SECURITY OPERATIONS CENTER FINAL PROJECT

DECISION, ANALYSIS AND RESOLUTION REPORT

Date: 20 March 2021

Report by

Balanagameena NAGASUBRAMANIAN

M.Sc., (Computer Security)-Spring 2020

Contents

Context

I am Meena, CTO of an MSSP (Managed Security Services Provider) type SOC i.e., I carry out security supervision for my customers. Within this context, my management asked me to draw up a technological roadmap for the coming years, to evaluate whether I should change the existing SIEM, see which EDR to acquire to offer a new service, and choose intelligence sources to increase the detection capabilities via Threat Intelligence.

SIEM vs Threat Intelligence

SIEM stands for Security and Information Event Management.

The idea of a SIEM is to gather security logs from a variety of sources (Active Directory, DNS, DHCP, Firewalls, O365 etc.) and then correlate them together. Once these logs are all there, they are then monitored by Security Analyst' for any security issues. This is done by rules which monitor the logs, along with threat hunting performed by experienced analysts.

Threat Intelligence is the gathering of intelligence such as IPs, URLs, Domains, Hashes, Email addresses etc. which are related to malicious actors / hackers. This information is then stored and monitored so that companies can detect and block when known malicious indicators appear or attempt to appear on their networks.

Objective

To propose threat intelligence sources and platforms to integrate with existing McAfee SIEM.

Why I choose threat intelligence sources without changing the SIEM? **McAfee Enterprise Security Manager (NitroView ESM)** is one of the best SIEM as per Gartner 2020 ratings. Also, the recent version 11 works faster. Hence, I prefer to go for integrating this SIEM with threat intelligence sources and platforms. This is simpler and cost efficient than going for change of SIEM.

McAfee SIEM

McAfee Enterprise Security Manager (McAfee ESM) is a security information and event management (SIEM) solution that gives you real-time visibility to all activity on your systems, networks, databases, and applications.

As the foundation of McAfee's SIEM solution, McAfee ESM:

1. Collects and aggregates event data from your security devices, network infrastructures, databases, and applications.

2. Applies intelligence to that data, by combining it with contextual information about users, assets, vulnerabilities, and threats.

3. Correlates information to find potential threat incidents.

4. Enables you to investigate and respond to incidents by using interactive, customizable dashboards.

We need to find the relevant threat intelligent platforms now to integrate with this SIEM to achieve the desired objective. So, now we see the list of threat intelligence technologies that are possible to integrate with McAfee SIEM.

List of technologies

1. Recorded future Intelligence Services by Recorded Future

2. Global Threat Intelligence (GTI) by McAfee

3. Kaspersky Threat Intelligence Services by Kaspersky

4. ThreatQ by ThreatQuotient

5. Anomali by Anomali

Additional information before proceeding to threat intelligence sources and platforms:

We can do manual search using haveIbeenpwned.com to get notifications when the user data has been breached somewhere across the internet. This platform is completely free.

We prefer to go for threat intelligent platform since we would be handling huge data and seeing in dashboard would also be convenient. This makes the process easy and cost effective.

