CYBER CERCLE

11 JUIN 2025
LYON
RENCONTRES CYBERSÉCURITÉ
AUVERGNE-RHÔNE-ALPES

#RCYBERARA
#TDFCYBER

RHÔNE
LE DÉPARTEMENT

DOSSIER PARTICIPANT

RCyberAra

Hôtel du Département du Rhône

11 JUIN 2025 - Lyon

Crédit photo Alain Zimeray

Bénédicte PILLIET
Présidente du CyberCercle

Edito

Les Rencontres de la Cybersécurité Auvergne-Rhône-Alpes : déjà la 7ème édition !

Lorsque nous avons lancé en 2019 les premières Rencontres de la Cybersécurité Auvergne-Rhône-Alpes à Lyon dans le cadre de notre Tour de France de la Cybersécurité, notre ambition était novatrice. Nous étions parmi les précurseurs, soutenus par notre écosystème de confiance, engagés dans une démarche fédératrice pour soutenir entreprises et collectivités de notre région autour de la cybersécurité.
Aujourd'hui, après six années d'évolution le contexte a bien changé. La cybersécurité, devenue un phénomène de mode, mais pour combien de temps, s'est insérée aux grands événements locaux autour du numérique, de l'intelligence artificielle, de l'industrie et des objets connectés. De nouveaux rendez-vous dédiés ont émergé, parfois sur un copier-coller de ce que nous faisons même si le mot « rendez-vous » remplace le mot « rencontres ».

Répondre aux besoins d'aujourd'hui

Mais la multiplication de ces évènements doit nous interpeler : sont-ils réellement adaptés aux enjeux actuels de la sécurité numérique ? Ainsi, un des enjeux majeurs pour « passer à l'échelle » comme le souhaite l'Etat, est aujourd'hui d'éclairer les décideurs publics et privés au fait que la cybersécurité est une priorité stratégique et une question de gouvernance avant d'être un « simple enjeu technique », de donner des clefs pour comprendre et mieux s'engager dans une stratégie de sécurité numérique cohérente. Cela nécessite de se poser, de travailler ensemble et du temps. Pour les non spécialistes cyber que sont les chefs d'entreprises et les élus, la multiplicité de sollicitations pour des évènements et d'offres renforce encore le sentiment d'être perdus. Avant de proposer le « avec quoi », il est plus que jamais nécessaire d'expliquer « le pourquoi », sous l'angle stratégique, pour que les organisations s'approprient la cybersécurité. Comme nous l'avons dit lors de notre audition à l'Assemblée nationale le 5 juin 2025 devant la commission spéciale sur le projet de loi « Résilience des infrastructures critiques et renforcement de la cybersécurité » : aujourd'hui il faut convaincre que la cybersécurité est un sujet stratégique, un pilier de croissance et de développement. Et pour les élus, un sujet politique. S'ils ne sont pas convaincus, nous devons nous demander pourquoi plutôt que de penser que la réglementation répondra aux besoins.

Quid des politiques publiques ?

Que dire des politiques publiques nationales ou locales : de multiples dispositifs, de multiples acteurs… mais pas toujours lisibles et qui se superposent parfois ; une abondance de contenus disponibles sur internet… mais que ne connaissent pas souvent ceux à qui ils s'adressent ; une vision volontariste et engagée… mais qui est trop souvent loin de la réalité du terrain et donc difficilement motivante pour les acteurs, avec la fameuse « première marche » trop haute.
L'absence d'une véritable stratégie de sécurité numérique au niveau national qui permettrait de nous donner un cadre d'action coordonnée, une vision commune et d'organiser efficacement une « équipe France » de la Cyber nous manque cruellement.
L'heure d'un certain bilan approche d'ailleurs pour certaines initiatives comme les campus cyber et les CSIRT qui se sont multipliés sur les territoires depuis 2021 dans la lignée de la « Stratégie » Nationale d'Accélération pour la Cybersécurité. Sauf en Auvergne-Rhône-Alpes, la Région ayant préféré prendre le temps de la réflexion avant de proposer sa stratégie pour la cybersécurité des entreprises qu'elle vient de publier mais qui finalement n'est que la poursuite des actions présentées ici même en 2019.

Un tournant stratégique

Ce « phénomène de mode ou d'opportunité » est lui-même alimenté avec les réglementations françaises et européennes qui s'accélèrent. Souvenons-nous du RGPD en 2018… Avec la transposition en cours d'examen devant le Parlement des trois textes européens disruptifs que sont NIS 2, DORA et REC, les règlements européens comme le CRA, la cybersécurité ne doit pas devenir un coup de « com' » aux effets souvent éphémères, auquel se succédera le même phénomène d'opportunité autour de l'IA - que l'on observe déjà d'ailleurs. Face aux enjeux d'aujourd'hui et aux exigences accrues à venir, un véritable travail de fond, posé et réfléchi, un dialogue public-privé, spécialistes-néophytes est plus que jamais nécessaire. Informer et former pour favoriser l'action des dirigeants et élus, avoir une approche métiers, sont de plus en plus indispensables pour faire comprendre et intégrer cette dimension dans leur stratégie. Envisager également, qu'au-delà des coûts, la cybersécurité est un facteur de développement et d'attractivité.

Ensemble pour une cybersécurité collective

Au CyberCercle, nous poursuivons cette ambition de travail de fond associée à une démarche d'intérêt général fondée sur près de quinze années d'expérience, à l'écoute des acteurs quels qu'ils soient, au Paris et sur les territoires, en déployant une agilité face au contexte et aux besoins, autour d'une triple conviction :

- « Seul, on ne va nulle part. Ensemble, on va plus loin et plus vite ».
- « La nécessité de construire ensemble une culture de sécurité et de confiance numériques partagée. »
- « La sécurité numérique doit être au service des métiers. »

D'où notre philosophie d'actions sur le terrain, de fédération d'acteurs publics et privés, de spécialistes cybersécurité et de responsables métiers, d'élus et de chefs d'entreprises, de partages d'expériences, d'approches sectorielles, de démarches pédagogiques… une politique d'animation tout au long de l'année de « Communautés d'Intérêt Cyber »… d'expertises et d'analyses de fond … qui nécessite du temps et de l'engagement.
C'est ce contexte global, notre analyse des besoins, notre volonté de faire encore mieux, qui nous poussent aujourd'hui à annoncer la fin des Rencontres Cybersécurité Auvergne-Rhône-Alpes : 7 est un bon chiffre !
Un arrêt pour un choix de plus de travail de fond tout au long de l'année dans des événements rémanents en format restreint, plus de groupes de travail, de contributions écrites… autant d'axes plus adaptés à l'ADN qui est le nôtre et à notre expertise, et qui répondent aux besoins des acteurs. Loin des effets de « com' » même si j'ai conscience que nous devons communiquer. Car dans le monde d'aujourd'hui il ne suffit pas de faire. Il faut aussi faire savoir.

Nous serons en tous cas heureux de vous y retrouver.
En attendant, je vous souhaite de bonnes – dernières - Rencontres !

8h00 ■›› OUVERTURE DU CAFE D'ACCUEIL DANS L'ESPACE DE RENCONTRES

8h30 ■›› OUVERTURE DES TRAVAUX

Bénédicte PILLIET, Présidente du CyberCercle
Christophe GUILLOTEAU, Président du Département du Rhône
Antoine GUERIN, Préfet délégué à la défense et la sécurité auprès de la Préfète de la région Auvergne Rhône Alpes, Préfète de la zone de défense et de la sécurité sud-est, Préfète du Rhône

9h00 à 10h30

■›› TABLE RONDE

Réglementation et Cybersécurité : du Projet de loi « Résilience des infrastructures critiques et Renforcement de la Cybersécurité » au Cyber Resilience Act... décryptage et enjeux de la mise en oeuvre

Bénédicte PILLIET, Présidente du CyberCercle
Stéphane MEYNET, Président de CERTitude NUMERIQUE, senior advisor du CyberCercle
Philippe LOUDENOT, senior advisor du CyberCercle
Philippe LATOMBE, député de Vendée, Président de la commission spéciale de l'Assemblée Nationale sur le projet de Loi « Résilience des infrastructures critiques et renforcement de la cybersécurité » (en visio)

10h30 ■›› PAUSE CAFE – NETWORKING – ESPACE DE RENCONTRES

Un moment d'échanges convivial qui permet de découvrir les stands répartis dans l'espace de Rencontres et de s'informer. L'Espace de Rencontres est activé au moment des pauses et du déjeuner afin de permettre aux auditeurs et exposants de participer aux travaux.

