Microsoft

# Microsoft Security Virtual Training Days: Modernize Security and Defend Against Threats

Microsoft

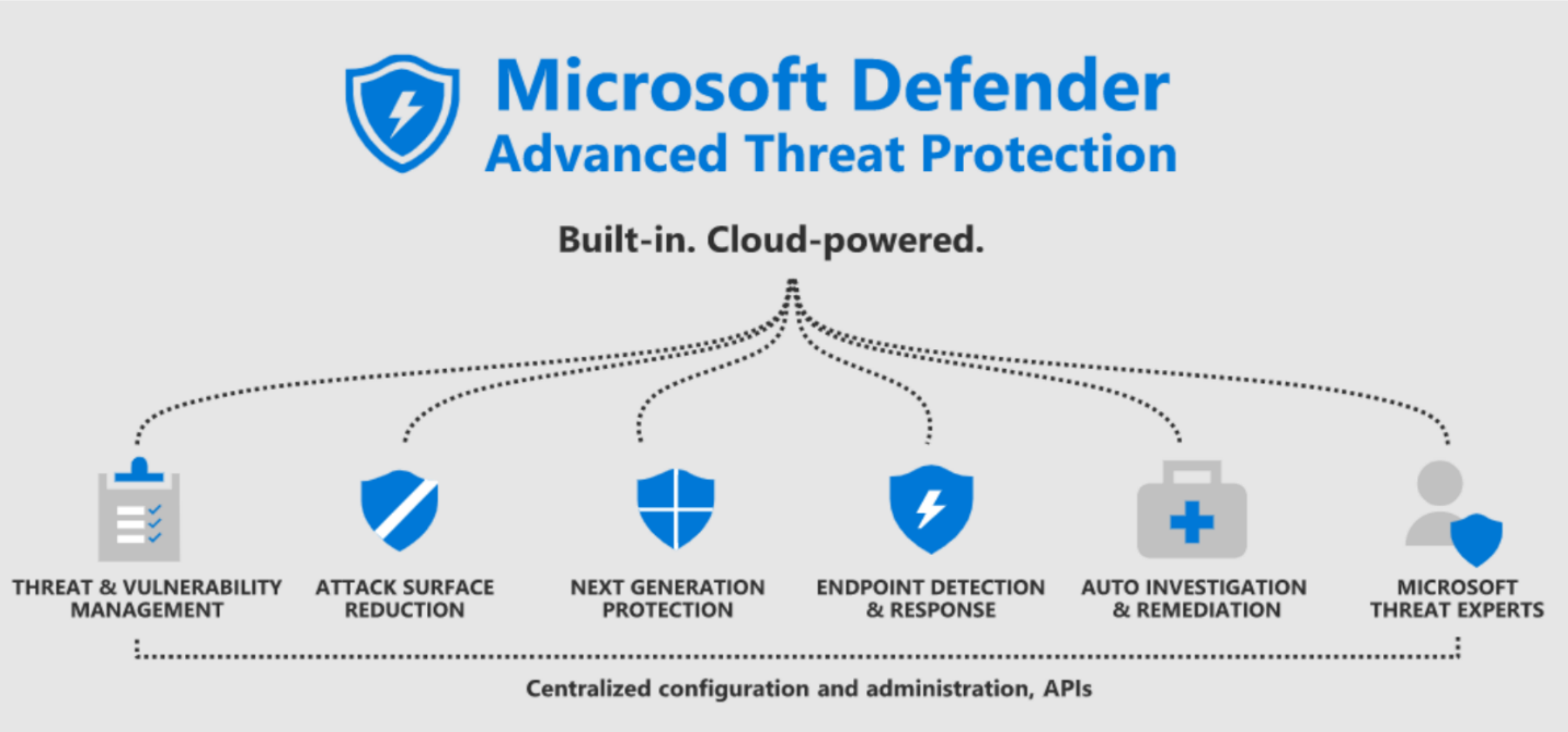
# Mitigate threats using Microsoft Defender for Endpoint

Microsoft

# Protect against threats with Microsoft Defender for Endpoint

# Microsoft Defender for Endpoint explained

Microsoft Defender for Endpoint is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats on their endpoints.


Microsoft Defender
Advanced Threat Protection
Built-in. Cloud-powered.
THREAT & VULNERABILITY MANAGEMENT
ATTACK SURFACE REDUCTION
NEXT GENERATION PROTECTION
ENDPOINT DETECTION & RESPONSE
AUTO INVESTIGATION & REMEDIATION
MICROSOFT THREAT EXPERTS
Centralized configuration and administration, APIs

# Practice security administration

- Threat and vulnerability management
- Attack surface reduction
- Next generation protection
- Endpoint detection and response
- Automated investigation and remediation
- Microsoft Threat Experts

Microsoft

# Deploy the Microsoft Defender for Endpoint environment

# Create your environment

## Microsoft Defender Security Center https://securitycenter.windows.com

### Data storage location:

Determine where you want to be hosted. You cannot change the location after this set up.

### Data retention:

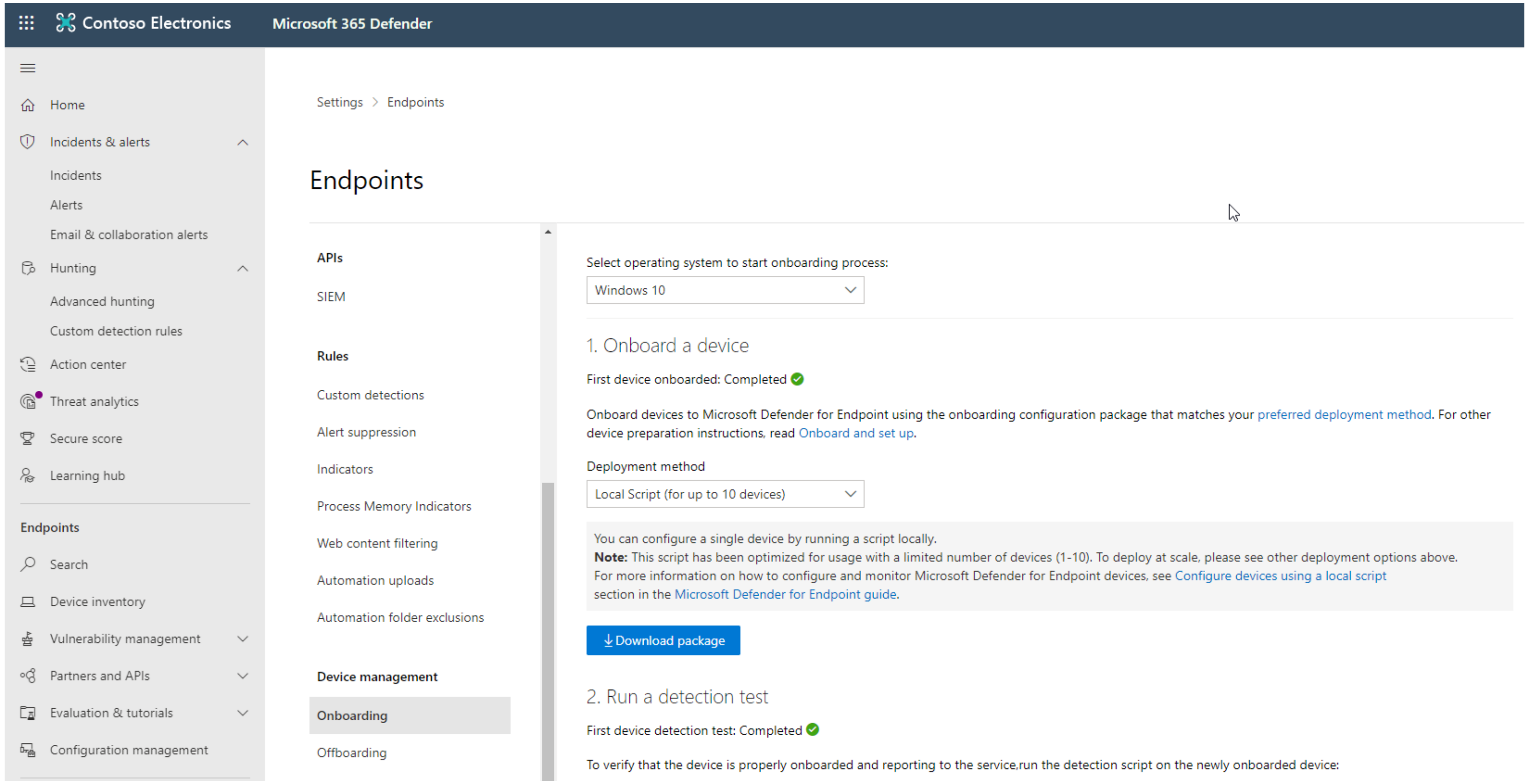
The default is six months.

### Enable preview features:

The default is on, can be changed later.

# Onboard devices

You'll need to go to the onboarding section of the Microsoft 365 Defender portal to onboard any of the supported devices. Depending on the device, you'll be guided with appropriate steps and provided management and deployment tool options suitable for the device.



Endpoints

Select operating system to start onboarding process: Windows 10

1. Onboard a device

First device onboarded: Completed ✓

Onboard devices to Microsoft Defender for Endpoint using the onboarding configuration package that matches your preferred deployment method. For other device preparation instructions, read Onboard and set up.

Deployment method: Local Script (for up to 10 devices)

You can configure a single device by running a script locally.
**Note:** This script has been optimized for usage with a limited number of devices (1-10). To deploy at scale, please see other deployment options above.
For more information on how to configure and monitor Microsoft Defender for Endpoint devices, see Configure devices using a local script section in the Microsoft Defender for Endpoint guide.

2. Run a detection test

First device detection test: Completed ✓

To verify that the device is properly onboarded and reporting to the service,run the detection script on the newly onboarded device:

# Manage access

Defender for Endpoint RBAC is designed to support your tier- or role-based model of choice and gives you granular control over what roles can see, devices they can access, and actions they can take.

## Control who can see information on a specific device group or groups:

Create device groups by specific criteria such as names, tags, domains, and others, then grant role access to them using a specific Azure Active Directory (Azure AD) user group.

## Control who can take specific actions:

Create custom roles and control what Defender for Endpoint capabilities they can access with granularity.

Microsoft

# Implement Windows 10 security enhancements

# Understand attack surface reduction

Strategies include the following:

- Attack surface reduction rules
- Hardware-based isolation
- Application control
- Exploit protection
- Web protection
- Controlled folder access
- Network firewall
- Network protection

# Enable attack surface reduction rules

## Sample ASR Rules:

- Block executable content from email client and webmail
- Block all Office applications from creating child processes
- Block Office applications from creating executable content
- Block Office applications from injecting code into other processes
- Block execution of potentially obfuscated scripts
- Use advanced protection against ransomware

## Rule options:

- Disable = 0
- Block (enable ASR rule) = 1
- Audit = 2

## Deployment options:

- Intune
- MDM
- Microsoft Endpoint Configuration Manager
- Group Policy

Microsoft

# Manage alerts and incidents

# Explain security operations in Microsoft Defender for Endpoint

- Defender for Endpoint detection and response capabilities provide advanced attack detections that are near real-time and actionable.

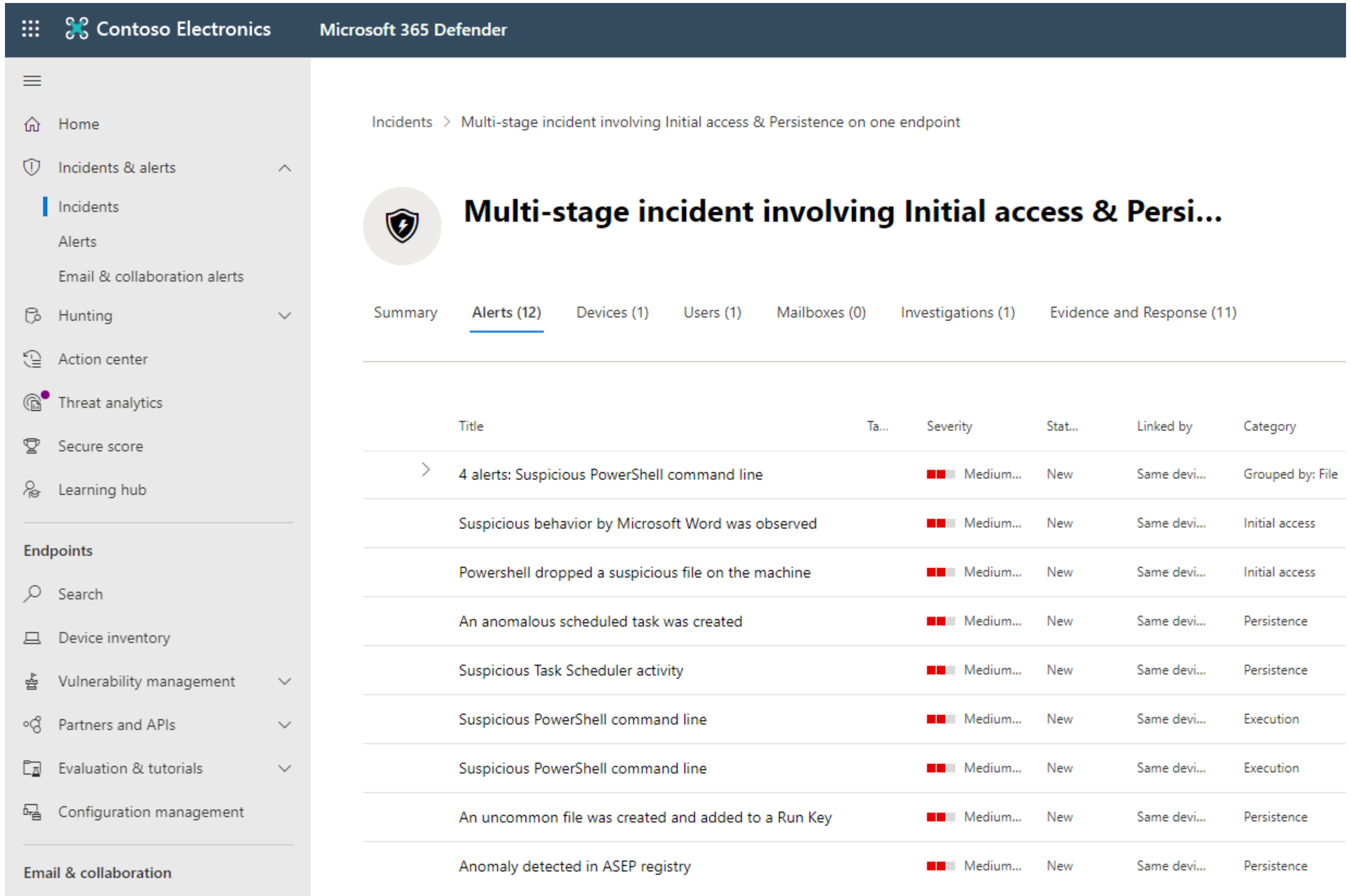
- When a threat is detected, alerts are created in the system for an analyst to investigate.

- Alerts with the same attack techniques or attributed to the same attacker are aggregated into an entity called an incident. Aggregating alerts in this manner makes it easy for analysts to investigate and respond to threats collectively.

- Inspired by the "assume breach" mindset, Defender for Endpoint continuously collects behavioral cyber telemetry. This includes process information, network activities, deep optics into the kernel and memory manager, user sign in activities, registry and file system changes, and others.

# Manage and investigate incidents

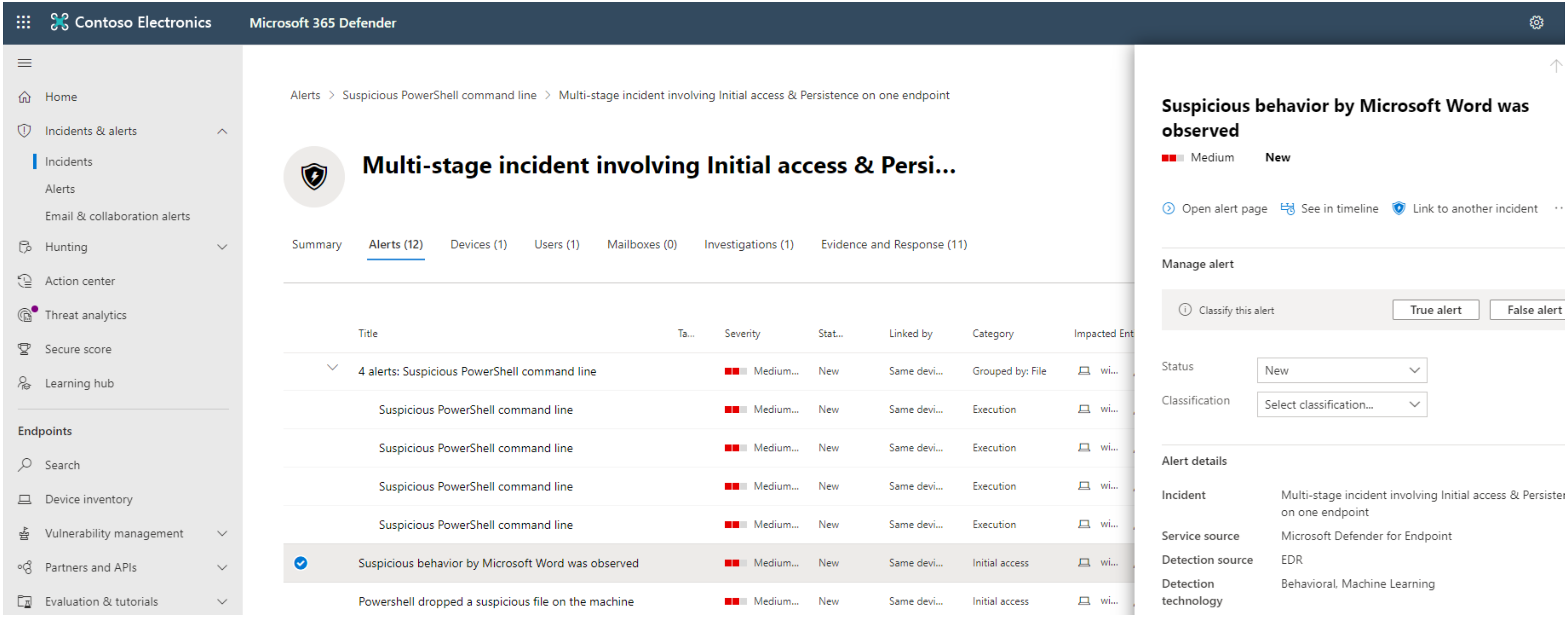
You can update Incident management information, view all related information, or jump to investigation pages for the associated data.



| Title | Ta... | Severity | Stat... | Linked by | Category |
|---|---|---|---|---|---|
| 4 alerts: Suspicious PowerShell command line | | Medium... | New | Same devi... | Grouped by: File |
| Suspicious behavior by Microsoft Word was observed | | Medium... | New | Same devi... | Initial access |
| Powershell dropped a suspicious file on the machine | | Medium... | New | Same devi... | Initial access |
| An anomalous scheduled task was created | | Medium... | New | Same devi... | Persistence |
| Suspicious Task Scheduler activity | | Medium... | New | Same devi... | Persistence |
| Suspicious PowerShell command line | | Medium... | New | Same devi... | Execution |
| Suspicious PowerShell command line | | Medium... | New | Same devi... | Execution |
| An uncommon file was created and added to a Run Key | | Medium... | New | Same devi... | Persistence |
| Anomaly detected in ASEP registry | | Medium... | New | Same devi... | Persistence |

# Manage and investigate alerts

You can update Incident management information, view all related information, or jump to investigation pages for the associated data.



Multi-stage incident involving Initial access & Persi...

| Title | Ta... | Severity | Stat... | Linked by | Category | Impacted Ent |
|---|---|---|---|---|---|---|
| 4 alerts: Suspicious PowerShell command line | | Medium... | New | Same devi... | Grouped by: File | wi... |
| Suspicious PowerShell command line | | Medium... | New | Same devi... | Execution | wi... |
| Suspicious PowerShell command line | | Medium... | New | Same devi... | Execution | wi... |
| Suspicious PowerShell command line | | Medium... | New | Same devi... | Execution | wi... |
| Suspicious PowerShell command line | | Medium... | New | Same devi... | Execution | wi... |
| Suspicious behavior by Microsoft Word was observed | | Medium... | New | Same devi... | Initial access | wi... |
| Powershell dropped a suspicious file on the machine | | Medium... | New | Same devi... | Initial access | wi... |

**Suspicious behavior by Microsoft Word was observed**

Medium **New**

Manage alert

Classify this alert

Status: New

Classification: Select classification...

Alert details

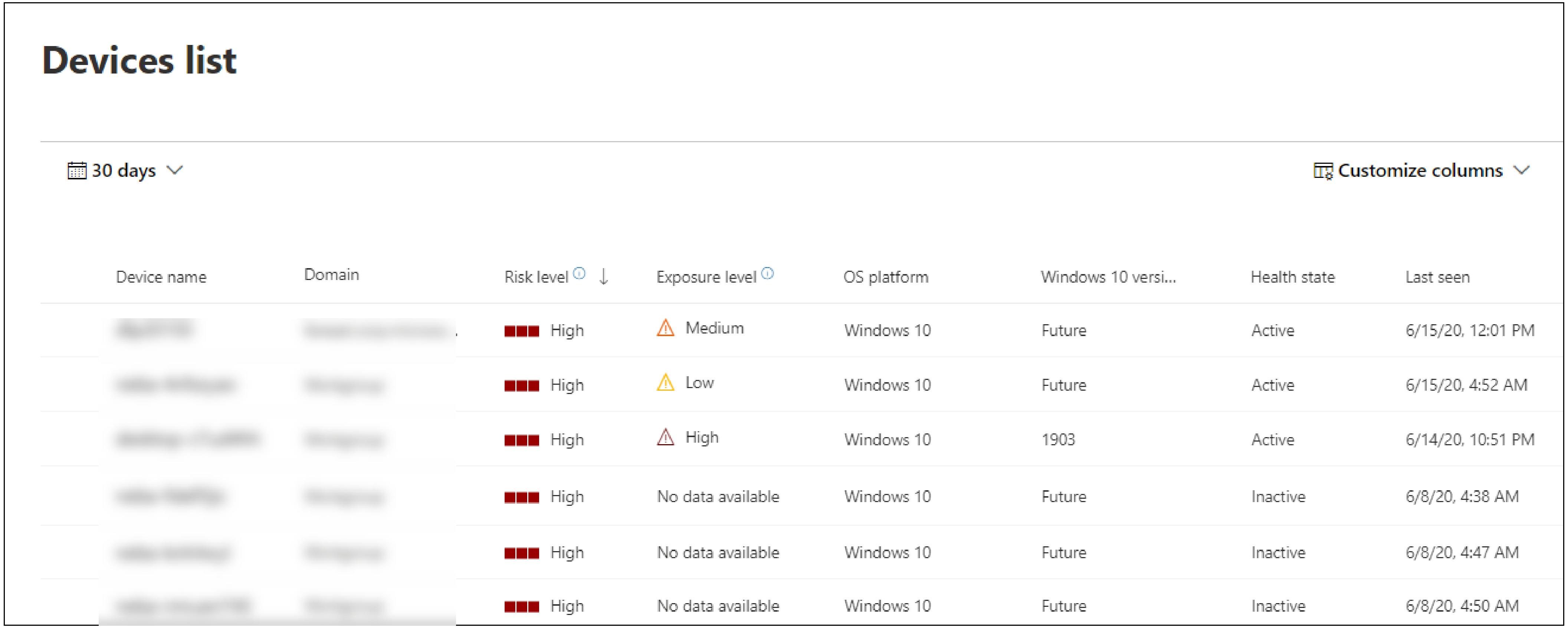
| | |
|---|---|
| **Incident** | Multi-stage incident involving Initial access & Persister on one endpoint |
| **Service source** | Microsoft Defender for Endpoint |
| **Detection source** | EDR |
| **Detection technology** | Behavioral, Machine Learning |

Microsoft

# Perform device investigations

# Use the device inventory list

The Device inventory page shows a list of the devices in your network where alerts were generated. By default, the queue displays devices with alerts seen in the last 30 days.

