# ThreatQ for Critical Infrastructure

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. As of November 2023, The UK's critical infrastructure sectors were facing a persistent and significant threat, partly due to the rise of state-aligned groups and an uptick in aggressive cyber activity, according to National Cyber Security Centre (NCSC). In May, the NCSC and international partner agencies issued a joint advisory highlighting how recent China state-sponsored activity had targeted critical infrastructure networks in the US and could be applied worldwide.[1] China is not the only one with cyber actors targeting critical infrastructure around the world. Both Russia and Iran have been identified as conducting malicious activities such as operating ransomware and 'ransomware as a service' models and targeted spear-phishing campaigns.

As threat actors continued to hone their skills and widen their targets, the 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 another 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.

**ATTACKS ON CRITICAL INFRASTRUCTURE**

Of the **2,825** ransomware attacks reported to the FBI last year, **1,193** hit critical infrastructure organizations in the United States.[5]

Across the world, there were **420 million** attacks on critical infrastructure between January and December 2023. That is a **30%** increase from 2022.[6]

## KEY CHALLENGES

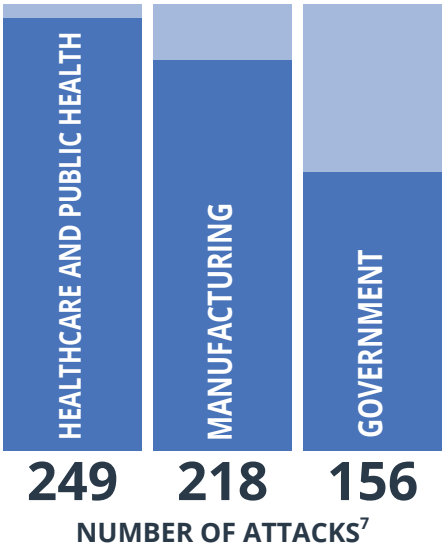
### RESOURCES

Research by Thales finds that the "human factor" is still considered the weakest link due to user error. The hybrid work model may be to blame, as the convergence of Information Technology (IT) and operational technology (OT) makes it easier for attackers to move laterally within organizations, turning IT problems into much more impactful OT system issues.[8]

Other issues include employee satisfaction and retention. 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.

**TOP 3 HARDEST HIT SECTORS BY RANSOMWARE ATTACKS IN 2023**




### 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 ICS 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.[9] 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 ICS and SCADA systems have been in place for years and lack the security necessary to deal with modern threats.

In more than half of OT/ICS incidents, SCADA systems are targeted at 53%, with PLCs (programmable logic controllers) as the next most common targeted at 22%.[10]

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 personnel need a way to collaborate as their environments begin to converge.

### INCREASING PROTECTION OF CRITICAL INFRASTRUCTURES

There were two pieces of legislation created to impact the manufacturing industry: The European Union Cyber Resilience Act and The U.S. Internet of Things Cybersecurity Improvement Act. Comprehending and adhering to the new standards will be essential for their business success.

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.

## CREATING A LEADING DATA-DRIVEN SECURITY OPERATIONS

The ThreatQ Platform gives Critical Infrastructure providers the context and security they need to make better decisions, accelerate threat 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 & internal threat intelligence and vulnerability data in a central repository.
- **ELIMINATE** noise and easily navigate through vast amounts of threat data to focus on critical assets and vulnerabilities.
- **PRIORITIZE** what matters most for your environment.
- **INTEGRATE** only relevant indicators into your security policies.
- **PROACTIVELY HUNT** for malicious activity which may signal malicious activity, denial of service attacks, other disruptions and potential harm to customers, employees and constituents.
- **FOCUS** on known security vulnerabilities in currently active exploits which may impact regulatory status and security posture.
- **ACCELERATE ANALYSIS** and response to attacks through collaborative threat analysis that enables shared understanding and coordinated response.
- **AUTOMATING** threat detection and response.

**Request a live demo of the ThreatQ Platform and ThreatQ TDR Orchestrator at www.threatq.com/demo.**

**Sources:**

1. NCSC, https://www.ncsc.gov.uk/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure#:~:text=The%20UK%27s%20cyber%20chief%20has,activity%2C%20and%20ongoing%20geopolitical%20challenges
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. Cybersecurity Dive, https://www.cybersecuritydive.com/news/ransomware-hitting-critical-infrastructure-fbi/709814/#:~:text=More%20than%202%20in%205,1%2C193%20hit%20critical%20infrastructure%20organizations.
6. Security Today, https://securitytoday.com/articles/2024/01/29/world-critical-infrastructure-suffered-13-cyber-attacks-every-second-in-2023.aspx
7. FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
8. Thales, 2022 Thales Data Threat Report, Critical Infrastructure Edition, https://cpl.thalesgroup.com/critical-infrastructure-data-threat-report#download-popup
9. 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-oiland-gas-digital-transformationand-the-workforce-surveycomplete-results.pdf
10. Forbes, https://www.forbes.com/sites/forbestechcouncil/2024/02/08/how-to-address-ot-and-ics-cyberattack-vulnerabilities/

### ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection, investigation and response (TDIR). ThreatQ is the first purpose-built, data-driven threat intelligence platform that helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading integration marketplace, data management, orchestration and automation (SOAR) capabilities support multiple use cases including threat intelligence management and sharing, incident response, threat hunting, spear phishing, alert triage and vulnerability management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.

TQ-IDB04-0624-03

THREATQUOTIENT™

20130 Lakeview Center Plaza, Suite 400 Ashburn, VA 20147
www.threatq.com | sales@threatq.com | +1 (703) 574-9885