PRÉSENTATION

# Améliorer la cyberrésilience : comment ThreatQ favorise la conformité aux exigences de la directive NIS2

La protection des infrastructures critiques contre les cybermenaces est devenue une préoccupation majeure des gouvernements et des entreprises. Pour relever ce défi, l'Union européenne (UE) a introduit la directive NIS2 en janvier 2023 afin de renforcer la cyberrésilience des infrastructures critiques. La directive énonce des exigences strictes en matière d'identification et d'atténuation des risques, de notification des incidents, de partage des informations et de supervision. Dans cette présentation, nous expliquons comment ThreatQ, une plate-forme de Threat Intelligence de pointe, répond aux exigences de la directive NIS2, améliorant ainsi la cybersécurité des entreprises soumises à ces réglementations.

## Comprendre la directive NIS2

La directive NIS2 exige que les entreprises responsables d'infrastructures critiques prennent des mesures exhaustives pour renforcer leur cybersécurité. Ces mesures englobent plusieurs disciplines, notamment la gestion des risques, la notification des incidents, le partage des informations et la supervision.

| Discipline | Article correspondant | Description de la mesure | Fonctionnalité fournie par la plate-forme de Threat Intelligence / SOAR |
|---|---|---|---|
| Gestion des risques | Article 14 | Identification et évaluation des vulnérabilités, menaces et impacts sur les infrastructures critiques | • Identification et évaluation des risques<br>• Priorisation des mesures correctives |
| Notification des incidents | Article 15 | Notification des incidents ayant un impact significatif sur les infrastructures critiques | • Amélioration de la réponse à incident |
| Partage des informations | Article 16 | Partage des données de Threat Intelligence et des meilleures pratiques avec les autres entreprises | • Partage des données de Threat Intelligence |
| Supervision | Article 17 | Permettre aux autorités de contrôle de surveiller le niveau de sécurité des entreprises et de répondre aux risques émergents | • Surveillance de la sécurité |

ThreatQ est une plate-forme d'opérations de sécurité de pointe qui allie à la fois les fonctionnalités d'une plate-forme de Threat Intelligence et d'une plate-forme SOAR (Security Orchestration, Automation and Response). Ensemble, ces fonctionnalités de cybersécurité sont à même d'aider les entreprises à mettre en œuvre les mesures décrites ci-dessus.

## 1. Gestion des risques (Article 14)

Une gestion efficace des risques est au cœur de la directive NIS2. Les plates-formes de Threat Intelligence peuvent jouer un rôle crucial à cet égard :

***Identification et évaluation des risques***
Les plates-formes de Threat Intelligence favorisent l'identification et l'évaluation des risques en fournissant aux entreprises des données de Threat Intelligence en temps réel. Elles agrègent des données provenant de diverses sources, notamment les flux open source de Threat Intelligence, les sources internes et les communautés de partage de données de Threat Intelligence à l'échelle mondiale. Cet ensemble de données extrêmement riche permet aux entreprises d'évaluer de façon exhaustive les vulnérabilités et menaces qui pèsent sur leurs infrastructures critiques.

***Priorisation des mesures correctives***
Toutes les menaces ne sont pas égales en termes de probabilité et d'impact. Pour prioriser la mise en œuvre des mesures correctives, les entreprises s'appuient sur les plates-formes de Threat Intelligence, qui offrent des renseignements sur la gravité des différentes menaces. Grâce à la plate-forme de Threat Intelligence, les équipes de sécurité peuvent déterminer les vulnérabilités qui requièrent une attention immédiate, pour une gestion des risques plus efficace et ciblée.

***Exemple représentatif***
Imaginons un opérateur de réseau électrique utilisant ThreatQ. La plate-forme collecte des données sur les nouvelles menaces qui pèsent sur le secteur de l'énergie, notamment des informations sur les vulnérabilités des systèmes critiques. Grâce à ThreatQ, l'opérateur identifie une menace grave susceptible de perturber la distribution d'énergie. Armé de ces informations, il peut prioriser l'application de correctifs et le renforcement des systèmes vulnérables afin de réduire efficacement les risques.

## 2. Notification des incidents (Article 15)

La notification des incidents est essentielle pour tenir les autorités informées des incidents de cybersécurité qui ont un impact sur les infrastructures critiques. Les plates-formes de Threat Intelligence et SOAR (Security Orchestration, Automation and Response) rationalisent le processus de notification des incidents :

***Amélioration de la réponse à incident***
Les plates-formes de Threat Intelligence améliorent la réponse à incident en offrant des données de Threat Intelligence en temps réel et en automatisant diverses tâches. Lorsqu'un incident de sécurité survient, la plate-forme de Threat Intelligence fournit aux analystes les informations les plus récentes sur les menaces, ce qui leur permet de prendre des décisions plus rapides et éclairées.

