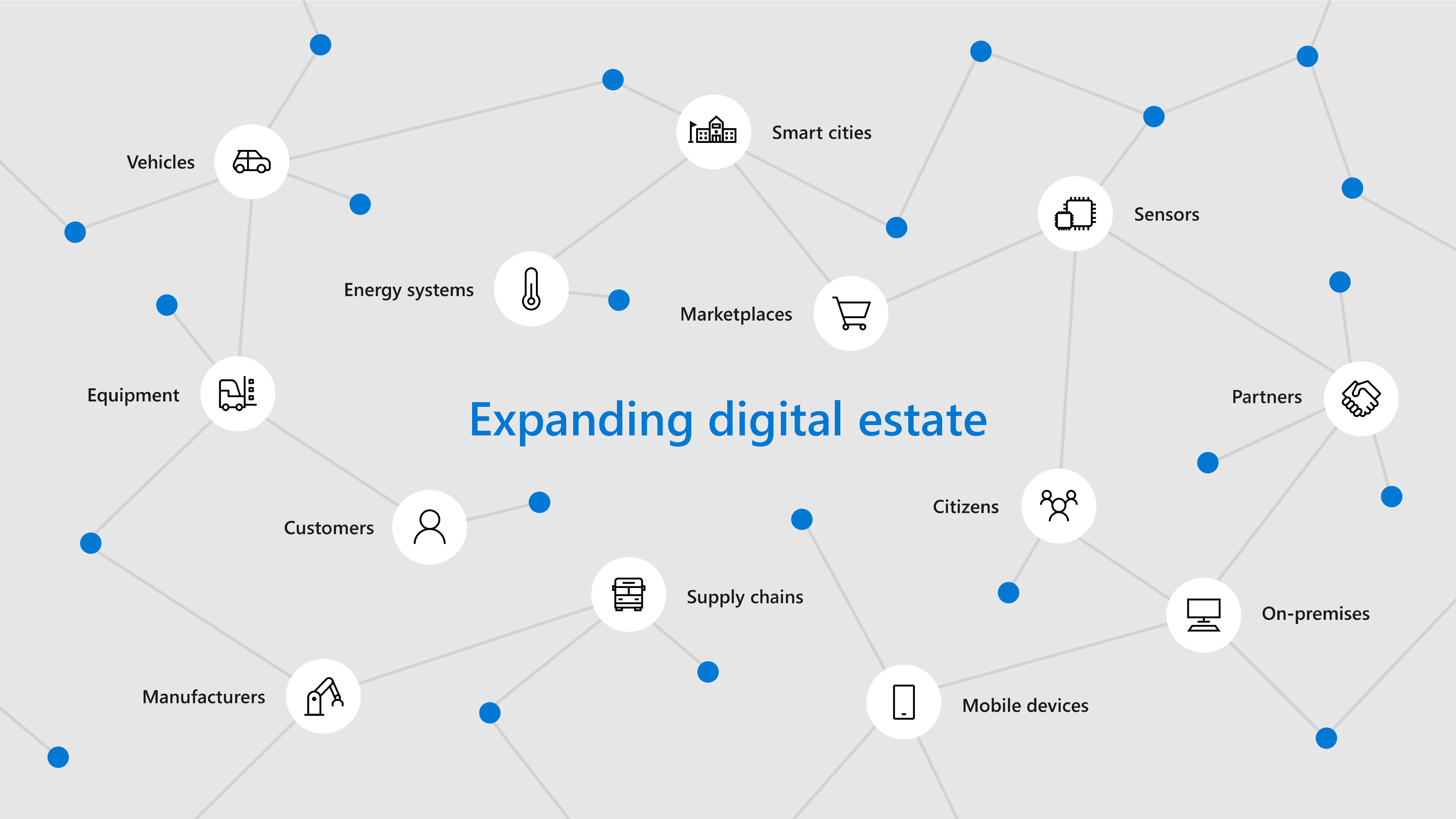
Protect yourself with Azure Sentinel

Ed Baker
@edbaker1965
MVP, MCT Regional Lead

Protect yourself with Azure Sentinel

Assets available at https://github.com/edbakermct/sentinel

Expanding digital estate



Vehicles

Smart cities

Sensors

Energy systems

Marketplaces

Equipment

Partners

Citizens

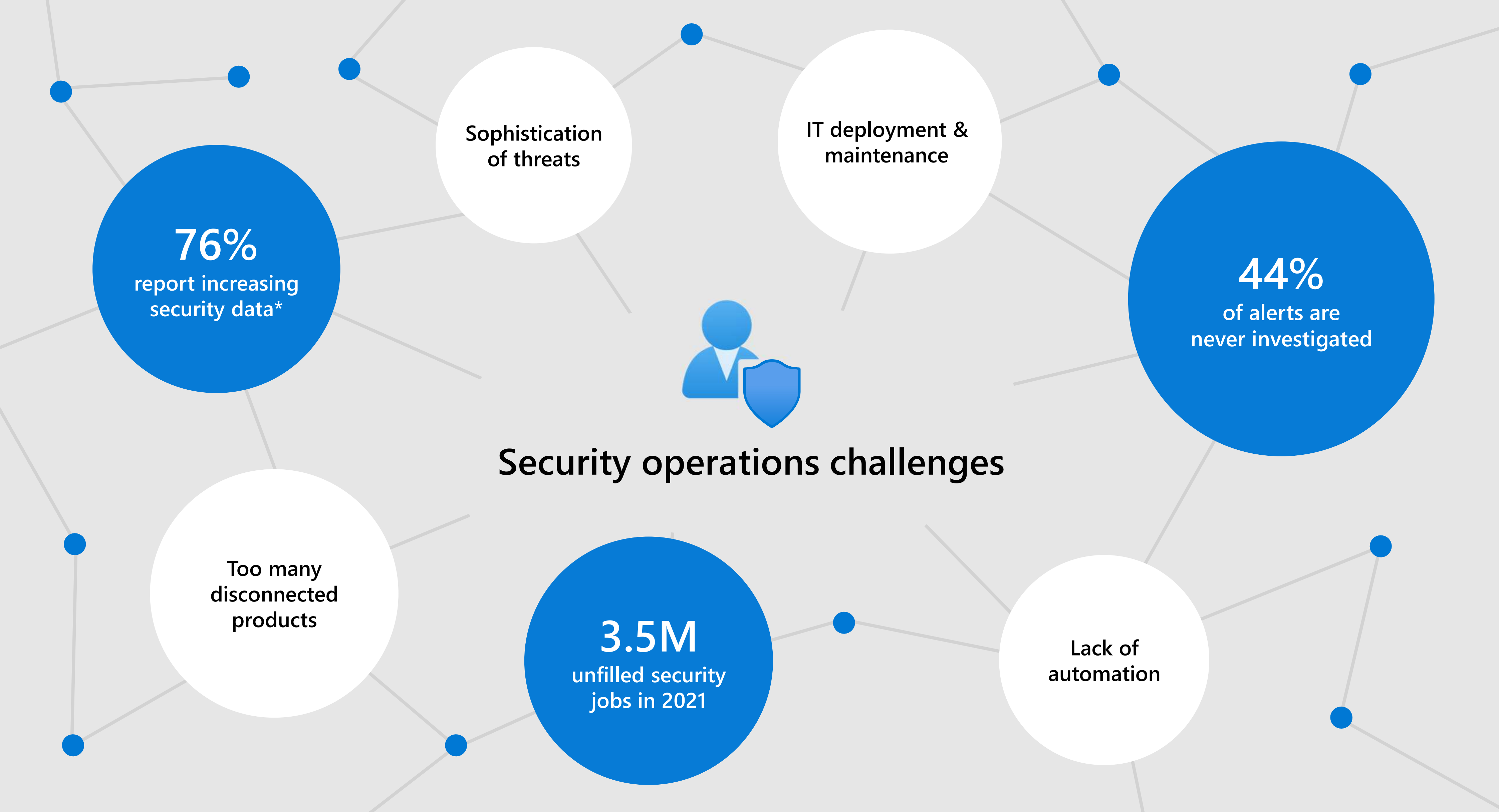
Customers

Supply chains

On-premises

Manufacturers

Mobile devices



Security operations challenges

76%
report increasing security data*

Sophistication of threats

IT deployment & maintenance

44%
of alerts are never investigated

Too many disconnected products

3.5M
unfilled security jobs in 2021

Lack of automation

*ESG: Security Analytics and Operations: Industry Trends in the Era of Cloud Computing 2019

