



# Azure Sentinel

**Pete Bryan**

高级工程师

Microsoft 威胁智能中心

2021 年 2 月 18 日

Solorigate 概述

# Microsoft Azure Sentinel 如何帮助你在整个企业中搜寻攻击者活动

01. 如何搜寻 Solorigate 攻击
02. 使用 Windows 事件日志和 Azure Sentinel
03. 在 Azure Sentinel 和 Microsoft Defender for Endpoint 中查找原始数据
04. 寻找窃取证书和 SAML 令牌的迹象
05. Microsoft 365 Defender 和 Sentinel 警报
06. 使用 Azure Sentinel 工作簿和 GitHub

# Azure Sentinel | Overview

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/) | Refresh | Last 14 days

- General
  - Overview
  - Logs
  - News & guides
- Threat management
  - Incidents
  - Workbooks
  - Hunting
  - Notebooks (Preview)
  - Entity behavior
  - Threat intelligence (Preview)
- Configuration
  - Data connectors
  - Analytics
  - Entity Settings (Preview)
  - Watchlist (Preview)
  - Playbooks
  - Community
  - Settings

50M ↑ 13.1M  
Events

1.2K ↑ 520  
Alerts

1.6K ↑ 936  
Incidents

Incidents by status

- New (1.6K)
- Active (6)
- Closed (True Positive) (1)
- Closed (False Positive) (1)

