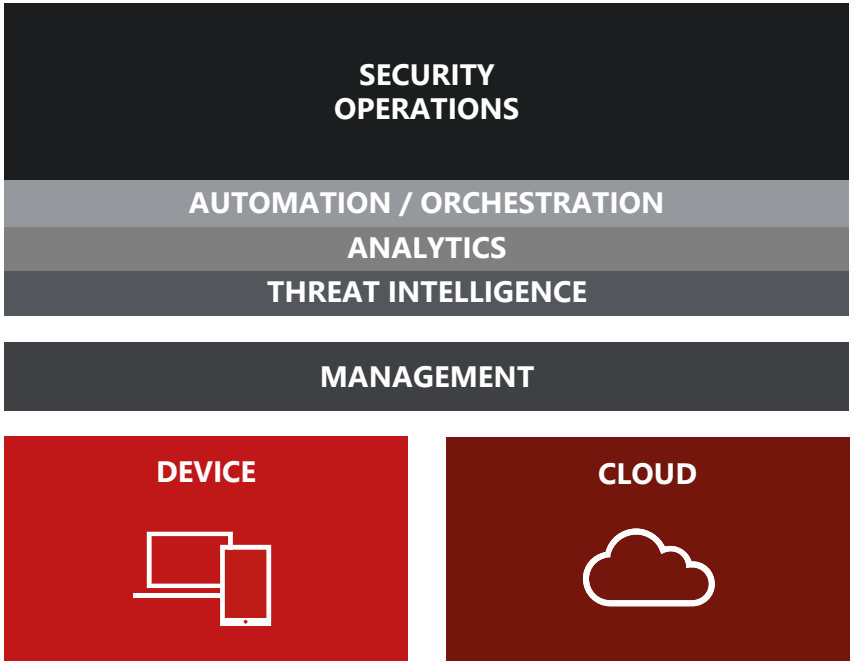
McAfee
Together is power.

Future Proofing Security Operations

Martin Ohl – Solution Architect EMEA

Security Operations

Stakeholder in enterprise resilience



Security Operations

Is part of a Data Protection Strategy

Is Part of a Threat Protection Strategy

Is Part of a Workplace Protection Strategy

Is Part of a Cloud Protection Strategy

Is Part of a ICS Protection Strategy

Is Part of a GDPR and NIS Compliance Strategy

Security Operations is critical to your security strategy!

Incident Response Management

Customer requirements

Reduce Mean Time to Respond (MTTR)

Improved Operational Efficiency

- Consolidate tooling and platforms to maximize available employees
- Utilize automation and orchestration to increase process speed, accuracy, and capacity

Time to Identify	Time to Investigate	Time to Contain
Improved Security Effectiveness		
Utilize sensors, analytic, and intelligence to improve indicator of attack detection and triage	Utilize analytics and intelligence combined with the right data to validate and scope an incident	Utilize interoperability, process control and automation to rapidly block indicators and contain affected assets

SOAPA

Technology reference

Cloud-based services and delivery:

- SaaS Applications
- Platform and Infrastructure
- Managed as a service (MSP)
- Analytics, shared threat intel

Automation and Orchestration layer

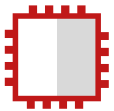
SIEM, network forensics, EDR, TIP, IRP, UEBA …

Analytics layer

Software services and integration layer

Security Controls:

