McAfee™
Together is power.

Threat Intelligence Orchestration and Automation

Martin Ohl – Solution Architect EMEA

Threat Intelligence Solutions

To many organizations, Threat Intelligence is a strategic capability. It provides insights to make better decisions that ultimately protect the business. Threat Intelligence solutions give us the opportunity to be more than a technology provider. It provides the opportunity to be a mission partner, strategic to their success. **Tell one story!**

1. Platform-Delivered Services
2. Threat Intel Professional Services
3. TIP Partnerships

Threat Intelligence Solutions

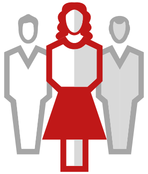
Cloud-Delivered Threat Intel

Problem: Lack of people and process

GTI (Global Threat Intelligence): Prevention with reputations

MVISION Insights: Seamless integrations with ePO leveraging Mcafee GTI, telemetry and research

Outcome: Better protection, seem-less integration, know you if are protected or not, know what campaigns are affecting you



Threat Intel Pro Services

Problem: Immature program, high cost of analysts, closed networks

Assessment: Build a CTI Program.

Intel as a Service: Threat Assessments, Intelligence analyst as a service

pGTI: Threat Intel for closed networks, research, and special requirements, Atlas dashboard

Outcome: Efficient processes, reduce cost, adaptable protection

THREATQ ANOMALI

MISP Threat Sharing eclectic iq

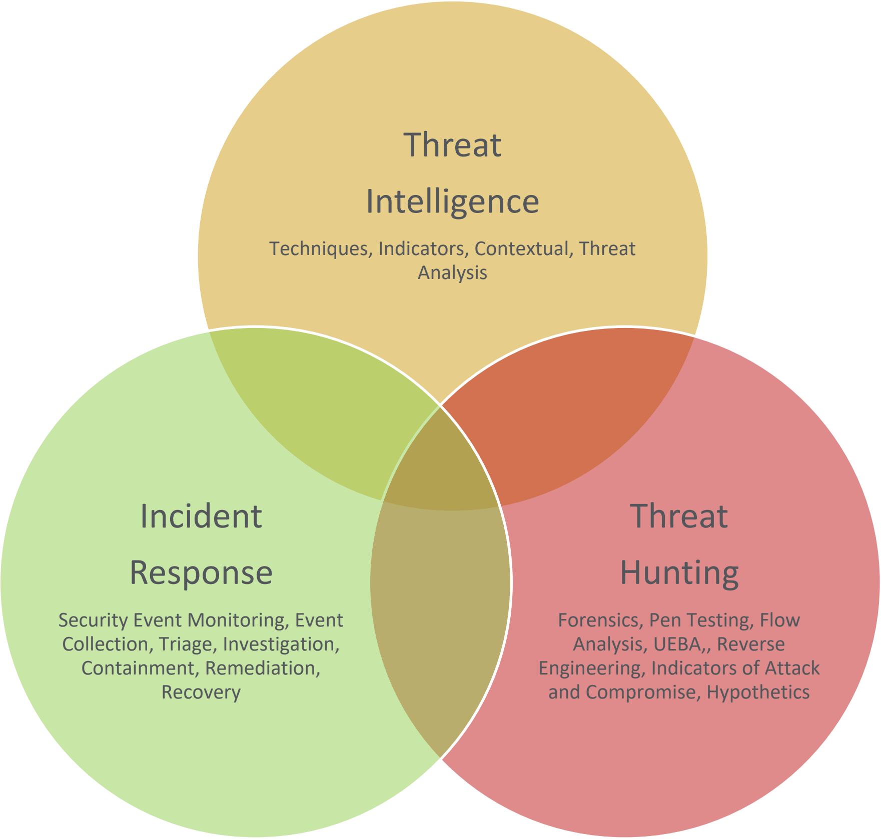
TIP Technology Integrations

Problem: Too much threat data, slow IR and Hunting processes

TIP Integrations: Integrate TIPs with endpoint, network and SIEM through DXL or Pro Services

Outcome: Reduced MTTR, increase value of threat data feeds, increased value of endpoint and network telemetry, intelligence sharing

