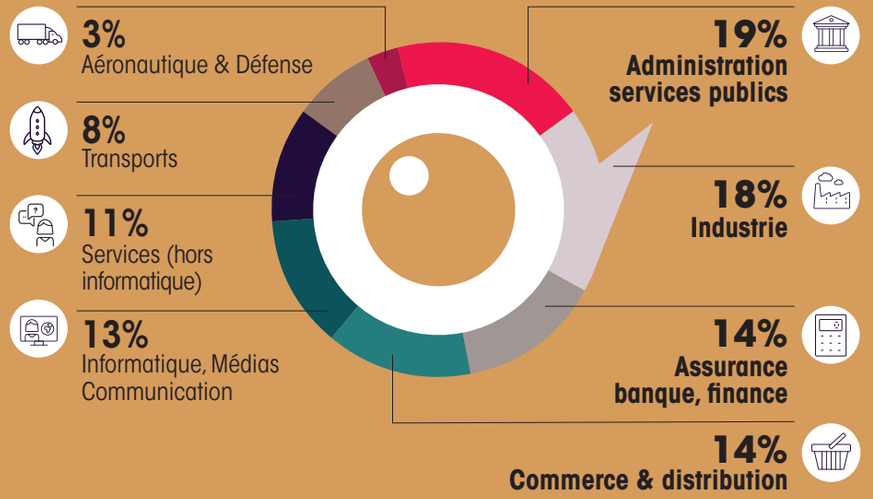
818 **RSSI & DSI**
REPRÉSENTANTS
538 SOCIÉTÉS

297 **NOUVEAUX INVITÉS**

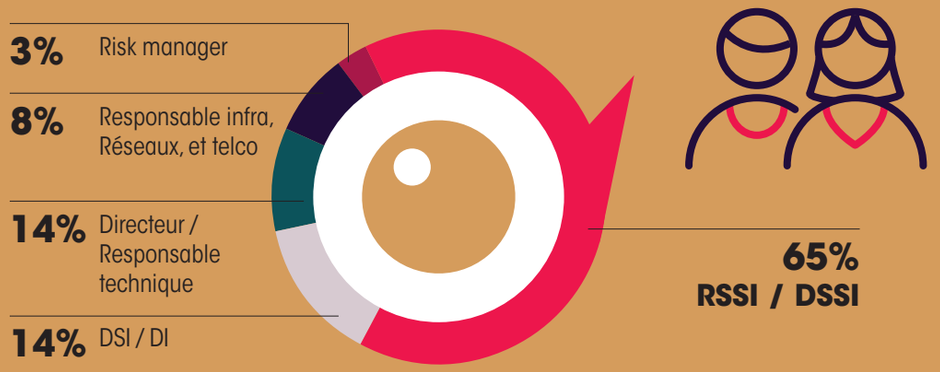
135 **PARTENAIRES**

84 **EXPERTS & JOURNALISTES**

→ LES INVITÉS PAR SECTEUR



→ LES INVITÉS PAR FONCTION



Trois questions à Olivier Ligneul,

Directeur Cybersécurité du Groupe EDF

QUE REPRÉSENTENT LES ASSISES EN TERMES D'INNOVATION CYBER ?

Les cyberattaquants s'adaptent constamment à nos moyens de défense, ils les testent, les étudient et réagissent aux processus établis afin d'identifier notre ligne Maginot. Napoléon Bonaparte indiquait que "les règlements sont faits pour les soldats et non pour les guerriers ; la bataille se rit du code, elle en exige un nouveau, innové par elle et pour elle et qui disparaît dès qu'elle est terminée." Dans le monde numérique de notre époque, les Assises nous permettent de trouver d'autres approches, d'identifier des solutions et de s'approprier de nouvelles technologies afin de réinventer constamment nos moyens de défense.

QUEL MESSAGE DONNER À DES JEUNES QUI VONT SE LANCER DANS LES CARRIÈRES DE LA CYBERSÉCURITÉ ?

Les années 2000 ont été celles des startups, celles de 2010 consacraient la transformation numérique, les années 2020 seront celles de la cybersécurité. La cybersécurité est devenue un métier à part entière, avec de multiples facettes, une richesse dans sa diversité et ses expertises. La cybersécurité, c'est également des femmes et des hommes qui partagent une passion commune, et œuvrent pour préserver la liberté de nos concitoyens, défendre les intérêts et les biens numériques de nos entreprises et aident à faire fructifier notre potentiel numérique dans un espace préservé.

VOUS ÊTES LE PRÉSIDENT DES ASSISES 2021 : QUELLE EST VOTRE FEUILLE DE ROUTE ?

Je me vois tout d'abord partie prenante d'un comité de pilotage foisonnant dont les personnalités fortes qui le composent forment un vivier d'idées, d'innovations et de créativité spectaculaire. Je pense que le rôle du président est également de rassembler nos points de vue et trouver le bon compromis afin de donner une unité et une cohérence à la thématique de cette nouvelle édition des Assises. L'année 2021 amorce la troisième décennie de cet événement annuel incontournable pour notre profession sans que l'anniversaire des 20 ans ait pu être pleinement consommé dans un contexte sanitaire contraignant. Il est également assez probable qu'en octobre, nous aurons retrouvé notre liberté de mouvement et une capacité à nous réunir, échanger dans le monde « réel » et fêter le simple fait de pouvoir nous retrouver enfin.

La communauté cyber a su s'organiser au fur et à mesure qu'elle prenait de la maturité. Les produits et services se sont perfectionnés et adaptés aux contraintes de la transformation numérique. La fonction cybersécurité a muri, se transformant en une filière professionnelle et se rapprochant du métier et des enjeux de nos organisations. Cependant, il convient de ne pas oublier que notre écosystème est désormais composé de plusieurs générations, avec plus de diversité et des compétences réparties dans un spectre plus large de technologies et de méthode, selon un panel de niveau d'expertises plus large.

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

Un nouveau tournant pour la cybersécurité

Guillaume Poupard, le Directeur Général de l'ANSSI a ouvert, « pour la septième fois » a-t-il rappelé, cette édition des Assises. Prenant le contre-pied de certains discours actuels, il s'est voulu optimiste « oui la menace grandit mais il faut être positif ». A l'appui de ses propos, plusieurs constats. D'abord « nous arrivons au terme d'une phase d'évangélisation » que ce soit auprès du grand public, des dirigeants d'entreprise ou des politiques. Par ailleurs, « être attaqué n'est plus honteux » et il a salué les victimes qui acceptent de témoigner. « Avec tous ces éléments » martèle le DG de l'ANSSI « les décideurs ne peuvent plus dire qu'ils ne savaient pas. Et s'ils le disent, ils sont fautifs ». Et pour les aider dans leur démarche, l'Agence met à leur disposition un nouveau guide intitulé « organiser un exercice de gestion de crise cyber ». Guillaume Poupard a également souligné le travail des industriels. Outre l'annonce d'un nouveau référentiel de qualification (PAMS, pour les prestataires d'administration et de maintenance sécurisée), il a confirmé qu'un « gros hébergeur du Nord de la France » sera prochainement qualifié « SecnumCloud » (il s'agit d'OVH). Ce fournisseur va donc rejoindre Oodrive et Outscale comme référence d'offres cloud à destination notamment des Opérateurs d'Importance Vitale (OIV). Enfin, il a souligné l'importance de l'humain dans les stratégies de cybersécurité. Que ça soit dans la sensibilisation dès le lycée afin par exemple de faire naitre des vocations, ou dans la réunion des talents car « c'est ensemble que nous pourrons lutter contre les menaces ».