Les plates-formes SOAR facilitent les tâches telles que l'investigation des alertes, la collecte de preuves et la notification, permettant ainsi aux entreprises de notifier les incidents aux autorités compétentes de façon efficace et rapide.

***Exemple représentatif***
Imaginons une entreprise de télécommunications utilisant ThreatQ. En cas d'attaque par déni de service distribué (DDoS) ciblant son réseau, ThreatQ identifie immédiatement les vecteurs d'attaque et les systèmes affectés. La fonctionnalité d'automatisation de ThreatQ déclenche un plan de réponse à incident prédéfini, qui comprend la documentation de l'incident et la notification aux autorités réglementaires, conformément aux exigences de la directive NIS2.

## 3. Partage des informations (Article 16)

Le partage des données de Threat Intelligence et des meilleures pratiques est essentiel à une protection collective contre les cybermenaces. Les plates-formes de Threat Intelligence favorisent la collaboration :

***Partage des données de Threat Intelligence***
Les plates-formes de Threat Intelligence facilitent le partage des données de Threat Intelligence avec les autres entreprises, ce qui permet de rester plus aisément informé des dernières menaces. Les équipes de sécurité peuvent participer à des communautés de partage d'informations sur les menaces et partager leurs propres découvertes. Cette approche collective renforce la capacité de l'ensemble de l'écosystème à répondre efficacement à l'évolution des menaces.

***Exemple représentatif***
Imaginons un établissement financier utilisant ThreatQ. L'entreprise participe à un groupe de partage de données de Threat Intelligence dédié aux menaces ciblant le secteur financier. Lorsqu'elle découvre une nouvelle souche de logiciels malveillants affectant ses systèmes, ThreatQ lui permet de partager ces informations avec d'autres membres du groupe, aidant ainsi l'ensemble du secteur à renforcer ses défenses contre cette menace spécifique.

## 4. Supervision (Article 17)

Les autorités de contrôle jouent un rôle crucial en s'assurant que les entreprises se conforment à la directive NIS2. Les plates-formes de Threat Intelligence peuvent également les aider :

***Surveillance de la sécurité***
Les autorités de contrôle peuvent utiliser une plate-forme de Threat Intelligence pour surveiller la sécurité des entreprises. En intégrant la plate-forme, les autorités bénéficient d'une visibilité sur les fonctionnalités de Threat Intelligence, d'évaluation des risques et de réponse à incident de l'entreprise. Ces informations les aident à identifier et à répondre aux risques émergents affectant les infrastructures critiques.

***Exemple représentatif***
Un organisme public chargé de superviser le secteur des transports s'associe à des entreprises du secteur pour surveiller leurs efforts en matière de cybersécurité. En intégrant ThreatQ, cet organisme peut évaluer efficacement la capacité de chaque entreprise à faire face aux menaces susceptibles de perturber les services de transport. Il peut prodiguer des conseils et offrir un soutien en fonction des données de Threat Intelligence en temps réel, améliorant ainsi la résilience globale du secteur.

## Conclusion

La directive NIS2 présente un cadre complet pour renforcer la cybersécurité des infrastructures critiques. En tant que plate-forme de Threat Intelligence de pointe, ThreatQ est particulièrement bien placée pour aider les entreprises à répondre efficacement aux exigences de la directive.

Grâce à ThreatQ, les entreprises peuvent identifier et évaluer les risques, prioriser les mesures correctives, améliorer la notification des incidents, partager les données de Threat Intelligence et faciliter la supervision par les autorités. Ces fonctionnalités permettent non seulement de renforcer la cybersécurité, mais aussi de garantir la conformité à la directive NIS2, protégeant ainsi les infrastructures critiques contre les cybermenaces.

Dans le paysage numérique actuel, ThreatQ se révèle un outil essentiel pour les entreprises et les autorités qui s'efforcent de renforcer leur cyberrésilience et de respecter les normes fixées par la directive NIS2.

Pour de plus amples informations, y compris des recommandations d'établissements financiers partenaires de ThreatQuotient, contactez-nous à l'adresse **www.threatq.com/demo/**





**Sales@ThreatQ.com • + 1 703.574.9885**