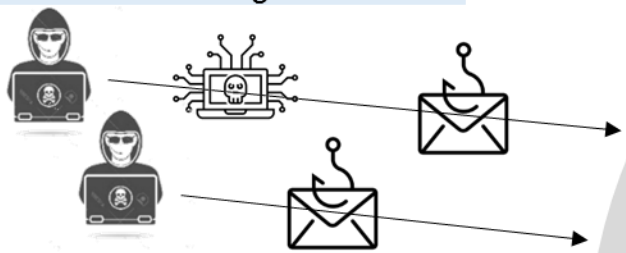
SOLUTIONS CYBERSECURITE L'OFFRE ISE-SYSTEMS

SENSIBILISER

ISE-PHISHING

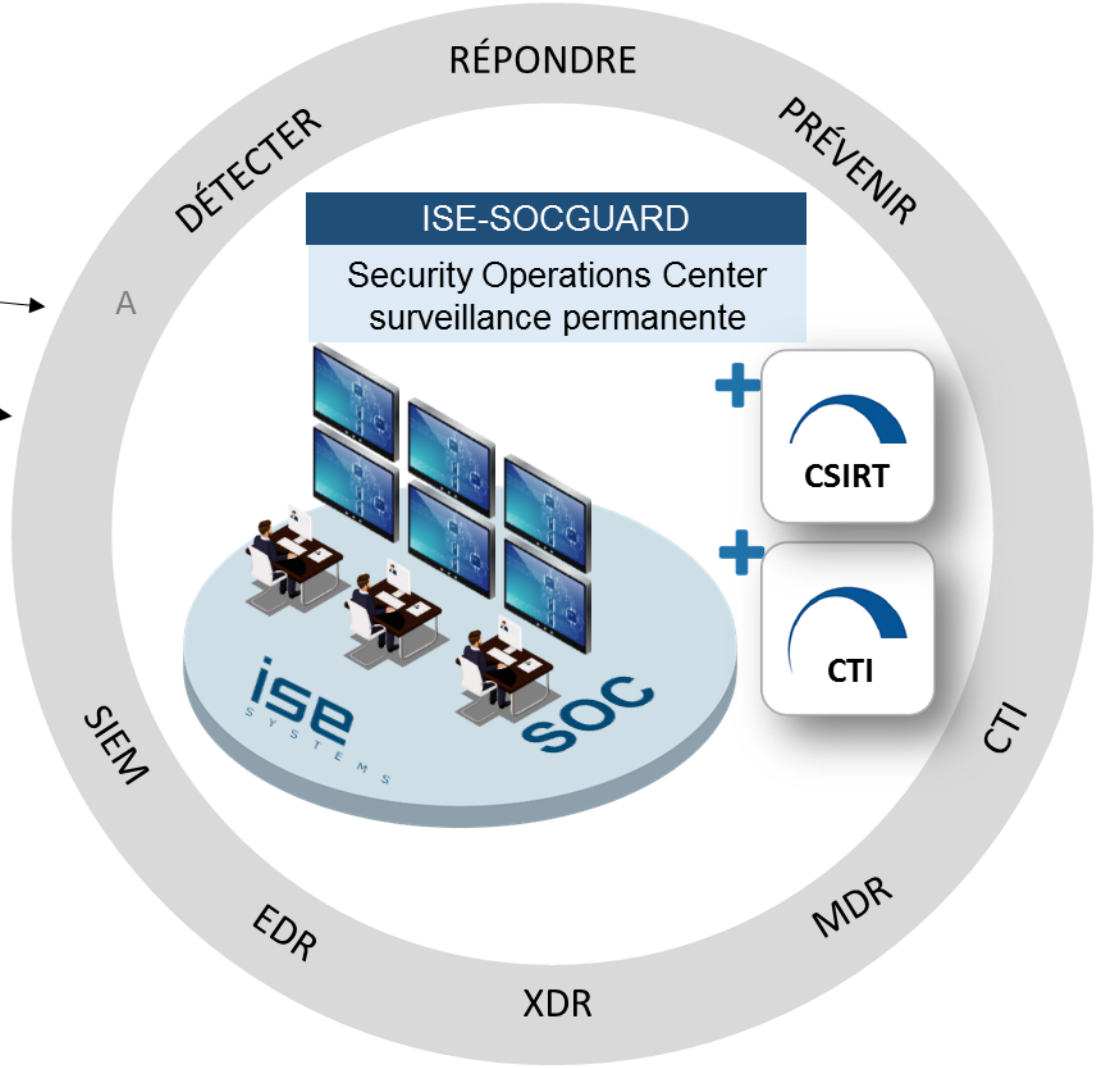
Campagnes de sensibilisation au Phishing



