



Microsoft CISO Workshop

4b - Threat Protection Strategy (DETECT-RESPOND-RECOVER)

Microsoft Cybersecurity Solutions Group

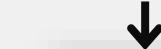


Threat protection (Detect-Respond-Recover)

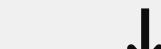
TRENDS



THREAT EVOLUTION



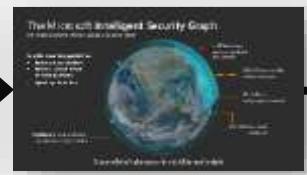
SOC MISSION EVOLUTION



EVOLUTION OF MICROSOFT SOC



STRATEGY



INTELLIGENCE

SUCCESS CRITERIA

RECOMMENDED APPROACH



SIEM & INTEGRATION

DEEP DIVES



BEHAVIOR ANALYTICS



MACHINE LEARNING

APPLYING TO OPERATIONS



TYPICAL KILL CHAIN



INTEGRATION



COMMUNITY EFFECT



INTEGRATED AUTOMATION

Observations and challenges



Threats increasing in volume and sophistication

Attacker business models evolve to maximize attacker return on investment (ROI)

Attack automation and evasion techniques evolving along multiple dimensions



Can't Stop All Attacks

Must balance investments across prevention, detection, and response

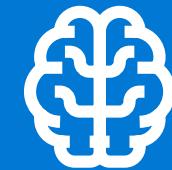
Prevention investments must be focused on real world attacks



Integration is required, but complex and costly

Threat Detection requires context from a diverse signal sources and high volumes of data

Efficient operations requires integration of tools and technology like machine learning



Humans and Automation

Need human expertise, adaptability, and creativity to combat human threat actors

Automation can reduce toil and repetitive tasks, enabling people to make their best contributions

Evolution trajectory of SOCs

Improved responsiveness & remediation by empowering humans with technology



Assistance from AI bots and augmented reality

ACT – Speed up response with Orchestration and Automation

DECIDE – Increase speed and quality with embedded guidance

ORIENT – Extract Context from mountain of data with AI, ML, UEBA, and Human Expertise

OBSERVE – Increase Field of view with vast intelligence data



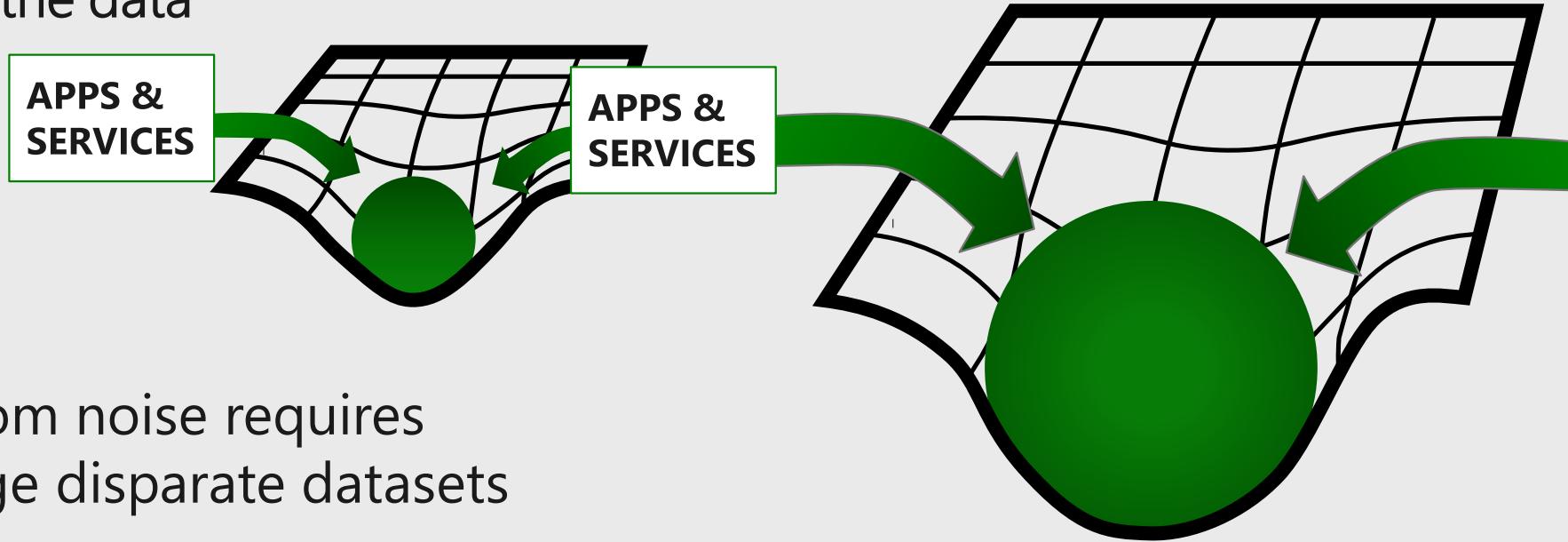
Available Today

Near Future



Data Gravity

Pulls analytics to the data



Getting signal from noise requires context from large disparate datasets

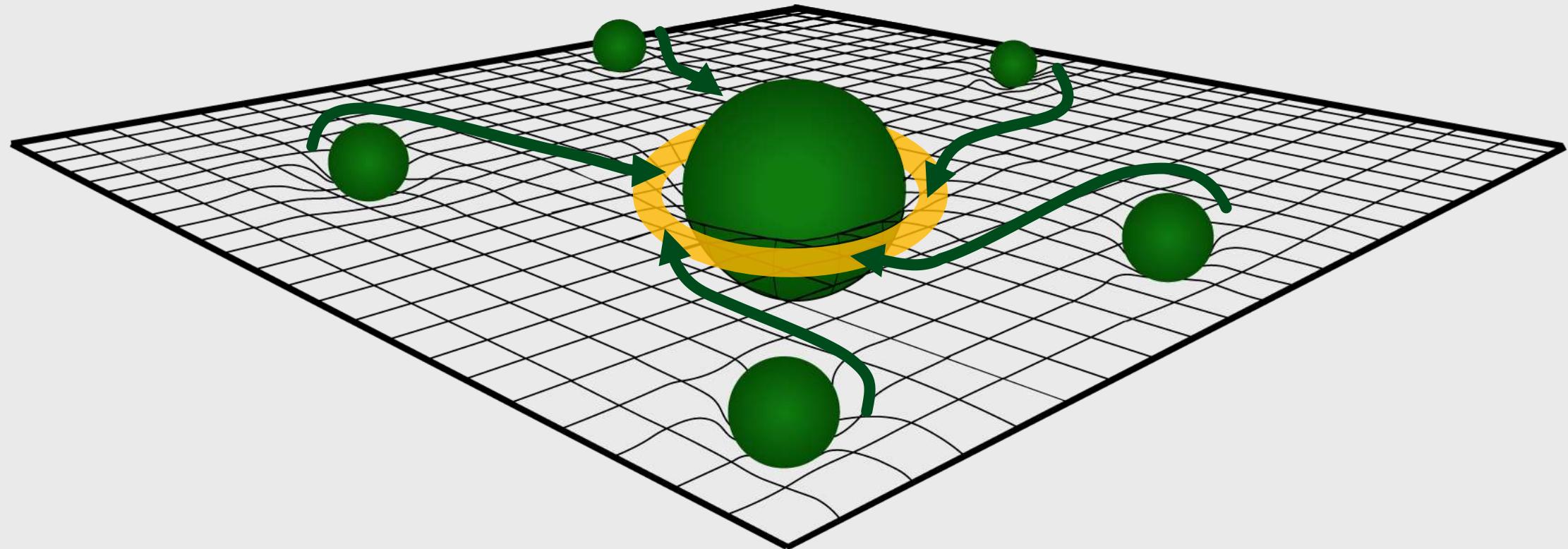
Can't copy all needed data to one location because of bandwidth

→ Need to leverage analytics from anywhere and centrally integrate

$$\frac{(\text{Data Mass} \times \text{Application Mass}) \times \text{Number of Requests per second}}{\left(\frac{\text{Latency in seconds}}{\text{Average Request Size in MBs}} + \left(\frac{\text{Bandwidth in MBs per second}}{\text{Bandwidth in MBs per second}} \right)^2 \right)}$$

SOC Signal Rationalization

Many data sources in a SOCs today

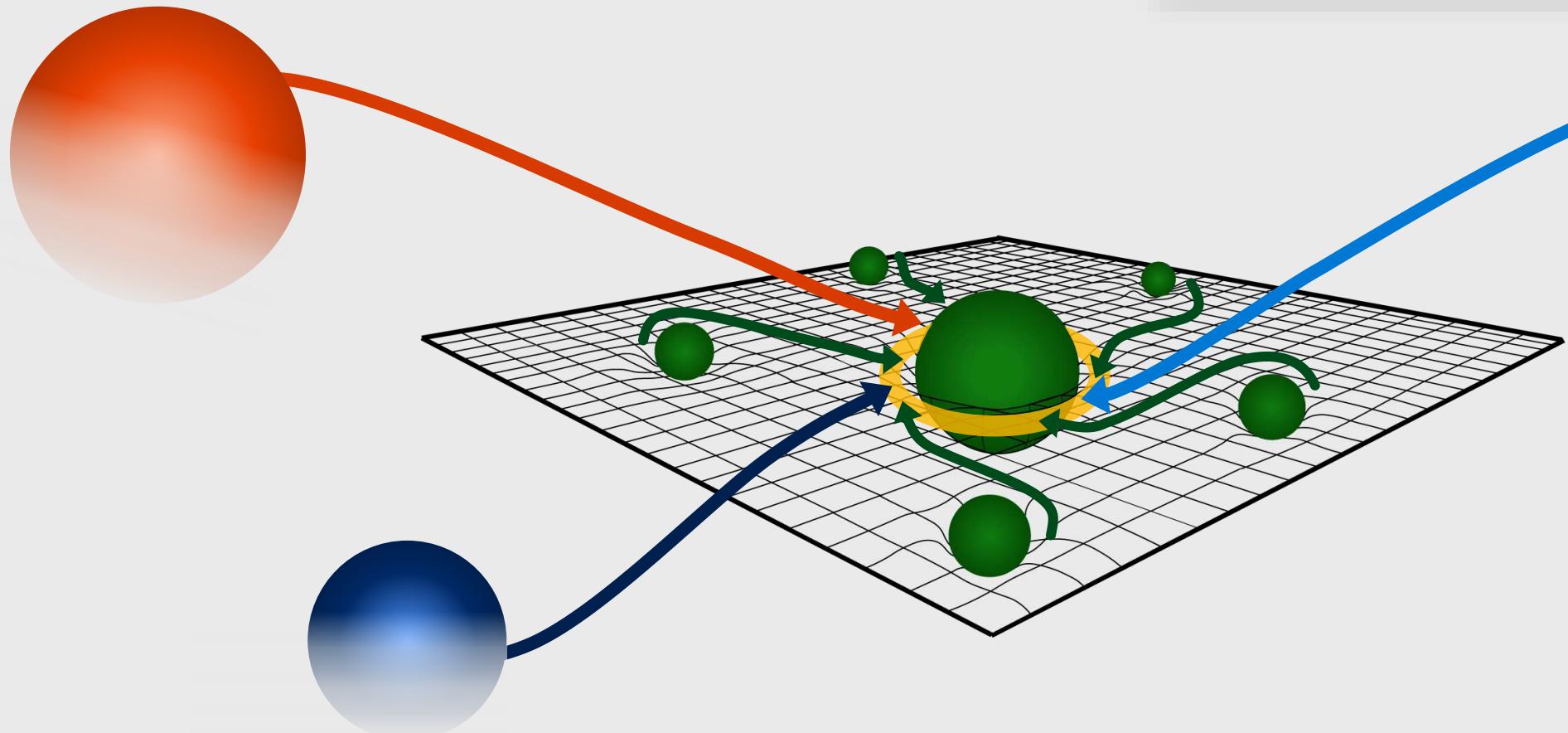


Microsoft Graph Security API allows analysts to get insights across local security datasets

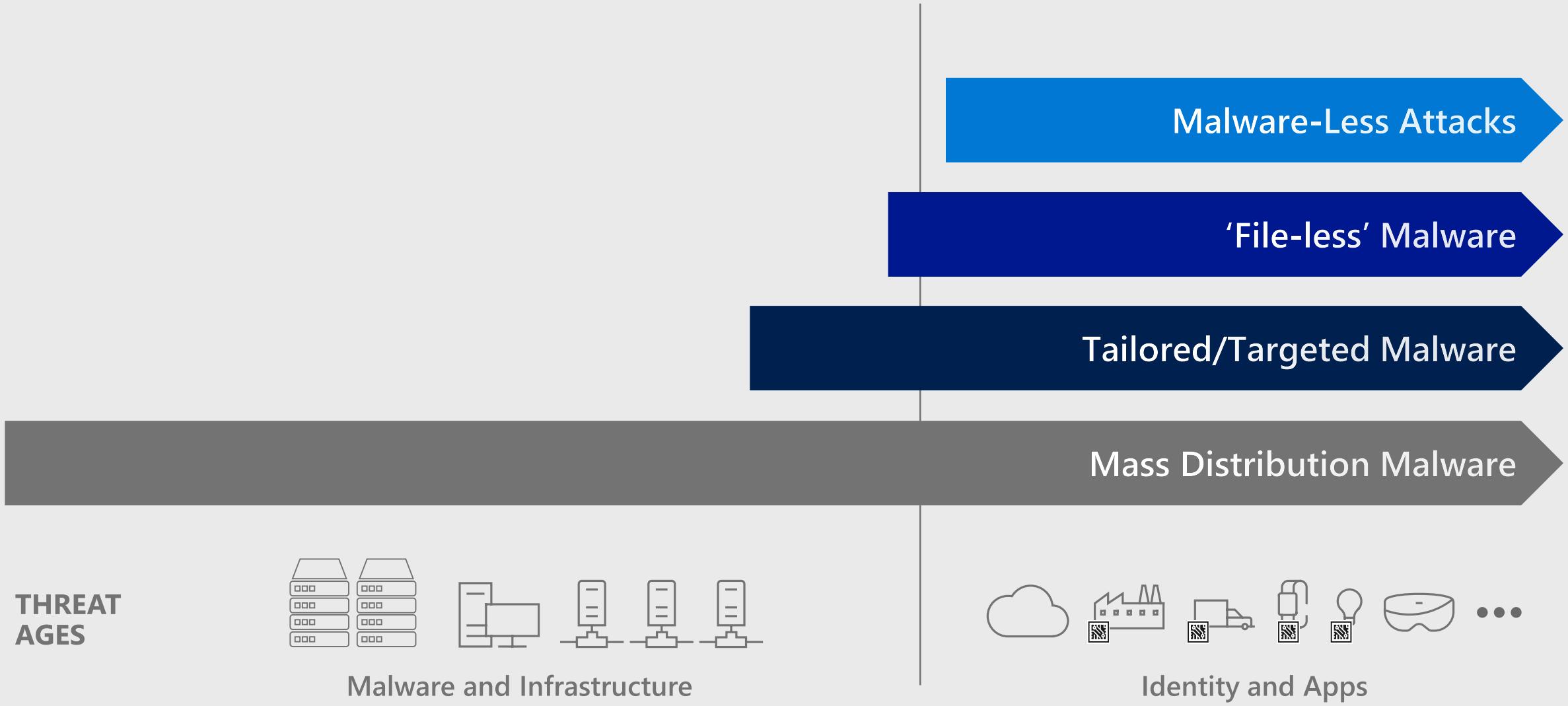
Graph Security API – Signal Unification

Allows analysts to get insights and context across
Local datasets and
Cloud hosted security datasets

