Microsoft

M365 Defender

Corina Feuerstein

Program Management Lead

M365 Defender

February 18, 2021

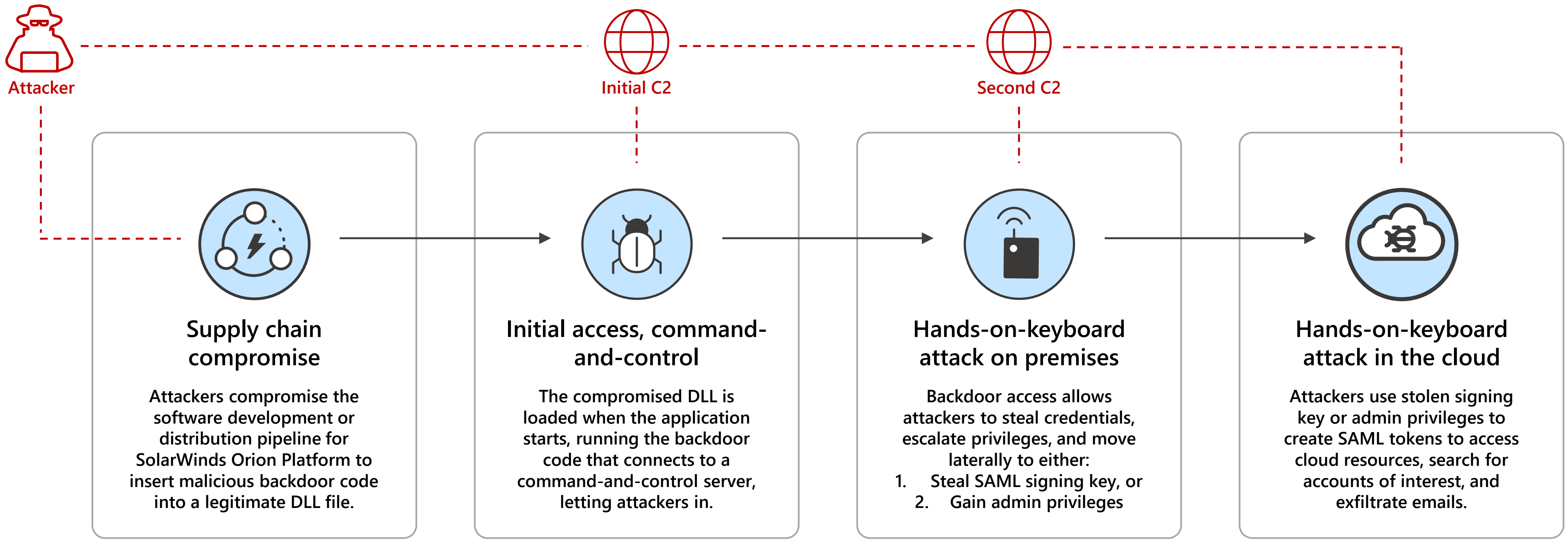
Solorigate Overview

Using Microsoft 365 Defender to Detect, Protect and Remediate

1. How the Solorigate attack happened
2. Detecting and blocking on-prem endpoint activity
3. Detecting identity compromise and pivot to cloud
4. Detecting and responding to suspect cloud app activity
5. Understanding org exposure and mitigations using Threat Analytics
6. Hunting across domains with Microsoft 365 Defender

Microsoft Security

Solorigate Overview



Supply chain compromise

Attackers compromise the software development or distribution pipeline for SolarWinds Orion Platform to insert malicious backdoor code into a legitimate DLL file.

Initial access, command-and-control

The compromised DLL is loaded when the application starts, running the backdoor code that connects to a command-and-control server, letting attackers in.

Hands-on-keyboard attack on premises

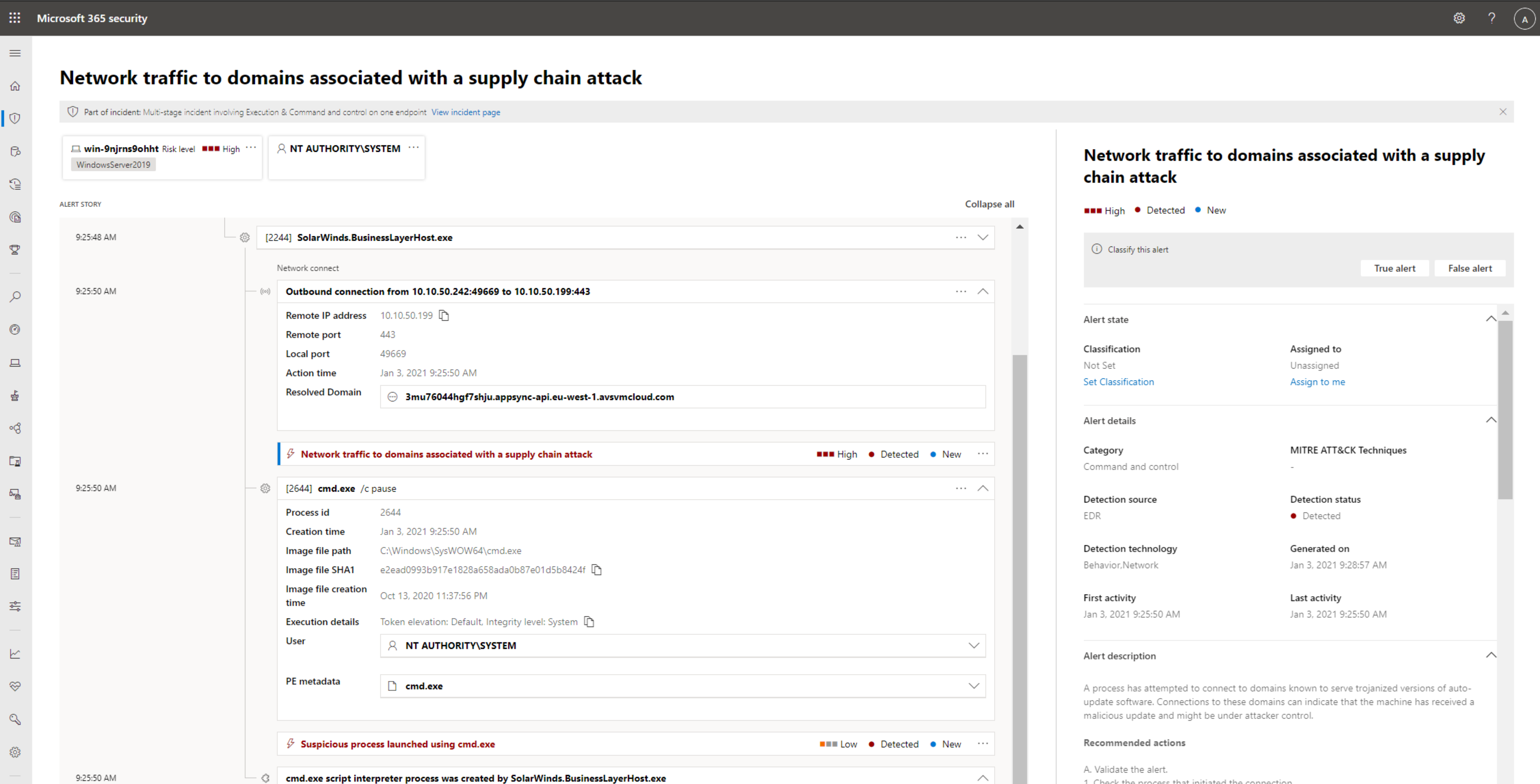
Backdoor access allows attackers to steal credentials, escalate privileges, and move laterally to either:

