

Putting Risk Management to Work

Joe Levy
CTO

February 2020

SOPHOS

Evolution of Threats



“Living off the Land”
techniques to evade
detection



“Automated Active Attacks”
combine automation and
manual steering

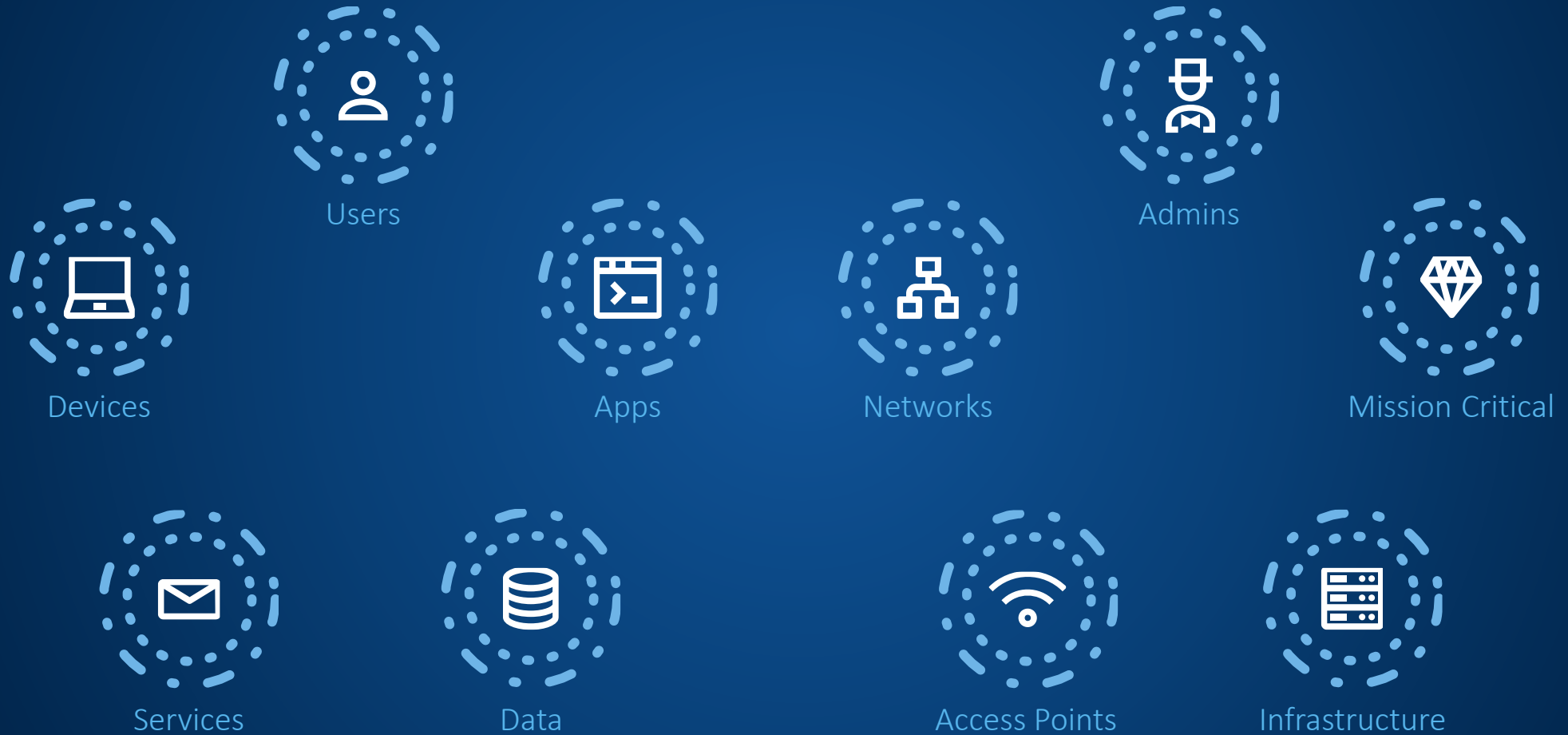


Covertly modifying security
controls to evade or prolong
detection



Exploiting third-party
vendors in the supply
chain

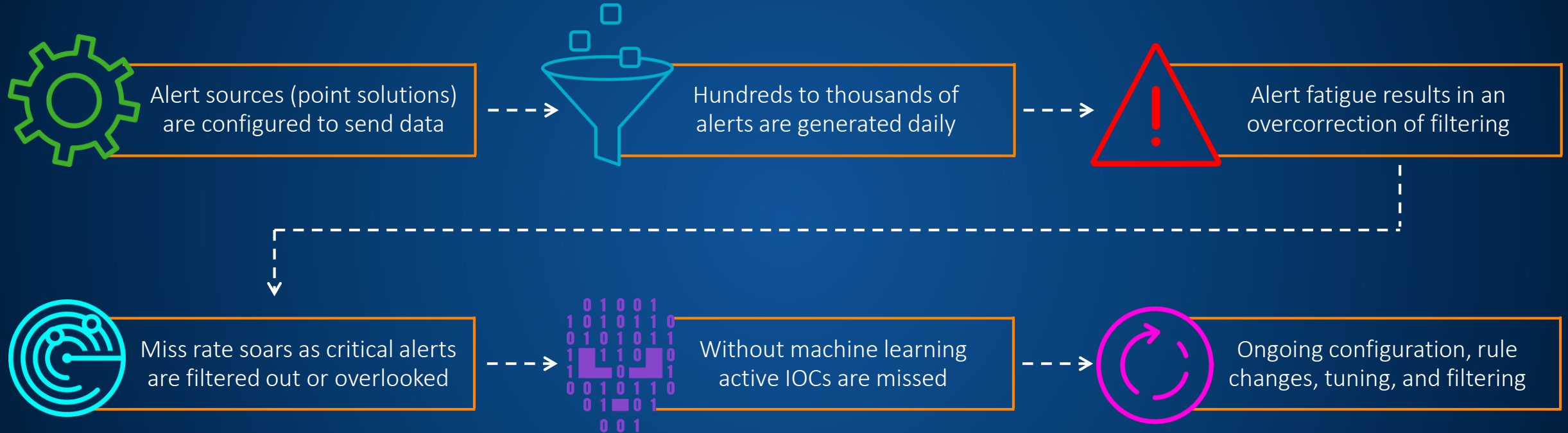
Evolution of Infrastructure



Evolutions in Security and IT Not Keeping Pace

SOPHOS

Alert Prioritization: Slow and Unreliable



Security and IT Limitations

SECURITY

Point Products

- Disparate, poorly integrated tools
- Closed system

Limited Intelligence

- Not implemented strategically
- Closed system

Static

- Post-intrusion detection
- Information-only, not response
- Static policies

IT

Reactive

- Assume infection
- Post-intrusion detection / response

Manual

- Identify baseline configurations
- Actions slow to implement / improve

Ad Hoc

- Processes not well-defined
- Response actions are limited
- Requires extensive experience

Resulting Risk Register

		Impact				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain				2	
	Likely			5 7	1 6	
	Possible			3 8	4	
	Unlikely					
	Rare					

Cybersecurity Risks

1. Unmanaged, unassimilated internal assets
2. Underinvestment in legacy products and services
3. Lack of staff with the right level of skills
4. Vendors with vulnerable systems
5. Use of non-standard systems and technologies
6. Nation state attack / APT leading to disruption
7. IT Security policies insufficient, inconsistent or not effectively enforced
8. Inconsistent identity and access management

