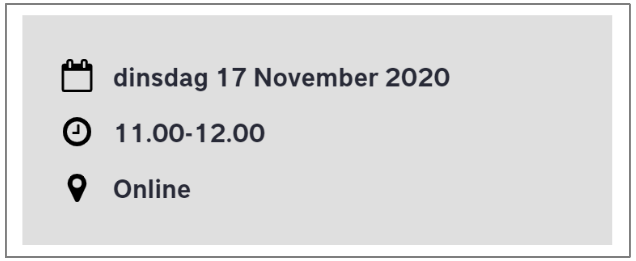
CRAIG SIMONSON – MICROSOFT 365 CONSULTANT

Microsoft 365 Defender Threat Protection: een gedegen security-oplossing?

REALDOLMEN
a Gfi Group company



📅 dinsdag 17 November 2020

🕘 11.00-12.00

📍 Online

Microsoft

MICROSOFT SECURITY PILLARS

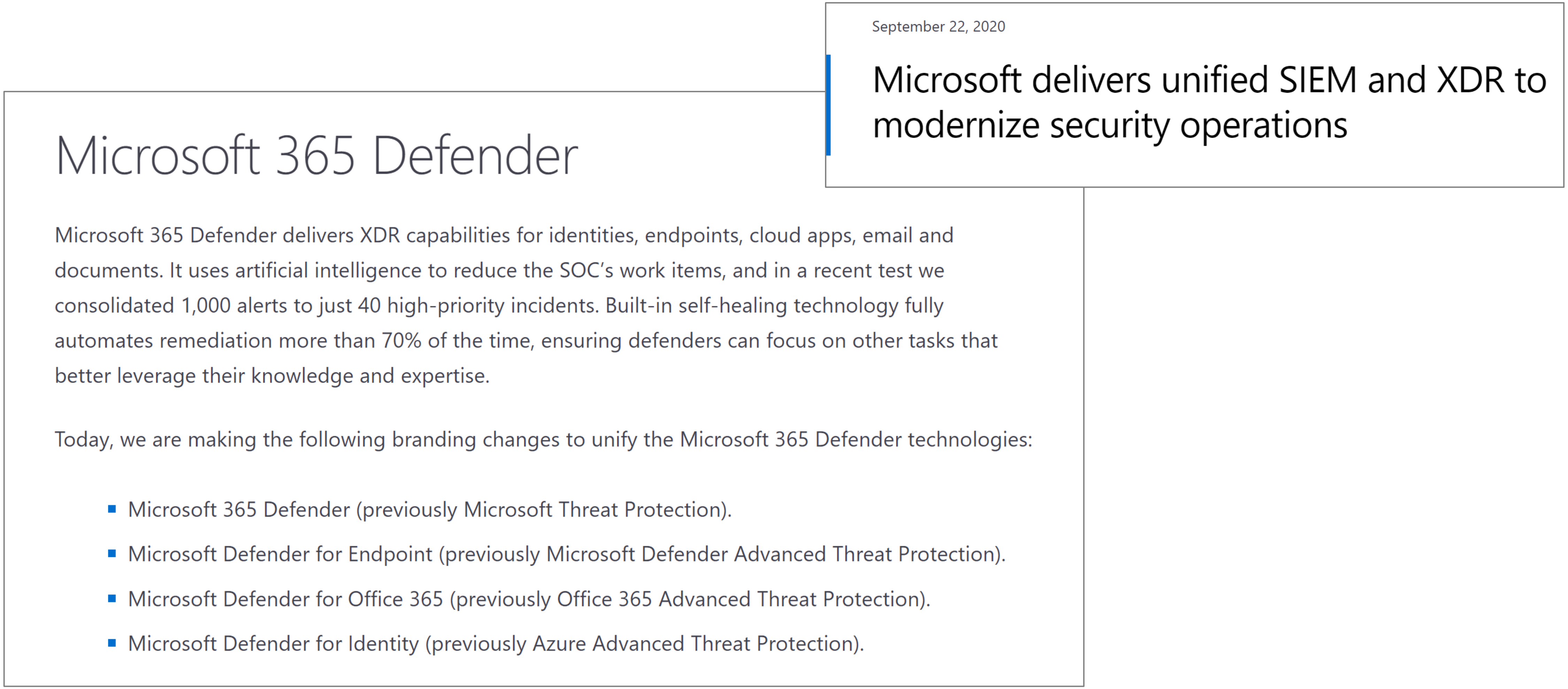
Identity & Access Management

Threat Protection

Information Protection

Security Management

~~Microsoft Threat Protection~~ → Microsoft Defender



September 22, 2020

Microsoft delivers unified SIEM and XDR to modernize security operations

Microsoft 365 Defender

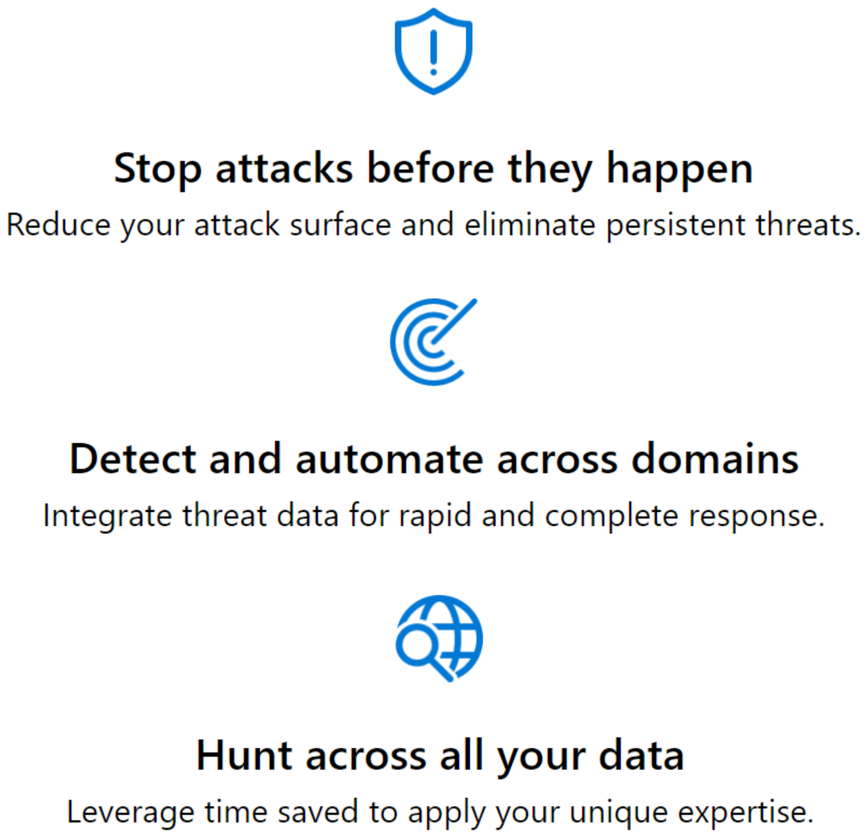
Microsoft 365 Defender delivers XDR capabilities for identities, endpoints, cloud apps, email and documents. It uses artificial intelligence to reduce the SOC's work items, and in a recent test we consolidated 1,000 alerts to just 40 high-priority incidents. Built-in self-healing technology fully automates remediation more than 70% of the time, ensuring defenders can focus on other tasks that better leverage their knowledge and expertise.

Today, we are making the following branding changes to unify the Microsoft 365 Defender technologies:

- Microsoft 365 Defender (previously Microsoft Threat Protection).
- Microsoft Defender for Endpoint (previously Microsoft Defender Advanced Threat Protection).
- Microsoft Defender for Office 365 (previously Office 365 Advanced Threat Protection).
- Microsoft Defender for Identity (previously Azure Advanced Threat Protection).

Source: https://www.microsoft.com/security/blog/?p=91813

MICROSOFT DEFENDER



Stop attacks before they happen

Reduce your attack surface and eliminate persistent threats.

Detect and automate across domains

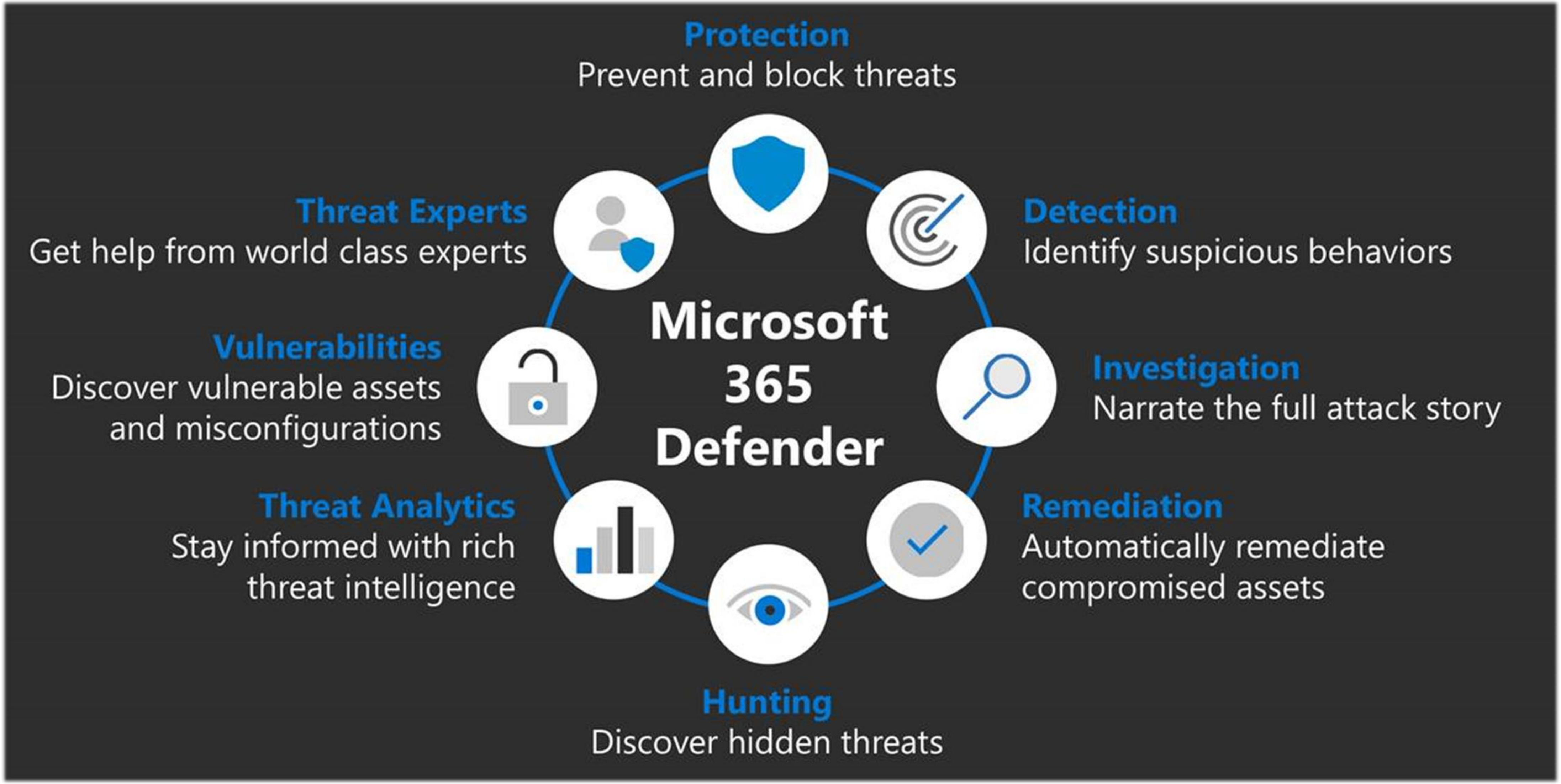
Integrate threat data for rapid and complete response.

Hunt across all your data

Leverage time saved to apply your unique expertise.