Campus Cyber : l'excellence de la cybersécurité française enfin réunie

Lors des Assises 2020, Michel Van Den Berghe, CEO d'Orange Cyberdefense est venu détailler le projet de Campus Cyber, suite à la mission qui lui avait été confiée en juillet 2019 par le Premier Ministre. Ce campus inspiré des modèles étrangers (CyberSpark israélien de Beer Sheva ; parc technologique russe de Skolkovo ; Cyber NYC de New York) se veut opérationnel et a pour objectif de rassembler sur un même site l'ensemble des acteurs représentant l'écosystème de la cybersécurité en France : grandes entreprises ; startups ; laboratoires de recherche ; écoles d'ingénieurs (dont l'EPITA); services de l'Etat… qui viendront installer tout ou partie de leurs effectifs dans un immeuble du quartier de la Défense baptisé ERIA (un deuxième site davantage orienté sur le monde industriel devrait être installé par la suite à Satory près de Versailles). D'ores et déjà, plus de 60 sociétés se sont déclarées intéressées et certaines ont déjà réservé leur espace. C'est le cas de l'ANSSI, Orange Cyberdefense, Airbus, Cap Gemini, Atos, Thales, Sopra-Steria mais aussi des startups comme Gatewatcher ou YesWeHack. Les 25 000 m2 de l'édifice se répartiront entre bureaux, espaces publics, show room et salles dédiées à la formation.

Keynote Tanium

Orion Hindawi, *CEO de Tanium* et
Dagobert Levy, *VP South EMEA*

Le contexte post-crise

Lors de cette keynote, Orion Hindawi, CEO de Tanium et Dagobert Levy, VP South EMEA ont rappelé que dans le contexte post-crise, de nouvelles technologies mais aussi de nouveaux risques cyber vont émerger. Le rôle (et même le devoir) des fournisseurs est d'accompagner leurs clients en simplifiant les offres car le marché souffre d'une multiplication des solutions qui rendent complexes l'administration des systèmes d'information. Une fragmentation qui peut s'avérer dangereuse pour la sécurité des SI. Faire comprendre ces risques à un niveau décisionnaire n'est pas simple. Rares sont les membres des conseils d'administration à posséder les connaissances techniques nécessaires pour réellement comprendre les implications d'une attaque informatique, et savoir y faire face. Pour Orion Hindaw dont la société est spécialisée dans la sécurité des end-point, il faut raisonner en termes d'impacts afin que les décideurs puissent mieux apprécier le risque. Il est aussi important d'insister sur le fait qu'une attaque aura inévitablement lieu, mais qu'il est possible d'en minimiser ses impacts.

Keynote Microsoft

Bernard Ourghanlian
Directeur Technique et Sécurité chez MICROSOFT France

Les conséquences de la pandémie sur l'entreprise

Lors de cette keynote, Bernard Ourghanlian, Directeur Technique et Sécurité chez MICROSOFT France est revenu sur les conséquences de la pandémie pour les entreprises. «Nous avons assisté à 2 ans de transformation numérique en 2 mois » a-t-il souligné. Mais si les entreprises ont su s'adapter à la situation, il en est de même pour les cybercriminels qui se sont servis de l'actualité dans la conception et la mise en œuvre de leurs attaques. Les organisations qui se sont le plus vite adaptées à cette situation sont celles ayant adopté une approche « Zero Trust ». Et de citer les grands principes de ce concept :

- **Vérification** de toutes les tentatives de connexion sur toutes les données disponibles (localisation, identité, configuration, etc..).
- Mise en place du **principe du moindre privilège** (accès accordé aux personnes uniquement lorsqu'elles en ont besoin et seulement pour la tâche spécifique qu'elles ont à accomplir)
- **Présupposer la violation**, partir du principe que tôt ou tard le système d'information sera compromis par un attaquant et donc prévoir un système résilient

Cette intervention fut suivie par le témoignage de Nicolas Denisse, Directeur des opérations chez Servier. Après avoir reconnu que son entreprise n'était pas préparée à la crise ni à mettre un grand nombre de collaborateurs en télétravail, la stratégie de Servier a d'abord été de définir les prioritées de l'entreprise, à savoir, continuer à produire des médicaments. Pour poursuivre l'activité, il a fallu couper les comptes de certains collaborateurs afin d'éviter qu'ils ne saturent la passerelle VPN ou encore migrer vers des solutions externes comme office 365.

Espace Startup Corner

Keynote Crowdstrike

Réduire les interventions humaines

Cette keynote a été l'occasion d'un échange entre **Shawn Henry et CJ Moses, respectivement CISO de Crowdstrike et CISO par intérim d'Amazon et tous les deux anciens agents du FBI.** Au cœur du débat : le rôle grandissant du RSSI dans l'entreprise qui doit considérer l'environnement des menaces dans son ensemble avec une vision à 360°. C'est-à-dire tant dans le monde virtuel que physique. Par ailleurs, dans un contexte d'attaques de plus en plus destructrices et sophistiquées, l'humain reste encore trop souvent le point d'entrée privilégié des attaquants. Pour faire face à ce type de menaces, CJ Moses préconise l'application stricte du principe du moindre privilège. Ainsi chez Amazon, les accès ont été réduits à hauteur de 80%, et des mécanismes de just in time access ont été mis en place. L'application à cette échelle de telles restrictions nécessite cependant de repenser totalement les méthodes de travail des équipes. Cela doit s'inscrire dans un contexte plus global de mise en place d'une culture de la sécurité dans l'entreprise. Pour que celle-ci soit un succès, tout l'écosystème (collaborateurs mais aussi prestataires) doit s'y conformer et la direction doit faire preuve d'exemplarité dans ce domaine.

Pour l'édition 2020 des Assises, l'espace startups accueillait huit entreprises qui ont eu l'opportunité de pitcher devant les professionnels de la cyber et de présenter leurs technologies. Cette année, une grande partie des solutions proposées partageaient un objectif commun: identifier et détecter plus rapidement et de manière plus exhaustive les menaces au sein d'un système d'Information, afin d'agir plus efficacement.

Ainsi **Cybernova** s'attaque aux problèmes des comptes à privilèges. La solution va se placer entre le service d'authentification et les outils de sécurité, et analyser les comportements des comptes à privilège, offrant un gain de temps et une visibilité accrue sur ces comptes très sensibles. Cette problématique de visibilité et de cartographie est ressentie comme un véritable besoin. **Bubo cybersec** cherche ainsi à offrir une première cartographie des comptes et des risques grâce à un dashboard qui vient se brancher directement sur un annuaire. Une solution plutôt adaptée aux petites entreprises. Dans la même veine, **Weakspot** propose une cartographie externe du SI pour visualiser en temps réel les secondary assets et le shadow IT, souvent difficile à détecter et monitorer. Grâce à une solution SaaS, il sera possible de surveiller en temps réel sa surface d'attaque. De son côté, **Sesame IT** propose une sonde réseau qui va analyser une copie des flux réseaux, et envoyer des alertes directement à un SOC ou même les afficher sur son propre dashboard.

De ces innovations en ressortent deux, qui cherchent à apporter leur contribution à la sécurisation du monde de demain : **Buster.Ai** (coup de cœur du jury du Prix de l'Innovation, cf. p.11) et **Cosmian**. Buster.Ai s'attaque à la propagation rapide de la désinformation grâce à des algorithmes poussés qui leur permettent de détecter des images ou vidéos modifiées voire générées, ainsi que du texte qui s'éloigne de faits vérifiés. Cosmian propose des solutions pour le traitement sur des données chiffrées, dans une optique de Zero-Trust, afin de permettre une collaboration avec des données mutualisées sans aucun déchiffrement, et donc garantissant la confidentialité des données.

Les deux autres startups présentes étaient Digitemis et Anozrway.

Olvid, Prix de l'Innovation 2020

Olvid, vainqueur du Prix de l'Innovation des Assises 2020, propose une solution de messagerie instantanée décentralisée qui se veut respectueuse des données.

Dans le segment des messageries instantanées, Olvid et sa messagerie éponyme font face à des solutions connues de tous comme WhatsApp, Telegram, WeChat ou encore Signal. « Le modèle de sécurité de toutes les messageries est basé sur un annuaire global. Les contacts de l'utilisateur sont comparés à cet annuaire et ce dernier retourne les clés publiques des contacts qu'il connait. En procédant ainsi, on se retrouve à faire confiance à un tiers pour la gestion des clés. Si le tiers se fait hacker, c'est toute la sécurité qui tombe » explique Matthieu Finiasz, Co-Fondateur d'Olvid.

