Les 5èmes Rencontres SSI Santé de l'APSSIS
Jeudi 13 novembre 2025

***A**ssociation **P**our la **S**écurité des **S**ystèmes d'**I**nformation de **S**anté*
https://apssis.com/117/les-rencontres-ssi-sante-de-lapssis-2025

---ooo---

En 2024, la Maison des Polytechniciens avait accueilli les 4èmes Rencontres SSI Santé de l'APSSIS. **Les 5èmes Rencontres SSI Santé** de l'APSSIS se sont tenues le jeudi 13 novembre 2025 dans les Salons de l'hôtel des Arts & Métiers, au 9 bis avenue d'IENA Paris 16ème.

Voici mes impressions sur cette merveilleuse et édifiante journée

Marie-Valentine BELLANGER, secrétaire de l'Association qui est un peu plus loin et en retrait sur la photo, avec à sa gauche Hélène DASPE au premier plan, directrice déléguée de l'APSSIS, nous accueillent, dès 10h00 pour le café de bienvenue et la distribution des badges. Vincent TRELY, président de l'APSSIS, n'est pas loin. A 10h30, il va nous inviter à gagner le salon où va se dérouler cette journée qui sera parfaitement réussie, et qui se terminera par un repas de gala jusqu'à 22h30.

110 invités, professionnels impliqués dans la sécurité de l'information (en particulier dans le domaine hospitalier), ingénieurs, juristes, institutionnels, journalistes, participent à cet évènement.

Cette journée, au cours de laquelle sont intervenus de nombreuses et de nombreux spécialistes, a été orchestrée par une journaliste, productrice de podcasts, **Anna PUJOL-MAZZINI**, qui a réalisé l'exploit de permettre à chaque intervenant de s'exprimer dans un temps contraint. L'horaire prévu a ainsi été scrupuleusement respecté.

Voici, en haut à gauche, Anna à l'œuvre, au cours de la journée avec un des intervenants. Même durant chaque pitch de seulement 10 minutes, il n'était pas question de dépasser l'horaire prévu. Tâche difficile mais accomplie avec délicatesse et avec le sourire. Bravo Anna !

Mais avant le début formel de l'évènement, je retrouve les amies et les amis de l'APSSIS. C'est aussi un des grands moments de ces rencontres.

Voici des photos prises avec mon smartphone, en mode selfie, nous sommes plongés dans l'ambiance amicale de ces rencontres.

Avec Thomas VADOT RSSI du CH Intercommunal de Haute-Comté

Avec Vincent TRELY président de l'APSSIS

Avec Cédric CARTAU RSSI du CHU de Nantes

Avec maître Omar Yahia Avocat au Barreau de Paris

Les groupes se forment, ça discute, poignées de main, échanges de cartes de visites, discussions avec les partenaires de l'évènement et on arrive à 10h 30.

Vincent TRELY ouvre ces 5èmes Rencontres SSIS

Nous gagnons nos places. Nous sommes, rappelons-le, le 13 novembre 2025. Aussi Vincent TRELY commence par rendre un hommage aux victimes des attaques terroristes de 2015.

Parmi les participants se trouve Thomas VADOT, visible sur le selfie au-dessus. Thomas a vécu, il y a un mois, une expérience très particulière, mais qui hélas peut arriver à d'autres participants assis dans la salle.

Parlons-en puisque j'écris mes impressions sur cette journée. Je connais bien Thomas qui a été, cette année, un de mes élèves du MBA Cybersécurité de De Vinci Executive Education, à Nanterre. Il a écrit sa thèse professionnelle, qui terminait son MBA sur le sujet : « *Impact des cyberattaques sur la continuité des soins dans les hôpitaux publics français : Études de cas et stratégies de mitigation* » qu'il a soutenu en septembre. 170 pages de théorie sur les cyberattaques et leur remédiation. Comme directeur pédagogique de sa thèse professionnelle, je lui avais mis une très bonne note.

Mais sa théorie allait dès le mois suivant, hélas, trouver une implication très pratique. Tôt dans la nuit du dimanche 19 octobre, le Centre Hospitalier de Pontarlier, pour lequel il est responsable de la cybersécurité, subissait une violente cyberattaque (attribuée à une mafia russe ? On connait un nom, pour cet agresseur, mais comme l'enquête est toujours en cours, on évitera d'en faire mention). Fichiers chiffrés, plus de SI, plus de téléphonie ! Retour au papier crayon. Cinq experts, cyber-pompiers de l'ANSSI sont venus au secours de son hôpital. Je vous laisse imaginer ce que Thomas a vécu.

