ThreatQ pour le secteur de l'industrie

Le secteur de l'industrie englobe notamment l'approvisionnement en matières premières, les processus de production, le contrôle qualité et la distribution. Des machines, une main-d'œuvre qualifiée, des technologies et des chaînes logistiques sont nécessaires pour transformer les matières premières en produits finis. Ce secteur, qui inclut entre autres l'industrie automobile, électronique et textile, contribue de manière significative à la croissance économique mondiale.

Le secteur de l'industrie est confronté à différents défis et problèmes pouvant impacter ses performances et sa viabilité globales, notamment :

Perturbations de la chaîne logistique : des événements tels que les catastrophes naturelles, les conflits géopolitiques et les pandémies peuvent perturber l'ensemble de la chaîne logistique et affecter le respect des délais de livraison des matières premières et des composants.

Adoption et intégration technologiques : suivre le rythme effréné des évolutions technologiques — automatisation, intelligence artificielle, concept d'industrie 4.0 — est un défi de taille. Pour rester compétitifs, les fabricants doivent acquérir et intégrer ces technologies.

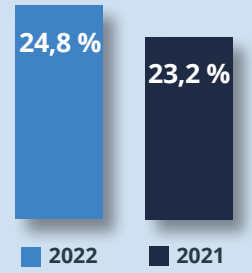
Cybermenaces : la connexion croissante des processus de fabrication par le biais de l'Internet des objets (IoT) et autres technologies numériques renforce la vulnérabilité du secteur aux cybermenaces. Il est indispensable de protéger les données sensibles et d'assurer la sécurité des systèmes interconnectés.

Gestion des coûts : la gestion des coûts de production, qui englobe le coût des matières premières, de l'énergie, de la main-d'œuvre et de l'efficacité opérationnelle, est un sujet de préoccupation constant.

PRINCIPAUX DÉFIS

Les fabricants doivent répondre à ces préoccupations de manière stratégique pour réussir à s'imposer dans le paysage dynamique de l'industrie. Implémenter une gestion robuste des risques, investir dans la technologie et l'innovation et promouvoir une main-d'œuvre qualifiée et adaptable sont les clés pour rester compétitif dans le secteur de l'industrie.

AUGMENTATION DU NOMBRE D'ATTAQUES PAR AN DANS LE SECTEUR DE L'INDUSTRIE



Source : IBM Security X-Force Threat Intelligence Index 2023[1]

Selon Statista, en 2022, près de

25 %

du nombre total de cyberattaques ont ciblé le secteur de l'industrie.

Source : Statista[2]

PERTURBATION DE LA CHAÎNE LOGISTIQUE

Les cyberattaques de la chaîne logistique ont pour objectif de manipuler les processus de fabrication d'une entreprise en interférant avec le matériel et les logiciels. Des logiciels malveillants peuvent être introduits à n'importe quel endroit de la chaîne logistique et potentiellement perturber ou interrompre les services de l'entreprise suite à cette cyberattaque.

RANSOMWARES

« Selon l'entreprise de cybersécurité Dragos[3], en 2022, le secteur de l'industrie a été victime d'au moins 437 attaques par ransomware, ce qui représente plus de 70 % de ces types d'attaques coûteuses et perturbatrices auxquelles les entreprises industrielles ont été exposées. »

L'un des problèmes rencontrés par les sites de fabrication est l'absence fréquente de visibilité des opérateurs sur leurs systèmes, auquel s'ajoute le partage d'identifiants sur les réseaux d'informations et les systèmes opérationnels.

Source : Dragos[3]

TECHNOLOGIES OBSOLÈTES

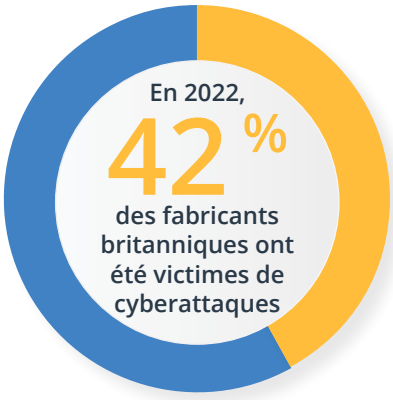
L'utilisation de technologies obsolètes, dépourvues des dernières fonctionnalités de sécurité, augmente le risque de compromissions. Ces systèmes, qui ne sont généralement plus pris en charge par les développeurs d'origine, ne disposent pas des correctifs et des mises à jour de sécurité essentiels. Alors que les cybercriminels ne cessent de trouver de nouveaux moyens pour accéder aux informations, l'utilisation de technologies obsolètes met en péril les données et peut également entraîner des dépenses supplémentaires en paiement de rançon ou perte de clients. Par conséquent, même s'il semble plus économique d'opter pour une ancienne technologie, les entreprises pourraient s'exposer à des risques significatifs et à des répercussions financières majeures.