1. Steal SAML signing key, or
2. Gain admin privileges

Hands-on-keyboard attack in the cloud

Attackers use stolen signing key or admin privileges to create SAML tokens to access cloud resources, search for accounts of interest, and exfiltrate emails.

Malicious C2 communication blocked by MDE



Network traffic to domains associated with a supply chain attack

Part of incident: Multi-stage incident involving Execution & Command and control on one endpoint View incident page

win-9njrns9ohht Risk level ■■■ High ···
WindowsServer2019

NT AUTHORITY\SYSTEM ···

ALERT STORY

Collapse all

9:25:48 AM [2244] SolarWinds.BusinessLayerHost.exe

Network connect

9:25:50 AM Outbound connection from 10.10.50.242:49669 to 10.10.50.199:443

Remote IP address	10.10.50.199
Remote port	443
Local port	49669
Action time	Jan 3, 2021 9:25:50 AM
Resolved Domain	3mu76044hgf7shju.appsync-api.eu-west-1.avsvmcloud.com

Network traffic to domains associated with a supply chain attack ■■■ High ● Detected ● New

9:25:50 AM [2644] cmd.exe /c pause

Process id	2644
Creation time	Jan 3, 2021 9:25:50 AM
Image file path	C:\Windows\SysWOW64\cmd.exe
Image file SHA1	e2ead0993b917e1828a658ada0b87e01d5b8424f
Image file creation time	Oct 13, 2020 11:37:56 PM
Execution details	Token elevation: Default, Integrity level: System
User	NT AUTHORITY\SYSTEM
PE metadata	cmd.exe

Suspicious process launched using cmd.exe ■■■ Low ● Detected ● New

9:25:50 AM cmd.exe script interpreter process was created by SolarWinds.BusinessLayerHost.exe

Network traffic to domains associated with a supply chain attack

■■■ High ● Detected ● New

Classify this alert

True alert | False alert

Alert state

Classification	Assigned to
Not Set	Unassigned
Set Classification	Assign to me

Alert details

Category	MITRE ATT&CK Techniques
Command and control	-
Detection source	Detection status
EDR	● Detected
Detection technology	Generated on
Behavior,Network	Jan 3, 2021 9:28:57 AM
First activity	Last activity
Jan 3, 2021 9:25:50 AM	Jan 3, 2021 9:25:50 AM

