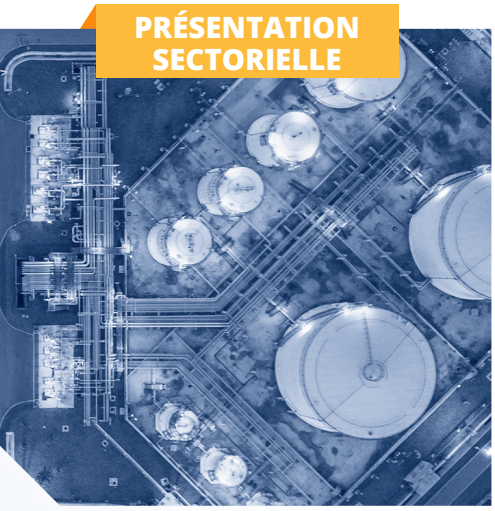
PRÉSENTATION SECTORIELLE



ThreatQ™ pour les infrastructures critiques

À travers le monde, les pirates informatiques s'attaquent inlassablement aux infrastructures critiques.

À travers le monde, les pirates informatiques s'attaquent inlassablement aux infrastructures critiques, mettant en danger les systèmes de contrôle industriel (SCI) et les systèmes de commande et d'acquisition de données de surveillance (Supervisory Control and Data Acquisition, SCADA) sous-jacents. En 2010, le ver Stuxnet a mis à mal le système iranien d'énergie nucléaire en infiltrant ses systèmes SCADA. Cinq ans plus tard, le logiciel malveillant BlackEnergy est entré dans l'histoire en Ukraine, avec la première cyberattaque ayant provoqué une panne générale des centrales électriques d'un pays. En 2017, une vague d'attaques imputables aux ransomwares WannaCry et NotPetya a fait des ravages.

En 2018, US-CERT a émis une alerte en conjonction avec le Centre national de cybersécurité du Royaume-Uni (NCSC, National Cyber Security Centre) et le FBI pour signaler que le gouvernement russe avait mené une attaque ciblant les infrastructures critiques dans toute une série de secteurs[1]. En 2020, alors que les acteurs malveillants continuaient à affiner leurs compétences et à étendre la portée de leurs attaques, US-CERT a mis en garde les entreprises contre des menaces dangereuses et imminentes[2] ciblant les 16 secteurs d'infrastructures critiques, et leur a recommandé de prendre certaines mesures pour s'en protéger, telles que comprendre et évaluer les risques en mettant en corrélation les données sur les menaces issues de diverses sources avec les informations contextuelles sur leur environnement. Cette mise en garde a été suivie par un avertissement plus précis[3] au sujet d'acteurs malveillants exploitant activement les vulnérabilités de systèmes d'ancienne génération dans les infrastructures exposées à Internet afin d'accéder aux systèmes, ainsi que par une alerte signalant une compromission de la chaîne logistique[4] qui permettait aux auteurs de menaces persistances avancées d'accéder à un large éventail d'infrastructures critiques et qui employait des techniques la rendant difficile à neutraliser.

Plus de la **moitié** des responsables IT dans l'industrie du pétrole et du gaz interrogés par EY affirment que l'intégration de technologies d'ancienne génération représente un défi majeur[6].

58 % des entreprises interrogées déclarent que le recrutement de personnel de cybersécurité ayant les compétences adéquates pour les SCI est un défi majeur[7].

64 % des professionnels des infrastructures critiques affirment que les attaques sophistiquées représentent un défi majeur[8].

PRINCIPAUX DÉFIS

RESSOURCES

D'après une étude d'(ISC)[2], il manque plus de 3 millions de professionnels de la cybersécurité dans le monde et 56 % des personnes interrogées estiment que leur entreprise est exposée à un risque moyen à extrême de cyberattaque à cause de ces postes non pourvus[5]. Souvent, les équipes de sécurité en fonction croulent sous les alertes et ne sont pas suffisamment représentées au niveau de la direction pour que leurs initiatives importantes bénéficient de la visibilité et du soutien qu'elles méritent. Pour optimiser les ressources dont elles disposent, les équipes de sécurité doivent comprendre et prioriser les données sur les menaces et les alertes dans le contexte de leur entreprise. Elles peuvent alors évoquer la sécurité sur cette base avec la direction exécutive, dans une perspective simple, claire et pertinente, et justifier la nécessité de ressources supplémentaires pour renforcer la sécurité.

PAYSAGE DES MENACES

Les attaques multivectorielles sont de plus en plus fréquentes. Or, il est plus difficile de s'en prémunir. L'alerte d'US-CERT évoquée ci-dessus énumérait une longue liste de tactiques, techniques et procédures utilisées, parmi lesquelles les e-mails de spear phishing, les attaques de point d'eau (watering-hole), la collecte d'informations d'identification et le ciblage spécifique d'infrastructures SCI et SCADA. On observe également une augmentation de la surface d'attaque, car nombre de fournisseurs d'infrastructures critiques transfèrent à présent leurs opérations dans le cloud et adoptent des dispositifs mobiles et connectés à l'Internet des objets (IoT), tout en continuant à prendre en charge des technologies d'ancienne génération. Plus de la moitié des responsables IT dans l'industrie du pétrole et du gaz affirment par exemple que l'intégration de technologies d'ancienne génération représente un défi majeur[6]. Pour protéger leur environnement numérique contre les menaces, les entreprises ont besoin d'une visibilité sur l'ensemble de leur infrastructure et doivent pouvoir réévaluer en permanence leur connaissance des menaces pour revoir leur priorisation.

