Threat Management Lifecycle Services

Proactively manage the cyber threat landscape

Empower your security organization to identify and understand unknown, hidden threats to your business. With advanced persistent threats (APTs) manifesting more and more frequently alongside the massive damage we see inflicted, we can no longer just react to incidents. Proactivity is the most promising way forward.

Benefits

- Early threat detection and situational awareness.
- Scalable, efficient threat management.
- Continuously refining threat detection and response capability.
- Provide a 360° view of active threats in the network.
- Leverage the power of the Intel Security Labs Cloud to provide telemetry and indicators of compromise (IoCs).
- Receive meaningful, contextual intelligence from our CTI Service.
- Techniques used in Threat Content Engineering (McAfee ePO dashboards, control configuration, rapid triage, etc.).
- Leverage Active Response where McAfee ePolicy Orchestrator® (McAfee ePO™) software is present and requirements are met.

Modern attacks are sophisticated and covert, conducted by criminals or nation states bent on stealing valuable data (or in some cases, total destruction of data) from targeted companies. Intrusions typically target end users via phishing campaigns or via weakly secured applications and infrastructure. Once in, they gain access to the environment to steal trade secrets, intellectual property, financials, computer source code, and any other valuable information.

Intel® Security Threat Management Lifecycle services encompass a set of proactive activities to:

- Understand the threat landscape and how it relates to you and your vertical or region.
- Discover threats in the environment that have been previously undetected.
- Enable rapid triage of threats to improve automation and efficiency.
- Capture lessons learned from hunting activities and threat intelligence to fine-tune controls for better detection and response.

McAfee Labs Support

Whether your company is global or regional, our Foundstone® Services team leverages a wealth of intelligence from our McAfee® Labs commercial and consumer malware monitoring of over ~500,000 malware events per day. This deep-dive into malware gives us a unique perspective of the threats and variances inside organizations, verticals, and regions.

Contextual Threat Intelligence

Our Open Source Contextual Threat Intelligence has over a decade of data to give our forensic analysts and incident response handlers the ability to conduct exhaustive online presence reporting. This can result in the identification of the responsible adversaries and provide context to the indicators of attack that may exist in your environment.

Threat Hunting

Our Foundstone consultants use endpoint management solution data, log data, and captures of network traffic to identify behavior indicative of beacon or command-and-control traffic. Once suspicious systems are identified, artifacts are collected to forensically analyze what is causing the anomalous behavior. This is a comprehensive approach to identifying outlier behavior and possibly undetected threats.

intel Security

Key Outcomes

- Improved situational awareness of emerging malware threats.
- Improved detection of anomalous events that involve domains, address space, or malware hashes.
- Increased assurance that undesirable activity goes unnoticed.
- Predictive telemetry that could indicate the intent of an attack before it happens.
- Trend identification to help prepare for possible attacks.

Approach

Strategically-placed sensors and probes provide real-time information about the emergence and propagation of both malware and vulnerabilities. Through automated analysis of collected samples, we provide the unique ability to intelligently assess the potential impact to your organization. The real-time tracking of domains and networks where threats are launched and hosted provides insight and predictive telemetry for emerging threat detection. Combine these items with human intellectual analysis of the real threats and risks targeting your organization, and your lines of efforts find greater prioritization and effectiveness. Our analysts correlate the information from the network to the endpoint and determine likely candidates of advanced threats in your network.

We start by setting up a network monitoring system with a customized set of threat feeds and alert feeds. This is matched against a threat scan of your endpoints with our custom rules. The combination gives us the ability to find sleeping and active threats in your environment allowing us to actively discover and monitor for potential incidents.

During initial setup, you provide the following information to our consultants:

- Relevant high-level network design for determining the placement of custom sensors or PCAPS of your network traffic, if adding sensors is not available.
- Relevant endpoint distribution mechanisms and malware removal tools.
- Relevant security information and event management (SIEM) and active response tools, if available.

Deployment Options

Full Access: The Foundstone team ships and configures a network probe to capture and analyze live traffic leaving the organization to the internet. We also ship and set up a second server that sits in the LAN and that is used for hunting indicators of compromise, triage, collecting, and analyzing artifacts of interest. This is the preferred setup that allows for 'live' traffic analysis, better correlation, and faster reaction to any threats detected in your network.

