

Azure Sentinel

Пит Брайан

Старший инженер

Центр аналитики угроз Майкрософт

18 февраля 2021 года

Как Microsoft Azure Sentinel помогает выявлять действия злоумышленников в сетях предприятия

- 01.** Как выявлять атаки Solorigate
- 02.** Используйте журналы событий Windows и Azure Sentinel
- 03.** Ищите необработанные данные в Azure Sentinel и Microsoft Defender для конечных точек
- 04.** Ищите признаки кражи сертификатов токенов SAML
- 05.** Оповещения Microsoft 365 Defender и Sentinel
- 06.** Используйте книгу Azure Sentinel и GitHub

Home > Azure Sentinel workspaces >

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

Events

Alerts

ALERTS 1.2K

AZUREDIAGNO... 18.2M

COMMONSECU... 8.4M

INSIGHTSMETR... 3.8M

OTHERS (55) 19.7M

Potential malicious events

POTENTIAL MALICIOUS EVENTS

Recent incidents

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

DnsEvents

AzureDiagnostics

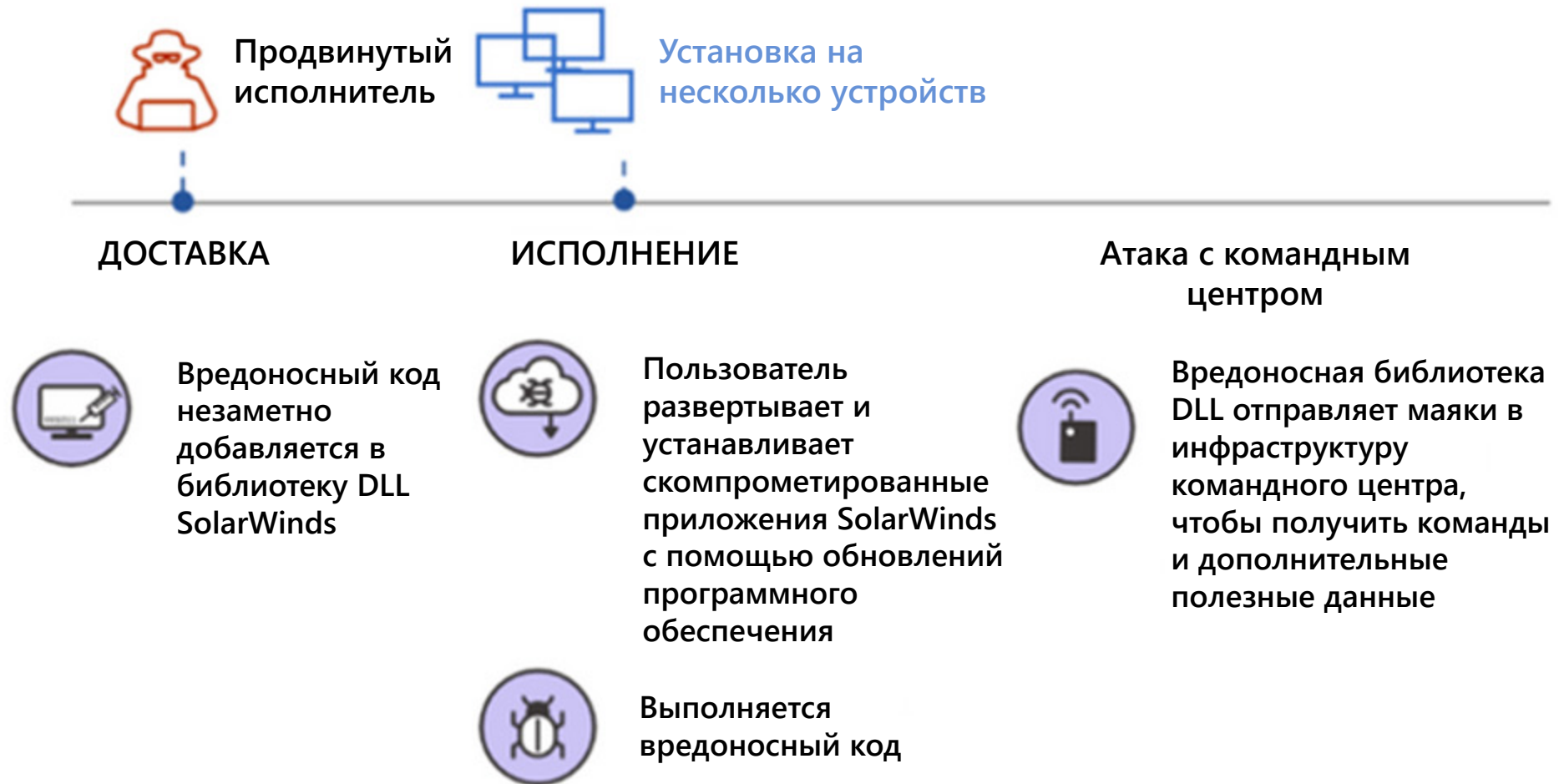


Схема атаки на цепочку поставок Solorigate

Microsoft Azure (Preview)