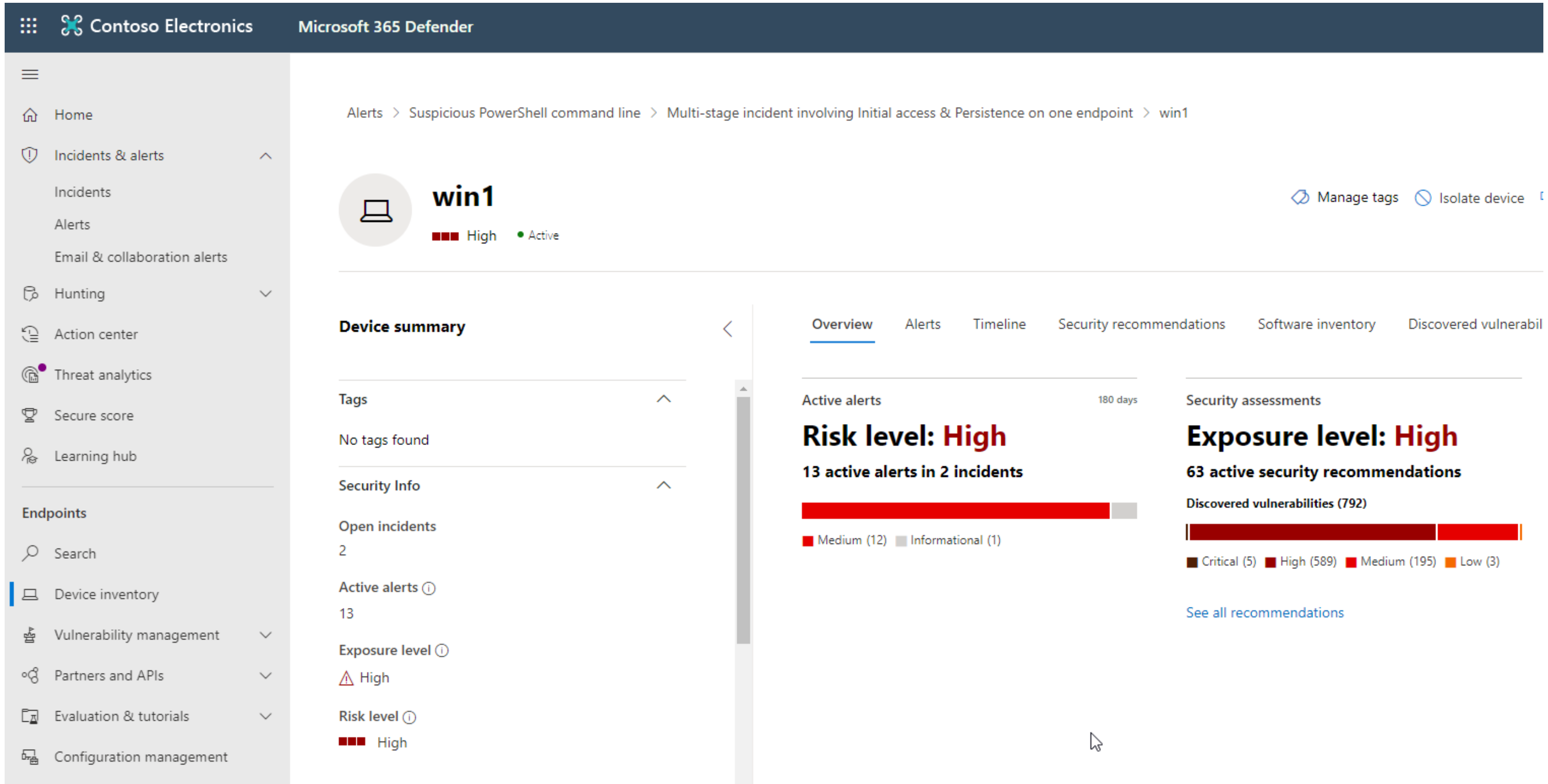


## Devices list

| Device name | Domain | Risk level ⓘ ↓ | Exposure level ⓘ | OS platform | Windows 10 versi... | Health state | Last seen |
|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | ■■■ High | ⚠ Medium | Windows 10 | Future | Active | 6/15/20, 12:01 PM |
| [redacted] | [redacted] | ■■■ High | ⚠ Low | Windows 10 | Future | Active | 6/15/20, 4:52 AM |
| [redacted] | [redacted] | ■■■ High | ⚠ High | Windows 10 | 1903 | Active | 6/14/20, 10:51 PM |
| [redacted] | [redacted] | ■■■ High | No data available | Windows 10 | Future | Inactive | 6/8/20, 4:38 AM |
| [redacted] | [redacted] | ■■■ High | No data available | Windows 10 | Future | Inactive | 6/8/20, 4:47 AM |
| [redacted] | [redacted] | ■■■ High | No data available | Windows 10 | Future | Inactive | 6/8/20, 4:50 AM |

# Investigate the device

When you investigate a specific device, you'll see: Device details, Response actions, Tabs for (overview, alerts, timeline, security recommendations, software inventory, discovered vulnerabilities, missing KBs), and Cards for (active alerts, logged on users, security assessment)



win1

High • Active

Device summary

Tags

No tags found

Security Info

Open incidents
2

Active alerts
13

Exposure level
High

Risk level
High

Active alerts — 180 days

Risk level: High

13 active alerts in 2 incidents

🟥 Medium (12) ▢ Informational (1)

Security assessments

Exposure level: High

63 active security recommendations

Discovered vulnerabilities (792)

■ Critical (5) ■ High (589) ■ Medium (195) ■ Low (3)

See all recommendations

Microsoft

# Perform actions on a device

# Explain device actions

When investigating a device, you can perform actions, collect data, or remotely access the machine. Defender for Endpoint provides the device control required.

Containment actions:

- **Isolate Device**
- **Restrict app execution**
- **Run antivirus scan**

Investigation actions:

- **Initiate Automated Investigation**
- **Collect investigation package**
- **Initiate Live Response Session**

# Collect investigation package from devices

As part of the investigation or response process, you can collect an investigation package from a device that contains the following folders:

- Autoruns
- Installed programs
- Network connections
- Prefetch files
- Processes
- Scheduled tasks
- Security event log

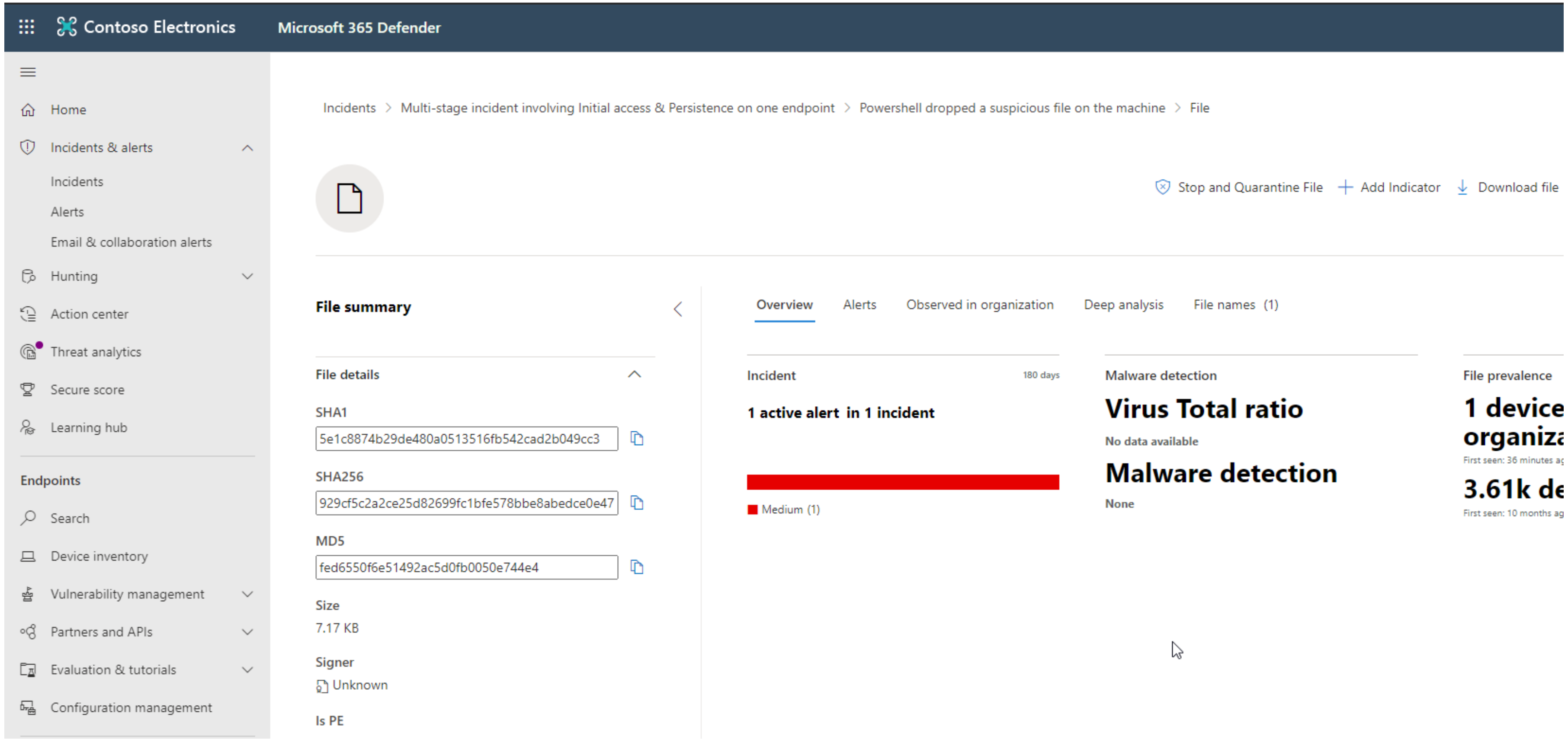
- Services
- Windows Server Message Block (SMB) sessions
- System information
- Temp directories
- Users and groups
- WdSupportLogs

Microsoft

# Perform evidence and entities investigations

# Investigate a file

Investigate the details of a file associated with a specific alert, behavior, or event to help determine if the file exhibits malicious activities, identify the attack motivation, and understand the potential scope of the breach.



File summary

File details

SHA1
5e1c8874b29de480a0513516fb542cad2b049cc3

SHA256
929cf5c2a2ce25d82699fc1bfe578bbe8abedce0e47

MD5
fed6550f6e51492ac5d0fb0050e744e4

Size
7.17 KB

Signer
Unknown

Is PE

Incident 180 days

1 active alert in 1 incident

🟥 Medium (1)

Malware detection

Virus Total ratio
No data available

Malware detection
None

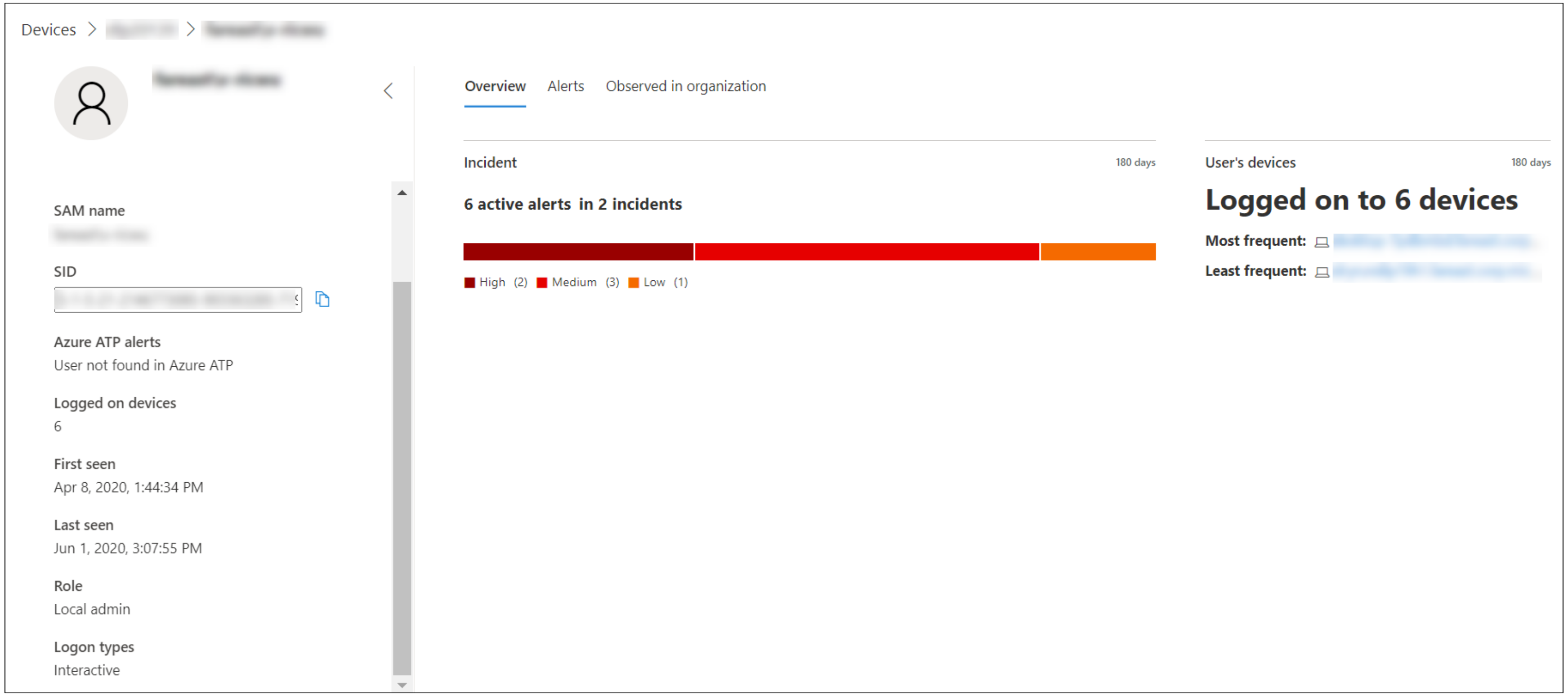
File prevalence

1 device organiza
First seen: 36 minutes ag

3.61k de
First seen: 10 months ag

# Investigate a user account

Identify user accounts with the most active alerts (displayed on the dashboard as "Users at risk") and investigate cases of potentially compromised credentials, or pivot on the associated user account when investigating an alert or device to identify possible lateral movement between devices with that user account.



Devices > [redacted] > [redacted]

[redacted]

SAM name
[redacted]

SID
[redacted]

Azure ATP alerts
User not found in Azure ATP

Logged on devices
6

First seen
Apr 8, 2020, 1:44:34 PM

Last seen
Jun 1, 2020, 3:07:55 PM

Role
Local admin

Logon types
Interactive

Overview  Alerts  Observed in organization

Incident  180 days

6 active alerts in 2 incidents

■ High (2) ■ Medium (3) ■ Low (1)

User's devices  180 days

Logged on to 6 devices

Most frequent: [redacted]
Least frequent: [redacted]

Microsoft

# Utilize Threat and Vulnerability Management

# Explore vulnerabilities on your devices

## Software inventory

The Software inventory page opens with a list of software installed in your network.

## Weaknesses

The Weaknesses page lists the software vulnerabilities your devices are exposed to by listing the Common Vulnerabilities and Exposures (CVE) ID.

## Event timeline

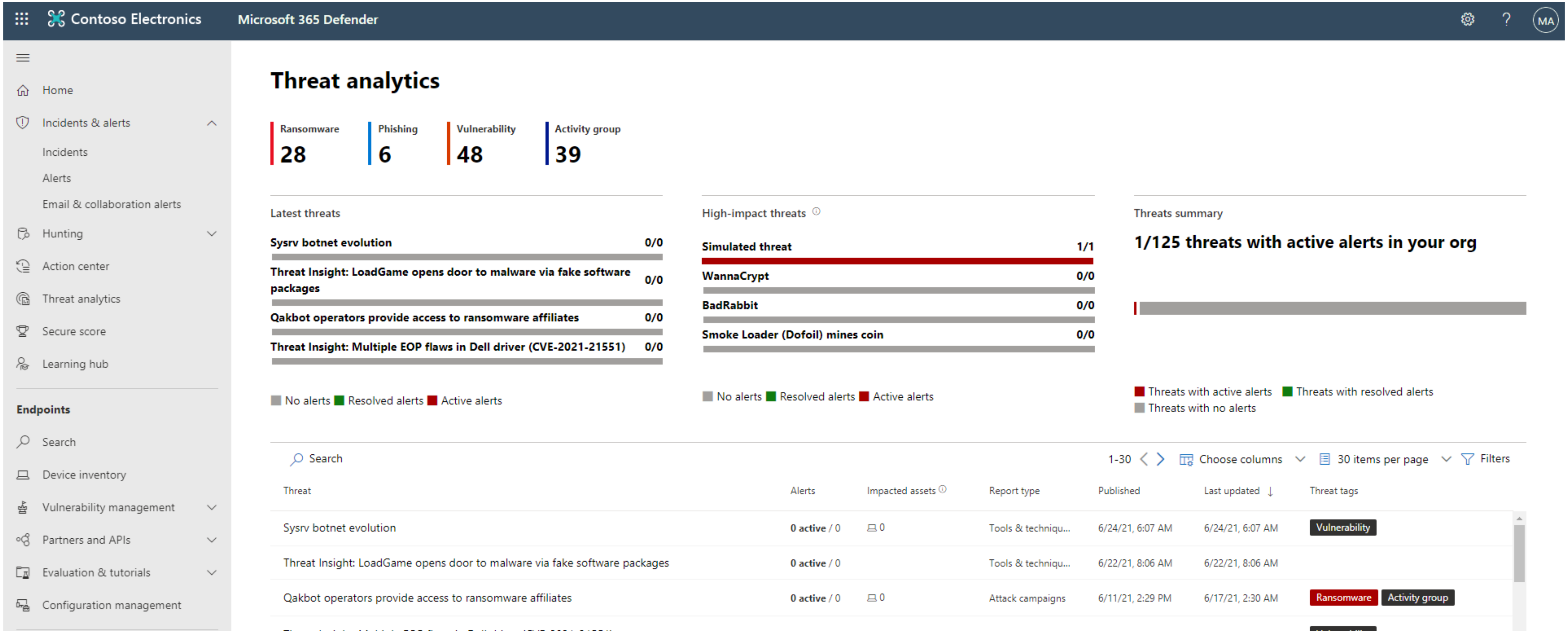
The Event timeline is a risk news feed that helps you interpret how risk is introduced into the organization through new vulnerabilities or exploits.

## Vulnerable devices report

The report shows graphs and bar charts with vulnerable device trends and current statistics.

# Track emerging threats with threat analytics

Assess the impact of new threats and review your resilience against or exposure to the threats.



## Threat analytics

| Ransomware | Phishing | Vulnerability | Activity group |
|---|---|---|---|
| 28 | 6 | 48 | 39 |

Latest threats

| | |
|---|---|
| Sysrv botnet evolution | 0/0 |
| Threat Insight: LoadGame opens door to malware via fake software packages | 0/0 |
| Qakbot operators provide access to ransomware affiliates | 0/0 |
| Threat Insight: Multiple EOP flaws in Dell driver (CVE-2021-21551) | 0/0 |

▨ No alerts 🟩 Resolved alerts 🟥 Active alerts

High-impact threats ⓘ

| | |
|---|---|
| Simulated threat | 1/1 |
| WannaCrypt | 0/0 |
| BadRabbit | 0/0 |
| Smoke Loader (Dofoil) mines coin | 0/0 |

▨ No alerts 🟩 Resolved alerts 🟥 Active alerts

Threats summary

1/125 threats with active alerts in your org

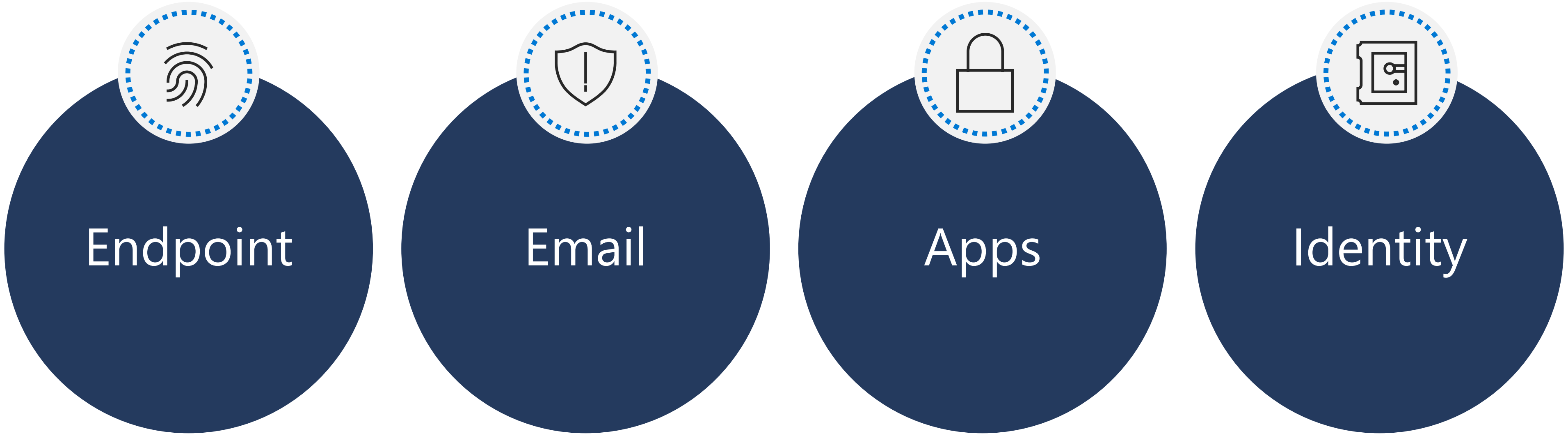
🟥 Threats with active alerts 🟩 Threats with resolved alerts
▨ Threats with no alerts

| Threat | Alerts | Impacted assets ⓘ | Report type | Published | Last updated ↓ | Threat tags |
|---|---|---|---|---|---|---|
| Sysrv botnet evolution | **0 active** / 0 | 0 | Tools & techniqu... | 6/24/21, 6:07 AM | 6/24/21, 6:07 AM | Vulnerability |
| Threat Insight: LoadGame opens door to malware via fake software packages | **0 active** / 0 | | Tools & techniqu... | 6/22/21, 8:06 AM | 6/22/21, 8:06 AM | |
| Qakbot operators provide access to ransomware affiliates | **0 active** / 0 | 0 | Attack campaigns | 6/11/21, 2:29 PM | 6/17/21, 2:30 AM | Ransomware<br>Activity group |

# Mitigate threats using Microsoft 365 Defender and Azure Defender

# Introduction to threat protection with Microsoft 365

# Introduction to threat protection



Endpoint

Email

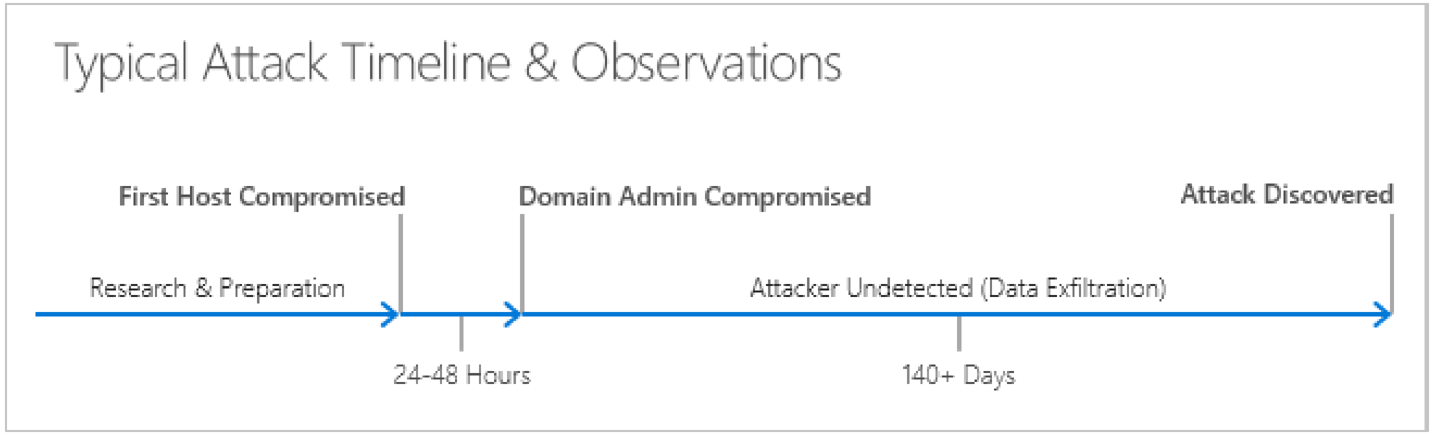
Apps

Identity

# Common threats

From a user perspective, the threat landscape includes the following:

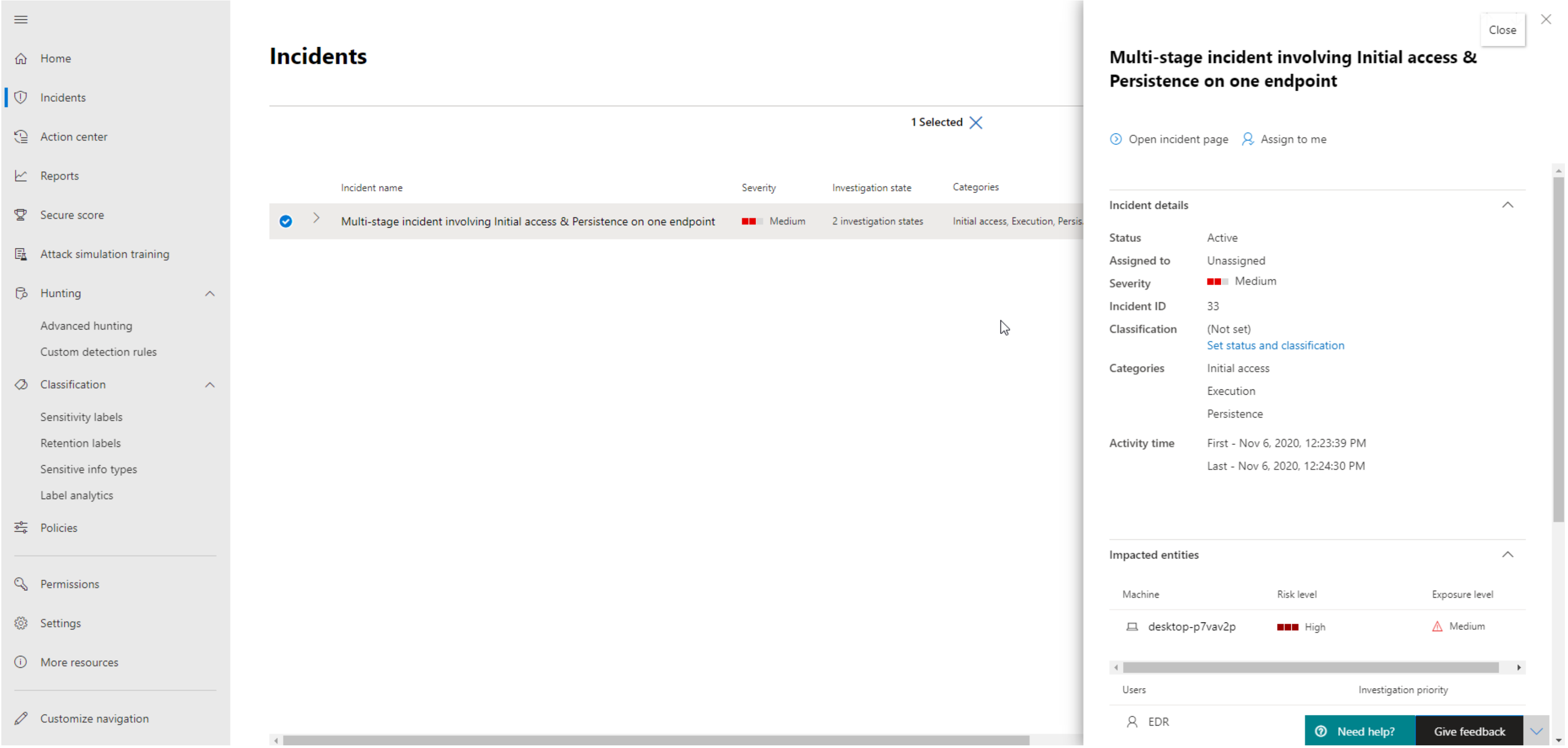
- Credential theft
- Malware
- Phishing
- Infrastructure attacks



# Mitigate incidents using Microsoft 365 Defender

# Manage incidents

Microsoft 365 Defender provides a cross domain threat correlation and purpose-driven portal to investigate threats.



