Cybersécurité

Implication utilisateurs

PHMG

Une approche proactive de la sensibilisation à la cybersécurité

En s'associant à MetaCompliance, PHMG a adopté une approche proactive de la sensibilisation à la cybersécurité, visant à améliorer la conscientisation des employés et à faire face de manière proactive aux problèmes de sécurité et de conformité.

Auparavant, PHMG n'avait pas mis en place de programme de formation officiel pour sensibiliser ses employés aux bonnes pratiques en matière de cybersécurité et pour établir des limites claires quant à leur comportement sécurisé. Afin d'engager les employés et de renforcer la résilience de l'organisation, il était essentiel que la formation soit attrayante et informative.

Création de cours de formation et de sensibilisation en cybersécurité personnalisés

Grâce à la bibliothèque eLearning, PHMG a pu créer des cours de formation et de sensibilisation en cybersécurité personnalisés, correspondant à l'image de marque de l'entreprise

Formation efficace pour se protéger contre le phishing en entreprise

Campagne de fishing simulés.
Les individus qui cliquent sur une simulation de phishing sont confrontés à une expérience d'apprentissage interactive qui fournit un retour d'information immédiat et informe les employés des mesures à prendre pour réduire le risque d'attaques futures.

Orange Cyberdefense

6 règles à suivre
Sensibiliser par le jeu

MailInBlack

Les enjeux de la cyberculture en entreprise

Michelin

Gestion surface d'attaque

SOC

Le Security Operations Center (SOC), ou centre des opérations de sécurité, est une entité centralisée chargée de surveiller, analyser et répondre aux incidents de sécurité pour protéger l'organisation des risques cyber. La mise en place d'un SOC nécessite une approche structurée et implique plusieurs étapes importantes. Voici les étapes principales pour créer un SOC efficace :

Définir les objectifs et la portée du SOC

- **Identification des besoins** : Évaluer les risques cyber auxquels l'organisation est confrontée et déterminer les services que le SOC doit fournir (surveillance en temps réel, détection d'incidents, réponse aux incidents, etc.).
- **Niveau de maturité** : Estimer le niveau de maturité en cybersécurité de l'organisation pour ajuster les capacités du SOC (SOC basique, SOC avancé, ou externalisation du SOC).
- **Définir les indicateurs de performance (KPI)** : Pour mesurer l'efficacité du SOC (temps de réponse, nombre d'incidents détectés, etc.).

Élaborer une équipe SOC

- **Rôles et responsabilités** : Créer une structure d'équipe avec des rôles définis comme :
  - Analystes SOC (Niveaux 1, 2, et 3),
  - Responsable SOC ou Chef de SOC,
  - Spécialistes en détection des menaces,
  - Ingénieurs sécurité,
  - Experts en réponse aux incidents.
- **Formation et certification** : S'assurer que l'équipe possède les compétences techniques nécessaires, par exemple, des certifications telles que CISSP, CEH, ou GIAC peuvent être exigées.
- **Formation continue** : Mettre en place des programmes de formation continue pour garder l'équipe à jour sur les nouvelles menaces et techniques de sécurité.

Choisir l'infrastructure et les outils

- **SIEM (Security Information and Event Management)** : Outil central du SOC pour collecter, corréler et analyser les journaux d'événements provenant de divers systèmes de l'organisation (serveurs, applications, pare-feu, etc.).
- **Systèmes de détection d'intrusion (IDS/IPS)** : Pour détecter les comportements anormaux

sur le réseau.
- **EDR (Endpoint Detection and Response)** : Pour surveiller les endpoints et réagir aux menaces ciblant ces points d'accès.
- **Outils d'automatisation (SOAR)** : Automatiser certaines tâches de réponse aux incidents pour réduire le temps de réaction.
- **Technologie de Threat Intelligence** : Pour collecter et analyser les informations sur les menaces extérieures.

Développer des processus et des procédures

- **Runbooks et Playbooks** : Création de procédures documentées pour gérer les incidents courants (ex. : attaque par ransomware, phishing, etc.).
- **Processus de gestion des incidents** : Inclut les étapes de détection, analyse, confinement, éradication, récupération, et retour d'expérience (post-mortem).
- **Plan de réponse aux incidents** : Élaborer un plan détaillé pour faire face aux incidents majeurs et coordonner les réponses avec d'autres départements (légal, communication, etc.).

Surveiller et analyser les menaces

- **Définir des cas d'usage pour le SIEM** : Identifier les types d'incidents que le SOC doit surveiller en priorité (tentatives d'intrusion, anomalies réseau, etc.).
- **Corrélation et analyse des événements** : Le SIEM doit corréler les informations provenant de plusieurs sources pour identifier les comportements suspects.
- **Surveillance en temps réel** : Les analystes SOC doivent être capables de surveiller en permanence les événements de sécurité et réagir rapidement.

Gestion des incidents

- **Analyse et évaluation des incidents** : Les analystes doivent examiner les alertes générées par le SIEM et autres outils pour déterminer la gravité des incidents.
- **Réponse rapide** : Déclencher une réponse appropriée (confinement, éradication de la menace, récupération des systèmes affectés).
- **Escalade des incidents** : Certains incidents critiques nécessitent l'intervention de niveaux supérieurs d'analystes ou d'équipes spécialisées.

Collaboration et communication

- **Coordination inter-départementale** : Le SOC doit collaborer avec d'autres départements (IT, juridique, communication) pour une réponse efficace.
- **Partage d'informations** : Si applicable, collaborer avec d'autres SOC ou partenaires externes pour partager des informations sur les menaces (threat intelligence).

Suivi et amélioration continue

- **Post-mortem des incidents** : Analyser les incidents après leur résolution pour améliorer les procédures et renforcer les défenses.
- **Tests réguliers** : Effectuer des tests de pénétration, des simulations d'incidents, et des audits pour évaluer l'efficacité du SOC.
- **Amélioration des capacités** : Mettre à jour les technologies, les outils et les processus pour s'adapter aux nouvelles menaces.

Externalisation ou internalisation du SOC

- Si l'organisation n'a pas les ressources pour créer un SOC interne, elle peut envisager l'externalisation auprès de fournisseurs de services de sécurité gérés (MSSP) ou adopter un modèle hybride (partiellement géré en interne, partiellement externalisé).