La principale différence d'Olvid par rapport à ses concurrents est l'absence de tiers de confiance. Bien qu'il soit possible d'utiliser un annuaire d'entreprise dans la version payante, le modèle de sécurité d'Olvid est basé sur un échange de clé directement entre les utilisateurs. De plus, les algorithmes et propriétés cryptographiques utilisées, notamment Forward Secrecy, assurent qu'en cas de compromission, les communications passées ne peuvent pas être déchiffrées. Enfin, toutes les données étant stockées sur les terminaux des utilisateurs, Olvid n'a connaissance ni de l'identité de ses utilisateurs, ni de leurs données.

Certifiée CSPN par l'ANSSI, validée par l'IACR, éprouvée par des Bug Bounty et désormais vainqueur du Prix de l'Innovation des Assises 2020, Olvid est un compétiteur reconnu pour ceux qui placent la sécurité au cœur de leurs échanges numériques.

A l'heure où certains de ses concurrents se voient reprocher leur politique de gestion des données personnelles, le Français pourrait vite prendre une ampleur mondiale.

Trois questions à Julien Mardas

CEO de Buster.Ai

BUSTER.AI EN QUELQUES MOTS ?

Buster.Ai développe des algorithmes d'intelligence artificielle qui sont capables d'assister l'humain dans sa tâche de vérification de l'information. Nous ne nous prononçons pas sur un résultat (« vrai » ou « faux »), mais fournissons une matching evidence à partir de bases de faits. De là, nos algorithmes vectorisent le texte en encodant son sens, pour savoir à quelle distance nous sommes d'un fait. Ce sont beaucoup de mathématiques appliquées à l'informatique. Notre outil s'adresse aux médias, aux institutions gouvernementales ainsi qu'à tout professionnel de l'information ayant besoin de savoir si une information relève du signal, du bruit ou si un signal très faible cache une autre information plus importante..

COMMENT SONT CONÇUS LES OUTILS QUE VOUS PROPOSEZ ?

Nous avons tout développé en France, à base de solutions Open Source. Toute la technologie est maîtrisée en interne, avec des stacks, et des modèles d'intelligence artificielle très avancés.

Nous avons actuellement trois produits :

- **Un portail web** qui permet de faire des analyses et avoir une vue à 360 degrés sur l'état des cybermenaces liées à la désinformation dans le monde, avec une mappemonde en cours de développement.
- **Une extension de navigateur,** qui permet au moment de la navigation, sur Twitter notamment, d'identifier les images qui auraient été altérées et de confronter les textes à différents types de sources (officielles, médiatiques, scientifiques). Ces analyses sont aussi réalisables via notre API pour traiter tous les volumes.
- **Une API** pour analyser des contenus textes et multimédias à l'échelle.

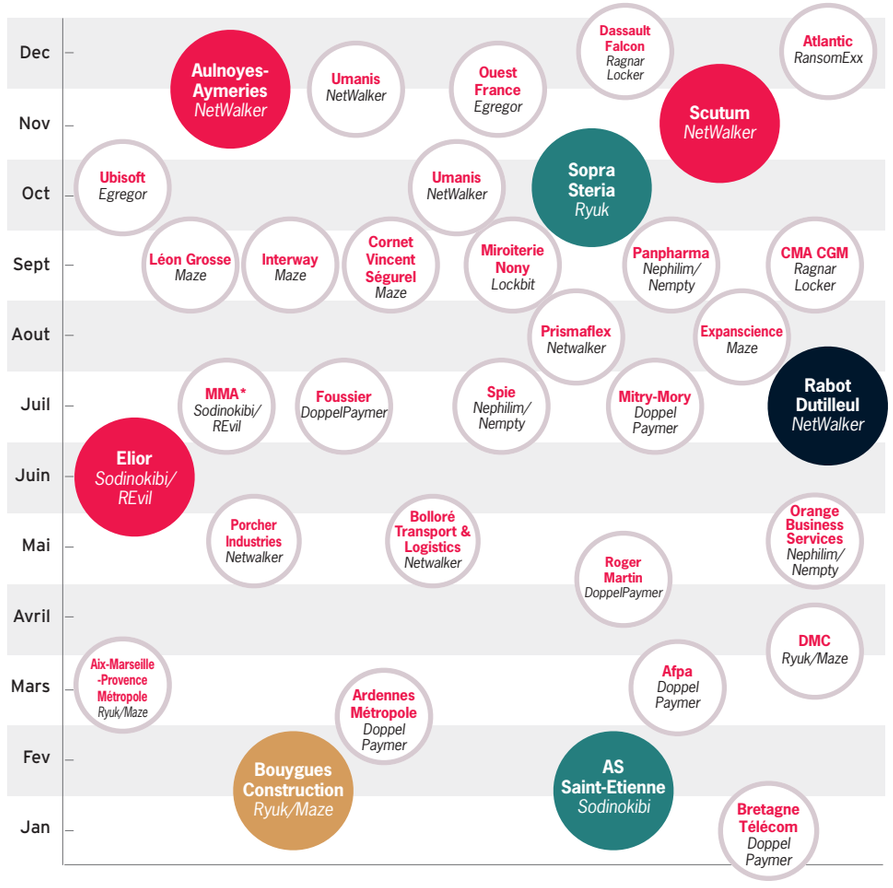
QUELLES SONT LES TENDANCES QUE VOUS AVEZ PU OBSERVER CES DERNIÈRES ANNÉES, NOTAMMENT AUTOUR DES TECHNOLOGIES DEEPFAKES ?

Nous avons vu des évolutions incroyables. Il y a deux cas qui sont clairement identifiables au niveau de la vidéo : le premier est une altération, via un réseau de neurones de type deepfakes, et le deuxième est une génération avec un GAN (Generative Adversarial Networks) d'une vidéo qui n'existait pas. Dans le premier cas, il est possible de faire dire à Donald Trump ou Emmanuel Macron des propos qu'ils n'ont pas tenus. Dans le second, on va par exemple générer des visages qui n'existent pas : en jouant sur le mouvement des lèvres avec les associations de parole, il est possible de générer une vidéo d'un faux visage qui dit tout et n'importe quoi !

RETOUR SUR 2020

// RANSOMWARES EN FRANCE EN 2020

L'année 2020 a donné lieu à une forte croissance des attaques de type ransomwares, avec certaines réclamant des rançons atteignant jusqu'à plus de 8 millions d'euros. En tout, plus de sept grandes entreprises ont rapporté une rançon de plus de 1 million d'euros, impliquant à chaque fois : **Ryuk**, **Maze** ou bien **NetWalker**. Une grande majorité des entreprises ne communique pas directement les montants des rançons, ce qui laisse supposer qu'elles pourraient elles aussi dépasser le million d'euros. Cette tendance semble se généraliser pour les entreprises françaises, qui doivent faire face à cette menace, qui présente un coût financier mais surtout réputationnel.