- Core
  - Defender for Endpoint
  - Defender for Office 365
  - Defender for Identity
- Related
  - Azure AD Identity Protection
  - Cloud App Security
  - Azure Defender

Microsoft Defender Capabilities



Microsoft 365 Defender

Protection
Prevent and block threats

Detection
Identify suspicious behaviors

Investigation
Narrate the full attack story

Remediation
Automatically remediate compromised assets

Hunting
Discover hidden threats

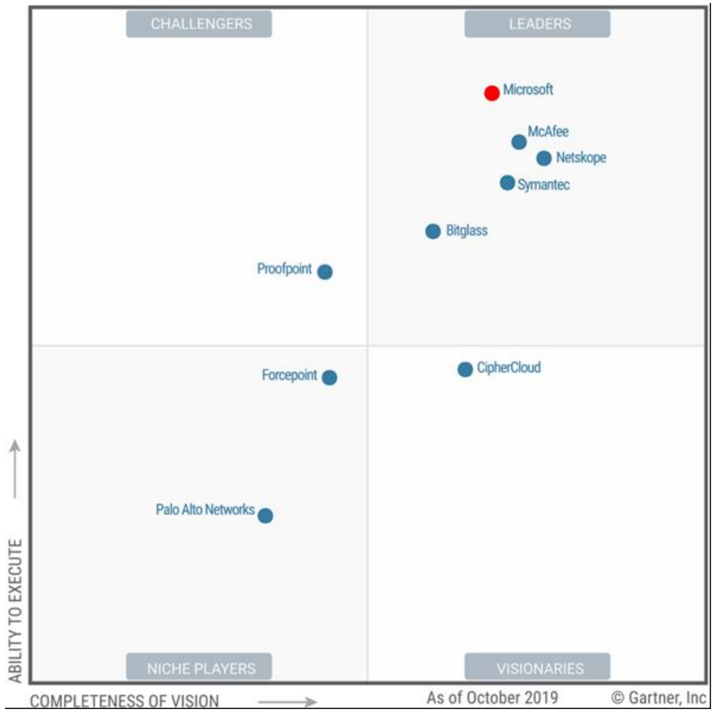
Threat Analytics
Stay informed with rich threat intelligence

Vulnerabilities
Discover vulnerable assets and misconfigurations

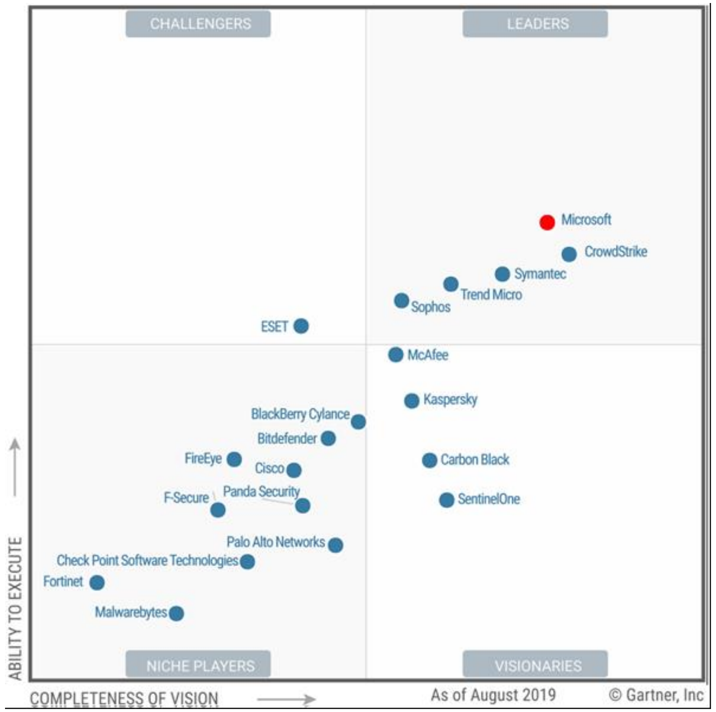
Threat Experts
Get help from world class experts

Gartner Magic Quadrant

Cloud Application Security Broker (CASB)

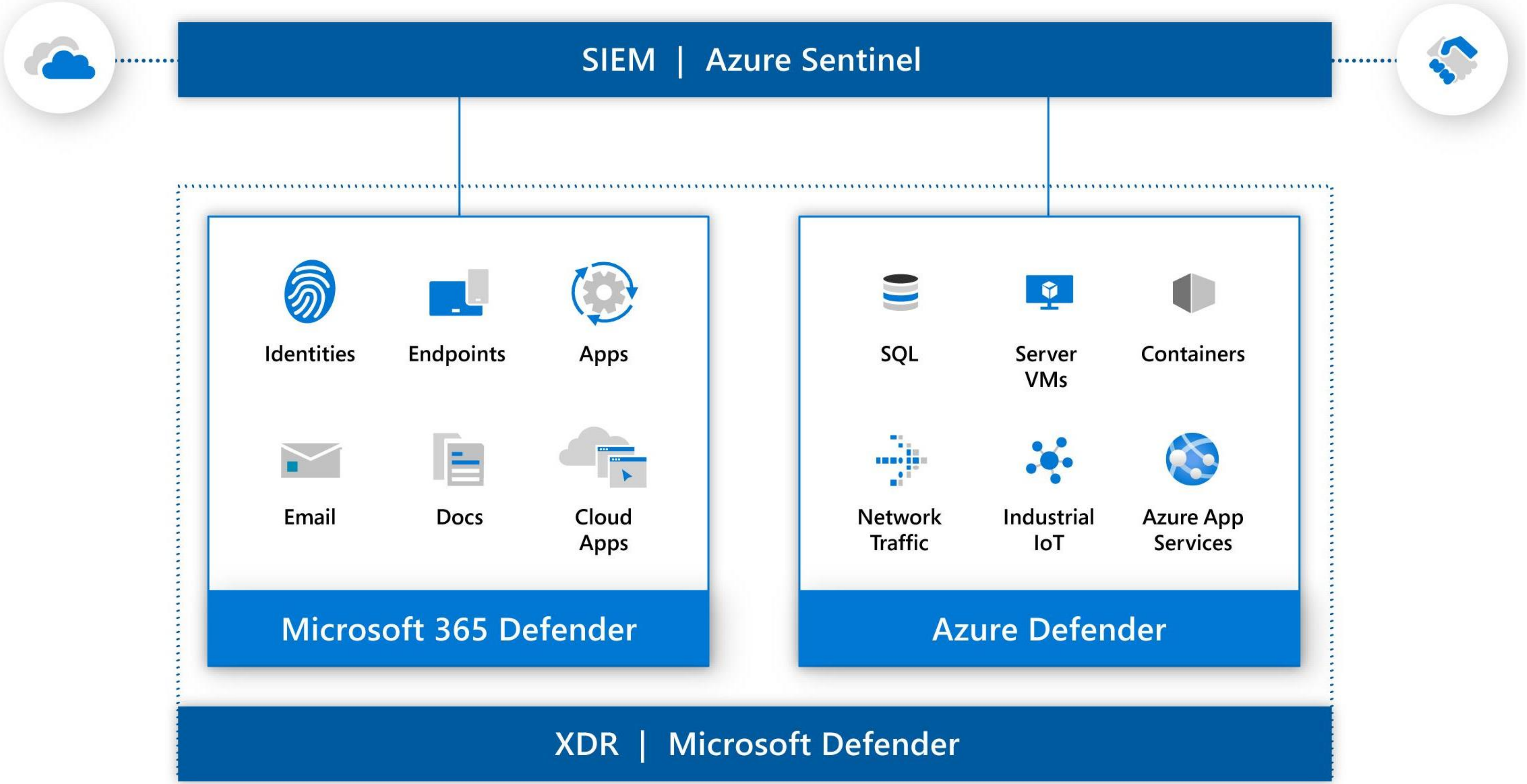


Endpoint Protection (EPP)



Source: https://www.microsoft.com/security/blog/2019/12/03/microsoft-security-leader-5-gartner-magic-quadrants/

Microsoft Defender XDR Integration



SIEM | Azure Sentinel

Identities

Endpoints

Apps

Email

Docs

Cloud Apps

Microsoft 365 Defender

SQL

Server VMs

Containers

Network Traffic

Industrial IoT

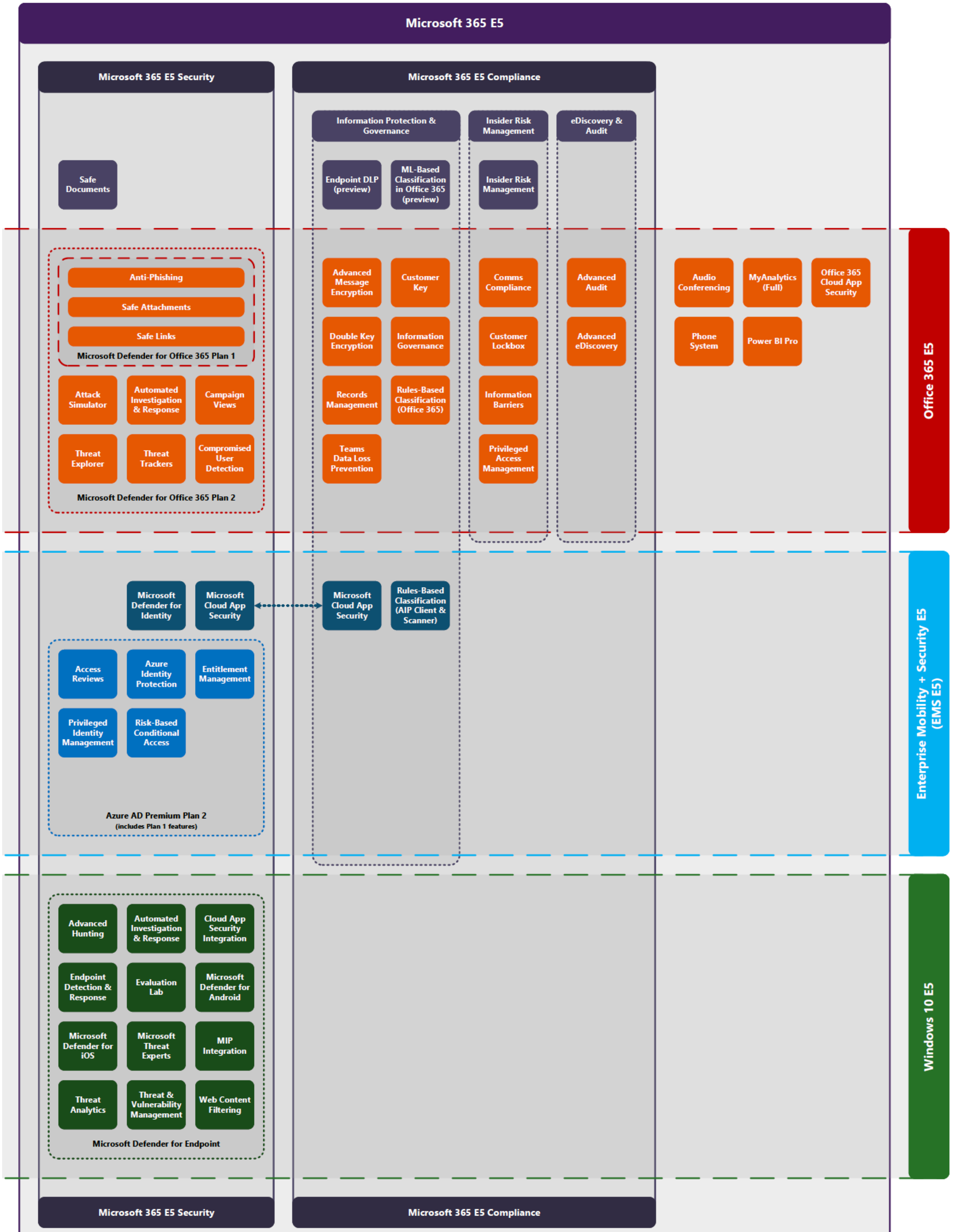
Azure App Services

Azure Defender

XDR | Microsoft Defender

Microsoft Defender Licensing

- M365 E5
- M365 E3 + M365 E5 Security Add-on
- Windows 10 E5
- Standalone via CSP



Microsoft 365 E5

Microsoft 365 E5 Security

Microsoft 365 E5 Compliance

Information Protection & Governance

Insider Risk Management

eDiscovery & Audit

Safe Documents

Endpoint DLP (preview)

ML-Based Classification in Office 365 (preview)

Insider Risk Management

Anti-Phishing

Safe Attachments

Safe Links

Microsoft Defender for Office 365 Plan 1

Attack Simulator

Automated Investigation & Response

Campaign Views

Threat Explorer

Threat Trackers

Compromised User Detection

Microsoft Defender for Office 365 Plan 2

Advanced Message Encryption

Customer Key

Double Key Encryption

Information Governance

Records Management

Rules-Based Classification (Office 365)

Teams Data Loss Prevention

Comms Compliance

Customer Lockbox

Information Barriers

Privileged Access Management

Advanced Audit

Advanced eDiscovery

Audio Conferencing

MyAnalytics (Full)

Office 365 Cloud App Security

Phone System

Power BI Pro

Office 365 E5

Microsoft Defender for Identity

Microsoft Cloud App Security

Microsoft Cloud App Security

Rules-Based Classification (AIP Client & Scanner)

Access Reviews

Azure Identity Protection

Entitlement Management

Privileged Identity Management

Risk-Based Conditional Access

Azure AD Premium Plan 2
(includes Plan 1 features)

Enterprise Mobility + Security E5 (EMS E5)

Advanced Hunting

Automated Investigation & Response

Cloud App Security Integration

Endpoint Detection & Response

Evaluation Lab

Microsoft Defender for Android

Microsoft Defender for iOS

Microsoft Threat Experts

MIP Integration

Threat Analytics

Threat & Vulnerability Management

Web Content Filtering

Microsoft Defender for Endpoint

Windows 10 E5

Microsoft 365 E5 Security

Microsoft 365 E5 Compliance

Microsoft Licensing Diagrams:
https://github.com/AaronDinnage/Licensing

How do you secure your organization against advanced threats?

