Solutions et services complets de cybersécurité

SPIE ICS SA

SPIE ICS SA
Rue de l'Industrie 58a
1030 Bussigny

T : +41 58 301 11 11

www.spie.ch

Novembre 2023

Introduction

Dans un contexte dans lequel les cybermenaces sont de plus en plus sophistiquées, omniprésentes et en constante évolution, les entreprises suisses doivent adopter une approche globale en termes de cybersécurité. Une méthode holistique de cybersécurité implique d'aborder la sécurité sous tous les angles et de considérer tous les aspects des opérations d'une organisation. C'est pourquoi SPIE ICS Suisse a développé une approche globale qui prend en compte les trois principaux aspects de la résilience en matière de cybersécurité - une combinaison de la responsabilisation des personnes, de la mise en œuvre des processus et de la technologie de pointe.

SPIE ICS Suisse offre un portefeuille solide de services et de solutions de cybersécurité conçus pour protéger votre infrastructure informatique, sauvegarder les données sensibles et maintenir l'intégrité de vos opérations. Ce document donne un aperçu de nos offres de cybersécurité, de nos méthodologies et de nos partenariats qui vous permettent de construire une posture de cybersécurité résiliente.

Harmoniser les personnes, les processus et la technologie: la triade de SPIE en matière de cybersécurité

SPIE ICS Suisse s'engage à fournir des services de cybersécurité de haut niveau, adaptés aux besoins uniques de chaque organisation. Nos partenariats et alliances nous permettent d'adopter une approche indépendante des fournisseurs, afin que SPIE ICS puisse toujours adapter ses produits et services aux besoins spécifiques de ses clients. Les sections suivantes permettent de comprendre notre approche et abordent l'ensemble des bénéfices de cette méthode. Dans le chapitre « Radar de Solutions», nous vous donnons un aperçu de notre portefeuille de services qui s'étend de l'évaluation des risques aux solutions de sécurité avancées, assurant ainsi une protection complète de votre paysage numérique.

Trouver le bon équilibre entre expertise humaine, flux de travail rationalisés et technologie de pointe avec SPIE

La cybersécurité n'est pas qu'une question de technologie. Il s'agit d'une démarche globale qui fait travailler en harmonie les personnes, les processus et la technologie. En abordant ces trois aspects avec la même attention et la même rigueur, SPIE garantit une posture de cybersécurité résiliente, adaptable et prête pour l'avenir. Pour les

organisations, cela se traduit par une tranquillité d'esprit, une confiance dans l'infrastructure et une base pour une croissance durable.

People

L'humain, la première ligne de défense: quel que soit le degré d'avancement d'une technologie, l'erreur humaine reste une vulnérabilité critique dans toute organisation. En mettant l'accent sur la formation et la sensibilisation, SPIE s'assure que tous les employés comprennent les menaces et sont équipés pour agir en tant que première ligne de défense de l'organisation.

Contrôles d'accès basés sur les rôles: tout le monde n'a pas besoin d'accéder à toutes les informations. SPIE met l'accent sur le principe du moindre privilège, en veillant à ce que les individus bénéficient uniquement de l'accès dont ils ont besoin, ce qui réduit les points de fuite potentiels des données.

Formation continue: le paysage de la cybersécurité est en constante évolution. Des sessions de formation régulières permettent de s'assurer que le personnel est toujours au courant des dernières menaces et des meilleures pratiques.

Process

Dans l'environnement dynamique des menaces d'aujourd'hui, les processus de sécurité statiques sont un handicap. Les protocoles de sécurité adaptatifs de SPIE évoluent en fonction des derniers renseignements sur les menaces.

Plan de réponse aux incidents: un processus bien défini d'identification, de réponse et d'apprentissage des incidents de sécurité permet d'atténuer rapidement les menaces et de réduire les temps d'arrêt.

Audits réguliers: des examens et des audits systématiques garantissent que les mesures de sécurité fonctionnent comme prévu et mettent en évidence les points à améliorer.

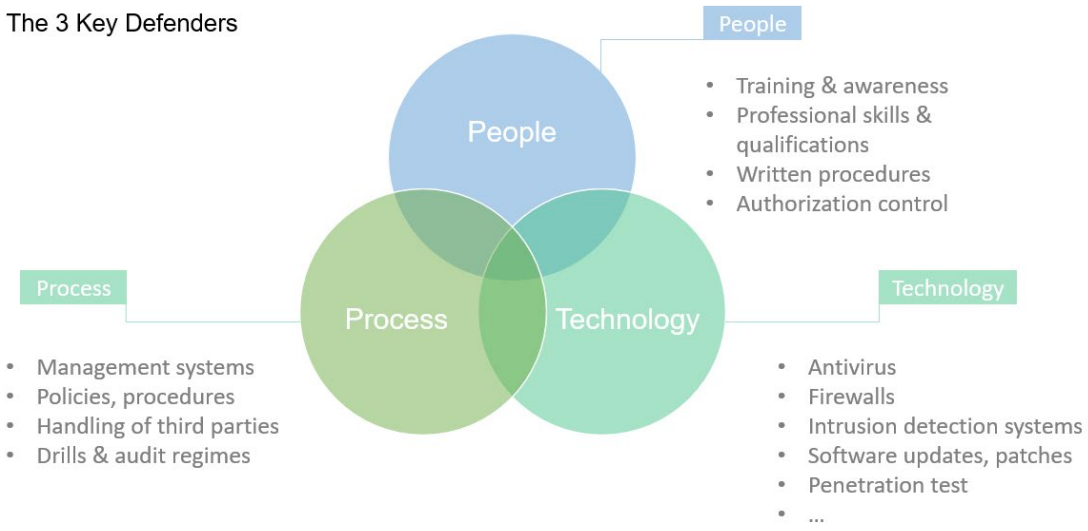
Technology

SPIE s'appuie sur des technologies de pointe pour détecter les anomalies et les menaces potentielles, souvent en temps réel, ce qui garantit des temps de réponse rapides.

Infrastructure sécurisée: de la sécurité des points de terminaison aux architectures réseau sécurisées, SPIE accorde la priorité aux investissements dans les technologies qui forment une défense multicouche contre les cybermenaces.

Intégration de l'intelligence artificielle et de l'apprentissage automatique: ces technologies permettent de prédire, d'identifier et d'atténuer les menaces d'une manière

qui était auparavant impossible. En intégrant l'intelligence artificielle et l'apprentissage automatique, SPIE garde une longueur d'avance sur les cyberadversaires.



Par essence, l'adoption d'une approche globale de la cybersécurité en intégrant les personnes, les processus et la technologie ne protège pas seulement l'organisation contre les menaces immédiates, mais la prépare également à un succès durable à long terme. C'est un investissement dans le présent et l'avenir.