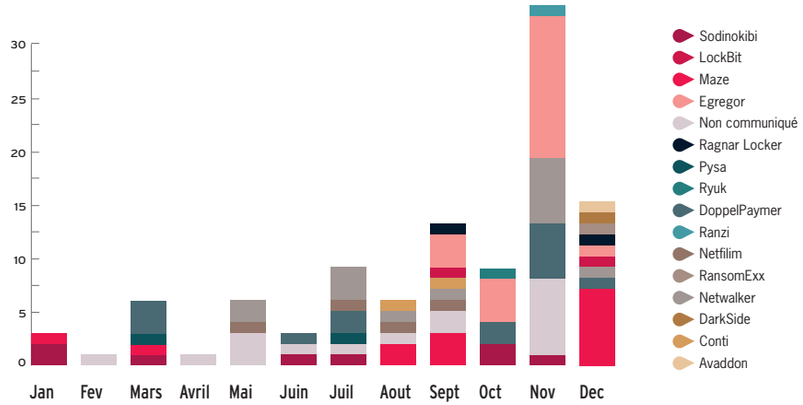


Graphiques réalisés sur la base des faits marquants identifiés par la presse

LES TEMPS FORTS DES ASSISES

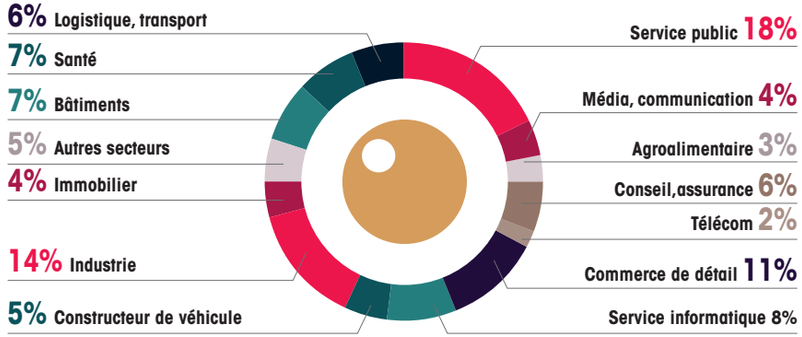
// RÉPARTITION DES ATTAQUES DE RANSOMWARES EN FRANCE EN 2020

La fin de l'année 2020 a été très touchée par de nombreuses attaques demandant des rançons. De septembre à novembre le rançongiciel **Egregor**, successeur notable de **Maze**, a fait grimper le nombre de victimes, dont Ouest-France fin novembre, mois le plus important en matière d'attaques. **NetWalker** s'est aussi imposé en France et a pris de l'ampleur dès juillet, qui aurait notamment touché MMA, géant de l'assurance. Ces attaques représentées ici ne sont que les cas connus, communiquées au grand public, et ne représentent peut être pas les véritables tendances en France.



// SECTEURS TOUCHÉS EN FRANCE EN 2020

Tous les secteurs sont impactés en France par les ransomwares. Et il ne semble pas s'y dégager de tendance discriminatoire. L'industrie et le secteur public semblent être davantage la cible de ce type d'attaque . Ces codes malveillants semblent ainsi s'attaquer à tout type de victime capable de verser une rançon dépassant le million d'euros, sans distinction du secteur, de l'entreprise ou de son statut.



Portrait du RSSI en 2021
l'acteur incontournable des métiers

Si la menace sur les systèmes d'information ne cesse de croître depuis des décennies, les responsabilités en matière de sécurité des systèmes d'information ont suivi une tendance parallèle, plongeant le RSSI dans un cycle d'évolution permanent. La fonction a gravi progressivement les échelons, jusqu'aux plus hautes instances décisionnelles.

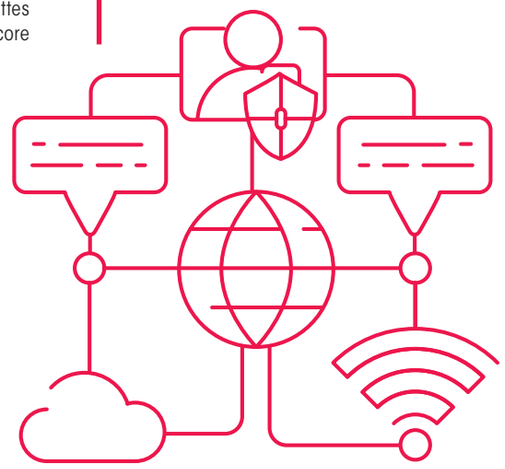
Mais peut-être a-t-il fallu la crise du Covid-19 et la vague de rançongiciels de 2019 et 2020 pour achever cette progression et hisser jusque dans les comités exécutifs ces hommes et femmes qui dans bien des cas ont joué un rôle critique dans la continuité, voir la survie du « business » pendant cette période. La résilience serait-elle la nouvelle compétence 2021 du RSSI ?

La fonction est de plus en plus englobante, et s'appuyait déjà sur de multiples domaines de compétences (stratégique, technologique, sociologique, juridique, en transformation d'organisation ou encore économique). Fort de cette diversité et de ces évolutions, le RSSI est devenu un acteur incontournable des métiers, un « business partner » à part entière. Une courroie au cœur des rouages d'une organisation.

Il doit pouvoir adapter son discours à tous les niveaux, être capable d'appréhender les enjeux et les risques, tout en recommandant des mesures acceptables. Ou encore traiter les crises et créer un environnement de confiance pour ces différents interlocuteurs et surtout le COMEX. La question du rattachement de ce mouton à cinq pattes anime encore la communauté. Le RSSI n'est pas encore systématiquement rattaché à la direction générale, mais pour combien de temps encore ? Dernier signe de cette évolution du RSSI ? De plus en plus de grandes entreprises font émerger une nouvelle fonction, celle de « Directeur de la Cybersécurité ».

Enfin une récente étude du CESIN montre d'ailleurs qu'actuellement 50% des RSSI sont âgés de 50 à 64 ans, ce qui va engendrer un nouveau challenge de recrutement, dans un secteur déjà sous tension mais va permettre en revanche l'émergence d'une nouvelle génération montante qui va devoir relever des défis et des enjeux toujours plus nombreux.

Une situation passionnante pour l'ensemble de ces professionnels du risque numérique, un défi pour les ressources humaines mais craignons-le « un puit sans fond ».



LE COVID & SES CONSÉQUENCES SUR LA SSI

La cybersécurité à l'heure du Covid-19

La crise du COVID 19 a accéléré la transformation numérique des entreprises et les a forcées à adopter de nouveaux modes de travail et de consommation afin d' assurer la continuité de leurs activités. Cette situation inédite a eu des conséquences majeures sur la sécurité des systèmes d'information (SI), notamment en raison d'une surface d'attaque grandissante.

De leurs côtés, les cybercriminels ont exploité pleinement le contexte en adaptant leurs méthodes et leurs narratifs aux événements. Ainsi, les techniques de social engineering, visant à exploiter la confiance de la cible sous toutes les formes ont été largement utilisées à des fins criminelles. Ces attaques ont été d'autant plus déstabilisantes que beaucoup d'organisations n'étaient pas préparées à un basculement soudain dans un mode de télétravail généralisé, passant de « l'entreprise étendue » à l'entreprise « atomisée ».

Au 2ème trimestre 2020, l'éditeur McAfee a observé une augmentation de 605 % des détections d'attaques liées au Covid-19 par rapport au premier trimestre

L'hygiène numérique joue un rôle encore plus capital dans ce nouvel environnement de travail.

La rapidité et la brutalité de la crise a pris tout le monde au dépourvu et pendant les Assises, nombreux ont été les échanges « d'expérience vécue » pour tenter d'en tirer de bonnes pratiques. D'après Bernard Ourghanlian, Directeur Technique et Sécurité chez Microsoft "les organisations qui ont le mieux géré la pandémie sont celles qui ont adopté une philosophie «Zero Trust», qui consiste à traiter chaque tentative d'accès comme provenant d'un réseau non-approuvé". Au contraire, "la plupart des entreprises ayant choisi de garder des moyens plus traditionnels tels que les pare-feu ou les VPN ont été plus sensibles aux menaces." (voir article page 8)

Un avis qui fait débat mais qui montre l'ampleur des enjeux rencontrés par les entreprises et les organisations pour passer dans cette nouvelle ère du numérique.

LE COVID ET SES CONSÉQUENCES SUR LA SSI

Table ronde Cesin

CESIN

COVID 19 – La réponse Cyber

Cette table ronde animée par le **CESIN** a choisi d'aborder les problèmes qui ont été soulevés par la crise et les leçons qu'il est possible d'en tirer.

