Taking the Right Actions Faster:

Enhanced Threat Intelligence in McAfee™ Deployments

by Christian Galladora, ThreatQuotient Threat Intelligence Engineer

ABSTRACT

The volume of available threat data has increased dramatically over the last decade, gradually becoming a cacophony of noise. Mature security organizations have raced to develop tools, teams and processes to turn threat data into timely and relevant threat intelligence. Once this is accomplished, the intelligence must be distributed to existing security tools across networks that may be isolated from one another, and the intelligence team must get feedback from internal sighting matches.

McAfee™ and ThreatQuotient™ have strengthened our Security Innovation Alliance partnership to develop integrations and use cases that help solve these problems for customers.

ThreatQuotient Products Involved

ThreatQ™ Threat Intelligence Platform

Security teams should start by understanding their threats when considering how to make their security operations most effective and efficient. In understanding their threats, an organization can make appropriate use of their universe of global intelligence to determine what is happening external to the organization. This means having a thorough and proactive understanding of the actors, campaigns and TTPs targeting an organization specifically. Internally, this requires broad visibility and pivoting to a threat-centric view of operations — using that information to add valuable context to gain a deeper understanding of risk. By using both external and internal information, an organization can determine what the threat means and set out a plan for how to prepare and how to take action faster when an event occurs.

Organizations need a threat-centric approach to security that integrates all teams, tools and processes into a single, systemic security architecture that continually improves. Teams should have the flexibility, visibility and control needed for increased security effectiveness and efficient threat intelligence management. This empowers it with a deeper understanding of threats, continuous prioritization, improved collaboration and coordination to take the right actions faster. Effective threat intelligence allows an organization to accelerate security operations — dramatically reducing the time to detect and respond, increasing productivity and making the most of an existing defense infrastructure.

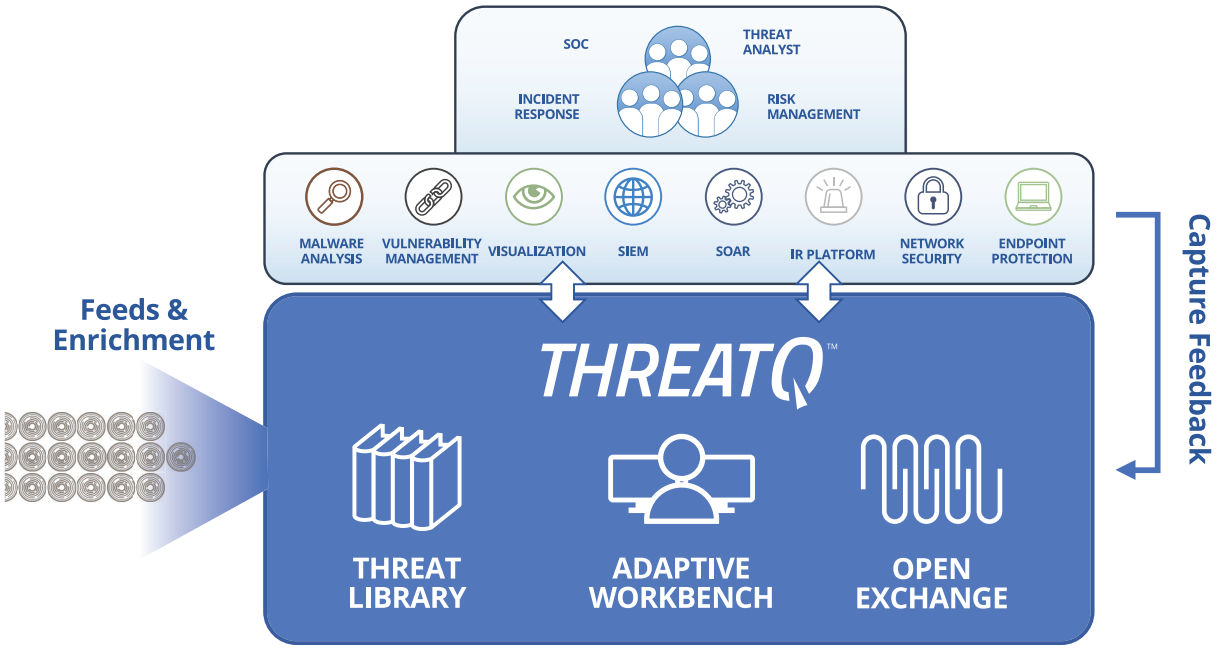

Figure 1: ThreatQ — Threat-Centric Security Operations

The ThreatQ™ Threat Intelligence Platform (TIP) allows customers to gain efficiencies across many different areas:

