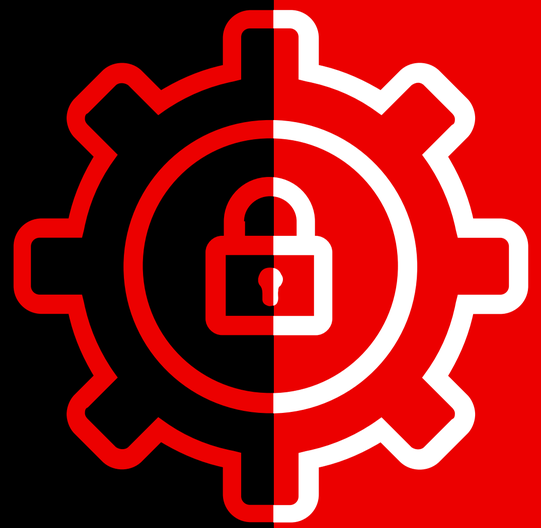
CROWDSTRIKE

Stopper les cybermenaces dans le secteur des services financiers

Respecter les réglementations, mais pas les cyberadversaires, à une époque où les cybermenaces s'intensifient



Les paysages concurrentiels et opérationnels des organisations de services financiers évoluent sans cesse. La demande d'expériences transparentes et personnalisées crée un besoin de sécurité et de confidentialité des données plus fort.

Si l'on ajoute à cette complexité la croissance exponentielle des données et des systèmes basés sur le cloud, les organismes financiers deviennent une cible privilégiée pour les cyberattaques. Le Global Threat Report montre que le nombre d'attaques contre les services financiers augmente chaque année.

La conformité réglementaire n'est pas négociable

Votre vitesse d'adaptation est-elle suffisante pour déjouer vos cyberadversaires ?

Faites-vous le nécessaire pour vous conformer aux réglementations à venir telles que la directive européenne NIS2 et la réglementation DORA (Digital Operational Resilience Act) ?

En restant à l'affût des tendances en matière de cybersécurité, vous éviterez les conséquences d'une attaque sur le plan opérationnel et financier, et préserverez votre réputation. Cela vous évitera également d'encourir des amendes importantes en cas de non-conformité.

Sanctions pour les entreprises du secteur financier qui ne se conforment pas aux règles ou ne signalent pas les incidents :

10 millions d'euros

Jusqu'à 10 millions d'euros ou 2 % des revenus annuels mondiaux totaux au titre de la réglementation NIS2.

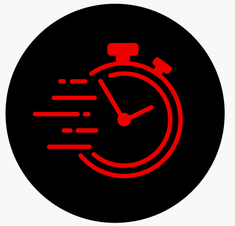
5 millions d'euros

Jusqu'à 5 millions d'euros ou 2 % des revenus annuels mondiaux totaux au titre de la réglementation DORA.

▶ **Nos experts en cybersécurité peuvent vous aider à vous y retrouver dans les derniers changements réglementaires.**

Que se passe-t-il dans le monde de la cybersécurité et quelles sont les conséquences pour les services financiers ?

7 POINTS CLÉS DU **GLOBAL THREAT REPORT 2024 DE CROWDSTRIKE** POUR LES ORGANISMES FINANCIERS



1. Les attaques sont plus sophistiquées et plus rapides

Le temps nécessaire pour accéder à un réseau a considérablement diminué :

- Le temps moyen de propagation est de 62 minutes, une durée presque 25 % plus courte qu'en 2023.
- L'attaque la plus rapide enregistrée n'a duré que 2 minutes et 7 secondes.

QUELLES MESURES PRENDRE ?

Conformité

Mettez à jour et testez régulièrement les plans de réponse à incident afin de répondre aux exigences de la directive NIS2 en matière de signalement et de gestion rapides des incidents.

Action

Accélérez la détection des cybermenaces et les délais de réponse grâce à des solutions avancées de détection et de réponse à incident (EDR).

- **Soyez rapidement opérationnel. Appuyez-vous sur une technologie axée sur le cyberadversaire qui offre le délai de détection le plus court (testé par MITRE ATT&CK® Evaluations) et qui est adaptée au secteur des services financiers.**

2. Les logiciels malveillants et les méthodes d'attaque évoluent

75 % des attaques ne reposent plus sur des logiciels malveillants, contre 40 % en 2019.