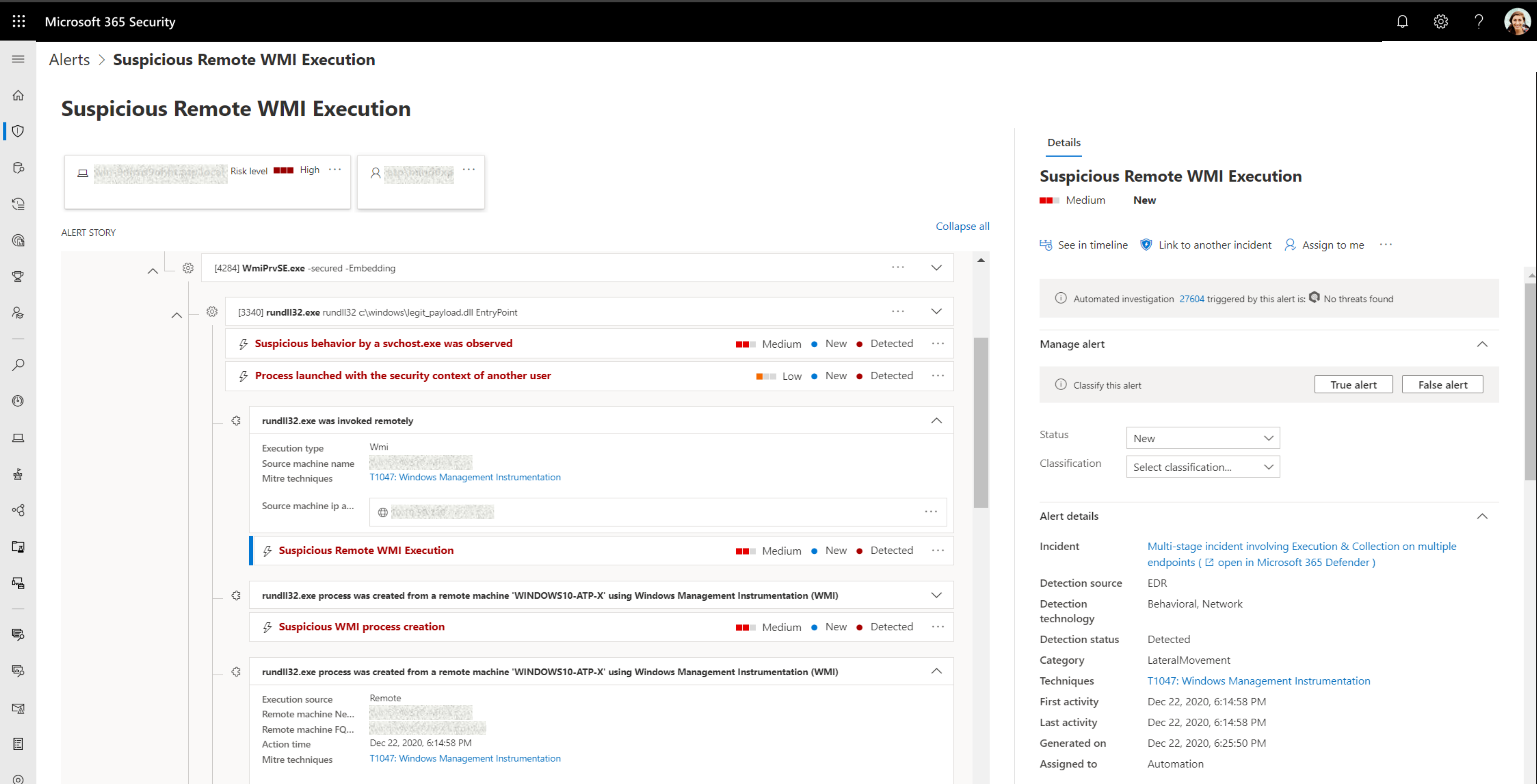
Alert description

A process has attempted to connect to domains known to serve trojanized versions of auto-update software. Connections to these domains can indicate that the machine has received a malicious update and might be under attacker control.

Recommended actions

A. Validate the alert.
1. Check the process that initiated the connection

Lateral movement detected by MDE



Microsoft 365 Security

Alerts > Suspicious Remote WMI Execution

Suspicious Remote WMI Execution

[redacted] Risk level ■■■ High ···

[redacted] ···

ALERT STORY

Collapse all

[4284] **WmiPrvSE.exe** -secured -Embedding

[3340] **rundll32.exe** rundll32 c:\windows\legit_payload.dll EntryPoint

Alert	Severity	Status	Detection status
Suspicious behavior by a svchost.exe was observed	Medium	New	Detected
Process launched with the security context of another user	Low	New	Detected

rundll32.exe was invoked remotely

Execution type	Wmi
Source machine name	[redacted]
Mitre techniques	T1047: Windows Management Instrumentation
Source machine ip a...	[redacted]

Alert	Severity	Status	Detection status
Suspicious Remote WMI Execution	Medium	New	Detected

rundll32.exe process was created from a remote machine 'WINDOWS10-ATP-X' using Windows Management Instrumentation (WMI)

Alert	Severity	Status	Detection status
Suspicious WMI process creation	Medium	New	Detected

rundll32.exe process was created from a remote machine 'WINDOWS10-ATP-X' using Windows Management Instrumentation (WMI)

Execution source	Remote
Remote machine Ne...	[redacted]
Remote machine FQ...	[redacted]
Action time	Dec 22, 2020, 6:14:58 PM
Mitre techniques	T1047: Windows Management Instrumentation

Details

Suspicious Remote WMI Execution

Medium **New**

See in timeline · Link to another incident · Assign to me ···

Automated investigation 27604 triggered by this alert is: No threats found

Manage alert

Classify this alert — True alert · False alert

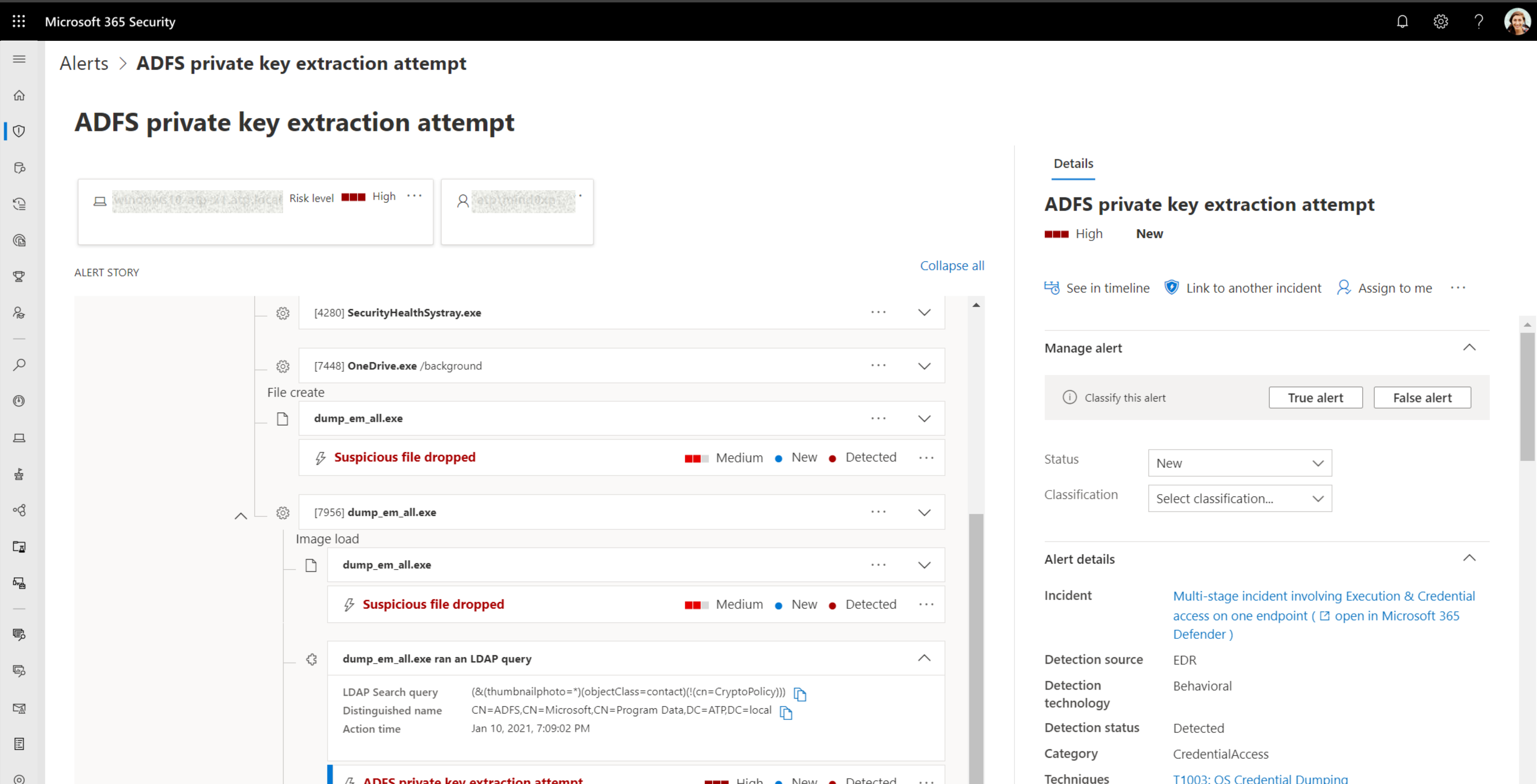
Status	New
Classification	Select classification...

