SOLUTION BRIEF

McAfee
Together is power.

Operationalizing Threat Intelligence

Behind just about every legitimate alert your IT security receives is an adversary using multiple attack techniques to penetrate your infrastructure and compromise your vital data assets or systems. Today's targeted multiphase attacks consist of a series of steps that make up the cyberattack chain: reconnaissance, scanning for vulnerabilities, exploitation, and, finally, exfiltration of valuable corporate data.

Security analysts are well aware of these techniques and depend on threat intelligence to glean insights into attack methods and motivations. They can detect and interrupt advanced threats, apply appropriate remediation, and be better prepared next time the security alarm sounds. But all too often, they either lack visibility into certain systems or are inundated with too much data and too little intelligence. According to the SANS Institute study, *Who's Using Cyberthreat Intelligence and How?*, "… only 11.9% of interviewees have achieved the ability to aggregate threat information from virtually every source, and only 8.8% have a full picture view that can combine events with IoCs."[1]

In a recent report, Forrester notes that 77% of North American and European enterprise security decision makers report that improving threat intelligence capabilities is a priority.[2] Cyberthreat intelligence promises to give security practitioners advance warning of cybercriminals targeting their region, industry, or even specific firms so that they have time to take action, but IT security still faces some big challenges:

- How to collect threat intelligence from external as well as internal sources.
- How to correlate the data and prioritize risks.
- How to distribute intelligence across multivendor security controls enterprise-wide.
- How to gain greater visibility into the IT landscape to enable appropriate and swift action.

Modern enterprises need an open, integrated architecture that eases the adoption of threat intelligence and enables them to reap its benefits—from basic threat data collection for forensics to using it to enrich security information and event management (SIEM) analytics. In other words, users need to put threat intelligence to work via automated processes that help analyze, digest, and manage it.

New Threats Call for a New Approach to Threat Intelligence

As attacks grow in complexity, precision, and volume, yesterday's approach to threat intelligence is no longer adequate. Investigating targeted attacks is no easy task. The dynamic behavior of the attackers, the greater variety and availability of local and global threat intelligence sources, and the diversity of threat intelligence data formats can make the aggregation and digestion of threat intelligence into security operations center (SOC) tools more challenging than ever before.

A mixed-vendor environment, which is typical of most enterprises, adds to the difficulty of sharing event data and promoting event visibility throughout the organization. As Gartner points out in its report, *Technology Overview for Threat Intelligence Platforms*, "An organization's inability to share TI is an advantage to cyber threat actors. TI sharing is a force multiplier and is becoming a key element in keeping up with the increasing number of threat actors and the attacks they use."[3]

But sharing threat intelligence alone will not necessarily result in sustainable corrective action and prevention. Security analysts can quickly become overwhelmed with

> **"For our security infrastructure, we needed much more than a technology vendor. It was absolutely essential that we built a relationship with a partner that could help us manage our diverse set of customer requirements and a constantly evolving threat situation. McAfee offers that partnership, and the ongoing security intelligence we receive from McAfee solutions is crucial to helping us keep our business operations on the cutting edge."**
>
> —Anurana Saluja, CISO and Vice President of Information Security, Sutherland Global Services

too much information. Most security teams are engaged in an exhausting manual process (see Figure 1) of analyzing millions of security events and suspicious files in an effort to piece together a mountain of data and try to reconstruct the targeted attack. Ultimately, this impairs the thoroughness and speed of the response process. With a less than complete comprehension of threats, security teams are struggling to contain attacks in a timely manner. According to a recent study, *Intel Security (now McAfee): When Minutes Count, 2014*, less than 25% of respondents stated that they could detect an attack within minutes.[4]

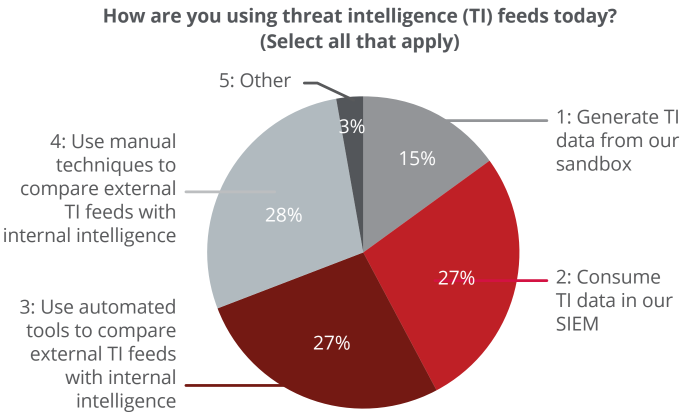


Figure 1. According to an Intel Security (now McAfee) survey conducted at BlackHat 2015, a large group of users still employ manual techniques to compare external threat intelligence feeds with internal threat intelligence.

