Security Connected
Solution Guide

Operationalize Intelligence-Driven Response

intel Security

Build a Resilient Cyberdefense

Intel Security delivers an integrated security system that empowers you to prevent and respond to emerging threats. We help you resolve more threats faster and with fewer resources through stronger protection, superior detection, and rapid correction. Our trusted on-premises and cloud-enabled solutions and services help secure your enterprise against advanced attacks. Our connected architecture and centralized management reduce complexity and improve operational efficiency across your entire security infrastructure. Intel Security is committed to being your number one security partner—providing a complete set of integrated security capabilities.

Download the latest resources at mcafee.com/securityconnected.

The cost of incident response increases the longer an attacker remains undiscovered. In the real world of budget constraints, resource efficiency measurements, and consolidation, nothing proves value like catching the bad guys.

Challenges

Government leaders know that if they want a resilient defense architecture, they need a response solution that actively roots out threat indicators—specifically, one with deep content visibility and correlated intelligence. Finding the advanced persistent threat (APT) and reducing the time to remediate requires a proactive, integrated approach. Intelligence-driven response incorporates speed, intelligence, and visibility.

The public sector is a target for malicious insiders, hacktivists, cybercriminals, and nation-states. These attackers often carry out long-term attacks that include targeting individuals, departments, or entire organizations; designing custom exploits; and using stealth to hide malware. Attacks are usually financially or politically motivated and can include sensitive data theft, extortion, and sabotage. The impact of such attacks can be devastating, leading to disrupted communications, failed campaigns, damaged or stolen assets, and even the loss of life.

Confronted with these challenges, the public sector needs to build a resilient cyberdefense architecture that provides mission assurance. Capabilities must include situational awareness for a real-time understanding of the existing threat posture, correlation of global and local intelligence that enriches decision-making capabilities, and actionable, prioritized incident response. This set of capabilities reduces the attack window and time to remediate.

Having a cyberdefense strategy with intelligence-driven response addresses several real-world challenges. Many organizations are being targeted by sophisticated attacks and don't even realize it until the damage is done. Many operations groups are inundated by so much data that they suffer from analysis paralysis and are unable to derive the actionable data needed to mount a timely response. Because of budget constraints, there is a growing need to reduce the impact that a security incident can have on the mission as well as the cost.

Security is no longer about point solutions solving point problems. Intelligence drives decisions, and that intelligence is based on an aggregation of multiple solutions. Disconnected security silos have no place in a robust decision framework where rapid threat intelligence acquisition and incident response are imperative.

The NATO Capability Framework

Communication and information systems (CIS) require security in the form of protecting the confidentiality, integrity, and availability of systems, as well as protecting information that is processed, stored, or transmitted. McAfee solutions map to multiple areas of the NATO Capability Framework to provide CIS security. McAfee offers specific and integrated solutions for key sections of the framework—including malicious activity detection, attack prevention and mitigation, dynamic risk assessment, visualization for situational awareness, timely decision making, attack recovery, and the management of cyberdefense information.[1]

Solutions

The answer is a connected security strategy that correlates information gleaned from endpoint, network, and data controls. With the Security Connected approach from McAfee, each security control improves the effectiveness of the others. In addition, a greater understanding of the assets needing protection in the form of continuous discovery ensures that the security controls are aligned with the reality of the operational environment. This level of deep insight is important for mitigating several attacks and is absolutely essential for mitigating stealth attacks that bypass traditional controls.

Resilient cyberdefense also requires a decision framework offering centralized intelligence exchange and workflow that can aid in discovery, prevention, detection, analysis, and response. Contextual awareness in the form of user identities, risk scores for assets, reputation information, and packet reconstruction yield previously unattainable results, such as prioritization for incident response. By operationalizing these fundamental systems and processes, speed and visibility can be greatly enhanced and intelligence-driven response becomes a reality. The high false positives and undetected attacks of the past are minimized. Thus detection rates increase and response times decrease.

There are three frameworks required for intelligence-driven response to be effective—decision, detection, and analysis.

Decision

The McAfee decision framework operates as a centralized command and control platform. It provides a connection between external threat intelligence feeds (providing global insights such as malicious IPs, files, emails, and URLs) and local intelligence.

Local intelligence consists of discovered assets, known vulnerabilities, active attacks, and even existing security countermeasures. Beyond intelligence, the decision framework acts as a central point to aggregate and correlate solutions for endpoint, network, and data security.

Detection

The McAfee detection framework is made up of security controls for endpoints, network, and data. These solutions provide preventative controls—and assist with incident detection by providing deep visibility and intelligent analysis of the inspected traffic. This combination is important for mitigating stealth malware. The detection framework is closely aligned with incident response and can detect suspicious activity and communicate with the decision framework to perform impact assessments and mount a response based on the most timely, relevant, correlated data.

Analysis

The McAfee analysis framework provides the deepest level of visibility into network traffic and data. It should be used to address the most sophisticated attacks. It is quite common today for an adversary to disguise malicious code within legitimate data that is processed by legitimate applications. The intelligence gained from full packet inspection coupled with code analysis is necessary to obtain an actionable response to a suspicious, yet well-disguised, file. Once a suspicious indicator is discovered, the depth and breadth of the multiple framework capabilities will result in a determination of the scope of the intrusion and reduction in incident response time.

Best Practices Considerations

- Scale to support the environments that public sector organizations operate—millions of endpoints and high-bandwidth networks.
- Centralize the decision framework.
- Feed the decision framework with local risk information and global threat intelligence.
- Demand the ability to use a combined framework to support rapid response.
- Augment real-time threat mitigation with forensic analysis capabilities.
- Reduce the time needed to find, fix, and remediate attacks.
- Lower costs associated with threat acquisition, indecent response, and incident impact.

The detection framework requires the ability to record network activity to improve situational awareness of advanced threats and data exfiltration and to augment forensic analysis. It also needs to be able to detect zero-day malware in order to provide the enhanced intrusion detection capabilities that public sector organizations require when combating today's threats.

Value Drivers

Solutions for intelligence-driven response need to provide enriched and empirical security controls, but they also need to reduce complexity and maximize return on investment. These solutions should:

- Centralize the command platform to minimize time and human resource requirements.
- Facilitate more rapid threat acquisition, thus reducing the threat window and incident impact.
- Generate contextually relevant alerts to provide more exacting and timely incident response.
- Minimize false positives and correctly prioritize critical events to focus time and resources more accurately.

For more information about Security Connected, visit: www.mcafee.com/securityconnected.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

1. http://en.wikipedia.org/wiki/NATO_Architecture_Framework