Security Operations Use Cases



Threat

Intelligence

Techniques, Indicators, Contextual, Threat Analysis

Incident

Response

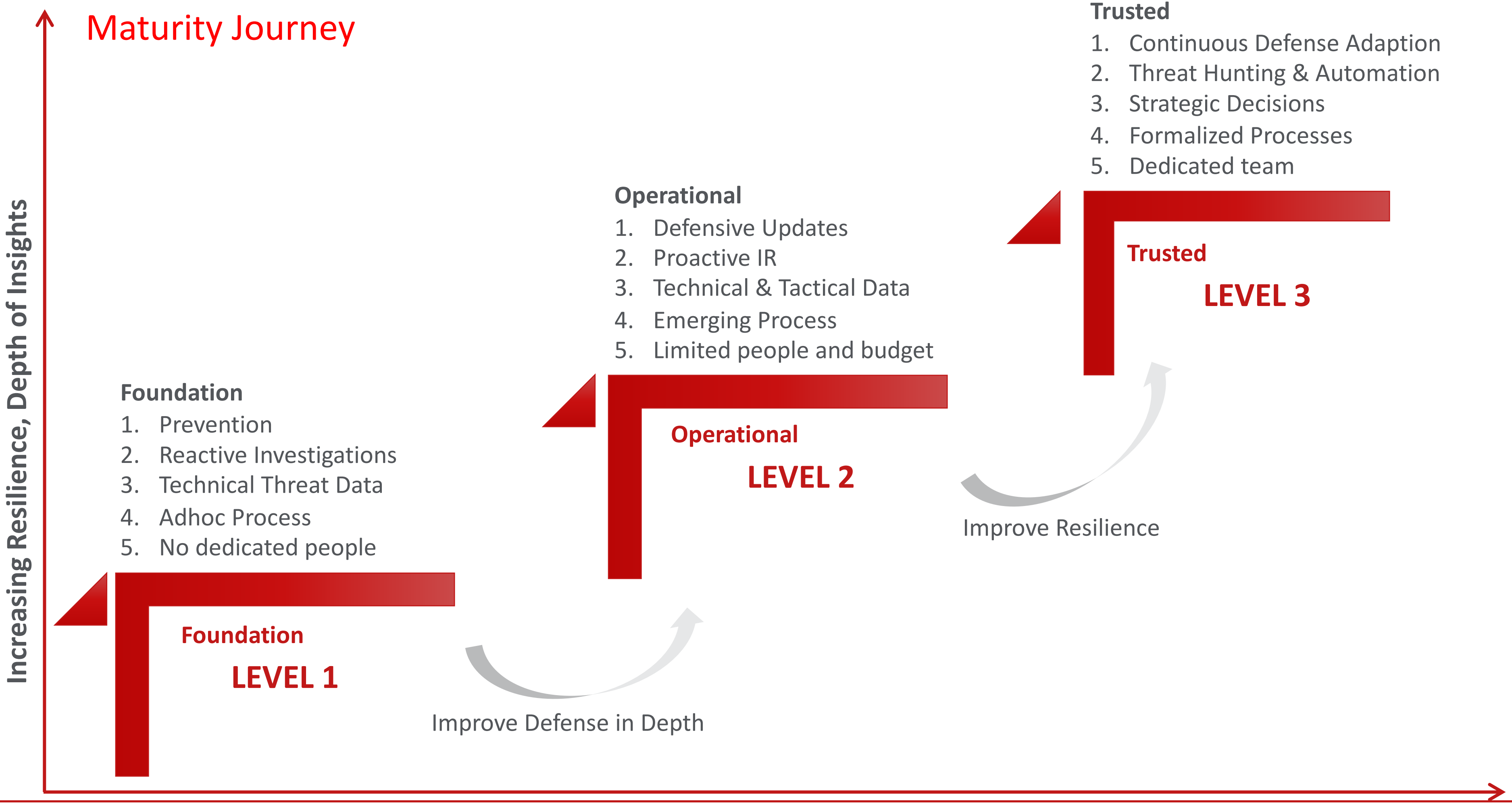
Security Event Monitoring, Event Collection, Triage, Investigation, Containment, Remediation, Recovery

Threat

Hunting

Forensics, Pen Testing, Flow Analysis, UEBA,, Reverse Engineering, Indicators of Attack and Compromise, Hypothetics