11h00 ■›› WORKSHOPS

Répartis en deux sessions horaires : de 11h00 à 11h40 – de 11h50 à 12h30
Ces 11 workshops de nos partenaires représentent une opportunité de s'informer de façon privilégiée sur une thématique définie, de mieux connaître les solutions pour y répondre et d'échanger avec des experts. Les deux sessions horaires vous permettent de faire deux choix.

➤ **Comment sensibiliser au plus près vos utilisateurs aux risques cyber ? La sensibilisation en temps réel est-elle possible ?**
Jean GEELAND de MERXEM, Directeur commercial adjoint, Responsable Vishing, Avant de Cliquer

➤ **Exposition externe : le talon d'Achille de votre politique cyber ?**
Julien LOPIZZO, Président fondateur, SEMKEL

➤ **RETEX – Mise en peuvre d'un projet PCRA cybersécurité au sein d'un établissement de santé**
Rodolphe BACA, Cybersecurity Manager, ATOS

➤ **IA et Cybersécurité**
Dr Michel DUBOIS, Directeur Scientifique et Technique à la Direction Cybersécurité, Groupe La Poste

➤ **Open source / libres, « root » vers la souveraineté ?**
Yoan ISSARTEL, CTO Elysium Security / Root Me Pro

➤ **Sensibilisation interne : stratégie et outillage**
Cyprien GUEYRAUD, Pilote de la sensibilisation Cyber au sein de la Cyber School, **Jordan BABEL**, Référent Cyber DR SIRHO et DR Alpes, et **Charles Edouard OUKRAT**, Cyber Animation Filière cyber, ENEDIS

➤ **La cybersécurité, ce n'est pas qu'une affaire de technologie complexe !**
Philippe LOUDENOT, Directeur Stratégie Cybersécurité, BLUEFILES

➤ **Souveraineté numérique, arrêtez de jouer avec le (pare) feu**
Olivier DEGARNE, Ingénieur Avant-Vente, Stormshield

➤ **Comment accélérer sa remédiation ?**
Flavien RIEHL, Responsable Pôle Renfort Sécurité, MGM Solutions

➤ **Cybersécurité et Sécurité Routière**
Maël VERY, Président, Security Road

➤ **L'IA cette évolution technologique dérangeante, vers un Humanisme cyber ?**
Alexandre FOUSSE, Président, STRAAD.A

12h30 ■›› **PAUSE DEJEUNER - NETWORKING**
Cocktail offert aux participants

14h30 à 16h30

■›› **SESSION ATELIERS DE TRAVAIL RÉSERVÉS AUX PROFESSIONNELS DE TOUS SECTEURS ET CONFERENCE OUVERTE À TOUS**

Les participants sont invités à choisir de participer à un des ateliers ou à la conférence.
Placés sous les règles de Chatham House, les ateliers durent deux heures et ont pour objectif de permettre aux participants d'échanger librement dans un cadre de confiance. Des orateurs ouvrent l'atelier par des interventions courtes pour apporter un éclairage sur le sujet puis l'ensemble des participants est invité par l'animateur de l'atelier à s'exprimer, soit pour poser des questions, soit pour apporter un témoignage, un retex ou une vision du sujet.
La conférence est ouverte à tous.

➤ **ATELIER 1**
L'IA dans les collectivités : opportunités et risques
Animé par **Bénédicte PILLIET**, Présidente du CyberCercle

Avec les interventions d'ouverture :
« Panorama de l'IA dans les collectivités aujourd'hui »
Henri SAILLARD, Directeur du déploiement des projets transverses du Groupe la Poste
« RETEX – les réflexions du Département du Rhône autour de l'IA »
Daniel COISSARD, Directeur des Usages Numériques du Département du Rhône
« Comparatif risques – opportunités : un équilibre à trouver »
Pascal NAHON, Directeur de la Région Auvergne-Rhône-Alpes, d'ATOS

➤ **ATELIER 2**
Faire de la cybersécurité un pilier transverse des organisations : quel leviers ? Quelle démarche ?
Animé par **Philippe LOUDENOT**, Senior advisor du CyberCercle, Directeur de la stratégie cybersécurité de BlueFiles

Avec les interventions d'ouverture :
« Le projet Papyrus »
Hervé PELLARIN, RSSI du Centre hospitalier d'Annecy Genevois
« Quelles actions conduites par l'Education Nationale en Auvergne-Rhône-Alpes pour développer l'esprit de cyberdéfense ? »
Denis MILLET, Délégué de région académique au numérique éducatif, Conseiller du recteur de l'académie de Lyon au Rectorat de Lyon
« Le facteur humain comme élément fédérateur de la cybersécurité : la démarche conduite au sein de la Police Nationale »
François BRIAT, Ingénieur projets au Laboratoire de recherche du Département recherche, valorisation et diplomation, de l'Ecole Nationale Supérieure de Police

➤ **CONFERENCE**
Se préparer à la gestion de crise cyber : l'intérêt des exercices

« Exercices de gestion de crise : les fondamentaux »
Jérôme SAIZ, senior advisor du CyberCercle, qui animera également les travaux
« RETEX – Exercice de gestion de crise d'origine cyber mené par le CyberCercle à Lyon en juin 2024 »
GCA (2S) Jacques HEBRARD, senior advisor du CyberCercle
« RETEX – Exercice de gestion de crise cyber mené au sein de GL EVENTS »
Bruno LEAL DE SOUSA, RSSI de GL EVENTS
« RETEX d'expert réponse à incident »
Yoan ISSARTEL, CTO d'Elysium Security

16h30 à 17h30

■›› **RAFRAICHISSEMENT - NETWORKING - ESPACE DE RENCONTRES**

Les intervenants

Christophe GUILLOTEAU

Président
Département du Rhône

Christophe Guilloteau est depuis 2015 président du département du Rhône, il a été réélu en 2021. Il est également 1er vice-président du SDMIS et vice-président de l'Assemblée des départements de France en charge des relations avec l'Assemblée Nationale.
Après avoir été assistant parlementaire puis chef de cabinet à la Mairie de Tarare de 1988 à 1994, il est devenu attaché territorial et collaborateur du Vice-président du Conseil Régional de Rhône-Alpes. Elu en 1998 Conseiller régional et Conseiller municipal de Vaugneray, il a été de 2008 à 2015, Conseiller général du Rhône et Vice-président du SDIS.
Elu Député du Rhône en 2003, il a été réélu en 2007 et 2012.
Christophe Guilloteau a été nommé en juillet 2012, membre titulaire de la commission chargée de l'élaboration du Livre blanc sur la Défense et la Sécurité nationale. Membre de la Commission de la Défense nationale et des Forces armées au sein de l'Assemblée Nationale, il a été vice-président, rapporteur pour le budget Air et président du Groupe d'étude Industrie de Défense, développant une expertise sur les sujets de Défense et de Sécurité Nationale.
Christophe Guilloteau est Chevalier de l'Ordre National du Mérite et Chevalier du Mérite agricole, Capitaine de vaisseau dans la Réserve citoyenne de la Marine et Membre de la Réserve citoyenne Cyberdéfense.

