En partenariat avec EPITA

LES ASSISES

Prenons de la hauteur !

Le regard des Assises et de l'EPITA

Édition 2023

Ready For IT!, l'évènement One to One incontournable pour les entreprises engagées dans la transition de sécurité numérique se tiendra du **14 au 16 mai 2024, à Monaco**

Sommaire

→ L'édition 2023 en quelques chiffres

Les chiffres clés des Assises

3 360 participants

11 300 rendez-vous one to one

1 470 invités

174 sociétés partenaires

21 startups

70 journalistes

50 experts

9 tables rondes experts

4 sessions de meetups

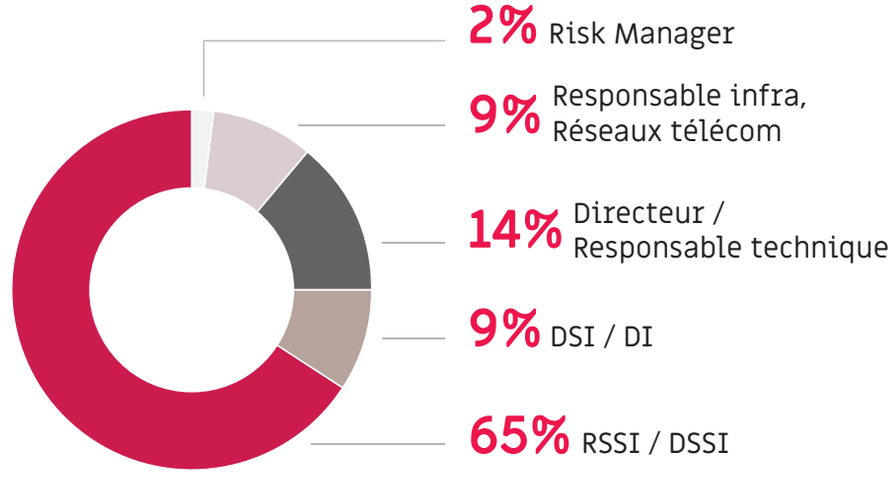
113 ateliers et cas clients

4 keynotes

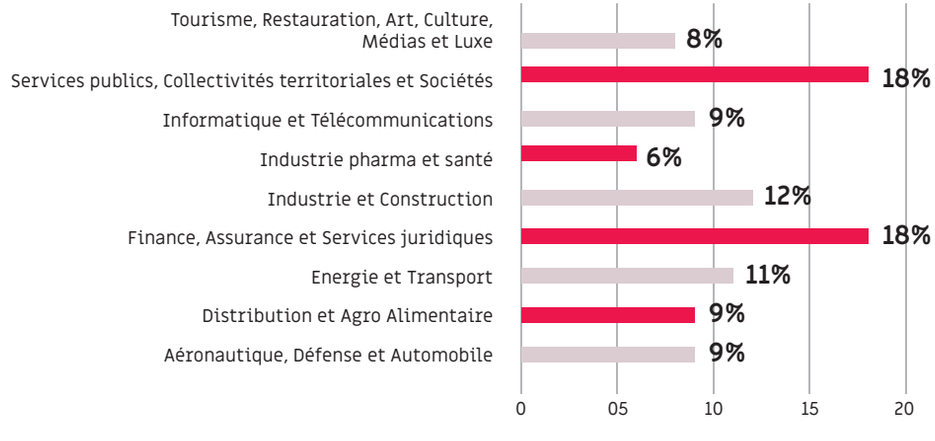
2 conférences

Les invités

par FONCTION



par SECTEUR D'ACTIVITÉ



3 questions à Paul Lemesle

Président d'Honneur des Assises 2024

Comment vois-tu l'évolution des menaces en cybersécurité et quelles actions prioritaires envisages-tu pour y faire face ?

Ce qui me frappe depuis le début du conflit en Ukraine est notre dépendance totale vis-à-vis des infrastructures (réseaux de gaz, d'électricité, d'eau potable) et la grande vulnérabilité de nos sociétés vis-à-vis de leur dysfonctionnement, comme l'ont encore montré les premières tempêtes hivernales. Notre dépendance de plus en plus forte aux réseaux de télécommunications et aux outils numériques augmente l'efficacité d'une attaque réussie. La cybersécurité devient donc un nouveau champ d'affrontement, un risque systémique qui va s'accentuer et qu'il convient d'aborder de manière plus globale. L'évolution de la réglementation européenne, à travers DORA, NIS2 ou encore le CRA, ne fait que prendre en compte cette évolution de la menace. Ainsi, il me semble essentiel d'échanger, de partager, de travailler ensemble et de coopérer pour mieux lutter contre la cybercriminalité et protéger nos entreprises et nos pays.

Quelles innovations ou tendances dans la cybersécurité te semblent les plus prometteuses pour l'avenir ?

Au risque de décevoir, je ne vais pas parler IA mais mots de passe. Je suis avec beaucoup d'attention, et ce depuis plusieurs mois, le travail réalisé par l'Alliance FIDO autour du standard "passkey". Son adoption par Google, Apple, Microsoft et d'autres acteurs majeurs des services numériques me fait espérer la disparition prochaine des mots de passe pour l'authentification. C'est à mon sens une vraie révolution qui me permet aujourd'hui de ne quasiment plus avoir à saisir mon mot de passe au travail. Si on combine cela avec la résistance du standard FIDO aux attaques de type "EvilProxy", nous tenons peut-être une vraie chance de combattre les attaques de type "hameçonnage" tout en simplifiant la vie de nos utilisateurs.

En tant que Président d'honneur de l'édition 2024, quelles initiatives souhaites-tu mettre en avant cette année pour renforcer l'impact des Assises de la Cybersécurité ?

Comme je l'écrivais plus tôt, je crois qu'il est essentiel de travailler ensemble ou de "travailler plus que jamais en réseaux " comme le rappelait Vincent Strubel en ouverture des Assises 2023. Cette préoccupation est au cœur des Assises depuis leur création, l'occasion nous étant donnée chaque année d'échanger avec l'ensemble de l'écosystème cyber français. J'espère que nous pourrons cette année:

- renforcer l'accueil des nouveaux RSSI et de nouveaux partenaires pour élargir nos réseaux;
- parler de l'engagement des réservistes de cyberdéfense, qui permet de renforcer le lien entre l'armée et la nation;
- découvrir les initiatives de coopération sectorielles. Je crois que nous avons beaucoup à gagner à dépasser le seul prisme de la concurrence pour lutter plus efficacement ensemble.
- mettre en avant des initiatives de sensibilisation à destination du grand public.

Paul Lemesle, Président d'honneur des Assises 2024, Chief Information Security Officer, Groupe Lactalis

→ Entretien

Laurent Amsel

Quelles sont les tendances en matière de cyber en 2023 et 2024 ?

Les attaquants préfèrent désormais cibler les partenaires et fournisseurs, car ils ont souvent des mesures de sécurité moins robustes. Ces derniers s'adaptent aussi plus efficacement à divers scénarios. L'utilisation de l'intelligence artificielle, comme les DeepFakes, crée de nouvelles opportunités pour les attaques.

Heureusement, les États, en particulier en Europe, sont de plus en plus conscients de la menace systémique liée à la cybersécurité. Ils mettent en place de nouvelles directives pour protéger les entreprises et renforcer la coopération entre les États.

La résistance au changement est-elle un frein dans la mise en place des projets de sécurité ?

La résistance au changement étant naturellement présente dans tout système, le domaine de la cybersécurité n'y échappe pas. L'image du « Triangle de la cyber » constituée du niveau de protection, du coût et de l'expérience utilisateur, est un bon exemple. Il n'est pas simple d'augmenter le niveau de défense sans avoir d'influence sur les coûts et l'expérience utilisateur. Il faut trouver des compromis entre ces trois axes pour trouver le meilleur équilibre.

Pour vaincre cette résistance aux changements, il est aussi important de mettre en place une bonne communication et une bonne écoute. C'est au RSSI de trouver la solution pour conjuguer un bon niveau de défense avec les besoins du métier. Chez Carrefour, la cybersécurité est agile et au service du business.

