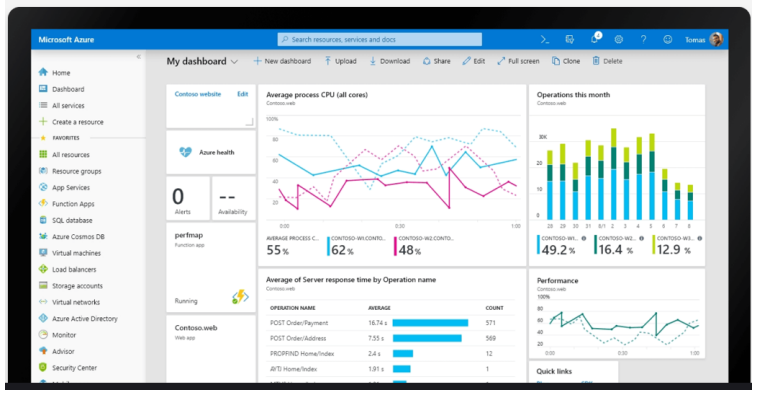
2019

Global Azure

BOOTCAMP



Microsoft Azure Sentinel

Intelligent security analytics at cloud scale with Azure Sentinel

Who am I ?

- Martin Boam
- Snr O365 Consultant @ Microsoft
- Retired Office Apps and Services MVP
- **@martinboam**
- I blog at **www.ucmart.uk**

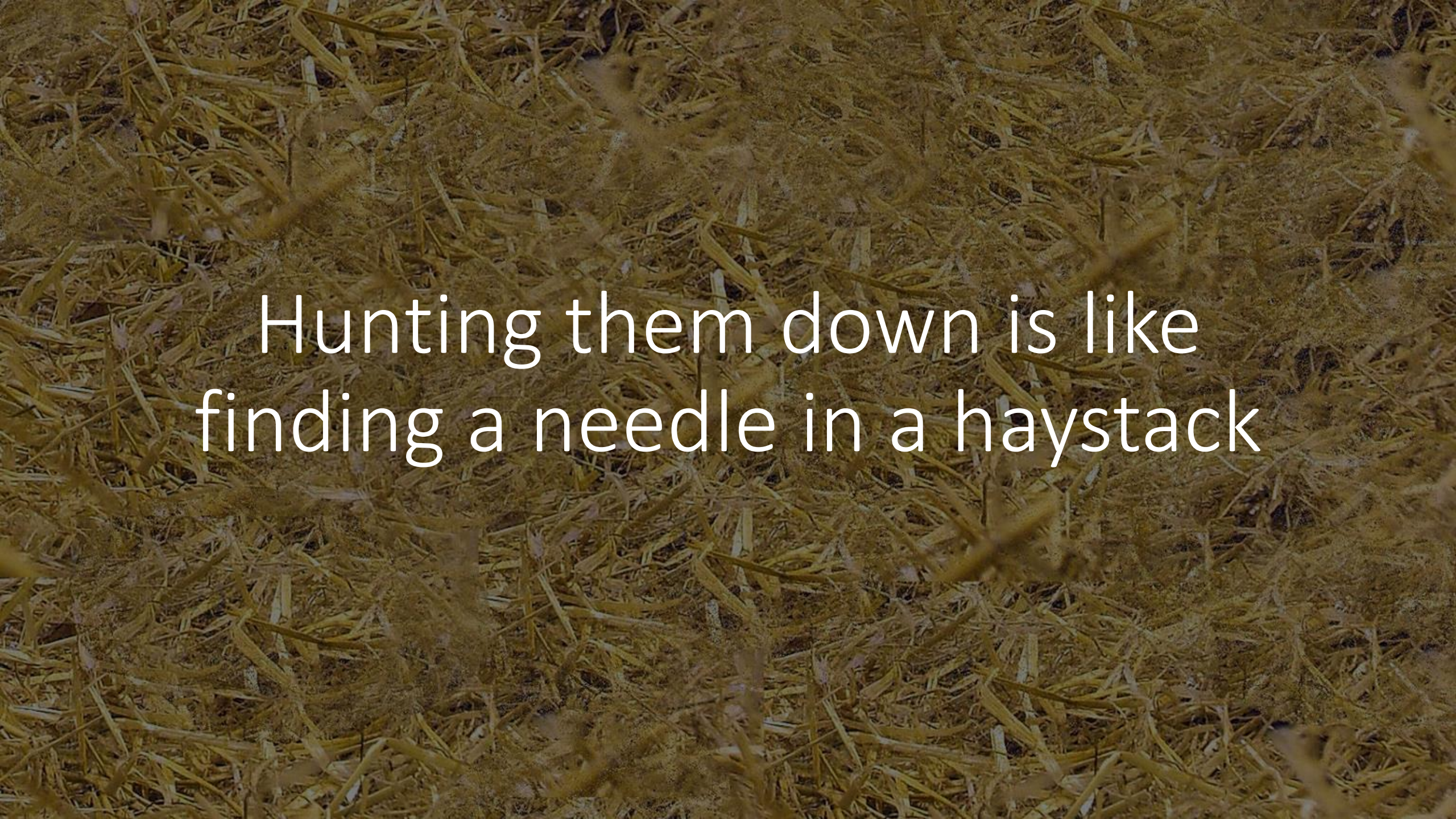
User Group Host

- **Microsoft Cloud User Group Manchester**
- **Microsoft Teams and SfB UG Manchester**

Agenda

- SecOps Challenges
- What is SIEM ?
- Microsoft Azure Sentinel
- Demo
- Q and A

Everyday, there are millions of cyber attacks


Hunting them down is like
finding a needle in a haystack

Security Operations (SecOps) Challenges

The SecOps mission of protecting organizations' information and assets is becoming increasingly difficult

Threats continue to grow in complexity and volume

Alert fatigue: SOCs see too many alerts from disconnected products

There is a global shortage of security analysts and experience

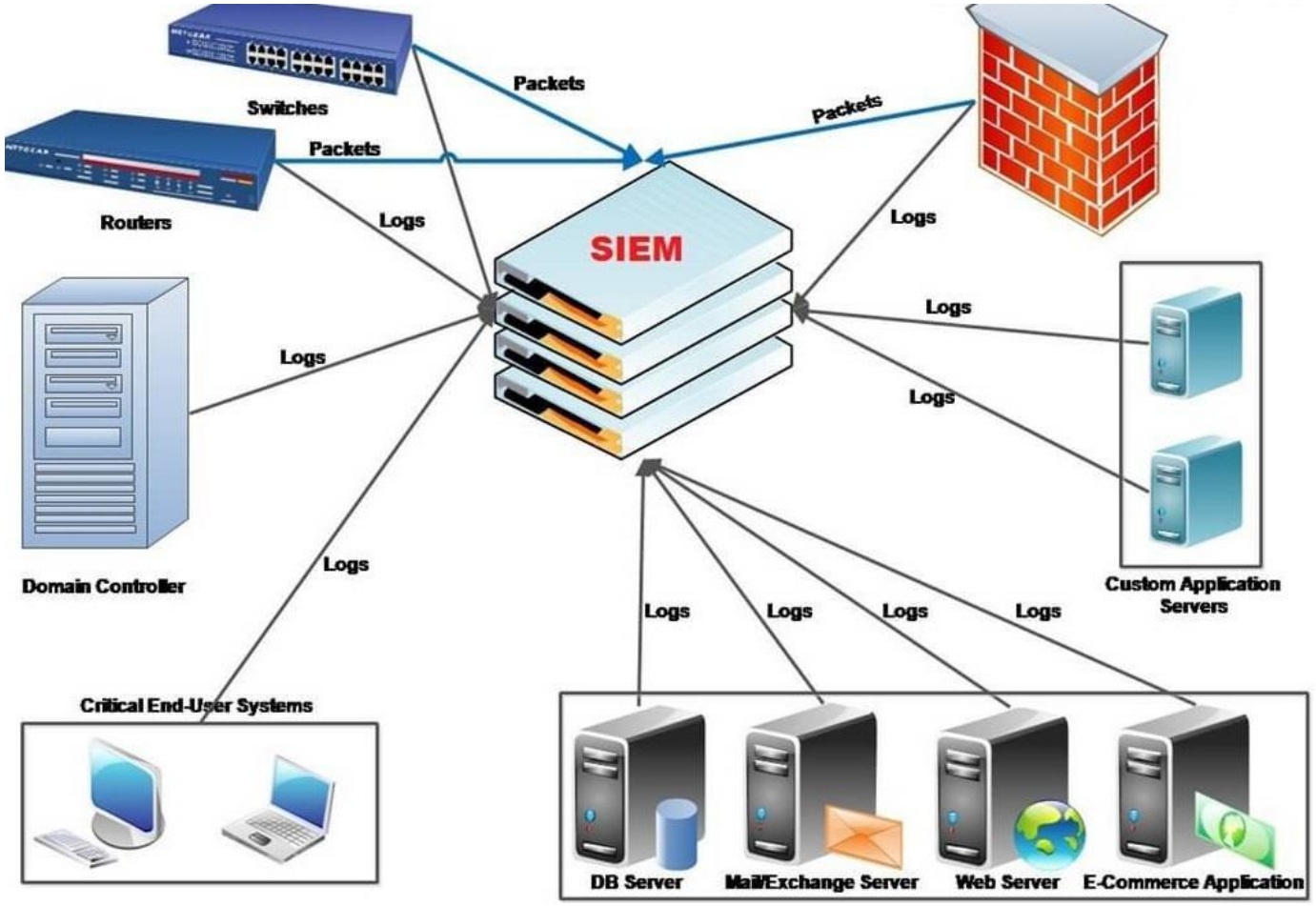
Investigation is complex and time-consuming

Current SIEM solutions are not architected for today's demands, or tomorrow's

Security Information and Event Management (SIEM)

- Software products and services combine security information management (SIM) and security event management (SEM).
- Provide real-time analysis of security alerts generated by applications and network hardware.
- Vendors sell SIEM as software, as appliances or as managed services; these products are also used to log security data and generate reports for compliance purposes.

Traditional SIEM



Introducing Microsoft Azure Sentinel

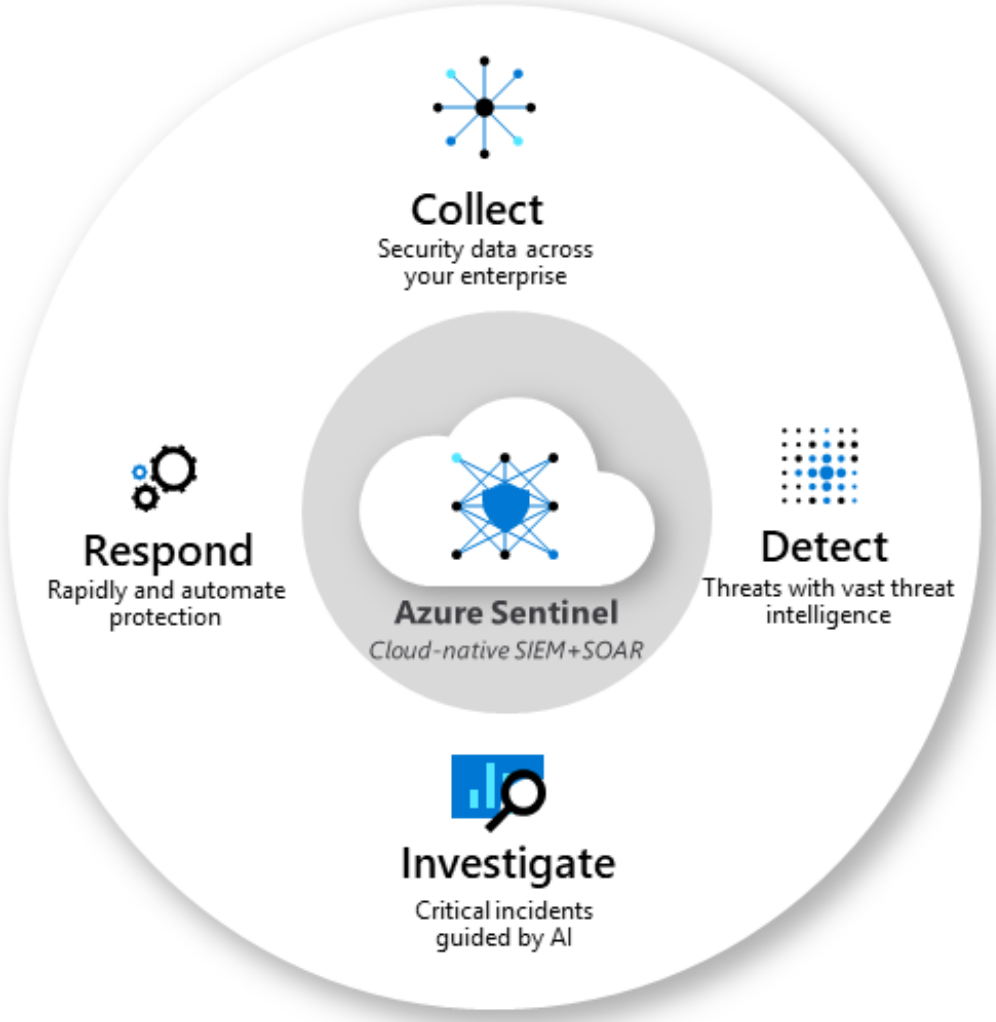
Cloud-native SIEM for intelligent security analytics for your entire enterprise

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

- Scalable, cloud-native, **security information event management (SIEM)** and **security orchestration automated response (SOAR)** solution.

