McAfee by Intel

GDPR

Opportunity for Security Transformation

Mo Cashman
Director, Enterprise Architects
Intel Principle Engineer
EMEA

How is *Your* Strategy Evolving?

Threats

Defenses

Environments

Threat Evolution - Changing and Familiar Face of Hacking

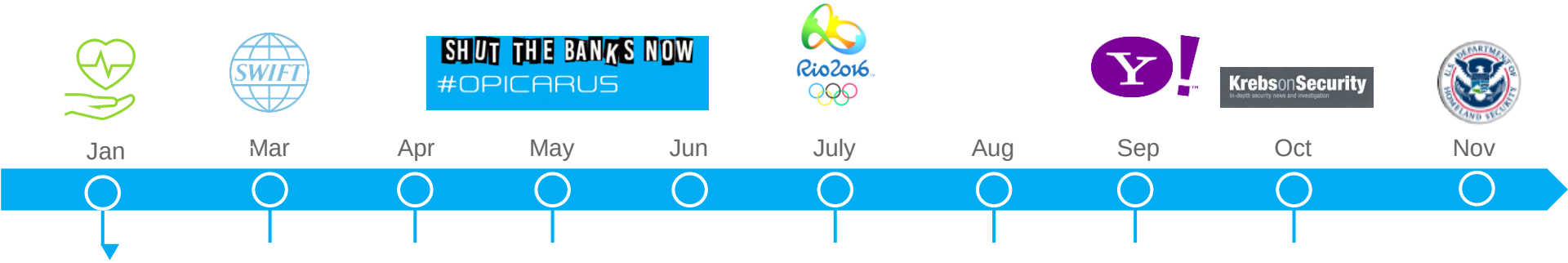
Cybercriminals / Organized Crime

Recreational / Vandals

Hacktivism / Reputation Attacks

State Sponsored Cyberespionage Cyberattacks

Threat Evolution – Key Cyber Incidents in 2016



Healthcare
Ransomware Attacks

Financial
Attacks on SWIFT Network

IOT
German Nuclear Malware Attack

Financial
OpIcarus DDoS Attacks

Reputation
WADA/IOC Attacks

State
South Korean Attacks

Yahoo
Breach Disclosure

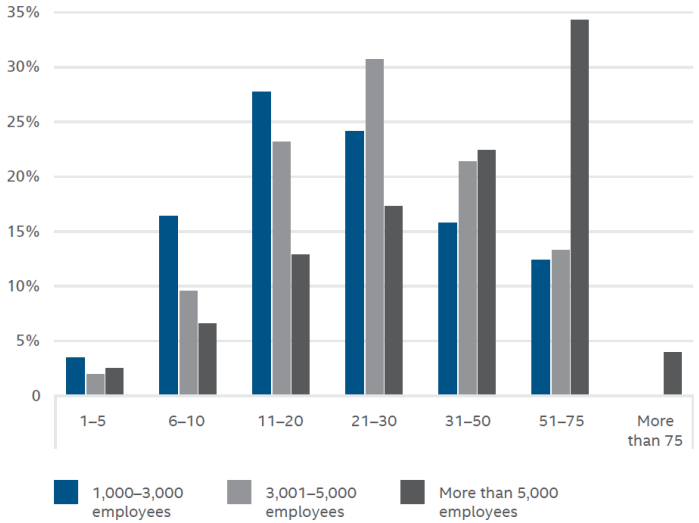
Krebs / Dyn
DDoS Attacks

Grizzly Steppe
US Election/DNC

Verticals and GDPR
Which could be most affected?