> ***Chez Carrefour, la cybersécurité est agile et au service du business.***

Laurent Amsel, RSSI Groupe
chez Carrefour

→ Entretien

Olivier Cahagne

Pouvez-vous nous parler de votre parcours professionnel ?
Bien sûr ! Diplômé de l'EPITA en 2001, j'ai travaillé chez Cisco, VMware, AWS, et je suis actuellement chez Cloudflare depuis 1 an et demi. Bien que ma formation ne soit pas spécifiquement en cybersécurité, mon expertise en infrastructure réseau et opérationnelle grâce à Cisco et mes certifications AWS sont précieuses dans ce domaine.

Quels ont été les faits marquants de Cloudflare aux Assises cette année ?
Les Assises de la cybersécurité sont un événement clé en France. Cloudflare a augmenté sa présence, attirant 130 rendez-vous avant l'ouverture. Cloudflare se positionne désormais comme un "cloud de connectivité" grâce à sa solution Zero-Trust. Michelle Zatlyn, notre COO, a également donné une keynote sur l'IA en cybersécurité.

Quelles sont les tendances en cybersécurité que vous avez observées récemment ?
Nous avons noté des attaques sur les DNS autoritaires, des DDoS éclairs, l'évolution du phishing avec plus de spearphishing et des attaques DDoS automatisées. Les Jeux Olympiques de Paris 2024 pourraient être des cibles, notamment pour de fausses billetteries. L'usurpation de hotspots publics facilite également les attaques.

Quel a été l'événement majeur en cybersécurité en 2023 ?
L'attaque sur le protocole HTTP/2 avec la technique du "Rapid Reset" en octobre 2023 a été le plus marquant. Cloudflare a enregistré sa plus grosse attaque en termes de volume, atteignant 209 millions de requêtes par seconde. Une CVE, CVE-2023-44487, a été publiée en collaboration avec GCP et AWS à la suite de cette menace.

Une citation pour conclure notre interview ?
Je dirais une citation de Boris Lecoeur, directeur de Cloudflare France, qui résume notre positionnement : "Cloudflare, Gardien de l'internet".

> ***Cloudflare, gardien de l'inernet.***

Olivier Cahagne, Solutions Engineer chez Cloudflare

→ Focus

L'IA, menace ou opportunité ?

Dans un monde en constante évolution, l'IA générative émerge comme un outil à double tranchant, offrant de nouvelles opportunités pour les attaquants ainsi que les défenseurs. Alors que la cybersécurité devient un enjeu de plus en plus critique, il est essentiel de comprendre l'impact de cette technologie à fort impact.

Si les cybercriminels utilisent déjà cette technologie pour lancer des attaques de phishing plus sophistiquées, ou encore identifier et exploiter des vulnérabilités, ces technologies se généralisent aussi dans tous les produits pour faciliter le travail des collaborateurs.

La cybersécurité n'y échappe pas. De nombreux produits sur Les Assises 2023 ont mis en avant ces assistants d'aide à la configuration ou de suivi. Serait-ce la solution tant attendue pour faire face à la pénurie de talents et la complexité toujours croissante en cybersécurité ? L'IA représente un atout pour les équipes de sécurité, facilitant la création de playbooks automatisant et en réduisant la fatigue des analystes confrontés à un flux continu d'alertes.

Toutefois ces technologies doivent interroger sur le futur de la cybersécurité sur différents angles. D'abord sous l'angle RH, l'IA et l'automatisation répondront-elles à la promesse de compenser le manque de RH en démultipliant ? Seront-elles un risque de perte d'expertise technique au profit des prompts IA ?

Ensuite, les nouveaux usages et l'intégration massive de ces algorithmes deviennent des sujets majeurs et urgents à prendre en compte à tous les niveaux de l'organisation et des politiques publiques. La cybersécurité des IA devient une nouvelle priorité, même si c'est une de plus. De nombreux risques émergent, tels le risque d'empoisonnement des données d'entraînement, l'export de ces données, la corruption des modèles auto-apprenants, etc. Sans compter les risques liés à la génération de contenu et un risque croissant exponentiellement aux usurpations de tous types.

Il est impératif de sécuriser l'IA et le contenu généré de manière durable. Pour comprendre comment y parvenir, il faut examiner les cas d'utilisation, les risques et les limites de l'IA (générative ou non). Des ateliers peuvent mettre en avant les conseils sur la gouvernance ou des cadres de gestion de risque comme le NIST AI RMF 1.0.

Comprendre et anticiper les défis de l'IA est essentiel pour garantir la cybersécurité et la société de l'information de demain.

→ On fait le point

Jean-Marie Letort

Au cœur de l'innovation de Microsoft en IA et cybersécurité.

L'intelligence artificielle : un nouvel horizon

Acteur majeur de l'innovation, Microsoft cherche à se distinguer dans la fusion de l'IA et de la cybersécurité. Jean-Marie Letort, à la tête de la solution de cybersécurité de Microsoft France, souligne l'impératif d'efficience que l'IA générative apporte dans la détection, et la remédiation des menaces.

Microsoft a révélé un engagement fort et novateur dans l'évolution de son "Copilot for Security", avec un système intégrant IA, EDR, et SIEM. M. Letort explique que la combinaison traduit une ambition de changer la dynamique de défense des entreprises.

Préparer le terrain de la sécurité future

L'usage de l'IA par les cyberattaquants s'intensifie, notamment dans le phishing ; l'identification et même l'exploitation des vulnérabilités. La détection pro-active s'impose désormais comme standard avec un accent sur la chasse aux menaces (hunting) avant qu'elles ne se concrétisent.

Les perspectives de Microsoft reflètent une philosophie de sécurité proactive et adaptative. La firme se positionne en avant-garde, vers un futur où l'IA est le bastion de la cybersécurité.

Ne pas oublier les enjeux sociétaux

Sur la confidentialité, Microsoft reste ferme sur sa maxime "Your Data is Your Data", pour garantir une gestion des données conforme au RGPD.
Les collectivités ou encore les services essentiels paient aujourd'hui un lourd tribut face aux cybermenaces. Ils doivent bénéficier de toutes ces avancées technologiques pour faire face aux pénuries croissantes de ressources humaines du domaine.

> ***Chaque jour, nous analysons 65 trillions de signaux et surveillons plus de 1,4 milliards d'appareils.***

Jean-Marie Letort, Head of Microsoft France Cybersecurity solution area

→ Entretien

Julien Touzeau

Julien, pouvez-vous nous parler de votre parcours ?

Je suis ingénieur de formation avec un complément en MBA à HEC. J'ai débuté dans l'informatique avant de plonger dans la cybersécurité au début des années 2000. Chez IBM, j'ai acquis une solide expérience en tant que consultant, puis chez Airbus, j'ai travaillé sur la sécurité des produits avioniques, notamment pour l'A380. Par la suite, j'ai gravi les échelons et je suis aujourd'hui à la tête du service de conseil chez Airbus Protect

Quels sont les domaines et enjeux émergents de la cybersécurité que vous considérez particulièrement critiques pour la période à venir ?

Les enjeux ne sont pas forcément nouveaux, mais ils évoluent avec la technologie. Les entreprises doivent s'adapter rapidement aux innovations, comme les IA génératives, qui sont déjà largement répandues. Le défi majeur est de rester agile et proactif face à ces avancées pour protéger les informations sensibles. La formation des collaborateurs est cruciale pour qu'ils comprennent les implications de leur travail sur la sécurité de l'entreprise.

Nous observons un intérêt croissant pour les IA génératives, qui représentent un potentiel autant pour les attaquants que pour la défense. En 2024, des réglementations comme NIS 2 et EASA Part-IS vont redéfinir les normes de sécurité pour de nombreux secteurs.

Un mot pour la fin ?

Il est essentiel d'embrasser les technologies émergentes et de former les collaborateurs aux risques associés. Chez Airbus Protect, nous croyons qu'il vaut mieux accompagner le changement que de tenter de le contrôler. La cybersécurité est un voyage constant d'adaptation et d'apprentissage, et nous sommes là pour guider les entreprises à chaque étape.

