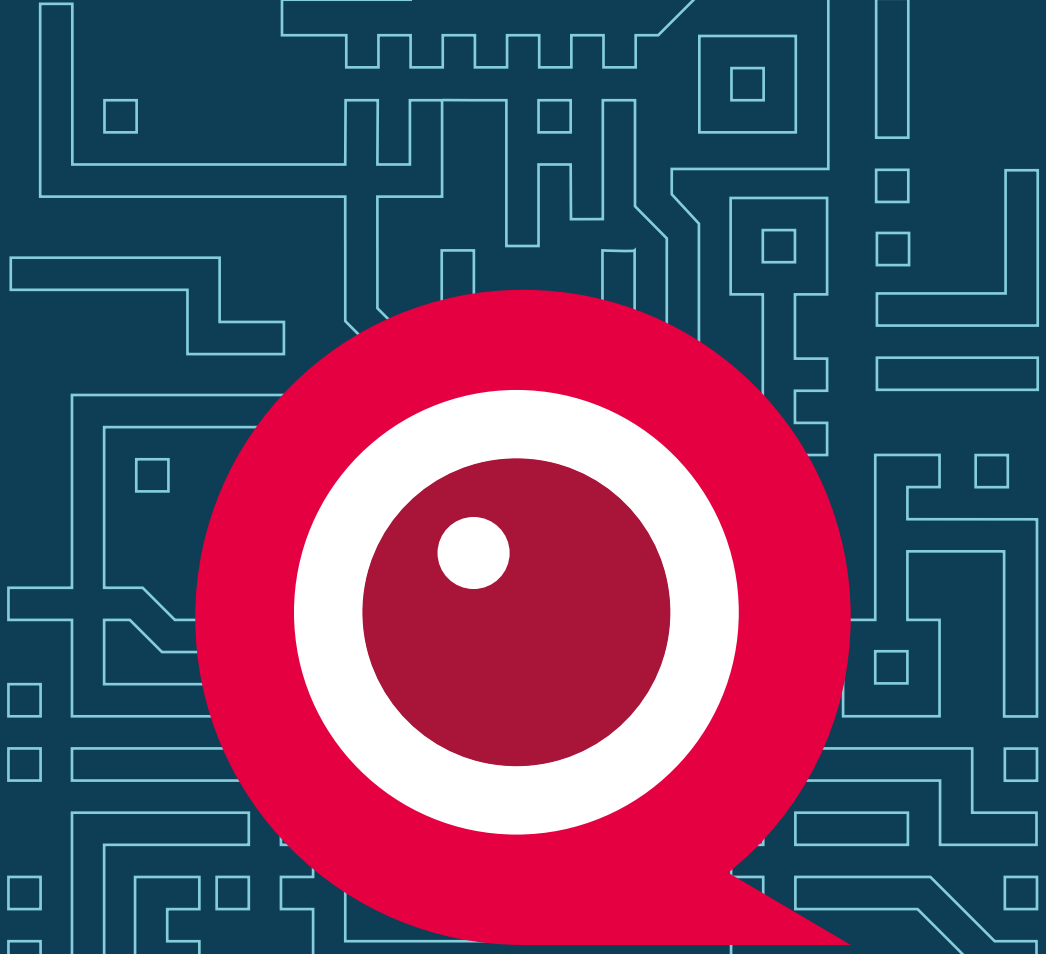


CYBERSÉCURITÉ & INNOVATIONS

ÉDITION 2022

Le regard des Assises et de l'EPITA

LES ASSISES

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

SOMMAIRE

CHIFFRES CLÉS DES ASSISES 2022

9400 rendez-vous one to one

3000 participants

175 ateliers tables rondes et conférences

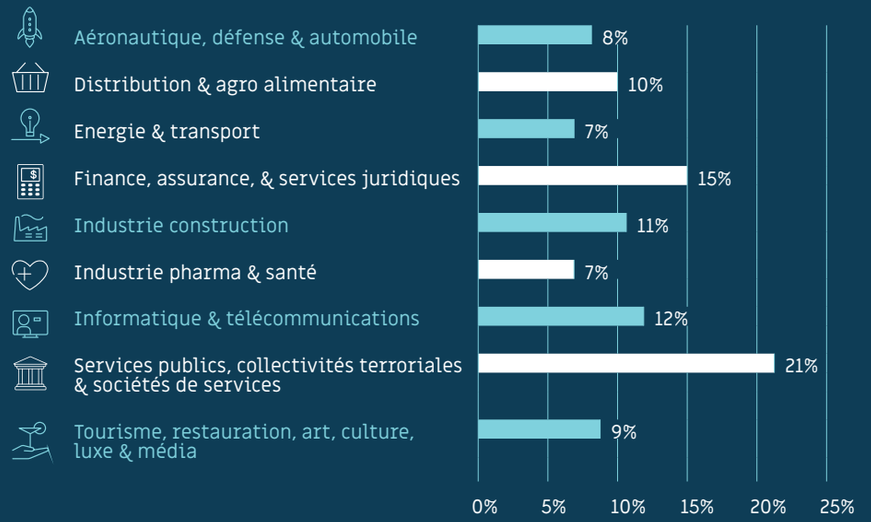
INVITÉS **1350**

164 SOCIÉTÉS PARTENAIRES

STARTUPS **20**

120 EXPERTS & JOURNALISTES

LES INVITÉS PAR SECTEUR



LES INVITÉS PAR FONCTION

/// TROIS QUESTIONS À SABRINE GUIHÉNEUF, *Présidente des Assises 2023, RSSI du groupe URW ; administratrice du Cesin ,Diplômée de l'Epita (Promo 2013)*

1/ POUVEZ VOUS NOUS DIRE QUELQUES MOTS SUR VOTRE PARCOURS ET POURQUOI LA CYBER ?

Après le Bac, j'ai rejoint la classe préparatoire intégrée de l'EPITA puis j'ai suivi le cycle ingénieur en me spécialisant sur la majeure « Système, Réseau, Sécurité » (SRS). La cyber m'a très tôt intéressée car ça me semblait mystérieux, et j'ai voulu comprendre concrètement comment il était possible de pirater un système et surtout comment s'en prémunir. Au travers de mes recherches puis de ma formation, j'ai découvert que ce secteur est extrêmement riche et qu'on ne s'y ennuie jamais. Cela a été une évidence.

2/ QUELS POSTES AVEZ VOUS OCCUPÉ AVANT CELUI, ACTUELLEMENT, DE RSSI DU GROUPE URW ?

A la sortie de l'école, j'ai occupé des postes de consultante en cybersécurité, d'abord chez Devoteam puis Lexsi. J'ai ensuite intégré le groupe Unibail-Rodamco en 2017 au poste de RSSI, qui était à l'époque une création de poste. Par la suite, l'entreprise a évolué avec l'acquisition de Westfield en 2018, et j'y ai occupé la fonction de RSSI Europe, puis RSSI du Groupe URW en 2019. Depuis 2021 j'ai en charge la cybersécurité et la gouvernance IT au sein du Groupe.

