WHITE PAPER

MANDIANT®
A FireEye® Company

How Government Agencies are Facing Cyber Security Challenges

FireEye

Introduction

The United States Federal Government relies heavily on information technology to drive efficiencies and increase citizen engagement. However, an uptick in cyber attacks and data breaches that affect government operations has created a perfect storm of risks and challenges. Cyber threats continue to have an outsized impact on department and agency operations, which can erode public trust and reduces the ability to deliver critical mission functions.

In response to destructive cyber attacks, data breaches, budget pressures and public expectations, the U.S. Government is changing how it addresses cyber threats and larger business risks. The government is now using four new strategies to secure its sensitive information and protect its vital infrastructure:

- Proactive cyber threat hunting[1]
- Increased use and sharing of cyber intelligence data[2]
- Continuous security monitoring, with an emphasis on boundary protection and security event lifecycle management[3]
- Automation and orchestration of security operations[4]

In 2017, increased investments were made by the U.S. Government to focus on implementing these innovative strategies to defend against and mitigate cyber attacks. It is anticipated that these investments will continue to increase in 2018 and beyond, as agencies continue to combat progressively sophisticated and pervasive adversaries.[5]

Based on government industry reports, public reports and FireEye's understanding of the current cyber threat landscape, this paper outlines the capabilities and processes government agencies need to develop enhanced cyber defense programs through the application of threat hunting, intelligence sharing, continuous program monitoring and deployed security orchestration. These programs assure the delivery of critical mission functions such as homeland security, law enforcement, health care and national defense.

Cyber Threat Hunting and Intelligence Sharing

The federal government is turning to cyber threat hunting as a proactive means of identifying dormant threats because traditional prevention and response measures are often ineffective against determined adversaries.[6] Mandiant, a FireEye company, has observed significant value and reduction in cyber risks from proactive threat hunting versus sifting through a wide range of time consuming data logs and feeds.

The ability to actively search endpoints and identify sophisticated threats is an ongoing process that requires advanced tools, technology and people to discover both the external origins of breaches and internal compromises of systems and data. Obtaining and maintaining full visibility of threat actors targeting a specific environment is important to enabling cyber threat hunting operations in complex settings. To ensure the appropriate amount of threat visibility is achieved for effective hunting operations within secure networks, Mandiant deems the establishment and maintenance of internal and external threat intelligence capabilities to be a best practice.

1 U.S. Department of the Interior Office of Inspector General (2017). Threat Hunting: A Proactive Technique for Finding Sophisticated Cyber Threats.
2 Richard Bejtlich, OP-ED (2015). Will Sharing Cyberthreat Information Help Protect the United States?
3 United States Federal Government. Department of Homeland Security (2018). Continuous Diagnostics and Mitigation (CDM).
4 FCW: The Business of Federal Technology (2018). Why DHS is changing the way agencies connect to the internet.
5 Whitehouse.gov (2018). CyberSecurity Funding.
6 U.S. Department of the Interior Office of Inspector General (2017). Threat Hunting: A Proactive Technique for Finding Sophisticated Cyber Threats.

For example, cross-agency Department of Defense cyber threat intelligence and information sharing had previously relied on basic functionality, often resulting in out-of-context or stale intelligence with indicators that were challenging to ingest and use in an automated manner. The level of effort required to consume, validate and apply shared indicators to existing processes made it very difficult for agencies to leverage shared threat data and perform real-time cyber operations.[7]

Intelligence gleaned from information sharing is now proactively incorporated into indicators of compromise (IOCs) to search for other signs of malicious activity, such as nefarious users who may be harvesting data and performing privilege escalation. Such activity likely stems from threats that have not been appropriately categorized or that include previously unknown malware. This gives analysts the ability to examine various system artifacts for IOCs linked to nation-state threat actors.

New hunting techniques include the use of advanced detection technology to search for specific IOCs and perform sweeps specifically associated with advanced threat actors targeting federal agencies. This technology allow analysts to examine various system artifacts for IOCs linked to nation-state, criminal, and other sophisticated threat actors. In addition to the automated IOC sweeps, analysts collect and analyze data using frequency of occurrence analysis to better discover anomalies that might have gone undetected with previous measures. This technique enables analysts to focus on finding deviations in the environment that IOCs did not detect.

