DATA SHEET

Cyber Defense for Election Infrastructure

Preserve Vote Integrity

HIGHLIGHTS

- **Enhance Existing Investments:** Managed detection and response capabilities that can be integrated with any security operation center (SOC).
- **Full Team of Experts:** Thousands of threat analysts, malware experts, incident responders, intelligence curators and forensic experts.
- **Systematic Hunting:** Analysts proactively deploy proprietary threat hunting techniques using FireEye products and expertise.
- **Real-Time Visibility:** Customizable portal serves as a conduit for communication, reporting and collaboration, as well as provides insights into ongoing assessments and response to emerging threats via our community protection dashboards.
- **Market-Leading Threat Intelligence:** Security analysts apply the latest machine, victim and adversary intelligence to locate and detail threats in your environment faster.
- **Threat Assessment Manager:** Security experts to serve as your main point of contact to facilitate additional support such as analysis of malware samples, in-depth forensic analysis or onsite incident response.
- **24x7 Coverage:** SOCs in the United States (Virginia and California), Ireland, Germany, Singapore, Sydney and Japan provide 24x7 coverage.

Critical government networks, including election systems infrastructure, are under a constant state of attack. As threats evolve, nation states, cyber criminals and hacktivists stress government cyber defenses, especially during election years.

Voting systems must be monitored around the clock for election interference, with solutions that can quickly and confidently differentiate between legitimate activity, malicious threats and inadvertent errors. A trusted security partner offering the right mix of technology, intelligence and expertise can help secure the foundation of your democratic process.

FireEye recommends that state and local municipalities start with FireEye Managed Defense to establish the strongest possible foundation for election cyber security.

Intelligence-Led Detection and Response

FireEye Managed Defense is a managed detection and response (MDR) service that enhances overall security posture to defend the most vulnerable aspects of the voting process, including voter registration, polling place identification, ballot submission and vote counting. FireEye analysts use frontline intelligence and expertise to drive detection and to guide hunting and investigation activities to reveal even the most sophisticated attacker. This includes attacks that target or mimic state and local officials.

FireEye Managed Defense includes:

- Our proprietary technology stack to provide real-time enterprise-grade visibility across the network, including ICS and cloud infrastructure.
- Expert threat analysts who adversary, victim and machine-based threat intelligence to detect, investigate and proactively hunt for known and previously undetected threats.

After signs of compromise are confirmed, FireEye professionals contact the client to review findings via a secure portal while the investigation continues.

A detailed summary report provides threat context along with remediation recommendations so organizations can form an effective response that helps prevent attackers from completing their mission.

In addition to Managed Defense, which continuously reviews systems for evidence of compromise, FireEye offers email security for communications related to voting systems and processes.

Protection against Email Threats

Available as FireEye Government Email Threat Prevention (ETP) Service in the FedRAMP Marketplace, FireEye Email Security provides indispensable protection for the world's number one threat vector: email. ETP meets FedRAMP security requirements and has been granted an Authority to Operate (ATO) by the U.S. Department of the Interior (DOI). It is the first cloud email security service focused on advanced threat protection to be FedRAMP authorized.

Additional Services

Mandiant Incident Response Retainer (IRR)

IRR establishes terms and conditions for incident response services before a cyber security event occurs. An IRR keeps a trusted partner on standby to significantly reduce incident response time and minimize the overall impact of a breach.

Mandiant Red Team Assessment

Mandiant red teams conduct realistic cyber attack scenarios in your organization's environment over two weeks. After working with your organization to establish a set of jointly agreed upon objectives, the team uses numerous methods to imitate attacker behavior to achieve those objectives. This helps assess your organizational security and improve its efficiency and effectiveness.

Web Monitoring

FireEye experts provide personalized reconnaissance monitoring to help protect your brand, data and VIPs. Our monitoring services inform decision making at every level -tactical, operational and executive - by identifying instances of plans, breaches or exposures in the open, deep and dark web.

The Value of Managed Defense

Experience
100,000+ hours of incident response experience per year from the most impactful breaches

Intelligence
Access to nation-state grade intelligence supported by 150+ intelligence analysts

In-region Expertise
Seven global SOCs with in-region technical engagement managers available 24x7

Adaptive Detection
In-depth understanding of adversary TTPs to focus on detecting attacker methods and behaviors

Powerful Defense
Proprietary tech stack leveraging FireEye technologies and intelligence.

- 50 billion+ virtual machine analyses daily
- 400,000 unique malware samples processed everyday
- 16 million intelligence-gathering sensors worldwide
- Rich contextual intelligence to support sensor data
- FireEye ecosystem updated every 60 minutes

To learn more about FireEye, visit: **www.FireEye.com**

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 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.

FireEye