3/ COMME PRÉSIDENTE 2023, VOUS AVEZ CHOISI LA PUNCHLINE, « PRENONS DE LA HAUTEUR ». POURQUOI CE CHOIX ?

Dans la continuité des éditions précédentes, durant lesquelles nous avons revu nos fondamentaux (en 2021) puis avons accéléré (en 2022), je pense qu'il nous faut aujourd'hui poser le stylo et prendre de la hauteur pour regarder nos problématiques sous de nouveaux angles. Cela nous permettra d'en sortir plus fort et mieux préparé face aux évolutions technologiques et aux menaces toujours plus fortes. Prendre de la hauteur aide également à élargir le débat sur des sujets qui ne sont pas fortement liés à la cyber, et qui peuvent enrichir la communauté dans son ensemble.

CONFÉRENCE D'OUVERTURE

Guillaume Poupard,
Directeur Général de l'ANSSI

Changer d'échelle pour élever collectivement notre niveau de cybersécurité

Pour sa dernière intervention aux Assises de la cybersécurité en tant que Directeur Général de l'ANSSI, Guillaume Poupard a choisi de concentrer son discours sur les enjeux à venir. Et d'insister sur le fait qu'il est primordial « de changer d'échelle pour élever collectivement notre niveau de cybersécurité ». Pour parvenir à cela, il faut faire en sorte que chacun « soit en mesure de se protéger et puisse recevoir la protection qui lui est dû. » Que ce soit une entreprise du CAC 40, une PME, une collectivité locale ou un simple citoyen, chacun est concerné et doit trouver des solutions adaptées à sa situation. Cela passe par plusieurs mesures à commencer par les réglementations qui de l'échelle européenne doivent être transposées au niveau national à l'instar de la directive NIS2.

La prévention bien sûr reste essentielle notamment dans les petites entreprises et les collectivités. Pour ces dernières, Guillaume Poupard a dévoilé un nouveau service « MonServiceSécurisé » qui a été lancé officiellement le 13 décembre 2022 et vise à faciliter la mise en conformité des téléservices au référentiel général de sécurité.

S'il a souligné que dans cette démarche, la protection de l'industrie restait également un point d'attention grâce aux nombreux référentiels (PASSI, PDIS...) qui arrivent à maturité, c'est sur la notion de Cloud de Confiance que Guillaume Poupard a particulièrement insisté « nous sommes dans un système où les entreprises doivent choisir leur camp entre ceux qui voudraient que tout soit fabriqué en France et ceux pour qui tout est mondialisé et que toute forme de souveraineté est vouée à l'échec ». Pour le Directeur de l'ANSSI, il y a un juste milieu : oui l'obsession de souveraineté nationale européenne doit bien rester une obsession car « elle permet de maîtriser les choses , de décider de son avenir et de ne pas être entre les mains des autres ». Mais au-delà de la maîtrise de la technologie, c'est bien la question de la gouvernance qui est ici mise en avant.

KEYNOTE OVH

Michel Paulin,
Directeur Général d'OVH

Sécurité, souveraineté, durabilité : bâtir une véritable résilience européenne via le numérique

Le cloud de confiance et la souveraineté numérique furent des sujets très débattus lors des Assises 2022. C'est pourquoi, il était particulièrement intéressant d'entendre s'exprimer Michel Paulin, le Directeur Général d'OVH Cloud, par ailleurs récemment nommé Président de la filière du numérique de confiance par le ministre de l'Économie et des Finances. Michel Paulin a rappelé l'enjeu stratégique que représentent aujourd'hui les données : enjeu réglementaire, de réputation, de souveraineté... le spectre est large d'autant que leur statut diffère en fonction des pays et des continents. Face à la Chine dont l'État contrôle les données et aux États-Unis pour lesquelles elles ont une valeur commerciale, l'Europe considère les données comme étant une propriété privée. Dans ce contexte, la gouvernance et la protection des données sont essentielles. Mais, s'inquiète Michel Paulin l'Europe a pris du retard et doit accélérer pour bâtir une véritable résilience. Pour lui, cela passe aussi par la souveraineté technologique qui permettra de faire émerger des acteurs européens capables de rivaliser avec leurs concurrents et au Vieux Continent de s'affranchir d'une quelconque dépendance.

Enfin, le Directeur Général d'OVH Cloud a tenu à réaffirmer ses engagements autour de la qualification SecNumCloud qui est devenu une « véritable référence en dehors de nos propres frontières. Cet investissement doit permettre de continuer à bâtir un cloud souverain et durable qui fédère un écosystème enrichi d'éditeurs logiciels pour porter les couleurs d'une technologie respectueuse de nos valeurs européennes. »

KEYNOTE CYBEREASON

Sam Curry,
CSO, Cybereason

Cybereason and Google : The Power to Solve the Threat Landscape Puzzle

Sam Curry, CSO de Cybereason, a une longue expérience dans la cybersécurité. Au fil des années, il s'est forgé sa propre définition à savoir « la cybersécurité est le fait de renverser l'avantage des attaquants ».

La tâche reste immense car bien que les investissements pour se protéger ne cessent d'augmenter, les attaquants semblent toujours avoir une longueur d'avance sur leurs victimes. Faisant un rapide historique des différents outils du marché, Sam Curry rappelle le chemin parcouru d'abord avec les SIEM puis avec les EDR dont la portée reste cependant limitée à la sécurité des end points. Insuffisant dans le contexte actuel où les flux de données sont immenses, continus, et hétérogènes. C'est pourquoi beaucoup d'espoirs reposent sur les XDR qui pourraient inverser la tendance en faveur des victimes. Certes prévient le CSO de Cybereason, « ces outils n'en sont qu'à leurs balbutiements » et les utilisateurs ont un rôle à jouer dans leur développement. Cependant grâce aux XDR, il va être non seulement possible d'arrêter les attaques mais également de les prévenir. Comme les XDR se concentrent principalement sur des analyses comportementales, ils mettent en évidence les liens entre les différentes étapes d'une attaque là où d'autres outils se contenteront d'analyser la technique d'attaque.

En partageant sa vision de la cybersécurité, Sam Curry a voulu souligner que l'on ne peut plus se contenter de seulement récupérer un maximum de données sur les endpoints. Mais qu'il faut avoir des outils capables de corréler les données afin d'assurer une détection et une analyse plus efficaces afin de fournir une réponse plus rapide.