- Can you detect suspicious activities on your network?
- How do you know if credentials have been compromised?
- How quickly can you remediate advanced threats?
- How do you protect your users from email threats?

Microsoft Threat Protection

Help stop damaging attacks with integrated and automated security

Protect the digital estate

Correlate across attack vectors

Detect & remediate breaches

Microsoft Threat Protection

Identities

Endpoints

User Data

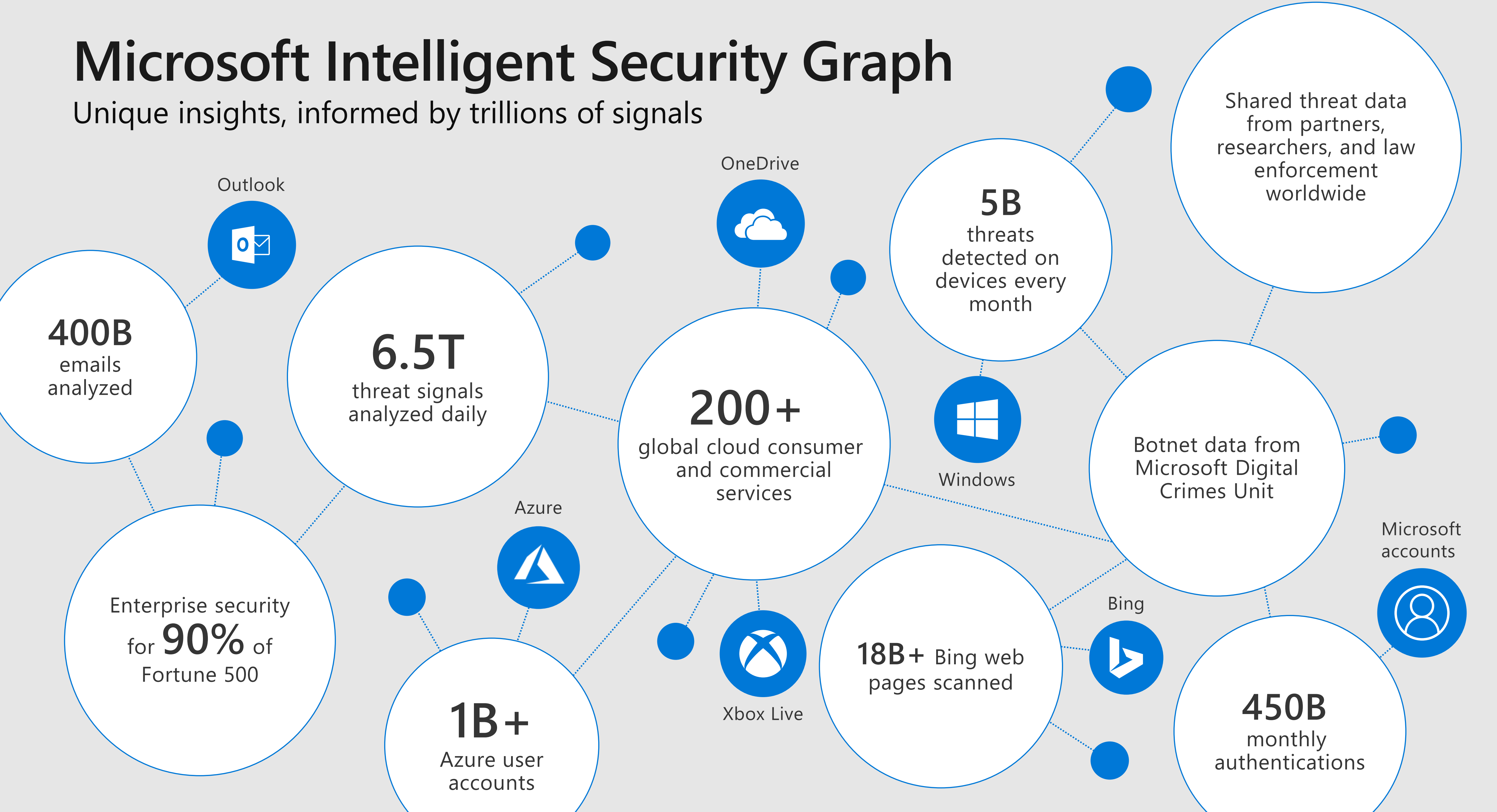
Cloud Apps

Infrastructure

Intelligent Security Graph | 6.5 TRILLION signals per day

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



400B emails analyzed

6.5T threat signals analyzed daily

200+ global cloud consumer and commercial services

5B threats detected on devices every month

Shared threat data from partners, researchers, and law enforcement worldwide

Botnet data from Microsoft Digital Crimes Unit

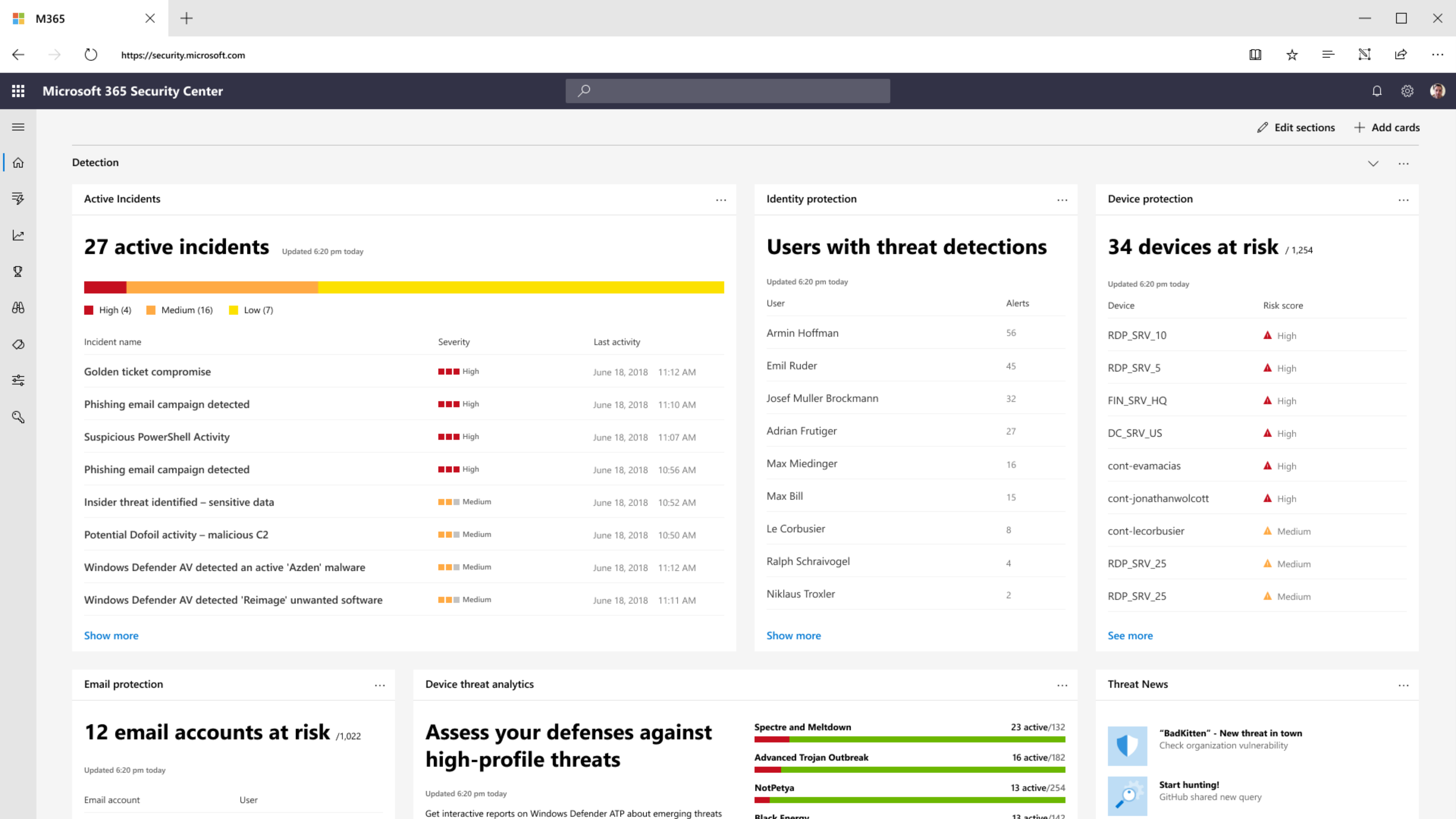
Enterprise security for **90%** of Fortune 500

1B+ Azure user accounts

18B+ Bing web pages scanned

450B monthly authentications

Microsoft Defender Overview



Detection

Active Incidents

27 active incidents

Updated 6:20 pm today

🟥 High (4) 🟧 Medium (16) 🟨 Low (7)

Incident name	Severity	Last activity
Golden ticket compromise	🟥🟥🟥 High	June 18, 2018 11:12 AM
Phishing email campaign detected	🟥🟥🟥 High	June 18, 2018 11:10 AM
Suspicious PowerShell Activity	🟥🟥🟥 High	June 18, 2018 11:07 AM
Phishing email campaign detected	🟥🟥🟥 High	June 18, 2018 10:56 AM
Insider threat identified – sensitive data	🟧🟧 Medium	June 18, 2018 10:52 AM
Potential Dofoil activity – malicious C2	🟧🟧 Medium	June 18, 2018 10:50 AM
Windows Defender AV detected an active 'Azden' malware	🟧🟧 Medium	June 18, 2018 11:12 AM
Windows Defender AV detected 'Reimage' unwanted software	🟧🟧 Medium	June 18, 2018 11:11 AM

Show more

Identity protection

Users with threat detections

Updated 6:20 pm today

User	Alerts
Armin Hoffman	56
Emil Ruder	45
Josef Muller Brockmann	32
Adrian Frutiger	27
Max Miedinger	16
Max Bill	15
Le Corbusier	8
Ralph Schraivogel	4
Niklaus Troxler	2

Show more

Device protection

34 devices at risk / 1,254

Updated 6:20 pm today

Device	Risk score
RDP_SRV_10	▲ High
RDP_SRV_5	▲ High
FIN_SRV_HQ	▲ High
DC_SRV_US	▲ High
cont-evamacias	▲ High
cont-jonathanwolcott	▲ High
cont-lecorbusier	▲ Medium
RDP_SRV_25	▲ Medium
RDP_SRV_25	▲ Medium

See more

Email protection

12 email accounts at risk /1,022

Updated 6:20 pm today

Email account	User

Device threat analytics

Assess your defenses against high-profile threats

Updated 6:20 pm today

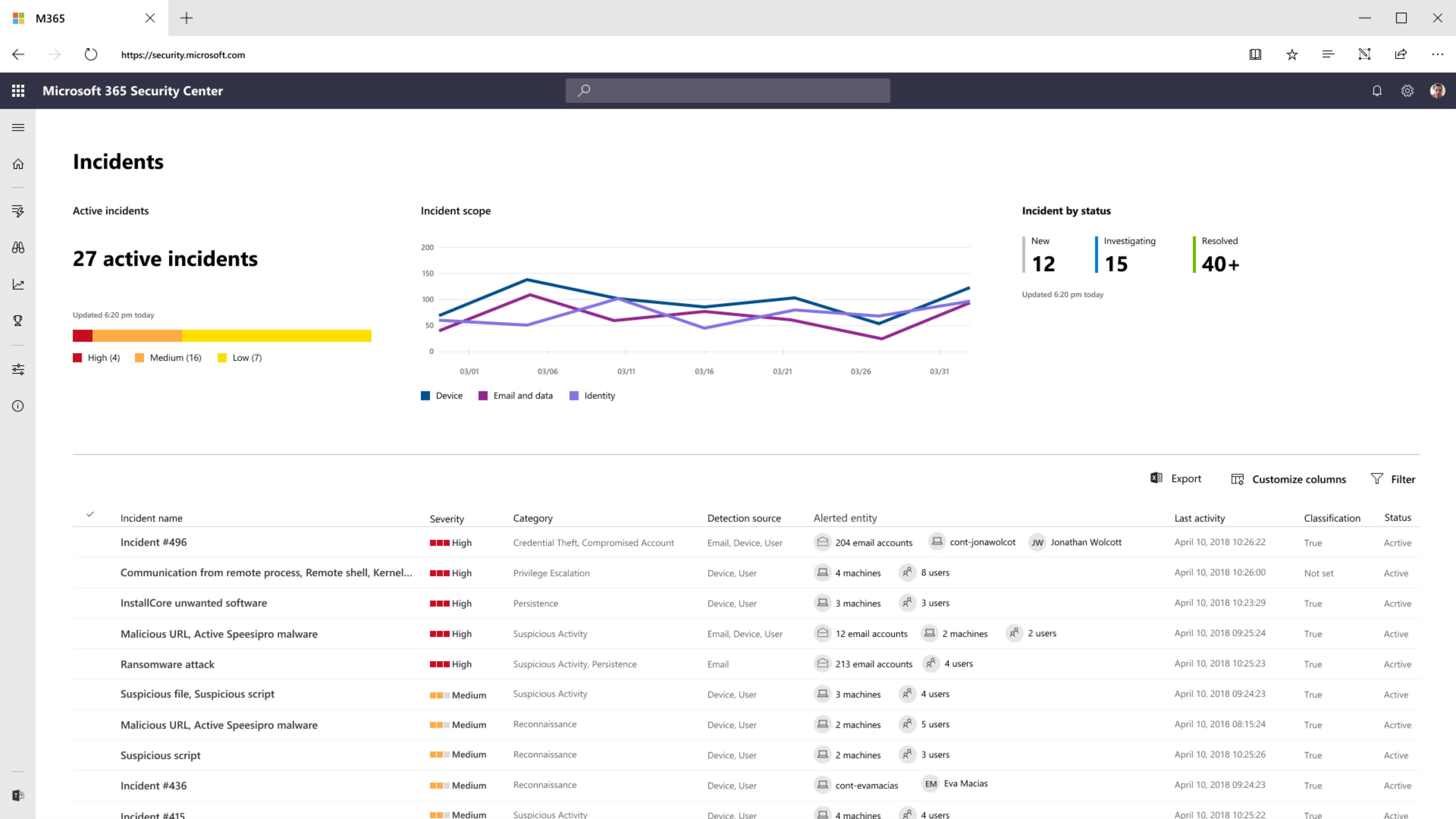
Get interactive reports on Windows Defender ATP about emerging threats