Enfin, le plan de continuité et le plan de reprise d'activité lui ont rendu son sourire, voyez sur le selfie. Thomas évoquera ce qui lui est arrivé durant la dernière conférence de la journée.

Vincent TRELY nous dit un mot sur la mésaventure de Thomas. Quelle belle illustration d'un cas concret ! Puis Vincent indique le déroulement de la journée : 6 conférences de 40 minutes, 11 pitchs de 10 minutes et une dernière conférence, le soir, avec Judith NICOGOSSIAN, Docteure en anthropologie, sur le sujet « *L'humain au cœur de la crise* ». Après les interventions plutôt techniques, le côté humain a trouvé sa place.

Il y aura des pauses, il y aura le buffet déjeunatoire et le dîner de gala. Autant d'occasions de se retrouver ou de faire connaissance.

Conférence institutionnelle – Interview de Christophe MATTLER par Vincent TRELY - Président de l'APSSIS et Auriane LEMESLE - Secrétaire générale de l'APSSIS

Christophe MATTLER est le Directeur du Programme CaRE (Cyber accélération et Résilience des Établissements) à la Délégation au Numérique en Santé (DNS) du ministère de la Santé.

Le programme CaRE vise à accélérer la mise à niveau des systèmes d'information hospitaliers face à l'état de la menace et à renforcer durablement la résilience des structures de soins.
230 M€ de financement sont alloués pour 2023/2024, et un budget de 750 M€ à l'horizon 2027.

Christophe MATTLER répond aux questions de Vincent TRELY et d'Auriane LEMESLE - Secrétaire générale de l'APSSIS et référente régionale cyber du groupement e-santé des Pays de la Loire.

Question d'Auriane LEMESLE (AL) : *Comment évoluent les incidents affectant l'écosystème du numérique ?*

> Le nombre d'incidents que nous avons connus est en diminution et les temps de réponses sont réduits. Les Directions Générales ont été sensibilisées et les budgets tant publics que privés sont pérennisés dans la durée.

Question de Vincent TRELY (VT): *La sécurité nécessite des technologies mais aussi des bras. Quel discours tenez-vous aux directions ?*

Il est sûr que nous disons aux RH que les DSI et les RSSI auront besoin de plus en plus de bras pour les accompagner dans les tâches de sécurisation du numérique.

VT : *Quels domaines futurs vous entrevoyez ?*

Pour 90% des structures de santé, il va y avoir des appels à projets médicaux-sociaux. Une priorité portera sur l'authentification des professionnels de santé et un point majeur sera d'apporter la confiance aux citoyens sur tout ce qui concerne le domaine de la santé. Ceci ne pourra se faire qu'avec l'aide des DRH et avec les sources de financement qui vont bien.

Les chantiers futurs seront :

- Tester ces dispositifs,
- Financer les accès distants pour améliorer la sécurité

Et Christophe MATTLER déclare : « **Je compte sur l'assistance des présents dans cette salle pour attirer l'attention des politiques sur ces sujets ».**

AL : *Quelle enveloppe générale est prévue pour le programme CaRE et comment sera-t-elle répartie ?*

Comme je l'ai dit, 750 M€ et on aura besoin d'avances pour atteindre nos objectifs.

VT : *Quelle place est prévue pour être conforme aux règlementations ?*

La directive NIS2 est en attente de transposition à l'Assemblée nationale, mais une commission spéciale de l'Assemblée a déjà validé un texte. Cela va prendre du temps pour qu'en France, la NIS2 soit portée par la loi. Nous pensons que, accompagné par l'ANSSI, tout sera totalement réglé dans les 3 ans.

Pour plus d'informations, vous pouvez également retrouver les propos de Christophe MATTER dans l'article de DSIH :
https://dsih.fr/articles/6072/journee-ssi-sante-apssis-2025-une-cybersecurite-plus-mature-mais-un-financement-toujours-sous-tension

Conférence 2 – ADISTA
Cybersécurité : Adista & Devensys (groupe inhérent) à l'intersection des axes de l'APSSIS
Alexandre MARGUERITE - Directeur technique et Cofondateur – DEVENSYS

Le groupe français « **inhérent** » se compose de quatre entités : Adista, Devensys Cybersecurity, Upper-link et Unyc.

Devensys est une société française, fondée à Montpellier, avec comme domaine d'expertise principal des solutions pour les Red, Blue et Purple Teams.

Adista est un opérateur de services hébergés en particulier pour les données de santé. Il gère 14 datacenters en France, et a obtenu la certification ISO 27001 pour ses activités dans les Clouds privés.