Report a bug

Search resources, services, and docs (G+)

Home > Azure Sentinel workspaces > Azure Sentinel

Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/)

New Query 1*

CyberSecuritySOC

TablesQueriesFilter

Search

FilterGroup 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

(union isfuzzy=true

(

SecurityEvent

| where EventID == '4688'

| where NewProcessName has 'SolarWinds'

| extend MachineName = Computer , Process = NewProcessName

),

(

DeviceProcessEvents

| where InitiatingProcessFolderPath has 'SolarWinds'

| extend MachineName = DeviceName , Process = InitiatingProcessFolderPath

)

)

| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), make_set(Process) by MachineName

ResultsChart

Columns

Add bookmark

Display time (UTC+00:00)

Group columns

Completed. Showing results from the last 24 hours.

00:00.54 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

Page 1 of 1

50 items per page

1 - 4 of 4 items

Microsoft Azure (Preview)

Report a bug

Search resources, services, and docs (G+)

pebryan@microsoft.com

MICROSOFT

Home > Azure Sentinel workspaces > Azure Sentinel

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 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

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"]

Page 1 of 1

50 items per page

1 - 2 of 2 items

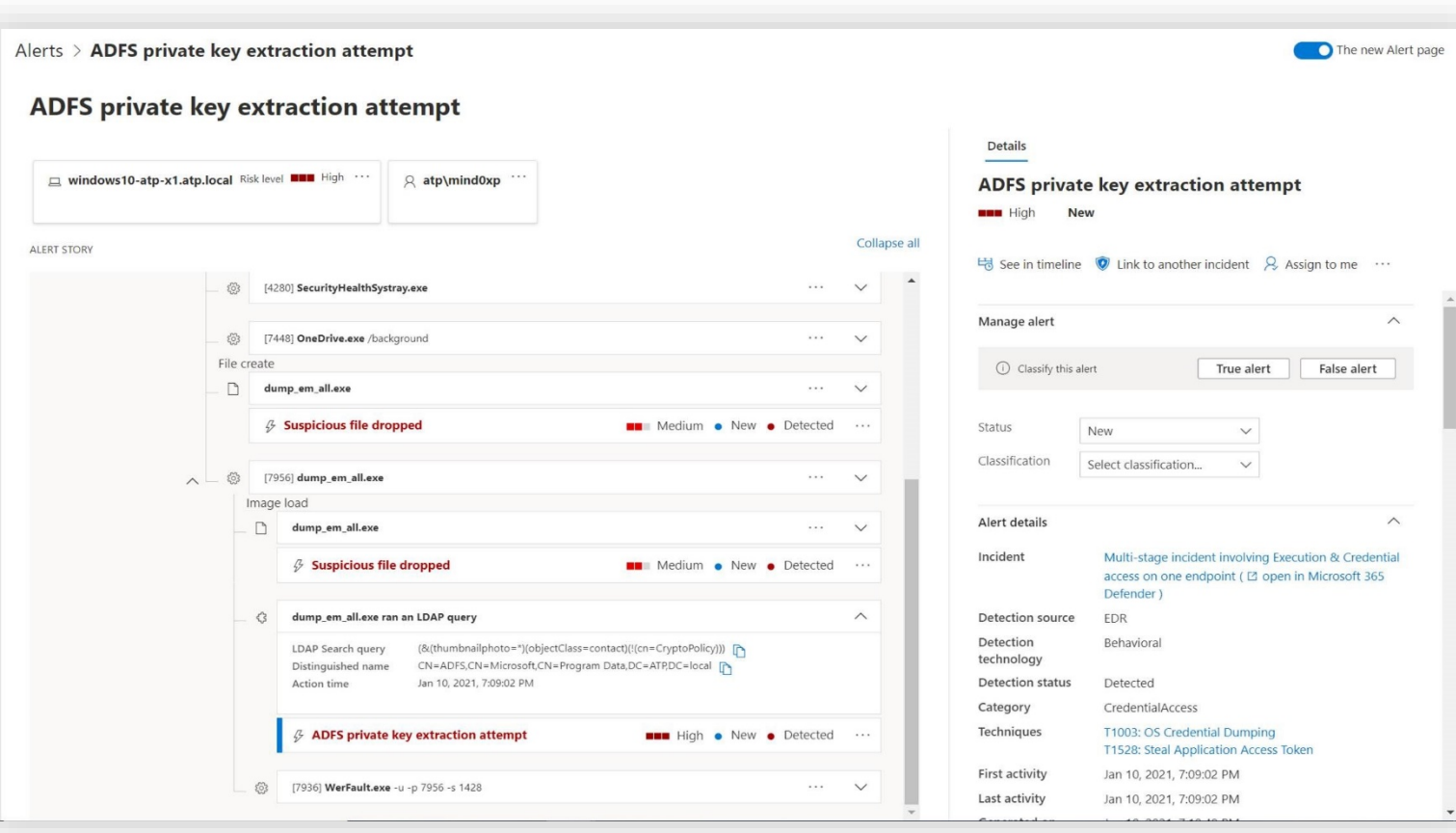
[Feedback](#)
[Queries](#)
[Query explorer](#)
[Settings](#)
[Help](#)

 Settings

- Functions

🕒 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.