Operationalize Threat Intelligence

Intelligence-driven threat detection and remediation require more than just manually importing adversarial IP addresses published on an open website into an SIEM watchlist table once a week. Instead, it calls for real-time threat intelligence ingestion and correlation of all facets of an attack, including methods and global campaigns, so that enterprises can preempt even the stealthiest and most rapidly adapting threats. Enterprise SOCs need a way to "operationalize threat intelligence" in order to get a full picture of attacks impacting their environments. They need a way to sift through the massive amount of data to analyze, correlate, and prioritize threat intelligence and determine what's relevant for their industry, their geography, and their company. And they need to be able to gain insights on unique attacks that may be occurring in the present, as well as insights on trends based on historical security event data. As Forrester points out, operationalizing threat intelligence is critical, as 75% of attacks spread from one victim to the next within 24 hours. Enterprises need to close the gap between "sharing speed and attack speed."[5]

Leverage the McAfee Integrated Architecture

McAfee provides a unified, collaborative platform with all the components for operationalizing threat intelligence, including global threat intelligence feeds, local intelligence creation, real-time sharing of threat information across the IT infrastructure, security information and event management (SIEM), and delivery of automated, adaptive protection.

Threat Intelligence Requirements	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
Collects threat intelligence from external sources	STIX, McAfee® Global Threat Intelligence (McAfee GTI) import, and VirusTotal	McAfee GTI Import	McAfee GTI, TAXII/STIX import, and HTTP threat feeds via the McAfee Enterprise Security Manager cyberthreat manager	McAfee GTI aggregates threat intelligence from multiple Cyber Threat Alliance partners and public sources. McAfee GTI extracts threat intelligence from millions of sensors on customer-deployed McAfee products, such as endpoint, web, mail, network intrusion prevention systems (IPS), and firewall devices.
Collects internal threat intelligence	Collects samples from McAfee VirusScan®, McAfee Application Control, McAfee Web Gateway, McAfee Advanced Threat Defense, McAfee Enterprise Security Manager, and from third-party vendor products sending information over McAfee Data Exchange Layer	Consumes sample files for detonation from McAfee Threat Intelligence Exchange or via the network	Via STIX/TAXII and McAfee Data Exchange Layer	
Produces local threat intelligence	Records incidents of suspicious files and creates a local database that records first contact and the trajectory of threats	Dissects and convicts malware, generates local threat intelligence, and distributes over McAfee Data Exchange Layer or as a STIX-formatted API	Creates threat intelligence watchlists, reports, and views based on correlated events	
Distributes threat intelligence across security controls	Via McAfee Data Exchange Layer	Via McAfee Data Exchange Layer and product API	Via McAfee Data Exchange Layer, product API and script integration	McAfee GTI is integrated with numerous McAfee products, such as McAfee Web Gateway, McAfee Enterprise Security Manager, and McAfee endpoint solutions
Offers visibility into collected threat intelligence	Via McAfee Threat Intelligence Exchange dashboards	Via reports	Via dashboards, views, and reports provided in content packs or customer-generated	Via McAfee Threat Center and quarterly McAfee Threats Report

Table 1. The McAfee integrated threat intelligence platform

Ingest, Analyze, and Propagate

McAfee Global Threat Intelligence

A good place to start building your integrated threat intelligence platform is McAfee Global Threat Intelligence (McAfee GTI), a comprehensive, real-time, cloud-based reputation service that is fully integrated into McAfee products and enables them to better block cyberthreats across all vectors—file, web, message, and network—swiftly. McAfee GTI provides reputation scores for billions of files, URLs, domains, and IP addresses based on threat data gathered from multiple sources: millions of global sensors monitored and analyzed by McAfee Labs, threat feeds from research partners and via the Cyber Threat Alliance, and cross-vector intelligence from web, email, and network threat data. Backed by high-quality, relevant threat feeds, McAfee GTI provides accurate risk advice that fosters informed policy decision-making and enables controls to block, clean, or allow, as required.