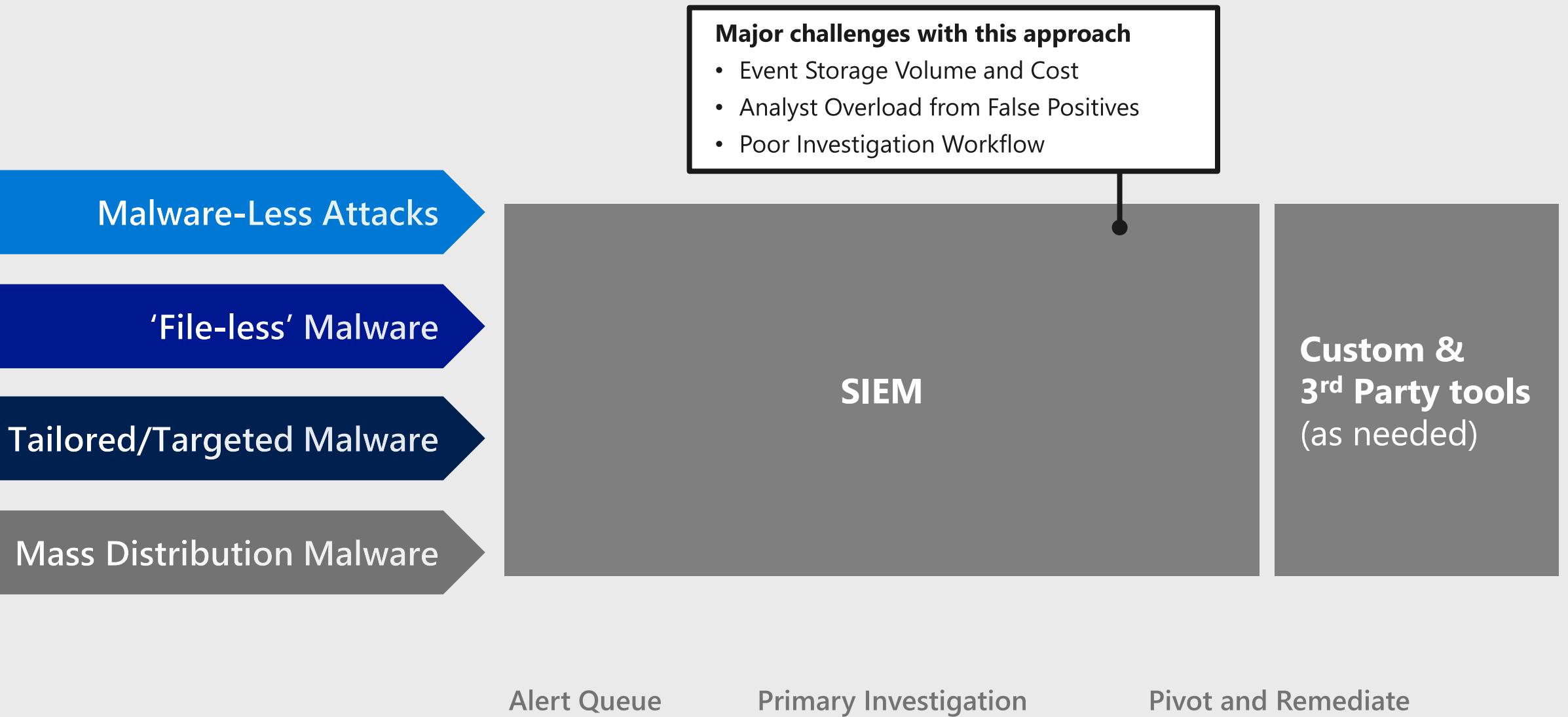
Microsoft's Intelligent Security Graph
Massive dataset + analytics powering
Microsoft threat detection capabilities



Threat evolution is accelerating

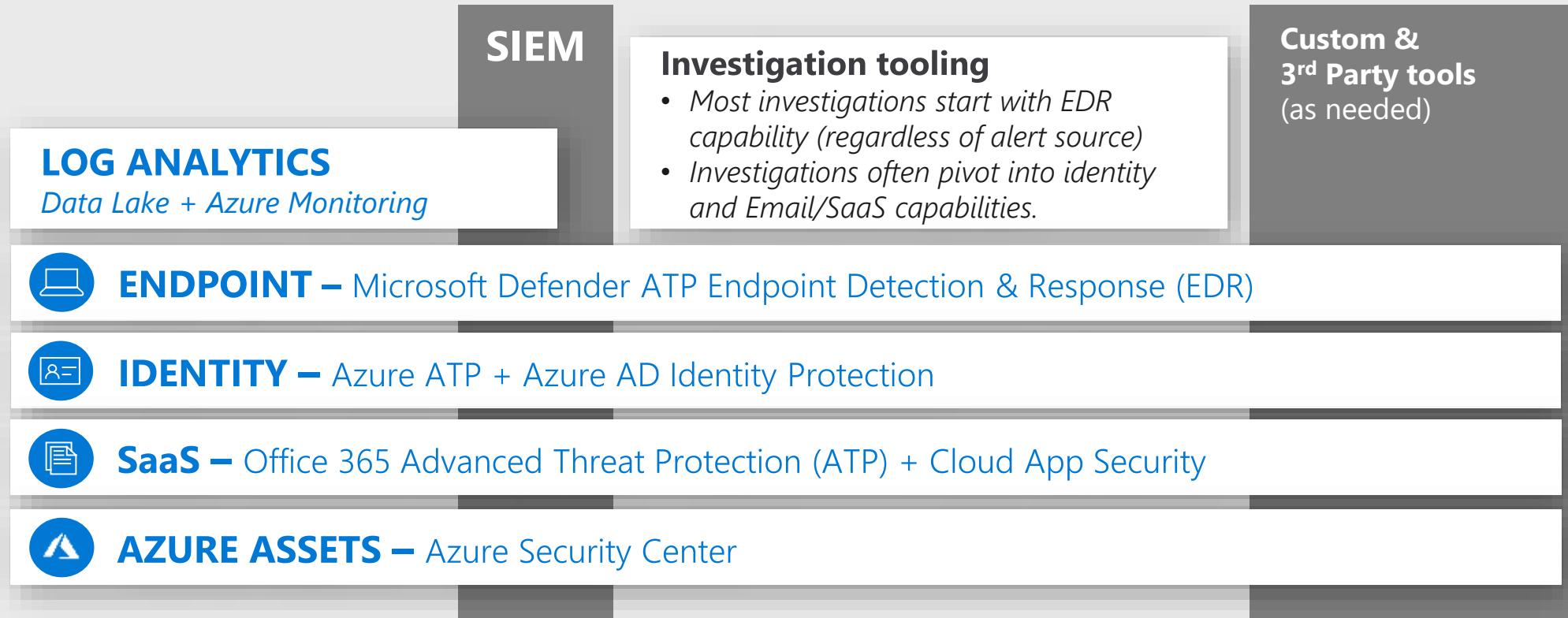


Corporate IT SOC – Started with Classic SIEM model



Corporate IT SOC – Evolved

Adopted specialized tooling + Cloud Native Analytics



Generate Alerts

Alert Queue

Investigation

Pivot and Remediate

Corporate IT SOC – Upgrading to Cloud Native SIEM

Breadth: Unified View

- *Unified Alert Queue*
- *Log Detections (UEBA/ML/Manual)*

SIEM + SOAR as a Service

Azure Sentinel (Pilot)

Custom &
3rd Party tools
(as needed)



ENDPOINT – Microsoft Defender ATP Endpoint Detection & Response (EDR)



IDENTITY – Azure ATP + Azure AD Identity Protection



SaaS – Office 365 Advanced Threat Protection (ATP) + Cloud App Security



AZURE ASSETS – Azure Security Center

Depth: Specialized Tools

- *High quality alerts*
- *End to end investigation and remediation*



NETWORK – 3rd party Logs and Tools



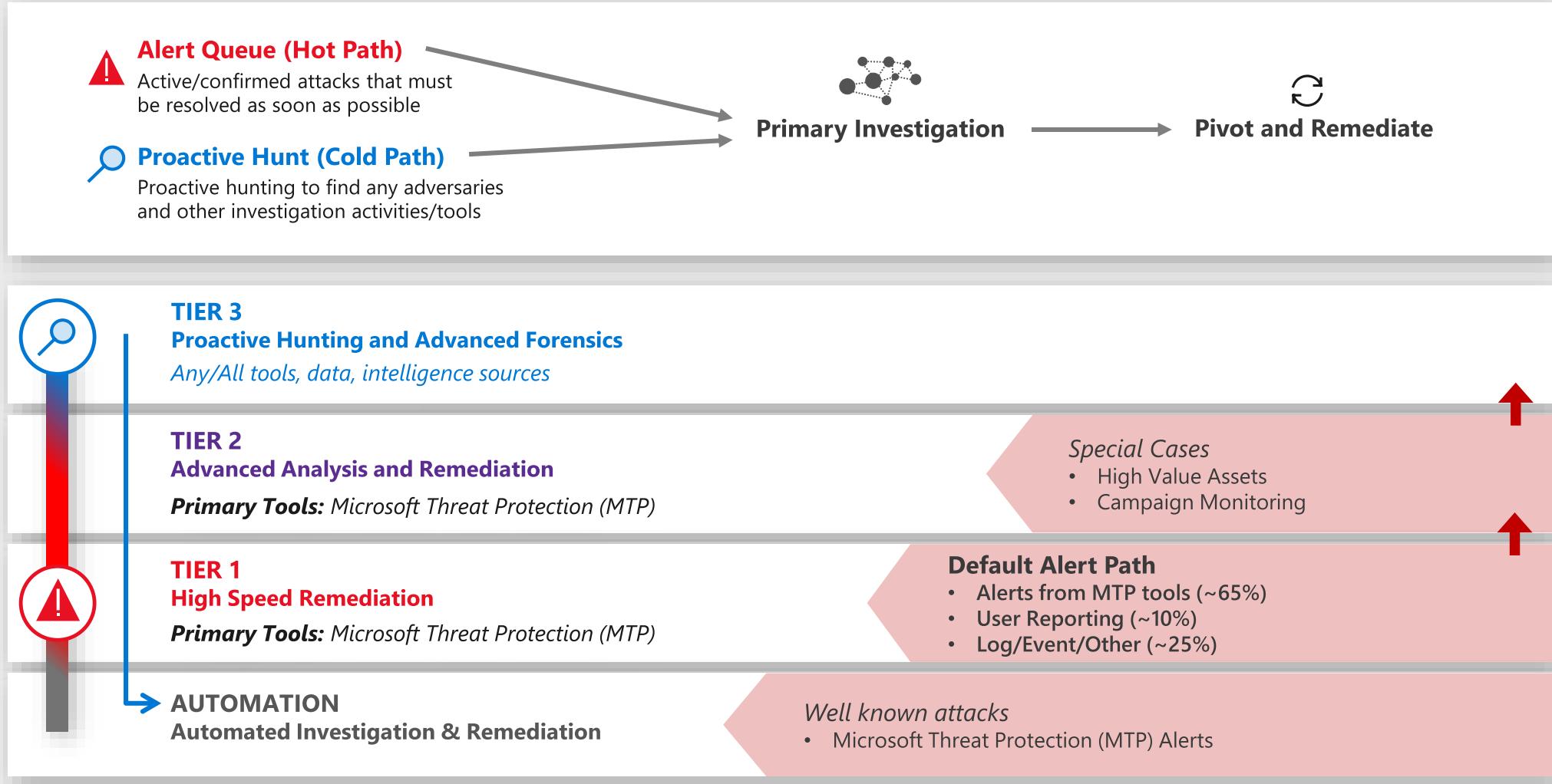
SERVERS – 3rd party and Microsoft Logs and Tools