Intelligence garnered from these hunting techniques is easily codified into the IOCs used to search for other signs of malicious activity, such as data harvesting and privilege escalation by unauthorized users. These techniques also enable proactive searching for other evidence of malicious activity such as non-targeted and commodity-based malware, which can often present damaging consequences (Fig. 1).

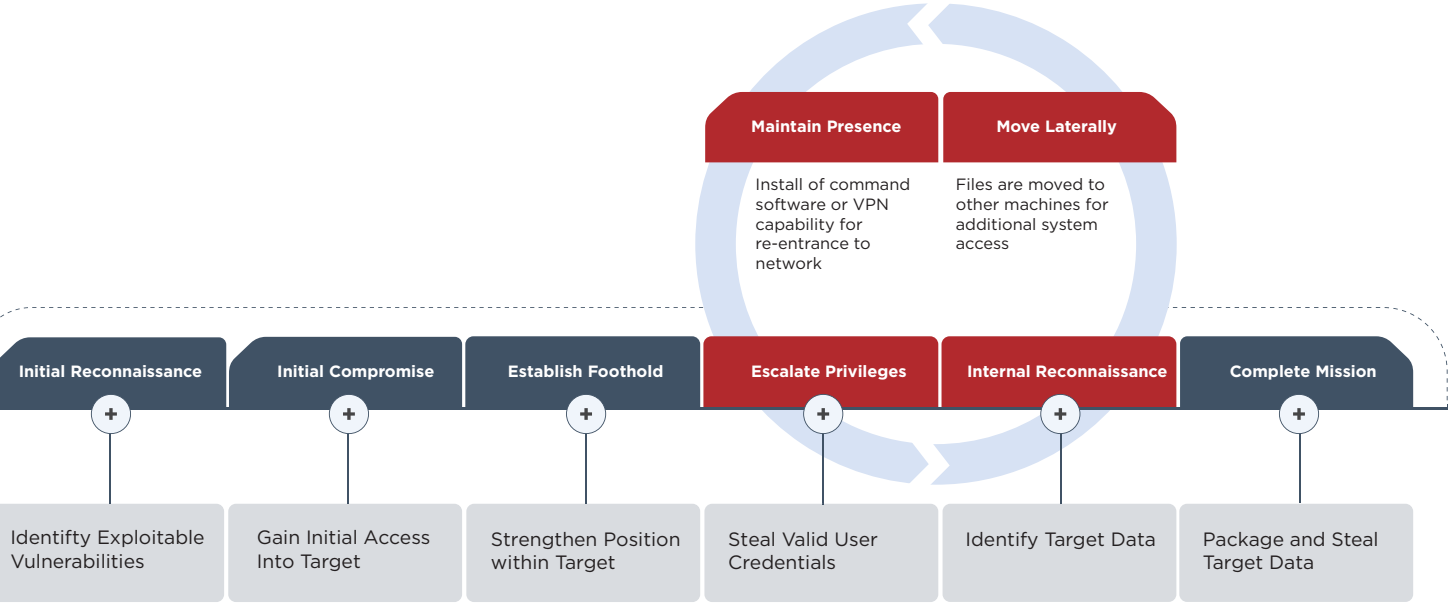

Figure 1. Attack lifecycle.

New hunting techniques include the use of advanced detection technology such as advanced network analysis sensors, advanced endpoint detection and response (EDR) tools, advanced data analytics, machine learning and artificial intelligence.

7 Richard Bejtlich, OP-ED (2015). Will Sharing Cyberthreat Information Help Protect the United States?

Continuous Management and Monitoring

In 2013, the Office of Management and Budget (OMB) created a sweeping cross-agency objective to enable continuous management and monitoring of all federal information technology systems.[8] This shift marked the initial acknowledgement of the shortfalls of a rigid, decade-old periodic assessment and authorization strategy hosted within a complex and interconnected information infrastructure. It also acknowledged the limitations of the government's ability to defend against the more significant threats arrayed against these systems. To support this widespread change in the government's approach to the protection of sensitive systems and data, the Department of Homeland Security (DHS) was authorized to create a new federal Continuous Diagnostics and Mitigation program (CDM).[9]