Security Operations Team

+

Cloud + Artificial Intelligence

Introducing Azure Sentinel

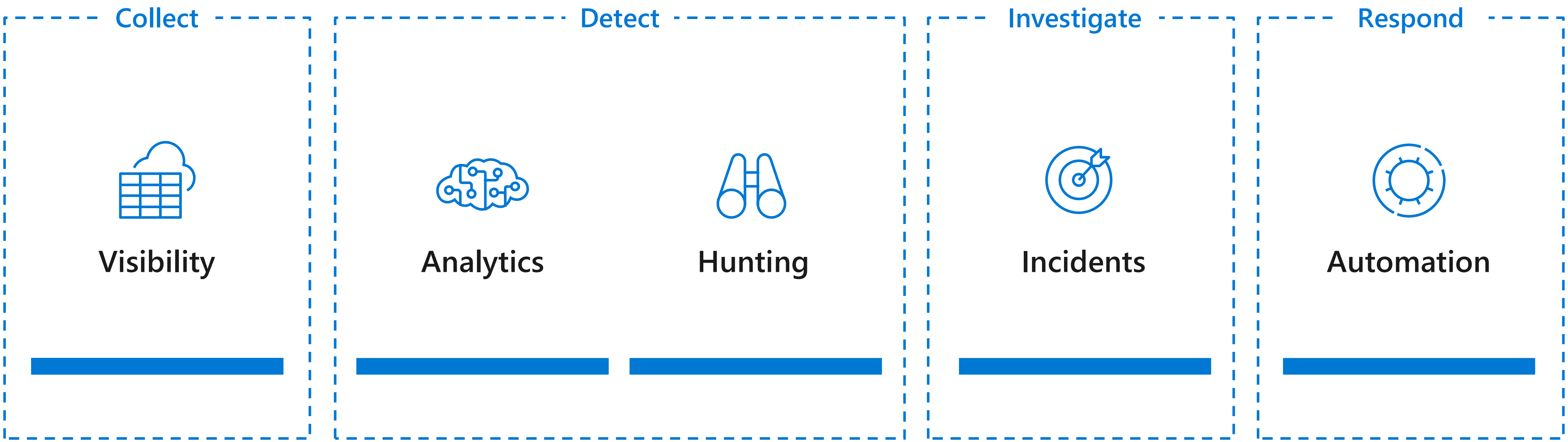
INTELLIGENT, CLOUD-NATIVE SIEM

Delivers instant value to your defenders

Scales to support your growing digital estate

Uses AI and automation to improve effectiveness

End-to-end solution for security operations



Collect

Visibility

Detect

Analytics

Hunting

Investigate

Incidents

Respond

Automation

Powered by community + backed by Microsoft's security experts

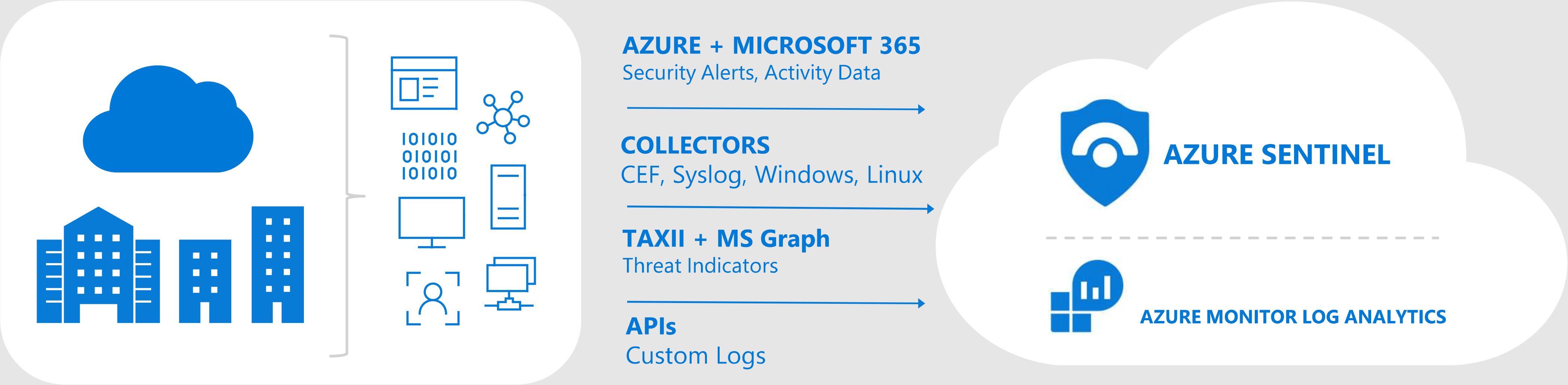
Microsoft Security Advantage

- $1B annual investment in cybersecurity
- 3500+ global security experts
- Trillions of diverse signals for unparalleled intelligence

11 steps to Protect yourself

Collection

1 Collect security data at cloud scale from any source



AZURE + MICROSOFT 365
Security Alerts, Activity Data

COLLECTORS
CEF, Syslog, Windows, Linux

TAXII + MS Graph
Threat Indicators

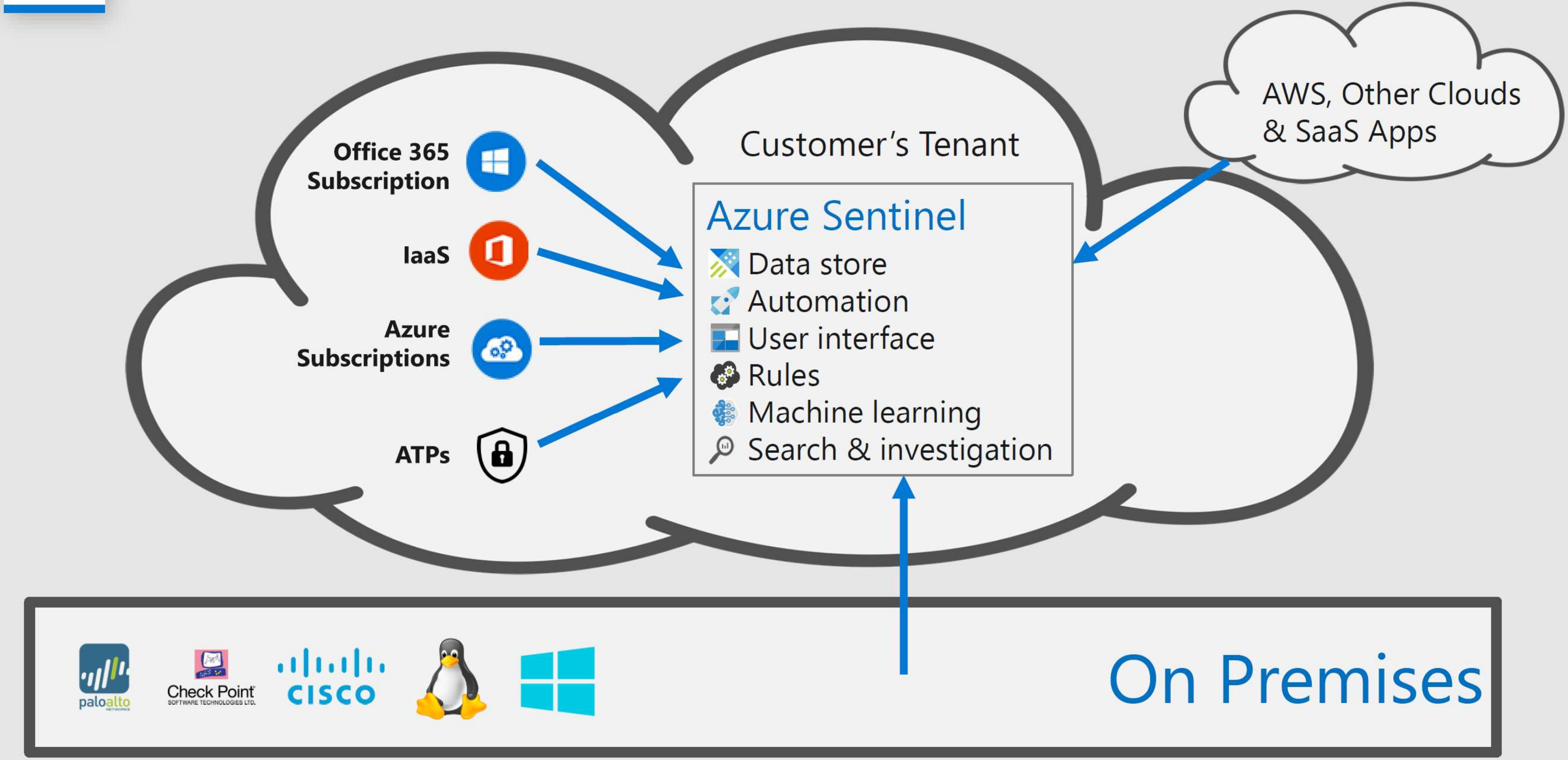
APIs
Custom Logs

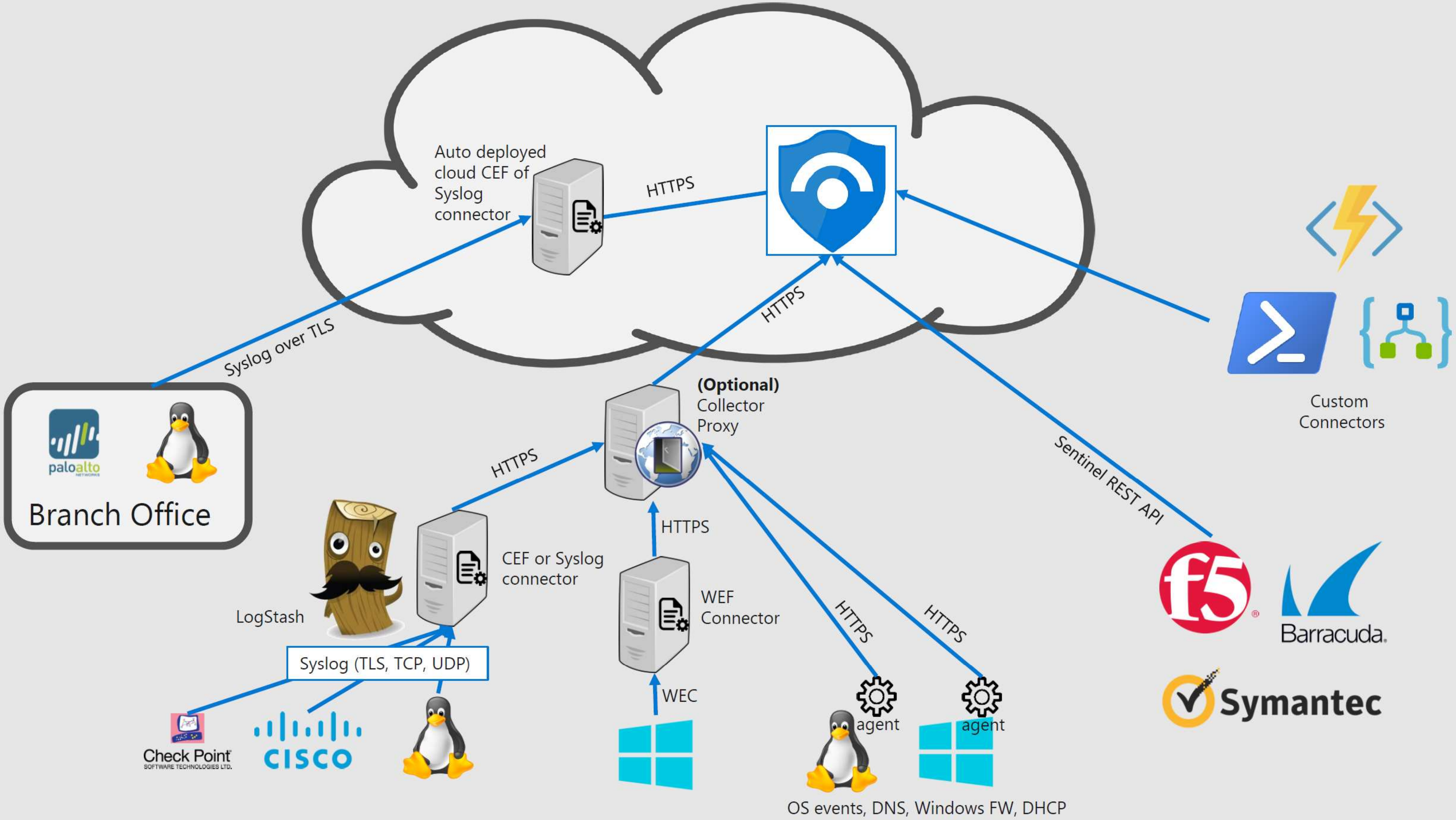
AZURE SENTINEL

AZURE MONITOR LOG ANALYTICS

1

Collect security data at cloud scale from any source





Auto deployed cloud CEF of Syslog connector

HTTPS

HTTPS

Syslog over TLS

Branch Office

(Optional) Collector Proxy

HTTPS

CEF or Syslog connector

LogStash

Syslog (TLS, TCP, UDP)

