Microsoft

Microsoft CISO Workshop
4b - Threat Protection Strategy (DETECT-RESPOND-RECOVER)

Microsoft Cybersecurity Solutions Group

Threat protection (Detect-Respond-Recover)

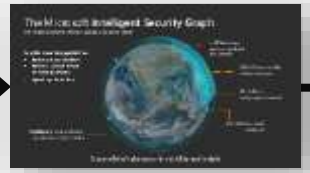
TRENDS

THREAT EVOLUTION

SOC MISSION EVOLUTION

EVOLUTION OF MICROSOFT SOC

STRATEGY



INTELLIGENCE

SUCCESS CRITERIA

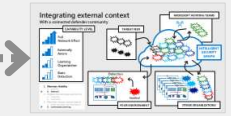
RECOMMENDED APPROACH

APPLYING TO OPERATIONS

SIEM INTEGRATION

INTEGRATED OPERATIONS

INTEGRATED AUTOMATION



COMMUNITY EFFECT

AND MORE

DEEP DIVES

TYPICAL KILL CHAIN

APPLYING MACHINE LEARNING

DARK MARKETS

GRAPH SECURITY API

Observations and challenges

Threats increasing in volume and sophistication

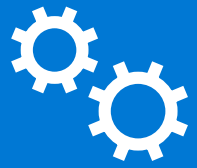
Attacker business models evolve to maximize attacker return on investment (ROI)

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

Reducing mean time to remediation (MTTR) by optimizing expert human decisions

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

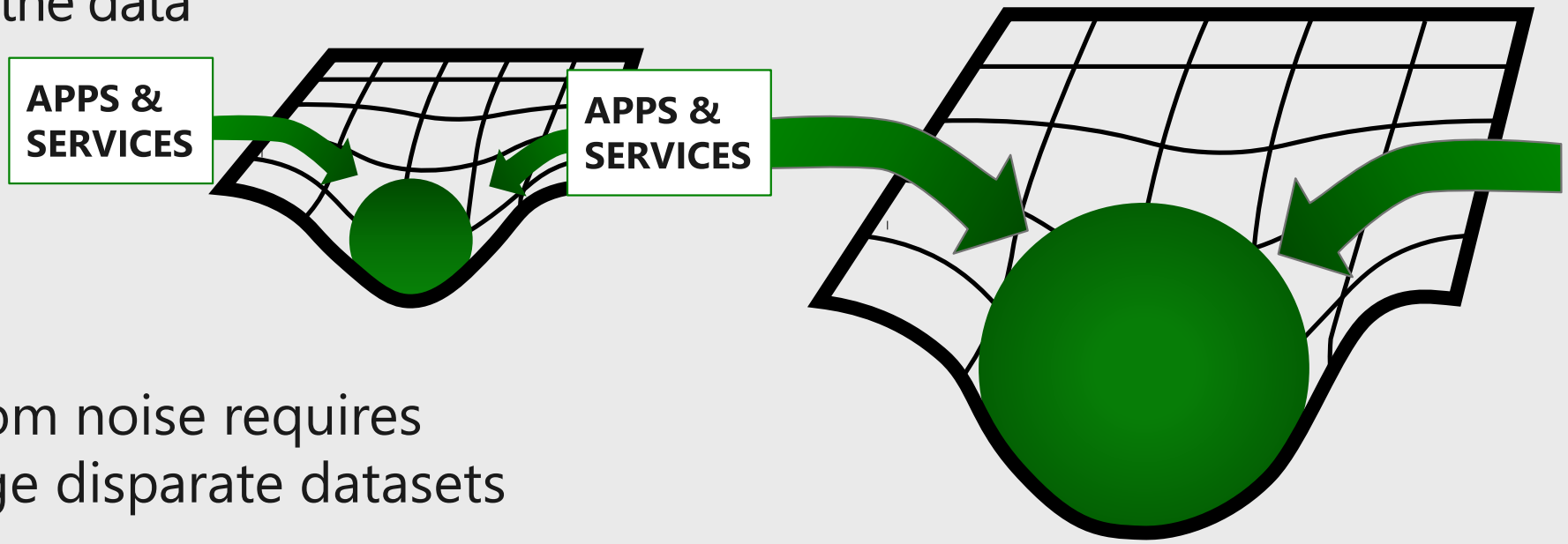
OBSERVE – Increase Field of view with vast intelligence data

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

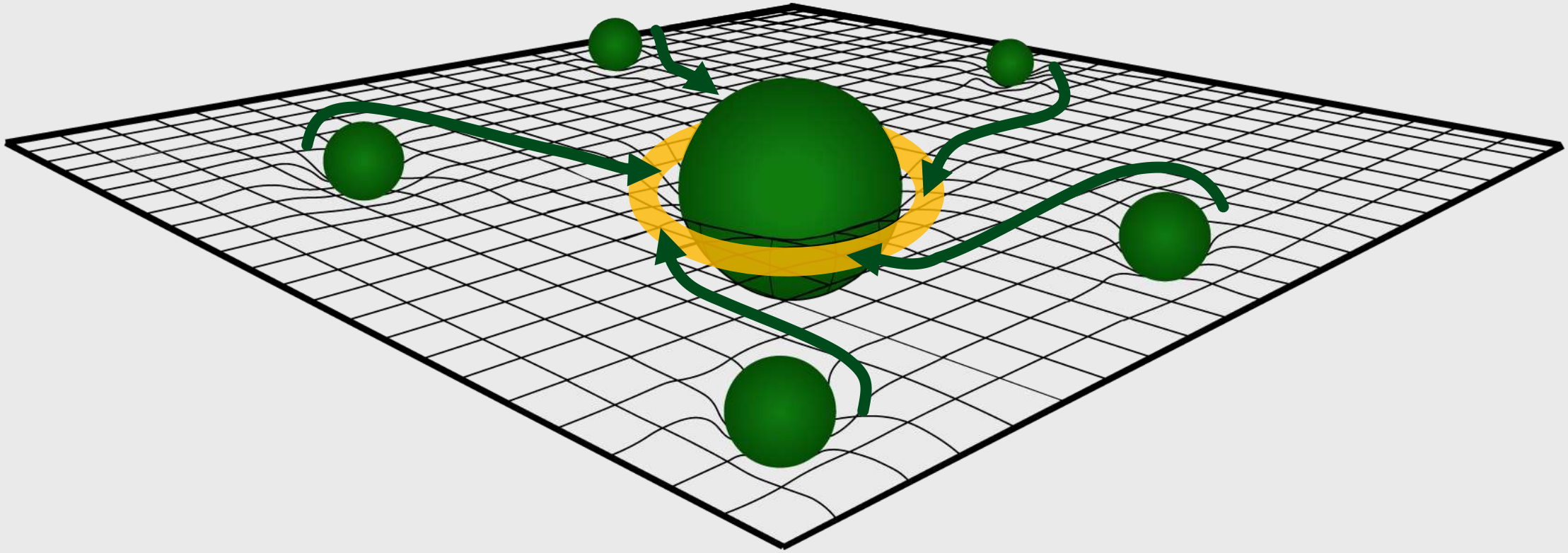
→ Need to leverage analytics from anywhere and centrally integrate

Data Gravity

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

SOC Signal Rationalization

Many data sources in a SOCs today



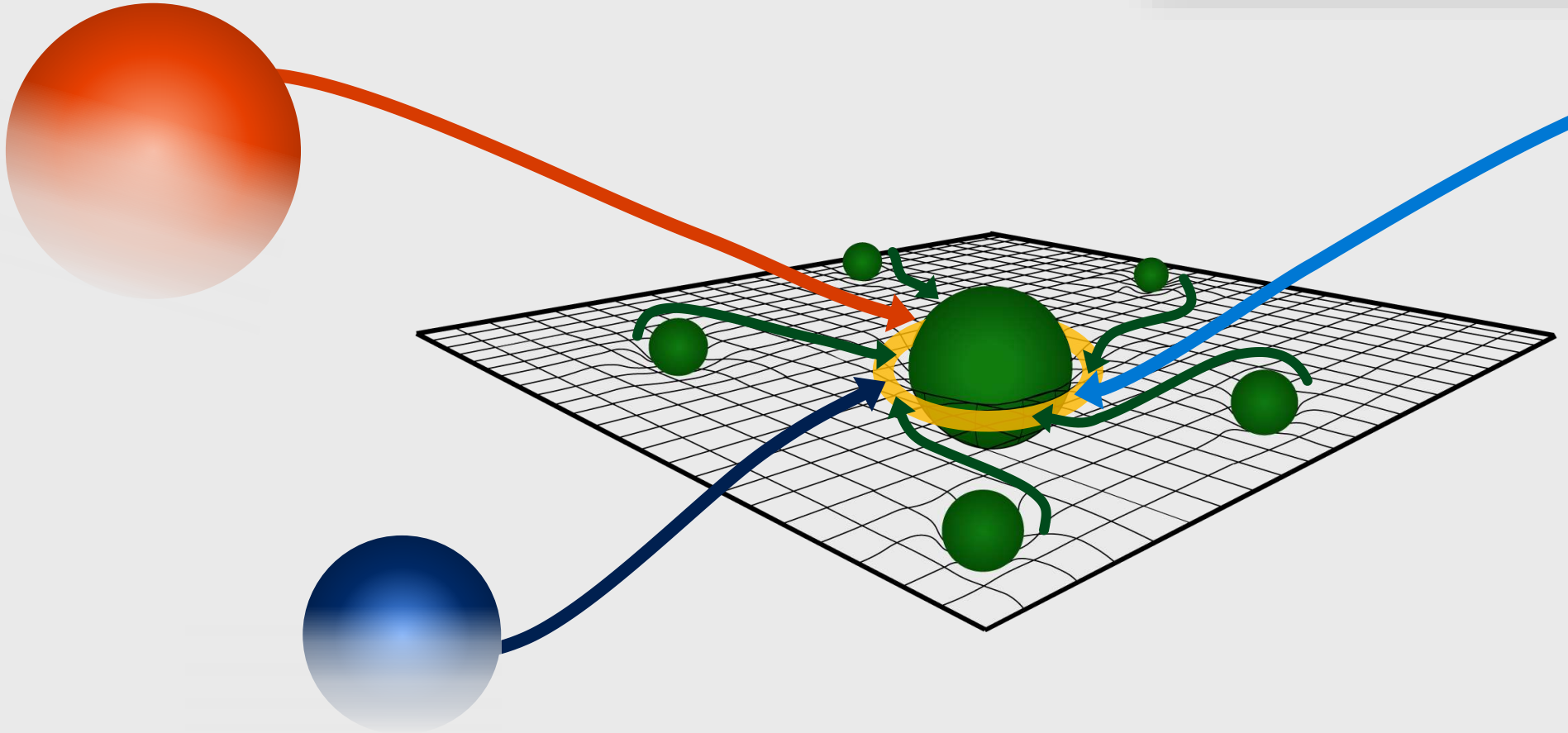
Microsoft Graph Security API allows analysts to get insights across local security datasets