> ***Il est essentiel d'embrasser les technologies émergentes.***

Julien Touzeau, Head of Cybersecurity Consulting, Airbus Protect

→ Entretien

Thiébaut Meyer

Quelles sont vos missions chez Google Cloud ?
Je suis dans l'équipe « Office of the CISO » de Google Cloud, qui est rattachée au CISO, Phil Venables. Notre équipe a deux rôles principaux. Le premier est de coordonner certains groupes de travail en interne pour s'assurer du bon niveau de sécurité de nos solutions. La seconde mission consiste à accompagner nos clients pour les aider à repenser leur stratégie de cybersécurité lorsqu'ils basculent dans le Cloud, notamment les changements à faire en termes d'approche cyber par rapport à ce qu'ils avaient l'habitude de faire sur leurs propres infrastructures. Nous travaillons avec eux pour qu'ils puissent tirer le maximum de bénéfices du Cloud et élever leur niveau de sécurité.

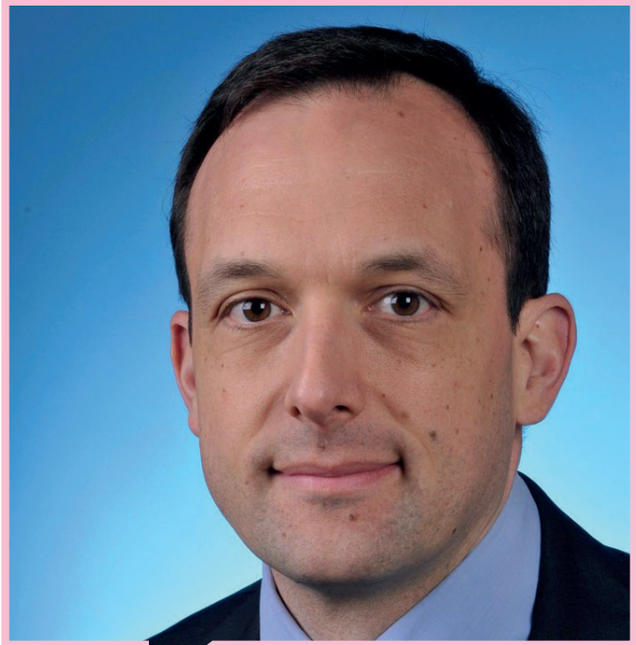
Quelles sont les principales tendances en cybersécurité actuellement ?
L'Intelligence Artificielle est un facteur de chamboulement majeur. Il y a aussi un intérêt croissant pour la sécurité des données, surtout avec la transition vers le cloud et les stratégies multicloud. Cela soulève des enjeux autour de la protection des données, souvent réparties entre différents fournisseurs, ainsi que la gestion de l'authentification, notamment avec l'approche du Zero Trust.

Comment l'IA affecte-t-elle la cybersécurité ?
L'IA change les techniques d'attaque, avec des innovations comme les deepfakes et la génération de code, mais elle aide aussi les équipes de sécurité, en comblant le manque de ressources. Par exemple, l'automatisation permet de générer des règles de détection et de faire du reverse engineering via le langage naturel, afin de maximiser la valeur ajoutée des opérateurs.

Vous avez mentionné la souveraineté. Pourquoi ne devrait-elle pas s'opposer à la sécurité ?
La souveraineté est complexe à définir. Il est nécessaire de préciser son périmètre. Est-ce une souveraineté nationale ? Est-ce une souveraineté européenne ? Entre les deux ? Chez Google Cloud, nous l'abordons avec trois piliers : la souveraineté des données, opérationnelle, et logicielle. Même si l'utilisation du cloud implique une perte de lien physique avec l'infrastructure, le contrôle n'est pas perdu. Il est essentiel de maintenir ce contrôle et la confiance des clients.

Comment se préparer à une crise cyber ?
La question n'est plus de savoir si une crise surviendra, mais quand, et si nous sommes prêts à réagir. Il est crucial de gérer la crise sous tous ses aspects, y compris la communication interne, avec les partenaires, les clients, et parfois les médias !

> ***Hope is not a strategy.***



Thiébaut Meyer, Director,
Office of the CISO, Google Cloud

→ Conférence d'ouverture

Vers une coopération européenne face aux menaces étatiques

> ***Notre défi principal est le passage à l'échelle.***

Lors de sa première intervention aux Assises de la Cybersécurité 2023 en tant que nouveau Directeur Général de l'ANSSI, Vincent Strubel invite à la fédération européenne face à l'évolution de la menace, principalement étatique. Il a souligné l'importance du travail en réseau à l'échelle européenne dont les débuts ont été « un succès qui a dépassé toutes nos attentes ». La menace ne cesse d'évoluer et de progresser pour devenir « un enjeu sociétal. Depuis 2 à 3 ans, il y a plus d'attaques opportunistes qui touchent les TPE, les hôpitaux et les collectivités »

Le Ministre d'État de Monaco, Pierre Dartout, a annoncé l'alignement de la principauté sur la directive NIS2, afin qu'elle respecte les mêmes standards de sécurité que l'Union Européenne.

Jean-Philippe Lecouffe, Directeur exécutif adjoint des opérations à Europol, partage cette même vision d'unification des forces qui ont fait leurs preuves dans certaines opérations telles que le démantèlement de Hive, Chipmixer ainsi que Qakbot. Selon lui, le partage d'informations au travers du décloisonnement de la sphère publique et privée est un atout clé pour ce type d'opération. Il évoque l'importance des outils au service du grand public comme l'Europol Malware Analysis System ainsi que la plateforme No More Ransom.

En conclusion de la conférence d'ouverture, Sabrine Guiheneuf, Présidente d'honneur des Assises 2023, a évoqué les outils de nouvelle génération, en particulier l'intelligence artificielle, soulignant leur importance tant à des fins défensives qu'offensives.

Maria Iacono, Directrice des Assises de la Cybersécurité, a ouvert une nouvelle édition dépassant les précédentes, dans un contexte toujours grandissant d'une pénurie de talents dans l'écosystème de la cybersécurité.

→ Focus photos sur la conférence d'ouverture

→ Keynote Thales

L’apocalypse quantique : mythe ou réalité ?

Serons-nous rattrapés par une apocalypse de la technologie quantique ou débordés par une guerre de machines dopée à l’IA ?

L’excellente keynote commence par souligner les investissements dans les secteurs de l’IA et de l’informatique quantique qui restent en 2023 en forte croissante avec même un croisement des investissements. L’IA a déjà un impact bien réel pour la cybersécurité, tandis que la temporalité pour le quantique reste inconnue à ce stade. Toutefois les modèles quantiques simulés affirment avec une certitude théorique que le chiffrement symétrique ou les algorithmes de hachage seront largement affaiblis. Mais c’est surtout le chiffrement asymétrique qui sera le plus touché selon Eric Brier et Pierre-Yves Jolivet.

Dans un premier temps, ils soulignent la nécessité de faire preuve d’humilité avec le quantique car de nombreux points dans ce domaine restent incertains comme l’échelle temporelle. Une certitude subsiste cependant au niveau théorique, les différents algorithmes de cryptographie devraient perdre en efficacité, voire devenir obsolètes.

Si à court terme, le risque quantique est écarté par nos intervenants, d’autres révolutions quantiques pourraient toutefois accélérer le calendrier. Souvenons-nous de la révolution des transistors en lieu et place des lampes. Le moment venu, l’accumulation et la sédimentation des systèmes deviendront de véritables défis. Il faudra faire évoluer rapidement des systèmes embarqués peu joignables, des logiques de chiffrement s’appuyant sur des algorithmes obsolètes ou encore changer des certificats ayant une durée de vie parfois de 20 ans.

> ***L'IA a déjà un impact bien réel pour la cybersécurité.***

Eric Brier, VP, Chief Technology Officer Cyber Defense Solution, Thales (à gauche)
Pierre-Yves Jolivet, Vice-Président business line Solutions de Cyber Defense, Thales (à droite)

→ Keynote Thales

L'apocalypse quantique : mythe ou réalité ?

Les ordinateurs quantiques basés sur la photonique seraient les plus intéressants car ils permettent une utilisation à température ambiante, ce qui n'est pas le cas pour les autres modèles qui nécessitent des températures proches du zéro absolu.

Si l'ordinateur quantique promet de nombreuses choses dans des domaines variés, il n'est pas la solution pour régler tous les problèmes. La perspective de disposer de QPU (quantum processor) en complément des traditionnels processeurs CPU et des très démocratisés GPU serait la perspective la plus probable pour disposer de la puissance du quantique là où cette technologie sera adaptée.

