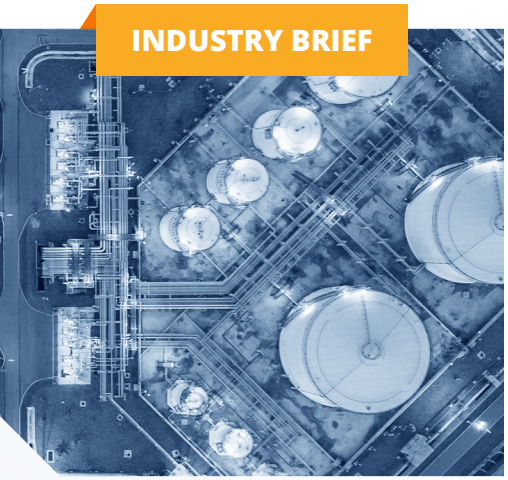
INDUSTRY BRIEF



ThreatQ™ for Critical Infrastructure

Hackers are relentlessly targeting critical infrastructure around the world.

Hackers are relentlessly targeting critical infrastructure around the world, compromising industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems that run such infrastructure. In 2010, the Stuxnet worm infiltrated SCADA systems, damaging Iran's nuclear power system. Five years later, the Ukraine BlackEnergy Power Grid hack left its mark as the first cyberattack to bring down a power grid, followed by the WannaCry ransomware outbreak in 2017 and NotPetya — a significant escalation in destructive exploits and damage.

In 2018, US-CERT issued a joint alert with the UK's National Cyber Security Centre (NCSC) and the FBI, warning that the Russian Government had carried out an attack targeting critical infrastructure across a wide swath of sectors.[1] As threat actors continued to hone their skills and widened their targets, in 2020 US-CERT warned of serious and imminent threats[2] to all 16 critical infrastructure sectors and provided a recommended set of actions including understanding and evaluating risk by correlating threat data from various sources with context about an organization's environment. The alert was followed by a more specific warning[3] of threat actors actively leveraging legacy vulnerabilities in internet-facing infrastructure to gain access to systems, and an alert of a supply chain compromise[4] that enabled an APT actor to gain access to a wide swath of critical infrastructure entities and whose complex tradecraft will make the actor challenging to remove.

More than **half** of oil and gas IT managers surveyed by EY say that integrating legacy technologies from different eras is a major challenge.[6]

58% of companies surveyed say that hiring ICS cybersecurity employees with the right skills is a major challenge.[7]

64% of critical infrastructure professionals say sophisticated attacks are a top challenge.[8]

KEY CHALLENGES

RESOURCES

Research by (ISC)[2] finds the worldwide shortage of cybersecurity professionals is over 3 million with 56% of respondents saying their companies are at a moderate or extreme risk of cybersecurity attacks as a result.[5] The security teams that are in place tend to be overwhelmed by a flood of alerts and often don't have adequate representation at the C-level to gain visibility and support for important initiatives. To optimize the resources they do have, security teams need a way to understand and prioritize threat data and alerts within the context of their organization. This will also enable teams to discuss security in a simple, clear and relevant way to executive leadership and justify additional resources to improve security operations.

THREAT LANDSCAPE

Multi-vector attacks are on the rise and are more difficult to protect against. The US-CERT alert mentioned above cited a variety of tactics, techniques and procedures (TTPs) used, including spear phishing emails, watering-hole domains, credential gathering and specific targeting of ICSs and SCADA infrastructure. The attack surface is also increasing because critical infrastructure providers are rapidly moving to the cloud and adopting mobile and Internet of Things (IoT) devices while still supporting legacy technologies. For example, more than half of oil and gas IT managers say that integrating legacy technologies from different eras is a major challenge.[6] In order to protect their digital landscape against threats, organizations need visibility across the entire infrastructure and must be able to continuously re-evaluate and reprioritize threat intelligence.

OUTDATED INFRASTRUCTURE

Many ICSs and SCADA systems have been in place for years and lack the security necessary to deal with modern threats. The number of vulnerabilities disclosed in SCADA systems keep increasing. However these systems are seldom updated because operators fear causing disruption. Despite increased attacks targeting critical infrastructure, protection has not increased and, in fact, is more tenuous as Internet connectivity across devices and systems proliferates without fully considering its security. Although they have different goals, processes, tools and languages, Information Technology and Operational Technology (OT) personnel need a way to collaborate as their environments begin to converge.

INCREASING PROTECTION OF CRITICAL INFRASTRUCTURES

Over 75% of companies surveyed state that it is very likely or at least quite likely to become a target of a cybersecurity attack in the OT/ICS space. Yet only 23% are compliant with minimal mandatory industry or government guidance and regulations around cybersecurity of ICSs.[7]

When news of an attack to critical infrastructure makes the headlines, it quickly becomes sensationalized. It is often difficult to sift through the noise and determine what the latest, large-scale cyber campaign means to the organization. Simply updating ICS and SCADA devices is not enough. A robust threat intelligence platform enables organizations to understand and act upon the most relevant threats and achieve more, faster with existing security infrastructure and people.

BRINGING ORDER TO CRITICAL INFRASTRUCTURE OPERATIONS

The ThreatQ platform gives critical infrastructure providers the context and security they need to make better decisions, accelerate detection and response, and advance team collaboration and learning for continuous improvement. There's no need to alter existing security infrastructure or workflows; all tools and technologies work seamlessly with ThreatQ's open architecture.

Achieve more with ThreatQ:

- **CONSOLIDATE** all sources of external (e.g., OSINT) and internal (e.g., SIEM) threat intelligence and vulnerability data in a central repository
- **GAIN** situational awareness of the entire infrastructure (on-premises, cloud, IoT, mobile and legacy systems) by integrating vulnerability data and threat intelligence in the context of active threats
- **ELIMINATE** noise and alert fatigue and easily navigate through vast amounts of threat data to focus on critical assets and vulnerabilities
- **PRIORITIZE** what matters most for your environment and reprioritize automatically as new data and learnings are available
- **PROACTIVELY HUNT** for malicious activity which may signal malicious activity, denial of service attacks and other disruptions and potential harm to customers, employees and constituents
- **FOCUS** beyond protection to include detection, response and recovery
- **ACCELERATE ANALYSIS** and response to attacks through collaborative threat analysis that enables shared understanding and coordinated response
- **AUTOMATICALLY** push relevant threat intelligence to detection and response tools

Request a live demo of the ThreatQ platform and ThreatQ Investigations at **threatq.com/demo.**

References

1. The 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. Cybersecurity & 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. Cybersecurity & 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. Cybersecurity & 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," July 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 mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, APAC and MENA. For more information, visit **www.threatquotient.com**.