Microsoft Security

Microsoft Defender XDR automatic attack disruption

Pawel Partyka, Principal Security Researcher – Microsoft Defender XDR

Agenda

Microsoft Defender XDR

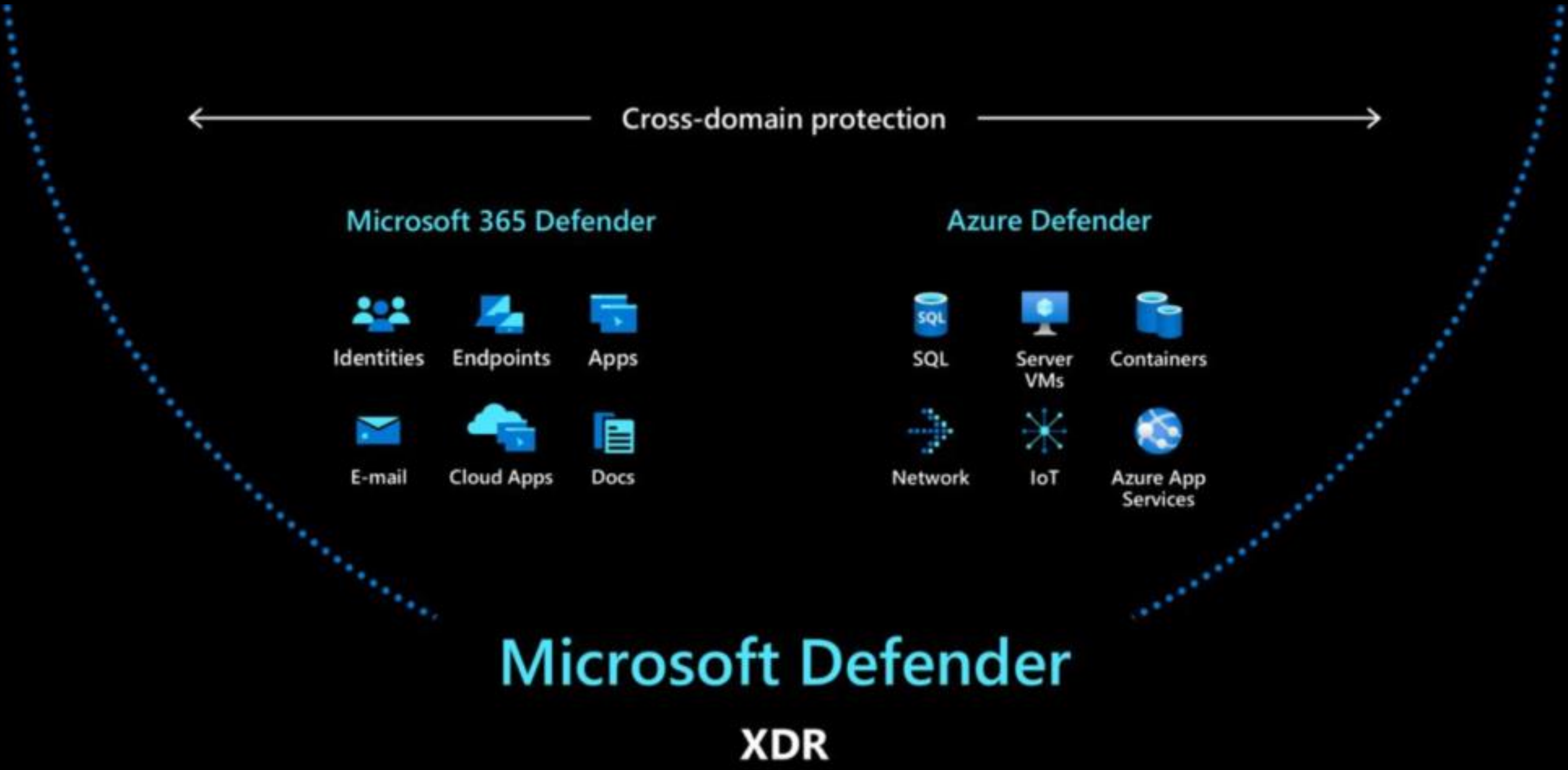
Motivation

Establishing high-confidence

Use Cases

Supported actions

Controls and Configurations



Cross-domain protection

Microsoft 365 Defender

Identities

Endpoints

Apps

E-mail

Cloud Apps

Docs

Azure Defender

SQL

Server VMs

Containers

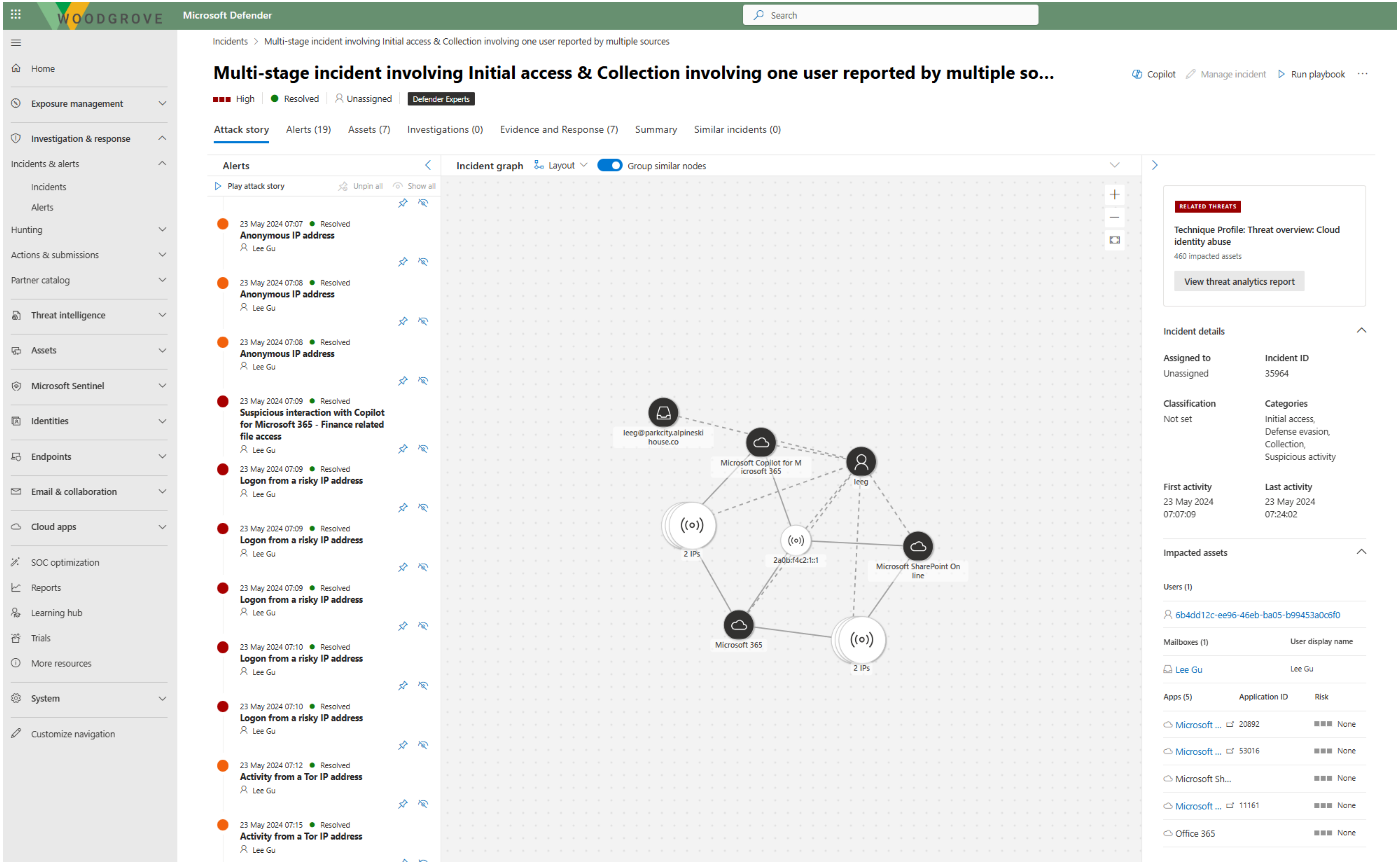
Network

IoT

Azure App Services

Microsoft Defender

XDR



Incidents > Multi-stage incident involving Initial access & Collection involving one user reported by multiple sources

Multi-stage incident involving Initial access & Collection involving one user reported by multiple so...

High · Resolved · Unassigned · Defender Experts

Alerts

- 23 May 2024 07:07 ● Resolved
  Anonymous IP address
  Lee Gu
- 23 May 2024 07:08 ● Resolved
  Anonymous IP address
  Lee Gu
- 23 May 2024 07:08 ● Resolved
  Anonymous IP address
  Lee Gu
- 23 May 2024 07:09 ● Resolved
  Suspicious interaction with Copilot for Microsoft 365 - Finance related file access
  Lee Gu
- 23 May 2024 07:09 ● Resolved
  Logon from a risky IP address
  Lee Gu
