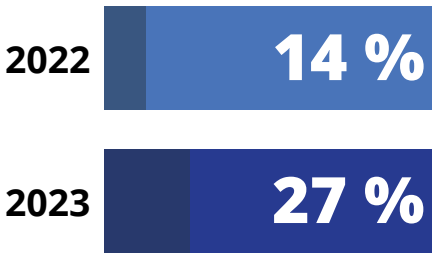
ThreatQ pour le secteur des transports

Le secteur des transports englobe le transport aérien, ferroviaire, maritime et routier, ainsi que l'entreposage. Tous partagent des éléments physiques et numériques, ce qui accroît leur vulnérabilité aux cyberattaques. Des systèmes essentiels, tels que les feux de signalisation et les tours de contrôle, sont très dépendants des technologies. Les cybercriminels ont recours à des tactiques telles que le phishing pour obtenir des données sensibles, à des malwares ou à des ransomwares pour perturber ou détruire des données, ainsi qu'à la compromission de systèmes cloud pour voler des informations.

Ils ciblent leurs victimes pour accéder à des informations sensibles telles que des données de carte de paiement, par le biais du phishing, voler des données ou mettre un système hors service par le biais de malwares ou de ransomwares et/ou obtenir un accès non autorisé à des données cloud entraînant des compromissions et des exfiltrations de données.

LES ESCROQUERIES PAR PHISHING ONT PRESQUE DOUBLÉ AU COURS DE L'ANNÉE ÉCOULÉE



Source : Travelers Risk Index[1]

PRINCIPAUX DÉFIS

Le secteur des transports est confronté à divers problèmes et considérations qui dépendent du mode de transport (aérien, ferroviaire, maritime, routier), ainsi que de la région ou du pays. Voici, pour chaque segment de ce secteur, les problèmes les plus couramment rencontrés, principalement dans le domaine de la cybersécurité :

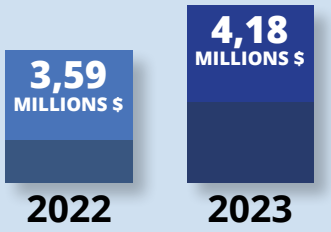
CONFORMITÉ RÉGLEMENTAIRE

Le secteur des transports est soumis à de nombreuses réglementations et normes qui varient selon les régions. Les entreprises doivent impérativement se conformer à ces réglementations, y compris celles relatives aux mesures de cybersécurité. Le respect des normes de cybersécurité assure la protection des données sensibles et des infrastructures critiques, ainsi que la résilience globale des systèmes de transport. Les programmes de formation et de sensibilisation à la cybersécurité sont indispensables pour prévenir les erreurs humaines à l'origine des compromissions de cybersécurité. Le recrutement et la fidélisation d'experts en cybersécurité qualifiés sont essentiels pour assurer la sécurité globale des services de transport.

AVANCÉES TECHNOLOGIQUES

La rapide intégration de technologies, telles que l'automatisation, l'intelligence artificielle et la numérisation, est à la fois source d'opportunités et de défis. Les sociétés de transport doivent s'adapter à ces innovations sans négliger pour autant les mesures de cybersécurité. La protection contre les cybermenaces potentielles est la clé pour préserver l'intégrité et la sécurité des technologies de transport avancées.

COÛT MOYEN D'UNE COMPROMISSION DE DONNÉES



Source : IBM[2]

Les signalements d'incidents de **ransomware**

PASSENT DE 13 %

du total en 2021
à 25 % en 2022[3]

Source : Infosecurity Magazine[3]

GESTION GLOBALE DE LA CHAÎNE LOGISTIQUE

Des événements tels que les catastrophes naturelles, les tensions géopolitiques ou les crises sanitaires mondiales peuvent perturber les chaînes logistiques et impacter la circulation des biens et des personnes. Des mesures de cybersécurité sont essentielles pour atténuer les risques de cyberattaques de systèmes logistiques interconnectés et assurer la sécurité et la continuité des opérations de transport.

Pour relever les défis du secteur des transports, une collaboration entre les gouvernements, les intervenants du secteur et des experts en cybersécurité est indispensable. Il convient d'intégrer la cybersécurité à tous les aspects des opérations de transport pour garantir la résilience et la fiabilité des systèmes de transport.

