Maximising your Microsoft Security E3/E5 investments

May 24, 2023

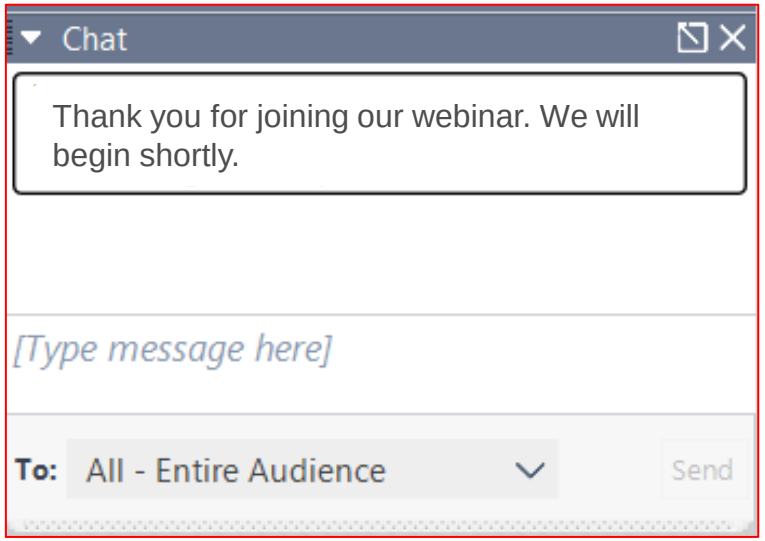
KROLL

Housekeeping

- Session is being recorded, You'll receive access to the recording in a couple days

- Ask questions via chat >

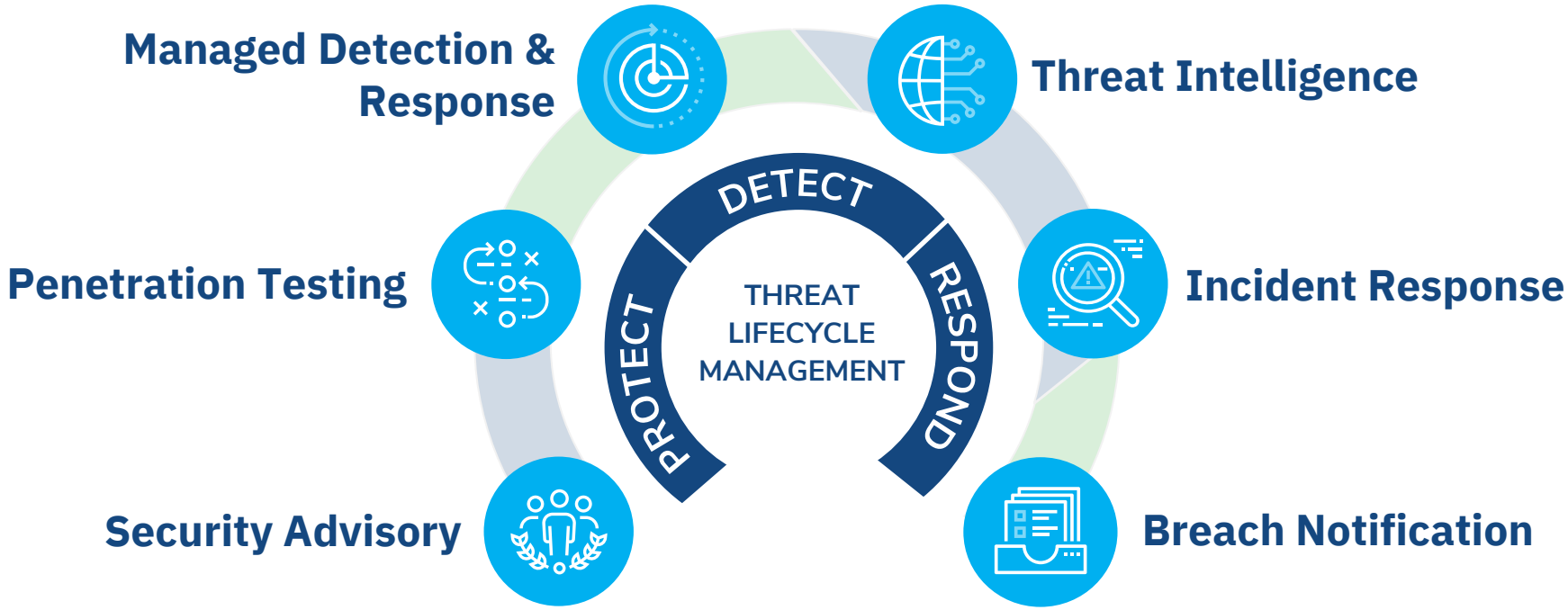
- We'll try to answer as many questions as possible