Stéphane MEYNET

Senior advisor
CyberCercle
Président-Fondateur
CERTitude NUMERIQUE

Stéphane Meynet, ingénieur de l'École des Mines d'Alès, a démarré sa carrière dans l'industrie de la micro-électronique. Après avoir été en charge pendant 10 ans de systèmes automatisés de contrôle de procédés industriels dans un contexte opérationnel, il a rejoint l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Dans un premier temps, il a conduit le projet sécurité des systèmes industriels en traitant les aspects de cybersécurité des infrastructures critiques de la nation. Puis, dans le cadre du déploiement de l'ANSSI au niveau territorial, il a été le délégué à la sécurité numérique pour la région Auvergne-Rhône-Alpes.
En janvier 2018 il décide de créer CERTitude NUMERIQUE, entreprise dédiée à la sécurité numérique, et plus particulièrement appliquée aux systèmes industriels. Depuis il accompagne de nombreuses entreprises de toutes tailles dans leurs politiques de sécurité numérique ou dans la formation des collaborateurs ou des comex. Il intervient également auprès d'entreprises de cybersécurité dans leurs démarches de labellisation.
Stéphane Meynet est senior advisor du CyberCercle depuis 2018.

Bénédicte PILLIET

Présidente
CyberCercle

Crédit photo Alain Zimeray

Bénédicte Pilliet est depuis 2011 présidente du CyberCercle, cercle de réflexion, d'échanges et de rencontres sur la sécurité et la confiance numériques qu'elle a créé. Diplômée de Sciences Po Paris, elle a acquis à travers son parcours professionnel une expertise reconnue dans la communication institutionnelle et les Affaires Publiques, sur les sujets de défense, de sécurité nationale et de sécurité numérique. Elle est créatrice et responsable pédagogique du Certificat Sécurité Numérique à l'Université Paris-Dauphine. Femme engagée, elle est Lieutenant-colonel de réserve (citoyenne) de l'armée de Terre depuis 2007, membre du Cercle Fontenoy, et a œuvré en tant que responsable du rayonnement pour la Réserve Citoyenne de Cyberdéfense de 2012 à 2018. Elle est également membre fondateur du Cercle K2 et membre du CESIN.
Bénédicte PILLIET est titulaire de la Médaille de la Défense nationale, échelon or, agrafe cyber, et de la Médaille des Services Militaires Volontaires, échelon bronze.

Antoine GUERIN

Préfet délégué à la défense et la sécurité
Préfecture région Auvergne Rhône Alpes

Succédant à Juliette Bossart-Trignat, Antoine Guérin reprend la délégation pour la défense et la sécurité en tant que préfet du Rhône, auprès de Fabienne Buccio, préfète de région Auvergne-Rhône-Alpes.
Diplômé de l'ENA il intégre le corps préfectoral en 1999 en tant que sous-préfet, directeur de cabinet du préfet dans les Deux-Sèvres avant de rejoindre les préfectures de la Haute-Normandie, du Loiret, comme secrétaire général, puis la préfecture de police de Paris comme directeur des transports et de la protection du public.
Après avoir également occupé diverses fonctions dans des cabinets ministériels, il a été nommé directeur de l'administration du ministère des Armées.

Philippe LOUDENOT

Directeur stratégie cybersécurité
BlueFiles

Après une carrière au sein du ministère de la Défense en sécurité des systèmes d'information, Philippe Loudenot rejoint les services du Premier ministre où il participe à la création et met en place un service du haut fonctionnaire de défense et de sécurité. Il en est nommé fonctionnaire de sécurité des systèmes d'information (FSSI) et conseille les autorités des services du Premier ministre, juridictions autorités administratives indépendantes en matière de cybersécurité. Il rejoint ensuite les ministères chargés des affaires sociales en tant que FSSI. En 2020, il rejoint la Région des Pays de la Loire où il est délégué cybersécurité pour puis en 2021 la société Forecomm comme Cyber Security Strategist.
Parallèlement il est ancien auditeur de l'IHEDN-IE, Senior Advisor du CyberCercle, membre du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN), du club EBIOS, de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information (ARCSI) et membre d'honneur de l'Association Pour la Sécurité des Systèmes d'Information de Santé (APSSIS).

Philippe LATOMBE

Député de Vendée
Assemblée Nationale

Philippe Latombe est le député de la première circonscription de Vendée – élu en 2017, réélu en 2022 et 2024 – appartenant au groupe Mouvement démocrate et Apparentés (Modem). Membre de la commission des lois, il est particulièrement investi sur les questions relatives au droit du numérique. Il a ainsi participé activement aux travaux du groupe de travail sur les droits et libertés constitutionnels à l'ère numérique ainsi que de la mission d'information parlementaire sur la blockchain. Philippe Latombe plaide pour un équilibre entre les évolutions technologiques et la protection des droits et libertés individuels garantis à la fois par notre Constitution et par le droit européen. Il a été rapporteur pour avis sur l'article 57 du projet de loi de finances portant sur la possibilité pour les administrations fiscale et douanière de collecter et exploiter les données rendues publiques sur les sites internet des réseaux sociaux et des opérateurs de plateforme. En outre, il a mis en garde le gouvernement et l'ensemble des députés sur les risques d'atteinte au droit à la vie privée de la loi visant à lutter contre la haine sur internet (Loi dite 'Avia'). Conformément aux observations de la Commission européenne sur la loi Avia, Philippe Latombe a voté contre ce texte et ce, contrairement à la position du groupe Modem. Passionné par les enjeux européens, le député a été orateur de son groupe pour la transposition de la directive relative au RGPD, pour la loi portant diverses dispositions d'adaptation au droit de l'UE dans le domaine de la sécurité et pour la loi de transposition de la directive relative à la protection du secret des affaires. Philippe Latombe a également pour projet de mettre en œuvre une Charte du Numérique à la fois au niveau national mais aussi à l'échelle européenne. Il est le rapporteur de la mission parlementaire « Bâtir et promouvoir une souveraineté numérique nationale et européenne.» Il est depuis novembre 2024 commissaire à la CNIL. Philippe Latombe a été nommé en avril 2025 Président de la commission spéciale de l'Assemblée nationale sur le Projet de Loi « Résilience des infrastructures critiques et renforcement de la cybersécurité ».

Jean GEELAND DE MERXEM

Chef de Ventes
Avant de Cliquer

Jean Geelhand De Merxem est Chef de Ventes au sein de la société de cybersécurité Avant de Cliquer, spécialisée en sensibilisation des utilisateurs face aux risques cyber.
Jean a débuté son cursus professionnel il y a plus de 12 ans en tant que militaire, plus précisément dans l'infanterie mécanisée. Après une reconversion réussie dans le secteur des assurances au niveau Master, il s'est spécialisé dans le domaine de la cybersécurité afin de proposer des réponses concrètes qui permettent de protéger les organisations des cyberattaques.
Depuis plus de 3 ans maintenant, il œuvre en ce sens en proposant la solution de sensibilisation Avant de Cliquer.

Julien LOPIZZO

Président & Directeur général
Semkel

Julien Lopizzo est le président & fondateur de la holding d'investissement 777 Corp.
Entrepreneur du numérique depuis 22 ans, il a investi dans une quinzaine de sociétés et créé en parallèle un fonds de dotation 777 Children qui a financé une quarantaine de projets à destination de l'Enfance depuis 2020.
Convaincu que la préparation et l'anticipation sont la meilleure défense face aux risques économiques et cyber, il a fondé Semkel SA, une société spécialisée dans la Risk & Threat Intelligence qui accompagne les organisations privées et publiques dans leur prise de décision et le renforcement de leur cyberdéfense.