Spectre and Meltdown	23 active/132
Advanced Trojan Outbreak	16 active/182
NotPetya	13 active/254
Black Energy	13 active/142

Threat News

"BadKitten" - New threat in town
Check organization vulnerability

Start hunting!
GitHub shared new query



Incidents

Active incidents

27 active incidents

Updated 6:20 pm today

🟥 High (4) 🟧 Medium (16) 🟨 Low (7)

Incident scope

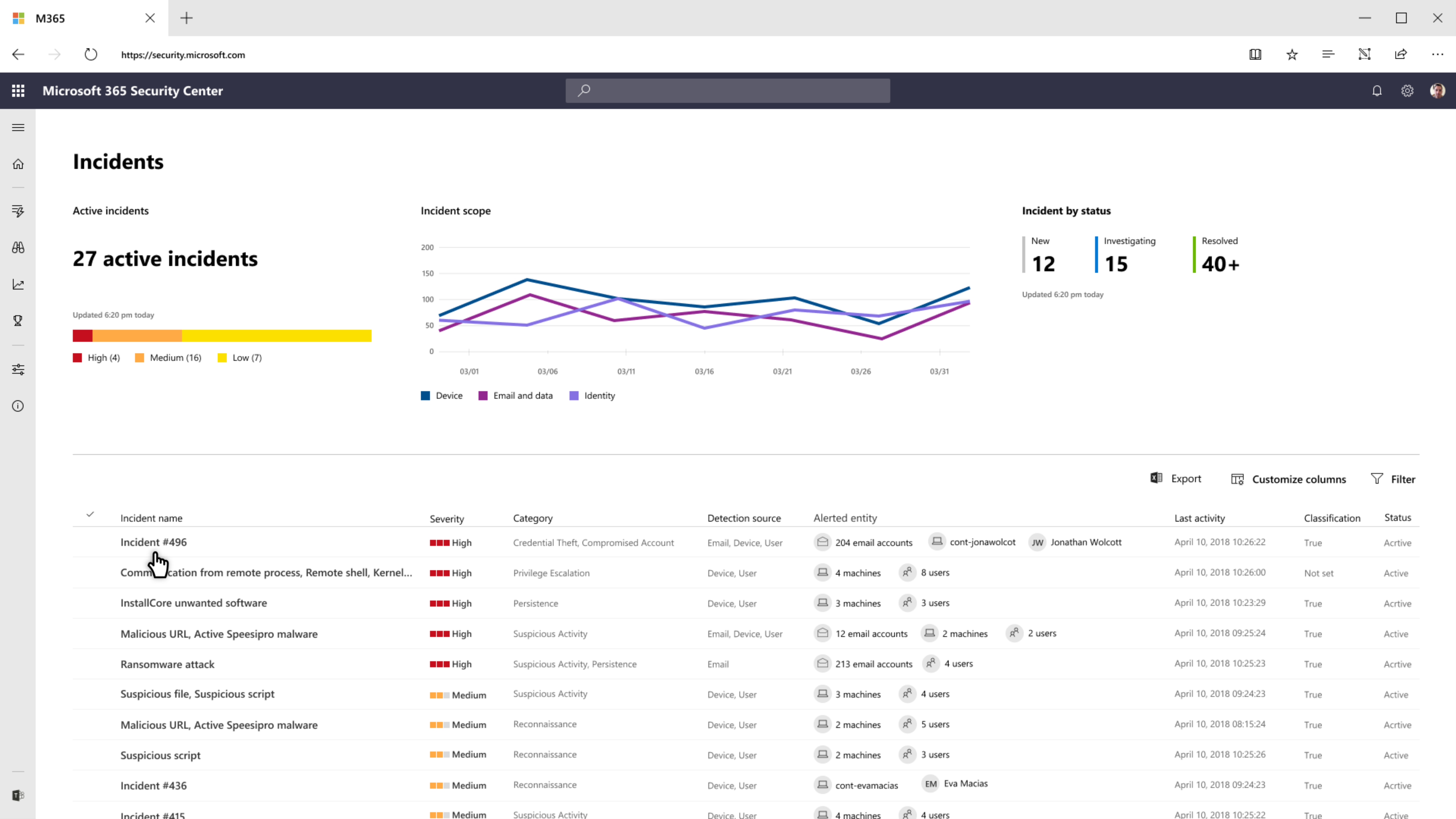
■ Device ■ Email and data ■ Identity

Incident by status

New	Investigating	Resolved
12	15	40+

Updated 6:20 pm today

✓ Incident name	Severity	Category	Detection source	Alerted entity	Last activity	Classification	Status
Incident #496	■■■ High	Credential Theft, Compromised Account	Email, Device, User	204 email accounts cont-jonawolcot JW Jonathan Wolcott	April 10, 2018 10:26:22	True	Active
Communication from remote process, Remote shell, Kernel...	■■■ High	Privilege Escalation	Device, User	4 machines 8 users	April 10, 2018 10:26:00	Not set	Active
InstallCore unwanted software	■■■ High	Persistence	Device, User	3 machines 3 users	April 10, 2018 10:23:29	True	Active
Malicious URL, Active Speesipro malware	■■■ High	Suspicious Activity	Email, Device, User	12 email accounts 2 machines 2 users	April 10, 2018 09:25:24	True	Active
Ransomware attack	■■■ High	Suspicious Activity, Persistence	Email	213 email accounts 4 users	April 10, 2018 10:25:23	True	Active
Suspicious file, Suspicious script	■■□ Medium	Suspicious Activity	Device, User	3 machines 4 users	April 10, 2018 09:24:23	True	Active
Malicious URL, Active Speesipro malware	■■□ Medium	Reconnaissance	Device, User	2 machines 5 users	April 10, 2018 08:15:24	True	Active
Suspicious script	■■□ Medium	Reconnaissance	Device, User	2 machines 3 users	April 10, 2018 10:25:26	True	Active
Incident #436	■■□ Medium	Reconnaissance	Device, User	cont-evamacias EM Eva Macias	April 10, 2018 09:24:23	True	Active
Incident #415	■■□ Medium	Suspicious Activity	Device, User	4 machines 4 users	April 10, 2018 10:25:22	True	Active



Incidents

Active incidents

27 active incidents

Updated 6:20 pm today

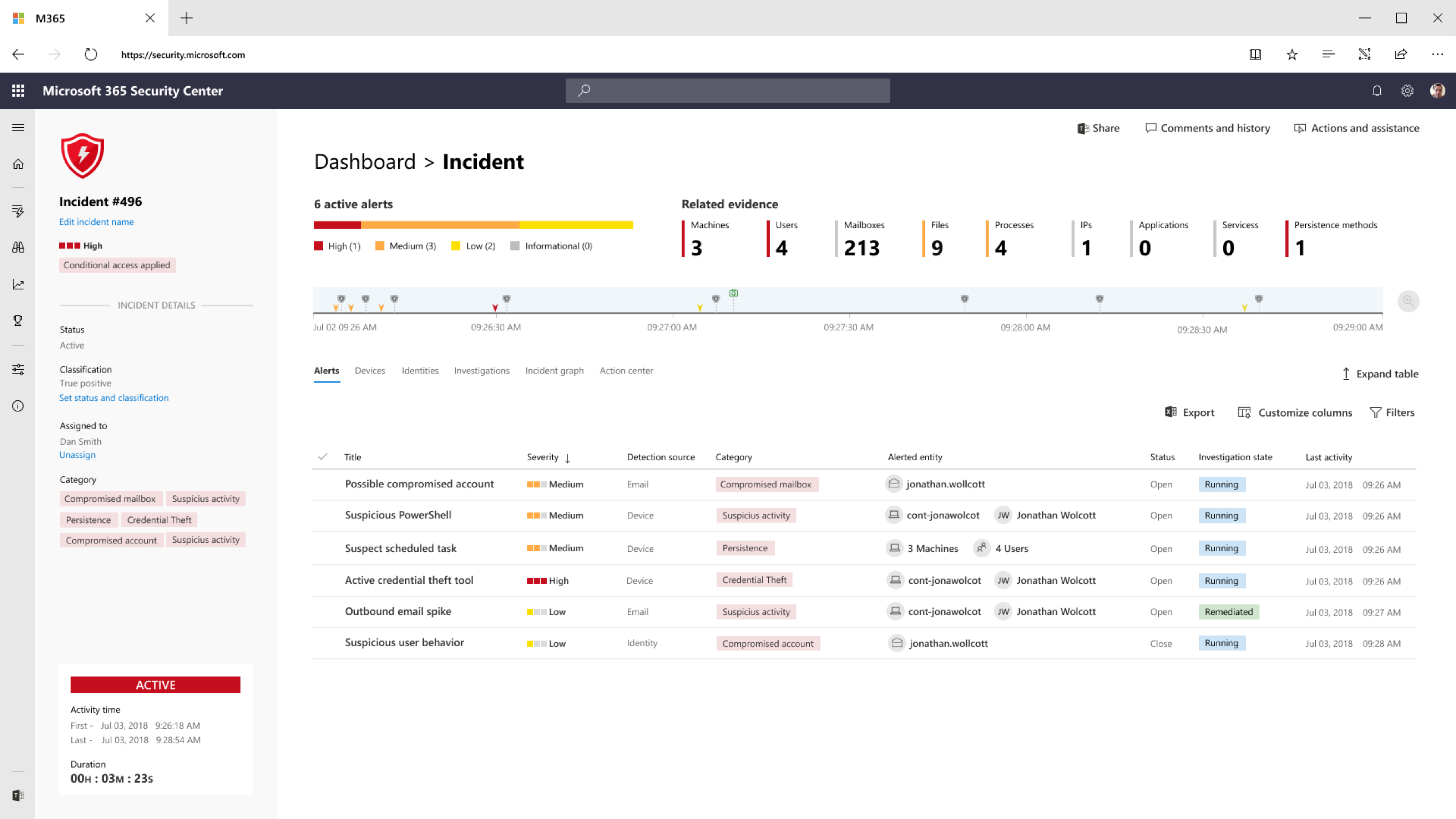
Incident scope

Incident by status

New	Investigating	Resolved
12	15	40+

Updated 6:20 pm today

Incident name	Severity	Category	Detection source	Alerted entity	Last activity	Classification	Status
Incident #496	High	Credential Theft, Compromised Account	Email, Device, User	204 email accounts cont-jonawolcot JW Jonathan Wolcott	April 10, 2018 10:26:22	True	Active
Comm…cation from remote process, Remote shell, Kernel...	High	Privilege Escalation	Device, User	4 machines 8 users	April 10, 2018 10:26:00	Not set	Active
InstallCore unwanted software	High	Persistence	Device, User	3 machines 3 users	April 10, 2018 10:23:29	True	Active
Malicious URL, Active Speesipro malware	High	Suspicious Activity	Email, Device, User	12 email accounts 2 machines 2 users	April 10, 2018 09:25:24	True	Active
Ransomware attack	High	Suspicious Activity, Persistence	Email	213 email accounts 4 users	April 10, 2018 10:25:23	True	Active
Suspicious file, Suspicious script	Medium	Suspicious Activity	Device, User	3 machines 4 users	April 10, 2018 09:24:23	True	Active
Malicious URL, Active Speesipro malware	Medium	Reconnaissance	Device, User	2 machines 5 users	April 10, 2018 08:15:24	True	Active
Suspicious script	Medium	Reconnaissance	Device, User	2 machines 3 users	April 10, 2018 10:25:26	True	Active
Incident #436	Medium	Reconnaissance	Device, User	cont-evamacias EM Eva Macias	April 10, 2018 09:24:23	True	Active
Incident #415	Medium	Suspicious Activity	Device, User	4 machines 4 users	April 10, 2018 10:25:22	True	Active