Les piliers d'une transformation numérique sécurisée: Vos principaux avantages

Confiance numérique (Digital Trust)

La confiance numérique ou Digital Trust est la base sur laquelle les entreprises modernes prospèrent et est devenue essentielle.

Cultiver le Digital Trust se traduit par une réputation de marque consolidée, permettant aux entreprises d'être reconnues comme des partenaires fiables dans le paysage numérique. Une présence numérique digne de confiance favorise une loyauté profondément enracinée, ce qui incite les clients non seulement à revenir, mais aussi à défendre la marque. Posséder une réputation de confiance numérique solide peut permettre à une organisation de se démarquer et de bénéficier d'un avantage concurrentiel unique.

En tant que titulaire des certifications ISO 27001, 9001 et 14001, SPIE ICS est votre partenaire de confiance pour soutenir votre activité et vous aider à prospérer.

Conformité

Dans un monde où les réglementations évoluent sans cesse, la conformité n'est pas seulement une exigence - c'est un atout stratégique.

La conformité assure la continuité des activités, évitant les interventions réglementaires ou les arrêts imprévus, et élimine le risque d'encourir des pénalités financières punitives. La conformité renforce également l'engagement d'une marque à l'égard de l'intégrité, en améliorant sa perception par le public et la confiance des parties prenantes.

SPIE ICS peut vous accompagner dans votre démarche de mise en conformité, qu'il s'agisse de faire appel à des consultants ISMS, des services de sécurité gérés ou des solutions s'appuyant sur les technologies de sécurité les plus récentes.

Disponibilité des compétences

L'expertise d'une équipe est l'élément vital d'une organisation.

En encourageant la formation des équipes, les organisations réduisent considérablement les risques découlant d'erreurs humaines involontaires. En outre, comme les cybermenaces se diversifient, une équipe qualifiée permet à l'organisation de rester agile et de mettre à jour ses défenses en fonction des besoins.

SPIE ICS, avec ses nombreux ingénieurs hautement qualifiés et certifiés, peut aider votre organisation et vos équipes à atteindre leurs objectifs.

Cyber-résilience

Face aux cybermenaces toujours plus nombreuses, la résilience est l'armure qui protège la continuité de l'activité. Les infrastructures résilientes garantissent que les entreprises restent opérationnelles, même lorsque les cybermenaces se font insistantes.

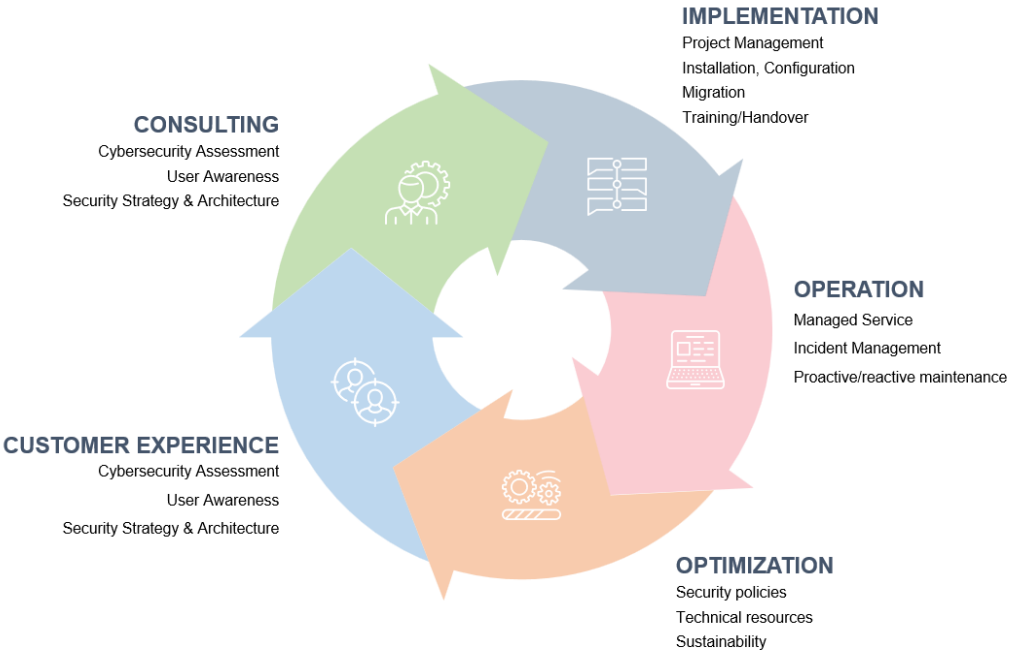
La résilience ne consiste pas seulement à faire face à une tempête, mais aussi à s'en remettre rapidement, en garantissant un temps d'arrêt opérationnel minimal. Une posture résiliente permet d'éviter les failles qui peuvent entraîner des pertes financières directes ou des pertes indirectes liées à l'atteinte à la réputation. Une organisation résiliente respire la confiance, assurant toutes les parties prenantes de sa capacité à résister aux cyber-attaques.

Grâce à son personnel, ses processus et sa technologie, SPIE ICS est le partenaire de choix pour accroître votre résilience et vous aider à prospérer, même lorsque les temps sont difficiles.

Pourquoi SPIE?

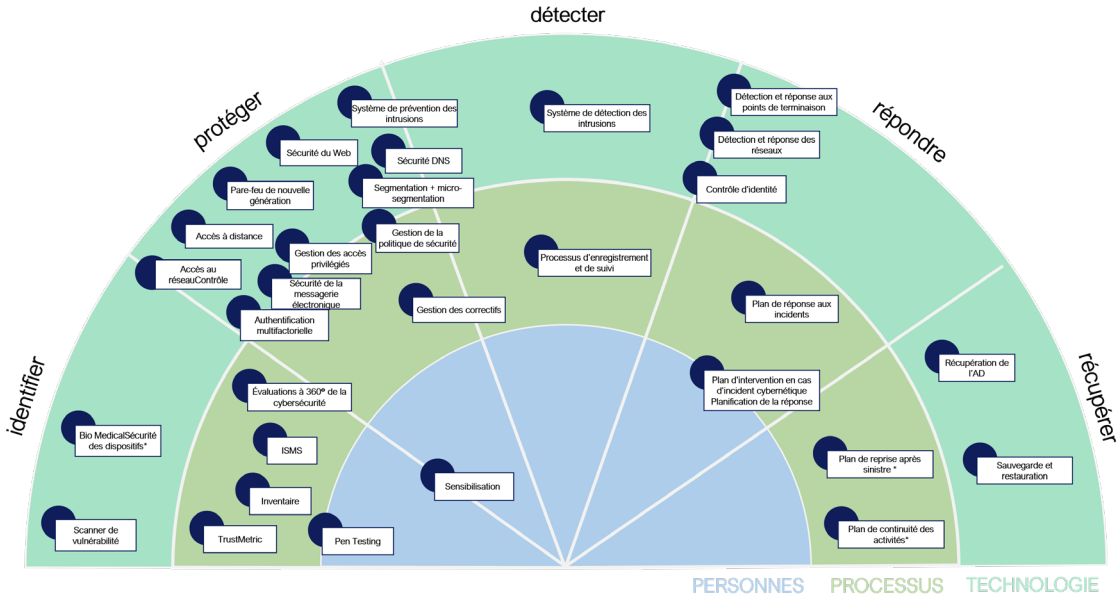
Conscients de l'évolution constante du paysage numérique, nous sommes fiers de définir les piliers uniques qui font de SPIE le partenaire optimal de votre parcours technologique; voici les éléments qui nous distinguent sur le marché.