Alert details

Incident	Multi-stage incident involving Execution & Collection on multiple endpoints (open in Microsoft 365 Defender)
Detection source	EDR
Detection technology	Behavioral, Network
Detection status	Detected
Category	LateralMovement
Techniques	T1047: Windows Management Instrumentation
First activity	Dec 22, 2020, 6:14:58 PM
Last activity	Dec 22, 2020, 6:14:58 PM
Generated on	Dec 22, 2020, 6:25:50 PM
Assigned to	Automation

ADFS compromise by stealing the SAML certificate key, or modifying federation trusts

Suspect ADFS key access



Microsoft 365 Security

Alerts > ADFS private key extraction attempt

ADFS private key extraction attempt

[redacted] Risk level ■■■ High ···

[redacted]

ALERT STORY

Collapse all

[4280] **SecurityHealthSystray.exe**

[7448] **OneDrive.exe** /background

File create

dump_em_all.exe

Suspicious file dropped ■■ Medium ● New ● Detected

[7956] **dump_em_all.exe**

Image load

dump_em_all.exe

Suspicious file dropped ■■ Medium ● New ● Detected

dump_em_all.exe ran an LDAP query

LDAP Search query	(&(thumbnailphoto=*)(objectClass=contact)(!(cn=CryptoPolicy)))
Distinguished name	CN=ADFS,CN=Microsoft,CN=Program Data,DC=ATP,DC=local
Action time	Jan 10, 2021, 7:09:02 PM

ADFS private key extraction attempt ■■■ High ● New ● Detected

Details

ADFS private key extraction attempt

■■■ High **New**

See in timeline · Link to another incident · Assign to me

Manage alert

Classify this alert True alert False alert

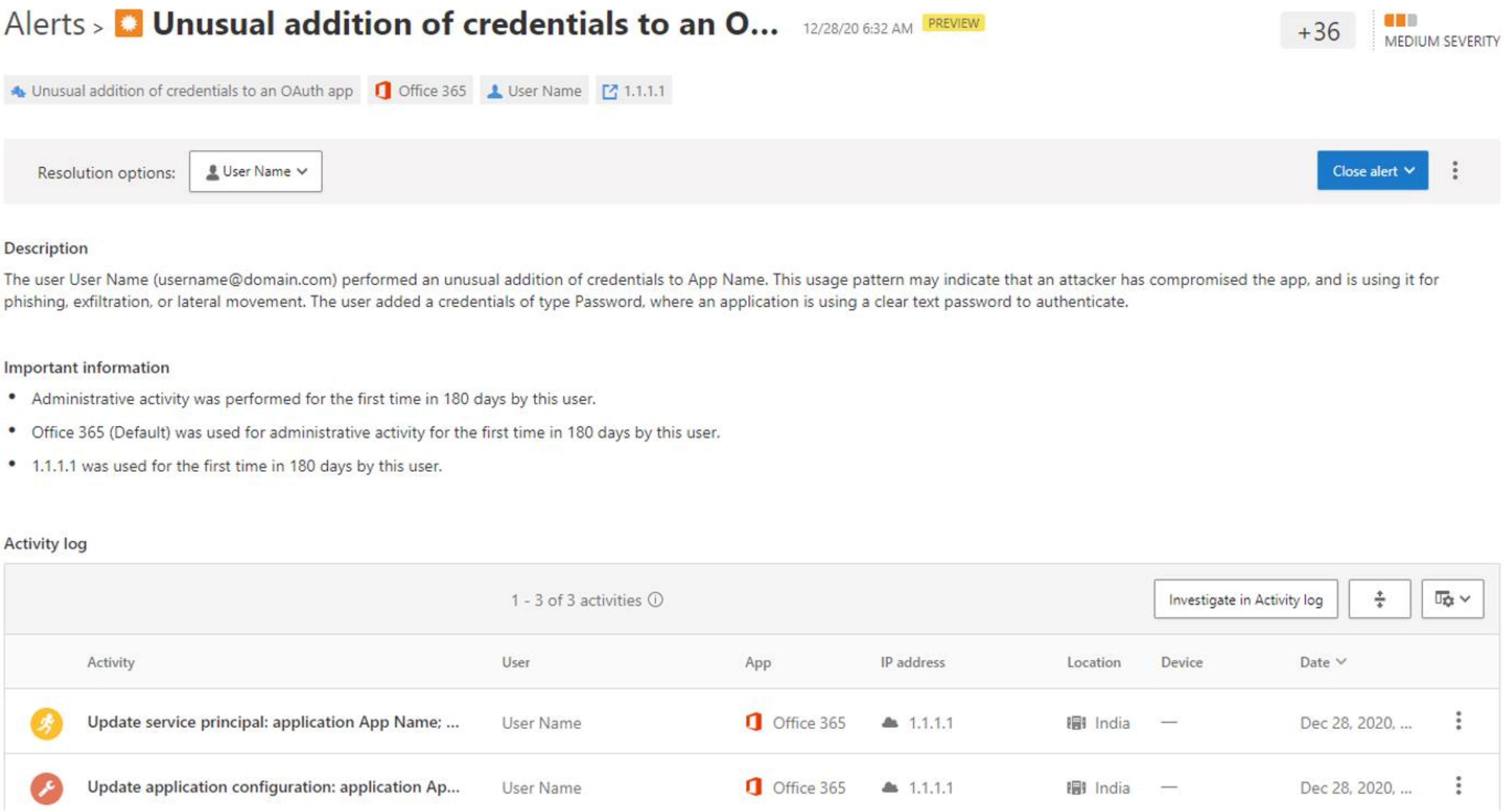
Status	New
Classification	Select classification...