- 23 May 2024 07:09 ● Resolved
  Logon from a risky IP address
  Lee Gu
- 23 May 2024 07:09 ● Resolved
  Logon from a risky IP address
  Lee Gu
- 23 May 2024 07:10 ● Resolved
  Logon from a risky IP address
  Lee Gu
- 23 May 2024 07:10 ● Resolved
  Logon from a risky IP address
  Lee Gu
- 23 May 2024 07:12 ● Resolved
  Activity from a Tor IP address
  Lee Gu
- 23 May 2024 07:15 ● Resolved
  Activity from a Tor IP address
  Lee Gu

Incident graph

Layout
Group similar nodes
leeg@parkcity.alpineskihouse.co
Microsoft Copilot for Microsoft 365
leeg
2 IPs
2a0b:f4c2:1::1
Microsoft SharePoint Online
Microsoft 365
2 IPs

RELATED THREATS

Technique Profile: Threat overview: Cloud identity abuse

460 impacted assets

Incident details

Assigned to Unassigned	Incident ID 35964
Classification Not set	Categories Initial access, Defense evasion, Collection, Suspicious activity
First activity 23 May 2024 07:07:09	Last activity 23 May 2024 07:24:02

Impacted assets

Users (1)

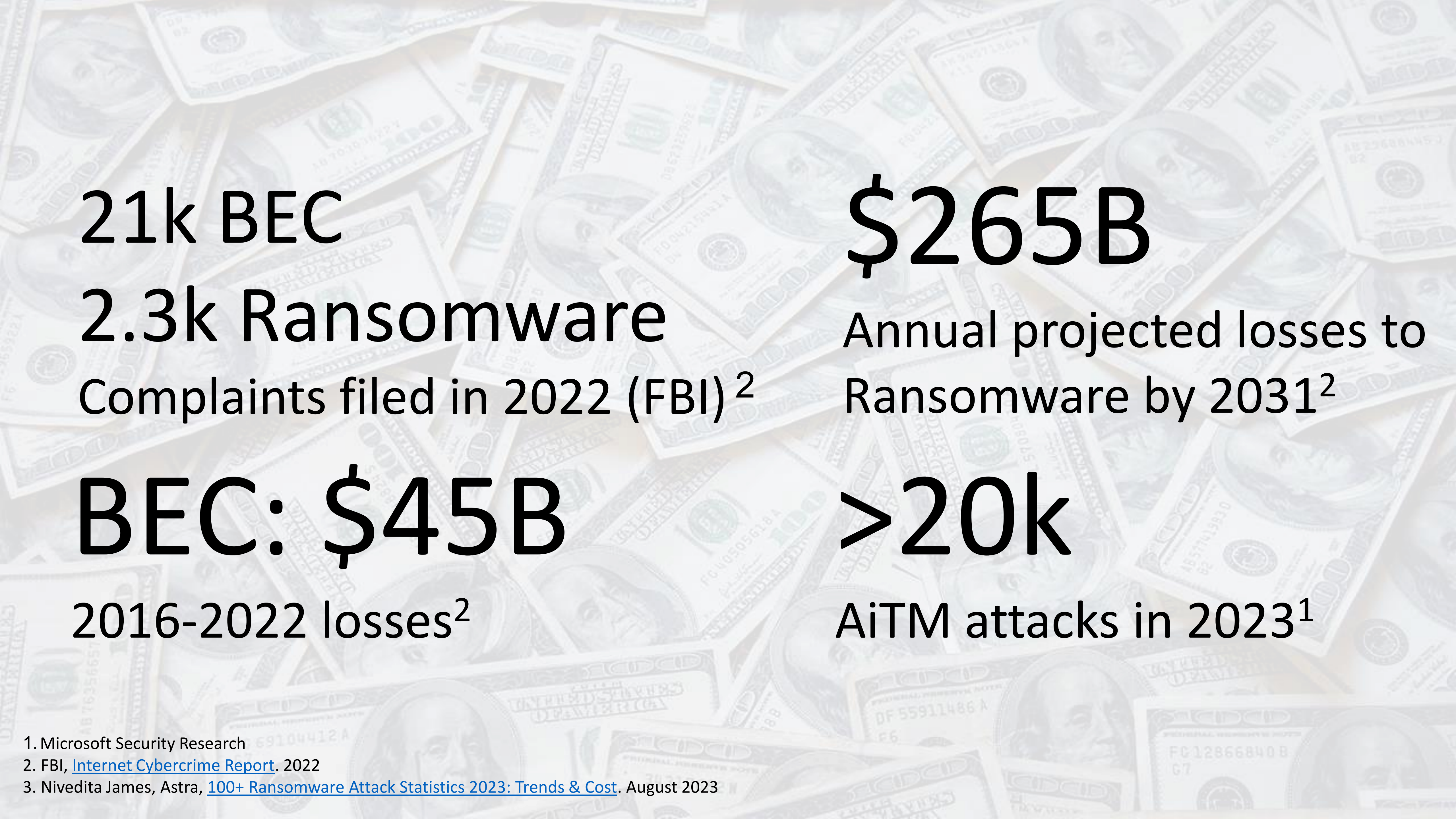
6b4dd12c-ee96-46eb-ba05-b99453a0c6f0

Mailboxes (1)	User display name
Lee Gu	Lee Gu

Apps (5)	Application ID	Risk
Microsoft ...	20892	■■■ None
Microsoft ...	53016	■■■ None
Microsoft Sh...		■■■ None
Microsoft ...	11161	■■■ None
Office 365		■■■ None

