Partner Data Sheet

Industry

SIEM

Website

www.intelsecurity.com

Company Overview

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world.

Product Overview

McAfee Enterprise Security Manager delivers a real-time understanding of the world outside—threat data, reputation feeds, and vulnerability status—as well as a view of the systems, data, risks, and activities inside your enterprise.

Solution Highlights

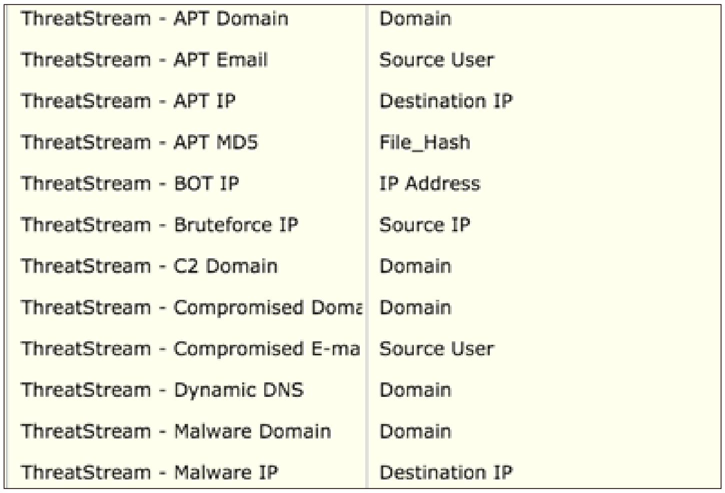
- Delivers performance
- Actionable intelligence
- Real-time situational awareness required understand and respond to stealthy threats
- Embedded compliance framework simplifies compliance

Next Generation Security Solutions

The threat landscape is continually expanding and organizations are under continuous attack and overwhelmed with alerts. Thousands of incidents occur each day and security professionals only have time to deal with dozens. This creates operational chaos. Security teams need next-generation security solutions to help them respond faster, defend proactively and invest smarter.

Just-in-Time Intelligence

The Anomali content for McAfee ESM adds real-time threat intelligence to data logged in your McAfee ESM deployment. Threat intelligence is continuously gathered, categorized and risk ranked (for severity and confidence) in Anomali's ThreatStream platform. It is then delivered in real-time to your Anomali content McAfee ESM for monitoring and detection of security threats in your enterprise infrastructure for the SOC and threat intelligence teams to quickly see high priority threats to your business. The intelligence is based on common industry-accepted Indicators of Compromise (IOC) such as source and destination IP addresses, email addresses, domains, URLs, and file hashes, but is enriched with factors such as risk score to add context and relevance to the delivered information.



ThreatStream - APT Domain	Domain
ThreatStream - APT Email	Source User
ThreatStream - APT IP	Destination IP
ThreatStream - APT MD5	File_Hash
ThreatStream - BOT IP	IP Address
ThreatStream - Bruteforce IP	Source IP
ThreatStream - C2 Domain	Domain
ThreatStream - Compromised Doma	Domain
ThreatStream - Compromised E-ma	Source User
ThreatStream - Dynamic DNS	Domain
ThreatStream - Malware Domain	Domain
ThreatStream - Malware IP	Destination IP

Benefits of Anomali

- Easy-to-use interface to view threat information received through STIX/TAXII feeds.
- Analyze and correlate data into actionable information: SIEM rules, reports, and dashboards.
- Pinpoint IOCs - quickly search for a specific indicator, search for an indicator type over a time range, and drill-down into details.
- Eliminate unnecessary, duplicative and irrelevant indicators - before they enter your infrastructure.
- Identify and prioritize the events that matter now - without DIY scripting.
- Machine-to-Machine learning algorithms scale to accommodate thousands of IOCs per minute across your environment.

Benefits of McAfee ESM

- Next Generation SIEM and Log Management
- Host Forensics and File Integrity Monitoring
- Network Forensics with Application ID and Full Packet Capture
- State-of-the art Machine Analytics
- Rapid, Intelligent Search
- Visibility. Know what's happening on every endpoint.
- Large data set analysis via visual analytics, pivot, and drill down

Benefits of the Joint Offering

McAfee ESM's collected security logs are correlated against rules provided by Anomali. The rules will match any outbound and inbound traffic to Anomali intelligence indicator types. The integration via Anomali's Anomali Link creates lists of IOCs that are retrieved by the McAfee ESM on a regular basis. Data is dynamically populated within a number of custom watchlists covering common indicators. New correlation rules built out within the McAfee ESM then trigger on a predetermined set of the most malicious attack types.

High Fidelity Threat Intelligence

Each individual indicator of compromise curated is categorized and risk ranked for severity and relevance using data analytics to identify relationships with known threats. A risk score is then assigned to each indicator before it is delivered to your security infrastructure.

Seamless and Automated

The Anomali content for McAfee ESM provides seamless and automated integration of indicator data, ensuring the delivery of real-time threat intelligence directly to your McAfee ESM. This ensures that you can start using consolidated and vetted threat feeds in meaningful ways more efficiently and effectively than ever before.

About Anomali

Anomali delivers earlier detection and identification of adversaries in your organizations network by making it possible to correlate tens of millions of threat indicators against your real time network activity logs and up to a year or more of forensic log data. Anomali's approach enables detection at every point along the kill chain, making it possible to mitigate threats before material damage to your organization has occurred.

About McAfee ESM

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world.

For more information contact Anomali sales at info@anomali.com