LES TEMPS FORTS DES ASSISES

KEYNOTE SENTINELONE

Tomer Weingarten,
CEO, SentinelOne

Révolution des données dans la cybersécurité. L'ère du XDR commence maintenant

Internet, Cloud... aujourd'hui ces technologies sont largement déployées au service de la production des entreprises. Mais pour Tomer Weingarten, la cyber-sécurisation des environnements n'a pas été assez rapide et si les outils de protection se sont multipliés, les attaquants ont souvent une longueur d'avance sur les organisations. Il faut donc changer de paradigme et voir le réseau en grand c'est-à-dire incluant les terminaux, la data et les logs. Si l'on est capable de surveiller tous ces flux, il devient alors possible de les contrôler. C'est le rôle de l'XDR qui décloisonne et propose une analyse heuristique permettant d'évaluer le risque comme un tout. Avec l'intelligence artificielle, l'XDR permet aux entreprises de réduire les faux positifs et de se concentrer sur les signaux importants. Les enjeux sont importants : ceux qui comprennent la manière d'exploiter au mieux la puissance de leurs données et savent en tirer parti pour aller plus vite garderont une longueur d'avance sur les adversaires d'aujourd'hui et de demain.

KEYNOTE DARKTRACE

Karim Benslimane,
Director of Cyber Intelligence AI Cyber Defence & Security

L'IA au service de la cyber des grands événements sportifs internationaux

Prenant exemple sur la Coupe du Monde de Rugby en 2023 et les Jeux Olympiques de Paris en 2024 Karim Benslimane a souhaité axer sa conférence sur la sécurité technologique des grands événements sportifs internationaux. Car depuis quelques années, ceux-ci sont devenus des cibles prioritaires pour les attaquants, que ce soit dans une démarche hacktiviste, cyber-terroriste ou purement financière. Le danger est d'autant plus grand que ces manifestations s'inscrivent dans un contexte de convergence IT où tout est interconnecté et où interviennent de nombreux opérateurs externes. Pour les organisateurs, les risques de réputation mais aussi de destruction physique sont considérables. Par ailleurs, du fait de la temporalité de ces événements, les experts en cybersécurité ont peu de temps pour agir. Il leur faut donc anticiper le risque, empêcher les attaques de se produire et éviter ainsi de mettre en place des mesures d'urgence pour limiter les dégâts. Pour le Directeur de la cyber-intelligence de Darktrace, il faut donc une sécurité proactive et cela n'est possible qu'avec le recours de l'intelligence artificielle qui permet de détecter les menaces et anomalies, de repérer les comportements suspects et donc de réagir plus rapidement et plus efficacement.

/// INTERVIEW DE LOÏS SAMAIN,

RSSI et CISO d'EDF Hydro

QUEL A ÉTÉ VOTRE PARCOURS PROFESSIONNEL ?

Je suis un ancien étudiant de l'EPITA, la meilleure école que vous connaissez tous ! J'ai effectué mon stage de fin d'études dans une société de conseil (HSC Consulting) où j'ai découvert les sujets de gouvernance. C'était assez nouveau pour moi car je pensais m'orienter vers la technique. J'ai eu alors l'opportunité de passer différentes certifications dont ISO27001 Lead Auditer, ISO 27001 Implementer et ISO27005 Risk Manager. Puis, je suis rentré chez BULL, mieux connu aujourd'hui sous le nom d'Atos, pour travailler à la base sur la cryptographie, puis en appui RSSI au sein de différentes administrations. J'ai ensuite travaillé dans un cabinet de conseil en intelligence stratégique et management des risques qui m'ont permis de me frotter à la géopolitique (une de mes passions !) et de travailler directement pour des acteurs étatiques en France comme le ministère de la Défense ou encore l'ANSSI.

Mais la technique me manquait et je suis devenu RSSI d'une ESN dans l'objectif d'une certification ISO 27001, avant de prendre le poste de RSSI adjoint d'EDF Renouvelables (en charge du périmètre éolien, solaire photovoltaïque et batteries) qui m'a ouvert une porte vers le monde industriel. Aujourd'hui, je suis RSSI d'EDF Hydro, la direction en charge de l'hydraulique chez EDF, qui est composée de 3600 ouvrages et lieux d'interventions, avec des barrages et prises d'eau, des usines ou centrales hydrauliques, des écluses. J'ai la charge le périmètre complet en cybersécurité : SI Métier, SI Industriel et SI Scientifique.

VOUS N'AVEZ PAS EU D'APPRÉHENSION À PASSER SUR LE SECTEUR INDUSTRIEL ?

C'est là qu'il est important d'avoir fait l'EPITA car cette école nous apprend à apprendre. Au début, certes, je ne connaissais pas vraiment le monde industriel mais je me suis formé, je suis allé sur le terrain, voir les métiers, poser énormément de questions aux automaticiens, exploitants, ingénieurs (surement « idiotes » au début) ...

Et c'est un secteur vraiment passionnant avec des passionnés : ce sont des personnes qui n'hésitent pas à prendre du temps pour expliquer leur métier et vous faire progresser si vous prenez le temps de les écouter. Et c'est grâce à tous ces collègues qui m'ont aidé depuis 6 ans que je commence à avoir une bonne compréhension et maitrise des problématiques du métier industriel... .

PRIX DE L'INNOVATION

Prix de l'Innovation 2022 : CryptoNext Security récompensé

Chaque année, le Prix de l'Innovation des Assises de la Cybersécurité récompense une start-up innovante qui permet aux RSSI d'évoluer dans leur métier et dans leur stratégie. La 18ème édition du Prix a récompensé CryptoNext Security, une entreprise qui travaille sur des solutions de cryptographie post-quantique. Créée en 2019, CryptoNext est l'aboutissement de 20 ans de recherche dans les laboratoires de Sorbonne Université, INRIA et CNRS.

Le postulat de départ est de répondre aux défis de l'ordinateur quantique dont la puissance de calcul va révolutionner la sécurité des systèmes cryptographiques à clés publiques, par sa capacité à casser d'ici quelques années les clés générées par les algorithmes actuels. (RSA, ECC...). Les récentes annonces et le contexte géopolitique ont encore accéléré la donne ; la complexité et le temps nécessaire à la mutation des crypto-systèmes à l'intérieur des applications et infrastructures au sein des organisations, ne laissent plus le temps de reporter ce sujet comme le recommandent les principales agences de sécurité dont l'ANSSI. Les défis sont multiples pour les RSSI qui devront dédier de plus en plus de temps à la cryptographie et ses problématiques, dont la gestion des clés, des certificats, ou pour connaître les différents types d'algorithmes. La cryptographie post-quantique (PQC), issue de recherches scientifiques, mathématiques et informatiques, est un outil essentiel donnant lieu à de nombreux projets pilotes et pré-production dans les organisations. Elle est devenue indispensable pour préserver la confidentialité des données, permettre l'authentification, les signatures électroniques de documents, ou la protection des échanges ; l'impact sera considérable pour la plupart des protocoles en place.