Evolving Risk Management

Advanced Intelligence

Data Science

Advanced Management

High Utility Management Platform

Advanced Threat Response

Fusion of Intelligence and Operators

Evolution in Data Science

SOPHOS

Multi-format File Detection

Files carved off device

- Fast signatures and heuristics applied on device
- If file is convicted, or suspicious, send to cloud analysis platform

... scanned in cloud

- A host of ML models is applied, and possibly a sandbox service
- If file hasn't been convicted on device, decision sent back

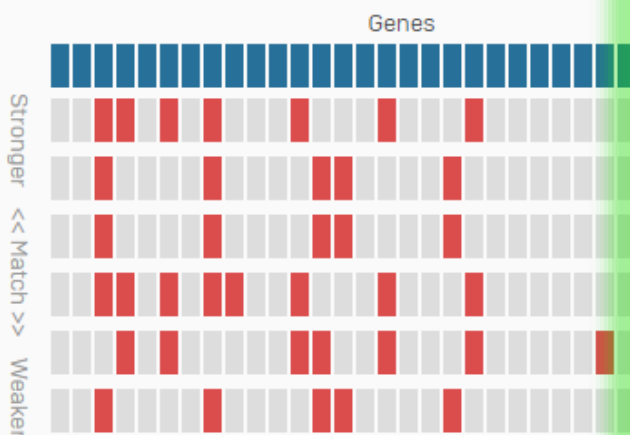
... visualized in UI

- User presented with derogatory or exonerating evidence about files
- This explains convictions to users, and enriches "grey area" observations

Analytics for Office, PDF, PE, RTF

Structure analysis

- Identifies 32 distinctive structural genes in the file
- Scans database for files with these genes
- Ascertains the likelihood of the genes' presence in good and bad files
- This test rates **info_07.25.doc** as **MALICIOUS**.
- The chart below shows 6 of the files in the sample set with the same structure



Total sample set consists of 1,012,735 known good and 1,012,735 known bad files

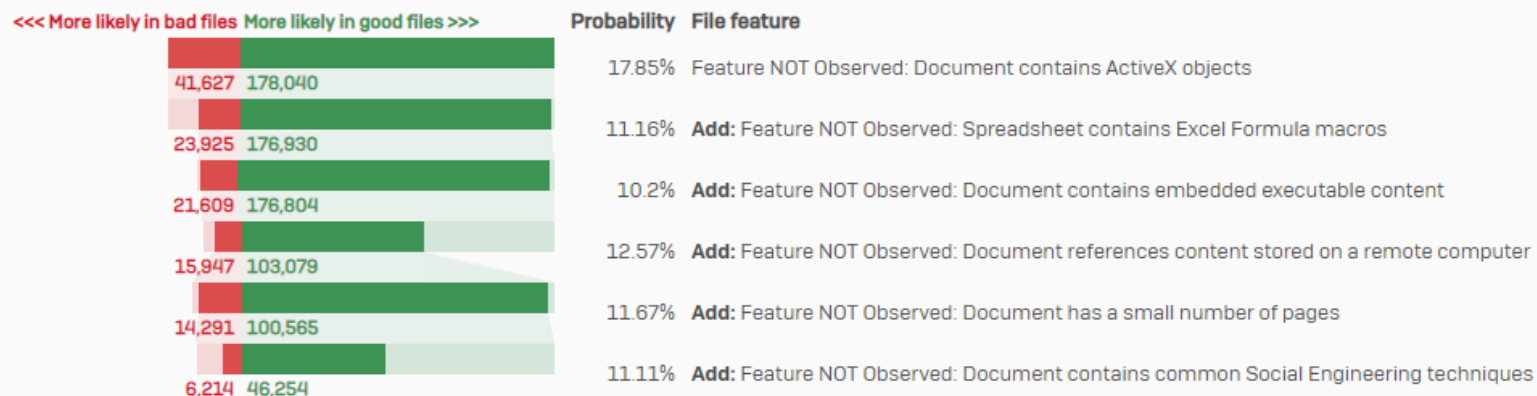
Feature analysis

- Identifies specific features of the file.
- Randomly selects one million (out of 118,928) known good and one million (out of 110,553) known bad files.
- Counts the number of good and bad sample files that have the same features. These simple counts are shown in the graph below.
- The verdict may also take into account more complex combinations of features
- This test rates **PurchaseOrder.xlsx** as **LIKELY CLEAN**.



