THREATQUOTIENT™

ThreatQ for U.S. Government Agencies

We all rely on our government agency computer systems for vital services and information. As government agencies are considered critical infrastructure, they are under constant attack from hackers, political activists and foreign state-sponsored actors. To illustrate this, one of the most public and potentially damaging breaches of record is the foreign adversary attack against the Federal Office of Personnel Management (OPM) resulting in exfiltration of over 20 million sensitive personnel records.[1]

The rate of attack is increasing and, unfortunately, government cyber defense is not keeping pace, particularly in the area of situational awareness. As the Office of Management and Budget (OMB) has stated in a past report, "The lack of threat information results in ineffective allocation of agencies' limited cyber resources." The report further indicates that situational awareness among federal agencies is so limited that 38% of the time, agencies could not identify the method of attack or the attack vector that compromised information or system functionality.[2] The first step to detecting, responding and recovering from incidents is finding a way to increase situational awareness.

As of July 2023, Biden-Harris Administration announced that eighteen agencies are leading initiatives in this whole-of-government plan demonstrating the Administration's deep commitment to a more resilient, equitable, and defensible cyberspace.[3] The National Cybersecurity Strategy Implementation Plan (NCSIP) to ensure transparency and a continued path for coordination. This plan details more than 65 high-impact Federal initiatives detailed in a 5 pillar plan.[4]

38%
of the time
federal agencies could not identify the method of attack or attack vector[2]

KEY CHALLENGES

RESOURCES

One of the most significant risk areas identified by federal government agency internal assessments is internal resources – people, technology and funding. These resource limitations lead OMB to assert that agencies "do not have the resources to combat the current threat environment."[3] Unfortunately, the prospect of significant hiring to augment this resource shortage is bleak, given a widening skills gap with currently 13,000 unfilled public-sector cybersecurity positions.[4]

Government IT and security teams are doing their best to establish situational awareness by combining raw threat feeds with existing security information and event management (SIEM) and log management tools. However, this approach fails to achieve this objective and ultimately drives up alert fatigue for an already overwhelmed staff. Eliminating alert fatigue and accelerating situational awareness requires prioritized, contextually relevant, real-time threat intelligence that seamlessly integrates with existing tools and practices. A threat intelligence platform (TIP) facilitates this integration. The result is the optimization of limited resources.

The number of cyber incidents on federal systems reported to DHS increased more than ten-fold between 2006 and 2015[5]

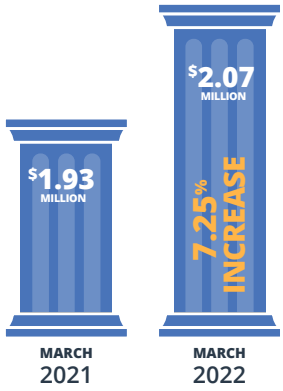
A recent report produced by AI-based cybersecurity company CloudSek shows cyberattacks against governments jumped 95% in the last half of 2022.[5]

In 2022 there was an increase in so-called hacktivist activity -- hacking for political purposes -- which accounted for about 9% of the recorded incidents reported in the government sector. Ransomware groups accounted for 6% of the total incidents reported. LockBit was the most prominent ransomware operator, the report noted.

Government agencies face the continual challenge of balancing access and transparency against protecting constituents' sensitive information. Doing this requires a level of openness that makes it impossible to prevent all intrusions. Complicating matters, most of the emphasis to date for government security has been on preventive tools, techniques and procedures. To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties.[6]

THREAT LANDSCAPE:
Government agencies are facing an ever-expanding threat landscape driven by two factors. First, the abundance of legacy IT provides a broad target for malicious actors due to the persistence of unpatched, unprotected and even unsupported operating systems and applications. Second, government agencies are moving to the cloud and adopting mobile and Internet of Things (IoT)[7] devices at an accelerating rate. These technologies are critical to delivering new levels of government service and constituent responsiveness, but at the same time, they significantly increase the government agency attack surface. Maintaining current visibility into the entire infrastructure and continually re-evaluating and reprioritizing threat intelligence helps government agencies protect an expanding digital world against a growing threat landscape.

AVERAGE COST OF A BREACH IN THE PUBLIC SECTOR



Meanwhile, the average total cost of a breach in the public sector increased from $1.93M to $2.07M

A 7.25% INCREASE

between March 2021 and March 2022 -- according to IBM.

CREATING A LEADING THREAT INTELLIGENCE OPERATION

A recent White House briefing released by the Biden Harris administration shows the National Cybersecurity Strategy (NCS) pillars[8] and strategic objectives are designed to detail more than 65 high-impact Federal initiatives, from protecting American jobs by combatting cybercrimes to building a skilled cyber workforce equipped to excel in our increasingly digital economy. A robust threat intelligence platform gives government agencies the prioritization, contextual awareness and real-time insight necessary to accelerate detection, collaborate on response, accelerate recovery and achieve a rapid response. ThreatQ 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:

- **CONSOLIDATE** all (structured or unstructured) sources of external (e.g., DHS-AIS, and OSINT feeds) and internal (e.g., SIEM) threat intelligence and vulnerability data.
- **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.

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

1. https://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/index.html
2. Executive Order 13800 - Federal Cybersecurity Risk Determination Report and Action Plan," Office of Management and Budget (OMB), May 2018.
3. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/
4. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
5. https://www.csoonline.com/article/574275/cyberattacks-against-governments-jumped-95-in-last-half-of-2022-cloudsek-says.html
6. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
7. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
8. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/

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.