Maturity Journey



Foundation

1. Prevention
2. Reactive Investigations
3. Technical Threat Data
4. Adhoc Process
5. No dedicated people

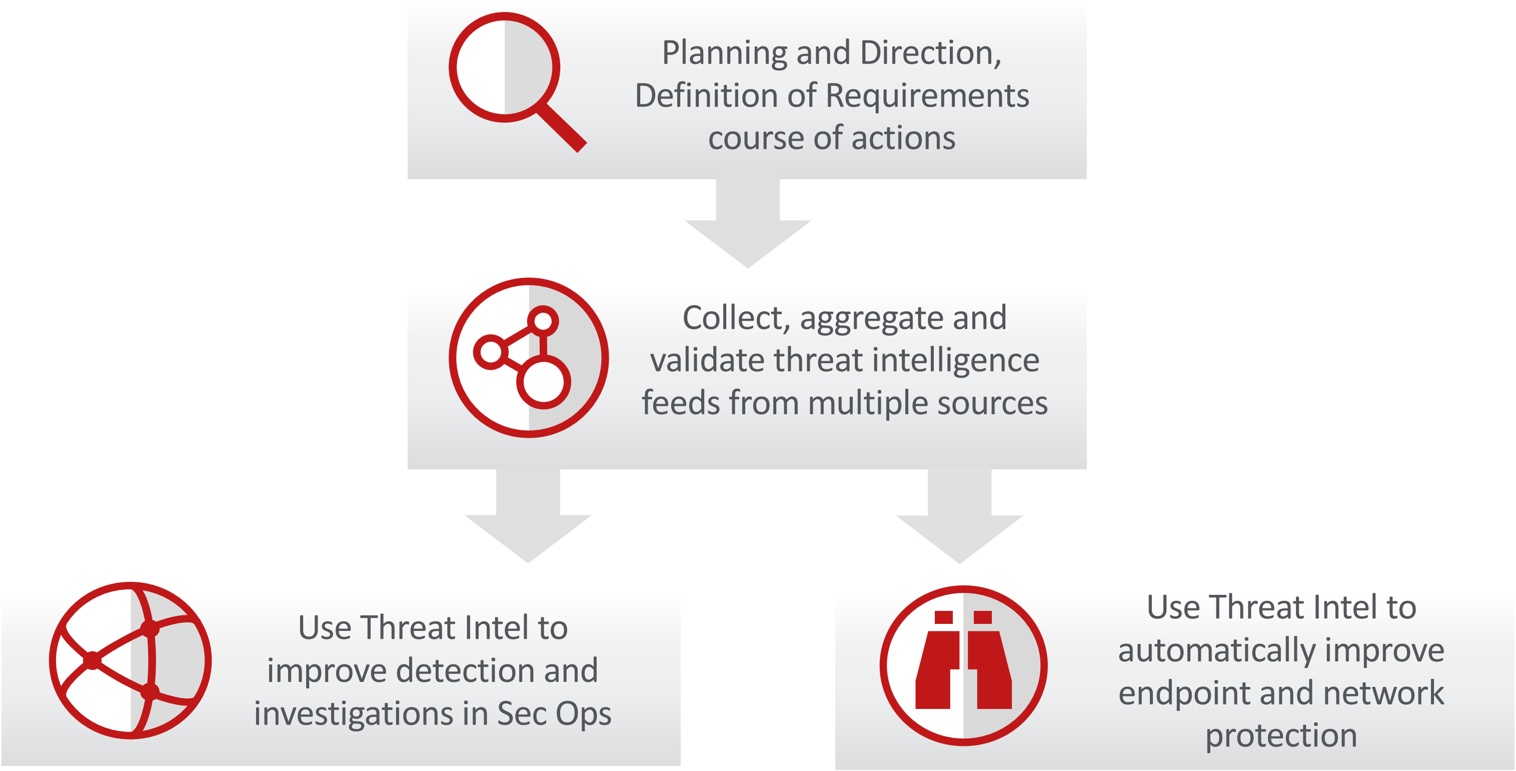
Operational

1. Defensive Updates
2. Proactive IR
3. Technical & Tactical Data
4. Emerging Process
5. Limited people and budget

Trusted

1. Continuous Defense Adaption
2. Threat Hunting & Automation
3. Strategic Decisions
4. Formalized Processes
5. Dedicated team

Threat Intel Common Patterns



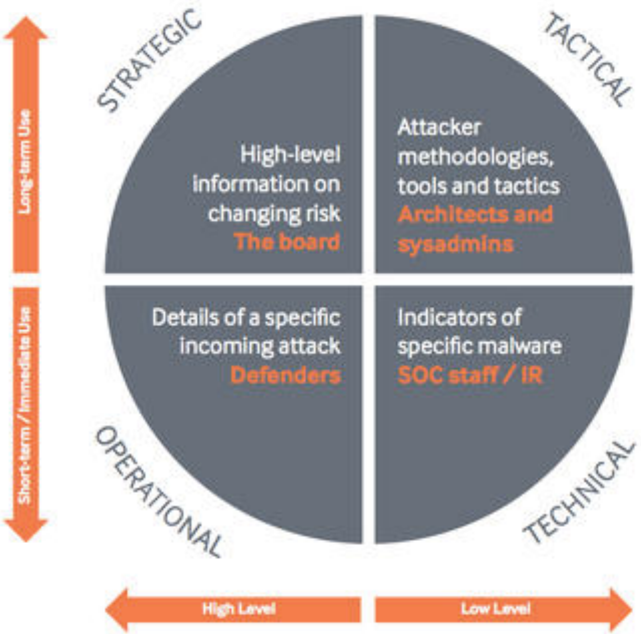
Planning and Direction, Definition of Requirements course of actions

Collect, aggregate and validate threat intelligence feeds from multiple sources

Use Threat Intel to improve detection and investigations in Sec Ops

Use Threat Intel to automatically improve endpoint and network protection

Threat Intelligence Types


STRATEGIC
TACTICAL
OPERATIONAL
TECHNICAL
High-level information on changing risk
The board
Attacker methodologies, tools and tactics
Architects and sysadmins
Details of a specific incoming attack
Defenders
Indicators of specific malware
SOC staff / IR
Long-term Use
Short-term / Immediate Use
High Level
Low Level

CERT Community
Vertical ISACs
Industry Reports
Cyber Kill Chains
Industry Conferences
Independent Researchers

Security Vendors
Threat Intel Vendors
Industry Reports
Vertical ISACs
CERT Community

Threat Intelligence Sources

FINANCIAL SERVICES ISAC

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Global Intelligence

- Intelligence from Global Providers and Open Source
- Reputation, APT Campaigns, Malware Attribution
- Social Media analysis and enterprise specific intelligence