- **Excellence du service:** nous nous faisons un point d'honneur d'offrir des services de premier ordre, en veillant à ce que chaque engagement réponde aux normes de qualité les plus élevées.
- **Ingénieurs experts:** notre équipe n'est pas seulement compétente, elle est aussi la meilleure dans son domaine. Avec SPIE, vous vous associez à des experts chevronnés qui se consacrent à la fourniture de solutions techniques inégalées.
- **Polyvalence dans tous les domaines:** notre présence dans de nombreux secteurs témoigne de notre flexibilité et de notre capacité à répondre à des besoins variés, en apportant une richesse de connaissances intersectorielles.
- **Solidité financière:** en tant que membre d'un grand groupe financièrement stable, SPIE garantit la fiabilité et la longévité de tous ses partenariats. Vous pouvez compter sur notre présence et notre engagement durables.
- **Réactivité inégalée:** nous nous distinguons de nos plus grands concurrents par notre rapidité d'intervention. Avec six points de présence en Suisse, nous garantissons une intervention sur site en moins de deux heures.
- **Assistance 24 heures sur 24:** notre dévouement à votre égard ne s'arrête jamais. Avec une assistance 24 heures/24, tous les jours de la semaine, nous sommes toujours là quand vous avez besoin de nous.
- **Expertise de niche:** en plus de notre large éventail de services, nous possédons une expertise spécialisée dans certaines solutions, ce qui vous garantit le meilleur dans ces domaines.
- **Des solutions sur mesure:** chez SPIE, il n'y a pas de solution unique. Nous évaluons avec diligence votre environnement et fournissons des solutions qui répondent au mieux à vos besoins spécifiques.
- **Neutralité vis-à-vis des fabricants:** SPIE ICS Switzerland propose des solutions ICT neutres vis-à-vis des fabricants. Nous adaptons les solutions technologiques à vos besoins spécifiques. Nos services englobent la planification, la mise en œuvre, la maintenance et la productivité, le tout fondé sur une approche axée sur la sécurité.
- **Expérience client:** nous combinons des informations analysées, des technologies innovantes et une interaction humaine empathique pour dépasser vos attentes et établir des partenariats durables fondés sur la confiance.


IMPLEMENTATION
Project Management
Installation, Configuration
Migration
Training/Handover
OPERATION
Managed Service
Incident Management
Proactive/reactive maintenance
OPTIMIZATION
Security policies
Technical resources
Sustainability
CUSTOMER EXPERIENCE
Cybersecurity Assessment
User Awareness
Security Strategy & Architecture
CONSULTING
Cybersecurity Assessment
User Awareness
Security Strategy & Architecture

Notre radar de solutions

Notre radar de solutions a été développé pour permettre aux entreprises d'employer une approche multiple pour protéger leurs actifs numériques et leur réputation. Ce chapitre examine les composantes d'une stratégie globale de cybersécurité. De la compréhension et de l'évaluation des menaces potentielles grâce à l'évaluation des risques de cybersécurité au renforcement des défenses à l'aide de solutions modernes telles que les pares-feux de nouvelle génération et les EDR. Nous explorons l'importance de la sensibilisation des utilisateurs dans le développement de la cyber-résilience, la criticité des contrôles d'accès sécurisés et le rôle central de la supervision d'experts sous la forme de CISO-as-a-Service. Chaque sujet abordé ici ne présente pas seulement une facette individuelle de la sécurité, mais fait partie intégrante du puzzle global qui garantit un paysage numérique fortifié et réactif fourni par SPIE ICS. Rejoignez-nous pour parcourir ces éléments essentiels et jeter les bases d'un avenir numérique sûr.



* En cours de développement

Évaluation des risques de cybersécurité: **évaluation complète des menaces**

Comprendre les menaces de cybersécurité et y répondre de manière préventive n'est pas seulement une nécessité, c'est un impératif pour l'entreprise. C'est pourquoi SPIE présente son service d'évaluation de la cybersécurité à 360°.

L'approche de SPIE ne consiste pas seulement à identifier les vulnérabilités individuelles, mais à comprendre la situation dans son ensemble. Nous évaluons les menaces internes et externes, en veillant à ce que tous les points d'entrée potentiels

soient examinés de près. Dans le cadre d'une évaluation des risques à 360°, SPIE évalue la maturité de votre cybersécurité, identifie les risques et fournit des recommandations exploitables. SPIE ICS Switzerland suit les normes internationales telles que ISO/IEC 27001, CIS Controls, NIST SP-800 et Swiss IKT pour garantir des évaluations complètes de la cybersécurité.

Grâce à une évaluation de la cybersécurité à 360°, vous pourrez:

- obtenir des informations sur la maturité de votre gouvernance et de vos processus. Grâce à des entretiens et à des vérifications rapides, nous confirmerons que votre cybersécurité est mise en œuvre conformément aux meilleures pratiques et aux normes.
- vérifier l'état de la sécurité de votre infrastructure technologique sur site et dans le cloud. Grâce à des tests et des vérifications complets, nous nous assurons que les contrôles sont efficaces.
- évaluer la sensibilisation de vos employés et proposer des formations.
- connaître votre niveau de risque en matière de cybersécurité avec une liste d'actions concrètes pour réduire le risque de manière efficace et efficiente.

Les résultats peuvent recommander des actions supplémentaires dans le domaine des processus de journalisation et de surveillance, de la gestion des correctifs ou de la gestion de l'inventaire. Ces domaines peuvent être traités séparément ou dans le cadre de l'audit.

SPIE peut également vous aider à concevoir un plan de réponse aux incidents, un plan de reprise après sinistre et un plan de continuité des activités, tant au niveau des processus que des outils.