- Building on the full range of existing Azure services, Azure Sentinel natively incorporates proven foundations, like Log Analytics, and Logic Apps.

- Enriches your investigation and detection with AI, and provides Microsoft's threat intelligence stream and enables you to bring your own threat intelligence.



Benefits

Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detect previously undetected threats, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.

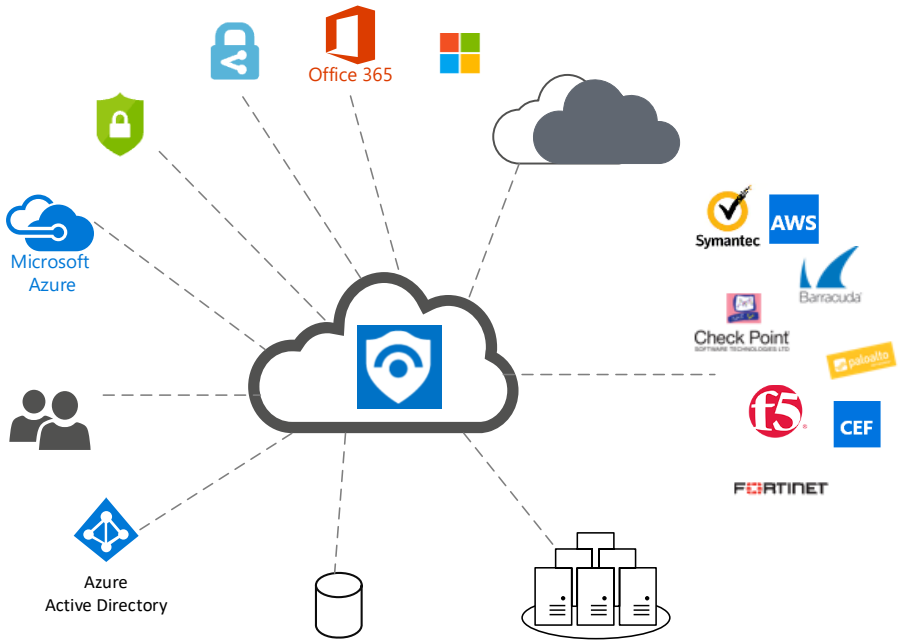
Respond to incidents rapidly with built-in orchestration and automation of common tasks.

No Infrastructure setup or maintenance

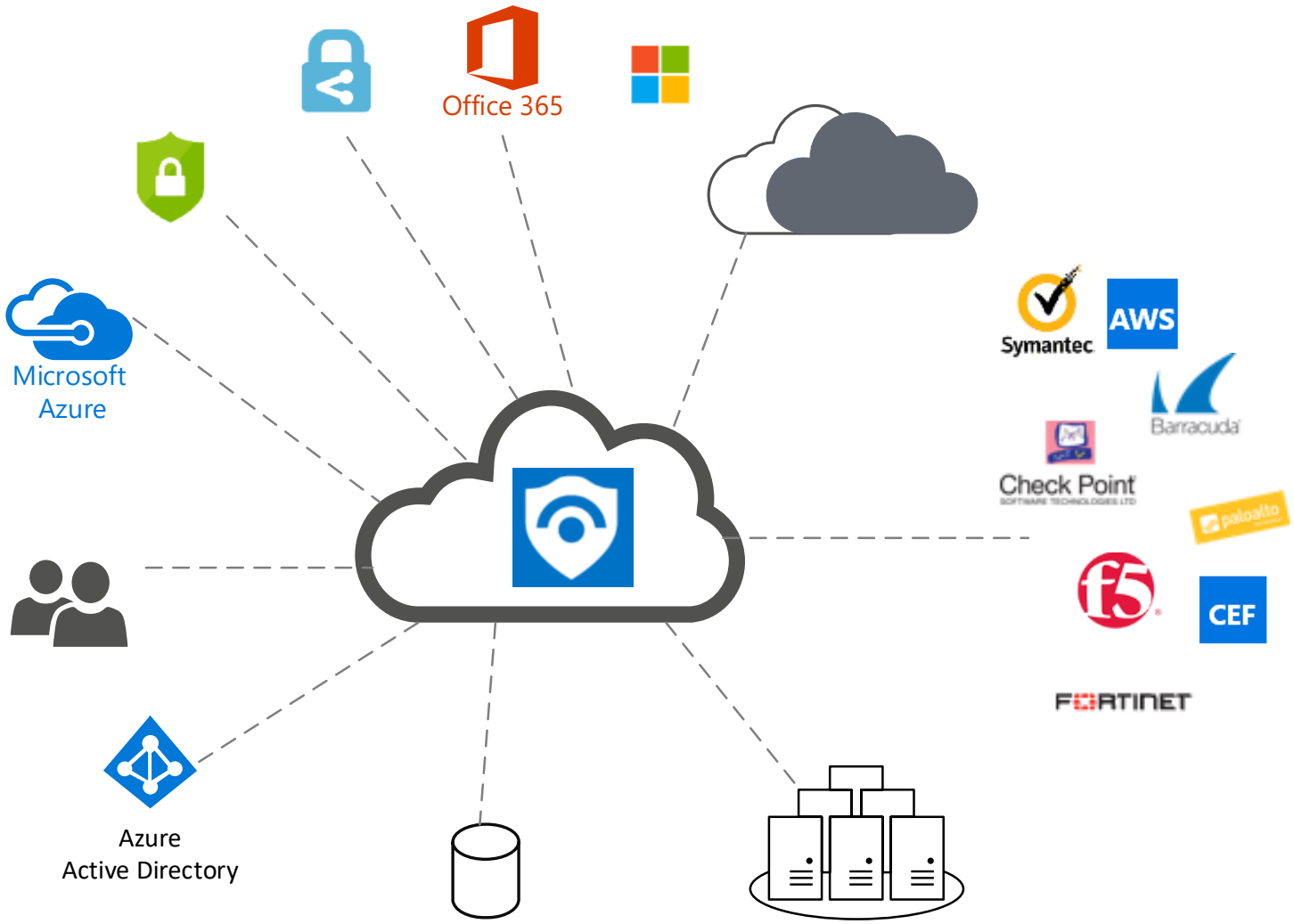
SIEM Service available in Azure Portal

Scale Automatically, put no limits to compute or storage resources

Data Connectors



Azure Sentinel

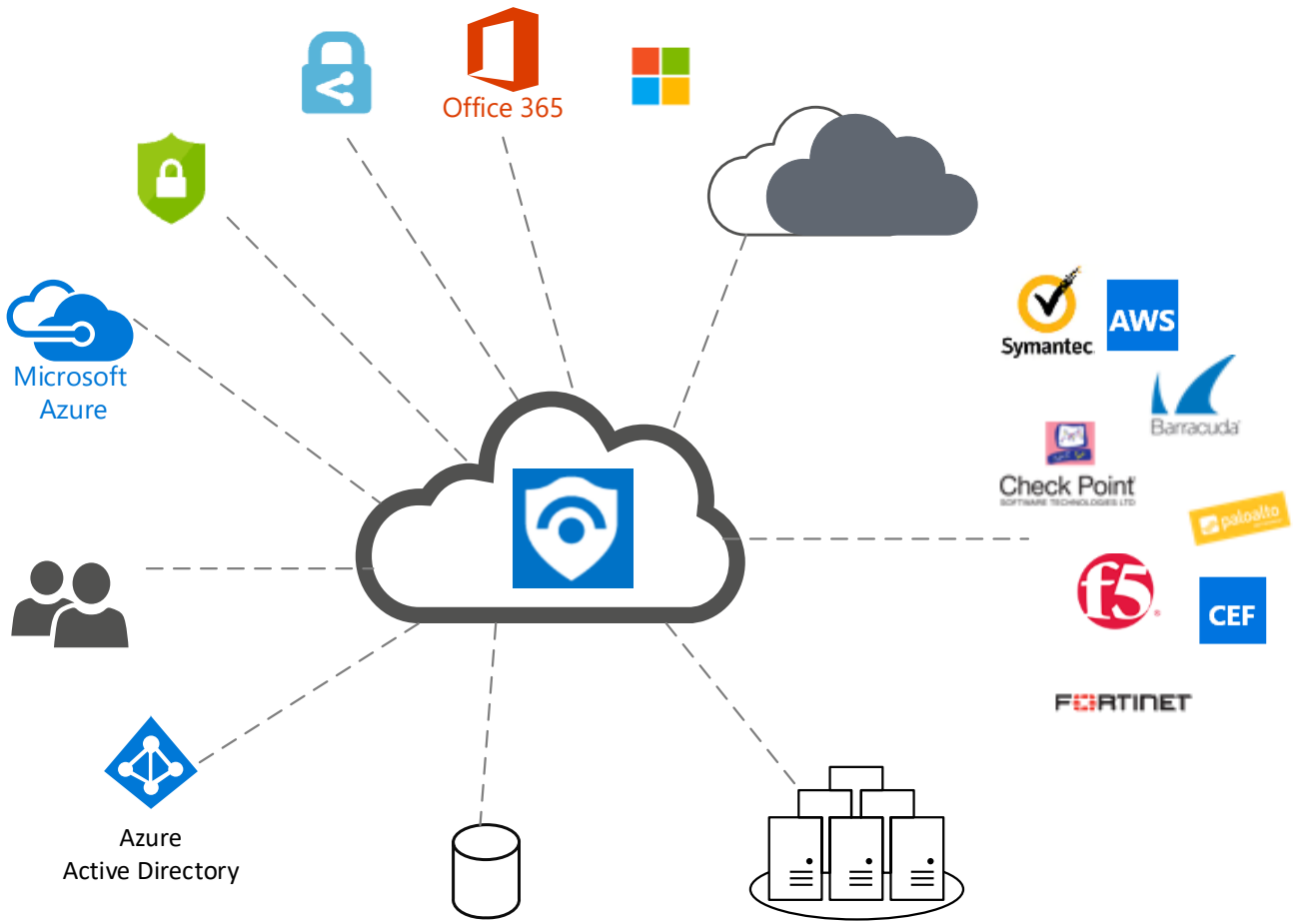


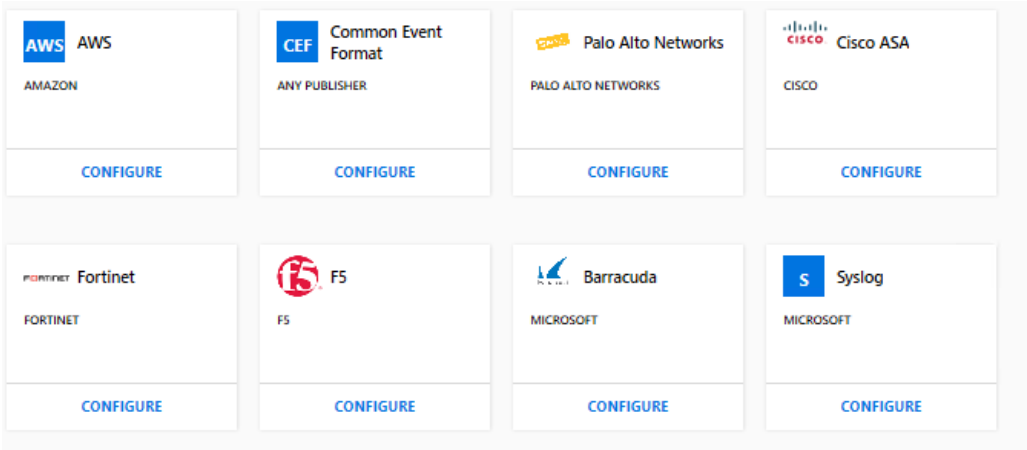
- Pre-wired integration with Microsoft solutions
- Connectors for many partner solutions
- Standard log format support for all sources