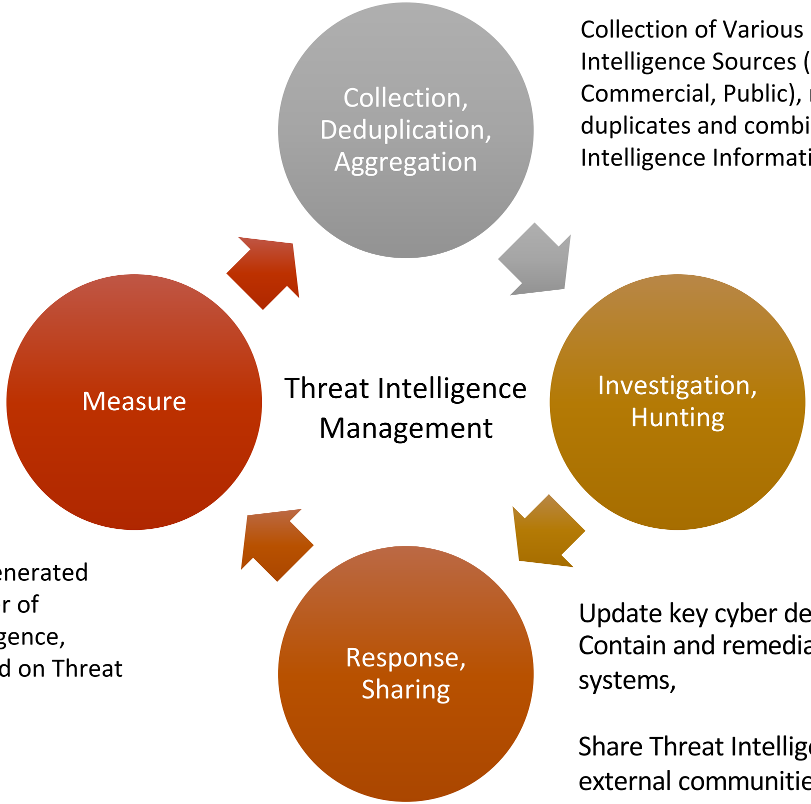
Community Intelligence

- Intelligence from fellow travelers in industry
- Indicators of Compromise
- IP, URL, Domains, Files are common indicators
- STIX/TAXII, OpenIOC, Web Portals, Emails, PDF

Local Enterprise Intelligence

- Intelligence derived from malware analytics
- Intelligence derived from data analytics on the enterprise data and users
- Indicators of Compromise and Attack

Threat Intelligence Process



Threat Intelligence Management

Collection, Deduplication, Aggregation

Collection of Various Intelligence Sources (Local, Commercial, Public), remove duplicates and combine Threat Intelligence Information

Investigation, Hunting

Identify Threat Intelligence related artifacts within the enterprise from historical and real time data sources

Response, Sharing

Update key cyber defenses, Contain and remediate infected systems,

Share Threat Intelligence with external communities and partners

Measure

Reduce MTTR, Number of IOC generated from Threat Intelligence, Number of Incidence generated from Intelligence, Number of Attacks Blocked based on Threat Intelligence

Threat Intelligence Platform (TIP)

Threat Intelligence Platform help organizations to aggregate, correlate and analyze threat data from multiple source to improve security posture

THREAT CONNECT™

Intsights
Detect. Analyze. Remediate.