Alexandre MARGUERITE, directeur technique et Cofondateur de Devensys Cybersecurity nous plonge au cœur d'un Pentest mené par une Red Team dans un groupement d'établissements de santé. Il présente les artefacts techniques et les preuves récoltées. Les scénarios d'attaque vont de la préparation de l'intrusion physique vers les zones sensibles jusqu'à la compromission des services IT.

- En phase 1 de l'attaque, il y a un repérage des ressources de la cible dans un temps très limité avant l'intrusion physique. On prépare les outils pour l'attaque, clés d'authentification, scanneurs de réseau, kit de crochetage de serrures, et autres outils…
- La phase 2 est l'intrusion physique vers le réseau interne de la cible, par des ports Internet non sécurisés et via des PC du personnel soignant à qui on demande leur mot de passe, et parfois, on l'obtient ! L'humain est le maillon faible principal qui est utilisé pour l'attaque. Le but est d'accéder à l'Active Directory. Une box mise à l'extérieur va permettre, ensuite, de procéder à des accès à distance avec un accès illimité aux serveurs de la cible.
- La phase 3 est l'intrusion sur la plateforme des patients avec dépose de malwares.

On voit à quel point une Red Team efficace peut être dangereuse pour le système ciblé. Il est à remarquer qu'il n'a pas été besoin à cette Red Team d'exploiter une vulnérabilité du système. Aidée par un deepfake vocal ou vidéo, la Red Team a pu obtenir les accès en s'adressant à un personnel non sensibilisé à la cybersécurité.

Les Pitchs du matin : TYREX, HORNETSECURITY, EVOLUCARE et RUBRIK ont 10 minutes pour s'exprimer

TYREX
Sécurisez vos échanges de données via USB
Caroline BERTAUX - Directrice Commerciale Associée - TYREX

Caroline BERTAUX monte sur scène. Elle présente la société, ses solutions de sécurisation des périphériques USB, et des cas d'usage dans l'écosystème de la santé.

Avec 4500 stations déployées dans le monde, sur l'IT et sur l'OT auprès de plus de 350 clients et un CA 2024 de 5,9 M€, TYREX est une société française pionnière de la décontamination des supports amovibles.

Avec des milliards d'appareil USB-C utilisés dans le monde, et un nombre de malwares multiplié par six en 5 ans, l'utilisation de l'USB-C comme chemin d'attaque par des assaillants est en pleine croissance.

Dans les photos ci-contre, on ne voit pas la console de management de la solution TYREX, seulement une borne de décontamination de périphériques USB-C. Le « K-REX TOTEM » de TYREX est placé à l'entrée de notre salle de conférence. Remarquez la petite tablette sur qui permet d'y poser un disque dur.

Tiens voilà Hélène DASPE, directrice déléguée de l'APSSIS, qui teste sa clé USB ! Alors, est-elle clean ta clé USB, Hélène ?

Si j'avais su, j'aurais emmené toutes les miennes. En tout cas, plus question que j'accepte une clé USB étrangère pour insertion sur mon PC sans qu'elle soit passée par une station de décontamination : **OTrust est devenue ma devise et le ZTNA** (Zero Trust Architecture), **une architecture qui va de soi !**

HORNETSECURITY
Il faut sauver le soldat Patrick
Stephen BONNE, ingénieur avant-vente, spécialisé en cybersécurité chez HORNETSECURITY

Stephen BONNE nous conte une histoire :

« Patrick », employé lambda, est victime d'un piratage. Hornetsecurity va le sauver au cours d'un thriller haletant, qui décortique une cyberattaque en temps réel.

HORNETSECURITY (qui s'appelait précédemment VADE) propose des solutions de sécurité sous Microsoft 365. Elles sont efficaces contre le spam et les malwares. Elles utilisent des technologies de détection basées sur l'IA. Ses solutions permettent aussi de lutter contre les APT (menaces persistantes avancées) qui sont parmi les cyberattaques les plus sophistiquées et les plus difficiles à contrer.

EVOLUCARE
La Sécurité des Tiers : point de vue du milieu de la chaîne
Lauranne PEYRON - RSSI & DPO – EVOLUCARE

Lauranne PEYRON coordonne les actions sur la cybersécurité, sensibilise les équipes, pilote les audits et gère les risques numériques des clients d'EVOLUCARE.

Qu'entend-on par « La sécurité des Tiers » ? Les Tiers sont les partenaires, les sous-traitants, les éditeurs et les intégrateurs qui composent l'écosystème du numérique des établissements de santé.

Les incidents cyber impliquent de plus en plus souvent un Tiers. Par des questionnaires, des preuves recueillies, par la connaissance de ses fournisseurs, EVOLUCARE sait évaluer le niveau de risques posé par les fournisseurs.