## Events and alerts over time



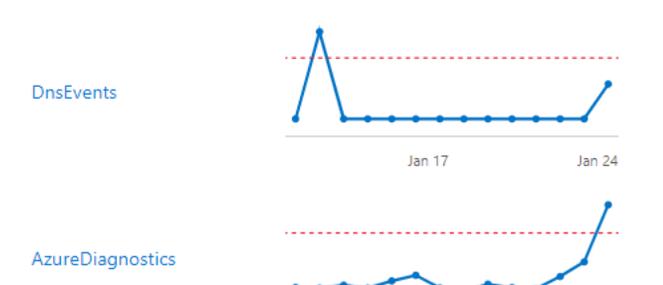
## Potential malicious events

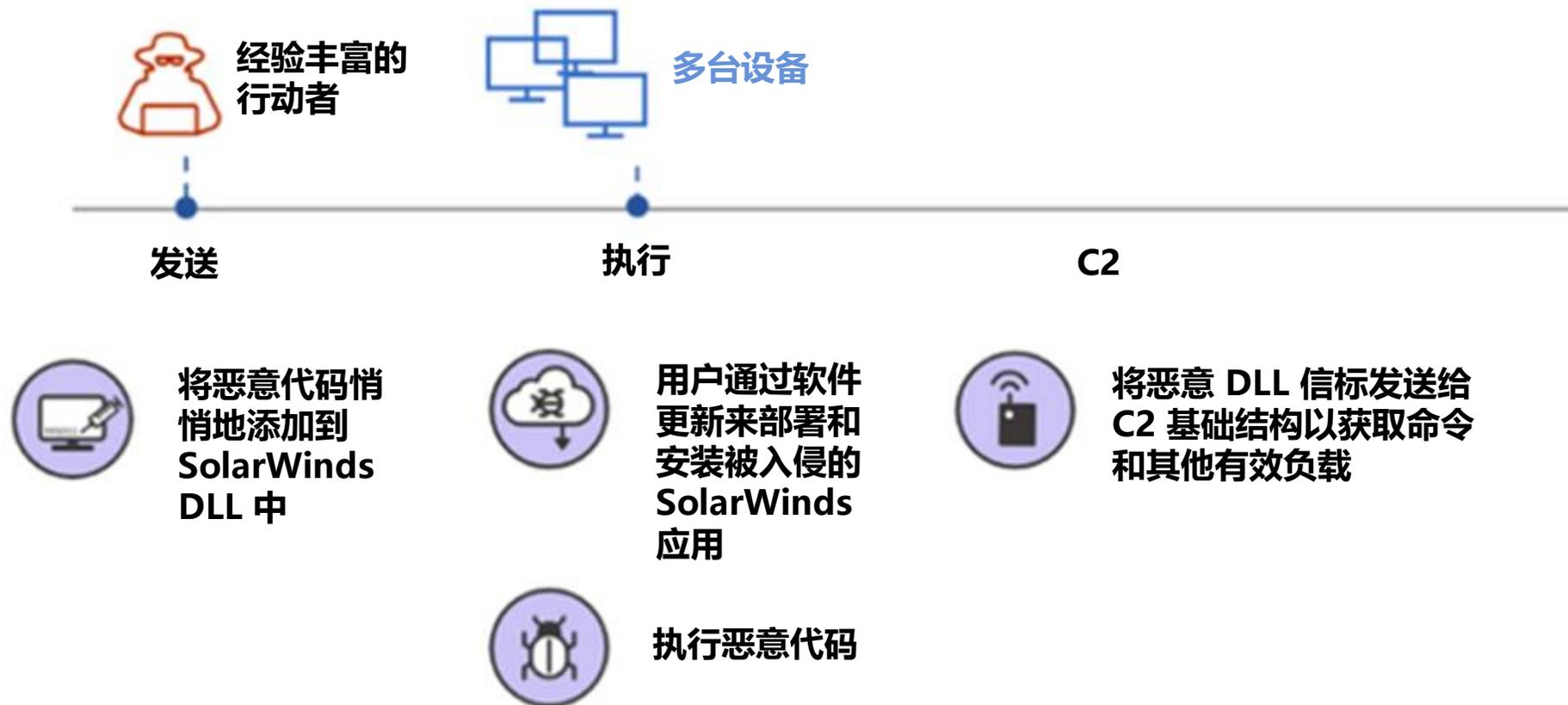


## Recent incidents

Severity	Incident Description	Count
Low	DDoS Attack mitigated for Public IP	1 Aler
High	DDoS Attack detected for Public IP	1 Aler
Medium	TI map IP entity to AzureActivity (enriched)	1 Aler
Medium	Time series anomaly detection for total v...	5 Aler
Low	DDoS Attack mitigated for Public IP	1 Aler

## Data source anomalies





Solorigate 供应链攻击图

# Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

- General
- Overview
- Logs**
- News & guides
- Threat management
  - Incidents
  - Workbooks
  - Hunting
  - Notebooks (Preview)
  - Entity behavior
  - Threat intelligence (Preview)
- Configuration
  - Data connectors
  - Analytics
  - Entity Settings (Preview)
  - Watchlist (Preview)
  - Playbooks
  - Community
  - Settings

**New Query 1\***

CyberSecuritySOC

Tables | Queries | Filter

Search

Filter | Group by: Solution

Collapse all

**Favorites**

You can add favorites by clicking on the ☆ icon

- Azure Monitor for VMs
- Azure Sentinel
- Azure Sentinel UEBA
- DNS Analytics (Preview)
- LogManagement
- Network Performance Monitor
- Security and Audit
- SecurityCenterFree
- SQL Vulnerability Assessment
- WindowsEventForwarding
- Custom Logs
- Functions

**Run** | Time range: Last 24 hours | Save | Copy link | New alert rule | Export | Pin to dashboard | Format query

```

13 (union isfuzzy=true
14 (
15 SecurityEvent
16 | where EventID == '4688'
17 | where NewProcessName has 'SolarWinds'
18 | extend MachineName = Computer , Process = NewProcessName
19 ),
20 (
21 DeviceProcessEvents
22 | where InitiatingProcessFolderPath has 'SolarWinds'
23 | extend MachineName = DeviceName , Process = InitiatingProcessFolderPath
24 )
25 )
26 | summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), make_set(Process) by MachineName
27
    
```

Results | Chart | Columns | Add bookmark | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 24 hours. 00:00.5 4 records