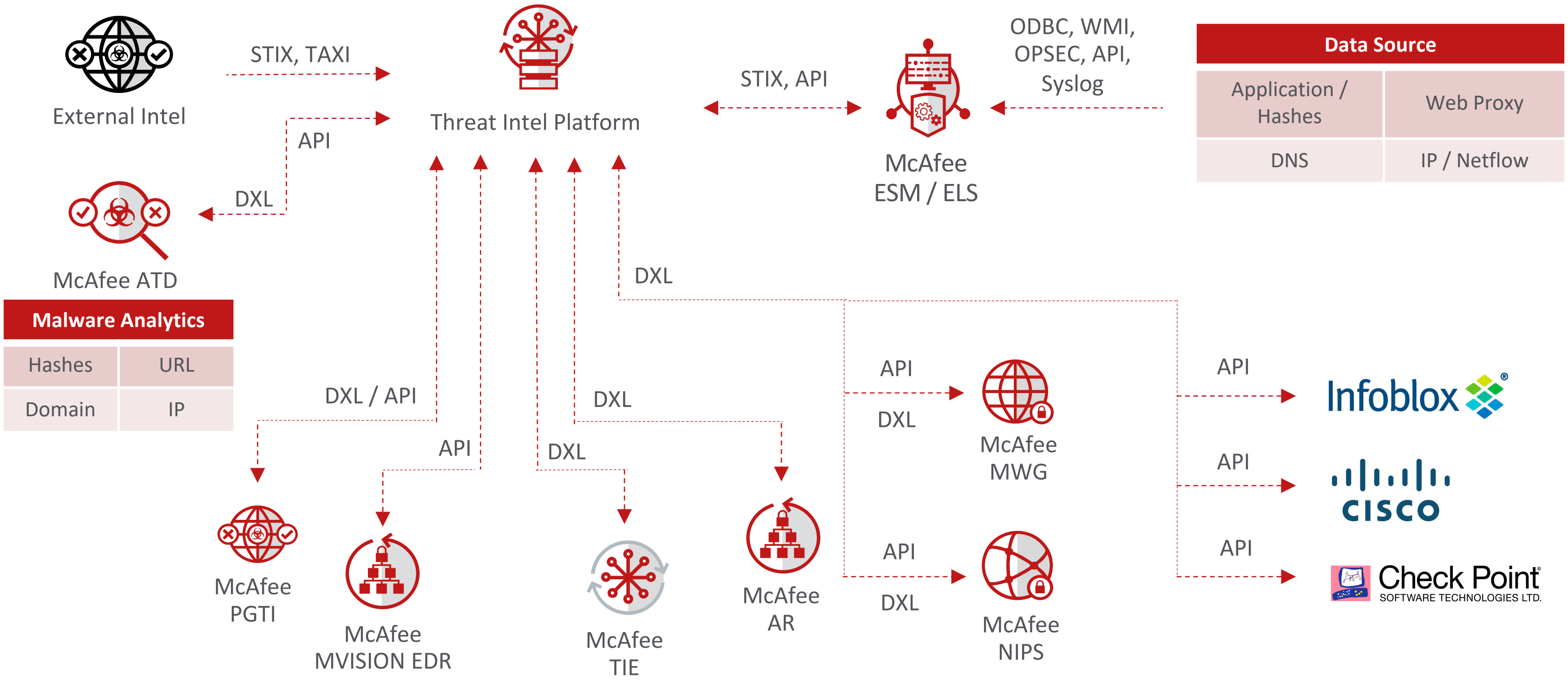
eclectic iq

MISP
Threat Sharing

THREATQ

ANOMALI

Architecture for Threat Intel Automation



External Intel

STIX, TAXI

API

DXL

Threat Intel Platform

STIX, API

McAfee ESM / ELS

ODBC, WMI, OPSEC, API, Syslog

Data Source	
Application / Hashes	Web Proxy
DNS	IP / Netflow

McAfee ATD

Malware Analytics	
Hashes	URL
Domain	IP

DXL / API

API

DXL

DXL

DXL

API

DXL

API

DXL

API

API

API

McAfee PGTI

McAfee MVISION EDR

McAfee TIE

McAfee AR

McAfee MWG

McAfee NIPS

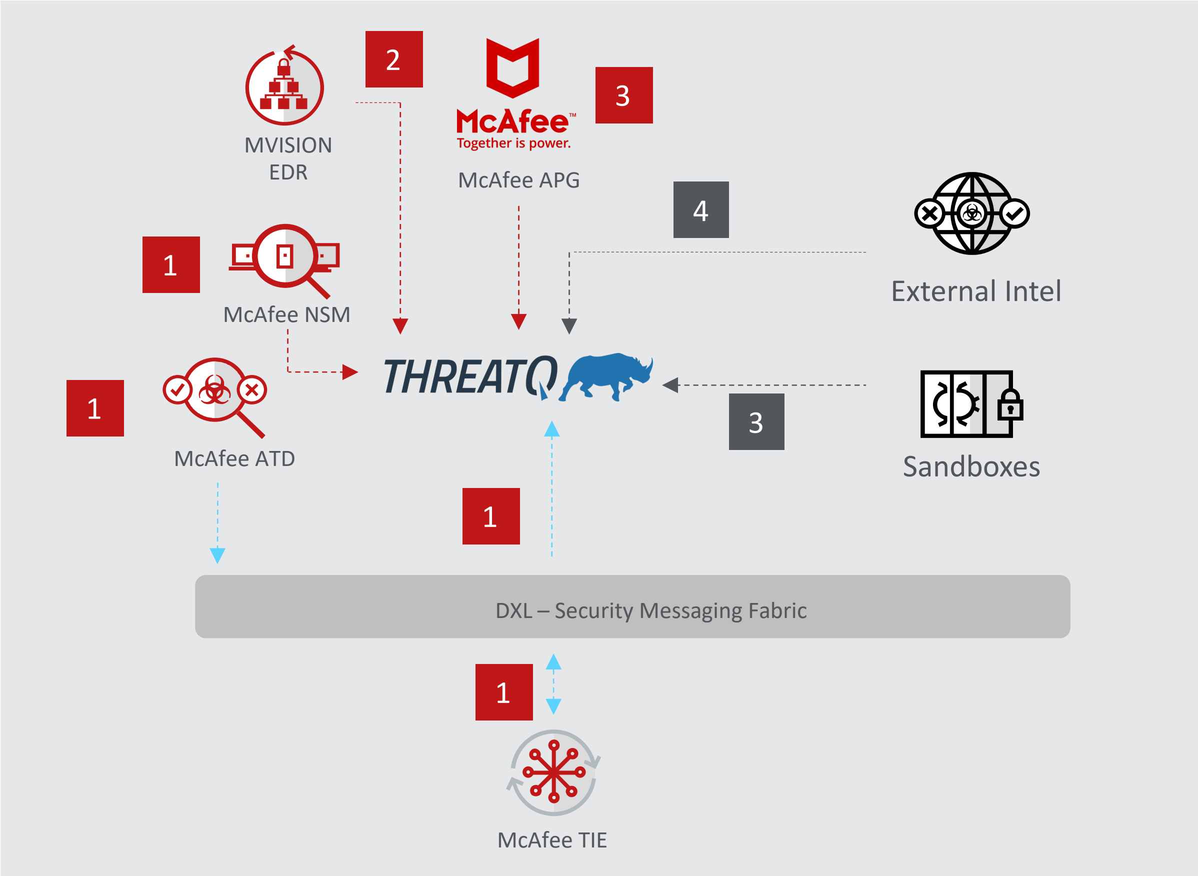
Infoblox

CISCO

Check Point SOFTWARE TECHNOLOGIES LTD.