The CDM program enables government departments and agencies to expand their continuous monitoring and diagnostic capabilities by increasing their sensor capacity, automating data collection, and prioritizing risks. The program was designed to integrate commercial technology with government networks and systems. The first two program phases, which took place from 2013 through 2017, focused on the foundational capabilities of asset and vulnerability management as well as identity, credentialing and access management. Phase three, which began in 2017 and will continue for several years to come, is dedicated to boundary protection and event management (Fig. 2).[10]

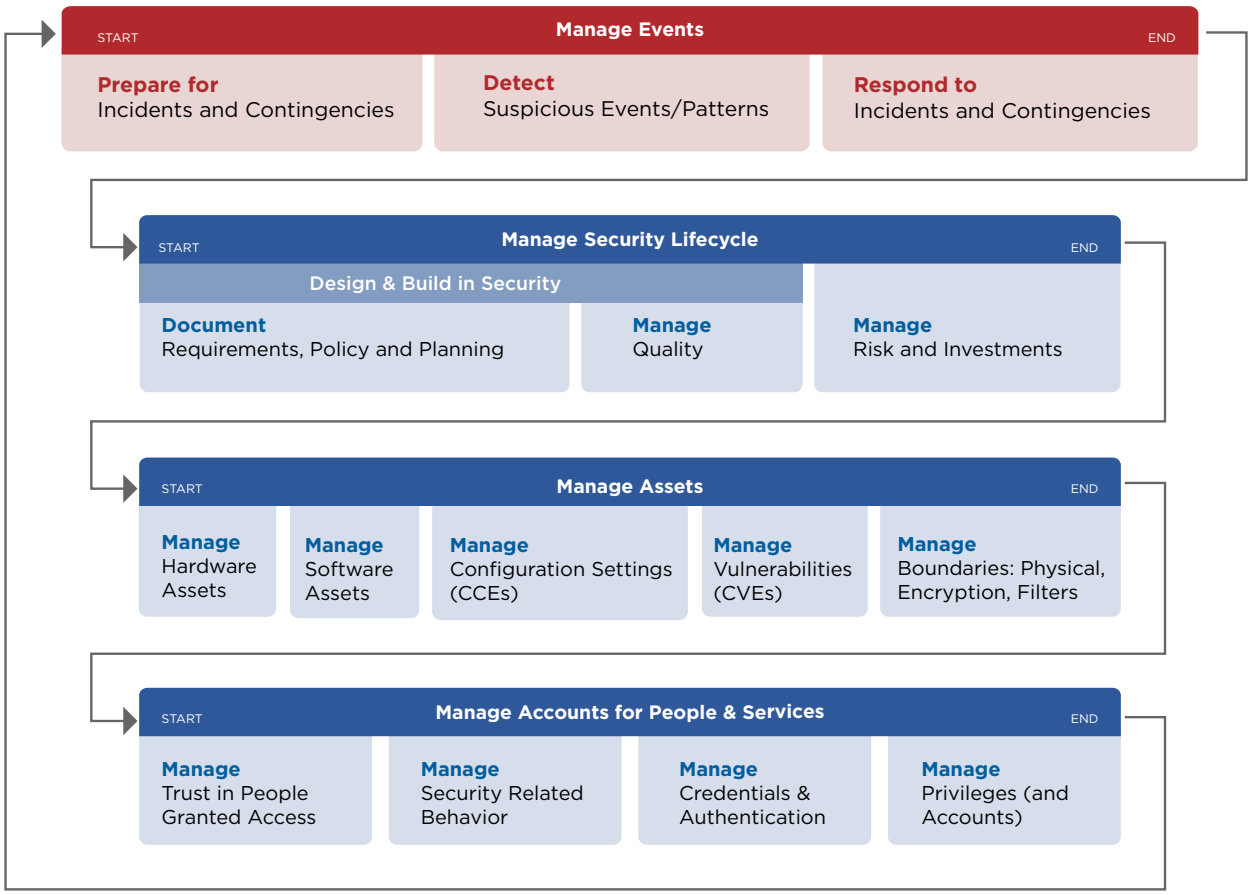

Figure 2. CDM program with phase three highlighted in red. Four areas of 15 capabilities must be applied to all assets.

8 United States Federal Government. Department of Homeland Security (2018). Continuous Diagnostics and Mitigation (CDM).
9 Ibid.
10 Ibid.