	MachineName	StartTime [UTC]	EndTime [UTC]	set_Process
>	SolWinds1	12/14/2020, 11:14:21.000 AM	12/14/2020, 11:21:41.000 AM	["c:\\program files (x86)\\solarwinds\\orion\\erlang\\erts-10.1\\bin\\erl.exe","c:\\program files (x86)\\sc...
>	SolWinds2	12/15/2020, 2:05:32.000 AM	12/15/2020, 2:05:32.000 AM	["c:\\program files (x86)\\solarwinds\\orion\\sqlexpress\\mssql14.solarwinds_orion\\mssql\\binn\\fdlau...
>	SolWinds3	12/7/2020, 4:48:29.000 PM	12/7/2020, 4:48:29.000 PM	["c:\\program files (x86)\\solarwinds\\orion\\sqlexpress\\mssql14.solarwinds_orion\\mssql\\binn\\fdlau...
>	SolWinds4	12/9/2020, 10:08:42.000 PM	12/9/2020, 10:08:42.000 PM	["c:\\program files (x86)\\solarwinds\\orion\\sqlexpress\\mssql14.solarwinds_orion\\mssql\\binn\\fdlau...

# Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/)

- General
- Overview
- Logs
- News & guides
- Threat management
  - Incidents
  - Workbooks
  - Hunting
  - Notebooks (Preview)
  - Entity behavior
  - Threat intelligence (Preview)
- Configuration
  - Data connectors
  - Analytics
  - Entity Settings (Preview)
  - Watchlist (Preview)
  - Playbooks
  - Community
  - Settings

New Query 1\*

CyberSecuritySOC

Run Time range: Last 24 hours Save Copy link New alert rule Export Pin to dashboard Format query

Tables Queries Filter

Search

Filter Group by: Solution

Collapse all

### Favorites

You can add favorites by clicking on the star icon

- Azure Monitor for VMs
- Azure Sentinel
- Azure Sentinel UEBA
- DNS Analytics (Preview)
- LogManagement
- Network Performance Monitor
- Security and Audit
- SecurityCenterFree
- SQL Vulnerability Assessment
- WindowsEventForwarding
- Custom Logs
- Functions

```

13 (union isfuzzy=true
14 (
15 SecurityEvent
16 | where EventID == '4688'
17 | where NewProcessName has 'SolarWinds'
18 | extend MachineName = Computer , Process = NewProcessName
19 ),
20 (
21 DeviceProcessEvents
22 | where InitiatingProcessFolderPath has 'SolarWinds'
23 | extend MachineName = DeviceName , Process = InitiatingProcessFolderPath
24 )
25 )
26 | summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), make_set(Process) by MachineName
27
28

```

Results Chart

Completed 00:03.4 0 records

**i** No query was selected  
 Type a query and place the cursor anywhere in the query.  
 A query can contain line breaks, but no blank lines.

# Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/)

New Query 1\*

CyberSecuritySOC

Run | Time range: Last 24 hours | Save | Copy link | New alert rule | Export | Pin to dashboard | Format query

- General
- Overview
- Logs
- News & guides
- Threat management
  - Incidents
  - Workbooks
  - Hunting
  - Notebooks (Preview)
  - Entity behavior
  - Threat intelligence (Preview)
- Configuration
  - Data connectors
  - Analytics
  - Entity Settings (Preview)
  - Watchlist (Preview)
  - Playbooks
  - Community
  - Settings

- Tables | Queries | Filter
- Search
- Filter | Group by: Solution
- Collapse all
- Favorites**
- You can add favorites by clicking on the ☆ icon
- Azure Monitor for VMs
  - Azure Sentinel
  - Azure Sentinel UEBA
  - DNS Analytics (Preview)
  - LogManagement
  - Network Performance Monitor
  - Security and Audit
  - SecurityCenterFree
  - SQL Vulnerability Assessment
  - WindowsEventForwarding
  - Custom Logs
  - Functions

```

8 (union isfuzzy=true
9   (Event
10    | where Source == "Microsoft-Windows-Sysmon"
11    | where EventID in (17,18)
12    | extend EvData = parse_xml(EventData)
13    | extend EventDetail = EvData.DataItem.EventData.Data
14    | extend NamedPipe = EventDetail.[5].["#text"]
15    | extend ProcessDetail = EventDetail.[6].["#text"]
16    | where NamedPipe contains '583da945-62af-10e8-4902-a8f205c72b2e'
17    | extend Account = UserName
18    | project-away EventDetail, EvData
19   ),
20   (
21    SecurityEvent
22    | where (EventID == '5145' and AccessList has '%4418' and RelativeTargetName contains '583da945-62af-10e8-4902-a8f205c72b2e')
23    or (EventID == "4688" and FilePath =~ "c:\\windows\\syswow64\\netsetupsvc.dll" or NewProcessName =~ "c:\\windows\\syswow64\\netsetupsvc.
24    (DeviceProcessEvents
25    | where FolderPath =~ "c:\\windows\\syswow64\\netsetupsvc.dll"))
26    | summarize FirstSeen = min(TimeGenerated), Processes=make_set(NewProcessName) by Computer, IPAddress

