

# THREATQ FOR GOVERNMENT AGENCIES

International government agencies serve as the backbone of our societal infrastructure, entrusted with safeguarding sensitive data and facilitating seamless operations across various sectors. However, this pivotal role also makes them prime targets for a myriad of threats ranging from cybercriminals to politically motivated entities and even state-sponsored actors from abroad.

Among the key challenges they confront are ransomware attacks, which can cripple operations and hold vital data hostage, denying access until exorbitant demands are met. Denial-of-service (DoS) attacks pose another formidable threat, disrupting services and causing widespread chaos by overwhelming systems with malicious traffic. Moreover, the integrity of critical national infrastructure hangs in the balance, as adversaries seek to exploit vulnerabilities and undermine the very foundations of societal functioning. As governments strive to uphold security and stability in the digital age, safeguarding against these multifaceted threats emerges as an urgent imperative.

## KEY CHALLENGES

### Ransomware

Ransomware is and remains the greatest threat<sup>1</sup>. These cyber attacks against government agencies happen for many reasons. Breached confidential information could mean leaked personal information from public records. Using old and outdated security software could result in catastrophe for public led services, processes and operations. While governments that are forced to pay a ransom could wind up losing trust from their citizens.

The French government is ramping up cyber defences after experiencing ransomware attacks. In December 2022, A cyber attack at a hospital in Versailles caused major damage and led to operations being cancelled and some patients being transferred to other locations.<sup>3</sup>

### Denial-of-Service

Attacks through denial-of-service operations. According to Spiceworks, A hacker group called Anonymous Sudan, which has long been considered pro-Russia, has claimed responsibility for the attacks, which were denial-of-service operations that occur by flooding a website with data to overwhelm its operational capacity.<sup>4</sup> The group has already attacked several targets in 2023, including the Israeli Prime Minister and the Swedish SAS Airlines.

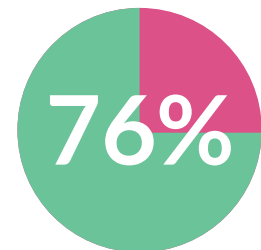
In March 2023, France's National Assembly website was hit with a distributed denial-of-service attack claimed by pro-Russian hackers.<sup>5</sup>

Computer attacks for extortion purposes also remained at a high level in 2023, as evidenced by the total number of ransomware attacks reported to ANSSI, which was 30% higher than over the same period in 2022. This

## HIGH LEVEL OF ATTACKS IN 2023



Computer attacks for extortion purposes also remained at a high level in 2023 as reported to ANSSI.<sup>2</sup>



76% of ransomware attacks on government institutions in 2023 were successful.<sup>1</sup>

A global study across 14 countries highlights that ransomware attacks on state and local governments have increased from **58%** to **69%** year over year.<sup>1</sup>

upsurge breaks with the decrease observed by the Agency in the previous Cyber Threat Overview.<sup>2</sup>

### Protecting Critical National Infrastructure

Critical National Infrastructure depends on a secure government network. Without the proper cyber defence plan put into place, this sector could face many potential threats.

The UK energy sector faces an expanding OT threat landscape: With the increase in attacks on the energy sector and the impact of the war in Ukraine on this sector, the need to collaborate on intelligence may be essential.<sup>6</sup>

After uncovering a potential cyber attack on countless Internet servers, the Federal Office for Information Security (BSI) asked IT managers to take countermeasures. In an official security warning, the BSI spoke of a “critical backdoor” in the Linux operating system that had to be closed.<sup>7</sup>

### RESOLUTIONS

Multiple international government agencies have put into place some strategic objectives:

DORA	NIS2	NCA
<a href="https://www.digital-operational-resilience-act.com/">https://www.digital-operational-resilience-act.com/</a>	<a href="https://digital-strategy.ec.europa.eu/en/policies/nis2-directive">https://digital-strategy.ec.europa.eu/en/policies/nis2-directive</a>	<a href="https://nca.gov.sa/en/news?item=1073">https://nca.gov.sa/en/news?item=1073</a>
<a href="https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en">https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en</a>	<a href="https://advisense.com/2024/02/15/introduction-of-nis-2/">https://advisense.com/2024/02/15/introduction-of-nis-2/</a>	<a href="https://nca.gov.sa/en/news?item=1054">https://nca.gov.sa/en/news?item=1054</a>

### CREATING A LEADING THREAT INTELLIGENCE OPERATION

A robust threat intelligence platform gives international government agencies the prioritization, contextual awareness and real-time insight necessary to accelerate detection, collaborate on response, accelerate recovery and achieve a rapid response. The ThreatQ Platform fully integrates with already-in-place threat feeds and SIEM systems to maximize existing resources – staff and technology. With ThreatQ, security staff gain the ability to prioritize vulnerability mitigation by addressing vulnerabilities in relation to currently active exploits.

### ACHIEVE MORE WITH THREATQ:

- ✓ **CONSOLIDATION** all sources of external (e.g., DHS-AIS, OSINT feeds) and internal (e.g., SIEM) threat intelligence and vulnerability data in a central repository.
- ✓ **ACHIEVE** situational awareness of the entire infrastructure (on-premises, cloud, IoT, mobile and legacy systems) by integrating vulnerability data and threat intelligence in context of active threats.
- ✓ **ELIMINATE** alert fatigue by providing context and prioritization to threat intelligence.
- ✓ **PRIORITIZE** response for government agencies by cutting through the noise and focusing on what matters most to government agencies.
- ✓ **PROACTIVELY HUNT** for malicious activity which may cause significant harm to constituent records.
- ✓ **FOCUS** beyond protection to include detection, response and recovery.
- ✓ **ACCELERATE ANALYSIS AND RESPONSE** to attacks through collaborative threat analysis that accelerates understanding, facilitates multi-agency interaction and dramatically improves response.
- ✓ **AUTOMATICALLY** push relevant threat intelligence to detection and response tools.

1. ProLion - <https://prolion.com/blog/ransomware-government/#:~:text=Ransomware%20Attacks%20on%20Governments%20Are%20on%20the%20Rise,-ln%20the%20U.S.&text=But%20it's%20not%20just%20the,to%2069%25%20year%20over%20year.>

2. République Française - <https://cyber.gouv.fr/en/actualites/anssi-publishes-2023-cyber-threat-overview>

3. TECHERATI - <https://www.techerati.com/news-hub/french-government-departments-hit-by-unprecedented-cyberattacks/>

4. Spiceworks - <https://www.spiceworks.com/it-security/cyber-risk-management/news/massive-cyberattack-targets-french-government-services/>

5. Politico - <https://www.politico.eu/article/french-national-assembly-website-russian-cyberattack-hack-kremlin-emmanuel-macron/>

6. SecurityIntelligence - <https://securityintelligence.com/articles/uk-energy-expanding-ot-threat-landscape/>

7. GERMANY & WORLD - <https://www.saechische.de/deutschland-welt>

8. Federal Office of Information Security - [https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht\\_node.html](https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html)

#### ABOUT THREATQUOTIENT, A SECURONIX COMPANY

ThreatQuotient transforms security operations by unifying data, tools, and teams for faster threat detection, investigation, and response. Their platform enhances threat intelligence, streamlines workflows, and automates processes with high-quality data—maximizing efficiency and precision. Integrate seamlessly, reduce noise, and focus on real threats. Learn more: [www.threatq.com](http://www.threatq.com).