OPÉRATIONS DE SÉCURITÉ DE POINTE ORIENTÉES SUR LES DONNÉES

La plate-forme ThreatQ, qui sert de centre d'opérations de renseignement pour de nombreux secteurs, assemble et corrèle les données structurées et non structurées issues d'une multitude de sources, internes comme externes. Dans la mesure où tous les outils et technologies s'intègrent et fonctionnent en toute transparence avec l'architecture ouverte de ThreatQ, il n'est pas nécessaire de modifier l'infrastructure ou les workflows de sécurité existants. L'automatisation avec peu ou pas de code élimine les tâches répétitives et chronophages, permettant ainsi aux analystes de se concentrer sur des opérations prioritaires et stratégiques. La plate-forme permet en outre de partager rapidement des données de Threat Intelligence organisées, des conseils et des rapports avec un large éventail de parties prenantes internes et externes, y compris du secteur des transports.

PRINCIPAUX ATOUTS DE THREATQ :

- **CONSOLIDATION** au sein d'un référentiel central de données de Threat Intelligence et sur les vulnérabilités, tant les sources externes (p. ex. ISAC) qu'internes (p. ex. SIEM)
- **ÉLIMINATION** des nombreuses données parasites, pour mieux cibler les renseignements sur les menaces pertinents et se concentrer sur les ressources et les vulnérabilités critiques
- **PRIORISATION** des mesures et ressources primordiales pour l'environnement du secteur des transports
- **INTÉGRATION** des seuls indicateurs pertinents dans les stratégies de sécurité du secteur des transports
- **TRAQUE PROACTIVE** des activités malveillantes susceptibles de porter gravement atteinte aux sociétés de transport
- **PRIORISATION** des vulnérabilités de sécurité connues et exploitées de manière active, risquant d'affecter la conformité réglementaire
- **ANALYSE ACCÉLÉRÉE** permettant de contrer plus rapidement les attaques visant plusieurs cibles, y compris les dispositifs connectés au réseau
- **DIFFUSION AUTOMATIQUE** des données de Threat Intelligence vers les outils de détection et de réponse à incident

Sources :

1. **Travelers Risk Index :** https://investor.travelers.com/newsroom/press-releases/news-details/2023/Travelers-Risk-Index-Amid-Fluctuating-and-Emerging-Business-Risks-Cyber-Threats-Remain-a-Leading-Concern/default.aspx (2023)
2. **IBM Security, Cost of a Data Breach Report 2023 :** https://www.ibm.com/reports/threat-intelligence
3. **Infosecurity Magazine :** https://www.infosecurity-magazine.com/news/ransomware-double-europes/

Rendez-vous sur threatq.com/demo pour demander une démonstration en direct de la plate-forme ThreatQ et de ThreatQ TDR Orchestrator.

À PROPOS DE THREATQUOTIENT™

ThreatQuotient améliore les opérations de sécurité en regroupant des sources de données, des outils et des équipes hétérogènes afin d'accélérer la détection des menaces, les investigations et la réponse à incident. ThreatQ, la première plate-forme de Threat Intelligence orientée sur les données de ThreatQuotient, permet aux équipes de prioriser les menaces, d'automatiser les tâches et de collaborer pour résoudre les incidents de sécurité. Elle permet une prise de décision plus ciblée et optimise les ressources limitées en intégrant les processus et technologies existants à un espace de travail unifié. Résultat : une réduction des informations parasites, des menaces prioritaires claires et la possibilité d'automatiser les processus avec des données extrêmement fiables.

La boutique d'intégrations ainsi que les fonctionnalités de pointe en matière de gestion, d'orchestration et d'automatisation des données de ThreatQuotient prennent en charge de nombreux scénarios d'utilisation, notamment la gestion et le partage de Threat Intelligence, la réponse à incident, le Threat Hunting, la lutte contre le spear phishing, le tri des alertes et la gestion des vulnérabilités. ThreatQuotient est basé dans le nord de la Virginie, et possède des filiales chargées des opérations internationales en Europe, en Asie-Pacifique et dans la région Moyen-Orient/Afrique du Nord. Pour plus d'informations, consultez le site www.threatquotient.com.

THREATQUOTIENT™

20130 Lakeview Center Plaza, Suite 400 Ashburn, VA 20147, États-Unis • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885

TQ-IDB09-0324-01