L'IA est le risque 2024. Pressée avec des déploiements mal maîtrisés, les risques sont faiblement anticipés. Pierre-Yves Jolivet souligne quelques exemples avec l'empoisonnement ou l'extraction des données d'entrainement, la corruption de modèles en particulier les autoapprenants, ou encore la conception de données spécialement conçues pour tromper l'IA.

Difficile d'appuyer tous les messages de cette keynote, tel que le message de la nécessaire évolution de la cybersécurité vers la frugalité pour faire face aux défis environnementaux. Mais la keynote appuie en conclusion que lorsque la technologie quantique sera pleinement opérationnelle, il y aura toute une part de la cybersécurité à réinventer. Tandis que l'IA accélère les processus et ouvre un changement d'échelle des cyberattaques, véritable défi auquel l'écosystème devra être confrontée.

→ Keynote Cloudflare

Stratégies pour un avenir internet défini par l'IA générative

Carrefour et Cloudflare ont parlé de l'intégration de l'intelligence artificielle dans leur activité et de l'impact que cela cause.

L'innovation étant au cœur de leur activité principale, Cloudflare, incarné par Michelle Zatlyn, se concentre sur des domaines tels que la cybersécurité, la connectivité et l'infrastructure indispensables aux entreprises pour assurer le bon fonctionnement de leurs services en ligne. D'autre part, Carrefour, représenté par Guillaume Cécile, exploite l'intelligence artificielle pour améliorer l'expérience de ses clients et optimiser l'efficacité de sa chaîne d'approvisionnement.

L'IA devient incontournable dans de nombreux domaines, et notamment en cybersécurité. Elle peut permettre de faire des prédictions sur des nouvelles attaques et de les stopper en amont. Cependant les IA génératives impliquent des risques et peuvent présenter des vulnérabilités, notamment sur la nécessité d'entrainer l'IA sur des quantités de données conséquentes. Dans cette masse de données peut se glisser des erreurs ou des aspects qui empêchent l'IA d'être sécurisée et en conformité avec le RGPD.

A ce titre, MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) présente une bibliothèque déjà très complète des tactiques et techniques contre des IA complémentaires au bien connu MITRE ATT@CK.

L'IA est donc un ensemble de technologies en pleine explosion qu'il faut suivre et manipuler avec attention. Plusieurs difficultés apparaissent comme celle soulignée lors de la keynote relative à la suppression des données client suite à une demande de suppression dans le cadre du RGPD.

Comment supprimer des données d'un modèle privé ou d'un modèle public ?

Les technologies d'IA sont des technologies nécessitant de garder un contrôle très fin sur l'ensemble de son cycle de vie.

Guillaume Cécile, RSSI Groupe Carrefour (à gauche)
Michelle Zatlyn, Co-founder, president and chief operating officer, Cloudflare (au centre)
Boris Lecoeur, Directeur Général France, Cloudflare (à droite)

→ Keynote Cisco

Cisco et les enjeux cyber des JO de Paris 2024

« Les JO vont impacter durablement le paysage de la cyber ».

Avec plus de 400 milliards de cyberattaques reportées pendant les Jeux Olympiques de Tokyo, l'organisation des JO de Paris se révèle être un défi majeur pour tous les acteurs de la cybersécurité.

Dans ce contexte, un dispositif de sécurité, orchestré par l'ANSSI en collaboration avec la DIJOP et le MIOM, a été mis en place et s'articule autour de cinq axes : parfaire la connaissance des menaces cyber pesant sur les Jeux, sécuriser les systèmes d'information critiques, protéger les données sensibles, sensibiliser l'écosystème des Jeux, se préparer à intervenir en cas d'attaque cyber affectant les Jeux.

La sensibilisation, l'accompagnement technique, les audits de cybersécurité font partie des éléments-clés de la stratégie, visant à renforcer la sécurité des acteurs critiques. Cisco, en première ligne, s'appuie sur son expérience avec la NFL pour déployer un SOC opérationnel 24/7. Les enjeux sont clairs : maintenir l'intégrité de l'écosystème numérique, en passant par les infrastructures de chronométrage, jusqu'aux plateformes de billetterie, tout en garantissant la protection des données traitées.

La collaboration étroite avec les partenaires et la préparation proactive sont la clé de cette architecture de sécurité, prête à résister et à se remettre d'attaques potentielles. La France se prépare à un tournant cyber durant les JO, où la réussite se doit d'être sportive et surtout numérique.

Anthony Grieco, CISO, Cisco (photo gauche)
Franz Regul, DSI, Paris 2024 (photo gauche)
Eric Greffier, Business and Technology Director, Cisco (photo droite)

→ Keynote Pentera

Comment la cybersécurité peut apprendre d'IKEA ?

L'approche novatrice d'IKEA, basée sur la simplicité, le caractère abordable et l'innovation ont révolutionné l'industrie du mobilier, mais peuvent-ils être appliqués à la Cybersécurité ?

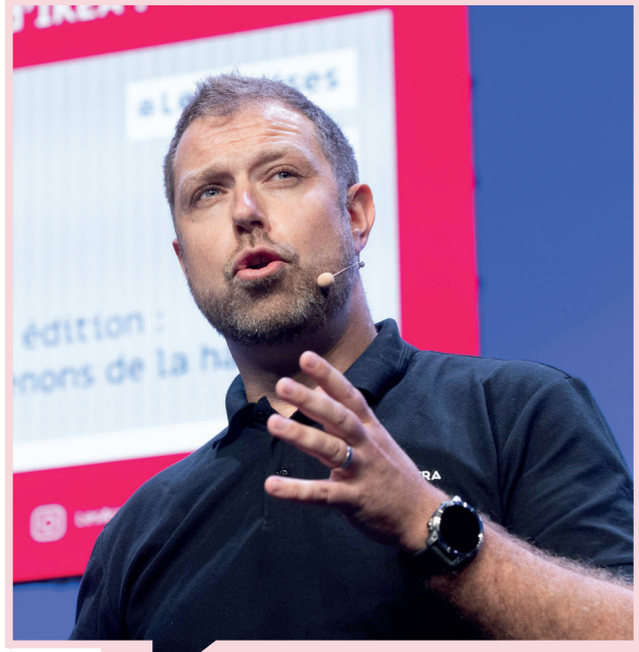
William Culbert, Sales Director, France & Benelux, Pentera, société spécialisée dans l'«Automated Security Validation™ », souligne l'augmentation et la complexification des attaques modernes et propose une nouvelle approche de la sécurité de l'information : une validation complète et continue de l'écosystème de sécurité.

Si le Framework du NIST est encore repris dans cette présentation, William Culbert met en avant aussi une prédiction 2023 de Gartner, que les entreprises doivent aller au-delà de la gestion de la menace pour s'étendre vers la gestion de l'exposition. Le défi dans la gestion de l'exposition est de connaitre la surface d'attaque, les vulnérabilités et de valider que le niveau de risque de l'ensemble est acceptable.

Comment répondre à ce défi avec des systèmes d'information dont l'exposition, les vulnérabilités et le niveau de risque changent dans des proportions industrielles ? L'idée de la conférence était de faire une jonction avec des industriels ayant mis l'accent sur l'automatisation pour être au cœur de cette stratégie de passage à l'échelle.

L'automatisation est là pour démultiplier les ressources humaines et sans faire de compromis. Il faut donc reprendre toutes les techniques connues telles que celles du MITRE ATTACK, les prioriser et traduire les efforts à mener. Le processus de validation de l'ensemble des SI est au cœur de l'optimisation des efforts face aux cyberattaques. L'objectif est d'identifier les techniques, tactiques et procédures utilisées par les cybercriminels et d'adapter la posture de cybersécurité. Pour réaliser cette promesse, il est nécessaire de mettre en place des moteurs offensifs, de prioriser les vulnérabilités et en adaptant dynamiquement les systèmes défensifs.

Enfin l'automatisation ne remplace pas des audits réguliers, essentiels pour valider la posture globale et la résilience.



William Culbert, Sales Director, France & Benelux, Pentera

→ Conférence plénière

Les notes qui s'aiment

Art et cybersécurité sont deux domaines que tout semble opposer, et pourtant, André Manoukian les rapproche avec habileté à travers l'histoire et les fondamentaux de la musique.

