Microsoft

Azure Sentinel

Pete Bryan

Senior Engineer

Microsoft Threat Intelligence Center

February 18, 2021

Solorigate Overview

How Microsoft Azure Sentinel can help you hunt for attacker activity across your enterprise

01. How to Hunt for Solorigate attacks

02. Use Windows Event logs and Azure Sentinel

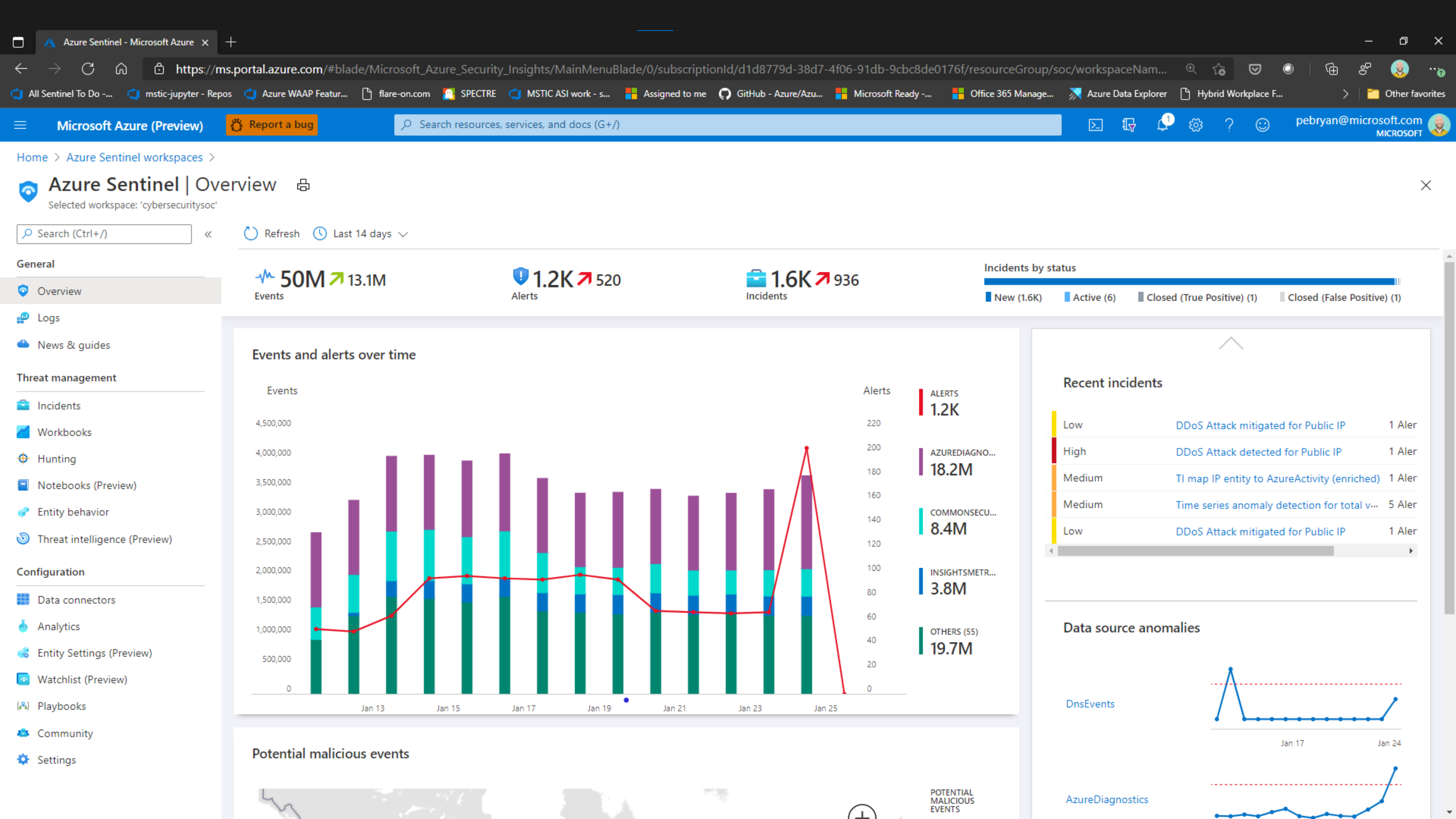
03. Look for raw data in Azure Sentinel and Microsoft Defender for Endpoints

04. Look for signs of stealing certificates SAML tokens

05. Microsoft 365 Defender & Sentinel alerts

06. Use the Azure Sentinel workbook and GitHub

Microsoft Security



Azure Sentinel | Overview

Selected workspace: 'cybersecuritysoc'