## Incidents

1 Selected

| Incident name | Severity | Investigation state | Categories |
|---|---|---|---|
| Multi-stage incident involving Initial access & Persistence on one endpoint | Medium | 2 investigation states | Initial access, Execution, Persis |

### Multi-stage incident involving Initial access & Persistence on one endpoint

Incident details

| | |
|---|---|
| Status | Active |
| Assigned to | Unassigned |
| Severity | Medium |
| Incident ID | 33 |
| Classification | (Not set)<br>Set status and classification |
| Categories | Initial access<br>Execution<br>Persistence |
| Activity time | First - Nov 6, 2020, 12:23:39 PM<br>Last - Nov 6, 2020, 12:24:30 PM |

Impacted entities

| Machine | Risk level | Exposure level |
|---|---|---|
| desktop-p7vav2p | High | Medium |

| Users | Investigation priority |
|---|---|
| EDR | |

# Investigate incidents

The incident page provides the following information and navigation links.

- Incident overview
- Alerts
- Devices
- Users
- Mailboxes
- Investigations
- Evidence

# Use the action center

Use the Action center to see the results of current and past investigations across your organization's devices and mailboxes.

Tabs:

- Pending
- History

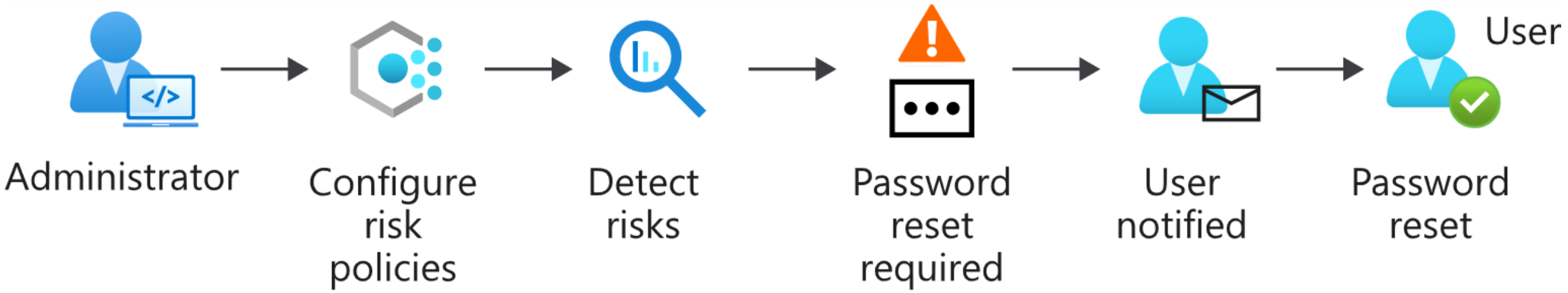
Sample Actions:

- Collect investigation package
- Isolate device
- Offboard machine
- Release code execution
- Quarantine
- Request sample
- Restrict code execution

# Protect your identities with Azure AD Identity Protection

# Azure AD Identity Protection explained

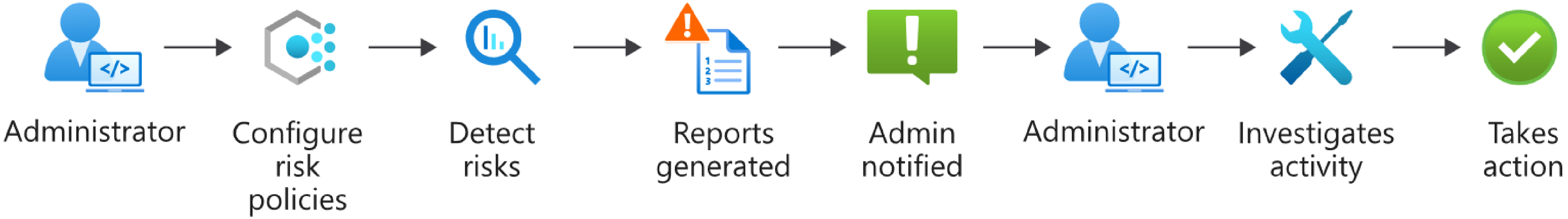
## Self-remediation workflow



Administrator → Configure risk policies → Detect risks → Password reset required → User notified → Password reset

User

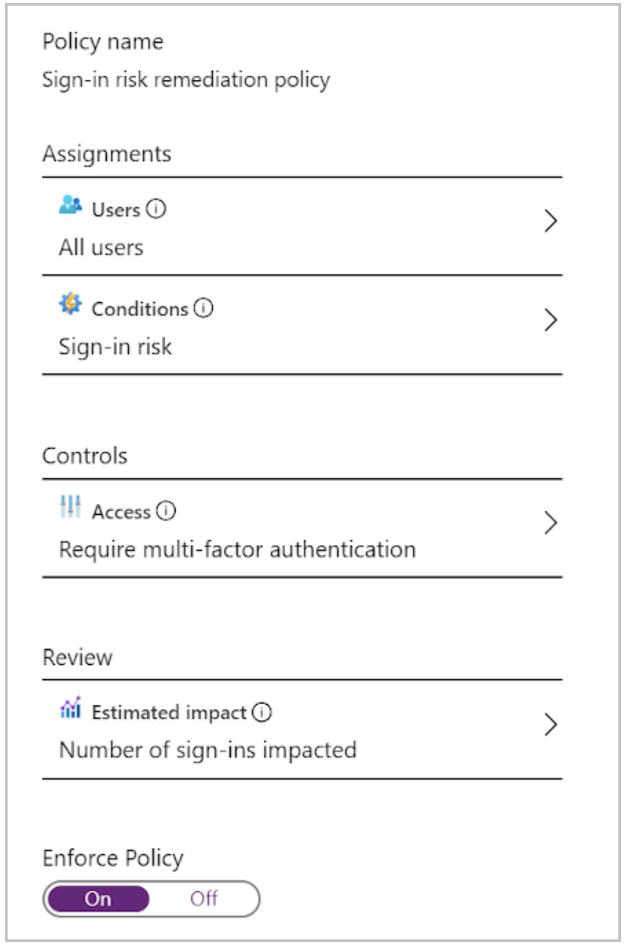
## Administrator remediation workflow



Administrator → Configure risk policies → Detect risks → Reports generated → Admin notified → Administrator → Investigates activity → Takes action

# Detect risks with Azure AD Identity Protection policies

## Sign-in risk policy



Policy name

Sign-in risk remediation policy

Assignments

Users ⓘ

All users

Conditions ⓘ

Sign-in risk

Controls

Access ⓘ

Require multi-factor authentication

Review

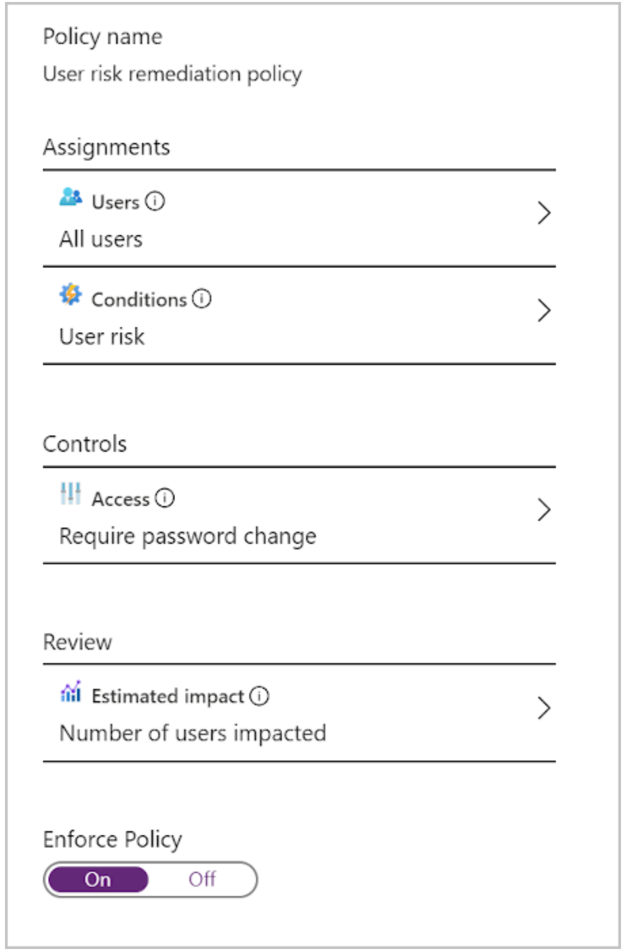
Estimated impact ⓘ

Number of sign-ins impacted

Enforce Policy

[✓ On] Off

## User risk policy



Policy name

User risk remediation policy

Assignments

Users ⓘ

All users

Conditions ⓘ

User risk

Controls

Access ⓘ

Require password change

Review

Estimated impact ⓘ

Number of users impacted

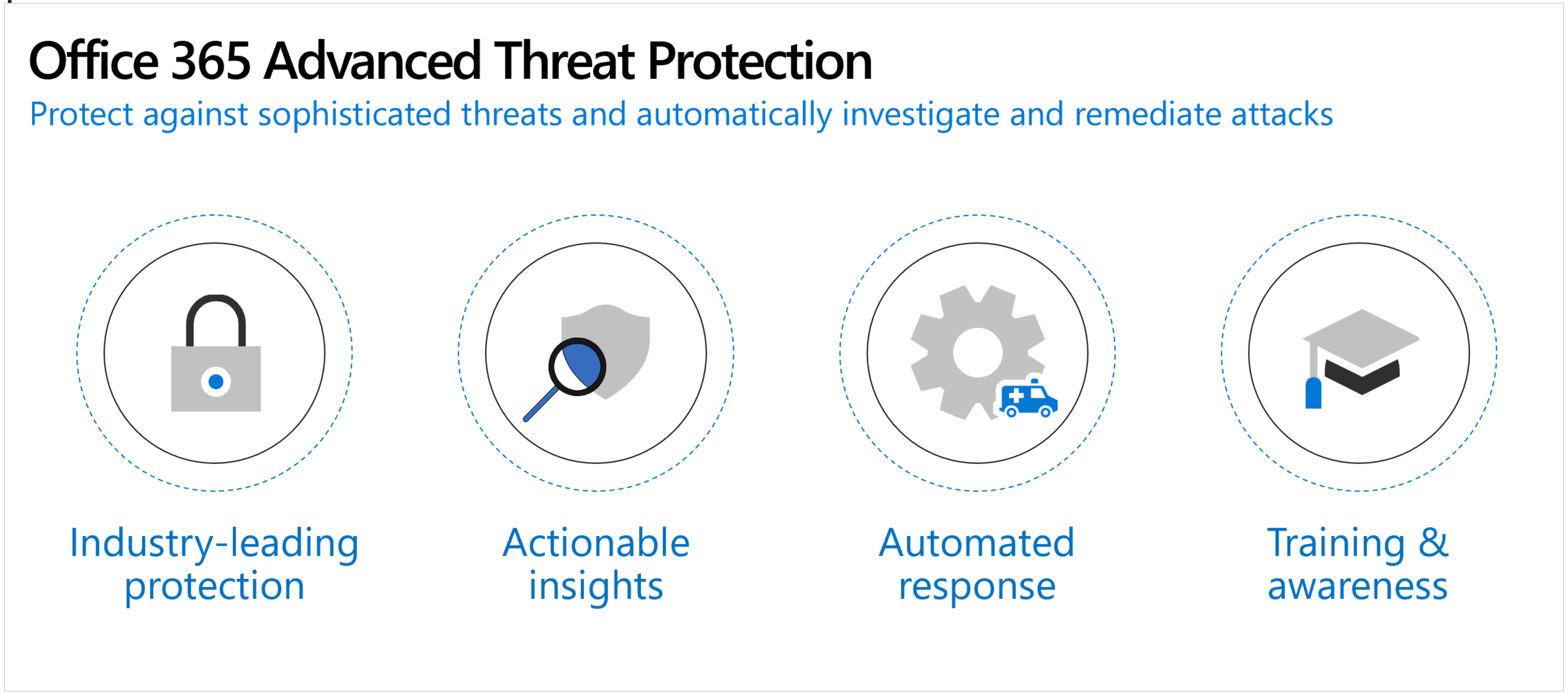
Enforce Policy

[✓ On] Off

# Remediate risks with Microsoft Defender for Office 365

# Microsoft Defender for Office 365 explained

Microsoft Defender for Office 365 is a cloud-based email filtering service that helps protect your organization against unknown malware and viruses by providing robust zero-day protection.

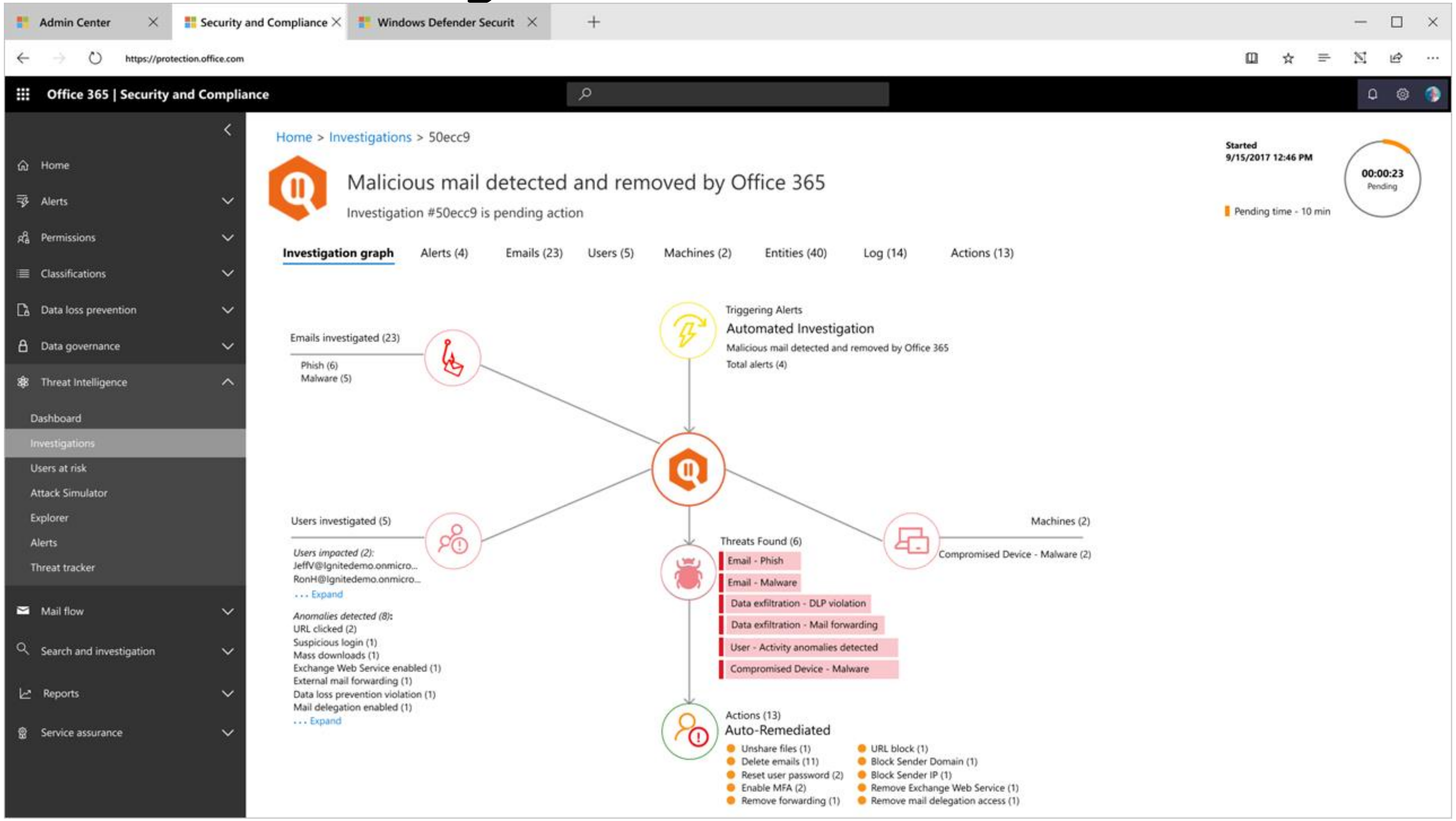


## Office 365 Advanced Threat Protection

Protect against sophisticated threats and automatically investigate and remediate attacks

- Industry-leading protection
- Actionable insights
- Automated response
- Training & awareness

# Automate, investigate, and remediate



Home > Investigations > 50ecc9

Malicious mail detected and removed by Office 365

Investigation #50ecc9 is pending action

Started
9/15/2017 12:46 PM

00:00:23
Pending

Pending time - 10 min

Triggering Alerts
Automated Investigation
Malicious mail detected and removed by Office 365
Total alerts (4)

Emails investigated (23)
Phish (6)
Malware (5)

Users investigated (5)
*Users impacted (2):*
JeffV@Ignitedemo.onmicro...
RonH@Ignitedemo.onmicro...
. . . Expand

*Anomalies detected (8)*:
URL clicked (2)
Suspicious login (1)
Mass downloads (1)
Exchange Web Service enabled (1)
External mail forwarding (1)
Data loss prevention violation (1)
Mail delegation enabled (1)
. . . Expand

Threats Found (6)
Email - Phish
Email - Malware
Data exfiltration - DLP violation
Data exfiltration - Mail forwarding
User - Activity anomalies detected
Compromised Device - Malware

Machines (2)
Compromised Device - Malware (2)

Actions (13)
Auto-Remediated
- Unshare files (1)
- Delete emails (11)
- Reset user password (2)
- Enable MFA (2)
- Remove forwarding (1)
- URL block (1)
- Block Sender Domain (1)
- Block Sender IP (1)
- Remove Exchange Web Service (1)
- Remove mail delegation access (1)

# Respond to data loss prevention alerts

# Describe data loss prevention alerts

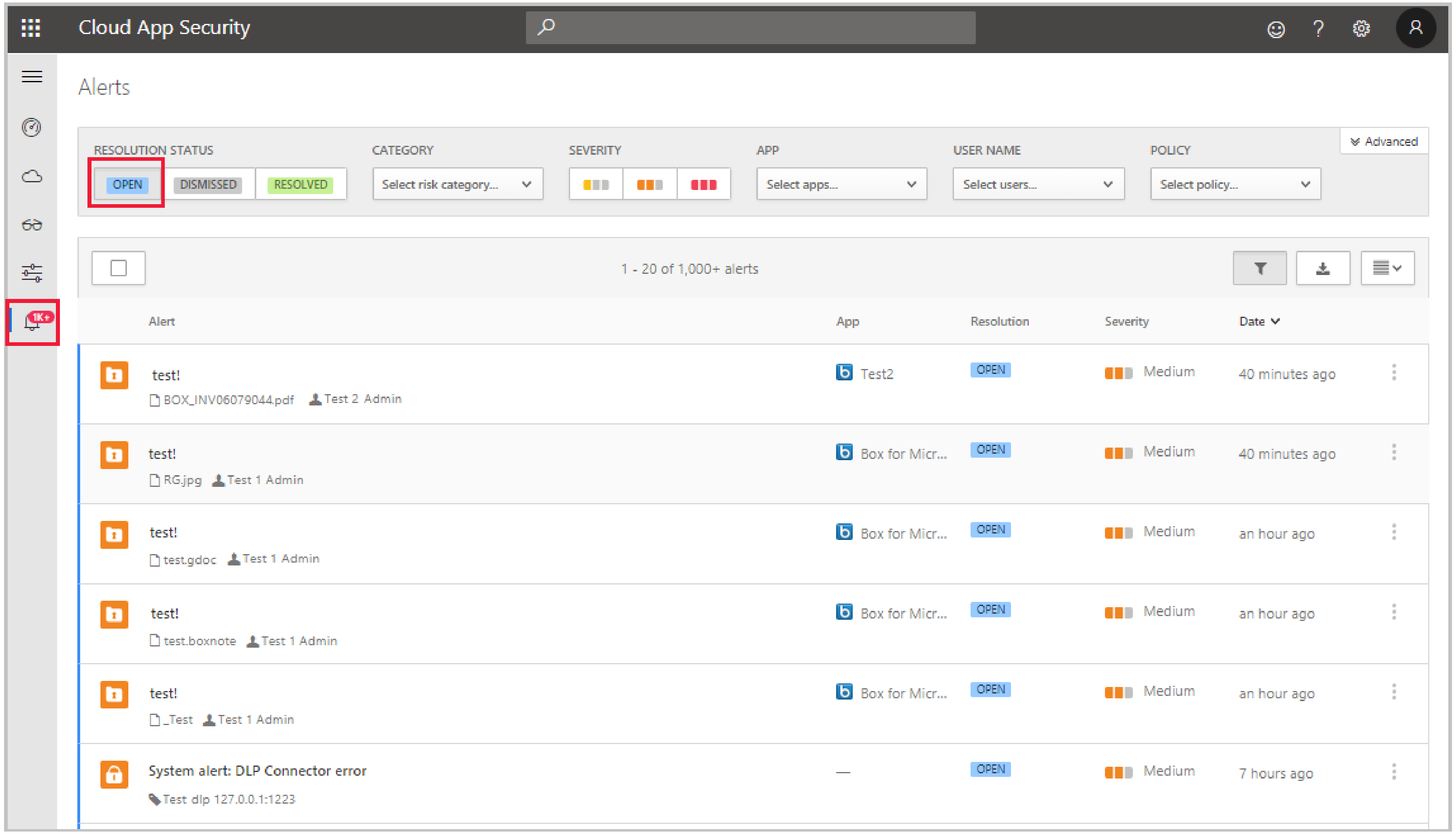
## With a DLP policy, you can:

- Identify sensitive information.
- Prevent the accidental sharing of sensitive information.
- Monitor and protect sensitive information in the desktop versions of Excel, PowerPoint, and Word.
- Help users learn how to stay compliant without interrupting their workflow.
- View DLP alerts and reports showing content that matches your organization's DLP policies.