Connect your Data

Azure Sentinel comes with a number of connectors for Microsoft and non-Microsoft solutions, available out of the box and providing real-time integration, including

- Microsoft
  - Office 365
  - Azure AD audit logs and sign-ins
  - Azure Activity
  - Azure AD Identity Protection
  - Azure Security Center
  - Azure Information Protection
  - Azure Advanced Threat Protection
  - Cloud App Security
  - Windows security events
  - Windows firewall



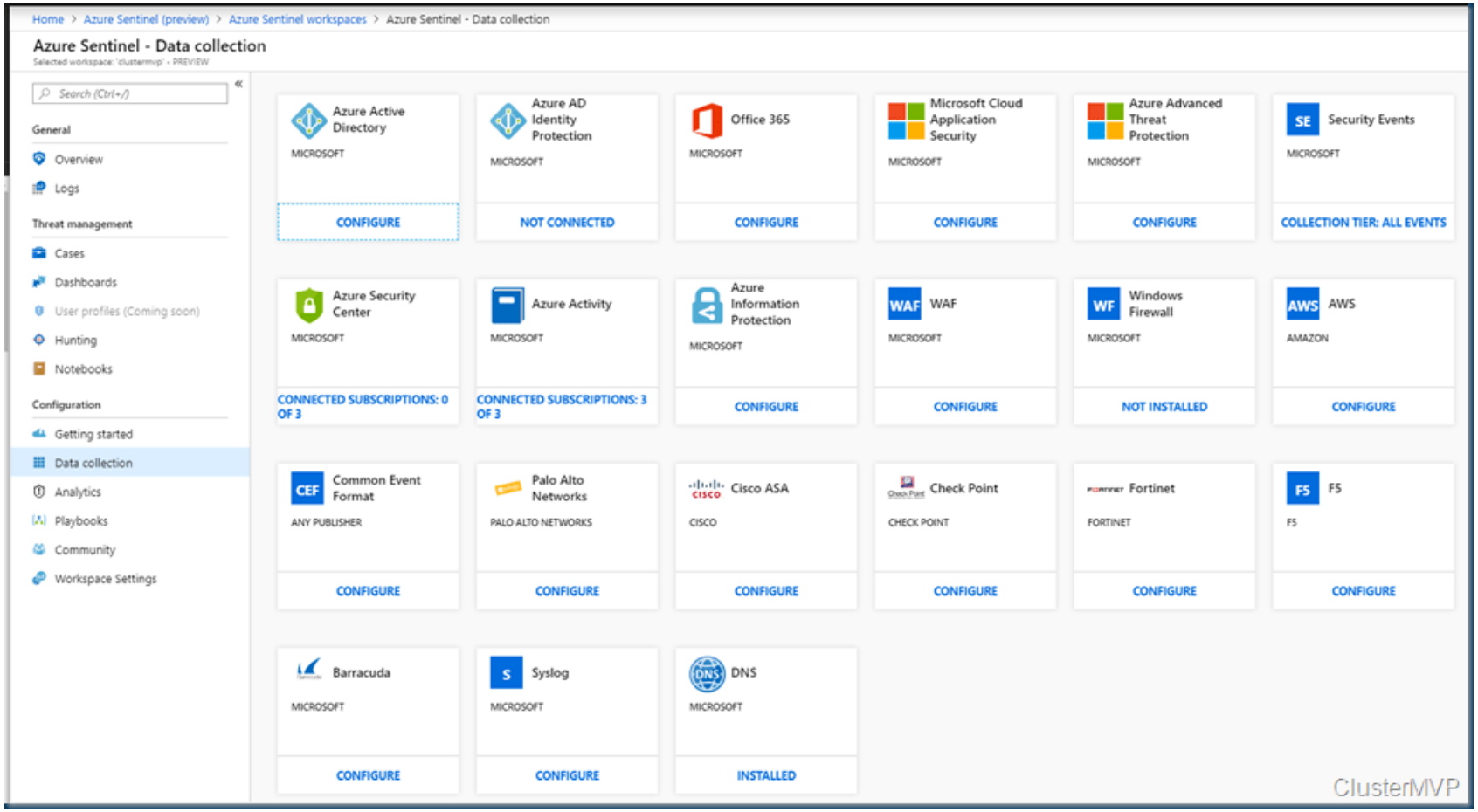


Other Data Connectors

In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions.

- Firewalls, proxies, and endpoints:
- F5
- Check Point
- Cisco ASA
- Fortinet
- Palo Alto
- Other CEF appliances
- Other Syslog appliances
- DLP solutions
- Threat intelligence providers
- DNS machines - agent installed directly on the DNS machine
- Linux servers
- Other clouds

Out the box Data connectors



Azure Sentinel can be connected to all other data sources that can perform real-time log streaming using the Syslog protocol, via an agent.

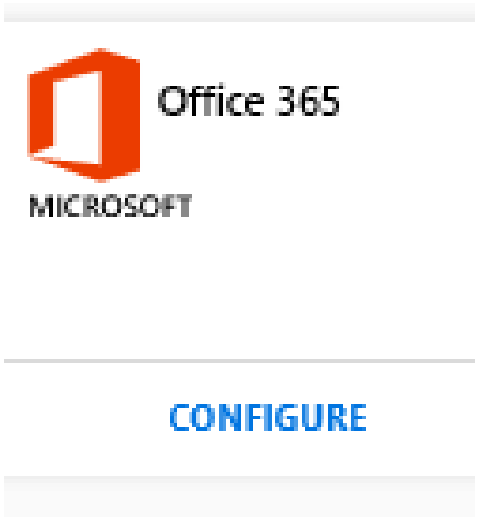
External solutions via agents

Agent connection options

The agent must be deployed on a dedicated machine (VM or on premises) to support the communication between the appliance and Azure Sentinel.

You can deploy the agent automatically or manually.

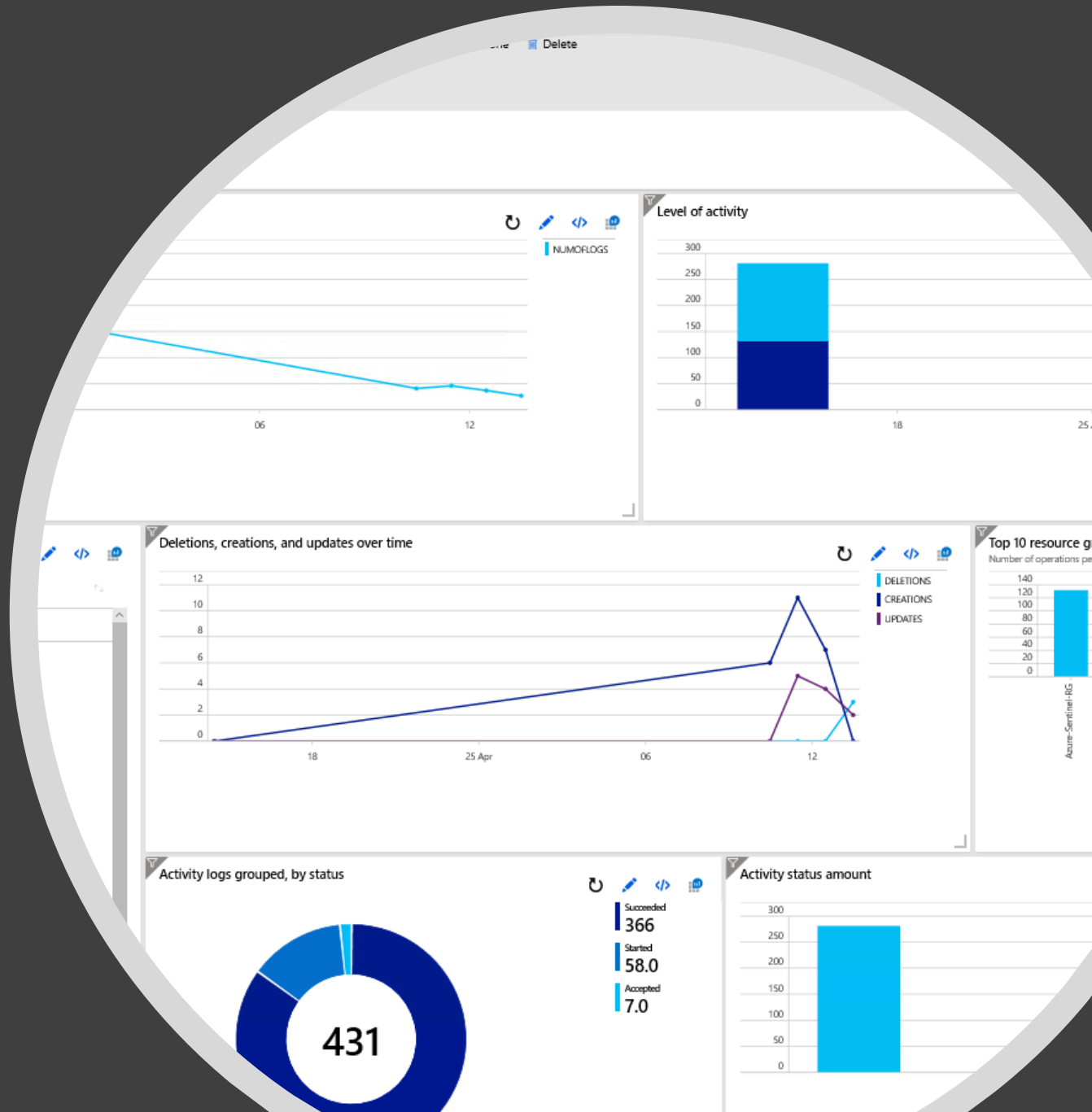
Automatic deployment is only available if your dedicated machine is a new VM you are creating in Azure.



Connect Office 365

- You can stream audit logs from Office 365 into Azure Sentinel with a single click.
- You can stream audit logs from multiple tenants to a single workspace in Azure Sentinel.
- The Office 365 activity log connector provides insight into ongoing user activities.
- You will get information about various user, admin, system, and policy actions and events from Office 365.
- By connecting Office 365 logs into Azure Sentinel you can use this data to view dashboards, create custom alerts, and improve your investigation process.