Feature combinations

- Counts the number of good and bad sample files that have one feature in common with your file.
- Adds an additional feature and counts the sample files that have both features.
- Continue adding features and counting sample files that combine all features.
- Combinations of features can provide a more precise indication than individual features.



AI-driven Web Content Analysis

Every URL customers visit gets submitted to lookup service

- Response time < 10ms
- Previously unseen URLs get added to an analysis queue

In the background, a large scale distributed crawler visits new URLs

- AI-based web content filtering models are applied
- AI-based web security models are applied

Most URLs get categorized immediately, some go to human analysts

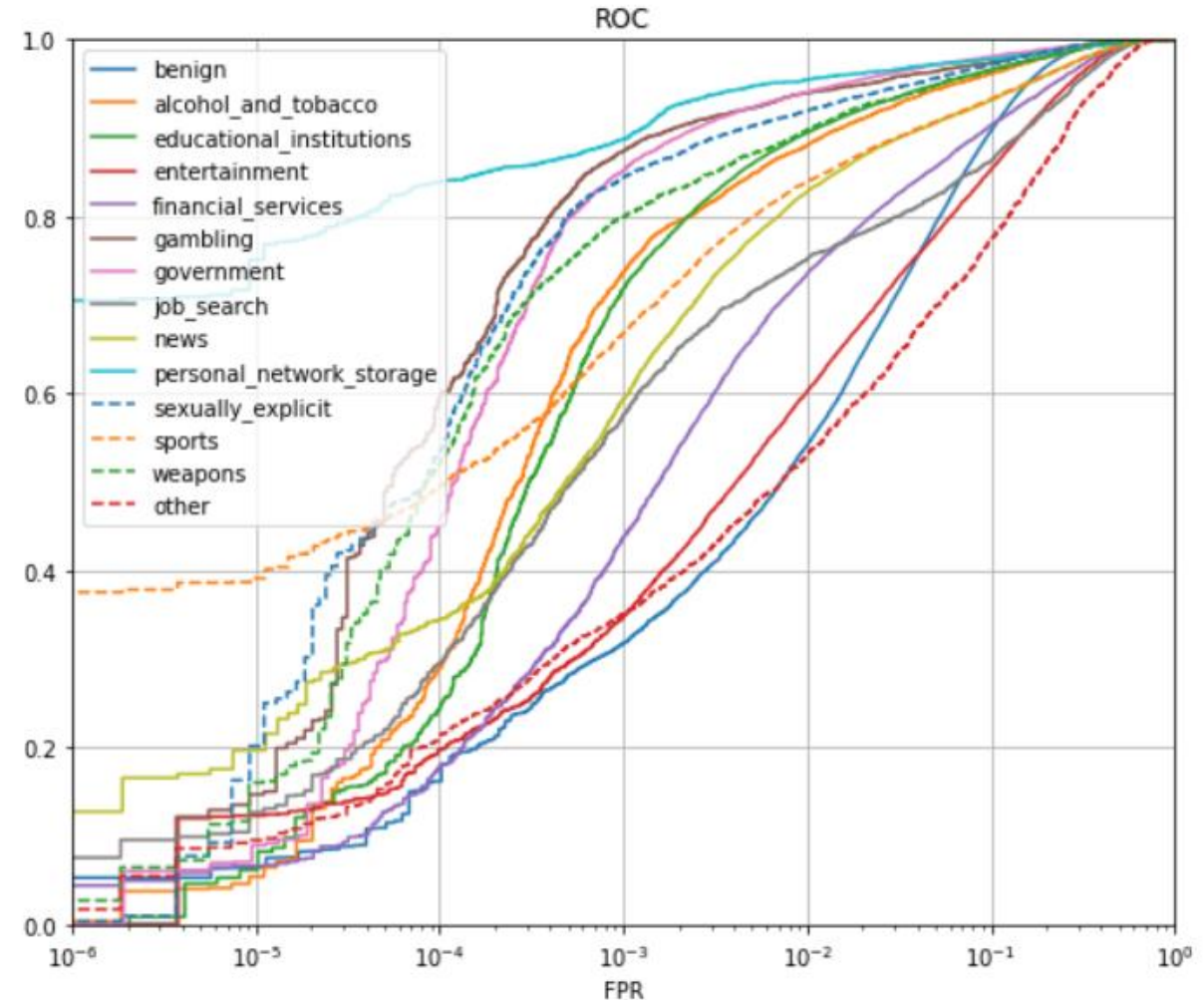
- URLs with high AI-based certainty get fed back to the lookup service
- Highly uncertain URLs are inspected by a human analyst team