De là, l'importance de la solution proposée par CryptoNext qui doit permettre aux organisations de migrer leurs infrastructures IT vers des solutions résistantes au quantique. Bâties autour d'une librairie post-quantique intégrant l'ensemble des algorithmes en cours de standardisation, celles-ci sont nativement hybrides et crypto-agiles conformément aux recommandations des agences de sécurité. Soutenue par le fonds Quantonation et par la BPI, CryptoNext est identifié par le cabinet Gartner parmi les 5 acteurs leaders du domaine.

Comment le/la RSSI doit se former aux soft skills ?

Le métier de RSSI a beaucoup évolué ces dernières années et les seules compétences techniques ne suffisent plus. **Les « soft skills » (résistance au stress, empathie, capacité de négociation...) sont de plus en plus importantes pour évoluer dans la fonction.** Ainsi la difficulté à communiquer est l'un des problèmes les plus souvent détectés de même que le vocabulaire utilisé qui n'est pas toujours compréhensible par les autres collaborateurs de l'entreprise (ni par le comex !). Le but de cette table ronde était de présenter aux RSSI, les soft skills attendus et les techniques permettant de les améliorer. Parmi lesquelles : prendre du temps pour soi afin de mieux se connaitre et ne pas se faire absorber par son travail ; avoir un coach ou suivre des formations (apprentissage du cerveau avec auto-ancrage) ; mener des activités en groupe ou participer à une association... Ces actions ne sont pas à faire une seule fois, mais il s'agit plutôt d'un entrainement sur du long terme. Avec à la clé, une meilleure efficacité professionnelle et personnelle.

Cette table-ronde réunissait

Sabrine Guiheneuf, RSSI & Administratrice du Cesin ; Nicolas Vielliard, Cybersecurity Operations Director de Danone & Administrateur du Clusif ; Gérard Le Comte, Directeur de programmes cybersécurité & Coach Professionnel

La cyber assurance : quelles alternatives ?

La problématique de l'assurance cyber est devenu un sujet de premier plan pour la majorité des grandes et moyennes entreprises. La situation est tellement tendue que certaines d'entre elles ont même décidé de ne plus assurer ce risque. En cause, l'augmentation drastique des primes pour un risque désormais qualifié de systémique. Les assureurs ont ainsi réévalué leurs modèles en tenant compte à la fois de la sinistralité potentielle d'un incident cyber (dont le montant peut atteindre plusieurs dizaines de millions d'euros) et de la maturité du système d'information de leurs clients. À charge pour ces derniers de fournir à travers des questionnaires de plus en plus complexes, les preuves de la protection de leur organisation. Pour tenter de sortir de l'impasse et alors que les attaques n'ont jamais été aussi nombreuses, les différents acteurs concernés proposent des solutions : création par les entreprises d'une assurance dédiée cyber ; **dissociation des petits et grands risques cyber afin de moduler le montant des primes ; répartition du risque entre plusieurs Business Unit... Le travail ne fait que commencer.**

Cette table-ronde réunissait

Gilles Berthelot, Directeur sécurité numérique groupe, SNCF ; Philippe Cotelle, Administrateur de l'AMRAE ; Anne Cridlig, Head of Professional Indemnity & Cyber Département Financial Lines, Zurich Insurance; Sébastien Heon, Cyber Solutions Deputy Chief Underwriting Officer Scor

ATELIER
/YESWEHACK

Après deux ans, quel bilan peut-on dresser de l'usage du bug bounty au sein de Decathlon ?

Lors de cet atelier, l'enseigne sportive a fait le bilan de son usage du bug bounty et a mis en avant quelques recommandations. Une des questions principales qui revient lorsqu'une entreprise veut mettre en place le bug bounty, est la distinction avec le pentest. En fait les deux démarches ne s'opposent pas mais se complètent, le bug bounty arrivant en complément du pentest. Si l'on veut schématiser, le pentester va chercher de façon méthodique et habituelle, là ou le hunter va réfléchir "outside the box". La mise en place de bug bounty au sein de l'entreprise traverse plusieurs phases. La première étant purement humaine pour expliquer au juriste, aux équipes et à l'organisation l'intérêt d'une telle approche. Il faut ensuite définir le périmètre, le service interne qui va payer puis être prêt à valider rapidement une vulnérabilité. Le bug bounty repose donc sur la confiance réciproque entre les hunters et l'entreprise. Ceux-ci sont notés sur le travail qu'ils produisent, là où l'entreprise est notée sur sa capacité à payer rapidement. De la même façon que pour le pentest, la correction des vulnérabilités doit être prévue en amont car lors d'un bug bounty, la question n'est pas de savoir s'il y aura des vulnérabilités, mais combien.

ATELIER
/SENTINELONE

Retex EDR/XDR avec le Groupe SeLoger - De 5 antivirus à un XDR automatisé : échecs, réussites et développements futurs ?

Cet atelier a été l'occasion de comprendre la complexité du choix, des tests et du déploiement d'un XDR autour d'un projet qui a duré près de 8 mois. Tout d'abord, les critères de choix ne sont pas forcément techniques mais tiennent compte aussi de la nationalité du fournisseur. Le benchmark évolue ensuite avec une série de tests réalisés par une équipe dédiée au projet. Vient alors une phase de PoC pour éprouver la robustesse des tests avec l'utilisation de différents malwares. Une fois la solution choisie, la phase de déploiement et de configuration a permis au client de comprendre et d'utiliser au mieux les APIs mis à disposition. Pour le Groupe SeLoger, il s'agissait de répondre d'abord à certains besoins urgents en termes de sécurité avant de déployer les autres fonctionnalités du produit.

LES TEMPS FORTS DES ASSISES

LES TENDANCES

Au fil des années, les menaces se sont diversifiées tant dans la forme que dans le mode opératoire. Cette évolution est liée à l'extension des surfaces d'attaque dans un monde globalement numérique et répond également aux mesures prises par les organisations pour renforcer leur sécurité, ce qui pousse les attaquants à utiliser des méthodes de plus en plus sophistiquées. Côté solutions, on note une réelle évolution des outils et technologies mais sur le temps long à l'instar de l'intelligence artificielle dont l'usage n'est pas encore exploitée pleinement.

Bilan de la cybermenace

La menace cyber continue de croitre dans un contexte géopolitique international très instable suite à la pandémie de Covid 19 (et de ses effets économiques), à la compétition entre les grandes puissances et à l'intensification des activités criminelles lucratives (aussi bien privées que soutenues directement ou indirectement par des Etats). Fin décembre une enquête du fournisseur Dell mentionnait que 86% des entreprises mondiales de plus de 250 personnes avaient été touchées par des cyberattaques en 2022. Dans ce contexte, la France n'est pas épargnée. L'ANSSI qui ne traite qu'une partie du tissu économique hexagonal avait déjà enregistré une augmentation de 37% des intrusions entre 2020 et 2021. Selon l'Agence, les secteurs les plus ciblés sont les collectivités territoriales, l'industrie et la santé. Autre constat : les grandes et moyennes organisations ne sont plus les seules touchées. De plus en plus de petites structures, moins informées et moins protégées se retrouvent la cible des attaquants avec parfois des conséquences dramatiques qui les poussent à la faillite. Les rançongiciels (ransomwares) restent l'une des méthodes les plus répandues pour infecter un système. D'autant plus que l'écosystème se professionnalise avec une spécialisation des acteurs sur les différents segments de la Kill Chain.