Enterprise Size

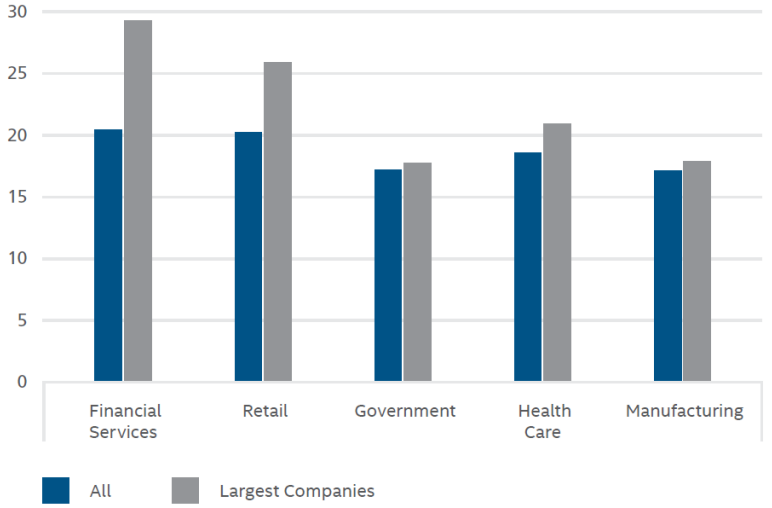
Average number of data loss incidents per day



Source: *Intel Security 2016 Data Protection Benchmark Study.*

Vertical Industry

Average number of data loss incidents per day



Source: *Intel Security 2016 Data Protection Benchmark Study.*

Digital Transformation and GDPR

IT Factors impacting Regulatory Compliance

Device and Data Proliferation

Increased Attack and Loss Surface as users go mobile and businesses become more data rich

Cloud Services

Increase risk of loss as more data and services are moved to or delivered from the cloud

DevOps

Applications are developed and put into production with vulnerabilities that can lead to data exposure

Environment Evolution – Cloud Services and GDPR

What are the key questions I need to ask of my CSP?

What are my responsibilities for security?

I don't have expertise, I need security as a service

Data Security and GDPR

What are the key challenges?

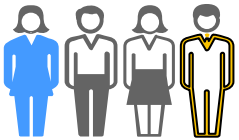
Lost Devices

About 40% of all data exfiltration incidents are reportedly carried out with the use of physical media.

External Attackers

About 59% of data loss incidents are the result of malware or application exploits from external attackers

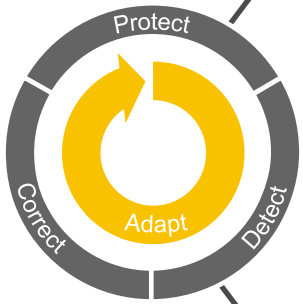
Employees and Suppliers



About 57% of data loss incidents are the result of accidental or malicious insider activity

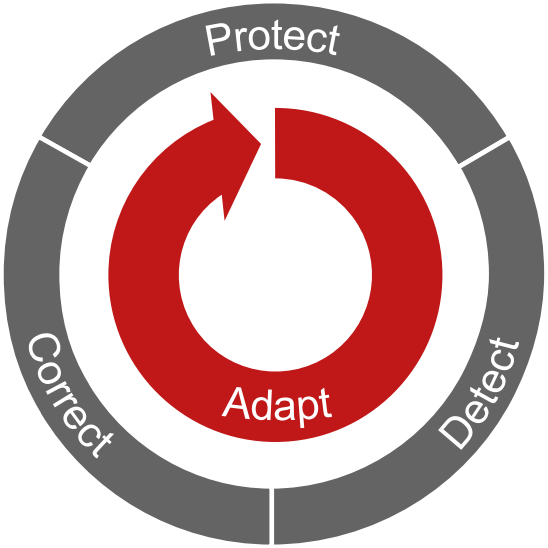
Over 50% of data loss incidents discovered externally!

Defensive Evolution – Thinking Security Outcomes



Neutralize Advanced Persistent Threats	Advanced Threat Protection, Detection and Response
Protect Customer and Business Data	Data Loss Protection for Data in Use, At Rest, in Motion anywhere
Protect Critical Environments	Threat Protection and Visibility for Datacenter, Cloud servers and apps
Optimize Security Operations	Fast Threat Detection and Response

Defensive Evolution – Think Security Capability



PROTECT – Continuous discovery and attack surface reduction against accidental, intentional and unintentional incidents across enterprise and cloud operating environments.