Kroll - Cyber Risk

Microsoft Solutions Partner
Security

Member of
Microsoft Intelligent
Security Association
Microsoft



60+	+90%	3,000+	650+	100+
CYBER INSURANCE CARRIER PANELS	CUSTOMER RETENTION RATE	IR ENGAGEMENTS PER YEAR	EXPERTS ACROSS 19 COUNTRIES	INDUSTRY CERTIFICATIONS

Table of Contents

Speaker Profiles

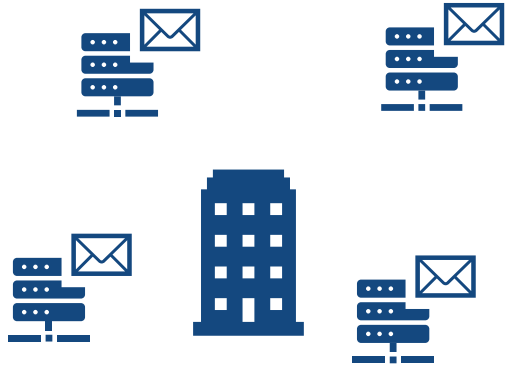
Scott Hanson
Associate Managing Director & Head of Global Security Operations
Cyber Risk

Rafael De Lima
Vice President and Solutions Architect
Cyber Risk

Thomas Hind
Vice President and Platform Architect
Cyber Risk

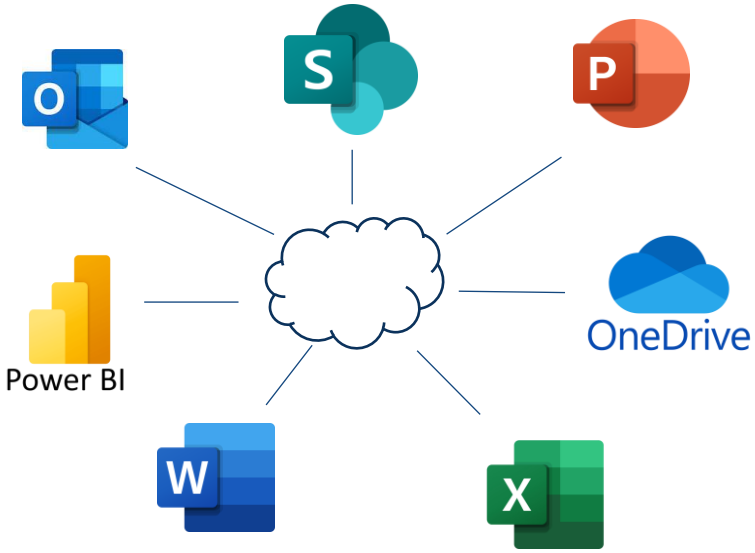
KROLL

Reasons for moving to cloud-native security



- Limited scalability
- Infrastructure costs
- Storage and compute needs increase during an incident

- You are still responsible for securing the data
- Misconfigurations are the leading cause of cloud breaches



- Easy integrations with other cloud services
- Scalable analysis of data
- Elastic storage

Microsoft Security licensing can be overwhelming!