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (SIEM) takes threat intelligence ingestion and analysis to the next level, providing a consolidation, analysis, and action hub for every type of threat intelligence. This 360-degree view allows full visibility and situational awareness to speed detection and response to targeted attacks. Its advanced data management system is purpose-built to store and assimilate high volumes of contextual data in real time.

McAfee Enterprise Security Manager collects activity and event data from all your systems, databases, networks, and applications. It also imports global threat feeds and consumes threat intelligence in standard formats and transports, such as Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) and Cybox, typically published by community or industry groups like the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Through advanced analytics, it translates the gathered information into understandable, actionable security intelligence. More significantly, it provides deeper visibility to emerging threats via real-time views and access to historical security information. This allows you to investigate backwards in time to understand the prevalence and patterns of an attack and also to create automated watchlists to detect occurrence or re-occurrence of events in the future. By enriching your system's sensitivity to events known to be malicious, you increase your ability to detect suspicious activities and patterns of activity at various phases of the attack chain and then prioritize response.

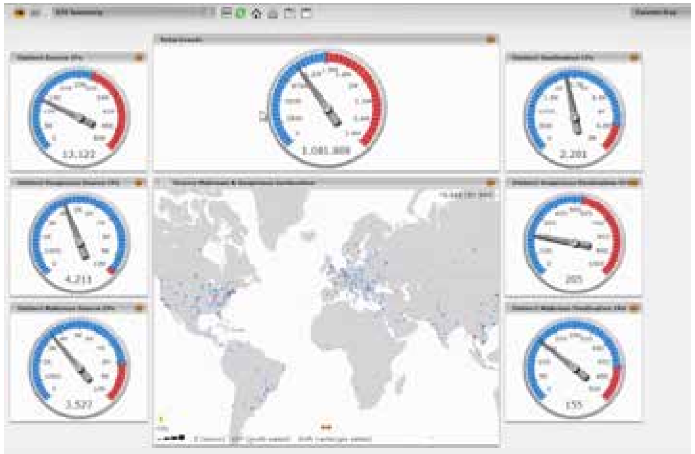


Figure 2. McAfee GTI view.

What Is the Cyber Threat Alliance?

The Cyber Threat Alliance is a group of security practitioners from organizations that work together to share threat information and help improve defenses against adversaries across member organizations and their customers. McAfee is among the founding members that have dedicated their resources to determine the most effective ways to share threat data, foster collaboration among members, and make united progress in the fight against sophisticated cybercriminals.

McAfee GTI for McAfee Enterprise Security Manager brings the power of McAfee Labs research capabilities to enterprise security monitoring. This constantly updated, rich McAfee GTI feed enhances situational awareness by enabling rapid discovery of events involving communications with suspicious or malicious IPs and allows security administrators to determine which enterprise hosts have communicated or are currently communicating with known bad actors.