La logique est le pilier sur lequel repose l'ensemble de la musique. Les notes, gammes, harmoniques, consonance et dissonance sont toutes liées à des principes mathématiques. Tout comme un ingénieur construit des édifices complexes à partir de bases élémentaires, les musiciens créent des chefs-d'œuvre en suivant des règles de base. Cette vision, bien que logique et méthodique, n'occlut aucunement l'intuition et l'inspiration, essentielles à tout créateur.

L'écoute est le fondement de toute collaboration fructueuse. La splendeur d'un orchestre émane de l'harmonie entre les musiciens attentifs et adaptatifs les uns aux autres. Un compositeur talentueux est celui qui perçoit 'les notes qui s'aiment' et sait les fusionner, une compétence qui n'est pas sans rappeler celle d'un bon manager.

L'audace, enfin. Les compositeurs, au fil des siècles, s'inspirent et transgressent les enseignements de leurs prédécesseurs. Remettre en question les connaissances acquises, se détacher des héritages et croire en sa capacité à surpasser l'existant requiert une confiance presque poétique. C'est cela le moteur de l'évolution des connaissances, c'est cela qu'il faut encourager.

André Manoukian
Auteur-compositeur, chroniqueur

→ Mise à l'honneur

Prix de l'Innovation

Le Prix de l'Innovation a mis à l'honneur cette année la société Patrowl, Lauréate du Prix de l'Innovation 2023 lors des Assises de la Cybersécurité 2023.

Dans un monde en constante évolution, les entreprises sont confrontées au défi de sécuriser leurs actifs exposés sur Internet, tels les sites web et applications SaaS. Dans ce domaine, la startup française fondée en 2020 se démarque en proposant une solution de sécurité offensive as-a-Service. Patrowl permet la gestion de l'exposition externe des clients ainsi que sa sécurisation tout en étant accessible sur le plan technique. Cette solution s'attaque particulièrement à trois défis majeurs. Elle aide à retrouver la visibilité sur les actifs exposés. Cette découverte en continue garantit une cartographie exhaustive même des éléments non gérés ou oubliés, donnant aux entreprises le contrôle nécessaire sur leurs surfaces vulnérables en ligne. En outre, les alertes en temps réel et la surveillance constante permettent de rester informé des menaces et vulnérabilités afin de réagir rapidement pour minimiser les risques. Patrowl automatise également de nombreuses tâches de cybersécurité, telles la qualification et hiérarchisation des risques, pour libérer du temps à l'entreprise. Cette démarche permet aux équipes de sécurité de se concentrer sur les projets stratégiques ainsi que faire face à la pénurie de talents en cybersécurité grâce à son accessibilité.

Succès et défis à venir

Vladimir Kolla, co-fondateur derrière le succès de Patrowl, partage les clefs qui ont poussé son entreprise à remporter le Prix de l'Innovation des Assises lors de l'édition 2023.

L'entreprise commercialise initialement un logiciel d'automatisation de tests d'intrusion. Ce premier logiciel a ensuite été remplacé par la solution que l'on connaît aujourd'hui, avec un niveau d'abstraction plus élevé. Cette transformation d'une solution technique et complexe vers un outil plus accessible constitue un tournant stratégique chez Patrowl.

La solution se positionne comme un rempart face à la montée en puissance du marché de la cybercriminalité. Les règlementations européennes comme NIS2 et DORA qui imposent une automatisation de certains tests d'intrusion devraient permettre à Patrowl de connaître une belle évolution.

Avec une évolution constante de la menace, propulsant le risque cyber parmi les premiers risques redoutés par les entreprises. Les budgets consacrés à la cybersécurité augmentent et avec l'approche des Jeux Olympiques, la France est confrontée à un vrai défi de sécurité numérique. La vision de Vladimir Kolla est claire : Patrowl cherche à se positionner comme une entreprise innovante afin de façonner l'avenir de la cybersécurité.

// Pour aller plus loin :
L'interview podcast de Vladimir Kolla, Co-fondateur de Patrowl, la success story du «hibou qui patrouille» !

Prix de l'Innovation LA 23

Patrowl

→ Podcast

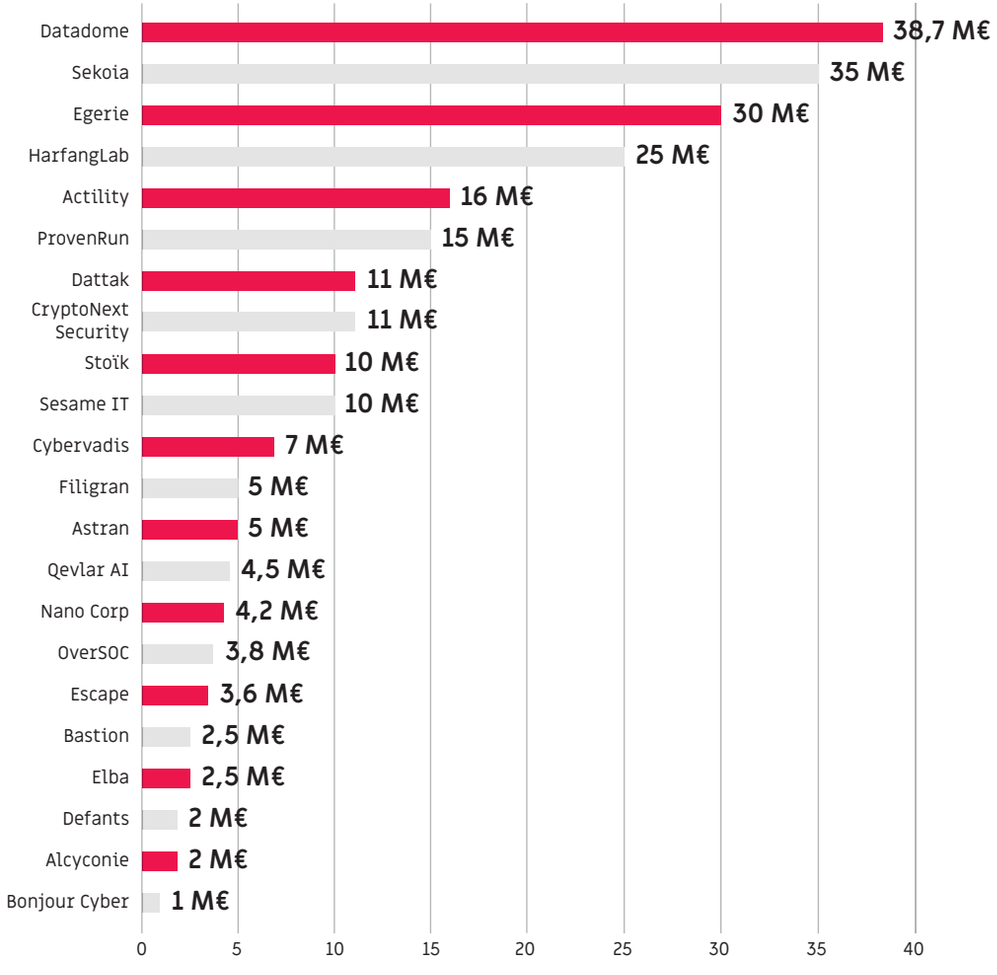
Vladimir Kolla

Vladimir Kolla,
Co-founder, Patrowl

→ Le radar des startups de l'édition 2023

Les belles levées de fonds de 2023 !

(en millions d'euros)



Elles ont fait parler d'elles en 2023 !

OLVID

Le Gouvernement adopte **Olvid** comme nouvelle messagerie sécurisée ! Clin d'œil à la start-up française élue Prix de l'innovation des Assises en 2021

PR0PH3CY

La start-up française de cybersécurité **Pr0ph3cy** rachetée par le fonds Carlyle pour un peu moins de 100 millions d'euros !

MINDFLOW

Mindflow qui a remporté la finale de l'European Cybersecurity Organisation à Bilbao lors du mois de juin 2023. Cette mise en lumière a contribué à lui donner de la visibilité auprès d'investisseurs dans l'objectif d'une levée de fonds prévue avant la fin de l'année.

