Guide de la cybersécurité

pour décideurs d'entreprise et

cadres dirigeants

Contactez-nous dès maintenant et
obtenez une démonstration gratuite !

SPIE

Les 10 cybermenaces les plus courantes

Menaces persistantes avancées (APT): les APT sont des attaques ciblées et sophistiquées souvent associées à des États-nations ou à des groupes cybercriminels organisés. Elles visent à passer inaperçues pendant de longues périodes tout en dérobant des données sensibles.

Violations de données: les violations de données impliquent un accès non autorisé à des données sensibles, ce qui peut entraîner le vol de données, des pertes financières et une atteinte à la réputation.

Ingénierie sociale: les attaques d'ingénierie sociale manipulent les individus pour qu'ils divulguent des informations confidentielles. Elles peuvent prendre différentes formes, telles que le pretexting, le baiting ou le tailgating.

Ransomware: les rançongiciels cryptent les données d'une organisation et exigent une rançon pour les décrypter. Il peut perturber les opérations et entraîner des pertes financières.

Vulnérabilités de type "jour zéro": il s'agit de vulnérabilités logicielles inconnues du fournisseur et qui peuvent être exploitées par des attaquants. Les attaques de type "jour zéro" peuvent être très préjudiciables.

Logiciels malveillants (par exemple, les virus, les rançongiciels, les chevaux de Troie): les malwares sont des logiciels malveillants conçus pour infiltrer ou endommager les systèmes informatiques. Ils peuvent entraîner des violations de données, des pertes financières et des interruptions de système.

Attaques par hameçonnage: le phishing est une tactique par laquelle les cybercriminels utilisent des courriels ou des messages trompeurs pour inciter les individus à révéler des informations sensibles, telles que des identifiants de connexion ou des données financières.

Vulnérabilités de l'IoT: alors que de plus en plus d'appareils sont interconnectés, les vulnérabilités des appareils de l'internet des objets (IoT) peuvent être exploitées pour obtenir un accès non autorisé aux réseaux.

Attaques par déni de service distribué (DDoS): les attaques DDoS submergent les services en ligne ou le site Web d'une entreprise, provoquant des perturbations et pouvant entraîner des temps d'arrêt et des pertes financières.

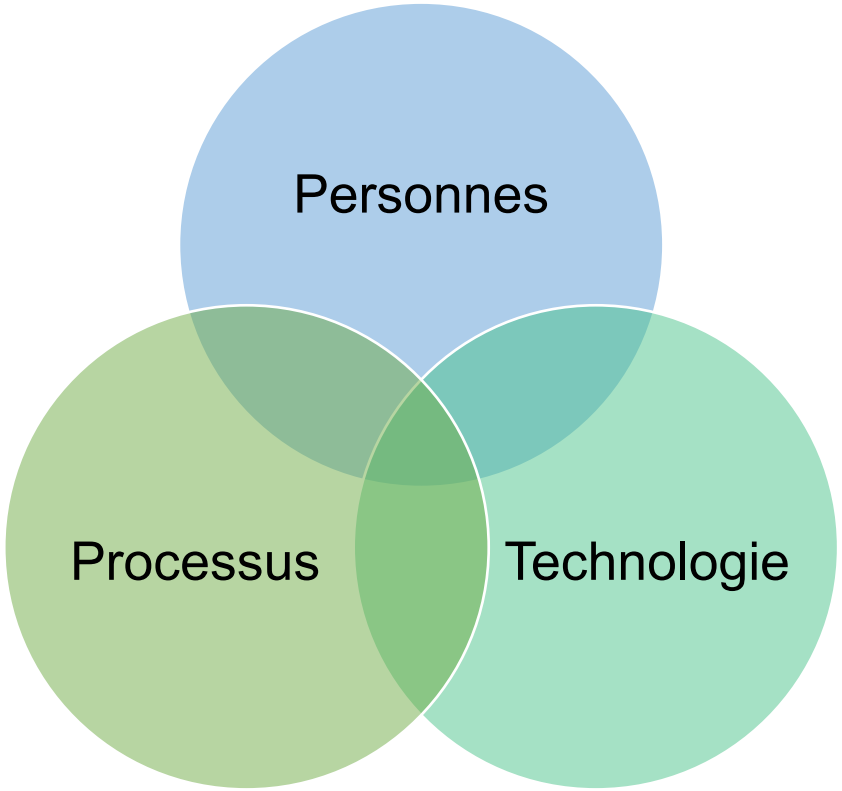
Menaces d'initiés: les menaces d'initiés proviennent d'employés actuels ou anciens, de sous-traitants ou de partenaires qui abusent de leurs privilèges d'accès pour voler des données ou nuire à l'organisation.

Contactez-nous dès maintenant et obtenez une démonstration gratuite !

SPIE

Les 3 défenseurs clés

L'approche People, Process, Technology de SPIE ICS reconnaît que la cybersécurité n'est pas seulement un défi technologique; c'est un **effort holistique** qui implique des individus, des processus bien définis et des technologies appropriées travaillant ensemble. Pour se protéger efficacement contre les cybermenaces, **les organisations doivent continuellement prendre en compte ces trois composantes** et s'adapter à l'évolution du paysage des menaces.



Contactez-nous dès maintenant et obtenez une démonstration gratuite !