Dr Michel DUBOIS

Directeur technique et scientifique
Direction de la Cybersécurité
Groupe La Poste

Michel Dubois est Directeur technique et scientifique au sein de la direction de la cybersécurité du Groupe La Poste. Ingénieur en informatique, titulaire d'un mastère spécialisé en Sécurité des Systèmes d'information et docteur en cryptologie, Michel a exercé pendant près de trente ans des fonctions de responsable de la SSI au sein du Ministère des Armées.
Il est, par ailleurs enseignant chercheur au sein du laboratoire de Cryptologie et de Virologie Opérationnelles de l'ESIEA à Laval. Il est membre du club des experts de la sécurité de l'information et du numérique (CESIN), de l'association des réservistes du chiffre et de la sécurité de l'information (ARCSI) et administrateur du club de la sécurité de l'information français (CLUSIF).

Rodolphe BACA

Cybersecurity Manager
ATOS

Les intervenants

Cyprien GUEYRAUD

Pilote de la sensibilisation Cyber
DSI – Pôle Cyber
Département CyberSchool
Enedis

Aujourd'hui pilote de la sensibilisation cyber à Enedis, Cyprien Gueyraud travaille à ancrer les bons réflexes cyber au sein des équipes. L'objectif : renforcer la culture cyber dans l'entreprise. Auparavant il a gagné son expérience en cybersécurité au cabinet de conseil HeadMind Partners. Son parcours repose sur une double formation : un master en cybersécurité obtenu à l'IIT Chicago, ainsi qu'un diplôme d'ingénieur à CyTech.

Charles-Edouard OUKRAT

Adjoint RSSI
Enedis

Charles-Edouard Oukrat est Adjoint RSSI d'Enedis, il est en charge de l'animation de la Filière cyber de l'entreprise. Son objectif le renforcement de la Cyber sécurité à travers l'animation d'un réseau de référents cyber présent dans chaque directions d'Enedis.
Membre du CESIN, il a plus de quinze ans expérience en cyber sécurité, avec une expertise particulière sur la gouvernance et l'accompagnement de RSSI et de chefs d'entreprise. Il a aussi eu une carrière d'entrepreneur et a participé à un dépôt de brevet concernant une technologie de zéro-trust adaptée à l'OT.

Olivier DEGARNE

Ingénieur Avant-Vente
Stormshield

Olivier Degarne a commencé sa carrière dans le secteur des logiciels chez ESKER, puis a rejoint STORMSHIELD où il a travaillé pendant 22 ans, occupant différents postes tels que formateur, responsable support et ingénieur avant-ventes. Il est actuellement ingénieur avant-ventes pour la région Grand-Est de la France, un rôle qu'il apprécie particulièrement. Sa mission est de montrer que la cybersécurité est une opportunité pour protéger les structures contre les attaques critiques.
Son challenge : « Faire de chaque jour une opportunité de prouver que la Cyber, c'est non seulement une belle histoire européenne (qui plus est française), mais aussi qu'elle est plus que jamais pertinente pour renforcer toute structure contre les attaques les plus critiques »

Yoan ISSARTEL

Co-fondateur - CTO
Elysium Security et Root-me PRO

Yoan Issartel est co-fondateur de la Société Elysium Security et de Root-Me PRO, version pro de la fameuse plateforme Root-Me dédiée à l'apprentissage de la cybersécurité. En tant que CTO, Yoan orchestre les projets et opérations de cybersécurité des deux sociétés. Avec plus de 10 années d'expérience en sécurité défensive, son expertise permet d'intervenir dans des contextes souvent sensibles pour répondre à des problématiques de sécurité complexes : réponse à incident, audit de sécurité, conception d'architecture sécurisée, déploiement de solutions de sécurité, recherche et développement...

Jordan BABEL

Référent cybersécurité en direction régionales Alpes et Sillon Rhodanien
Enedis

Jordan Babel est référent cybersécurité en directions régionales Alpes et Sillon Rhodanien chez Enedis.
Son objectif : garantir l'appropriation des risques et contraintes cyber au plus proche du terrain et favoriser l'amélioration de la vigilance collective.
Ses missions : assurer la sensibilisation de tous les acteurs métiers des organisations ; accompagner les utilisateurs lors des incidents cyber ; conduire le changement amené par les nouveaux risques cyber dans notre quotidien professionnel, mais également personnel ; mesurer et faire progresser la maturité cyber de nos organisations.
Issu des filaires opérationnelles, il a pu, à l'issu d'un parcours certifiant RSSI, intégrer les équipes cyber. Cette double casquette terrain / cyber est un atout pour adapter le langage de la sûreté numérique aux populations non initiées et garantir la montée en puissance de la résilience cyber, ainsi que l'appropriation des règles de sécurisation par tous les acteurs de l'organisation.

Flavien RIEHL

Responsable Pôle Renfort Sécurité
MGM Solutions

Flavien Riehl a intégré M.G.M. Solutions en tant que technicien support. Son immersion progressive dans les différents aspects techniques de l'entreprise lui permet de renforcer ses compétences et sa compréhension globale des enjeux IT.
Grâce à sa curiosité, son sérieux et sa capacité d'adaptation, Flavien s'est rapidement imposé comme un collaborateur fiable et investi. Il participe activement à la gestion des systèmes et à la sécurisation des infrastructures,

Alexandre FOUSSE

Président
STRAAD.A

Depuis 2023, Alexandre Fousse est Président et Associé fondateur de STRAAD.A, cabinet de conseil et expertise en sécurité globale positionné comme un partenaire de l'anticipation et de la maitrise des risques qu'ils soient liés à des thématiques de cybersécurité, sûreté, sécurité économique ou encore de résilience.
Alexandre Fousse opère avec ses équipes des activités de sûreté bâtimentaire, de cybersécurité indus et bâtimentaire, de résilience et d'homologation de SI supports et métiers.

Daniel COISSARD

Directeur des Usages Numériques
Département du Rhône

Après avoir dirigé le GIP Maximilien (2017-2021), première plateforme d'e-administration, et développé la plateforme e-bourgogne, la toute première plateforme de marchés publics (2008-2016), Daniel Coissard a rejoint, courant septembre 2021, le département du Rhône, en tant que Directeur des Usages Numériques. Fort de 30 ans d'expérience dans le domaine informatique (développement de jeux dans les années 80, formation, réseaux-télécommunication et gestion de projets de dématérialisation de procédures administratives et facturation), son travail est toujours axé sur :

- L'organisation, la coordination et la conduite de projets ouverts et innovants.
- La relation et la satisfaction de mes clients (internes ou externes).
- La sécurité des biens, des données et des personnes.

Ses motivations au quotidien :

- définir une stratégie, la décliner en plans d'action et piloter sa mise en œuvre,
- créer de nouveaux services numériques sécurisés répondant à un besoin ou une évolution réglementaire,
- optimiser le fonctionnement de l'organisation et coordonner l'action des développeurs, des chefs de projets et des clients,
- innover dans la recherche de solutions et l'optimisation de résultats,
- construire en commun une dynamique d'équipe et contribuer à développer le potentiel de chacun.

Henri SAILLARD

Directeur Projets transverses
Groupe La Poste

Après avoir occupé différentes fonctions en management opérationnel, en logistique ou en marketing au sein de grands groupes internationaux, Henri Saillard a rejoint La Poste où, durant 13 ans, il a contribué au développement et à la transformation des activités courrier, colis et services de proximité en territoire, notamment en Normandie et en Ile de France en tant que Directeur Exécutif.
Il est depuis trois ans en charge du déploiement d'un des programmes stratégiques d'accélération du groupe La Poste, dédié au développement territorial. A ce titre, il accompagne les différentes entités qui composent le groupe La Poste dans le développement des services de proximité humaine ainsi que des services numériques de confiance, auprès des territoires.
C'est dans ce cadre qu'il conduit, en partenariat avec la Banque des Territoires, les travaux autour de la note de conjoncture « Data, intelligence artificielle et cybersécurité dans les territoires ».