HTTPS

WEF Connector

WEC

HTTPS

HTTPS

agent

agent

OS events, DNS, Windows FW, DHCP

Sentinel REST API

Custom Connectors

Visualization

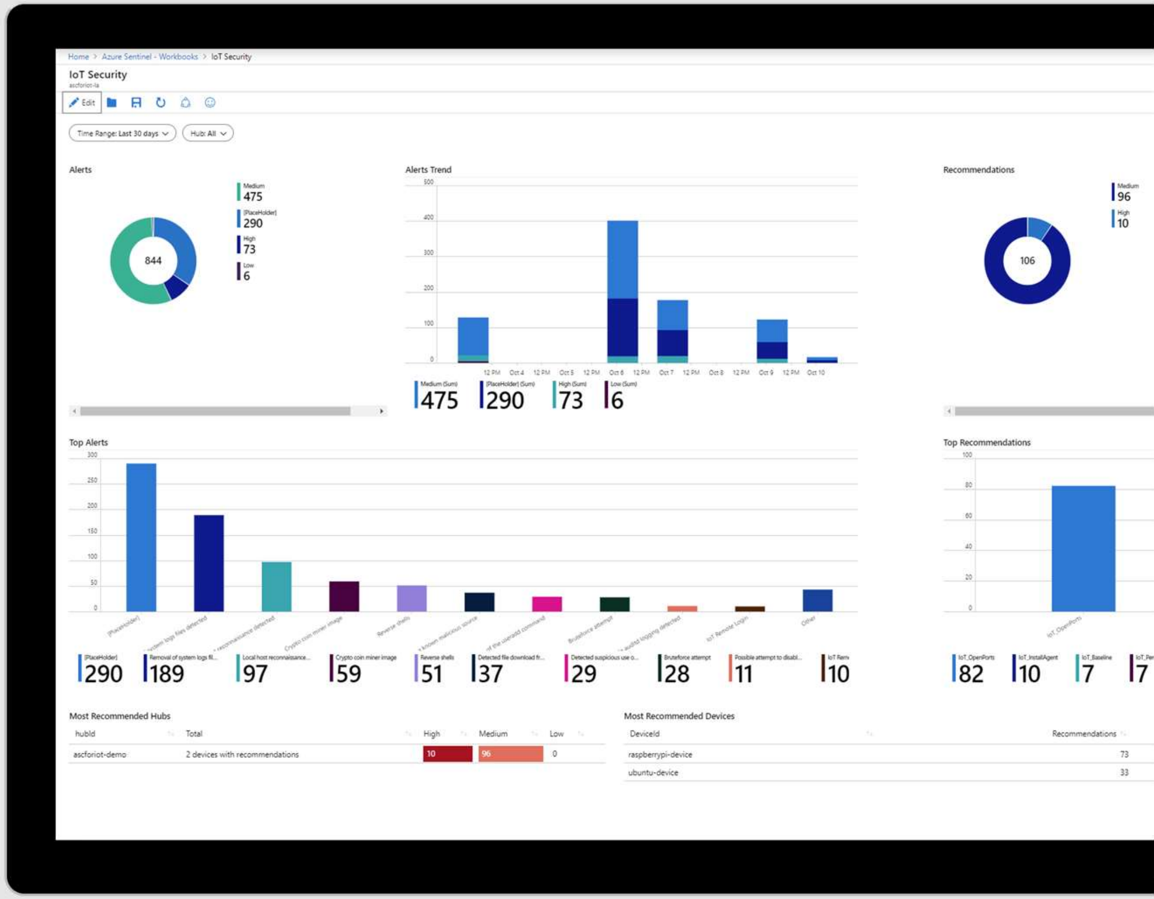
2 Use workbooks to power interactive dashboards

Choose from a gallery of workbooks

Customize or create your own workbooks using queries

Take advantage of rich visualization options

Gain insight into one or more data sources



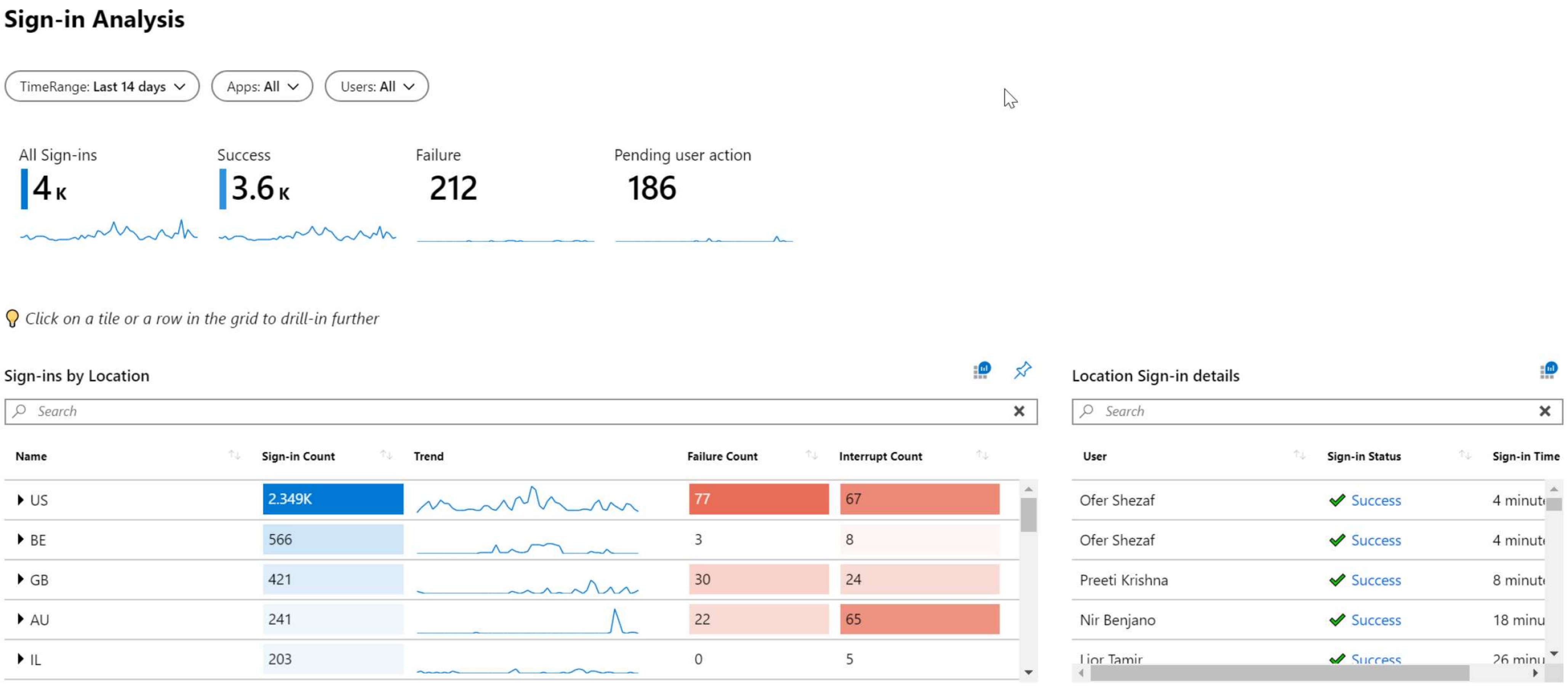
Most Recommended Hubs

hubId	Total	High	Medium	Low
ascforiot-demo	2 devices with recommendations	10	96	0

Most Recommended Devices

DeviceId	Recommendations
raspberrypi-device	73
ubuntu-device	33

Workbooks: interactive dashboarding



Sign-in Analysis

TimeRange: **Last 14 days** | Apps: **All** | Users: **All**

All Sign-ins	Success	Failure	Pending user action
4 K	3.6 K	212	186

Click on a tile or a row in the grid to drill-in further

Sign-ins by Location

Search

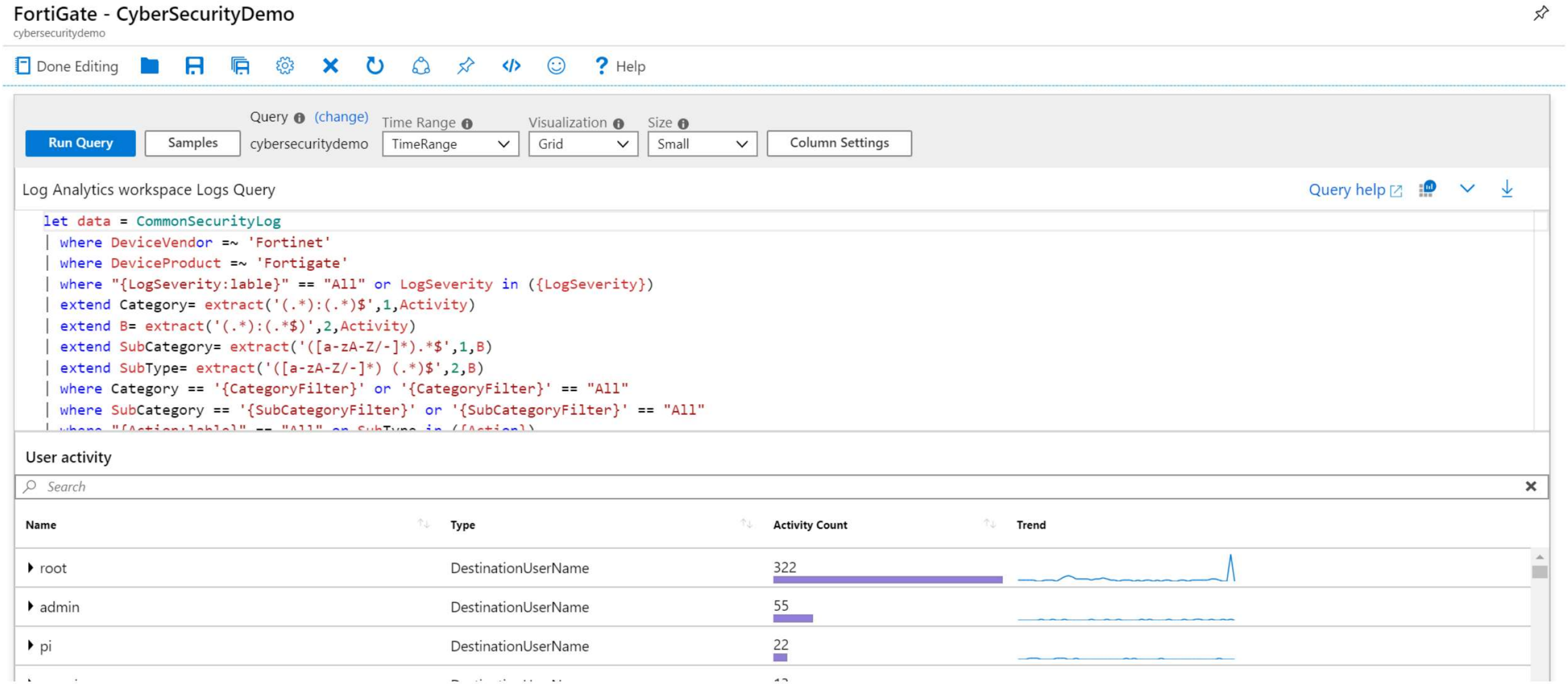
Name	Sign-in Count	Trend	Failure Count	Interrupt Count
US	2.349K		77	67
BE	566		3	8
GB	421		30	24
AU	241		22	65
IL	203		0	5

Location Sign-in details

Search

User	Sign-in Status	Sign-in Time
Ofer Shezaf	✓ Success	4 minut
Ofer Shezaf	✓ Success	4 minut
Preeti Krishna	✓ Success	8 minut
Nir Benjano	✓ Success	18 minu
Lior Tamir	✓ Success	26 minu

Workbooks: full customization



FortiGate - CyberSecurityDemo
cybersecuritydemo

Query (change): cybersecuritydemo
Time Range: TimeRange
Visualization: Grid
Size: Small