En résumé, 'la fonction « Évaluation des risques de cybersécurité de SPIE: évaluation complète des menaces» de SPIE est plus qu'une simple évaluation - c'est un outil stratégique qui permet aux organisations de comprendre, de prévoir et de traiter efficacement le paysage des menaces à multiples facettes. Avec SPIE comme partenaire, vous ne protégez pas seulement votre présent, mais vous fortifiez votre avenir.

Pentesting: évaluer votre posture de sécurité

Les tests d'intrusion, souvent appelés « pentesting », constituent un moyen efficace de mesurer l'état de préparation d'une organisation en matière de cyberdéfense. Grâce à l'offre spécialisée de SPIE dans ce domaine, les organisations peuvent obtenir une évaluation objective de leurs mesures de sécurité dans des scénarios réels.

Le pentesting est un processus systématique et contrôlé d'évaluation de la sécurité d'un système informatique, d'un réseau ou d'une application par la simulation d'attaques. L'équipe de hackers éthiques et de professionnels de la cybersécurité de SPIE utilise des techniques sophistiquées pour simuler des cyberattaques réelles, garantissant ainsi une évaluation complète de vos mécanismes de défense. Au-delà des vulnérabilités de surface, notre équipe explore en profondeur vos systèmes, découvrant les faiblesses cachées qui pourraient être exploitées dans des attaques à plusieurs niveaux. Notre objectif est de trouver des points d'entrée potentiels que des acteurs malveillants pourraient utiliser pour obtenir un accès non autorisé ou compromettre des informations sensibles. Dans ce contexte, SPIE fournit une feuille de route claire pour améliorer votre posture de sécurité, vous assurant de prendre des mesures rapides et efficaces. Grâce à une série de tests contrôlés, le pentesting aide les organisations à identifier et à combler les lacunes en matière de sécurité, à améliorer leur position globale en matière de cybersécurité et à se protéger contre les cybermenaces potentielles.

En conclusion, le service Pentesting de SPIE offre aux organisations une vision critique à travers laquelle elles peuvent voir et améliorer leurs mesures de cybersécurité. Avec SPIE, vous ne vous contentez pas d'identifier les vulnérabilités, vous les transformez en forces.

SPIE ICS Suisse propose différents types de tests de pénétration. Pour plus d'informations, veuillez contacter info.ch@spie.com

Sensibilisation à la sécurité en tant que service: renforcer la cyber-résilience

Les défenses technologiques sont indéniablement vitales. Cependant, un aspect souvent négligé est le comportement humain qui, sans une sensibilisation adéquate, peut devenir par inadvertance un maillon faible de la chaîne de sécurité. Consciente de cette dimension critique, SPIE présente son programme Security awareness as a

service, une initiative complète visant à cultiver une culture organisationnelle soucieuse de la cybersécurité.

En fonction de vos besoins, nous proposons des contenus sur mesure en e-formation, et des formations sur site sur des sujets spécifiques. Cela permet d'établir les bases théoriques de la résilience souhaitée. Notre programme est complété par des simulations d'attaques de phishing ciblées et actualisées. La sensibilisation à la sécurité est encore renforcée par nos mesures d'accompagnement, qui permettent des rappels constants sans effort supplémentaire de la part de vos employés. Au-delà de l'apprentissage individuel, le programme de SPIE se concentre sur la promotion d'une conscience collective de la cybersécurité, transformant l'ensemble de la culture organisationnelle en une culture de vigilance et de résilience.

L'offre Security awareness as a service de SPIE n'est pas un simple programme de formation, c'est un changement de mentalité. En inculquant une connaissance et une compréhension approfondies des cybermenaces à tous les niveaux de l'organisation, SPIE s'assure que chaque individu devient un défenseur proactif, contribuant collectivement à une posture de sécurité améliorée. Ensemble, nous créons la première et la plus importante ligne de défense contre les cyberattaques: le pare-feu humain.

TrustMetric: mesurer et améliorer la maturité cybernétique

Dans notre environnement numérique en réseau, la confiance dans l'intégrité et la sécurité de nos systèmes est d'une importance capitale. TrustMetric est un service innovant d'évaluation des risques qui fournit des informations précises sur l'écosystème complexe de la confiance et de la sécurité dans la cybersphère. Notre service permet de mesurer et d'améliorer continuellement la maturité cybernétique, d'identifier les vulnérabilités potentielles et de fournir des recommandations ciblées pour l'amélioration. Avec TrustMetric, vous identifiez non seulement les vulnérabilités de manière proactive, mais vous priorisez également les mesures de sécurité et vous comparez automatiquement votre maturité cybernétique aux normes de l'industrie. Ce service offre les avantages suivants:

- **Des informations précises:** naviguez dans les réseaux complexes du monde numérique avec des informations claires et précises, révélant les nuances de la confiance et de la sécurité dans votre cyberenvironnement.
- **Évaluation dynamique de la maturité cybernétique:** au-delà des évaluations statiques, TrustMetric facilite la mesure et l'amélioration continues de la maturité cybernétique de votre organisation, en s'adaptant à l'évolution du paysage numérique.
- **Plans d'action prioritaires:** dans le vaste domaine de la cybersécurité, toutes les menaces potentielles ne peuvent pas être traitées simultanément. TrustMetric aide à établir des priorités, ce qui vous permet d'allouer des ressources là où elles auront le plus d'impact.

- **Comparaison avec les meilleurs:** juxtaposez automatiquement votre niveau de maturité cybernétique avec les références de l'industrie, ce qui vous permet de vous positionner plus justement dans le contexte plus large de l'industrie.

Avec TrustMetric à vos côtés, vous ne vous contentez pas de réagir aux défis du monde numérique, mais vous renforcez proactivement vos cyberdéfenses. Découvrez le prochain niveau de maturité en matière de cybersécurité avec TrustMetric de SPIE.