ATTACK DISRUPTION

Automated response actions aimed to quickly and effectively **contain an attack in progress**, based on **high-confidence**, cross-workload and 3p signals.



21k BEC

2.3k Ransomware

Complaints filed in 2022 (FBI)[2]

$265B

Annual projected losses to Ransomware by 2031[2]

BEC: $45B

2016-2022 losses[2]

>20k

AiTM attacks in 2023[1]

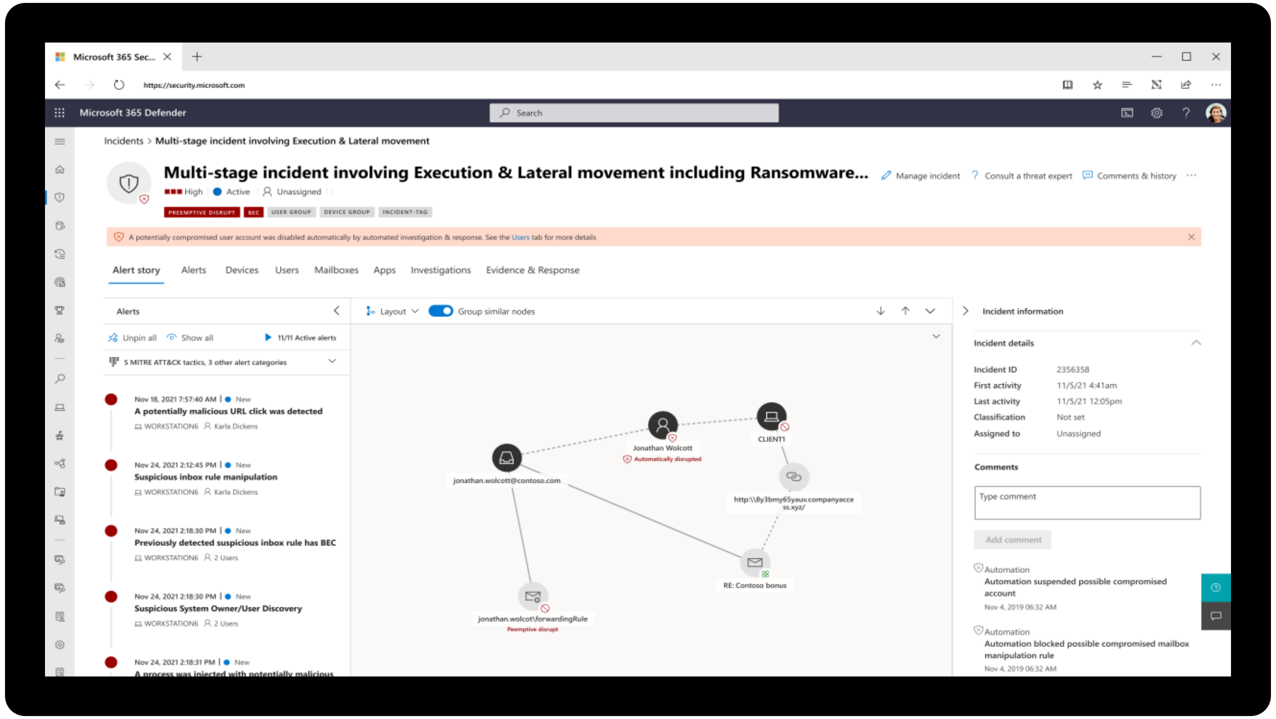
[1] Microsoft Security Research

[2] FBI, Internet Cybercrime Report. 2022

[3] Nivedita James, Astra, 100+ Ransomware Attack Statistics 2023: Trends & Cost. August 2023

Attack disruption at machine speed

XDR-level intelligence and AI automatically disrupt advanced attacks incl. ransomware, BEC, and AiTM



Incidents > Multi-stage incident involving Execution & Lateral movement

Multi-stage incident involving Execution & Lateral movement including Ransomware...

Manage incident · Consult a threat expert · Comments & history

High | Active | Unassigned

PREEMPTIVE DISRUPT · BEC · USER GROUP · DEVICE GROUP · INCIDENT-TAG

A potentially compromised user account was disabled automatically by automated investigation & response. See the Users tab for more details

Alerts

Unpin all · Show all · 11/11 Active alerts

5 MITRE ATT&CK tactics, 3 other alert categories

Nov 18, 2021 7:57:40 AM | New
A potentially malicious URL click was detected
WORKSTATION6 · Karla Dickens

Nov 24, 2021 2:12:45 PM | New
Suspicious inbox rule manipulation
WORKSTATION6 · Karla Dickens

Nov 24, 2021 2:18:30 PM | New
Previously detected suspicious inbox rule has BEC
WORKSTATION6 · 2 Users

Nov 24, 2021 2:18:30 PM | New
Suspicious System Owner/User Discovery
WORKSTATION6 · 2 Users

Nov 24, 2021 2:18:31 PM | New
A process was injected with potentially malicious

Incident information

Incident details

Incident ID	2356358
First activity	11/5/21 4:41am
Last activity	11/5/21 12:05pm
Classification	Not set
Assigned to	Unassigned

Comments

Type comment

Add comment

Automation
Automation suspended possible compromised account
Nov 4, 2019 06:32 AM

Automation
Automation blocked possible compromised mailbox manipulation rule
Nov 4, 2019 06:32 AM

AI-powered **automation** disrupts lateral movement

Leaves the SOC team in full control of investigating and remediating

Reduces the overall cost and limits the impact of an attack by stopping lateral movement