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

Malware-Less Attacks

'File-less' Malware

Tailored/Targeted Malware

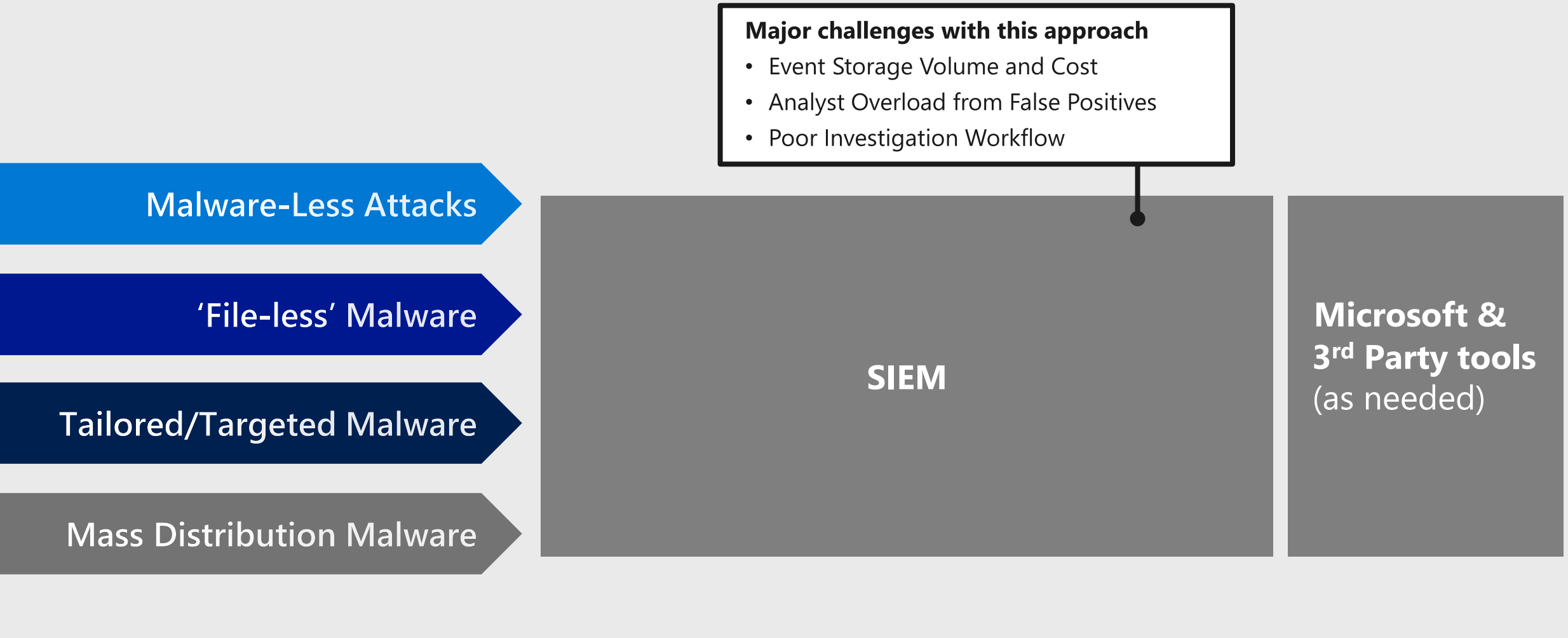
Mass Distribution Malware

THREAT AGES

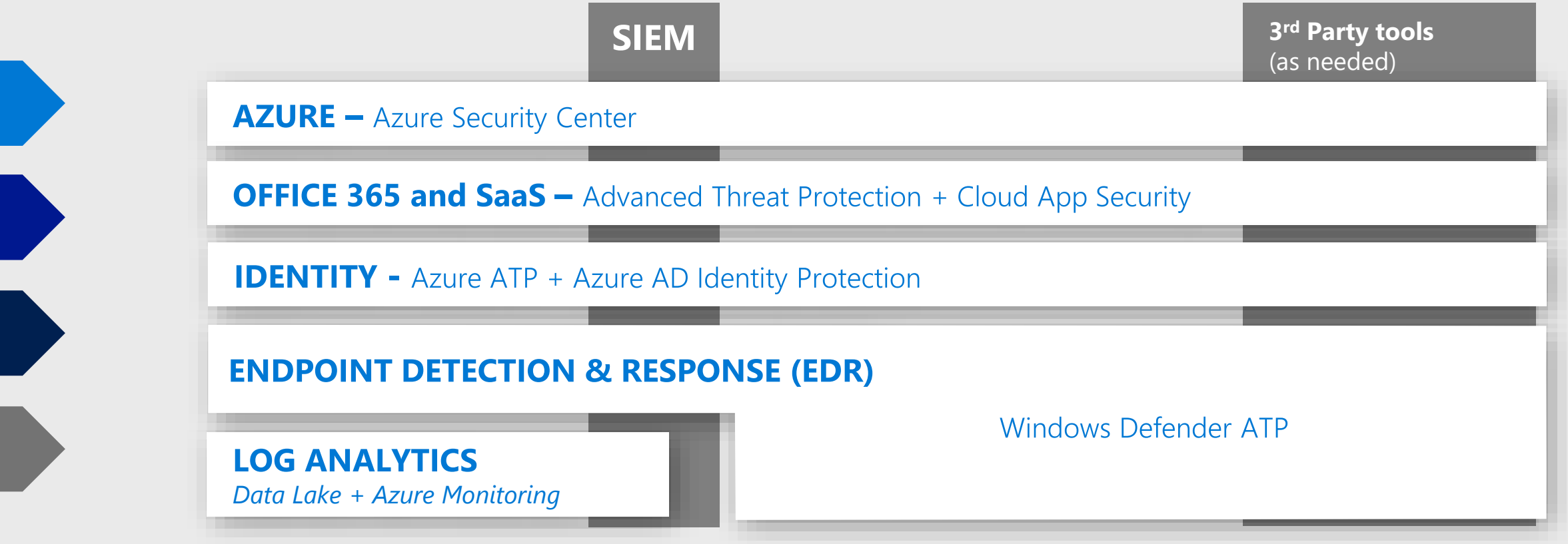
Malware and Infrastructure

Identity and Apps

Corporate IT SOC – Started with Classic SIEM model



Corporate IT SOC – Evolved to adopt specialized tooling



SOC Reference Operational Model

THREAT INTELLIGENCE

Provide External Context to inform decisions

Investigations | Hunting | Leadership | Technical Detections and Defenses

SUCCESS METRIC: Mean Time to Remediation (MTTR)

INCIDENT / BREACH MANAGEMENT

Coordinate Data Breaches and Major Incidents with:

Leadership | Legal | Communications | Risk Management | Others

SOC ANALYST

Tier 3
Tier 2
Tier 1

Lead technical incident through lifecycle (across cloud and on-premises)
Escalate Incident to higher tier as needed

Lower Tiers may be automated and/or outsourced to MSSP

DETECT 〉 RESPOND 〉 RECOVER

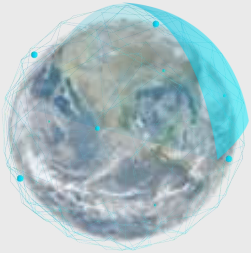
Threat protection

THREAT PROTECTION LIFECYCLE

Goal: *Increase attacker cost as rapidly and efficiently as possible*

STRATEGIC IMPERATIVES

1. **Prevent as many threats as possible**
   (Best Security ROI when available)
2. **Rapidly Detect and Respond**
   (highest coverage of assets/scenarios)
3. **Continually apply learnings**
   (continuous attack cost increase)



Committed to your success

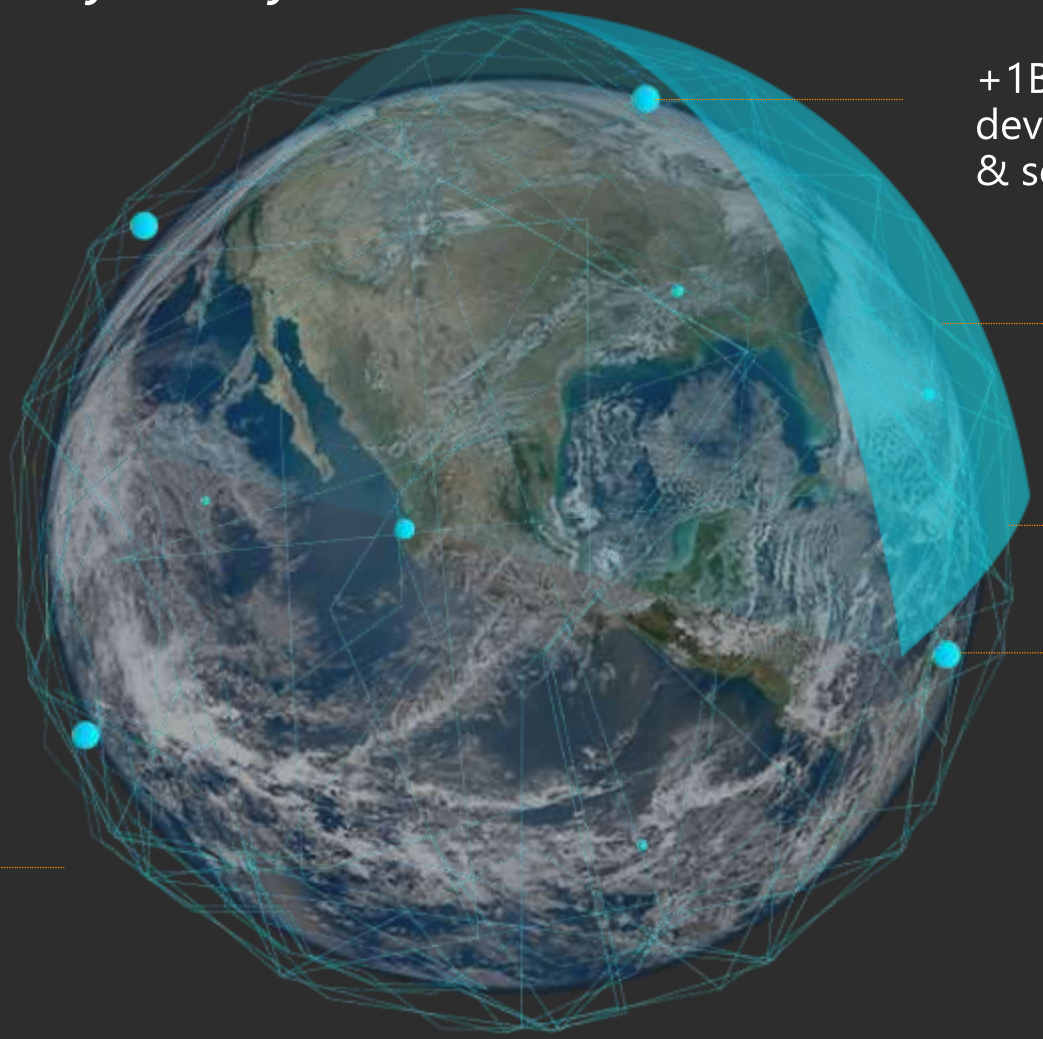
Accelerate your ability to manage threats by providing secure platforms and products, security capabilities, services, and recommendations