Les startups qui se sont démarquées

ONEKEY · ASTRAN · dust MOBILE · escape · FILIGRAN · Patrowl · ANOZR WAY PEOPLE-CENTRIC CYBER PROTECTION · sekoia · mindflow

→ Table ronde

On a oublié que la porte d'un bâtiment s'ouvre

Cette table ronde a abordé le sujet sensible de la sécurité physique des systèmes d'information est un enjeu crucial pour les DSI, notamment en raison de l'essor de l'Internet des Objets (IoT) et des bâtiments intelligents (smart building). Un nouveau monde supplémentaire objet de défis pour les DSI habitués à sécuriser et gérer des systèmes d'information classiques. Mais qu'en est-il de systèmes informatiques de climatisation, de sécurité physique ou encore des capteurs incendies ? La table ronde revient donc sur l'état de la situation. Si historiquement, tous ces silos fonctionnels d'un bâtiment étaient séparés et isolés (AirGap), ils sont aujourd'hui de plus en plus interconnectés (en radio ou en filaire), ouverts et pilotés par des applications pour valoriser les usages d'un bâtiment. Le smart bulding dé-silote les fonctions, les usages et les problèmes.

Même si l'état de l'art de ce qu'il faudrait faire est connu par les professionnels, le bilan dressé de la réalité dans la table ronde peut paraître une nouvelle fois inquiétant. D'abord parce que les attaques exploitant ces faiblesses physiques pour mener une cyberattaque sont moins documentées, ensuite parce que ces bâtiments prennent encore rarement en compte lors de la conception ces besoins de cybersécurité. Il faut concevoir des bâtiments qui auront une durée de vie de plusieurs dizaines d'années et des cas d'usage qui évolueront.

Le COVID a par exemple nécessité d'ouvrir des accès à distance à de nombreux systèmes de maintenance exposant ainsi des fonctions critiques à de nouvelles attaques. L'explosion des bureaux flex a déresponsabilisé les collaborateurs sur la vigilance de proximité, par exemple face à un équipement pirate connecté au SI.

La table ronde a souligné toutefois que les équipementiers d'IoT ont pris le sujet en main et que la recherche de vulnérabilités sur les objets est de plus en plus complexe. Mais elle n'enlève pas les mauvais usages comme les identifiants par défaut, encore trop souvent présents.

Si la sensibilisation des collaborateurs reste une nécessité pour des scénarios simples tels que réussir à passer la sécurité en portant des cartons, il devient nécessaire aussi de prendre en compte de nouveaux scénarios comme la démocratisation des drones pour atteindre en proximité les systèmes d'information et la gestion technique bâtimentaire (GTB).

Sont intervenu.e.s sur cette table-ronde
(photo du haut, de gauche à droite) **:**

Annick Rimlinger, Directrice Sûreté-Sécurité, Cyber & DataProtection, Aéma Groupe

Frank Van Caenegem, VP Cybersecurity, CISO EMEA, Schneider Electric | Board member, CESIN

Amaury Pitrou, Co-fondateur & Directeur Général Smalt - Bouygues Construction

(photo du bas, de gauche à droite) **:**

Brice Augras, Président-fondateur, BZHunt

Victor Poucheret, Directeur Technique Associé, BZHunt

→ Table ronde

Chamboulement du monde et offensive réglementaire : un nouveau casse-tête pour les RSSI ?

Cette table ronde passionnante a abordé l'une des plus grandes difficultés pour les RSSI, concilier les enjeux de compliance à géométrie variable, de gestion du risque et de déclinaison dans les organisations.

Devant cette avalanche, cette inflation de réglementations sectorielles et géographiques, sans oublier les conditions générales d'usage des solutions, il est devenu impossible pour le RSSI de ne pas rechercher des appuis dans l'organisation et des arbitrages. Aligner le système d'information n'a jamais été aussi difficile et nécessite toujours plus de ressources qualifiées et d'embarquer des approches de cybersécurité cohérente dans les solutions.

La table ronde dresse ainsi quelques constats. L'apparition massive de réglementations en Asie, impactant significativement le choix des solutions. La localisation des données est typiquement au cœur de cet enjeu. Cette régionalisation des réglementations balkanise un peu plus le cyberespace. L'UE n'est pas en reste, avec l'effet post-COVID et la proximité des élections, qui entrainent une sortie massive de textes et de propositions dont les différentes autorités locales peinent à décliner les transpositions et modalités pratiques (cyberscore, NIS2, etc.).

NIS2 a entraîné une augmentation de 22% des projets de cybersécurité, engendrant des problématiques structurelles, de planifications et d'homologations. Les ressources limitées et les retards dans les normes commerciales sont des obstacles majeurs et le déséquilibre entre les moyens des entreprises et les réglementations est évident, seules les grandes entreprises peuvent s'y conformer efficacement. 160 000 organismes sont concernés dans l'UE et cela va nécessiter à des entreprises non régulées jusque-là de franchir un gap de maturité et de parfois s'adapter à ces spécificités locales.

Les intervenants de la table ronde conseillent que le RSSI soit inclus au comité des risques de l'entreprise pour faire valoir ses enjeux et les chartes informatiques et être constamment mises à jour. Toutefois, la conformité ne garantit pas la sécurité.

Modérateur : Eric Domage,
observateur des univers IT B2B

Sont intervenu.e.s sur cette table-ronde

Maricela Pelegrin-Bomel, RSSI, EFS

Rayna Stamboliyska, CEO at RS Strategy & Digital
EU Ambassador at European Commission

Thierry Auger, Deputy CIO and CSO, Lagardère

→ Table ronde

Numérique responsable : nous ne pouvons pas regarder ailleurs

> ***Le numérique est responsable de 4% des émissions à effet de serre.***

Le numérique est responsable de 4 % des émissions de gaz à effet de serre, en raison des évolutions technologiques et de nos pratiques qui augmentent la consommation de ressources naturelles. Pour limiter son impact environnemental, il est nécessaire d'intervenir sur toute la chaîne de production, depuis l'extraction des matériaux jusqu'au recyclage des appareils. Comme souligné au cours de cette table ronde, le numérique doit aussi être un acteur de la transition écologique et sociale, en encourageant une collaboration globale face aux défis du Green IT, de l'IT for Green et de l'inclusion numérique.

Ces enjeux de numérique responsable ont suscité des attentes chez les clients des prestataires de cybersécurité. Les participants à la table ronde ont exposé plusieurs initiatives mises en œuvre au sein de leurs organisations, comme l'intégration d'objectifs RSE dans les chartes, l'allongement de la durée de vie des appareils ou la diminution des documents stockés en doublon. Il existe ainsi un lien entre le numérique responsable et la cybersécurité, reposant sur des méthodologies parallèles et complémentaires. Cependant, les mesures évoquées lors de la table ronde manquent encore d'un référentiel complet et unifié, qui permettrait une évaluation et une comparaison efficaces.

Sont intervenu.e.s sur cette table-ronde *(de gauche à droite)* **:**

Andrada Dugan, Innovation & Sustainability Director, ISS France

Marie Ait Daoud, Green IT Manager - DSI Groupe VINCI

Pierre-Luc Refalo, VP - Head of Group «IT & Cyber Security» Audit, Capgemini

Sabrine Guihéneuf, Directrice Groupe Cybersécurité et Gouvernance IT URW et Administratrice du CESIN

→ Table ronde

Threat Intelligence ı / Cybercriminels o !

Les signaux en CTI (Cyber Threat Intelligence) sont essentiels pour permettre aux organisations de détecter efficacement les menaces. Certains signaux peuvent ne pas être considérés comme suspects mais sont parfois les prémices d'une attaque. Ces événements pris individuellement vont souvent générer des faux positifs mais dans des contextes particuliers, ils généreront des alertes. On peut qualifier ces événements de signaux faibles.

Les signaux faibles sont souvent identifiés à la suite d'un incident. Les intervenants pensent donc qu'une approche communautaire est une bonne piste afin de faciliter la qualification de ces signaux. La collecte massive de données semble donc être essentielle au succès de ces détections.

L'accent est aussi mis sur les signaux répétitifs et que les signaux faibles dépendent fortement du contexte et évoluent dans le temps. Plusieurs signaux considérés comme faibles aujourd'hui peuvent devenir un signal fort demain.

La gestion des signaux faibles nécessite de fait une équipe spécialisée, composée d'experts techniques, de pentesters, d'administrateurs et de spécialistes des processus.