```

Results | Chart | Columns | Add bookmark | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 24 hours. 00:00.5 2 records

Computer	IpAddress	FirstSeen [UTC]	Processes
Computer	SolWinds1		
IpAddress	10.7.1.15		
FirstSeen [UTC]	2020-12-16T07:54:01Z		
Processes	["c:\\windows\\syswow64\\netsetupsvc.dll"]		

# Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/)

New Query 1\* x +

Feedback Queries Query explorer Format query

## General

Overview

Logs

News & guides

## Threat management

Incidents

Workbooks

Hunting

Notebooks (Preview)

Entity behavior

Threat intelligence (Preview)

## Configuration

Data connectors

Analytics

Entity Settings (Preview)

Watchlist (Preview)

Playbooks

Community

Settings

CyberSecuritySOC

Run Time range: Last 24 hours Save Copy link New alert rule Export Pin to dashboard Format query

Tables Queries Filter

Search

Filter Group by: Solution

Collapse all

### Favorites

You can add favorites by clicking on the star icon

- Azure Monitor for VMs
- Azure Sentinel
- Azure Sentinel UEBA
- DNS Analytics (Preview)
- LogManagement
- Network Performance Monitor
- Security and Audit
- SecurityCenterFree
- SQL Vulnerability Assessment
- WindowsEventForwarding
- Custom Logs
- Functions

```

8 (union isfuzzy=true
9 (Event
10 | where Source == "Microsoft-Windows-Sysmon"
11 | where EventID in (17,18)
12 | extend EvData = parse_xml(EventData)
13 | extend EventDetail = EvData.DataItem.EventData.Data
14 | extend NamedPipe = EventDetail.[5].["#text"]
15 | extend ProcessDetail = EventDetail.[6].["#text"]
16 | where NamedPipe contains '583da945-62af-10e8-4902-a8f205c72b2e'
17 | extend Account = UserName
18 | project-away EventDetail, EvData
19 ),
20 (
21 SecurityEvent
22 | where (EventID == '5145' and AccessList has '%4418' and RelativeTargetName contains '583da945-62af-10e8-4902-a8f205c72b2e')
23 or (EventID == "4688" and FilePath =~ "c:\\windows\\syswow64\\netsetupsvc.dll" or NewProcessName =~ "c:\\windows\\syswow64\\netsetupsvc.
24 dll")),
25 (DeviceProcessEvents
26 | where FolderPath =~ "c:\\windows\\syswow64\\netsetupsvc.dll"))
27 | summarize FirstSeen = min(TimeGenerated), Processes=make_set(NewProcessName) by Computer, IPAddress

```

Results Chart

Completed 05:54.7 0 records

**i** No query was selected  
Type a query and place the cursor anywhere in the query.  
A query can contain line breaks, but no blank lines.

Alerts > ADFS private key extraction attempt

### ADFS private key extraction attempt

windows10-atp-x1.atp.local Risk level High atp\mind0xp

ALERT STORY

[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

[7936] WerFault.exe -u -p 7956 -s 1428

The new Alert page

#### 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 T1528: Steal Application Access Token

First activity Jan 10, 2021, 7:09:02 PM

Last activity Jan 10, 2021, 7:09:02 PM

“可能尝试访问 ADFS 密钥材料”——当可疑的 LDAP 查询正在 AD 中搜索敏感密钥材料时进行检测。

“ADFS 私钥提取”——检测 ADFSDump 等工具中的模式。

# Azure Sentinel | Overview

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/) Refresh Last 14 days

- General
  - Overview
  - Logs
  - News & guides
- Threat management
  - Incidents
  - Workbooks
  - Hunting
  - Notebooks (Preview)
  - Entity behavior
  - Threat intelligence (Preview)
- Configuration
  - Data connectors
  - Analytics
  - Entity Settings (Preview)
  - Watchlist (Preview)
  - Playbooks
  - Community
  - Settings