Evolution des solutions de cybersécurité

Automatisation (notamment pour pallier au manque de ressources humaines), SIEM, EDR,... les outils et les solutions ne cessent de s'adapter au fur et à mesure de la sophistication des menaces. Difficile néanmoins de parler de révolution car il s'agit plutôt d'évolution. Ainsi des outils de détection de la menace qui ces dernières années se sont beaucoup transformés grâce à l'émergence de nouvelles technologies comme l'Intelligence artificielle. Historiquement, la détection de menaces se basait sur des règles statiques telles que la reconnaissance de hash de programmes malveillants, d'adresse IP connues et d'enchainement d'actions. Ces mécanismes, efficaces contre des attaques de bas niveaux, restent limités lorsqu'elles sont plus élaborées. L'IA doit permettre de résoudre en partie cette problématique. On le voit déjà avec l'arrivée massive de la technologie XDR, évolution de l'EDR. En consolidant plusieurs produits au sein d'une plateforme unique de détection des incidents et de réponse l'XDR apparaît comme une solution renforcée de prévention des cyberattaques. Citons également le SASE (Secure Access Service EDGE) une architecture basée sur le cloud qui fournit des services réseau et de sécurité destinés à protéger les utilisateurs, les applications et les données. **Et dans un futur proche peut être, le chiffrement homomorphe qui permettra d'effectuer des traitements sur des données chiffrées sans que celles-ci soient exposées en clair.**

TYPES D'ATTAQUES ET TENDANCES

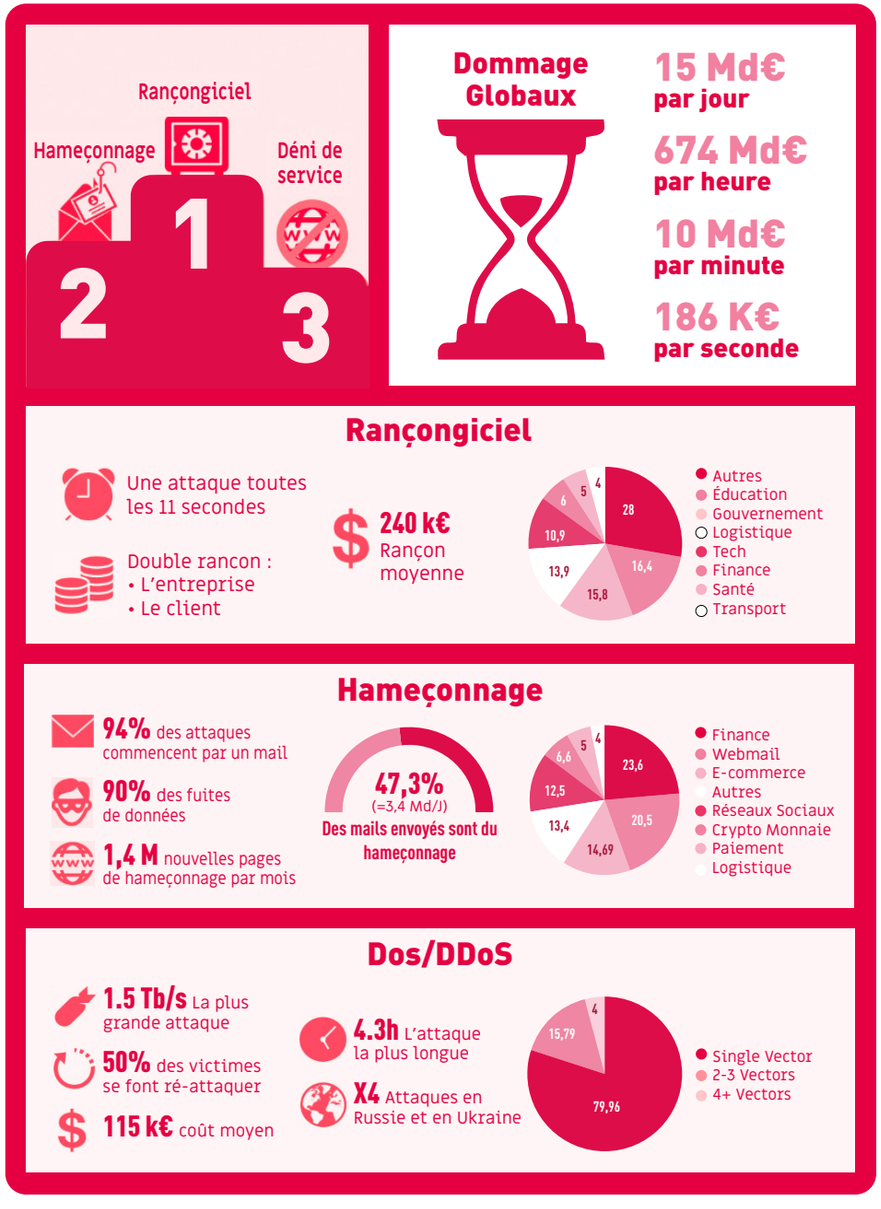


Table-ronde : Les innovations permettent-elles de faire face aux menaces ?

Comment l'écosystème cyber (et donc les RSSI) peut-il profiter de l'innovation ? Telle était la question sous-jacente de cette table-ronde dont les intervenants ont proposé au préalable de classer l'innovation en deux catégories : celle d'usage et celle de rupture.

Les catégories d'usage s'appréhendent facilement par les entreprises, car il s'agit d'une amélioration de l' existant. De façon opposée, l'innovation de rupture est difficile à intégrer, car la rupture est par définition un état nouveau. La solution consiste donc à combiner l'intégration d'innovation d'usage (forme de mise à jour continue) et celle de rupture pour ne pas risquer de manquer un tournant majeur.

Le marketing des innovations de rupture, en étant trop flou ou trop agressif peut entrainer une méfiance de la part des experts SSI. Les « innovateurs » doivent donc rétablir cette confiance et il est alors important de s'appuyer sur les retours d'expérience des premiers clients. De leur côté, les entreprises pionnières qui ont bénéficié d'une innovation de rupture, peuvent grâce à leurs retours, faire évoluer le produit afin qu'il corresponde mieux au besoin des clients. On le comprend, l'échange avec l'écosystème est primordial. Par ailleurs, les intervenants ont rappelé que le RSSI doit faire de la veille, s'intéresser aux concours d'innovation (comme le Prix des Assises), suivre certains réseaux sociaux, faire travailler son réseau et consulter certains fonds d'investissement qui ont des startups dans leurs portefeuilles.