Alors que l'identification des cybermenaces s'améliore, les cyberadversaires trouvent de nouveaux moyens de déjouer la sécurité. Les identifiants volés et les attaques d'ingénierie sociale rendent les brèches plus difficiles à repérer.

QUELLES MESURES PRENDRE ?

Conformité

Mettez en place des contrôles d'accès stricts et surveillez les activités des utilisateurs pour répondre aux exigences de la directive NIS2 en matière de sécurisation des réseaux et des systèmes d'information.

Action

Renforcez la protection de l'identité grâce à l'authentification multifacteur (MFA).

- **Utilisez les services de Threat Hunting pour vous avertir des nouvelles techniques des cyberadversaires.**

3. Les intrusions dans le cloud se sont multipliées

Les intrusions liées au cloud ont augmenté de **110 %** en un an.

Les cyberadversaires exploitent les faiblesses des configurations de sécurité du cloud pour attaquer à partir du service cloud de la victime.

QUELLES MESURES PRENDRE ?

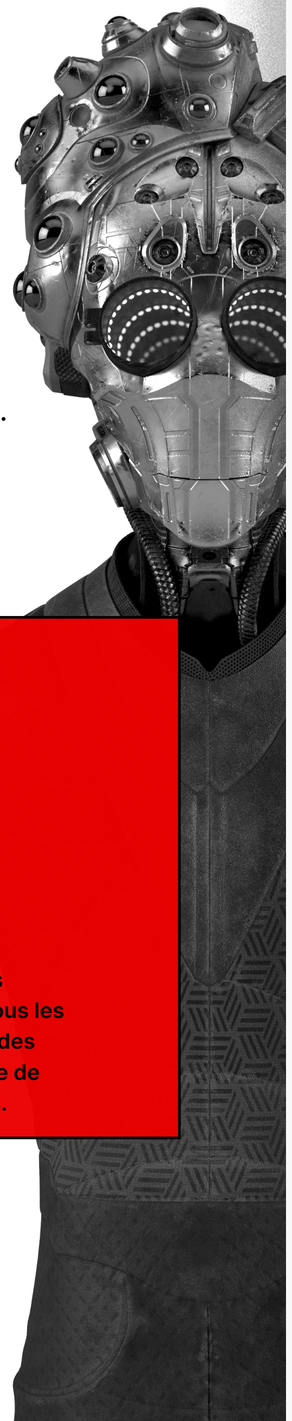
Conformité

Assurez-vous que les fournisseurs de services cloud adhèrent aux normes et aux bonnes pratiques NIS2 pour protéger les données et les services basés sur le cloud.

Action

Adoptez des frameworks de sécurité complets pour le cloud, qui incluent la gestion des identités et des accès (IAM), le chiffrement et la surveillance continue.

- **N'attendez pas que des cyberadversaires s'introduisent dans vos systèmes financiers. Faites appel à des experts pour prévenir les attaques.**



4. Les relations avec des tiers sont exploitées

Les logiciels commerciaux issus du secteur technologique sont à l'origine de la plupart des compromissions de relations de confiance.

Les cyberadversaires ciblent de plus en plus les fournisseurs tiers et les supply chains pour accéder aux réseaux des institutions financières, en exploitant leur réputation de fiabilité et leur niveau d'interconnexion.

QUELLES MESURES PRENDRE ?

Conformité

Développez et appliquez des règles de gestion des risques des tiers afin de répondre aux exigences renforcées de la directive NIS2 en matière de sécurité de la supply chain.

Action

Procédez à des évaluations et à des audits rigoureux de la sécurité de tous les fournisseurs tiers. Mettez en place des exigences contractuelles en matière de cybersécurité pour les fournisseurs.

- **Les attaques contre les relations avec les tiers sont très rentables pour les cyberadversaires. Veillez à ce que les normes de sécurité de vos fournisseurs soient aussi rigoureuses que les vôtres.**

5. Les cyberadversaires tirent parti de l'IA générative

L'IA peut être utilisée à mauvais escient pour les opérations d'information des cyberadversaires, en particulier lorsque le public est moins familiarisé avec les technologies numériques.

L'IA générative a abaissé le niveau de connaissances requis pour créer des attaques sophistiquées et étendues.

QUELLES MESURES PRENDRE ?