Log Analytics workspace Logs Query

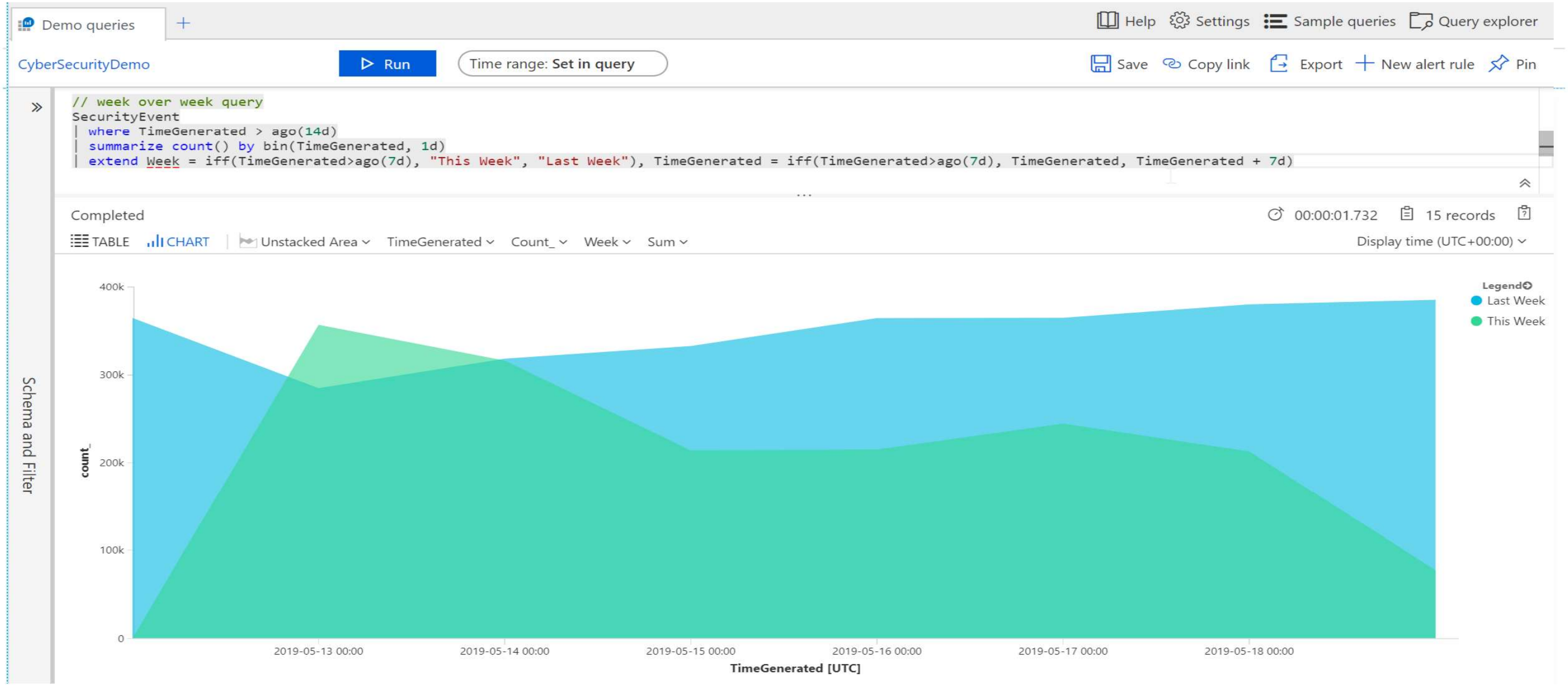
```
let data = CommonSecurityLog
 | where DeviceVendor =~ 'Fortinet'
 | where DeviceProduct =~ 'Fortigate'
 | where "{LogSeverity:lable}" == "All" or LogSeverity in ({LogSeverity})
 | extend Category= extract('(.*):(.*)$',1,Activity)
 | extend B= extract('(.*):(.*$)',2,Activity)
 | extend SubCategory= extract('([a-zA-Z/-]*).*$',1,B)
 | extend SubType= extract('([a-zA-Z/-]*) (.*)$',2,B)
 | where Category == '{CategoryFilter}' or '{CategoryFilter}' == "All"
 | where SubCategory == '{SubCategoryFilter}' or '{SubCategoryFilter}' == "All"
 | where "{Action:lable}" == "All" or SubType in ({Action})
```

User activity

Search

Name	Type	Activity Count	Trend
root	DestinationUserName	322	
admin	DestinationUserName	55	
pi	DestinationUserName	22	

Chart search results



```
// 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)
```

Time range: Set in query

Completed

00:00:01.732 15 records

Unstacked Area TimeGenerated Count_ Week Sum

Display time (UTC+00:00)

Analytics

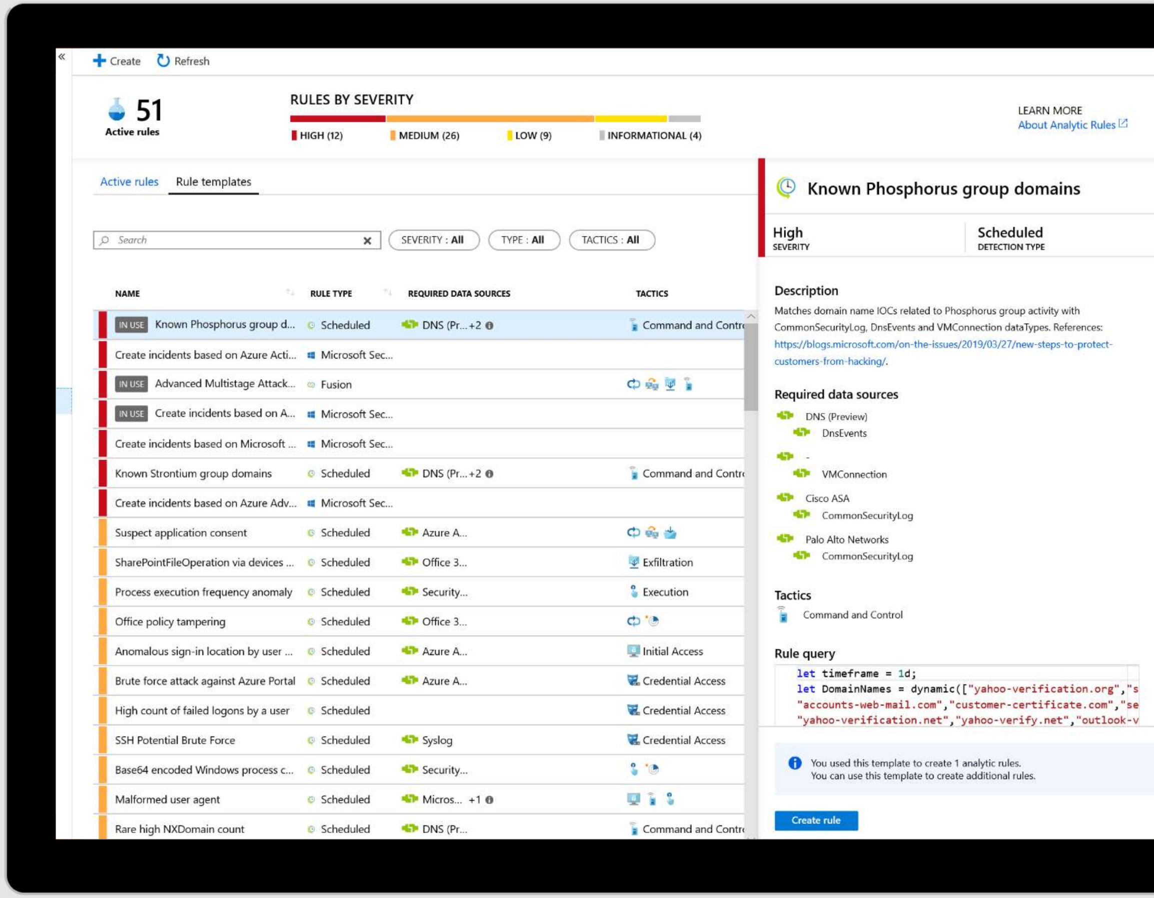
3 Leverage analytics to detect threats

Choose from more than 100 built-in analytics rules

Customize and create your own rules using KQL queries

Correlate events with your threat intelligence and now with Microsoft URL intelligence

Trigger automated playbooks



51 Active rules

RULES BY SEVERITY

HIGH (12) MEDIUM (26) LOW (9) INFORMATIONAL (4)

LEARN MORE
About Analytic Rules

NAME	RULE TYPE	REQUIRED DATA SOURCES	TACTICS
IN USE Known Phosphorus group d...	Scheduled	DNS (Pr... +2	Command and Contr
Create incidents based on Azure Acti...	Microsoft Sec...		
IN USE Advanced Multistage Attack...	Fusion		
IN USE Create incidents based on A...	Microsoft Sec...		
Create incidents based on Microsoft ...	Microsoft Sec...		
Known Strontium group domains	Scheduled	DNS (Pr... +2	Command and Contr
Create incidents based on Azure Adv...	Microsoft Sec...		
Suspect application consent	Scheduled	Azure A...	
SharePointFileOperation via devices ...	Scheduled	Office 3...	Exfiltration
Process execution frequency anomaly	Scheduled	Security...	Execution
Office policy tampering	Scheduled	Office 3...	
Anomalous sign-in location by user ...	Scheduled	Azure A...	Initial Access
Brute force attack against Azure Portal	Scheduled	Azure A...	Credential Access
High count of failed logons by a user	Scheduled		Credential Access
SSH Potential Brute Force	Scheduled	Syslog	Credential Access
Base64 encoded Windows process c...	Scheduled	Security...	
Malformed user agent	Scheduled	Micros... +1	
Rare high NXDomain count	Scheduled	DNS (Pr...	Command and Contr

Known Phosphorus group domains

High
SEVERITY

Scheduled
DETECTION TYPE

Description

Matches domain name IOCs related to Phosphorus group activity with CommonSecurityLog, DnsEvents and VMConnection dataTypes. References: https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/.

Required data sources

- DNS (Preview)
  - DnsEvents
- -
  - VMConnection
- Cisco ASA
  - CommonSecurityLog
- Palo Alto Networks
  - CommonSecurityLog

Tactics

Command and Control

Rule query

```
let timeframe = 1d;
let DomainNames = dynamic(["yahoo-verification.org","s
"accounts-web-mail.com","customer-certificate.com","se
"yahoo-verification.net","yahoo-verify.net","outlook-v
```

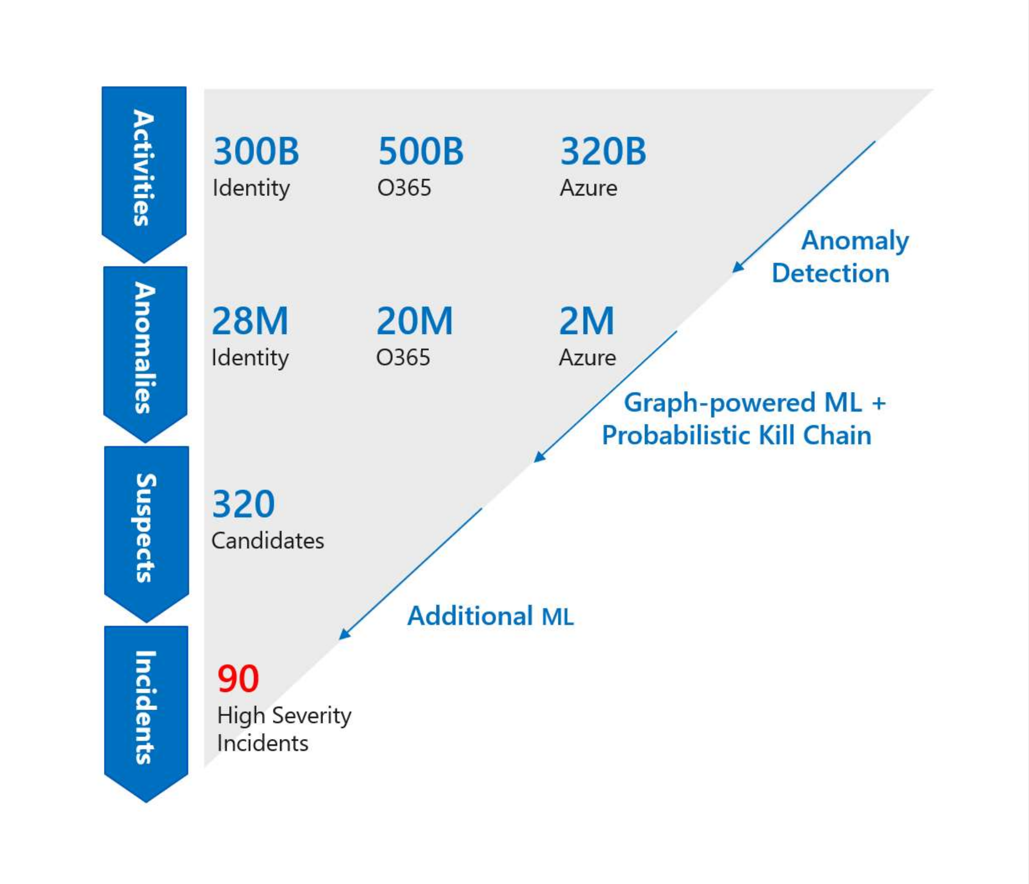
You used this template to create 1 analytic rules.
You can use this template to create additional rules.