CISOaaS: construire votre stratégie de sécurité

Principales caractéristiques de CISOaaS by SPIE

- **L'expertise au bout des doigts:** tirez parti des connaissances et de l'expérience de professionnels de la sécurité chevronnés qui ont été à l'avant-garde de la stratégie et de l'exécution en matière de cybersécurité.
- **Des solutions évolutives:** que vous soyez une startup en pleine croissance ou une entreprise bien établie, notre CISOaaS s'adapte à vos besoins, vous garantissant des informations et des conseils sur mesure.
- **Rentabilité:** évitez les dépenses liées à l'embauche d'un cadre à temps plein tout en bénéficiant d'une expertise de classe mondiale. Optez pour le niveau d'engagement qui correspond à votre budget et à vos besoins.
- **Supervision holistique de la sécurité:** de l'évaluation des risques à la formulation de la politique de sécurité, de la planification de la réponse aux incidents à la conformité réglementaire, nos professionnels CISO fournissent une vue d'ensemble de votre paysage de cybersécurité.
- **Intégration transparente:** nos experts s'intègrent facilement à vos équipes existantes, apportant une approche collaborative pour renforcer la posture de sécurité de votre organisation.
- **Restez à jour:** avec le CISOaaS de SPIE, vous avez toujours une longueur d'avance. Vous bénéficiez de mises à jour permanentes sur les menaces émergentes, les meilleures pratiques les plus récentes et les mandats réglementaires en constante évolution.
- **Confidentialité et confiance:** soyez assuré que notre engagement privilégie la confidentialité. Faites confiance aux antécédents irréprochables de SPIE en matière de traitement des informations sensibles avec la plus grande intégrité.

Cette offre fusionne le meilleur des deux mondes - une expertise de classe mondiale sans les frais généraux - rendant le leadership en matière de cybersécurité accessible aux organisations de toutes tailles et de tous secteurs.

Gestion des vulnérabilités: prendre en compte le cycle de vie des actifs

La gestion des vulnérabilités est un processus systématique utilisé en cybersécurité pour identifier, évaluer, hiérarchiser et atténuer les faiblesses de sécurité des systèmes informatiques et des logiciels. Ses principaux objectifs consistent à réduire le risque de failles de sécurité en s'attaquant de manière proactive aux vulnérabilités connues. Les principales étapes de la gestion des vulnérabilités sont l'identification, l'évaluation, la hiérarchisation, la remédiation, la vérification, l'établissement de rapports et la surveillance continue. Elle implique également la gestion des correctifs, la sensibilisation à la sécurité et la conformité aux réglementations. Ce processus aide les organisations à maintenir un environnement informatique sécurisé et à minimiser l'impact potentiel des incidents de sécurité.

SPIE peut vous aider à définir votre processus de gestion des vulnérabilités et à suivre les activités correspondantes avec les outils adéquats.

Contrôle d'accès au réseau: garantir un accès autorisé

Les réseaux numériques devenant de plus en plus complexes, il est primordial d'en protéger les limites. Le « contrôle d'accès au réseau » de SPIE joue le rôle de gardien vigilant. Le contrôle d'accès au réseau (NAC) est une approche de la sécurité qui garantit que seuls les appareils et les utilisateurs autorisés et conformes peuvent accéder à un réseau. En appliquant des politiques et des protocoles, le contrôle d'accès au réseau protège contre les accès non autorisés, améliore la visibilité du réseau et réduit les risques de sécurité. Il implique des processus tels que l'authentification des appareils, l'identification des utilisateurs et l'évaluation des terminaux pour garantir que seules les entités de confiance peuvent se connecter au réseau, empêchant ainsi les menaces et les vulnérabilités potentielles de compromettre l'intégrité du réseau et la sécurité des données.

Faites confiance à SPIE pour maintenir le caractère sacré de votre réseau, en protégeant vos données et vos ressources contre les intrusions injustifiées.

Authentification multifactorielle: renforcer l'authentification des utilisateurs

Face à l'évolution des cybermenaces, les simples protections par mot de passe ne suffisent plus. L'offre « Multi-factor Authentication (MFA) » de SPIE est votre ligne de défense avancée. L'authentification multifactorielle renforce considérablement la sécurité en ajoutant une couche supplémentaire de protection au-delà du simple mot de passe, ce qui rend plus difficile l'accès des utilisateurs non autorisés aux informations et systèmes sensibles, même s'ils connaissent le mot de passe. Qu'il s'agisse de biométrie, de jetons de sécurité ou de codes SMS, SPIE propose une série d'outils d'authentification adaptés aux besoins uniques de chaque organisation. Ces facteurs se

répartissent généralement en trois catégories: une information connue (comme un mot de passe ou un code PIN), un appareil que vous détenez (comme un smartphone ou une carte à puce) et un élément d'identité (des données biométriques comme les empreintes digitales ou la reconnaissance faciale).

Avant tout, SPIE ICS garantit une expérience utilisateur transparente. Tout en renforçant la sécurité, SPIE s'assure que le processus d'authentification reste convivial, avec un accès rapide.

Faites confiance à SPIE pour améliorer la sécurité d'accès de votre organisation, en trouvant le bon équilibre entre une protection robuste et le confort de l'utilisateur.

Sécurité du DNS: sauvegarder l'intégrité des domaines

Dans la vaste étendue numérique, le système de noms de domaine (DNS) joue un rôle crucial en dirigeant le trafic et en assurant une connectivité sans faille. La sécurisation du système de noms de domaine (DNS) est essentielle, car il peut être exploité par des attaquants pour perturber les services, rediriger les utilisateurs vers des sites Web malveillants ou compromettre l'intégrité des données. L'offre « DNS Security » de SPIE protège ce composant fondamental.

Filtrage DNS et contrôle de contenu

Les solutions filtrent les contenus malveillants ou indésirables, tels que les logiciels malveillants, les sites d'hameçonnage et les serveurs de commande et de contrôle de réseaux de zombies. Elles empêchent les utilisateurs d'accéder à des sites Web nuisibles en bloquant la résolution DNS pour les domaines malveillants.

Pare-feu DNS

Les solutions de pare-feu DNS inspectent le trafic DNS à la recherche de signes d'activité malveillante, notamment de noms de domaine et d'adresses IP suspects. Elles peuvent bloquer l'accès à des sites malveillants connus et générer des alertes en vue d'une enquête plus approfondie.

Intégration des renseignements sur les menaces

Les solutions de sécurité DNS intègrent des flux de renseignements sur les menaces pour toujours garder un œil sur les menaces émergentes et les domaines malveillants, ce qui facilite l'identification et le blocage en temps réel des sites malveillants. Notre partenaire pour la sécurité DNS est Cisco, qui propose une suite Umbrella complète.

Avec SPIE, assurez-vous que votre domaine continue à vous guider en toute confiance dans le monde numérique, à l'abri des perturbations et des vulnérabilités.

Segmentation et micro-segmentation: limiter les surfaces d'attaque

Dans le réseau complexe des réseaux modernes, les frontières sont essentielles. La segmentation des réseaux renforce la sécurité en contrôlant et en isolant les flux de trafic, en réduisant l'impact des incidents de sécurité et en minimisant les surfaces d'attaque. L'offre « Segmentation and Micro-segmentation » de SPIE affine ces limites jusqu'à une clarté quasi parfaite.