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

ALERTS 1.2K

AZUREDIAGNO... 18.2M

COMMONSECU... 8.4M

INSIGHTSMETR... 3.8M

OTHERS (55) 19.7M

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

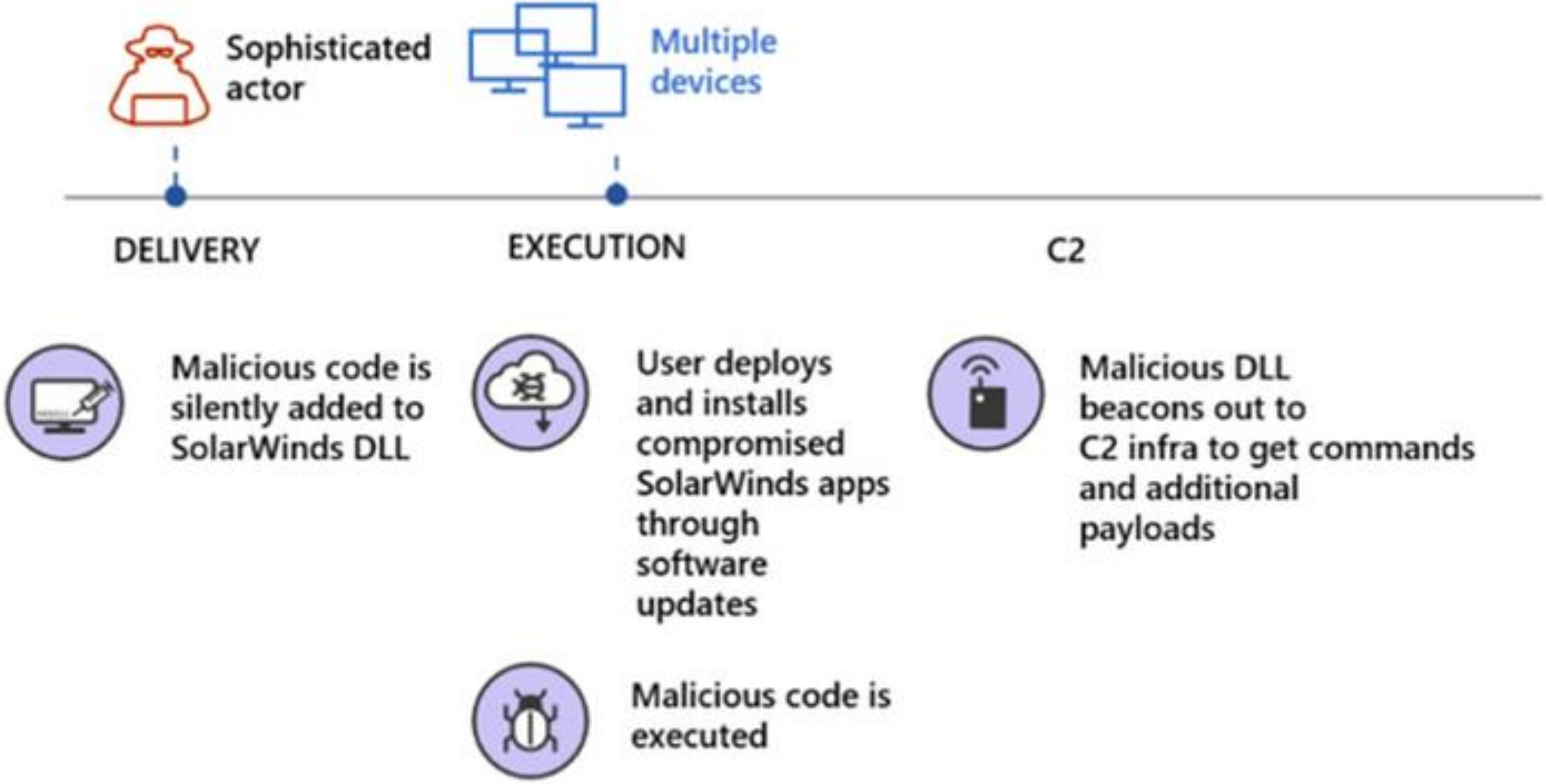
Data source anomalies

DnsEvents

AzureDiagnostics

Potential malicious events

POTENTIAL MALICIOUS EVENTS



Sophisticated actor

Multiple devices

DELIVERY

Malicious code is silently added to SolarWinds DLL

EXECUTION

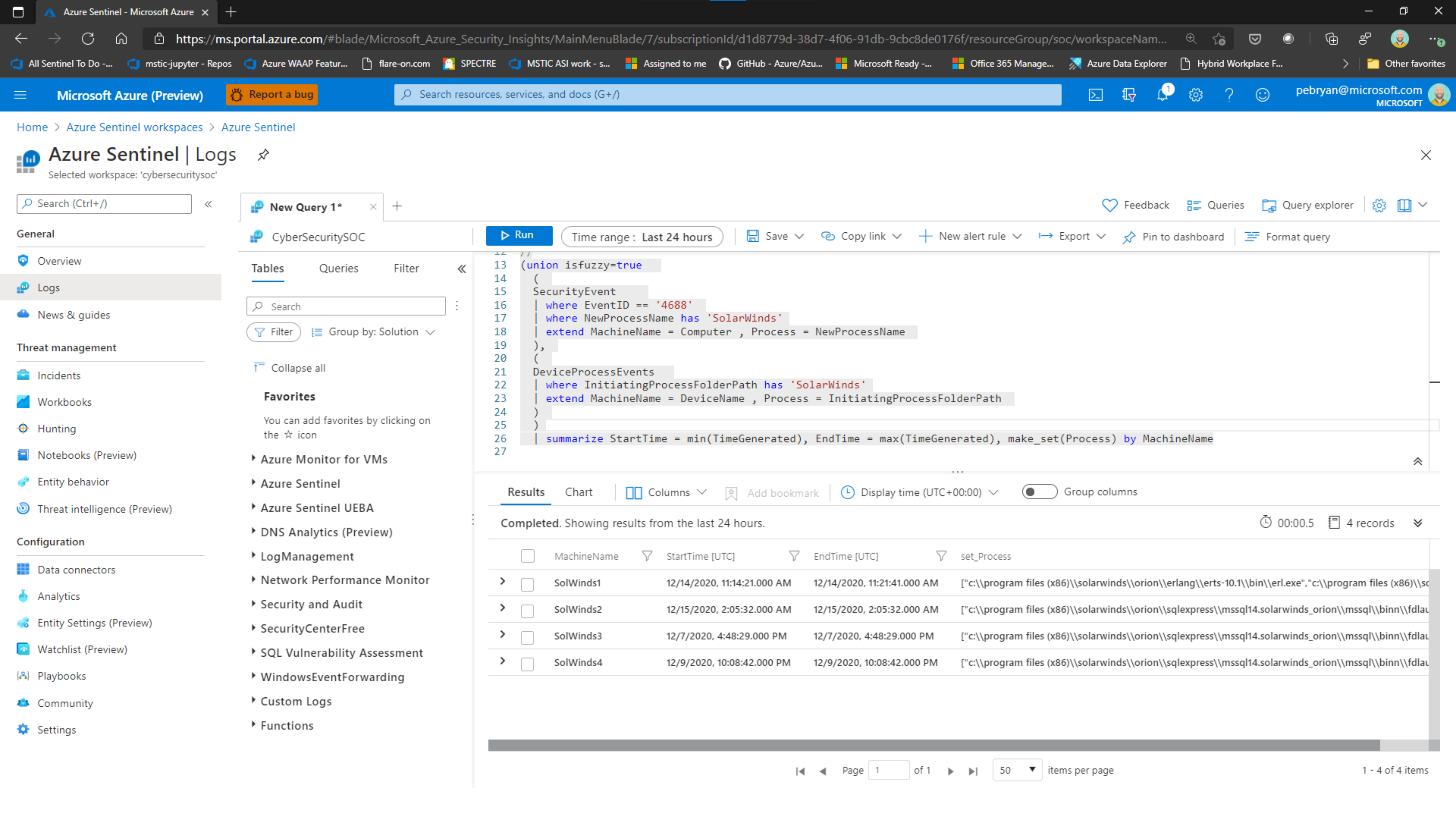
User deploys and installs compromised SolarWinds apps through software updates

Malicious code is executed

C2

Malicious DLL beacons out to C2 infra to get commands and additional payloads

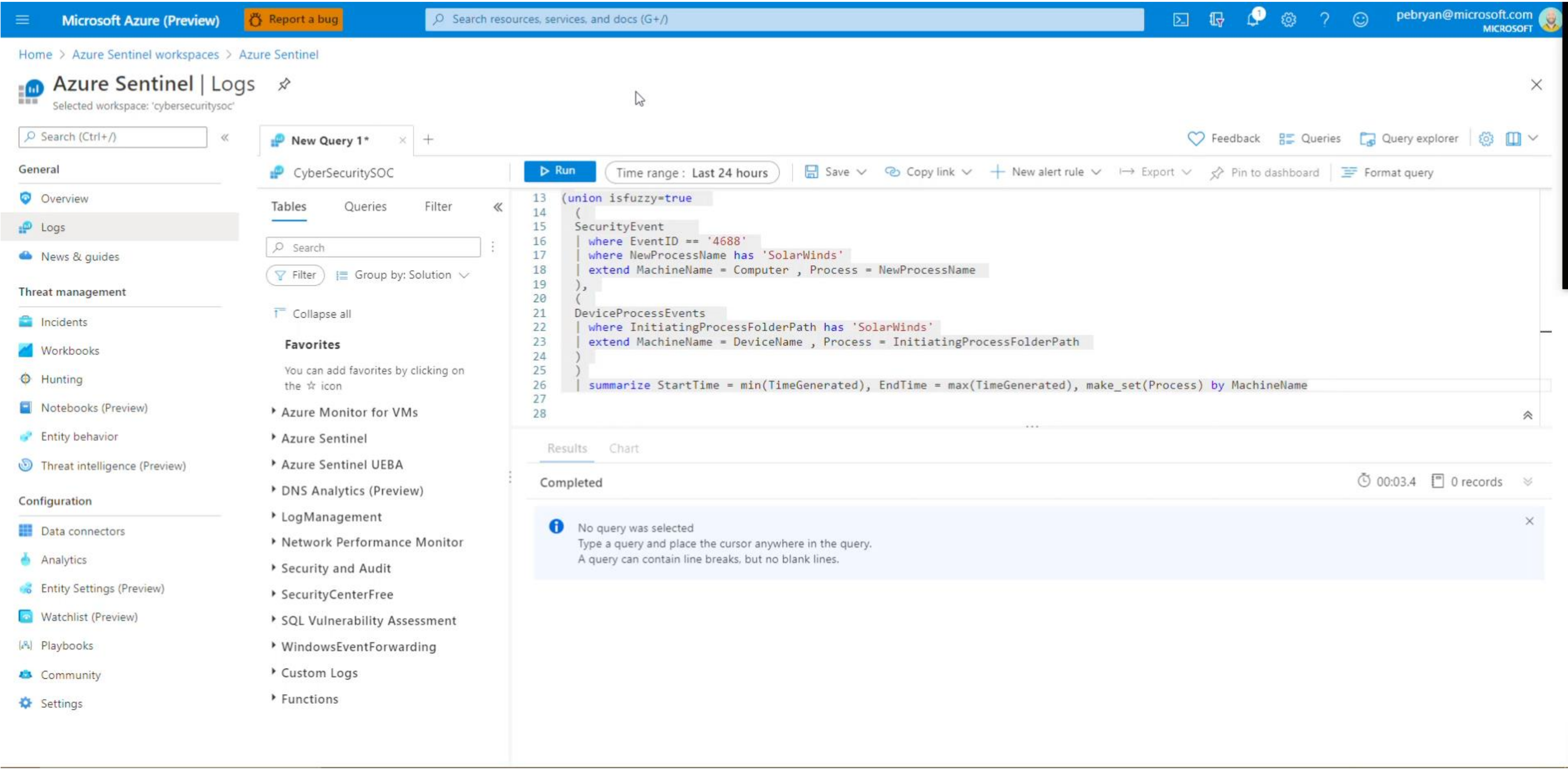
Solorigate supply chain attack diagram



```
//
(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
```

Completed. Showing results from the last 24 hours.

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

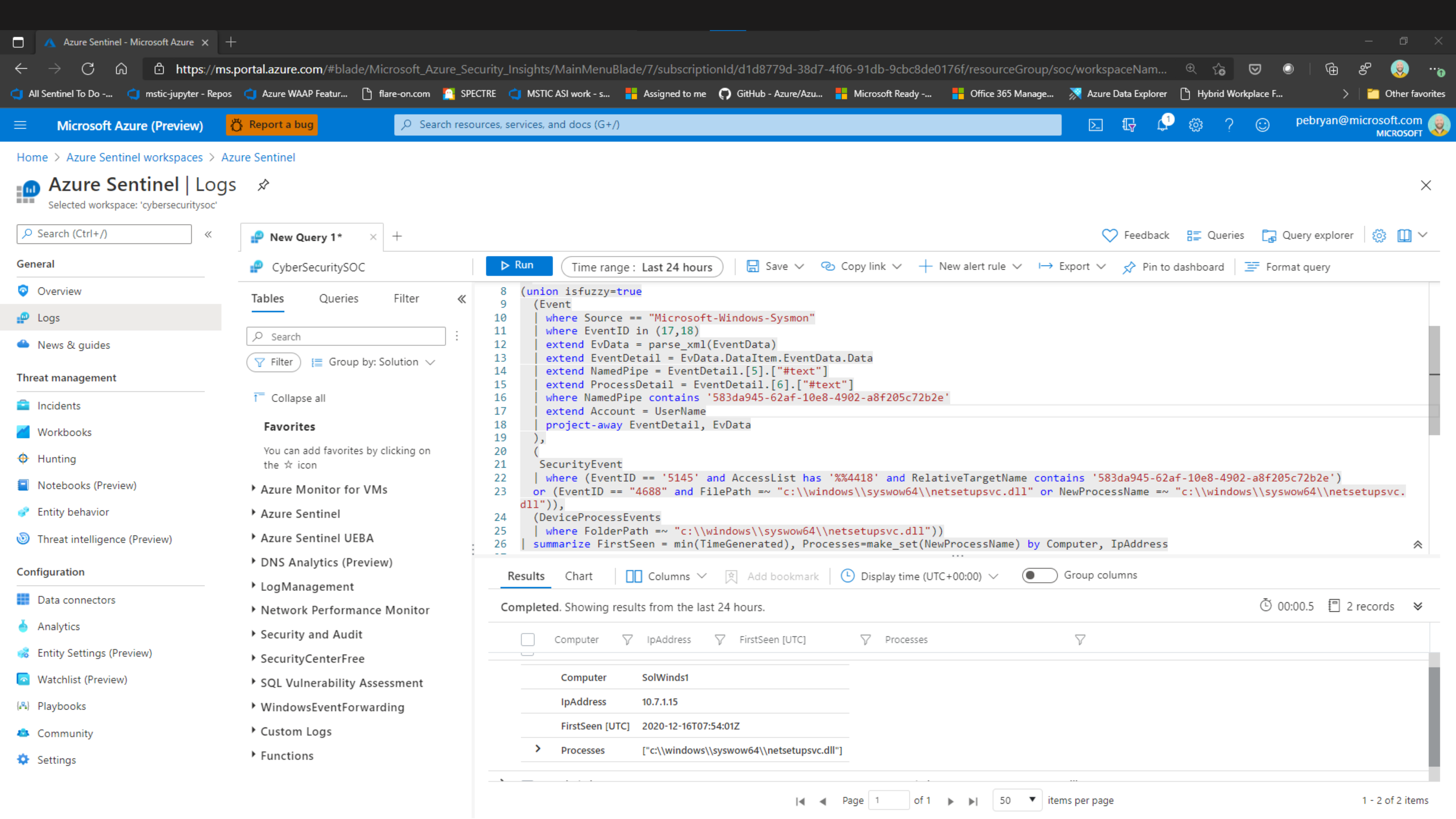


```
(union isfuzzy=true
  (
  SecurityEvent
  | where EventID == '4688'
  | where NewProcessName has 'SolarWinds'
  | extend MachineName = Computer , Process = NewProcessName
  ),
  (
  DeviceProcessEvents
  | where InitiatingProcessFolderPath has 'SolarWinds'
  | extend MachineName = DeviceName , Process = InitiatingProcessFolderPath
  )
  )
  | summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), make_set(Process) by MachineName
```

Completed

00:03.4 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.



Azure Sentinel | Logs

Selected workspace: 'cybersecuritysoc'

Time range : Last 24 hours

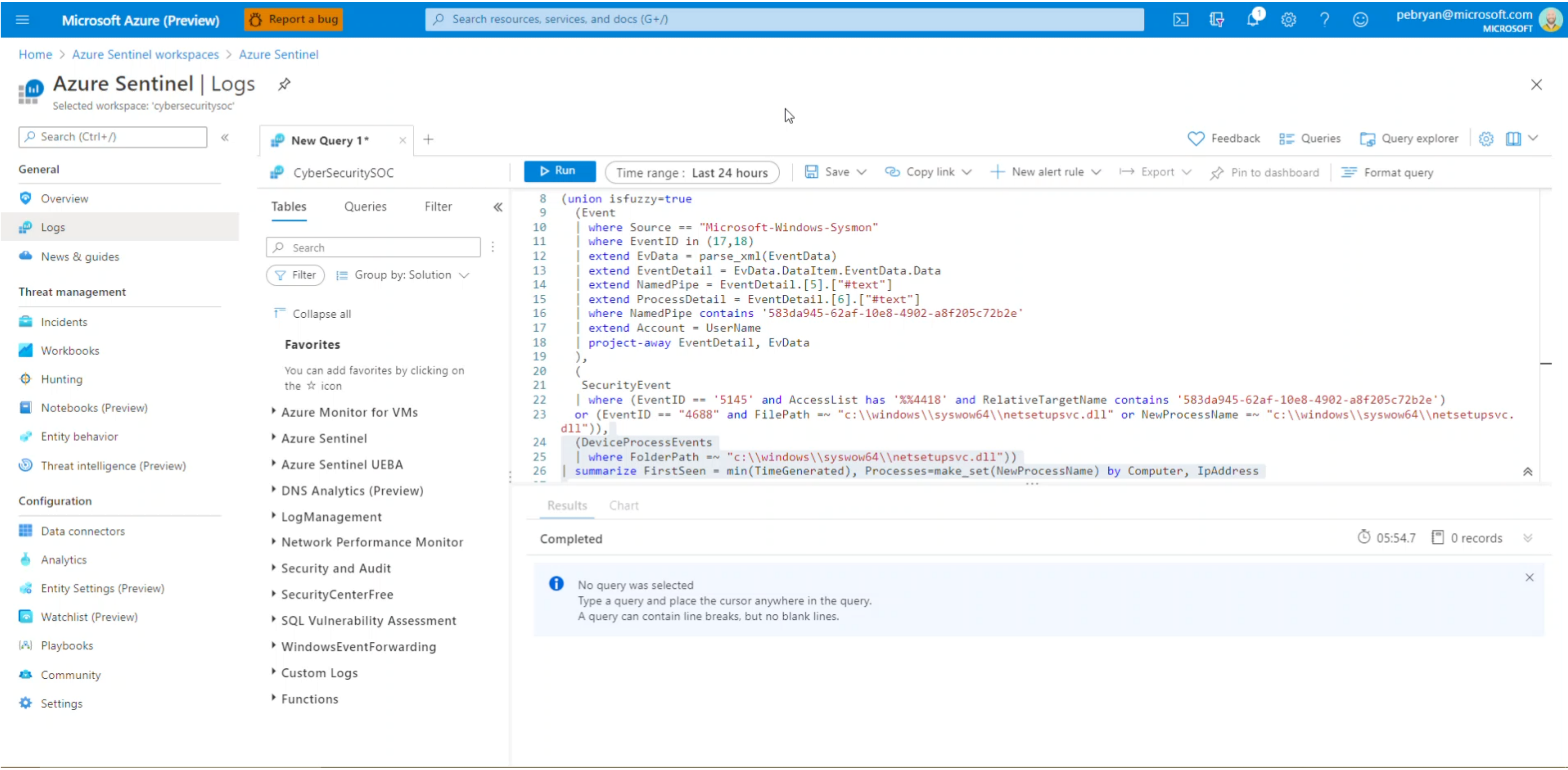
```
(union isfuzzy=true
  (Event
  | where Source == "Microsoft-Windows-Sysmon"
  | where EventID in (17,18)
  | extend EvData = parse_xml(EventData)
  | extend EventDetail = EvData.DataItem.EventData.Data
  | extend NamedPipe = EventDetail.[5].["#text"]
  | extend ProcessDetail = EventDetail.[6].["#text"]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

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"]



Selected workspace: 'cybersecuritysoc'

Time range : Last 24 hours

Group by: Solution

You can add favorites by clicking on the ☆ icon

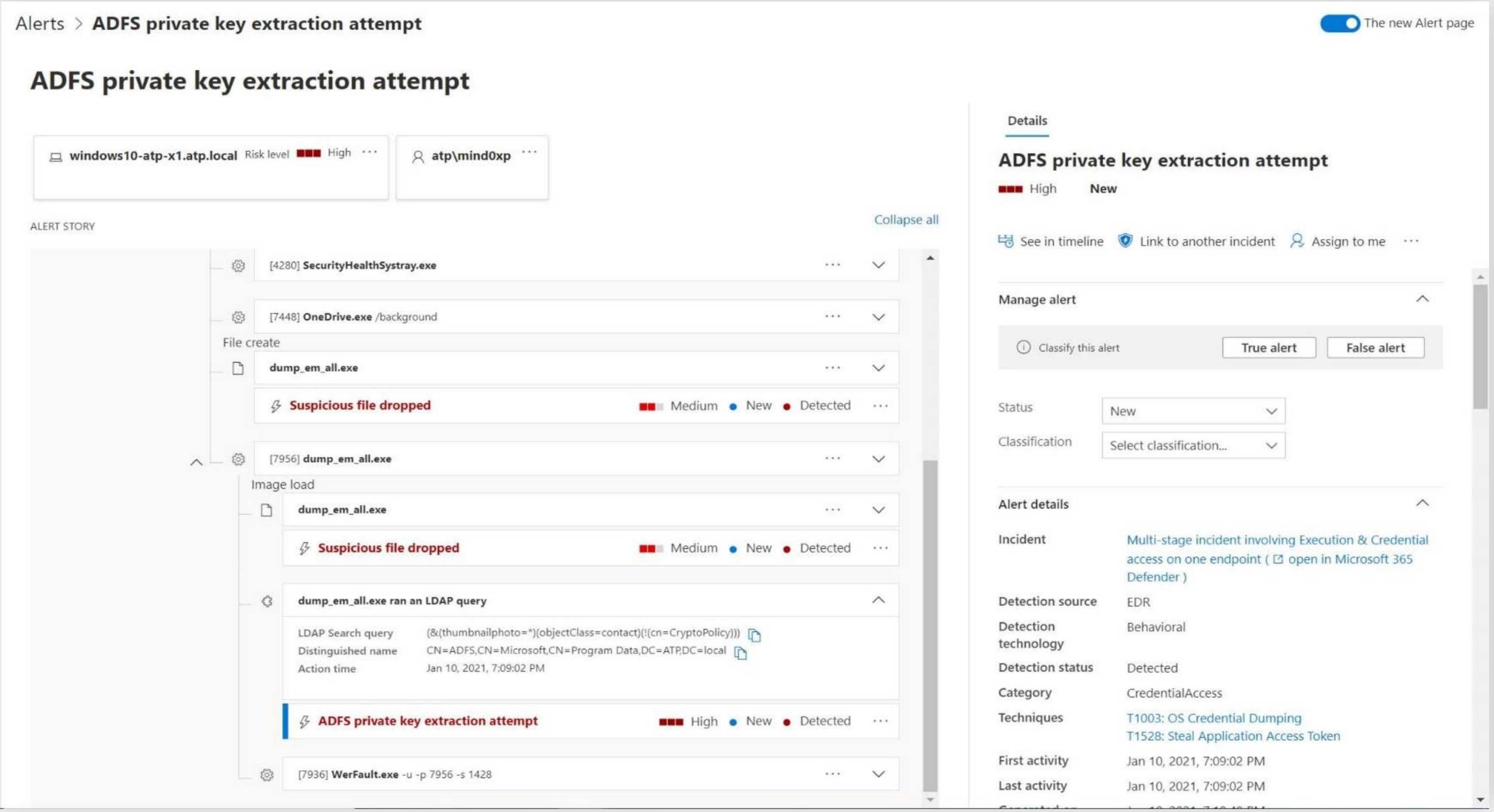
```
(union isfuzzy=true
  (Event
   | where Source == "Microsoft-Windows-Sysmon"
   | where EventID in (17,18)
   | extend EvData = parse_xml(EventData)
   | extend EventDetail = EvData.DataItem.EventData.Data
   | extend NamedPipe = EventDetail.[5].["#text"]
   | extend ProcessDetail = EventDetail.[6].["#text"]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

Completed

05:54.7 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.

Solorigate Overview video



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

Details

ADFS private key extraction attempt

■■■ High New

Manage alert

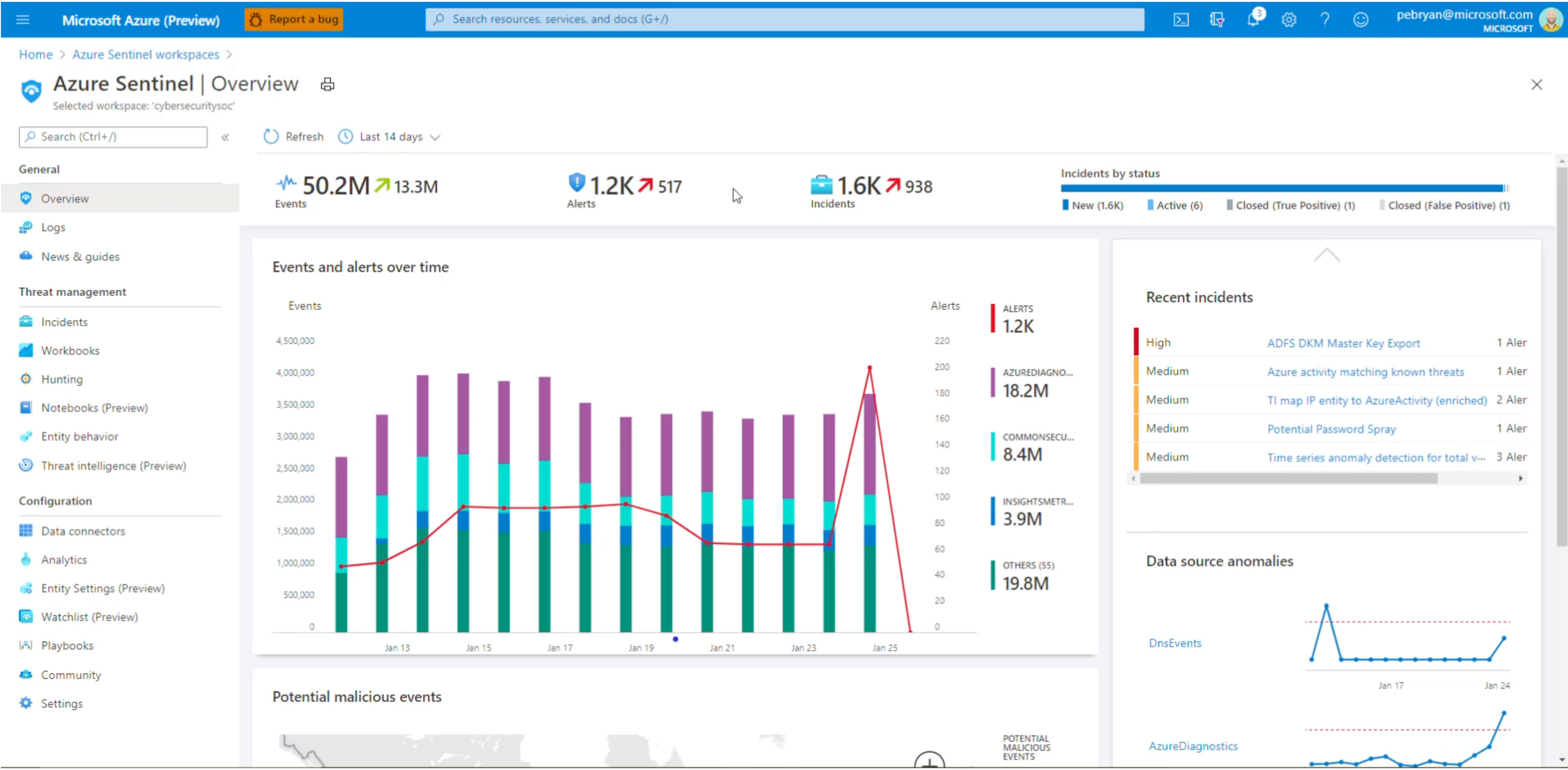
Status	New
Classification	Select classification...

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

“Possible attempt to access ADFS key material”— detects when a suspicious LDAP query is searching for sensitive key material in AD.

“ADFS private key extraction” — detects patterns from tools such as ADFSDump.



Microsoft Azure (Preview) | Report a bug | Search resources, services, and docs (G+/) | pebryan@microsoft.com MICROSOFT

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

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)

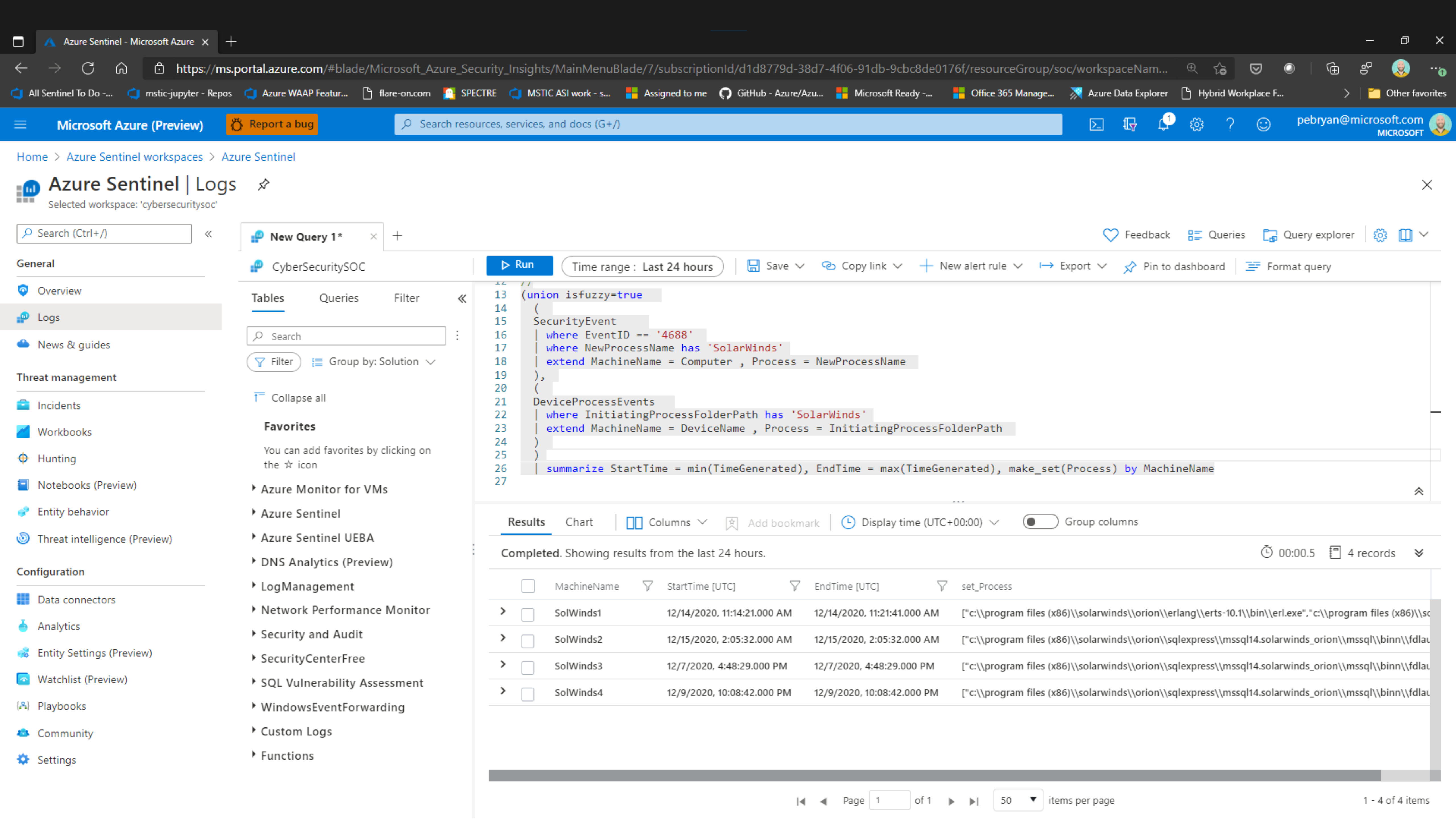
Events and alerts over time

Recent incidents

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

Potential malicious events

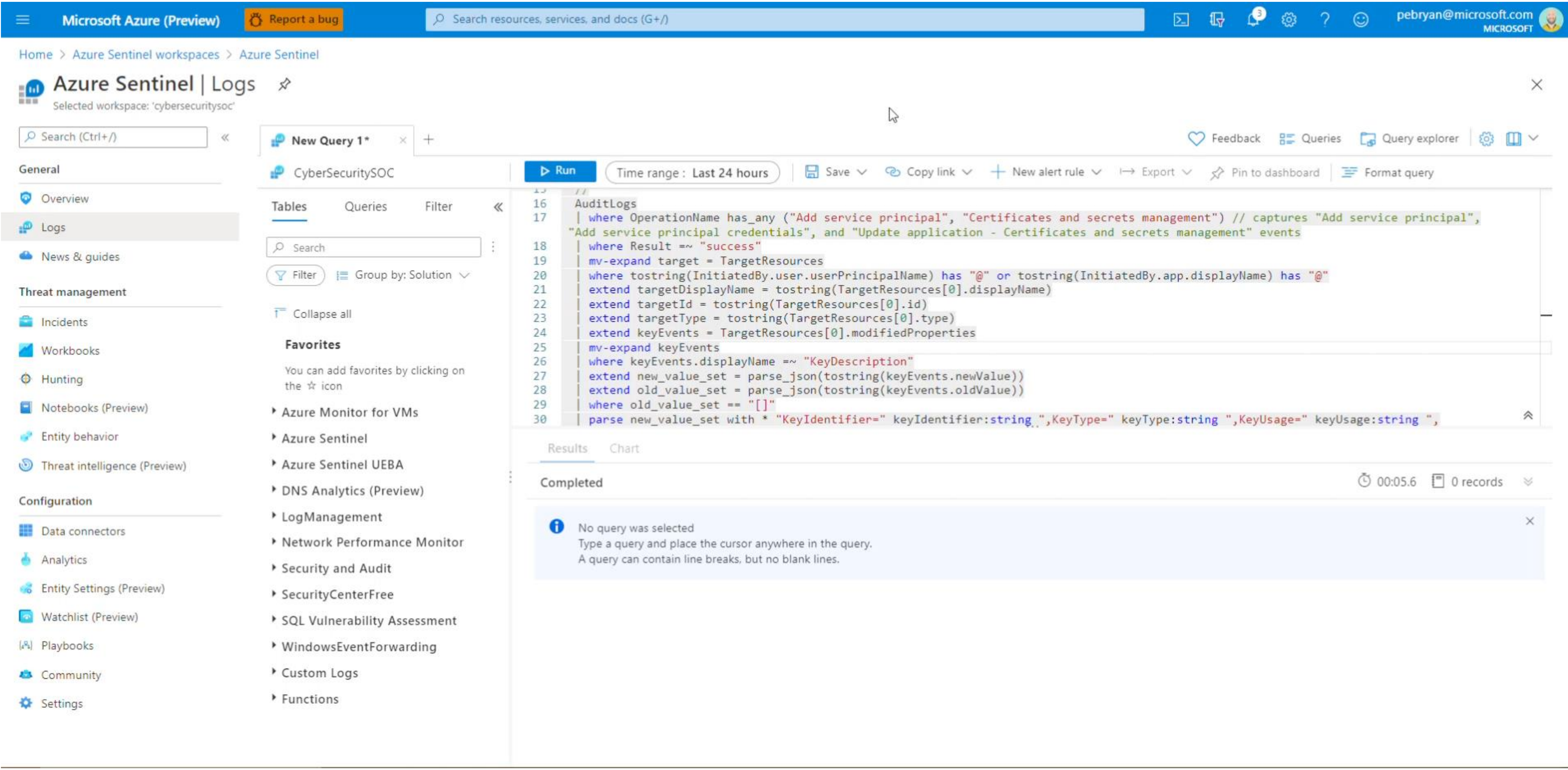
Data source anomalies



```
(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
```

Completed. Showing results from the last 24 hours.