4 Tap into the power of ML increase your catch rate without increasing noise

Use built–in models – no ML experience required

- Detects anomalies using transferred learning
- Fuses data sources to detect threats that span the kill chain
- Simply connect your data and learning begins

Bring your own ML models (coming soon)



Incidents

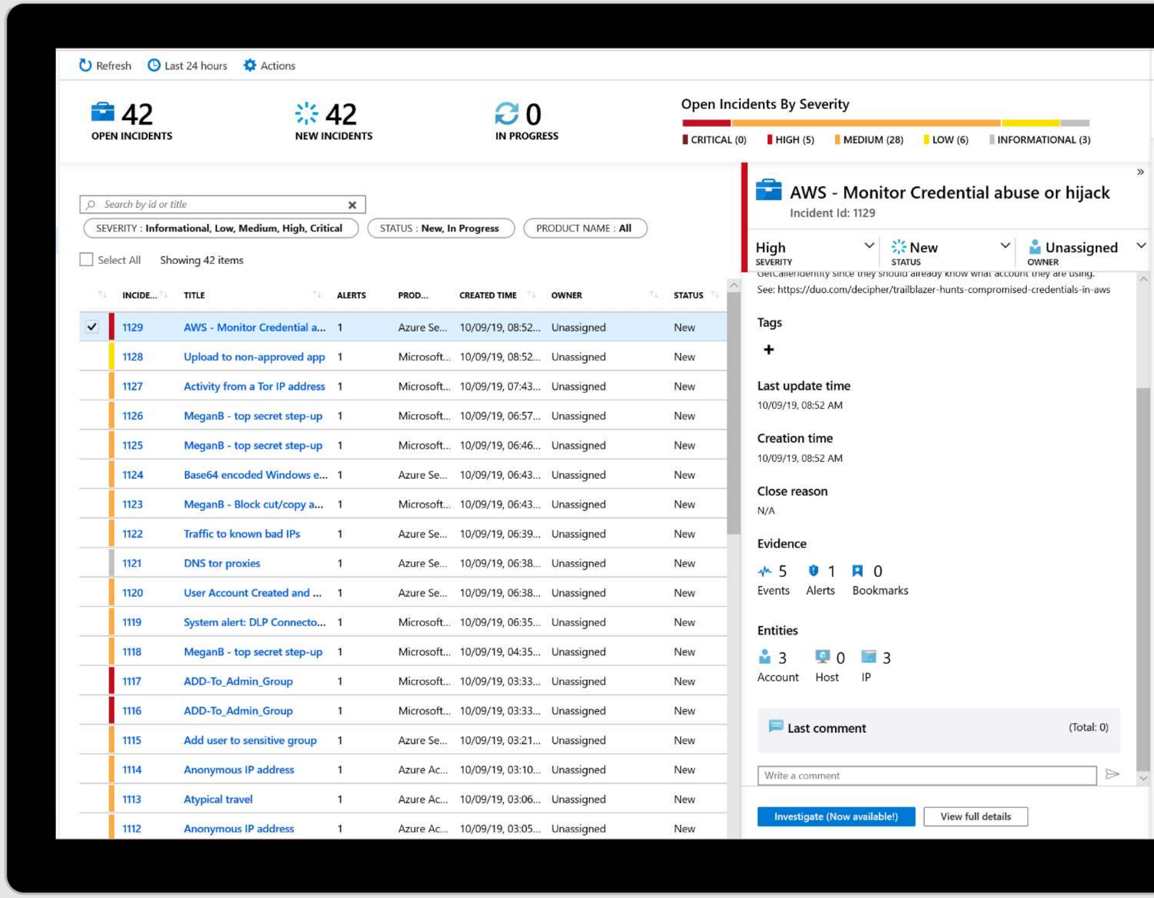
5 Start and track investigations from prioritized, actionable security incidents

Use incident to collect related alerts, events, and bookmarks

Manage assignments and track status

Add tags and comments

Trigger automated playbooks



42 OPEN INCIDENTS

42 NEW INCIDENTS

0 IN PROGRESS

Open Incidents By Severity

CRITICAL (0) HIGH (5) MEDIUM (28) LOW (6) INFORMATIONAL (3)

SEVERITY : **Informational, Low, Medium, High, Critical**   STATUS : **New, In Progress**   PRODUCT NAME : **All**

□ Select All   Showing 42 items

	INCIDE...	TITLE	ALERTS	PROD...	CREATED TIME	OWNER	STATUS
✓	1129	AWS - Monitor Credential a...	1	Azure Se...	10/09/19, 08:52...	Unassigned	New
	1128	Upload to non-approved app	1	Microsoft...	10/09/19, 08:52...	Unassigned	New
	1127	Activity from a Tor IP address	1	Microsoft...	10/09/19, 07:43...	Unassigned	New
	1126	MeganB - top secret step-up	1	Microsoft...	10/09/19, 06:57...	Unassigned	New
	1125	MeganB - top secret step-up	1	Microsoft...	10/09/19, 06:46...	Unassigned	New
	1124	Base64 encoded Windows e...	1	Azure Se...	10/09/19, 06:43...	Unassigned	New
	1123	MeganB - Block cut/copy a...	1	Microsoft...	10/09/19, 06:43...	Unassigned	New
	1122	Traffic to known bad IPs	1	Azure Se...	10/09/19, 06:39...	Unassigned	New
	1121	DNS tor proxies	1	Azure Se...	10/09/19, 06:38...	Unassigned	New
	1120	User Account Created and ...	1	Azure Se...	10/09/19, 06:38...	Unassigned	New
	1119	System alert: DLP Connecto...	1	Microsoft...	10/09/19, 06:35...	Unassigned	New
	1118	MeganB - top secret step-up	1	Microsoft...	10/09/19, 04:35...	Unassigned	New
	1117	ADD-To_Admin_Group	1	Microsoft...	10/09/19, 03:33...	Unassigned	New
	1116	ADD-To_Admin_Group	1	Microsoft...	10/09/19, 03:33...	Unassigned	New
	1115	Add user to sensitive group	1	Azure Se...	10/09/19, 03:21...	Unassigned	New
	1114	Anonymous IP address	1	Azure Ac...	10/09/19, 03:10...	Unassigned	New
	1113	Atypical travel	1	Azure Ac...	10/09/19, 03:06...	Unassigned	New
	1112	Anonymous IP address	1	Azure Ac...	10/09/19, 03:05...	Unassigned	New

AWS - Monitor Credential abuse or hijack

Incident Id: 1129

High SEVERITY   New STATUS   Unassigned OWNER

GetCallerIdentity since they should already know what account they are using.

See: https://duo.com/decipher/trailblazer-hunts-compromised-credentials-in-aws

Tags

+

Last update time

10/09/19, 08:52 AM

Creation time

10/09/19, 08:52 AM

Close reason

N/A

Evidence

5 Events   1 Alerts   0 Bookmarks

Entities

3 Account   0 Host   3 IP

Last comment (Total: 0)

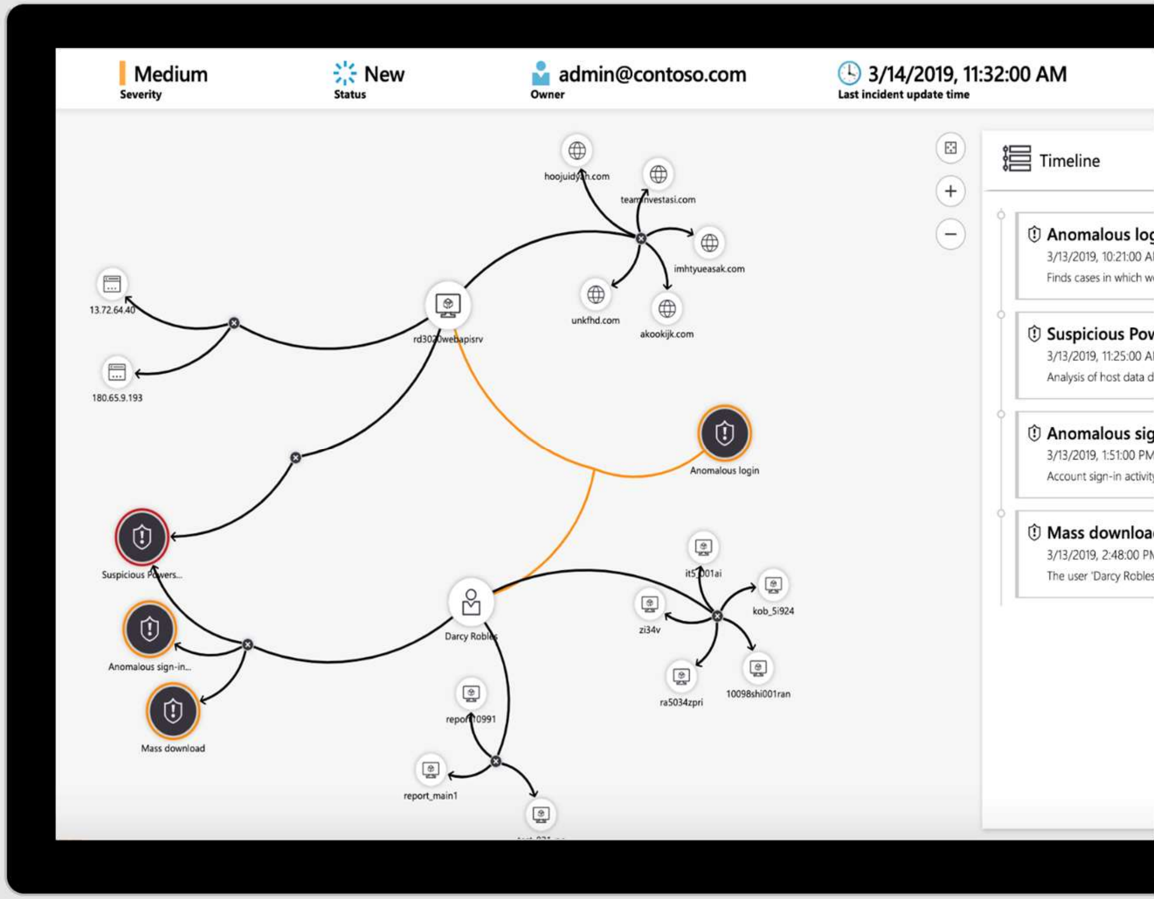
6 Visualize the entire attack to determine scope and impact