Web Security and Content Classification

TABLE I

DETECTION RATES FOR DIFFERENT MALWARE FAMILIES, AS WELL AS THE PERCENTAGE OF MALWARE SAMPLES IN WHICH THAT TAG APPEARS

Family Category	DR@10e-3	Prevalence (%)
Code Injection XSS	0.999	16.1
Browser Exploit	0.998	14.4
iFrame Mischief	0.998	14.9
Malicious Browser Redirect	0.997	3.3
Blackhat SEO	0.995	49.6
Ramnit Malware Family	0.995	39.7
Fake JQuery	0.977	.5
All Malware	0.972	100
Facebook Hacking	0.971	13.8
Changes Browser Startpage	0.937	5.2
Ransomware	0.931	1.2
Auto Click	0.902	.6
Phishing	0.895	.5



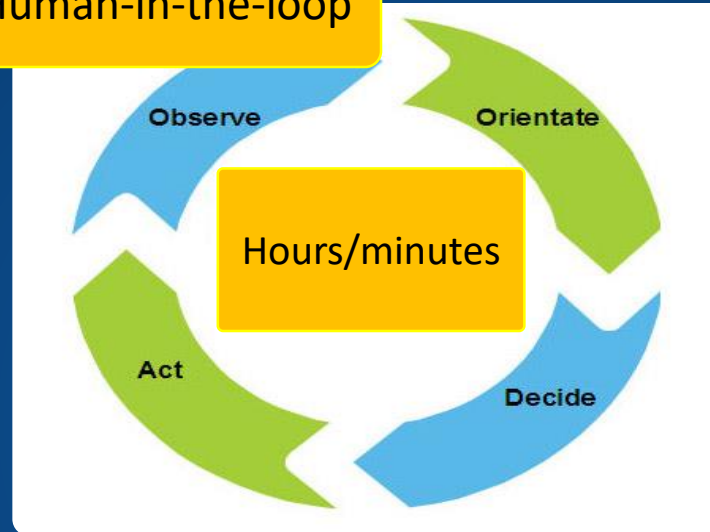
ML and The OODA Loop ...

Fail



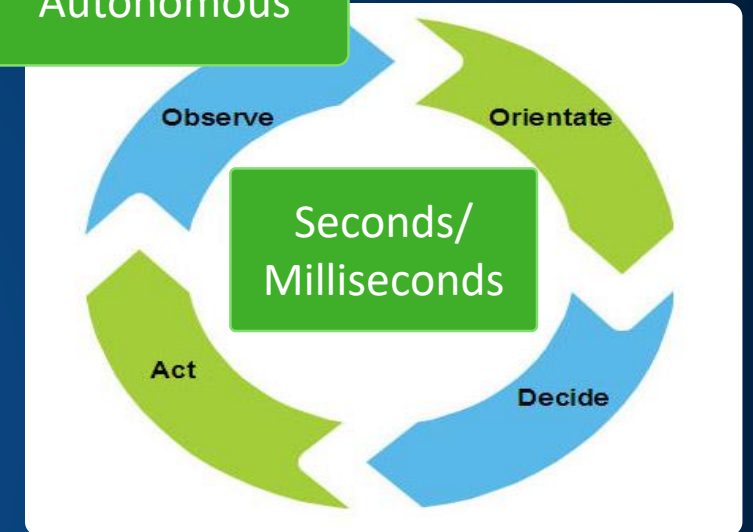
Data science role:
Help eliminate these loops

Human-in-the-loop



Data science role:
Time compress these loops using
clustering, alert prioritization,
large scale search

Autonomous



Data science role:
Convert human-in-the-loop to
autonomous processes using ML,
optimize autonomous accuracy
and speed

The Goal: Move From “Thinking” to “Doing”

Thinking (Reactive)



- Sift through events and alerts
- Prioritize from high to medium to low
- Search for adjacent indicators
- Confirm validity and scope
- Evaluate response options



Doing (Proactive)

- Analyze alerts and TTP-based detections
- Verify if malicious or benign
- Neutralize confirmed threats
- Reinforce learning model
- Improve response time