La directive NIS2 et la norme ISO 27001 soulignent l'importance de la sécurité des Tiers. EVOLUCARE nous partage son retour d'expérience sur le suivi de la sécurité de ses fournisseurs, et les réponses faites aux demandes de ses clients.

Lauranne PEYRON nous propose un éclairage concis (les seulement dix minutes de Pitch obligent) sur :

- les principaux risques liés aux Tiers,
- les bonnes pratiques et outils internes mis en œuvre par EVOLUCARE pour auditer et sécuriser ses relations partenaires,
- une vision opérationnelle du rôle d'interface occupé par un éditeur dans la chaîne de cybersécurité Santé.

RUBRIK
Comment sécuriser l'identité numérique face à la montée des cybermenaces ?
François MARTI – Channel Sales Engineer chez RUBRIK

La société RUBRIK est spécialiste des technologies Zero Trust, de la cyber-résilience et de la récupération des données.

La mission de RUBRIK consiste à protéger les identités numériques, cible privilégiée des cyberattaques. Les menaces sur l'Information et les systèmes d'information se multiplient. Les incidents concernant l'Identité numérique ont connu un bond de 90% dans les 12 derniers mois et les attaques visant l'Active Directory ont augmenté de 50% au cours des deux dernières années.

Pouvoir récupérer les données d'identité après une attaque permet au personnel d'une entreprise de rester en ligne, et à l'entreprise d'être résiliente. Ceci permet aux employés d'évoluer dans un cyberespace sécurisé.

Voilà la mission que se fixe RUBRIK, basée sur une visibilité en temps réel des risques divers qui menacent l'identité numérique, en permettant à ses clients de rester résilients tout en conservant leur confiance face à ces cyberattaques.

12h40 L'heure du buffet déjeunatoire a sonné

Réunions autour des buffets jusqu'à 14h00, dans plusieurs salles adjacentes à l'espace de conférences. Nous pouvons nous restaurer dans une ambiance stimulante et nous avons tout le temps d'échanger avec les partenaires de l'évènement, de faire d'intéressantes rencontres et découvertes sur les services et produits de cybersécurité proposés. Ajoutons que nous avons aussi l'occasion d'accéder à des documentations et à des goodies. J'en ramène plusieurs chez moi en souvenir de cette journée (dont une tablette de chocolat).

14h00 Reprise des conférences

Conférence 3 – IGEL
L'hôpital connecté, oui — mais sécurisé : l'approche IGEL pour des postes de travail de confiance en milieu hospitalier
Avec Maxence MICHARDIERE, Ingénieur avant-vente et Fatima YOUALLA, Responsable de Comptes Santé.

IGEL est une société européenne qui commercialise IGEL OS12, un système d'exploitation sécurisé pour points d'accès des entreprises avec des postes de travail sécurisés et simples à gérer.

IGEL propose des solutions prêtes à l'emploi pour le cloud, avec un chiffrement de bout en bout, dans une approche Zero Trust.

Avec IGEL, le personnel médical travaille en confiance sur des postes de travail équipés, sans jamais compromettre les données des patients. Avec sa plateforme d'OS sécurisée pour les terminaux, IGEL est la clé d'un hôpital connecté, agile et sécurisé — au service des soins des patients.

Conférence 4 – SENTINELONE
Le Management et l'optimisation des SOC de dernière génération
Mathieu VIALETAY - Presales Engineering secteur public - SentinelOne France

Mathieu VIALETAY commence par dresser un panorama des cybermenaces actuelles et des cyberattaques globales. Il évoque en particulier l'attaque PhantomCaptcha qui visait, le 8 octobre, les organisations d'aide à l'Ukraine, comme la Croix-Rouge et l'UNICEF, avec exécution de commandes et exfiltration de données. Attaque attribuée au FSB russe.

Il poursuit en évoquant la NIS2 et le RGPD, puis en expliquant comment on gère et optimise un SOC - Security Operation Center – de dernière génération, dans le respect des normes, des directives et des règlements. SentinelOne se développe par acquisition de sociétés impliquées dans l'IA comme Prompt et Observo.ai.

Mathieu termine sa conférence par une démonstration de la plateforme Singularity et indique des cas d'usage concrets. Singularity combine l'EDR, le XDR, la sécurité des Identités numériques et le SIEM qui faisant appel à des technologies d'Intelligence Artificielle.
L'offre SENTINELONE permet de passer d'une sécurité réactive à une sécurité proactive.

Les Pitchs de l'après-midi : RESAH, VARONIS et JIZO AI ont 10 minutes pour s'exprimer.