Correlation

Detection

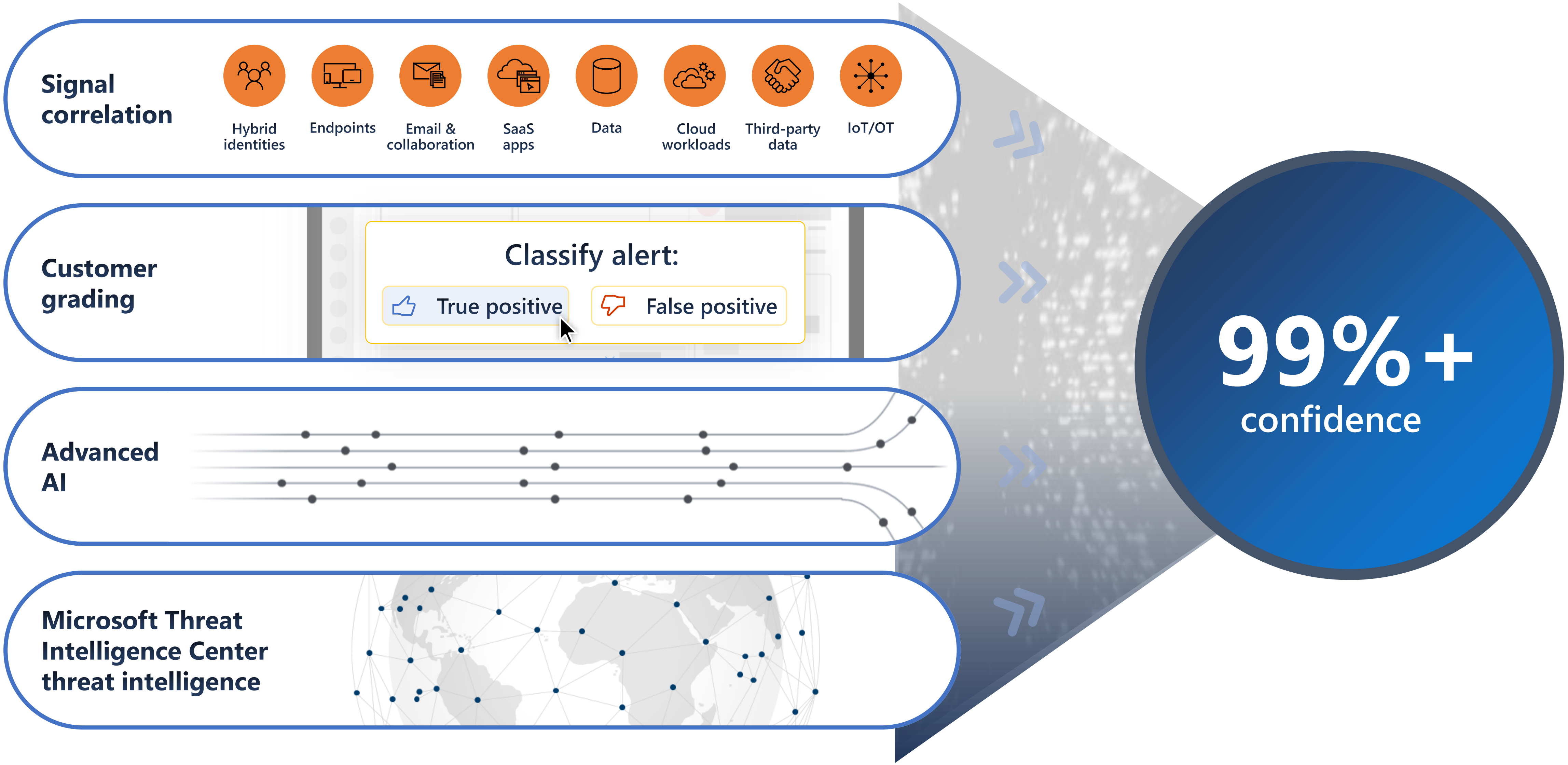
Attack disruption

Correlates signals from multiple sources

Detects attack with **high confidence**, **identify** compromised assets

Automatically contains infected devices and suspends compromised accounts in real-time

Under the hood



Signal correlation

Hybrid identities

Endpoints

Email & collaboration

SaaS apps

Data

Cloud workloads

Third-party data

IoT/OT

Customer grading

Classify alert:

True positive

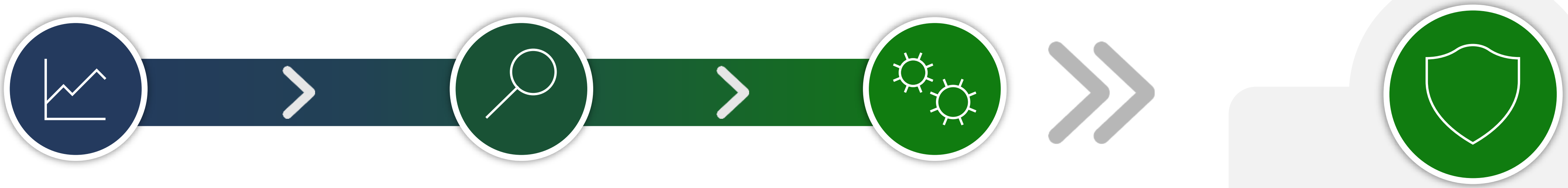
False positive

Advanced AI

Microsoft Threat Intelligence Center threat intelligence

99%+ confidence

How Microsoft 365 Defender takes XDR-automated actions to stop BEC attacks



Correlation

XDR-correlated alerts:

- Unfamiliar sign-in
- Inbox rule creation
- Sending and deletion of emails
- Reading emails

Detection

Identifies attack type and compromised assets:

- BEC attack
- Fraud attempt
- Compromised user and mailbox

Disruption

Automatic response is triggered:

Disables the user account to disrupt the attack—preventing follow-up conversations and the wire instructions from being acted upon.

Zero auto purge reverses certain mailbox actions such as the removal of forwarding rules or moving emails to quarantine.

Enhanced protection and SOC efficiency

Limits a threat actor’s progress early on.

SOC team in full control to investigate all actions automatically taken by Microsoft 365 Defender and where needed, heal any remaining, affected assets.

How Microsoft 365 Defender takes XDR-automated actions to stop AiTM phishing

Correlation

XDR correlated alerts:

- Unfamiliar sign-in
- Network connections from Defender for Endpoint managed device
- Microsoft Defender for Office 365 URL click information
- Threat intelligence signals

Detection

Identifies the attack type and compromised assets:

- AiTM phishing
- Compromised user and mailbox
- Fraud attempt

Disruption

Automatic response is triggered:

Disables compromised user account in Active Directory and Entra ID.

The stolen session cookie will be automatically revoked, preventing the attacker from using it for additional malicious activity.

