



Réponse aux incidents

Réagissez rapidement et efficacement face aux incidents cybernétiques avec Eye Security

Vous venez d'être attaqué,
que faites vous?

Gérez vous l'incident
vous-même?

1

L'isolement et la maîtrise de la menace sont des compétences spécifiques en sécurité informatique. Cela prend du temps et vous n'en avez pas forcément, alors que le potentiel d'attaque s'aggrave.

Possédez-vous un plan
de réponse aux incidents?

2

Est-ce qu'il prend en compte tous les types de menaces ainsi que leurs conséquences? Pour ce faire, vous aurez besoin de l'expérience de tous les types d'attaques.

Comptez vous sur
votre logiciel de
sécurité informatique?

3

Une fois qu'une attaque a eu lieu, il est déjà trop tard et le logiciel a ses limites – vous ne bénéficierez pas forcément du soutien nécessaire.

Engagez-vous des
experts externes?

4

Établir une collaboration avec des experts externes peut s'avérer difficile sans une expertise spécialisée, et cela peut vous faire perdre du temps. Résoudra-t-il les vulnérabilités à long terme?

Personne ne souhaite être victime d'une cyberattaque, mais tant que cela ne vous est pas arrivé, vous ne réalisez pas le niveau d'expertise nécessaire pour la contrôler immédiatement. Les attaques modernes sont sophistiquées et les individus malveillants compétents rendent de plus en plus difficile pour les entreprises de se protéger et de se remettre d'une cyberattaque. Pourtant, lorsque cela se produit, agir rapidement et efficacement est crucial pour limiter les dommages et les coûts élevés.

1/5

Probabilité de 1/5
d'une cyberattaque

4 mins

Temps moyen de
réponse de 4 minutes
à un incident

Votre solution:

Si vous êtes attaqué, vous voulez vous associer aux meilleurs – une équipe d'experts, avec des années d'expérience acquises dans des domaines tels que les agences de renseignement et de sécurité nationales, entre autres domaines spécialisés. Ces experts sont disponibles 24/7, pour garantir que vos processus opérationnels sont rapidement remis en service. Certains des incidents auxquels nous sommes fréquemment confrontés sont:

- Cryptage de fichiers à la suite d'une attaque par ransomware
- Comportement inexplicable dans les systèmes opérationnels
- E-mails frauduleux envoyés par un individu malveillant

Nous avons rencontré tous types d'attaques et notre mission est de résoudre rapidement le problème et d'être là pour vous comme un membre de l'équipe étendue, en apaisant les tensions et en vous soutenant.

Les avantages de la réponse aux incidents

Réponse rapide

Dès que vous contactez notre hotline de réponse aux incidents, nous lançons l'analyse et prenons des mesures immédiates pour atténuer la menace.

Dommages limités

En déployant notre expertise grâce à un logiciel de détection et de réponse géré, nous sécurisons vos systèmes pour empêcher d'autres dommages.

Retour rapide à l'activité

Avec une équipe de réponse aux incidents aussi expérimentée, nous garantissons un retour rapide à la normale, minimisant les interruptions de votre activité.



Comment fonctionne la réponse aux incidents

- **Évaluation initiale**
Identification rapide du type d'incident et évaluation de son impact sur la disponibilité, la confidentialité et l'intégrité de vos données.
- **Démarrage**
Une réunion immédiate pour définir le processus de réponse aux incidents, garantissant une compréhension claire et attribuant des responsabilités à toutes les parties impliquées.
- **Maîtrise**
Analyse, maîtrise et minimisation des conséquences néfastes de l'incident. Actions méticuleuses pour sécuriser vos actifs numériques.
- **Récupération**
Élimination de la menace et restauration de vos systèmes avec une approche méthodique pour remettre vos processus opérationnels en ligne.
- **Évaluation**
Actionner les trois précieuses leçons tirées de l'incident, renforcement de la sécurité du réseau, affinement du plan de continuité des activités (PCA) et optimisation de la réponse.

Rencontrez l'équipe

Pourquoi nos clients font-ils confiance à notre équipe pour leur sécurité informatique

Les membres de notre équipe apportent une expérience précieuse des services secrets et des environnements de sécurité de haut niveau. Avec un historique de navigation à travers des menaces complexes, nous combattons intelligemment et calmement les défis cybernétiques, en nous appuyant sur les enseignements tirés de scénarios réels.



 

 **Vaisha**

 Spécialiste principal en cybersécurité

 13+ Ans d'expérience en sécurité informatique



  *Investigateur privé agréé*

 **Lodi Hensen**

 Vice-président des opérations de sécurité

 15 Ans d'expérience en sécurité informatique (forensics réponse aux incidents)



 

 **Michael de Klein**

 Spécialiste principal en cybersécurité et responsable d'équipe MDR

 5+ Ans d'expérience (offensive et défensive)



 

 **Niels Teusink**

 Spécialiste principal en cybersécurité

 17 Ans d'expérience à temps plein en sécurité informatique



 

 **Bas van den Berg**

 Spécialiste principal en cybersécurité

 8+ Ans d'expérience en sécurité informatique



 

 **Davy**

 Spécialiste senior en cybersécurité

 6+ Ans d'expérience en informatique

Notre processus de réponse aux incidents:



Votre liste de contrôle pour la réponse aux incidents:

1 Identification

- ✓ Reconnaître et confirmer rapidement la survenue d'un incident de sécurité
- ✓ Définir la portée et la nature de l'incident

2 Maîtrise

- ✓ Isoler les systèmes ou réseaux affectés pour éviter de nouveaux dommages
- ✓ Mettre en œuvre des mesures temporaires pour minimiser l'impact

3 Éradication

- ✓ Identifier et éliminer la cause profonde de l'incident
- ✓ Supprimer les logiciels malveillants, combler les vulnérabilités et corriger les faiblesses

4 Récupération

- ✓ Restaurer les systèmes affectés à un fonctionnement normal
- ✓ Valider que l'environnement est sécurisé et exempt de restes de l'incident

5 Communication et documentation

- ✓ Notifier les parties prenantes pertinentes, y compris la direction, les équipes informatiques, et, si nécessaire, les forces de l'ordre
- ✓ Documenter l'incident, les actions entreprises, et les leçons apprises pour les améliorations futures

Eye Security est une société de cybersécurité par abonnement qui propose aux entreprises européennes des services de cybersécurité et d'assurance réalisables. Avec une équipe croissante d'experts en sécurité et en assurance, Eye Security offre un service de sécurité tout-en-un de haute qualité et abordable en combinant la détection et la réponse étendues gérées (MDR) et la cyber-assurance. Fondée en 2020, Eye Security opère en Europe avec des bureaux aux Pays-Bas, en Belgique, en Allemagne et par l'intermédiaire de ses partenaires.

Visitez

eye security