Tenexa

5 ÉTAPES EN CAS DE CYBERATTAQUE

1 DÉTECTER & ALERTER

Déterminer l'origine de l'attaque, les systèmes affectés et l'ampleur de l'incident avec des outils adaptés. Alerter les parties prenantes internes et externes.

Conseil : Intégrez un SOC avec des capacités de détection et de réponse en temps réel (24/7).

2 ISOLER & PRÉSERVER

Isoler les systèmes infectés pour empêcher la propagation de la menace. Préserver les preuves de l'attaque (indicateurs, journaux...)

Conseil : Tenez un registre des événements et des actions réalisées.

3 ÉVALUER

Analyser la portée de l'attaque en identifiant les données compromises et les systèmes affectés.

Conseil : Travaillez en collaboration avec des équipes internes et externes.

4 AUDITER, NETTOYER & RECONSTRUIRE

Identifier les vecteurs d'intrusion et supprimer tous les éléments malveillants (malwares, portes dérobées etc.).

Conseil : Effectuez un audit de sécurité pour identifier et corriger les vulnérabilités. De plus, il est parfois nécessaire et plus sûr, de procéder à une reconstruction des systèmes affectés.

5 TIRER DES LEÇONS

Documenter les détails de l'attaque et la réponse pour améliorer vos protocoles de sécurité et former vos équipes.

Conseils :

- Mettez à jour vos processus de sécurité.
- Planifiez des exercices de simulation pour tester les équipes.
- Documentez l'incident.