Alert details

Incident	Multi-stage incident involving Execution & Credential access on one endpoint (open in Microsoft 365 Defender)
Detection source	EDR
Detection technology	Behavioral
Detection status	Detected
Category	CredentialAccess
Techniques	T1003: OS Credential Dumping

Use forged SAML tokens to persist in the cloud, access cloud resources, and exfiltrate email.

Unusual manipulation of Oauth app detected by MCAS



Alerts > Unusual addition of credentials to an O... 12/28/20 6:32 AM PREVIEW

+36 MEDIUM SEVERITY

Unusual addition of credentials to an OAuth app | Office 365 | User Name | 1.1.1.1

Resolution options: User Name

Description

The user User Name (username@domain.com) performed an unusual addition of credentials to App Name. This usage pattern may indicate that an attacker has compromised the app, and is using it for phishing, exfiltration, or lateral movement. The user added a credentials of type Password, where an application is using a clear text password to authenticate.

Important information

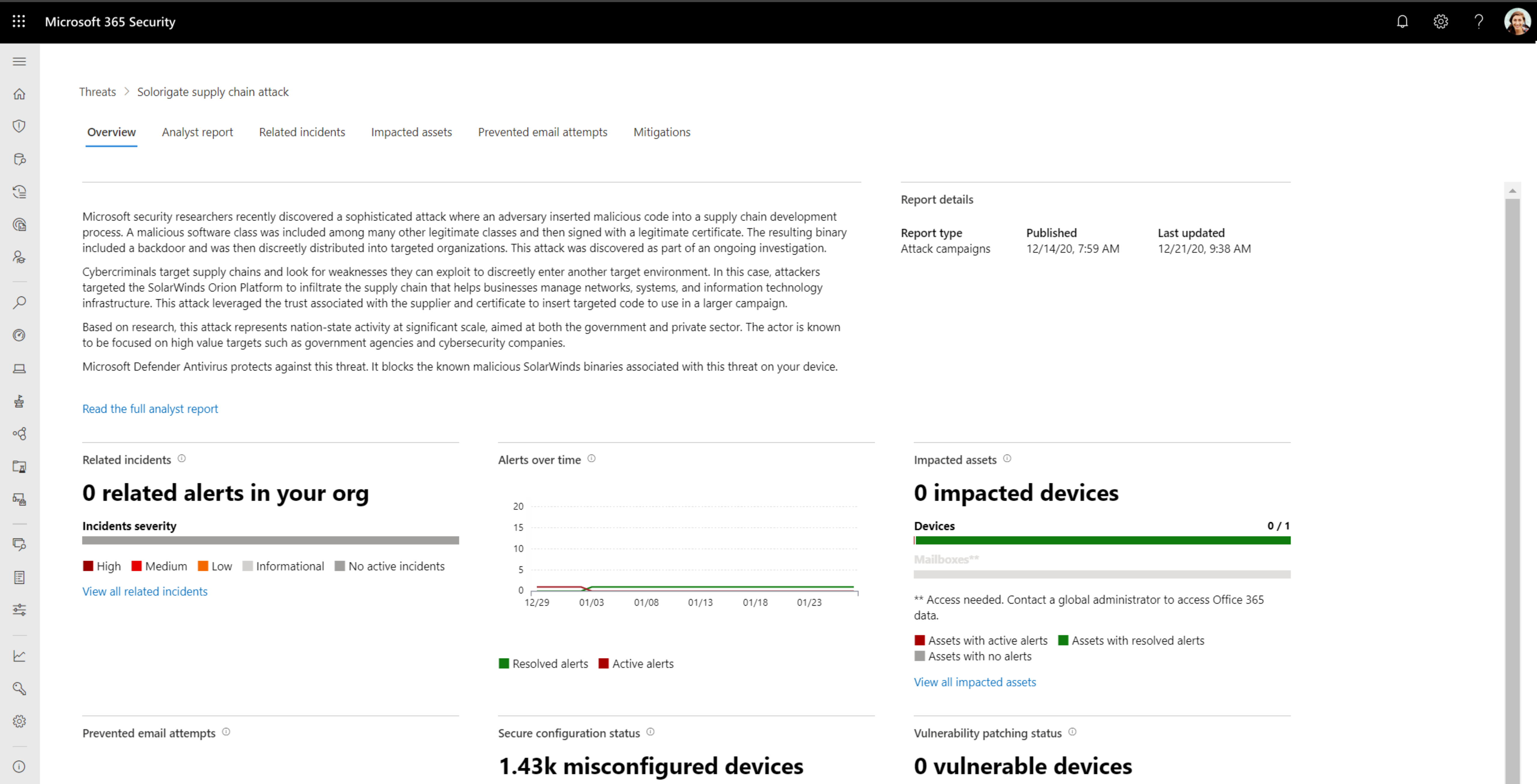
- Administrative activity was performed for the first time in 180 days by this user.
- Office 365 (Default) was used for administrative activity for the first time in 180 days by this user.
- 1.1.1.1 was used for the first time in 180 days by this user.

Activity log

1 - 3 of 3 activities

Activity	User	App	IP address	Location	Device	Date
Update service principal: application App Name; ...	User Name	Office 365	1.1.1.1	India	—	Dec 28, 2020, ...
Update application configuration: application Ap...	User Name	Office 365	1.1.1.1	India	—	Dec 28, 2020, ...

Threat Analytics Solorigate Report



Threats > Solorigate supply chain attack

Microsoft security researchers recently discovered a sophisticated attack where an adversary inserted malicious code into a supply chain development process. A malicious software class was included among many other legitimate classes and then signed with a legitimate certificate. The resulting binary included a backdoor and was then discreetly distributed into targeted organizations. This attack was discovered as part of an ongoing investigation.