50.2M ↑ 13.3M Events

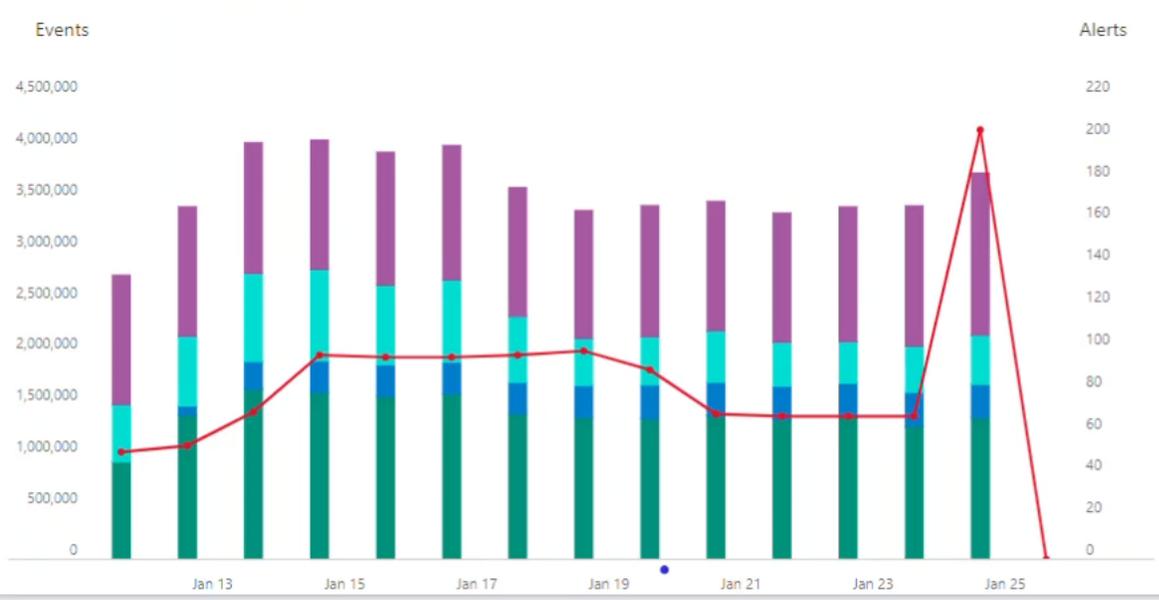
1.2K ↑ 517 Alerts

1.6K ↑ 938 Incidents

Incidents by status

New (1.6K) Active (6) Closed (True Positive) (1) Closed (False Positive) (1)

## Events and alerts over time



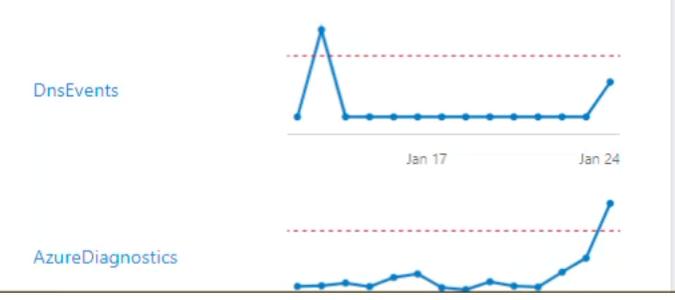
## Potential malicious events



## Recent incidents

Severity	Incident Name	Alert Count
High	ADFS DKM Master Key Export	1 Aler
Medium	Azure activity matching known threats	1 Aler
Medium	TI map IP entity to AzureActivity (enriched)	2 Aler
Medium	Potential Password Spray	1 Aler
Medium	Time series anomaly detection for total v...	3 Aler