## Data loss prevention components:

- Sensitive information types
- Sensitivity labels
- Data loss prevention policy
- Cloud App Security file policy

# Investigate DLP alerts in Microsoft Cloud App Security



Alerts

RESOLUTION STATUS: OPEN | DISMISSED | RESOLVED

CATEGORY: Select risk category...

SEVERITY

APP: Select apps...

USER NAME: Select users...

POLICY: Select policy...

Advanced

1 - 20 of 1,000+ alerts

| Alert | App | Resolution | Severity | Date |
|---|---|---|---|---|
| test!<br>BOX_INV06079044.pdf  Test 2 Admin | Test2 | OPEN | Medium | 40 minutes ago |
| test!<br>RG.jpg  Test 1 Admin | Box for Micr... | OPEN | Medium | 40 minutes ago |
| test!<br>test.gdoc  Test 1 Admin | Box for Micr... | OPEN | Medium | an hour ago |
| test!<br>test.boxnote  Test 1 Admin | Box for Micr... | OPEN | Medium | an hour ago |
| test!<br>_Test  Test 1 Admin | Box for Micr... | OPEN | Medium | an hour ago |
| System alert: DLP Connector error<br>Test dlp 127.0.0.1:1223 | — | OPEN | Medium | 7 hours ago |

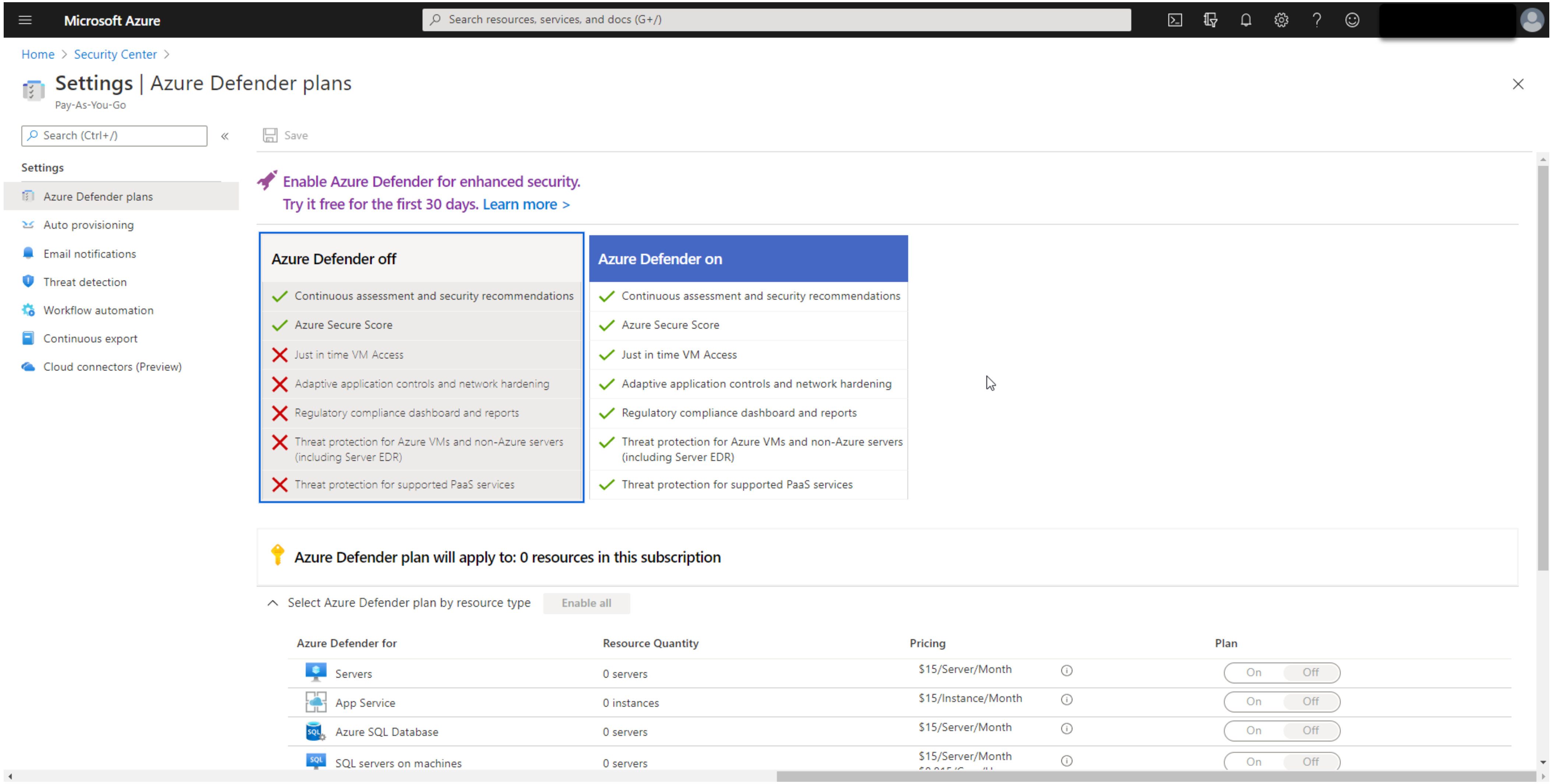
# Plan for cloud workload protections using Azure Defender

# Explain Azure Security Center

- Strengthen security posture
- Manage organization security policy and compliance
- Continuous assessments
- Optimize and improve security by configuring recommended controls
- Network map
- Automatically discover and onboard Azure resources with automatic provisioning

# Enable Azure Defender

To enable Azure Defender, you first enable Azure Security Center, then Azure Defender, and finally configure your coverage type.



Enable Azure Defender for enhanced security.
Try it free for the first 30 days. Learn more >

| Azure Defender off | Azure Defender on |
|---|---|
| ✓ Continuous assessment and security recommendations | ✓ Continuous assessment and security recommendations |
| ✓ Azure Secure Score | ✓ Azure Secure Score |
| ✗ Just in time VM Access | ✓ Just in time VM Access |
| ✗ Adaptive application controls and network hardening | ✓ Adaptive application controls and network hardening |
| ✗ Regulatory compliance dashboard and reports | ✓ Regulatory compliance dashboard and reports |
| ✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR) | ✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR) |
| ✗ Threat protection for supported PaaS services | ✓ Threat protection for supported PaaS services |

Azure Defender plan will apply to: 0 resources in this subscription

Select Azure Defender plan by resource type   Enable all

| Azure Defender for | Resource Quantity | Pricing | Plan |
|---|---|---|---|
| Servers | 0 servers | $15/Server/Month | On Off |
| App Service | 0 instances | $15/Instance/Month | On Off |
| Azure SQL Database | 0 servers | $15/Server/Month | On Off |
| SQL servers on machines | 0 servers | $15/Server/Month | On Off |

# Explain cloud workload protections in Azure Defender

# Azure Defender for servers

- Azure Defender for servers adds threat detection and advanced defenses for your Windows and Linux machines.

- For Windows, Azure Defender integrates with Azure services to monitor and protect your Windows-based machines. Security Center presents the alerts and remediation suggestions from all of these services in an easy-to-use format.

- For Linux, Azure Defender collects audit records from Linux machines by using auditd, one of the most common Linux auditing frameworks. auditd lives in the mainline kernel.

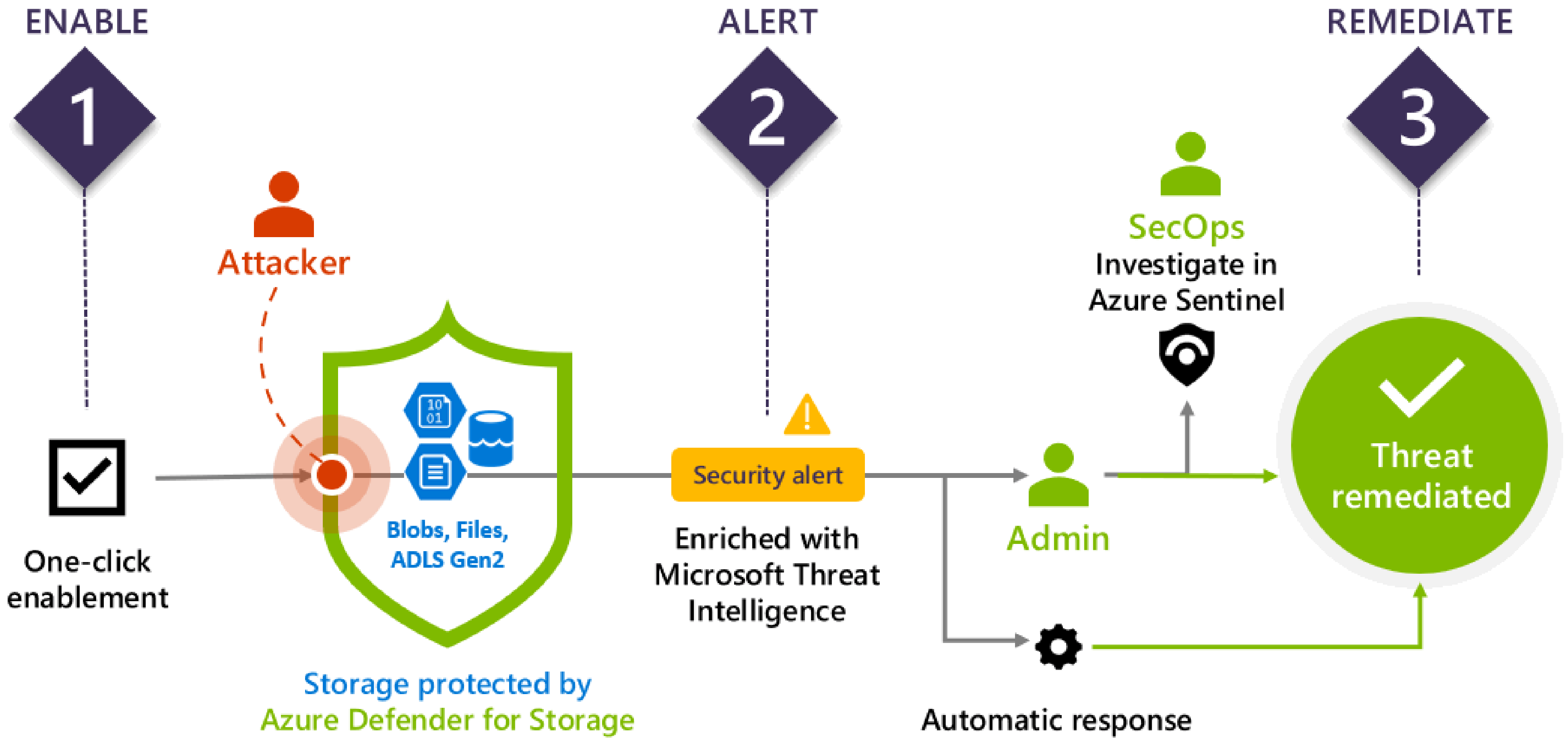
# Azure Defender for App Service

Azure Defender for App Service uses the scale of the cloud to identify attacks targeting applications running over App Service.

Attackers probe web applications to find and exploit weaknesses. Before being routed to specific environments, requests to applications running in Azure go through several gateways, where they're inspected and logged.

This data is then used to identify exploits and attackers and learn new patterns that will be used later.

# Azure Defender for Storage



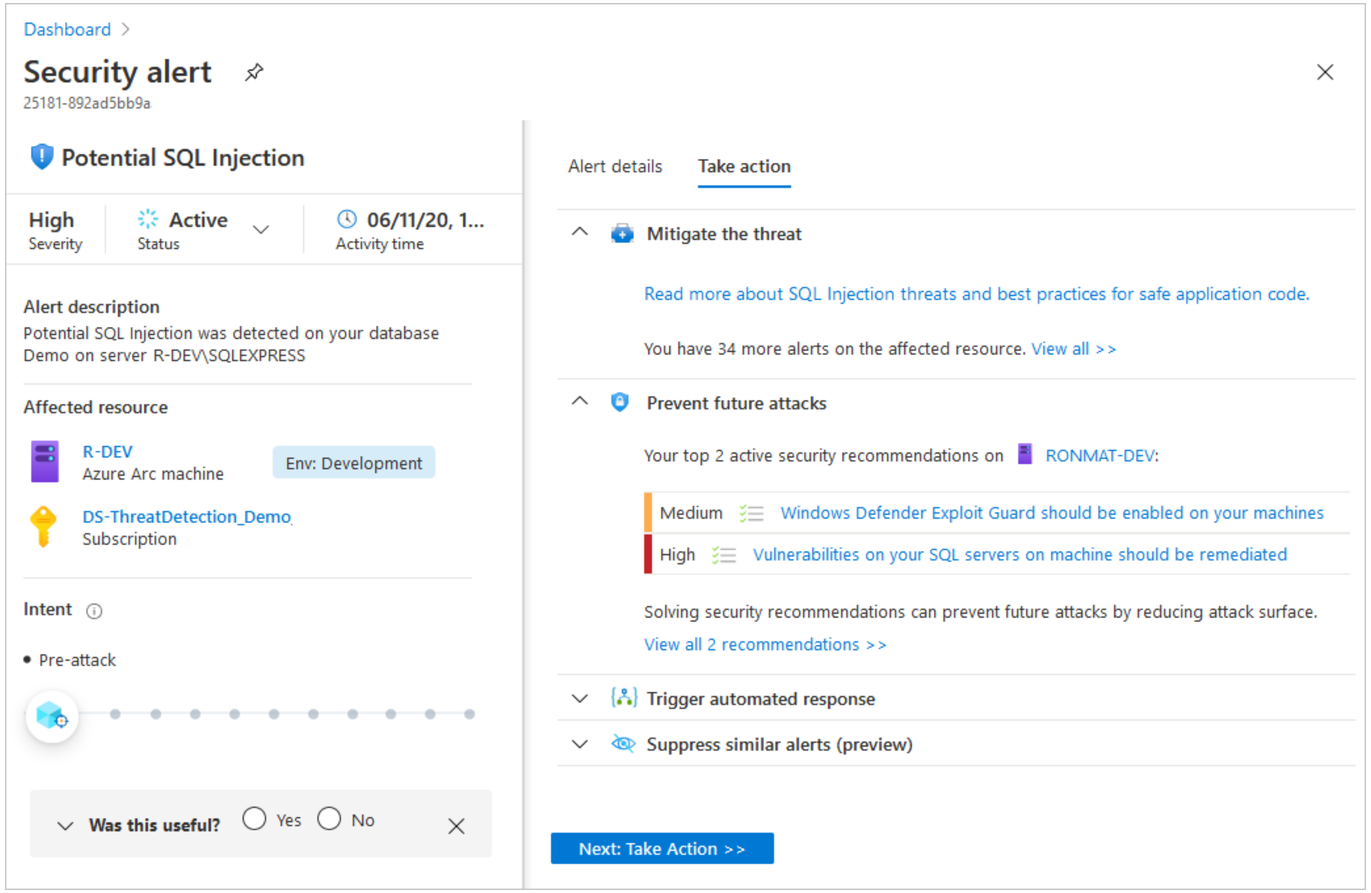
# Remediate security alerts using Azure Defender

# Explain security alerts

- Security alerts and incidents
- Detecting Threats
- Alert classification
- Continuous monitoring and assessments
- Alert types

# Remediate alerts

Azure Defender provides actionable tasks to mitigate the threat, prevent future attacks, trigger automated response, suppress similar alerts.



Dashboard >

## Security alert

25181-892ad5bb9a

**Potential SQL Injection**

| High | Active | 06/11/20, 1... |
|---|---|---|
| Severity | Status | Activity time |

**Alert description**

Potential SQL Injection was detected on your database Demo on server R-DEV\SQLEXPRESS

**Affected resource**

R-DEV
Azure Arc machine
Env: Development

DS-ThreatDetection_Demo
Subscription

**Intent**

- Pre-attack

**Was this useful?** ○ Yes ○ No

Alert details | Take action

**Mitigate the threat**

Read more about SQL Injection threats and best practices for safe application code.

You have 34 more alerts on the affected resource. View all >>

**Prevent future attacks**

Your top 2 active security recommendations on RONMAT-DEV:

| | |
|---|---|
| Medium | Windows Defender Exploit Guard should be enabled on your machines |
| High | Vulnerabilities on your SQL servers on machine should be remediated |

Solving security recommendations can prevent future attacks by reducing attack surface.
View all 2 recommendations >>

**Trigger automated response**

**Suppress similar alerts (preview)**

Next: Take Action >>

Microsoft

# Create queries for Azure Sentinel using Kusto

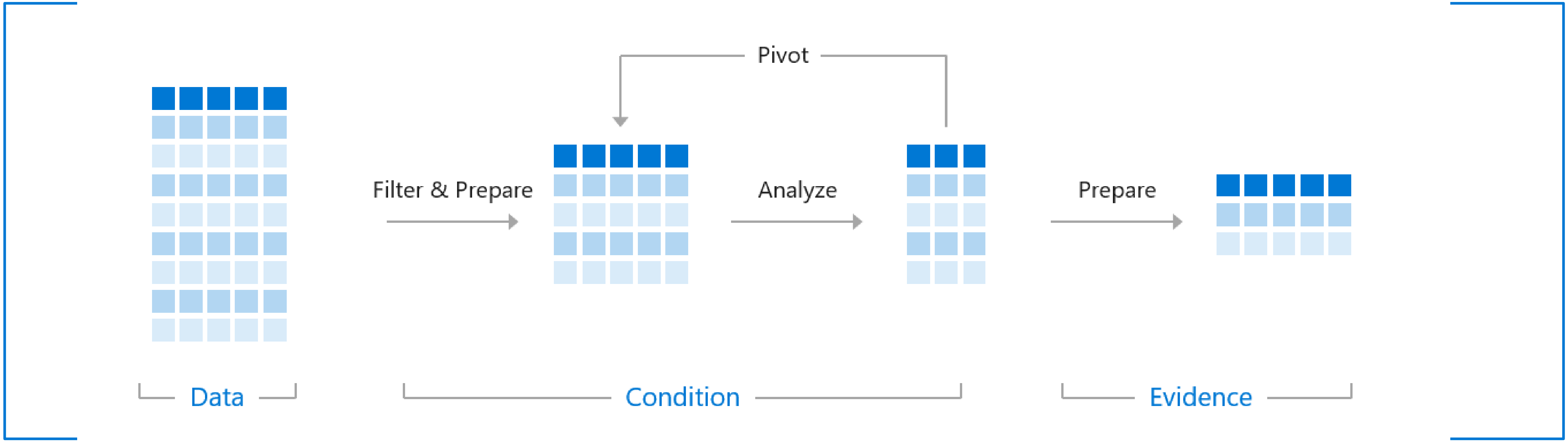
Microsoft

# Construct KQL statements for Azure Sentinel

# The Kusto Query Language statement structure

A KQL query is a read-only request to process data and return results. The request is stated in plain text, using a data-flow model designed to make the syntax easy to read, write, and automate.

```
SecurityEvent | where EventID == “4626” | summarize count() by Account | limit 10
```



# Use the let statement

```
let timeOffset = 7d;
let discardEventId = 4688;
SecurityEvent
| where TimeGenerated > ago(timeOffset*2) and TimeGenerated < ago(timeOffset)
| where EventID != discardEventId



let LowActivityAccounts =
    SecurityEvent
    | summarize cnt = count() by Account
    | where cnt < 10;

LowActivityAccounts | where Account contains "Mal"
```

# Use the where operator

```
SecurityEvent
| where TimeGenerated > ago(1d)

SecurityEvent
| where TimeGenerated > ago(1h) and EventID == "4624"

SecurityEvent
| where TimeGenerated > ago(1h)
| where EventID == 4624
| where AccountType =~ "user"

SecurityEvent | where EventID in (4624, 4625)
```

# Use the extend operator

```
let timeframe = 1d;

let DomainList = dynamic(["tor2web.org", "tor2web.com"]);

Syslog
| where TimeGenerated >= ago(timeframe)
| where ProcessName contains "squid"
| extend
  HTTP_Status_Code = extract("(TCP_(([A-Z]+)…-9]{3}))",8,SyslogMessage),
  Domain = extract("(([A-Z]+ [a-z]{4…Z]+ )([^ :\\/]*))",3,SyslogMessage)
| where HTTP_Status_Code == "200"
| where Domain contains "."
| where Domain has_any (DomainList)
```

# Use the order by operator

```
SecurityAlert
| where TimeGenerated > ago(7d)
| extend severityOrder = case (
    AlertSeverity == "High", 3,
    AlertSeverity == "Medium", 2,
    AlertSeverity == "Low", 1,
    AlertSeverity == "Informational", 0,
    -1)
| order by severityOrder desc
```

# Use the project operators

```
SecurityEvent
| project Computer, Account

SecurityAlert
| where TimeGenerated > ago(7d)
| extend severityOrder = case (
    AlertSeverity == "High", 3,
    AlertSeverity == "Medium", 2,
    AlertSeverity == "Low", 1,
    AlertSeverity == "Informational", 0,
    -1)
| order by severityOrder
| project-away severityOrder
```

| Operator | Description |
|---|---|
| **project** | Select the columns to include, rename or drop, and insert new computed columns. |
| **project-away** | Select what columns from the input to exclude from the output. |
| **project-keep** | Select what columns from the input to keep in the output. |
| **project-rename** | Select the columns to rename in the resulting output. |
| **project-reorder** | Set the column order in the resulting output. |

Microsoft

# Analyze query results using KQL

# Use the summarize operator

```
SecurityEvent
| summarize count() by Process, Computer

let timeframe = 1d;
SigninLogs
| where TimeGenerated >= ago(timeframe)
| where ResultType == "50057"
| where ResultDescription =~ "User
account is disabled. The account has been
disabled by an administrator."
| summarize applicationCount =
dcount(AppDisplayName) by
UserPrincipalName, IPAddress
| where applicationCount >= 3
```

| Function(s) | Description |
|---|---|
| **count(),<br>countif()** | Returns a count of the records per summarization group |
| **dcount(),<br>dcountif()** | Returns an estimate for the number of distinct values taken by a scalar expression in the summary group. |
| **avg(), avgif()** | Calculates the average of Expr across the group. |
| **Max(), maxif()** | Returns the maximum value across the group. |
| **sum(), sumif()** | Calculates the sum of Expr across the group. |

# Use the render operator to create visualizations

```
SecurityEvent
| summarize count() by Account
| render barchart

SecurityEvent
| summarize count() by bin(TimeGenerated,
1d)
| render timechart
```

| Visualizations |
|---|
| areachart |
| barchart |
| columnchart |
| piechart |
| scatterchart |
| timechart |

Microsoft

# Build multi-table statements using KQL

# Use the union operator

```
SecurityEvent
| union SecurityAlert


union Security*
| summarize count() by Type
```

# Use the join operator

```
SecurityEvent
| where EventID == "4624"
| summarize LogOnCount=count() by EventID, Account
| project LogOnCount, Account
| join kind = inner (
     SecurityEvent
     | where EventID == "4634"
     | summarize LogOffCount=count() by EventID, Account
     | project LogOffCount, Account
) on Account
```

Microsoft

# Work with string data using KQL statements

# Extract data from unstructured string fields

Extract function:

```
let top5 = SecurityEvent
| where EventID == 4625 and AccountType == 'User'
| extend Account_Name = extract(@"^(.*\\)?([^@]*)(@.*)?$", 2, tolower(Account))
| summarize Attempts = count() by Account_Name
| where Account_Name != ""
| top 5 by Attempts
| summarize make_list(Account_Name);

SecurityEvent
| where EventID == 4625 and AccountType == 'User'
| extend Name = extract(@"^(.*\\)?([^@]*)(@.*)?$", 2, tolower(Account))
| extend Account_Name = iff(Name in (top5), Name, "Other")
| where Account_Name != ""
| summarize Attempts = count() by Account_Name
```

Microsoft

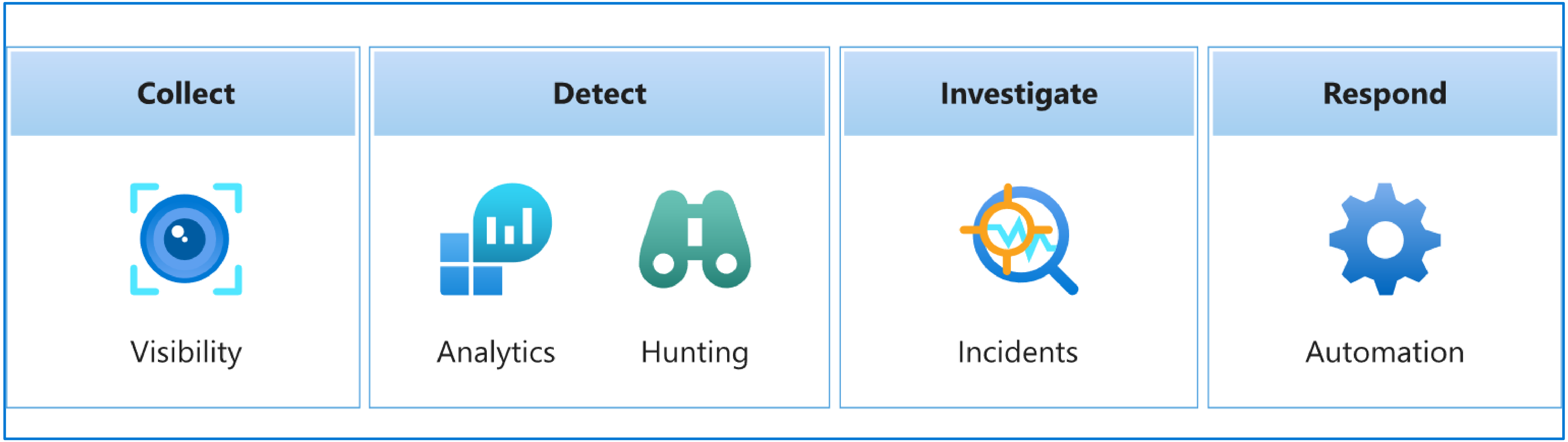
# Configure your Azure Sentinel environment

Microsoft

# Introduction to Azure Sentinel

# Azure Sentinel explained

Azure Sentinel is a cloud-native SIEM. A SIEM system is a tool that an organization uses to collect, analyze, and perform security operations on its computer systems.