Threat Intelligence Solution Designs

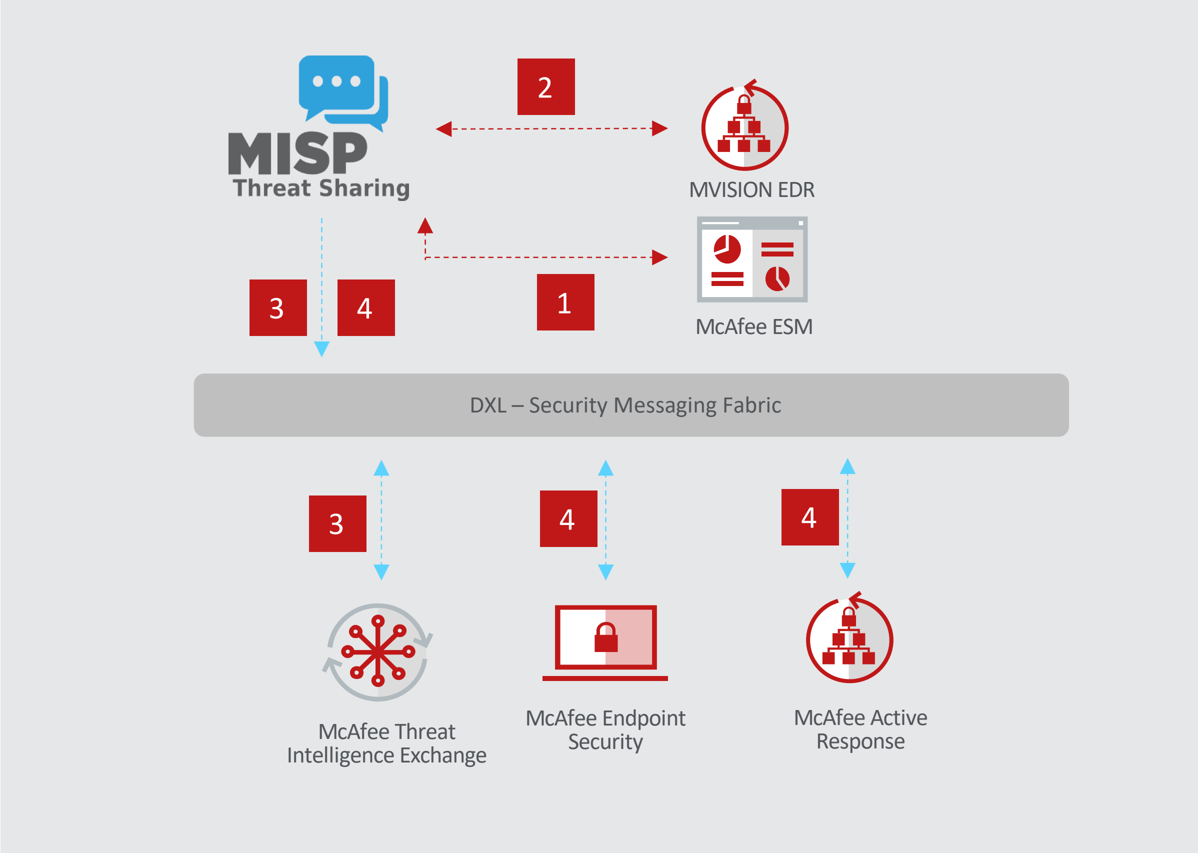
ThreatQ Use Case 1 - Threat Intelligence Aggregation



Scenario Overview

1	ThreatQ receives IOC from McAfee ATD, TIE and NSM
2	ThreatQ subscribed to Activity Feeds from MVISION EDR
3	ThreatQ receives intelligence from McAfee APG
4	ThreatQ receives intelligence from various other sandboxes
5	ThreatQ receives intelligence from various external intelligence feeds

MISP Use Case 2 - Investigation with Threat Intelligence



Scenario Overview

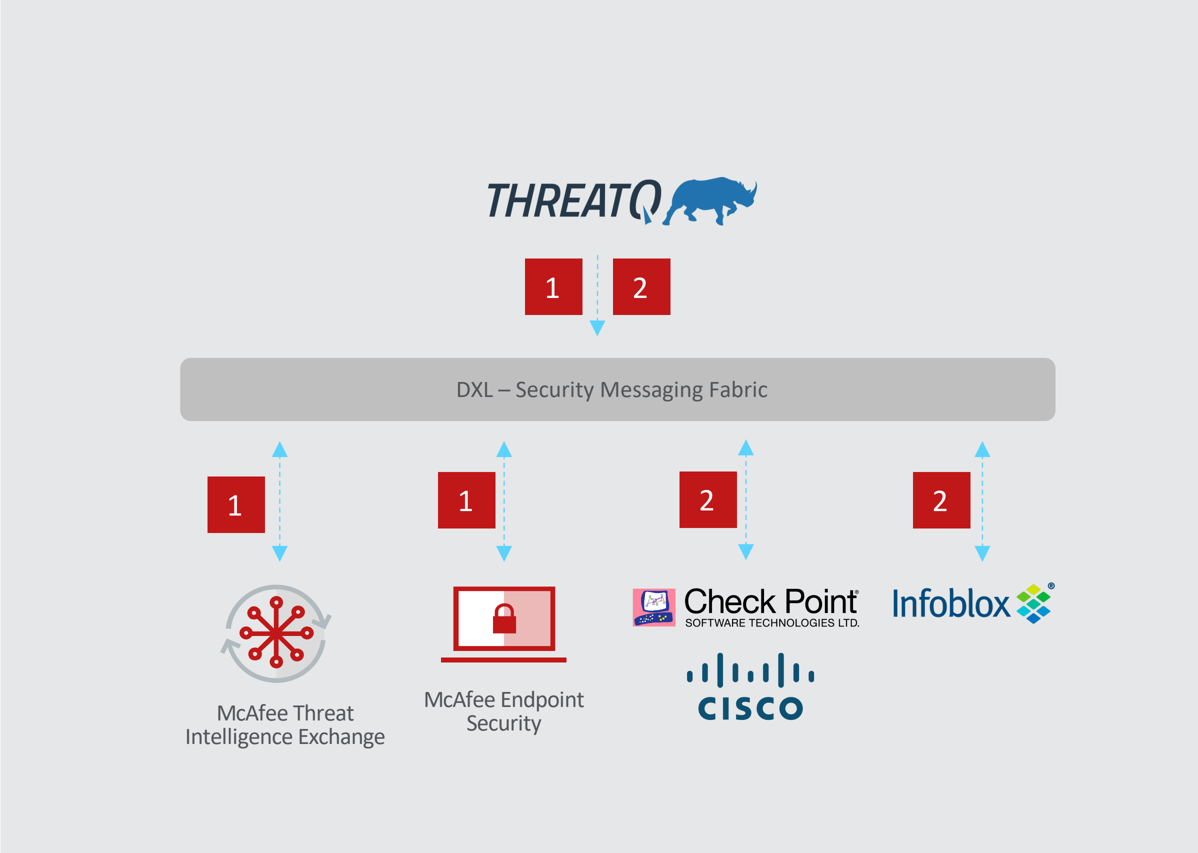
1 MISP exports IOCs via STIX and API for ingest in ESM