OTHERS – 3rd party and Microsoft Logs and Tools

Built on Azure Monitor, Logic Apps, and Microsoft's UEBA/ML Technology

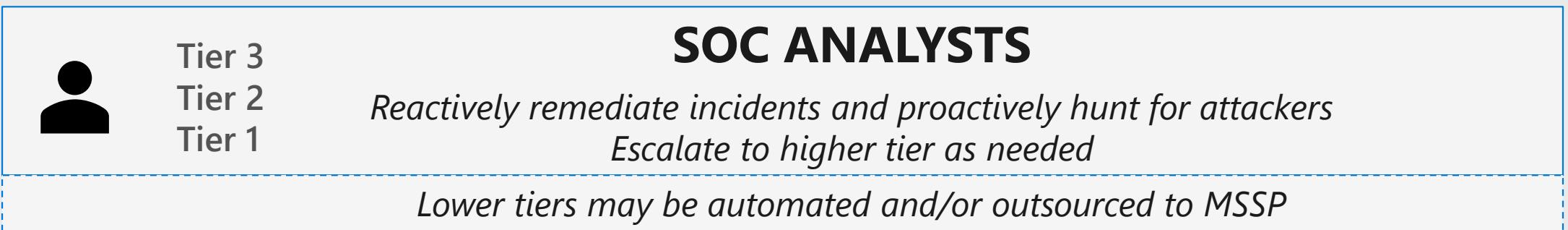
Microsoft's Corporate IT SOC – Tiers and Tools



SOC Reference Operational Model



Mean Time to Acknowledge (MTTA) / Remediate (MTTR)



DETECT



RESPOND



RECOVER

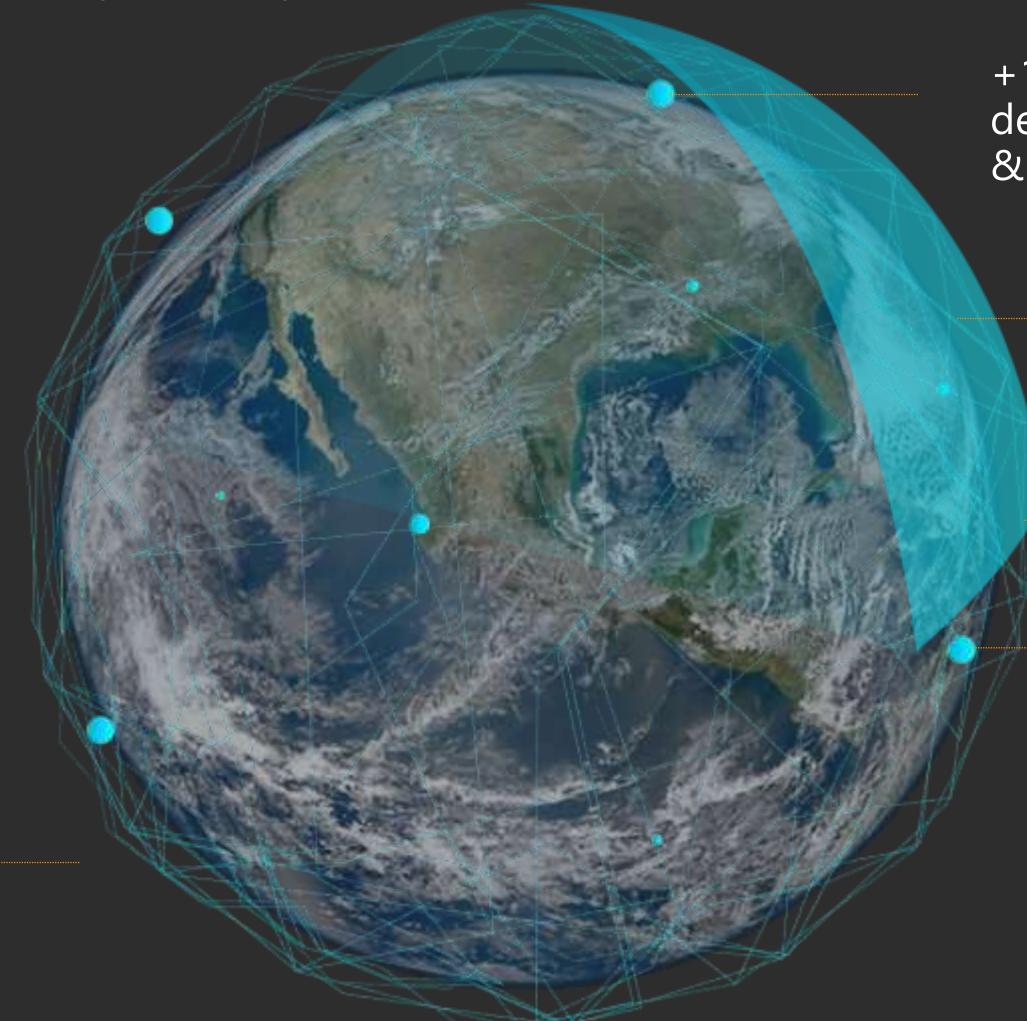
The Microsoft Intelligent Security Graph

6.5 trillion diverse threat signals analyzed daily

Machine learning applied to:

- Reduce manual effort
- Reduce wasted effort on false positives
- Speed up detection

5 billion threats detected on devices every month



+1B Windows devices updated & scanned

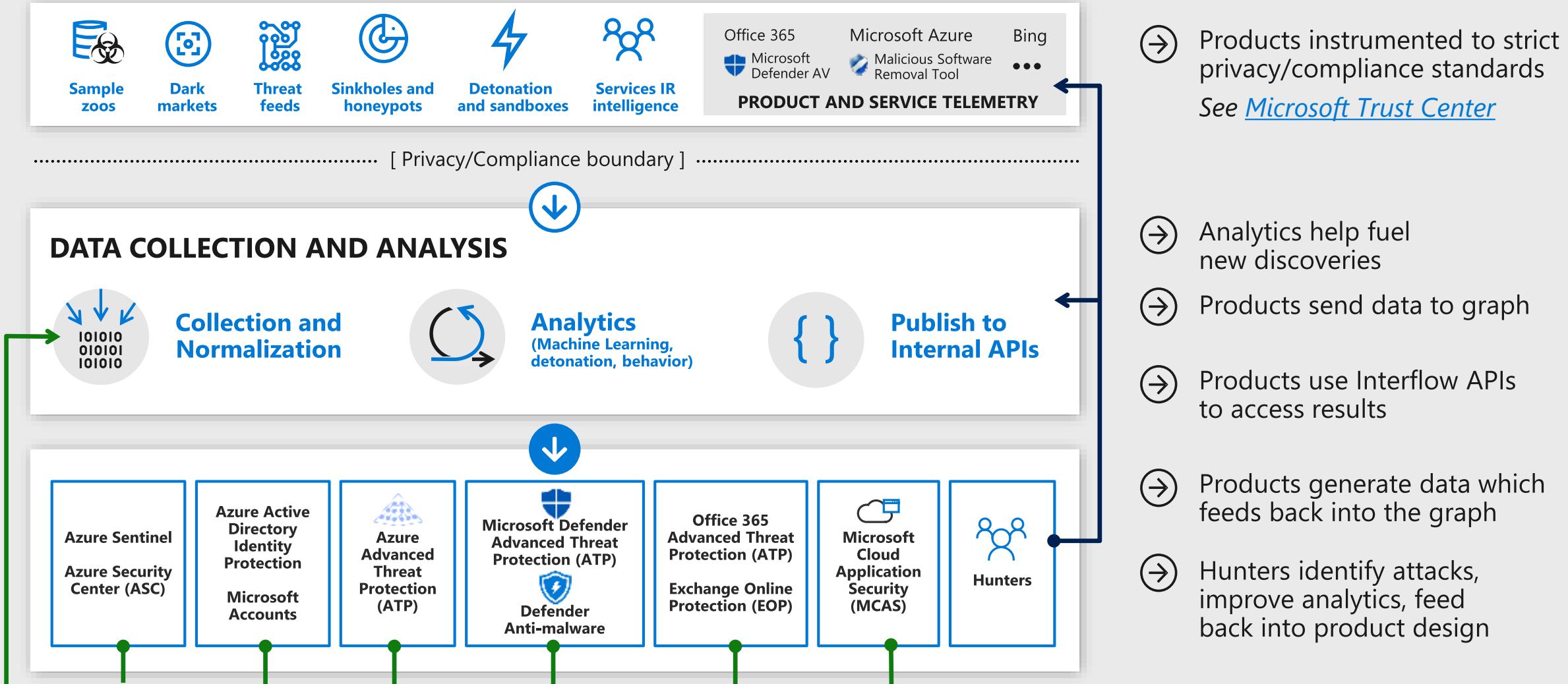
630 billion monthly authentications

18+ billion web pages scanned

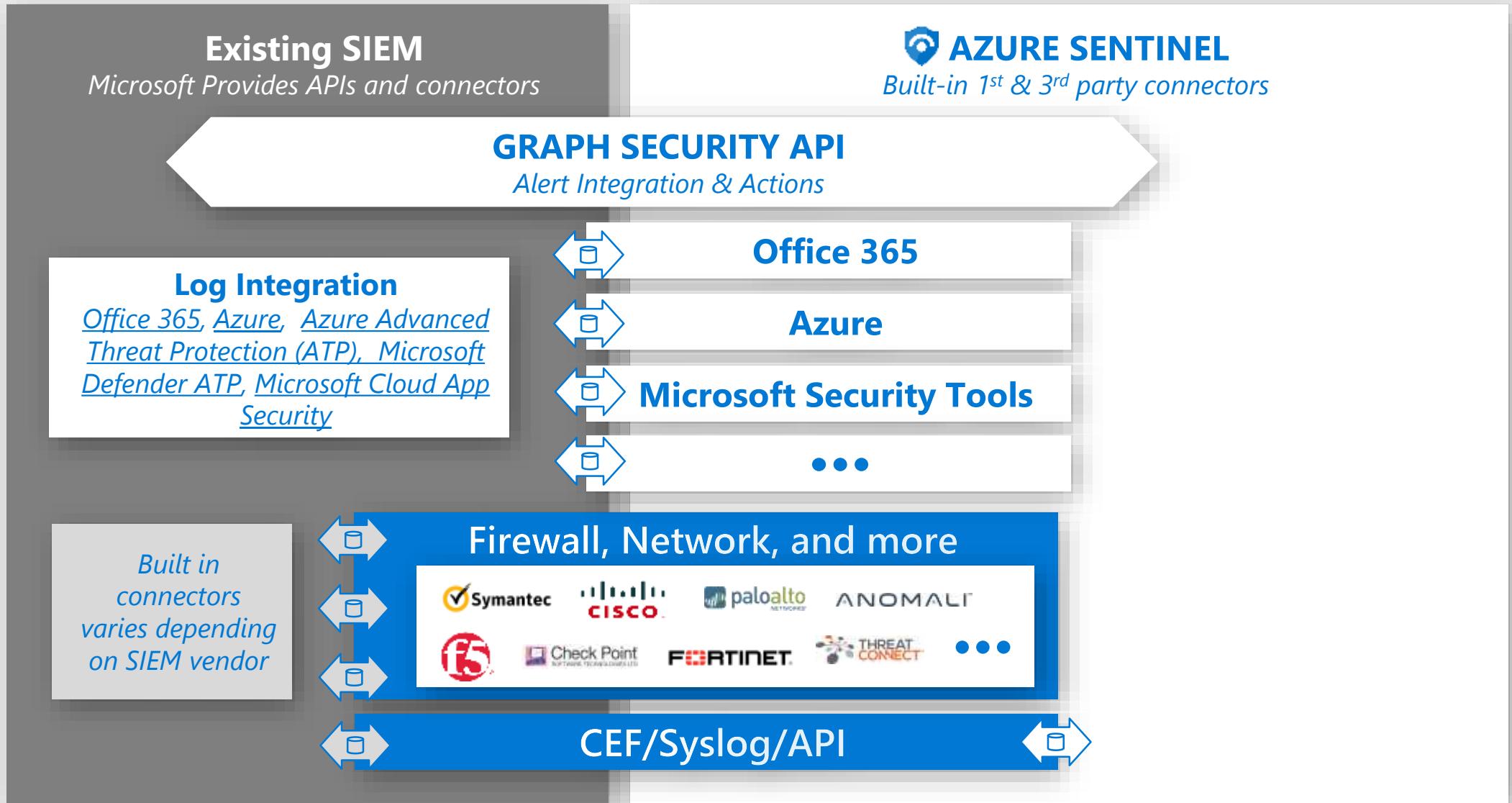
470 billion e-mails analyzed

Unparalleled cybersecurity visibility and insight

Inside The Intelligent Security Graph

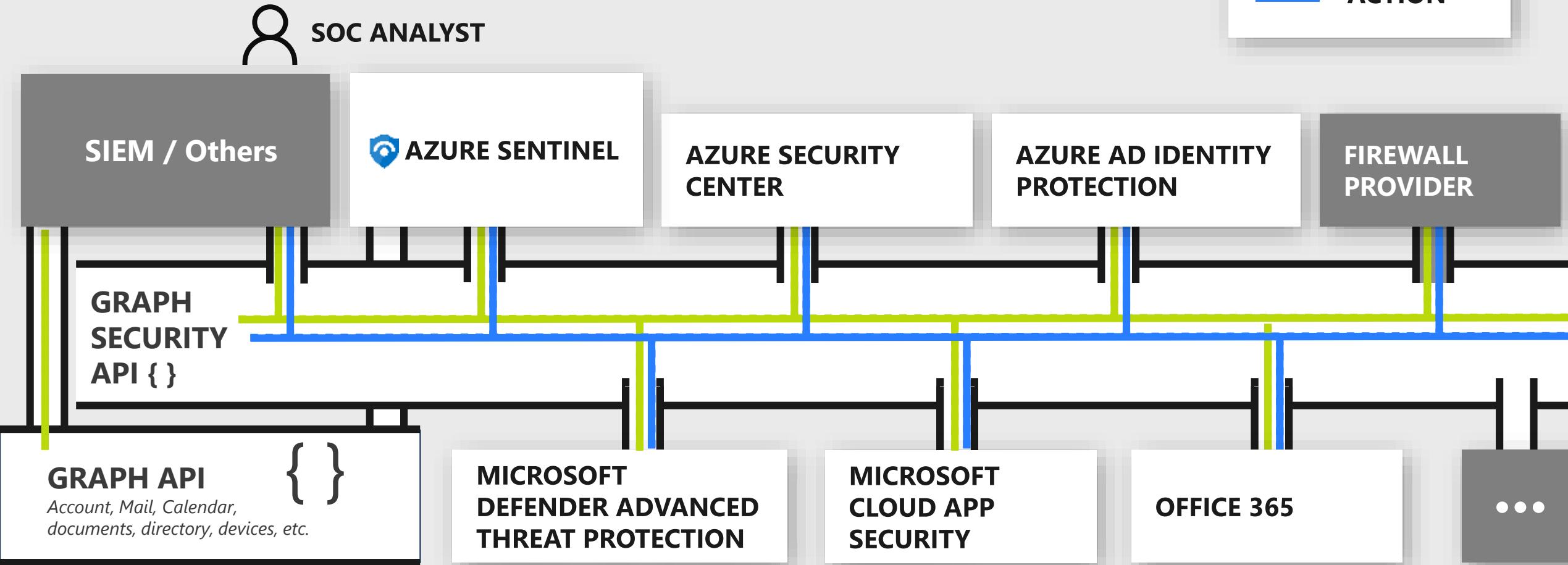


SIEM Integration



SOC Integration

Unifying and Informing Analysts



<http://aka.ms/graphsecurityapi> | <https://aka.ms/graphsecuritydocs>

AZURE SENTINEL

Core capabilities

Collect

Microsoft Services



Apps, users, infrastructure



Public Clouds



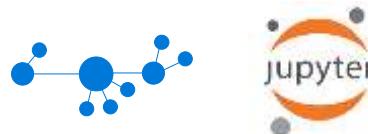
Security solutions

Analyze & detect threats



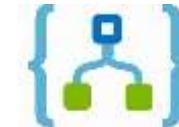
Machine learning,
UEBA

Investigate & hunt suspicious activities



Interactive Attack Visualization,
Azure Notebooks

Automate & orchestrate response



Playbooks

Integrate



ServiceNow



Other tools

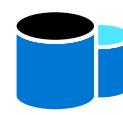


Community

Enrichment with Intelligence (Geo location, IP Reputation)