Collect

Visibility

Detect

Analytics

Hunting

Investigate

Incidents

Respond

Automation

# How Azure Sentinel works

Components of Azure Sentinel

Data connectors

Log retention

Workbooks

Analytics alerts

Threat hunting

Incidents and investigations

Automation playbooks

# When to use Azure Sentinel

Azure Sentinel is a solution for performing security operations on your cloud and on-premises environments.

**Use Azure Sentinel if you want to:**

- Collect event data from various sources.
- Perform security operations on that data to identify suspicious activity

**Security operations could include:**

- Visualization of log data.
- Anomaly detection.
- Threat hunting.
- Security incident investigation
- Automated response to alerts and incidents.

**Decide whether it's the right fit for you:**

- Cloud-native SIEM. There are no servers to provision, so scaling is effortless.
- Benefits of Microsoft research and machine learning.
- Support for hybrid cloud and on-premises environments.
- SIEM and a data lake all in one.

**Clear requirements:**

- Support for data from multiple cloud environments
- Features and functionality required for a security operations center (SOC), without too much administrative overhead

Microsoft

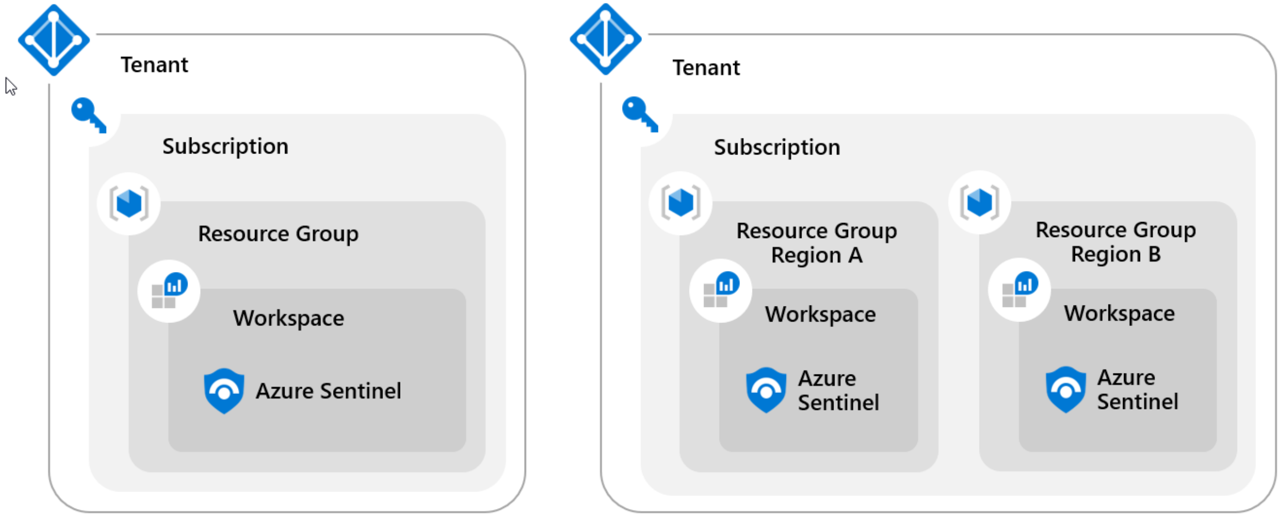
# Create and manage Azure Sentinel workspaces

# Plan for the Azure Sentinel workspace

1 Single-Tenant with a single Azure Sentinel Workspace

2 Single-Tenant with regional Azure Sentinel Workspaces

3 Multi-Tenant



# Create an Azure Sentinel workspace

### Azure Sentinel installation prerequisites

Have the required permissions for the Azure Subscription.

1

### Create and configure a Log Analytics Workspace

Plan for the Region selection.

2

### Add Azure Sentinel to the workspace

Select the newly created Log Analytics Workspace.

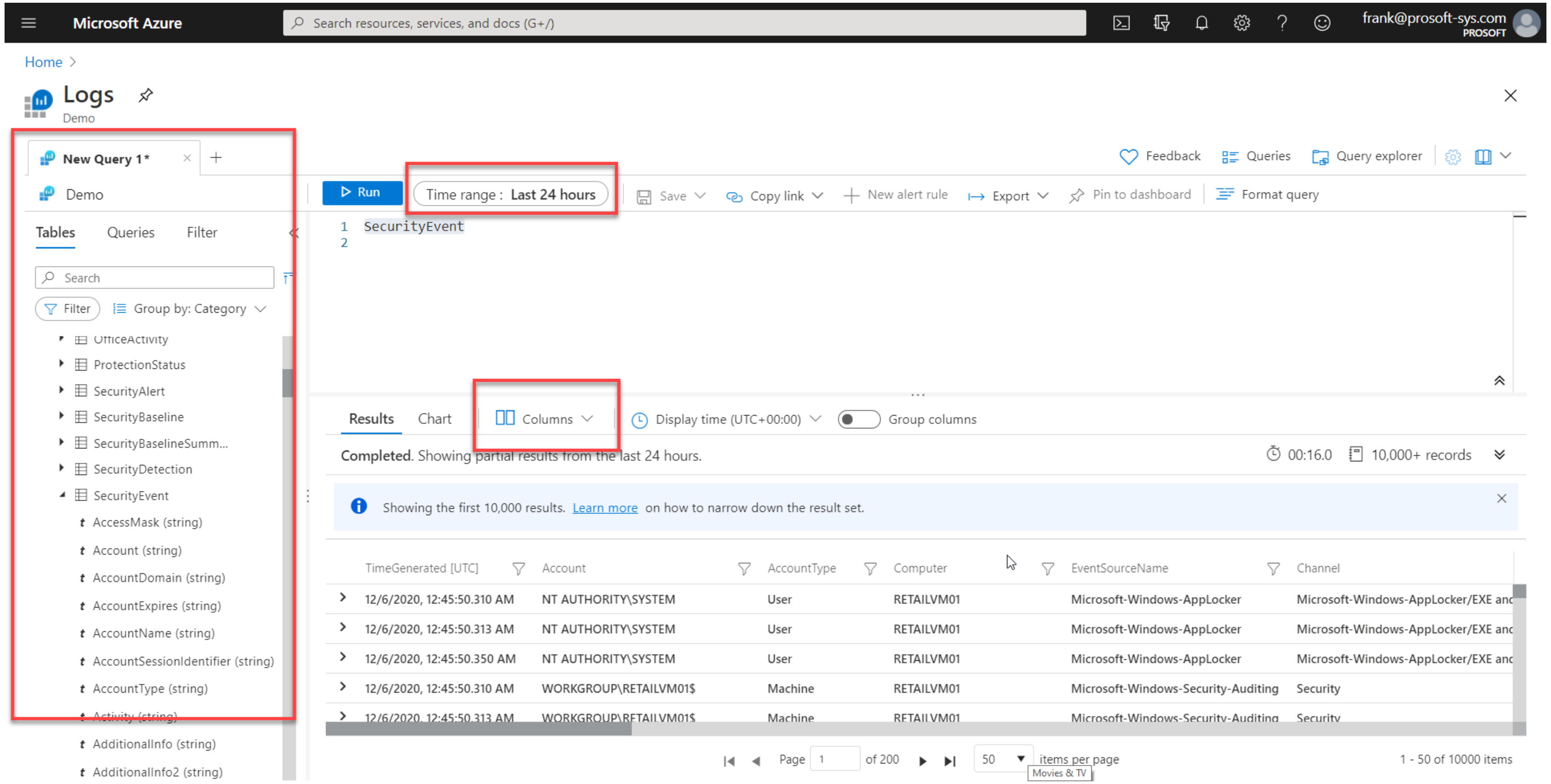
3

Microsoft

# Query logs in Azure Sentinel

# Query logs in the logs page

The query window allows you to run queries, save queries, run saved queries, create a new alert rule, and export.



Time range : Last 24 hours

```
SecurityEvent
```

Completed. Showing partial results from the last 24 hours.

Showing the first 10,000 results. Learn more on how to narrow down the result set.

| TimeGenerated [UTC] | Account | AccountType | Computer | EventSourceName | Channel |
|---|---|---|---|---|---|
| 12/6/2020, 12:45:50.310 AM | NT AUTHORITY\SYSTEM | User | RETAILVM01 | Microsoft-Windows-AppLocker | Microsoft-Windows-AppLocker/EXE and |
| 12/6/2020, 12:45:50.313 AM | NT AUTHORITY\SYSTEM | User | RETAILVM01 | Microsoft-Windows-AppLocker | Microsoft-Windows-AppLocker/EXE and |
| 12/6/2020, 12:45:50.350 AM | NT AUTHORITY\SYSTEM | User | RETAILVM01 | Microsoft-Windows-AppLocker | Microsoft-Windows-AppLocker/EXE and |
| 12/6/2020, 12:45:50.310 AM | WORKGROUP\RETAILVM01$ | Machine | RETAILVM01 | Microsoft-Windows-Security-Auditing | Security |
| 12/6/2020, 12:45:50.313 AM | WORKGROUP\RETAILVM01$ | Machine | RETAILVM01 | Microsoft-Windows-Security-Auditing | Security |

# Understand Azure Sentinel tables

| Table: | Description |
|---|---|
| **SecurityAlert** | Contains Alerts Generated from Sentinel Analytical Rules. Also, it could include Alerts created directly from a Sentinel Data Connector |
| **SecurityIncident** | Alerts can generate Incidents. Incidents are related to Alert(s). |
| **ThreatIntelligenceIndictor** | Contains user-created or data connector ingested Indicators such as File Hashes, IP Addresses, Domains. |
| **Watchlist** | An Azure Sentinel watchlist contains imported data. |

# Understand common tables

| Table: | Description |
|---|---|
| **AzureActivity** | Entries from the Azure Activity log |
| **AzureDiagnostics** | Stores resource logs for services that use Azure Diagnostics mode. |
| **AuditLogs** | Audit log for Azure Active Directory. |
| **CommonSecurityLog** | Syslog messages using the Common Event Format (CEF). |
| **OfficeActivity** | Audit logs for Office 365 tenants (Exchange, SharePoint and Teams). |
| **SecurityEvent** | Security events collected from windows devices. |
| **SigninLogs** | Azure Activity Directory Sign in logs. |
| **Syslog** | Syslog events on Linux computers using the Log Analytics agent. |
| **Event** | Sysmon Events collected from a Windows host. |
| **WindowsFirewall** | Windows Firewall Events |

# Understand Microsoft 365 Defender tables

| Table: | Description |
|---|---|
| **DeviceEvents** | Device events table contains information about various event types. |
| **DeviceFileEvents** | File creation, modification, and other file system events. |
| **DeviceImageLoadEvents** | DLL loading events. |
| **DeviceInfo** | Including their OS version, active users, and computer name. |
| **DeviceLogonEvents** | User logons and other authentication events. |
| **DeviceNetworkEvents** | Network connections and related events. |
| **DeviceNetworkInfo** | Including network adapters, IP and MAC addresses, and connected networks or domains. |
| **DeviceProcessEvents** | Process creation and related events. |
| **DeviceRegistryEvents** | Creation and modification of registry entries. |

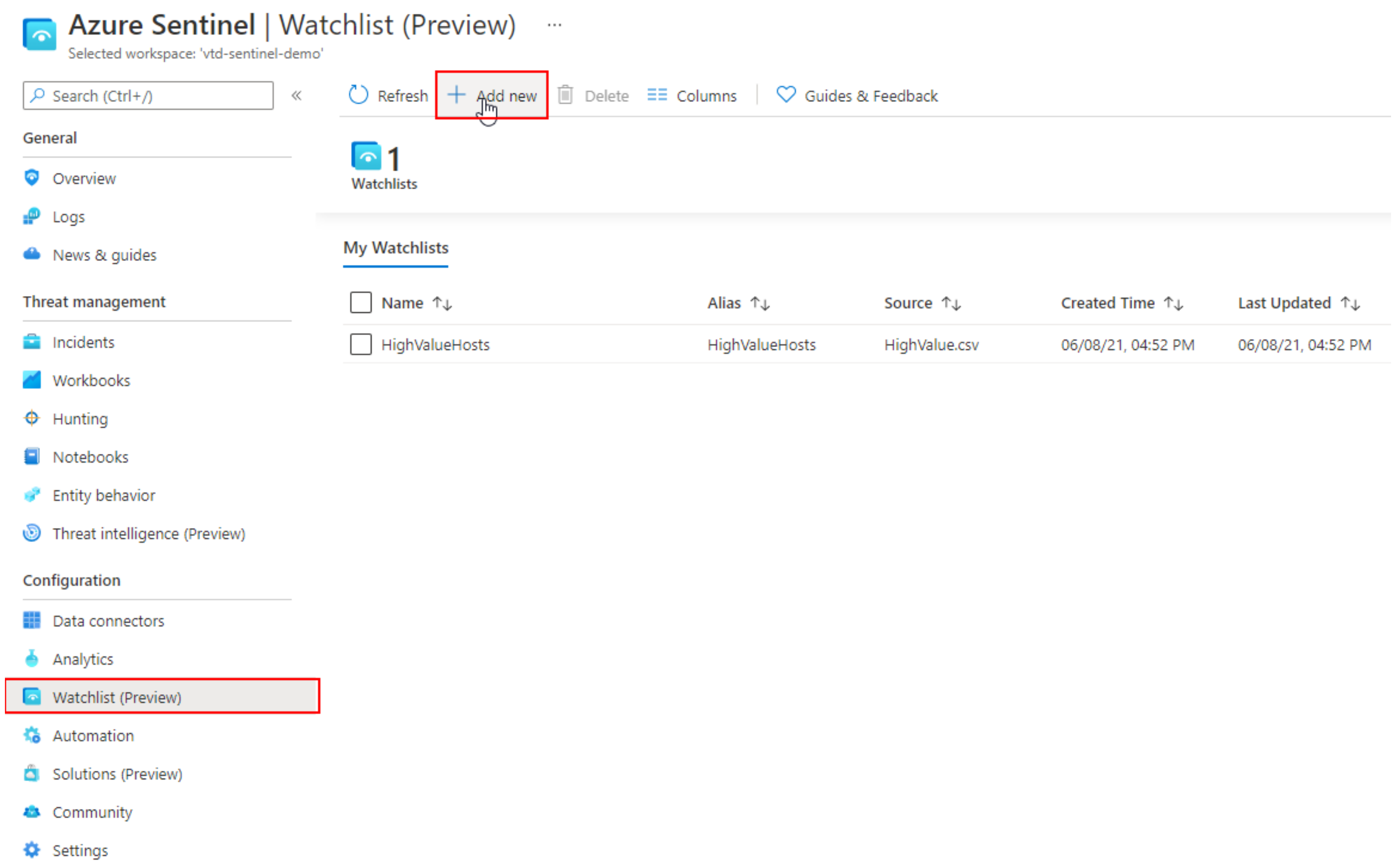
Microsoft

# Use watchlists in Azure Sentinel

# Watchlists

- In Azure Sentinel, a watchlist is a table to store list data that can be accessed by Kusto Query Language (KQL) queries.
- Common scenarios for using watchlists:
  - Investigating threats and responding to incidents
  - Importing business data as a watchlist.
  - Reducing alert fatigue.
  - Enriching event data.

# Create a watchlist



| □ Name ↑↓ | Alias ↑↓ | Source ↑↓ | Created Time ↑↓ | Last Updated ↑↓ |
|---|---|---|---|---|
| □ HighValueHosts | HighValueHosts | HighValue.csv | 06/08/21, 04:52 PM | 06/08/21, 04:52 PM |

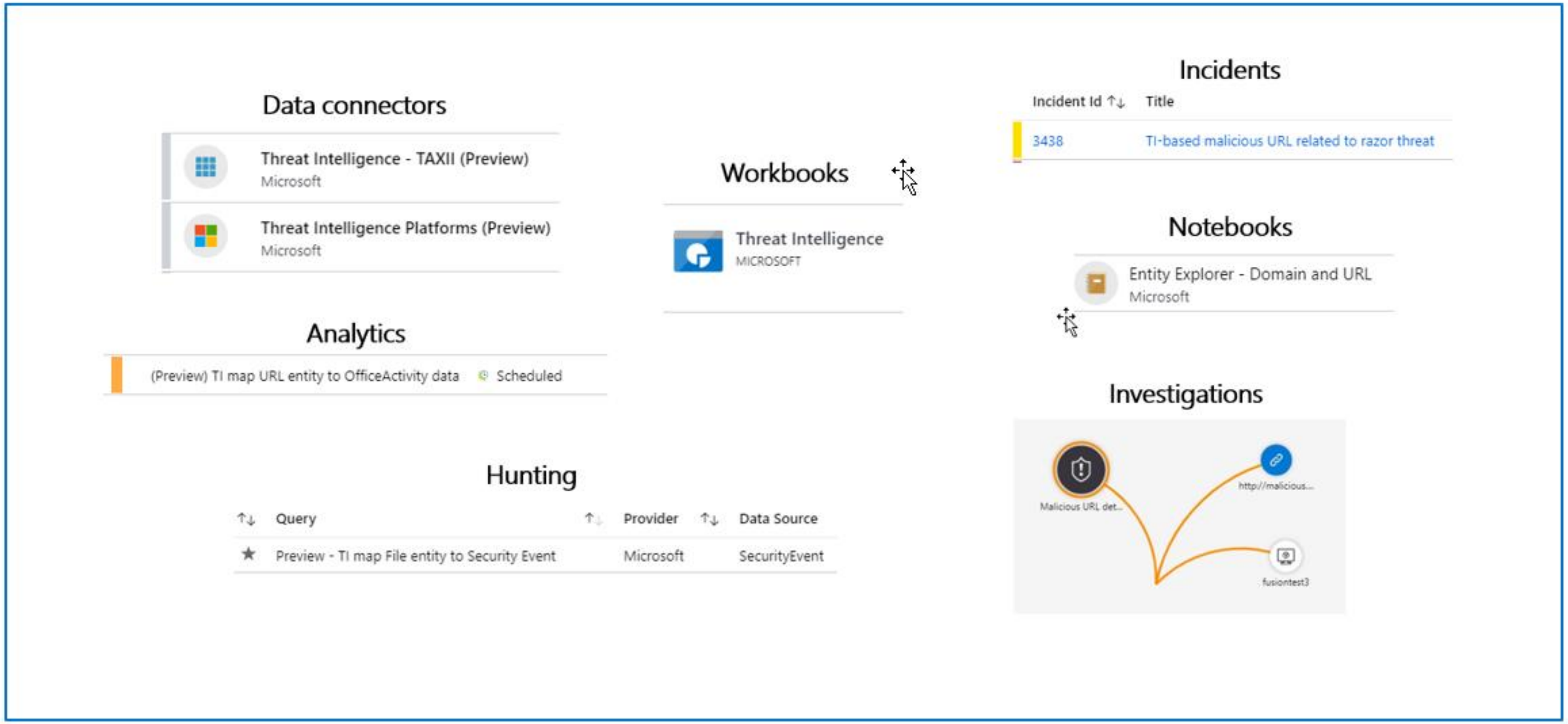
To use the watchlist data in KQL, use the KQL function **_GetWatchlist('WATCHLISTNAME').**

Microsoft

# Utilize threat intelligence in Azure Sentinel

# Define threat intelligence

Threat indicators are data that associate observations such as URLs, file hashes, or IP addresses with known threat activity such as phishing, botnets, or malware.



## Data connectors

Threat Intelligence - TAXII (Preview)
Microsoft

Threat Intelligence Platforms (Preview)
Microsoft

## Workbooks

Threat Intelligence
MICROSOFT

## Incidents

| Incident Id ↑↓ | Title |
|---|---|
| 3438 | TI-based malicious URL related to razor threat |

## Notebooks

Entity Explorer - Domain and URL
Microsoft

## Analytics

(Preview) TI map URL entity to OfficeActivity data Scheduled

## Hunting

| ↑↓ | Query | ↑↓ | Provider | ↑↓ | Data Source |
|---|---|---|---|---|---|
| ★ | Preview - TI map File entity to Security Event | | Microsoft | | SecurityEvent |

## Investigations

# View your threat indicators with KQL

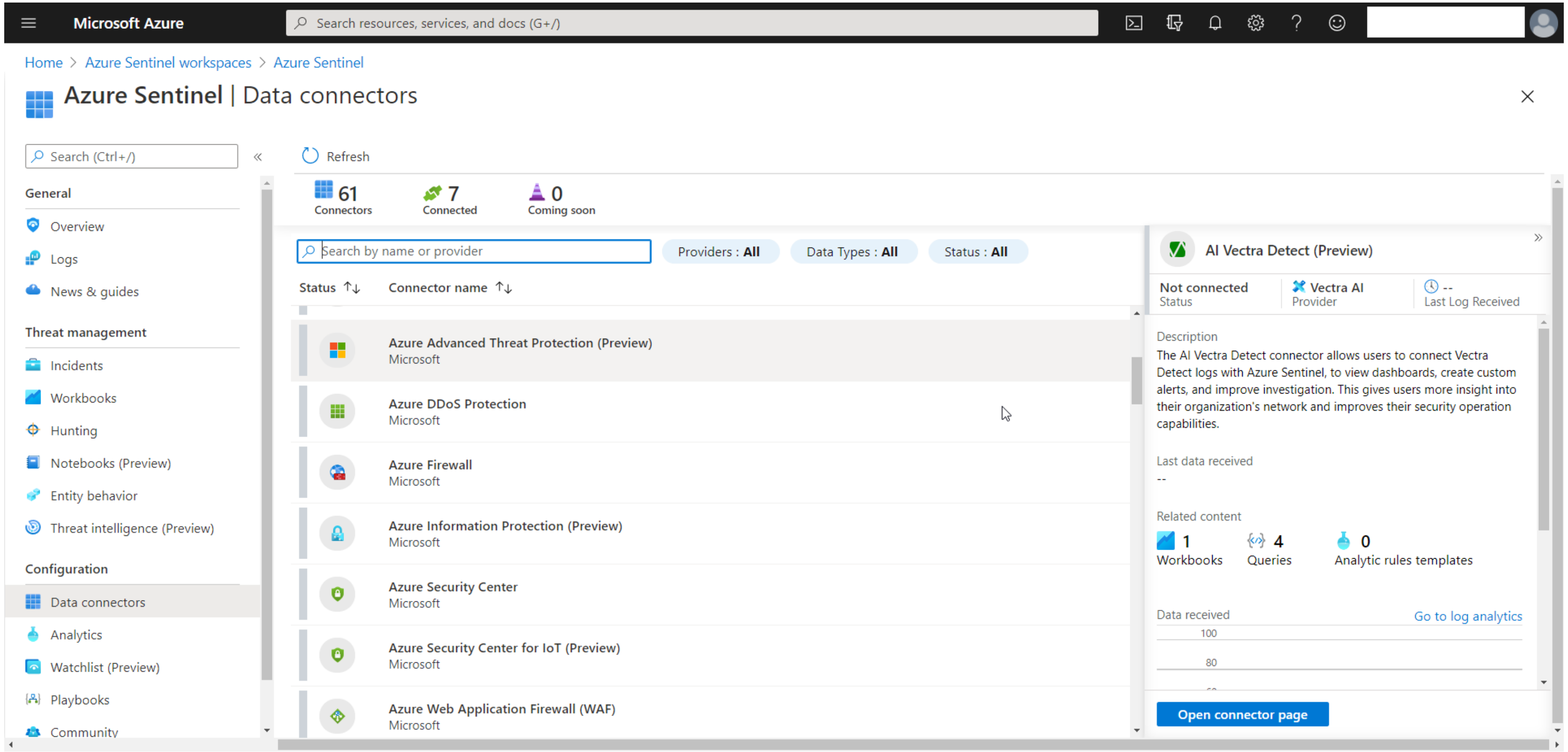
```
The indicators can be accessed in KQL by querying the
ThreatIntelligenceIndicator
table.

//KQL
ThreatIntelligenceIndicator
```

Microsoft

# Connect data to Azure Sentinel using data connectors

# Ingest log data with data connectors

To collect log data, you need to connect your data sources with Azure Sentinel Connectors.