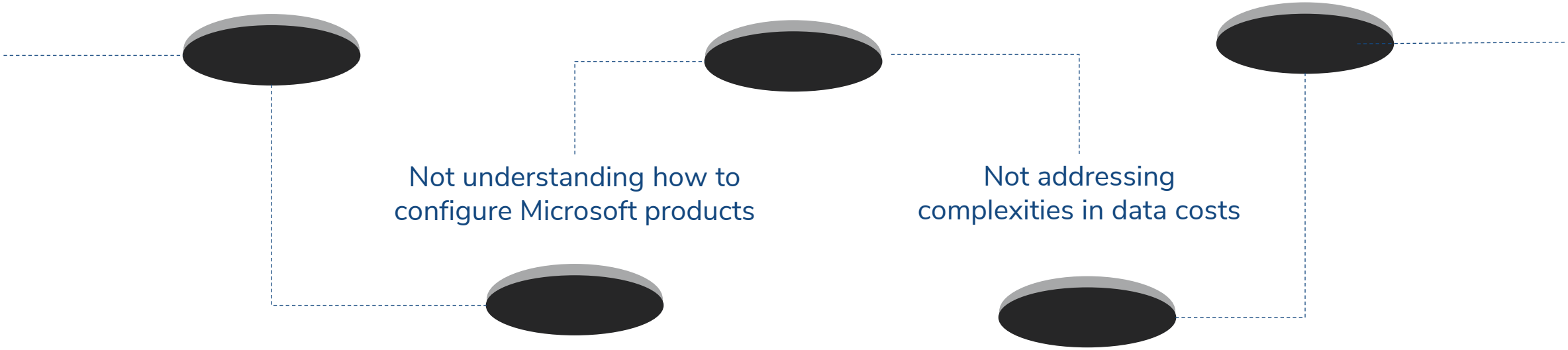
Microsoft 365 E3	Enterprise Mobility + Security E5 (step-up)	Microsoft 365 E5	Microsoft Azure
✓ Azure AD Premium P1	✓ Azure AD Premium P2	✓ Defender for Endpoint P2	✓ Microsoft Sentinel
✓ Microsoft Information Protection	✓ Defender for Cloud Apps	✓ Defender for Cloud Apps	✓ Microsoft Defender for Cloud
✓ Defender for Endpoint Plan 1	✓ Defender for Identity	✓ Defender for Office Plan 2	✓ Microsoft Defender for IoT
		✓ Defender for Identity	
		✓ Microsoft Purview	
		✓ And much more!	

Common pitfalls when adopting the Microsoft Security suite

Being unsure of which controls to implement first?

Not leveraging native integrations and automations

Not leveraging cloud security posture management



Not understanding how to configure Microsoft products

Not addressing complexities in data costs

Read our eBook for more information on how to avoid these pitfalls

#1 You only get as much as you put in

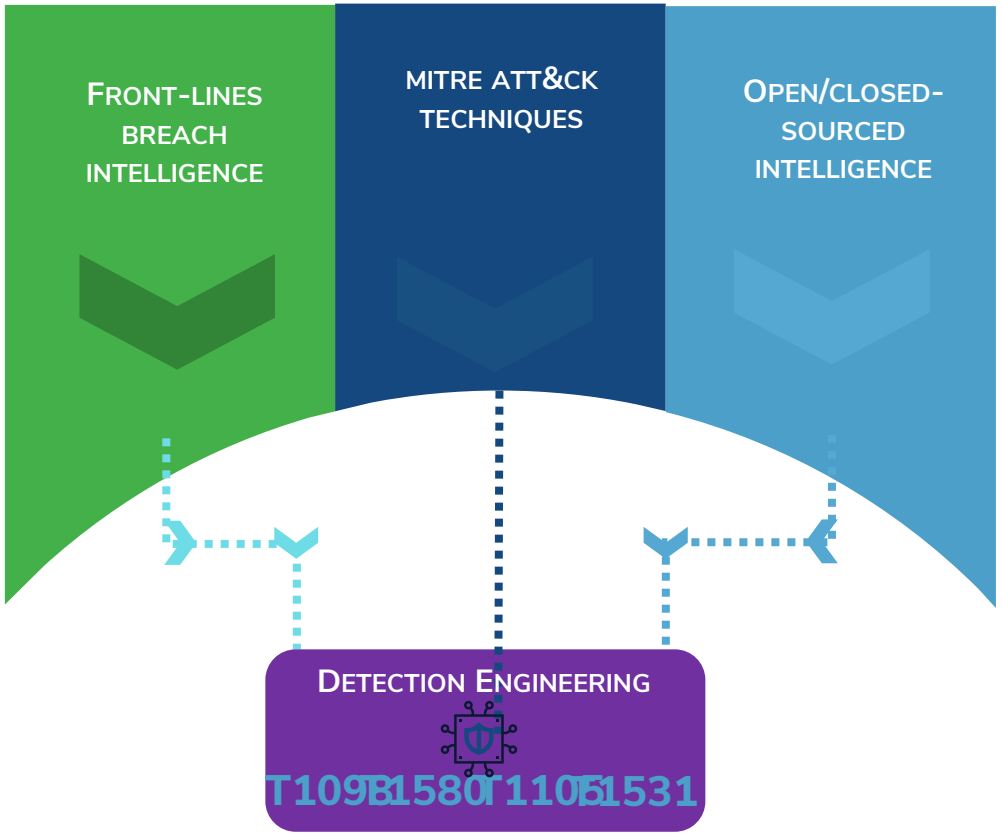
Key sources of intel to drive accurate detection