The NIST framework focuses on using business drivers to guide cyber security activities and considers cyber security risks as part of an organization's risk management process. This framework consists of three parts: the core, the implementation tiers and the profiles. The core is a set of cyber security activities, outcomes and informative references that are common across sectors and critical infrastructure.

Mandiant believes phase three of the CDM program will result in significant and rapid advances of security maturity — most notably accelerating capabilities aligned closely to the National Institute of Standards and Technology (NIST) cyber security framework in the incident response areas of detection, analysis, response, containment and recovery.

Phase three is challenged by the federal government's rapid adoption of cloud services. Government agencies are currently evaluating how the legacy Trusted Internet Connection framework adapts to newer network monitoring controls and requirements paired with constant governance changes and IT consolidation efforts. DHS and their technology partners are working closely with these agencies to address cloud-related operational challenges, which include visibility into cloud platforms and infrastructure as well as access to critical security event data for monitoring and response.[11]

Security Orchestration

Agencies that must defend the federal government's critical infrastructure with existing tools and capabilities face four major limitations:

- Lack of skilled staff to analyze the growing number of incidents
- Slow incident remediation time
- Error-prone and inconsistent manual remediation processes
- Inexperienced staff spending less time hunting for new threats and more time remediating false alerts

Security orchestration can help combat these limitations through the process of connecting security tools and integrating disparate security systems to drive automation and reduce human analysis and interactions. It requires that the organization have a mature security environment and appropriately classify actionable incidents.

Mature Security Environment

A mature security environment provides a holistic and accurate view of events that are occurring in the network at any given time, while limiting the amount of noise (false alerts). It lets analysts know what is on the network, controls access to it, and watches it. Its functions relate directly to the first two phases of the CDM program.

11 FCW: The Business of Federal Technology (2018). Why DHS is changing the way agencies connect to the internet.

Classification of Actionable Incidents

Orchestration can reduce the overall security workload for a very specific subset of cyber security challenges. It will not replace manual review of specific incidents that require closer analysis and instinct or human intuition. When incidents that should be analyzed manually are auto-remediated, the incident may not be successfully or fully resolved.

Before orchestration and automation protocols are implemented, incidents must first be categorized into one of two classes: an actionable event that can be automated or a non-actionable event that requires manual analysis. Event categorization requires the application of two criteria: reliability and confidence, and accepted risk of automated action.

Reliability and confidence is established when the type of incident, along with the totality of supporting logs and third-party intelligence, supports a single confirming story. The following example incident satisfies this criteria with extensively corroborated logs:

Network sensor detects hostile command and control communications from a target host.

Third-party threat feed provides reliable IOCs which would be found on the target host, if infected.

A host agent on the target machine detects external communication to the command and control system and leverages the third-party threat feed to determine the hostile process.

After an incident has been reliably detected, the accepted risk of automated action must be assessed based on the severity and impact of the incident, along with the possibility of the mitigation causing added harm. Potential mitigation actions can be as benign as notifying a system administrator, escalating to perimeter filtering or automatic isolation and reimaging of systems. Mandiant recommends common orchestration techniques to its clients, including government agency customers, such as alert enrichment, automatic blocking of high-confidence detected threats, spam or malware submission mailbox enrichment and ticket generation and prioritization.

Alert enrichment is supported by data such as reputational, domain and external intelligence.

Mailbox enrichment includes further sender details such as domain and header data.

Conclusion

Changes to the federal government's security program capabilities in 2017 are primary elements of a paradigm shift from a previously federated, decentralized and reactive cyber defense footing, to a consolidated, centralized and proactive approach to defending critical network infrastructure and cyber threat data. This represents a significant transformation in how departments and agencies at all levels are ensuring the security and operational readiness of their information networks.

FireEye anticipates that over time, these changes will result in amplified coverage of defensive capabilities and an improved ability to adapt and enhance those capabilities to meet the government's evolving threat landscape.

The benefits of proactive hunting and information sharing include a significant reduction in detection time, manpower and costs associated with the incident response process. Mandiant forensic investigations show that the most meaningful cyber security enhancements reported by the federal government are those which improve the speed of response and minimize the attack surface to reduce the overall risks and impacts of cyber attacks and data breaches.

Case studies and examples are drawn from our experiences and activities working for a variety of customers, and do not represent our work for any one customer or set of customers.

Learn more about Mandiant consulting services at **www.FireEye.com/services.html**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

FireEye®