High Utility Management Platform

SOPHOS

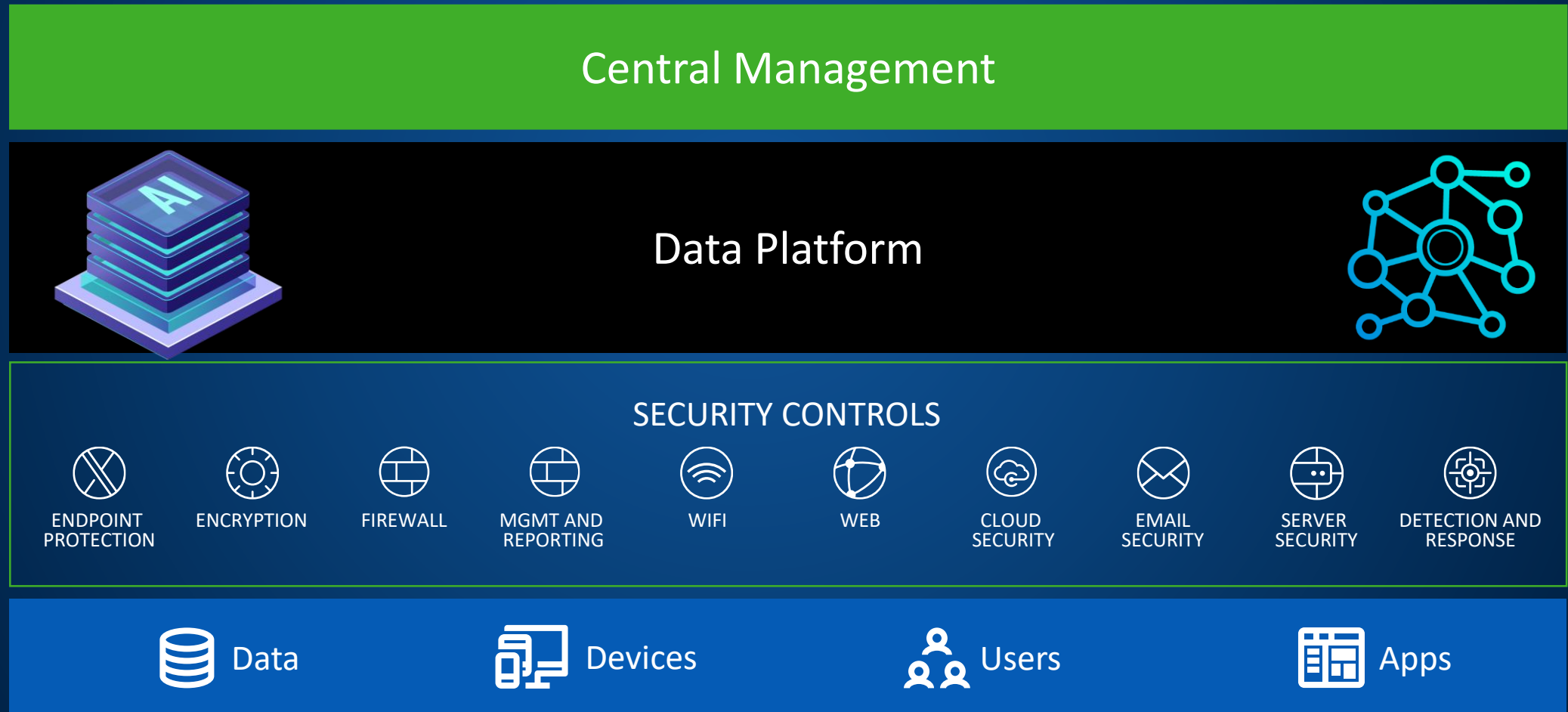
High Utility Management Platform

Stage 1: Integrated Security Control System



High Utility Management Platform

Stage 2: Cybersecurity as a Synchronized, Predictive and Adaptive System

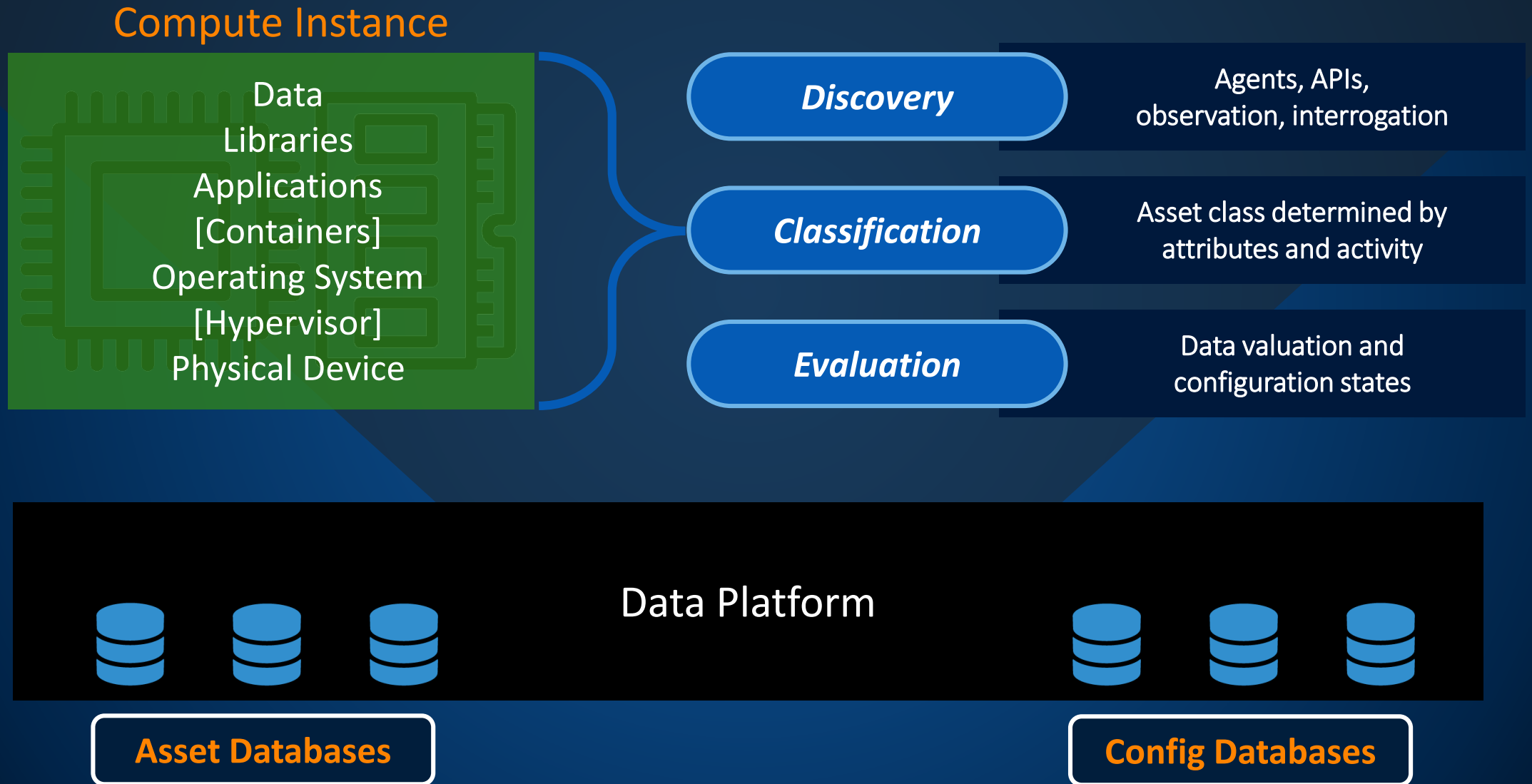


High Utility Management Platform

Stage 3: Cybersecurity as a Synchronized, Predictive and Adaptive Ecosystem

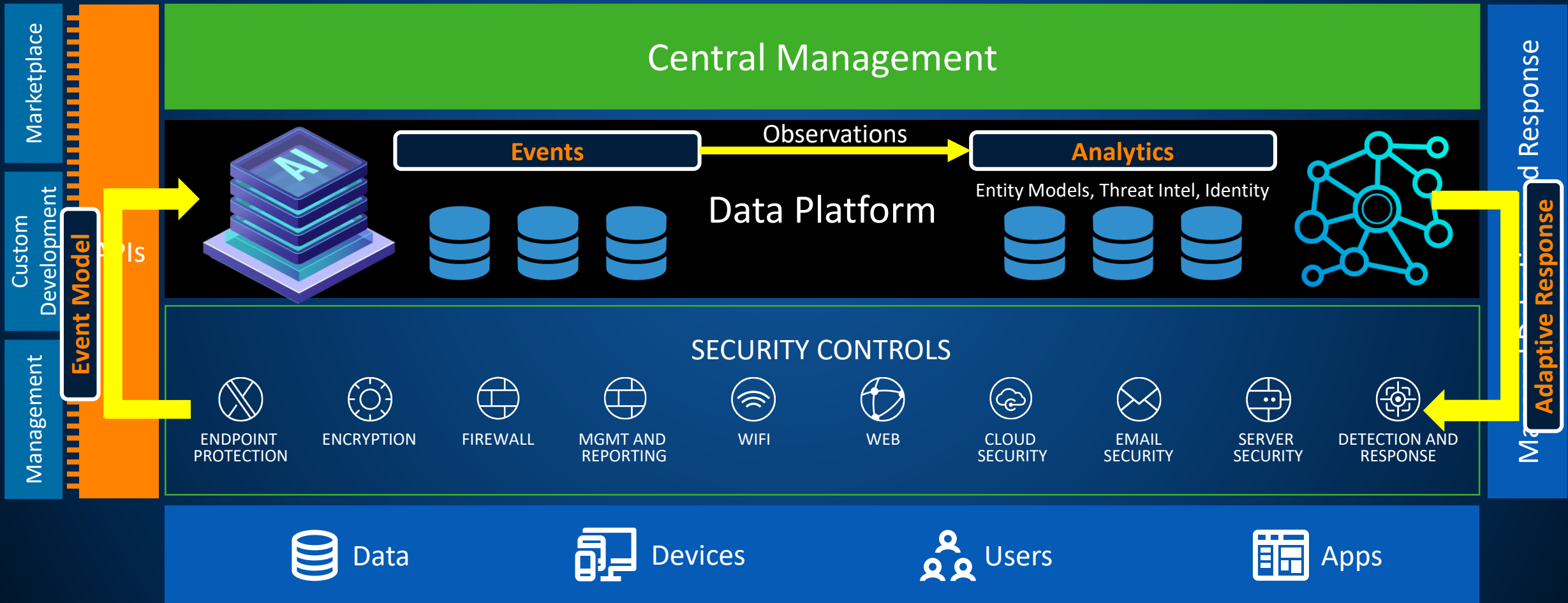


Asset Discovery



High Utility Management Platform