Les répercussions de cette crise sanitaire s'annoncent profondes. Les entreprises sont fortement touchées sur le plan économique et doivent également veiller à ne pas subir de crise cyber. A cela s'ajoute le dimensionnement des réseaux qui est l'une des problématiques récurrentes. Cela se traduit notamment par l'élargissement des possibilités de connexion à distance.

En raison de la crise économique mondiale, le budget consacré à la cybersécurité, jusqu'ici en phase de croissance, connaît seulement un ralentissement. Les entreprises prenant peu à peu conscience de l'importance de protéger leurs actifs numériques

Noms de domaine réservés par millions contenant le mot "covid", multiplication des attaques de phishing, augmentation du nombre de cyberattaques liées aux cryptolocker... un constat important qui induit une importante charge de travail du côté de la défense : "Aujourd'hui le modèle économique est clair, c'est essentiellement de la cybercriminalité", déclare Philippe Loudenot, ancien FFSI au Ministère des Affaires sociales.

Pour agir efficacement, la maîtrise de la temporalité est primordiale. En effet, il est important de remonter au plus vite les incidents de sécurité : lors de l'attaque contre le CHU de Rouen par exemple, la gestion a été rapide et efficace grâce à une très bonne réactivité.

Cependant, de nombreux points positifs sont à tirer de la pandémie. Une "cyber solidarité" des éditeurs/constructeurs qui ont proposé leurs services pour aider les structures de santé est à noter. D'autre part, la crise a permis la généralisation du MFA (Multi Factor Authentication) qui n'était pas commun au sein des organisations. Ainsi, malgré l'impact économique de la crise sur les entreprises, la pandémie a tout de même entrainé une accélération de la transformation numérique des entreprises.

SOUVERAINETÉ

Atelier Datadome

DATADOME

Avec le confinement et l'accélération du numérique tant pour les usages personnels que professionnels, les attaques se sont multipliées. Beaucoup d'entre elles provenaient de **"bad bots",** ou **robots malveillants** qui représentent une véritable menace pour certaines entreprises, notamment les sites d'e-commerce, de voyages et de petites annonces.

Cet atelier a été l'occasion de faire un rappel du phénomène et de voir s'il est possible d'y faire face. En effet, aujourd'hui, ces systèmes automatisés sont très sophistiqués, capables d'imiter le comportement d'un humain, en utilisant de véritables appareils et des adresses IP de bonnes réputations. Ainsi, il est difficile de les combattre avec les méthodes utilisées jusqu'alors (pare-feu avec règles statiques, filtrage de trafic). Ces robots représentent un manque à gagner conséquent pour une entreprise s'ils ne sont pas détectés et bloqués.

On observe différentes attaques, partant du DDOS au scraping de site d'e-commerce, en passant par la réservation en masse de paniers factices, compromettant la disponibilité de certains articles. Certains bots peuvent aussi réaliser des attaques par force brute d'informations bancaires, en réalisant des requêtes de paiement répétées. Tout ceci peut engendrer des coûts supplémentaires pour les entreprises. Datadome constate que 10% du chiffre d'affaires réalisé en ligne est perdu à cause de ces bots.

Datadome propose une solution avec un moteur d'analyse du trafic, de détection et de filtrage en temps réel. Le modèle est fondé sur du machine learning et mutualise les informations pour la détection de bad bots sur l'intégralité du globe. Ainsi, Datadome dit détecter, toutes les 10 millisecondes en moyenne, une nouvelle empreinte de ces systèmes automatisés, qui est ajoutée à sa base de connaissances pour la détection de trafic malveillant.

Atelier Orange

orange™

Cyberdéfense

Cet atelier a été l'occasion pour Orange Cyberdefense de montrer l'efficacité du micro-SOC

→ **Contexte**

Les méthodes d'attaque ont évolué notamment pendant les confinements. Une solution face à ce problème pourrait être la mise en place de micro-SOC. Celui-ci est dérivé du SOC traditionnel dont la spécificité est de se focaliser sur la détection d'un unique type de menace en adoptant un périmètre de surveillance bien précis.

→ **Méthode**

Il est généralement observé un délai important entre le moment de l'infection et celui où la charge active est déployée. Il existe un besoin d'analyser ces comportements et de les détecter, pour pouvoir endiguer au plus vite les machines contaminées. Le temps de réaction est ainsi réduit grâce à l'optimisation du temps de détection par l'action du micro-SOC.

→ **Mise en œuvre**

Dans le micro-SOC, des campagnes de phishing peuvent être proposées afin d'identifier les personnes auprès desquelles la sensibilisation est particulièrement importante ou dont les postes de travail nécessitent une surveillance particulière. Dans un second temps, la sensibilisation pourra être adaptée aux différentes populations de l'entreprise ce qui est d'autant plus important dans le contexte du télétravail général où les équipes sont séparées physiquement.

La notion de **souveraineté** au coeur de tous les débats

La crise du Covid-19, au-delà de l'aspect sanitaire, a testé dans des conditions extrêmes et planétaires, les dépendances de toutes les organisations. Ce stress test grandeur nature, a mis en lumière la dépendance aux solutions et fournisseurs étrangers.

D'un point de vue matériel, ce sont les chaînes d'approvisionnement qui sont maintenant au cœur de réflexion sur l'autonomie stratégique et le risque systémique pour une organisation.

Consécutivement à la crise sanitaire et économique, les organisations ont basculé des pans entiers de leur activité vers le numérique et accéléré significativement la migration de services vers le cloud. L'émergence de nouveaux usages tel que le télétravail et l'évolution des modes de consommation a entraîné un effet de concentration sur certains acteurs.

Les services en ligne collaboratifs, les réseaux sociaux d'entreprise, les systèmes de communications unifiées essentiellement non-européens ont cristallisé ces débats sur la souveraineté. Avec à la clé, des questions sur la gestion des données personnelles et d'entreprise, sur la sécurité des échanges en visioconférence ou sur l'hébergement des données de santé.

La notion de souveraineté, voire d'autonomie stratégique, s'étant invitée dans tous les débats nationaux et internationaux pendant la crise du COVID-19, les États et les sociétés ont dû accélérer leurs compréhensions de la problématique.

Cette situation a été aussi révélatrice de la nécessité d'une souveraineté, française, mais aussi à une plus grande échelle, probablement européenne. GAIA-X est une de ces nombreuses initiatives lancées en 2020.

Mais au-delà du constat, plusieurs questions restent aujourd'hui encore ouvertes. Les états membres ont-ils les compétences techniques nécessaires ? Les entreprises sont-elles capables de rivaliser avec leurs concurrentes étrangères, avec un cadre adapté ? La géopolitique et ses enjeux sont-ils correctement appréhendés par tous ?

Beaucoup d'interrogations qui ont alimenté les débats lors de cette 20ème édition des Assises et qui resteront encore au cœur de l'actualité 2021.

Table ronde
Le Cybermonde, un enjeu géopolitique

4 experts renommés intervenaient sur cette table-ronde : **Frédérick Douzet** (professeure de géopolitique et Directrice de Geode), **Loïc Guézo** (Directeur en stratégie cybersécurité et Administrateur du Clusif), **Julien Nocetti** (enseignant à l'école de St Cyr\Coëtquidan et chercheur associé à l'IFRI) et le Général **Didier Tisseyre** (commandant de la cyberdéfense).

Lors de ce débat, les intervenants ont pu exposer leurs points de vue sur les enjeux actuels et géopolitiques du cybermonde, notamment avec un échange sur le concept de « cyber puissance ». Cette table ronde a ainsi abordé les capacités offensives et défensives, la structure mise en place afin de pouvoir utiliser pleinement ces capacités et la gouvernance de ces moyens, des doctrines et du nécessaire cadre juridique aidant à déterminer comment caractériser et agir dans le cyberespace.

Une « cyber puissance » se doit aussi d'avoir une industrie du cyber qui lui permette d'assurer son autonomie stratégique et la capacité de combiner le cyber avec des opérations plus conventionnelles.