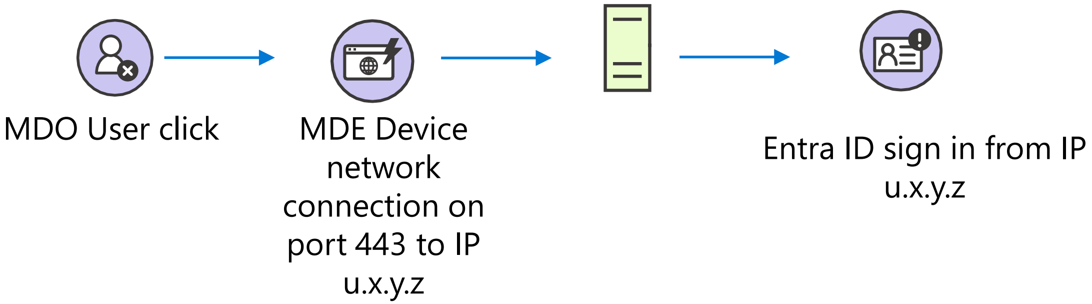
Enhanced protection and SOC efficiency

Limits a threat actor’s progress early on.

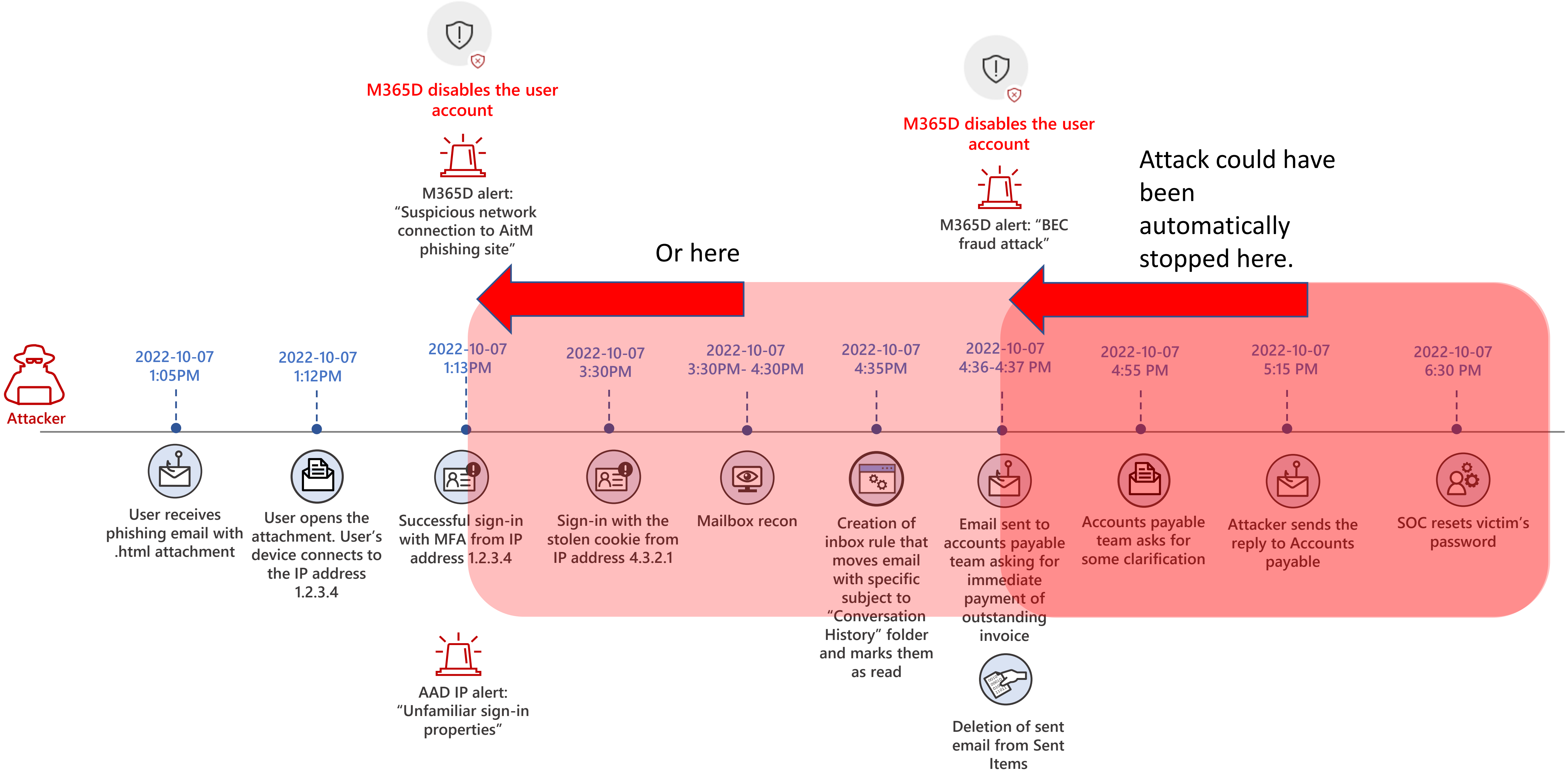
SOC team in full control to investigate all actions automatically taken by Microsoft 365 Defender and where needed, heal any remaining, affected assets.

Example of multi-product detection

- Correlates **risky sign-in** signal from Entra Identity Protection to commonly used appIDs with **network connection** to the same IP address and Microsoft Defender for Office 365 **url click event** in close time proximity


MDO User click
MDE Device network connection on port 443 to IP u.x.y.z
Entra ID sign in from IP u.x.y.z

BEC – Potential successful disruption
Logistics customer - US



Attacker

2022-10-07 1:05PM
User receives phishing email with .html attachment

2022-10-07 1:12PM
User opens the attachment. User's device connects to the IP address 1.2.3.4

2022-10-07 1:13PM
Successful sign-in with MFA from IP address 1.2.3.4

M365D disables the user account

M365D alert: "Suspicious network connection to AitM phishing site"

AAD IP alert: "Unfamiliar sign-in properties"

Or here

2022-10-07 3:30PM
Sign-in with the stolen cookie from IP address 4.3.2.1

2022-10-07 3:30PM- 4:30PM
Mailbox recon

2022-10-07 4:35PM
Creation of inbox rule that moves email with specific subject to "Conversation History" folder and marks them as read

2022-10-07 4:36-4:37 PM
Email sent to accounts payable team asking for immediate payment of outstanding invoice

Deletion of sent email from Sent Items

M365D disables the user account

M365D alert: "BEC fraud attack"