Share Comments and history Actions and assistance

Dashboard > Incident

Incident #496

Edit incident name

🟥🟥🟥 High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

Duration
00H : 03M : 23S

6 active alerts

🟥 High (1) 🟧 Medium (3) 🟨 Low (2) ⬜ Informational (0)

Related evidence

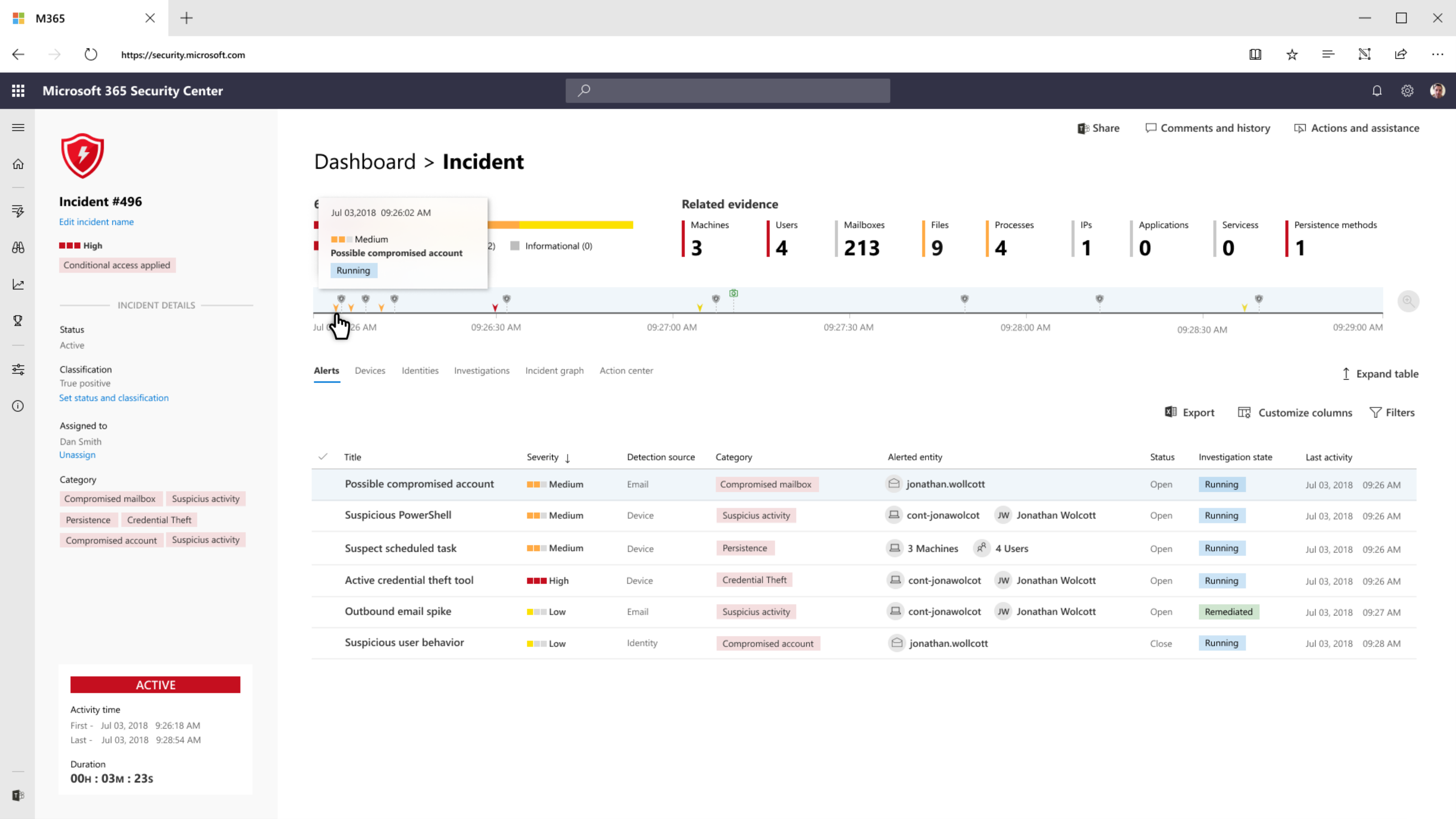
Machines	Users	Mailboxes	Files	Processes	IPs	Applications	Servicess	Persistence methods
3	4	213	9	4	1	0	0	1

Alerts Devices Identities Investigations Incident graph Action center

Expand table

Export Customize columns Filters

✓	Title	Severity ↓	Detection source	Category	Alerted entity	Status	Investigation state	Last activity
	Possible compromised account	Medium	Email	Compromised mailbox	jonathan.wollcott	Open	Running	Jul 03, 2018 09:26 AM
	Suspicious PowerShell	Medium	Device	Suspicius activity	cont-jonawolcot JW Jonathan Wolcott	Open	Running	Jul 03, 2018 09:26 AM
	Suspect scheduled task	Medium	Device	Persistence	3 Machines 4 Users	Open	Running	Jul 03, 2018 09:26 AM
	Active credential theft tool	High	Device	Credential Theft	cont-jonawolcot JW Jonathan Wolcott	Open	Running	Jul 03, 2018 09:26 AM
	Outbound email spike	Low	Email	Suspicius activity	cont-jonawolcot JW Jonathan Wolcott	Open	Remediated	Jul 03, 2018 09:27 AM
	Suspicious user behavior	Low	Identity	Compromised account	jonathan.wollcott	Close	Running	Jul 03, 2018 09:28 AM



Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox · Suspicius activity · Persistence · Credential Theft · Compromised account · Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

Duration
00H : 03M : 23S

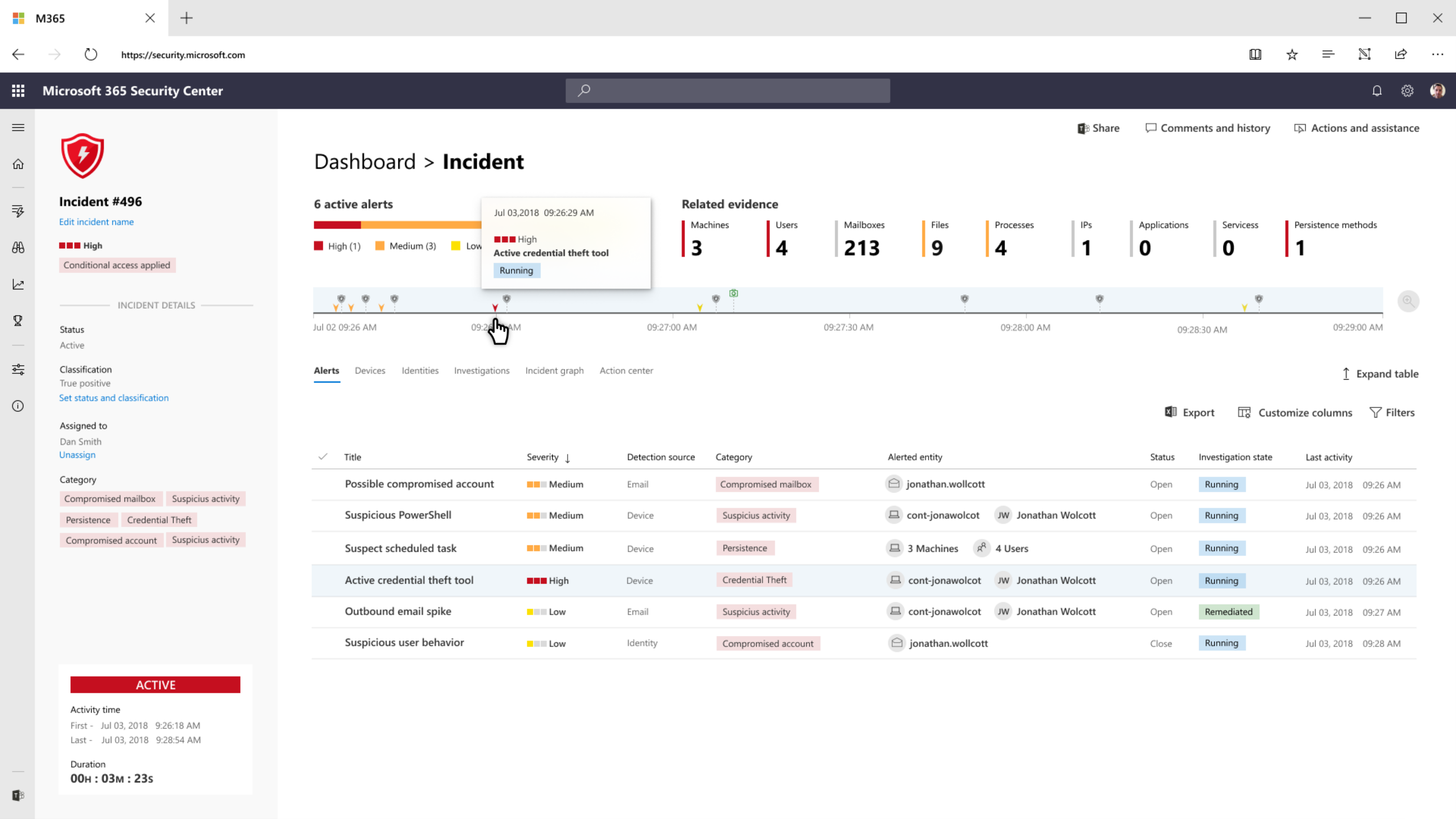
Dashboard > Incident

Related evidence

Machines	Users	Mailboxes	Files	Processes	IPs	Applications	Servicess	Persistence methods
3	4	213	9	4	1	0	0	1

Alerts · Devices · Identities · Investigations · Incident graph · Action center

Title	Severity ↓	Detection source	Category	Alerted entity	Status	Investigation state	Last activity
Possible compromised account	Medium	Email	Compromised mailbox	jonathan.wollcott	Open	Running	Jul 03, 2018 09:26 AM
Suspicious PowerShell	Medium	Device	Suspicius activity	cont-jonawolcot JW Jonathan Wolcott	Open	Running	Jul 03, 2018 09:26 AM
Suspect scheduled task	Medium	Device	Persistence	3 Machines 4 Users	Open	Running	Jul 03, 2018 09:26 AM
Active credential theft tool	High	Device	Credential Theft	cont-jonawolcot JW Jonathan Wolcott	Open	Running	Jul 03, 2018 09:26 AM
Outbound email spike	Low	Email	Suspicius activity	cont-jonawolcot JW Jonathan Wolcott	Open	Remediated	Jul 03, 2018 09:27 AM
Suspicious user behavior	Low	Identity	Compromised account	jonathan.wollcott	Close	Running	Jul 03, 2018 09:28 AM



Dashboard > **Incident**

Incident #496

🟥🟥🟥 High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive

Assigned to
Dan Smith

Category
Compromised mailbox | Suspicius activity
Persistence | Credential Theft
Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