- Remediation
- Policy updates



- Publish/subscribe
- Transaction processing
- Message bus …

Common distributed data services

- Collection
- Normalization
- De-duplication
- Compression/encryption …

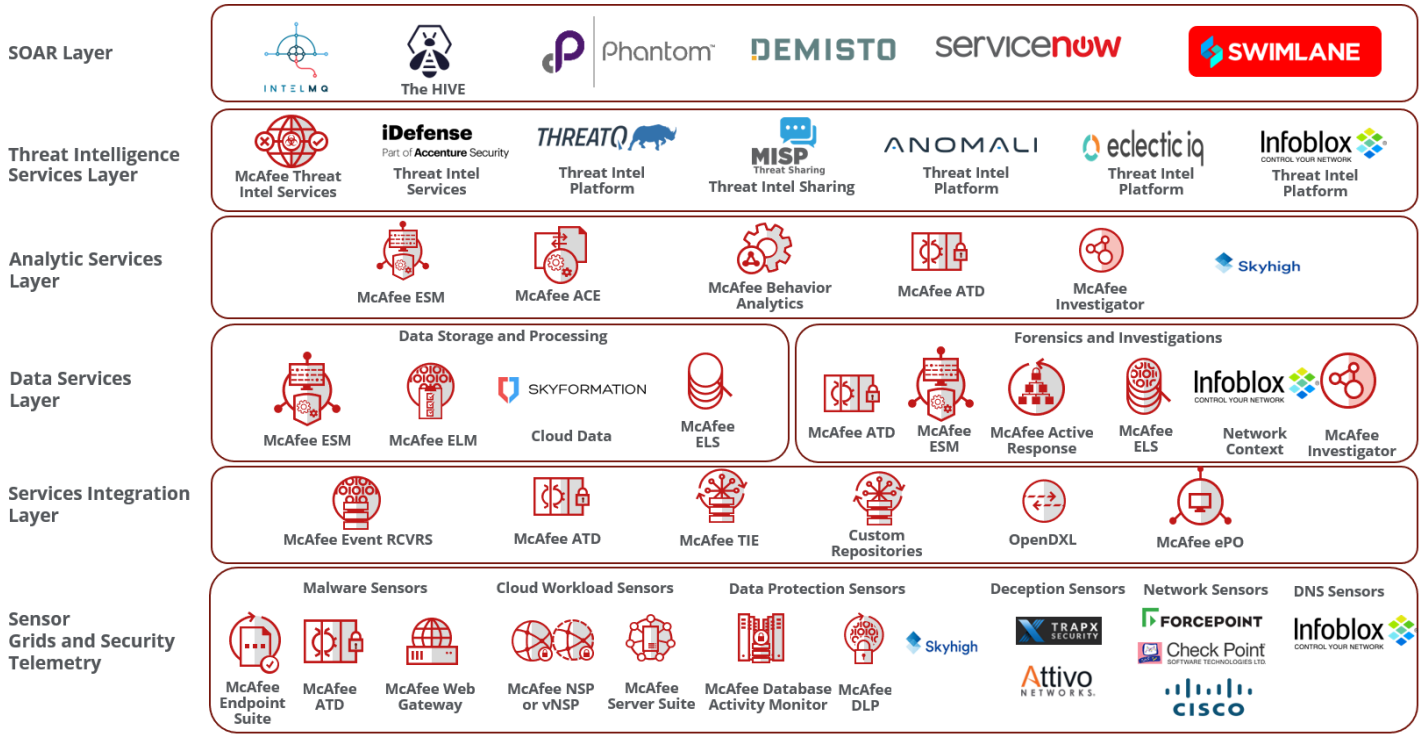
Security Telemetry

(Logs, flows, network and host sensors, threat intelligence, IAM, cloud services, vulnerability, …)