De son côté, le cyberespace apparait comme un terrain touché par plusieurs conflictualités et notamment la guerre de l'information en plein essor. Le tournant noté lors de la table ronde fut l'élection américaine de 2016, où depuis cette époque circule une crainte d'ingérence dans toutes les élections.

La stratégie nationale française met en valeur l'importance d'une stricte séparation entre offensif et défensif, et accorde un effort important au volet défensif via l'ANSSI. L'arme cyber est une arme d'emploi, grandement utilisée par les états dans l'ensemble des conflits modernes, notamment pour la France au Sahel et au Levant.

Dans ce contexte, le cyberespace est devenu un terrain d'affrontement entre une multitude d'acteurs (étatiques ou non) utilisant de nombreux outils cyber qui peuvent être volés puis réemployés par des cybercriminels Cette prolifération mène donc à une montée en compétences de ces criminels qui menacent alors la stabilité du cyberespace et des entreprises. La table-ronde a débattu de l'importance de la coopération, et l'adoption de règles de comportement propres au cyberespace. Ces questions sont aujourd'hui au cœur des rivalités entre les différentes puissances.

Le cyberespace a ouvert un espace, permettant des actions d'état, que certains nomment hybrides, jouant sur l'ambiguïté civilo-militaire et l'application du droit international.

Concernant le renforcement de la coopération, la mise en place en Europe du réseau de coopération CyCLONe (Cyber Crisis Liaison Organization Network) est un bon exemple de cette montée en puissance européenne, sans oublier les principes de la directive NIS et le travail de ces instances comme l'ENISA. L'Appel de Paris de novembre 2018 est un autre exemple d'une vision ambitieuse pour la stabilisation du cyberespace.

Table ronde

Bâtir et promouvoir une souveraineté nationale et Européenne

Les Assises ont accueilli Philippe Latombe, Député de Vendée, et Jean-Michel Mis, Député de la Loire respectivement Rapporteur et Vice-Président de la mission d'information parlementaire **« Bâtir et promouvoir une souveraineté numérique nationale et européenne »** venus présenter les objectifs et les premiers travaux de cette mission parlementaire. Comme le note Philippe Latombe, il s'agit de construire une réglementation minimale et efficace qui viendra s'intégrer directement au sein de projets de loi.

La notion de souveraineté étant complexe à définir, les Etats membres de l'Union devront s'accorder sur une définition commune. Il s'agira de ne pas tomber dans l'isolationnisme, tel qu'il est pratiqué en Chine, ni dans une démarche hégémoniste à la manière des Etats-Unis, mais simplement, selon Philippe Latombe, d'être en mesure d'opérer ses propres choix lorsque la France en aura besoin.

Cette mission n'a pas pour vocation l'élaboration de nouvelles solutions, mais bien celle de créer une situation propice à l'élévation des entreprises françaises déjà à l'état de l'art afin de les amener sur le marché européen. Pour ce faire, les ETI et PME ont surtout besoin de commandes importantes et sur le long terme. Cela passe, entre autres, par l'élaboration d'appels d'offre plus ciblés, taillés sur mesure pour les entreprises hexagonales, à l'instar de ce que font certains de nos voisins européens comme l'Allemagne.

Malheureusement, et malgré l'invalidation du Privacy Shield par la cour de justice européenne, certaines décisions récentes ne semblent pas aller dans la direction souhaitée. Les deux députés notent ainsi la mise en place du Health Data Hub avec Microsoft, les accords entre Palantir et la DGSI ou encore entre BPI France et AWS.

Il ne faut plus tomber dans la facilité de notre prudence culturelle, mais "retrouver cette capacité à être audacieux dans la commande publique" selon Philippe Latombe, et cela passera par la réalisation, sur un temps long, de cette mission parlementaire dont la première version est attendue à la fin juin 2021.

TENDANCES

Atelier
Cybereason

cybereason

Pourquoi est-ce compliqué de détecter une attaque ?

Les solutions de cybersécurité déployées dans les organisations restent encore trop centrées sur des fonctionnalités de protection, telles que des firewalls ou des outils de gestion de correctif de sécurité, sans porter un effort aussi conséquent sur les capacités de détection de cyberattaque. Ce qui reste assez paradoxal, au regard de la prise de conscience généralisée qu'une cyberattaque réussie surviendra tôt ou tard.

Les gains potentiels, les moyens et la volonté d'attaquants dorénavant très organisés ne sont plus à démontrer. Malheureusement la détection reste une activité complexe à mettre en œuvre, dont les résultats opérationnels sont aujourd'hui perfectibles surtout pour la détection de comportements anormaux. Véritable critère d'ambition, de performance, tout en étant très spécifique à chaque organisation, le temps de détection d'une cyberattaque est devenu un enjeu majeur.

Toutefois il reste difficile, même pour des personnes qualifiées et équipées d'outils de détection industriels, de gérer la totalité des évènements de sécurité. Il est donc nécessaire de toujours rechercher l'amélioration de la précision de la détection et d'augmenter la capacité afin d'atteindre les objectifs attendus.

La méthode choisie par Cybereason est l'utilisation du machine learning ainsi que la corrélation de toutes les données collectées, afin d'être capable de déduire un contexte derrière chaque évènement. Ce type de solution permet de reconnaître certaines caractéristiques irrégulières ou au contraire des caractéristiques d'attaques connues, mais aussi de les lier les unes aux autres afin de vérifier leur cohérence. Il devient alors possible de faire remonter non seulement une alerte mais aussi un déroulé ou la trajectoire prise par l'attaque: les machines infectées, la méthode d'intrusion ou les comptes compromis.

La solution proposée par Cybereason se base sur trois piliers :

- **Une protection des terminaux** (end point) : des outils de préventions basés sur l'EDR pour fournir du contexte et de la visibilité aux administrateurs ;.
- Des **capacités d'analyse** et de caractérisation avancée ;
- Une approche analytique pour permettre de remonter l'**information en temps réel.**

Avec l'utilisation de graphes et du machine learning, il devient possible de traiter les informations ainsi récoltées, afin d'en déduire de potentiels comportements anormaux.

Table ronde
Zero Trust

Cette table ronde sur laquelle intervenaient Thierry Auger (CSO Deputy et CISO du groupe Lagardère), Gilles Berthelot (RSSI Groupe SNCF) et Nicolas Ruff (Security Engineer) a été l'occasion de comprendre - à la lueur des enseignements de ces derniers mois - **en quoi le Zero Trust amène à repenser la cybersécurité.**

D'abord qu'est-ce que le Zero Trust ? Une philosophie ? Ou au moins, un concept qui vise à s'assurer que toute personne tentant de se connecter sur un système d'information est une personne dont l'identité est vérifiée à chaque connexion. Il ne s'agit pas d'un outil, ni d'une technologie mais bien de principes qui nécessitent des changements fondamentaux dans la manière de concevoir les réseaux ainsi que l'architecture des systèmes d'information. Plus qu'une simple authentification, c'est une gestion d'identité permettant l'exposition des services nécessaires sur internet en toute sécurité. Car le nombre d'appareils déployés sur un réseau croît constamment et la redirection de tous ces flux par un VPN au sein de l'entreprise est coûteuse et peut s'avérer dangereuse. En clair Zero Trust vise à utiliser toutes les données à disposition pour contextualiser la connexion et la rendre légitime.

Bien que cette approche ne soit pas nouvelle, la situation sanitaire due au COVID-19 a accéléré le déploiement de ces architectures. Cela s'explique par une observation effectuée durant la pandémie : les infrastructures d'accueil des employés à distance étaient sous-dimensionnées par rapport au nombre d'utilisateurs en raison de la généralisation du télétravail. Or la mise en place d'une architecture Zero Trust permet de pallier cela, en plus de rajouter une couche de sécurisation par l'authentification forte. Aussi, rediriger les flux par l'intérieur pour accéder à un service depuis l'extérieur n'est plus nécessaire, les partenaires et prestataires de l'entreprise bénéficient aussi de ces avantages.