Navigate the relationships between related alerts, bookmarks, and entities

Expand the scope using exploration queries

View a timeline of related alerts, events, and bookmarks

Gain deep insights into related entities – users, domains, and more



Medium
Severity

New
Status

admin@contoso.com
Owner

3/14/2019, 11:32:00 AM
Last incident update time

Timeline

Anomalous log
3/13/2019, 10:21:00 A
Finds cases in which w

Suspicious Pow
3/13/2019, 11:25:00 A
Analysis of host data d

Anomalous sig
3/13/2019, 1:51:00 PM
Account sign-in activity

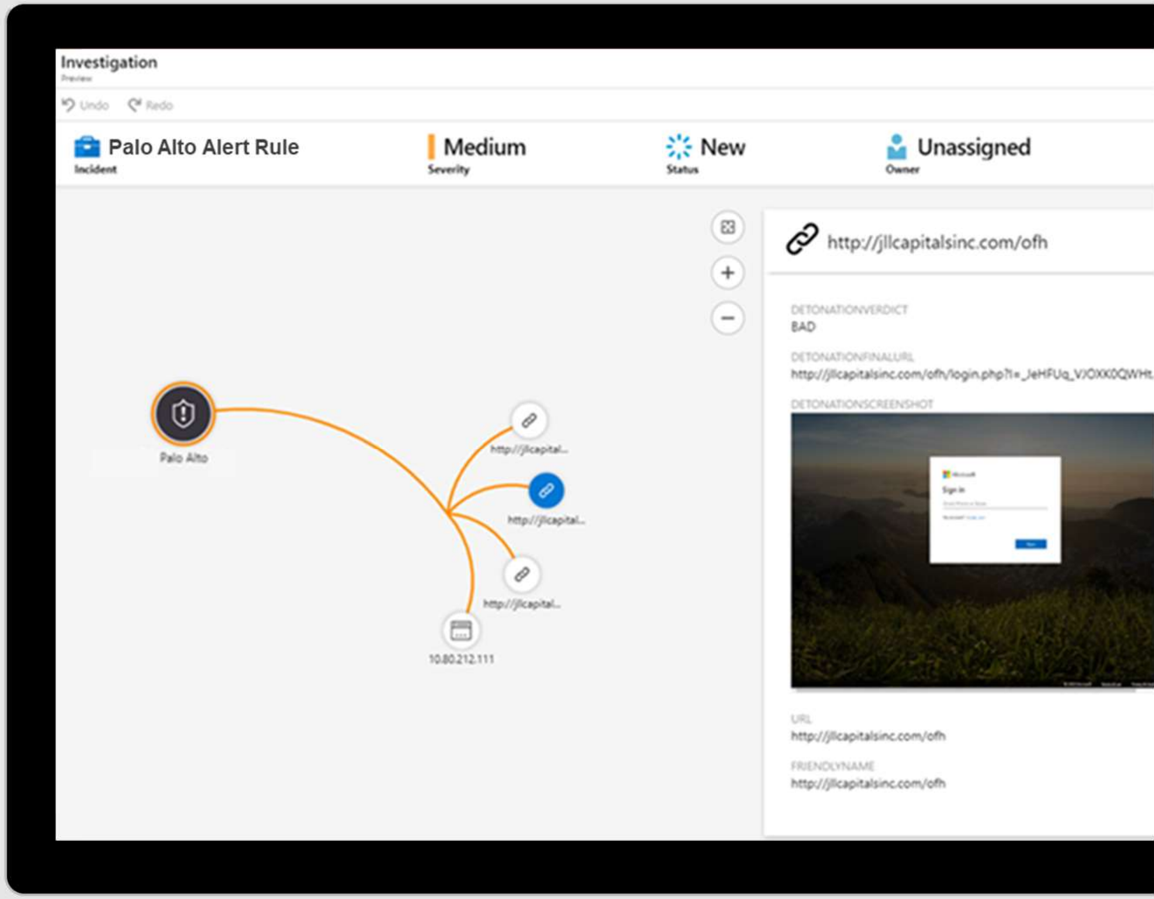
Mass downloa
3/13/2019, 2:48:00 PM
The user 'Darcy Robles

7 Gain deeper insight with built-in automated detonation

Configure URL Entities in analytics rules

Automatically trigger URL detonation

Enrich alerts with Verdicts, Final URLs and Screen Shots (e.g. for phishing sites)



Palo Alto Alert Rule
Incident

Medium
Severity

New
Status

Unassigned
Owner

http://jllcapitalsinc.com/ofh

DETONATIONVERDICT
BAD

DETONATIONFINALURL
http://jllcapitalsinc.com/ofh/login.php?l=_JeHFUq_VJOXK0QWHt

DETONATIONSCREENSHOT

URL
http://jllcapitalsinc.com/ofh

FRIENDLYNAME
http://jllcapitalsinc.com/ofh

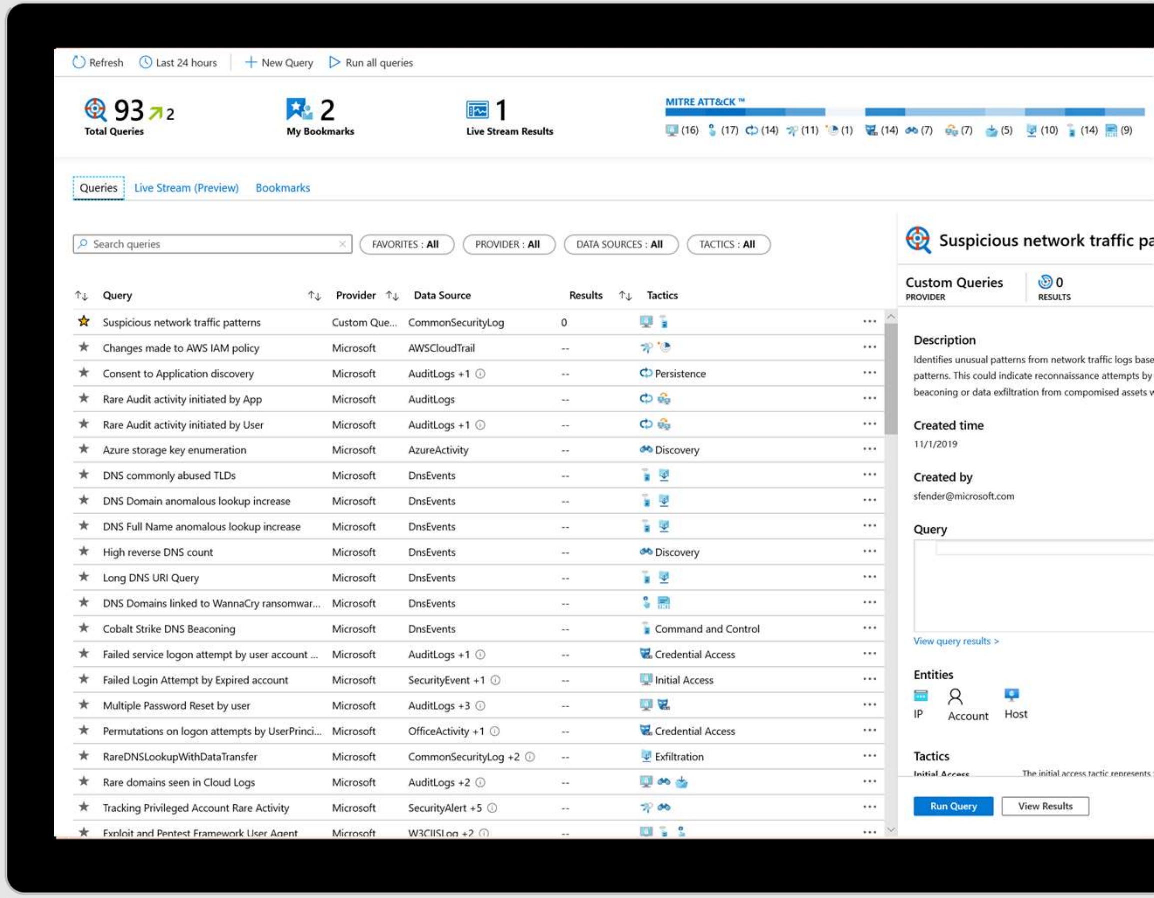
Hunting

8 Start hunting over security data with fast, flexible queries

Run built-in threat hunting queries - no prior query experience required

Customize and create your own hunting queries using KQL

Integrate hunting and investigations



93 ↗ 2 Total Queries

2 My Bookmarks

1 Live Stream Results

MITRE ATT&CK ™ (16) (17) (14) (11) (1) (14) (7) (7) (5) (10) (14) (9)

Query	Provider	Data Source	Results	Tactics
Suspicious network traffic patterns	Custom Que...	CommonSecurityLog	0	
Changes made to AWS IAM policy	Microsoft	AWSCloudTrail	--	
Consent to Application discovery	Microsoft	AuditLogs +1	--	Persistence
Rare Audit activity initiated by App	Microsoft	AuditLogs	--	
Rare Audit activity initiated by User	Microsoft	AuditLogs +1	--	
Azure storage key enumeration	Microsoft	AzureActivity	--	Discovery
DNS commonly abused TLDs	Microsoft	DnsEvents	--	
DNS Domain anomalous lookup increase	Microsoft	DnsEvents	--	
DNS Full Name anomalous lookup increase	Microsoft	DnsEvents	--	
High reverse DNS count	Microsoft	DnsEvents	--	Discovery
Long DNS URI Query	Microsoft	DnsEvents	--	
DNS Domains linked to WannaCry ransomwar...	Microsoft	DnsEvents	--	
Cobalt Strike DNS Beaconing	Microsoft	DnsEvents	--	Command and Control
Failed service logon attempt by user account ...	Microsoft	AuditLogs +1	--	Credential Access
Failed Login Attempt by Expired account	Microsoft	SecurityEvent +1	--	Initial Access
Multiple Password Reset by user	Microsoft	AuditLogs +3	--	
Permutations on logon attempts by UserPrinci...	Microsoft	OfficeActivity +1	--	Credential Access
RareDNSLookupWithDataTransfer	Microsoft	CommonSecurityLog +2	--	Exfiltration
Rare domains seen in Cloud Logs	Microsoft	AuditLogs +2	--	
Tracking Privileged Account Rare Activity	Microsoft	SecurityAlert +5	--	
Exploit and Pentest Framework User Agent	Microsoft	W3CIISLog +2	--	

Suspicious network traffic pa

Custom Queries
PROVIDER

0
RESULTS

Description

Identifies unusual patterns from network traffic logs base patterns. This could indicate reconnaissance attempts by beaconing or data exfiltration from compomised assets w

