Foundstone Contextual Threat Intelligence

Get a handle on the rapidly evolving threat landscape

Empower your organization through a comprehensive understanding of the rapidly evolving threat landscape globally, regionally, and in your specific market vertical.

24/7 Coverage

- Crawling internet segments leveraging sentiment-based tracking, where attackers congregate in underground discussion forums, chat rooms, and on social media

Sensor Network

- Real-time information about the emergence and propagation of both malware and vulnerabilities

Real-Time Tracking

- Domains and networks from which threats are launched and hosted provide insight and predictive detection

Situational Awareness

- Reporting on the threat landscape in your vertical/region
- Includes the trends of attacks and vulnerabilities that put your organization at risk

Modern cybercrime has changed, and threat actors have adopted a multifaceted approach to put your organization at risk. Foundstone® Services provides complete coverage by proactively and forensically monitoring the threat vectors cybercriminals use. Foundstone Contextual Threat Intelligence Services provides 24/7 coverage, operating intelligent robots that crawl the darkest segments of the internet, where attackers congregate in underground discussion forums, chat rooms, and on social media.

Strategically placed sensors and probes provide real-time information about the emergence and propagation of both malware and vulnerabilities.

Foundstone Contextual Threat Intelligence Services provide flexible and customizable real-time reporting of incidents involving your network, brand, or intellectual property. These alerts can be integrated into existing enterprise security products to potentially block attacks before they happen.

Benefits

- Early threat detection and situational awareness
- Ability to leverage existing security products to act on threat intelligence
- Intellectual property and brand reputation monitoring
- Unparalleled access to intelligence on threat actors
- Intelligence Partner integration

Contextual Insight

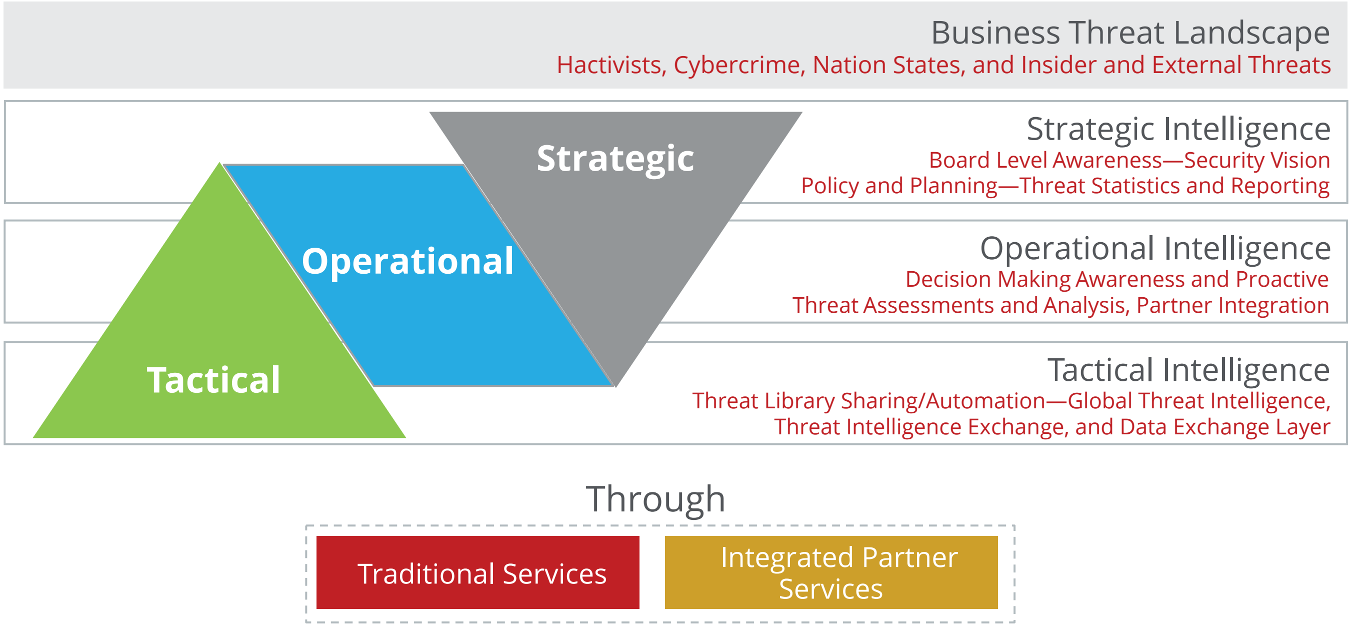
We leverage our wealth of intelligence to correlate data on your specific market vertical. The power of threat intelligence comes from making strategic security decisions to protect your organization before an incident occurs.

Already Been Attacked?

Foundstone Open Source Contextual Threat Intelligence Services has more than 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 cybercriminals.

Your Region, Your Risk

Whether your company is global or regional, the Foundstone Services team provides situational awareness reporting on the threat landscape in your region or your vertical, including the trends of attacks and vulnerabilities that put your organization at risk. Reporting can be customized based on your specific requirements.



Business Threat Landscape
Hactivists, Cybercrime, Nation States, and Insider and External Threats

Strategic Intelligence
Board Level Awareness—Security Vision
Policy and Planning—Threat Statistics and Reporting

Operational Intelligence
Decision Making Awareness and Proactive
Threat Assessments and Analysis, Partner Integration

Tactical Intelligence
Threat Library Sharing/Automation—Global Threat Intelligence,
Threat Intelligence Exchange, and Data Exchange Layer

Through

Traditional Services

Integrated Partner Services

Figure 1. Complete Intelligence Coverage.

Related Services

We offer many related services and training classes including:

- Open Source Intelligence Investigations
- DDoS Defense Assessments
- IR Program Development
- IR 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
- Targeted Malware Threat Analysis Comprehensive Infrastructure and Network Assessment

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. Additionally, 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 effort find greater prioritization and effectiveness. It's about preventing an attacker's actions by understanding what the attacker is looking for, as well as their motivations and intentions.

We start by setting up a profile in its contextual threat intelligence system. This is matched against the threats that the center is currently discovering and monitoring to watch for potential incidents. With this intelligence, customers are better informed and kept up to date on the latest threats with respect to industry vertical and country of presence. During the initial setup, you provide the following information to our consultants:

- Relevant IP-addresses/ASN numbers
- Relevant websites/URLs
- Relevant keywords and identifying intellectual data
- Contact email addresses

Our team provides situational awareness reporting on the threat landscape in your region and industry vertical, including the trends of attacks and vulnerabilities that put your organization at risk. This reporting can also be customized based on specific requirements.

Benefits

- Improved situational awareness of emerging malware threats
- Improved detection of anomalous events that involve domains, address space, or intellectual property
- 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

The Foundstone Difference

All Foundstone 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 Foundstone Services—part of the McAfee® global professional services 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. You can get more information at www.foundstone.com.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com