La gestion de l'identité est un paramètre vital au Zero Trust, puisqu'il est nécessaire de s'assurer que la personne soit correctement authentifiée, qu'elle est bien celle qu'elle prétend être, que son poste ne soit pas compromis, et qu'elle ait les bons droits avant de se connecter à un service. Ainsi en utilisant les données pour créer un contexte et rendre une connexion légitime, nous pourrions bien voir de nouvelles techniques d'authentification émerger grâce au Zero Trust.

Zero Trust,
Cryptographie et IA en première ligne

Le cyberespace est en constante évolution et la menace ne cesse de croître. 2020 sera toutefois l'année d'une généralisation des victimes, cibles d'une cybercriminalité décomplexée et agressive, aux techniques de plus en plus sophistiquées.

Les modes de défense doivent évoluer, restant à ce jour encore trop souvent dans une posture réactive basée sur l'identification de nouvelles vulnérabilités et l'ajustement des solutions.

Néanmoins, des tendances jusque-là émergentes, semblent avoir passées un nouveau cap pour tenter de remédier à la situation.

Lors des Assises, trois d'entre elles se sont distinguées :

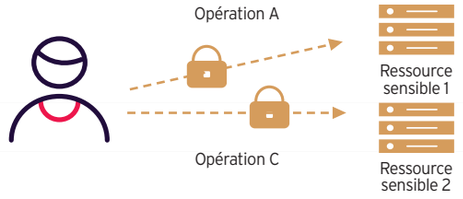
- Le concept de Zero Trust, qui vise à repenser complètement la notion de confiance, d'identité et d'autorisation au sein d'un système d'Information, en rendant potentiellement obsolète les paradigmes de zones sécurisées (VPNs, zones démilitarisées). De nombreux cloud providers intègrent aujourd'hui des technologies Zero Trust dans leurs produits, témoignant de l'importance de cette approche.
- Les nouvelles solutions de cryptographie, notamment homorphiques offrant des possibilités de mutualisation de données, ou des algorithmes résistants au calcul quantique. Certains acteurs, tels que Cosmian donnent un accès aux dernières avancées en cryptographie.
- L'usage de l'intelligence artificielle pour la défense des systèmes d'information. Même si l'IA reste un sujet de recherche et d'investissement, l'intégration dans les produits de sécurité commence à produire de véritables solutions. Les outils de threat hunting intelligent de Cybereason souligne cette tendance, par exemple à travers la combinaison de l'intelligence de l'analyste et l'intelligence artificielle pour détecter rapidement et réagir à une menace.

Dans un contexte compliqué, avec une surface d'attaque grandissante - suite aux conséquences de la pandémie - et des vagues de rançongiciels en forte croissance, ces tendances vont-elles s'imposer? Difficile de le dire mais elles présentent aujourd'hui de sérieux espoirs.

// LEAST PRIVILEGE ACCESS

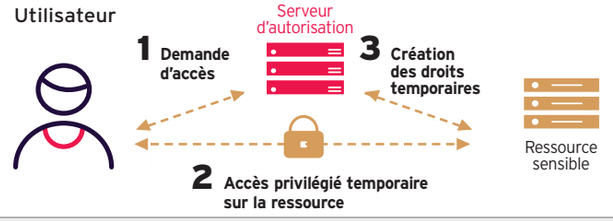
Fonctionnement et avantages du principe de moindre privilèges (LeastPrivilege Access)

Définition de l'ANSSI
«Le principe de moindre privilège stipule qu'une tâche ne doit bénéficier que des privilèges strictement nécessaires à l'éxécution du code menant à bien ses fonctionnalités. En d'autres termes, une tâche ne devrait avoir la possibilité de mener à bien que les actions dont l'utilité fonctionnelle est avérée.»
Source : ANSSI

Besoins	Utilisateur	Accès classique
✓ Droit A, 2 ✗ Reste Droits ✓ Tous		✗ Accès classique ✗ Permissions excessives ✗ Droits non granulaires ✗ Aucune mitigation en cas de compromission
Besoins	**Utilisateur**	**Accès Least Privilege**
✓ Droit A, 1 ✓ Droit C, 2 ✗ Reste Droits, ✓ Droit A, 1 ✓ Droit C, 2 ✗ Reste		✓ Droits alignés sur les besoins ✓ Granularité et traçabilité ✓ Impact limité en cas de compromission ✓ Approche **Zero Trust**

// JUST IN TIME ACCESS (JIT)

Fonctionnement et avantages de l'accès Just in Time au sein d'un SI d'entreprise

Utilisateur	Accès classique
	✗ Privilège contant ✗ Accès non granulaire ✗ Révocation non-immédiate
Utilisateur	**Accès Just in Time**
	✓ Privilège temporaire ✓ Accès fin et granulaire ✓ Révocation immédiate ✓ Approche **Zero Trust**

L'alpha d'une nouvelle ère ?

Si la crise sanitaire et économique a marqué définitivement les esprits en 2020, ce fût aussi l'année d'une accélération sans précédent, voire même inimaginable jusqu'alors, pour la transformation numérique des organisations. Nouveaux usages, transformations en profondeur de la Société ou encore regains d'intérêt pour les questions de souveraineté, ont rythmé le numérique en 2020.

Facteur d'opportunités et de développement, mais aussi par besoin de résilience, cette évolution presque darwinienne ne doit pas faire oublier son cortège de faiblesses et de menaces qu'elle a fait émerger dans son sillage.

Parmi ces conséquences, on soulignera :

- l'augmentation de la surface d'exposition des systèmes d'information, par un déploiement accéléré parfois mal maitrisé de nouveaux services, pour répondre en urgence à ce contexte sanitaire et économique ;
- l'explosion des rançongiciels ou des cyberattaques indirectes sur l'écosystème (via la « supply chain », les éditeurs logiciel ou encore les fournisseurs de services numériques) ;
- l'ambivalence d'une ère de l'information rythmée par des médias sociaux. L'environnement informationnel a définitivement muté avec cette crise creusant ainsi de véritables défis sociétaux. L'information couplée aux média sociaux, comme arme de déstabilisation massive, n'est définitivement plus un phénomène émergent.

Il est aussi intéressant d'avoir un regard particulier sur l'affaire SolarWinds. Cette cyberattaque d'ampleur concluant l'année 2020, sera un élément majeur à suivre en 2021. Elle fera probablement évoluer la prise de conscience de ce type d'attaque au niveau politique et économique, et de ses conséquences. Renforcement de la régulation, ou encore nouvelles normes de comportement dans le cyberespace seront peut-être de nouvelles pistes ouvertes par cette affaire hors norme, dont les conséquences animeront certainement une partie de l'actualité cyber.

Sebastien Bombal,
En charge du pôle stratégie du ComCyber, Ministère des Armées

Une perspective d'un omega ?

Définitivement les métiers du domaine ne cesseront d'étonner chaque année par cette nécessité permanente d'anticipation et d'adaptation même aux scénarios les plus improbables. La cybersécurité est un puits sans fond. Le régime de croisière semble inatteignable tant la menace, le domaine et le milieu évoluent continuellement. Nous n'avons pas encore vu tout l'alphabet CYBER, et ce ne sera pas pour demain.

Les défis concernant les ressources humaines, tout comme les efforts en matière protection, de résilience et de détection restent des priorités pour de nombreuses organisations, sans oublier la résolution difficile de l'équation de la souveraineté.

Les étudiants de l'école d'ingénieur à l'EPITA dans la majeure Système Réseau et Sécurité ont mené un effort de prospective sur le dernier trimestre 2020, à travers de nombreux entretiens menés aux Assises de la cybersécurité et avec des partenaires dans un contexte difficile. Il n'y a pas de cybersécurité sans partenariats et échanges, et la communauté et son édition des Assises 2020 a permis un de ces rares moment-clé d'échange et de convivialité, riche en partage d'expériences.

Ainsi je tenais à remercier toute l'équipe des Assises, et particulièrement Florence Puybareau et surtout les étudiants de l'EPITA, qui ont permis la réalisation de cette troisième édition du livret, fruit de ce travail prospectif.