Duration
00H : 03M : 23S

6 active alerts

🟥 High (1) 🟧 Medium (3) 🟨 Low

Jul 03,2018 09:26:29 AM
🟥🟥🟥 High
Active credential theft tool
Running

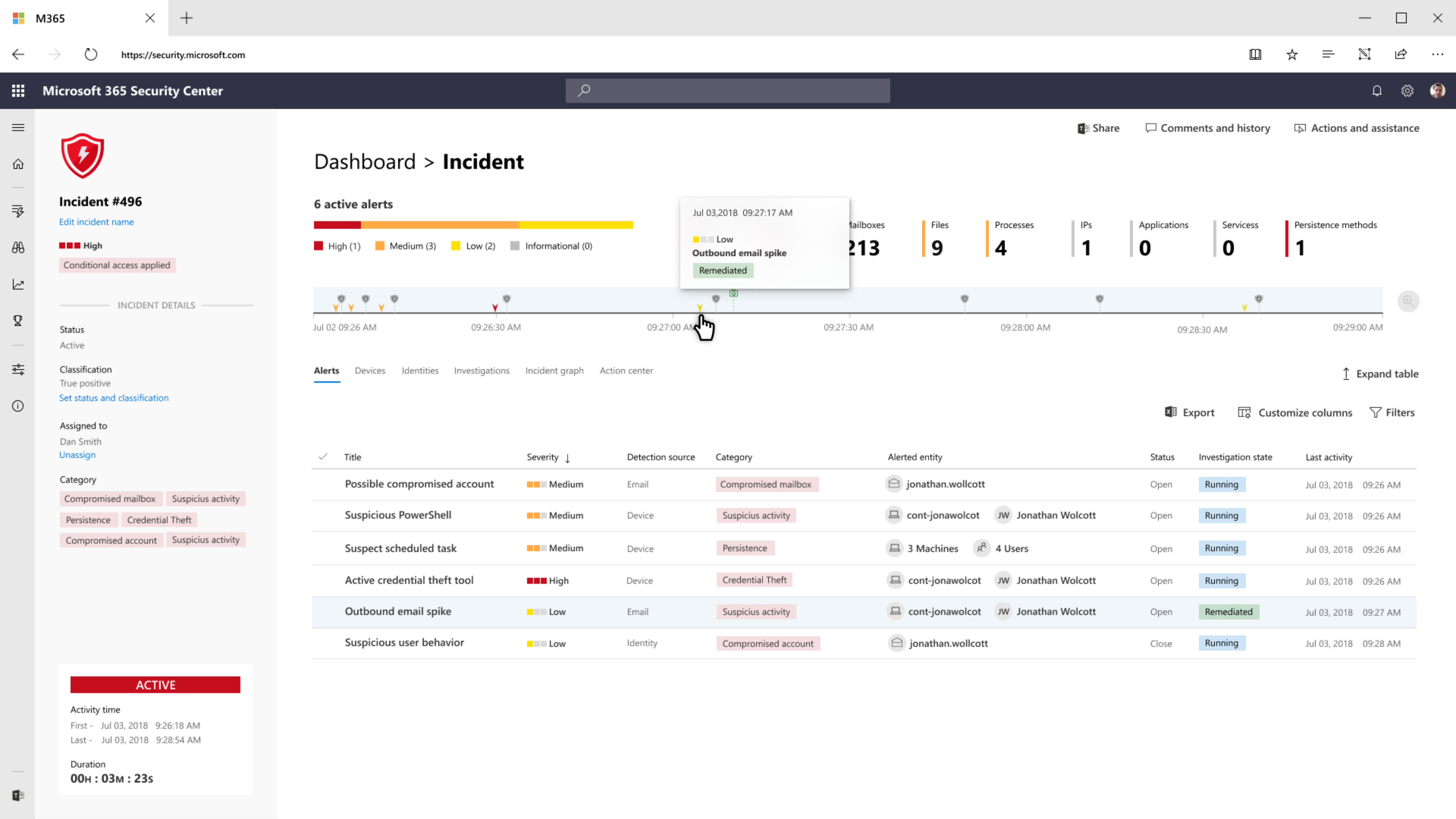
Jul 02 09:26 AM | 09:26 AM | 09:27:00 AM | 09:27:30 AM | 09:28:00 AM | 09:28:30 AM | 09:29:00 AM

Related evidence

Machines	Users	Mailboxes	Files	Processes	IPs	Applications	Servicess	Persistence methods
3	4	213	9	4	1	0	0	1

Alerts | Devices | Identities | Investigations | Incident graph | Action center

Title	Severity ↓	Detection source	Category	Alerted entity	Status	Investigation state	Last activity
Possible compromised account	Medium	Email	Compromised mailbox	jonathan.wollcott	Open	Running	Jul 03, 2018 09:26 AM
Suspicious PowerShell	Medium	Device	Suspicius activity	cont-jonawolcot JW Jonathan Wolcott	Open	Running	Jul 03, 2018 09:26 AM
Suspect scheduled task	Medium	Device	Persistence	3 Machines 4 Users	Open	Running	Jul 03, 2018 09:26 AM
Active credential theft tool	High	Device	Credential Theft	cont-jonawolcot JW Jonathan Wolcott	Open	Running	Jul 03, 2018 09:26 AM
Outbound email spike	Low	Email	Suspicius activity	cont-jonawolcot JW Jonathan Wolcott	Open	Remediated	Jul 03, 2018 09:27 AM
Suspicious user behavior	Low	Identity	Compromised account	jonathan.wollcott	Close	Running	Jul 03, 2018 09:28 AM



Dashboard > **Incident**

Incident #496

Edit incident name

🟥🟥🟥 High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity
Persistence | Credential Theft
Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

Duration
00H : 03M : 23S

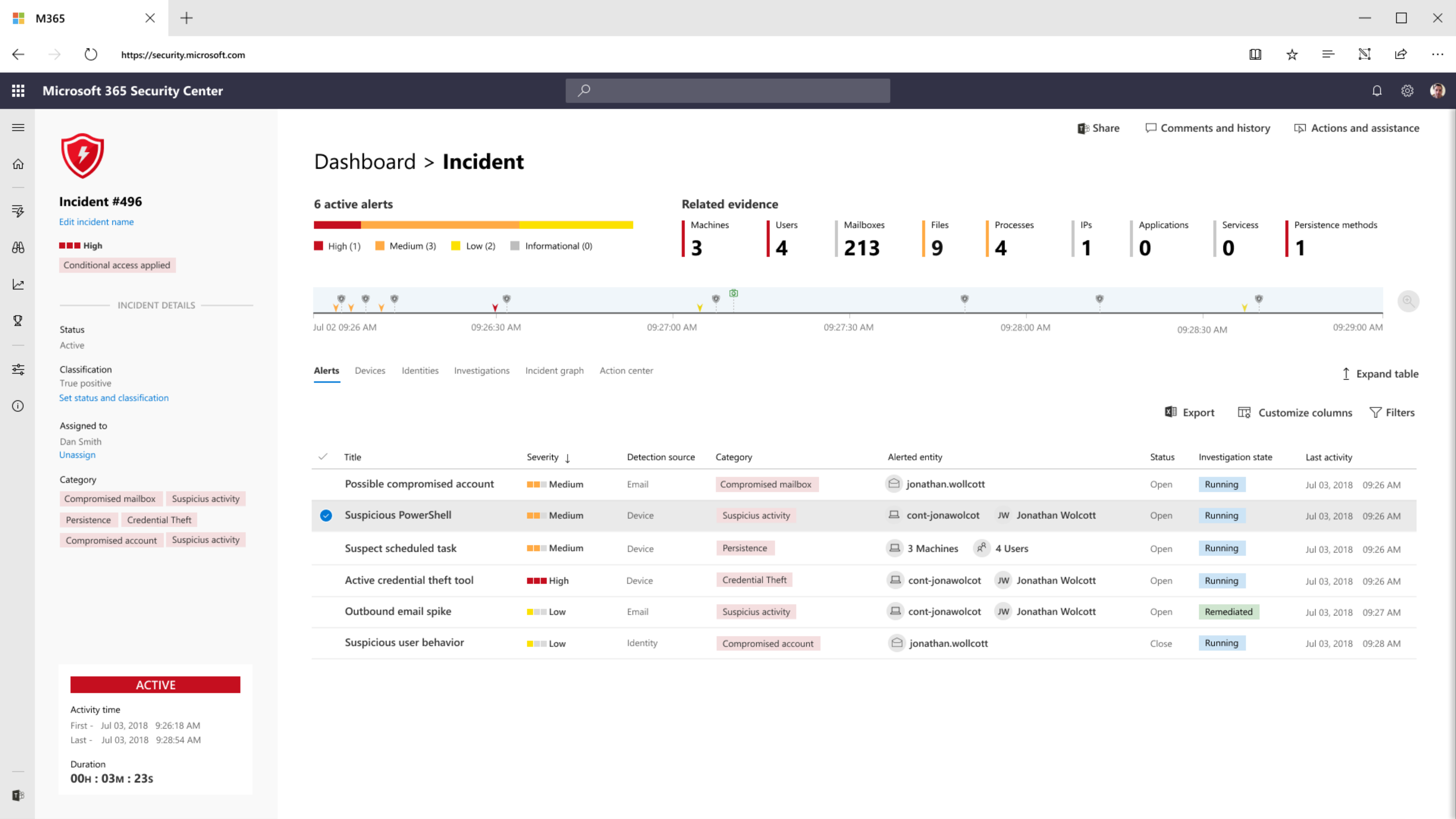
6 active alerts

🟥 High (1) 🟧 Medium (3) 🟨 Low (2) ⬜ Informational (0)

Jul 03,2018 09:27:17 AM
🟨 Low
Outbound email spike
Remediated

Mailboxes	Files	Processes	IPs	Applications	Servicess	Persistence methods
213	9	4	1	0	0	1

✓	Title	Severity ↓	Detection source	Category	Alerted entity	Status	Investigation state	Last activity
	Possible compromised account	Medium	Email	Compromised mailbox	jonathan.wollcott	Open	Running	Jul 03, 2018 09:26 AM
	Suspicious PowerShell	Medium	Device	Suspicius activity	cont-jonawolcot JW Jonathan Wolcott	Open	Running	Jul 03, 2018 09:26 AM
	Suspect scheduled task	Medium	Device	Persistence	3 Machines 4 Users	Open	Running	Jul 03, 2018 09:26 AM
	Active credential theft tool	High	Device	Credential Theft	cont-jonawolcot JW Jonathan Wolcott	Open	Running	Jul 03, 2018 09:26 AM
	Outbound email spike	Low	Email	Suspicius activity	cont-jonawolcot JW Jonathan Wolcott	Open	Remediated	Jul 03, 2018 09:27 AM
	Suspicious user behavior	Low	Identity	Compromised account	jonathan.wollcott	Close	Running	Jul 03, 2018 09:28 AM



M365

https://security.microsoft.com

Microsoft 365 Security Center

Share   Comments and history   Actions and assistance

Incident #496

Edit incident name

🟥🟥🟥 High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox   Suspicius activity
Persistence   Credential Theft
Compromised account   Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

Duration
00H : 03M : 23S

Dashboard > Incident

6 active alerts

🟥 High (1)   🟧 Medium (3)   🟨 Low (2)   ⬜ Informational (0)

Related evidence

Machines	Users	Mailboxes	Files	Processes	IPs	Applications	Servicess	Persistence methods
3	4	213	9	4	1	0	0	1

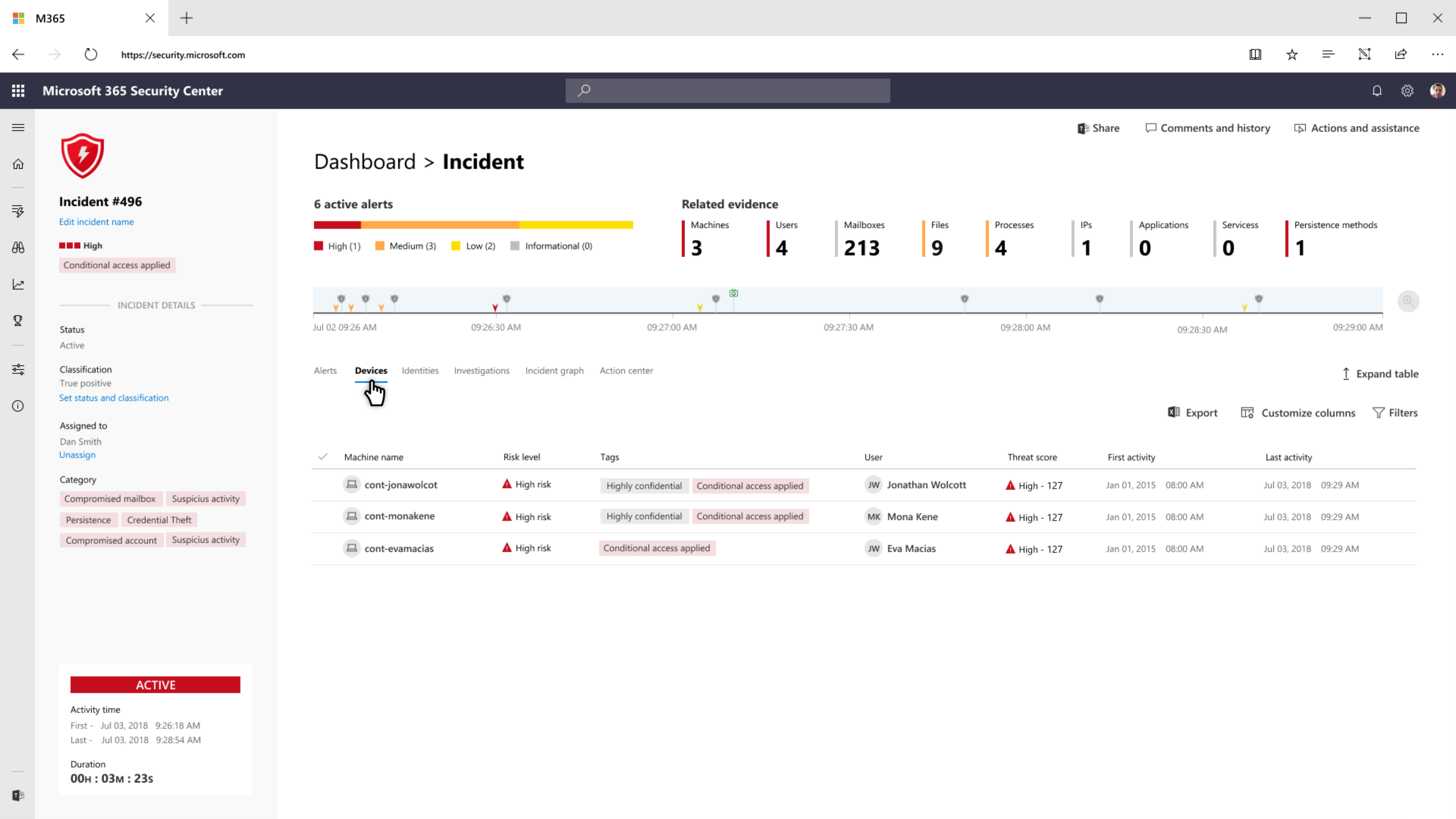
Jul 02 09:26 AM   09:26:30 AM   09:27:00 AM   09:27:30 AM   09:28:00 AM   09:28:30 AM   09:29:00 AM

