SERMA
SAFETY & SECURITY

CYBERSÉCURITÉ DES SYSTÈMES D'INFORMATION

SERMA Safety and Security couvre l'ensemble du spectre de la cybersécurité. L'ensemble des problématiques de prévention, détection, protection et remédiation sont traitées afin de faire face aux attaques informatiques.

La sécurité des systèmes d'information est devenue un enjeu important au sein des organisations et encore plus depuis le recours au télétravail. Il est essentiel de veiller à sécuriser les systèmes d'information dès la phase de conception et ce jusqu'au suivi de leur fonctionnement, en passant par leur implémentation et leur gouvernance.

L'ouverture des systèmes d'information aux utilisateurs, partenaires et fournisseurs de services de l'entreprise les expose à de nouvelles menaces. De la même manière, les outils collaboratifs, le nomadisme, le cloud et les SaaS permettent non seulement aux utilisateurs d'avoir accès aux ressources mais aussi de transporter une partie du système d'information en dehors de l'infrastructure sécurisée de l'entreprise.
Ces nouveaux paysages et écosystèmes représentent des défis en matière de sécurisation pour lesquels un accompagnement par des experts est essentiel.

Il est essentiel pour votre entreprise :

- de connaître vos ressources en matière de systèmes d'information et de définir les périmètres sensibles à protéger afin de garantir une exploitation maîtrisée et raisonnée de ces ressources au travers de campagnes d'audits;
- de mettre en place des plans stratégiques, roadmaps, démarches et mesures pour évaluer les risques et définir les objectifs de sécurité à atteindre à l'aide de méthodologies à l'état de l'art comme EBIOS Risk Manager, ISO 27XXX...;
- de mettre en place des solutions de sécurité adaptées à vos systèmes d'information dans l'intérêt de protéger les infrastructures et les environnements On-premise ou Cloud, les données et les applications, les terminaux et les accès aux ressources de l'entreprise au travers de différentes approches (micro-segmentation, Zero Trust, SASE, IAM, Bastion, MFA...);
- de superviser en continu la sécurité des actifs essentiels à l'aide de solutions d'EDR Managé ou d'infogérance des équipements de sécurité. Ceci pouvant être étendu à des services avancés de sécurité grâce à la mise en place d'un SOC (Security Operation Center).

OFFRE

GOUVERNANCE, RISQUES ET CONFORMITÉ

SÉCURITÉ OFFENSIVE

INTÉGRATION DE SOLUTIONS

CENTRE OPÉRATIONNEL DE LA SÉCURITÉ (SOC)

NOTRE SAVOIR-FAIRE

GOUVERNANCE, RISQUES ET CONFORMITÉ

- Compréhension et identification des processus métiers
- Évaluation et diagnostic du niveau de sécurité
- Conformité par rapport à des référentiels de sécurité existants (ISO 2700X, NIS2, LPM, RGPD, ...)
- Audit organisationnel
- Analyse de risques
- Mise en place des processus et du corpus documentaire (PSSI, PAS, ...) visant à élever le niveau de sécurité du système y compris ce qui attrait à la résilience (gestion de crise, gestion des incidents, plan de continuité et reprise d'activité,...)
- Diagnostic Cyber-Défense et France Relance parcours cybersécurié
- Sensibilisation

SÉCURITÉ OFFENSIVE

- Audits qualifiés PASSI RGS et PASSI LPM
- Test d'intrusion – Infrastructure (boite noire, blanche, grise, DSP2 ...)
- Test d'intrusion – Applicatif
- Red Team
- Audit de configuration
- Audit d'architecture (On-Premise et Cloud)
- Audit de code source
- Audit, support et suivi des fournisseurs (ISO/IEC)
- Audit systèmes techniques
- Campagne de phishing
- Analyse et identification des vulnérabilités
- Remédiation et durcissement
- Reverse Engineering

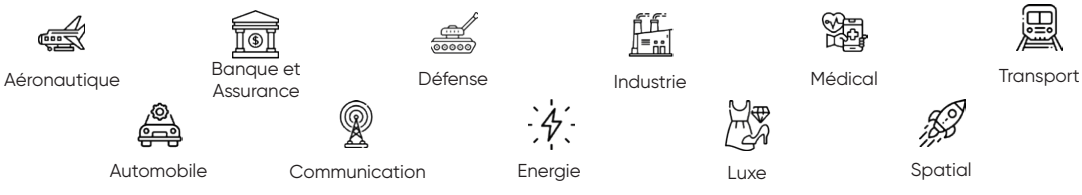
INTÉGRATION DE SOLUTIONS

- Audit, étude et conseil
  - Audit d'architecture et de configuration;
  - Étude et proposition de solution technique;
  - Comparatifs techniques et POC des solutions;
  - Rédaction des documents de synthèse;
  - Accompagnement sur l'évaluation des réponses d'AO et RFP.
- Intégration de solutions et expertise technique
  - Design et conception d'architectures dans le contexte client en suivant les bonnes pratiques sécurité;
  - Documentations techniques : DAT, DI, DR, DEX;
  - Pilote / Déploiement / Migration / Mise en production;
  - Transfert de compétence;
  - Expertise technique spécifique.
- Support, maintenance et service d'assistance technique
  - Support des solutions
  - Maintenance
  - Service d'Assistance Technique (SAT)
  - Vérification périodique
  - Veille technologique
  - Evolution

CENTRE OPÉRATIONNEL DE LA SÉCURITÉ

- Prévention
  - Veille en cybersécurité;
  - Scénarios de détection sur-mesure et adaptés à l'environnement client;
  - Scans de vulnérabilité pour identifier le niveau d'exposition aux actes malveillants;
  - Infogérance des équipements de sécurité réseaux principalement sur les firewalls Palo Alto, Check Point, Cisco.
- Détection
  - Déploiement d'un socle de détection (SIEM) afin de surveiller en temps réel, détecter, qualifier et réaliser les investigations en cas de menace avérée aboutissant à un incident de sécurité. Déploiement On-Premise ou Cloud sur architecture dédiée ou mutualisée;
  - Maîtrise de nombreuses solution SIEM telles que Microsoft Azure Sentinel, Splunk, Qradar;
  - Service de détection opéré en 24/7.
- Réaction / Réponse à incidents
  - Intervention, à distance ou sur site, pour endiguer la menace en cours et éradiquer le risque;
  - Investigation pour comprendre d'où provient la menace et comment elle se propage.
- Remédiation
  - Accompagnement à la récupération des données;
  - Plan de remédiation;
  - Vérification de la reprise à la normale des activités.

NOS DOMAINES D'EXPERTISE



contact_S3@serma.com
www.serma-safety-security.com

www.serma.com