## Data source anomalies



# Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

- Search (Ctrl+/)
- General
- Overview
  - Logs
  - News & guides
- Threat management
- Incidents
  - Workbooks
  - Hunting
  - Notebooks (Preview)
  - Entity behavior
  - Threat intelligence (Preview)
- Configuration
- Data connectors
  - Analytics
  - Entity Settings (Preview)
  - Watchlist (Preview)
  - Playbooks
  - Community
  - Settings

New Query 1\*

CyberSecuritySOC

Run Time range: Last 24 hours

Save Copy link New alert rule Export Pin to dashboard Format query

Tables Queries Filter

Search

Filter Group by: Solution

Collapse all

**Favorites**

You can add favorites by clicking on the ☆ icon

- Azure Monitor for VMs
- Azure Sentinel
- Azure Sentinel UEBA
- DNS Analytics (Preview)
- LogManagement
- Network Performance Monitor
- Security and Audit
- SecurityCenterFree
- SQL Vulnerability Assessment
- WindowsEventForwarding
- Custom Logs
- Functions

```

13 (union isfuzzy=true
14 (
15 SecurityEvent
16 | where EventID == '4688'
17 | where NewProcessName has 'SolarWinds'
18 | extend MachineName = Computer , Process = NewProcessName
19 ),
20 (
21 DeviceProcessEvents
22 | where InitiatingProcessFolderPath has 'SolarWinds'
23 | extend MachineName = DeviceName , Process = InitiatingProcessFolderPath
24 )
25 )
26 | summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), make_set(Process) by MachineName
27

```

Results Chart Columns Add bookmark Display time (UTC+00:00) Group columns

Completed. Showing results from the last 24 hours. 00:00.5 4 records

MachineName	StartTime [UTC]	EndTime [UTC]	set_Process
SolWinds1	12/14/2020, 11:14:21.000 AM	12/14/2020, 11:21:41.000 AM	["c:\program files (x86)\solarwinds\orion\erlang\erts-10.1\bin\erl.exe","c:\program files (x86)\sc...
SolWinds2	12/15/2020, 2:05:32.000 AM	12/15/2020, 2:05:32.000 AM	["c:\program files (x86)\solarwinds\orion\sql\express\mssql14.solarwinds_orion\mssql\bin\fdlau...
SolWinds3	12/7/2020, 4:48:29.000 PM	12/7/2020, 4:48:29.000 PM	["c:\program files (x86)\solarwinds\orion\sql\express\mssql14.solarwinds_orion\mssql\bin\fdlau...
SolWinds4	12/9/2020, 10:08:42.000 PM	12/9/2020, 10:08:42.000 PM	["c:\program files (x86)\solarwinds\orion\sql\express\mssql14.solarwinds_orion\mssql\bin\fdlau...

# Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/)

- General
- Overview
- Logs**
- News & guides
- Threat management
  - Incidents
  - Workbooks
  - Hunting
  - Notebooks (Preview)
  - Entity behavior
  - Threat intelligence (Preview)
- Configuration
  - Data connectors
  - Analytics
  - Entity Settings (Preview)
  - Watchlist (Preview)
  - Playbooks
  - Community
  - Settings

New Query 1\* x +

CyberSecuritySOC

Run Time range: Last 24 hours Save Copy link New alert rule Export Pin to dashboard Format query

Tables Queries Filter

Search

Filter Group by: Solution

Collapse all

**Favorites**

You can add favorites by clicking on the ☆ icon

- Azure Monitor for VMs
- Azure Sentinel
- Azure Sentinel UEBA
- DNS Analytics (Preview)
- LogManagement
- Network Performance Monitor
- Security and Audit
- SecurityCenterFree
- SQL Vulnerability Assessment
- WindowsEventForwarding
- Custom Logs
- Functions

```

16 AuditLogs
17 | where OperationName has_any ("Add service principal", "Certificates and secrets management") // captures "Add service principal",
"Add service principal credentials", and "Update application - Certificates and secrets management" events
18 | where Result == "success"
19 | mv-expand target = TargetResources
20 | where tostring(InitiatedBy.user.userPrincipalName) has "@" or tostring(InitiatedBy.app.displayName) has "@"
21 | extend targetDisplayName = tostring(TargetResources[0].displayName)
22 | extend targetId = tostring(TargetResources[0].id)
23 | extend targetType = tostring(TargetResources[0].type)
24 | extend keyEvents = TargetResources[0].modifiedProperties
25 | mv-expand keyEvents
26 | where keyEvents.displayName == "KeyDescription"
27 | extend new_value_set = parse_json(tostring(keyEvents.newValue))
28 | extend old_value_set = parse_json(tostring(keyEvents.oldValue))
29 | where old_value_set == "[]"
30 | parse new_value_set with * "KeyIdentifier=" keyIdentifier:string ",KeyType=" keyType:string ",KeyUsage=" keyUsage:string ",