Source: Enterprise Strategy Group, 2017

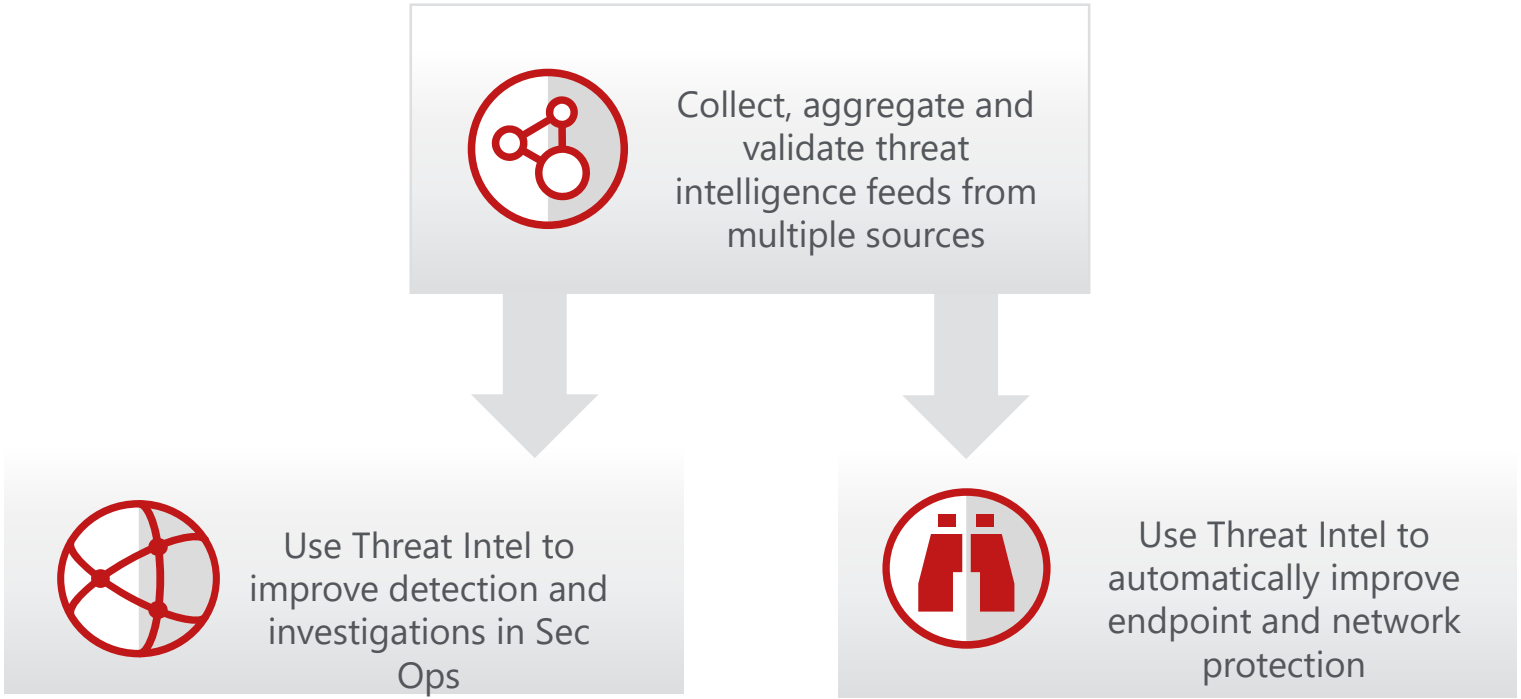
Security Operations Architecture

McAfee® security operations reference architecture

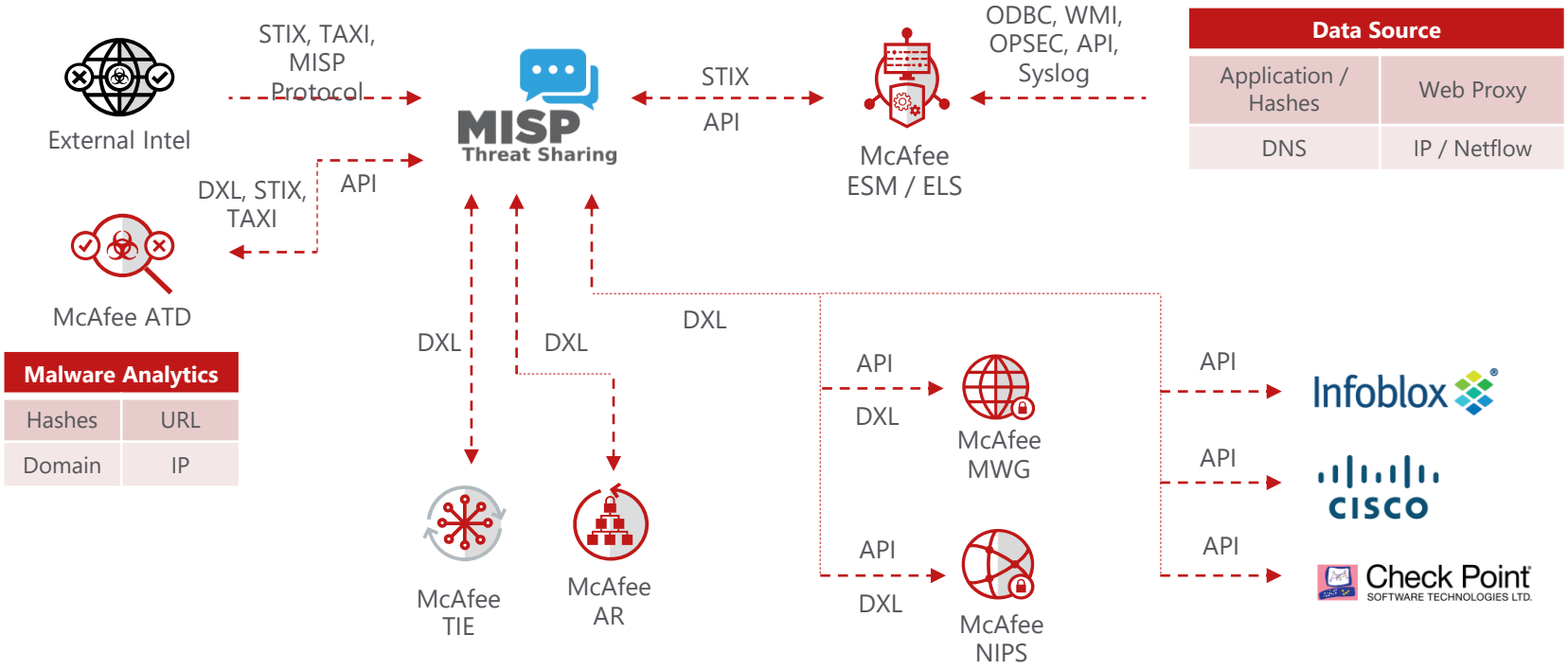


Threat Intelligence Solution Designs

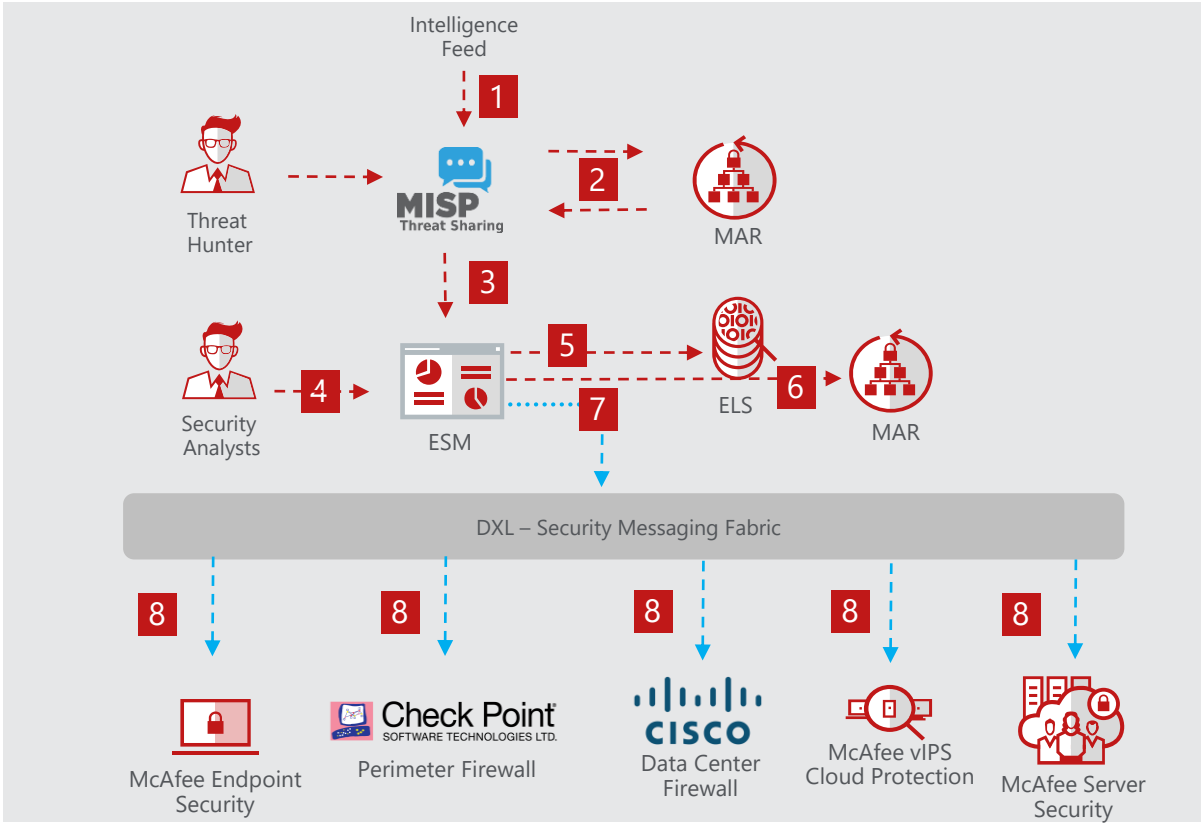
Threat Intel Common Patterns



High Level Architecture Diagram



Security Operations Simulations



Scenario Overview

Incident Identification

1. MISP receives Intelligence Feeds from various paid and open sources
2. MISP automatically queries for indicators using MAR, analysts prioritizes the intelligence
3. MISP exports an intelligence alert into ESM in STIX format

Incident Investigation

4. Analysts receives visual alert
5. Analyst performs validation with ELS
6. Analyst performs scoping with MAR

Incident Containment

7. Analyst uses ESM to update Cyber Defense Countermeasures via DXL
8. Endpoint and Network countermeasures are updated automatically via Security Messaging