ÉPROUVER / PRÉVENIR

ISE-ESTIMATE

Sécurité des SI, infrastructure et durcissement



PRÉPARER / ENTRAÎNER

ISE-CYBERGAME

Simulation et entraînement à la Cyberdéfense

ISE-CYBERRESILIENCE

Préparer vos équipes à affronter une crise cyber

SOLUTIONS
CYBERSECURITE

L'OFFRE
ISE-SYSTEMS

ISE-CYBERGAME

Simulation et entraînement à la Cyberdéfense

Formation et entrainement à la cyberdéfense

Objectif : Améliorez la cyber-résilience de votre SI en vous entrainant à détecter, investiguer et remédier aux attaques plus rapidement avec ISE-CYBERGAME

65% des professionnels de l'IT français* considèrent que le manque de préparation représente le plus grand obstacle pour pouvoir se relever d'attaques informatiques.
La détection de cyberattaques et la réponse à incident requièrent une méthodologie, des processus rodés et des reflexes acquis lors de sessions d'entrainements intensifs.

(*Etude Ponemon Institute sur la cyber-résilience)

Réalisations
- Sessions d'entrainement sur simulateur d'attaques (Blue/Red Team)
- Tests d'une large gamme d'impacts les équipements du SI (intégrité des données, disponibilité du service et confidentialité)
- Entraînement sur les outils périphériques de cybersécurité nécessaires à l'identification et l'investigation de cyber attaques en vue d'une immersion totale dans des situations opérationnelles de Cyber Défense (QRADAR, SPLUNK, ARCSIGHT, CHECKPOINT, PALO ALTO, ZENOSS,…)

Livrables
- Debriefs vidéo sur la plateforme
- Certification et notation individuelle des stagiaires et évaluation collective de l'équipe

Type de mission
- Formation Inter et intra Entreprise

Périmètre
- Présentiel et/ou à distance (de 5 à 12 stagiaires/session)
- SI et scénarios standard, Personnalisation possible à définir…

SOLUTIONS
CYBERSECURITE

L'OFFRE
ISE-SYSTEMS

ISE-CYBERRESILIENCE

Préparer vos équipes à affronter une crise cyber

Cyber Résilience 360°

Objectif : s'entrainer pour pratiquer et s'améliorer en cas de crise cyber sécurité

Acquisition de compétences des salariés en gestion de crise cyber sécurité afin d'apprendre à :

- Tester les plans et méthodes de défense de l'entreprise
- Mettre en place une organisation adaptée pour répondre aux situations de crise
- Elaborer une communication cohérente
- Eviter les pièges induits par les situations de crise

Formations sur Cyber Range avec participation présentielle sur 1 ou plusieurs jours.

Prise en compte de vos besoins spécifiques et choix de scénarios et d'architectures modulables.

Réalisations

L'exercice de crise sur simulateur permet d'éprouver l'organisation sur l'ensemble de ses niveaux (technique, opératif, business et stratégique) à la crise cyber. Elle permet d'impliquer tous les collaborateurs et profils impliqués dans les cellules de crise établies par le Plan de Gestion de Crise Cyber (PGCC).
Les exercices de crise cyber sont opérés sur un environnement de simulation du SI du client. Les attaques sont lancées au travers de simulateur d'attaque (Cyber Range) et l'exercice est animé par nos experts cybersécurité et gestion de crise cyber.

Livrables

L'objectif pédagogique affiché est de faire acquérir à chacun des participants de bons réflexes de gestion de crise cyber, à savoir :

- Bonnes pratiques immédiates en cas d'alerte virale en particulier celles du RSSI
- Bonne réaction face à une cyber attaque
- Priorisation des besoins métiers
- Bonne circulation de l'information à tout niveau
- Bonne exploitation des données brutes pour parvenir à un processus décisionnel
- Appréciation de situation en cas de crise
- Connaissance et application des plans de gestion de crise
- Mise en place et organisation d'une cellule de crise
- Maîtrise de la communication interne, externe et relation aux autorités
- Préparation à une situation qui peut s'inscrire dans la durée

A travers ce type de simulation au plus près du réel, il s'agit d'aider les participants à :

- Identifier quels processus de gestion de crise sont bien maîtrisés
- Identifier quels besoins matériels, organisationnels ou décisionnels doivent être approfondis
- **Anticiper la prochaine crise**

SOLUTIONS
CYBERSECURITE

L'OFFRE
ISE-SYSTEMS

ISE-ESTIMATE

Sécurité des SI, infrastructure et durcissement

Renforcement de la sécurité des Systèmes d'Information

Afin de vous aider à mettre en place des solutions de protection efficaces, il est indispensable d'identifier au préalable les risques métiers qui pèsent sur votre activité.
ISE-ESTIMATE est un ensemble de prestations liées à la gouvernance et à l'audit de la sécurité des Systèmes d'Information.
Ces services permettent de mettre en place une approche dite TOP-DOWN, c'est à dire d'identifier les risques métiers de nos clients et d'en déduire des indicateurs de surveillance les plus représentatifs des contraintes métiers.