Cette table-ronde réunissait

Thomas Anglade Head of Data Science Seckiot, Sabine d'Argoeuves IS/IT Corporate Security Manager Danone et Maxime Cartan, CEO Citalid

Un contexte géopolitique source de tension cyber

L'année 2022 aura été marquée par un contexte géopolitique très tendu entrainant des répercussions sur le secteur de la cybersécurité . Certes, auparavant de nombreuses attaques semblaient déjà être la conséquence directe ou indirect de conflits entre états (à l'instar de Wannacry) mais l'invasion de l'Ukraine par la Russie en février 2022 a amplifié le phénomène. Dans un rapport publié fin 2022, l'ENISA (European Union Agency for Cybersecurity) souligne que le conflit russo-ukrainien a mis en lumière « de nouvelles façons » de mener des campagnes de désinformation ».

Les cyberattaques menées souvent en parallèle avec des actions militaires sur le terrain ont pour objectif de dégrader les infrastructures critiques et les moyens de défense. On a vu également apparaître de nouvelles formes d'attaques dites inversées. Diligentées par des groupes de hackers de type Anonymous, elles ont ciblé les entreprises occidentales pour les inciter à clore leurs opérations en Russie.

Mais cette instabilité n'est pas limitée à cette région du monde. Aujourd'hui toutes les organisations publiques ou privées peuvent devenir des cibles potentielles de cybercriminels qui profitent de la confusion ambiante et agissent par opportunité. « Exploitation de vulnérabilités O-day, désinformation, deepfakes activées par l'IA... de plus en plus d'attaques malveillantes et généralisées émergent » précise l'ENISA qui s'attend à « voir davantage de cyber-opérations motivées par la géopolitique ».

Même s'il est difficile de pouvoir attribuer des attaques à un Etat, de plus en plus d'experts n'hésitent pas à faire le lien entre groupe de cybercriminels et une entité étatique. Ainsi d'APT28 qui serait lié au gouvernement russe, APT42 à l'Iran ou TA423 à la Chine.

Malheureusement, la situation ne devrait guère s'améliorer en 2023 avec un nombre accru de tensions internationales à travers la planète et la sophistication des outils numériques.

Christian-Marc Lifländer
chef de la Section Cyberdéfense de l'OTAN

L'impact de la situation géopolitique sur les sujets de cybersécurité

Le contexte géopolitique actuel et ses conséquences cyber furent au cœur de l'intervention de Christian-Marc Lifländer, chef de la Section Cyberdéfense de l'OTAN lors de l'ouverture des Assises 2022. De fait, la guerre entre la Russie et l'Ukraine a montré que le cyberespace est devenu un élément clé dans les conflits militaires actuels (et futurs) avec des cyberattaques lancées pour influer le champ de bataille physique.
L'importance stratégique de la cybersécurité est indéniable et cela ne va cesser de croître. Et dans cet environnement instable, mouvant et dangereux, il est donc essentiel de se préparer.
L'exemple de l'Ukraine là encore est riche d'enseignement. Si les attaques ont eu un effet déstabilisateur (sur les communications, les ressources énergétiques...) et la capacité du gouvernement à bien fonctionner, le pays a réussi à faire face.

De cet exemple, il faut retenir la résilience qui sera le mot clé des prochaines années mais aussi les choix que doivent faire les acteurs concernés. Christian-Marc Lifländer appelle les états à être plus proactifs, à mieux connaitre leurs vulnérabilités afin de développer les technologies de défense adéquates et surtout à mettre en place davantage de partenariats avec les autres acteurs du cyberespace que ce soit dans le domaine public, privé, civil, militaire, national ou international. Dans ce contexte, l'OTAN a un rôle important à jouer, d'abord en adaptant son modèle de cyberdéfense à ces nouveaux environnements mais aussi en garantissant l'intégrité des valeurs des Etats membres. D'autant que de nouveaux dangers guettent : des technologies telles que l'Intelligence artificielle, la biotechnologie , le quantique... vont changer le monde et la vie quotidienne mais elles créent de également de nouvelles menaces car elles présentent des failles qui peuvent être exploitées. Malgré tout dans sa conclusion, Christian-Marc Lifländer insiste sur le fait de ne pas sacrifier les besoins de sécurité sur le long terme pour des bénéfices économiques court-termistes. « La liberté des hommes étant » martèle-t-il « plus importante que la liberté des échanges ».

ATELIER
/ESET

Ukraine: points marquants de la guerre numérique actuelle, et retour sur les précédentes cyberattaques

Il y a déjà plusieurs années que l'Ukraine subit des cyberattaques mais depuis le début de la guerre contre la Russie en février 2022, celles-ci se sont intensifiées avec pour principaux objectifs l'espionnage, le sabotage, la destruction et le besoins de la part des attaquants de montrer leur pouvoir de nuisance.

Les experts de la société ESET ont aidé l'Ukraine dans sa défense cyber technologique et lors de cet atelier, ils ont présenté certaines attaques qu'ils ont pu déjouer. L'une des plus importantes a été celle d'Industroyer2, une évolution de Industroyer, un malware déjà utilisé en 2016 par le groupe Sandworm APT pour couper l'alimentation électrique de l'Ukraine. Eset a fourni aux ukrainiens une analyse cruciale de cette menace, qui, si elle avait réussi aurait pu avoir comme conséquence de plonger 2 millions de personnes dans le noir.

La seconde attaque repérée, IsaacWiper, a débuté peu après l'invasion militaire russe et a touché un réseau gouvernemental ukrainien. Elle avait été de peu précédée par d'autres attaques destructrices HermeticWiper (qui efface les données) ; HermeticWizard (pour la propagation sur le réseau local) et HermeticRansom (qui agit comme un ransomware leurre). Il ressort des analyses réalisées par les experts d'ESET sur des éléments de ces malwares que ces attaques avaient étaient planifiées bien des mois avant l'invasion russe.

Téléphones : Quelles menaces ? Quels risques ?

Aujourd'hui plus de 5 milliards de personnes utilisent un téléphone mobile dans le monde. Autant dire que cet objet qui émet, reçoit et contient des données, parfois sensibles, est un véritable vecteur de risque. Surtout que les mesures de sécurité (comme par exemple la mise à jour de l'OS) ne sont pas toujours appliquées et que beaucoup d'utilisateurs cliquent imprudemment sur des pièces jointes, téléchargent des applications malveillantes ou exposent des informations personnelles et/ou confidentielles sur les réseaux sociaux. Avec à la clé, des vols de données, une atteinte à la réputation et pour certaines personnalités des risques d'espionnage. Selon un rapport publié par Proofpoint, le nombre d'attaque de malware sur les smartphones a augmenté de 500% en 2022.

Les entreprises qui ont largement équipé leurs collaborateurs et leurs dirigeants ne sont pas épargnées. L'affaire Pegasus qui a été dévoilée en 2021 est à cet égard riche d'enseignement.