Cybercriminals target supply chains and look for weaknesses they can exploit to discreetly enter another target environment. In this case, attackers targeted the SolarWinds Orion Platform to infiltrate the supply chain that helps businesses manage networks, systems, and information technology infrastructure. This attack leveraged the trust associated with the supplier and certificate to insert targeted code to use in a larger campaign.

Based on research, this attack represents nation-state activity at significant scale, aimed at both the government and private sector. The actor is known to be focused on high value targets such as government agencies and cybersecurity companies.

Microsoft Defender Antivirus protects against this threat. It blocks the known malicious SolarWinds binaries associated with this threat on your device.

Read the full analyst report

Report details

Report type	Published	Last updated
Attack campaigns	12/14/20, 7:59 AM	12/21/20, 9:38 AM

Related incidents ⓘ

0 related alerts in your org

Incidents severity

🟥 High 🟥 Medium 🟧 Low ⬜ Informational ⬜ No active incidents

View all related incidents

Alerts over time ⓘ

🟩 Resolved alerts 🟥 Active alerts

Impacted assets ⓘ

0 impacted devices

Devices **0 / 1**

Mailboxes**

** Access needed. Contact a global administrator to access Office 365 data.

🟥 Assets with active alerts 🟩 Assets with resolved alerts
⬜ Assets with no alerts

View all impacted assets

Prevented email attempts ⓘ

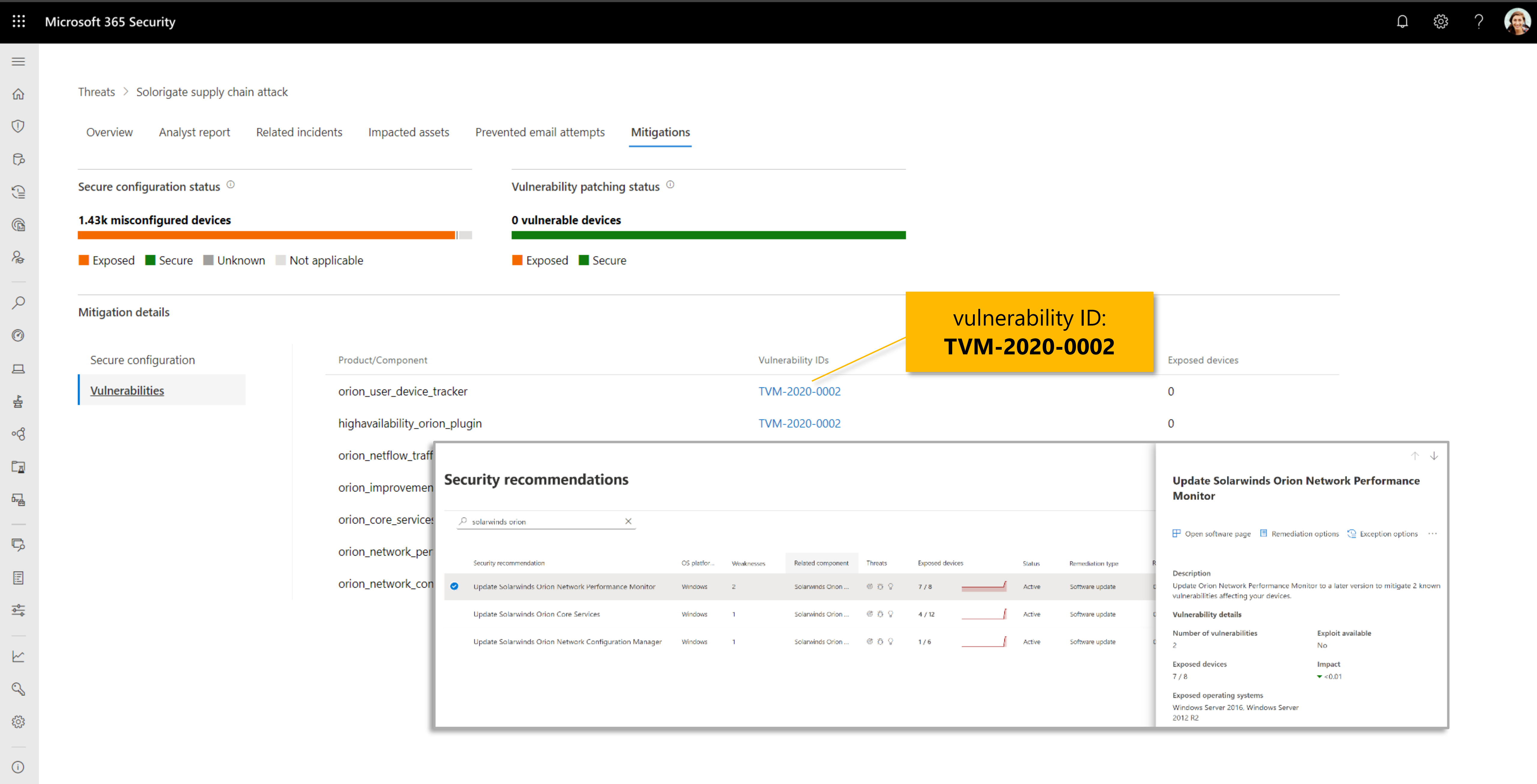
Secure configuration status ⓘ

1.43k misconfigured devices

Vulnerability patching status ⓘ

0 vulnerable devices

Threat Analytics Solorigate Report



Secure configuration status

1.43k misconfigured devices

🟧 Exposed 🟩 Secure ▨ Unknown □ Not applicable

Vulnerability patching status

0 vulnerable devices

🟧 Exposed 🟩 Secure

Mitigation details

Secure configuration

Vulnerabilities

Product/Component	Vulnerability IDs	Exposed devices
orion_user_device_tracker	TVM-2020-0002	0
highavailability_orion_plugin	TVM-2020-0002	0
orion_netflow_traff		
orion_improvemen		
orion_core_service		
orion_network_per		
orion_network_con		

vulnerability ID:
TVM-2020-0002

Security recommendations

solarwinds orion

	Security recommendation	OS platfor...	Weaknesses	Related component	Threats	Exposed devices	Status	Remediation type
✓	Update Solarwinds Orion Network Performance Monitor	Windows	2	Solarwinds Orion ...		7 / 8	Active	Software update
	Update Solarwinds Orion Core Services	Windows	1	Solarwinds Orion ...		4 / 12	Active	Software update
	Update Solarwinds Orion Network Configuration Manager	Windows	1	Solarwinds Orion ...		1 / 6	Active	Software update