Security Operations Simulations

Threat intelligence scenario

Process Efficiency Goals

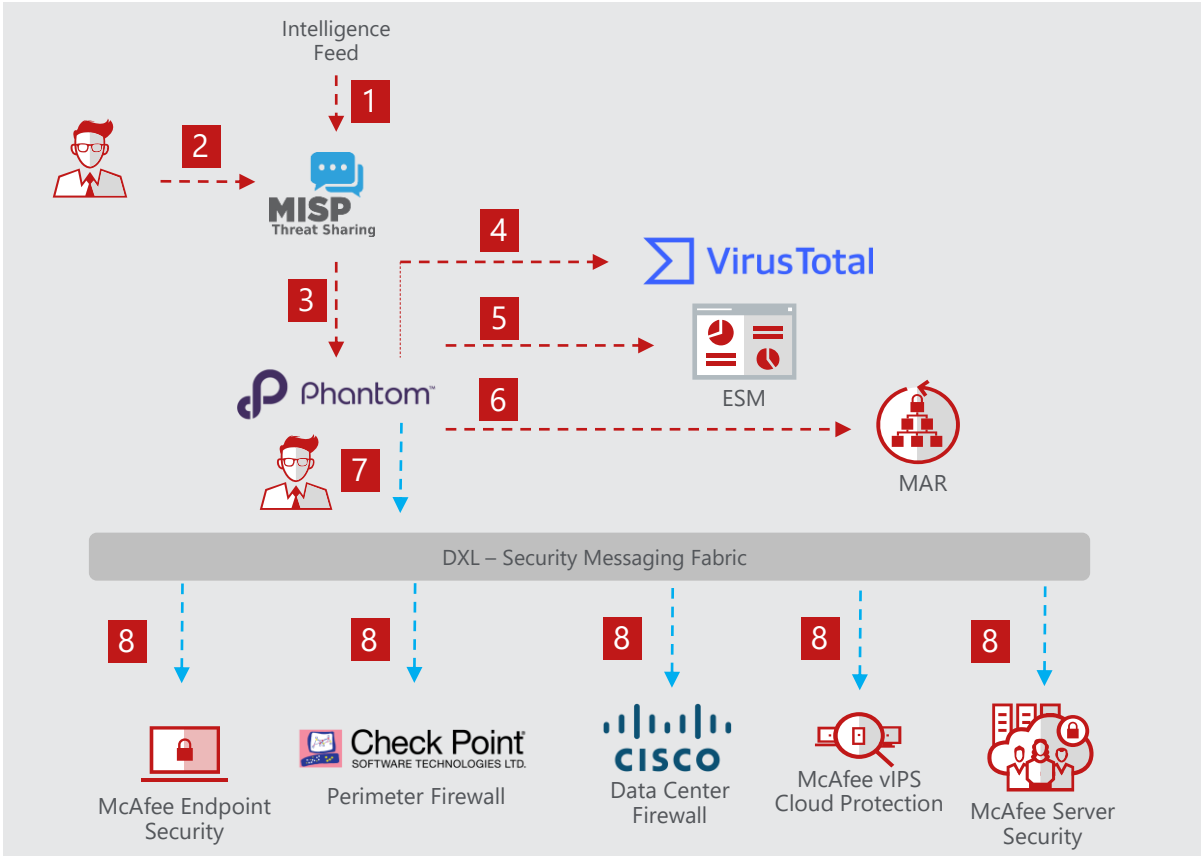
2 Analysts in this Use Case Accessed **3 Consoles** Only

AVG 60 % Process Automation with **MTTR of Under 9 Minutes**

Security Effectiveness Goals

Time to Identify	Time to Investigate	Time to Contain
Detection: Threat Intelligence	**Investigation:** McAfee® ESM, McAfee® ELS, McAfee® MAR	**Containment:** McAfee® ESM, DXL, Third-Party
Process Automation: **High, 85%**	**Process Automation:** **Low, 20%**	**Process Automation:** **High, 70%**
Analysts: 1	Analysts: 1	Analysts: 0
Consoles: 1	Consoles: 2	Consoles: 1

Security Operations Simulations



Scenario Overview

Incident Identification

1. MISP receives Intelligence Feeds from various paid and open sources
2. Analyst prioritizes the intelligence via tagging
3. Phantom pulls tagged events including artifacts

Incident Investigation

4. Phantom checks reputation with Virustotal
5. Phantom performs historical checks with McAfee ESM
6. Phantom performs automated Active Response Lookups

Incident Containment

7. Analyst approves containment actions
8. Endpoint and Network countermeasures are updated automatically via Security Messaging

Security Operations Simulations

Threat Intelligence Automation Scenario

Process Efficiency Goals

2 Analysts in this Use Case Accessed **2 Consoles**

95% Process Automation with **MTTR of about 6 Minutes**

Security Effectiveness Goals

Detection:
Threat Intelligence, McAfee® ATD

Process Automation:
100
Analysts: 1
Consoles: 1

Investigation:
McAfee® AR, McAfee ATD, Intelligence

Process Automation:
100
Analysts: 0
Consoles: 0

Containment:
McAfee® ESM, DXL, Third-Party

Process Automation:
90
Analysts: 1
Consoles: 1