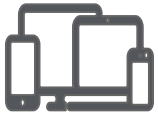
DETECT – Continuous processes and orchestrated workflows to identify, analyze and validate key indicators of a data breach and understand the full scope of a data breach

CORRECT – Efficient processes and orchestrated workflows to contain a breach through pre-planned response actions such as privilege and data isolation

ADAPT – Orchestrate protection updates and automated intelligence-sharing to identify or prevent a reoccurrence of an attack in the enterprise, cloud or industry partnerships

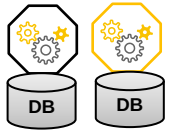
Solution Design: Protection Capability

Covering the Attack Surface



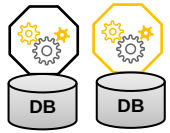
Mobile Devices and Office Services

Cloud Storage



Databases

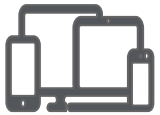
SaaS Services



Apps and API

Privileges

Covering Loss Vectors



Accidental Device Loss

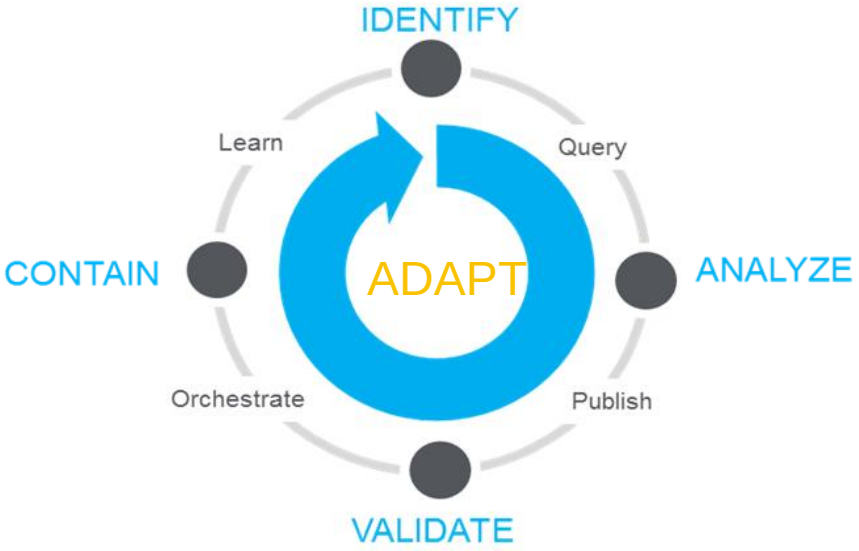
Policy Violations

Cloud Services

Malicious Exfiltration

Insider Threat

Solution Design: Detection and Correction Capability



Triage Workflow

- Data analytics to produce indicators of compromise
- Historical Data Hunting and Analysis
- Real Time Endpoint Hunting and Analysis