- Relevant Threat Intelligence — Combines ThreatQ's advanced threat scoring methodology and real-time knowledge, while the Threat Library™ self-tunes based on new knowledge.
- Improve Situational Understanding — Understand threats through context and adversary profiling, enabling defenders to anticipate threats and proactively update security posture to mitigate risk in the future.
- Accelerate Detection and Response — Combine external and internal threat data to provide context and relevance, empowering better decision making and automated actions.
- Maximize Existing Security Investments — Automate intelligence distribution to an existing sensor grid.
- Advance Team Collaboration — Enables security teams to be more efficient and effective through greater information sharing and knowledge transfer.

There are three main components in the ThreatQ platform:

1. Threat Library

The Threat Library is a central repository that aggregates external and internal threat data and events to provide contextual intelligence that is relevant to your unique environment. The Threat Library dynamically scores and prioritizes threat intelligence based on parameters the company sets. Prioritization is calculated across many separate sources, both external and internal, using the aggregated context provided to deliver a single source of truth. As more data and context enter the system, the Threat Library learns and adjusts, re-scoring and reprioritizing to ensure clarity on what is important. This removes noise, the risk of false positives, and enables our customers to focus on the data that really matters.

In sum, the self-tuning Threat Library allows for:

- Advanced scoring
- Context to be added from external and internal data
- Structured and unstructured data imports

2. Adaptive Workbench™

With the Adaptive Workbench, security experts have an extensible work area where they can define configurations and integrations to incorporate ThreatQ into their existing operations, using the processes and tools that already exist in the environment. Customizable workflows and customer-specific enrichment expand the types of intelligence that can be managed and used. Multiple teams can work in concert, sharing knowledge through the Threat Library. This streamlines investigations and analysis and automates the intelligence life cycle.

3. Open Exchange™

The ThreatQ platform allows companies to integrate tools, teams and workflows through standard interfaces, including using an API and SDK. The ThreatQ Open Exchange includes over 150 pre-defined integrations with existing security infrastructure products and threat feeds. ThreatQ also allows for STIX/TAXII imports and exports.

McAfee Products

Enterprise Security Manager (ESM)

McAfee Enterprise Security Manager is a security information and event management (SIEM) solution that delivers actionable intelligence and integrations to prioritize, investigate and respond to threats.

Advanced Threat Detection (ATD)

Targeted attacks are designed to defeat security systems by confusing or evading defenses. McAfee Advanced Threat Defense combines in-depth static code analysis, dynamic analysis (malware sandboxing) and machine learning to increase zero-day threat detection, including threats that use evasion techniques and ransomware.

Threat Intelligence Exchange (TIE)

McAfee Threat Intelligence Exchange verifies the reputation of executable programs.

Data Exchange Layer (DXL)

The Data Exchange Layer communication fabric connects and optimizes security actions across multiple vendor products, as well as internally developed and open source solutions. Enterprises gain secure, real-time access to new data and lightweight, instant interactions with other products.

McAfee Active Response (MAR)

McAfee Active Response is an endpoint detection and response tool for advanced threats. MAR is able to capture and monitor events, files, host flows, process objects, context and system state changes that may be indicators of attack (IoAs) or attack components lying dormant.

Global Threat Intelligence (GTI)

Based on activity from millions of sensors world-wide and an extensive research team, McAfee Labs publishes timely, relevant threat activity via McAfee GTI. This always-on, cloud-based threat intelligence service enables accurate protection against known and fast-emerging threats by providing threat determination and contextual reputation metrics.

McAfee Endpoint Security (ENS)

McAfee Endpoint Security is a modern, integrated endpoint security platform. It replaces several legacy McAfee products that were deployed as point products (VirusScan Enterprise, McAfee SiteAdvisor, McAfee Host Intrusion Prevention and others) with a single-agent architecture and integrated advanced defenses like machine learning analysis, containment and endpoint detection and response (EDR).

McAfee Network Security Platform (NSP)

Network Security Platform (McAfee NSP) is a next-generation intrusion prevention system (IPS) that discovers and blocks sophisticated malware threats across the network. It utilizes advanced detection and emulation techniques, moving beyond mere pattern matching to defend against stealthy attacks with a high degree of accuracy.

McAfee ePolicy Orchestrator (ePO)

McAfee ePolicy Orchestrator (McAfee ePO) provides a centralized management console that simplifies and accelerates your security effectiveness with visibility and control from device to cloud.