Conçu par l'entreprise israélienne NSO, Pegasus est un spyware (logiciel espion) qui a été installé sur les téléphones en combinant des techniques zero-click (pas besoin d'interaction avec l'utilisateur) à travers par exemple des apps (comme iMessage, WhatsApp ou FaceTime sur les terminaux Apple) avec des failles 0-day présentes sur les OS. Des failles achetées sur le Darknet ou découvertes par les ingénieurs de NSO. Une fois dans la machine, Pegasus permet non seulement d'écouter les appels téléphoniques, mais surtout d'absorber tout le contenu du téléphone - photos, données, messages, d'enregistrer le contenu des conversations sans que rien n'indique à son propriétaire qu'il a été piraté. Commercialisé en principe uniquement à des Etats, Pegasus a été employé à travers le monde pour espionner des opposants politiques, des journalistes et des dirigeants d'autres états que le commanditaire.

Les câbles sous-marins : un enjeu stratégique

Véritables vecteurs des télécommunications mondiales, les câbles sous-marins font transiter aujourd'hui près de 95% des liaisons internet de la planète. Il s'agit donc d'une infrastructure stratégique et d'un possible terrain de confrontation.

Une grande partie de ces câbles est aujourd'hui contrôlée par les GAFAM dont les moyens financiers sont considérables. Cet état de fait pose des problèmes de souveraineté lourds d'enjeux politiques. Ainsi la rivalité croissante entre les Etats-Unis et la Chine se traduit aussi dans ce domaine. Dans la région Pacifique où les deux pays se livrent une lutte économique et d'influence intense la Commission fédérale des communications (FCC) s'est opposée à ce que le câble Apricot de Meta et Alphabet passe par Hong-Kong.

Dans ce contexte , quels sont les risques ? Souvent situés dans des eaux profondes, difficiles d'accès, soumis aux tempêtes, aux séismes et aux filets de pêche, les câbles sous-marins peuvent être également être des cibles pour des (cyber) criminels ou dans le cadre de conflits militaires. Lors de l'invasion de la Crimée en 2014, la Russie avait déjà coupé les câbles vers l'Ukraine, plongeant le pays dans un début de black out. En 2021, le navire « océanographique » russe Yantar avait été aperçu au-dessus d'un nœud de câbles en mer d'Irlande laissant craindre un sabotage. Mais le danger vient aussi des points d'entrée et de sortie des câbles sur terre ainsi que dans les risques de piratage des écoutes électromagnétiques sous-marines. D'ores et déjà, entre 2012 et 2014, la NSA américaine aurait espionné plusieurs dirigeants européens dont la chancelière allemande Angela Merkel via les câbles sous-marins danois.

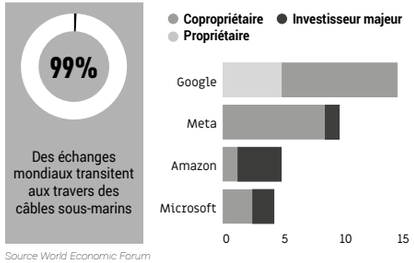
UN CONTEXTE DE TENSION

La guerre entre la Russie et l'Ukraine ainsi que les événements des gazoducs NordStream et dans l'Arctique (coupure de câbles) renforcent les craintes concernant des potentielles attaques sur les câbles sous-marins.

INFRASTRUCTURE STRATÉGIQUE

Les câbles font transiter une grande partie du trafic mondial (réseau Swift, communication inter-étatiques) et représentent ainsi un point critique pouvant mener à de graves problèmes économisques, stratégiques ou de réputation.

LES GAFAM ET LES BATAILLES DES CÂBLES SOUS-MARINS EN 2019



Source World Economic Forum

DIFFÉRENTS TYPES DE MENACES

ACCIDENTS

Les fonds marins sont des endroits souvent méconnus et il n'est pas rare qu'avec les conditions extérieures extrêmes, à cause de bateau de pêches ou de certains animaux que les câbles soient endommagés.

ESPIONNAGE

Comme l'avait révélé Snowden en 2013, la NSA et les services secrets britanniques surveillaient et espionnaient certains caâbles. En effet, il est possible pour un Etat ou un attaquant de se positionner sur les câbles afin d'écouter et espionner les données qui tranlsitent.

SABOTAGE PHYSIQUE

Des acteurs malintentionnés peuvent attaquer de façon physique (explosion, coupure de câbles ou d'électricité) les Infrastructures, les câbles eux-mêmes ou les bateaux qui les posent ou les réparent.

CYBERATTAQUES

Comme tout ce qui est connecté, les infrastructures gérant les câbles peuvent être la cible de cyberattaques.

LES TENDANCES

EDITO Sébastien Bombal

Responsable de la Majeure SRS de l'EPITA

De la guerre, à l'écologie la technologie et la cybersécurité au coeur des enjeux

Déjà la 5ème édition et c'est toujours avec un grand plaisir et une certaine émotion que je remercie la merveilleuse équipe des assises et mes 50 étudiants SRS (Système Réseau et Sécurité)? qui se sont essayés aux difficiles exercices de prospective, d'interview et de synthèse.

J'aimerai vous dire que la menace sur le cyberespace ne va pas croître en 2023 mais malheureusement l'enchaînement et l'intensité des crises, le durcissement des relations géopolitiques, le niveau de la criminalité organisée et les tendances économiques ne vont pas dans ce sens.

La revue nationale stratégique de 2022, publiée par le SGDSN, synthétise très bien notre environnement et les défis auxquels nous devrons faire face, quel que soit notre secteur professionnel. La résilience, la supériorité informationnelle, la souveraineté ou encore une économie numérique adaptée n'ont jamais été autant au cœur des défis cyber et de notre autonomie stratégique.

Les difficultés d'approvisionnement et la prise en compte des défis climatiques seront sûrement rapidement des nouveaux prismes d'analyse pour les métiers du cyberespace

Ce livre blanc aborde modestement quelques-uns des aspects qui préoccupent les participants des Assises. La ligne éditoriale n'a pas été facile à définir, mais je tiens à souligner une nouvelle fois le travail remarquable mené par Florence Puybareau et son équipe avec l'aide des étudiants EPITA.

Ce livre blanc démontre aussi à travers les années, que notre métier lié au cyberespace évolue sans cesse à un rythme effréné, il se complexifie et nos ressources disponibles sont toujours aussi comptées.

2022 a été aussi une année importante au niveau européen. Les évolutions juridiques pour le cyberespace (NIS v2, DMA, DSA), le conflit ukrainien ou encore la présidence française 2022 ne sont que quelques exemples des sujets qui vont nous impacter significativement et durablement.

L'évolution technologique n'attend pas et les innovations techniques et opérationnelles sont toujours plus impressionnantes et passionnantes. L'EPITA contribue à cette innovation et les assises restent un endroit privilégié en France pour en prendre toute la mesure dans un esprit de pionnier et d'excellence.