Conformité

Mettez régulièrement à jour vos stratégies de cybersécurité pour faire face aux nouvelles cybermenaces liées à l'IA et vous aligner sur les critères plus stricts de la directive NIS2 sur la gestion proactive des cybermenaces.

Action

Restez informé des cybermenaces liées à l'IA et envisagez d'intégrer des outils de cybersécurité basés sur l'IA pour détecter et contrer les techniques avancées.

- **Utilisez le potentiel de transformation de l'IA générative sur les workflows de sécurité pour défendre votre entreprise.**

6. La protection de l'identité est la priorité

Notre Global Threat Report 2024 présente des exemples concrets dans lesquels le phishing et l'exploitation de vulnérabilités logicielles ont permis de collecter des identifiants.

Les identités sont une cible privilégiée des cyberintrusions, et de plus en plus d'attaques s'appuient sur des identifiants volés pour obtenir un accès non autorisé.

QUELLES MESURES PRENDRE ?

Conformité

Adoptez les bonnes pratiques du secteur en matière de gestion des identités et des accès (IAM), comme nous l'avons fait, pour vous conformer aux exigences de protection des identités de la directive NIS2.

Action

Mettez en place des solutions robustes de gestion des identités et des accès (IAM), dont la surveillance et la détection des anomalies en temps réel.

▶ **Devancez les cybermenaces modernes avec une plateforme unifiée pour éviter les attaques basées sur l'identité.**

7. Il faut réduire le temps de détection des incidents et les délais de réponse

Les cyberadversaires cherchent généralement à étendre leur accès au-delà du point de compromission initial, ce qui prend environ une heure en moyenne. Ils peuvent ensuite faire des ravages en quelques secondes.

Une détection et une réponse rapides face aux cyberincidents sont essentielles. Les retards peuvent aggraver les dommages causés par une brèche.

QUELLES MESURES PRENDRE ?

Conformité

Développez et testez régulièrement des plans de réponse à incident afin de garantir une action rapide et de respecter les délais de signalement très stricts de la NIS2.

Action

Investissez dans des outils de surveillance et d'analyse avancés qui offrent une visibilité en temps réel de l'activité du réseau.

La conformité réglementaire n'est pas négociable, en particulier pour les institutions financières. En faisant cavalier seul, vous exposez votre organisation et vos clients à des risques inutiles.

Constituez une équipe dédiée à la conformité pour suivre l'évolution de la réglementation et veiller à ce que les pratiques en matière de cybersécurité soient à jour. Veillez à ce qu'elle effectue régulièrement des audits de conformité et mette à jour les politiques pour les aligner sur NIS2, DORA et d'autres frameworks pertinents.

Des experts en cybersécurité peuvent vous aider à vous y retrouver dans les derniers changements réglementaires.

Lisez le Global Threat Report 2024 de CrowdStrike

7 points clés du Global Threat Report 2024 de CrowdStrike

1. Les attaques sont plus sophistiquées et plus rapides
2. Les logiciels malveillants et les méthodes d'attaque évoluent
3. Les intrusions dans le cloud se sont multipliées
4. Les relations avec des tiers sont exploitées
5. Les cyberadversaires tirent parti de l'IA générative
6. La protection de l'identité est la priorité
7. Il faut réduire le temps de détection des incidents et les délais de réponse

TÉLÉCHARGER LE RAPPORT

CROWDSTRIKE

À propos de CrowdStrike

CrowdStrike (Nasdaq : CRWD), leader mondial de la cybersécurité, redéfinit la sécurité avec sa plateforme cloud native la plus avancée au monde, conçue pour protéger les ressources critiques des entreprises, à savoir les endpoints, les workloads cloud, les identités et les données.

Optimisée par l'architecture de sécurité cloud de CrowdStrike et une intelligence artificielle de pointe, la plateforme CrowdStrike Falcon® s'appuie sur des indicateurs d'attaque en temps réel, le renseignement sur les cybermenaces, l'évolution des techniques des cybercriminels et des données télémétriques enrichies récoltées à l'échelle de l'entreprise pour assurer une détection ultraprécise, une protection et une correction automatisées, un Threat Hunting de pointe et une observation priorisée des vulnérabilités.

Spécialement conçue dans le cloud au moyen d'une architecture à agent léger unique, la plateforme Falcon offre un déploiement rapide et évolutif, une protection et des performances de haut niveau, une complexité réduite et une rentabilité immédiate.

CrowdStrike. We stop breaches.