RESAH
Simplifier la cybersecurité pour mieux protéger et moins consommer
Hasina BESSE-RAMASINIRINA - Directrice du pôle achats Réseaux & Télécom - RESAH

Le RESAH (Réseau des acheteurs hospitaliers) est un groupement d'intérêt public dont l'objectif est d'appuyer la mutualisation et la professionnalisation des achats et de la logistique pour les acteurs intervenant dans les secteurs sanitaires et médico-sociaux, mais aussi dans le secteur social, public et privé (EHPAD, SDIS, centres de santé…).

L'ambition du RESAH est de passer du rôle de collectionneur de solutions à celui de bâtisseur d'une architecture claire et durable. Ceci peut être fait en répertoriant les solutions existantes dans le domaine du SIEM, de l'EDR, du XDR, du CASB, du SOAR, pour en simplifier l'usage en regroupant, dans la mesure du possible, ces briques de sécurité. Mieux vaut, pour un RSSI, intégrer ces solutions plutôt que de les accumuler.

Hasina BESSE-RAMASINIRINA nous propose un nouveau mot : La **cybersobriété** par laquelle on réduit la complexité de la solution de cybersécurité. De plus, en réduisant le nombre de serveurs, on réduit l'empreinte écologique. Elle souhaite que ce mot « cybersobriété » se retrouve un jour dans le Robert.

VARONIS
La protection de vos données comme traitement de fond
Marvin LOOZ, Manager avant-vente Public & Mid-Market sectors pour la France et la Suisse.

La cible finale d'une cyberattaque, c'est la donnée, actif précieux mais très vulnérable. Protéger les données sur site ou dans un Cloud, en automatisant la détection des menaces et en gérant les accès est la vocation des solutions de cybersécurité de VARONIS.

86% des violations de données sont dues à des identifiants volées. Inutile d'utiliser la force brute pour s'introduire dans un système, il suffit de posséder les bons paramètres d'identification et d'authentification.

Pour sécuriser les données, VARONIS propose une plateforme centralisée qui fait appel à l'IA pour classifier et protéger les données sensibles, et alerter les opérateurs en cas de problèmes. Voilà une sécurité proactive !

JIZO AI
L'observabilité IT/OT/IoT pour adopter une posture de cyberdéfense éclairée
Audrey AMEDRO, CEO & Fondatrice de Sesame it (devenue JIZO AI).

Le coût de la cybercriminalité, d'ici 2028, est estimé à 13 820 milliards de dollars. Les hôpitaux présentent une immense surface d'attaque. De plus, l'IA permet de créer des menaces adaptatives qui sont indétectables par les solutions de sécurité traditionnelles.

Les structures de santé sont complexes, interconnectées, et interopérables. Elles sont vitales mais bien sûr soumises à des contraintes budgétaires.

JIZO AI présente une solution française de plateforme d'observabilité qui permet :

- De tout voir et de tout comprendre en s'appuyant sur les flux réseaux, avec une vision fiable et complète de ses équipements et de son environnement,
- de traiter l'IT, l'OT et le biomédical,
- d'apporter de manière automatique des réponses aux attaques,
- de déployer la solution, de manière centralisée et sans perturber l'existant.

Avec JIZO AI, on obtient une cartographie et une topologie du réseau qui permet d'établir une surveillance efficace.

15h50, c'est la pause de l'après-midi, une occasion de revoir les partenaires de l'évènement, de discuter avec les participants et de prendre une collation.

16h30, **les conférences reprennent.** Tout le monde est revenu dans la salle de conférence pour suivre 2 conférences (IMPRIVATA et BITDEFENDER) suivies par 4 pitchs (ZSCALER, AKAMAI, CLAROTY et INFOBLOX) puis par la conférence finale de Judith NICOGOSSIAN, avant de nous retrouver pour le dîner de gala.

Conférence 5 - IMPRIVATA
Sécuriser sans freiner : comment concilier conformité et efficacité du soin
Amélie LEROUX, Directrice commerciale et **Ayoub BAHAR**, Ingénieur solutions.

IMPRIVATA, qui compte 45 bureaux dans le monde, et plus de 4400 clients, assure des accès numériques simples et sécurisés afin que chaque seconde de soin soit pleinement consacrée au patient (ceci est dans leur ADN depuis 20 ans).

Protéger la donnée médicale, c'est protéger la continuité du soin, la responsabilité des équipes et la confiance du patient.

Un soignant passe en moyenne 45 minutes par jour à gérer ses accès numériques avec des authentifications nombreuses et parfois sujettes à des attaques pouvant entrainer des fuites de données et une surcharge du support IT.