INFRASTRUCTURES OBSOLÈTES

De nombreux systèmes SCI et SCADA sont installés depuis de longues années et n'offrent pas la sécurité requise pour lutter contre les menaces modernes. Le nombre de vulnérabilités détectées dans des systèmes SCADA ne cesse d'augmenter, mais ces systèmes sont rarement mis à jour, car les opérateurs craignent que cela n'entraîne des perturbations. Malgré la multiplication des attaques ciblant les infrastructures critiques, la protection n'a pas été consolidée. En réalité, elle s'est même affaiblie à mesure que la connectivité des dispositifs et des systèmes à Internet s'est répandue, sans que les risques de sécurité y afférents soient pleinement pris en considération. Même si leurs objectifs, leurs processus, leurs outils et leurs langages sont différents, les acteurs des technologies de l'information et des technologies opérationnelles (OT) doivent prendre conscience que leurs environnements convergent peu à peu et trouver une formule pour collaborer.

AMÉLIORATION DE LA PROTECTION DES INFRASTRUCTURES CRITIQUES

Plus de 75 % des entreprises sondées considèrent qu'il est très probable, ou au moins relativement probable, qu'elles soient ciblées par une cyberattaque dans l'espace OT/SCI. Seules 23 % d'entre elles respectent les lignes directrices et réglementations obligatoires minimales de leur secteur ou des autorités en matière de cybersécurité des SCI[7].

Lorsque les médias consacrent leurs gros titres à une attaque d'infrastructures critiques, ils tombent rapidement dans le sensationnalisme. Au milieu de ces données parasites, il devient souvent difficile de déterminer les implications de la dernière cybercampagne en date à grande échelle pour son entreprise. Se contenter de mettre à jour les dispositifs SCI et SCADA ne suffit pas. Une plate-forme solide de Threat Intelligence est le seul moyen pour les entreprises de comprendre les menaces les plus pertinentes, d'y réagir et d'obtenir de meilleurs résultats, plus vite, avec leurs infrastructures et leurs équipes de sécurité existantes.

RATIONALISATION DES OPÉRATIONS DES INFRASTRUCTURES CRITIQUES

La plate-forme ThreatQ procure aux fournisseurs d'infrastructures critiques le contexte et la sécurité dont ils ont besoin pour prendre des décisions plus avisées, accélérer la détection et la réponse à incident, et favoriser l'apprentissage et la collaboration entre équipes pour assurer une amélioration continue. 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.

Principaux atouts de ThreatQ :

- **CONSOLIDATION** au sein d'un référentiel central de toutes les sources de renseignements sur les menaces et les vulnérabilités, tant externes (p. ex. OSINT) qu'internes (p. ex. SIEM)
- **ACQUISITION** d'une connaissance situationnelle de l'infrastructure complète (sur site, cloud, IoT, systèmes mobiles et d'ancienne génération) par l'intégration des renseignements sur les vulnérabilités et les menaces dans le contexte des menaces actives
- **ÉLIMINATION** des nombreuses données parasites et de la désensibilisation aux alertes due à la lassitude, 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 votre environnement et redéfinition automatique des priorités à mesure que de nouvelles données et de nouveaux enseignements sont disponibles
- **TRAQUE PROACTIVE** des activités malveillantes pouvant indiquer des attaques par déni de service ou d'autres perturbations susceptibles de nuire aux clients, aux collaborateurs et aux parties prenantes
- **OBSERVATION** dépassant la protection pour inclure la détection, la réponse à incident et la reprise sur sinistre
- **ANALYSE ET RÉPONSE ACCÉLÉRÉES** permettant de contrer les attaques par une analyse collaborative des menaces, permettant une compréhension commune et une réaction coordonnée
- **DIFFUSION AUTOMATIQUE** des données pertinentes de Threat Intelligence vers les outils de détection et de réponse à incident

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

Références

1. CISA (Cybersecurity and Infrastructure Security Agency), « Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors », 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A
2. CISA (Cybersecurity and Infrastructure Security Agency), « NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems », 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-205a
3. CISA (Cybersecurity and Infrastructure Security Agency), « APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations », 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-283a
4. CISA (Cybersecurity and Infrastructure Security Agency), « Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations », 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-352a
5. (ISC)², « Cybersecurity Workforce Study », 2020, https://www.isc2.org/Research/Workforce-Study#
6. EY, « EY Oil and Gas Digital Transformation Workforce Survey », juillet 2020, https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/oil-and-gas/ey-oil-and-gas-digital-transformation-and-the-workforce-survey-complete-results.pdf
7. Wolfgang Schwab, Mathieu Poujol, « The State of Industrial Cybersecurity 2018 », 2018, https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf
8. Homeland Security Today, « 54 Percent in Utility Sector Expect Cyber Attack on Critical Infrastructure in Next Year », 2019, https://www.hstoday.us/subject-matter-areas/infrastructure-security/54-percent-in-utility-sector-expect-cyber-attack-on-critical-infrastructure-in-next-year/

ThreatQuotient s'est donné pour mission d'améliorer l'efficacité des opérations de sécurité à l'aide d'une plate-forme entièrement axée sur les menaces. En intégrant les technologies et les processus existants d'une entreprise dans une architecture de sécurité unique, ThreatQuotient accélère et simplifie les investigations et la collaboration, non seulement au sein des équipes mais également entre les outils. Grâce à l'automatisation, la priorisation et la visualisation, les solutions ThreatQuotient réduisent le bruit et mettent en évidence les menaces prioritaires afin de permettre aux ressources souvent limitées de se concentrer sur les événements à haut risque et de prendre des décisions avisées. 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, Inc.