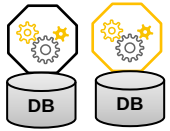
Response Actions

- Host Isolation
- Data Isolation
- User Isolation

Solution Design: People and Process Capability

Discovery and Classification

Identity and Access



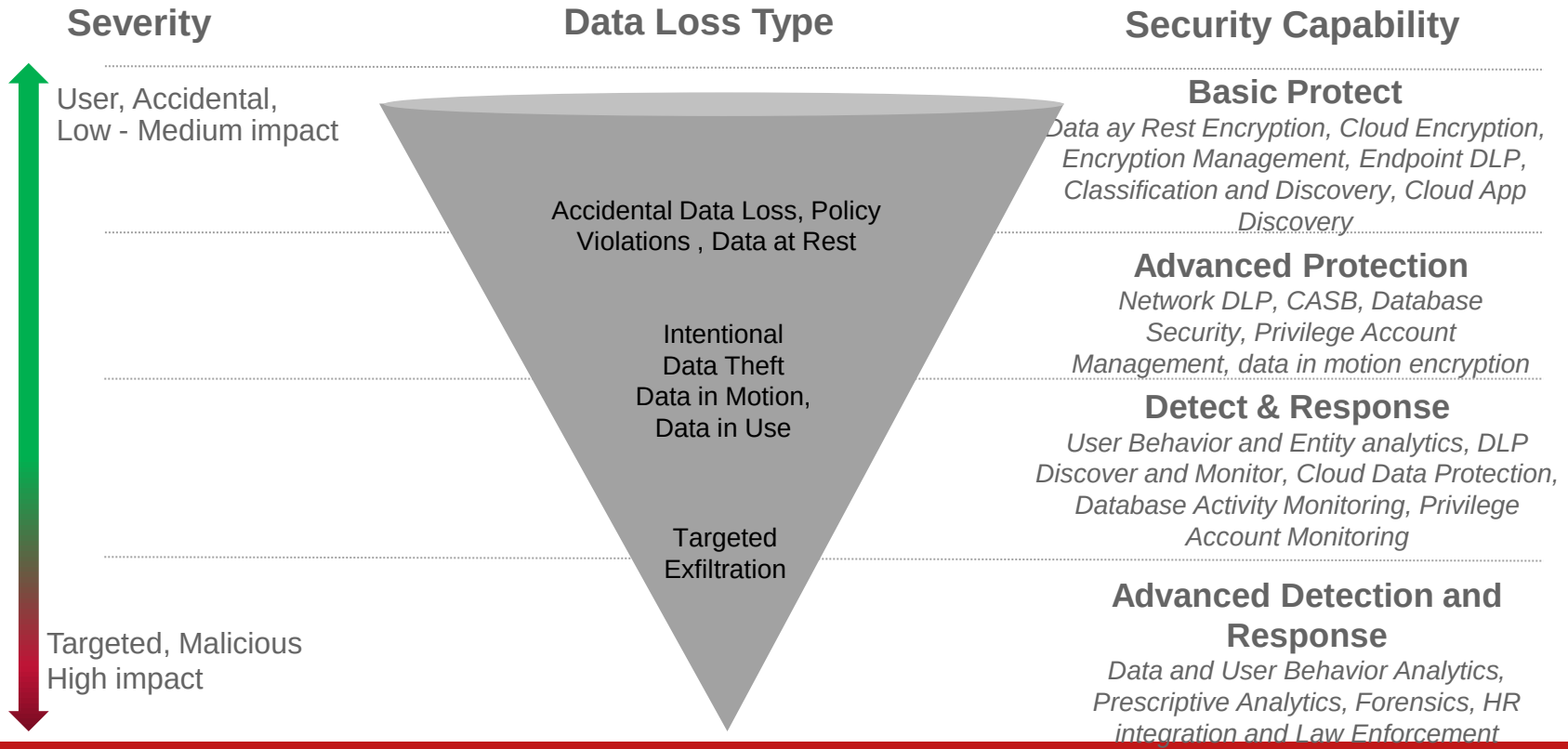
Database Security

Breach Detection

Management Reporting

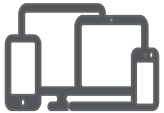
How can McAfee help?

General Capability Alignment



How can McAfee help?
General Capability Alignment

Concerned about Physical Device Loss



- File and Removable Media Protection
- Full Disk Encryption
- Management of Native Encryption
- ePO for Compliance Reporting

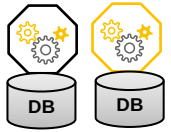
Insider Threat Breach Prevention and Detection

- DLPe, DAM, DLPn, Web Gateway
- Sec Ops Professional Services
- ESM for Log Collection and Monitoring
- Interset User Behavior Analytics

Adopting Cloud Services

- DLPe, Web Gateway, DLPn and CASB
- Data Center Security Suite
- ESM Log Collection and Monitoring
- Interset User Behavior Analytics