McAfee Threat Intelligence Exchange

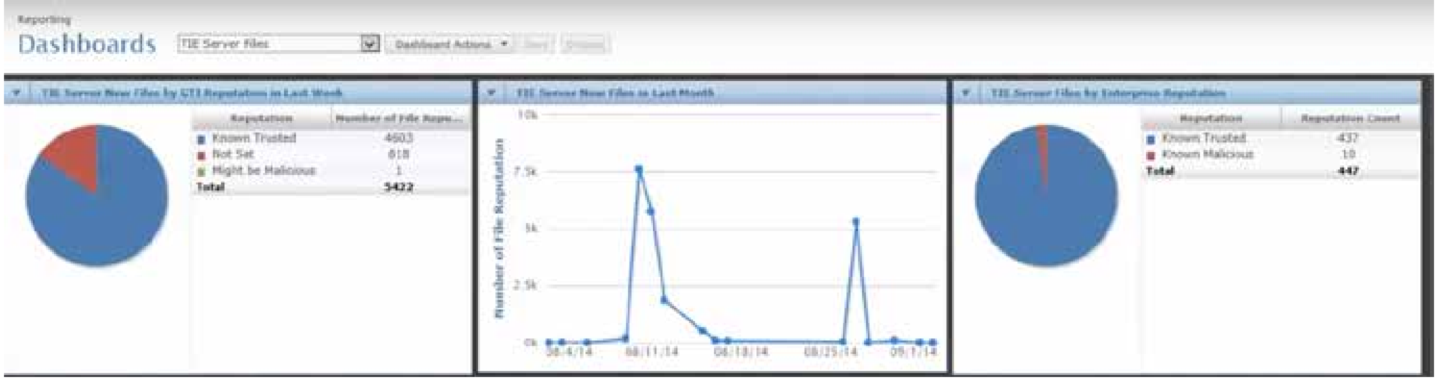
The third component you can add as you develop an integrated, threat intelligence ecosystem is McAfee Threat Intelligence Exchange, which aggregates and shares file reputation intelligence across the entire security infrastructure. McAfee Threat Intelligence Exchange receives threat information from McAfee GTI, STIX file imports, threat feeds coming via McAfee Enterprise Security Manager, and information coming from endpoint, application control, mobile devices, gateway, data centers, and sandboxing technologies from both McAfee solutions and solutions from other vendors.

Collecting data from all points in your infrastructure provides information on threats that may be present only in your environment, as many targeted attacks tend to be. In turn, file reputation information is instantly shared across the entire ecosystem to all products and solutions connected to McAfee Threat Intelligence Exchange via the McAfee Data Exchange Layer. For example, if McAfee Threat Intelligence Exchange pushes out information about a malicious executable file, McAfee Data Loss Prevention receives this information over the McAfee Data Exchange Layer and will then start monitoring that executable for any sensitive file access.

Threat data shared over McAfee Data Exchange Layer includes file reputations, data classifications, application integrity, and user context data, which is shared with and among products integrated into the McAfee Data Exchange Layer fabric. Any product or solution can be integrated onto the McAfee Data Exchange Layer and then configured to determine what information to publish to the system and what information to listen for and subscribe to.

McAfee Threat Intelligence Exchange works closely with the advanced sandbox solution, McAfee Advanced Threat Defense, which feeds malware analysis data to McAfee Threat Intelligence Exchange. If a file is found to be malicious, McAfee Threat Intelligence pushes out a file reputation update to all connected systems over the McAfee Data Exchange Layer. This also works the other way around. When McAfee Threat Intelligence Exchange-enabled endpoints encounter files with unknown reputations, they can be submitted to McAfee Advanced Threat Defense to determine if the object is malicious, eliminating blind spots from out-of-band payload delivery. These two products work together to deliver automated, adaptive protection from emerging threats. Information about discovered attacks is delivered across your environment to help block the cyberattack chain before more damage is done.

McAfee Threat Intelligence Exchange enables adaptive threat detection and response by operationalizing intelligence across your endpoint, gateway, network, and



Reporting
Dashboards
TIE Server Files
Dashboard Actions
TIE Server New Files by GTI Reputation in Last Week
TIE Server New Files in Last Month
10k
7.5k
5k
2.5k
0k
Number of File Reputation
08/4/14
08/11/14
08/18/14
08/25/14
09/1/14
TIE Server Files by Enterprise Reputation

Reputation	Number of File Repu...
🟦 Known Trusted	4603
🟥 Not Set	818
🟩 Might be Malicious	1
Total	**5422**

Reputation	Reputation Count
🟦 Known Trusted	437
🟥 Known Malicious	10
Total	**447**

Figure 3. McAfee Threat Intelligence Exchange dashboard..

data center security solutions in real time. Combining imported global threat information with locally collected intelligence and sharing it instantly, it allows your security solutions to operate as one, exchanging and acting on shared intelligence.