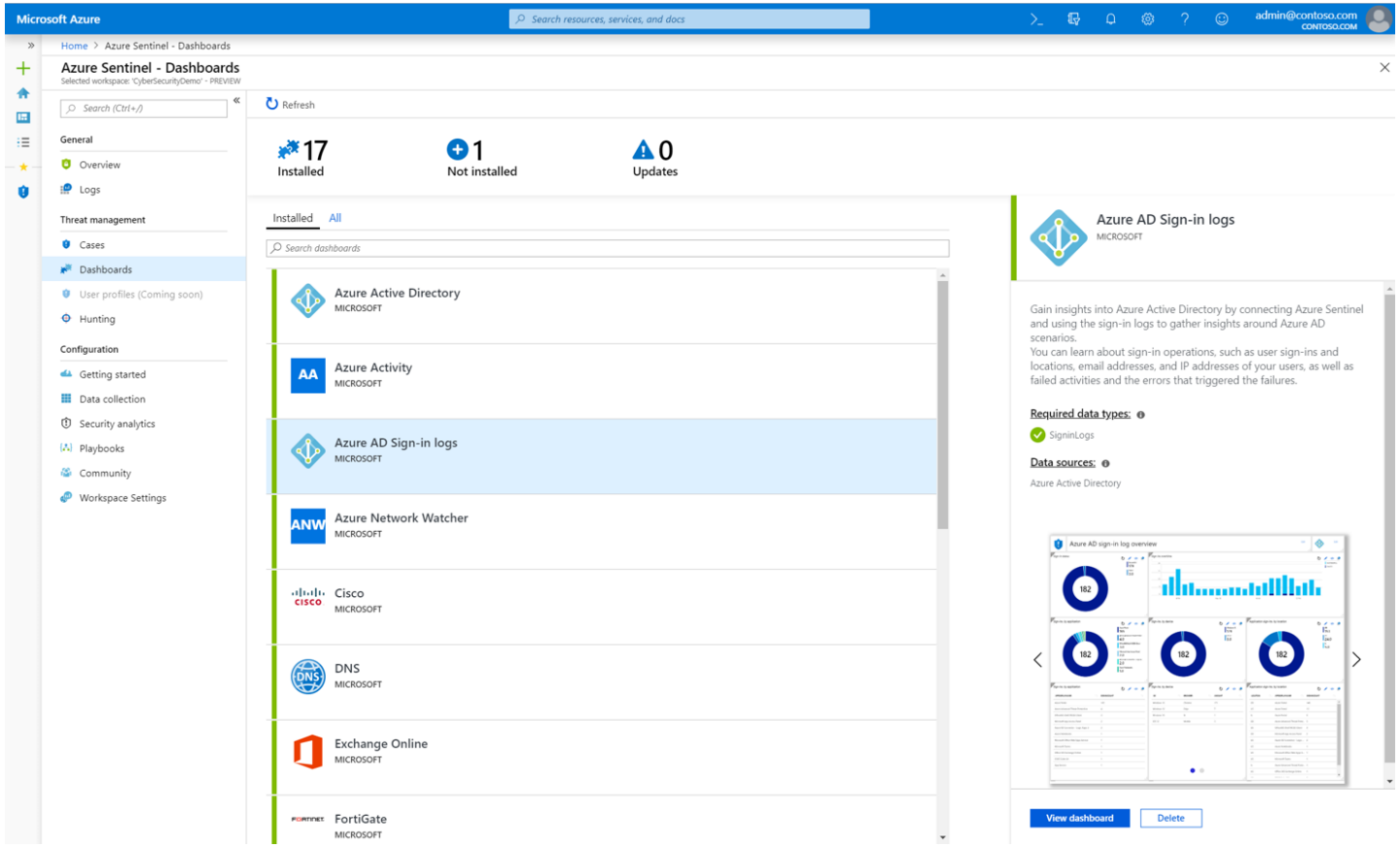
Dashboards


Delete
NUMOFLOGS
Level of activity
300
250
200
150
100
50
0
06
12
18
Deletions, creations, and updates over time
DELETIONS
CREATIONS
UPDATES
12
10
8
6
4
2
0
18
25 Apr
06
12
Top 10 resource g
Number of operations pe
140
120
100
80
60
40
20
0
Azure-Sentinel-RG
Activity logs grouped, by status
Succeeded
366
Started
58.0
Accepted
7.0
431
Activity status amount
300
250
200
150
100
50
0

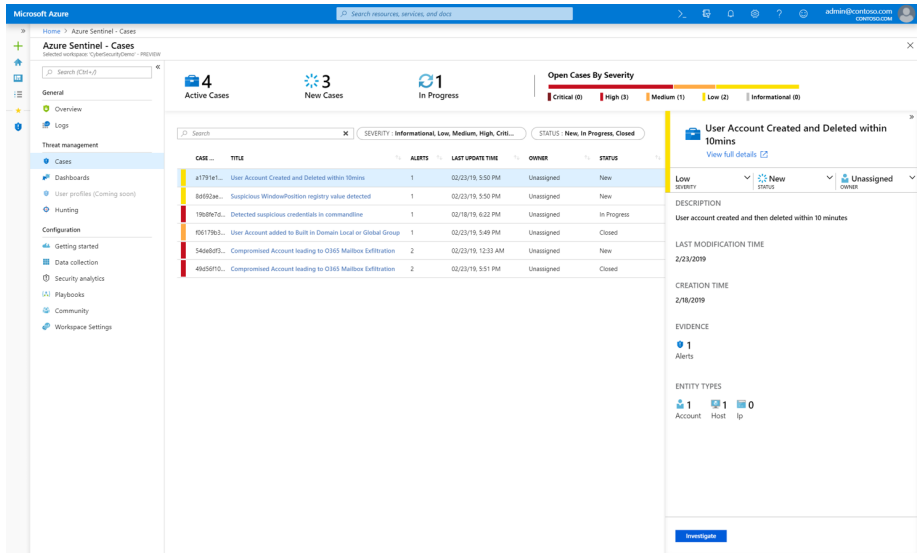
Dashboards

- After connecting data sources you can choose from a gallery of expertly created dashboards that surface insights from your data sources.

- Each dashboard is fully customizable - you can add your own logic or modify queries, or you can create a dashboard from scratch.



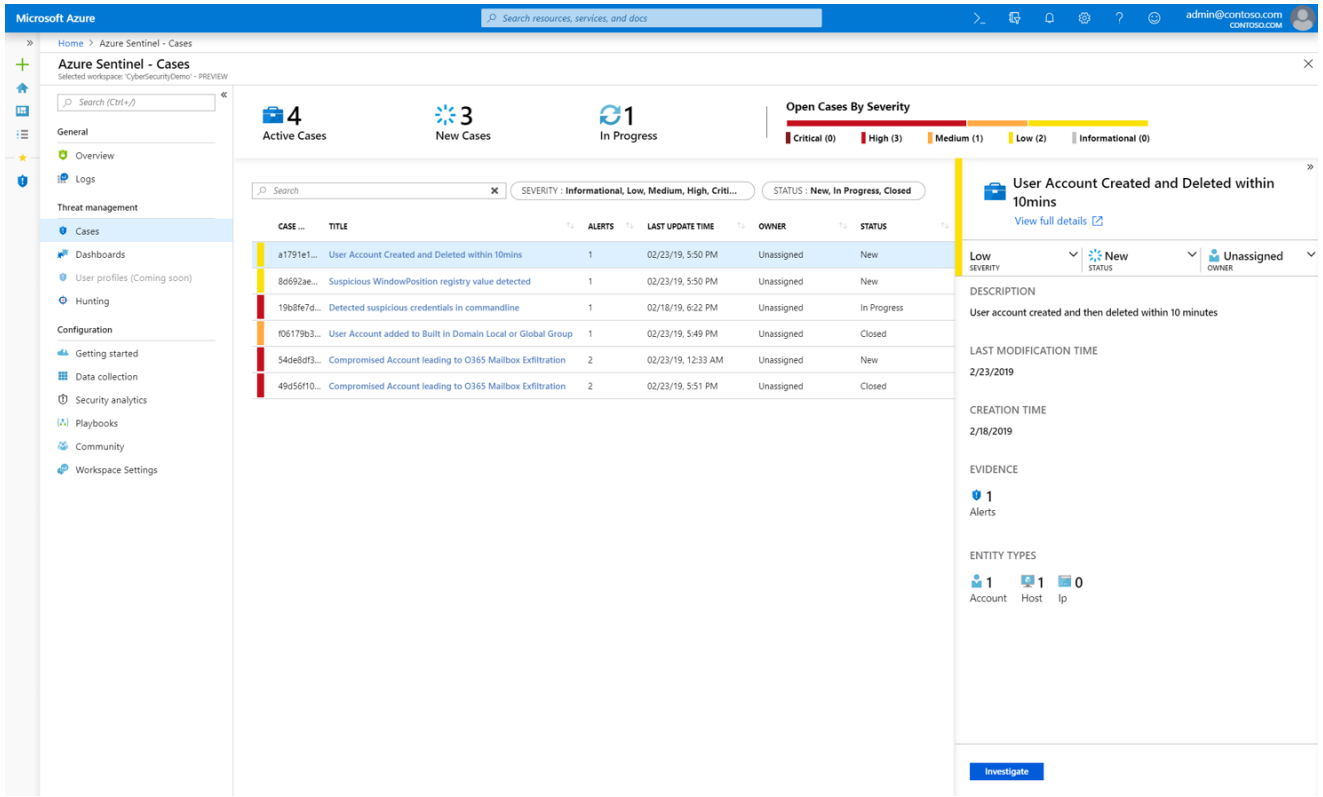
Analytics


Microsoft Azure
Azure Sentinel - Cases
4
Active Cases
3
New Cases
1
In Progress
Open Cases By Severity
Critical (0)
High (3)
Medium (1)
Low (2)
Informational (0)
User Account Created and Deleted within 10mins
View full details
DESCRIPTION
User account created and then deleted within 10 minutes
LAST MODIFICATION TIME
2/23/2019
CREATION TIME
2/18/2019
EVIDENCE
1
Alerts
ENTITY TYPES
Account
Host
Ip
Investigate

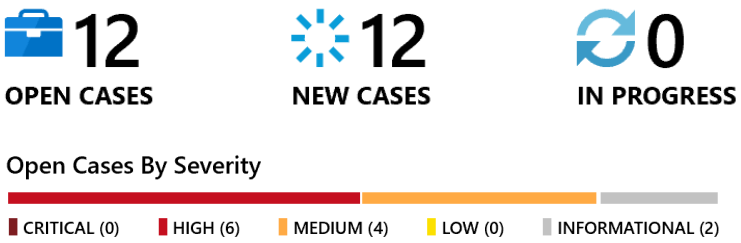
Reduce noise with Analytics

- To help you reduce noise and minimize the number of alerts you have to review and investigate, Azure Sentinel uses analytics to correlate alerts into cases.

- Cases are groups of related alerts that together create an actionable possible-threat that you can investigate and resolve.