Une infrastructure de base avec journalisation, un SIEM, plateforme de CTI et SIRP est requise avant de monter une telle équipe. Les résultats attendus sont des règles de détection, des scénarios d'attaque et un catalogue de procédures.

Détecter des signaux faibles, est-ce un puits sans fond pour la cybersécurité ?

Sont intervenu.e.s sur cette table-ronde :

Photo de gauche (de gauche à droite) :
Julien Bachelet, Global CISO & Directeur Cybersécurité, Hermès
Sabine D'Argœuves, Responsable Cyberdéfense, d'un grand groupe industriel
Axel Castadot, Directeur National Crise des Systèmes d'Information à la SNCF
Arnaud Kopp, Chef du Bureau Coordination et partenariats opérationnels à l'ANSSI

Photo de droite :
Jérôme Saiz, Expert en protection des entreprises chez OPFOR Intelligence

→ Table ronde

Industrie 4.0, « un grand pouvoir implique de grandes responsabilités »

Une table ronde pour mettre en valeur un défi majeur de la cybersécurité, celui relatif à l'industrie. L'industrie française est un pilier incontournable de notre économie représentant 13,5% du PIB marchand. L'arrivée de l'industrie 4.0 dans ce paysage s'annonce comme une révolution, plaçant la donnée au cœur de la transformation pour améliorer la productivité, optimiser les processus, assurer la traçabilité et le tout en intégrant de nouvelles technologies.

Les environnements industriels 4.0 sont complexes et hétérogènes. Pour bien démarrer une transformation digitale, il est important de comprendre comment ils fonctionnent et soutiennent les processus industriels. Seule une vision holistique permet d'être pertinente dans l'approche de la transformation et crédibilise auprès de toutes les parties prenantes.

Les intervenants de la table ronde recommandent ainsi la définition d'un framework adapté permet d'avoir les mêmes fondamentaux sur tous les sites pour travailler sur des bases solides. Ce framework organisationnel, technologique et opérationnel doit être réfléchi sans oublier les acteurs du terrain et se déployer progressivement.

La transformation s'appuie sur 3 points clés. Le premier est la standardisation des technologies dans tous les sites tout en s'adaptant aux besoins de chacun. Elle permet d'homogénéiser les processus et faciliter la gestion opérationnelle. Le second est le modèle opérationnel à adopter. Il passe par la confiance entre les acteurs ainsi que la confection de standards globaux et locaux. Il doit également intégrer les partenaires dans cette transition.

La table ronde souligne une nouvelle fois le besoin RH. Qui va s'occuper de la cybersécurité et de ces technologies ? Recruter des talents ayant la bonne réponse et au bon moment est un challenge permanent. Les intervenants recommandent aussi de ne pas négliger le développement des équipes existantes attirées par la cybersécurité.

Transformer l'organisation autant que sa technologie pour prendre en compte la cybersécurité, le RSSI est au cœur des enjeux.

Modératrice : Sabine D'Argœuves, Responsable Cyberdéfense, Danone

Sabri Khemissa, Group ICS/OT Cybersecurity Manager, Imerys
Thierry Manciot, Head of Cyber Security for network and Manufacturing & Supply, Sanofi
Bertrand Aït-Touati, Industrial CyberSecurity Program Director, Suez

→ Meet-up

Venez découvrir les vulnérabilités de votre organisation grâce à l'OSINT

L'OSINT (Open Source Intelligence) ou ROSO (Renseignement d'Origine Sources Ouvertes) consiste en la collecte et l'analyse d'informations publiquement accessibles. Sylvain Hajri, co-fondateur de la communauté OSINT-FR et fondateur du service Epieos, a mis en lumière lors de ce meetup illustré par de nombreux exemples pratiques, l'importance des informations librement accessibles de l'organisation et des individus qui la compose, pour mener à bien des cyberattaques.

Dans le domaine de la cybersécurité, l'OSINT n'est pas une nouveauté. Toutefois l'OSINT a globalement pris une part significative dans toutes les actions de renseignement, de ciblage ou encore visant à réaliser une fraude. Qu'il soit d'ordre criminel, lié au service de renseignement, aux forces de l'ordre ou aux professionnels de l'intelligence économique, ce savoir-faire se diffuse de plus en plus et doit devenir aussi une composante de la cybersécurité des organisations. Il faut connaitre et maitriser l'exposition numérique des organisations et de ses individus.

Sylvain Hajri cite d'ailleurs le LTG Samuel V Wilson, ancien directeur de la DIA, où 90% du renseignement serait d'origine en source ouverte. Le conflit russo-ukrainien est pour lui une révolution en matière d'usage de l'imagerie satellite en source ouverte pour suivre ou connaitre des éléments sensibles du conflit. La sécurité physique d'une organisation (localisation d'un site sensible, reconnaissance des accès du bâtiment, badge et technologie employés, etc.) est aujourd'hui facilement collectable. Des intrusions physiques comme élément d'action dans une cyberattaque sont aujourd'hui une réalité.

Sylvain Hajri, Spécialiste de l'OSINT et de la cybersécurité, Fondateur de Epieos, co-fondateur de OSINT-FR

→ Meet-up

Venez découvrir les vulnérabilités de votre organisation grâce à l'OSINT

Si ces informations sont de plus en plus accessibles, Sylvain Hajri présente aussi de nombreux points de vigilance pour une organisation à contrôler régulièrement. Les sources citées restent bien connues (linkedin, archives.org, ..) mais il « faut savoir chercher l'information et savoir l'exploiter ». Il démontre par exemple la nécessité de protéger en profondeur les organisations jusque dans la sphère privée.

S'il est interdit et même contrôlé que les employés n'exposent pas leur appartenance à une entreprise sensible sur linkedin, il cite l'exemple des communautés sportives spontanées de type STRAVA où les courses à pied du midi pourraient bien avoir raison de l'organisation avec l'appartenance et le comportement prévisible des employés.

Dans ce meetup, Sylvain Hajri démontre aussi que l'internet n'oublie pas et regorge de sources permettant de disposer d'informations avec une profondeur historique. Ces mines d'informations largement accessibles sur la sphère personnelle et professionnelle permettent ainsi d'apporter à l'attaquant une supériorité informationnelle et ainsi une crédibilité pour mener à bien des opérations de fraude et d'ingénierie sociale.

L'OSINT est un savoir-faire exploitant les détails et un état d'esprit visant à détourner toutes les fonctionnalités et informations exposées. Un véritable défi pour une organisation pour faire face et un savoir-faire à mettre en place pour s'en protéger.

→ Meet-up

Directive NIS2 : Comment l'anticiper ? Le compte à rebours est lancé !

En décembre 2022, la Commission européenne a adopté la Directive NIS2, destinée à renforcer la cybersécurité au sein de l'Union européenne. La transposition de cette directive en droit français est prévue avant le 17 octobre 2024, mais la loi de transposition demeure pour l'instant inconnue. Des ateliers de travail sont en cours avec l'ANSSI afin de guider cette transition.

La portée de la NIS2 s'étend bien au-delà de son prédécesseur, la directive NIS1 de 2016. Ce nouveau texte impactera également les entités de petite taille (plus de 50 salariés), indépendamment du chiffre d'affaires ou du secteur d'activité.

Une étude d'impact révèle une augmentation significative des budgets en cybersécurité, avec 22% pour les entreprises et 30% pour les administrations. Les lois de transposition varieront d'un État membre à l'autre en Europe, introduisant des différences de formalismes et de délais.

La sensibilisation des dirigeants est cruciale, avec des sanctions administratives pouvant atteindre des chiffres d'affaires en millions d'euros. La responsabilité pénale individuelle des dirigeants reste floue, tout comme son éventuelle gestion par l'ANSSI.

NIS2 énumère des mesures de sécurité détaillées dans le cadre d'actes d'exécution, avec une approche harmonisée entre les États membres. En France, cela se traduit aussi par des mesures de sécurité liées à la « cyber hygiène » (robustesse des mots de passe, récurrence des sauvegardes, etc.).

La définition d'un incident de sécurité majeur est renvoyée au législateur, mais l'ANSSI exige des points de contact définis et un délai de 24 heures pour signaler un incident. Des formulaires d'application harmonisés sont espérés pour faciliter les déclarations.

La gestion des entreprises travaillant avec plusieurs acteurs européens nécessitera une coordination complexe, avec plusieurs déclarations et des chefs de projet dédiés. Les petites entreprises en bas de la chaîne de production s'inquiètent quant à elles de l'applicabilité réaliste de la directive.