Analytics System



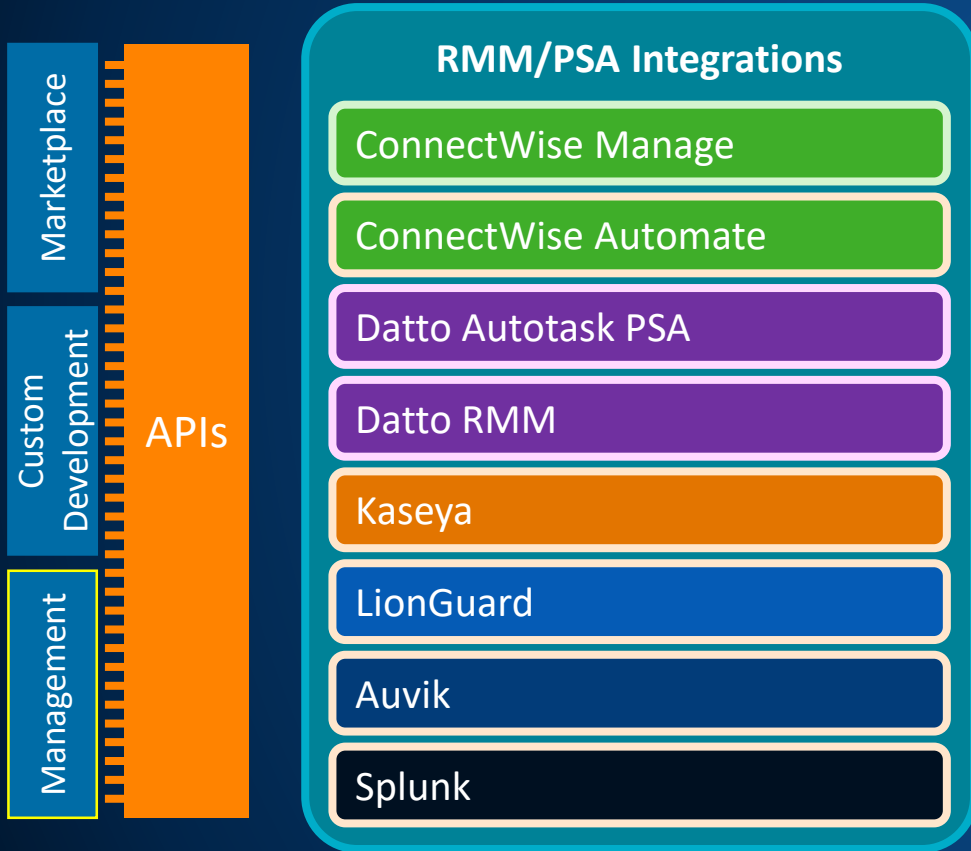
High Utility Management Platform

Ecosystem



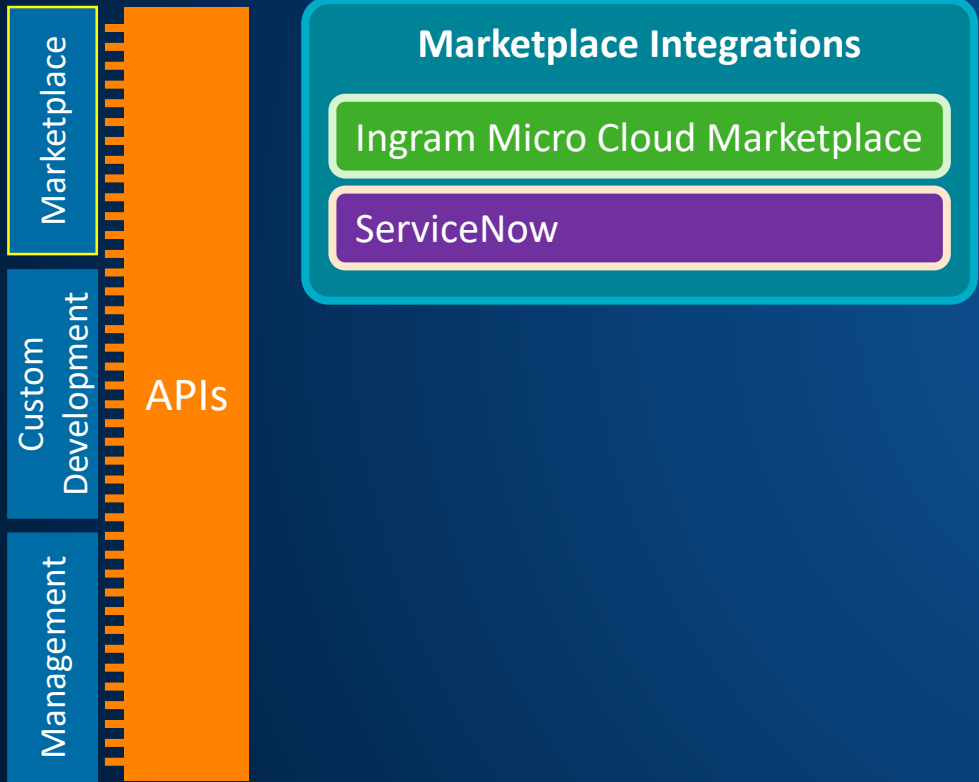
High Utility Management Platform

Ecosystem




High Utility Management Platform

Ecosystem



Fusion of Intelligence and Operators

SOPHOS



“As the threats organizations face increase in both volume and sophistication, it’s become apparent that the collection of IT security point products most organizations rely on today for cybersecurity needs to give way to a service-based approach infused by artificial intelligence (AI).”

— Kris Hagerman, Sophos CEO

Fusion of Intelligence and Operators

Intelligence



Rapidly processes massive pools of data to detect potential malicious activity

Draws correlations based on patterns or behaviors

Takes automatic actions in near real-time to block or terminate confirmed malicious activities (strong signals)

Derives conclusions based on the data previously fed into the system (“only as good as its teacher”)