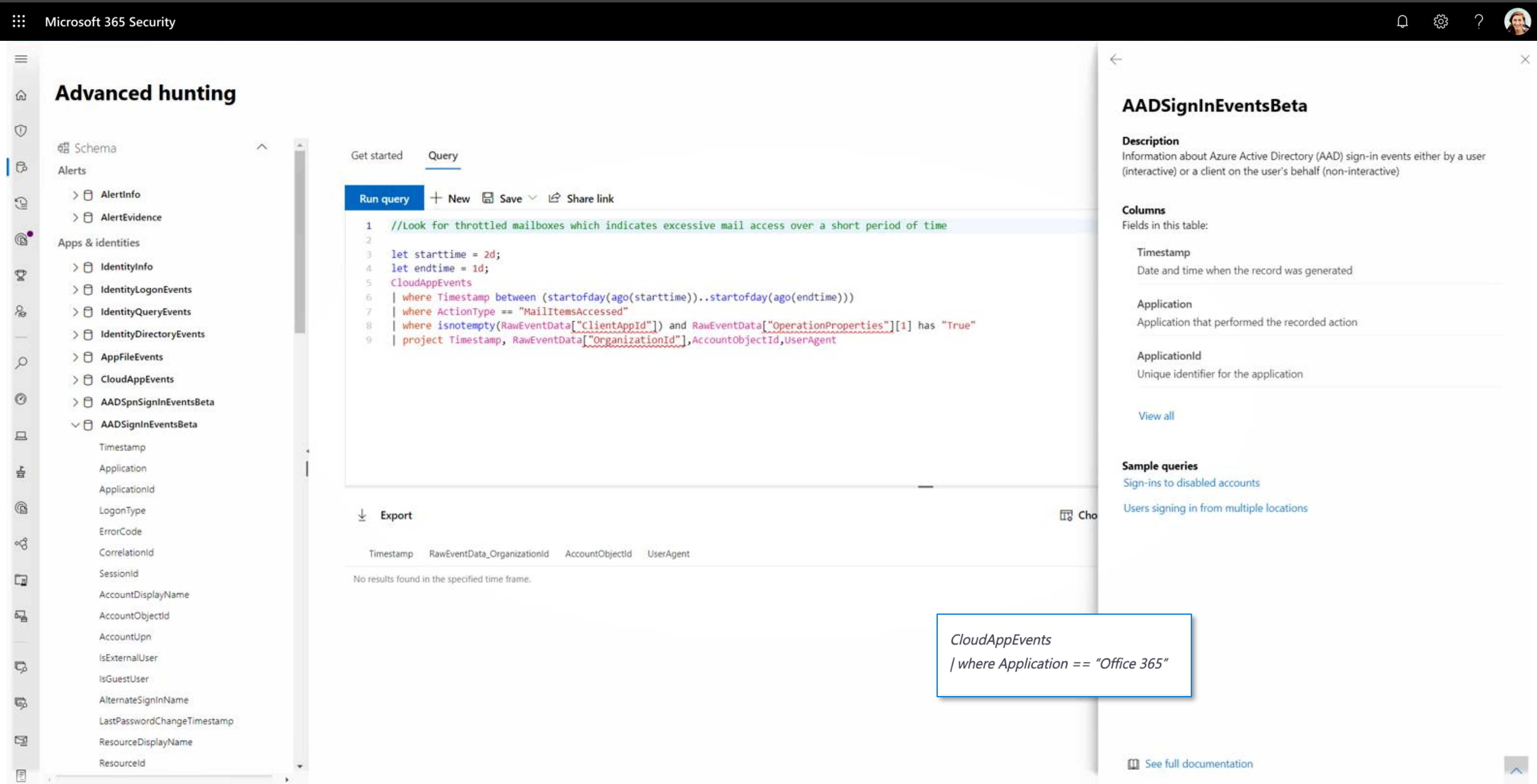
Update Solarwinds Orion Network Performance Monitor

Description
Update Orion Network Performance Monitor to a later version to mitigate 2 known vulnerabilities affecting your devices.

Vulnerability details

Number of vulnerabilities: 2
Exploit available: No
Exposed devices: 7 / 8
Impact: ▼ <0.01
Exposed operating systems: Windows Server 2016, Windows Server 2012 R2

New Azure AD and Cloud App data in Advanced Hunting



Microsoft 365 Security

Advanced hunting

Schema

Alerts
- AlertInfo
- AlertEvidence

Apps & identities
- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- AppFileEvents
- CloudAppEvents
- AADSpnSignInEventsBeta
- AADSignInEventsBeta
  - Timestamp
  - Application
  - ApplicationId
  - LogonType
  - ErrorCode
  - CorrelationId
  - SessionId
  - AccountDisplayName
  - AccountObjectId
  - AccountUpn
  - IsExternalUser
  - IsGuestUser
  - AlternateSignInName
  - LastPasswordChangeTimestamp
  - ResourceDisplayName
  - ResourceId

Get started | Query

Run query | New | Save | Share link

```
//Look for throttled mailboxes which indicates excessive mail access over a short period of time

let starttime = 2d;
let endtime = 1d;
CloudAppEvents
| where Timestamp between (startofday(ago(starttime))..startofday(ago(endtime)))
| where ActionType == "MailItemsAccessed"
| where isnotempty(RawEventData["ClientAppId"]) and RawEventData["OperationProperties"][1] has "True"
| project Timestamp, RawEventData["OrganizationId"],AccountObjectId,UserAgent
```

Export | Cho

Timestamp	RawEventData_OrganizationId	AccountObjectId	UserAgent

No results found in the specified time frame.