Intelligence-Driven Detections:

- Front-lines breach intelligence
- Coverage of Cloud-related MITRE ATT&CK techniques (O365, Azure AD, etc.)
- Open-source and closed-source intelligence

Enables:

- Early detection of emerging threats
- Rapid triage, with enhanced insight and attribution
- High-fidelity, low-noise alerting



KROLL

MITRE ATT&CK Coverage

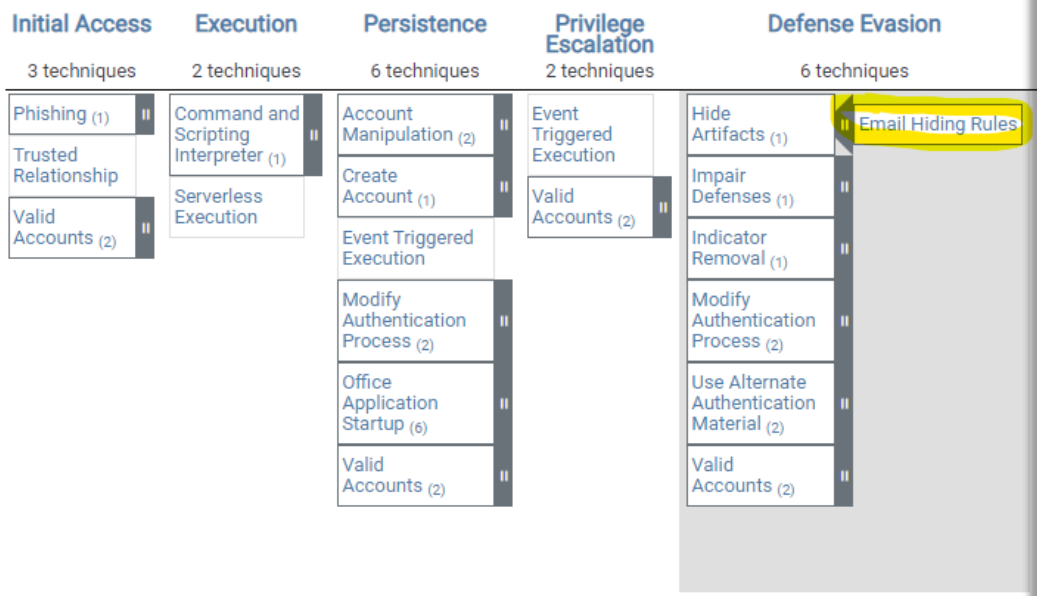
Office 365 Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the Office 365 platform.

View on the ATT&CK® Navigator

Version Permalink

layout: side | show sub-techniques | hide sub-techniques | help



Rule Title	T1564.008 - O365 - Suspiciously Named Inbox Rule
Description	Suspiciously Named Inbox Rule
Detection objective	Inbox rules named with a single special character rule names are highly unusual and have been seen in many true positives for Business Email Compromise (BEC). Filtering emails to Deleted Items or Junk is a technique is used by threat actors to prevent a compromised user from ever receiving warnings from IT that they've been compromised.
Detection Category	Adversary Detection
Data Source	Office 365
Mitre tactic(s) covered	TA0005 - Defense Evasion
Mitre technique(s) covered	T1564 - Hide Artifacts
Mitre sub-technique(s) covered	T1564.008 - Email Hiding Rules
Associated Detection Technology	Microsoft Sentinel

Configuration Inputs

Data Retention	• Compliance requirements • Threat hunting
• Anti-malware/Anti-phishing • Alert suppression • Indicators	Threat Policies and Rules
Permissions and Roles	• Admin roles • Active Directory groups • Tier-based/role-based access
• Notifications • Response actions • Live Response/AIR	Automations

#2 Take advantage of the wider Defender suite

Where to start?