Data Ingestion



Data Repository



Data Search

Azure Monitor
(log analytics)

Azure

Integrated toolset for rapid threat remediation

Microsoft Threat Protection

Cloud Native SIEM + SOAR - Azure Sentinel (Preview)

Built on Azure Monitor, Logic Apps, and Microsoft's UEBA/ML Technology

Microsoft Security Center



ENDPOINT

Microsoft Defender ATP
Endpoint Detection & Response (EDR)



IDENTITY

Azure ATP + Azure AD
Identity Protection



SaaS

Office 365 Advanced Threat Protection (ATP) + Cloud App Security



AZURE

Azure Security Center



NETWORK

3rd party and Microsoft Logs and Tools



SERVERS



OTHER

Depth

- *High quality alerts*
- *End to end investigation and remediation*

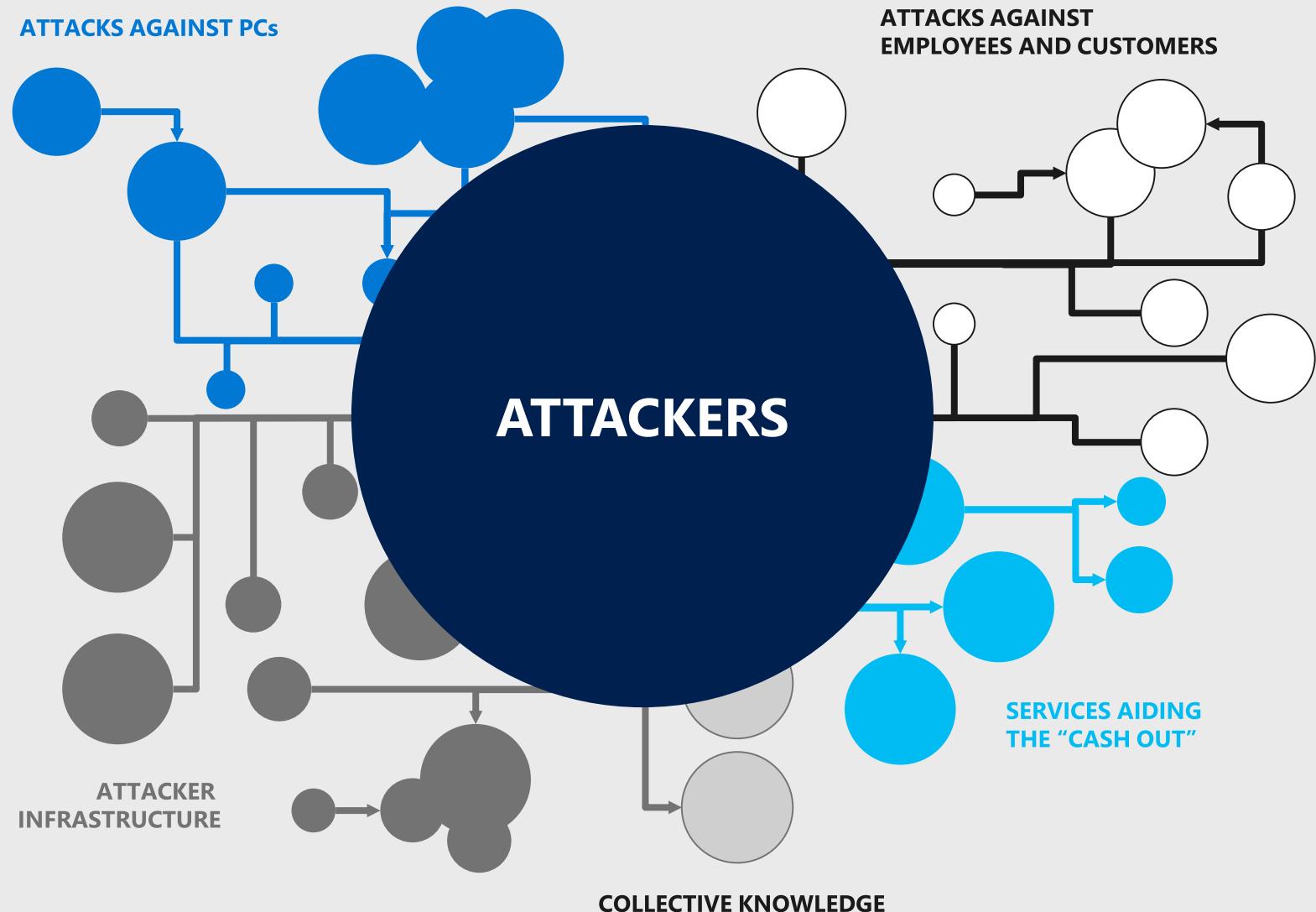
Breadth

- *Unified Alert Queue*
- *Customized Alerts*

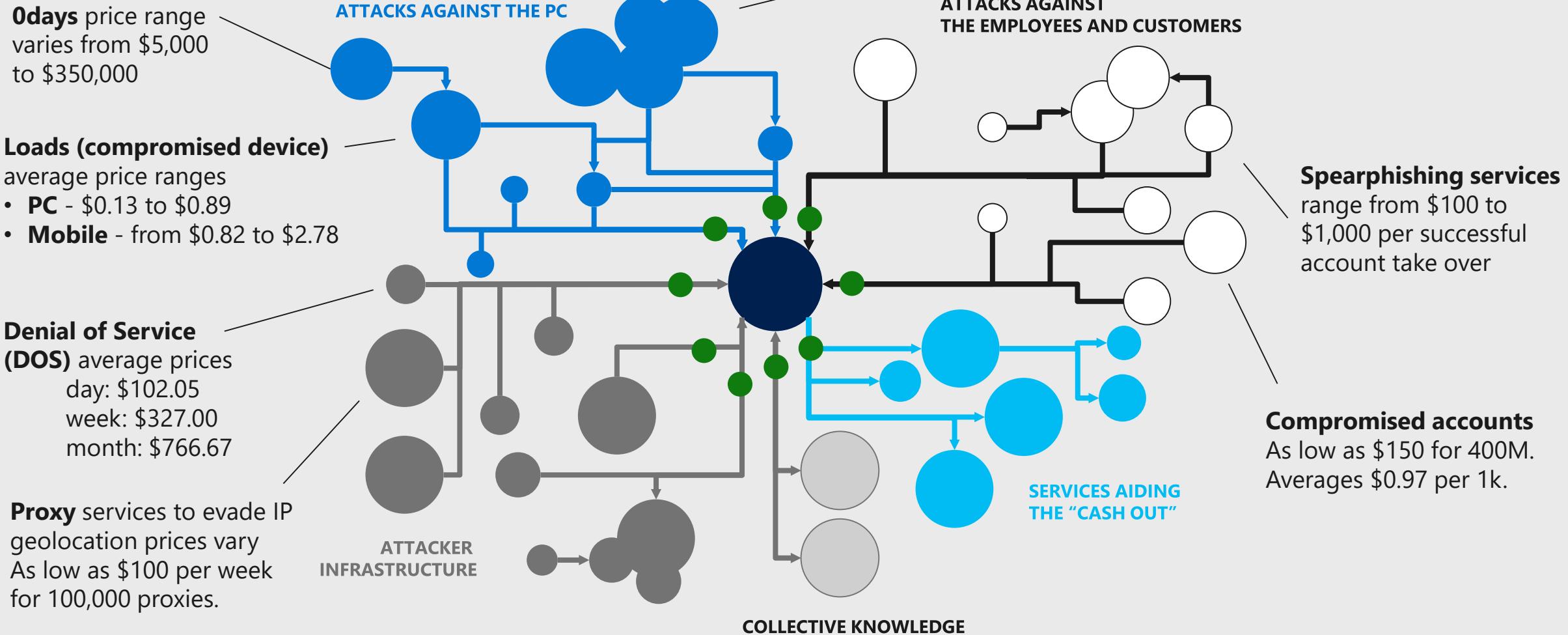
Most attackers have a supply chain

You face **ecosystems**,
not just hackers and
malware

Defenses must address
current attacker methods



Yes, attack services are inexpensive



Yes, attack services are inexpensive

0days price range varies from \$5,000 to \$350,000

Loads (compromised device)

average price ranges

- PC - \$0.13 to \$0.89
- Mobile - from \$0.82 to \$2.78

Proxy services to evade IP geolocation prices vary
As low as \$100 per week for 100,000 proxies.

Denial of Service (DOS)

average prices

day: \$102.05

week: \$327.00

month: \$766.67

PRIORITIZE HYGIENE OVER 'ZERO DAY' DEFENSES

Zero day vulnerabilities are expensive and impractical for many attacks. Focus first on critical security hygiene like rapidly applying security updates/patches (which have much lower cost to attackers) <https://aka.ms/CyberHygiene> has guidance from Microsoft + NIST + CIS + DHS NCCIC

SHIFT FROM NETWORK TO ZERO TRUST STRATEGIES

Attackers can easily evade traditional network defenses. You should shift security strategy towards 'zero trust' of your network that focuses on

- Endpoint and Identity security capabilities as the front line
- Data centric security that prioritizes highest value assets
- Application / SaaS protections
- Centralized access control (such as Microsoft's Conditional Access)

LIMIT EFFORTS TO RESTRICT TRAFFIC BY GEOGRAPHY

Blocking IP addresses by geography (e.g. hostile countries) can be easily and cheaply evaded, so focus your security efforts elsewhere.

DDoS Protection FOR CRITICAL SERVICES

Ensure that your business critical services have DDoS protection from Azure platform or a capable 3rd parties

Ransomware:

\$66 upfront

Or

30% of the profit (affiliate model)

Spearphishing services

range from \$100 to \$1,000 per successful account take over

Compromised accounts

As low as \$150 for 400M.
Averages \$0.97 per 1k.

Pragmatic intelligence investment

Attacks are commoditized and cheap

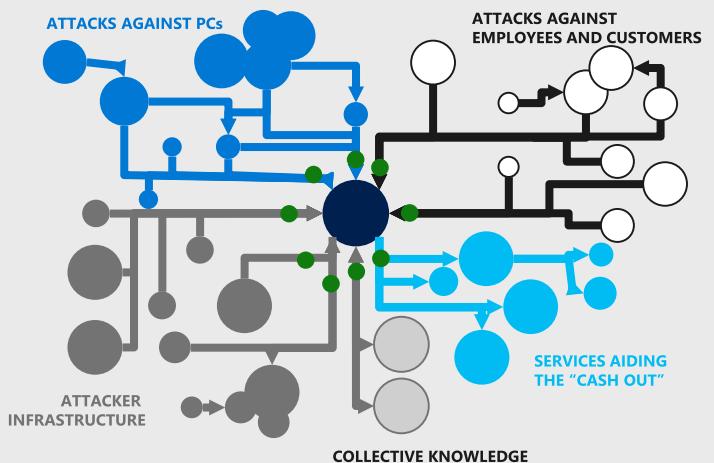
Complicates attack attribution

Enables new entrants with affiliate models

Recommend a two part strategy

1. **“Outsource” commodity threat intelligence**
2. **Focus on developing your unique intelligence**

1. Which attackers would be interested in you
2. What they would target
3. What would damage your business/mission most



Microsoft's intelligent security graph includes actionable dark market threat intelligence

Machine Learning

Helps overcome human limitations using large datasets

1. Scales out Human Expertise



2. Shines a light in human blind spots

Machine Learning **also brings risks**

Must manage potential negative consequences

1. Can amplify human bias



2. Can inadvertently reveal private/secret information

3. Can miss critical context and implications

(e.g. Confuse innocent "John Smith" with another "John Smith" with criminal record and same birthdate)

4. Can be fed false/malicious data

Microsoft Mitigation Approach – <https://aka.ms/ProtectingML>

Machine Learning in Microsoft Security

We use machine learning extensively to

- Reduce manual effort
- Reduce wasted effort on false positives
- Speed up detection



Examples:

- Defender ATP Antivirus - rapid detection and blocking of new threats
- Azure - Rule recommendations for Application whitelisting
- Azure - Threat detection via Malicious User Profiling, Compromised VM behavior