Overview of the list of technologies

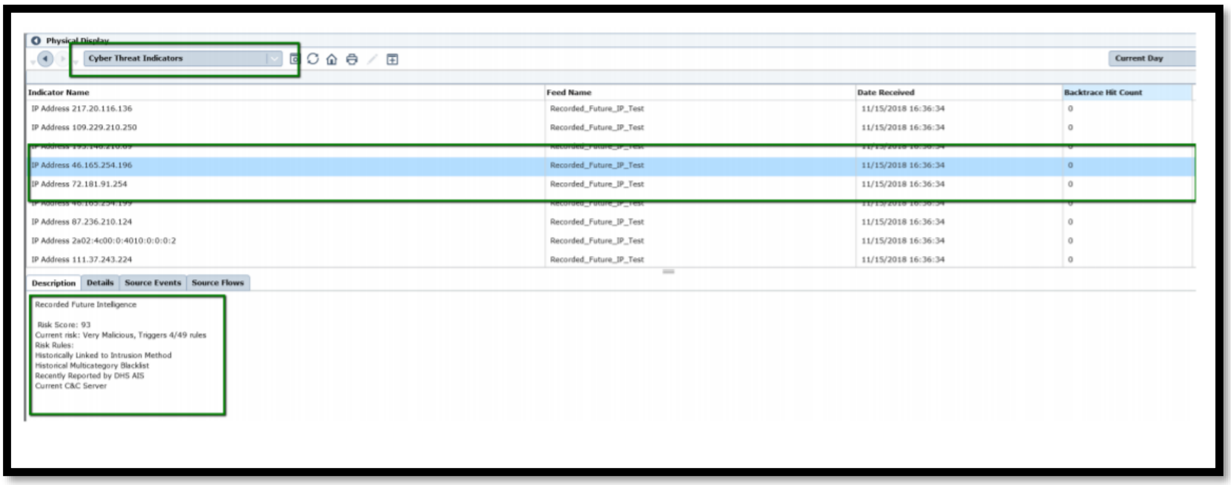
1. Recorded future Intelligence Services by Recorded Future

Recorded Future integrates seamlessly with existing security tools, delivering role-based intelligence that is timely, accurate and actionable. By enriching security solutions with real-time intelligence from Recorded Future, we can expect to identify 22% more security threats before impact; resolve security threats 63% faster; and increase team efficiency by 32%.

Recorded Future is continually collecting and analyzing information from all over the internet to deliver the largest commercial security intelligence repository available. From this, Recorded Future creates frequently updated lists of high risk, malicious Indicators of Compromise (IOCs). These IOCs are delivered via STIX/TAXII and can be ingested as Watchlists within ESM, one for each IOC type (i.e., IP's, URL's, Hash and Domains). These watchlists can then be correlated against internal telemetry for threat detection. When potential threats are discovered, Recorded Future can further assist with triage by providing additional context, such as indicator Risk Score and the associated evidence. Please note that this configuration represents a basic integration setup. Fine tuning of both the risk indicators ingested and the associated detection rules can result in a more efficient and organization-specific security posture.

Challenges Overcome through Integration with McAfee SIEM:

Security operations center (SOC) teams are inundated with alerts and events. By joining forces through a seamless integration, security event management from McAfee ESM and security intelligence from Recorded Future helps analysts reduce manual research time and make informed verdicts. SOC analysts can efficiently dismiss false positives and capture threat context for true incidents.



Indicator Name	Feed Name	Date Received	Backtrace Hit Count
IP Address 217.20.116.136	Recorded_Future_IP_Test	11/15/2018 16:36:34	0
IP Address 109.229.210.250	Recorded_Future_IP_Test	11/15/2018 16:36:34	0
IP Address 193.148.210.69	Recorded_Future_IP_Test	11/15/2018 16:36:34	0
IP Address 46.165.254.196	Recorded_Future_IP_Test	11/15/2018 16:36:34	0
IP Address 72.181.91.254	Recorded_Future_IP_Test	11/15/2018 16:36:34	0
IP Address 46.165.254.199	Recorded_Future_IP_Test	11/15/2018 16:36:34	0
IP Address 87.236.210.124	Recorded_Future_IP_Test	11/15/2018 16:36:34	0
IP Address 2a02:4c00:0:4010:0:0:0:2	Recorded_Future_IP_Test	11/15/2018 16:36:34	0
IP Address 111.37.243.224	Recorded_Future_IP_Test	11/15/2018 16:36:34	0

Recorded Future Intelligence

Risk Score: 93
Current risk: Very Malicious, Triggers 4/49 rules
Risk Rules:
Historically Linked to Intrusion Method
Historical Multicategory Blacklist
Recently Reported by DHS AIS
Current C&C Server

Above figure shows the output of the recorded future when recorded with McAfee ESM. It shows the risk score of the external IP address.

We can create a watchlist based on our requirements.

For instance, we can create watchlist for vendors like the ip's they use and the domains from which they are connecting to us. Whenever the vendor site is breached, we would get an alert and hence we can block their traffic immediately and alert the employees accordingly.