SPIE ICS : Votre one-stop-shop en matière de cybersécurité

IMPLEMENTATION

Project Management

Installation, Configuration

Migration

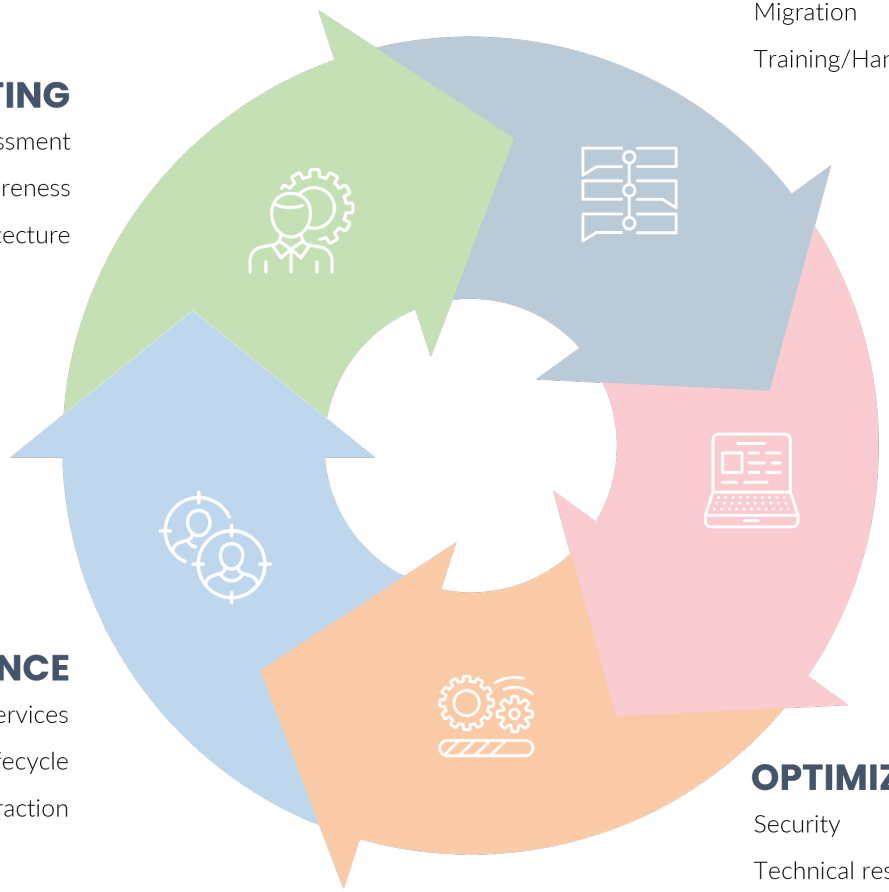
Training/Handover

CONSULTING

Cybersecurity Assessment

User Awareness

Security Strategy & Architecture



OPERATION

Managed Service

Incident Management

Proactive/reactive maintenance

Training/Handover

CUSTOMER EXPERIENCE

Adoption services

HW/SW lifecycle

Value extraction

OPTIMIZATION

Security

Technical resources

Sustainability

Contactez-nous dès maintenant et
obtenez une démonstration gratuite !

Vos 8 avantages

Réduction des coûts: si l'investissement dans des mesures de cybersécurité engendre des coûts, une approche holistique permet d'optimiser ces investissements. À long terme, vous allouerez les ressources plus efficacement et vous ferez des économies.

Gestion simplifiée: le fait de traiter avec SPIE ICS en tant que fournisseur unique de services rationalise la gestion de votre infrastructure de cybersécurité. Vous disposez d'un point de contact unique pour tous vos besoins en cybersécurité, ce qui simplifie la communication et le dépannage.

Protection de la réputation: une faille de sécurité nuit à votre réputation et érode la confiance des clients. Les dirigeants qui adoptent une approche holistique de la cybersécurité sont mieux préparés à prévenir les incidents et à réagir rapidement lorsqu'ils se produisent, minimisant ainsi les atteintes à la réputation.

Résilience à long terme: notre stratégie holistique de cybersécurité est axée sur la résilience à long terme plutôt que sur les solutions à court terme. Vous prenez des décisions éclairées qui renforcent la capacité de votre organisation à résister à l'évolution des cybermenaces.

Avantage concurrentiel: les organisations qui accordent la priorité à la cybersécurité avec SPIE ICS utilisent leur engagement en matière de sécurité comme un facteur de différenciation concurrentielle. Les clients et les partenaires choisissent de faire des affaires avec des organisations qui s'engagent fermement à protéger les données et la vie privée.

Soutien à l'innovation: une base de cybersécurité solide alimentée par SPIE ICS permet de sécuriser les efforts d'innovation et de transformation numérique. Vous explorez en toute confiance de nouvelles technologies et de nouveaux modèles commerciaux tout en maintenant la sécurité.

Confiance du conseil d'administration et des parties prenantes: les dirigeants qui adoptent une approche holistique de la cybersécurité avec SPIE ICS inspirent confiance au conseil d'administration, aux investisseurs et aux autres parties prenantes. Cela a un impact positif sur la gouvernance globale de l'organisation.

Sécurité de la chaîne d'approvisionnement: une approche holistique s'étend aux fournisseurs et partenaires tiers. SPIE ICS s'assure que votre chaîne d'approvisionnement respecte les normes de sécurité, minimisant ainsi les vulnérabilités provenant de connexions externes.

Contactez-nous dès maintenant et
obtenez une démonstration gratuite !

SPIE