Results from Machine Learning

A former rules-based Microsoft system scored

28% of logins
as suspicious

With 1 billion logins per day
=280 million "suspicious" logins

Noisy Results

- 🌐 Company Proxy
- 📱 Cellphone networks
- 🚗 Vacations/Travel

After applying Machine Learning with rules, the rate dropped to less than

0.001%

Work by Mace et. al, Microsoft

Machine Learning in Microsoft Defender AV

Local ML models, behavior-based detection algorithms, generics, heuristics

Client ML

Cloud ML

Protection in milliseconds

Most common malware blocked by high-precision detection on the client

Protection in milliseconds

ML powered cloud rules evaluate suspicious files based on metadata

Protection in seconds

A sample is uploaded for inspection by multi-class ML classifiers

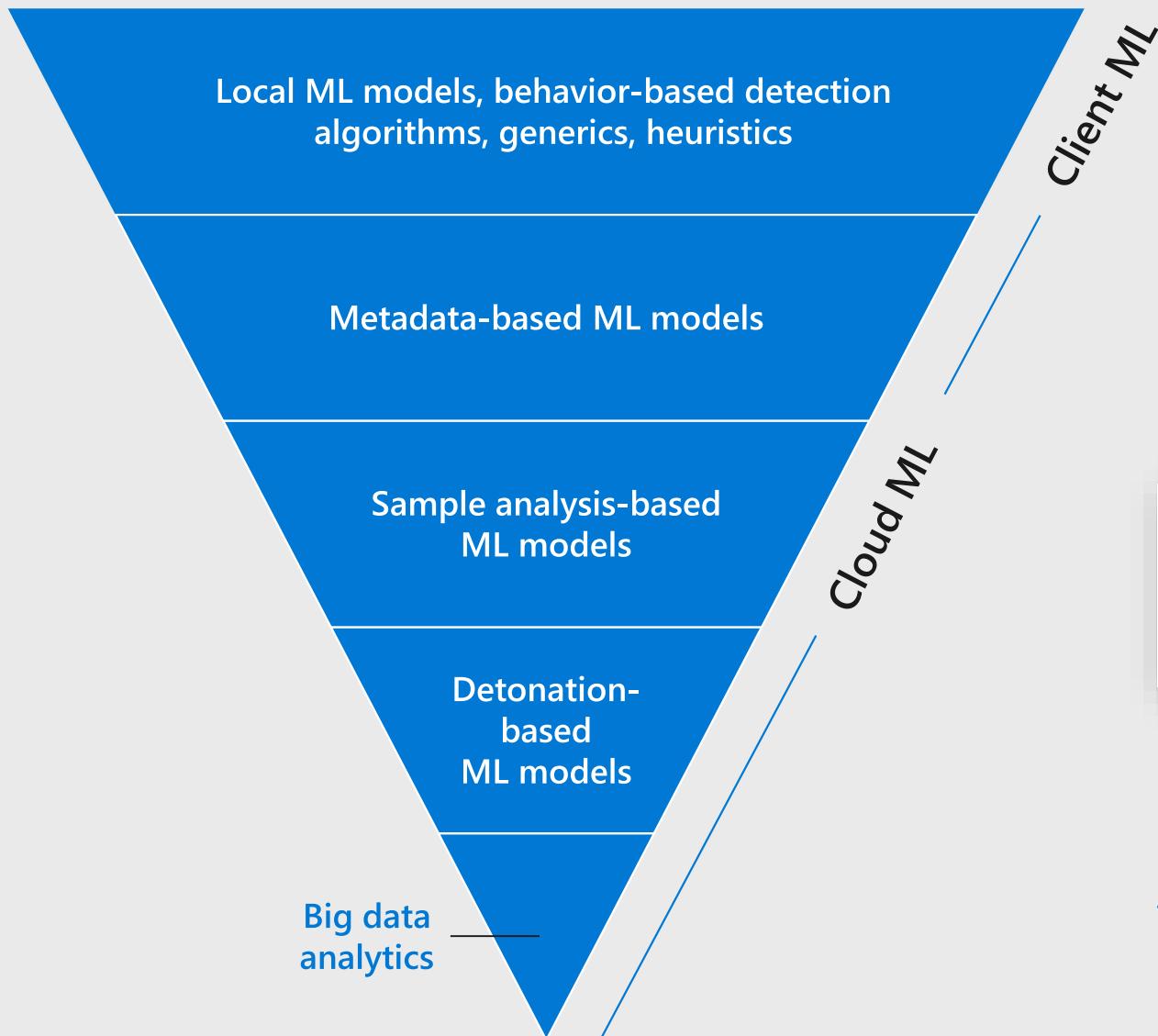
Protection in minutes

Sample run in sandbox for dynamic analysis by multi-class ML classifiers

Protection in hours

ML models and expert rules correlate signals from a vast network of sensors to classify threats

Real world example – Dofoil / Smoke Loader



Protection in milliseconds

Just before noon, behavior-based algorithms detected a massive campaign

Protection in milliseconds

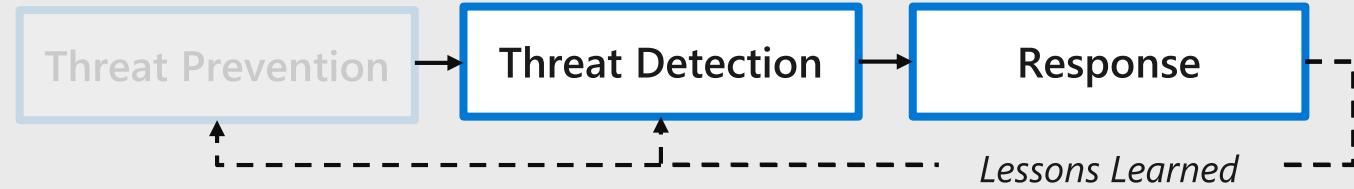
Most components of the attack were blocked at first sight by metadata-based ML models

Protection in seconds

Additional Protection was provided by sample analysis-based ML models for some components

On March 6, Microsoft Defender Antivirus blocked more than 400,000 instances of several sophisticated trojans
<http://aka.ms/dofoil>

Other recent cases: [Emotet](#) | [Bad Rabbit](#)



At some point the adversary has
to do something anomalous—



**You have to be able to spot that
and quickly take action on it**



Making better decisions faster

① Maximize Visibility

Internal – Sensor coverage completeness and diversity

External – Threat Feed Diversity and fidelity

② Reduce manual steps (and errors)

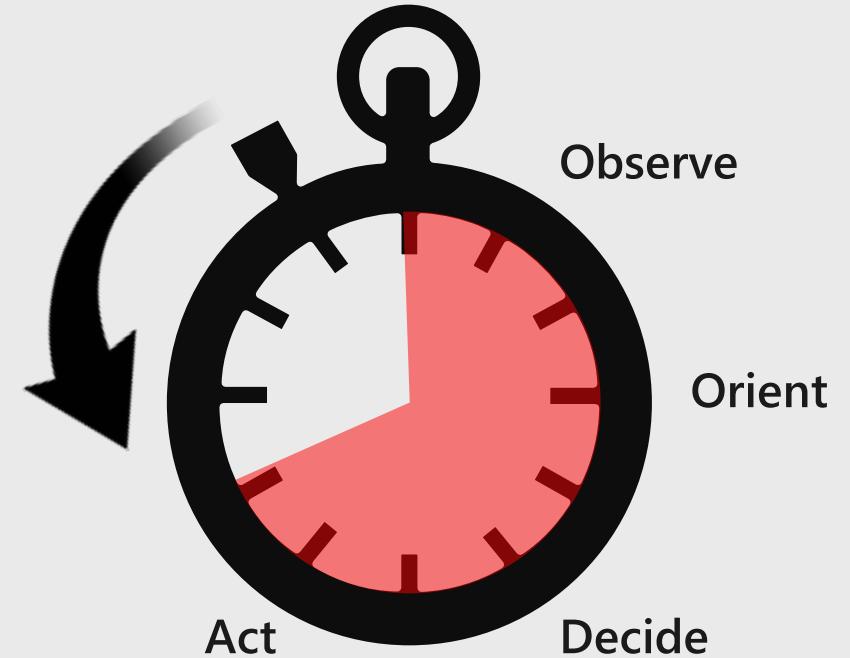
Automate detection and response tasks

Integrate investigation tools

③ Maximize human impact

Provide analysts with access to **deep expertise and intelligence**

Continuous Learning– Observe attacks and integrate learnings into defenses



DEFENDER DECISION CYCLE

DETECT

RESPOND

RECOVER

Observe

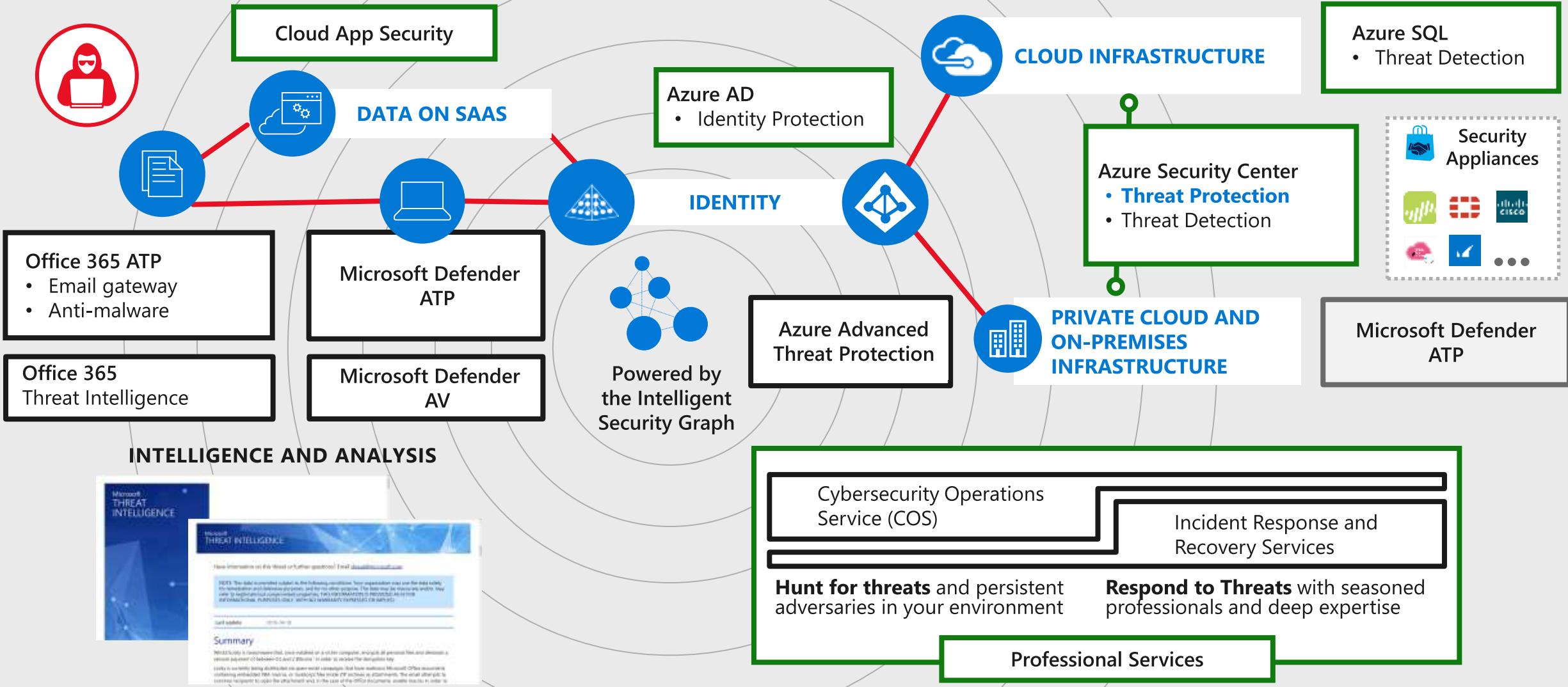
Orient

Decide

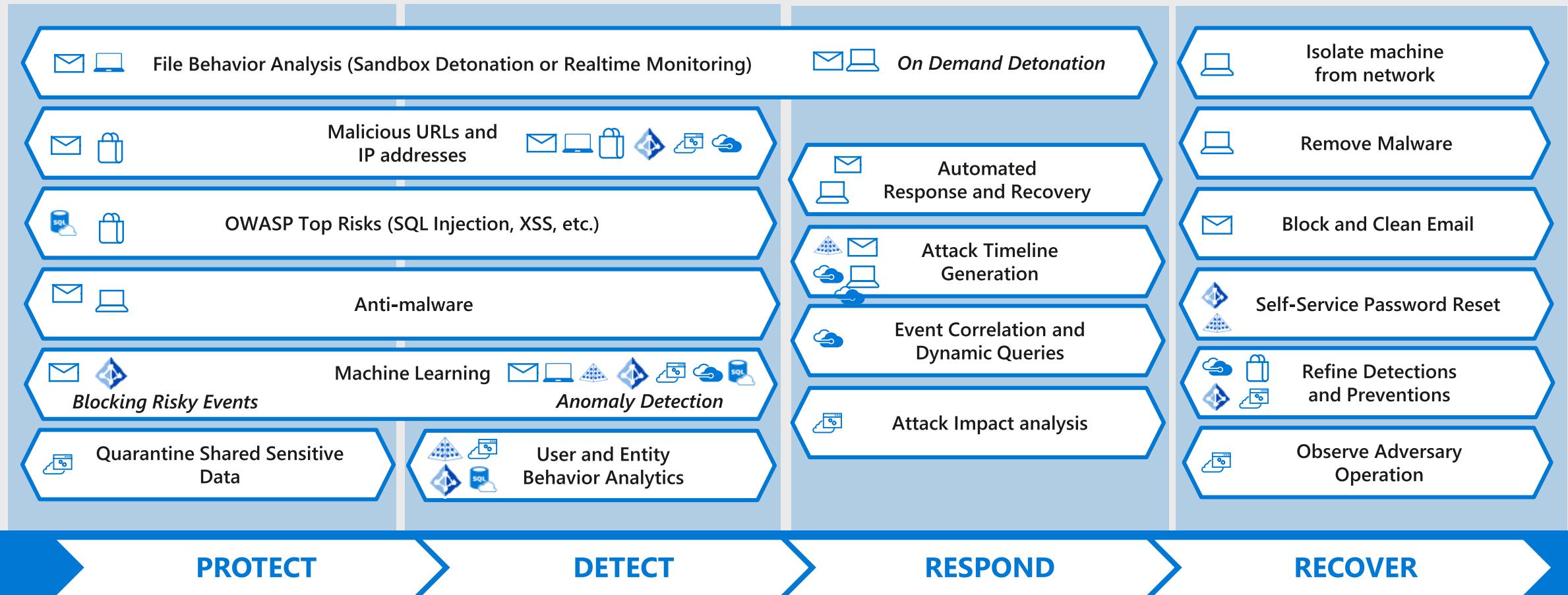
Act

Maximize internal visibility

Apply Threat Insights Across Your Hybrid Cloud Estate



Automate and enable threat protection



Azure AD Identity Protection

Azure ATP / Identity Manager

Office 365 ATP

Microsoft Defender ATP / Defender AV

Microsoft Cloud App Security

Azure Security Center

Azure Web App Firewall / SQL Threat Detection

Azure Marketplace Partner Capability

Threat protection



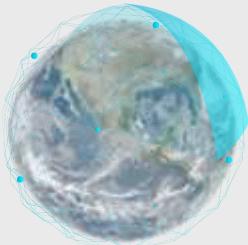
Goal: Increase attacker cost as rapidly and efficiently as possible

- 1** Prevent as many threats as possible
(Best Security ROI when available)

STRATEGIC IMPERATIVES

- 2** Rapidly Detect and Respond
(highest coverage of assets/scenarios)

- 3** Continually apply learnings
(continuous attack cost increase)



Committed to your success

Accelerate your ability to manage threats by providing secure platforms and products, security capabilities, services, and recommendations



Questions?