We can create a watchlist for c-level officers by collecting their Gmail ids and official id's. If it is reported/breached somewhere on the internet, we can alert them to change their password and ask them to enable two factor authentications if not present.

We can create a watchlist for the required domains. For instance, giving this keyword “epita”, “epita.com” which creates an alert when someone is using this id for doing any online purchase which is against the practice. If someone is using “epita” like if any domain is registered with the similar name, we would be getting an alert.

Advantages of using recorded future:

1. Delivers the expected business outcomes that were promised.

2. Transition would be delivered on time, within budget, and with high quality.

3. It has good flexibility and adaptability in negotiating final contracts.

Disadvantages:

1. Cost to bring in automation is expensive.

Reference:

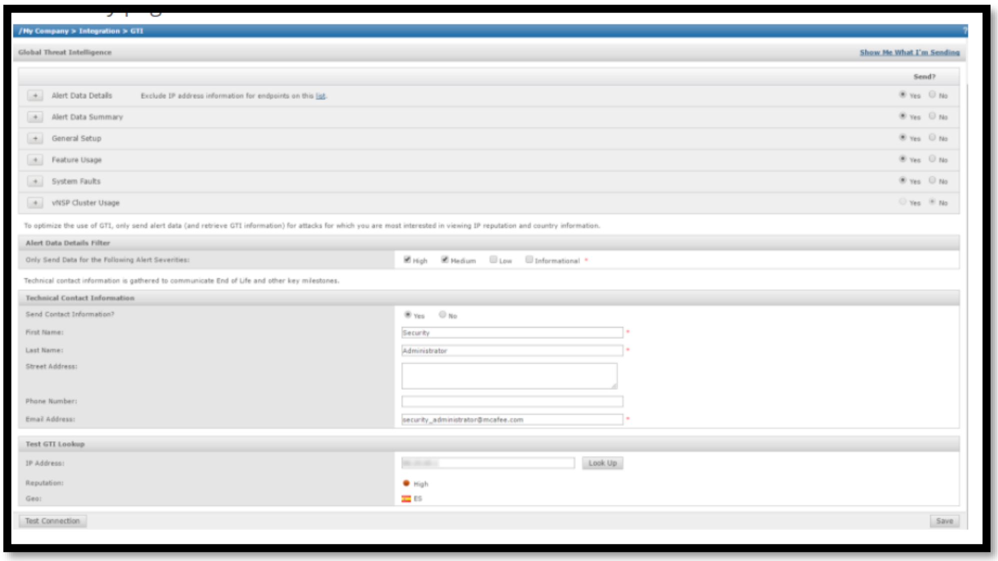
1. https://go.recordedfuture.com/hubfs/install-guides/mcafee-esm-configuration.pdf

2. https://www.gartner.com/reviews/market/security-threat-intelligence-services/vendor/recorded-future/product/recorded-future-intelligence-services/review/view/3454311

2. Global Threat Intelligence by McAfee

When using a SIEM to identify compromised systems and emerging threats, it's important to have visibility into where threats are in the greater world. McAfee's Global Threat Intelligence (GTI) provides one constantly updated, rich feed for ESM that enhances situational awareness by highlighting events involving communications with suspicious or malicious IPs. In today's rapidly moving threat landscape, many customers find it advantageous to leverage multiple threat feeds to provide additional insights.

GTI is 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.



		Send?
Alert Data Details	Exclude IP address information for endpoints on this list.	● Yes ○ No
Alert Data Summary		● Yes ○ No
General Setup		● Yes ○ No
Feature Usage		● Yes ○ No
System Faults		● Yes ○ No
vNSP Cluster Usage		○ Yes ● No

To optimize the use of GTI, only send alert data (and retrieve GTI information) for attacks for which you are most interested in viewing IP reputation and country information.

Alert Data Details Filter

Only Send Data for the Following Alert Severities: ☑ High ☑ Medium □ Low □ Informational *

Technical contact information is gathered to communicate End of Life and other key milestones.