Enhanced Threat Intelligence in McAfee Deployments

Reach: Communication Across Multiple McAfee Environments

ThreatQuotient and McAfee have partnered together to help analysts utilize threat intelligence across multiple communication fabrics and channels from a single device. By acting as a central repository of global threat intelligence, ThreatQ is able to correlate that intelligence against events gathered from a variety of McAfee sources.

ThreatQ is then able to provide curated and actionable threat intelligence to infrastructure on each fabric. In this way, the intelligence team can offer value to multiple McAfee-based ecosystems under their watch, whether delineated by business unit, geographic region or enterprise subsidiary. This integration expands the capability to distribute actionable intelligence to multiple security teams in an automated and near-real-time distribution architecture to better enhance intelligence within McAfee deployments.

Feedback: Continuous Evaluation of an Organization's Threats

ThreatQ has a customizable scoring policy that continuously evaluates the relevance of threat indicators to the security teams' unique environment. This means the score of an indicator will be re-calculated when additional information is obtained about it — increasing or decreasing its risk score based on your pre-defined scoring algorithm.

ThreatQ's Security Innovation Alliance (SIA) partnership with McAfee allows Enterprise Security Manager (ESM), Threat Intelligence Exchange (TIE) and Advanced Threat Defense (ATD) to provide an "inside" view to the Threat Library, enabling the scoring policy to evaluate the threat landscape based on the correlation between external threats and internal activity.

The availability of internal sources of data can create a controlled feedback loop within the scoring policy — a threat reported by an external intelligence feed may have a moderately high score based off the relevance to an architecture. However, this score is automatically increased when activity correlated with the threat is detected by your internal infrastructure. A higher score for the newly detected threat could trigger enforcement or move the indicator to the top of the analysts' research stack. These outcomes mean faster response-to-detection and a more realistic view of malicious activity targeting a business.

For example, an IP Address is imported from a McAfee Threat Advisory about the Emotet Malware. It is evaluated against the scoring policy and a Medium score is determined based on the reported context. Highlighted below, the expanded flag view shows the characteristics of this IP address (i.e. detection name, malware class, malware family, exploit phase, etc.) that is matched by customer's pre-defined scoring policy. Based on the status and score, it is published to a customer's ESM watch list as shown on figure 2.