© Copyright Microsoft Corporation. All rights reserved. Microsoft, Windows, and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

References



Additional Resources – Threat Protection

Incident Response Reference Guide (IRRG) - <https://aka.ms/IRRG>

Updates to Windows Hello for Business – [Video](#)

Updates to Microsoft Defender ATP's EDR - [Blog](#)

Office 365 Attack Simulation - [Video](#) | [Documentation](#)

Privileged Access Management in O365 – [Video](#)

Shielded VMs for PAWs

<https://blogs.technet.microsoft.com/datacentersecurity/2017/11/29/why-use-shielded-vms-for-your-privileged-access-workstation-paw-solution/>

Microsoft Azure Security Response in the Cloud

<https://gallery.technet.microsoft.com/Azure-Security-Response-in-dd18c678>

Advanced Threat Protection Videos

1. WDATP Automated investigation and response [[YouTube link](#)]

Animation shows how Microsoft Defender ATP frees up time for them to do more advanced hunting and strategic work by automating investigation and response tasks

2. WDATP Secure Score [[YouTube link](#)]

Animation shows how Windows Secure Score helps organizations to stay more secure using PowerBI reports to easily look for CVE's and automatic pushing of Emergency Outbreak Updates.

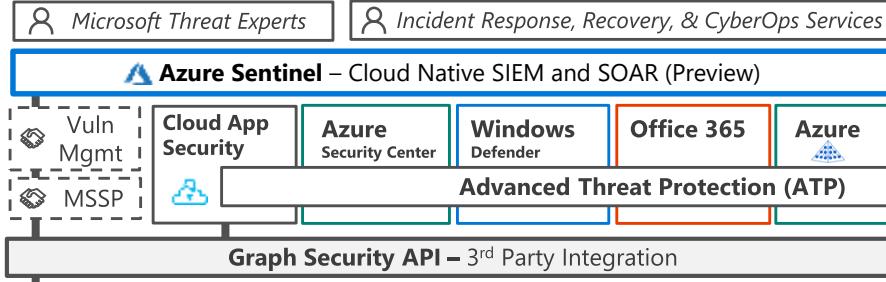
3. WDATP & Azure AD & Intune integration [[YouTube link](#)]

Animation shows how Microsoft Intune will receive the device risk level from Microsoft Defender ATP and CA will block access to data until threat is remediated (and device conforms with policy again).

4. OATP & WDATP detection sharing [[YouTube link](#)]

Video It shows how Microsoft 365 Threat Protection shares signals through the Intelligent Security Graph (ISG) to better protect our customers.

Security Operations Center (SOC)



Cybersecurity Reference Architecture

May 2018 – <https://aka.ms/MCRA> | [Video Recording](#) | [Strategies](#)

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. [Securing Privileged Access](#)
2. [Office 365 Security](#)
3. [Rapid Cyberattacks \(Wannacrypt/Petya\)](#)

Software as a Service

Office 365

- Secure Score
- Customer Lockbox

Dynamics 365



Identity & Access

Azure Active Directory

Information Protection

Conditional Access – Identity Perimeter Management

Cloud App Security

Azure Information Protection (AIP)

- Discover
- Classify
- Protect
- Monitor

Hold Your Own Key (HYOK)

AIP Scanner

- Azure AD Identity Protection
- Leaked cred protection
- Behavioral Analytics

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM



Active Directory

ESAC Admin Forest



Clients

Unmanaged & Mobile Devices



Intune MDM/MAM

Managed Clients



System Center Configuration Manager

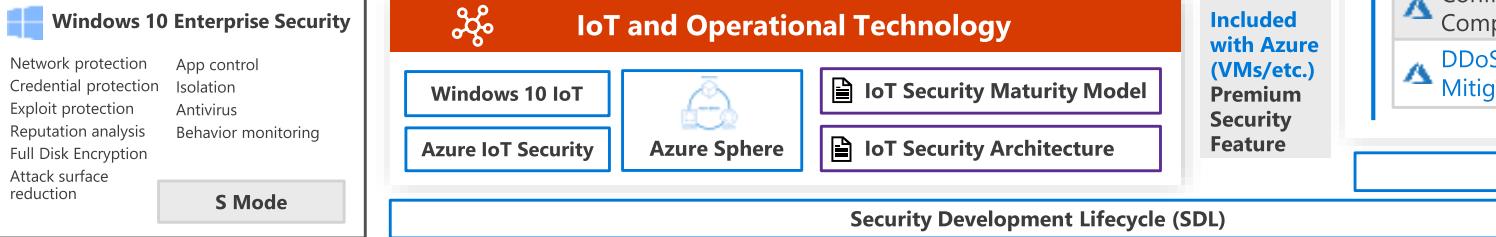
Microsoft Defender ATP



Windows 10 Enterprise Security

- Network protection
- Credential protection
- Exploit protection
- Reputation analysis
- Full Disk Encryption
- Attack surface reduction
- App control
- Isolation
- Antivirus
- Behavior monitoring

S Mode



Conditional Access – Identity Perimeter Management

Cloud App Security

Azure Information Protection (AIP)

- Discover
- Classify
- Protect
- Monitor

Hold Your Own Key (HYOK)

AIP Scanner

- Azure AD Identity Protection
- Leaked cred protection
- Behavioral Analytics

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM



Active Directory

ESAC Admin Forest



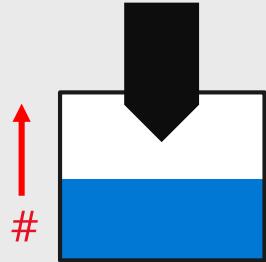
Trust Center

Intelligent Security Graph

Platform security approach



← BACK TO TIMELINE



REDUCE VULNERABILITY COUNT AND SEVERITY

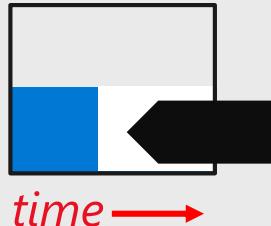
Security Development Lifecycle (SDL)

SD3+C: Secure in

- Design
- Development
- Deployment
- + Communications

<https://www.microsoft.com/SDL>

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44378



REDUCE TIME OF EXPOSURE

Rapid Response

- Bug Bounty
- Rigorous Testing
- Response Center
- Automatic Updates

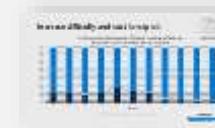
<https://technet.microsoft.com/en-us/security/dn440717.aspx>



INCREASE DIFFICULTY AND COST TO EXPLOIT

Platform Mitigations

- Eliminate classes of vulnerabilities
- Break exploit techniques
- Contain damage
- Prevent persistence
- Limit exploit opportunity window

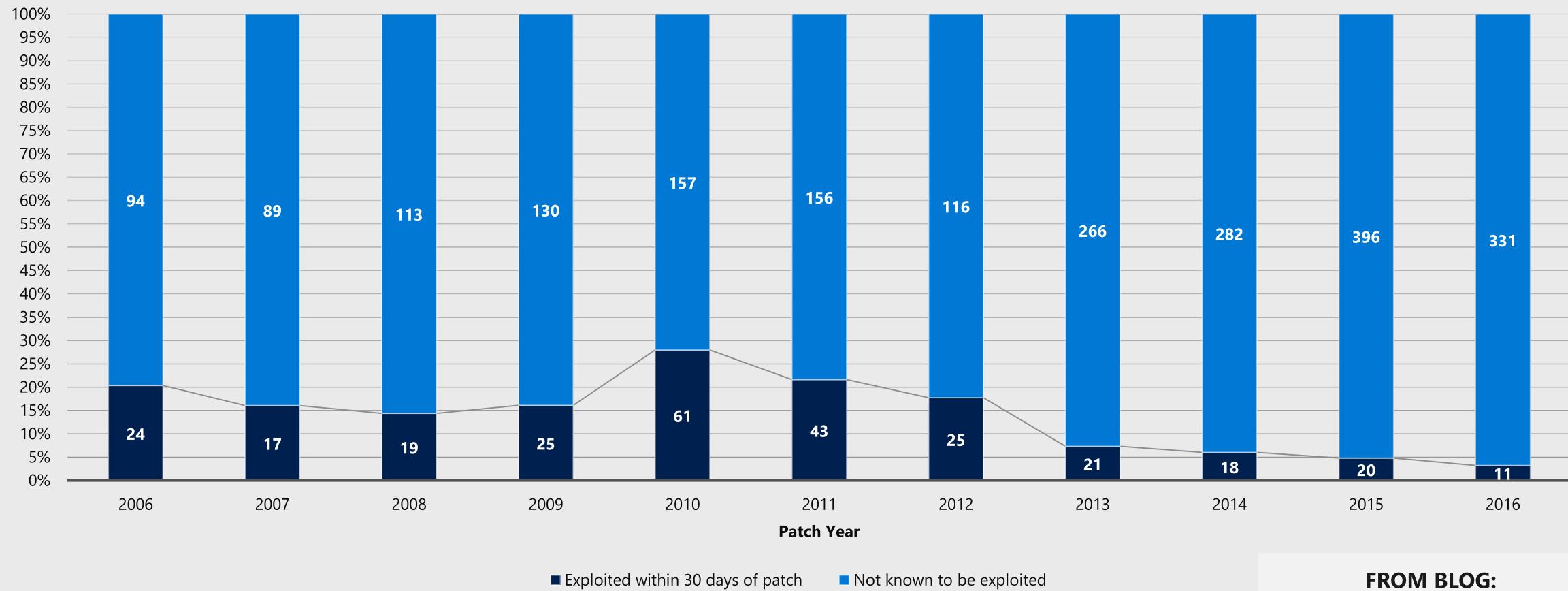




Increase difficulty and cost to exploit

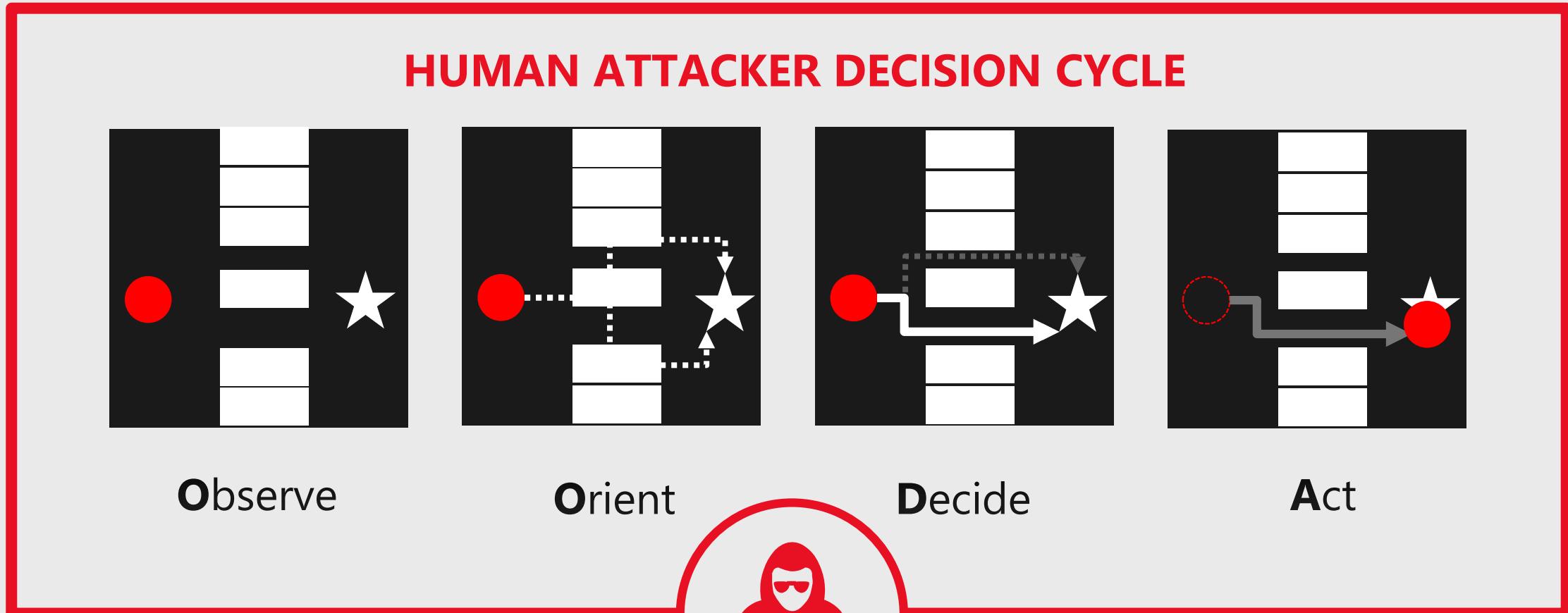
[← BACK TO TIMELINE](#)