Secure Digital Applications

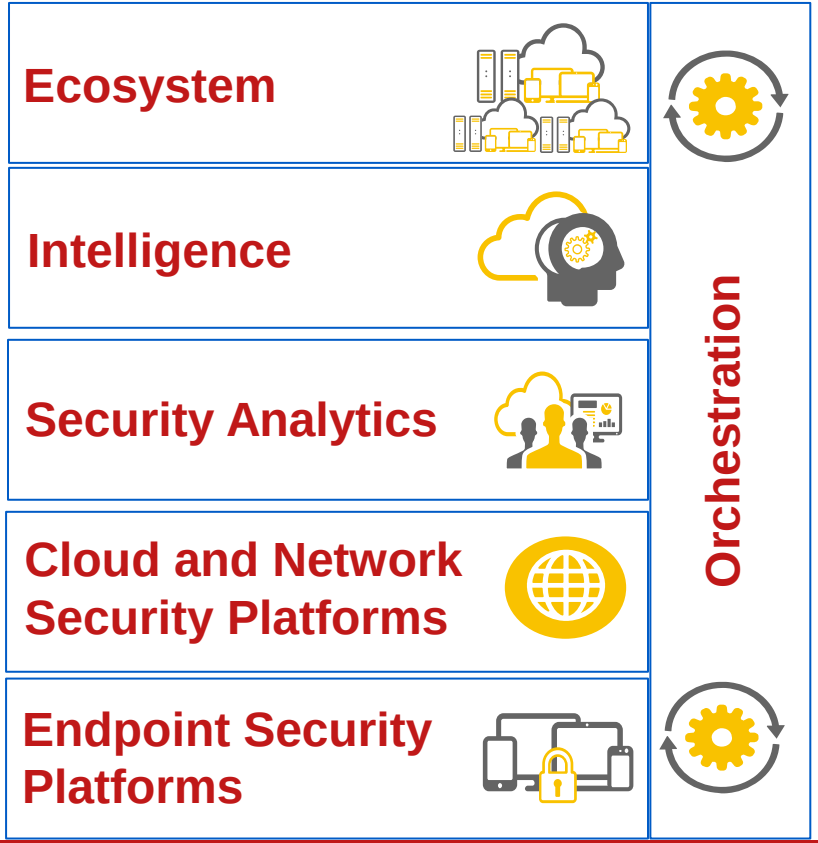


- Database Activity Monitoring
- App Security Professional Services
- ESM Log Collection and Monitoring

How can McAfee help?
Protecting Cloud Services

Governance Measures	Areas McAfee can contribute to risk mitigation
Data Security	McAfee Pervasive Data Security solutions protect data at rest, in motion and in use
Infrastructure Security	McAfee Hybrid Data Center and Advanced Threat Protection solutions protect critical servers and applications on the enterprise or in the cloud
Beach Detection and Response	McAfee Intelligent Security Operations solution and services provides diagnostics and visibility to proactively identify data exfiltration
Access Control	Database Activity Monitor provides control and visibility over access to sensitive databases
Data Usage and Export	McAfee Pervasive Data Security solutions protect data in use or in motion
Data Residency	McAfee Pervasive Data Security solutions help discover and classify sensitive data to simplify the application of the appropriate controls
Prove Compliance	McAfee ePO and ESM provide central reporting and policy management for data security

Defensive Evolution – Think Security Systems



Are you Platform-Ready?

Do you want to accelerate Security Maturity growth?

Planning to build standardized cyber defense platform to simplify management?

Do you have a business driver to reduce cost or improve efficiency of security in general?

Do you want to improve situational awareness and risk management decisions?

Do you want to enable and simplify cross product integration to improve security effectiveness?