Created time

11/1/2019

Created by

sfender@microsoft.com

Query

Tactics

Initial Access The initial access tactic represents

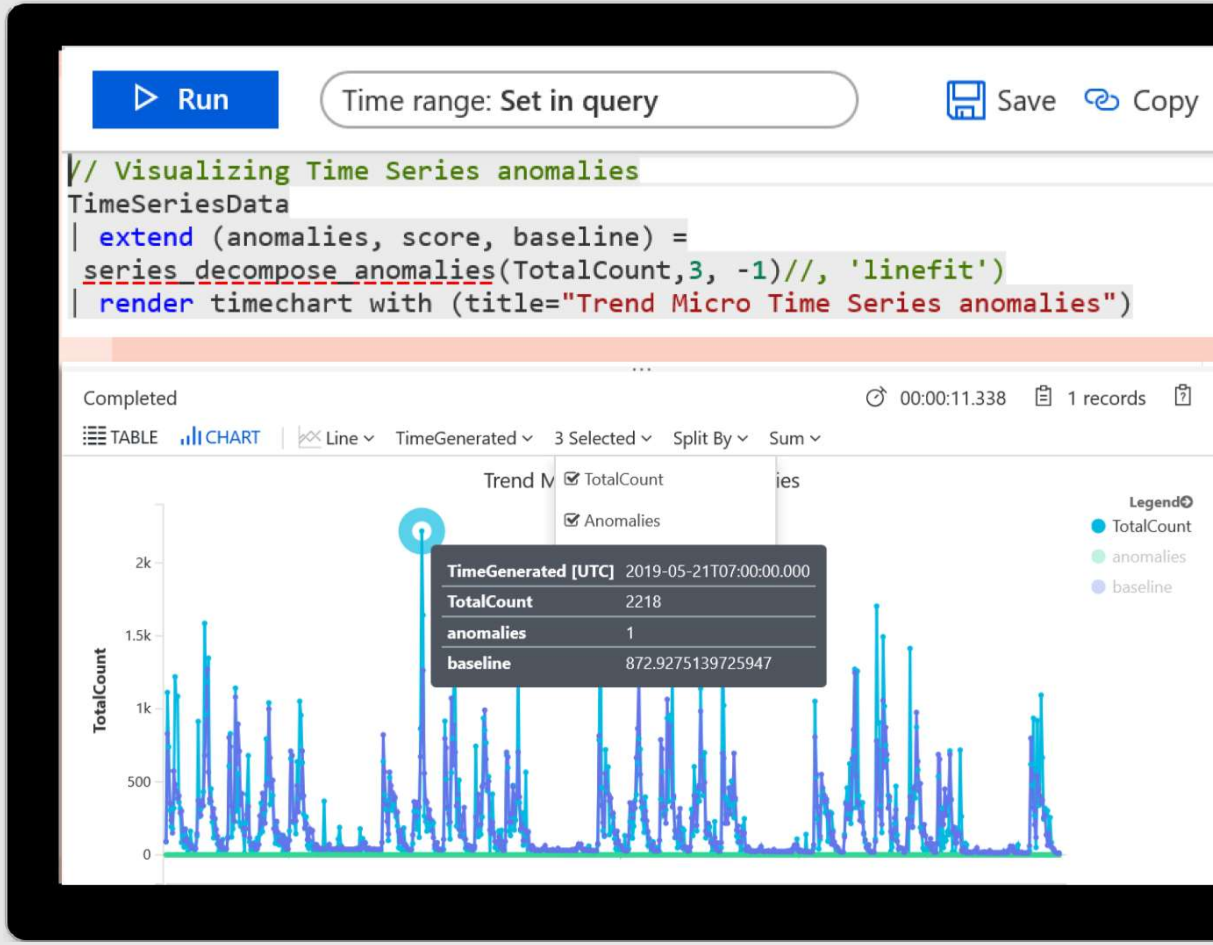
9 Explore data sets

Search using free text or fields

Tabulate your data

Visualize query results

Automatically detect and plot anomalies in data



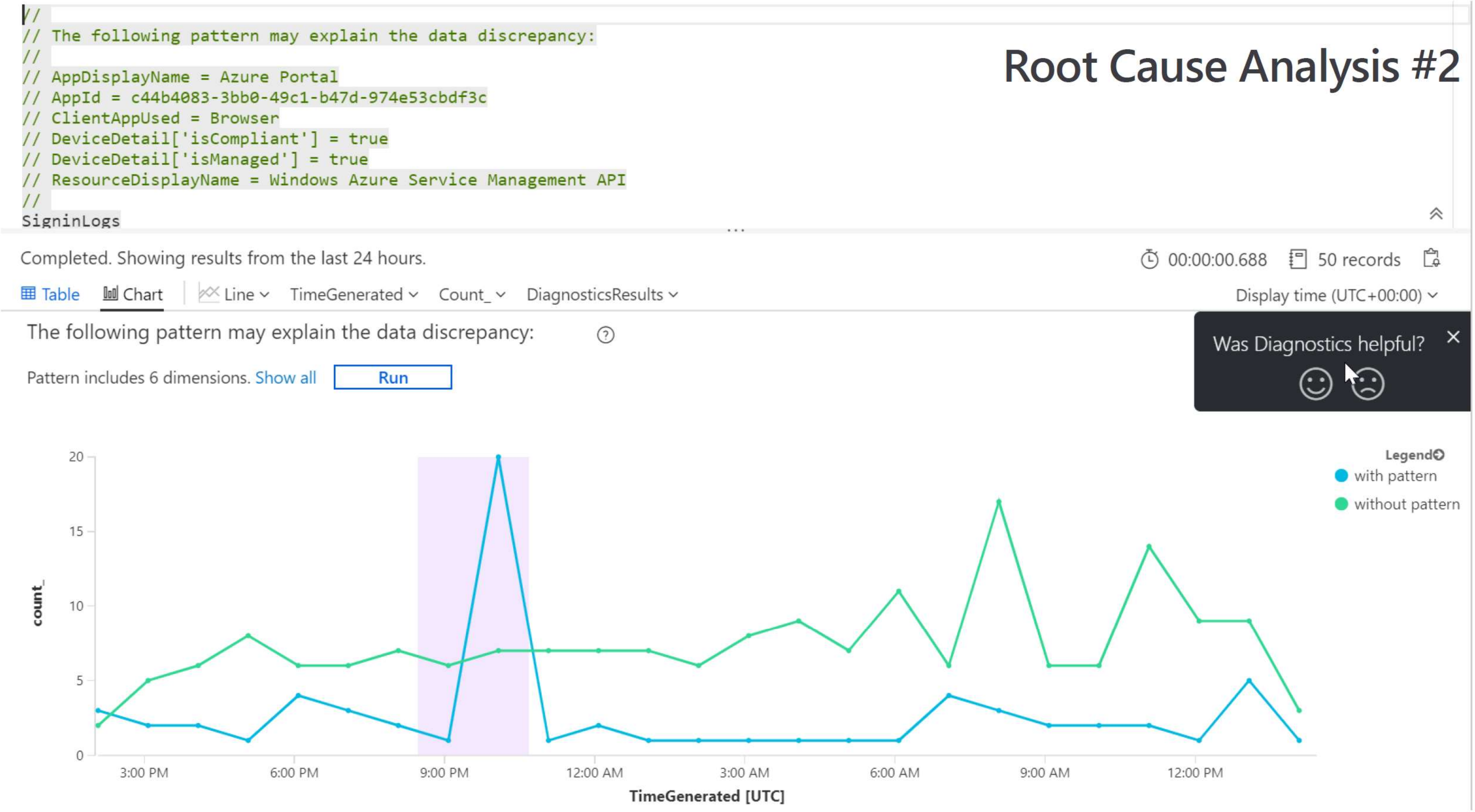
```
// Visualizing Time Series anomalies
TimeSeriesData
| extend (anomalies, score, baseline) =
 series_decompose_anomalies(TotalCount,3, -1)//, 'linefit')
| render timechart with (title="Trend Micro Time Series anomalies")
```

Time range: Set in query

Completed 00:00:11.338 1 records

TimeGenerated [UTC]	2019-05-21T07:00:00.000
TotalCount	2218
anomalies	1
baseline	872.9275139725947

Root Cause Analysis #2



```
//
// The following pattern may explain the data discrepancy:
//
// AppDisplayName = Azure Portal
// AppId = c44b4083-3bb0-49c1-b47d-974e53cbdf3c
// ClientAppUsed = Browser
// DeviceDetail['isCompliant'] = true
// DeviceDetail['isManaged'] = true
// ResourceDisplayName = Windows Azure Service Management API
//
SigninLogs
```

Completed. Showing results from the last 24 hours.

00:00:00.688 50 records

The following pattern may explain the data discrepancy:

Pattern includes 6 dimensions. Show all

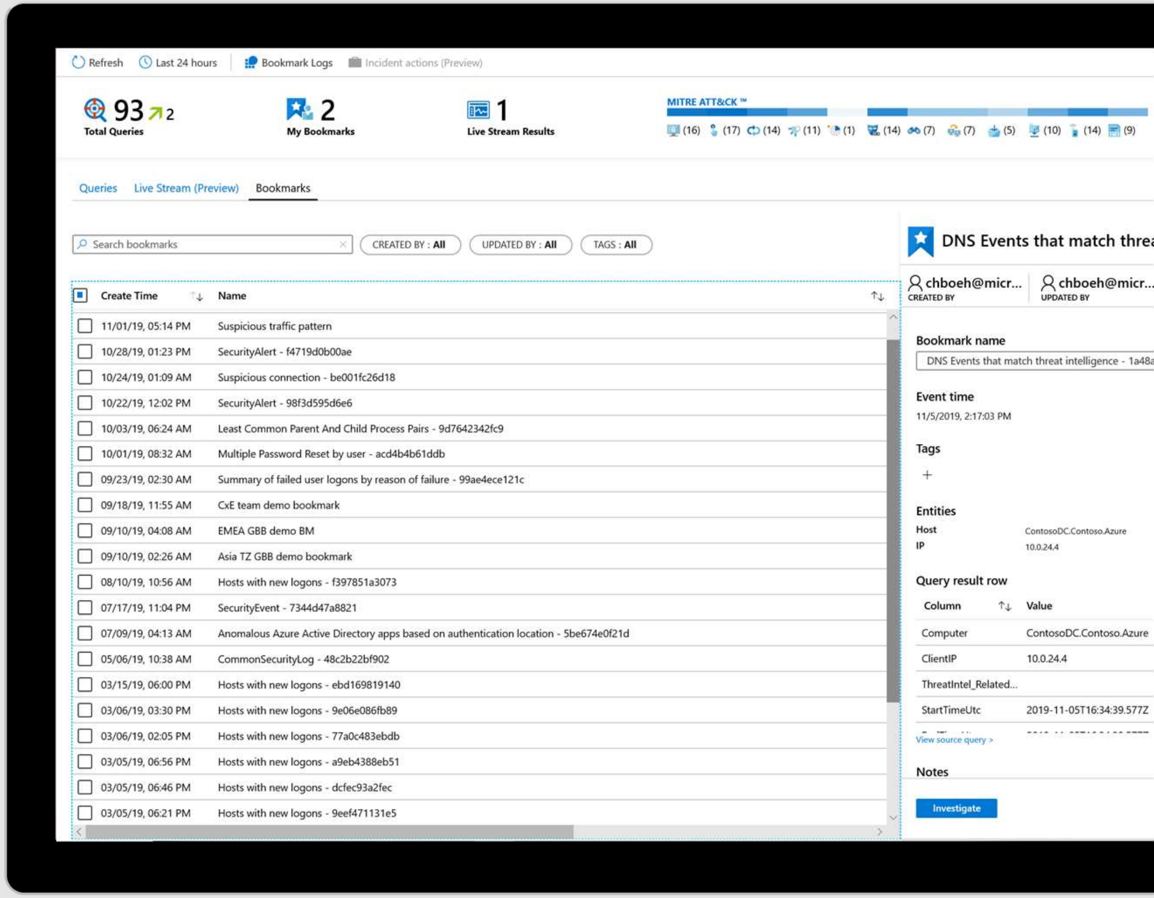
Was Diagnostics helpful?