Technical Contact Information

Send Contact Information?	● Yes ○ No
First Name:	Security *
Last Name:	Administrator *
Street Address:	
Phone Number:	
Email Address:	security_administrator@mcafee.com *

Test GTI Lookup

IP Address:	[redacted]
Reputation:	● High
Geo:	ES

Advantages:

1. Doesn't require any integration or installation as it is already present and needs to be activated.

2. Provides timely threat intelligence that helps protect organizations and users from both known and emerging cyberthreats, regardless of the source of those threats.

3. Closes the threat window with timely, often predictive, reputation-based threat intelligence, reducing the probability of attack.

Disadvantages:

1. License is expensive.

Reference:

1. https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-operationalizing-threat-intelligence.pdf

2. https://www.mcafee.com/enterprise/en-us/threat-center/global-threat-intelligence-technology.html

3. https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-global-threat-intelligence.pdf

4.https://kc.mcafee.com/corporate/index?page=content&id=KB74230

5. https://docs.mcafee.com/bundle/network-security-platform-9.1.x-integration-guide-unmanaged/page/GUID-7CA3EB50-DBEE-4ECC-A207-1F0BC49B1ADE.html

3. Kaspersky Threat Intelligence Services by Kaspersky

Kaspersky CyberTrace is a Threat Intelligence Platform that helps analysts make timely and better-informed decisions. Kaspersky CyberTrace uses continuously updated threat data feeds to timely detect cyber threats, prioritize security alerts and effectively respond to information security incidents.

Kaspersky CyberTrace integrates threat intelligence (such as threat intelligence feeds from Kaspersky, other vendors, OSINT, internal Threat Intelligence, or even custom sources) with SIEM solutions and log sources so that users can immediately leverage threat intelligence for security monitoring and IR activities in their existing security operations workflow. If Indicators of Compromise (IoC) from the threat intelligence feeds are found in your environment, Kaspersky CyberTrace will automatically send alerts to SIEM solutions for monitoring, validation, and uncovering additional contextual evidence of ongoing security incidents.

Kaspersky CyberTrace for McAfee ESM allows you to check URLs, file hashes, and IP addresses contained in events that arrive in McAfee ESM. The URLs, file hashes, and IP addresses are checked against threat data feeds from Kaspersky, or from other vendors or sources loaded to CyberTrace. During the matching process, Kaspersky CyberTrace determines the indicator category and generates an event supplemented with actionable context.

To integrate Kaspersky Threat Data Feeds using Kaspersky CyberTrace with McAfee ESM:

1. Download and install Kaspersky CyberTrace for Other SIEMs.

2. Configure Kaspersky CyberTrace for integration with McAfee ESM according to the guide.

Note:<< Guide is found in the reference 1 below>>

3. Configure forwarding events from McAfee ESM to Kaspersky CyberTrace according to the guide.

4. Configure sending events from Kaspersky CyberTrace and parsing them in McAfee ESM according to the guide.

5. After this, you can browse CyberTrace events, that contains actionable information from Kaspersky Threat Data Feeds as well as from other vendors or sources, in McAfee ESM to identify existing breaches or newly launched attacks and inform your business or clients about the risks and implications associated with the threat.

Following the guide, you will be able to integrate any supported version of Kaspersky CyberTrace with McAfee SIEM v10 and v11. This integration allows McAfee users to take advantage of Kaspersky Data Feeds and operationalize Threat Intelligence management leveraging the full capabilities of the Cybertrace TI Plaform.

Advantages:

1. Good security services

2. Kaspersky Threat Intelligence Portal provides detailed threat information about: URL, domains, IP-addresses, hashes, threat names, WHOIS, DNS data, etc.

Disadvantages:

1. Integration is required.

2. It is little expensive.

References:

1. **Guide:** https://media.kaspersky.com/EN/Kaspersky%20CyberTrace%20with%20McAfee%20Enterprise%20Security%20Manager.pdf

2. https://support.kaspersky.com/13850

4. ThreatQ by ThreatQuotient

ThreatQuotient's integration with McAfee Enterprise Security Manager allows the threat intelligence team to publish relevant, targeted indicators to multiple McAfee Enterprise Security Manager instances. Each McAfee Enterprise Security Manager instance will then have curated watchlists based on the latest expertise of the threat intelligence team.