2 MISP able to launch new Investigation and query in MVISION EDR

3 MISP launches lookups against TIE

4 MISP launches MAR or EDR lookups as part of an investigation

ThreatQ Use Case 3 - Containment with Threat Intelligence

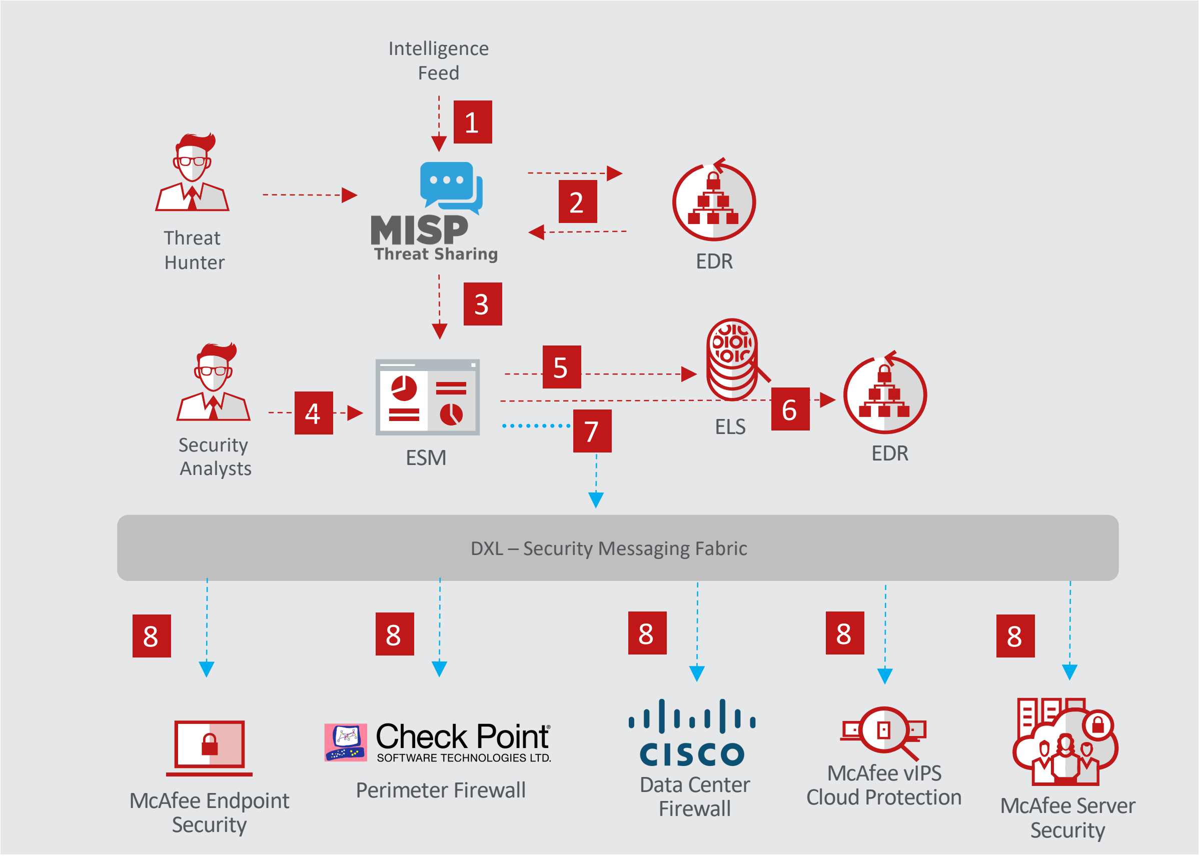

THREATQ
1
2
DXL – Security Messaging Fabric
1
1
2
2
McAfee Threat Intelligence Exchange
McAfee Endpoint Security
Check Point SOFTWARE TECHNOLOGIES LTD.
Infoblox
CISCO