Garance Mathias, Avocat Associée, Mathias Avocats
Cynthia Chassigneux, Avocate, CHX Avocat

→ Regards croisés

Comment est perçue la cybersécurité par les métiers ?

L'intervention de Bruno Bouygues, PDG de Gys, ETI française de 1000 employés, nous partage sa vision stratégique en cybersécurité.

Initialement spécialisée en métallurgie, Gys est un constructeur de postes à souder et de chargeurs de batterie. Cette entreprise consacre aujourd'hui 13% de ses dépenses informatiques en cybersécurité et vise un parc d'objets connectés de 10 millions d'unités d'ici 10 ans. Les principaux défis rencontrés par ce genre d'entreprise sont la sécurisation des usines et la complexité croissante des produits, devenant des vecteurs de problèmes de cybersécurité dans une chaîne de production plus complexe chez leurs clients.

La stratégie de l'entreprise est parfois confrontée à des demandes divergentes. La volonté des collaborateurs de numériser tous les processus de fabrication et d'utiliser le cloud comme vecteur, face à une direction générale soucieuse de protéger ses usines et de limiter les interactions avec ce type de solution. Les clients sont également une source d'exigences variées, comme le secteur du nucléaire qui attend une traçabilité maximale, tandis que le secteur de l'automobile préfère limiter les communications réseaux.

Selon Bruno Bouygues, la cybersécurité des produits souffre du manque de standards, nécessitant une adaptation à chaque projet, sans communication entre les fournisseurs. La certification TISAX (Trusted Information Security Assessment eXchange), qui est un référentiel international de sécurité de l'information pour l'industrie automobile, est un premier pas vers une mise en place de normes sectorielles pour son activité.

Le dernier défi est de résoudre l'équation économique. La question de mettre en place aujourd'hui un EDR ou encore de sécuriser des îlots numériques industriels ne se posent plus. Comme le domaine RSE pour une entreprise, la cybersécurité évolue vite et nécessite de s'adapter à ses nouveaux défis.

Le point de vue stratégique a permis de comprendre l'intérêt de la cybersécurité et les aspects de son entreprise à protéger. Les secrets de production étant moins sensibles selon lui chez les constructeurs, que la protection cruciale du processus de production.

Paul Lemesle, Chief Information Security Officer, Groupe Lactalis
Bruno Bouygues, PDG, GYS

→ L'édito de Sébastien Bombal

La cyber tous azimuts

Le grand rassemblement annuel des RSSI lors des Assises de la cybersécurité a bien montré dans cette édition l'amplitude toujours plus importante des domaines à traiter, les chocs qui nous attendent et les défis technologiques et organisationnels à relever.

Cette édition 2023 esquisse comme toujours les tendances de l'année à venir avec par exemple l'incontournable sécurité des grands évènements tels que les JO 2024 ou encore la prise en compte des risques et opportunités de l'OSINT, ou ceux de la cybersécurité des IA et de ces nouveaux usages avec l'explosion des « Large Language Model » LLM et des IA génératives.

Le corpus réglementaire n'est pas en reste d'évolutions pour le RSSI avec l'arrivée de la transposition de NIS2, DORA, CER soulignant encore une fois l'importance de la prise en compte du besoin de résilience face aux risques cyber.

Mais ces nouveautés ne sauraient faire oublier les nombreux sujets déjà présents dont il reste tant à faire.

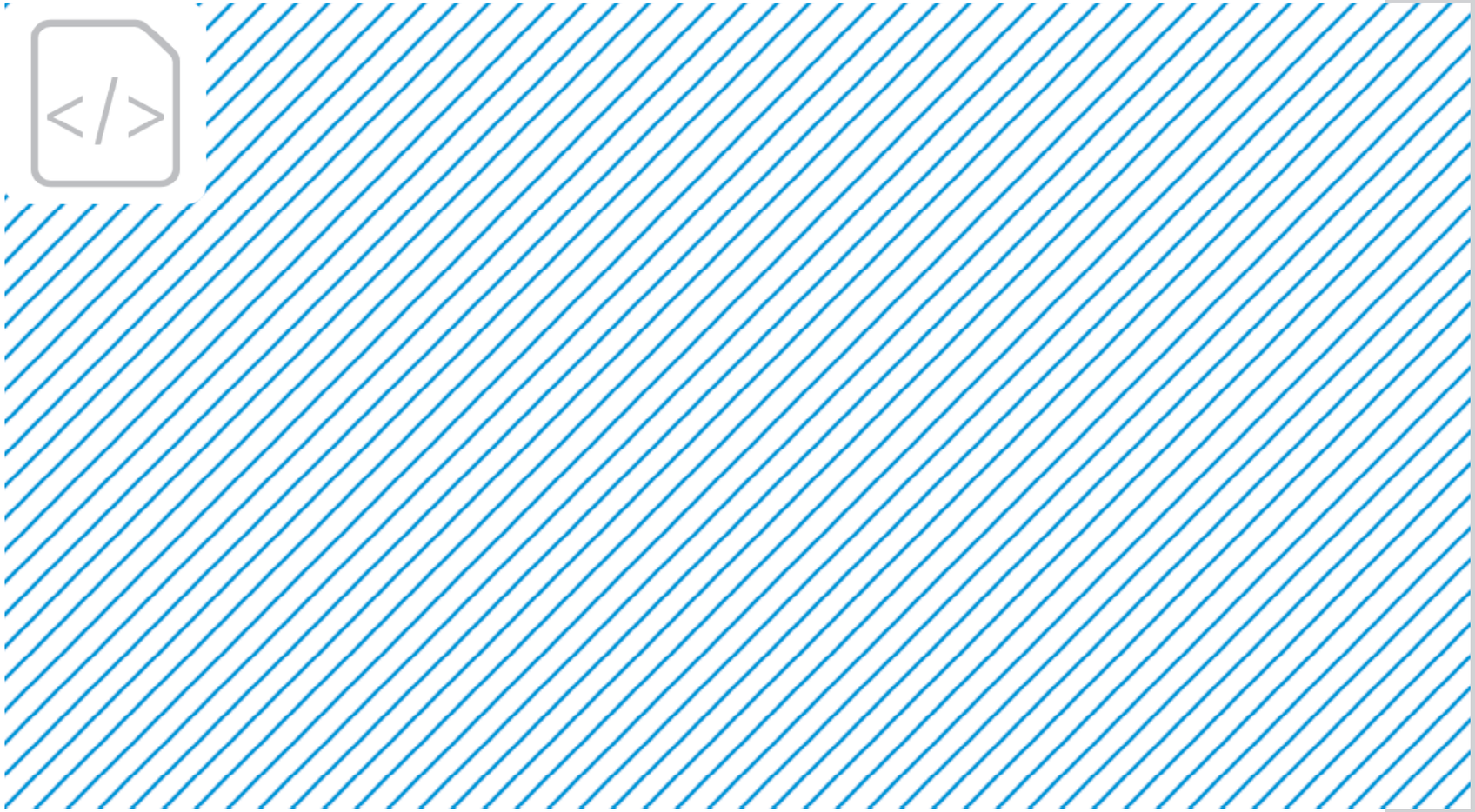
Si la politique publique s'invite maintenant pleinement dans les débats, les stratégies et le financement de l'écosystème, cette édition 2023 marque une nouvelle étape de maturité dans le domaine. Les éditions des Assises se succèdent mais ne se ressemblent pas.

L'innovation toujours aussi présente atteste du dynamisme et de la santé du secteur, avec en particularité une progression fulgurante de l'IA et de l'automatisation dans les produits pour aider et soulager les experts.

Ce 6ème livre blanc réalisé par les étudiants de la majeure système réseau et sécurité de l'EPITA, en partenariat avec l'organisation des Assises, essaie de synthétiser modestement quelques prismes de cet écosystème bouillonnant. Je tiens à les remercier profondément pour cette réalisation, sans oublier Maria Iacono, Axel Vergnerie et toute l'équipe des Assises, sans qui tout ceci n'aurait pu voir le jour.

Sébastien Bombal,
Directeur Technique douanes

→ Votre avis compte !



À l’année prochaine !
09.10 → 12.10.2024