Prove the Value

85%
Less People and Technology Required for Endpoint Data protection

90%
Less training required to operate DLP Endpoint

100 %
Of SANs recommended Controls

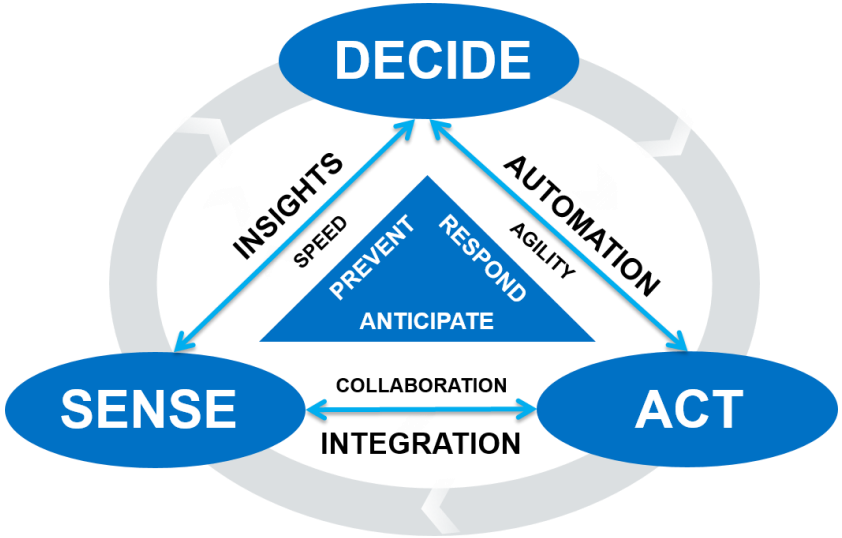
45%
triage automation

11 Min
Average Time to Respond*

100 %
Response Actions**

*internal testing
**with SIA Partners

Defensive Evolution – Think Automation and Orchestration



Compress the OODA Loop

What is safe to do?