Philippe Dewost
CEO EPITA

© Géraldine

Florence Puybareau
Directrice des Contenus, DG Consultants

Retour aux Assises après une année 2022 marquée par une extension du domaine de la lutte à des secteurs jusqu'ici sanctuarisés comme l'hôpital. Si les cyber-attaques de Corbeil-Essonne et de Versailles ont rappelé l'urgence à former des milliers d'experts, il faudra toujours 3 ans pour diplômer un Bachelor Cyber, et 5 ans pour un ingénieur en Computer Science.

Le partenariat noué depuis 5 ans entre les Assises et l'EPITA puise tout son sens dans cette asymétrie entre émotion et formation, urgence et patience. Chaque année il faut attendre un peu avant de revisiter, à travers le regard exigeant et neuf, les temps forts de ce rendez-vous annuel. Il vous revient maintenant d'en découvrir et d'en apprécier le résultat.

Confier l'élaboration de ce Livre Blanc «Cybersécurité & Innovations» à celles et ceux qui assureront la relève était une intuition géniale. Le contenu de cette cinquième édition en démontre la justesse et la qualité de sa mise en œuvre.

Cette intuition fut d'abord celle d'une grande dame ; j'avais eu l'occasion de croiser Florence Puybareau dans une vie antérieure, je l'avais retrouvée avec un immense plaisir, je la vois reprendre le large et le sentiment qui domine tous les autres est résolument celui de la gratitude.

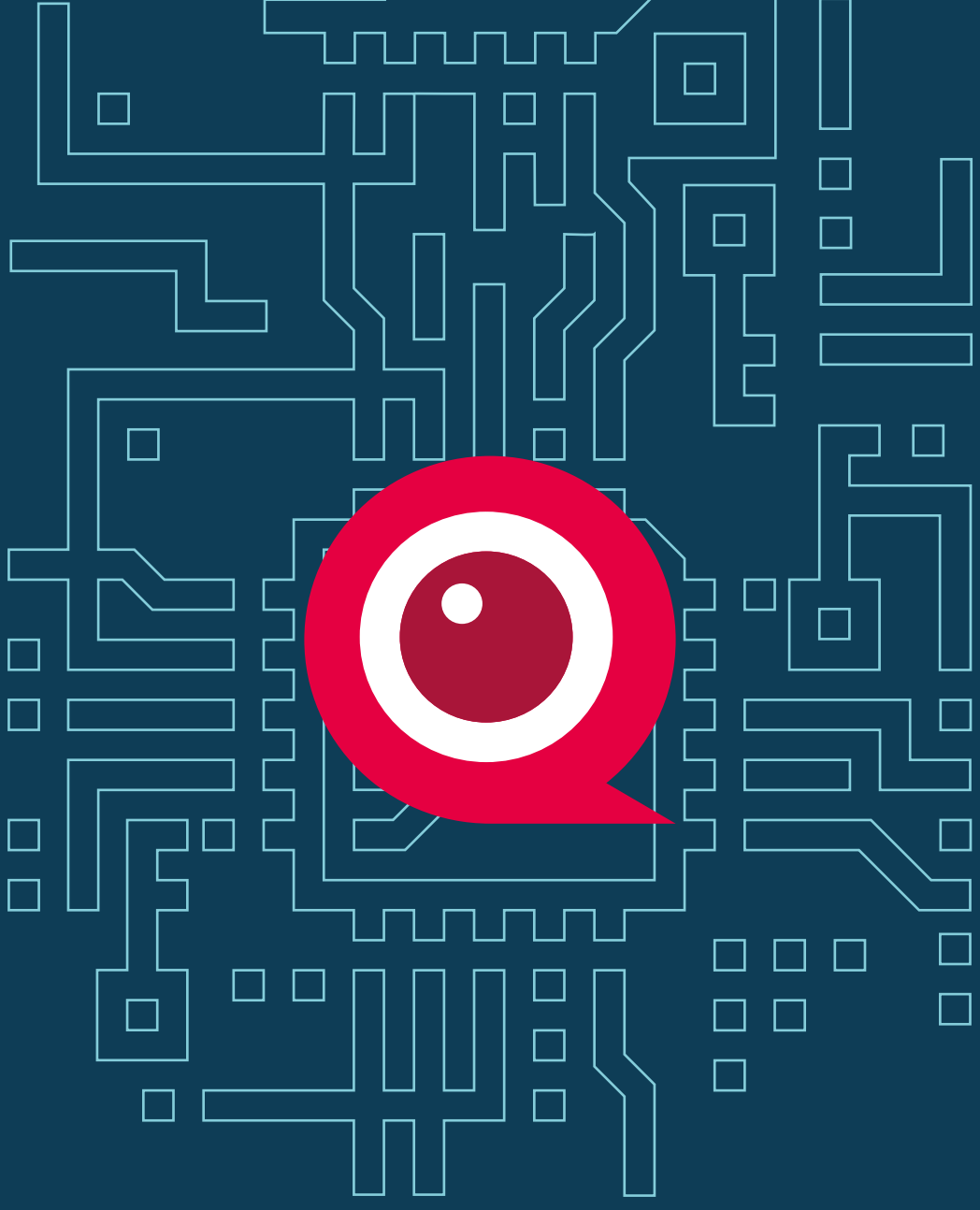
Merci et rendez-vous à tous aux Assises 2023

Partager la magie des Assises

Cette année encore, travailler avec la majeure SRS de l'EPITA fut un vrai plaisir. Faire découvrir aux futurs professionnels de la cyber ce qu'est aujourd'hui ce marché, les métiers qu'il recèle et tout ce riche écosystème qu'ils rejoindront bientôt apporte toujours beaucoup de satisfaction. Il s'agit autant de faire œuvre de pédagogie que de leur partager la magie des Assises. Il est vrai que l'actualité (heureusement ou malheureusement) ne cesse de nous rappeler la place de la cybersécurité dans nos vies numériques et surtout l'importance d'avoir un vivier d'experts bien formés qui demain sauront protéger nos organisations et nos institutions. Tel est l'un des rôles de l'EPITA que je remercie encore pour son engagement auprès des Assises.

Merci également aux étudiants de la promotion 2023 qui se sont transformés pour un temps en rédacteurs avisés de cet ouvrage.

Et à titre personnel, je voudrais dire un très grand merci à Philippe Dewost, le Directeur général de l 'EPITA, Marie Moin, Directrice de Securesphere et surtout Sebastien Bombal, le Directeur de la majeure SRS qui, il y a 5 ans m'a proposé de réaliser ce Livre Blanc et m'a toujours honorée de sa confiance.



DG CONSULTANTS www.lesassisesdelacybersecurite.com COMEXPOSIUM

@Les_Assises @Les_Assises #LesAssises Les Assises