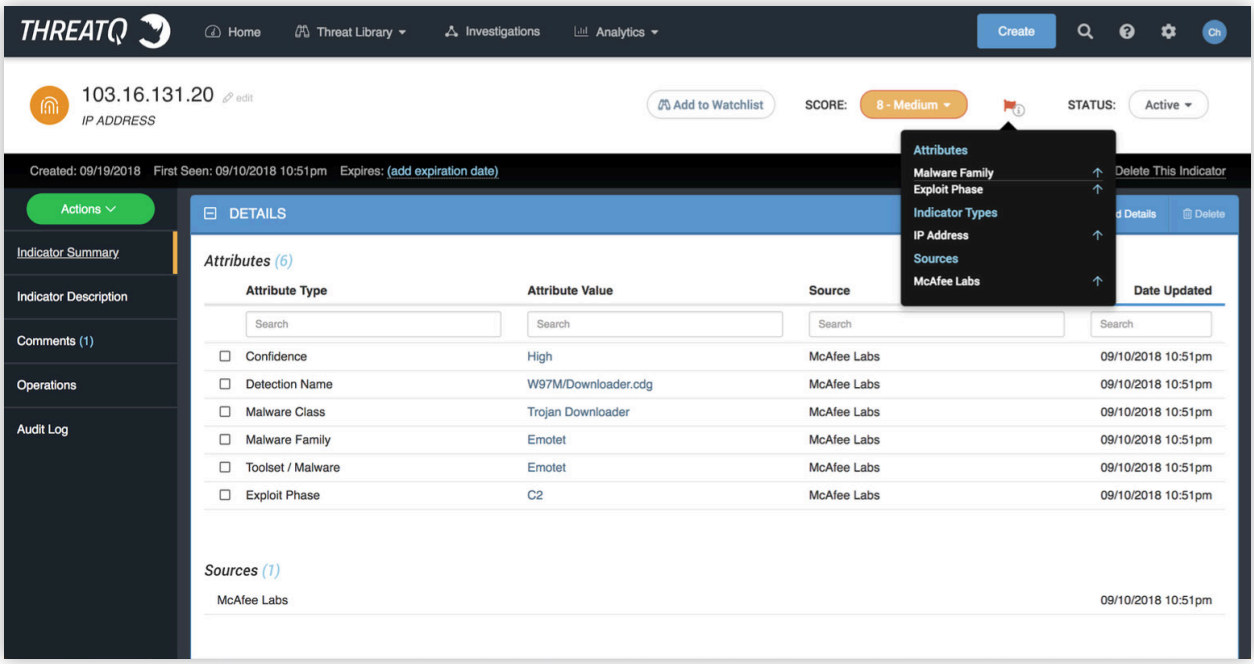

Figure 2: ThreatQ — McAfee ESM Watch List

Several days later, the ESM has a sighting of the published IP address and an alarm is generated as shown below. The alarm is reported as a Sighting in ThreatQ's Threat Library as shown in figure 3.

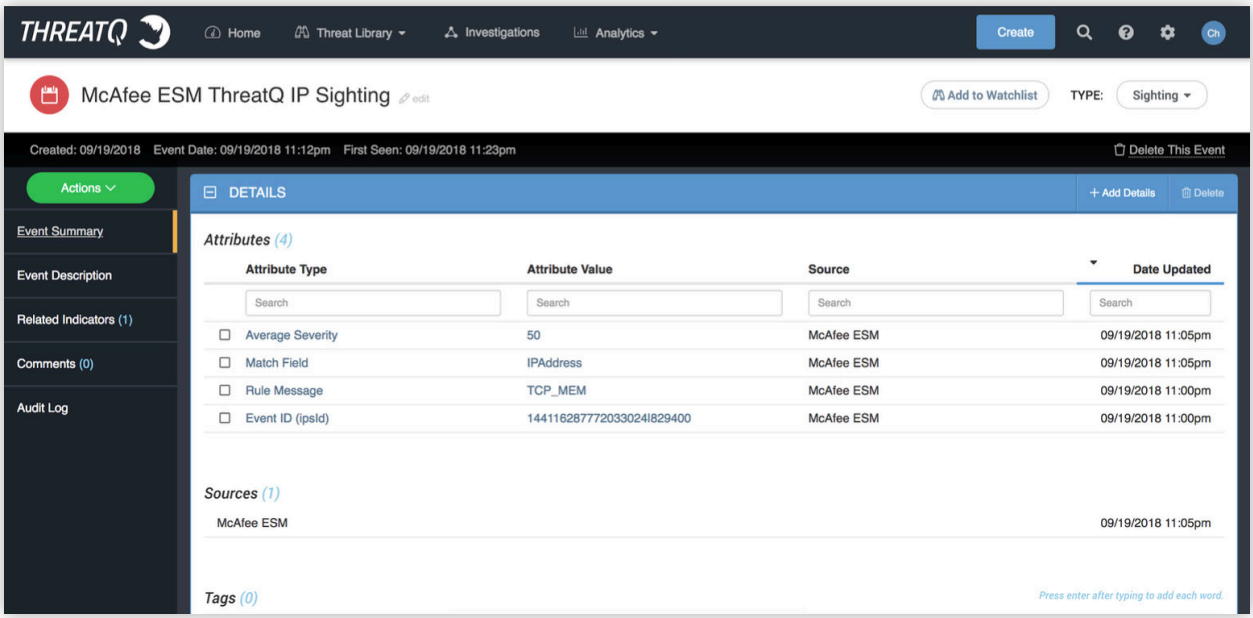

Figure 3: ThreatQ Library ESM Sighting

Lastly, as shown in figure 4, a source of McAfee ESM is added to the indicator in the Threat Library. This bi-directional feedback loop of the internal sighting causes the threat relevance to the organization to be re-evaluated to a 10 - Very High, based on the internal sighting.

Based on the automatically recalculated score of 10 - Very High, the IP Address will be published to a firewall blocklist or blackholed at the domain name system (DNS) to ensure any other infected hosts on the network will be unable to communicate to the malicious IP while simultaneously notifying a security analyst of the infection. The analyst can then pivot to McAfee Active Response to study the network flow to this IP address and decide on enforcement actions.