Pascal NAHON

Directeur Cybersécurité
Directeur Région Paris / Ile de France
ATOS

Avec une carrière impressionnante dans la tech et la cybersécurité, Pascal est une figure incontournable du secteur. Depuis plus de 30 ans, il explore les arcanes du numérique, de l'exploitation des systèmes à la gouvernance SSI, en passant par les tests d'intrusion, la gestion de crise et l'IA.
Aujourd'hui Directeur Cybersécurité de l'agence Atos Paris / Ile de France, il conjugue expertise technique, vision stratégique et capacité à embarquer les organisations dans une véritable culture cyber. Passé par la banque, le retail, la santé ou encore la supply chain — sans oublier une aventure entrepreneuriale à l'international de plus d'une décennie — Pascal a vu le numérique évoluer… et les cybermenaces avec.
Son regard éclairé sur les enjeux actuels de la cybersécurité et de l'IA en fait un interlocuteur qui compte, capable de vulgariser sans simplifier, et de faire réfléchir sans moraliser.
Sans prétention, mais avec conviction, il continue de sensibiliser, d'accompagner et de faire progresser les structures.
Toujours avec un pas de côté et un brin d'humour, Pascal partage son expérience sans dogmatisme. Il sait que la cybersécurité n'est jamais acquise, que les certitudes sont souvent les premières failles, et que le bon sens fait parfois plus que les grandes théories. Il sait que dans ce métier, on n'a jamais vraiment « tout vu ». Et tant mieux : c'est ce qui le pousse à rester alerte, à apprendre encore, et à transmettre sans jamais se prendre trop au sérieux. Il préfère les échanges concrets aux discours figés, et les discussions humaines aux grandes incantations techniques. Bref, un passionné qui garde les pieds sur terre — et les systèmes sous contrôle, autant que possible.

Les intervenants

Hervé PELLARIN

RSSI
Centre hospitalier Annecy Genevois

Hervé Pellarin est un bidouilleur, curieux compulsif, touche à tout, en poste comme RSSI dans le secteur de la santé, au Centre hospitalier Annecy Genevois. C'est à travers son regard de RED TEAMER qu'il protège ses établissements de santé en mettant l'accent sur la continuité d'activité, car l'hôpital, comme le monde, ne s'arrête jamais.

François BRIAT

Ingénieur projets
Laboratoire de recherche
Ecole Nationale Supérieure de la Police

François Briat est Ingénieur projet au Laboratoire de Recherche de l'Ecole Nationale Supérieure de la Police, en charge du pôle « Recherche & Innovation ».
Dans ce cadre il est notamment le représentant du ministère de l'Intérieur pour le projet ANR « ARCO » sur les baignades et les noyades en rivières urbaines, ainsi que pour le projet européen « TEAM-UP » sur les nouveaux équipements NRBC et la gestion de crise.
Il est également gestionnaire de la collection criminalistique de l'ENSP.

Denis MILLET

Délégué de région académique au numérique éducatif,
Conseiller du recteur de l'académie de Lyon
Rectorat de Lyon

Après quelques années dans le monde industriel, Denis Millet a exercé pendant 10 ans comme enseignant en Sciences et Techniques Industrielles (STI), puis durant les 10 années suivantes en tant qu'inspecteur en Sciences et Techniques Industrielles. Il a ensuite occupé le poste de délégué académique au numérique, conseiller du recteur de l'académie de Lyon. Depuis 2025, il est délégué de région académique au numérique éducatif, conseiller du recteur de la région académique Auvergne-Rhône-Alpes. En parallèle des missions afférentes aux différents postes occupés, Denis Millet a participé à de nombreuses actions et coopérations au niveau du ministère de l'Éducation nationale (création et rénovation de diplômes, lien avec le monde professionnel...) ainsi qu'à l'international (missions avec l'OCDE, missions interministérielles à l'étranger).

Jérôme SAIZ

Fondateur
OPFOR INTELLIGENCE

Jérôme Saiz est consultant en protection des entreprises et fondateur de la société OPFOR Intelligence, où il accompagne les entreprises dans la gestion des crises cyber. Il intervient également en tant que Crisis Manager & Incident Handler @ CERT-Intrinsec.
Il est auditeur de l'Institut National des Hautes Etudes pour la Sécurité et la Justice (18e session SNS), titulaire du titre RNCP-1 d'expert en protection des entreprises et certifié CT CERIC en sûreté / lutte contre la malveillance par le Centre National de Prévention et de Protection (CNPP), réserviste citoyen auprès de la Mission Numérique de la Gendarmerie Nationale, membre du Cybersecurity and cybercrime Advisors Network (CyAN) et senior advisor du CyberCercle.
Jérôme SAIZ a été auparavant expert sécurité, responsable de la communauté RSSI au sein de la société Qualys, un éditeur de solutions d'analyses de vulnérabilités, et journaliste spécialisé dans les questions de cyberdéfense. Il a enseigné durant 11 ans à l'école d'ingénieurs EPITA (cycle Systèmes, Réseaux & Sécurité) et au Centre National de Prévention et de Protection. Il intervient également au profit de nombreux autres centres d'enseignements (Université Paris Dauphine, Pôle Universitaire Léonard de Vinci, etc.).

GCA (2S) Jacques HEBRARD

Senior advisor
CyberCercle

Le Général de corps d'armée (2S) Jacques Hebrard est ingénieur de l'École de l'Air et spécialiste en criminalistique. Après une formation en gendarmerie et plusieurs postes de commandement, il joue un rôle clé dans la création de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN), avant de diriger de 2011 à 2015 le Pôle Judiciaire de la Gendarmerie Nationale (PJGN), contribuant à la construction du site de Pontoise. Commandant de la Région Gendarmerie des Hauts-de-France et de la Gendarmerie pour la zone de défense et de sécurité Nord de 2015 à 2018, il est ensuite placé en deuxième section des officiers généraux. Il est depuis coordonnateur national d'assistance aux victimes et familles de victimes de catastrophes auprès de la Délégation Interministérielle à l'Aide aux Victimes, et senior advisor du CyberCercle. Le GCA (2S) Jacques HEBRARD est auditeur de la 43ème session du Centre des Hautes Etudes de l'Armement (CHEAr) et titulaire du diplôme postgrade de criminalistique chimique de l'Université de Lausanne, lauréat de cette université. Il est Officier de la Légion d'Honneur et Commandeur de l'Ordre National du Mérite.

Bruno LEAL DE SOUSA

RSSI Groupe
GL Events

Bruno Leal De Sousa est un Chief Information Security Officer (CISO) expérimenté, spécialisé dans la cybersécurité et la gouvernance des systèmes d'information. Fort de plus de 10 ans d'expérience en management des systèmes d'informations et cybersécurité avancée, il évolue dans des environnements complexes à forte dimension internationale.
Actuellement RSSI Groupe chez GL events, il pilote la stratégie de sécurisation, la gouvernance SSI et la préparation d'événements majeurs tels que les JOP 2024, la COP16 ou encore les WorldSkills 2024.
Certifié ISO 27032, Bruno est également formateur en école d'ingénieurs, transmettant son expertise aux futures générations de professionnels du numérique. Il a construit et dirigé plusieurs départements cybersécurité et projets, mettant en place des structures robustes adaptées aux enjeux stratégiques des entreprises. Rodé aux situations de crise grâce à son solide parcours dans l'infrastructure SI, il a développé, au fil de ses expériences, des organisations de gestion de crise efficaces, capables de détecter, réagir et se relever rapidement face aux incidents majeurs.

RENCONTRES CYBERSÉCURITÉ AUVERGNE-RHÔNE-ALPES

Les intervenants

RENCONTRES
CYBERSÉCURITÉ
AUVERGNE-RHÔNE-ALPES

MERCI À NOS PARTENAIRES

AvantdeCliquer.com
L'humain au cœur de la cybersécurité

Un programme innovant de sensibilisation AUTOMATIQUE créée SUR MESURE pour développer des réflexes de cybersécurité !

Réduisez le risque d'hameçonnage sereinement grâce à notre Algorithme intelligent.

Avant de Cliquer divise par 10 le risque de cyberattaque grâce à la sensibilisation de vos collaborateurs sans besoin de l'intervention du responsable informatique.