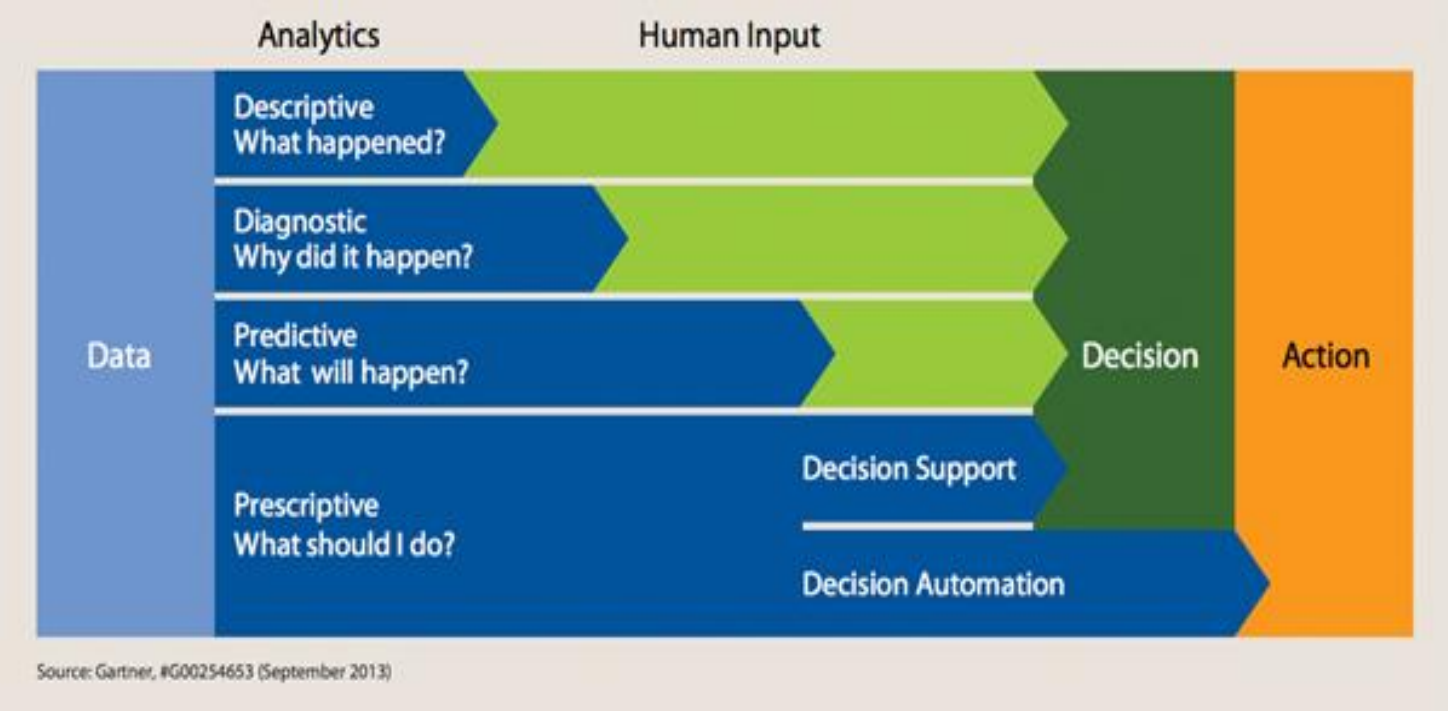
Automated Threat Analysis

Triage Automation

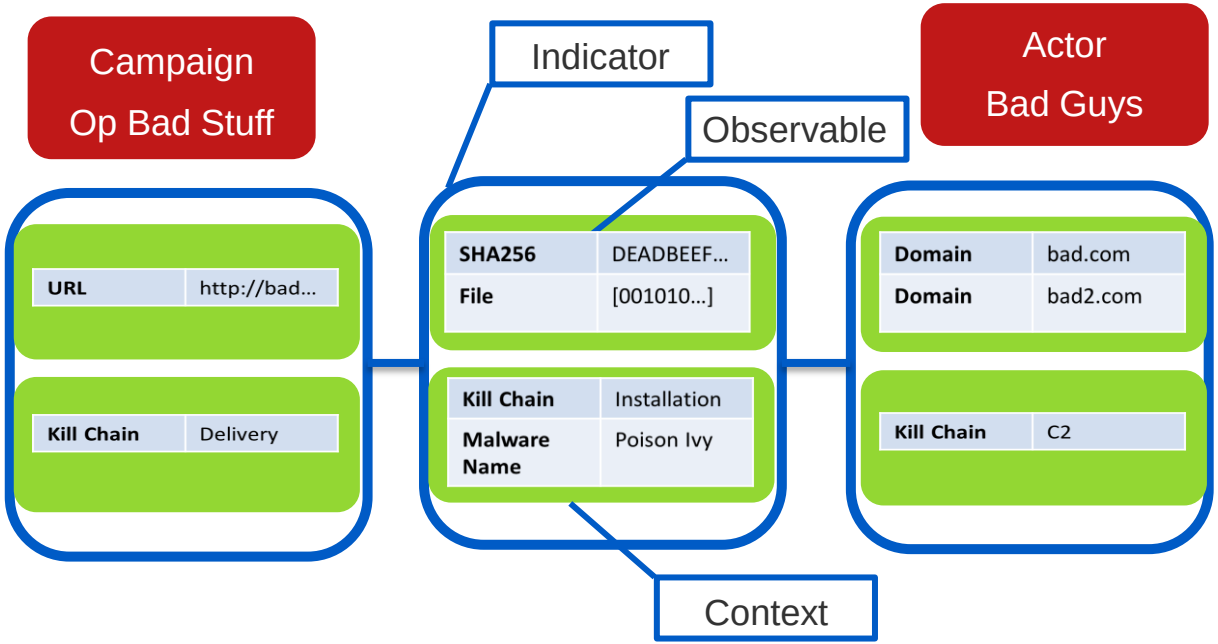
Intelligence Automation

Response Action Orchestration

Defensive Evolution – Apply Security Analytics



Defensive Evolution…Strategic Collaboration



CYBER THREAT ALLIANCE

Call to Action

Have a conversation about GDPR and Data Security implications

Ask questions of your cloud security and service provider

Review your current security architecture strategy

GDPR - General Overview

- New EU regulation that affects the full data lifecycle from collection, processing, storage, usage and destruction; affects companies doing business with EU
- Requires organizations to implement *appropriate measures* to protect privacy-related data but is not prescriptive in the specific controls
- Significant penalties assessed for data unreported data breaches
- Appropriate measures could include the following:
  - **Data Security (Data at Rest, In Motion, In Use)**
  - **Infrastructure Security and Resilience (Anti-Malware, Network Segmentation)**
  - **Breach Detection, Notification, Audit (SOC, DPO)**
  - **Data Residency**
  - **Data Usage and Export**
  - **Retention (Right to be forgotten)**
  - **Access Control**
  - **Policy and Governance**