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Azure Sentinel workspaces > Azure Sentinel

Azure Sentinel | Data connectors

Search (Ctrl+/)

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks (Preview)
- Entity behavior
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics
- Watchlist (Preview)
- Playbooks
- Community

Refresh

61 Connectors | 7 Connected | 0 Coming soon

Search by name or provider | Providers : All | Data Types : All | Status : All

| Status ↑↓ | Connector name ↑↓ |
|---|---|
| | Azure Advanced Threat Protection (Preview)<br>Microsoft |
| | Azure DDoS Protection<br>Microsoft |
| | Azure Firewall<br>Microsoft |
| | Azure Information Protection (Preview)<br>Microsoft |
| | Azure Security Center<br>Microsoft |
| | Azure Security Center for IoT (Preview)<br>Microsoft |
| | Azure Web Application Firewall (WAF)<br>Microsoft |

AI Vectra Detect (Preview)

| Not connected | Vectra AI | -- |
|---|---|---|
| Status | Provider | Last Log Received |

Description

The AI Vectra Detect connector allows users to connect Vectra Detect logs with Azure Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives users more insight into their organization's network and improves their security operation capabilities.

Last data received

--

Related content

1 Workbooks | 4 Queries | 0 Analytic rules templates

Data received | Go to log analytics

Open connector page

# Understand data connector providers

- Microsoft 365 Defender and related Defender services
- Microsoft 365 and Azure Services
- Vendor connectors
- Custom connectors using the Log Analytics API
- Logstash plugin
- Common Event Format (CEF) and Syslog connector

Microsoft

# Create detections and perform investigations using Azure Sentinel

Microsoft

# Threat detection with Azure Sentinel analytics

# Azure Sentinel Analytics explained

## Overview

Azure Sentinel Analytics analyzes data from various sources to identify correlations and anomalies.

By using analytics rules, you can trigger alerts based on the attack techniques that are used by known malicious actors.

You can set up these rules to help ensure your SOC is alerted to potential security incidents in your environment in a timely fashion.

## Common security analytics use cases include:

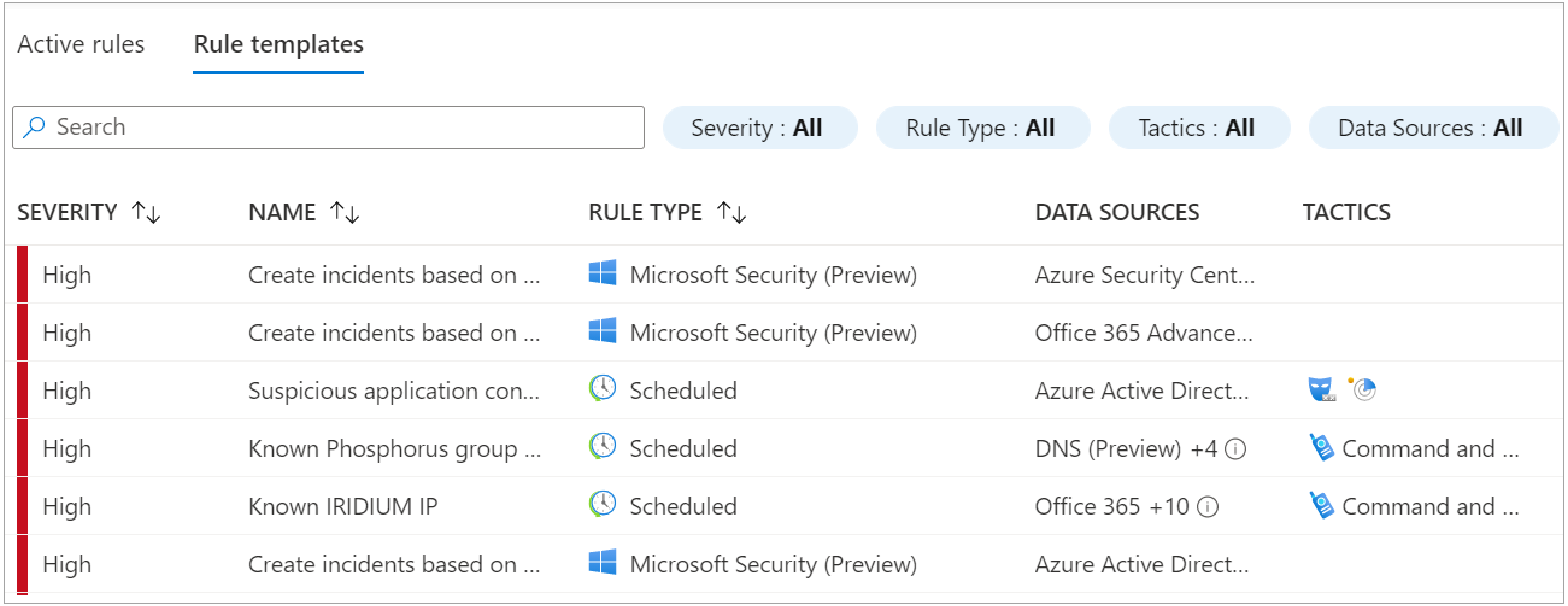
- Identification of compromised accounts
- User behavior analysis to detect potentially suspicious patterns
- Network traffic analysis to locate trends indicating potential attacks
- Detection of data exfiltration by attackers
- Detection of insider threats

# Types of analytics rules

- Microsoft security
- Scheduled alerts
- Fusion
- Machine learning (ML) behavior analytics

# Create an analytics rule from a template

The Analytics section in Azure Sentinel contains rule templates that are preloaded from the Azure Sentinel GitHub repository. You can use these templates to create a rule to detect security threats.



Active rules    **Rule templates**

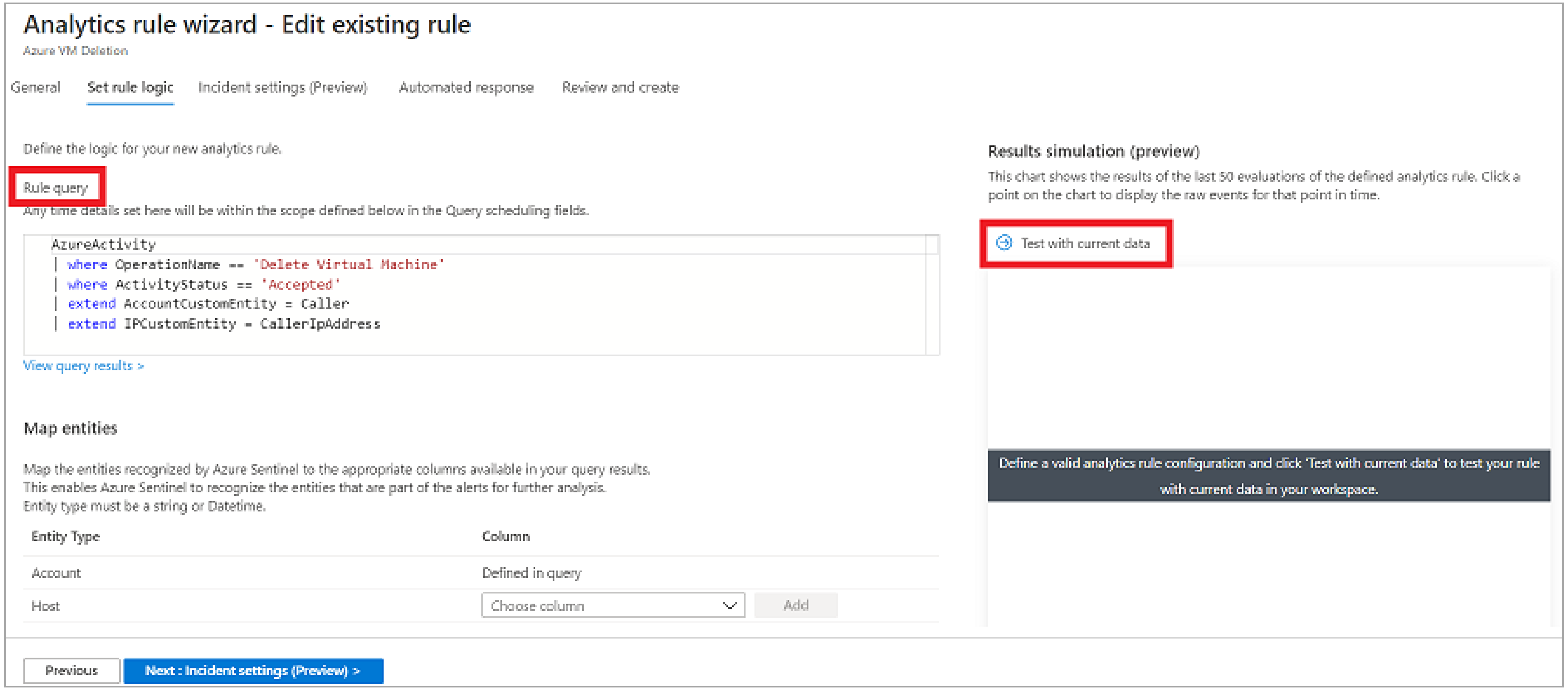
Search

Severity : **All**    Rule Type : **All**    Tactics : **All**    Data Sources : **All**

| SEVERITY ↑↓ | NAME ↑↓ | RULE TYPE ↑↓ | DATA SOURCES | TACTICS |
|---|---|---|---|---|
| High | Create incidents based on ... | Microsoft Security (Preview) | Azure Security Cent... | |
| High | Create incidents based on ... | Microsoft Security (Preview) | Office 365 Advance... | |
| High | Suspicious application con... | Scheduled | Azure Active Direct... | |
| High | Known Phosphorus group ... | Scheduled | DNS (Preview) +4 ⓘ | Command and ... |
| High | Known IRIDIUM IP | Scheduled | Office 365 +10 ⓘ | Command and ... |
| High | Create incidents based on ... | Microsoft Security (Preview) | Azure Active Direct... | |

# Create an analytics rule from a wizard

Creating a custom rule from the scheduled query rule type provides you with the highest level of customization. You can define, your own KQL code, set a schedule to run the alerts, or provide an automated action by associating an Azure Sentinel Playbook.