"Ayez l'esprit tranquille, on s'occupe de tout !"

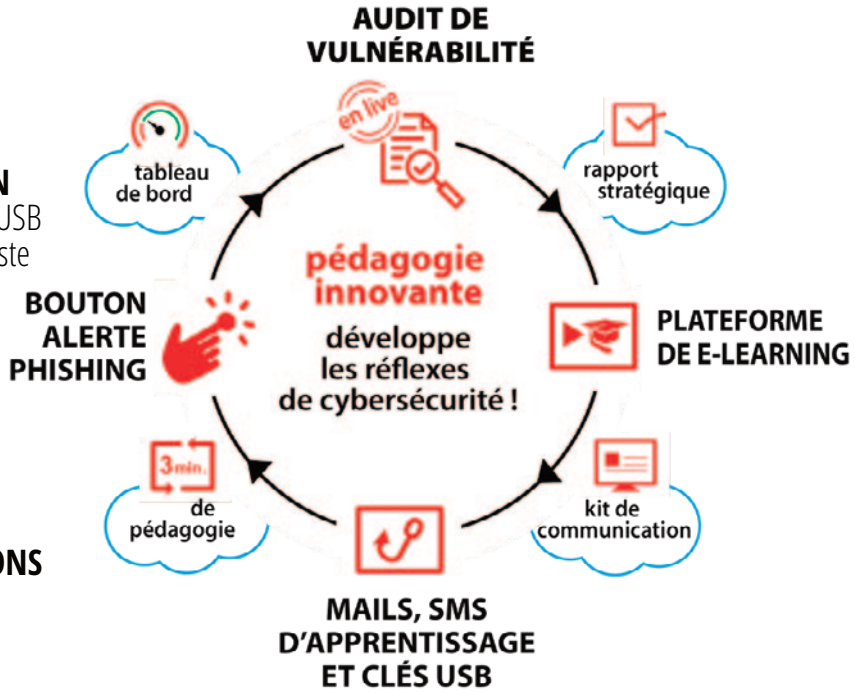
Conçu, crée et hébergé en France

APPRENTISSAGE THÉORIQUE
kit de communication et plateforme d'e-learning

APPRENTISSAGE PAR L'ACTION
E-mails automatiques ciblés, SMS, USB
Sensibilisation immédiate sur le poste

ACCOMPAGNEMENT
Chargé(e) de compte dédié(e),
Actions spécifiques à l'organisation
Programme personnalisé

REMONTÉE D'INFORMATIONS
Tableaux de bord
Bouton Alerte Phishing



Algorithme intelligent

Faites de vos collaborateurs des acteurs efficaces de la lutte contre le Phishing.

Mention Spéciale Expoprotection – Sureté-Sécurité et Cyberprévention
Lauréat de l'Innovation SANTEXPO – Transformation Digitale & Cybersécurité
Lauréat de l'intelligence économique – Trophées de l'agroalimentaire
Finaliste du prix de l'innovation du Salon des Maires et des Collectivités Locales
BPI France – Solution pertinente pour sensibiliser les utilisateurs à la cybersécurité

HEXATRUST CYBERSECURITY & DIGITAL TRUST
ACN
Référencé GouvTech | RÉPUBLIQUE FRANÇAISE
FFCYBER
FRANCE CYBER SECURITY
FRANCE RELANCE
C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière
UGAP

SUR TOUS LES FRONTS

PRODUITS NEMESIS

Solutions souveraines

En tant que Dirigeant, DSI ou RSSI, vous êtes garant de la sécurité du système d'information de votre organisation. Le marché de la cybersécurité fourmille de solutions qui s'avèrent bien souvent insuffisantes, complexes ou trop coûteuses.

Les challenges sont nombreux, le risque omniprésent et de nombreuses questions se posent.

C'est en partant de ces constats que nous avons développé la suite NEMESIS :
une suite de sécurité souveraine, conçue pour offrir une protection globale, opérationnelle et accessible à tous types d'organisations.

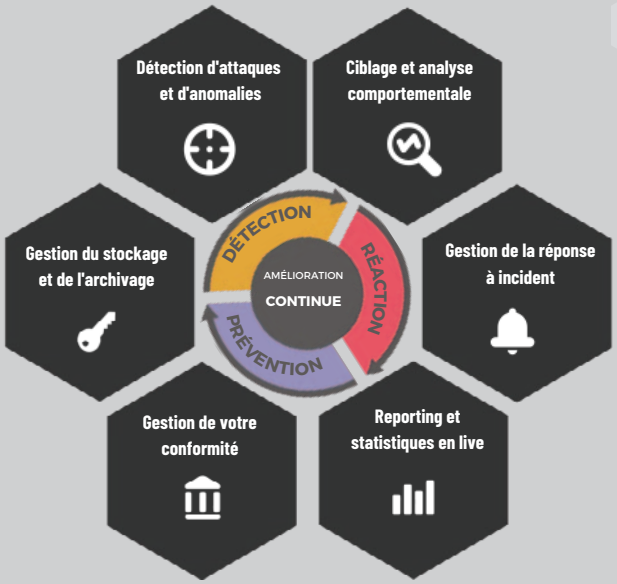
VOS PROBLÉMATIQUES

- EXPOSITION ACCRUE À LA MENACE
- MANQUE DE VISIBILITÉ SUR VOTRE PROTECTION RÉELLE
- MANQUE DE RESSOURCES ET DE COMPÉTENCES
- ACCESSIBILITÉ DES SOLUTIONS DE PROTECTION

NEMESIS UNIFIED PROTECTION

Grâce a des capacités unifiées de détection et de réponse aux incidents de sécurité, **NEMESIS UP (SIEM, SOAR, INTEL)** agit comme un système d'alarme dédié.

Il offre une **protection centralisée en temps réel** des systèmes d'information de tous types (IT/OT) tout en vous permettant de **réduire vos coûts d'exploitation** et de **répondre à vos obligations de conformité.**



- **SIEM** — CORRÉLER LES INFORMATIONS DE SÉCURITÉ ET DÉTECTER LES MENACES
- **SOAR** — ORCHESTRER ET AUTOMATISER LES PROCESSUS DE RÉPONSE AUX INCIDENTS
- **INTEL** — ENRICHIR, CONTEXTUALISER ET OPTIMISER LES FONCTIONS DE DÉTECTION ET RÉPONSE

- PROTECTION CONTINUE <24/7>
- VISION GLOBALE ET UNIFIEE
- ACCESSIBLE À TOUS

NEMESIS SECURE LOG

Avec NEMESIS SL : **centralisez, archivez, protégez** et consultez l'ensemble des **traces et événements de sécurité** générés par votre système d'information. Idéal pour réaliser des investigations numériques ou répondre aux exigences de conformité.

NEMESIS OPEN xDR

Avec NEMESIS Open xDR : **raccordez des solutions de sécurité complémentaires** et **open source** sur une interface unique afin de centraliser leur gestion quotidienne et réduire les coûts d'exploitation associés.

La Région Auvergne-Rhône-Alpes soutient nos activités de R&D et d'innovation autour de NEMESIS

www.elysium-security.com

DE VOTRE PROTECTION

ELYSIUM SECURITY

COMPTOIR SÉCURITÉ

Vous manquez d'une expertise ou de temps pour traiter une problématique de sécurité ?

L'abonnement au Comptoir Sécurité Elysium vous permet de profiter d'un lien permanent et privilégié avec nos experts, capables d'intervenir sous des délais garantis et à des coûts préférentiels.

SERVICES OFFENSIFS ET DEFENSIFS

Des réponses concrètes pour une défense adaptée, cohérente et conforme aux normes et bonnes pratiques.

- **Tests d'intrusion & Audit de sécurité**
- **Investigation & Réponse à incident**
- **Conseil & Expertise technique**

FORMATIONS EN CYBERSECURITÉ

Des formations pour tous niveaux, conçues et animées par des experts et s'appuyant sur des environnements pratiques innovants (dont Root-Me PRO).