% of Remote Code Execution (RCE) and Elevation of Privilege (EOP) CVEs exploited within 30 days of patch



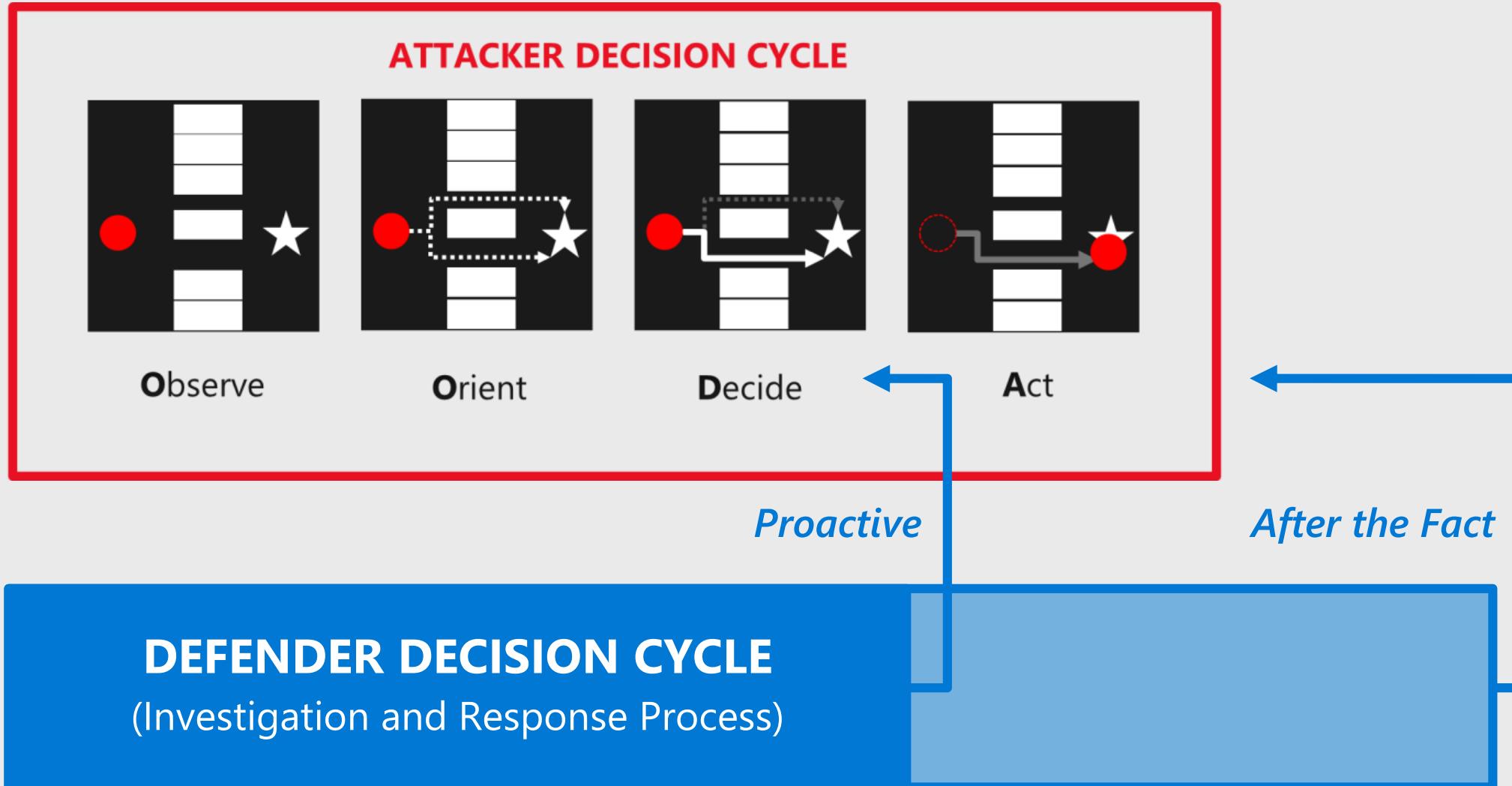
FROM BLOG:
[Mitigating arbitrary native code execution in Microsoft Edge](#)

Rapidly detect and respond



Get inside their OODA loop

Better and Faster Investigation and Response Decisions



Analyst Workflow Integration

- Analysts use an integrated experience for rapid and accurate investigations and remediation
- Analysts quickly pivot from detection to deep investigation of host/identity/email to rapid remediation (blocking email, cleaning malware, resetting credentials, and more)



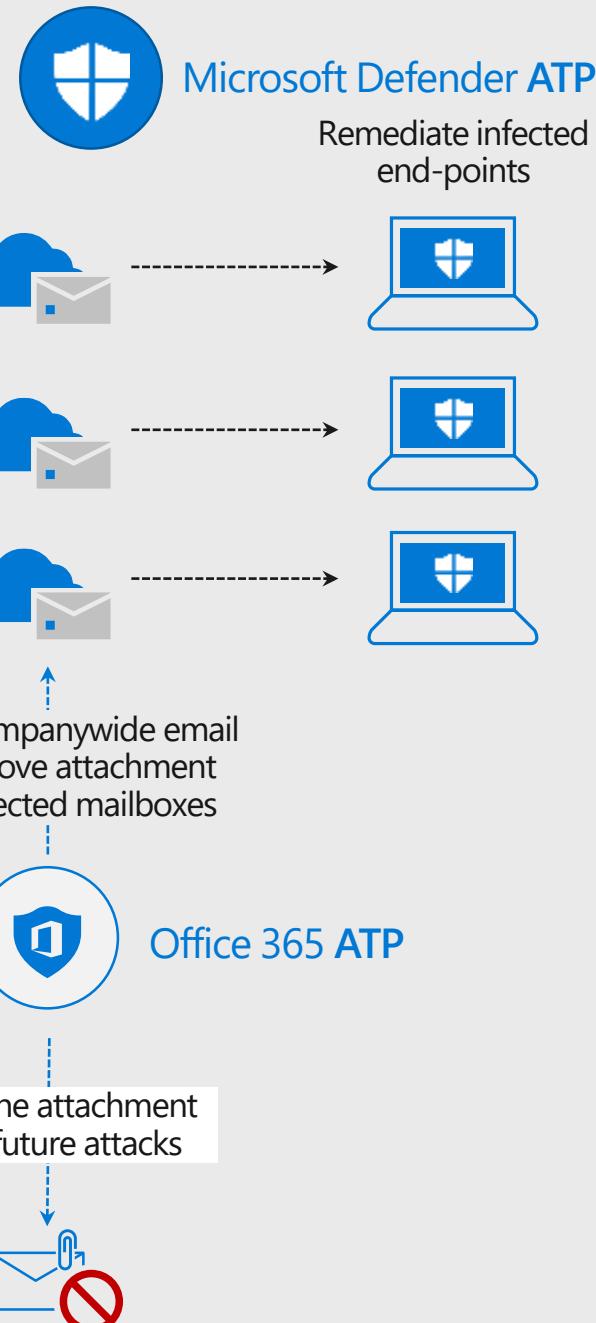
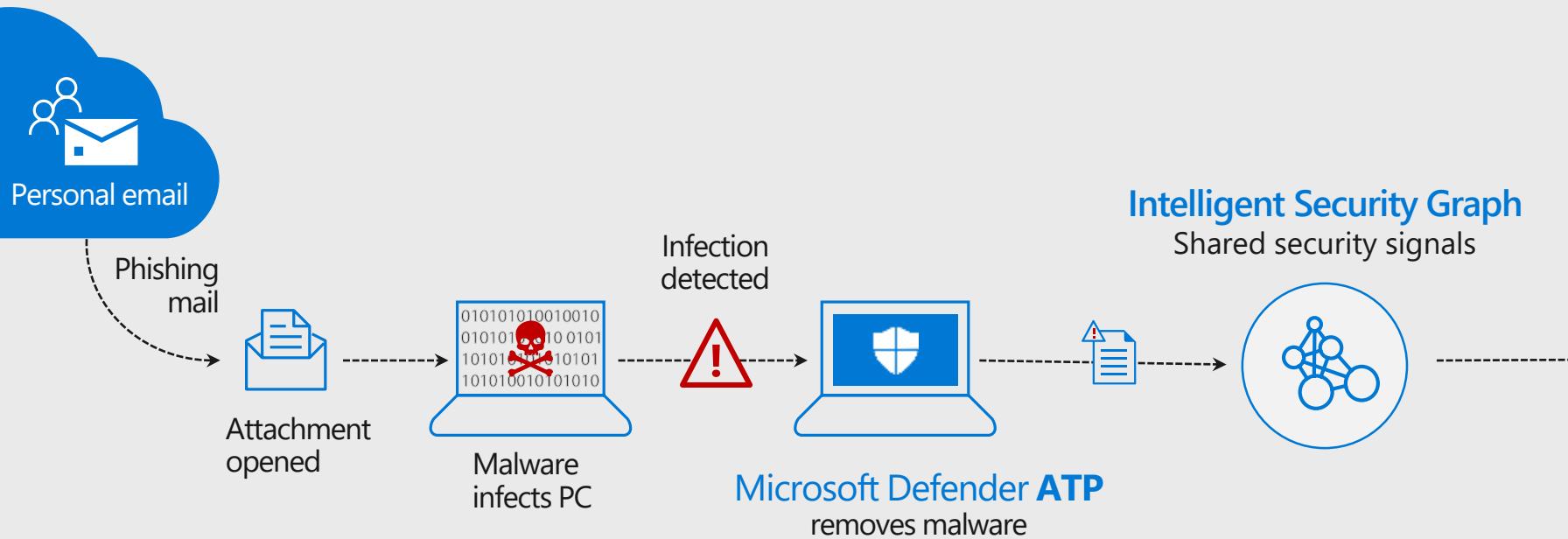
Office 365 Threat Explorer

Microsoft Defender Security Center

Azure Advanced Threat Protection (ATP)

Intelligence Integration + Automation

SCENARIO: Malware gets onto a work PC through a personal email inbox.



Because Minutes Matter

The screenshot shows the Office 365 Security and Compliance center with a focus on an investigation graph for investigation #50ecc9. The graph highlights various threat signals and remediation actions.

Malicious emails found (Callout pointing to the main title area)

User anomalies suggest identity compromise (Callout pointing to the left sidebar under Threat Intelligence)

Malicious mail detected and removed by Office 365 (Main title of the investigation graph)

Triggering Alerts: Automated Investigation, Malicious mail detected and removed by Office 365, Total alerts (4)

Emails investigated (23): Phish (6), Malware (5)

Users investigated (5): Users impacted (2): JeffV@ignitedemo.onmicrosoft.com, RonH@ignitedemo.onmicrosoft.com

Anomalies detected (8): URL clicked (2), Suspicious login (1), Mass downloads (1), Exchange Web Service enabled (1), External mail forwarding (1), Data loss prevention violation (1), Mail delegation enabled (1)

Threats Found (6): Email - Phish, Email - Malware, Data exfiltration - DLP violation, Data exfiltration - Mail forwarding, User - Activity anomalies detected, Compromised Device - Malware

Machines (2): Compromised Device - Malware (2)

Actions (13): Auto-Remediated (13 items listed)

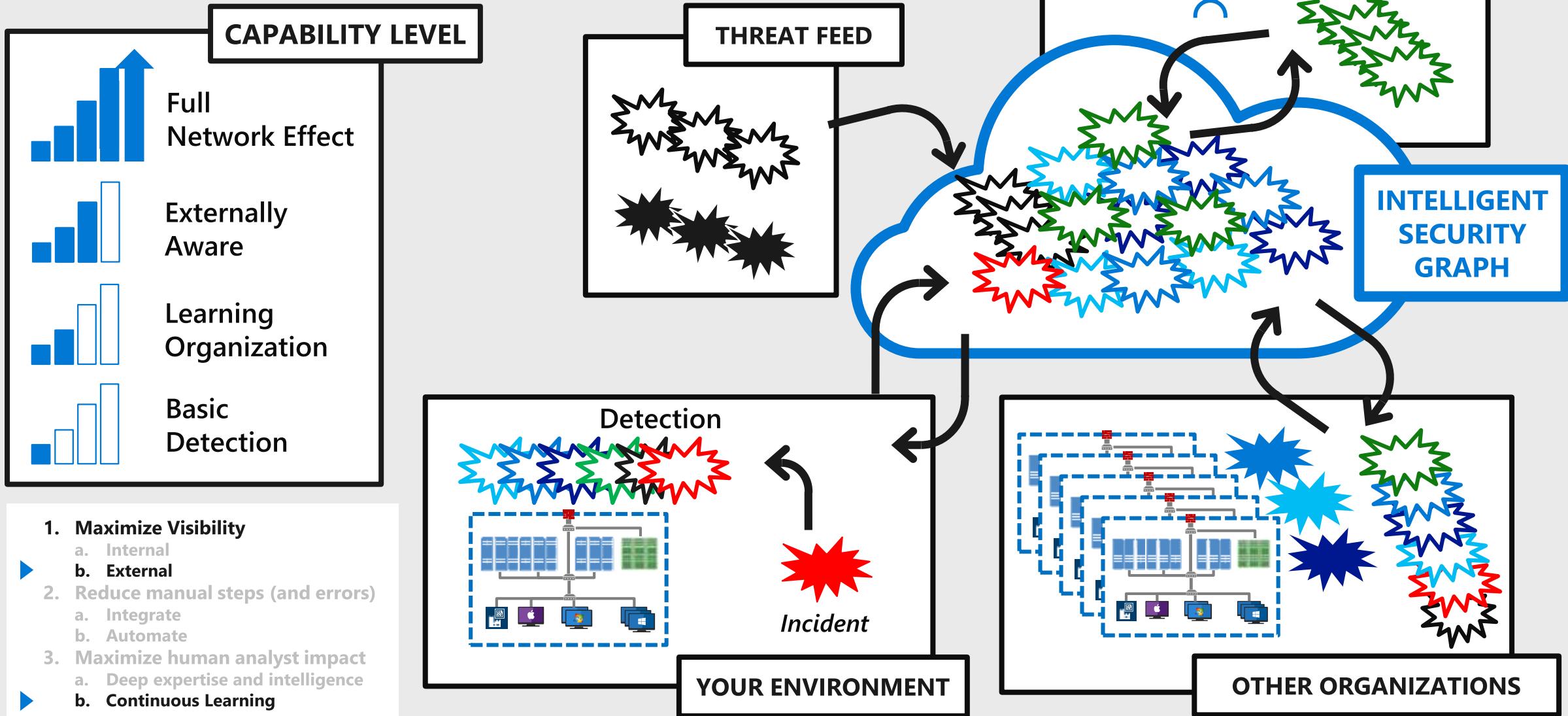
Started: 9/15/2017 12:46 PM
Pending time: 10 min
00:00:23 Pending (Circular timer icon)