Les techniques utilisées sont les réseaux locaux virtuels (VLAN), le sous-réseau, les pares-feux, les routeurs et les listes de contrôle d'accès (ACL). SPIE est spécialisée dans la micro-segmentation, particulièrement utile pour sécuriser les applications modernes et distribuées dans les centres de données ou les environnements cloud, où la sécurité traditionnelle basée sur le périmètre est moins efficace. La micro-segmentation s'appuie souvent sur des solutions de réseaux définis par logiciel (SDN) ou des appareils de sécurité réseau.

Équipez votre organisation de l'expertise de SPIE et transformez votre réseau étendu en un labyrinthe où l'accès illicite n'est pas seulement difficile, mais presque impossible.

Surveillance de l'identité: contrôler l'identification des utilisateurs

À l'ère de l'interconnexion numérique, la protection des identités individuelles est cruciale pour assurer la sécurité globale de l'organisation. L'offre « Identity Monitoring » de SPIE est votre bouclier complet.

La surveillance des identités consiste à suivre et à gérer activement les identités des utilisateurs et les droits d'accès qui leur sont associés au sein de l'environnement informatique d'une organisation. Le contrôle et l'analyse continus des activités des utilisateurs, des autorisations et des mécanismes d'authentification sont essentiels pour la sécurité et la conformité. Les principales fonctionnalités comprennent la gestion des comptes utilisateurs, le contrôle d'accès, l'authentification, l'audit et la journalisation, la détection des anomalies, les rapports de conformité, la gestion des mots de passe, l'authentification unique (SSO) et la fédération d'identités.

Avec SPIE à la barre, installez une culture de la sécurité qui s'articule autour de l'utilisateur, en veillant à ce que l'identité numérique de chacun reste intacte et digne de confiance. SPIE se concentre sur la gestion des accès privilégiés en collaboration avec ses partenaires Wallix et Fortinet.

Détection et réponse des points de terminaison: garantir la sécurité des points d'accès

Dans un monde où les réseaux numériques sont de plus en plus étendus, les points d'accès individuels - des ordinateurs portables aux appareils mobiles - deviennent souvent les maillons les plus faibles. La solution Endpoint Detection and Response (EDR/XDR) de SPIE renforce ces points critiques:

- **Chasse proactive aux menaces**
- **Analyse en temps réel**
- **Réponse automatisée**
- **Approche globale**

L'EDR/XDR de SPIE recherche en permanence et en temps réel les signes de compromission. Nos solutions détectent, étudient et répondent aux menaces avancées et aux incidents de sécurité au niveau des points de terminaison. Elles surveillent en permanence les activités, collectent et analysent les données des points de terminaison, fournissent des détails sur l'investigation des incidents, soutiennent les actions de réponse, offrent une visibilité sur les points de terminaison, permettent la chasse aux menaces, facilitent l'analyse médico-légale et s'intègrent à d'autres solutions de sécurité.

SPIE s'associe à Cynet, Fortinet et d'autres pour fournir des solutions EDR/XDR efficaces. En vous associant à SPIE, vous faites en sorte que chaque appareil de votre réseau devient une forteresse impénétrable.

Détection et réponse des réseaux (NDR): analyser le trafic réseau

Il est vital que chaque octet de données qui circule dans un réseau reste sécurisé et non compromis. Avec le service Network Detection and Response (NDR) de SPIE, vous disposez d'une sentinelle vigilante pour vos flux de données.

Les solutions et services NDR de SPIE surveillent le trafic réseau à la recherche d'activités malveillantes, d'anomalies et de menaces potentielles. Ils fournissent une visibilité sur le trafic réseau, offrent des capacités de chasse aux menaces, soutiennent les enquêtes sur les incidents, permettent des actions de réponse et assurent une visibilité complète sur le réseau de l'organisation.

Grâce à la solution NDR de SPIE, votre entreprise peut naviguer en toute confiance sur les mers numériques, assurée que chaque vague de données est surveillée, analysée et protégée. Les partenaires NDR privilégiés de SPIE sont Cisco avec Stealthwatch et Fortinet.

Récupération AD: restauration de l'intégrité d'Active Directory

La restauration d'Active Directory (AD) est cruciale pour les décideurs des organisations en raison de son rôle dans la garantie de la disponibilité et de l'intégrité des services critiques de gestion des identités et des accès. Après un incident de sécurité, Active Directory permet d'atténuer les dommages et de maintenir l'intégrité des objets AD. Il s'agit de restaurer les comptes d'utilisateurs, les stratégies de groupe, les paramètres de sécurité et d'autres informations liées au réseau. Les services et solutions de récupération AD de SPIE sont les suivants:

- **Restauration rapide:** en cas de corruption ou d'altération malveillante de votre Active Directory, la solution de SPIE assure une restauration rapide vers un état antérieur validé, minimisant ainsi les temps d'arrêt et les perturbations opérationnelles.
- **Fonctionnalités d'instantanés:** des instantanés périodiques de l'environnement AD sont pris, ce qui permet un retour à l'état souhaité en toute souplesse, garantissant l'exactitude des données et la cohérence opérationnelle.
- **Pistes d'audit:** l'enregistrement complet de toutes les modifications apportées à l'environnement AD vous permet de savoir clairement ce qui a été modifié, quand et par qui, ce qui facilite les enquêtes et la responsabilisation.
- **Surveillance proactive:** au-delà de la récupération, l'offre de SPIE surveille continuellement les signes de falsification d'AD ou les vulnérabilités potentielles, ce qui permet de prendre des mesures préventives avant qu'une crise ne se produise.

Choisissez SPIE comme partenaire de votre solution de restauration AD et contactez notre équipe d'experts via info.ch@spie.com

Sauvegarde et restauration: protéger la disponibilité et l'intégrité des données

Dans le paysage numérique d'aujourd'hui, les données ne sont pas seulement un actif, elles constituent le poumon de votre organisation. Assurer leur sauvegarde et leur récupération rapide en cas d'adversité est vital pour la continuité de l'activité, la conformité et la protection contre les diverses menaces. En outre, en cas de perte de données ou de défaillance du système, les logiciels de sauvegarde de sécurité minimisent les temps d'arrêt (Wang & Li, 2017). Les logiciels de sauvegarde de sécurité garantissent la confidentialité, l'intégrité et la disponibilité des données pendant la sauvegarde et le stockage.

C'est là que la solution de sauvegarde et de restauration de SPIE entre en jeu: SPIE fournit des sauvegardes chiffrées et redondantes de vos données essentielles, garantissant qu'elles sont non seulement stockées en toute sécurité, mais aussi protégées contre la corruption et les menaces externes. En cas de violation, SPIE assure la reprise rapide de vos activités. Adaptée à vos besoins, SPIE propose des solutions de stockage sur site et dans le cloud, garantissant que vos sauvegardes sont non seulement sécurisées, mais aussi accessibles et conformes aux politiques de votre organisation.