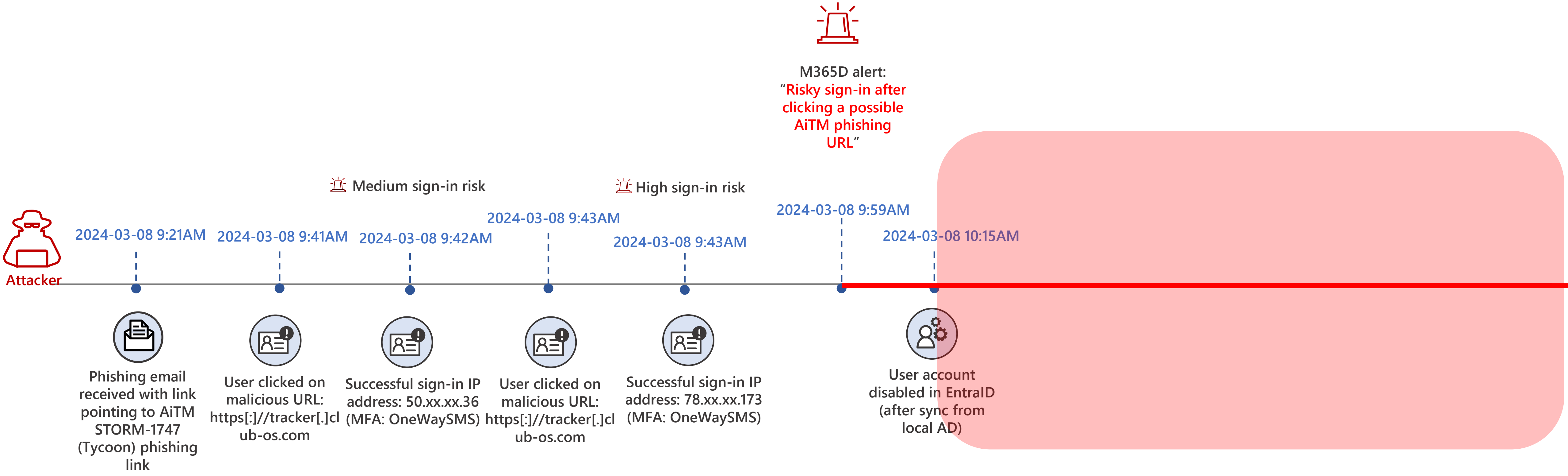
Attack could have been automatically stopped here.

2022-10-07 4:55 PM
Accounts payable team asks for some clarification

2022-10-07 5:15 PM
Attacker sends the reply to Accounts payable

2022-10-07 6:30 PM
SOC resets victim's password

Swedish construction company



Attacker

2024-03-08 9:21AM

Phishing email received with link pointing to AiTM STORM-1747 (Tycoon) phishing link

2024-03-08 9:41AM

User clicked on malicious URL: https[:]//tracker[.]club-os.com

Medium sign-in risk

2024-03-08 9:42AM

Successful sign-in IP address: 50.xx.xx.36 (MFA: OneWaySMS)

2024-03-08 9:43AM

User clicked on malicious URL: https[:]//tracker[.]club-os.com

High sign-in risk

2024-03-08 9:43AM

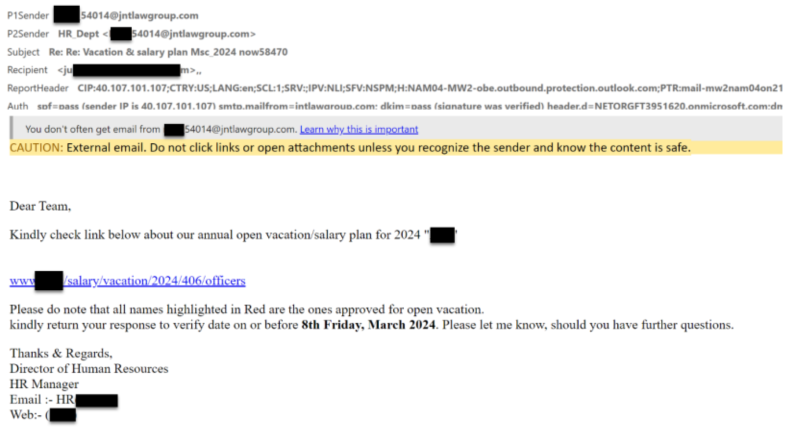
Successful sign-in IP address: 78.xx.xx.173 (MFA: OneWaySMS)

M365D alert:
“Risky sign-in after clicking a possible AiTM phishing URL”

2024-03-08 9:59AM

2024-03-08 10:15AM

User account disabled in EntraID (after sync from local AD)



P1Sender [redacted]54014@jntlawgroup.com
P2Sender HR_Dept <[redacted]54014@jntlawgroup.com>
Subject Re: Re: Vacation & salary plan Msc_2024 now58470
Recipient <ju[redacted]m>,,
ReportHeader CIP:40.107.101.107;CTRY:US;LANG:en;SCL:1;SRV:;IPV:NLI;SFV:NSPM;H:NAM04-MW2-obe.outbound.protection.outlook.com;PTR:mail-mw2nam04on21
Auth spf=pass (sender IP is 40.107.101.107) smtp.mailfrom=jntlawgroup.com; dkim=pass (signature was verified) header.d=NETORGFT3951620.onmicrosoft.com;dn

You don't often get email from [redacted]54014@jntlawgroup.com. Learn why this is important

CAUTION: External email. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Dear Team,

Kindly check link below about our annual open vacation/salary plan for 2024 "[redacted]'

www[redacted]/salary/vacation/2024/406/officers

Please do note that all names highlighted in Red are the ones approved for open vacation.
kindly return your response to verify date on or before **8th Friday, March 2024**. Please let me know, should you have further questions.

Thanks & Regards,
Director of Human Resources
HR Manager
Email :- HR[redacted]
Web:- ([redacted]

Pre-requisites

Disruption **is enabled by default**, but more Defender products deployed, the better.

Action pre-requisites:

- Microsoft Defender for Identity (for hybrid users)