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



+1B Windows devices updated & scanned

630 billion monthly authentications

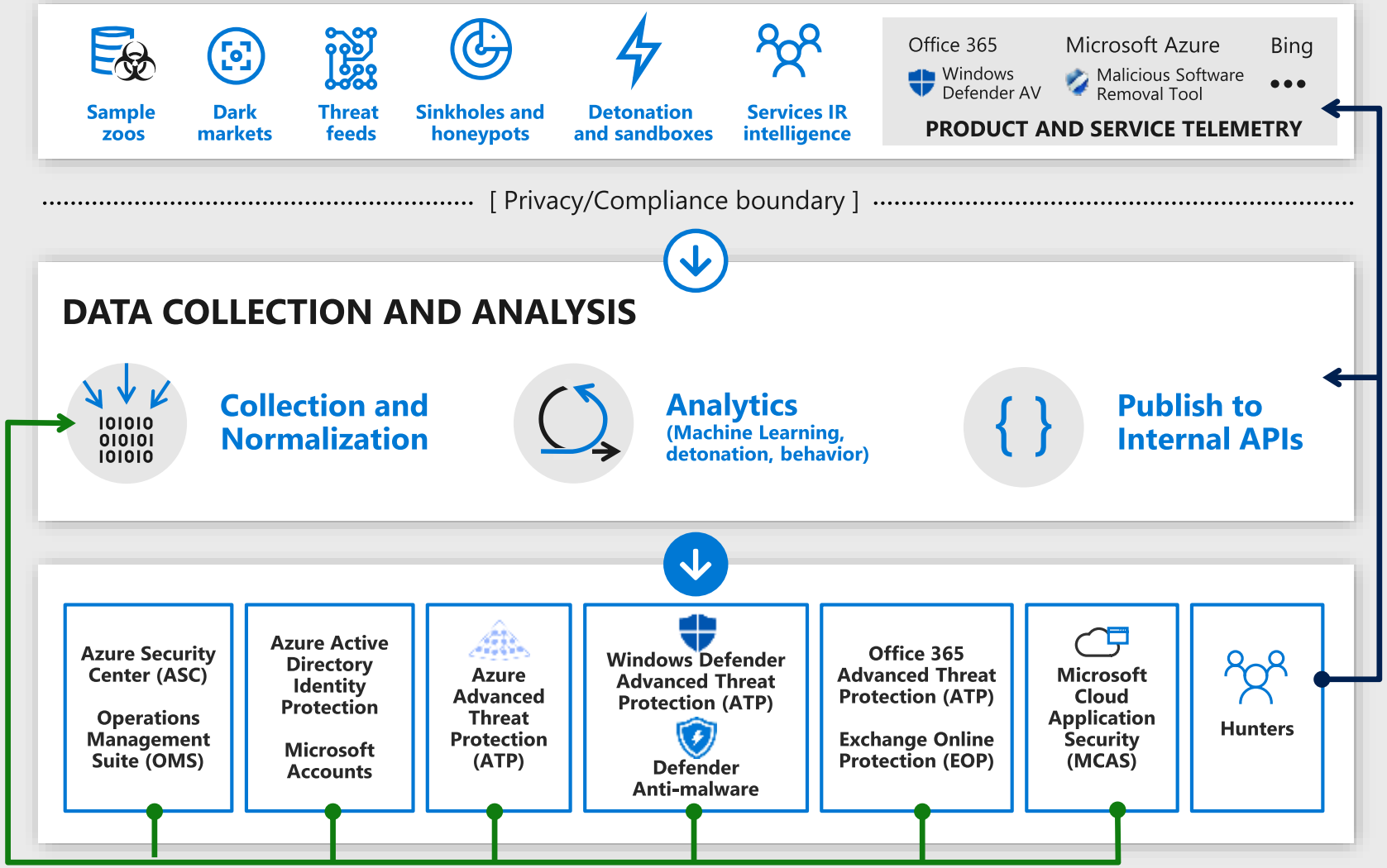
18+ billion web pages scanned

470 billion e-mails analyzed

5 billion threats detected on devices every month

Unparalleled cybersecurity visibility and insight

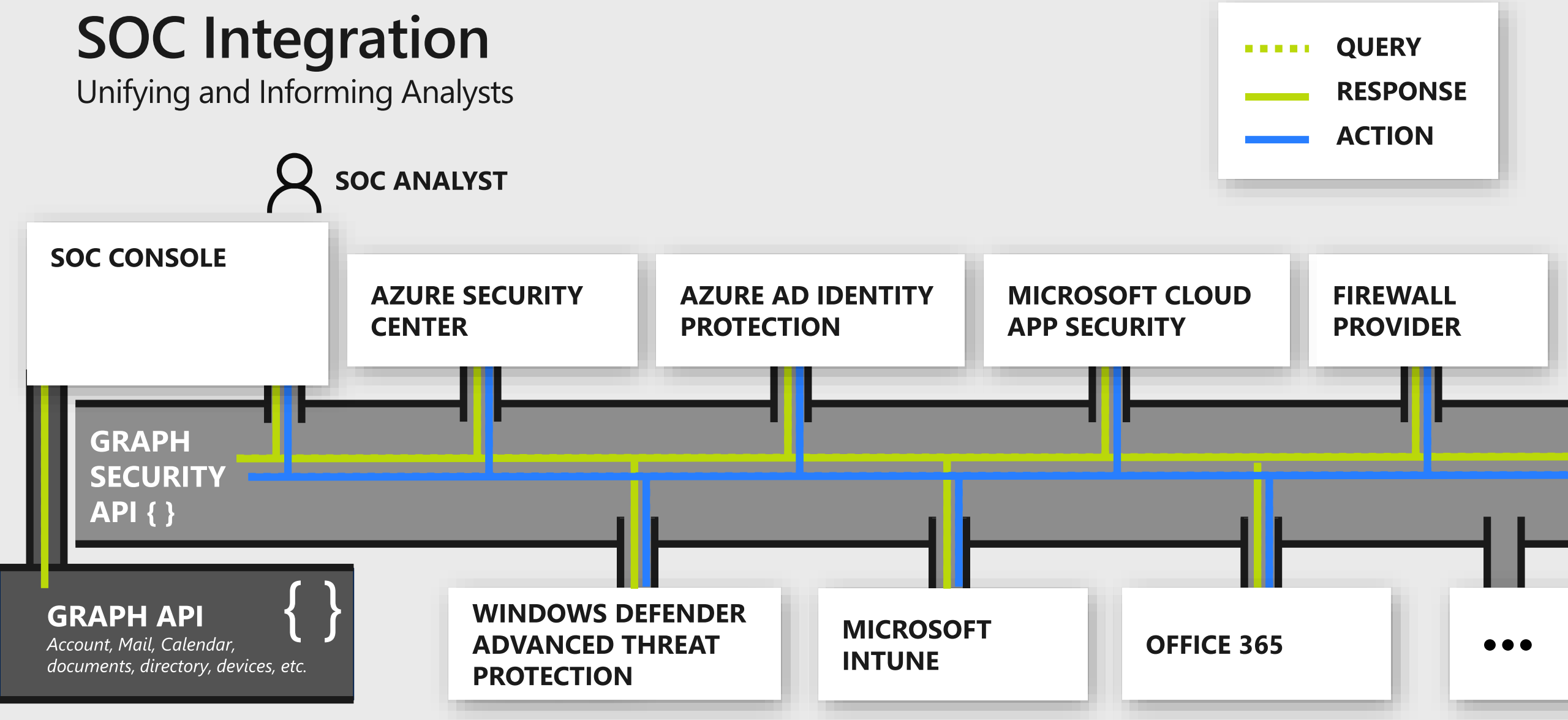
Inside The Intelligent Security Graph



- Products instrumented to strict privacy/compliance standards
  See [Microsoft Trust Center]
- Analytics help fuel new discoveries
- Products send data to graph
- Products use Interflow APIs to access results
- Products generate data which feeds back into the graph
- Hunters identify attacks, improve analytics, feed back into product design