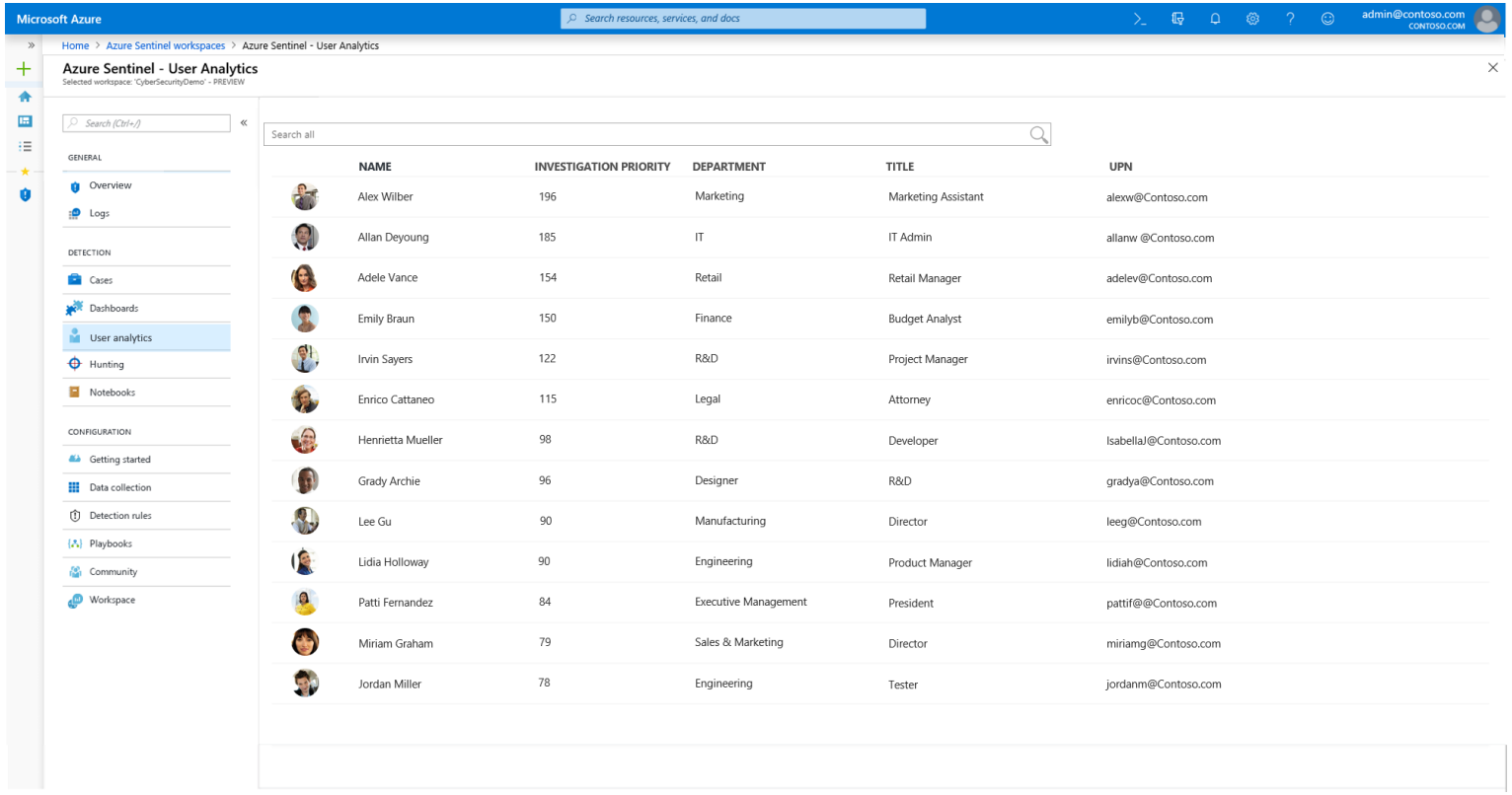
Cases



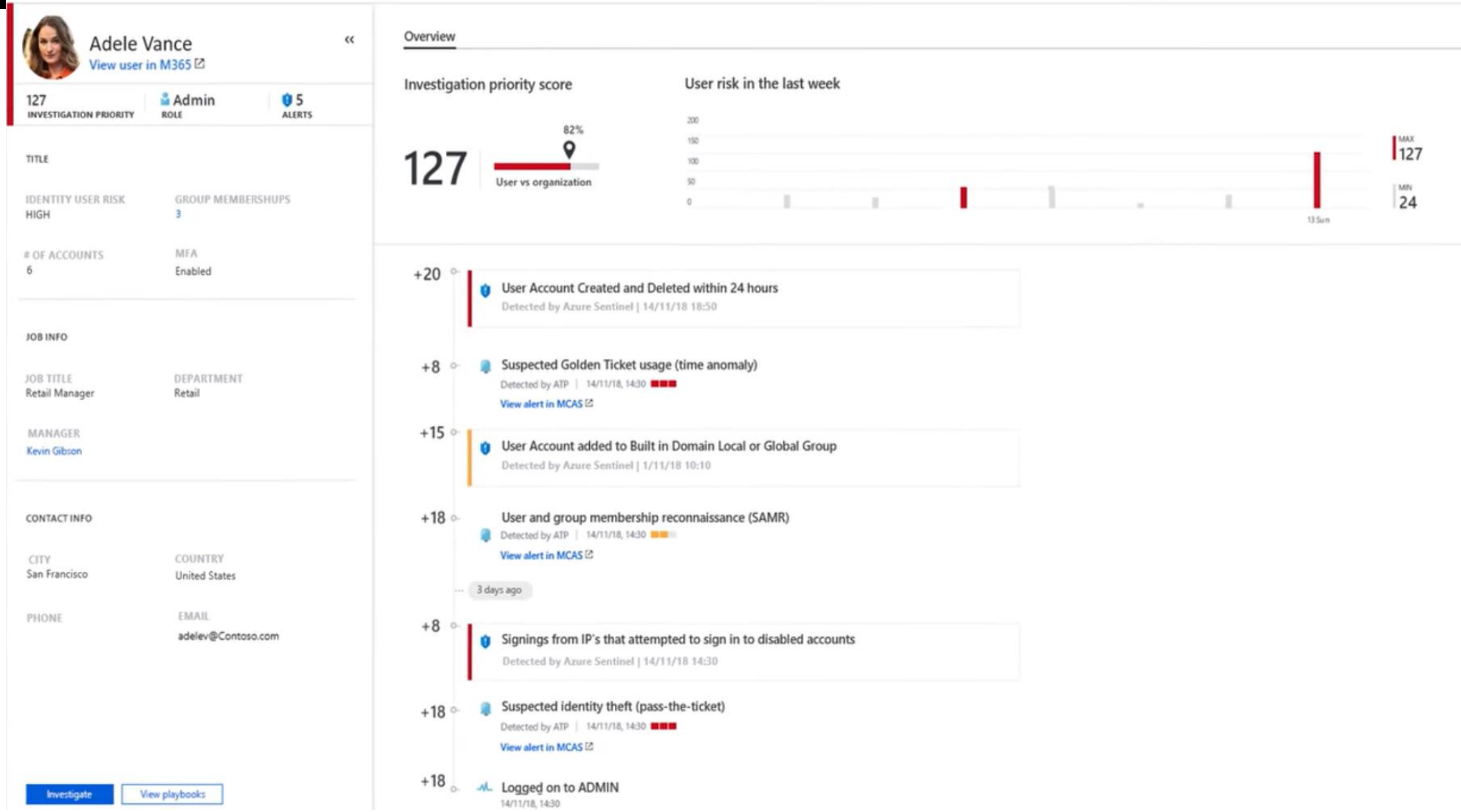
- **Cases** are groups of related alerts that together create an actionable possible-threat that you can investigate and resolve.
- Use the built-in correlation rules as-is, or use them as a starting point to build your own.
- Azure Sentinel also provides machine learning rules to map your network behaviour and then look for anomalies across your resources.
- These analytics connect the dots, by combining low fidelity alerts about different entities into potential high-fidelity security incidents.

User Analytics

- Azure Sentinel can help detect threats quickly with native integration of machine learning (ML), and user analytics,
- Azure Sentinel seamlessly integrates with Azure Advanced Threat Protection to analyze user behavior and prioritize which users you should investigate first, based on their alerts, and suspicious activity patterns across Azure Sentinel and Microsoft 365.