Threat signal shared with WDATP for auto remediation (Callout pointing to the right side of the graph)

Automatic remediation actions complete (Callout pointing to the bottom right of the graph)

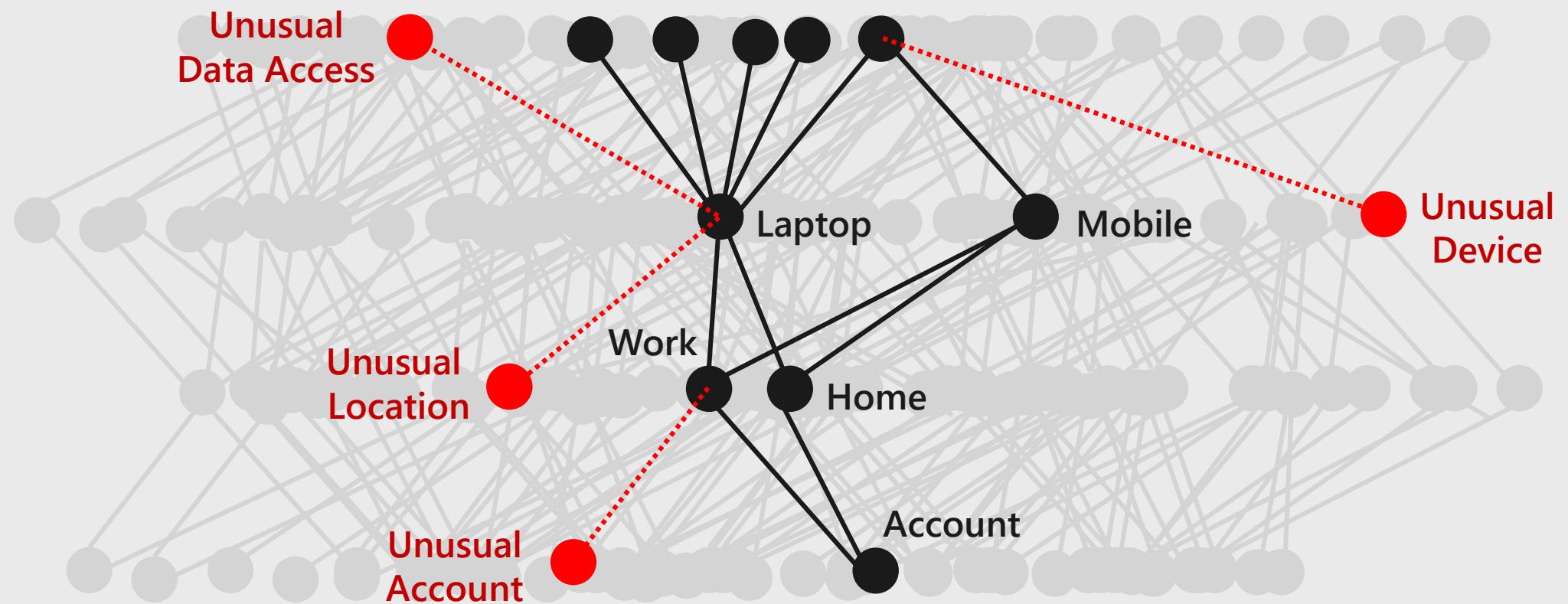
Integrating external context

With a connected defender community

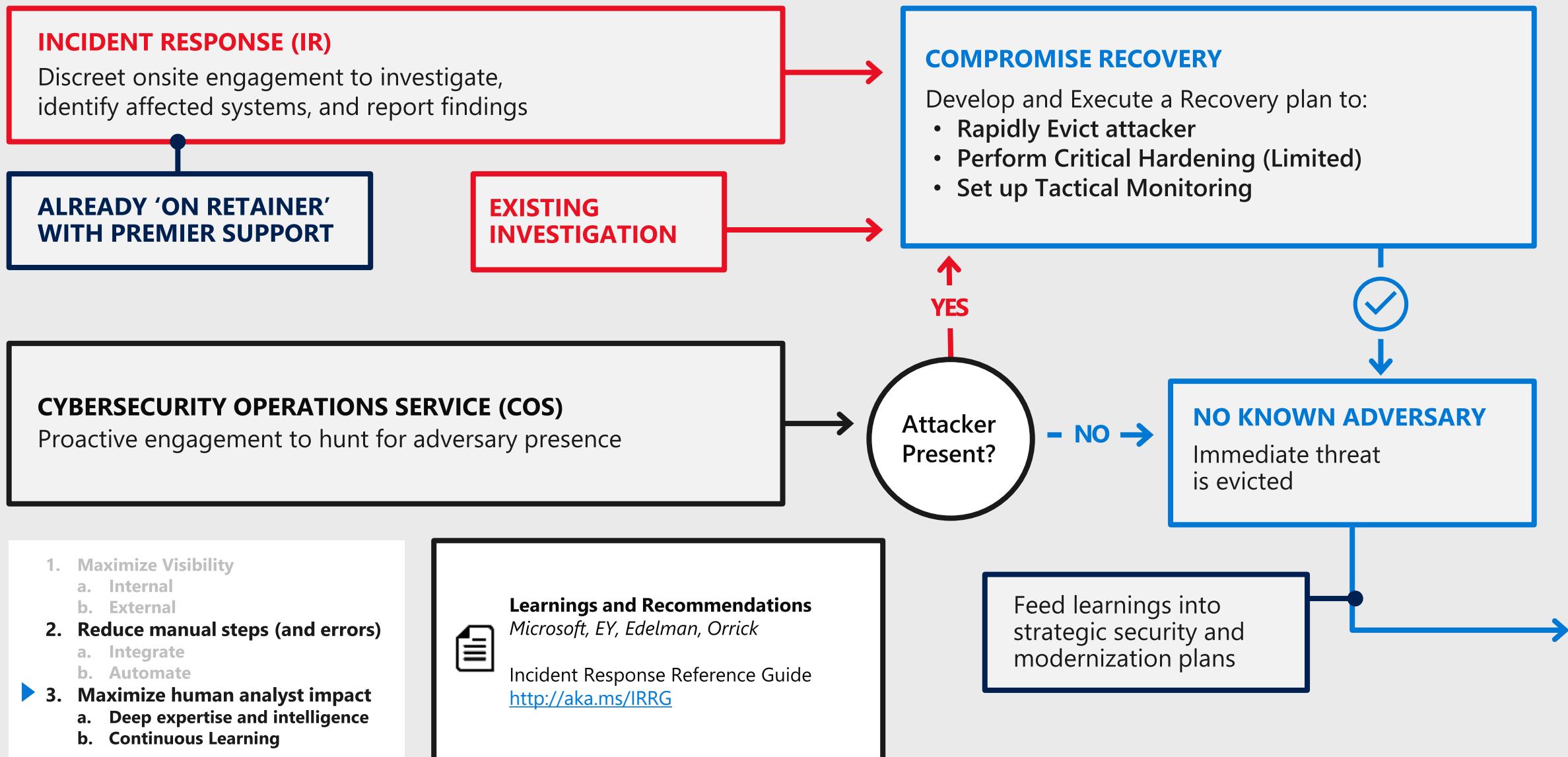


Behavior Analysis

- Unusual behavior lost gets lost in aggregate
- Easier to spot anomalies in individual behavior



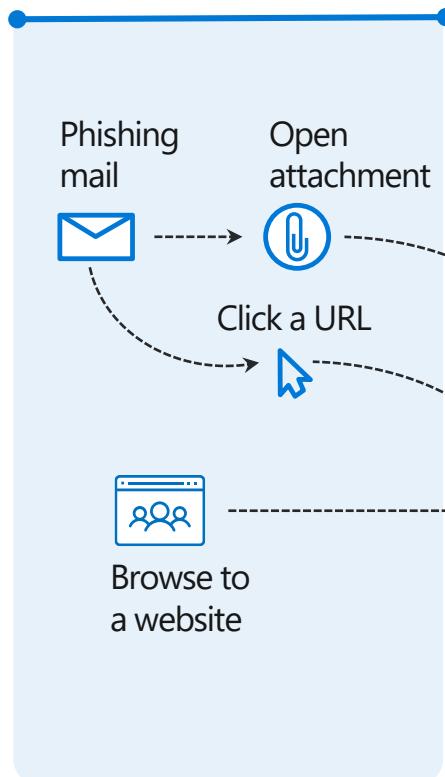
Microsoft incident response services



Protection across an attack kill chain

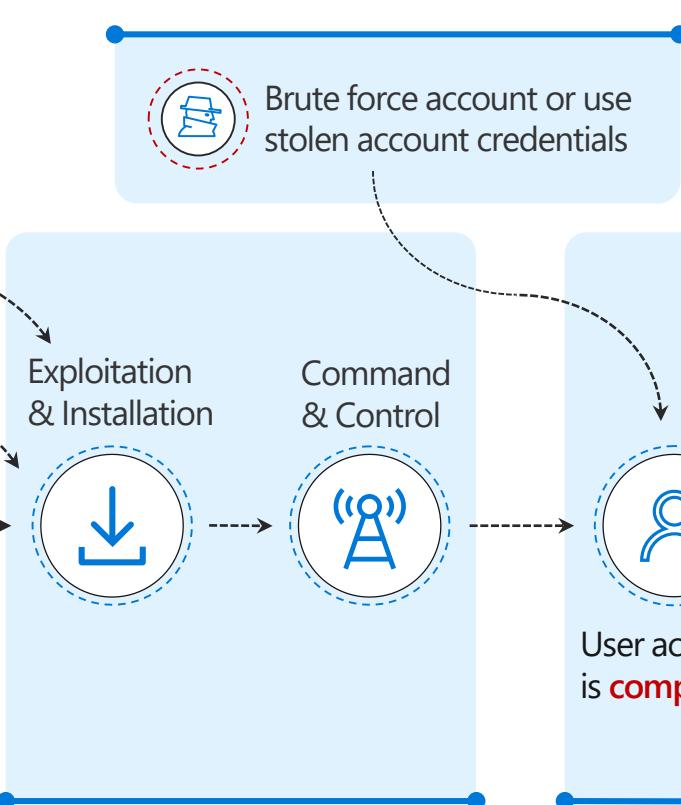
Office 365 ATP

Malware detection, safe links, and safe attachments



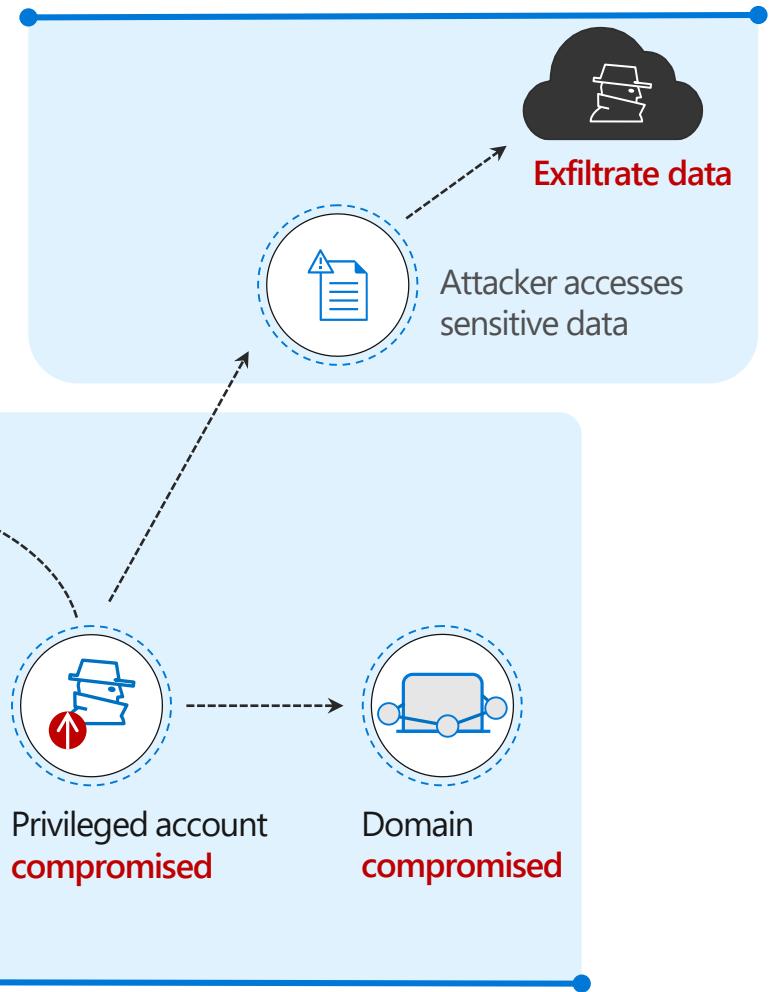
Azure AD Identity Protection

Identity protection & conditional access



Microsoft Cloud App Security

Extends protection & conditional access to other cloud apps



Microsoft Defender ATP

Endpoint Detection and Response (EDR) & End-point Protection (EPP)

Azure ATP

Identity protection