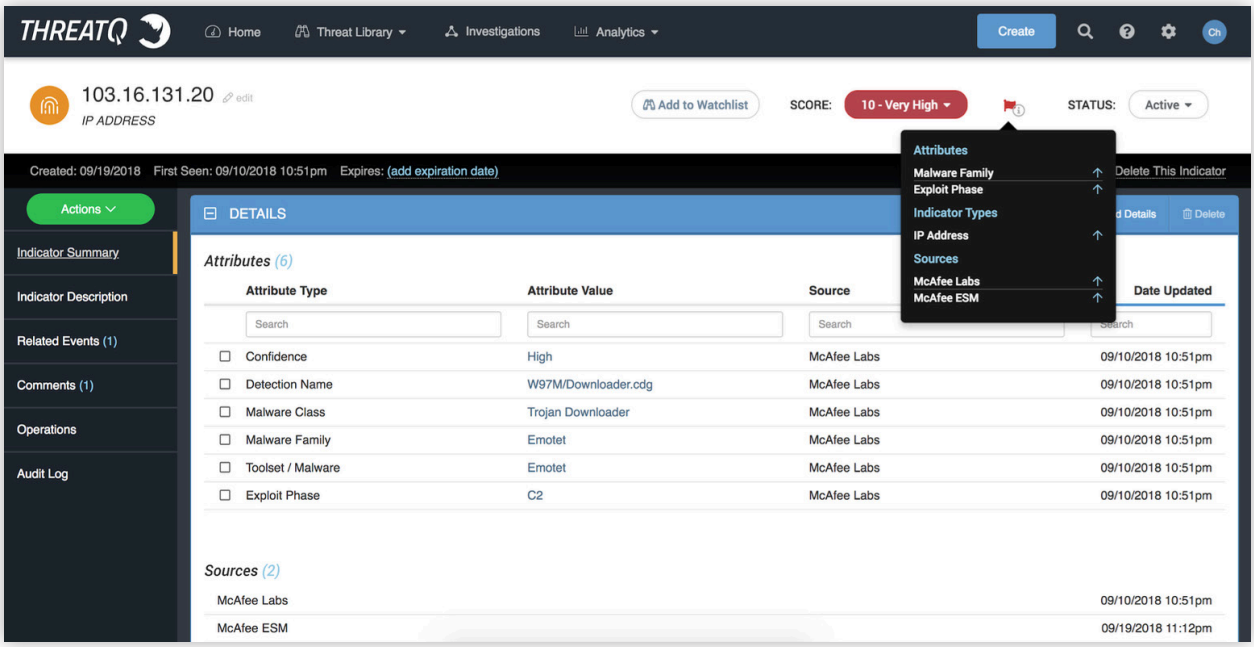

Figure 4: McAfee ESM ThreatQ Score Adjustment

ThreatQ and McAfee Integrations

ThreatQ and McAfee Threat Intelligence Exchange (TIE)

ThreatQ's core feature set includes the ability to ingest threat data from a wide variety of sources, including commercial, open source, community-ISACs, private sharing communities and internal feeds. ThreatQ then integrates with Threat Intelligence Exchanges on multiple DXL fabrics. Using the Set Reputation topic, ThreatQ will provide a Threat Intelligence Exchange with information about the maliciousness of indicators.

The Threat Intelligence Exchange will be armed with curated intelligence for enforcement. Third-party indicators from virtually any provider can be evaluated and then made available for McAfee Agents on the DXL. Large data sets are trimmed into intelligence that matters for the organization in question and then made available for enforcement.

ThreatQ and McAfee Enterprise Security Manager (ESM)

ThreatQ's integration with McAfee Enterprise Security Manager allows the threat intelligence team to publish relevant, targeted indicators to multiple ESM instances on different fabrics that an organization may have. Each Enterprise Security Manager instance will then have curated watchlists based on the latest expertise of the threat intelligence team.

In the event an item on a watchlist, such as an IP Address or a File Hash is seen by the Enterprise Security Manager, an alarm will be generated and an event created in the ThreatQ Threat Library. The event in the Threat Library will include important context, such as any additional and relevant indicators.

The additional context the ESM returns can be used in the ThreatQ customizable scoring policy. The threat intelligence team is therefore able to automatically re-evaluate the relevance of certain features to the organization based on external reports and internal sightings.

ThreatQ and McAfee Advanced Threat Defense (ATD)

ThreatQ's integration with McAfee Advanced Threat Defense gives the analyst the tools to easily send malware or URLs for detonation. The resulting threat data set will immediately be added to the Threat Library, where it is evaluated or reevaluated for relevance. This process initiates actionable intelligence to be distributed to other McAfee products such as ESM and TIE. This seamless and transparent workflow allows a security team to move from sample research to analysis and enforcement within one pane of glass.