```

Results Chart

Completed 00:05.6 0 records

**i** No query was selected  
Type a query and place the cursor anywhere in the query.  
A query can contain line breaks, but no blank lines.

Microsoft Azure (Preview) Search resources, services, and docs (G+)

Home > Azure Sentinel workspaces > Azure Sentinel

### Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/) New Query 1\* CyberSecuritySOC

```

27 | join (
28 | OfficeActivity
29 | where TimeGenerated > ago(7d)
30 | where OfficeWorkload ~ "Exchange" and Operation ~ "MailItemsAccessed" and ResultStatus ~ "Succeeded"
31 | extend timekey = bin(TimeGenerated, 1h)
32 | on $left:TimeGenerated == $right:timekey
33 | project-away Total, baseline, RecordType, timekey, TimeGenerated
34 | project-reorder TimeGenerated1, anomalies, Operation, UserId, Client_IPAddress, UserAgent

```

Results Chart Columns Add bookmark Display time (UTC+00:00) Group columns

Completed 00:00.8 8 records

TimeGenerated1 [UTC]	anomalies	Operation	UserId	Client_IPAddress	score	Organizationid	Orga
1/20/2021, 4:57:35.000 AM	1	MailItemsAccessed	MeganB@seccxp.ninja	34.207.252.21	1.667	4b2462a4-bbee-495a-a0e1-f23ae524cc9c	4b24
1/20/2021, 4:57:35.000 AM	1	MailItemsAccessed	MeganB@seccxp.ninja	34.207.252.21	1.667	4b2462a4-bbee-495a-a0e1-f23ae524cc9c	4b24
1/20/2021, 4:40:23.000 AM	1	MailItemsAccessed	MeganB@seccxp.ninja	174.129.96.41	1.667	4b2462a4-bbee-495a-a0e1-f23ae524cc9c	4b24
1/20/2021, 4:40:23.000 AM	1	MailItemsAccessed	MeganB@seccxp.ninja	174.129.96.41	1.667	4b2462a4-bbee-495a-a0e1-f23ae524cc9c	4b24
1/21/2021, 8:07:28.000 AM	1	MailItemsAccessed	MeganB@seccxp.ninja	3.9457.166	1.452	4b2462a4-bbee-495a-a0e1-f23ae524cc9c	4b24
1/21/2021, 8:07:28.000 AM	1	MailItemsAccessed	MeganB@seccxp.ninja				
1/21/2021, 8:37:48.000 AM	1	MailItemsAccessed	MeganB@seccxp.ninja				
1/21/2021, 8:37:48.000 AM	1	MailItemsAccessed	MeganB@seccxp.ninja				

Microsoft Azure (Preview) Search resources, services, and docs (G+)

Home > Azure Sentinel workspaces > Azure Sentinel

### Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/) New Query 1\* CyberSecuritySOC

```

14 | mv-expand total to typeof(double), TimeGenerated to typeof(datetime), anomalies to typeof(double), score to typeof(double),
15 | baseline to typeof(long)
16 | where anomalies > 0
17 |
18 | let TimeSeriesAlerts = TimeSeriesData
19 | extend (anomalies, score, baseline) = series_decompose_anomalies(Total, scorethreshold, -1, 'linefit')
20 | mv-expand Total to typeof(double), TimeGenerated to typeof(datetime), anomalies to typeof(double), score to typeof(double),
21 | TimeSeriesAlerts
22 | render timechart

```

Results Chart Display time (UTC+00:00)