Limited Access: Client sets up the network probes and collect the network traffic using your own hardware. Traffic captures are collected during different periods of time and are shared with Foundstone consultants for offline analysis. The Foundstone team ships and sets up a second server that sits in the LAN and is used for hunting indicators of compromise, triage, and collecting and analyzing artifacts of interest. This setup is intended for environments where our consultants cannot deploy their own network probes, yet it's possible to deploy a server in the LAN.

Restricted Access: No Foundstone servers or probes are deployed on the network. Client sets up the network probes and capture the traffic using your own hardware. Traffic captures are collected during different periods of time and are shared with Foundstone team for offline analysis. Our consultants can share some tools and scripts for you to run in your environment to do a restricted hunt for indicators of compromise, triage, and collection of artifacts.

Threat Hunting	Restricted	Limited	Full Access
Live Network Analysis (based on provided information)			X
Static Network Analysis	X	X	
Network Threats Report	X	X	X
McAfee ePO Threats Dashboard (if available)	X	X	X
Endpoint Threat Report	X	X	X
Advanced Threat Assessment		X	X
Continuous Monitoring Dashboards for SIEM (based on provided information)		X	X
Remote Malware Analysis	X	X	X

Table 1. Threat hunting service options.

Related Services

We offer many related services and classes including:

- Custom Open Source Intelligence Research
- DDoS Defense Assessments
- IR Program Development
- Policy and Procedure Definition Review
- IR GAP Analysis
- Investigative Services
- Digital Forensics
- Emergency Incident Response
- Advanced Malware Analysis
- Expert Testimony
- Malware Forensics and Incident Response (MFIRE) Class
- Contextual Threat Intelligence Services

Threat Content Engineering

Our Foundstone consultants leverage several decades of experience using open source and Intel Security tools (including McAfee ePO software, McAfee SIEM solutions, and McAfee Intrusion Prevention System), with network monitoring and log analysis to gain the ability to peer into your systems and build reports and dashboards that help you proactively and rapidly find anomalies, and measure your success in protecting your environment.

The Intel Security Difference

All of our Foundstone Services projects are managed using our proven Security Engagement Process (SEP) for project management. A pivotal aspect of this process is continual communication with your organization to ensure the success of your consulting engagements.

Learn More about Foundstone Services

Fill the gaps in your information security program with trusted advice from the Foundstone Services team—a global organization that provides security consulting, customized product deployments, and training and advisory services. Let our consultants help your organization assess current policies, create new programs that meet compliance goals, and cost-effectively prepare for security emergencies. Speak with your technology advisor about integrating our services or email us at **Foundstone@intel.com**. You can get more information at **www.foundstone.com**.

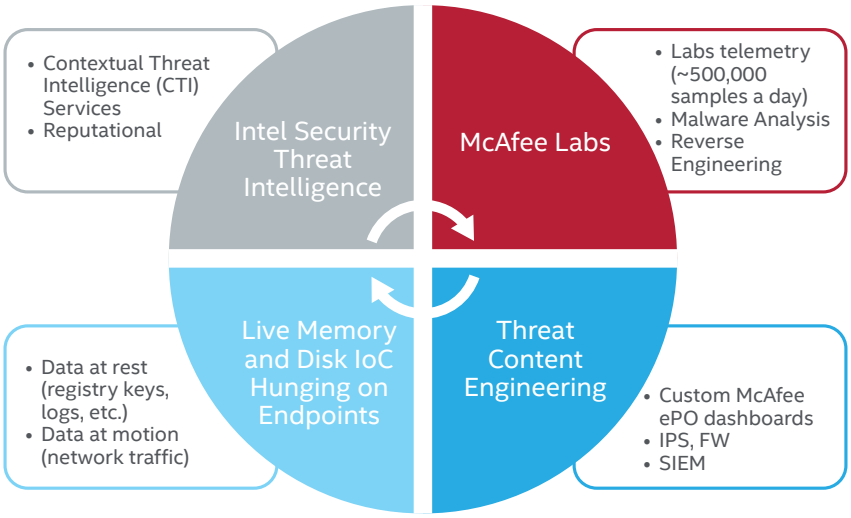

Figure 1. Threat identification and discovery assessment components.

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