Secure the device

Endpoint

Secure the user

Identity

Secure the workflow

Information

Microsoft Defender products to prioritize

Defender for Endpoint

Endpoint

- Detects advanced threats on workstations, virtual machines, servers and mobile devices
- Includes vulnerability management and next gen antivirus

Defender for Identity/ Azure Active Directory

Identity

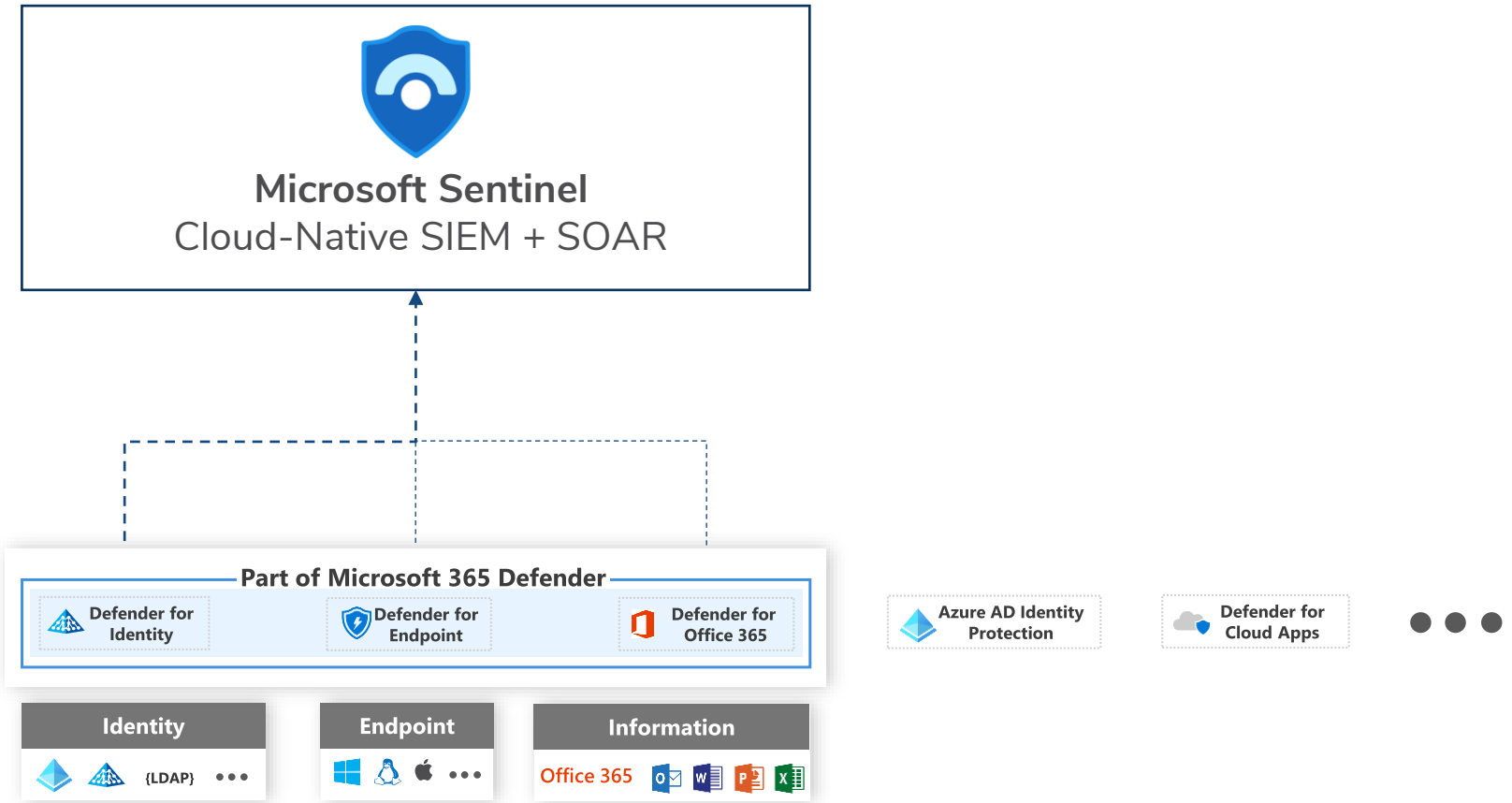
- A central identity and authentication source across third party resources and Software as a Service (SaaS) environments
- Identity-centric view of users' activity and behaviour to highlight malicious activity.