Interrupt the cyberattack chain

Regardless of where the first point of contact by an unknown malware file occurs, once it is convicted, the entire connected environment is updated immediately. When a file is convicted by McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange will publish this conviction via a reputation update, which is disseminated through McAfee Data Exchange Layer to all security controls within your organization. McAfee Threat Intelligence Exchange-enabled gateways prevent the file from entering your infrastructure. Through coordinated sharing of threat intelligence across all your security controls, it becomes easier to interrupt the attack chain and prevent further harm without the need for manual intervention.

Digest and Apply: Detect with Accuracy and Make Better Decisions

After threat data is consumed, McAfee Enterprise Security Manager acts as a central point of visibility, correlating the McAfee GTI, McAfee Threat Intelligence Exchange feeds, and STIX/TAXII-formatted indicators of compromise (IoCs) with event data, detected in real time or historically when nodes on your network are communicating with known bad actors or suspicious domains. The threat management dashboard provides analysts with a single, comprehensive view of collected threat indicators, the source feeds, hit rate against the indicators, and the most significant human-readable details on indicators of compromise (IoCs).

Using the McAfee SIEM system in conjunction with other collaborative threat intelligence tools results in reduced operational expenses associated with configuring correlation rules, which is usually a cumbersome manual process. For instance, security analysts can

The following McAfee products support STIX-formatted threat intelligence:

- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Detection
- McAfee Enterprise Security Manager

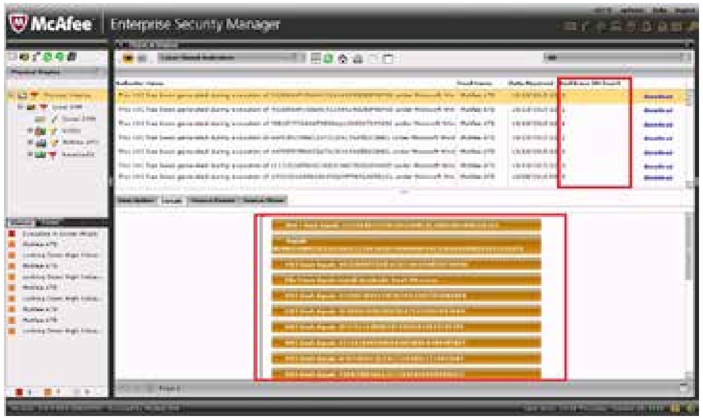


Figure 4. McAfee Enterprise Security Manager cyberthreat indicators, backtrace hits, and IoC threat details.

directly review the newly received threat information in a human-readable format, allowing for better understanding of new detected threats. More important, received threat intelligence can automatically be adopted by real-time or historical correlation rules, thus reducing the time to detect ongoing or new adversarial activity. Users can also follow the progress of reported threats throughout your IT environment, as well as via contextual information in alarm views, enabling better, more informed decisions. All of this collected intelligence improves and speeds up detection and investigation of targeted attacks.

Since threats blaze their paths through the IT infrastructure quickly and are designed to change over time, McAfee Enterprise Security Manager can periodically refresh all acquired threat intelligence, eliminating old, less relevant data. For example, removed command and control servers or cleaned-up websites with lower malicious reputation scores are automatically cleared out to eliminate false positives that can distract your security staff and keep them from chasing real threats.

Summary

Integrated threat intelligence from McAfee operationalizes the ingestion, digestion, and management of threat intelligence, enabling you to increase threat detection accuracy, eliminate manual efforts, and stop adversaries from harming your business. With improved visibility and enhanced insights on malicious activity across your entire security ecosystem, you are better prepared to identify and preempt targeted attacks today and prevent them in the future.

Learn More

For more information on the building blocks of the McAfee integrated threat intelligence platform, visit:

- McAfee Global Threat Intelligence
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee Enterprise Security Manager
- How to Use a TAXII Feed with McAfee Enterprise Security Manager

1. https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767
2. https://www.forrester.com/The+State+Of+The+Cyberthreat+Intelligence+Market/fulltext/-/E-RES123011
3. https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms
4. http://www.mcafee.com/us/resources/reports/rp-when-minutes-count.pdf
5. https://www.rsaconference.com/writable/presentations/file_upload/cxo-t08r-threat-intelligence-is-like-three-day-potty-training.pdf

Together is power.

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

62161brf_threat-intel_1015
OCTOBER 2015