ThreatQ and McAfee Global Threat Intelligence (GTI) Private Cloud

ThreatQ and McAfee have demonstrated the ability to send reputation data to a GTI Private Cloud instance for availability across vast global and potentially federated entities. In this configuration, the GTI Private Cloud will report malicious indica-

tors to the Threat Library. In doing so, the security team is able to operationalize intelligence from third-party sources in the largest of organizations.

ThreatQ and McAfee Active Response (MAR)

As part of the ThreatQ integration with McAfee Active Response, the analyst can query for malicious activity within their environment based on intelligence in their ThreatQ global Threat Library. An analyst having the ability to query data across their infrastructure is a vital component of every investigation and becomes the cornerstone of MTTD and MTTR activities. Additionally, triggers can be crafted in MAR based on ThreatQ's exports, allowing for enterprise-wide indicator sweeps across McAfee endpoints.

The integration of ThreatQ and MAR arms the team to detect and respond to malicious activity quickly and effectively. In the event of a malicious sighting, the team will have the associated context available to respond in ThreatQ, potentially including the tactics, techniques and procedures associated with the threat, allowing for a more timely and accurate response.

ThreatQ and McAfee Endpoint Security (ENS)

ThreatQ can pass relevant and prioritized indicators through TIE or DXL to ENS to block the threat on the endpoint. This creates a "Dynamic Endpoint" that is able to ingest and react quickly to emerging threats and adversaries by creating blocking rules based on threat intelligence from many different sources.

Customer Use Cases

1. **ATD / ThreatQ Use Case:** ATD publishes any analysis result onto the DXL Messaging fabric. ThreatQ captures any new messages and creates an event within the Threat Library. Any threat data which is associated with the ThreatQ Event is then scored and sent to the infrastructure products in a mixed-vendor environment.

   The analysis report and (optionally) malware samples are also captured and related to the relevant pieces of threat data within the Threat Library. This information may be used to offer additional contextually relevant data to analysts and incident responders from within the ThreatQ GUI.

2. **ATD / ThreatQ Use Case:** ThreatQ receives sample malware from an external feed source. Users may then leverage a ThreatQ Operation to send files and URLs to ATD for evaluation and detection. All results are published back onto the DXL messaging fabric and made visible to all technologies that are subscribed to the ATD DXL topic. This includes passing data that scores above a user-defined "maliciousness" back to ThreatQ.

   The bidirectional feedback loop from ATD back into TQ permits users to detonate files and URLs in ATD, and then automatically capture detailed analysis results in the Threat Library. This is critical to the intelligence process because it streamlines data and extends the ecosystem integration bridging malware teams, intelligence teams and security analysts performing the investigations.

3. **TIE / ENS / ThreatQ Use Case:** ThreatQuotient and McAfee have built an integration to distribute intelligence across large deployments. This use case highlights the importance of sharing intelligence between disparate business units quickly using McAfee's DXL and TIE.

   Business Unit 1 — Business unit 1 discovers a malicious indicator locally (found out from ATD or ESM). The reputation of the newly discovered indicator is communicated to ThreatQ and it is scored high based on its associated attributes. ThreatQ publishes the indicator and reputation to TIE through DXL at Sites 2 through N.

   Business Units 2 through N — The reputation is now available in TIE at sites 2 through N, and informs ENS locally to block the indicator across all endpoints.

4. **ESM / ENS / MAR / ThreatQ Use Case:** ThreatQ brings in threat data from many different sources (ISACs, open source, DHS-AIS, etc.). This threat data is de-duplicated and scored in the system and considered relevant enough to send to ESM. The integration is bidirectional, meaning a sighting by the ESM will be reflected in the threat library as an additional source. The score is then edged higher and the indicator is pushed to the infrastructure products, like McAfee Endpoint Security or McAfee Active Response (MAR), to automatically block this particular indicator.

   An analyst pivots on the indicator within ThreatQ and realizes it is related to a particular adversary. The scoring algorithm is adjusted to automatically increase the score of any indicator associated with this adversary. Based on the new scoring policy, the system recalculates all the indicators associated with that adversary and, as a result, new indicators exceed the threshold for export and are sent to ESM and other enforcement infrastructure for blocking.

CONCLUSION

Well-intended security teams have tried to bring threat intelligence into their organization, only to find the volume of published data is overwhelming and difficult to manage. Teams often report difficulty in marrying what is being reported outside with what is being observed inside the SOC.

ThreatQ gives analysts the flexibility, visibility and control to successfully operationalize and manage their threat intelligence. ThreatQ's integrations with the McAfee line of products makes the intelligence seamless to act on and easily distributed, increasing the effectiveness of the security operations and accelerating detection and response.