Defender for Office 365

Information

- Protects against malicious threats posed by email messages, links (URLs), and collaboration tools.
- Secure email gateway in front of your exchange servers
- Threat investigation and response capabilities

Security monitoring using Microsoft Sentinel



#3 Enable more agile and complete response

Types of included Microsoft Security playbooks

 Notification	Triggered when an alert or incident is created, a notification is sent to a configured destination, such as Microsoft Teams, Slack or Outlook email.
 Blocking	Triggered when an alert or incident is created, they gather entity information like the account, IP address and host, and block them from further actions.
 Changing incident severity	Triggered by an incident or alert when attached to an automation rule or analytics rule, the incident severity is changed based on a specific username that is part of the incident user entity.

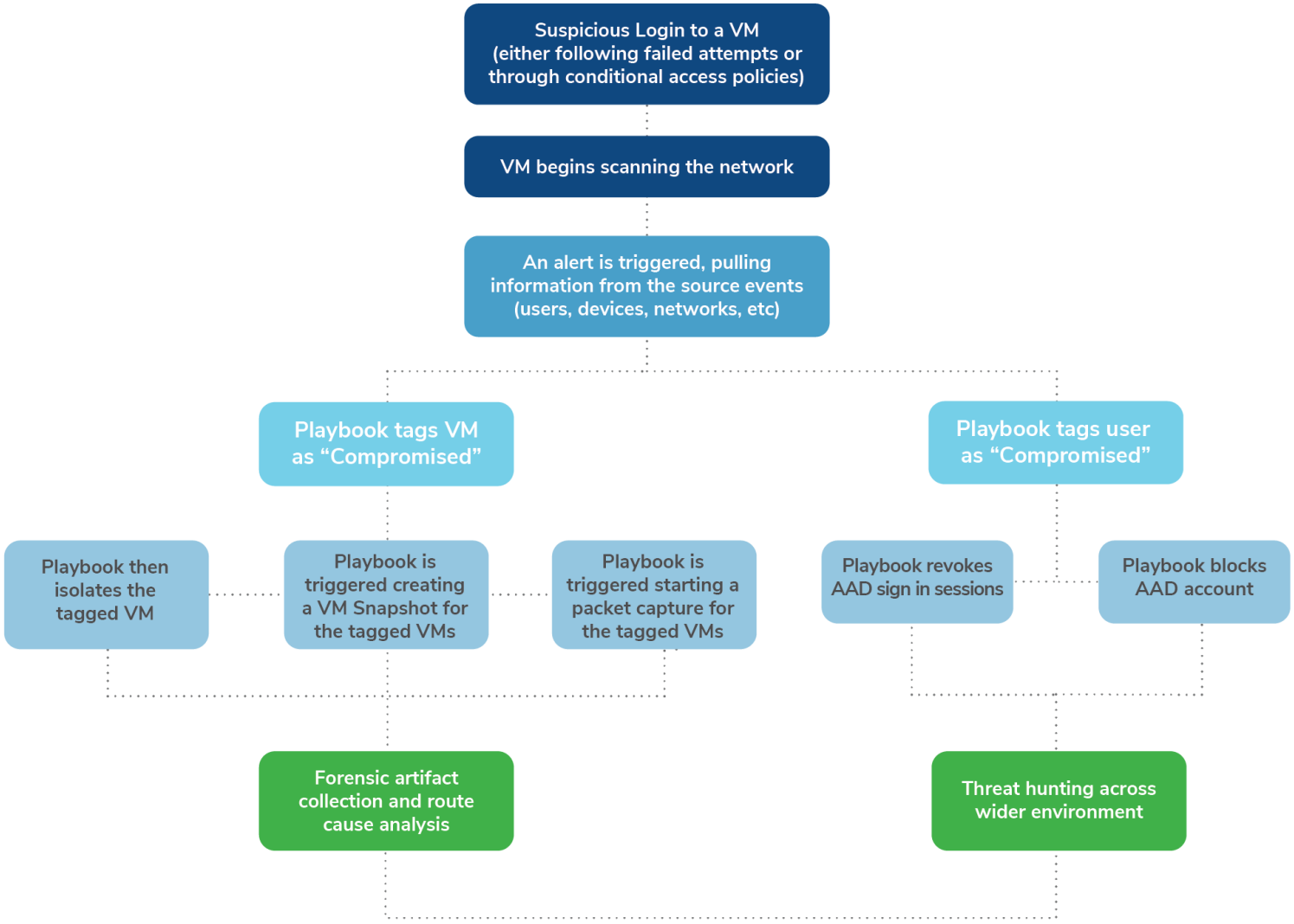
Example of a more ‘complete response’