The integration of McAfee Enterprise Security Manager and ThreatQuotient helps organizations accelerate detection and response. You can reduce noise and minimize false positives by quickly identifying relevant threat data.

ThreatQuotient brings in threat data from many different sources (ISACs, open source, DHS-AIS, and others). After threat data is deduplicated and scored, high-relevance indicators are sent to McAfee Enterprise Security Manager watchlists. The integration is bidirectional, meaning that a sighting by McAfee Enterprise Security Manager 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, to automatically block this indicator.

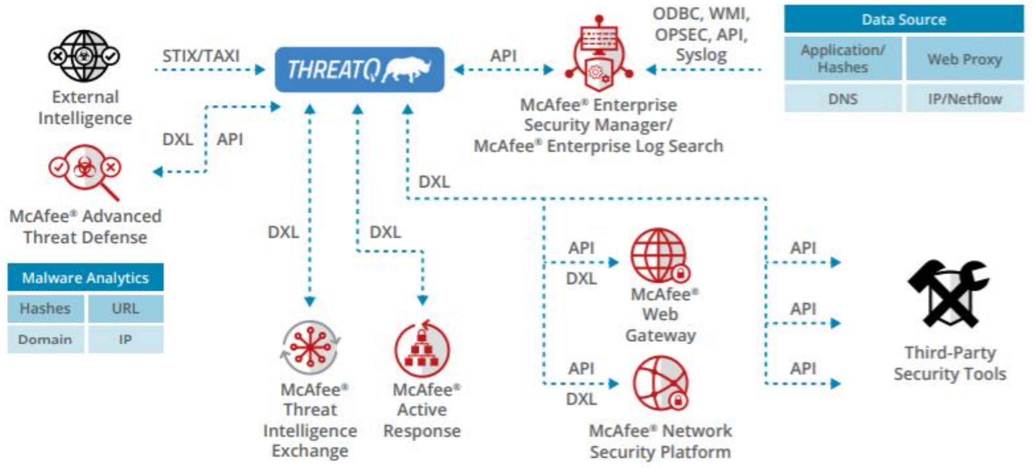

External Intelligence
STIX/TAXI
THREATQ
API
ODBC, WMI, OPSEC, API, Syslog
Data Source
Application/ Hashes
Web Proxy
DNS
IP/Netflow
McAfee® Enterprise Security Manager/ McAfee® Enterprise Log Search
DXL
API
McAfee® Advanced Threat Defense
Malware Analytics
Hashes
URL
Domain
IP
DXL
DXL
DXL
API
DXL
McAfee® Web Gateway
API
API
API
API
DXL
Third-Party Security Tools
McAfee® Threat Intelligence Exchange
McAfee® Active Response
McAfee® Network Security Platform

Figure 1. The power of McAfee and ThreatQuotient.

Advantages:

1. Accelerate event triage by providing a searchable and single source of threat knowledge.

2. Automatically consume sightings in ThreatQuotient to deliver customer-specific scoring, allowing for the identification of relevant threats.

3. Understand the details and context behind indicators and their associated events.

4. Enable analysts to make better, more informed decisions by providing context and situational understanding of threats.

5. Deliver qualified and contextual threat data to automate searching for relevant threats in McAfee Enterprise Security Manager.

Disadvantages:

1. Automation is not easy when required.

References:

1. https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-threat-quotient-esm.pdf

5. Anomali by Anomali

The Anomali integration adds real-time threat intelligence to data logged in McAfee ESM. Threat intelligence is continuously gathered, categorized and risk ranked for severity and confidence in Anomali's ThreatStream platform. The intelligence is then delivered in real-time to McAfee ESM for monitoring and detection of security threats in enterprise infrastructures so that SOC and threat intelligence teams can quickly see high priority threats impacting their businesses.

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, and enriched with risk score to add context and relevance to the delivered information.