Qualiopi processus certifié — RÉPUBLIQUE FRANÇAISE

RootMe PRO

ROOT-ME PRO

La version Pro de la fameuse plateforme Root-Me (plus de 700K membres) qui fédère une communauté de passionnés de la cybersécurité autour de nombreux challenges et CTF.

- OUTILLER LA FORMATION ET LE SUIVI DE VOS COLLABORATEURS
- FÉDÉRER VOS COLLABORATEURS AUTOUR D'ÉVÉNEMENTS EXCLUSIFS
- DIFFUSER VOS OFFRES ET IDENTIFIER VOS FUTURS EXPERTS
- VOUS IMPLIQUER AUPRÈS DE LA COMMUNAUTÉ ET GAGNER EN VISIBILITÉ

STORMSHIELD

Le choix européen de la cybersécurité

Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin d'assurer la cybersécurité de leurs infrastructures critiques, de leurs données sensibles et de leurs environnements opérationnels. Les technologies Stormshield, certifiées et qualifiées au plus haut niveau européen, répondent aux enjeux de l'IT et de l'OT afin de protéger leurs activités.

Notre mission : cyber-séréniser nos clients pour qu'ils puissent se concentrer sur leur cœur de métier, si cruciale pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations. Choisir Stormshield, c'est privilégier une cybersécurité européenne de confiance.

En France, **Stormshield détient plusieurs Visas de Sécurité de l'ANSSI**. Par ailleurs :

- La solution **Stormshield Network Security** est la première et seule gamme de « firewall chiffreur » **qualifiée au niveau Standard et agréée DR**.
- La solution **Stormshield Data Security** est la première et la seule solution de chiffrement des données **certifiée CSPN**, disponible sur Google Workspace.
- La solution **Stormshield Endpoint Security Evolution** est la solution EDR de Stormshield **certifiée CSPN**.

En Espagne, nous sommes également le seul éditeur de pare-feux à avoir obtenu les deux qualifications « Producto CCN Aprobado » et « Producto CCN Cualificado ».

Nos solutions sont alignées sur les meilleurs standards. Nos expertises et la robustesse de nos produits nous permettent d'accompagner les entreprises dont la criticité cyber est extrême. Et surtout, lorsque l'IT & l'OT deviennent des éléments vitaux sur les plans économiques, sociétaux, techniques et humains, il est primordial d'être cyber-résilient.

Des technologies de confiance

Stormshield propose un portefeuille de produits mature permettant une large couverture des besoins de protection des environnements IT/OT. Nos expertises nous permettent d'accompagner les entreprises dont la criticité est extrême par rapport aux problèmatiques de cybersécurité. C'est pourquoi, nous œuvrons dans le développement d'une protection durable contre les menaces les plus avancées, au travers de trois gammes de produits.

STORMSHIELD NETWORK SECURITY

Une gamme de pare-feux & VPN de nouvelle génération

STORMSHIELD DATA SECURITY

Un chiffrement de bout en bout multi-devices et multi-applications

STORMSHIELD ENDPOINT SECURITY

Une protection avancée des postes et serveurs Windows

La gamme Stormshield Network Security englobe une offre industrielle via la mise à disposition de pare-feux renforcés, le SNi40, le SNi20 et le SNi10 (les seuls pare-feux industriels qualifiés par l'ANSSI), pour les environnements à fortes contraintes. Ces boîtiers de sécurité, co-désignés avec des partenaires industriels de renom, s'intègrent facilement aux environnements opérationnels et garantissent une détection et protection sans aucun impact sur l'activité industrielle.

Par ailleurs, Stormshield a lancé en 2021 le SNxr1200, un pare-feu ultra durci qui répond parfaitement aux exigences et enjeux complexes de la sécurité des environnements critiques. Développé en respectant un certain nombre de standards militaires, il dispose de nombreuses certifications environnementales lui permettant d'être déployé dans des contextes contraints.

Un réseau mondial de partenaires certifiés

Stormshield, c'est aussi un réseau de partenaires de confiance, qui portent nos engagements et qui nous permettent de faire rayonner nos valeurs françaises et européennes bien au-delà de nos frontières.

Nous avons créé ce qui est le 1er réseau de partenaires cybersécurité en France. Stormshield, c'est plus de 800 partenaires certifiés sur le territoire (plus de 1500 personnes par an) et plus globalement, une présence dans 40 pays qui nous permettent d'avoir une visibilité et une présence au plus près de nos clients.

Cette proximité se révèle déterminante pour co-construire des offres de sécurité plus simples et plus fiables qui proposent une alternative robuste aux solutions américaines et israéliennes. Des solutions de confiance, auditées en toute transparence et garanties sans backdoors !

Pour en savoir plus : www.stormshield.com

Semkel

RISK & THREAT INTELLIGENCE

Parce qu'aucune menace ne reste isolée.

Cyberattaque. Dénigrement en ligne. Fraude. Intrusion. Prédation économique.

Les menaces s'hybrident, se combinent, frappent là où l'on ne regarde pas. **Chez SEMKEL**, nous intégrons l'intelligence stratégique au cœur de la sûreté.

Nous accompagnons les décideurs publics et privés dans la **détection des signaux faibles**, la **protection des actifs critiques** et l'**élaboration de réponses efficaces face aux menaces contemporaines**.

Sûreté économique. Sûreté informationnelle. Sûreté cyber.
Trois dimensions. Une seule exigence : vous protéger.

www.semkel.com

+33 (0) 4 78 51 13 79

Lyon / Paris - Périmètre d'intervention monde

Investigation - Surveillance - Remédiation

Menaces informationnelles

Désinformation | Attaque réputationnelle | Mésinformation

Menaces cyber

Ingénierie sociale | Exploitation de vulnérabilités | Cyberattaques

Vol d'identifiants | Ransomware / Malware | Fuite de données

Menaces économiques

Espionnage | Prédation économique | Actes malveillants

Crise systémique | Fraude et tromperie | Atteinte aux dirigeants

Géopolitique

Supply-chain

Activisme

Cybercriminalité

Faille interne

Crime organisé

M&A

SÛRETÉ 360°

- Surveillance deep & dark web (CTI / EASM):
  - 4,3 milliards d'adresses IP scannées quotidiennement.
  - Plus de 300 milliards de données, marketplaces et forums du dark web.
  - Telegram, Discord, etc.
- Surveillance clear web (OSINT / SOCINT) :
  - Réseaux sociaux, médias, sites internet.
  - Forums : Reddit, 4chan, etc.
- Bases spécialisées : sanctions, KYC, législations, etc.

Des process et ressources dédiés :

- Service managé
- Analystes dédiés et comitologie personnalisée
- Rapports et bulletins d'analyse
- Alertes en temps réel

Semkel
RISK & THREAT INTELLIGENCE

STRAAD.A

incubateur de vos ambitions

Cyber Sécurité

Appuyer votre stratégie d'anticipation du risque et la mise en oeuvre de solutions adaptées

Sûreté

Optimiser l'existant et construire les modèles de protection de demain

Sécurité Économique

Déployer les démarches opérationnelles garantissant la sécurisation de vos actifs stratégiques

Résilience

Anticiper, structurer et tester votre capacité à répondre aux évènements perturbateurs

Data & IA

Intégrer sereinement et efficacement leurs usages dans le quotidien du management des risques

Nos appuis pour les ETI & PME

Prestations réalisées au forfait et/ou à travers notre centre de conseil et expertise externalisé

Transfert de savoir-faire à la carte
Bibliothèque de 30 thématiques
(vulgarisation, programme, technique)

Réponse aux exigences des AO clients finaux
(PAS, SI dédié, processus et procédures, cotation)

Conformité NIS 2
(organisationnelle et technique)

Étude pour choix solutions et services
(Cyber, Prestataire IT, sûreté, partenaire clé)

Pilotage des prestataires critiques
(Cloud provider, Télé mainteneur, gestionnaire IT)

Obtention de certifications et autorisations
(ISO 27001 et suite, environnements réglementés)

Ecosystème souverain

dust MOBILE
EGERIE
FROGTRUST
PRIVATE DISCUSS
RESO
SAFE
SafeCloudBox
SECKIOT
Teria

MGM SOLUTIONS

LA CYBERSÉCURITÉ, VOTRE PROCHAINE PRIORITÉ.