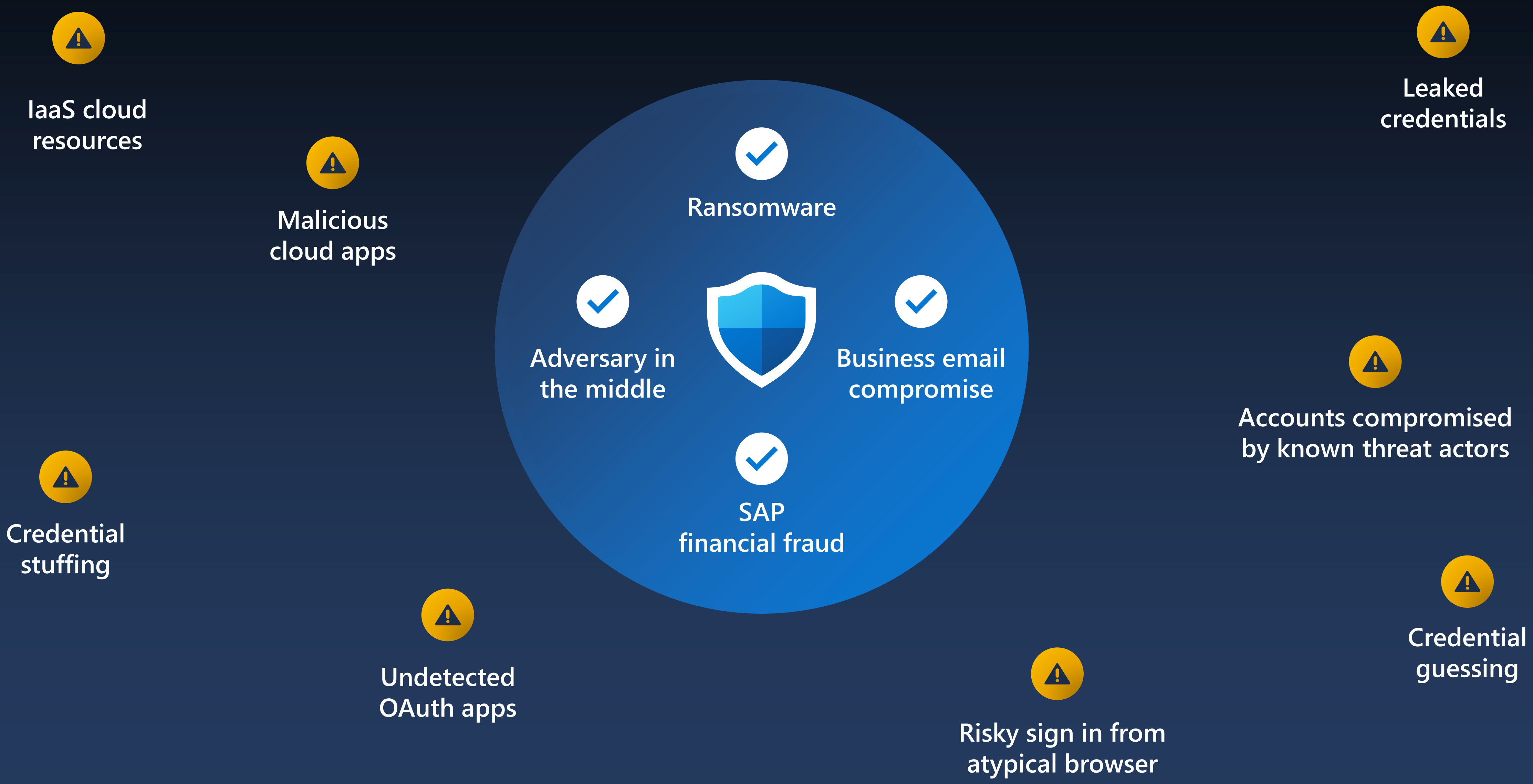
Detection pre-requisites:

- Microsoft Defender for Cloud Apps (important for BEC detections)
- Microsoft Defender for Office 365 (important for AiTM)
- Microsoft Defender for Endpoint (important for HumOR and AiTM
- Entra ID P1 (all)

Current disrupt attack scenarios

1. Business Email Compromise (BEC) – Financial Fraud
2. Human Operated Ransomware (HumOR)
3. Adversary in the Middle (AiTM)
4. Account compromised by a known threat actor
5. A user account compromised by a credential guessing or stuffing attack
6. SAP process manipulation
7. IaaS cloud resource abuse

Attack disruption expansion



IaaS cloud resources

Malicious cloud apps

Leaked credentials

Ransomware

Adversary in the middle

Business email compromise

SAP financial fraud

Accounts compromised by known threat actors

Credential stuffing

Undetected OAuth apps

Credential guessing

Risky sign in from atypical browser

Attack disruption expansion

- ✓ IaaS cloud resources
- ✓ Malicious cloud apps
- ✓ Attacker in the middle
- ✓ Credential stuffing
- ✓ Undetected OAuth apps
- ✓ Ransomware
- ✓ SAP financial fraud
- ✓ Business email compromise
- ✓ Risky sign in from atypical browser
- ✓ Leaked credentials
- ✓ Accounts compromised by known threat actors
- ✓ Credential guessing

Microsoft Security

Demo

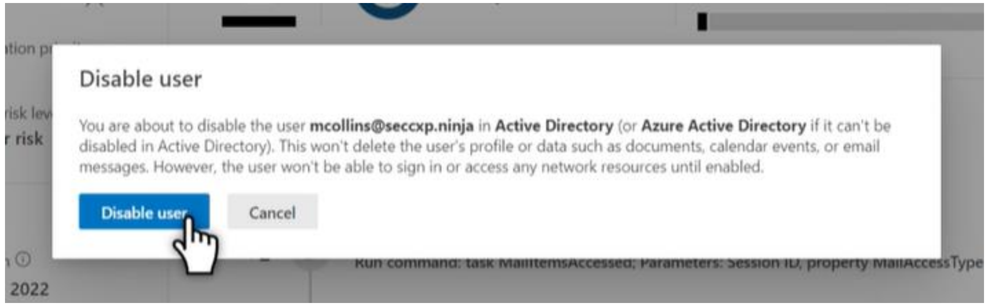
Microsoft Security

Supported automated response actions

Supported Actions

Disable user in Active Directory

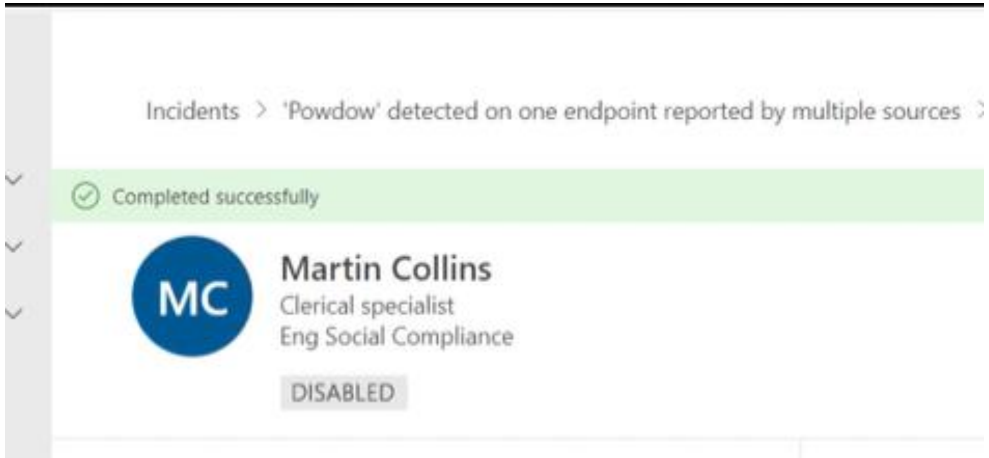
- Leverages Defender for Identity
- Prevents on-premises log-in
- Identity status is synched to AAD



Disable user

You are about to disable the user **mcollins@seccxp.ninja** in **Active Directory** (or **Azure Active Directory** if it can't be disabled in Active Directory). This won't delete the user's profile or data such as documents, calendar events, or email messages. However, the user won't be able to sign in or access any network resources until enabled.