Analytics rule wizard - Edit existing rule

Azure VM Deletion

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where OperationName == 'Delete Virtual Machine'
| where ActivityStatus == 'Accepted'
| extend AccountCustomEntity = Caller
| extend IPCustomEntity = CallerIpAddress
```

View query results >

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results.
This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis.
Entity type must be a string or Datetime.

| Entity Type | Column |
|---|---|
| Account | Defined in query |
| Host | Choose column |

Results simulation (preview)

This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

Define a valid analytics rule configuration and click 'Test with current data' to test your rule with current data in your workspace.

Microsoft

# Threat response with Azure Sentinel playbooks

# Azure Sentinel playbooks explained

### Azure Sentinel as a SIEM and SOAR solution

Security Orchestration, Automation and Response (SOAR) solution

### Azure Sentinel playbooks

Security playbooks are collections of procedures based on Azure Logic Apps that run in response to an alert.

### Azure Logic Apps

Azure Logic Apps is a cloud service that automates the operation of your business processes.

### Logic Apps Connector

A connector is a component that provides an interface to a service.

### Triggers and Actions

A trigger is an event that occurs when a specific set of conditions is satisfied. An action is an operation that performs a task.

### Azure Sentinel Logic Apps connector

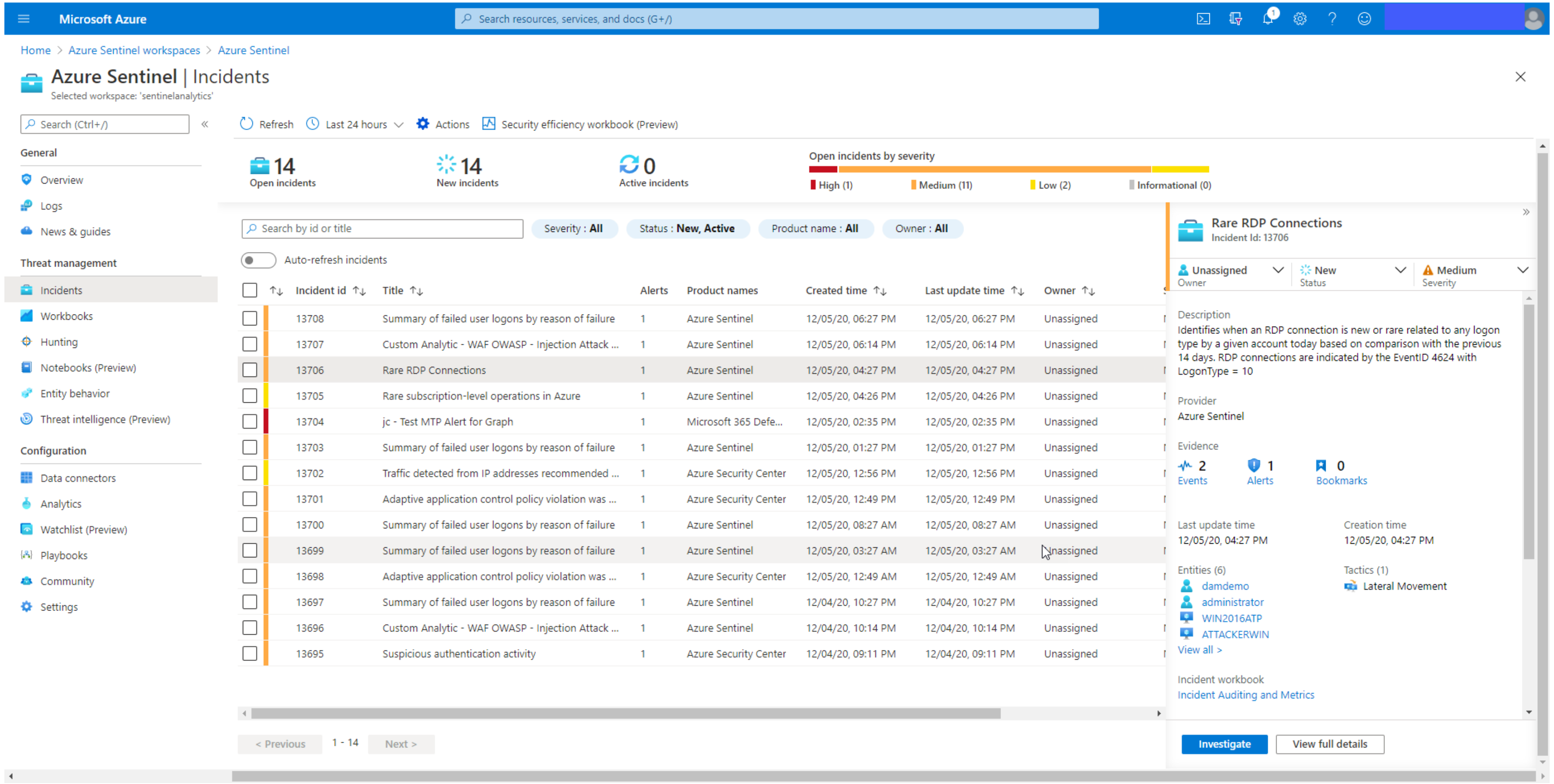
An Azure Sentinel playbook uses an Azure Sentinel Logic Apps connector.

Microsoft

# Security incident management in Azure Sentinel

# Describe incident management

Incident management is the complete process of incident investigation, from creation, to in-depth investigation, and finally to resolution.



Azure Sentinel | Incidents

Selected workspace: 'sentinelanalytics'

14 Open incidents | 14 New incidents | 0 Active incidents

Open incidents by severity: High (1) | Medium (11) | Low (2) | Informational (0)

Severity : **All** | Status : **New, Active** | Product name : **All** | Owner : **All**

Auto-refresh incidents

| Incident id | Title | Alerts | Product names | Created time | Last update time | Owner |
|---|---|---|---|---|---|---|
| 13708 | Summary of failed user logons by reason of failure | 1 | Azure Sentinel | 12/05/20, 06:27 PM | 12/05/20, 06:27 PM | Unassigned |
| 13707 | Custom Analytic - WAF OWASP - Injection Attack ... | 1 | Azure Sentinel | 12/05/20, 06:14 PM | 12/05/20, 06:14 PM | Unassigned |
| 13706 | Rare RDP Connections | 1 | Azure Sentinel | 12/05/20, 04:27 PM | 12/05/20, 04:27 PM | Unassigned |
| 13705 | Rare subscription-level operations in Azure | 1 | Azure Sentinel | 12/05/20, 04:26 PM | 12/05/20, 04:26 PM | Unassigned |
| 13704 | jc - Test MTP Alert for Graph | 1 | Microsoft 365 Defe... | 12/05/20, 02:35 PM | 12/05/20, 02:35 PM | Unassigned |
| 13703 | Summary of failed user logons by reason of failure | 1 | Azure Sentinel | 12/05/20, 01:27 PM | 12/05/20, 01:27 PM | Unassigned |
| 13702 | Traffic detected from IP addresses recommended ... | 1 | Azure Security Center | 12/05/20, 12:56 PM | 12/05/20, 12:56 PM | Unassigned |
| 13701 | Adaptive application control policy violation was ... | 1 | Azure Security Center | 12/05/20, 12:49 PM | 12/05/20, 12:49 PM | Unassigned |
| 13700 | Summary of failed user logons by reason of failure | 1 | Azure Sentinel | 12/05/20, 08:27 AM | 12/05/20, 08:27 AM | Unassigned |
| 13699 | Summary of failed user logons by reason of failure | 1 | Azure Sentinel | 12/05/20, 03:27 AM | 12/05/20, 03:27 AM | Unassigned |
| 13698 | Adaptive application control policy violation was ... | 1 | Azure Security Center | 12/05/20, 12:49 AM | 12/05/20, 12:49 AM | Unassigned |
| 13697 | Summary of failed user logons by reason of failure | 1 | Azure Sentinel | 12/04/20, 10:27 PM | 12/04/20, 10:27 PM | Unassigned |
| 13696 | Custom Analytic - WAF OWASP - Injection Attack ... | 1 | Azure Sentinel | 12/04/20, 10:14 PM | 12/04/20, 10:14 PM | Unassigned |
| 13695 | Suspicious authentication activity | 1 | Azure Security Center | 12/04/20, 09:11 PM | 12/04/20, 09:11 PM | Unassigned |

Rare RDP Connections

Incident Id: 13706

Owner: Unassigned | Status: New | Severity: Medium

Description

Identifies when an RDP connection is new or rare related to any logon type by a given account today based on comparison with the previous 14 days. RDP connections are indicated by the EventID 4624 with LogonType = 10

Provider

Azure Sentinel

Evidence

2 Events | 1 Alerts | 0 Bookmarks

Last update time

12/05/20, 04:27 PM

Creation time

12/05/20, 04:27 PM

Entities (6)

damdemo
administrator
WIN2016ATP
ATTACKERWIN
View all >

Tactics (1)

Lateral Movement

Incident workbook

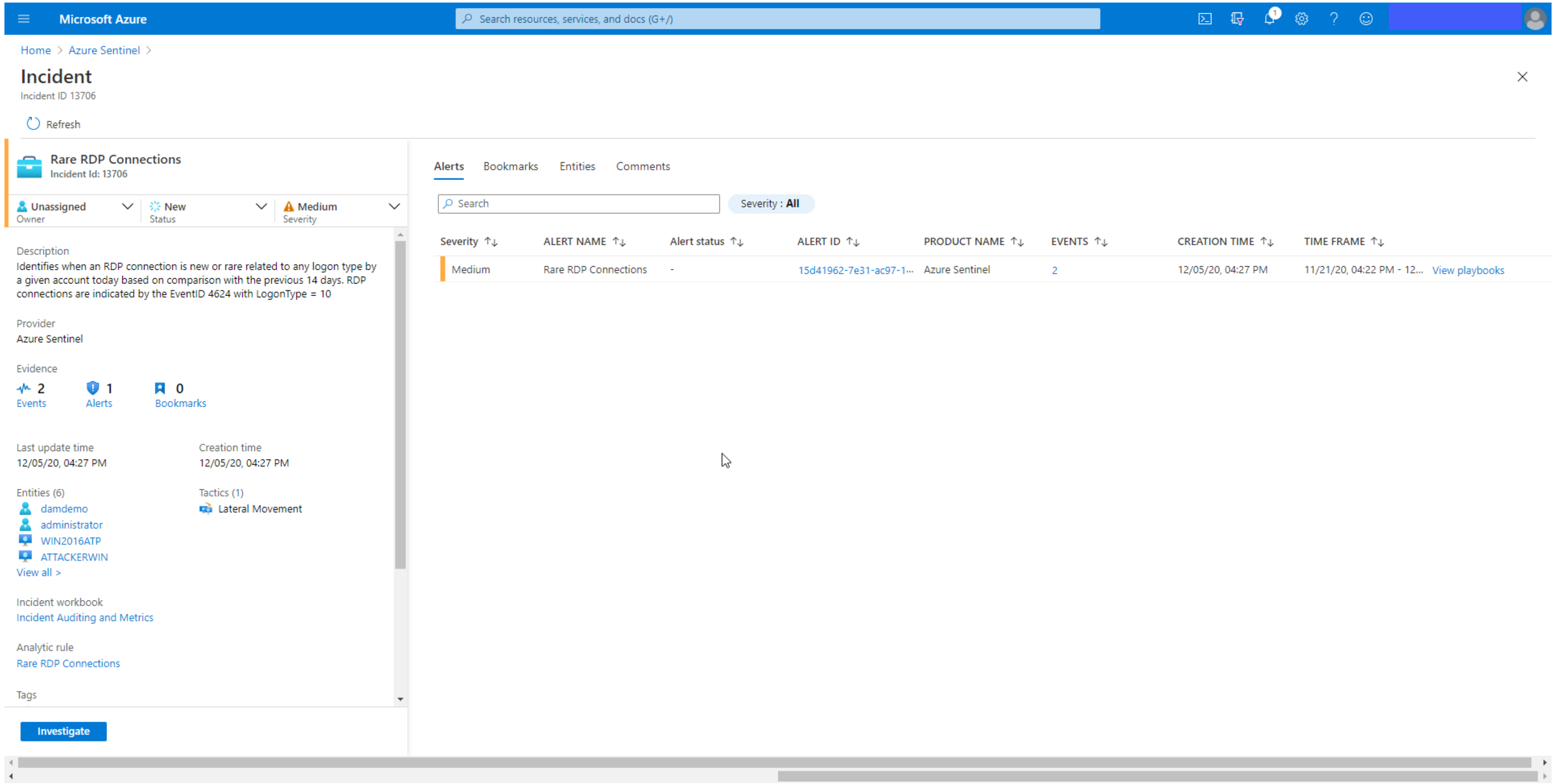
Incident Auditing and Metrics

# Explain evidence and entities

- Events
- Alerts
- Entities
- Bookmarks

# Investigate incidents

Incident management is the complete process of incident investigation, from creation, to in-depth investigation, and finally to resolution.



Incident

Incident ID 13706

Rare RDP Connections

Incident Id: 13706

Owner: Unassigned
Status: New
Severity: Medium

Description
Identifies when an RDP connection is new or rare related to any logon type by a given account today based on comparison with the previous 14 days. RDP connections are indicated by the EventID 4624 with LogonType = 10

Provider
Azure Sentinel

Evidence
2 Events
1 Alerts
0 Bookmarks

Last update time
12/05/20, 04:27 PM

Creation time
12/05/20, 04:27 PM

Entities (6)
damdemo
administrator
WIN2016ATP
ATTACKERWIN
View all >

Tactics (1)
Lateral Movement

Incident workbook
Incident Auditing and Metrics

Analytic rule
Rare RDP Connections

Tags

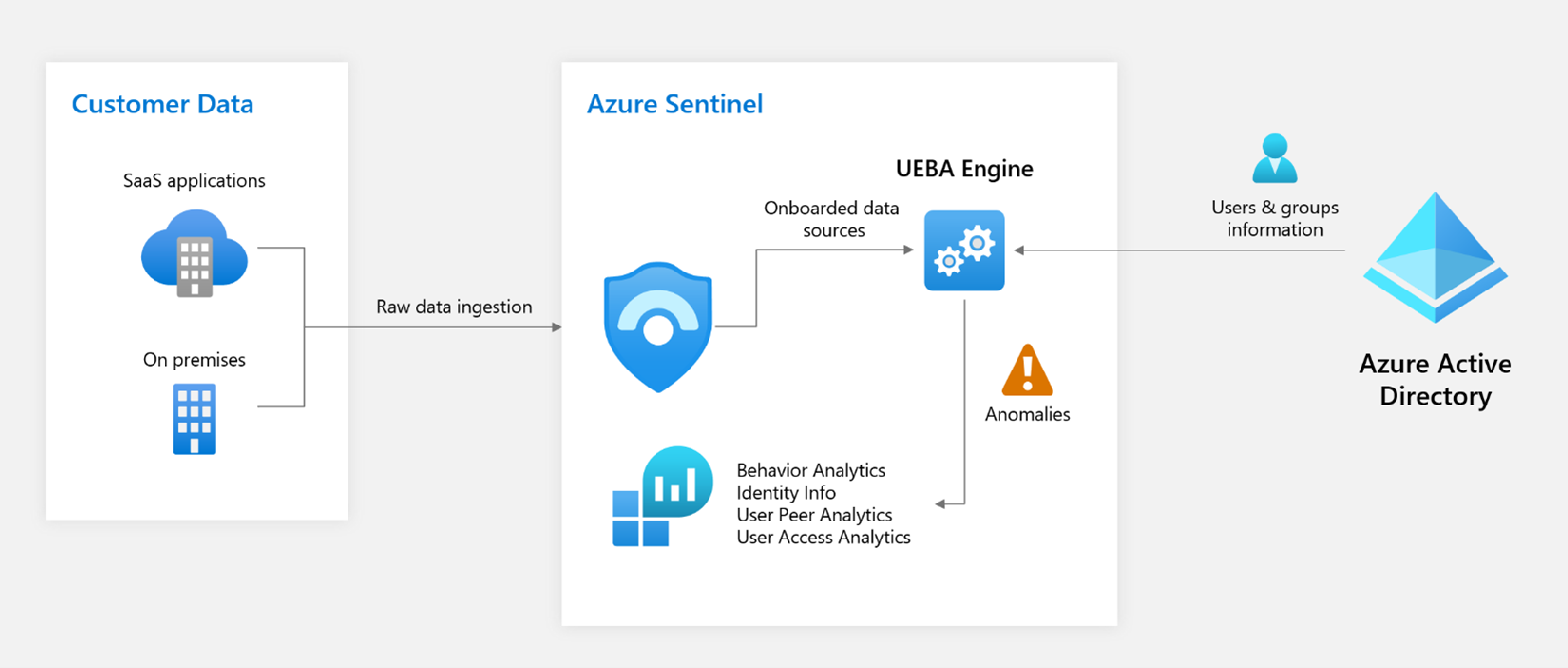
Severity : **All**

| Severity ↑↓ | ALERT NAME ↑↓ | Alert status ↑↓ | ALERT ID ↑↓ | PRODUCT NAME ↑↓ | EVENTS ↑↓ | CREATION TIME ↑↓ | TIME FRAME ↑↓ | |
|---|---|---|---|---|---|---|---|---|
| Medium | Rare RDP Connections | - | 15d41962-7e31-ac97-1... | Azure Sentinel | 2 | 12/05/20, 04:27 PM | 11/21/20, 04:22 PM - 12... | View playbooks |

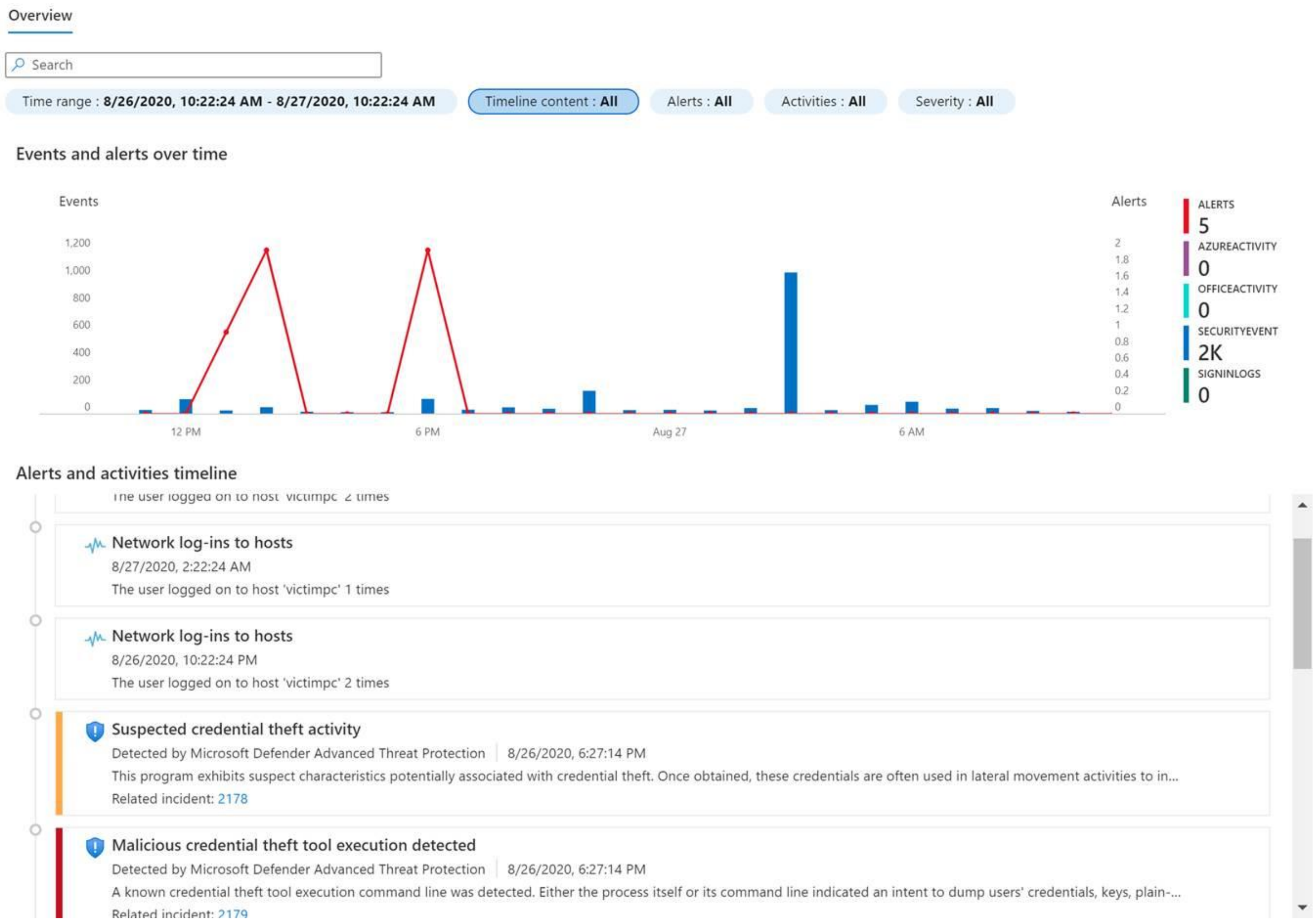
Microsoft

# Use entity behavior analytics in Azure Sentinel

# User and entity behavior analytics explained



# Explore entities



Time range : **8/26/2020, 10:22:24 AM - 8/27/2020, 10:22:24 AM**

Timeline content : **All**

Alerts : **All**

Activities : **All**

Severity : **All**

Events and alerts over time

ALERTS 5

AZUREACTIVITY 0

OFFICEACTIVITY 0

SECURITYEVENT 2K

SIGNINLOGS 0

Alerts and activities timeline

The user logged on to host 'victimpc' 2 times

Network log-ins to hosts
8/27/2020, 2:22:24 AM
The user logged on to host 'victimpc' 1 times

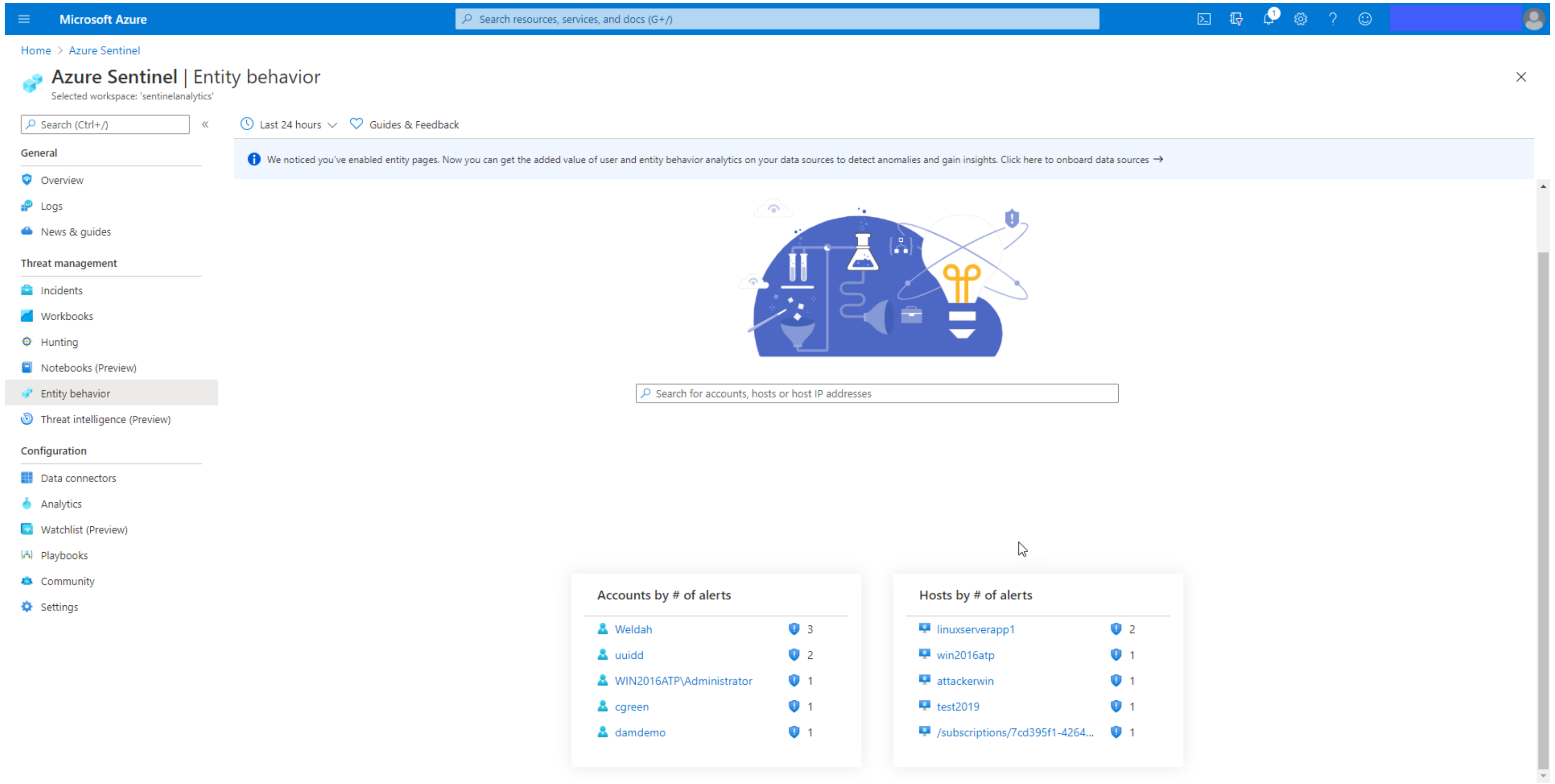
Network log-ins to hosts
8/26/2020, 10:22:24 PM
The user logged on to host 'victimpc' 2 times

Suspected credential theft activity
Detected by Microsoft Defender Advanced Threat Protection | 8/26/2020, 6:27:14 PM
This program exhibits suspect characteristics potentially associated with credential theft. Once obtained, these credentials are often used in lateral movement activities to in...
Related incident: 2178

Malicious credential theft tool execution detected
Detected by Microsoft Defender Advanced Threat Protection | 8/26/2020, 6:27:14 PM
A known credential theft tool execution command line was detected. Either the process itself or its command line indicated an intent to dump users' credentials, keys, plain-...
Related incident: 2179

# Display entity behavior information

The Entity behavior page allows you to search for entities or select from the list of already displayed entities. Once selected the Entity page is displayed with information and timeline of alerts and activities



We noticed you've enabled entity pages. Now you can get the added value of user and entity behavior analytics on your data sources to detect anomalies and gain insights. Click here to onboard data sources →

| Accounts by # of alerts | |
|---|---|
| Weldah | 3 |
| uuidd | 2 |
| WIN2016ATP\Administrator | 1 |
| cgreen | 1 |
| damdemo | 1 |

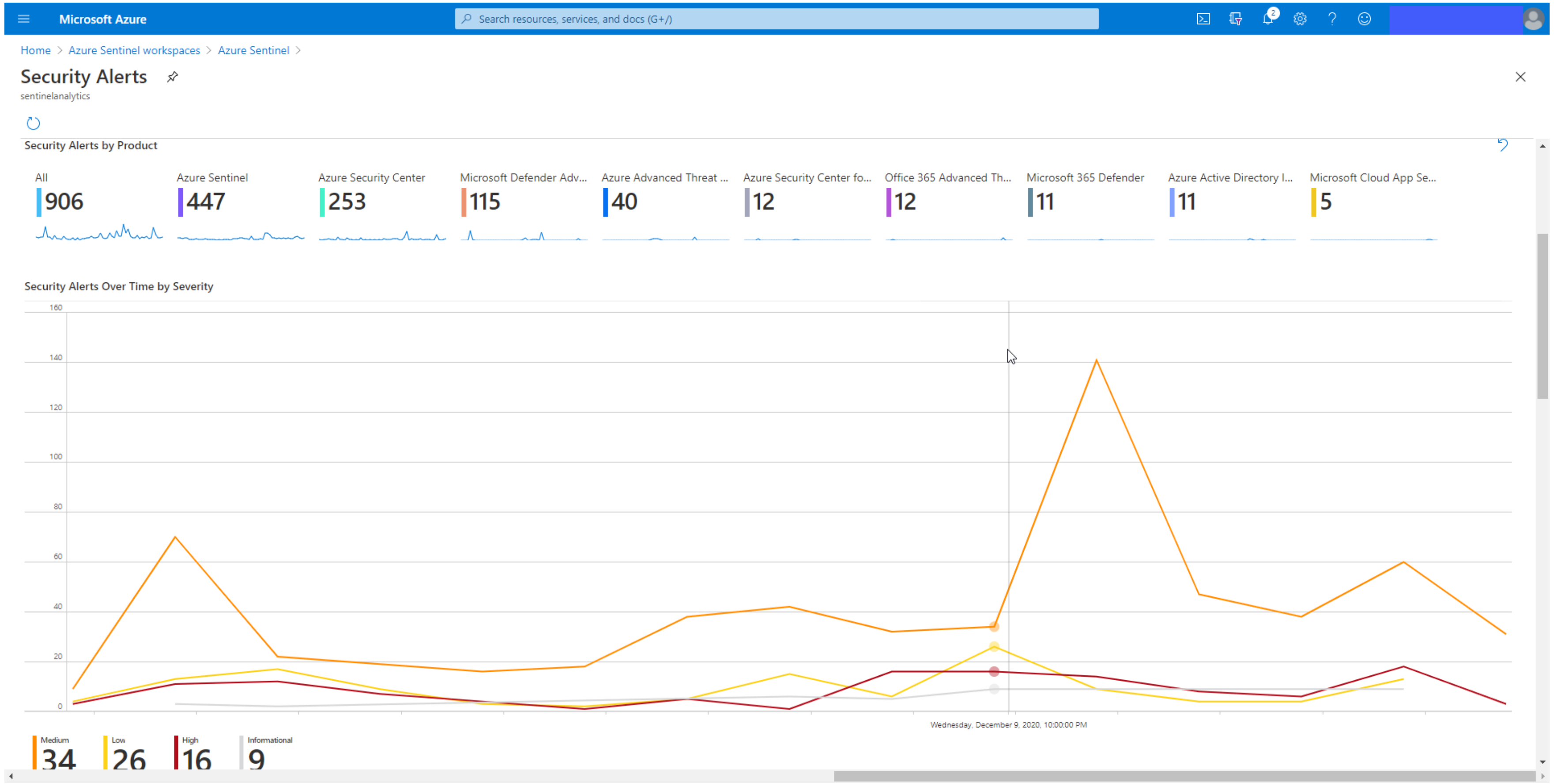
| Hosts by # of alerts | |
|---|---|
| linuxserverapp1 | 2 |
| win2016atp | 1 |
| attackerwin | 1 |
| test2019 | 1 |
| /subscriptions/7cd395f1-4264... | 1 |

Microsoft

# Query, visualize, and monitor data in Azure Sentinel

# Azure Sentinel Workbooks

Workbooks provide a dashboard like interface. There are Workbooks provided by Azure Sentinel and the community. You can also create your own Workbooks.



Home > Azure Sentinel workspaces > Azure Sentinel >

Security Alerts

sentinelanalytics

Security Alerts by Product

| All | Azure Sentinel | Azure Security Center | Microsoft Defender Adv... | Azure Advanced Threat ... | Azure Security Center fo... | Office 365 Advanced Th... | Microsoft 365 Defender | Azure Active Directory I... | Microsoft Cloud App Se... |
|---|---|---|---|---|---|---|---|---|---|
| 906 | 447 | 253 | 115 | 40 | 12 | 12 | 11 | 11 | 5 |

Security Alerts Over Time by Severity

| Medium | Low | High | Informational |
|---|---|---|---|
| 34 | 26 | 16 | 9 |

# Create a new Azure Sentinel Workbook

1. Text visualizations
2. Query item
3. Chart visualizations
4. Grid visualizations
5. Parameters
6. Links/tabs
7. Metric steps

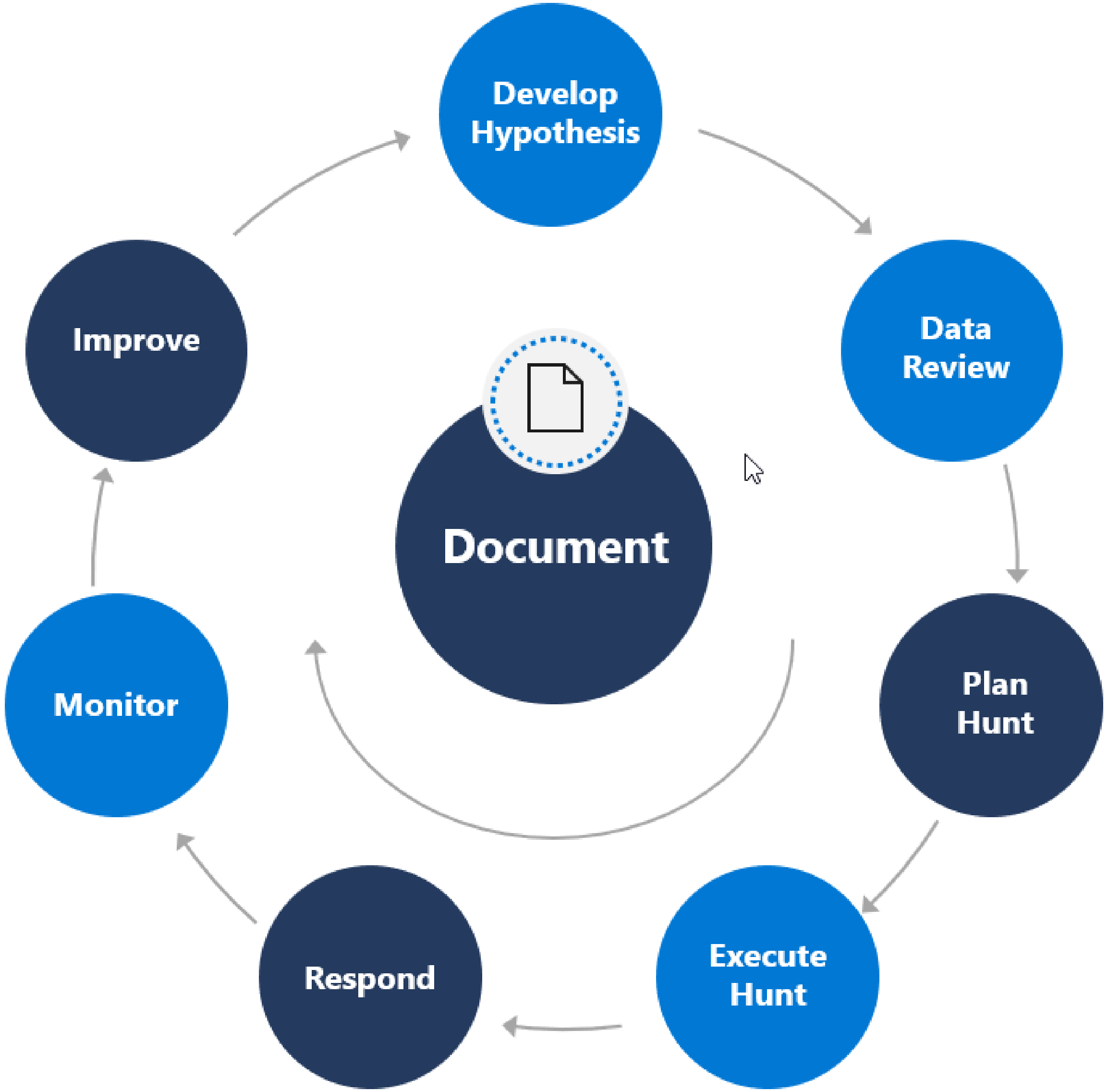
Microsoft

# Perform threat hunting with Azure Sentinel

Microsoft

# Threat hunting with Azure Sentinel

# Cybersecurity threat hunting



# Develop a threat hunting hypothesis

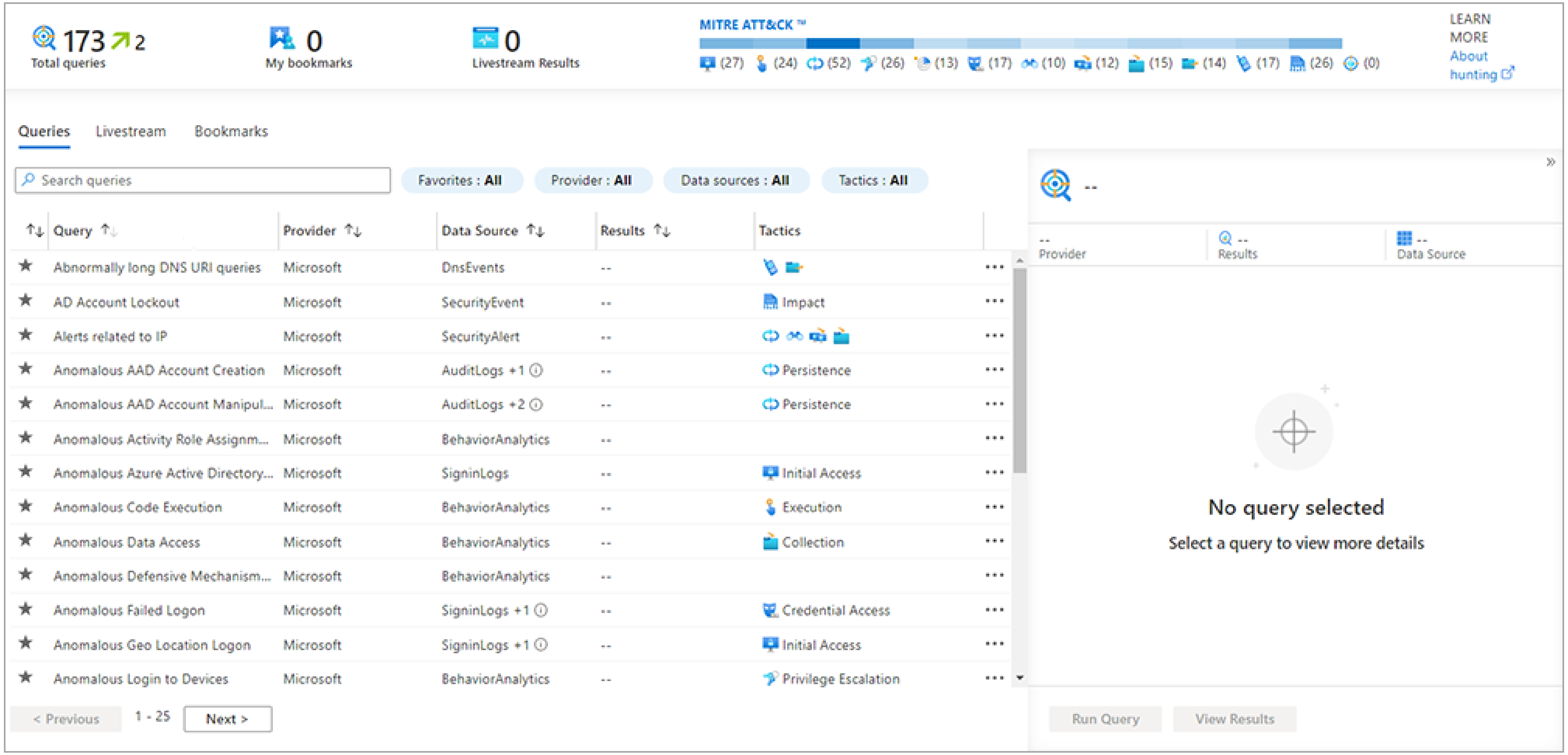
1. Keep it achievable.
2. Keep the scope narrow.
3. Keep it time-bound.
4. Keep it useful and efficient.
5. Keep it related to the threat model that you are defending against.

Microsoft

# Threat hunting with Azure Sentinel (continued)

# Manage Azure Sentinel threat-hunting queries

Create and run hunting queries to search for isolated security threats and unwanted activity.



173 ↗ 2
Total queries

0
My bookmarks

0
Livestream Results

MITRE ATT&CK ™
(27) (24) (52) (26) (13) (17) (10) (12) (15) (14) (17) (26) (0)

LEARN MORE
About hunting

Queries   Livestream   Bookmarks

Search queries

Favorites : All   Provider : All   Data sources : All   Tactics : All

| ↑↓ | Query ↑↓ | Provider ↑↓ | Data Source ↑↓ | Results ↑↓ | Tactics | |
|---|---|---|---|---|---|---|
| ★ | Abnormally long DNS URI queries | Microsoft | DnsEvents | -- | | ••• |
| ★ | AD Account Lockout | Microsoft | SecurityEvent | -- | Impact | ••• |
| ★ | Alerts related to IP | Microsoft | SecurityAlert | -- | | ••• |
| ★ | Anomalous AAD Account Creation | Microsoft | AuditLogs +1 ⓘ | -- | Persistence | ••• |
| ★ | Anomalous AAD Account Manipul... | Microsoft | AuditLogs +2 ⓘ | -- | Persistence | ••• |
| ★ | Anomalous Activity Role Assignm... | Microsoft | BehaviorAnalytics | -- | | ••• |
| ★ | Anomalous Azure Active Directory... | Microsoft | SigninLogs | -- | Initial Access | ••• |
| ★ | Anomalous Code Execution | Microsoft | BehaviorAnalytics | -- | Execution | ••• |
| ★ | Anomalous Data Access | Microsoft | BehaviorAnalytics | -- | Collection | ••• |
| ★ | Anomalous Defensive Mechanism... | Microsoft | BehaviorAnalytics | -- | | ••• |
| ★ | Anomalous Failed Logon | Microsoft | SigninLogs +1 ⓘ | -- | Credential Access | ••• |
| ★ | Anomalous Geo Location Logon | Microsoft | SigninLogs +1 ⓘ | -- | Initial Access | ••• |
| ★ | Anomalous Login to Devices | Microsoft | BehaviorAnalytics | -- | Privilege Escalation | ••• |

< Previous   1 - 25   Next >

--

-- Provider   -- Results   -- Data Source

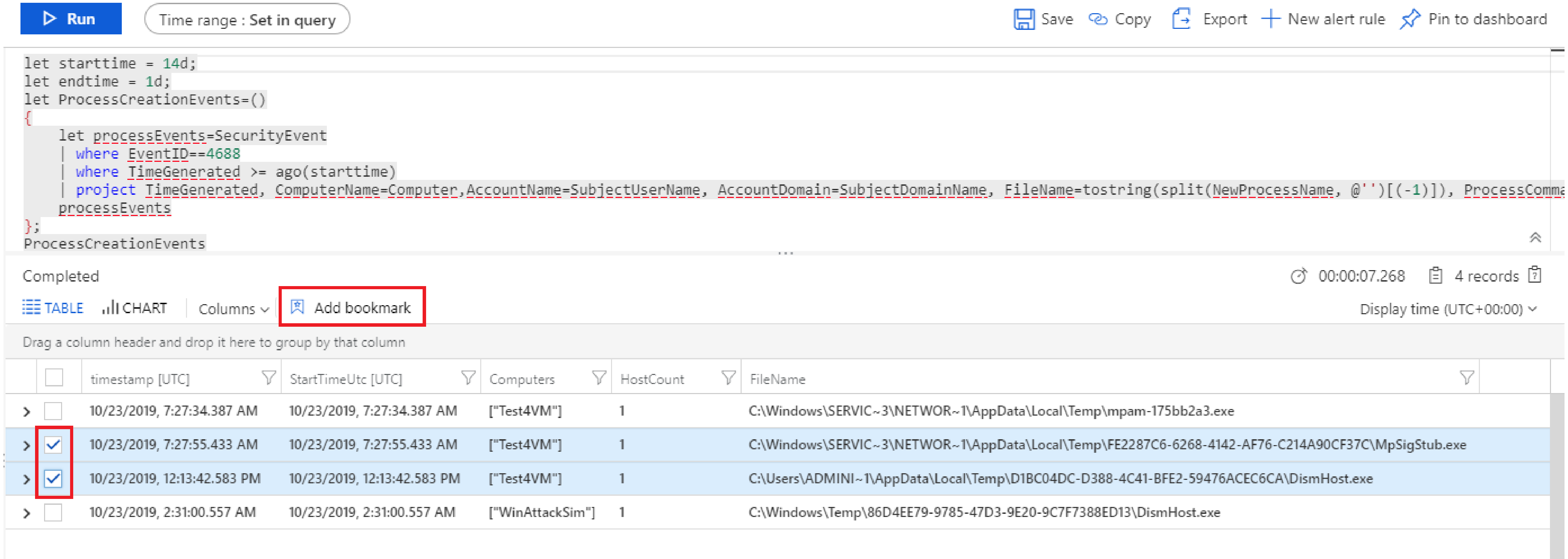
No query selected

Select a query to view more details

Run Query   View Results

# Save key findings with bookmarks

Bookmarks in Azure Sentinel can help you hunt for threats by preserving the queries you ran in Azure Sentinel, along with the query results that you deem relevant.