Scenario Overview

1 ThreatQ set Enterprise reputation in TIE

2 ThreatQ sends a DXL message incl IP to update various countermeasures

MISP Use Case 4 - Advanced Threat Hunting



Scenario Overview

Incident Identification

1 MISP receives Intelligence Feeds from various paid and open sources

2 MISP queries for indicators using EDR, analysts prioritizes the intelligence

3 MISP exports intelligence data into ESM via API (Watchlists)

Incident Investigation

4 Analysts receives visual alert

5 Analyst performs validation with ELS

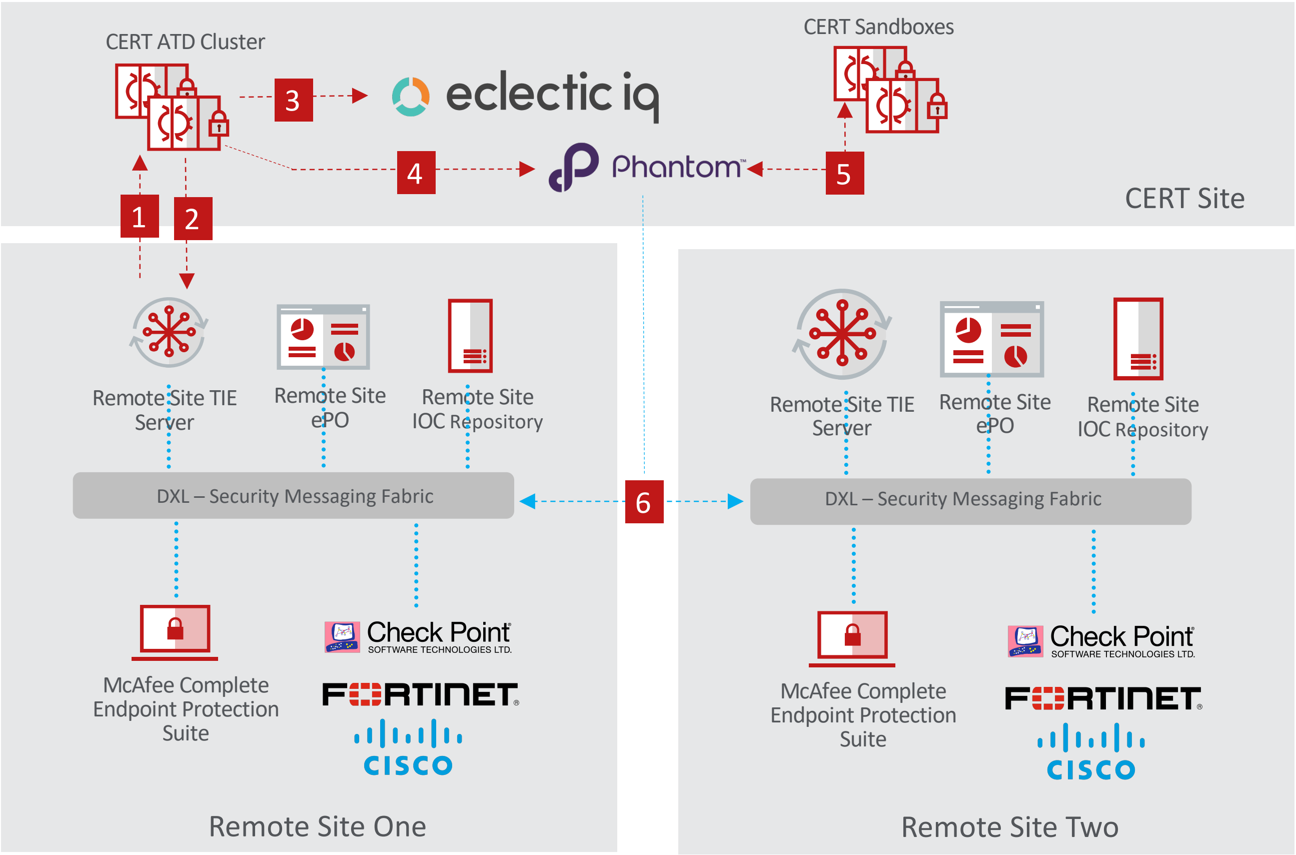
6 Analyst performs scoping with EDR

Incident Containment

7 Analyst uses ESM to update Cyber Defense Countermeasures via DXL

8 Endpoint and Network countermeasures are updated automatically via Security Messaging

Use Case 5 - Multi Department or Agency Intelligence Sharing


CERT ATD Cluster
3
eclectic iq
CERT Sandboxes
4
Phantom
5
CERT Site
1
2
Remote Site TIE Server
Remote Site ePO
Remote Site IOC Repository
DXL – Security Messaging Fabric
6
McAfee Complete Endpoint Protection Suite
Check Point SOFTWARE TECHNOLOGIES LTD.
FORTINET
CISCO
Remote Site One
Remote Site TIE Server
Remote Site ePO
Remote Site IOC Repository
DXL – Security Messaging Fabric
McAfee Complete Endpoint Protection Suite
Check Point SOFTWARE TECHNOLOGIES LTD.
FORTINET
CISCO
Remote Site Two

Scenario Description

1 TIE Server sends suspicious file received form an endpoint to ATD via HTTPS using REST API

2 File Analysis results automatically sent back to site TIE server via HTTPS and REST API

3 IOC Information shared with Threat Intel Platform (EclecticIQ)

4 Phantom receives notification of new file and retrieves file from ATD

5 Phantom sends file to additional sandboxes and receives results

6 Phantom publishes convicted file hashes and other IOC information via DXL to remote site TIE servers and IOC Repository

McAfee™

Together is power.