Disable user
Cancel
Run command: task MailItemsAccessed; Parameters: Session ID, property MailAccessType
2022

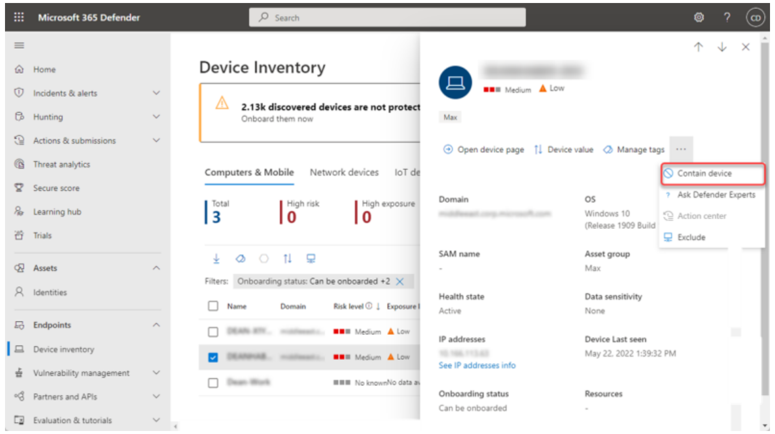


Incidents > 'Powdow' detected on one endpoint reported by multiple sources

Completed successfully

Martin Collins
Clerical specialist
Eng Social Compliance
DISABLED

Supported Actions



Device Inventory

⚠ **2.13k discovered devices are not protect**
Onboard them now

Computers & Mobile | Network devices | IoT de

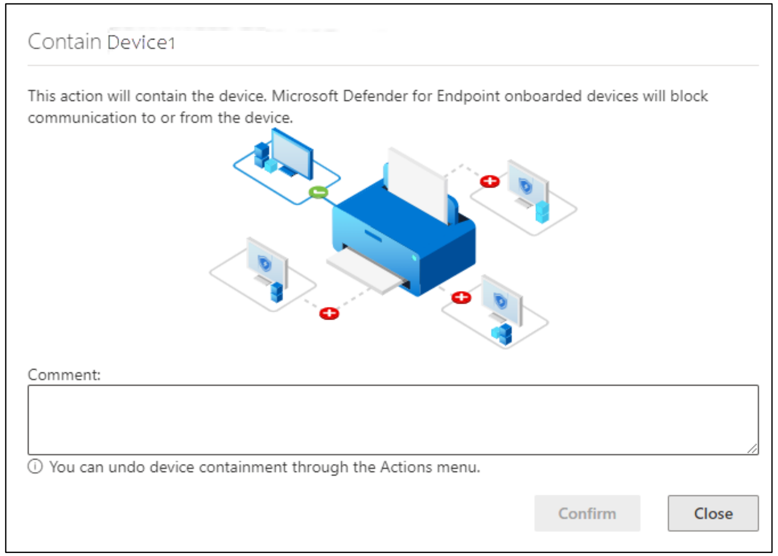
Total 3 | High risk 0 | High exposure 0

Filters: Onboarding status: Can be onboarded +2 ✕

☐	Name	Domain	Risk level ⓘ ↓	Exposure l
☐	[redacted]	[redacted]	Medium	Low
☑	[redacted]	[redacted]	Medium	Low
☐	[redacted]		No known	No data a

[redacted]
Medium ▲ Low
Max

Domain: [redacted]
OS: Windows 10 (Release 1909 Build
SAM name: -
Asset group: Max
Health state: Active
Data sensitivity: None
IP addresses: [redacted]
See IP addresses info
Device Last seen: May 22, 2022 1:39:32 PM
Onboarding status: Can be onboarded
Resources: -



Contain Device1

This action will contain the device. Microsoft Defender for Endpoint onboarded devices will block communication to or from the device.

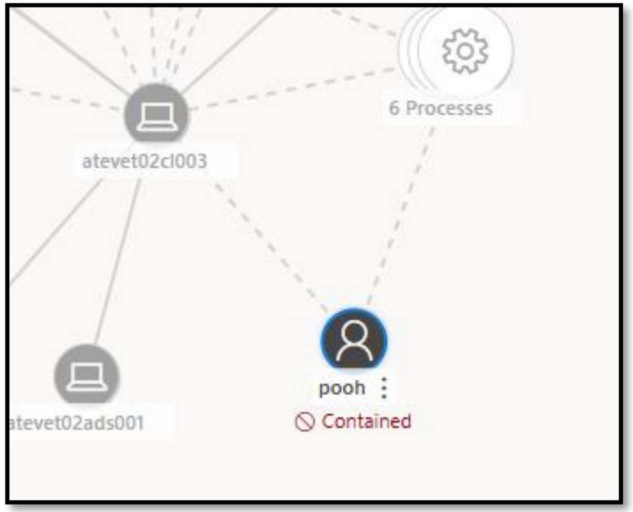
Comment:

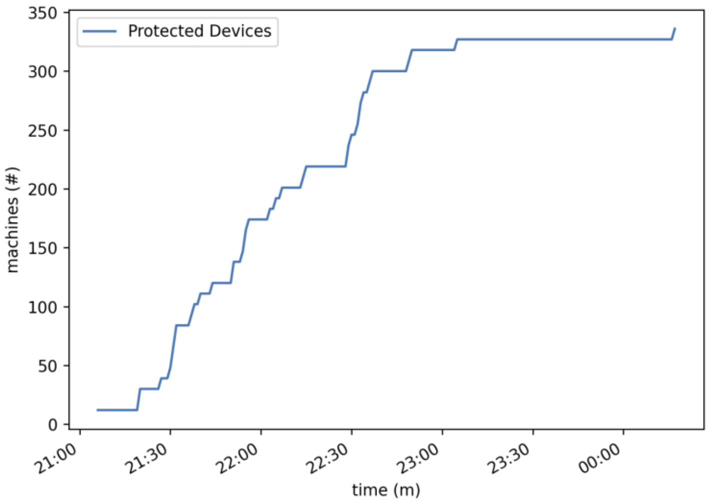
ⓘ You can undo device containment through the Actions menu.

Contain unmanaged device

- Enforces a policy that blocks incoming/outgoing communication with suspected devices
- If a contained device changes its IP address, containment is updated accordingly.

Supported Actions





Contain user

- Any device enrolled to MDE will block attempts to initiate interactive sessions, modify files, pass WMI commands, create scheduled tasks, and other potentially malicious activities from a remote machine
- Blocks lateral movement techniques such as remote execution, and network-level exploitation (PSexec, RDP, SMB and more)
- Granular to maximize productivity
- Decentralized by design to reduce attack surface

Future response actions – work in progress

Cloud identity actions, e.g., disable user in EntraID (directly)

Delete email (e.g., for BEC attacks)

Disable oAuth application (e.g., app consent phishing case)

Thank you. Questions?

Can we collaborate? Please reach out!

Eyal Haik - eyalhaik@microsoft.com

Pawel Partyka – ppartyka@microsoft.com