Source : Infosec[4]

ESCROQUERIES PAR PHISHING

Des campagnes de phishing de grande envergure permettent aux cybercriminels de collecter diverses formes d'informations sensibles, y compris des coordonnées bancaires, des numéros de sécurité sociale et des données de carte de crédit/débit. Les cybercriminels peuvent également contraindre la victime à faire un virement sur leurs comptes bancaires. Le phishing peut avoir d'autres objectifs, notamment l'acquisition de données sensibles pour entacher la réputation de l'entité ciblée ou la distribution de logiciels malveillants pour semer le chaos sur les ressources physiques et les équipements de l'entreprise.

« Selon le rapport de NNT Security, au cours du deuxième trimestre 2017, 58 % des malwares ciblant le secteur de l'industrie ont été distribués par le biais de téléchargements sur Internet, soit par des chevaux de Troie, soit par des injecteurs. La reconnaissance, qui consiste à collecter les vulnérabilités de l'ordinateur de la victime une fois celui-ci piraté par le cybercriminel, a représenté 33 % des cyberattaques ciblant le secteur. » Infosec[4]



Source : BlackBerry[5]

ÉTENDUE DES DOMMAGES

« Selon une nouvelle étude réalisée en Grande-Bretagne par The Manufacturers' Organization et BlackBerry, 42 % des fabricants du pays ont été victimes de cyberattaques au cours des 12 derniers mois. Encore plus inquiétant, un quart (26 %) d'entre eux ont subi des "pertes financières substantielles" résultant de ces attaques, comprises entre 62 000 et 310 000 dollars (soit entre 50 000 et 250 000 livres).

65 % des entreprises victimes d'une cyberattaque ayant abouti ont signalé des interruptions d'activité. Dans ce cas, les pertes sont bien supérieures. L'étude révèle également que 43 % des entreprises indiquent que l'attaque dont elles ont été victimes a porté préjudice à leur réputation, impactant leurs relations actuelles et les ventes futures. » BlackBerry[5]

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 forme 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 de l'industrie.

PRINCIPAUX ATOUTS DE THREATQ :

- **CONSOLIDATION** au sein d'un référentiel central de données de Threat Intelligence et sur les vulnérabilités, tant externes (p. ex. ME-ISAC) qu'internes (p. ex. SIEM)
- **AUTOMATISATION** des actions d'enrichissement en masse, notamment la mise en corrélation de données, l'établissement de relations et l'ajout d'attributs et d'éléments contextuels supplémentaires afin de mieux comprendre les menaces et d'analyser les tendances
- **ÉLIMINATION** des nombreuses données parasites, pour mieux cibler les renseignements sur les menaces pertinents et se concentrer sur les ressources et les vulnérabilités critiques
- **ATTRIBUTION D'UN SCORE** aux sources de Threat Intelligence et de gestion automatique des dates d'expiration en fonction de exigences afin de produire des renseignements extrêmement fiables
- **PRIORISATION** des données primordiales pour les différentes parties prenantes et redéfinition automatique des priorités à mesure que de nouvelles données et de nouveaux enseignements sont disponibles
- **INTÉGRATION** aux outils et aux sources de Threat Intelligence existants par le biais d'une bibliothèque complète d'API et de connecteurs personnalisés
- **PARTAGE** des renseignements et réponse immédiate aux demandes de renseignements provenant du SOC et d'autres entités internes
- **ACCÉLÉRATION DE L'ANALYSE** des attaques et réduction du temps nécessaire à la création de rapports (de plusieurs jours à quelques heures)

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

Sources :

1. IBM Security X-Force Threat Intelligence Index 2023 : https://www.ibm.com/reports/threat-intelligence
2. Statista : https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/
3. Dragos : https://cyberscoop.com/ransomware-manufacturing-dragos/
4. Infosec : https://resources.infosecinstitute.com/topics/phishing/phishing-attacks-manufacturing-industry/
5. BlackBerry : https://blogs.blackberry.com/en/2023/01/manufacturing-and-cyberattacks-new-research

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 et la réponse à incident. La plate-forme d'opérations de sécurité 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 dans 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. Les fonctionnalités de pointe en matière de gestion, orchestration et automatisation des données de ThreatQuotient prennent en charge de nombreux scénarios d'utilisation, notamment la réponse à incident, le Threat Hunting, la lutte contre le spear phishing, le tri des alertes et la priorisation des vulnérabilités. Par ailleurs, elles peuvent également servir de plate-forme de Threat Intelligence. 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.

TQ-IDB10-0324-01

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