AADSignInEventsBeta

Description
Information about Azure Active Directory (AAD) sign-in events either by a user (interactive) or a client on the user's behalf (non-interactive)

Columns
Fields in this table:

Timestamp
Date and time when the record was generated

Application
Application that performed the recorded action

ApplicationId
Unique identifier for the application

View all

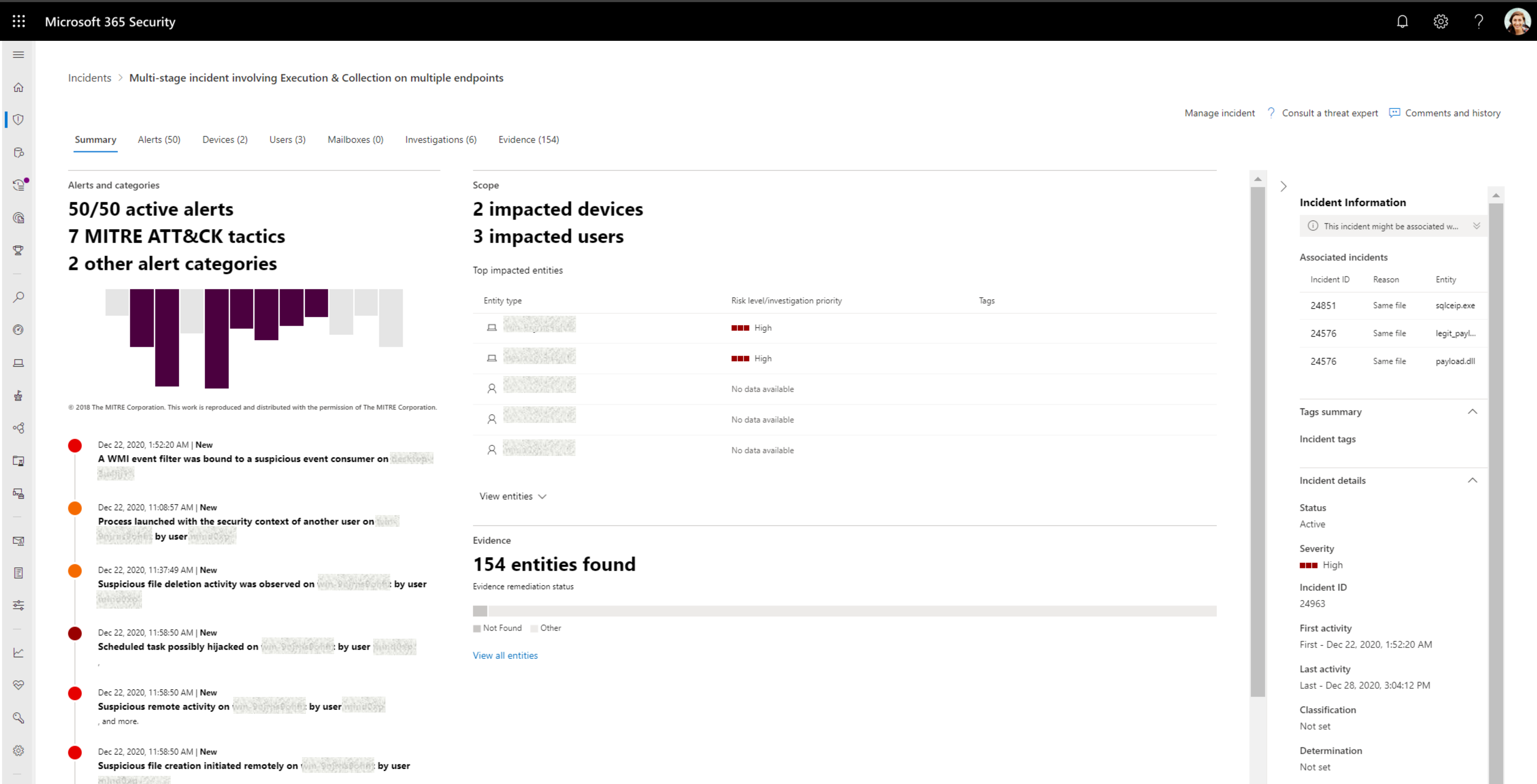
Sample queries
Sign-ins to disabled accounts

Users signing in from multiple locations

See full documentation

CloudAppEvents
| where Application == "Office 365"

Investigating Solorigate related alerts and incidents in Microsoft 365 Defender



Microsoft 365 Security

Incidents > Multi-stage incident involving Execution & Collection on multiple endpoints

Manage incident | Consult a threat expert | Comments and history

Summary | Alerts (50) | Devices (2) | Users (3) | Mailboxes (0) | Investigations (6) | Evidence (154)

Alerts and categories

50/50 active alerts
7 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.

Dec 22, 2020, 1:52:20 AM | **New**
A WMI event filter was bound to a suspicious event consumer on [redacted]

Dec 22, 2020, 11:08:57 AM | **New**
Process launched with the security context of another user on [redacted] **by user** [redacted]

Dec 22, 2020, 11:37:49 AM | **New**
Suspicious file deletion activity was observed on [redacted] **by user** [redacted]

Dec 22, 2020, 11:58:50 AM | **New**
Scheduled task possibly hijacked on [redacted] **by user** [redacted]
,

Dec 22, 2020, 11:58:50 AM | **New**
Suspicious remote activity on [redacted] **by user** [redacted]
, and more.

Dec 22, 2020, 11:58:50 AM | **New**
Suspicious file creation initiated remotely on [redacted] **by user** [redacted]

Scope

2 impacted devices
3 impacted users

Top impacted entities

Entity type	Risk level/investigation priority	Tags
[redacted]	■■■ High	
[redacted]	■■■ High	
[redacted]	No data available	
[redacted]	No data available	
[redacted]	No data available	

View entities

Evidence

154 entities found

Evidence remediation status

■ Not Found ■ Other

View all entities

Incident Information

This incident might be associated w...

Associated incidents

Incident ID	Reason	Entity
24851	Same file	sqlceip.exe
24576	Same file	legit_payl...
24576	Same file	payload.dll

Tags summary

Incident tags

Incident details

Status
Active

Severity
■■■ High

Incident ID
24963

First activity
First - Dec 22, 2020, 1:52:20 AM

Last activity
Last - Dec 28, 2020, 3:04:12 PM

Classification
Not set

Determination
Not set

Solorigate Video Series

Next Steps

01. Watch the Solorigate Video series at this location

02. Visit Microsoft Security for more updates: www.microsoft.com/en-us/security/business

03. Read the blog posts on: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft