Acknowledgement of Country

We wish to acknowledge the traditional custodians of the land we are meeting on, the Whadjuk people of the Noongar nation, and pay respect to Elders past and present.

We recognise and respect their cultural heritage, beliefs and relationship with the land, as well as acknowledge the contribution they make to the life of this city and this region.

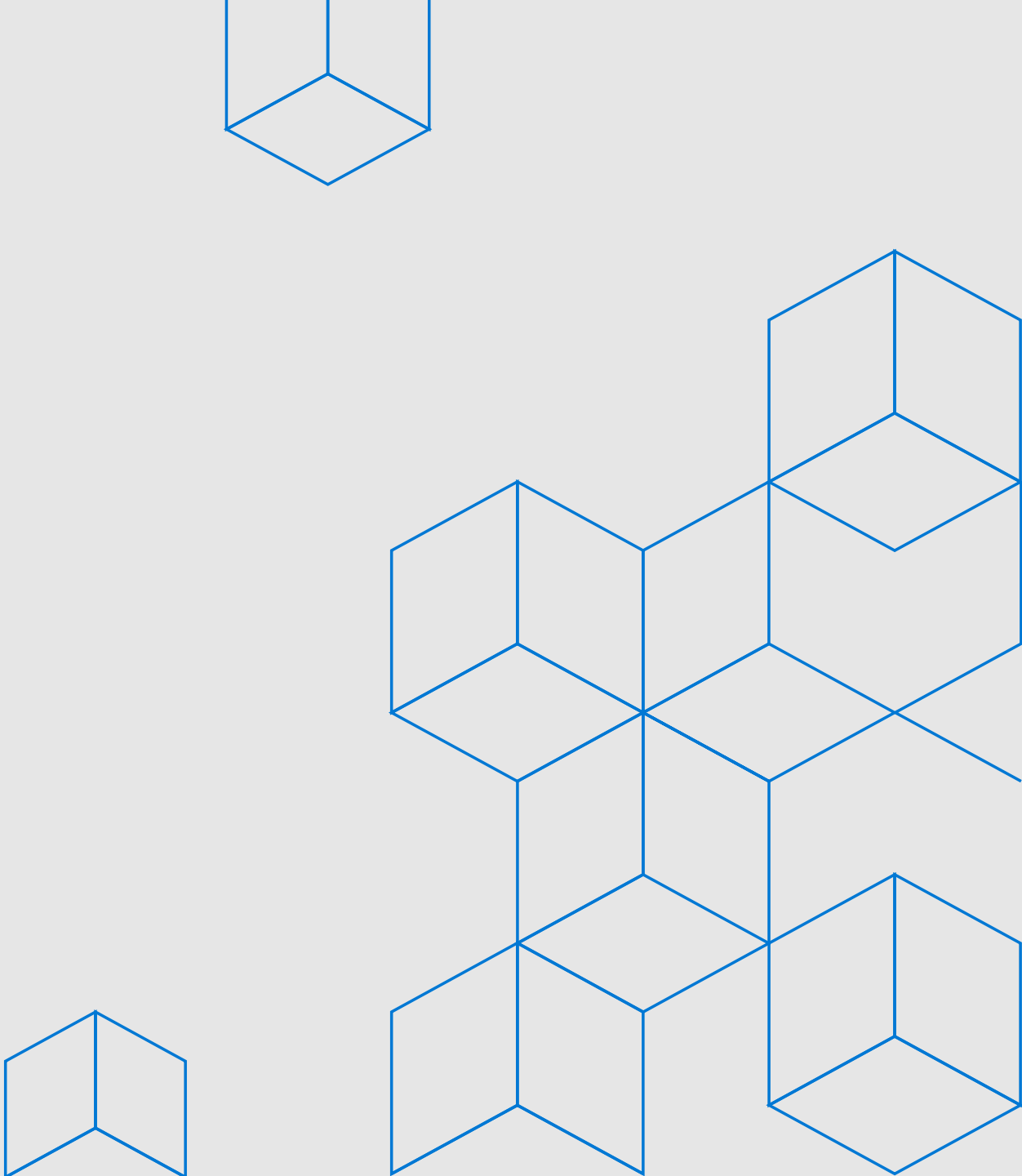
Microsoft

South West Aboriginal Land & Sea Council

Microsoft

Azure Sentinel

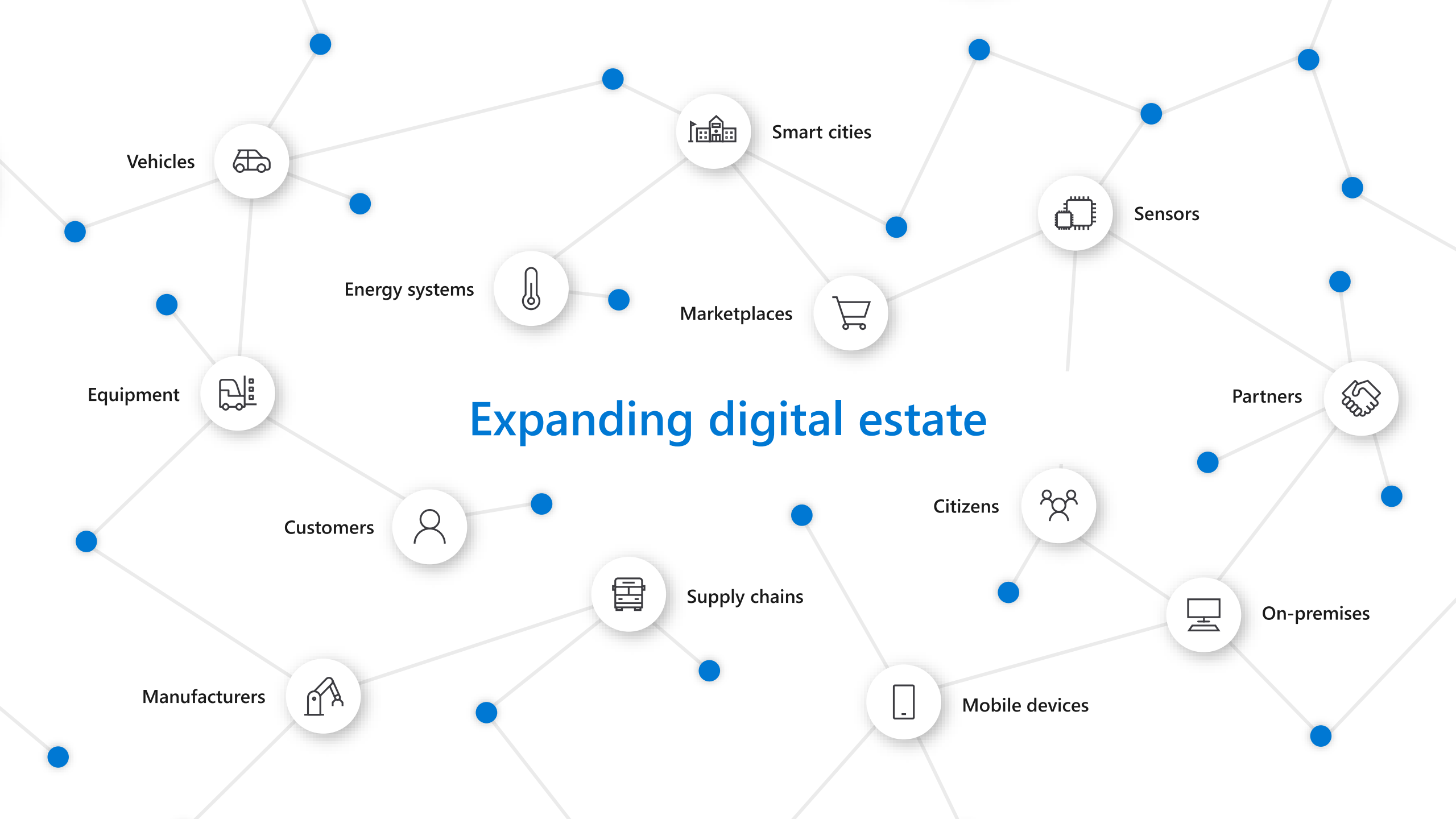
Technical Training



Azure Sentinel Training Agenda

- Tech Overview
- Collection architecture
- KQL Workshop
- Lunch
- Playbook, Hunting & Alerts
- Hands on Labs

Introducing Azure Sentinel



Expanding digital estate

Traditional SOC Challenges

Sophistication of threats

High volume of noisy alerts

IT deployment & maintenance

Rising infrastructure costs and upfront investment

Too many disconnected products

Lack of automation

Security skills in short supply

Security
Operations Team

Cloud + Artificial Intelligence

Microsoft Security Advantage

$1B annual investment in cybersecurity

3500+ global security experts

Trillions of diverse signals for unparalleled intelligence

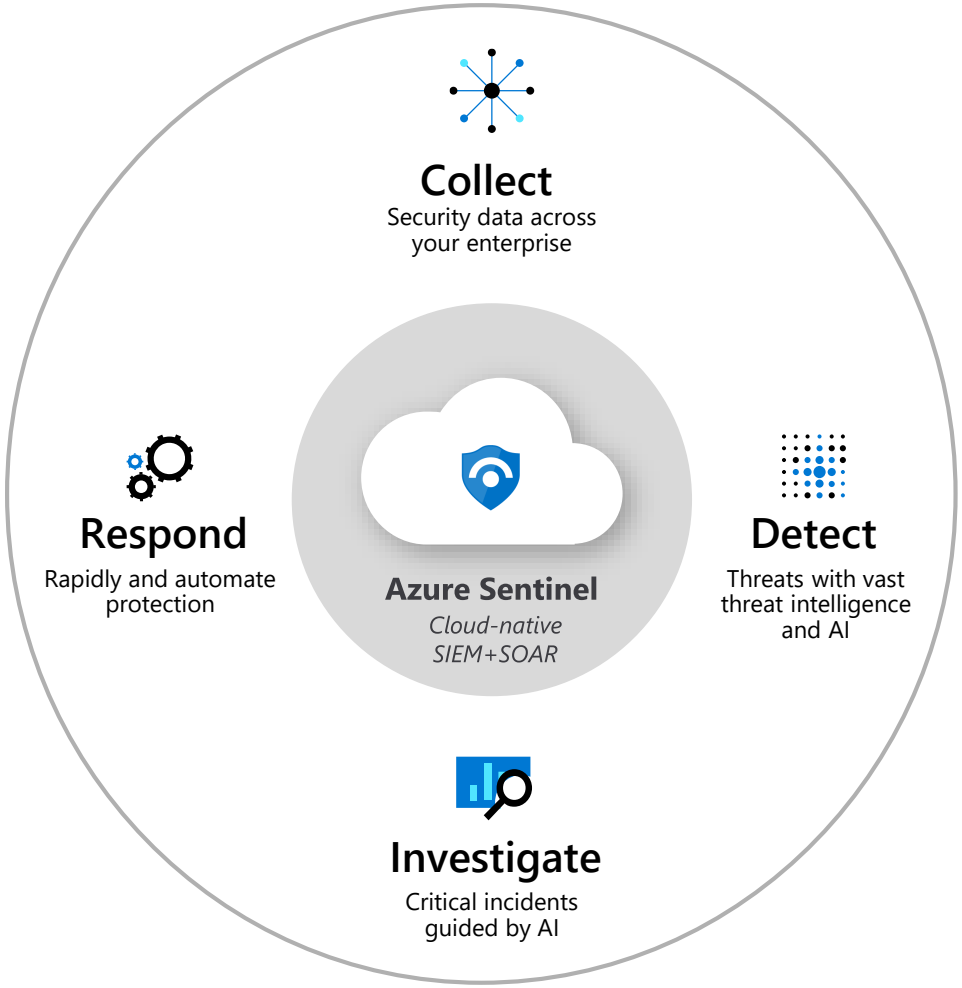
Introducing Microsoft Azure Sentinel

Cloud-native SIEM for intelligent security analytics for your entire enterprise

Limitless cloud speed and scale

Easy integration with your **existing tool set**

Faster threat protection with **AI by your side**



Cloud native

Focus on security, unburden SecOps from IT tasks

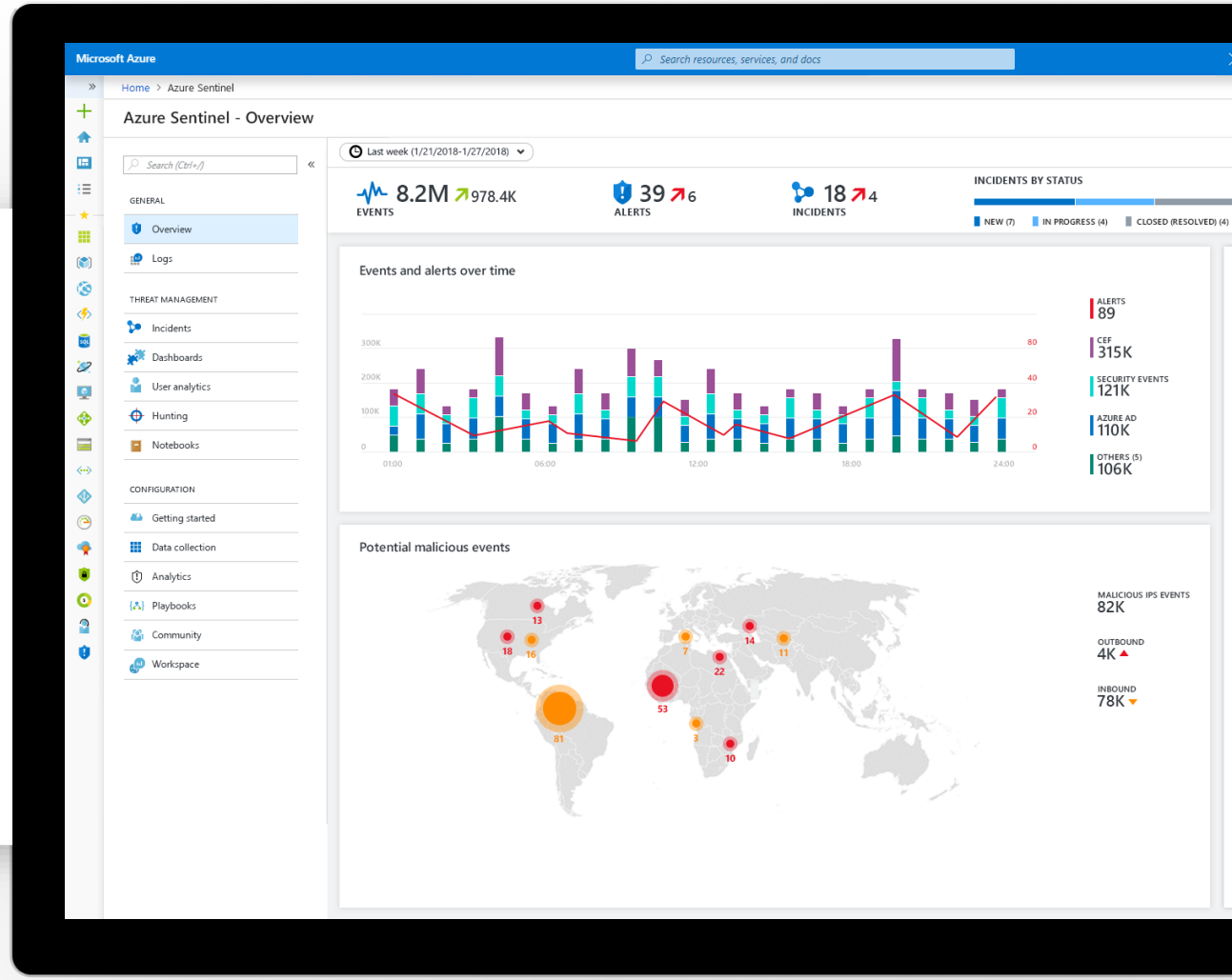
No infrastructure cost, setup or maintenance

Simple, serverless integration

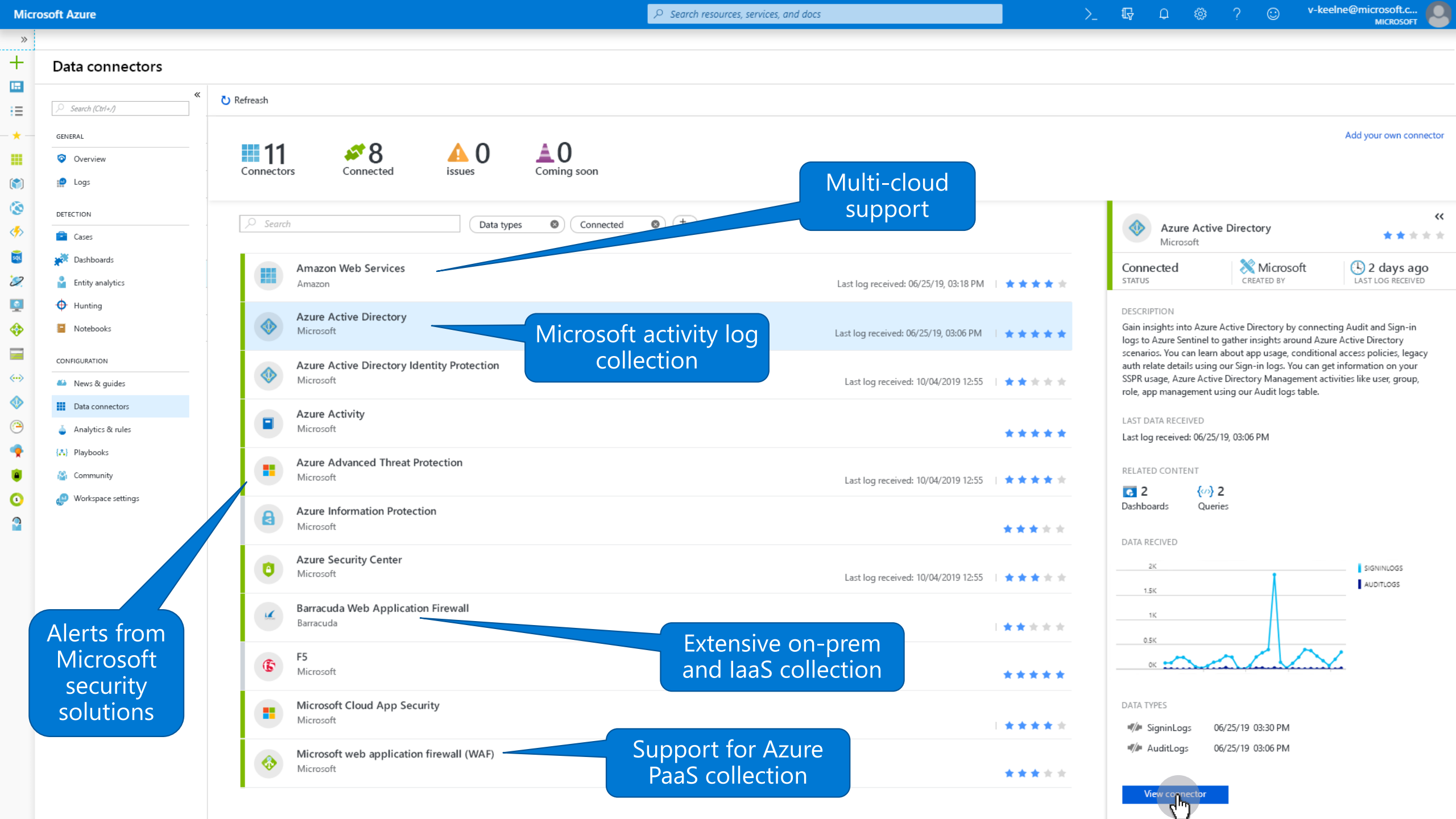
No limits to compute or storage resources

Scale automatically from a single use case to a full SIEM and data lake.

AI at cloud scale



Connect


Microsoft Azure
Search resources, services, and docs
v-keelne@microsoft.c...
MICROSOFT
Data connectors
Search (Ctrl+/)
GENERAL
Overview
Logs
DETECTION
Cases
Dashboards
Entity analytics
Hunting
Notebooks
CONFIGURATION
News & guides
Data connectors
Analytics & rules
Playbooks
Community
Workspace settings
Refresh
11 Connectors
8 Connected
0 issues
0 Coming soon
Add your own connector
Search
Data types
Connected
Amazon Web Services
Amazon
Last log received: 06/25/19, 03:18 PM
Azure Active Directory
Microsoft
Last log received: 06/25/19, 03:06 PM
Azure Active Directory Identity Protection
Microsoft
Last log received: 10/04/2019 12:55
Azure Activity
Microsoft
Azure Advanced Threat Protection
Microsoft
Last log received: 10/04/2019 12:55
Azure Information Protection
Microsoft
Azure Security Center
Microsoft
Last log received: 10/04/2019 12:55
Barracuda Web Application Firewall
Barracuda
F5
Microsoft
Microsoft Cloud App Security
Microsoft
Microsoft web application firewall (WAF)
Microsoft
Multi-cloud support
Microsoft activity log collection
Extensive on-prem and IaaS collection
Support for Azure PaaS collection
Alerts from Microsoft security solutions
Azure Active Directory
Microsoft
Connected
STATUS
Microsoft
CREATED BY
2 days ago
LAST LOG RECEIVED
DESCRIPTION
Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your SSPR usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.
LAST DATA RECEIVED
Last log received: 06/25/19, 03:06 PM
RELATED CONTENT
2 Dashboards
2 Queries
DATA RECIVED
2K
1.5K
1K
0.5K
0K
SIGNINLOGS
AUDITLOGS
DATA TYPES
SigninLogs 06/25/19 03:30 PM
AuditLogs 06/25/19 03:06 PM
View connector

Azure Active Directory

Refreash

Azure Active Directory
Microsoft

Connected
STATUS

Microsoft
CREATED BY

2 days ago
LAST LOG RECEIVED

DESCRIPTION

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your SSPR usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

LAST DATA RECEIVED

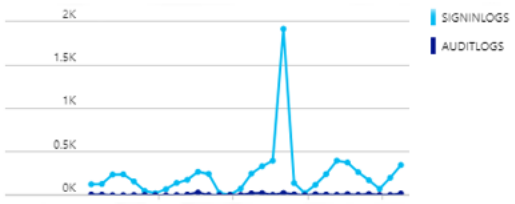
Last log received: 06/25/19, 03:06 PM

RELATED CONTENT

2 Dashboards

2 Queries

DATA RECIVED



DATA TYPES

SigninLogs	06/25/19 03:30 PM
AuditLogs	06/25/19 03:06 PM

Instructions | Data Insights

Recommended dashboards (2)

Go to dashboard gallery >

Azure AD Sign-in logs
MICROSOFT User behavior analytics

Azure AD Audit logs
MICROSOFT User behavior analytics

Query samples (2)

All logs

```
(SigninLogs)
take 1000
| sort by TimeGenerated
```

Run

Summarize by 1 hour bins

```
C(AuditLogs)
| summarize count() by bin(TimeGenerated, 1h)
| sort by TimeGenerated
```

Run

Alert rules (3)

Go to log analytics >

ALERT NAME	DESCRIPTION	CREATION TIME
User created and logged on to critical	Some long description of the alert togive some	01/24/2019 10:18 AM
Suspicious process execution after...	Some long description of the alert togive some	01/24/2019 10:18 AM
Computers with cleaned event logs	Some long description of the alert togive some	01/24/2019 10:18 AM

Hunting queries (3)

Go to Hunting>

Visualize and search

Azure AD Sign-ins - CyberSecurity... | New dashboard | Upload | Download | Edit | Unshare | Full screen | Clone | Delete

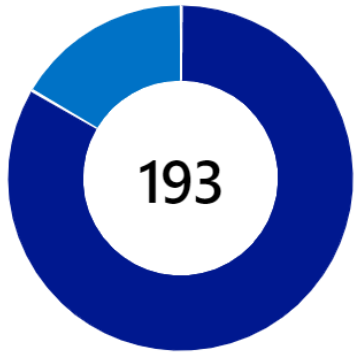
UTC Time : **Past 24 hours**

Azure AD sign-in log overview

Edit

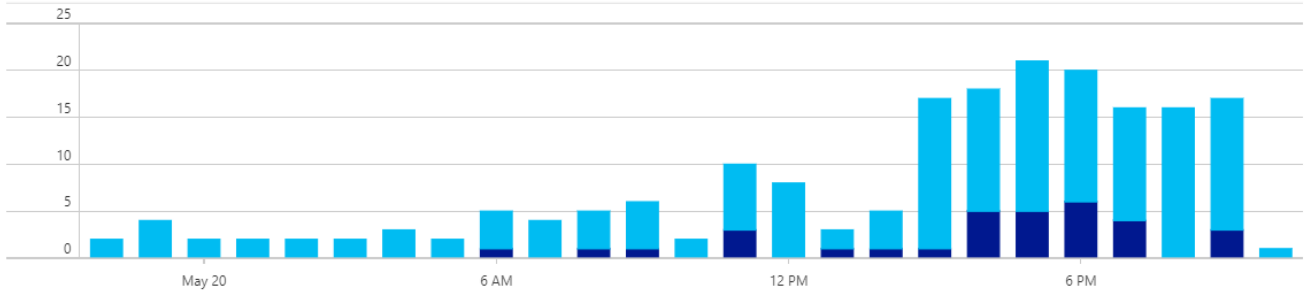
Edit

Sign-in status

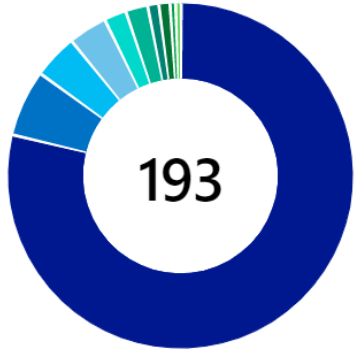


Successful
161
Failed
32.0

Sign-ins overtime

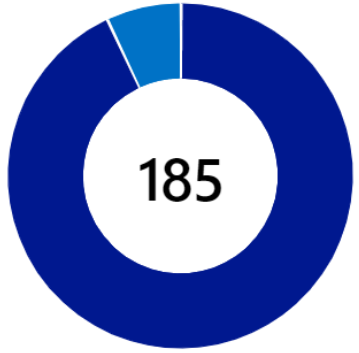


Sign-ins, by application



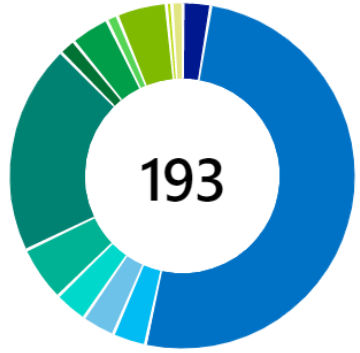
Azure Portal
152
Azure Advanced Threat Prote...
12.0
Office 365 Exchange Online
8.0
Azure Notebooks
7.0
Microsoft Cloud App Security
4.0
Microsoft Azure CLI
4.0

Sign-ins, by device



Windows 10
172
MacOs
13.0

Application sign-ins, by location



US
98.0
GB
38.0
BE
10.0
JP
9.0
BR
7.0
IL
6.0

Dashboards

Sign-ins, by device

OS	BROWSER	AMOUNT

Application sign-ins, by location

LOCATION	APPDISPLAYNAME	SIGNINCOUNT

Palo Alto Networks Threat - Cyber...

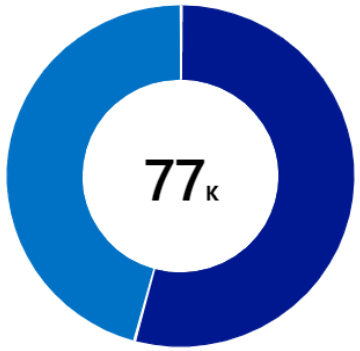
New dashboard | Upload | Download | Edit | Unshare | Full screen | Clone | Delete

UTC Time : **Past 24 hours**

Palo Alto network threat

Edit

WildFire verdicts

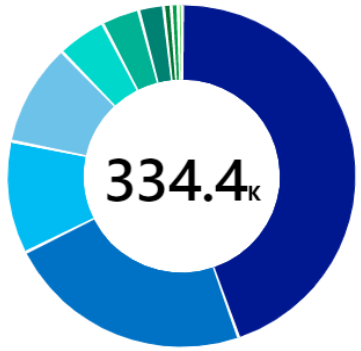


malicious 42 K
benign 35 K

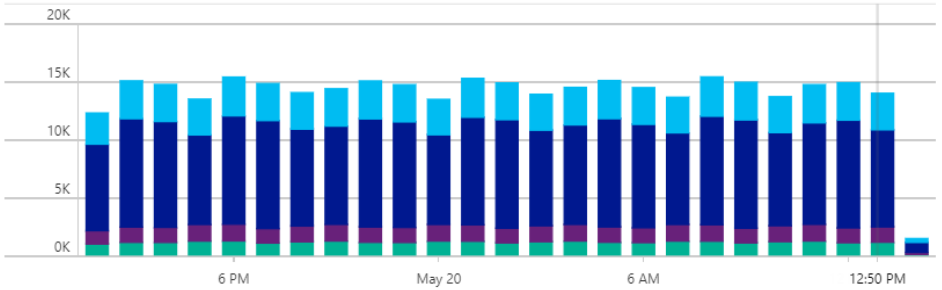
Threats, by subtypes

vulnerability 211 K
wildfire 77 K
virus 33 K
wildfire-virus 30 K

Threats, by application

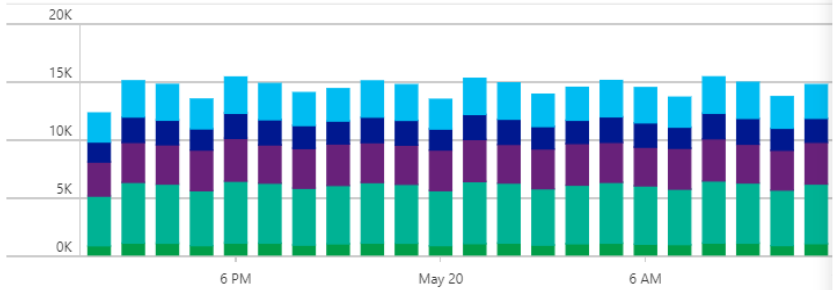


Threat subtypes over time



WILDFIRE
VULNERABILI...
VIRUS
WILDFIRE-VI...

Threat severity over time



Top vulnerability events

THREATID	LOGSEVERITY	COUNT_
UTTP GET Requests Long URL Anomaly(3	low	16.07 K

Top virus and malware events

REQUESTURL	DEVICEEVENTCLASSID	DESTINATIONIP	SOURCEIP
"UPadJGNZEXqNifnEtEi	virus	74.125.127.113	10.154.229.79

All dashboards

Type
Shared dashboards

Subscriptions: Microsoft Azure Sponsorship 2

- Azure AD Sign-ins - CyberSecurityDemo
- Azure Firewall - CyberSecurityDemo
- AzureNetworkWatcher - CyberSecurityDemo
- Azure web application firewall (WAF) - Cyber...
- Check Point Software Technologies Dashboar...
- Cisco - CyberSecurityDemo
- Exchange Online - CyberSecurityDemo
- F5 BIGIP ASM - CyberSecurityDemo
- FortiGate - CyberSecurityDemo
- Identity & Access - CyberSecurityDemo
- Insecure Protocols - CyberSecurityDemo
- Juniper - CyberSecurityDemo
- LinuxMachinesDashboard - CyberSecurityDe...
- Office 365 - CyberSecurityDemo
- Palo Alto Networks - CyberSecurityDemo
- Palo Alto Networks Threat - CyberSecurityDe...
- SharePoint & OneDrive - CyberSecurityDemo
- Symantec File Threats Overview Dashboard - ...
- Symantec File Threats Overview Dashboard - ...
- Symantec Security Overview Dashboard - Cy...
- Symantec Security Overview Dashboard - Cy...
- Symantec URL Threats Overview Dashboard -...
- Symantec URL Threats Overview Dashboard -...
- Threat Intelligence Dashboard - CyberSecurit...

4.8M ↘ 4.3K
Events

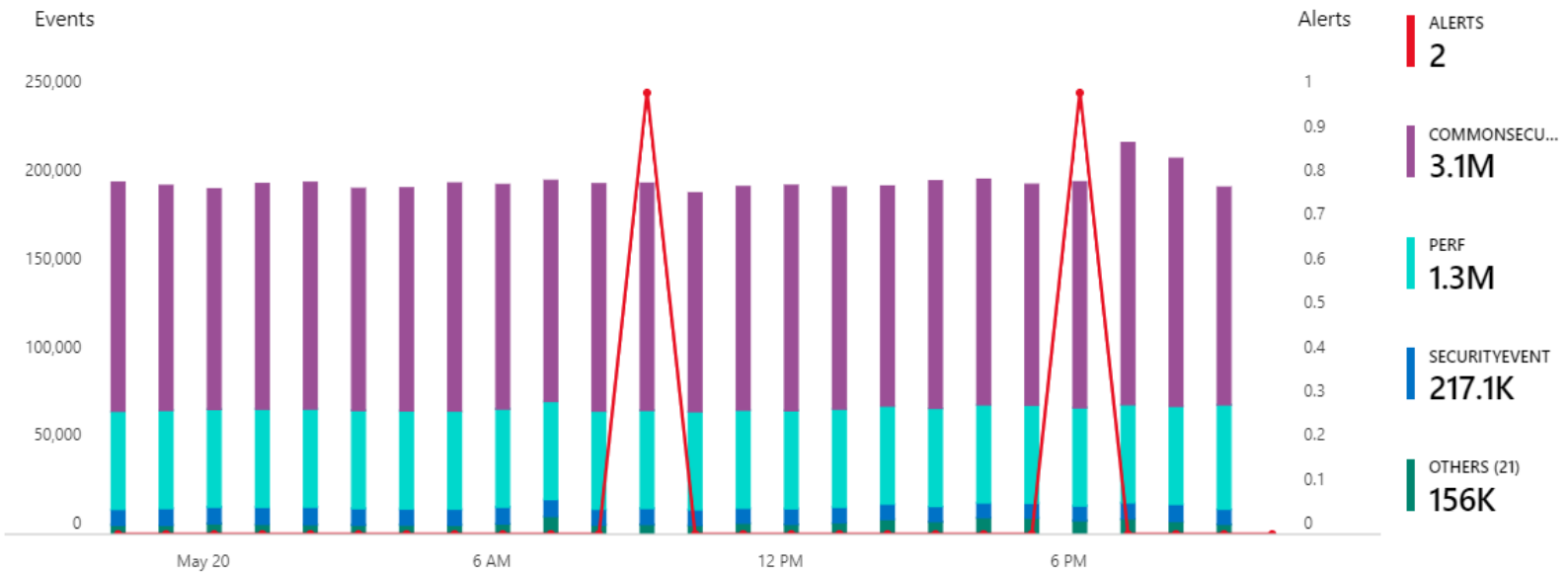
2 ↘ 5
Alerts

8
Cases

CASES BY STATUS

NEW (8) | IN PROGRESS (0) | CLOSED (RESOLVED) (0) | CLOSED (DISMISSED) (0)

Events and alerts over time



ALERTS
2

COMMONSECU...
3.1M

PERF
1.3M

SECURITYEVENT
217.1K

OTHERS (21)
156K

Potential malicious events

POTENTIAL MALICIOUS EVENTS
10

OUTBOUND
0 ▲

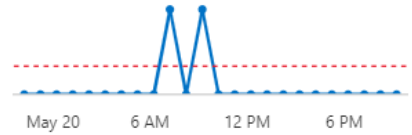
INBOUND AND UNKNOWN
10 ▼

Recent cases

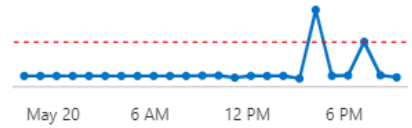
Anomalous login	1 Alerts
User Account Created and Deleted within 24 hours	1 Alerts
DNS tor proxies	1 Alerts
Signins from IP's that attempted to sign in to disa...	1 Alerts
Base64 encoded Windows executables in process ...	1 Alerts

Data source anomalies

DnsEvents



AzureActivity



Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

Overview

Demo queries

Help Settings Sample queries Query explorer

CyberSecurityDemo

Run

Time range: Set in query

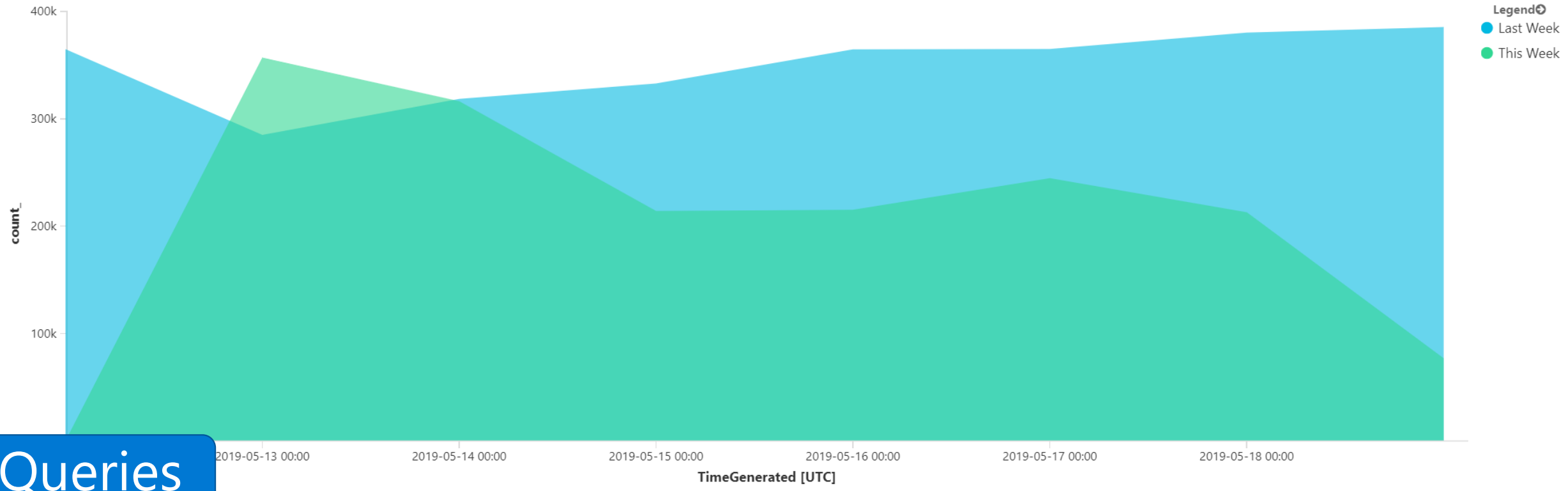
Save Copy link Export New alert rule Pin

```
// week over week query
SecurityEvent
| where TimeGenerated > ago(14d)
| summarize count() by bin(TimeGenerated, 1d)
| extend Week = iff(TimeGenerated>ago(7d), "This Week", "Last Week"), TimeGenerated = iff(TimeGenerated>ago(7d), TimeGenerated, TimeGenerated + 7d)
```

Completed

00:00:01.732 15 records

TABLE CHART Unstacked Area TimeGenerated Count_ Week Sum Display time (UTC+00:00)



Schema and Filter

Queries

Detect and Investigate

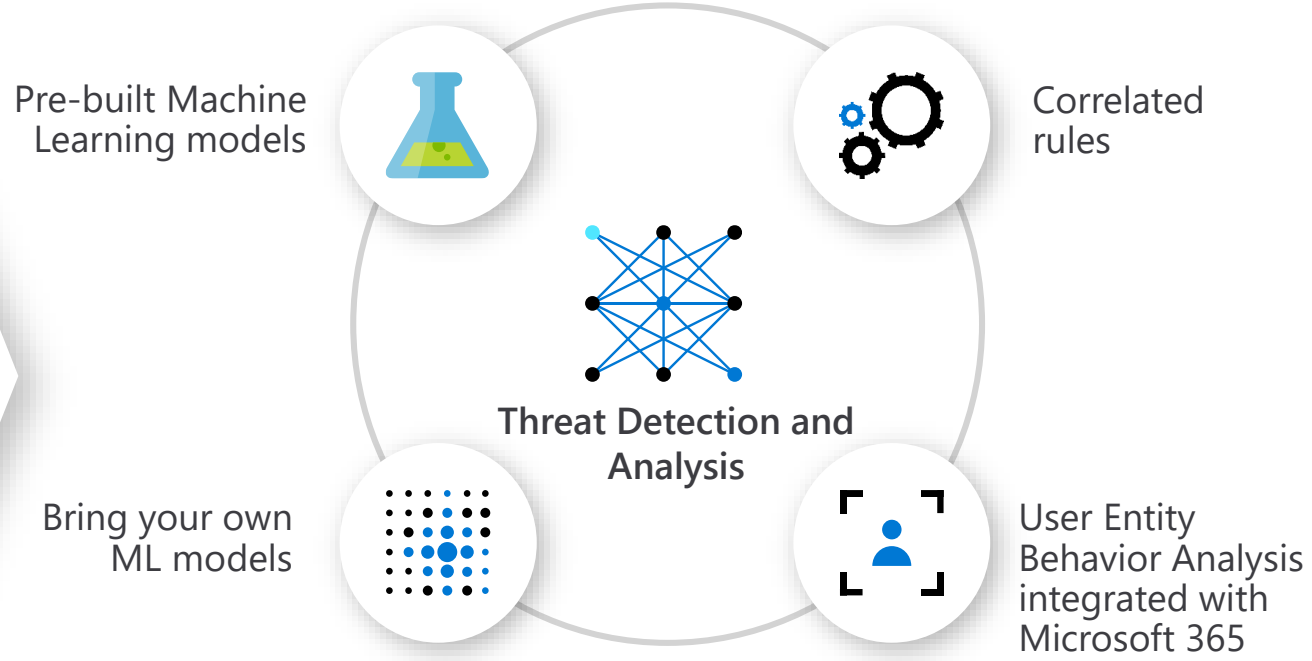
Detect threats and analyze security data quickly with AI

ML models based on **decades of Microsoft security experience and learnings**

Millions of signals filtered to few **correlated and prioritized incidents**

Insights based on vast **Microsoft threat intelligence** and your own TI

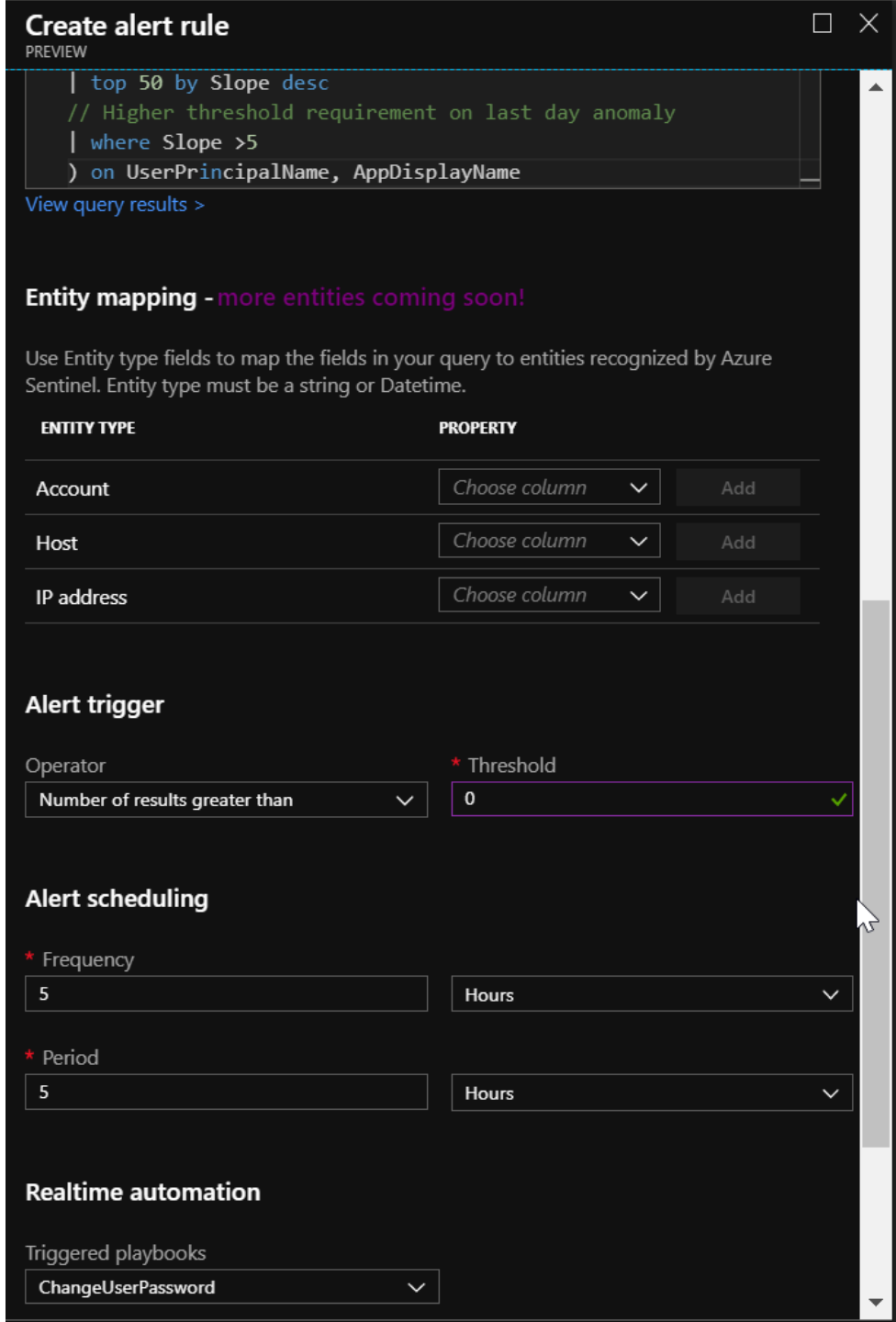
Reduce alert fatigue by up to 90%



Microsoft Azure

Correlation rules

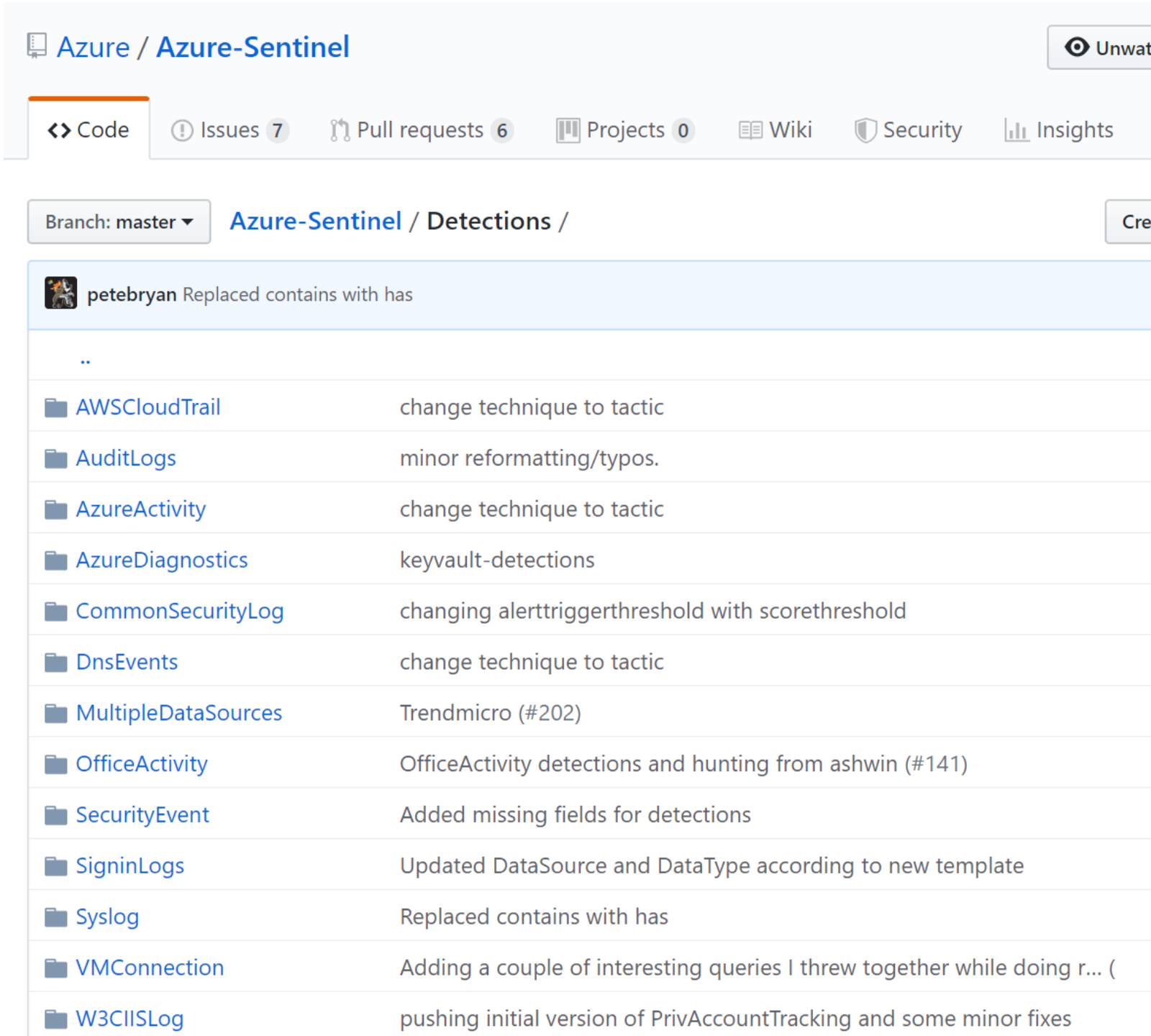
1. Query based
2. Simulation predicts alerts volume
3. Map entities
4. Automatically run playbooks



Microsoft Azure

Out of the Box Detection

1. GitHub: Microsoft and community rules.
2. Built-in ML
3. Microsoft TI



Microsoft Azure

Fusion

Analyzing activities across multiple cloud services into high-fidelity security cases using Graph-powered Machine Learning

Activity

- Identity (300 billion)
- Office 365 activity (500 billion)
- Azure activity (320 billion)

Anomalous signals

- Identity signals (280 million)
- Anomalous Office 365 signals (20 million)
- Anomalous Azure signals (2 million)

Graph-powered ML + probabilistic kill chain

Suspicious candidates (320)

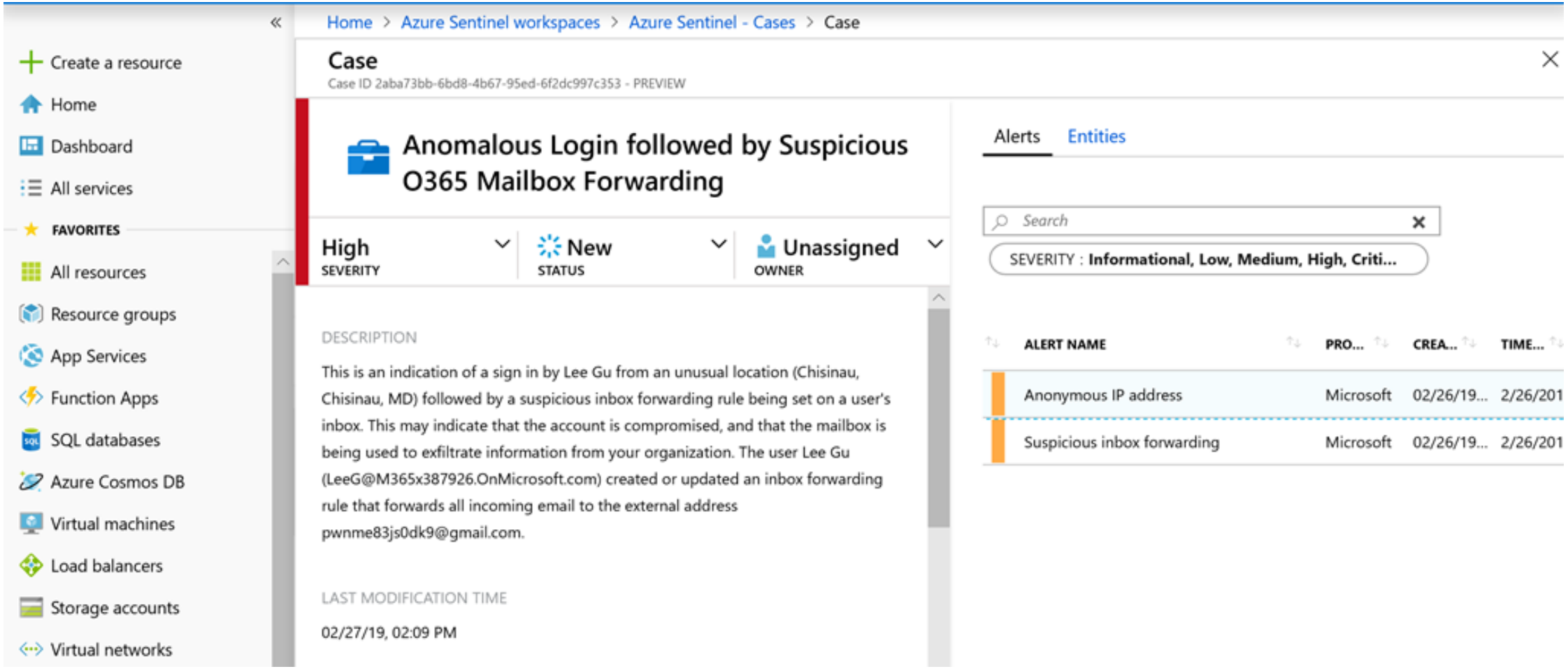
Further ML analysis

90 cases
Across 70 customers

All metrics across all Azure and Office 365 Tenants for 30 days

Microsoft Azure

Fusion example

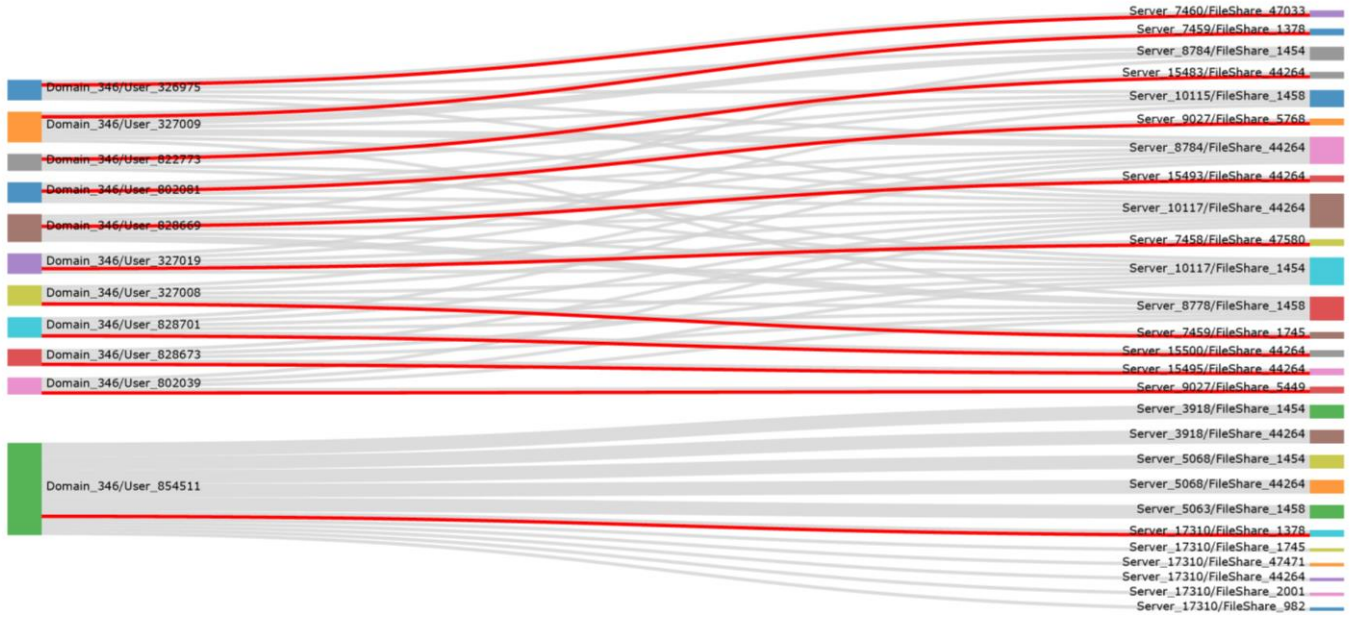


Microsoft Azure

Bring your own ML

- Behavioral correlation rules
- Jupyter notebooks
- API Access
- Use Spark & Databricks
- Microsoft research and community building blocks

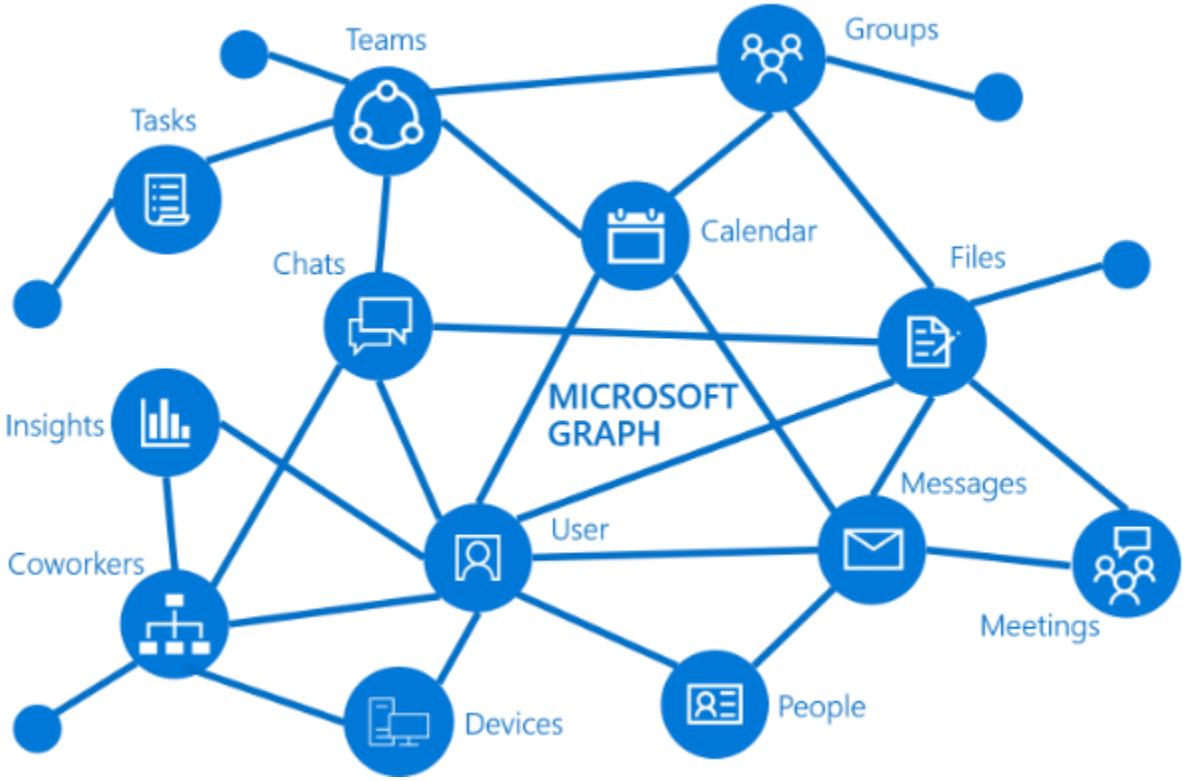
```
Cmd 15

1  pred_df = access_anomaly_model.transform(ptesting)

▸ pred_df:  pyspark.sql.dataframe.DataFrame = [tid: string, res: string ... 4 more fields]

Command took 0.11 seconds -- by anilth@microsoft.com at 2/26/2019, 10:14:49 AM on SentinelRSA2019

Cmd 16

1  pred_df.first()

▸ (1) Spark Jobs

Out[12]: Row(tid='0', res='Server_10067/FileShare_44181', user='Domain_346/User_275057', timestamp=datetime.datetime(2019,
ted_score=5.246539300750731)
```



Microsoft Azure

Threat intelligence

- Built in Microsoft TI
- Using the Graph API
- Automation based enrichment



Azure Sentinel - Cases

Selected workspace: 'CyberSecurityDemo' - PREVIEW

Refresh | Last 24 hours

8 OPEN CASES

8 NEW CASES

0 IN PROGRESS

Open Cases By Severity

CRITICAL (0) | HIGH (2) | MEDIUM (5) | LOW (0) | INFORMATIONAL (1)

Search

SEVERITY : **Informational, Low, Medium, High, Critical**

STATUS : **New, In Progress**

TITLE	ALERTS	CREATED TIME	OWNER	STATUS
Anomalous login	1	03/14/19, 11:32 AM	admin@contoso.com	New
User Account Created and Deleted within 24 hours	1	05/20/19, 6:50 PM	Unassigned	New
DNS tor proxies	1	05/20/19, 6:48 PM	Unassigned	New
Signins from IP's that attempted to sign in to disabled accounts	1	05/20/19, 6:47 PM	Unassigned	New
Base64 encoded Windows executables in process commandlines	1	05/20/19, 6:45 PM	Unassigned	New
AWS - Login to AWS Management Console without MFA	1	05/20/19, 6:44 PM	Unassigned	New
Malware in the recycle bin	1	05/20/19, 6:41 PM	Unassigned	New
Kerberos service ticket was requested	1	05/20/19, 10:05 AM	Unassigned	New
AWS - Monitor Credential abuse or hijack	1	05/20/19, 10:03 AM	Unassigned	New

Anomalous login

Medium — SEVERITY | New — STATUS | admin@con. — OWNER

DESCRIPTION

LAST UPDATE TIME

03/14/19, 11:32 AM

CREATION TIME

03/14/19, 11:32 AM

EVIDENCE

1 Alerts

ENTITIES

1 Account | 1 Host | 0 IP

Investigate | View full details

Incidents and alerts

Malware execution after malware campaign delivery

Save

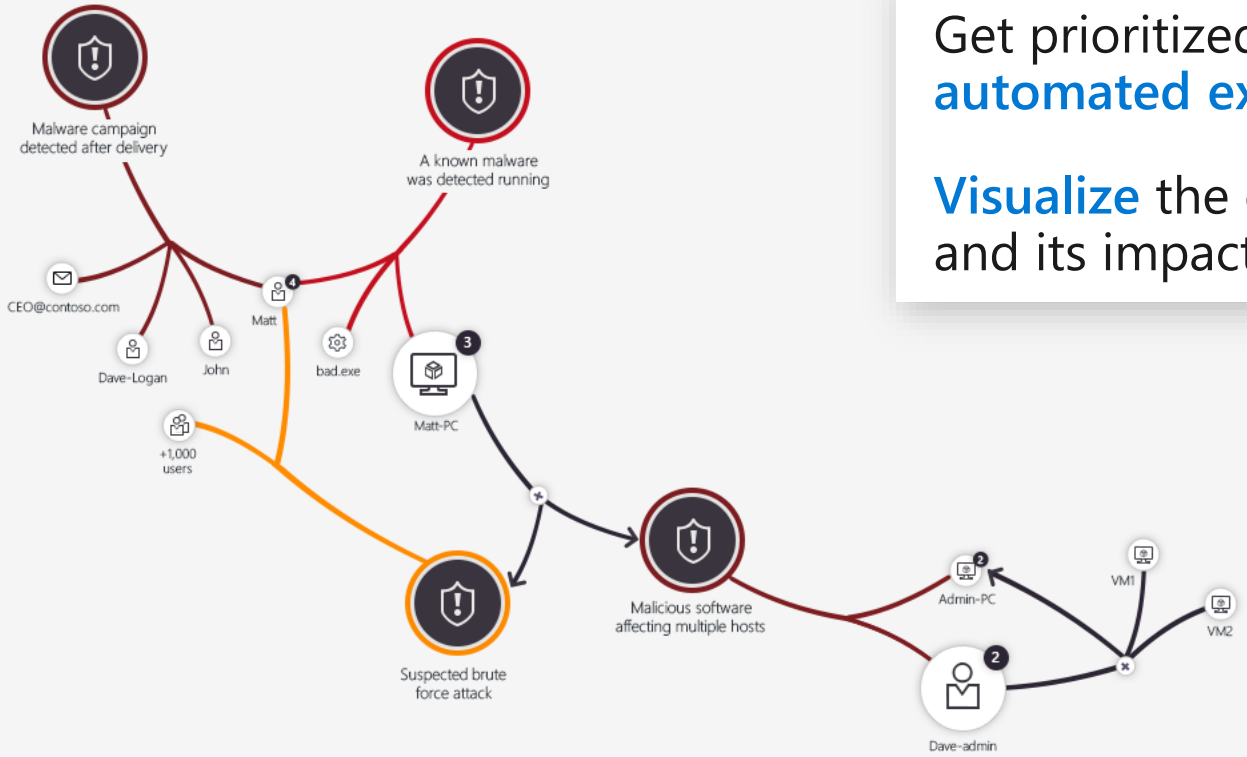
AWS - Monitor Cr...
Case

Medium
Severity

New
Status

Unassigned
Owner

2/1/2019, 08:45 AM
Last modification time



Get prioritized alerts and **automated expert guidance**

Visualize the entire attack and its impact

Timeline

Malware campaign detected after...
1/1/2019, 10:45 PM 3 1
Generates an alert when an unusually large number of messages containing malware a...

A known malware was detected...
2/1/2019, 08:30 AM 1 1
The file "bad.exe" was first detected on a local disk. The device was on the corporate netwo...

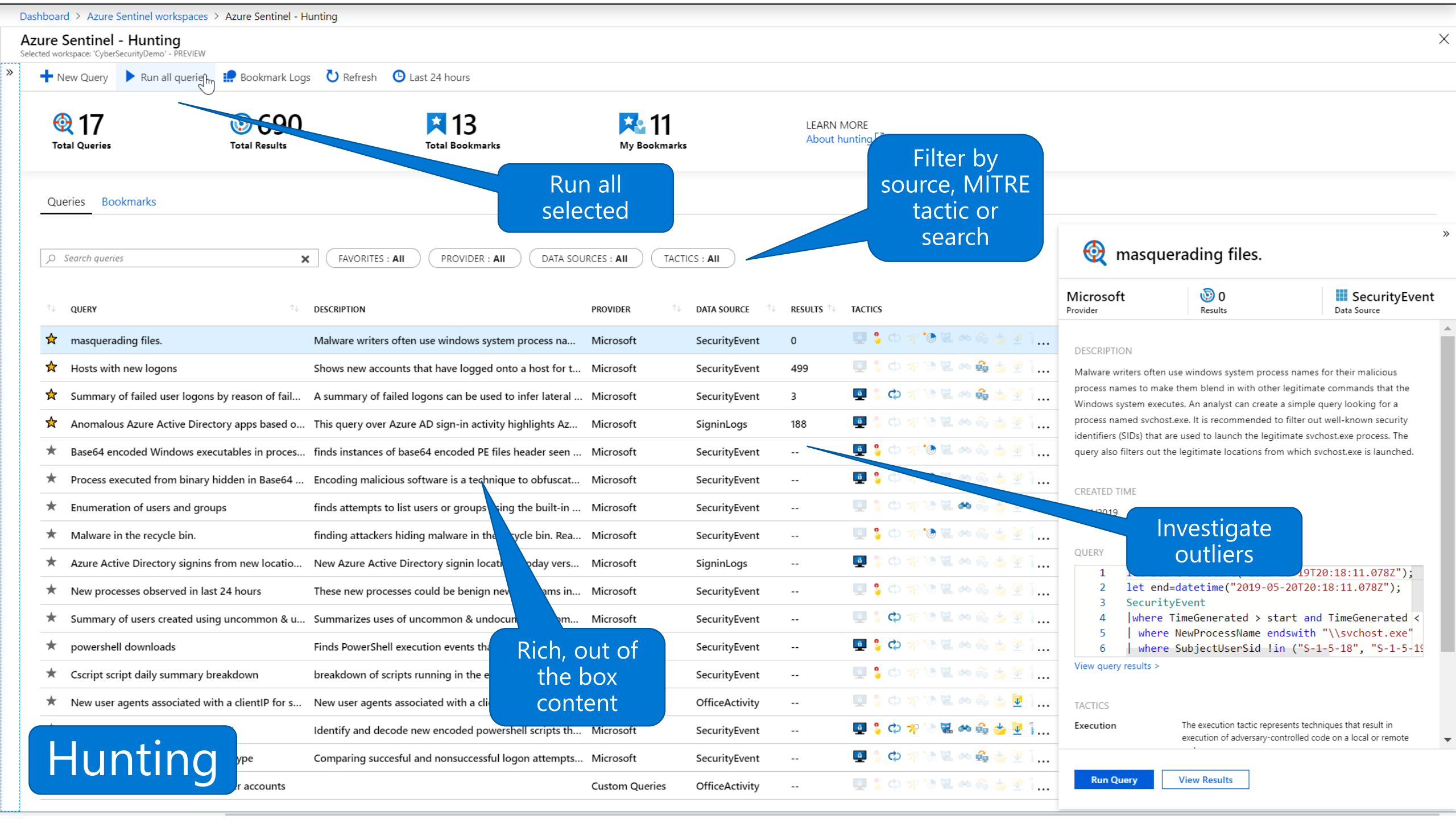
User and IP Address Reconnaissanc...
2/1/2019, 11:04 AM 1,000+ 1
Enumeration enables attackers to get information about where users recently...

Malicious software (Hacking Tool)...
2/1/2019, 03:02 PM 3
The application mimikatz.exe read memory from a system security process (lsass.exe)...

Timeline
Info
Entities
Post GA
Playbooks
Audit
Insights

Investigation

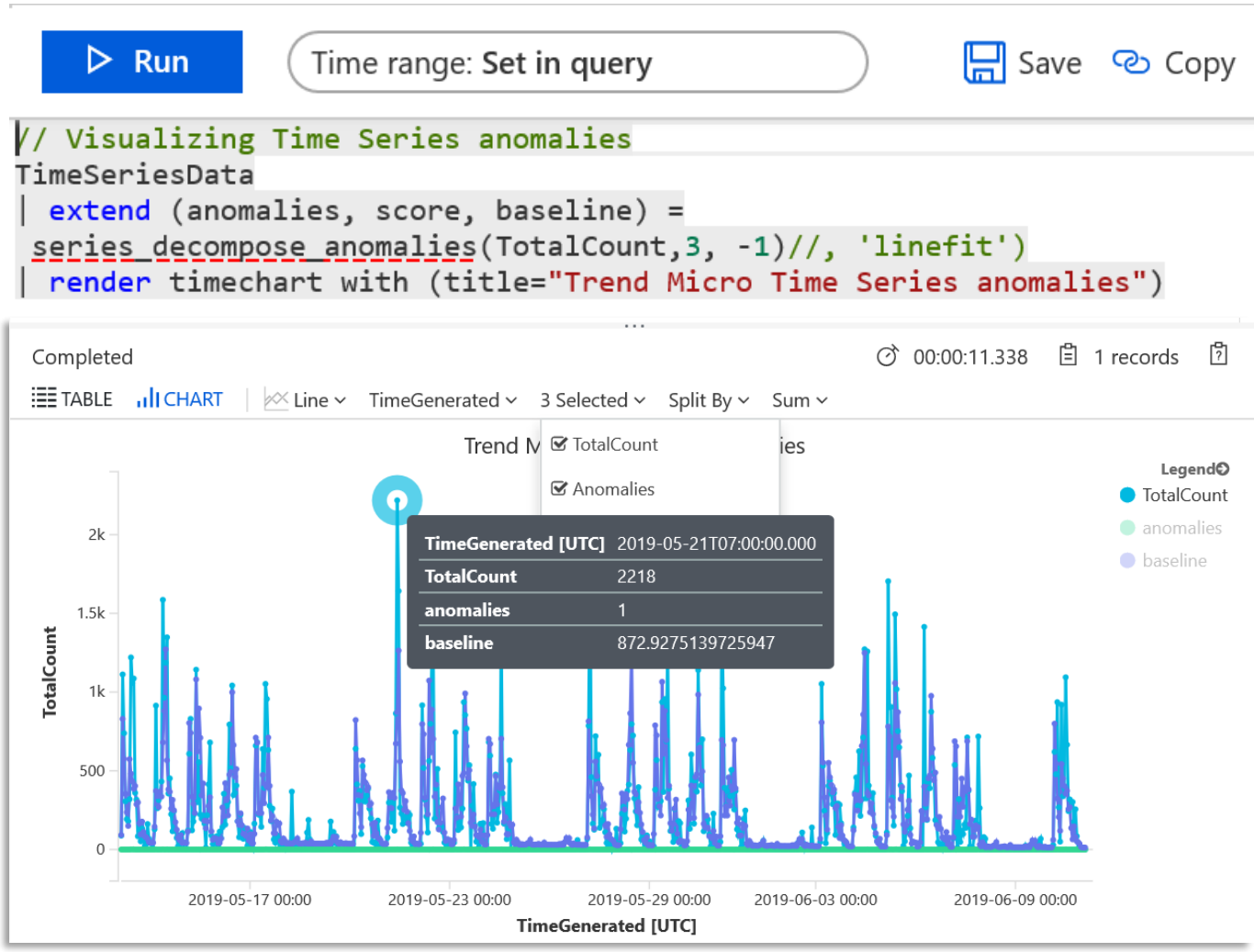
Hunt


Dashboard > Azure Sentinel workspaces > Azure Sentinel - Hunting
Azure Sentinel - Hunting
Selected workspace: 'CyberSecurityDemo' - PREVIEW
New Query
Run all queries
Bookmark Logs
Refresh
Last 24 hours
17
Total Queries
690
Total Results
13
Total Bookmarks
11
My Bookmarks
LEARN MORE
About hunting
Run all selected
Filter by source, MITRE tactic or search
Queries
Bookmarks
Search queries
FAVORITES : All
PROVIDER : All
DATA SOURCES : All
TACTICS : All
QUERY
DESCRIPTION
PROVIDER
DATA SOURCE
RESULTS
TACTICS
masquerading files.
Malware writers often use windows system process na...
Microsoft
SecurityEvent
0
Hosts with new logons
Shows new accounts that have logged onto a host for t...
Microsoft
SecurityEvent
499
Summary of failed user logons by reason of fail...
A summary of failed logons can be used to infer lateral ...
Microsoft
SecurityEvent
3
Anomalous Azure Active Directory apps based o...
This query over Azure AD sign-in activity highlights Az...
Microsoft
SigninLogs
188
Base64 encoded Windows executables in proces...
finds instances of base64 encoded PE files header seen ...
Microsoft
SecurityEvent
--
Process executed from binary hidden in Base64 ...
Encoding malicious software is a technique to obfuscat...
Microsoft
SecurityEvent
--
Enumeration of users and groups
finds attempts to list users or groups using the built-in ...
Microsoft
SecurityEvent
--
Malware in the recycle bin.
finding attackers hiding malware in the cycle bin. Rea...
Microsoft
SecurityEvent
--
Azure Active Directory signins from new locatio...
New Azure Active Directory signin locati oday vers...
Microsoft
SigninLogs
--
New processes observed in last 24 hours
These new processes could be benign ne ams in...
Microsoft
SecurityEvent
--
Summary of users created using uncommon & u...
Summarizes uses of uncommon & undocu m...
Microsoft
SecurityEvent
--
powershell downloads
Finds PowerShell execution events th
SecurityEvent
--
Cscript script daily summary breakdown
breakdown of scripts running in the e
SecurityEvent
--
New user agents associated with a clientIP for s...
New user agents associated with a cli
OfficeActivity
--
Identify and decode new encoded powershell scripts th...
Microsoft
SecurityEvent
--
ype
Comparing succesful and nonsuccessful logon attempts...
Microsoft
SecurityEvent
--
r accounts
Custom Queries
OfficeActivity
--
Rich, out of the box content
Investigate outliers
masquerading files.
Microsoft
Provider
0
Results
SecurityEvent
Data Source
DESCRIPTION
Malware writers often use windows system process names for their malicious process names to make them blend in with other legitimate commands that the Windows system executes. An analyst can create a simple query looking for a process named svchost.exe. It is recommended to filter out well-known security identifiers (SIDs) that are used to launch the legitimate svchost.exe process. The query also filters out the legitimate locations from which svchost.exe is launched.
CREATED TIME
QUERY
let end=datetime("2019-05-20T20:18:11.078Z");
SecurityEvent
|where TimeGenerated > start and TimeGenerated <
| where NewProcessName endswith "\\svchost.exe"
| where SubjectUserSid !in ("S-1-5-18", "S-1-5-19
View query results >
TACTICS
Execution
The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote
Run Query
View Results
Hunting

Microsoft Azure

Visualize data sets

Automatically detect and plot anomalies in data



Demo queries

Help Settings Sample queries Query explorer

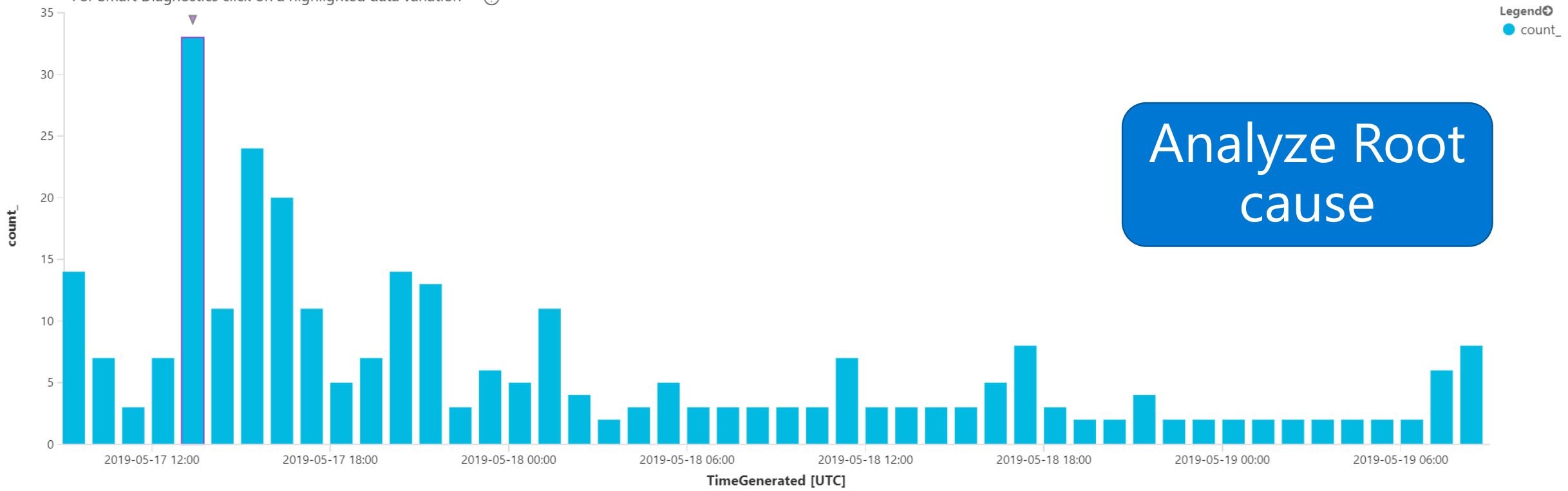
CyberSecurityDemo Run Time range: Last 48 hours Save Copy link Export New alert rule Pin

```
| extend Week = iff(TimeGenerated>ago(7d), "This Week", "Last Week"), TimeGenerated = iff(TimeGenerated>ago(7d), TimeGenerated, TimeGenerated + 7d)

SigninLogs
| summarize count() by bin(TimeGenerated, 1h)
```

Completed. Showing results from the last 48 hours. 00:00:00.871 48 records

TABLE CHART Stacked Column TimeGenerated Count_ Sum Display time (UTC+00:00)

For Smart Diagnostics click on a highlighted data variation



Analyze Root cause

Schema and Filter

Demo queries | Diagnose R... * | Help | Settings | Sample queries | Query explorer

CyberSecurityDemo | Run | Time range: Last 48 hours | Save | Copy link | Export | New alert rule | Pin

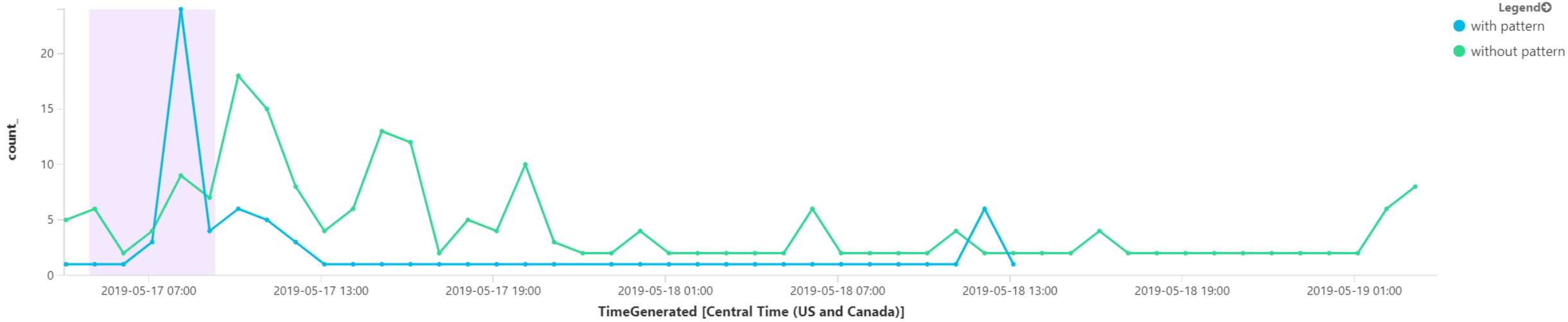
```
//
// The following pattern may explain the data discrepancy:
//
// DeviceDetail['browser'] = Chrome 76.0.3782
//
SigninLogs
| extend DiagnosticsResults = iff(DeviceDetail['browser'] == "Chrome 76.0.3782", 'with pattern', 'without pattern' )
| summarize count() by DiagnosticsResults,  bin(TimeGenerated, 1h)
| render timechart
```

Completed. Showing results from the last 48 hours. 00:00:00.537 | 81 records

TABLE | CHART | Line | TimeGenerated | Count_ | DiagnosticsResults | Sum | Display time (UTC-05:00)

The following pattern may explain the data discrepancy:

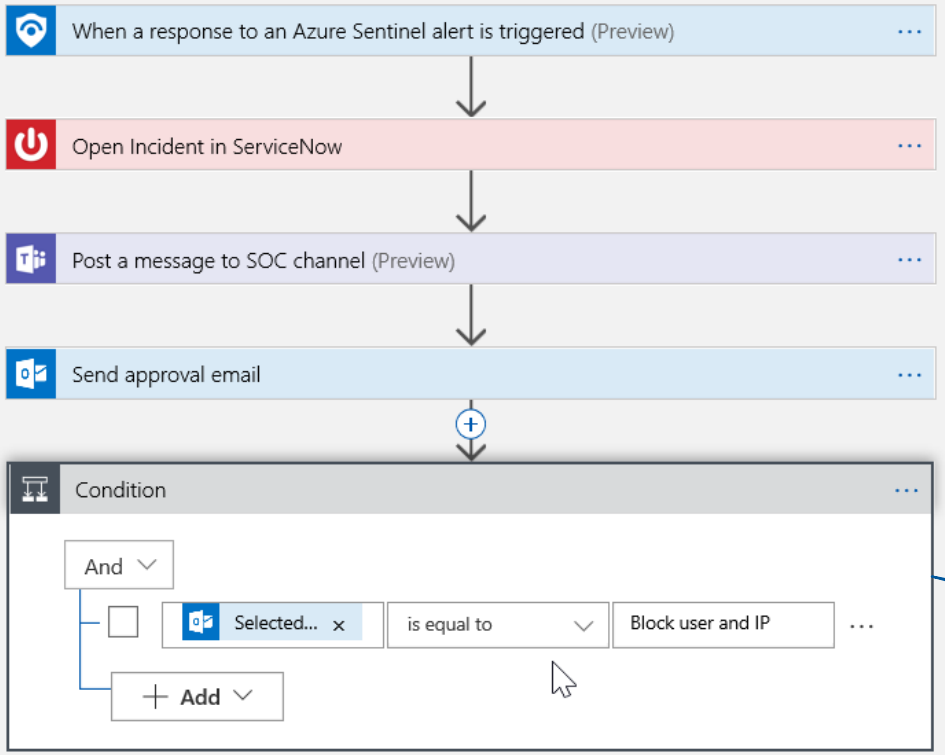
DeviceDetail['browser'] == "Chrome 76.0.3782" Run



Schema and Filter

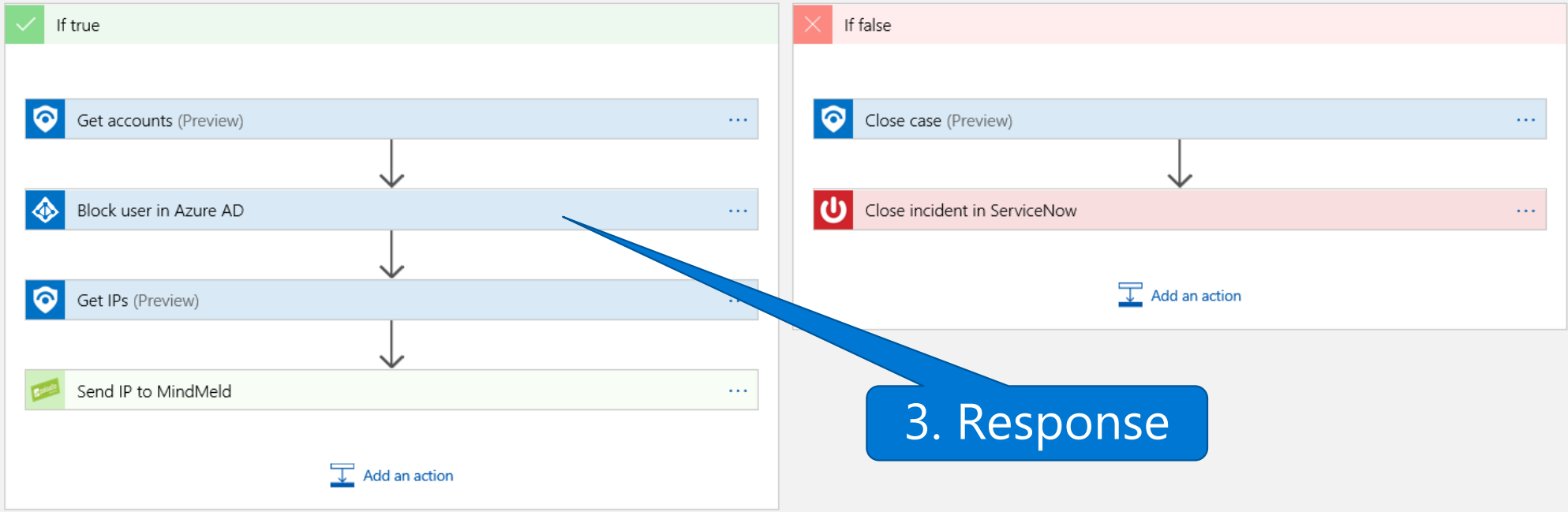
Automate and respond

playbooks use cases



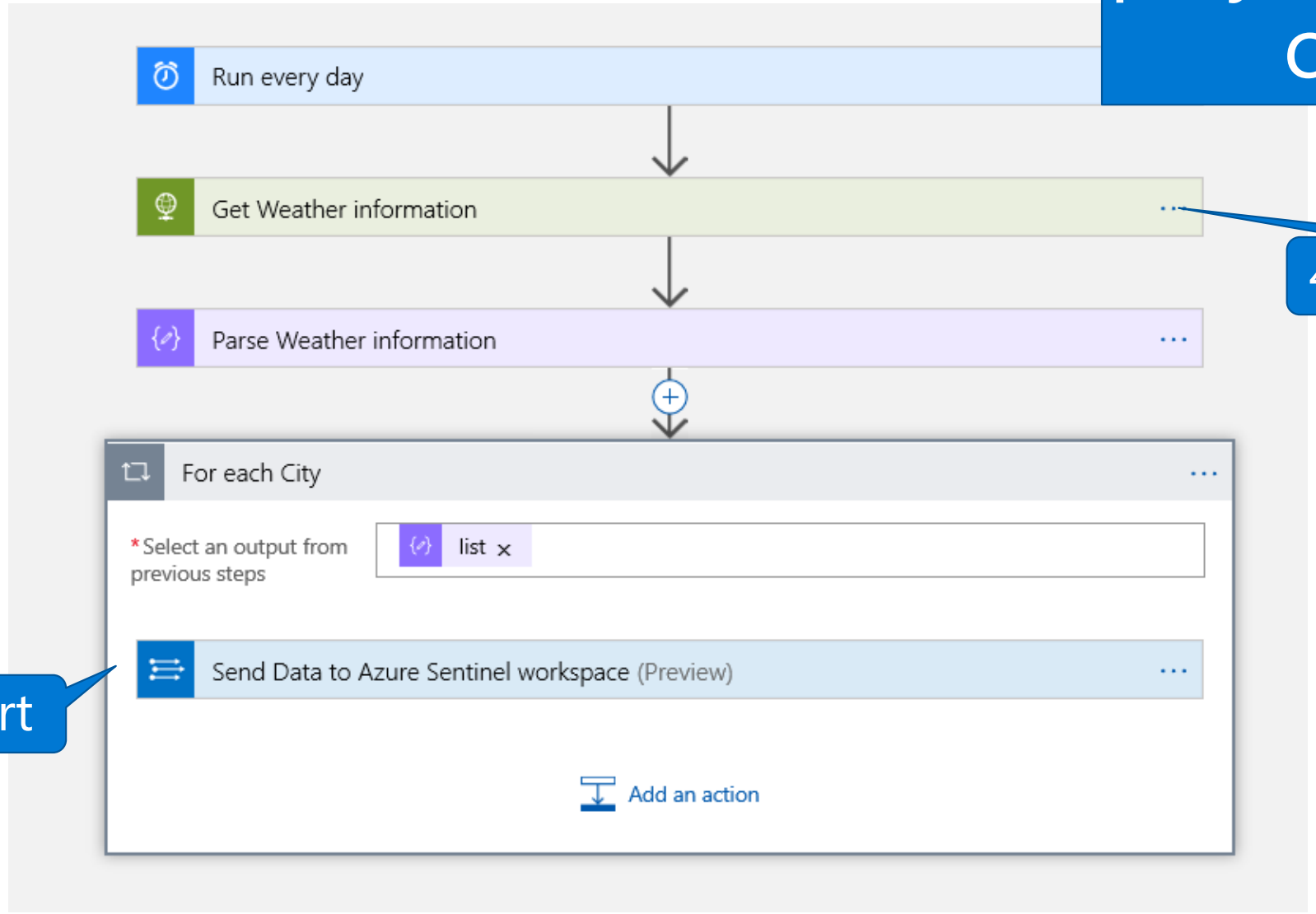
1. Integration

2. Workflow



3. Response

playbooks use cases



4. Enrichment

5. Data import

Where to go from here?

https://aka.ms/AzureSentinel

KQL Analytics

- Looking for unknown anomalies - what is normal? Time Series analysis & its applications in Security
- Performing Additional Security Monitoring of High-Value Accounts
- Anomalous sign-in location by user account and authenticating application

Built in ML

- Reducing security alert fatigue using machine learning in Azure Sentinel

Jupyter notebook

- Why (and when to) use Jupyter for security investigations?
- Using Jupyter Notebooks: Part 1, Part 2, Part 3

Fusion

Advanced Multi-Stage Attack Detection