Alerts   Devices   Identities   Investigations   Incident graph   Action center

Expand table

Export   Customize columns   Filters

✓	Title	Severity ↓	Detection source	Category	Alerted entity	Status	Investigation state	Last activity
	Possible compromised account	Medium	Email	Compromised mailbox	jonathan.wollcott	Open	Running	Jul 03, 2018 09:26 AM
✓	Suspicious PowerShell	Medium	Device	Suspicius activity	cont-jonawolcot JW Jonathan Wolcott	Open	Running	Jul 03, 2018 09:26 AM
	Suspect scheduled task	Medium	Device	Persistence	3 Machines 4 Users	Open	Running	Jul 03, 2018 09:26 AM
	Active credential theft tool	High	Device	Credential Theft	cont-jonawolcot JW Jonathan Wolcott	Open	Running	Jul 03, 2018 09:26 AM
	Outbound email spike	Low	Email	Suspicius activity	cont-jonawolcot JW Jonathan Wolcott	Open	Remediated	Jul 03, 2018 09:27 AM
	Suspicious user behavior	Low	Identity	Compromised account	jonathan.wollcott	Close	Running	Jul 03, 2018 09:28 AM



M365

https://security.microsoft.com

Microsoft 365 Security Center

Share | Comments and history | Actions and assistance

Incident #496

Edit incident name

🟥🟥🟥 High

Conditional access applied

INCIDENT DETAILS

Status

Active

Classification

True positive

Set status and classification

Assigned to

Dan Smith

Unassign

Category

Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

Activity time

First - Jul 03, 2018 9:26:18 AM

Last - Jul 03, 2018 9:28:54 AM

Duration

00H : 03M : 23S

Dashboard > Incident

6 active alerts

🟥 High (1) 🟧 Medium (3) 🟨 Low (2) ⬜ Informational (0)

Related evidence

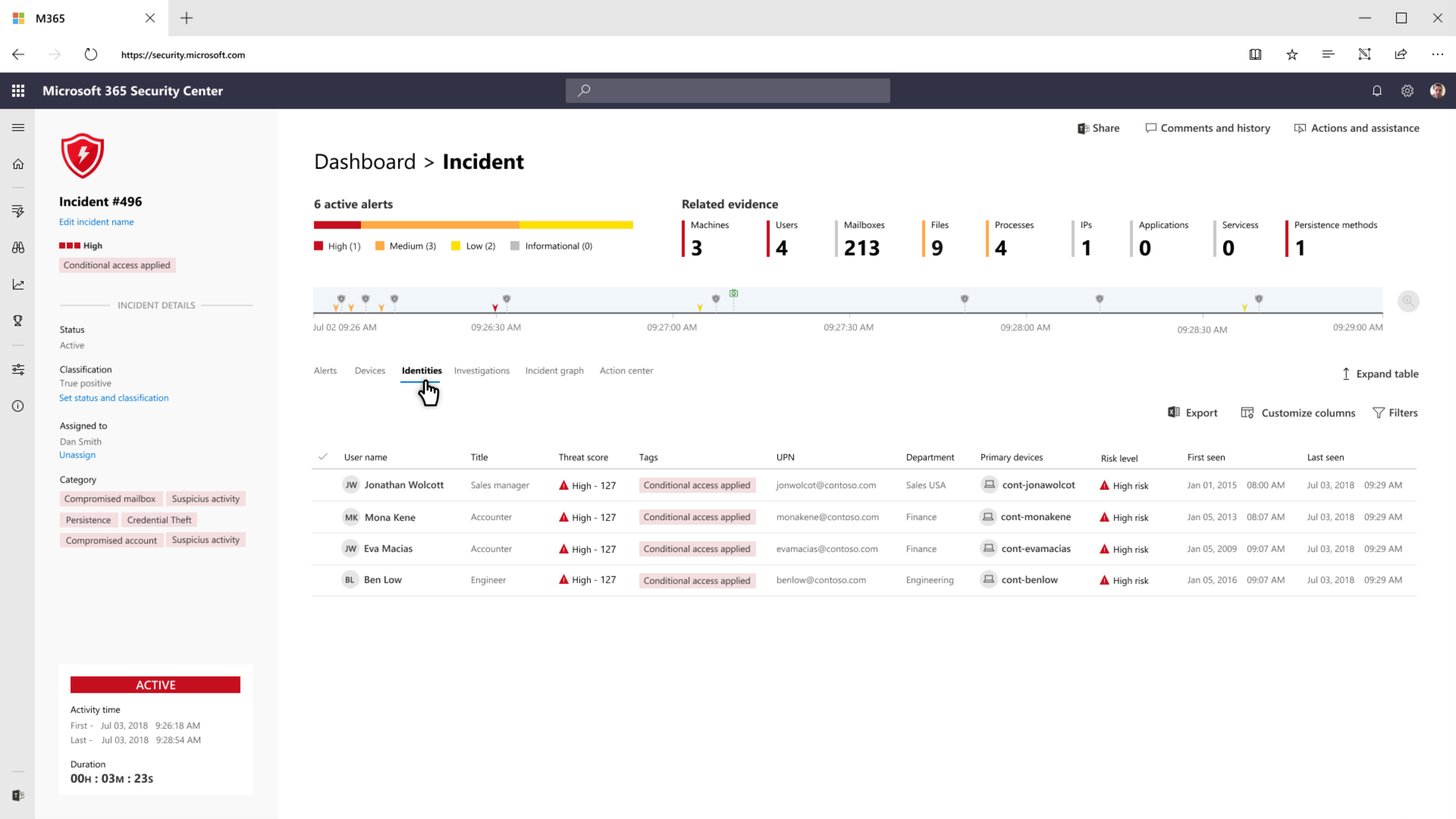
Machines	Users	Mailboxes	Files	Processes	IPs	Applications	Servicess	Persistence methods
3	4	213	9	4	1	0	0	1

Alerts | **Devices** | Identities | Investigations | Incident graph | Action center

Expand table

Export | Customize columns | Filters

✓	Machine name	Risk level	Tags	User	Threat score	First activity	Last activity
	cont-jonawolcot	High risk	Highly confidential Conditional access applied	JW Jonathan Wolcott	High - 127	Jan 01, 2015 08:00 AM	Jul 03, 2018 09:29 AM
	cont-monakene	High risk	Highly confidential Conditional access applied	MK Mona Kene	High - 127	Jan 01, 2015 08:00 AM	Jul 03, 2018 09:29 AM
	cont-evamacias	High risk	Conditional access applied	JW Eva Macias	High - 127	Jan 01, 2015 08:00 AM	Jul 03, 2018 09:29 AM



Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

Duration
00H : 03M : 23S

Dashboard > **Incident**

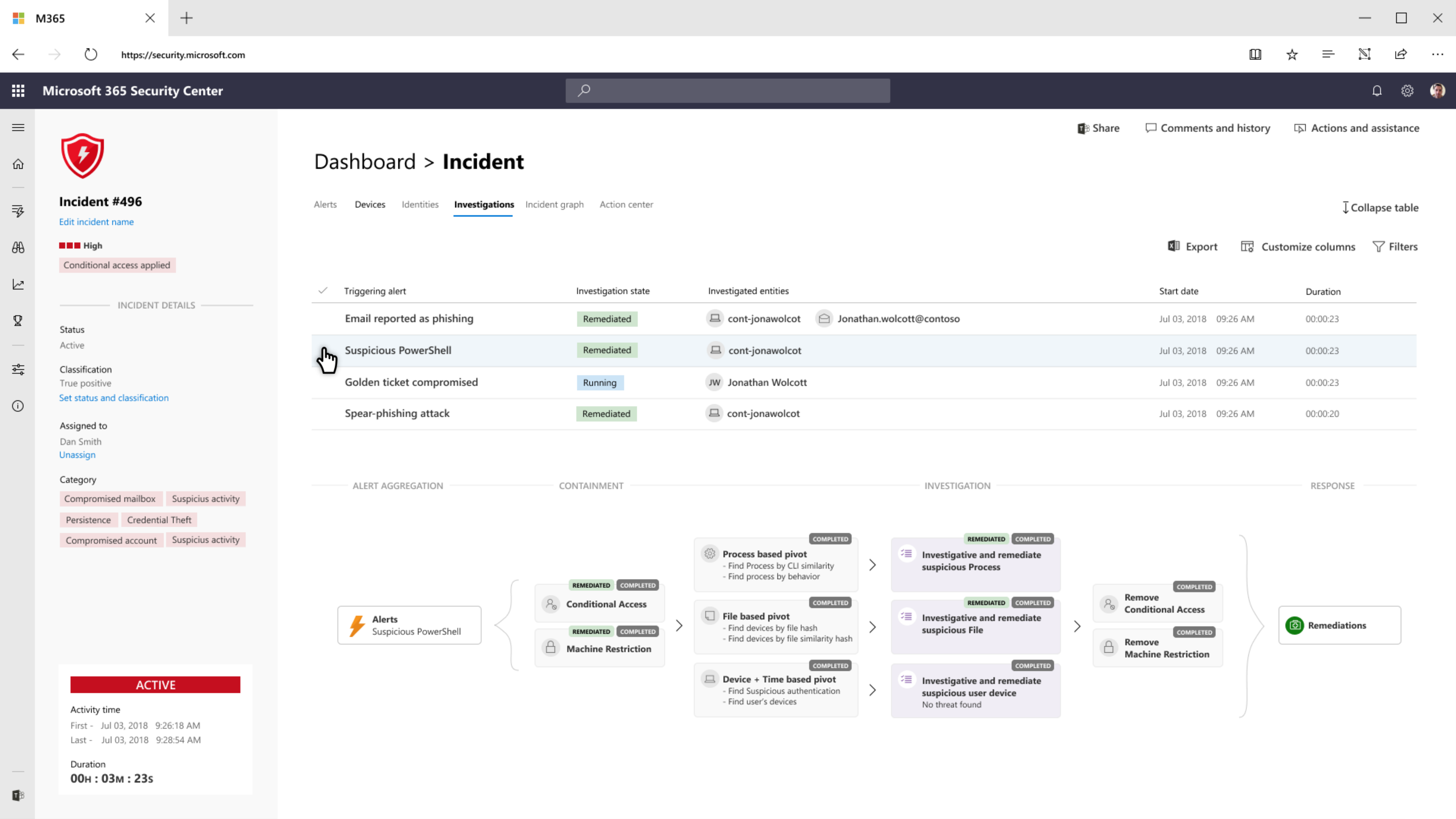
6 active alerts

🟥 High (1) 🟧 Medium (3) 🟨 Low (2) ⬜ Informational (0)

Related evidence

Machines	Users	Mailboxes	Files	Processes	IPs	Applications	Servicess	Persistence methods
3	4	213	9	4	1	0	0	1

User name	Title	Threat score	Tags	UPN	Department	Primary devices	Risk level	First seen	Last seen
JW Jonathan Wolcott	Sales manager	High - 127	Conditional access applied	jonwolcot@contoso.com	Sales USA	cont-jonawolcot	High risk	Jan 01, 2015 08:00 AM	Jul 03, 2018 09:29 AM
MK Mona Kene	Accounter	High - 127	Conditional access applied	monakene@contoso.com	Finance	cont-monakene	High risk	Jan 05, 2013 08:07 AM	Jul 03, 2018 09:29 AM
JW Eva Macias	Accounter	High - 127	Conditional access applied	evamacias@contoso.com	Finance	cont-evamacias	High risk	Jan 05, 2009 09:07 AM	Jul 03, 2018 09:29 AM
BL Ben Low	Engineer	High - 127	Conditional access applied	benlow@contoso.com	Engineering	cont-benlow	High risk	Jan 05, 2016 09:07 AM	Jul 03, 2018 09:29 AM



Dashboard > **Incident**

Incident #496

Edit incident name

🟥🟥🟥 High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

Duration
00H : 03M : 23S

✓	Triggering alert	Investigation state	Investigated entities	Start date	Duration
	Email reported as phishing	Remediated	cont-jonawolcot Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
	Suspicious PowerShell	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
	Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
	Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20

ALERT AGGREGATION — CONTAINMENT — INVESTIGATION — RESPONSE

Alerts
Suspicious PowerShell

REMEDIATED COMPLETED
Conditional Access

REMEDIATED COMPLETED
Machine Restriction

COMPLETED
Process based pivot
- Find Process by CLI similarity
- Find process by behavior

COMPLETED
File based pivot
- Find devices by file hash
- Find devices by file similarity hash