La société Rubrik est le partenaire privilégié de SPIE pour les sauvegardes sécurisées. Contactez-nous dès aujourd'hui, SPIE sera votre gardien numérique.

Sécurité du Web: protéger les ressources Web

À une époque où les entreprises évoluent et prospèrent en ligne, l'intégrité et la sécurité de vos ressources Web ne sont pas négociables. En tant que décideur, vous devez faire de la sécurité du Web l'une de vos priorités, en raison de son rôle critique dans la protection des données sensibles, le maintien de la confiance des clients et la protection contre les diverses cybermenaces.

La solution «Web Security» de SPIE est une sentinelle solide pour assurer votre présence numérique:

- **Détection des menaces en temps réel:** en s'appuyant sur des algorithmes avancés et des renseignements sur les menaces, SPIE recherche et neutralise en permanence les menaces ciblant vos ressources Web, garantissant ainsi des opérations en ligne ininterrompues.
- **Filtrage du contenu:** tenez à distance les contenus malveillants ou inappropriés. La solution de SPIE permet d'appliquer les politiques de l'entreprise et les exigences de conformité, garantissant ainsi un environnement Web sécurisé et professionnel.
- **Passerelles Web sécurisées:** avec SPIE, chaque transaction de données entre votre site Web et ses visiteurs est chiffrée et protégée, empêchant les violations de données et les attaques de type man-in-the-middle.
- **Protection DDoS dédiée:** les attaques DDoS devenant de plus en plus fréquentes et sophistiquées, la solution Web Security offre des défenses spécialisées, garantissant que vos plateformes en ligne restent accessibles même en cas d'attaques coordonnées.

Choisissez l'offre Web Security de SPIE pour naviguer en toute confiance dans le monde numérique, en sachant que chaque facette de votre présence en ligne est fortifiée, protégée et surveillée en permanence.

Sécurité de la messagerie électronique: se défendre contre les menaces par e-mail

Le courrier électronique reste l'une des principales voies de collaboration et de communication au sein des organisations, c'est pourquoi il est également un vecteur privilégié de cybermenaces. La sécurité de la messagerie électronique désigne l'ensemble des mesures et des protocoles conçus pour protéger les communications par courrier électronique contre les accès non autorisés, les violations de données, les attaques par hameçonnage, la diffusion de logiciels malveillants et d'autres cybermenaces. Elle englobe diverses technologies, politiques et pratiques visant à sécuriser à la fois le contenu et la transmission des e-mails.

La solution «Email Security» de SPIE est conçue pour fournir une protection inébranlable à ce canal de communication critique et garantit les éléments suivants:

- **Protection contre les menaces avancées**
- **Filtres anti-spam**
- **Prévention des fuites de données**
- **Chiffrement des e-mails**

La mise en œuvre de mesures robustes de sécurité de la messagerie avec SPIE réduit le risque d'incidents de sécurité au sein de votre entreprise et offre divers avantages tangibles, notamment des économies de coûts et une amélioration de la productivité, que ce soit sur site ou dans le cloud. SPIE ICS Switzerland s'associe à Cisco et pour fournir une défense avancée contre les menaces par e-mail.

Gestion des politiques de sécurité: assurer la cohérence et la conformité des politiques

Le maintien de politiques de sécurité cohérentes et conformes est essentiel pour préserver les actifs et la réputation d'une organisation.

La gestion de la politique de sécurité fait référence à la planification, à la mise en œuvre, au contrôle et à l'application systématiques des politiques de sécurité dans le cadre de la sécurité de l'information d'une organisation. Ces politiques définissent les règles, les lignes directrices et les meilleures pratiques qui régissent la façon dont une organisation protège ses actifs numériques, gère l'accès et atténue les risques de sécurité. SPIE présente sa solution complète de gestion des politiques de sécurité, conçue pour rationaliser, normaliser et assurer la conformité de vos protocoles de sécurité dans l'ensemble de votre entreprise.

- **Amélioration de la posture de sécurité:** grâce à des politiques de sécurité cohérentes et conformes, vous renforcez les défenses de votre organisation contre les menaces potentielles.
- **Efficacité et réduction des coûts:** réduisez le temps et les ressources consacrés aux vérifications et audits manuels des politiques, ce qui permet de réaliser d'importantes économies.
- **Respect des réglementations:** gardez une longueur d'avance sur les exigences réglementaires en constante évolution et respectez-les, ce qui permet d'atténuer les ramifications juridiques et financières potentielles.
- **Prise de décision éclairée:** grâce à une compréhension claire de votre politique de sécurité, prenez des décisions stratégiques qui s'alignent sur les objectifs de l'organisation et la tolérance au risque.
- **Confiance des parties prenantes:** démontrez une approche proactive de la cybersécurité et gagnez la confiance des parties prenantes, des partenaires et des clients.

Avec la solution de gestion des politiques de sécurité de SPIE, vous êtes non seulement assuré d'une mise en œuvre cohérente des politiques, mais vous êtes également équipé

d'un outil dynamique qui évolue avec le domaine de la cybersécurité en perpétuelle mutation.

Pare-feu de nouvelle génération (NGFW): renforcer la sécurité globale

Face à la complexité et à l'ampleur croissantes des cybermenaces, les pares-feux traditionnels ne suffisent plus. Voici le pare-feu de nouvelle génération (NGFW) de SPIE - une solution avant-gardiste conçue pour répondre aux défis contemporains en matière de sécurité, tout en offrant une protection globale à votre entreprise.

Un pare-feu de nouvelle génération (NGFW) est un dispositif de sécurité réseau sophistiqué qui combine les capacités d'un pare-feu traditionnel avec des fonctions de sécurité avancées, telles que la prévention des intrusions, la connaissance des applications et l'inspection approfondie des paquets. Les NGFW sont conçus pour offrir une protection complète contre un large éventail de cybermenaces, notamment les logiciels malveillants, le phishing et les menaces persistantes avancées (APT).

Face à l'évolution des cybermenaces, le pare-feu de nouvelle génération de SPIE se présente comme l'emblème de la protection moderne, conçu pour les organisations qui souhaitent mettre en œuvre une sécurité globale sans entraves. Avec le NGFW de SPIE, vous pouvez naviguer en toute confiance dans le monde numérique, en sachant que chaque paquet de données, application et activité de l'utilisateur est surveillé de près.

SPIE ICS Switzerland propose des solutions NGFW pour tous les cas d'utilisation avec les partenaires Fortinet, Checkpoint et Palo Alto.