```
let starttime = 14d;
let endtime = 1d;
let ProcessCreationEvents=()
{
    let processEvents=SecurityEvent
    | where EventID==4688
    | where TimeGenerated >= ago(starttime)
    | project TimeGenerated, ComputerName=Computer,AccountName=SubjectUserName, AccountDomain=SubjectDomainName, FileName=tostring(split(NewProcessName, @'')[(-1)]), ProcessComma
    processEvents
};
ProcessCreationEvents
```

Completed

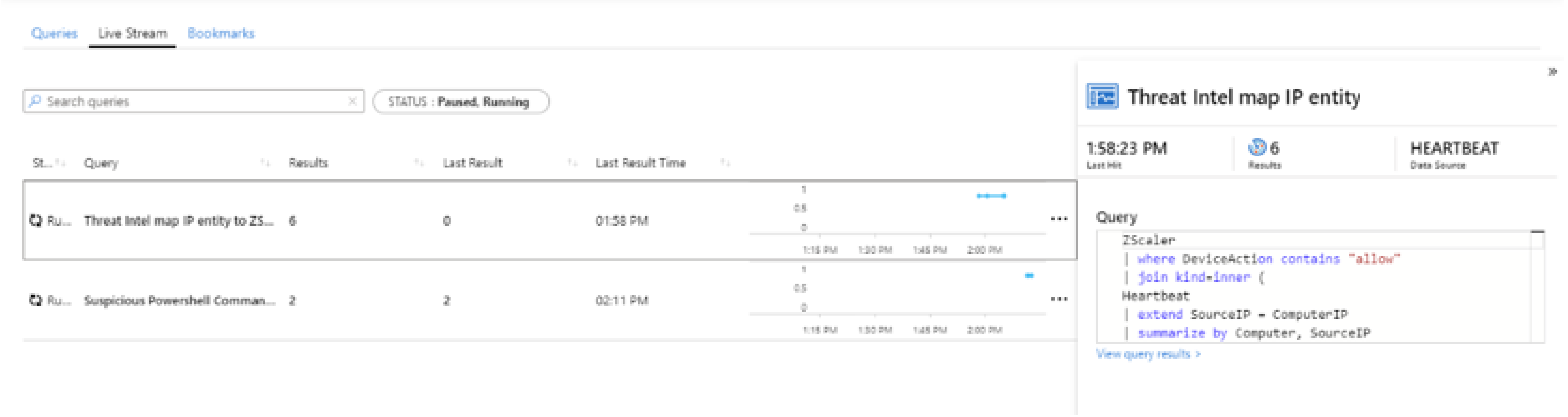
00:00:07.268  4 records

TABLE
CHART
Columns
Add bookmark
Display time (UTC+00:00)
Drag a column header and drop it here to group by that column

| | □ | timestamp [UTC] | StartTimeUtc [UTC] | Computers | HostCount | FileName |
|---|---|---|---|---|---|---|
| > | □ | 10/23/2019, 7:27:34.387 AM | 10/23/2019, 7:27:34.387 AM | ["Test4VM"] | 1 | C:\Windows\SERVIC~3\NETWOR~1\AppData\Local\Temp\mpam-175bb2a3.exe |
| > | ☑ | 10/23/2019, 7:27:55.433 AM | 10/23/2019, 7:27:55.433 AM | ["Test4VM"] | 1 | C:\Windows\SERVIC~3\NETWOR~1\AppData\Local\Temp\FE2287C6-6268-4142-AF76-C214A90CF37C\MpSigStub.exe |
| > | ☑ | 10/23/2019, 12:13:42.583 PM | 10/23/2019, 12:13:42.583 PM | ["Test4VM"] | 1 | C:\Users\ADMINI~1\AppData\Local\Temp\D1BC04DC-D388-4C41-BFE2-59476ACEC6CA\DismHost.exe |
| > | □ | 10/23/2019, 2:31:00.557 AM | 10/23/2019, 2:31:00.557 AM | ["WinAttackSim"] | 1 | C:\Windows\Temp\86D4EE79-9785-47D3-9E20-9C7F7388ED13\DismHost.exe |

# Observe threats over time with livestream

You can use the hunting livestream to test queries against live events as they occur. Livestream provides interactive sessions that can notify you when Azure Sentinel finds matching events for your query.



| St... | Query | Results | Last Result | Last Result Time |
|---|---|---|---|---|
| Ru... | Threat Intel map IP entity to ZS... | 6 | 0 | 01:58 PM |
| Ru... | Suspicious Powershell Comman... | 2 | 2 | 02:11 PM |

Threat Intel map IP entity

| 1:58:23 PM | 6 | HEARTBEAT |
|---|---|---|
| Last Hit | Results | Data Source |

Query

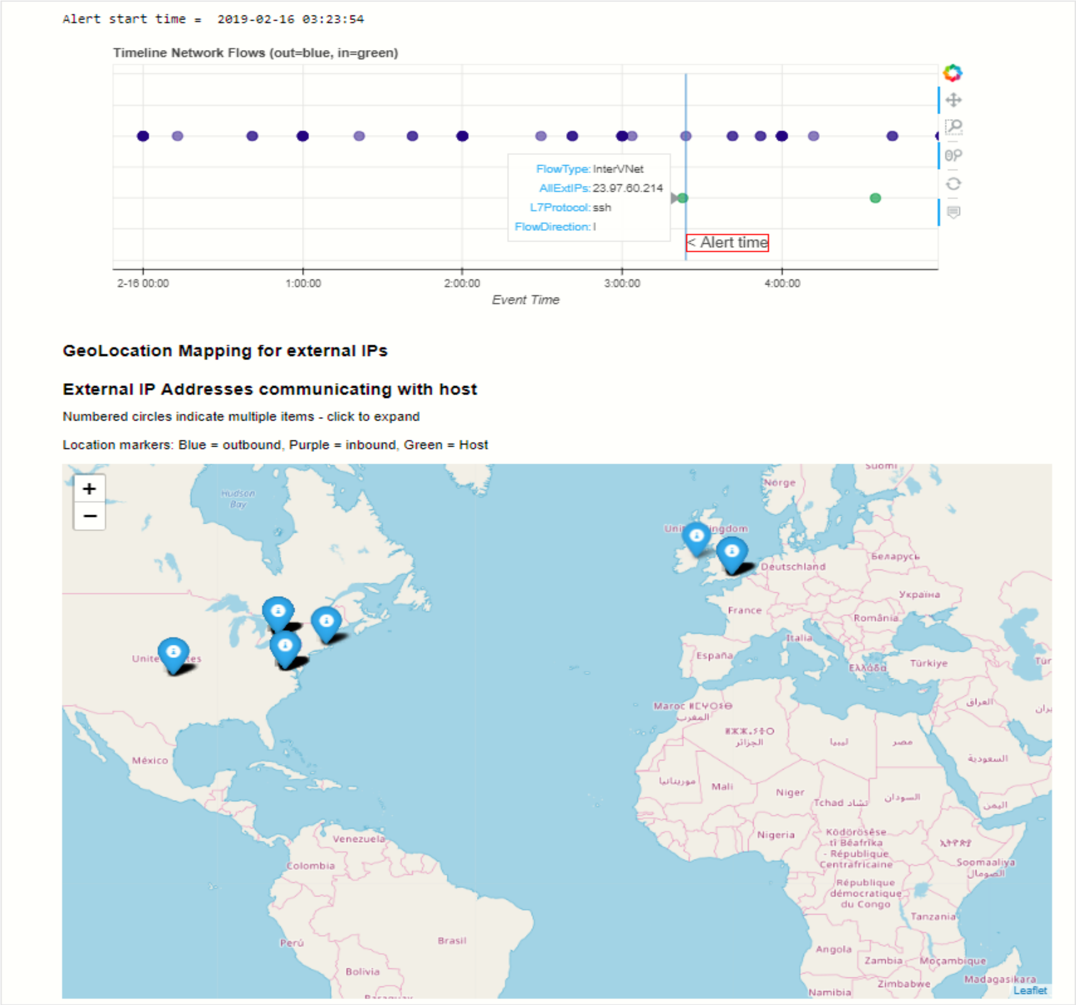
```
ZScaler
| where DeviceAction contains "allow"
| join kind=inner (
Heartbeat
| extend SourceIP = ComputerIP
| summarize by Computer, SourceIP
```

View query results >

Microsoft

# Hunt for threats using notebooks in Azure Sentinel

# Hunt with notebooks



```
Alert start time =  2019-02-16 03:23:54
```

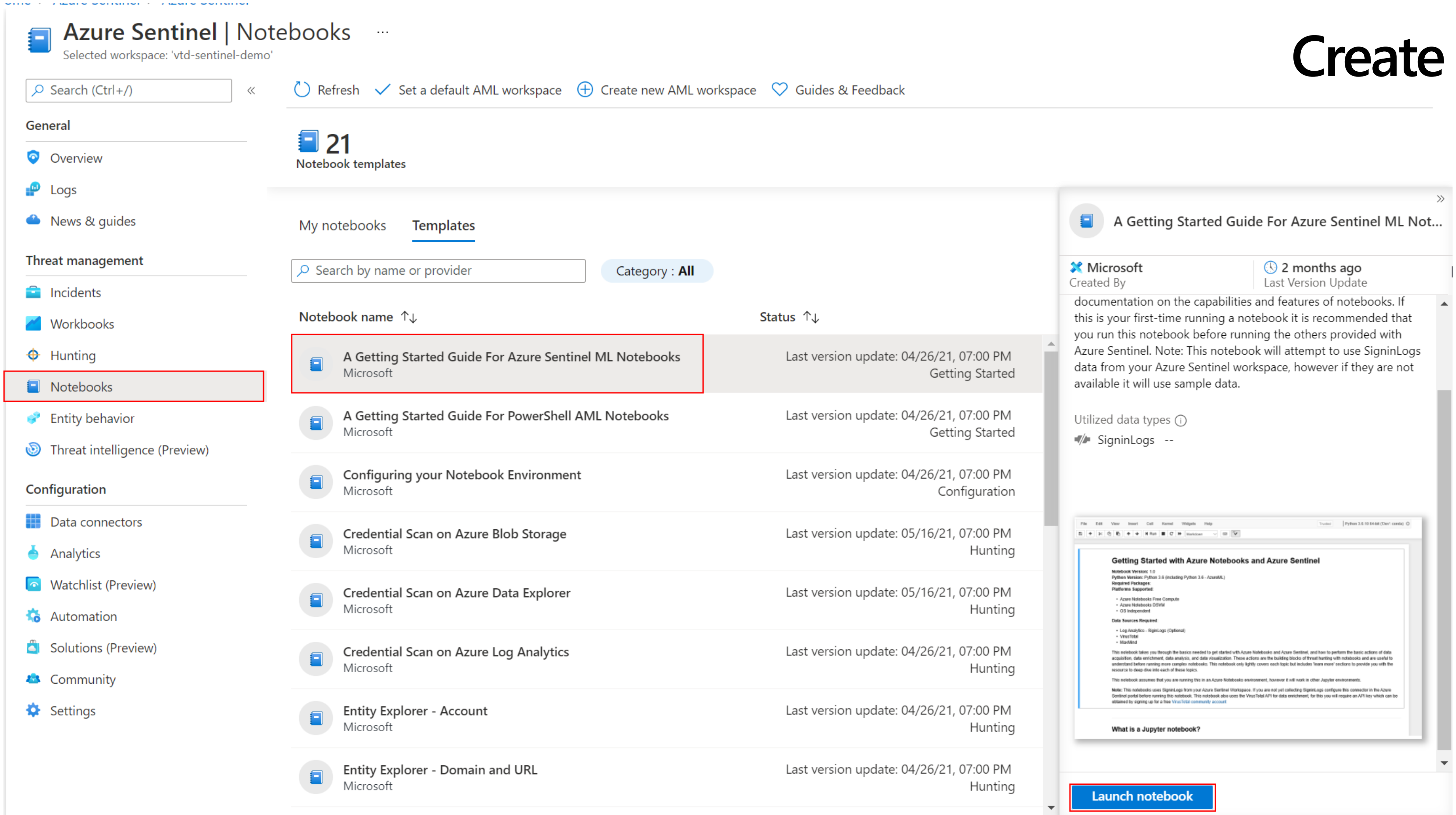
**GeoLocation Mapping for external IPs**

**External IP Addresses communicating with host**

Numbered circles indicate multiple items - click to expand

Location markers: Blue = outbound, Purple = inbound, Green = Host

# Create a notebook



## Azure Sentinel | Notebooks

Selected workspace: 'vtd-sentinel-demo'

21
Notebook templates

Category : **All**

| Notebook name | Status |
|---|---|
| A Getting Started Guide For Azure Sentinel ML Notebooks<br>Microsoft | Last version update: 04/26/21, 07:00 PM<br>Getting Started |
| A Getting Started Guide For PowerShell AML Notebooks<br>Microsoft | Last version update: 04/26/21, 07:00 PM<br>Getting Started |
| Configuring your Notebook Environment<br>Microsoft | Last version update: 04/26/21, 07:00 PM<br>Configuration |
| Credential Scan on Azure Blob Storage<br>Microsoft | Last version update: 05/16/21, 07:00 PM<br>Hunting |
| Credential Scan on Azure Data Explorer<br>Microsoft | Last version update: 05/16/21, 07:00 PM<br>Hunting |
| Credential Scan on Azure Log Analytics<br>Microsoft | Last version update: 04/26/21, 07:00 PM<br>Hunting |
| Entity Explorer - Account<br>Microsoft | Last version update: 04/26/21, 07:00 PM<br>Hunting |
| Entity Explorer - Domain and URL<br>Microsoft | Last version update: 04/26/21, 07:00 PM<br>Hunting |

A Getting Started Guide For Azure Sentinel ML Not...

Microsoft
Created By

2 months ago
Last Version Update

documentation on the capabilities and features of notebooks. If this is your first-time running a notebook it is recommended that you run this notebook before running the others provided with Azure Sentinel. Note: This notebook will attempt to use SigninLogs data from your Azure Sentinel workspace, however if they are not available it will use sample data.

Utilized data types
SigninLogs --

**Getting Started with Azure Notebooks and Azure Sentinel**

**Notebook Version:** 1.0
**Python Version:** Python 3.6 (including Python 3.6 - AzureML)
**Required Packages:**
**Platforms Supported:**

- Azure Notebooks Free Compute
- Azure Notebooks DSVM
- OS Independent

**Data Sources Required:**

- Log Analytics - SigninLogs (Optional)
- VirusTotal
- MaxMind

This notebook takes you through the basics needed to get started with Azure Notebooks and Azure Sentinel, and how to perform the basic actions of data acquisition, data enrichment, data analysis, and data visualization. These actions are the building blocks of threat hunting with notebooks and are useful to understand before running more complex notebooks. This notebook only lightly covers each topic but includes 'learn more' sections to provide you with the resource to deep dive into each of these topics.

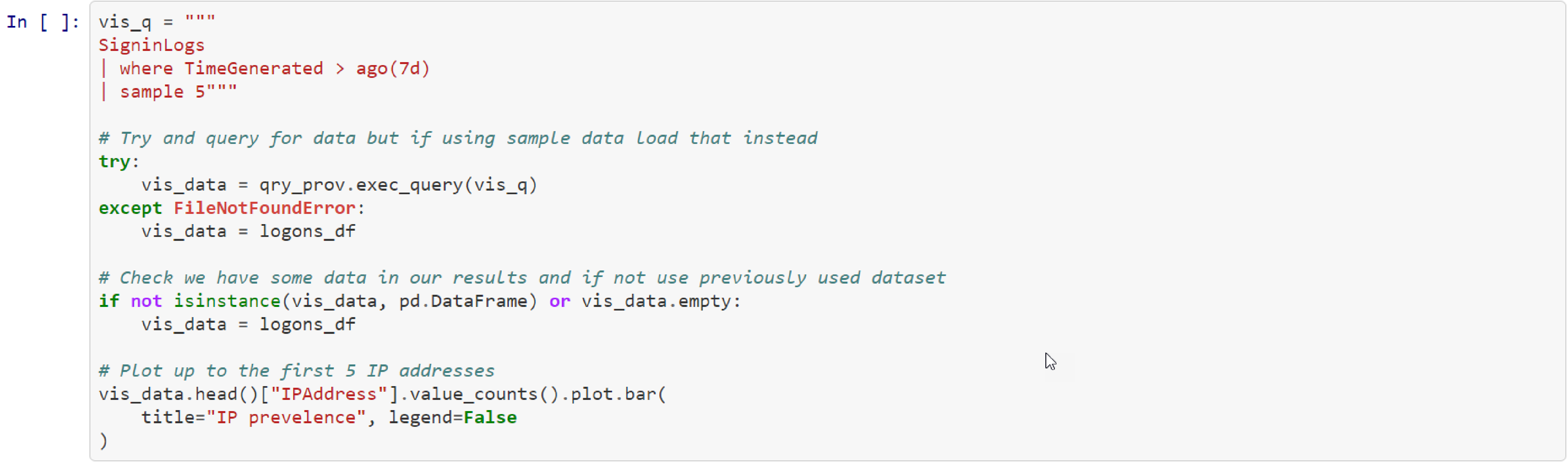
This notebook assumes that you are running this in an Azure Notebooks environment, however it will work in other Jupyter environments.

**Note:** This notebooks uses SigninLogs from your Azure Sentinel Workspace. If you are not yet collecting SigninLogs configure this connector in the Azure Sentinel portal before running this notebook. This notebook also uses the VirusTotal API for data enrichment, for this you will require an API key which can be obtained by signing up for a free VirusTotal community account

**What is a Jupyter notebook?**

# Explore notebook code

The following code blocks of the "Getting Started Guide For Azure Sentinel ML Notebooks" notebook provide a representative example of working with Azure Sentinel data.



In [ ]:

```
vis_q = """
SigninLogs
| where TimeGenerated > ago(7d)
| sample 5"""

# Try and query for data but if using sample data load that instead
try:
    vis_data = qry_prov.exec_query(vis_q)
except FileNotFoundError:
    vis_data = logons_df

# Check we have some data in our results and if not use previously used dataset
if not isinstance(vis_data, pd.DataFrame) or vis_data.empty:
    vis_data = logons_df

# Plot up to the first 5 IP addresses
vis_data.head()["IPAddress"].value_counts().plot.bar(
    title="IP prevelence", legend=False
)
```