User Details

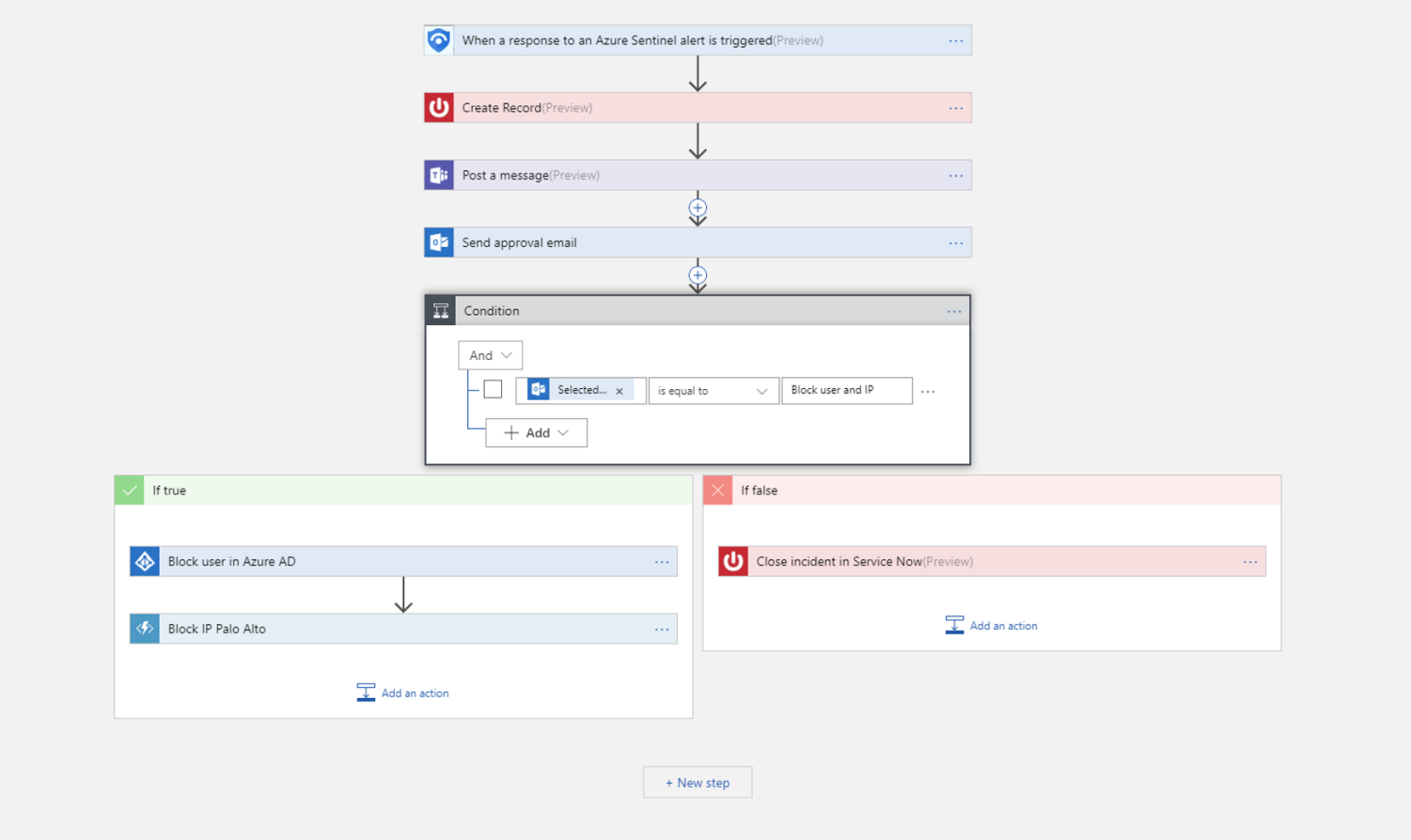


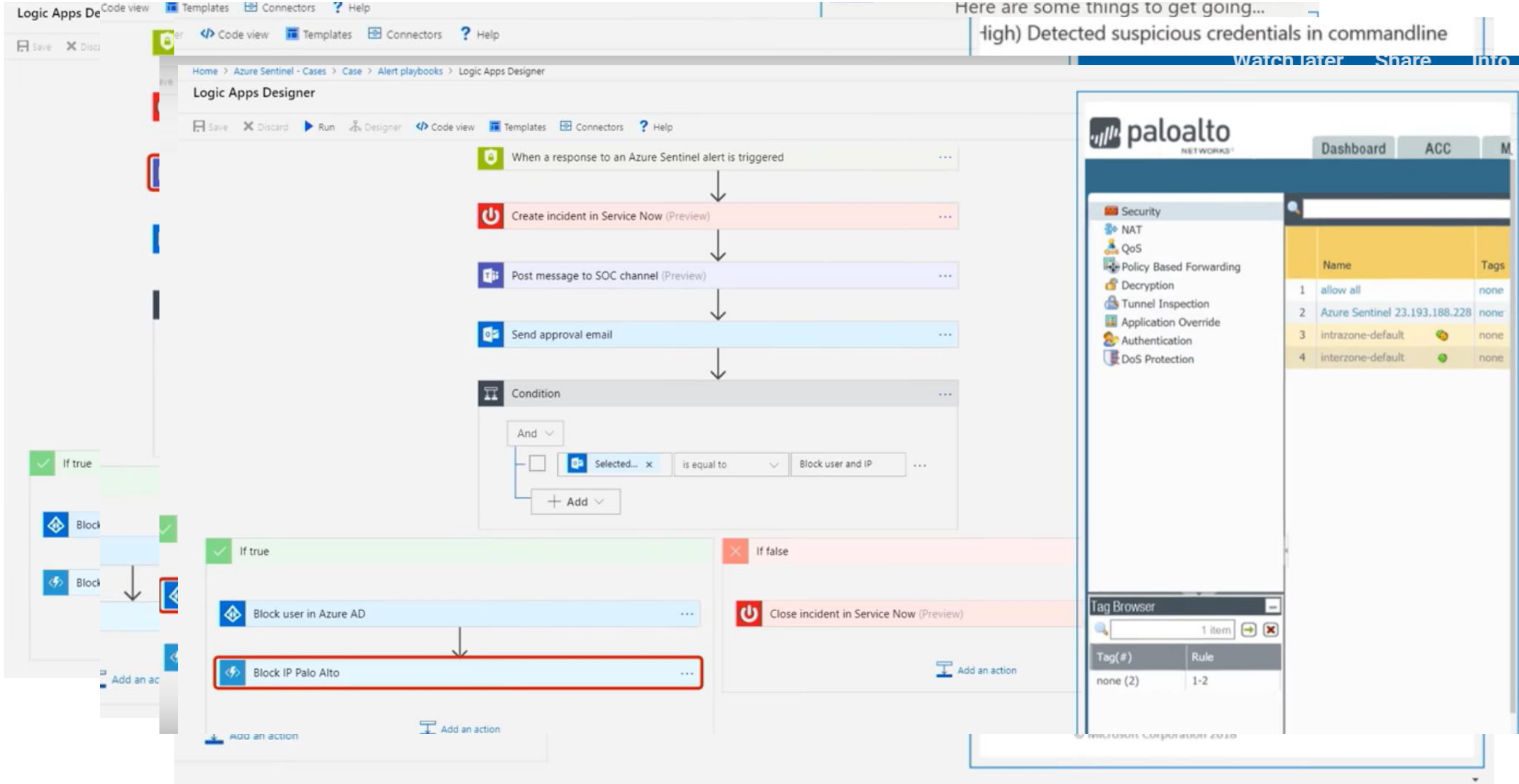
Security automation & orchestration

- Automate your response, common tasks and simplify security orchestration with playbooks that integrate with Azure services as well as your existing tools.
- To build playbooks with Azure Logic Apps, you can choose from a growing gallery of built-in playbooks.
- These include 200+ connectors for services such as Azure functions.
- The connectors allow you to apply any custom logic in code, ServiceNow, Jira, Zendesk, HTTP requests, Microsoft Teams, Slack, Windows Defender ATP, and Cloud App Security.

Respond rapidly with Playbooks

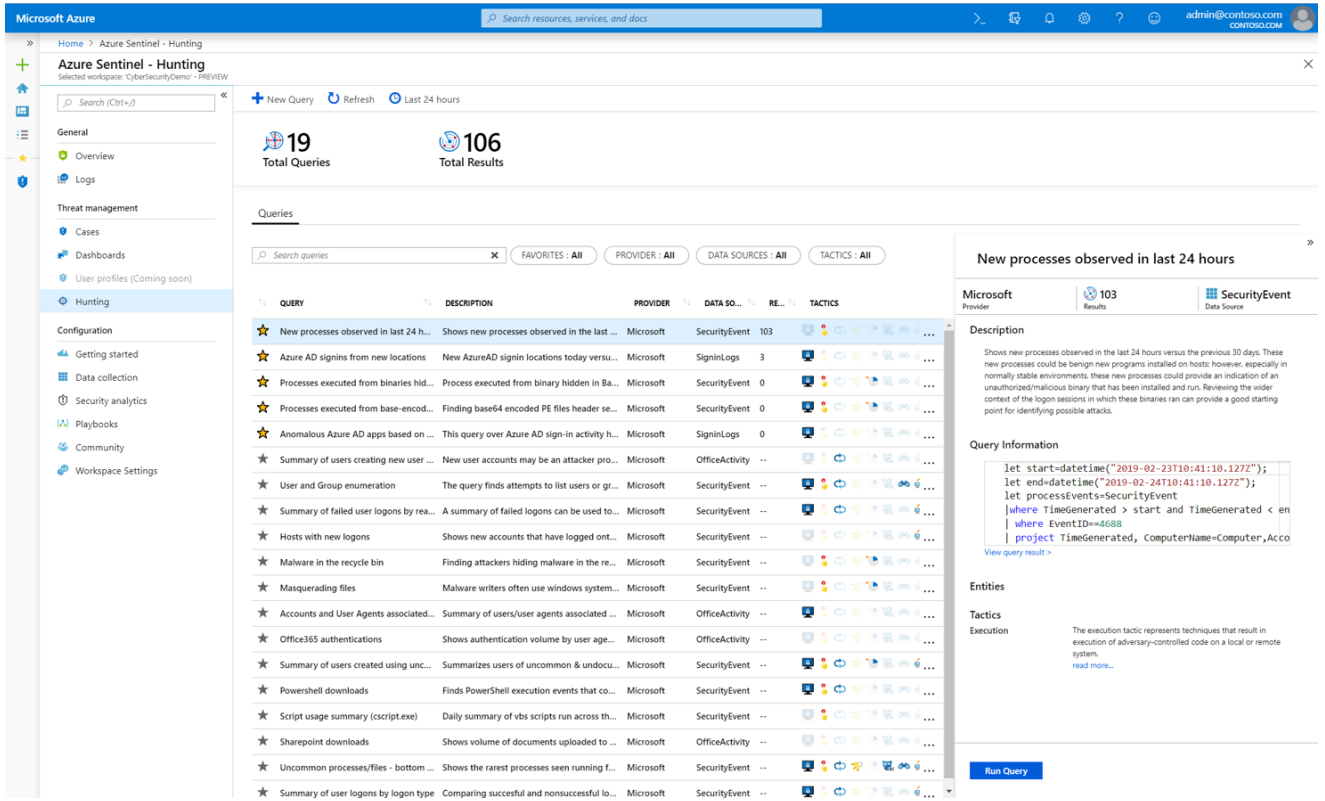
- Example, if you use the ServiceNow ticketing system, you can use the tools provided to use Azure Logic Apps to automate your workflows and open a ticket in ServiceNow each time a particular event is detected.

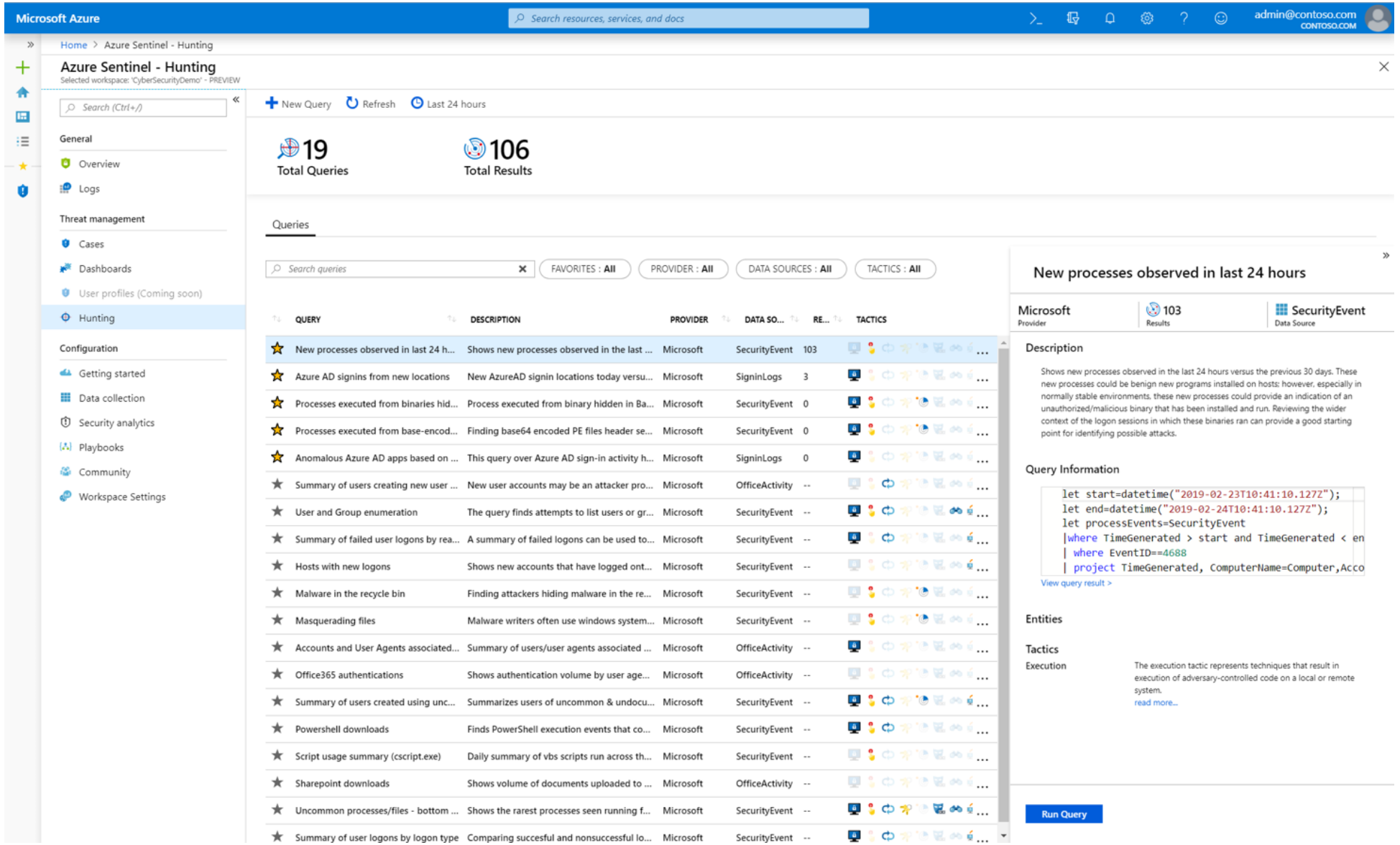



Logic Apps Designer
Home > Azure Sentinel - Cases > Case > Alert playbooks > Logic Apps Designer
Save
Discard
Run
Designer
Code view
Templates
Connectors
Help
When a response to an Azure Sentinel alert is triggered
Create incident in Service Now (Preview)
Post message to SOC channel (Preview)
Send approval email
Condition
And
Selected...
is equal to
Block user and IP
Add
If true
Block user in Azure AD
Block IP Palo Alto
Add an action
If false
Close incident in Service Now (Preview)
Add an action
Here are some things to get going...
high) Detected suspicious credentials in commandline
Watch later
Share
paloalto
NETWORKS
Dashboard
ACC
Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
Name
Tags
1 allow all none
2 Azure Sentinel 23.193.188.228 none
3 intrazone-default none
4 interzone-default none
Tag Browser
1 item
Tag(#)
Rule
none (2)
1-2