Advantages:

1. It has highly versatile data processing capability and data is processed in various formats.

Disadvantages:

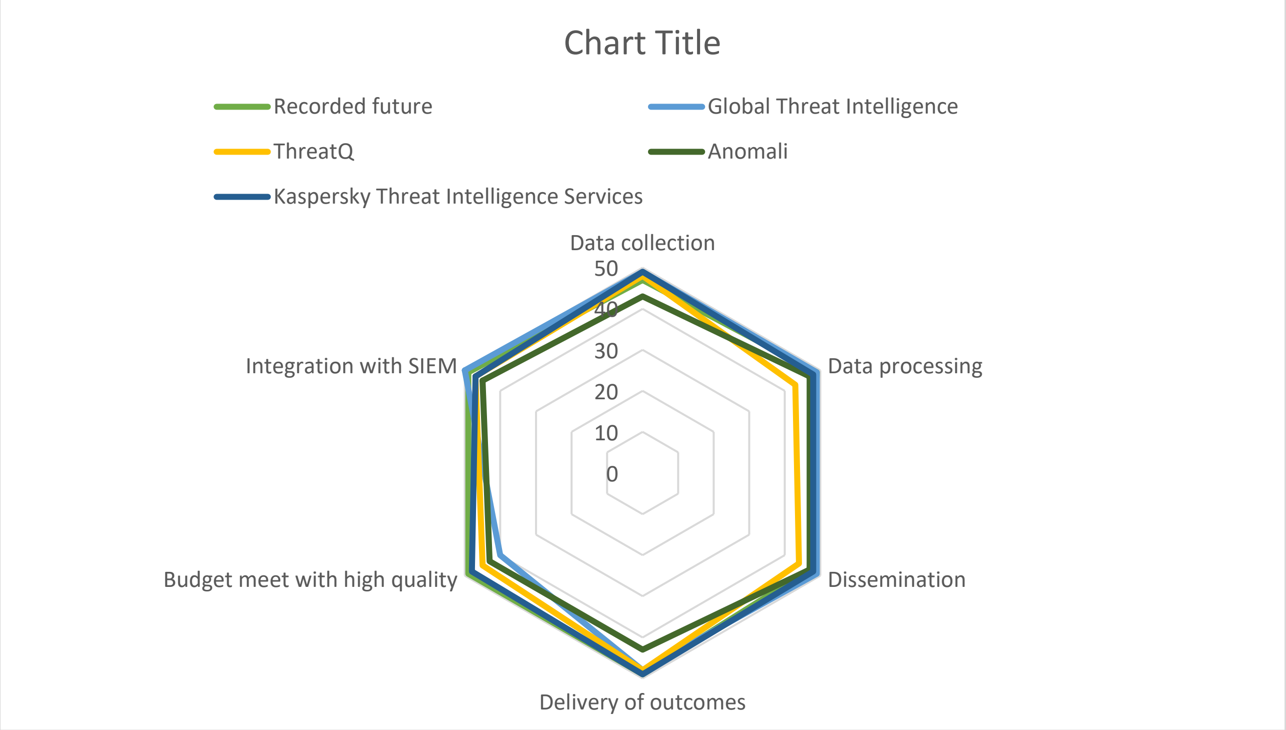
1. It seems to be rigid when it comes to customisation.

Reference:

1. Anomali Furthers Collaboration with McAfee to Provide Real-Time Threat Intelligence to Joint Customers | Anomali

2. Anomali Reviews, Ratings, & Alternatives - Gartner 2021

Radar graph for the above threat intelligence services



Properties	Recorded future (out of 50)	Global Threat Intelligence (out of 50)	ThreatQ (out of 50)	Anomali (out of 50)	Kaspersky Threat Intelligence Services (out of 50)
Data collection	47	49	48	43	49
Data processing	49	49	43	47	48
Dissemination	47	49	44	47	48
Delivery of outcomes	49	48	48	43	49
Budget meet with high quality	49	40	45	43	48
Integration with SIEM	49	50	47	45	47

Recommendation

Based on the above radar graph and the analysis done, I conclude that choosing Recorded Future Intelligence Services by Recorded Future would be the best solution to integrate with McAfee ESM SIEM.

Preference order

Recorded future > Kaspersky Threat Intelligent Services > ThreatQ >Global Threat Intelligence> Anomali