« Une école d'excellence pour répondre aux besoins croissants de cybersécurité»

Joël Courtois
Directeur général de l'EPITA

Les Assises constituent chaque année un moment fort dans le monde de la Cybersécurité.

L'EPITA est très fière de ce Partenariat avec les Assises qui, dans un sens, donne la possibilité à ses étudiants de s'immerger dans l'écosystème quelques mois avant la fin de leurs études et, en retour, offre à tous les acteurs des Assises un ouvrage de synthèse sur la Cyber et l'Innovation. Ce partenariat s'inscrit dans le programme ambitieux de l'école en termes de développement de ses formations et de son activité de recherche dans la cybersécurité.

La majeure cyber de l'EPITA (SRS), labellisée SecNumEdu par l'ANSSI, est l'une des spécialisations du diplôme d'ingénieur de l'école parmi les plus reconnues par les professionnels de la sécurité.

Son centre de formation professionnelle continue, SECURESPHERE by EPITA, propose des formations courtes ou longues, certifiantes ou diplômantes, en français ou en anglais, en présentiel ou en distanciel, et est sollicité aussi bien par les professionnels du secteur que par toutes les entreprises souhaitant renforcer leur protection aux risques cyber.

Déjà membre actif du Pôle d'Excellence Cyber (PEC) l'EPITA a décidé de rejoindre le programme du Campus Cyber de la Défense, futur lieu totem de la cybersécurité française, ce qui va lui permettre à partir de septembre 2021 de renforcer ses activités de recherche et de compléter son offre de formation, en partenariat avec les membres du Campus, par un nouveau programme de Bachelor en Sécurité du Numérique.

Une actualité riche pour répondre aux besoins toujours croissants dans ce domaine essentiel de la cybersécurité, pour le développement d'un climat de confiance dans un monde de plus en plus numérique.

Alors, merci pour sa confiance à toute l'équipe des organisateurs de ce grand évènement que sont les Assises, et en particulier à Florence Puybareau, merci à Sébastien Bombal qui malgré ses responsabilités professionnelles continue d'animer la majeure SRS, et toujours dans la recherche de l'excellence, et merci aux étudiants de l'EPITA qui résistent aux attraits de l'environnement des Assises pour se donner à fond dans la préparation de ce livre blanc.

Un partenariat solide et dans le temps

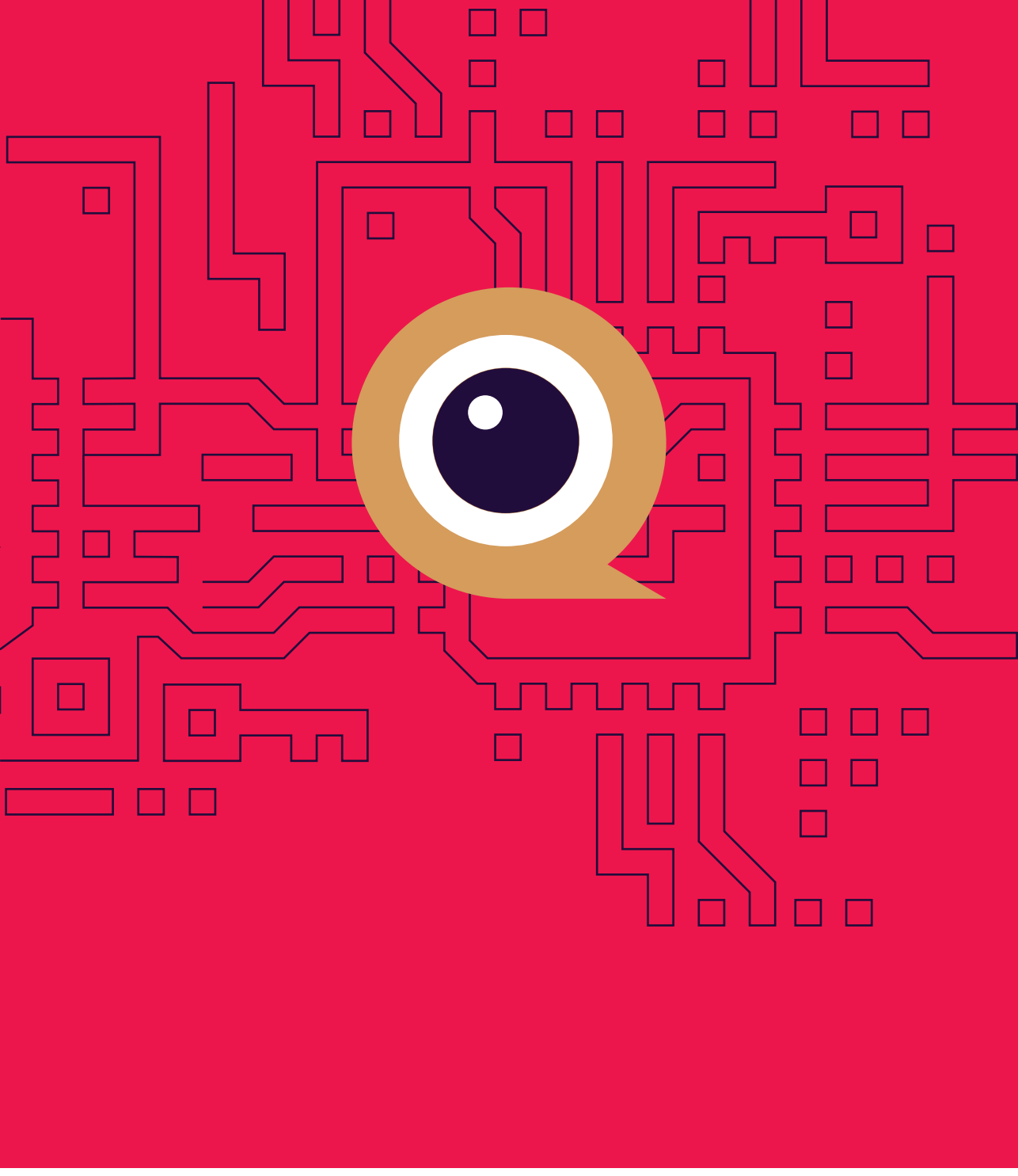
La troisième édition de cet ouvrage recèle plusieurs motifs de satisfaction. D'abord parce qu'il est l'émanation des Assises de la cybersécurité qui ont pu se tenir en présentiel malgré tous les aléas que nous avons connus. Avec quelques mois de recul, l'organisation de cet événement reste encore aujourd'hui un moment fort et nous pouvons remercier les visiteurs et partenaires qui nous ont fait confiance et qui étaient présents pour partager ce grand-rendez-vous de la cybersécurité.

Satisfaction aussi car l'innovation était au rendez-vous : conférences, ateliers, keynotes, tables-rondes, One-to-one… : les échanges furent variés, nombreux, riches, à l'image du secteur, en plein ébullition et qui ne cesse d'évoluer et de monter en maturité. Le startup Corner en est l'un des exemples. De même que les « démos » techniques et autres discussions technologiques entre experts qui ont ponctué les trois jours de Rencontres. Les enjeux pointés lors des Assises montrent que le binôme « Cybersécurité et Innovation » va conserver toute son actualité pendant encore de nombreuses années.

Satisfaction enfin car ce livre est le fruit du partenariat solide qui existe entre les Assises de la cybersécurité et l'EPITA. C'est grâce à la confiance de cette grande école d'ingénieurs, à l'engagement de Sébastien Bombal, au travail des élèves de la majeure Système Réseau et Sécurité que nous avons pu mener à bien ce travail. Je les en remercie et je nous souhaite de pouvoir en réaliser encore beaucoup d'autres.

Bonne lecture

Florence Puybareau
Directrice des Contenus et de la Communication, DG Consultants



DG CONSULTANTS @Les_Assises @Les_Assises #AssisesSI COMEXPOSIUM

www.lesassisesdelasecurite.com