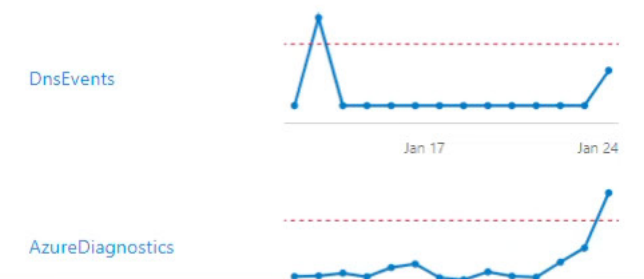


«Возможная попытка доступа к материалу ключа ADFS» —

обнаруживает, когда подозрительный запрос LDAP ищет конфиденциальный материал ключа в AD.

«Извлечение закрытого ключа ADFS» —

обнаруживает шаблонные действия таких инструментов, как ADFSDump.

 Settings

Microsoft Azure (Preview)

Report a bug

Search resources, services, and docs (G+)

Home > Azure Sentinel workspaces > Azure Sentinel

Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+)

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

14

15

16

17

18

19

20

21

22

23

24

25

26

27

(union isfuzzy=true

(

SecurityEvent

| where EventID == '4688'

| where NewProcessName has 'SolarWinds'

| extend MachineName = Computer , Process = NewProcessName

),

(

DeviceProcessEvents

| where InitiatingProcessFolderPath has 'SolarWinds'

| extend MachineName = DeviceName , Process = InitiatingProcessFolderPath

)

| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), make_set(Process) by MachineName

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\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\sqlexpress\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\sqlexpress\mssql14.solarwinds_orion\mssql\bin\fdlau

Page 1 of 1

50 items per page

1 - 4 of 4 items

Microsoft Azure (Preview)

Report a bug

Search resources, services, and docs (G+)

>

🔖

🗨️3

⚙️

?

😊

pebryan@microsoft.com

MICROSOFT

Home > Azure Sentinel workspaces > Azure Sentinel

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

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

//

AuditLogs

| 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

| where Result == "success"

| mv-expand target = TargetResources

| where tostring(InitiatedBy.user.userPrincipalName) has "@" or tostring(InitiatedBy.app.displayName) has "@"

| extend targetDisplayName = tostring(TargetResources[0].displayName)

| extend targetId = tostring(TargetResources[0].id)

| extend targetType = tostring(TargetResources[0].type)

| extend keyEvents = TargetResources[0].modifiedProperties

| mv-expand keyEvents

| where keyEvents.displayName =~ "KeyDescription"

| extend new_value_set = parse_json(tostring(keyEvents.newValue))

| extend old_value_set = parse_json(tostring(keyEvents.oldValue))

| where old_value_set == "[]"

| parse new_value_set with * "KeyIdentifier=" keyIdentifier:string, "KeyType=" keyType:string, "KeyUsage=" keyUsage:string,

Results

Chart

Completed

00:05.6

0 records

📘

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) Report a bug Search resources, services, and docs (G+)

Home > Azure Sentinel workspaces > Azure Sentinel

Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/)

New Query 1* x +

CyberSecuritySOC

Run Time range: Set in query Save Copy link New alert rule Export Pin to dashboard Format query

```
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	3.94.57.166	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				

Page 1 of 1

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

Home > Azure Sentinel workspaces > Azure Sentinel

Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/)

New Query 1* x +

CyberSecuritySOC

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

```
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 | let TimeSeriesAlerts = TimeSeriesData
18 | extend (anomalies, score, baseline) = series_decompose_anomalies(Total, scorethreshold, -1, 'linefit')
19 | mv-expand Total to typeof(double), TimeGenerated to typeof(datetime), anomalies to typeof(double), score to typeof(double),
20 | baseline to typeof(long);
21 | TimeSeriesAlerts
22 | render timechart
```

Results Chart Display time (UTC+00:00)

Completed 00:00.7 264 records

Chart formatting

Microsoft Azure (Preview)

Report a bug

Search resources, services, and docs (G+)

pebryan@microsoft.com

Home > Azure Sentinel workspaces > Azure Sentinel >

SolarWinds Post Compromise Hunting

cybersecuritysoc

Edit

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 ▾

ⓘ

 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

↑ ↓

**Используйте Azure
Sentinel GitHub**



Серия видео о Solorigate

Дальнейшие действия

- 01.** Посмотрите серию видео о Solorigate по этому адресу
- 02.** Следите за новостями на веб-сайте Microsoft Security:
www.microsoft.com/en-us/security/business
- 03.** Ознакомьтесь с публикациями в блоге:
www.microsoft.com/security/blog

<https://aka.ms/solorigate>