Completed 00:00.7 264 records

Chart formatting

# Azure Sentinel | Workbooks

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/) Refresh Add workbook

- General
  - Overview
  - Logs
  - News & guides
- Threat management
  - Incidents
  - Workbooks
  - Hunting
  - Notebooks (Preview)
  - Entity behavior
  - Threat intelligence (Preview)
- Configuration
  - Data connectors
  - Analytics
  - Entity Settings (Preview)
  - Watchlist (Preview)
  - Playbooks
  - Community
  - Settings

82 Saved workbooks 86 Templates 0 Updates

My workbooks Templates

Search

- SolarWinds Post Compromise Hunting MICROSOFT
- Syslog Workbook
- Sysmon Threat Hunting AZURE SENTINEL COMMUNITY
- Teams Collaboration Graph
- Threat Intelligence MICROSOFT
- TSGGuide1
- User And Entity Behavior Analytics MICROSOFT
- Users Travel Map
- Visualizations Demo

### SolarWinds Post Compromise Hunting

MICROSOFT

This hunting workbook is intended to help identify activity related to the Solorigate compromise and subsequent attacks discovered in December 2020

Required data types: ⓘ

- ✓ CommonSecurityLog
- ✓ SigninLogs
- ✓ AuditLogs
- ✓ AADServicePrincipalSignInLogs
- ✓ OfficeActivity
- ✓ BehaviorAnalytics
- ✓ SecurityEvent
- ✓ DeviceProcessEvents
- ✓ SecurityAlert
- ✓ DnsEvents

Relevant data connectors: ⓘ

- AzureActiveDirectory
- SecurityEvents
- Office365
- MicrosoftThreatProtection
- DNS



# SolarWinds Post Compromise Hunting

cybersecuritysoc  
Edit Save Refresh Share Settings

## Solorigate Post Compromise Hunting

This hunting workbook is intended to help identify activity related to the SolarWinds compromise and subsequent attacks discovered in December 2020. This activity is referred to as Solorigate and UNC2452. More details can be found in the following reports:

- <https://aka.ms/solorigate>
- <https://aka.ms/sentinel-solorigate-hunt>
- <https://techcommunity.microsoft.com/t5/azure-active-directory-identity/understanding-quot-solorigate-quot-s-identity-iocs-for-identity/ba-p/2007610>
- <https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/>
- <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- <https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html>
- <https://www.solarwinds.com/securityadvisory>
- <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
- <https://www.fireeye.com/content/dam/collateral/en/wp-m-unc2452.pdf>

- Suspicious Signins
- Suspicious App Modifications
- Suspicious Lateral Movement
- Suspicious Host Activity
- Suspicious Network Activity

### Suspicious Signin Activity

## Suspicious Signins

This section hunts for suspicious sign-in events within your Azure AD tenant. It takes TTPs reported by Microsoft, FireEye and the NSA to identify logon events from known VPS provider IP ranges where the only logons using SAML tokens provided by external identity providers, or refresh tokens have been used. This helps identify instances where an attacker is using SAML tokens minted by stolen ADFS key material to access your environment and bypass MFA. This hunting query may produce false positive if users are accessing services via VPN services.

Select a user session in the initial query to populate the further queries that provide context on the users other logon activity, this is to help distinguish legitimate logons from malicious ones.

Hunting Timeframe ⓘ : Last 30 days ▾

**i** Set the timeframe you wish to hunt in using the dropdown to the right. Note that using a large timeframe may cause queries to timeout depending on the size of your environment. If you have difficulties try reducing your timeframe.

Successful User Signins from VPS providers where only Tokens were used to authenticate.

IPAddress	UserPrincipalName	StartTime	EndTime
-----------	-------------------	-----------	---------

**使用 Azure Sentinel  
GitHub**



Solorigate 视频系列

# 后续步骤

01. 在此位置观看 Solorigate 视频系列
02. 请访问 Microsoft 安全以获取更多更新：[www.microsoft.com/zh-cn/security/business](http://www.microsoft.com/zh-cn/security/business)
03. 阅读博客文章：  
[www.microsoft.com/security/blog](http://www.microsoft.com/security/blog)

<https://aka.ms/solorigate>