SOC Integration

Unifying and Informing Analysts

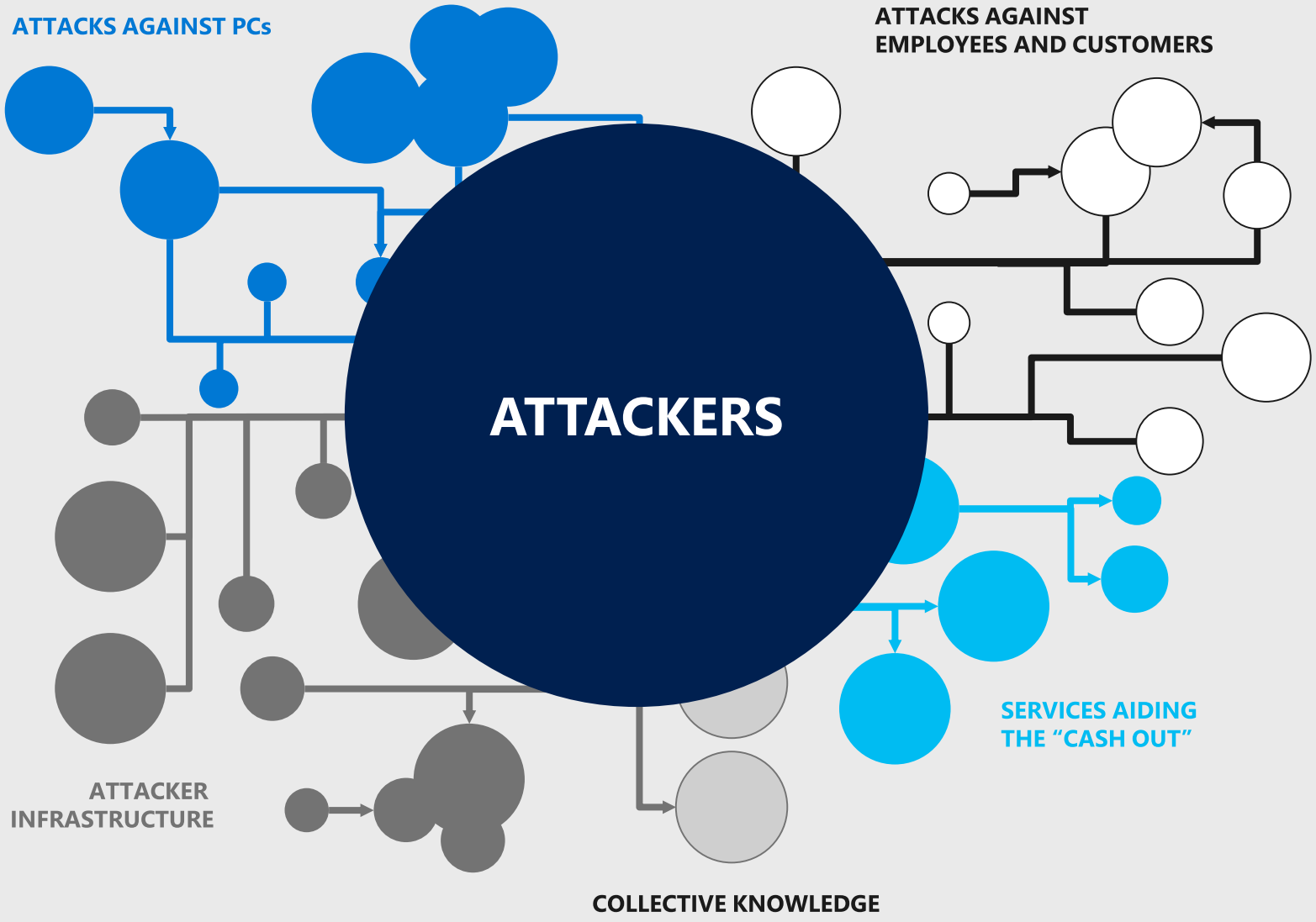


http://aka.ms/graphsecurityapi | https://aka.ms/graphsecuritydocs

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

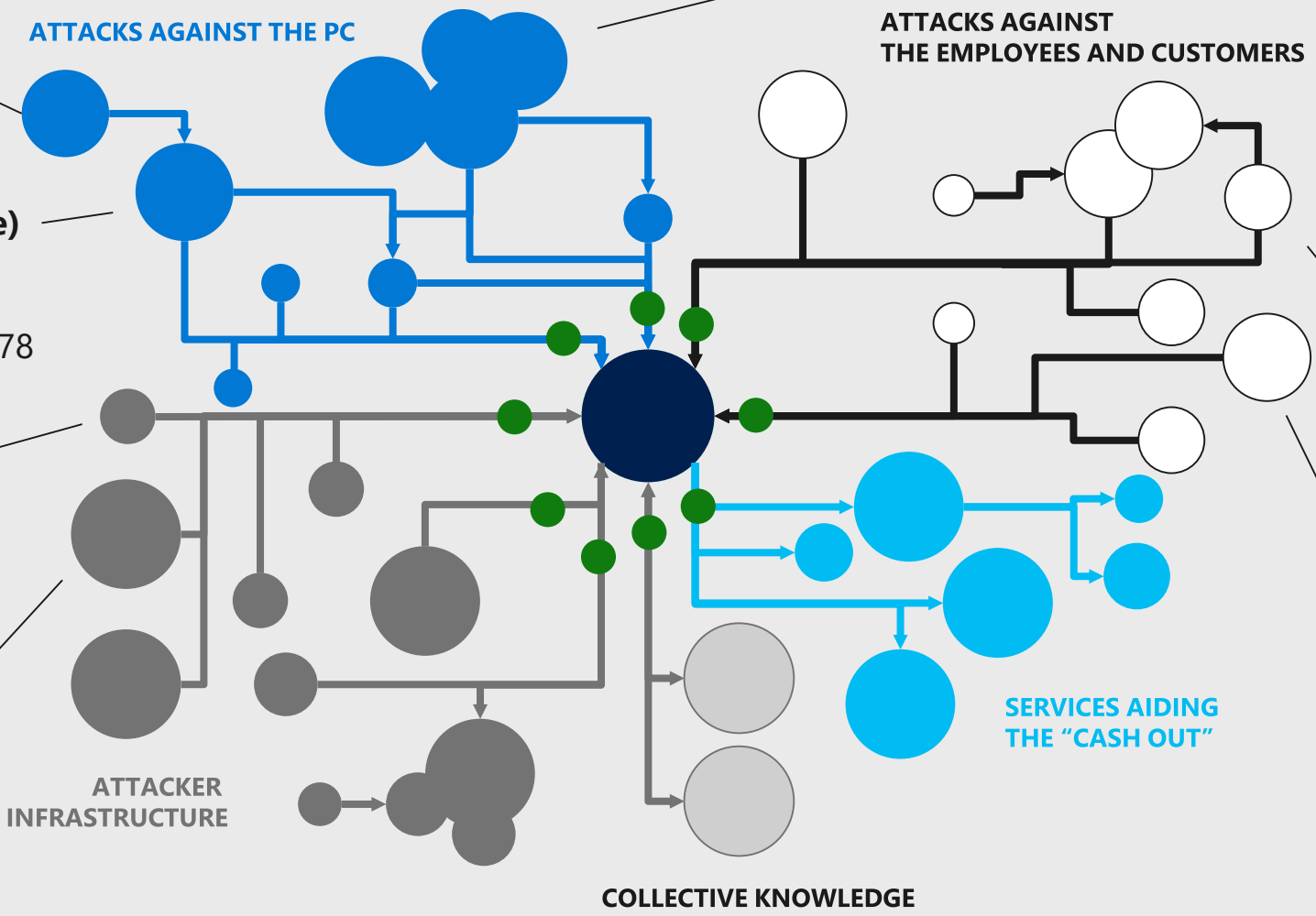
Ransomware:
$66 upfront
Or
30% of the profit (affiliate model)

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

Denial of Service (DOS) average prices
day: $102.05
week: $327.00
month: $766.67

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



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.

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

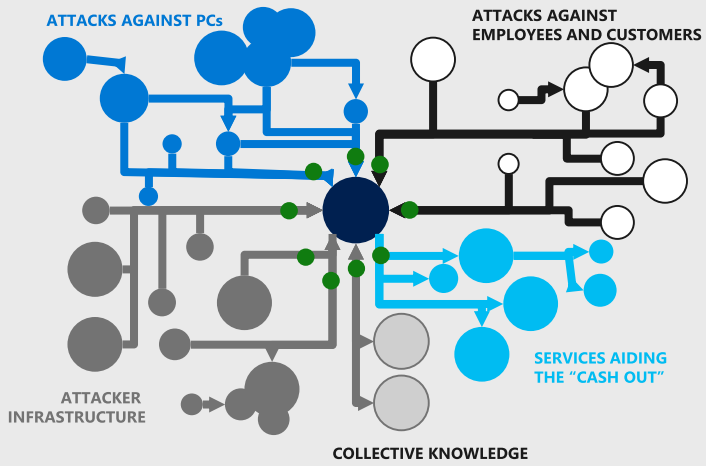
Compromised accounts
As low as $150 for 400M.
Averages $0.97 per 1k.

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

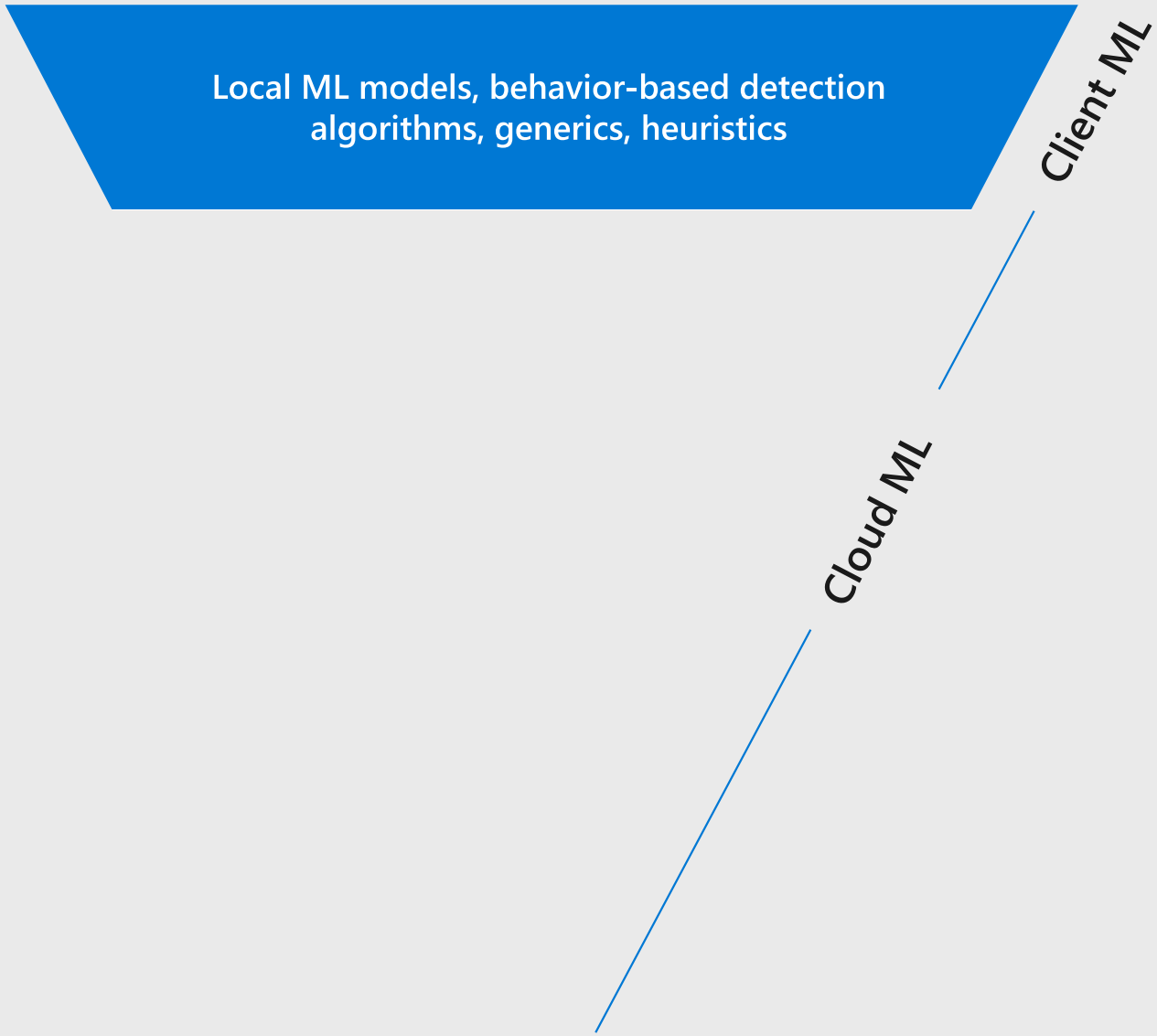
- Company Proxy
- Cellphone networks
- Vacations/Travel

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

0.001%

Work by Mace et. al, Microsoft

Machine Learning in Windows Defender AV



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

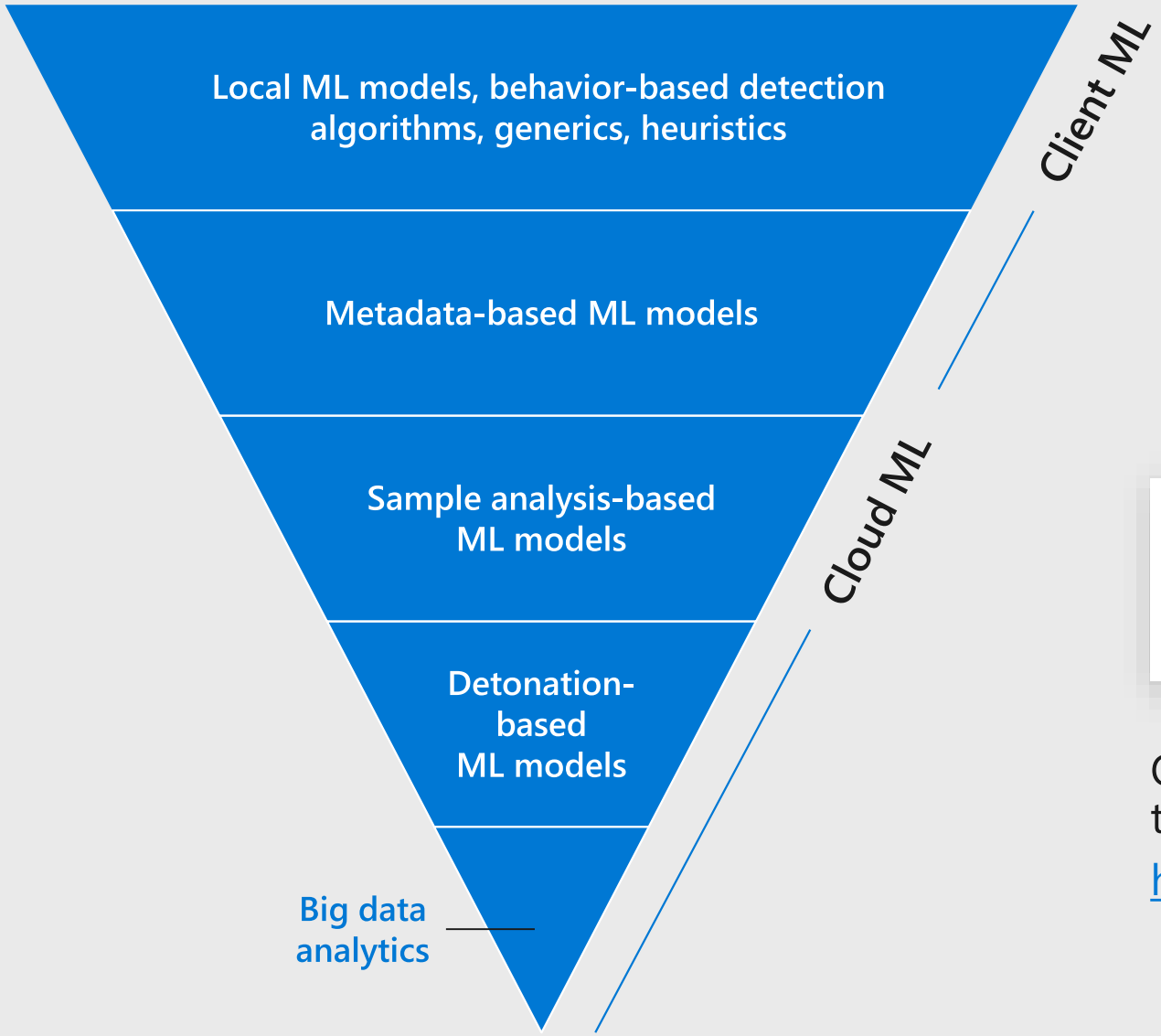
Protection in minutes

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

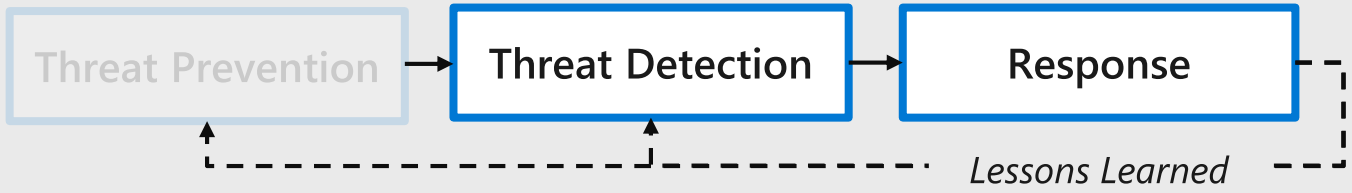
Protection in seconds

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

On March 6, Windows Defender Antivirus blocked more than 400,000 instances of several sophisticated trojans

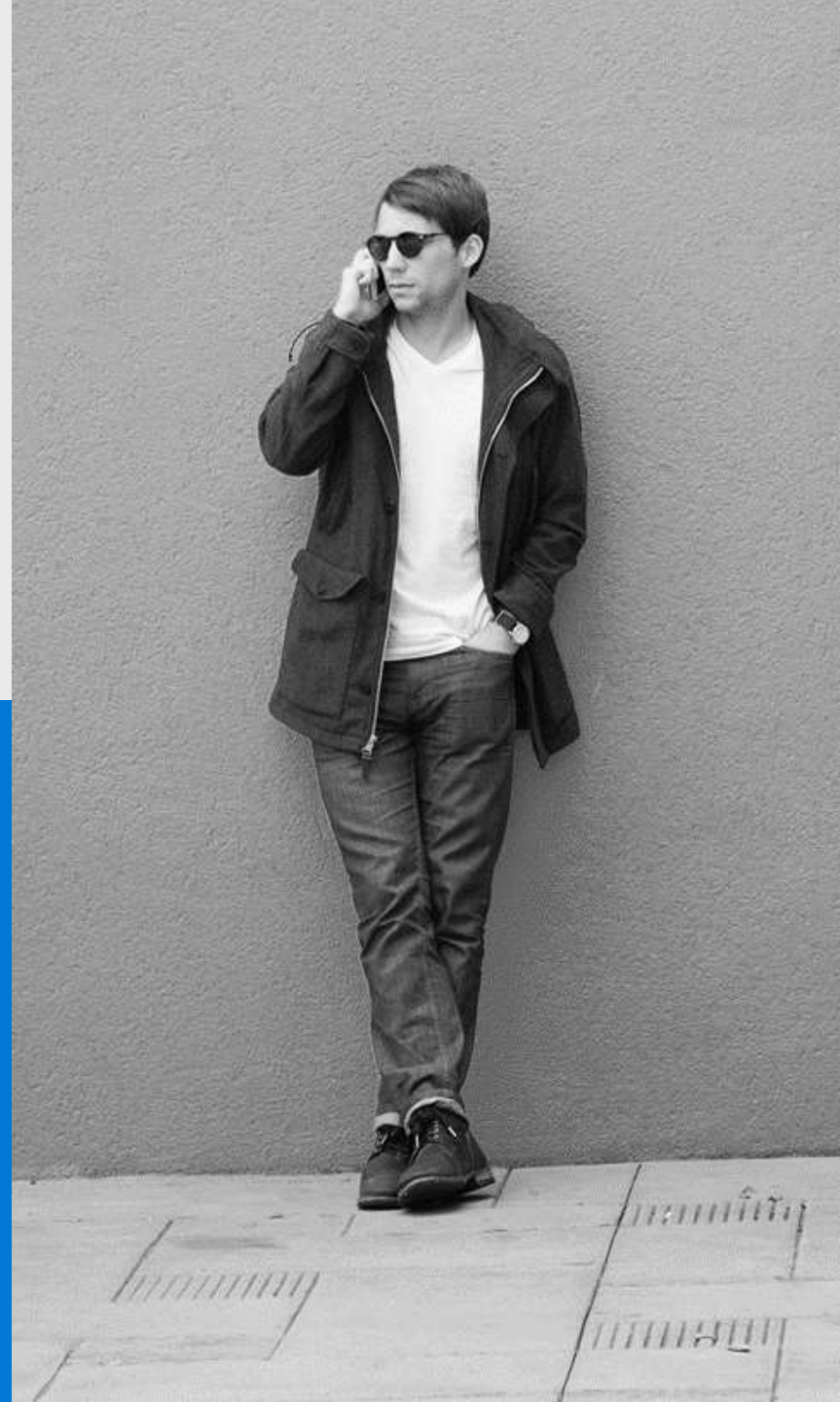
http://aka.ms/dofoil

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)

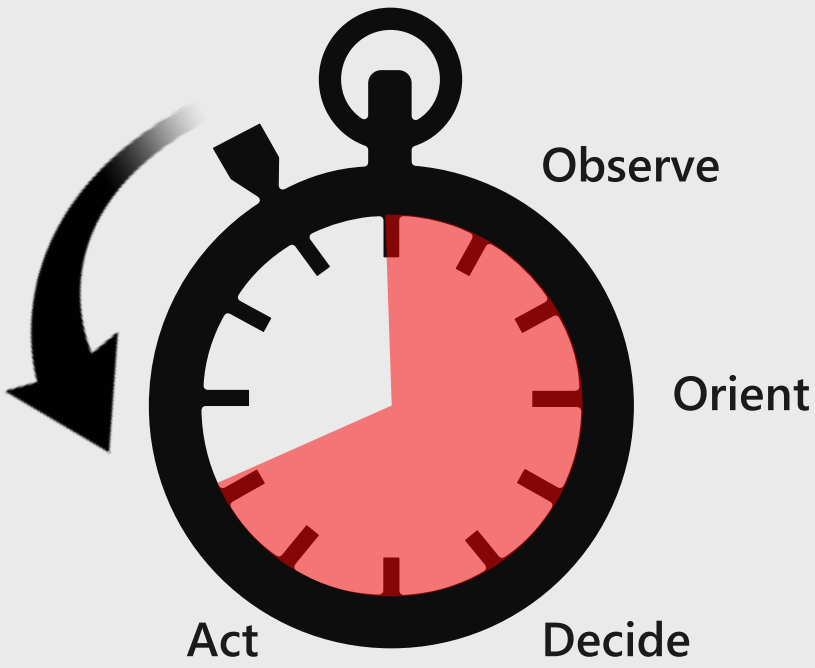
Automate detection and response tasks

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

Cloud App Security

DATA ON SAAS

Office 365 ATP
- Email gateway
- Anti-malware

Office 365
Threat Intelligence

Windows Defender ATP

Windows Defender AV

IDENTITY

Azure AD
- Identity Protection

Powered by the Intelligent Security Graph

CLOUD INFRASTRUCTURE

Azure SQL
- Threat Detection

Azure Security Center
- **Threat Protection**
- Threat Detection

Security Appliances

Azure Advanced Threat Protection

PRIVATE CLOUD AND ON-PREMISES INFRASTRUCTURE

Windows Defender ATP

INTELLIGENCE AND ANALYSIS

Cybersecurity Operations Service (COS)

Incident Response and Recovery Services

Hunt for threats and persistent adversaries in your environment

Respond to Threats with seasoned professionals and deep expertise

Professional Services

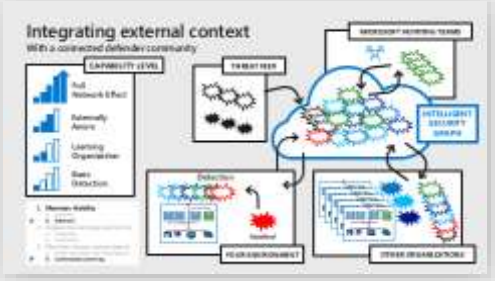
Microsoft threat protection

SIEM Integration

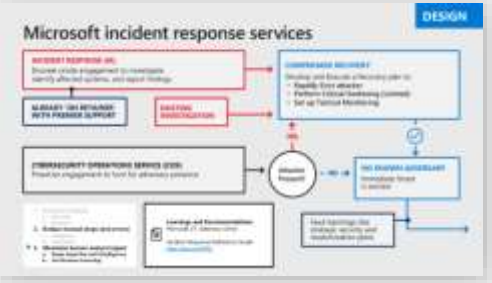
Product and Cross Platform Integration

Office 365 Threat Intelligence

Machine Learning and UEBA



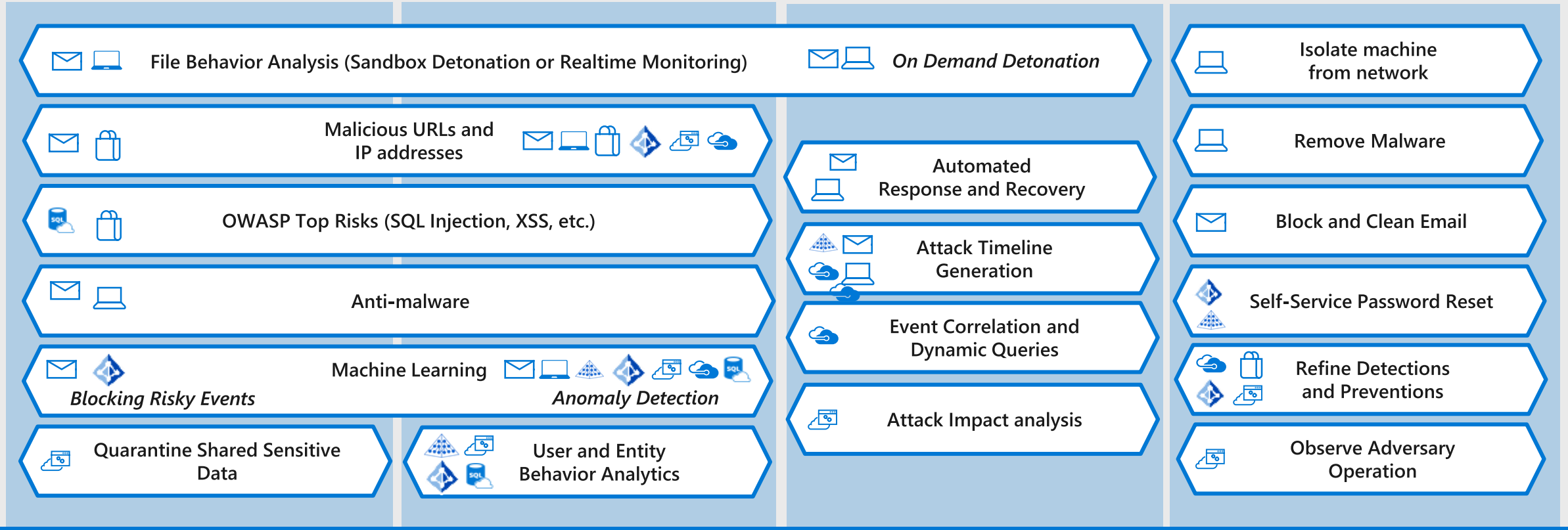
Community Effect



Incident Response and Hunting

Summary and Close →

Automate and enable threat protection



- Azure AD Identity Protection
- Azure ATP / Identity Manager
- Office 365 ATP
- Windows Defender ATP / Defender AV
- Microsoft Cloud App Security
- Azure Security Center
- Azure Web App Firewall / SQL Threat Detection
- Azure Marketplace Partner Capability

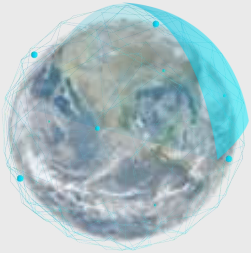
Threat protection

THREAT PROTECTION LIFECYCLE

Goal: *Increase attacker cost as rapidly and efficiently as possible*

STRATEGIC IMPERATIVES

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

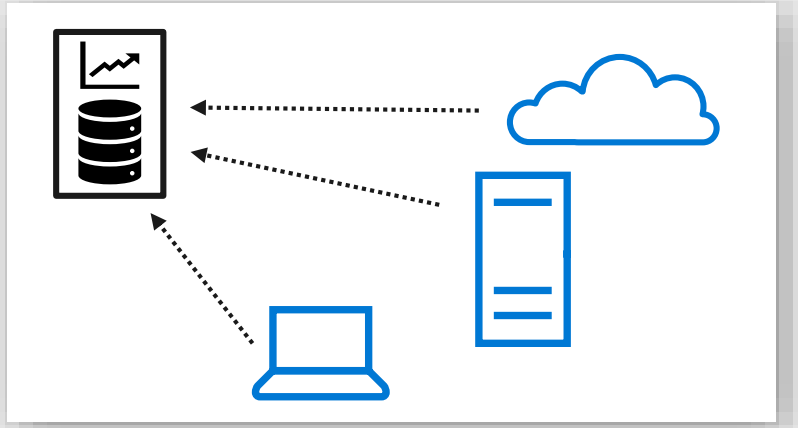
Microsoft

Questions?

References

Integrating with your SIEM

Two different approaches to connect to your existing SIEM tool and processes



1. Graph Security API

SIEM Integration - https://docs.microsoft.com/en-us/graph/security-siemintegration

Solutions already Integrated - https://docs.microsoft.com/en-us/graph/api/resources/security-api-overview?view=graph-rest-1.0

2. Individual Capabilities

- **Windows Defender ATP**

  https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/enable-siem-integration-windows-defender-advanced-threat-protection

- **Azure Advanced Threat Protection**

  https://docs.microsoft.com/en-us/azure-advanced-threat-protection/cef-format-sa

- **Office 365**

  https://docs.microsoft.com/en-us/office365/securitycompliance/siem-server-integration

  https://docs.microsoft.com/en-us/office365/securitycompliance/siem-integration-with-office-365-ti

- **Cloud App Security**

  https://docs.microsoft.com/en-us/cloud-app-security/siem

- **Azure SIEM Integration (includes Azure AD)**

  https://docs.microsoft.com/en-us/azure/azure-monitor/overview

Additional Resources – Threat Protection

Incident Response Reference Guide (IRRG) - https://Aka.ms/IRRG

Updates to Windows Hello for Business – Video

Updates to Windows 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 Windows 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 looks 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 Windows 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.

Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies

Security Operations Center (SOC)

- Vulnerability Management
- MSSP
- SIEM + Analytics
- Cybersecurity Operations Service (COS)
- Incident Response and Recovery Services
- Azure Security Center
- Windows Defender
- Office 365 Security & Compliance
- Azure
- Cloud App Security
- Advanced Threat Protection (ATP)
- Graph Security API *(Public Preview)*
- Alert & Log Integration

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
- Conditional Access – Identity Perimeter Management
- 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
- Azure ATP
- Active Directory
- ESAE Admin Forest

Information Protection

- Cloud App Security
- Azure Information Protection (AIP)
  - Discover
  - Classify
  - Protect
  - Monitor
  - *Hold Your Own Key (HYOK)*
  - AIP Scanner
- Classification Labels
- Office 365
  - Data Loss Protection
  - Data Governance
  - eDiscovery
- Azure SQL Threat Detection
- SQL Encryption & Data Masking
- Azure SQL Info Protection *(Preview)*
- Endpoint DLP

Clients

- Unmanaged & Mobile Devices
- Intune MDM/MAM
- Managed Clients
- System Center Configuration Manager
- Windows Defender ATP
  - Secure Score
  - Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

Extranet

- NGFW
- Edge DLP
- SSL Proxy
- IPS

Security Appliances

Express Route

Intranet Servers

- Windows Server 2016 Security
  Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...
- Shielded VMs
- Azure Stack
- VMs

Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Application & Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation+Monitor

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

IoT and Operational Technology

- Windows 10 IoT
- Azure IoT Security
- Azure Sphere
- IoT Security Maturity Model
- IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

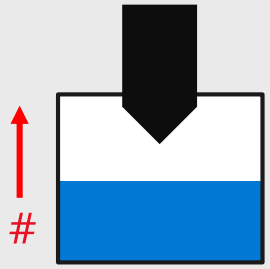
Security Development Lifecycle (SDL)

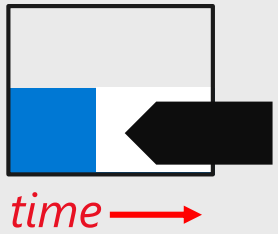
Trust Center | Intelligent Security Graph

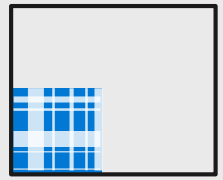
Microsoft

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

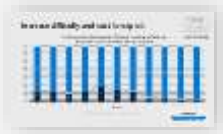
→ Bug Bounty
→ Rigorous Testing
→ Response Center
→ Automatic Updates

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

+

INCREASE DIFFICULTY AND COST TO EXPLOIT

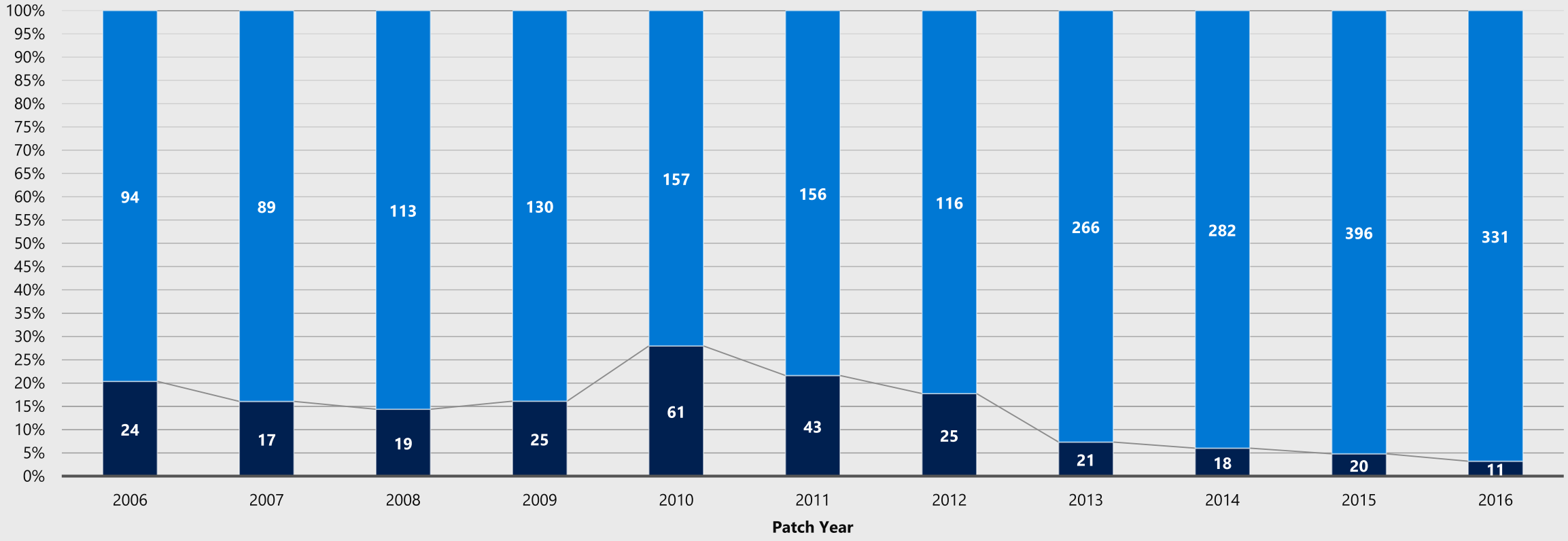
Platform Mitigations
- Eliminate classes of vulnerabilities
- Break exploit techniques
- Contain damage
- Prevent persistence
- Limit exploit opportunity window



Increase difficulty and cost to exploit

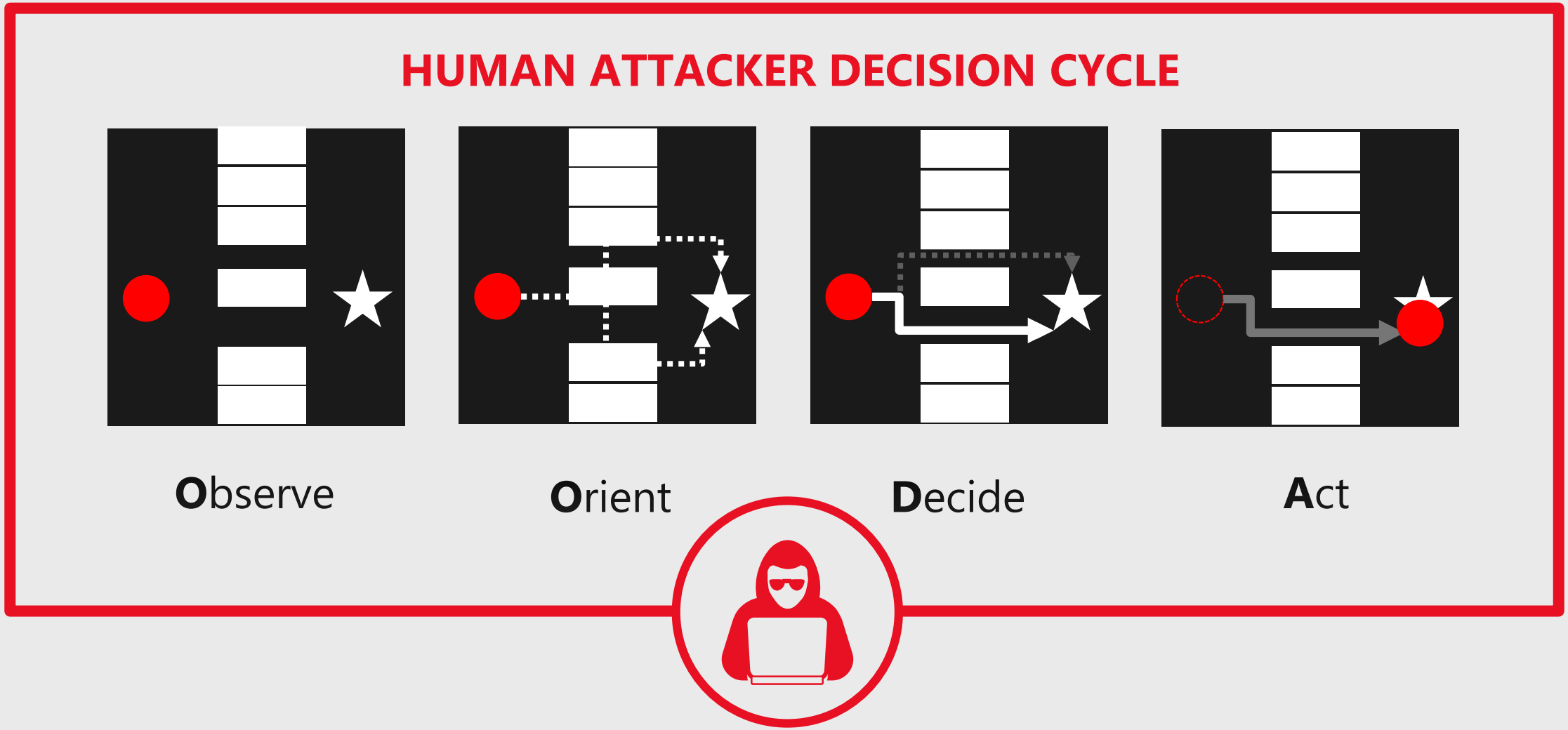
← BACK TO TIMELINE

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



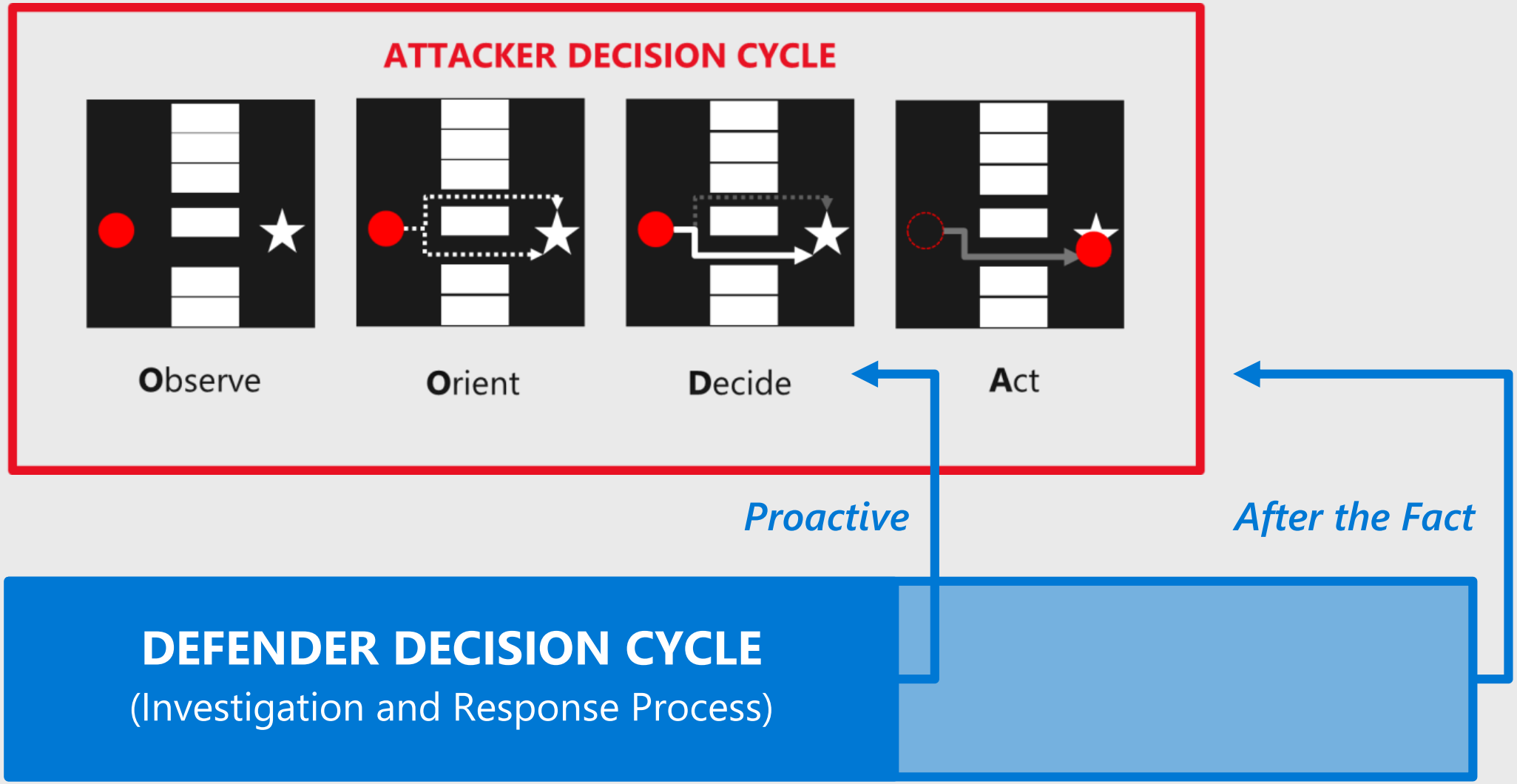
FROM BLOG:
[Mitigating arbitrary native code execution in Microsoft Edge]

Rapidly detect and respond



Get inside their OODA loop

Better and Faster Investigation and Response Decisions



Faster remediation

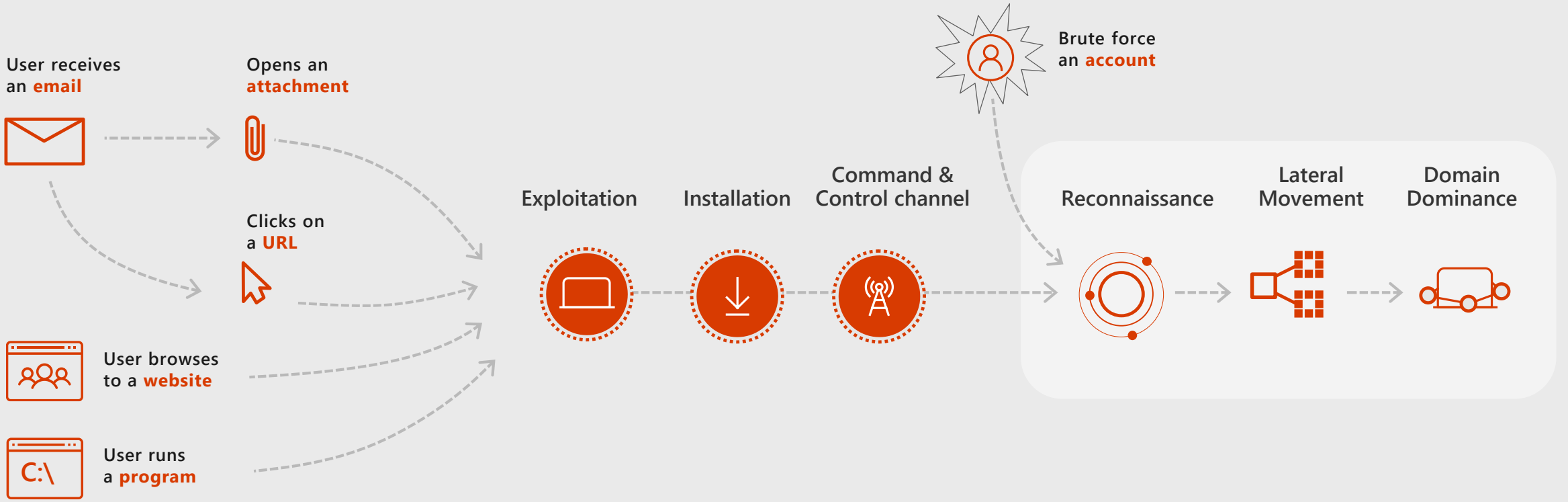
Threat detection

integrated across Microsoft 365

Email protection
Office 365 ATP

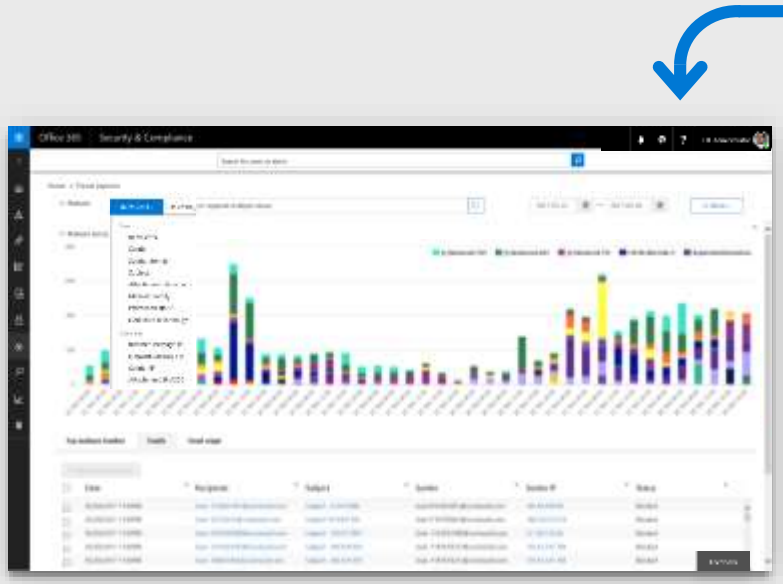
Endpoint protection
Windows Defender ATP

Identity protection
Azure ATP

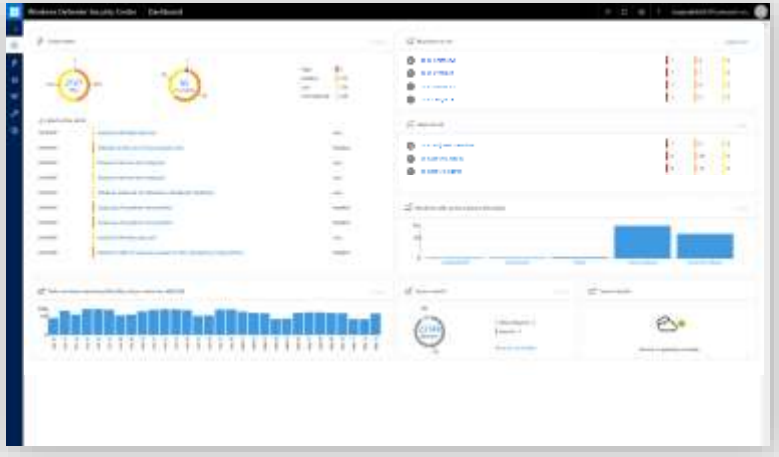


Investigate and respond to threats across our consoles

- No blind spots anymore – Visibility across email, endpoint, and identity
- Incorporate data from Office 365 ATP into the Windows Defender Security Center to conduct a holistic security investigation across Office 365 mailboxes and Windows Defender ATP endpoints.
- Investigate across the stack, without losing context



Office 365 Threat Explorer



Windows Defender Security Center

Azure Advanced Threat Protection (ATP)

Integration to reduce investigation time and missed signals

Zero Hour Auto Purge (ZAP)
Cleans mailboxes as new detections are released

Office 365

Azure Security Center monitors threats across a hybrid infrastructure:
- **Azure + On-premises / other clouds**
- **Windows + Linux**

Office 365 ATP
- Email gateway
- Anti-malware

ROADMAP

Azure Security Center
- **Threat Protection**
- Threat Detection

Azure SQL
- Threat Detection

Windows Defender ATP

Powered by the Intelligent Security Graph

Security Appliances

Investigators can pivot easily across emails, hosts, and identities

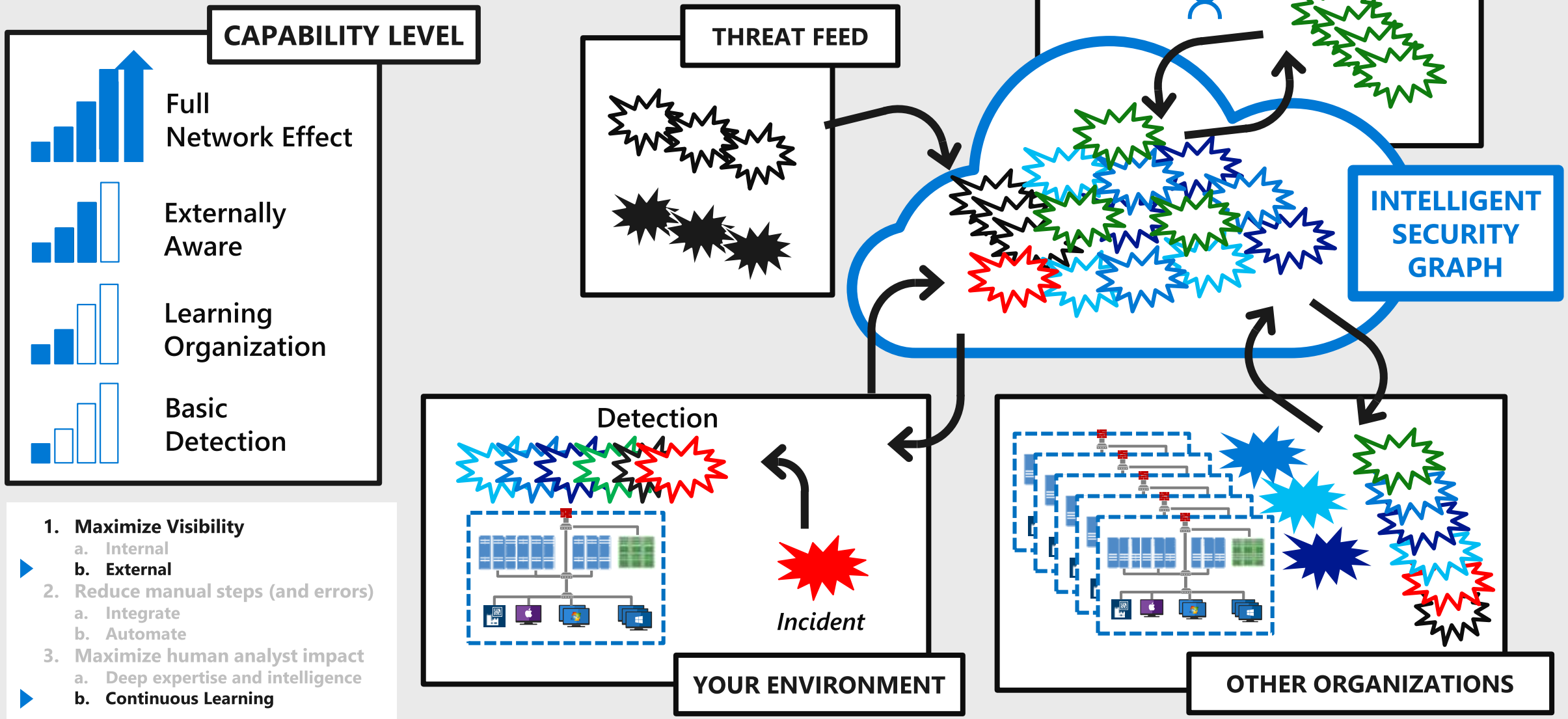
Azure Advanced Threat Protection

Click for Screenshots

Log Integration
Product Integration

Integrating external context

With a connected defender community



1. **Maximize Visibility**
   a. Internal
   b. **External**
2. Reduce manual steps (and errors)
   a. Integrate
   b. Automate
3. Maximize human analyst impact
   a. Deep expertise and intelligence
   b. **Continuous Learning**

DESIGN

Microsoft incident response services

INCIDENT RESPONSE (IR)
Discreet onsite engagement to investigate, identify affected systems, and report findings

ALREADY 'ON RETAINER' WITH PREMIER SUPPORT

EXISTING INVESTIGATION

CYBERSECURITY OPERATIONS SERVICE (COS)
Proactive engagement to hunt for adversary presence

COMPROMISE RECOVERY
Develop and Execute a Recovery plan to:
- Rapidly Evict attacker
- Perform Critical Hardening (Limited)
- Set up Tactical Monitoring

YES

Attacker Present?

NO

NO KNOWN ADVERSARY
Immediate threat is evicted

Feed learnings into strategic security and modernization plans

1. Maximize Visibility
   a. Internal
   b. External
2. **Reduce manual steps (and errors)**
   a. Integrate
   b. Automate
3. **Maximize human analyst impact**
   a. **Deep expertise and intelligence**
   b. **Continuous Learning**

Learnings and Recommendations
Microsoft, EY, Edelman, Orrick

Incident Response Reference Guide
http://aka.ms/IRRG

Common attack steps and mitigations