Operators

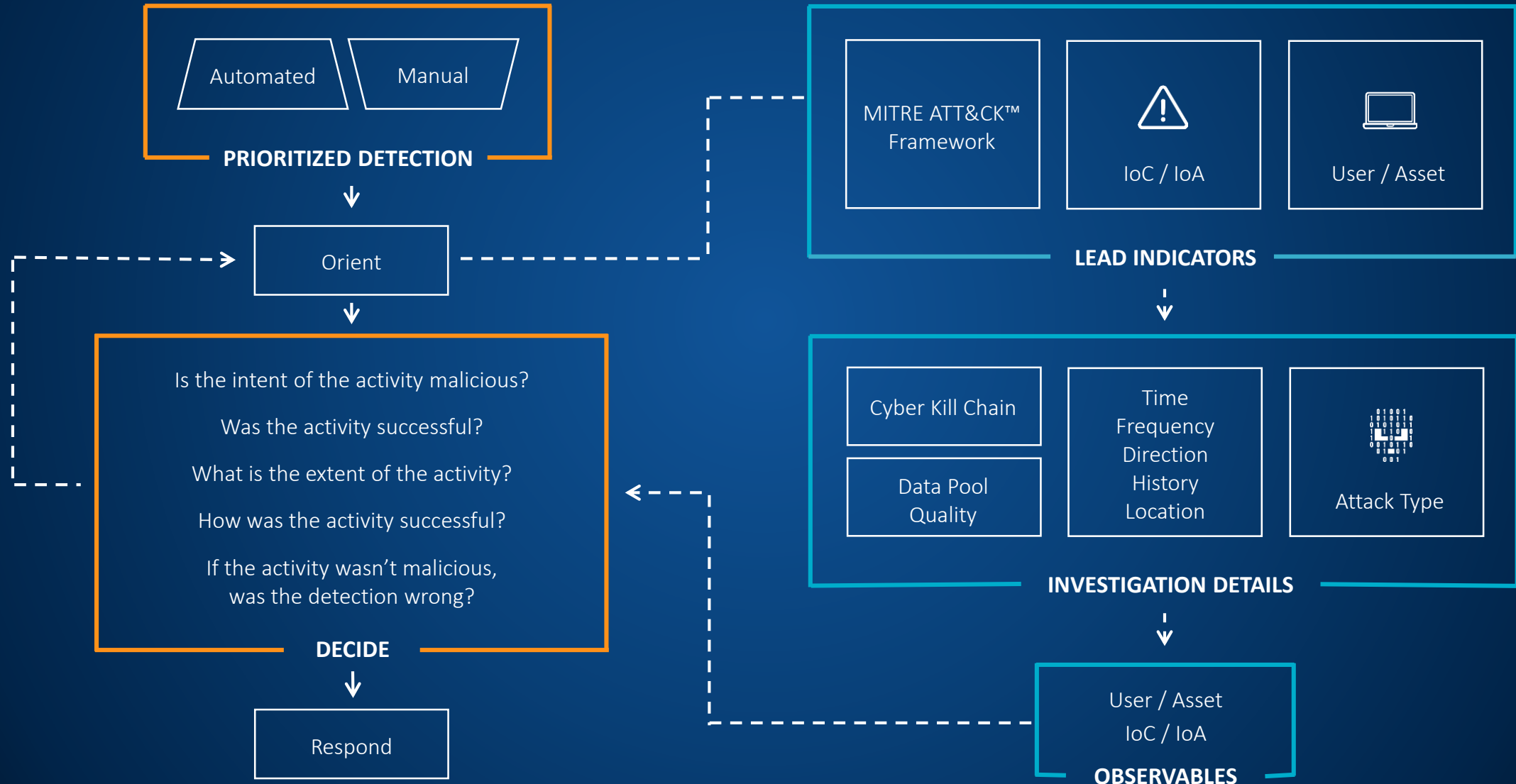
Uses investigative techniques to conclude whether a suspicious activity is malicious or benign

Applies the business context of why an attacker might be after a piece of data and potential motivations

Investigates causal and adjacent events (weak signals) to discover new or previously undetected threats

Evaluates multiple sources and employs creative thinking and problem solving to make decisions

Fusion of Intelligence and Operators



Risk Management Evolution

SECURITY

Synchronized

- Integrated security sensors
- Open platform
- Automated actions

Predictive

- Asset and ID aware
- ML-based

Adaptive

- Identify baseline configurations
- Detect and respond to anomalies
- Automatically learn and optimize

IT

Proactive

- Assume secure
- Automatic system detection and response

Optimized

- Optimized configurations
- Detect and respond to anomalies

Strategic

- Automatic and machine-assisted incident response

Use Case Examples

File-less Cryptomining Attack

Use Case

Customer Overview

- Devices: 4,600
- Industry: Manufacturing
- Response Mode: Authorize

Ops team identifies malicious activity originating from file-less cryptominer malware

Rather than using a file-based attack, the attackers used Windows Management Instrumentation (WMI), to execute a file-less attack to avoid detection

Present on all Windows operating systems, WMI comprises a powerful set of administrator tools used to manage Windows systems both locally and remotely. Similar to PowerShell, WMI usage is expected in organizations to some degree, which can make identification of malicious activity difficult.

Attackers can use WMI to connect to remote systems, modify the registry, access event logs, and most important, execute commands. Aside from an initial logon event, remote WMI commands often leave little evidence on the accessed system.

After conducting a full investigation to confirm the scope and severity of the attack, the Ops team rapidly initiated response actions to neutralize and remove the threat

Malicious PowerShell Attack

Use Case

Customer Overview

- Devices: 1,280
- Industry: Manufacturing
- Response Mode: Notify

The Operations team observed a suspicious PowerShell command being executed on a customer asset

A subsequent analyst-led investigation revealed that the malicious PowerShell command stemmed from a malware infection that originated from a removeable storage device (USB drive)

Operations team delivers detailed notes on the investigation with recommendations for how to neutralize and remediate the threat. These recommendations included isolating the device, deleting the directory and file, and prohibiting the use of the removeable device.

Following the resolution of the incident, the Response Mode changed to Collaborate, enabling the Operations team to initiate more response actions as a service

PowerShell Leads to TrickBot Discovery

Use Case

Customer Overview

- Devices: 400
- Industry: Entertainment/Hospitality
- Response Mode: Notify

Through a combination of tool-based detections and analyst-led threat hunts, the Ops team identified PowerShell Empire executions in the environment. PowerShell Empire is often used by malicious actors to execute attacks once a victim's system has been compromised

The Ops team discovered several assets across the environment that contained PowerShell Empire registry keys, including a compromised user account with administrator privileges

A subsequent investigation and asset discovery exercise conducted by the Operations team revealed that the compromised administrator account was associated with two unique and infrequently-used assets that did not have proper levels of protection installed

Deployed managed threat response on the previously unmanaged assets which immediately identified that one of the assets was running persistent PowerShell scripts and was infected with an extremely persistent strain of malware known as TrickBot that primarily targets sensitive financial information, such as login credentials for online banking sessions

Immediately removed the compromised asset from the network and confirmed that no further assets were infected with TrickBot or malicious PowerShell scripts

SOPHOS
Cybersecurity evolved.