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



```
//
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 ",
```

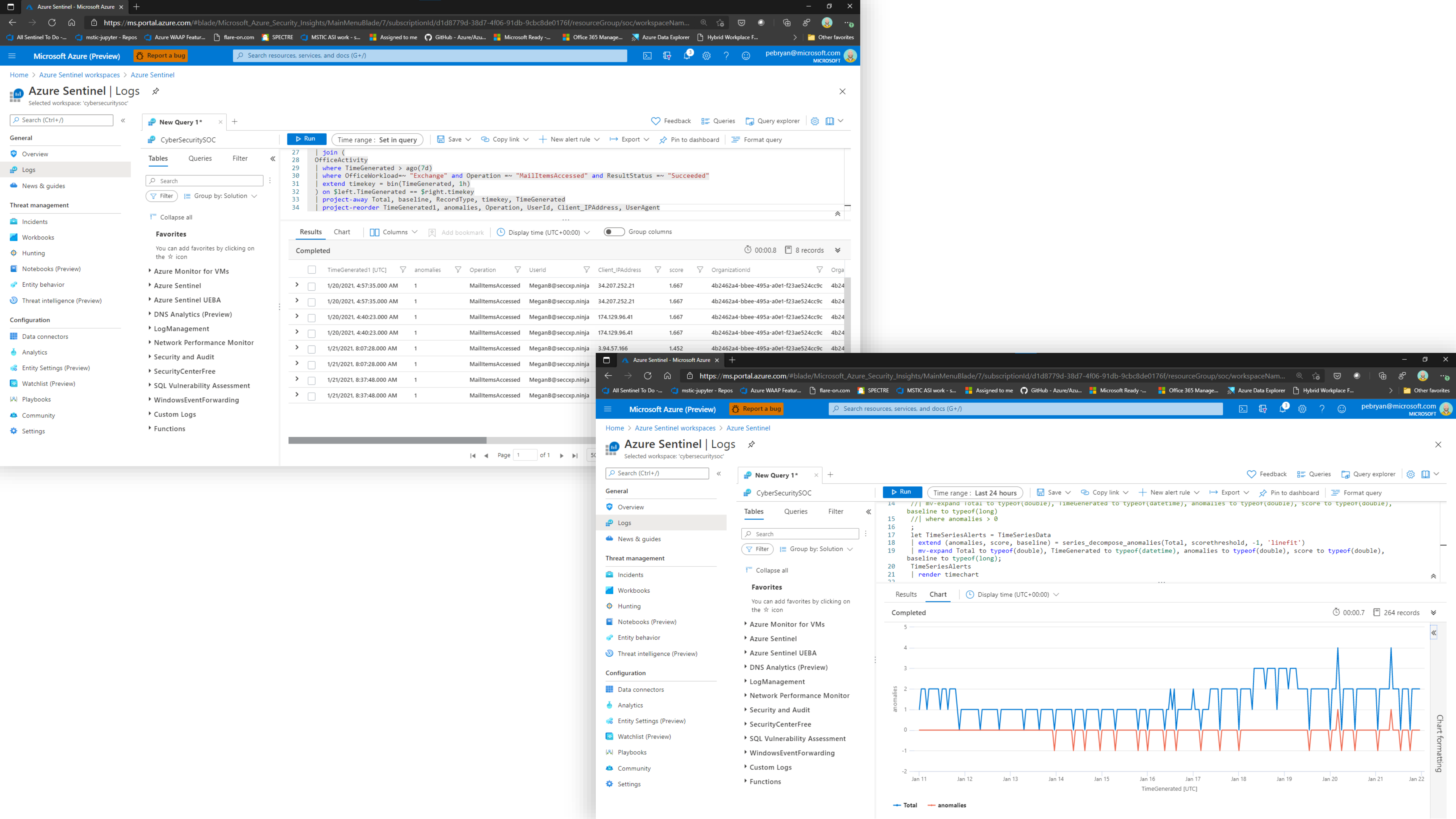
Completed

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.



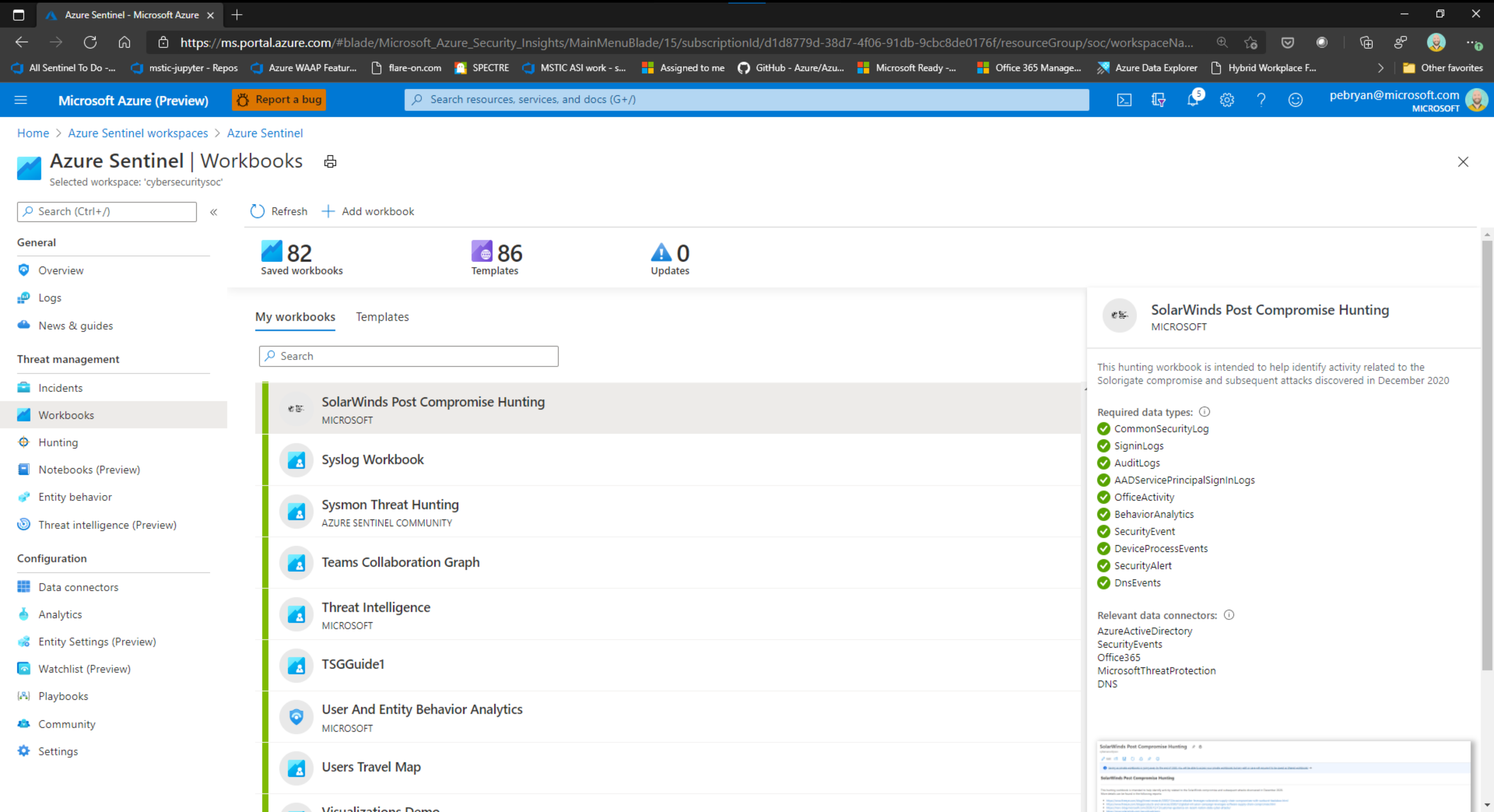
```
| join (
OfficeActivity
| where TimeGenerated > ago(7d)
| where OfficeWorkload=~ "Exchange" and Operation =~ "MailItemsAccessed" and ResultStatus =~ "Succeeded"
| extend timekey = bin(TimeGenerated, 1h)
) on $left.TimeGenerated == $right.timekey
| project-away Total, baseline, RecordType, timekey, TimeGenerated
| project-reorder TimeGenerated1, anomalies, Operation, UserId, Client_IPAddress, UserAgent
```