COMPLETED
Device + Time based pivot
- Find Suspicious authentication
- Find user's devices

REMEDIATED COMPLETED
Investigative and remediate suspicious Process

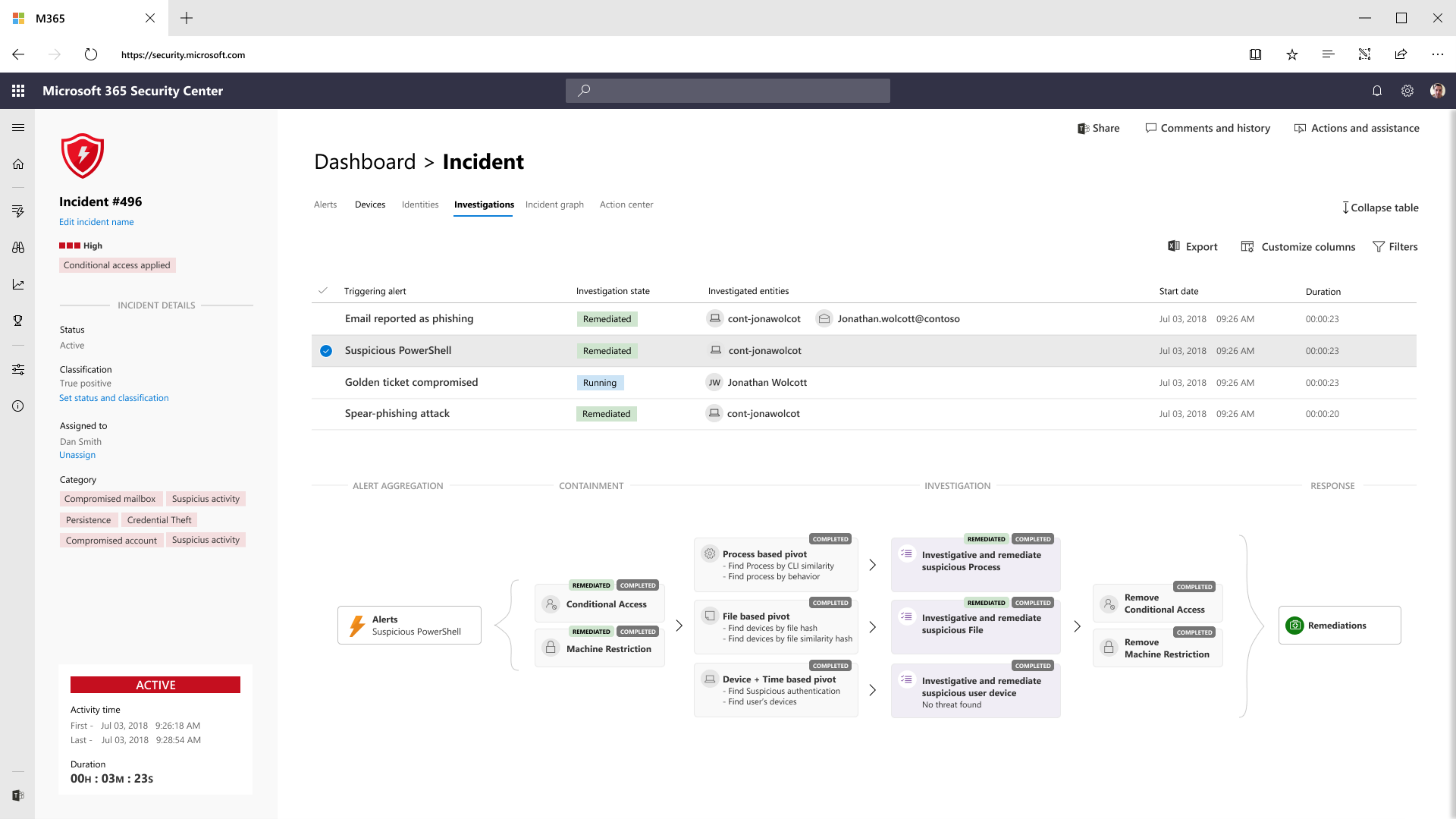
REMEDIATED COMPLETED
Investigative and remediate suspicious File

COMPLETED
Investigative and remediate suspicious user device
No threat found

COMPLETED
Remove Conditional Access

COMPLETED
Remove Machine Restriction

Remediations



M365

https://security.microsoft.com

Microsoft 365 Security Center

Share Comments and history Actions and assistance

Dashboard > **Incident**

Alerts Devices Identities **Investigations** Incident graph Action center

Collapse table

Export Customize columns Filters

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox Suspicius activity
Persistence Credential Theft
Compromised account Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

Duration
00H : 03M : 23S

✓	Triggering alert	Investigation state	Investigated entities	Start date	Duration
	Email reported as phishing	Remediated	cont-jonawolcot Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
✓	Suspicious PowerShell	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
	Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
	Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20

ALERT AGGREGATION CONTAINMENT INVESTIGATION RESPONSE

Alerts
Suspicious PowerShell

REMEDIATED COMPLETED
Conditional Access

REMEDIATED COMPLETED
Machine Restriction

COMPLETED
Process based pivot
- Find Process by CLI similarity
- Find process by behavior

COMPLETED
File based pivot
- Find devices by file hash
- Find devices by file similarity hash

COMPLETED
Device + Time based pivot
- Find Suspicious authentication
- Find user's devices

REMEDIATED COMPLETED
Investigative and remediate suspicious Process

REMEDIATED COMPLETED
Investigative and remediate suspicious File

COMPLETED
Investigative and remediate suspicious user device
No threat found

COMPLETED
Remove Conditional Access

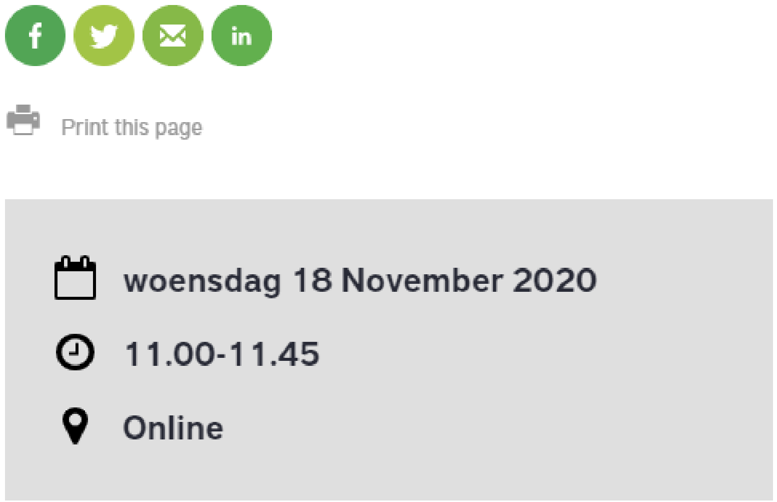
COMPLETED
Remove Machine Restriction

Remediations

INSPIRE

Event
Hou grip op uw documenten met Azure Information Protection

https://www.realdolmen.com/nl/webinar-azure-information-protection



Print this page

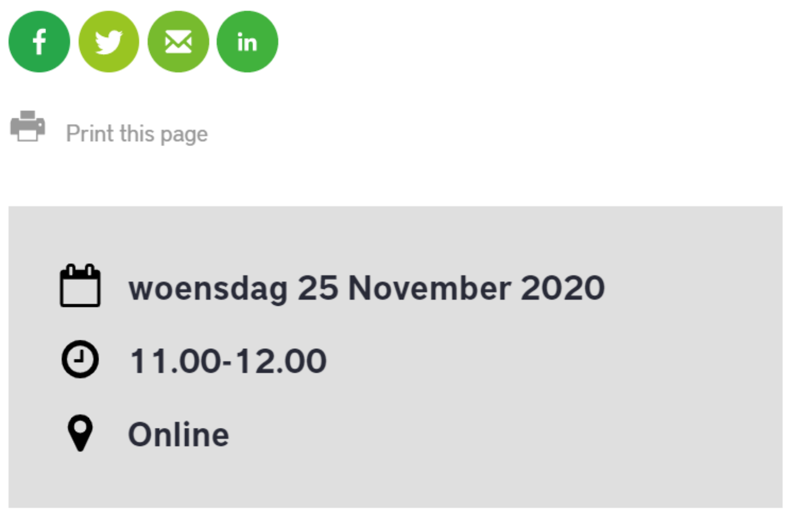
woensdag 18 November 2020

11.00-11.45

Online

Event
Simplify and Delegate Office 365 Management with Role-Based Access Control, Automation and Hybrid Support

https://www.realdolmen.com/nl/coreview

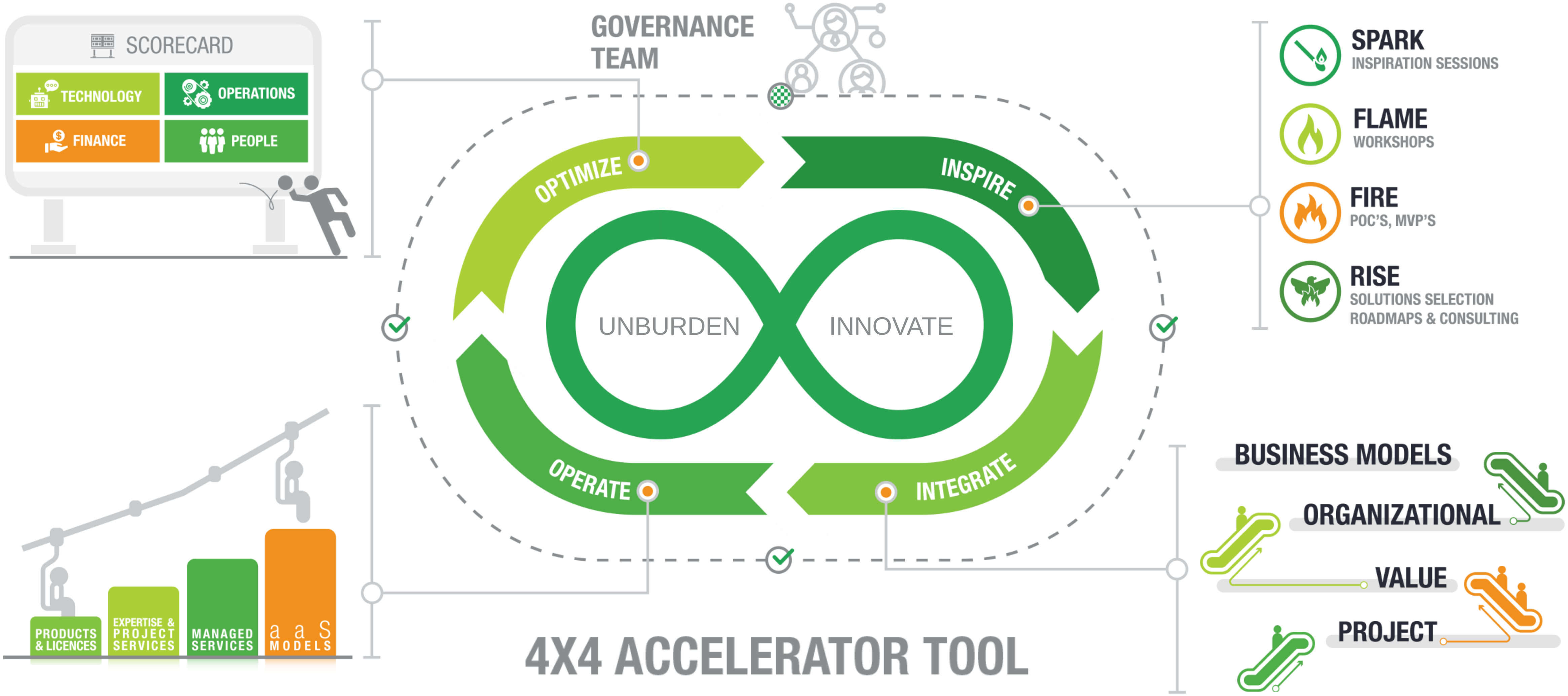


woensdag 25 November 2020

11.00-12.00

Online

How can we help you to **accelerate** your Digital Transformation **into the Digital Flow?**



SCORECARD

TECHNOLOGY

OPERATIONS

FINANCE

PEOPLE

GOVERNANCE TEAM

SPARK
INSPIRATION SESSIONS

FLAME
WORKSHOPS

FIRE
POC'S, MVP'S

RISE
SOLUTIONS SELECTION
ROADMAPS & CONSULTING

OPTIMIZE

INSPIRE

UNBURDEN

INNOVATE

OPERATE

INTEGRATE

PRODUCTS & LICENCES

EXPERTISE & PROJECT SERVICES

MANAGED SERVICES

aaS MODELS

BUSINESS MODELS

ORGANIZATIONAL

VALUE

PROJECT

4X4 ACCELERATOR TOOL

To get there, together

REALDOLMEN

HQ Realdolmen Huizingen
A. Vaucampslaan 42
B-1654 Huizingen
+32 2 801 55 55

www.realdolmen.com