Hunting

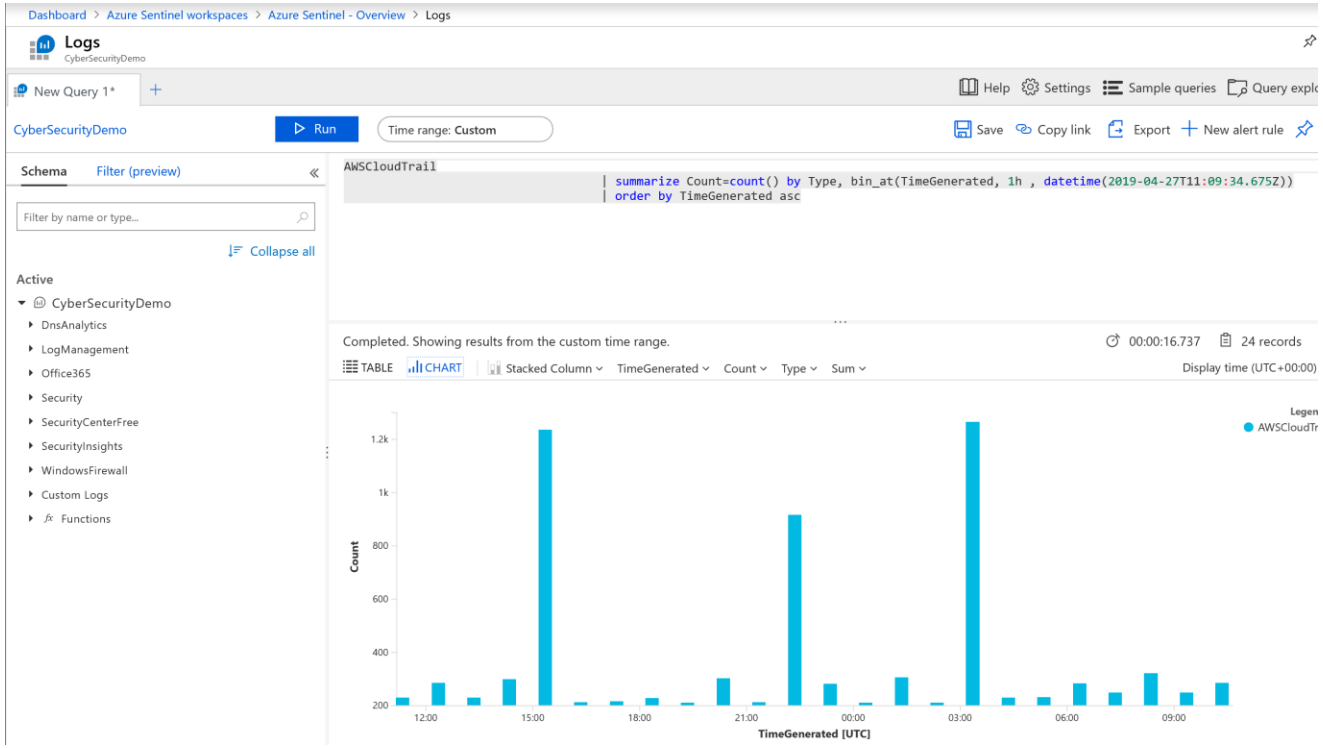
- Proactive hunting of suspicious activities is another critical task for the security analysts.
- Azure Sentinel provides two capabilities that enable you to automate your analysis by building **hunting queries** and **Azure Notebooks** that are based on Jupyter notebooks.




Microsoft Azure
Search resources, services, and docs
admin@contoso.com
CONTOSO.COM
Home > Azure Sentinel - Hunting
Azure Sentinel - Hunting
Selected workspace: 'CyberSecurityDemo' - PREVIEW
Search (Ctrl+/)
General
Overview
Logs
Threat management
Cases
Dashboards
User profiles (Coming soon)
Hunting
Configuration
Getting started
Data collection
Security analytics
Playbooks
Community
Workspace Settings
New Query
Refresh
Last 24 hours
19
Total Queries
106
Total Results
Queries
Search queries
FAVORITES : All
PROVIDER : All
DATA SOURCES : All
TACTICS : All
QUERY
DESCRIPTION
PROVIDER
DATA SO...
RE...
TACTICS
New processes observed in last 24 h... Shows new processes observed in the last ... Microsoft SecurityEvent 103
Azure AD signins from new locations New AzureAD signin locations today versu... Microsoft SigninLogs 3
Processes executed from binaries hid... Process executed from binary hidden in Ba... Microsoft SecurityEvent 0
Processes executed from base-encod... Finding base64 encoded PE files header se... Microsoft SecurityEvent 0
Anomalous Azure AD apps based on ... This query over Azure AD sign-in activity h... Microsoft SigninLogs 0
Summary of users creating new user ... New user accounts may be an attacker pro... Microsoft OfficeActivity --
User and Group enumeration The query finds attempts to list users or gr... Microsoft SecurityEvent --
Summary of failed user logons by rea... A summary of failed logons can be used to... Microsoft SecurityEvent --
Hosts with new logons Shows new accounts that have logged ont... Microsoft SecurityEvent --
Malware in the recycle bin Finding attackers hiding malware in the re... Microsoft SecurityEvent --
Masquerading files Malware writers often use windows system... Microsoft SecurityEvent --
Accounts and User Agents associated... Summary of users/user agents associated ... Microsoft OfficeActivity --
Office365 authentications Shows authentication volume by user age... Microsoft OfficeActivity --
Summary of users created using unc... Summarizes users of uncommon & undocu... Microsoft SecurityEvent --
Powershell downloads Finds PowerShell execution events that co... Microsoft SecurityEvent --
Script usage summary (cscript.exe) Daily summary of vbs scripts run across th... Microsoft SecurityEvent --
Sharepoint downloads Shows volume of documents uploaded to ... Microsoft OfficeActivity --
Uncommon processes/files - bottom ... Shows the rarest processes seen running f... Microsoft SecurityEvent --
Summary of user logons by logon type Comparing succesful and nonsuccessful lo... Microsoft SecurityEvent --
New processes observed in last 24 hours
Microsoft
Provider
103
Results
SecurityEvent
Data Source
Description
Shows new processes observed in the last 24 hours versus the previous 30 days. These new processes could be benign new programs installed on hosts; however, especially in normally stable environments, these new processes could provide an indication of an unauthorized/malicious binary that has been installed and run. Reviewing the wider context of the logon sessions in which these binaries ran can provide a good starting point for identifying possible attacks.
Query Information
let start=datetime("2019-02-23T10:41:10.127Z");
let end=datetime("2019-02-24T10:41:10.127Z");
let processEvents=SecurityEvent
|where TimeGenerated > start and TimeGenerated < en
| where EventID==4688
| project TimeGenerated, ComputerName=Computer,Acco
View query result >
Entities
Tactics
Execution
The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system.
read more...
Run Query

Logs

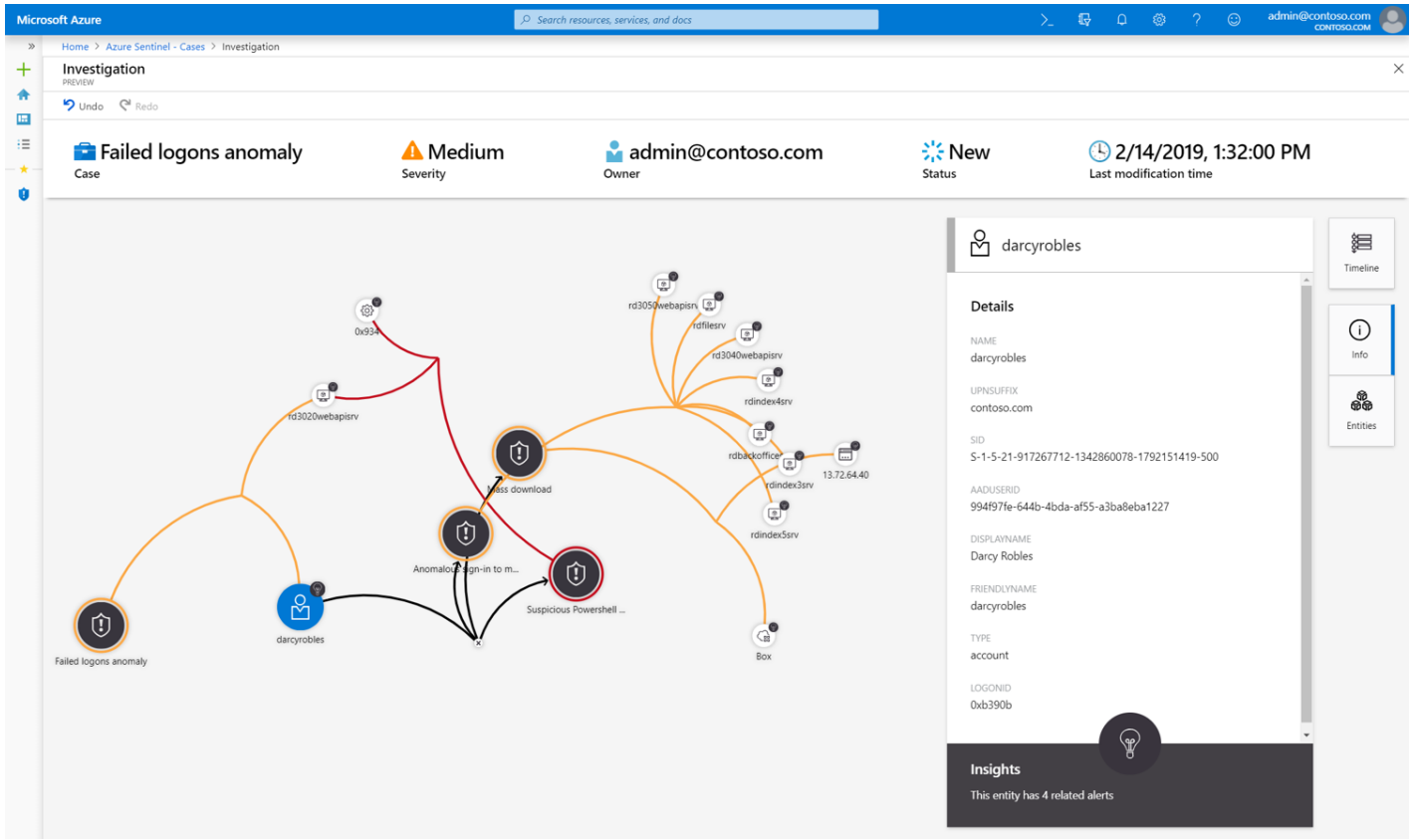
- Azure Monitor log queries
- Uses Kusto Query Language
- Create Alerts
- View as tables and charts
- Sample Queries



Investigation

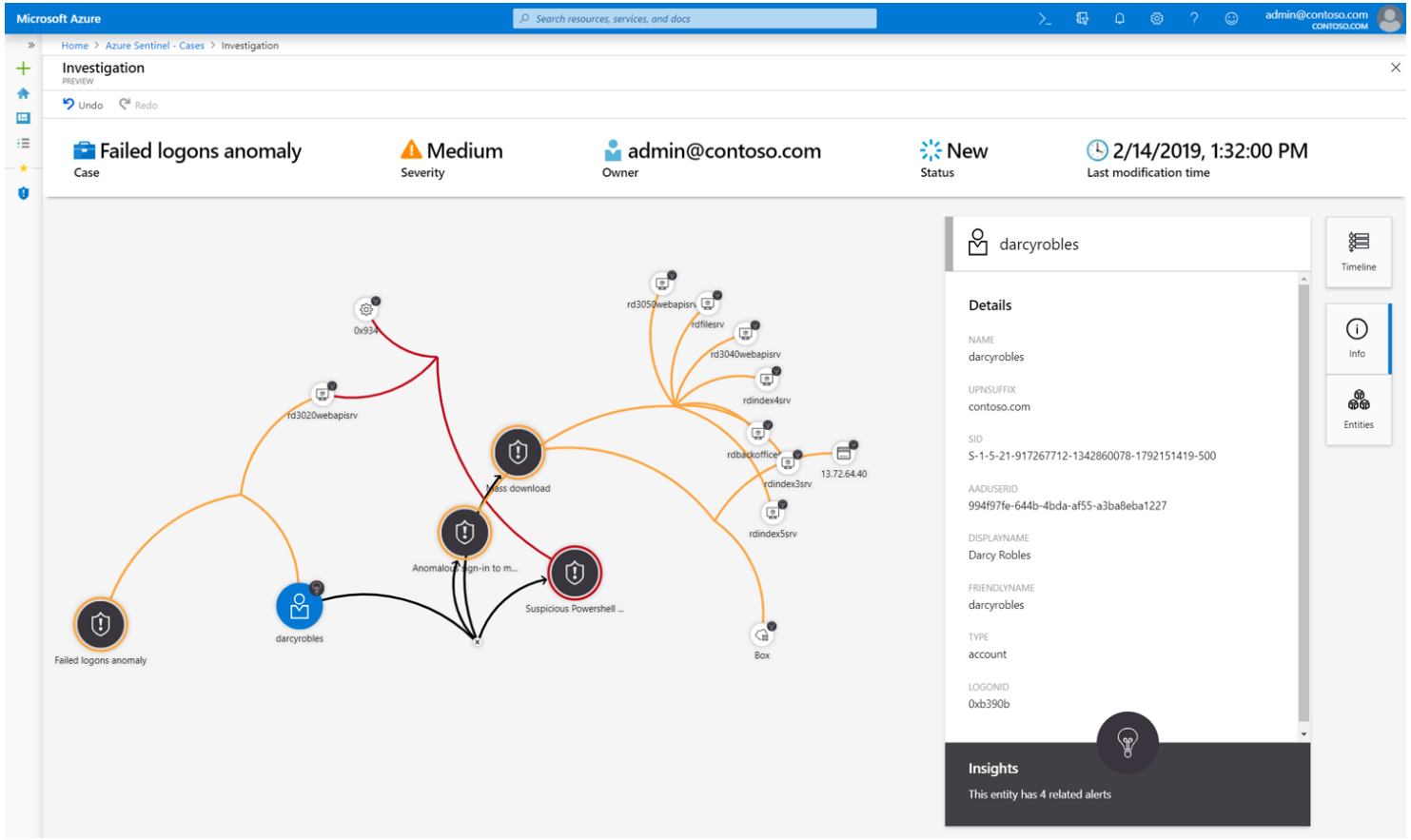
- Azure Sentinel deep investigation tools help you to understand the scope and find the root cause, of a potential security threat.