La gestion des accès et des identités est devenue un enjeu stratégique de conformité, avec la NIS2 et CaRE Hospiconnect qui propose des moyens d'identification électroniques. Cette obligation de conformité à la directive NIS2 implique la Direction des établissements de santé. Les projets numériques, en particulier avec le Cloud, s'accélèrent mais les ressources en personnel et en budget sont limitées.

Les freins recontrés par le personnel soignant sur les accès aux processus métiers et aux dossiers médicaux résultent essentiellement d'une gestion trop souvent chronophage et de processus d'authentifications parfois trop complexes. Cela laisse moins de temps aux missions stratégiques. Donc il est nécessaire de simplifier ces processus pour réduire le stress causé par des interruptions répétées, et des risques d'erreurs. La qualité des soins s'en trouve ainsi renforcée.

Dans l'idéal, la sécurité doit être invisible. Remplacer la multiplicité des mots de passe par du SSO (Single Sign On) avec accès par badges sans contacts avec le Tap & Go. Utiliser le MFA (Authentification Multi Facteurs) avec le Tap & Smile, au moyen d'un badge et par reconnaissance faciale. Et les données d'authentification ne persistent pas quand l'utilisateur change d'appareil.
Imprivata Mobile Device Acces assure cette sécurité avec authentification par badge sans contact. Le personnel accepte ainsi plus facilement l'usage des outils mobiles.

Conférence 6 - BITDEFENDER
Souveraineté, surface d'attaque et conformité : la protection des données à 360
Emmanuel MEYRIEUX, directeur de la sécurité pour les clients chez OVHcloud et Stéphane BROVADAN, Sales Engineer Team Leader chez BITDEFENDER.

Fort de 24 ans d'expérience et de 2400 collaborateurs, dont 1100 ingénieurs en R&D, **BITDEFENDER** développe des technologies antimalwares en interne. Avec plus de 589 brevets déposés parmi lesquels du Machine Learning, de l'IA et de la détection avancée des menaces, BITDEFENDER bloque 50 milliards de menaces chaque année, au bénéfice de centaines de millions d'utilisateurs.

OVHcloud compte plus de 2900 employés et 1,6 millions de clients répartis dans 140 pays. Il aligne 44 Datacenters avec un CA de 993 M€ en 2024. OVHcloud se veut être le leader mondial du cloud de confiance avec une offre conforme aux standards européens et qualifiée SecNumCloud.

Le siège de BITDEFENDER est sur le territoire de l'Union européenne. BITDEFENDER propose une solution de cybersécurité souveraine GravityZone, son application SandBox Windows et son réseau de protection Nimbus. Toutes les données et les métadonnées sont stockées chez OVHcloud et restent en France. Son EASM – External Attack Surface Management – voit l'invisible et détecte les éléments vulnérables pour réduire la surface d'attaque et atténuer les risques.

GravityZone Compliance Manager permet de contrôler la conformité aux directives et règlements tels que la NIS2, DORA et le RGPD, aux normes telles que l'ISO27001 et d'apporter des preuves de cette conformité : Ça rassure !

Les Pitchs du soir : ZSCALER, AKAMAI, CLAROTY et INFOBLOX ont 10 minutes pour s'exprimer

Mais seulement 10 minutes, **Anna PUJOL-MAZZINI y veille !**

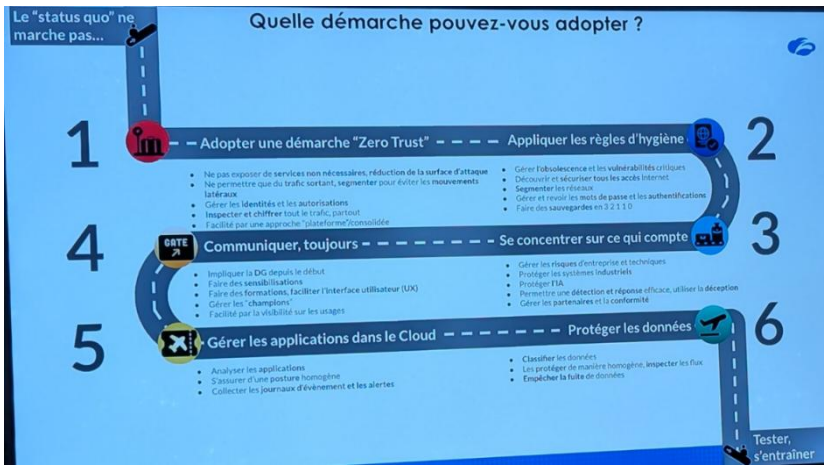
ZSCALER
Sécuriser les hôpitaux grâce à l'approche Zéro Trust : 3 cas d'usages éprouvés
Cédric BONAMIGO, Public Sector et Olivier DALOY, Cybersecurity Expert

ZSCALER sécurise les hôpitaux avec une approche 0Trust. On ne fait jamais confiance, on vérifie tout.