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				

```
 //| mv-expand Total to typeof(double), TimeGenerated to typeof(datetime), anomalies to typeof(double), score to typeof(double),
baseline to typeof(long)
 //| where anomalies > 0
 ;
 let TimeSeriesAlerts = TimeSeriesData
 | extend (anomalies, score, baseline) = series_decompose_anomalies(Total, scorethreshold, -1, 'linefit')
 | mv-expand Total to typeof(double), TimeGenerated to typeof(datetime), anomalies to typeof(double), score to typeof(double),
baseline to typeof(long);
 TimeSeriesAlerts
 | render timechart
```

Completed 00:00.7 264 records



Azure Sentinel - Microsoft Azure

https://ms.portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/15/subscriptionId/d1d8779d-38d7-4f06-91db-9cbc8de0176f/resourceGroup/soc/workspaceNa...

All Sentinel To Do -... | mstic-jupyter - Repos | Azure WAAP Featur... | flare-on.com | SPECTRE | MSTIC ASI work - s... | Assigned to me | GitHub - Azure/Azu... | Microsoft Ready -... | Office 365 Manage... | Azure Data Explorer | Hybrid Workplace F... | Other favorites

Microsoft Azure (Preview) | Report a bug | Search resources, services, and docs (G+/) | pebryan@microsoft.com MICROSOFT

Home > Azure Sentinel workspaces > Azure Sentinel

Azure Sentinel | Workbooks

Selected workspace: 'cybersecuritysoc'

Search (Ctrl+/)

Refresh | Add workbook

82 Saved workbooks | 86 Templates | 0 Updates

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

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

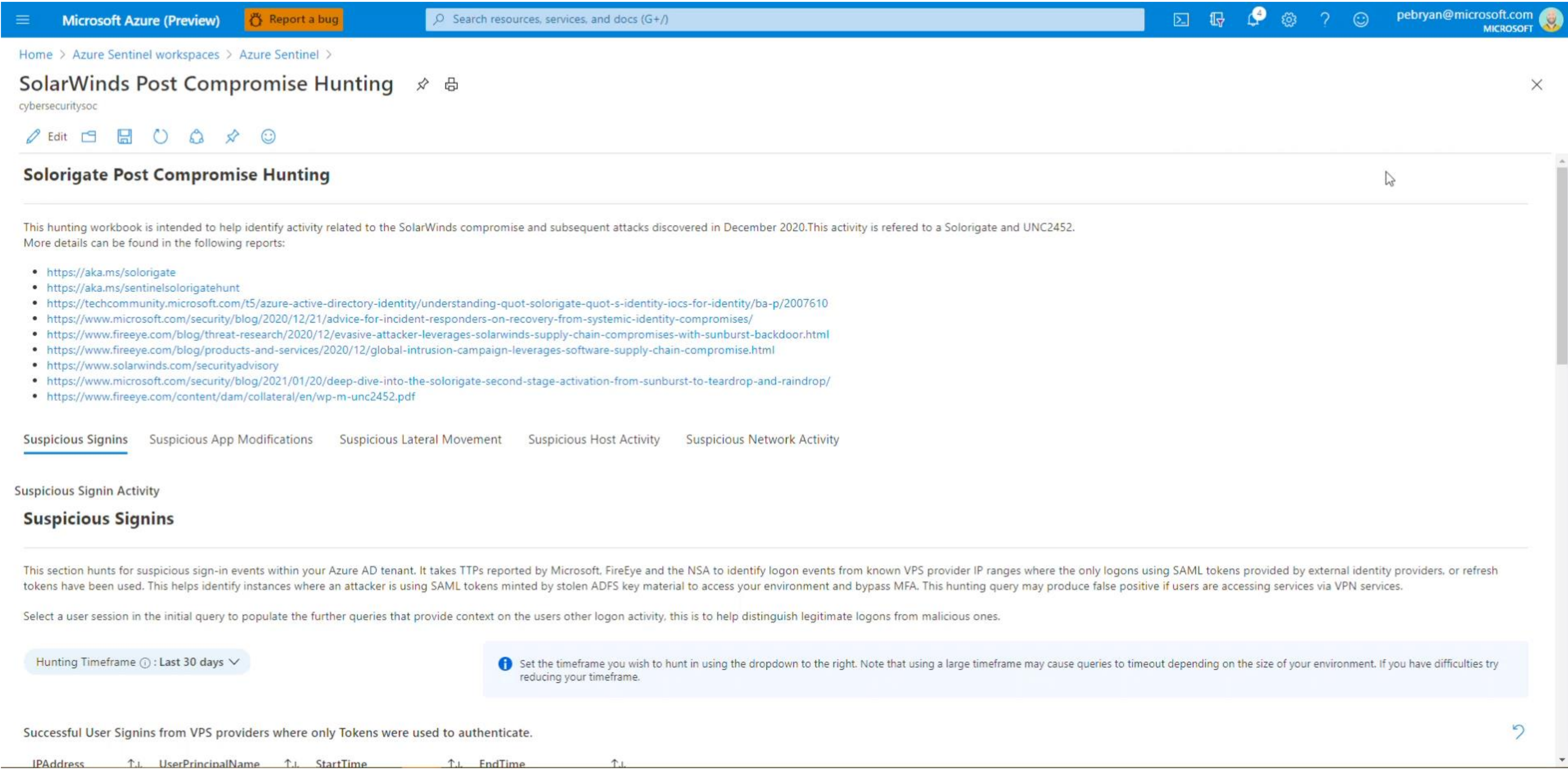
This hunting workbook is intended to help identify activity related to the Solorigate compromise and subsequent attacks discovered in December 2020

Required data types:

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

Relevant data connectors:

AzureActiveDirectory
SecurityEvents
Office365
MicrosoftThreatProtection
DNS



Microsoft Azure (Preview)
Report a bug
Search resources, services, and docs (G+/)
pebryan@microsoft.com
MICROSOFT
Home > Azure Sentinel workspaces > Azure Sentinel >
Edit

SolarWinds Post Compromise Hunting

cybersecuritysoc

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 refered to a Solorigate and UNC2452.
More details can be found in the following reports:

- https://aka.ms/solorigate
- https://aka.ms/sentinelsolorigatehunt
- 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

Use Azure Sentinel GitHub

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