- You can choose an entity on the interactive graph to ask interesting questions for a specific entity, and drill down into that entity and its connections to get to the root cause of the threat.



Interactive graph

- Get prioritized alerts and automated expert guidance
- Visualize the entire attack and its impact
- Hunt for suspicious activities using pre-built queries and Azure Notebooks



Azure Notebooks

- Azure Notebooks is a free hosted service to develop and run Jupyter notebooks in the cloud with no installation.
- Jupyter is an open source project that lets you easily combine markdown text, executable code (Python, R, and F#), persistent data, graphics, and visualizations onto a single, sharable canvas called a notebook.
- Interactive Azure Notebooks provides security insights and actions to investigate anomalies and hunt for malicious behaviors.

Azure Sentinel Notebooks Include:

Alert Investigation and Hunting

Quickly triage different classes of alerts by enriching them with related activity and events from multiple data sources.

Endpoint Host Guided Hunting

Hunt for signs of a compromise by drilling down into the security relevant activities related to specific endpoint hosts.

Office Logon Anomalies Guided Hunting

Investigate suspicious logons in Office365 data by visualizing geographic data and displaying unusual logon patterns.

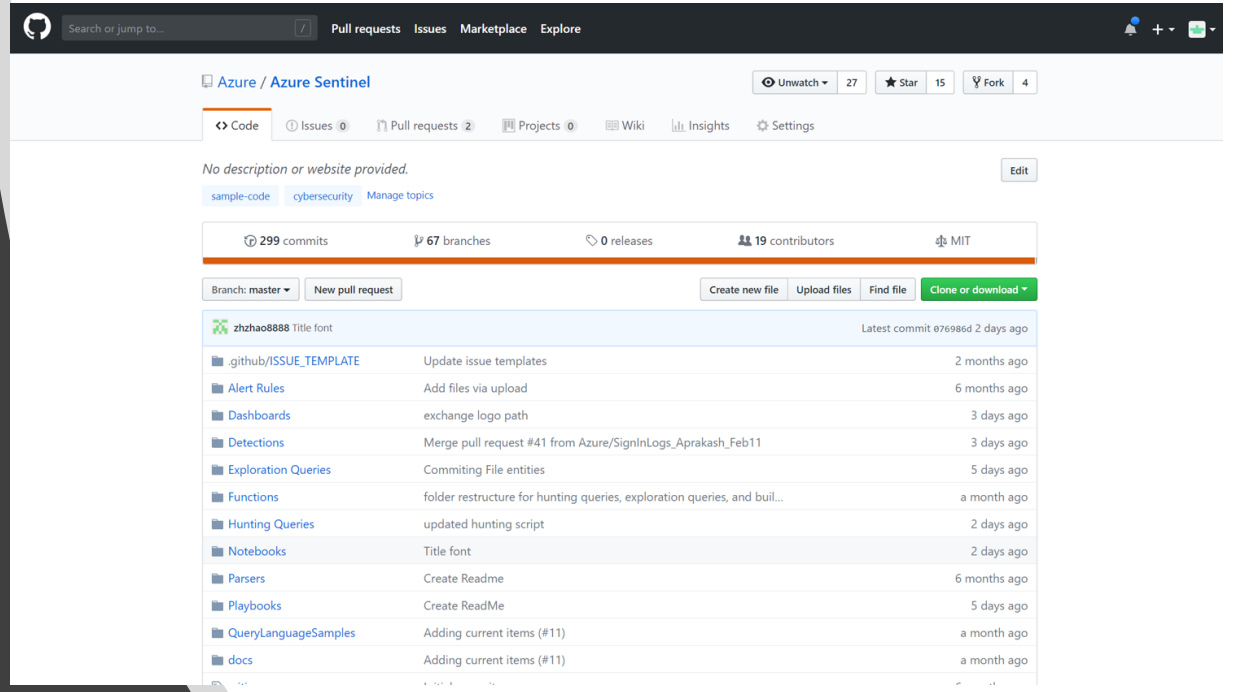
"As the threat landscape evolves, so will our queries and Azure Notebooks. We will provide new queries and Azure Notebooks via the Azure Sentinel GitHub community"

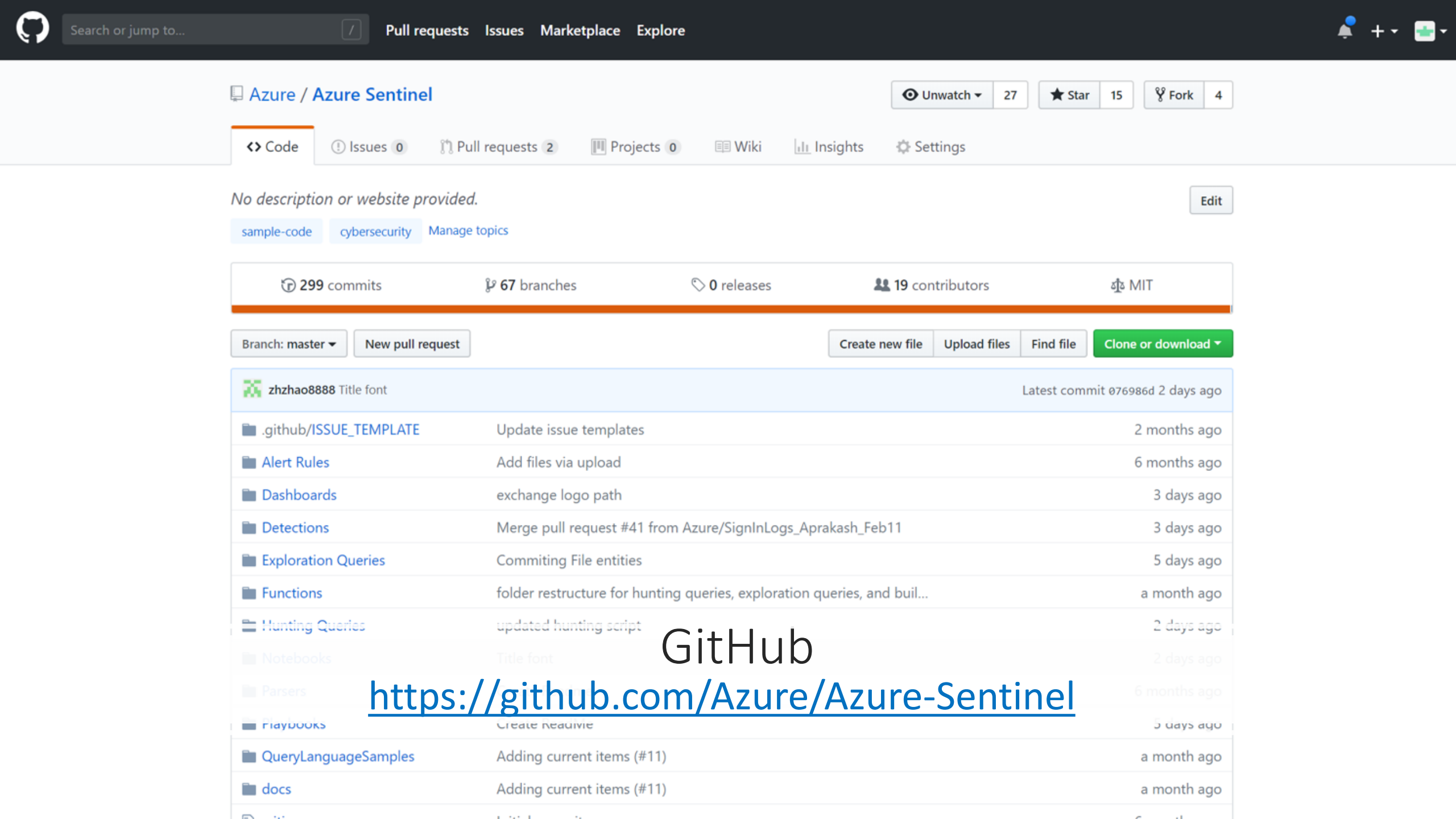
Share and consume content with the Community

THE AZURE SENTINEL COMMUNITY IS A POWERFUL RESOURCE FOR THREAT DETECTION AND AUTOMATION.

OUR MICROSOFT SECURITY ANALYSTS CONSTANTLY CREATE AND ADD NEW DASHBOARDS, PLAYBOOKS, HUNTING QUERIES, AND MORE, POSTING THEM TO THE COMMUNITY FOR YOU TO USE IN YOUR ENVIRONMENT.

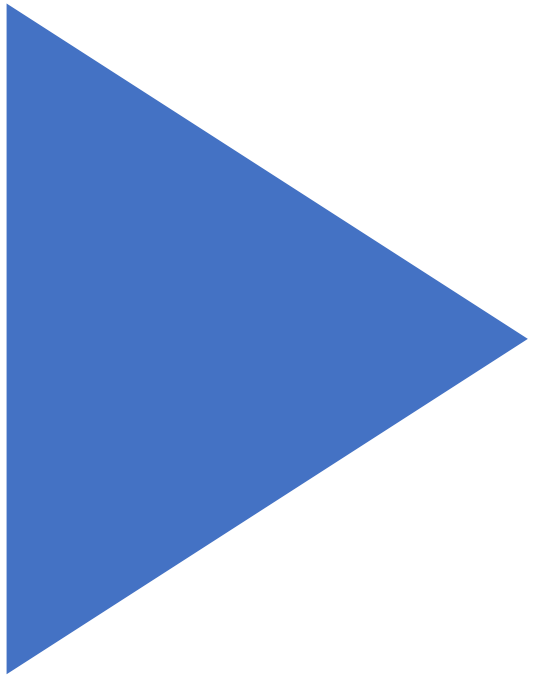
YOU CAN DOWNLOAD SAMPLE CONTENT FROM THE PRIVATE COMMUNITY GITHUB REPOSITORY TO CREATE CUSTOM DASHBOARDS, HUNTING QUERIES, NOTEBOOKS, AND PLAYBOOKS FOR AZURE SENTINEL.





GitHub

https://github.com/Azure/Azure-Sentinel



Demo

2019 Global Azure BOOTCAMP

Get started with the preview today !

https://aka.ms/AzureSentinel

2019
Global Azure
BOOTCAMP

Thank you

Any Questions ?

2019 Global Azure BOOTCAMP