Accès à distance (VPN): sécuriser l'accès depuis n'importe où

Alors que votre organisation est de plus en plus dispersée géographiquement et que votre personnel est de plus en plus mobile, l'accès à distance sécurisé est crucial. La solution d'accès à distance (VPN) de SPIE garantit que votre équipe peut se connecter aux données essentielles de l'entreprise en toute sécurité, où qu'elle se trouve dans le monde.

L'accès à distance (VPN) fait référence à la technologie et aux pratiques qui permettent aux utilisateurs de se connecter à un réseau privé ou à 'Internet en toute sécurité à partir d'un emplacement distant. Les VPN créent un tunnel chiffré sur un réseau non sécurisé, tel qu''Internet, permettant aux utilisateurs distants d'accéder aux ressources, aux données et aux services du réseau de l'entreprise comme s'ils étaient physiquement présents au bureau.

Les VPN fournissent un tunnel sécurisé pour la transmission des données, protégeant ainsi les informations sensibles et aidant les organisations à se conformer à la protection des données.

Vos avantages en bref:

- **Transmissions de données protégées:** veillez à ce que les informations sensibles restent confidentielles et sécurisées lorsque vous y accédez à distance.
- **Productivité accrue:** les employés peuvent accéder en toute sécurité aux ressources nécessaires, où qu'ils se trouvent et à tout moment, ce qui favorise la continuité des opérations.
- **Respect de la conformité:** respectez les exigences réglementaires en matière de protection des données, en particulier lorsqu'il s'agit d'informations sensibles ou personnelles.
- **Réduction des risques de cybersécurité:** grâce au chiffrement avancé et à l'authentification multifactorielle, les risques associés aux points d'accès à distance sont réduits.
- **Rentabilité:** réduisez les frais généraux liés à l'infrastructure physique tout en tirant parti des avantages d'une main-d'œuvre à distance.

La solution d'accès à distance (VPN) de SPIE répond aux exigences modernes des entreprises qui demandent de la flexibilité sans compromettre la sécurité. Permettez à votre équipe d'opérer au-delà des limites du bureau, en sachant que la technologie VPN de pointe de SPIE protège chaque interaction numérique.

SPIE ICS Switzerland garantit un accès à distance sécurisé avec les partenaires Cisco et Fortinet.

Détection et prévention des intrusions (IDS/IPS): détection et blocage des menaces

Il ne suffit pas d'identifier les vulnérabilités potentielles; les organisations doivent surveiller activement et réagir rapidement à toute activité illicite dans leur environnement numérique. Cela nécessite un système robuste de détection et de prévention des intrusions.

Les systèmes de détection et de prévention des intrusions (IDS/IPS) sont des technologies et des pratiques de cybersécurité conçues pour surveiller le trafic réseau et les systèmes afin de détecter les signes d'activités non autorisées ou malveillantes. Les IDS identifient les modèles ou les comportements suspects, tandis que les IPS prennent des mesures pour prévenir ou atténuer les menaces potentielles en temps réel. Ces systèmes jouent un rôle essentiel dans l'amélioration du dispositif de sécurité d'une organisation. Les fonctionnalités IDS/IPS sont intégrées dans les NGFW ou déployées en tant qu'appareils autonomes pour détecter et bloquer les menaces. L'offre IDS/IPS de SPIE se distingue par sa capacité à détecter et à contrer les cybermenaces potentielles en temps réel. De plus, notre offre est conçue pour s'intégrer sans effort à votre infrastructure existante, garantissant ainsi une mise en œuvre en douceur et sans interruption.

SPIE vous accompagne à chaque étape. De l’installation initiale aux mises à jour continues en passant par les consultations d’experts, notre équipe s’assure que vos défenses restent à la pointe de la technologie.

Nos références

Centre hospitalier Bienne

Vue d'ensemble du projet:

- 2 backbones
- 3 sites
- ~2000 utilisateurs
- >1700 ports
- 330 points d'accès WLAN

Les services que nous proposons:

- Infrastructure réseau Cisco avec composants LAN et WLAN Services
- WAN entre le site de Vogelsang et ARB AG et Localmed
- SM: Portail de service, tableau de bord de service
- Services de sécurité gérés: Accès à Internet, sécurité du Web, sécurité de la messagerie électronique, zones réseau (pare-feu), transition vers les réseaux partenaires, contrôle d'accès au réseau.
- Infrastructure de CU gérée

Canton de Berne

Vue d’ensemble du projet:

- ~700 sites
- >20’000 ports

Les services que nous proposons:

- Services LAN gérés (ports utilisateurs, ports serveurs)
- Service MPLS WAN pour 700 sites avec un accès partiel via le réseau mobile et VPN IPSec site-à-site
- WLAN géré sur des sites à accès multiples (SSIDs)
- Service d'accès à distance avec authentification forte
- Gestion de service (Portail de service, Tableau de bord de service)
- Services réseau (DNS, DHCP, IPAM, NTP)
- Services de sécurité gérés : accès Internet, sécurité web (proxy), sécurité e-mail, zones réseau (pare-feu), transition vers les réseaux partenaires, contrôle d'accès réseau (projet d'introduction).
- Centre de service 24/7

Nos partenaires de cybersécurité

Conclusion

En conclusion, une approche globale de la cybersécurité est essentielle pour que les entreprises puissent atténuer les diverses cybermenaces auxquelles elles sont confrontées. Il ne s'agit pas seulement de technologie, mais aussi de personnes et de processus pour créer une défense solide contre le paysage en constante évolution des cybermenaces.

Dans cette vue d'ensemble, SPIE ICS Switzerland a présenté ses offres étendues en matière de cybersécurité, couvrant une large gamme de services et de partenariats. Notre engagement en faveur des principes de la « sécurité d'abord » garantit que votre organisation reste résiliente face aux menaces émergentes.

La cybersécurité n'est pas une entreprise à taille unique. C'est pourquoi SPIE ICS Switzerland se spécialise dans l'adaptation de solutions à vos besoins uniques, vous donnant ainsi l'assurance que votre entreprise est protégée. Nous vous invitons à découvrir nos offres et à vous associer à nous pour préserver l'avenir numérique de votre organisation.

Pour plus d'informations et de demandes, veuillez contacter info.ch@spie.com

Ouvrages cités

Cyllective. (2022). Penetration Testing Services. Retrieved from https://cyllective.com/penetration-testing

Johnson, K., & Lee, S. (2018). Ensuring Data Security and Compliance through Remote Access. Journal of Information Security Management, 33(2), 164-178.

Wang, Q., et al. (2017). Minimizing Downtime with Security Backup Software. International Journal of Cybersecurity Resilience, 45(2), 153-167.