Cette sécurisation pose des défis polymorphes. Elle pose des problèmes stratégiques comme la nécessité d'engager la responsabilité de la Direction, des problèmes tactiques comme gérer l'obsolescence et les changements fréquents, et enfin des problèmes techniques comme détecter les signaux faibles et gérer les identités et les accès.

Attention aux fausses bonnes idées humaines comme limiter la sensibilisation à la cybersécurité ; fausses bonnes idées technologiques comme rejeter le Cloud ou déconnecter l'IT et l'OT des réseaux gérés et fausses bonnes idées de process comme permettre trop d'accès extérieurs.

La menace évolue avec l'IA qui facilite les attaques ciblées, alors quelle démarche adopter pour garantir la continuité des soins ?



AKAMAI
L'approche micro-segmentation d'un CHU pour l'homogénéité de la sécurité et de la conformité de son infrastructure
Laurence COZLIN - Entreprise Executive Senior France.

Avec 10750 employés et 8000 clients, AKAMAI génère un CA annuel de 4 milliards de dollars. Ses solutions se décomposent entre la sécurité des API, le Zéro Trust avec le AKAMAI Guardicore Segmentation, le MFA, et aussi autour de la sécurité des infrastructures.

En 2024, les ransomwares ont constitué le principal vecteur d'attaques, suivi par la compromission d'identifiants. Des données ont été chiffrées et volées et la reprise d'activité a demandé beaucoup de temps (en moyenne un mois).

Comment réduire sa surface d'attaque et éviter la propagation des menaces ? Par la micro-segmentation pour les environnements critiques comme les dossiers patients.

Le AKAMAI Guardicore empêche la propagation des ransomwares sans entrainer des coupures dans la production des soins. Les DNS Firewalls bloquent les tentatives de connexions vers des domaines malveillants (DNS AKAMAI possède une immense base de réputation des sites web malveillants).

Protéger les soins sans jamais les interrompre est l'approche de sécurité by design prônée par AKAMAI.

CLAROTY
État de la menace des systèmes cyberphysiques dans les établissements de santé en 2025
Sébastien Brals, Directeur commercial chez CLAROTY France et Renaud Menier - Manager Public Sector chez NTT DATA Inc.

Claroty est un éditeur de logiciel spécialisé dans la cybersécurité des systèmes connectés en milieu de santé (IT, IoT et IoMT – Internet of Medical Things). Ses solutions sécurisent les équipements biomédicaux, cartographient les actifs connectés et supervisent les réseaux hospitaliers.

En 2025, 351 établissements ont été analysés par Claroty, qui alignaient 2,25 millions d'appareils IoMT et 647 000 appareils OT tels que des ascenseurs. Il est apparu que les appareil IoMT présentent de nombreuses vulnérabilités.

La première cible des attaquants, contre les hôpitaux, concerne l'imagerie médicale (IRM, scanners, radiologie numérique) et ces attaques peuvent entrainer des risques directs sur les patients.

NTT est une très grande entreprise de télécommunication avec un CA annuel de 100 milliards de dollars, et 330 000 employés. NTT DATA est un intégrateur de solutions IOT, IoMT et de Cybersécurité.

NTT DATA qui intègre et supporte la solution **Claroty xDome**, conforme à la norme ISO27001, permet à ses clients de protéger leurs actifs cyberphysiques (OT, IoT, IoMT). Dans le domaine de la santé, Claroty offre une bonne visibilité des équipements et systèmes médicaux connectés qui sont exposés à des vulnérabilités et des exploits connus, à des rançongiciels et à toute attaque exploitant des connexions non-sécurisées.

INFOBLOX
Sécuriser les fondements invisibles du réseau hospitalier : le DDI au cœur de la cyber-résilience
Ed DANIEL, Ingénieur avant-vente INFOBLOX Europe.

Le **DDI** regroupe la gestion du **D**NS, du **D**HCP et de l'**I**PAM (les adresses IP). Dans le monde ultra-connecté d'aujourd'hui, INFOBLOX aide les établissements de santé à sécuriser et automatiser leurs réseaux. Ceci est primordial car, d'après une étude de Wavestone, 68% des établissements de santé français n'ont pas une visibilité suffisante sur leurs flux réseaux et sur les équipements qui y sont connectés. Le DNS – Domain Name System – est un maillon critique.