Detection and Notification

Investigation and Enrichment

Containment

Root Cause Analysis and Hunting



To summarize

1. Drive detections with intelligence

- Front-lines breach intelligence
- Coverage of Cloud-related MITRE ATT&CK techniques (O365, Azure AD, etc.)
- Open-source and closed-source intelligence

2. Configure your Microsoft Security products

- Data retention
- Security policies
- Threat detection rules
- Permissions & Roles

3. Take advantage of wider suite

- Secure the user and the access
- Secure the device the user is working from
- Secure the workflows between users

4. Enable more complete response

- Native Microsoft playbooks
- Automate relevant SOC workflows such as threat intel enrichment and incident response
- DFIR-driven response to understand root-cause
- Prevent reinfection

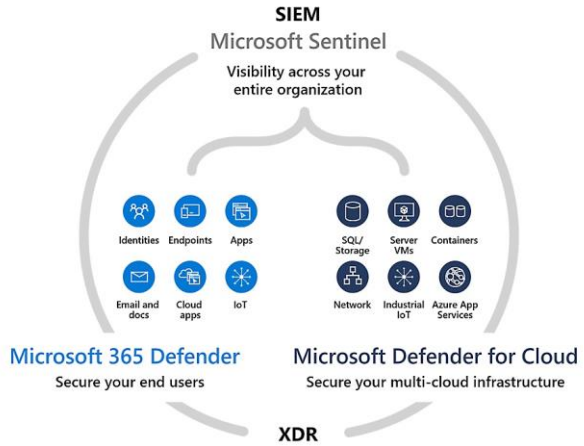
Questions?

Solving the skills gap

How MDR services can help

Skills gap

Filling the security skills gap by **augmenting your team** with Microsoft Security-certified threat detection and response experts



Microsoft product coverage

Leverage a provider who **can help navigate the entire Microsoft Security product range** and help prioritize coverage areas

Wide exposure to incident data

Exposure to Microsoft-related security incidents of all sizes, types and complexity ensures they **will have the threat intelligence and detection rules needed** to detect these threats.

WE'RE A SECRET GIANT

TRUSTED EXPERTS

9/10
AV. RATING FOR SECURITY ADVICE

PREFERRED VENDOR FOR
60+
CYBER INSURANCE CARRIERS

100+
INDUSTRY CERTIFICATIONS (CISA, CRISC, CISSP, PFI, QSA, GPEN, CREST, ETC.)

INDUSTRY RECOGNITION

Bloor
NAMED CHAMPION IN 2022 MDR RESEARCH

FORRESTER
NAMED STRONG PERFORMER IN 2022 IR SERVICES RESEARCH

Gartner
RECOGNIZED AS REPRESENTATIVE VENDOR FOR MDR, DFIR & MANAGED SIEM

KROLL

For more information, please contact: your local Kroll office or today's presenters:

Scott Hanson
Associate Managing Director & Head of
Global Security Operations
Cyber Risk

Rafael De Lima
Vice President and Solutions Architect
Cyber Risk

Thomas Hind
Vice President and Platform Architect
Cyber Risk

Follow Us:

@Kroll Cyber Risk

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's team of more than 6,500 professionals worldwide continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.

Thank You