15+
cyber-incidents remédiés avec succès

Service n°1

PRÉVENTION

Réduisez votre exposition aux cyberattaques et formez vos utilisateurs.

Service n°2

SUPERVISION

Améliorez votre capacité de détection et de réaction aux incidents.

Les 360° de la cybersécurité

Service n°3

REMÉDIATION

Une réponse immédiate à la suite d'une attaque sur vos systèmes, une évaluation de l'impact et une assistance technique.

Service n°4

SÉCURISATION

Optimisez la sécurisation de votre système d'information et augmentez votre résilience.

NOS RÉFÉRENCES

Centre Hospitalier Les Franciliens
HNO Hôpitaux Nord-Ouest Villefranche-sur-Saône
AXA
caluire et cuire
Oniris VetAgroBio Nantes École Nationale
april

11 ANS

D'expertise dans la gestion des systèmes d'information et la résolution d'incidents cyber.

+25

Équipe d'experts passionnés

Notre identité

Prévention

Supervision

Remédiation

Sécurisation

Le juste positionnement du curseur entre production et sécurisation !

M.G.M. Solutions est un **acteur majeur** dans le domaine de la **cybersécurité** grâce à son expertise dans la **remédiation des systèmes d'information**, la sécurisation des systèmes ainsi que la **prévention des risques.**

Historiquement positionné comme concepteur et intégrateur de **solutions d'infrastructures**, notre **vision globale** permet d'accompagner nos clients vers une **transformation numérique complète et sécurisée**.

Forte de son expérience en **reconstruction de nombreux systèmes d'information**, la Business Unit cybersécurité M.G.M. Solutions vous accompagne également **post-cyberattaque.**

Dès lors d'une confirmation d'un acte cyber, nos experts vous apporteront le **soutien et l'accompagnement** nécessaires pour une **reprise d'activité dans les plus brefs délais.**

Contactez-nous

04 82 53 84 65 commercial@mgmsolutions.fr

En cas d'urgence cyber, contactez le **CERT by M.G.M. : 04 28 29 79 85**

BlueFiles est une solution française de transfert de fichiers, qui permet d'envoyer des documents et des messages chiffrés en toute sécurité. Elle s'adresse aux professionnels en leur offrant la possibilité de communiquer de manière protégée avec tous leurs interlocuteurs, incluant ceux situés à l'extérieur de leur structure. Elle est destinée aux entreprises de toutes tailles, et particulièrement celles dans les domaines de la santé, de l'informatique ou de la justice, qui partagent de nombreuses données privées au quotidien.

Une solution de transfert de fichiers performante et facile à prendre en main

BlueFiles sécurise l'ensemble de vos échanges. BlueFiles dispose de plusieurs visas et certifications, gages de confiance en matière de sécurité et de traitement des données

Une protection optimale pour assurer la confidentialité de vos données

BlueFiles protège l'envoi de fichiers vers tous types de destinataires grâce au chiffrement de bout en bout et la mise en place d'un hébergement certifié. Pour renforcer la sécurité des données partagées, la solution propose également :

Des tarifs adaptés à vos besoins et votre structure

Concernant les tarifs, l'outil propose plusieurs offres en fonction de vos besoins, de la taille de votre entreprise et du nombre d'utilisateurs.

www.BlueFiles.com

CYBER CERCLE

Missions / Vocation

Le CyberCercle est un cercle de réflexion créé en 2011 lorsque la sécurité numérique – la cybersécurité - n'était encore trop souvent qu'à ses débuts pour de nombreuses organisations et l'apanage des experts techniques.

Convaincu que la sécurité et la confiance numériques ne pourront progresser qu'à la condition d'œuvrer collectivement, le CyberCercle s'est fixé 5 objectifs :

- Être un cadre d'échanges privilégiés pour les questions de sécurité et la confiance numériques
- Être une plateforme de collaboration Public-Privé réunissant l'ensemble des parties prenantes
- Décrypter le cadre réglementaire et les politiques publiques de sécurité et confiance numérique
- Être une force de propositions pour accompagner la réflexion et le travail des parlementaires et des élus locaux sur ces questions
- Favoriser le développement d'une culture de sécurité numérique, au delà de la sphère des experts techniques

La sécurité et la confiance numériques ne constituent pas une finalité en soi mais un ensemble de disciplines et d'expertises à réunir aux services des métiers.
Dans cette perspective, le CyberCercle traite de sujets sectoriels avec une forte expertise dans les domaines de la santé, du maritime, de la défense, des territoires et des collectivités et de sujets thématiques comme la réglementation, l'innovation et la recherche, la formation, l'industrie 4.0, ...

Valeurs

Si la sécurité numérique représente un marché en tant que tel, ce qui montre son utilité économique et sa meilleure prise en compte par les organisations, nous ne devons pas oublier que la sécurité et la confiance numériques sont avant toute chose des enjeux de développement, de sécurité et de souveraineté, que ce soit au niveau national, européen mais aussi territorial.

Ce sont ces dimensions fondamentales au service de tous qui animent l'action du CyberCercle dont la philosophie s'appuie sur des valeurs d'engagement, de confiance, de sens du collectif et d'éthique.

Activités

Les activités du CyberCercle s'articulent autour de matinales, de journées de rencontres, de publications et de modules de formation, orchestrées au travers de la définition d'un schéma de cohérence et d'organisation des thèmes et des actions.

Ce schéma s'est construit principalement ces dernières années autour de 3 thèmes majeurs :

- Confiance numérique et politiques publiques au niveau national et européen
- Confiance numérique des territoires
- Financement et leviers de la sécurité numérique

Positionnement

Le CyberCercle a un positionnement unique.

Il est à la fois :

- un « think tank » par la production de contenus, réflexions et propositions issues de travaux collectifs, par la diffusion d'analyses de personnalités et par son travail d'animation de communautés ;
- un organisateur d'événements par la création et la gestion d'événements adaptés pour diffuser les éléments d'acculturation à la sécurité numérique sur l'ensemble du territoire et valoriser le travail parlementaire ;
- un acteur du conseil et de la formation pour accompagner les infrastructures dans leur réflexion sur leur politique interne de sécurité numérique ;
- un cadre d'influence par son travail avec les pouvoirs publics.

Il représente un cadre de confiance qui œuvre sur des sujets d'intérêt collectif, une entité fédératrice en lien et partenariat avec de nombreuses associations et organisations publiques et privées.

Le CyberCercle a souvent été précurseur, parfois suivi ou imité, et après tout tant mieux. Cela montre que nous oeuvrons dans la bonne direction, dans ce domaine où les certitudes sont peu nombreuses et souvent de fausses amies, ce domaine qui demande en permanence d'être à l'écoute, de s'adapter, de réagir mais toujours au service des métiers et de l'intérêt général.

Le CyberCercle depuis 2012

- 140 Matinales à Paris
- 32 Matinales en région (depuis 2019)
- 4 Cycles annuelles Défense & Cyber (depuis 2022)
- 39 journées de Rencontres
- + de 750 intervenants
- + de 12100 participants
- 128 Paroles d'Experts (depuis 2020)
- 18 senior advisors et ambassadeurs en région

CYBER CERCLE

EN QUELQUES PHOTOS

CYBER CERCLE

MERCI À NOS PARTENAIRES & SOUTIENS

CYBER CERCLE

92 Cours Lafayette - 69003 Lyon • contact@cybercercle.com • cybercercle.com • @CyberCercle