INFOBLOX, qui compte plus de 13 000 clients dans le monde, dont en France les CHU de Limoges et de Lille, assure, par son offre, une disponibilité avec une continuité de services, une visibilité et une traçabilité qui permettent de réduire le temps de résolution des incidents. L'automatisation des réseaux réduit le temps de leur administration.

Infoblox Threat Defense analyse les requêtes vers les DNS et bloque les tentatives d'accès à des domaines réputés malveillants. Intercepter les attaques en amont pour ne pas les subir est l'avantage de l'offre de INFOBLOX.

Anna PUJOL-MAZZINI a veillé à ce que les temps de parole de chaque intervenant ne dépassent pas la durée décidée au préalable. Place maintenant à la dernière conférence de cette édifiante journée, un sujet humain.

Conférence de clôture
L'humain au cœur de la crise
Judith NICOGOSSIAN, Docteure en anthropologie.

Nous avons le plaisir d'accueillir **Judith NICOGOSSIAN** de l'Association Française d'Anthropologie - Ecole de Grenoble qui va nous parler de la gestion de crise dans une dimension humaine et psychologique, et de la gestion du stress qui l'accompagne.

Dans la gestion de crise, la culture informatique et la culture locale ne s'entendent pas forcément. Plusieurs facteurs entrent en jeux, citons :

- La protection de son identité par rapport aux autres collaborateurs,
- la chasse aux sorcières en occultant la protection du personnel,
- l'attaque par l'IA générative, attaque très anxiogène,

Il est possible de faire un test biologique de résistance au stress.

Judith indique le combat entre le chevalier noir (celui qui fait que le stress augmente) et le chevalier blanc (celui qui s'attache à le diminuer) et donne 18 recommandations, avant, pendant et après la crise.

Une question est posée : Quels conseils donner pour aider à vaincre le stress ?

- S'occuper de soi-même avant de penser aux autres et garder la confiance,
- pouvoir communiquer fait du bien,
- être solidaire des autres employés et augmenter la cohésion des équipes
- veiller aux soutiens psychologiques pendant la crise avec des réunions fréquentes.

Judith nous indique l'étude PSYBER qu'elle a écrit avec trois autres experts du sujet :
« *Impacts psychologiques et dimension humaine d'une crise d'origine cyber sur une organisation : résultats de l'étude interdisciplinaire PSYBER* ».

PSYBER : PSY et CYBER

https://hal.science/hal-05294731v1

Cette étude propose un ensemble de recommandations d'atténuation et d'amélioration d'une crise cyber.

La dimension humaine des cyberattaques, dans sa prise en charge et dans son traitement apparait dans le témoignage de Thomas Vadot dont nous avons déjà parlé et qui prend la parole.

Quelle merveilleuse occasion d'illustrer la conférence de Judith par un cas réel et très récent (octobre 2025) d'attaque sur un Centre hospitalier !

Thomas VADOT, avec sa verve et sa passion de tout ce qui concerne la cybersécurité a parfaitement illustré le comportement d'un responsable de la sécurité du SI d'un Centre Hospitalier, confronté au stress, mais aussi pouvant faire preuve d'une grande efficacité.

Recommandation de Judith NICOGOSSIAN à Thomas VADOT : Prenez soin de vous et courage !

Il est **19h30**, le temps d'intervention accordé à Judith NICOGOSSIAN est arrivé à son terme. Anna PUJOL-MAZZINI déclare que c'est la fin des interventions de la journée. Place maintenant

au Président de l'APSSIS, Vincent TRELY qui remercie le public de la salle et nous donne rendez-vous pour le dîner de gala.

Nous voici tous dans la salle de restaurant de l'hôtel des Arts & Métiers.

Après la coupe de champagne, nous prenons place autour de petites tables rondes. Très bien pour les échanges ! Il est 20h00, derrière la verrière du salon, la Tour Eiffel clignote de mille éclats et Vincent TRELY nous annonce que les **Rencontres SSI Santé 2026** de l'APSSIS se tiendront exceptionnellement sur deux jours à Aix-en-Provence, les jeudi 4 et vendredi 5 juin 2026.

Le repas de gala est un grand moment de convivialité qui s'ajoute aux autres moments de convivialité de la journée.

Voici le menu :

Et nous voilà attablés :

22h30 marque la fin de cette magnifique journée.

Je regagne le métro Iéna, tout proche pour rentrer chez moi, la tête pleine de souvenirs et la hâte d'écrire mes impressions sur cette journée. Au revoir à toutes et à tous et au revoir Hôtel des Arts & Métiers qui éclaire la nuit.

et merci aux sponsors de l'évènement :

Je signe :

A bientôt.

Gérard