Réalisations
- Analyse de risque : identification des actifs critiques, analyse des menaces & vulnérabilités, traitement des risques
- Audit d'architecture : cloisonnement, dimensionnement, …
- Audit réseau : filtrage, protection, …
- Audit système : serveurs web, serveurs base de données, …
- Rédaction des documents synthétisants les exigences en matière de sécurité en ligne complète avec votre business

Livrables
- Rapport d'analyse de risque
- Rapport d'audit d'architecture sécurisée
- Politique de sécurité du SI (PSSI) : recommandations, priorités, calendrier d'actions

Type de mission
- Mission d'expertise en Assistance Technique

Périmètre
- A définir…

SOLUTIONS
CYBERSECURITE

L'OFFRE
ISE-SYSTEMS

ISE-PHISHING

Campagnes de sensibilisation au Phishing

Campagnes de sensibilisation de vos collaborateurs au phishing & à la cybersécurité

Objectif : Transformer le comportement des collaborateurs, en assurant une préparation continue de l'entreprise contre les menaces de phishing.

La solution proposée par ISE SYSTEMS a été conçue pour élaborer et diffuser automatiquement les campagnes de phishing dans toutes ses dimensions (phishing email, programmation, langues, contenus pédagogiques, fréquences…).

Elle inclut également un programme de sensibilisation à tous les thèmes de la cybersécurité grâce à des « piqures de rappel » (Cybersecurity Awareness Bytes), quiz pédagogiques au format court et ludique.

Réalisations

- Configuration simple des campagnes (contenu, programmation, ciblage)
- Mise en œuvre simples import en masse des emails cibles)
- Résultats individuels et par niveau d'organisation
- Adaptation automatique du niveau de difficulté des campagnes en fonction des résultats obtenus sur les différentes populations ciblées
- Catalogue de modèles d'emails (templates) de Phishing, basé sur les menaces et attaques récentes
- Formation pour les utilisateurs sous forme de quizz (CAB)
- Séance de sensibilisation sur l'empreinte numérique, la cybercriminalité, les bonnes pratiques, l'ingénierie sociale et le phishing multiforme (SMS, Emails, QRCode, Téléphone…)

Livrables

- Tableaux de bord temps réel (indicateurs de performances)
- Rapport hebdomadaire & présentation managériale mensuelle

Type de mission

- Mission en service managé (Mode SaaS & Success manager)

SOLUTIONS
CYBERSECURITE

L'OFFRE
ISE-SYSTEMS

ISE-SOCGUARD

Security Operations Center
surveillance permanente

Service de supervision de la Sécurité en temps réel 24/7 (SOC, CSIRT, CERT)

SIEM, EDR, XDR, MDR, CTI

Objectif :
survenir à tout moment en cas d'incident ou d'attaque sur votre SI ; assurer une identification et une remédiation le plus rapidement possible afin de limiter les impacts financiers et réputationnels.

Notre équipe de surveillance et de réponse à incident est opérationnelle 24h/24, 7j/7. Elle s'appuie sur le SOC de ISE SYSTEMS, des plateformes technologiques capables de superviser les flux réseaux et évènements systèmes & applicatifs pour détecter les tentatives d'attaque et générer des alertes.

En lien avec vos équipes cyber, elle renforce également la prévention, et permet en cas de crise d'améliorer sensiblement le niveau de cyber-résilience de votre organisation.

Réalisations

SOC
- Supervision Sécurité du SI
- Gestion des évènements et des incidents de sécurité
- Coordination des informations sur la Cybersécurité

CSIRT
- Conduite de la réponse sur incident
- Aide à la décision & réponses
- Support à la sécurité opérationnelle
- Tracé / investigation / rejeu des attaques

CERT
- Veille sur les menaces et nouvelles vulnérabilités (CTI)
- Forensic en live ou post-mortem
- Reverse engineering et sandboxes de malwares

- Détection contre la fuite de données
- Support à la maîtrise de l'empreinte internet
- Lutte contre la fraude
- Prévention contre les risques cyber via la Threat Intelligence

Livrables
- Remontées d'alerte en temps réel
- Rapports d'incidents et tableau de bords
- Rapports détaillés de tous les incidents
- Bulletins d'information génériques (nouvelles vulnérabilités et remédiations)
- Notes ciblées sur des menaces spécifiques

Type de mission
- Mission d'expertise en service managé (abonnement)