9 Use bookmarks and live stream to manage your hunts

Bookmark notable data

Start an investigation from a bookmark or add to an existing incident

Monitor a live stream of new threat related activity



☐	Create Time	Name
☐	11/01/19, 05:14 PM	Suspicious traffic pattern
☐	10/28/19, 01:23 PM	SecurityAlert - f4719d0b00ae
☐	10/24/19, 01:09 AM	Suspicious connection - be001fc26d18
☐	10/22/19, 12:02 PM	SecurityAlert - 98f3d595d6e6
☐	10/03/19, 06:24 AM	Least Common Parent And Child Process Pairs - 9d7642342fc9
☐	10/01/19, 08:32 AM	Multiple Password Reset by user - acd4b4b61ddb
☐	09/23/19, 02:30 AM	Summary of failed user logons by reason of failure - 99ae4ece121c
☐	09/18/19, 11:55 AM	CxE team demo bookmark
☐	09/10/19, 04:08 AM	EMEA GBB demo BM
☐	09/10/19, 02:26 AM	Asia TZ GBB demo bookmark
☐	08/10/19, 10:56 AM	Hosts with new logons - f397851a3073
☐	07/17/19, 11:04 PM	SecurityEvent - 7344d47a8821
☐	07/09/19, 04:13 AM	Anomalous Azure Active Directory apps based on authentication location - 5be674e0f21d
☐	05/06/19, 10:38 AM	CommonSecurityLog - 48c2b22bf902
☐	03/15/19, 06:00 PM	Hosts with new logons - ebd169819140
☐	03/06/19, 03:30 PM	Hosts with new logons - 9e06e086fb89
☐	03/06/19, 02:05 PM	Hosts with new logons - 77a0c483ebdb
☐	03/05/19, 06:56 PM	Hosts with new logons - a9eb4388eb51
☐	03/05/19, 06:46 PM	Hosts with new logons - dcfec93a2fec
☐	03/05/19, 06:21 PM	Hosts with new logons - 9eef471131e5

DNS Events that match threa

chboeh@micr... CREATED BY

chboeh@micr... UPDATED BY

Bookmark name

DNS Events that match threat intelligence - 1a48a

Event time

11/5/2019, 2:17:03 PM

Tags

+

Entities

Host	ContosoDC.Contoso.Azure
IP	10.0.24.4

Query result row

Column	Value
Computer	ContosoDC.Contoso.Azure
ClientIP	10.0.24.4
ThreatIntel_Related...	
StartTimeUtc	2019-11-05T16:34:39.577Z

10 Use Jupyter notebooks for advanced hunting

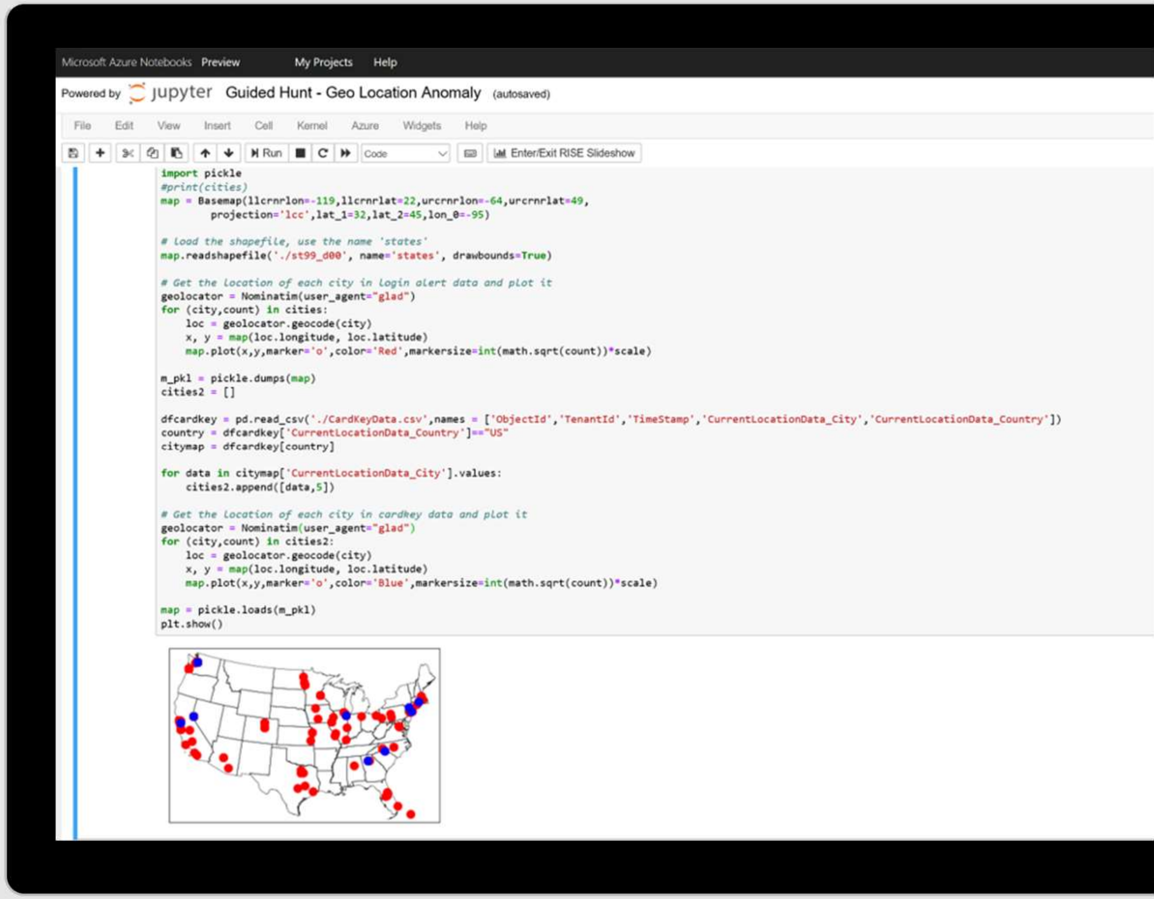
Run in the Azure cloud

Save as sharable HTML/JSON

Query Azure Sentinel data

Bring external data sources

Use your language of choice - Python, SQL, KQL, R, …


Microsoft Azure Notebooks Preview
My Projects
Help
Powered by jupyter
Guided Hunt - Geo Location Anomaly (autosaved)
File
Edit
View
Insert
Cell
Kernel
Azure
Widgets
Help
Run
Code
Enter/Exit RISE Slideshow

```
import pickle
#print(cities)
map = Basemap(llcrnrlon=-119,llcrnrlat=22,urcrnrlon=-64,urcrnrlat=49,
        projection='lcc',lat_1=32,lat_2=45,lon_0=-95)

# Load the shapefile, use the name 'states'
map.readshapefile('./st99_d00', name='states', drawbounds=True)

# Get the location of each city in login alert data and plot it
geolocator = Nominatim(user_agent="glad")
for (city,count) in cities:
    loc = geolocator.geocode(city)
    x, y = map(loc.longitude, loc.latitude)
    map.plot(x,y,marker='o',color='Red',markersize=int(math.sqrt(count))*scale)

m_pkl = pickle.dumps(map)
cities2 = []

dfcardkey = pd.read_csv('./CardKeyData.csv',names = ['ObjectId','TenantId','TimeStamp','CurrentLocationData_City','CurrentLocationData_Country'])
country = dfcardkey['CurrentLocationData_Country']=="US"
citymap = dfcardkey[country]

for data in citymap['CurrentLocationData_City'].values:
    cities2.append([data,5])

# Get the location of each city in cardkey data and plot it
geolocator = Nominatim(user_agent="glad")
for (city,count) in cities2:
    loc = geolocator.geocode(city)
    x, y = map(loc.longitude, loc.latitude)
    map.plot(x,y,marker='o',color='Blue',markersize=int(math.sqrt(count))*scale)

map = pickle.loads(m_pkl)
plt.show()
```

Automation

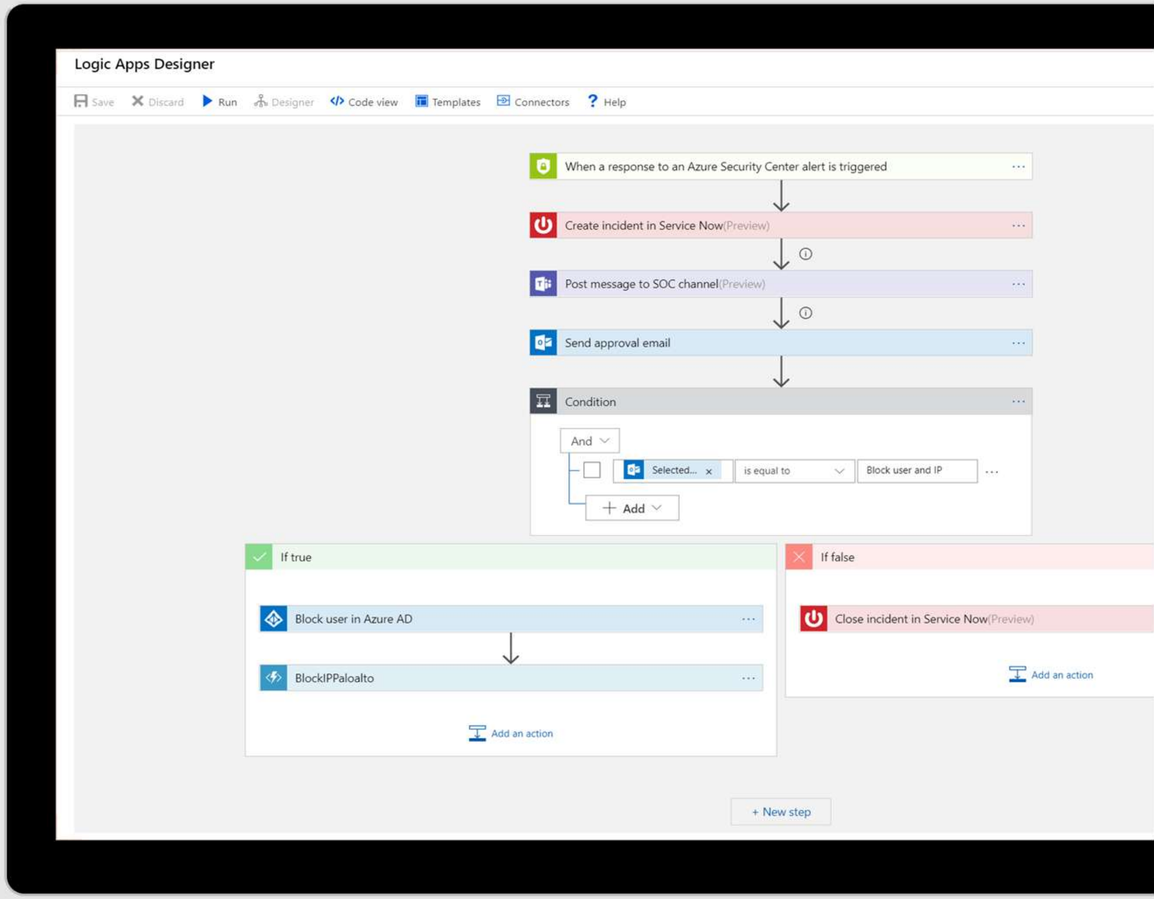
11 Automate and orchestrate security operations using integrated Azure Logic Apps

Build automated and scalable playbooks that integrate across tools

Choose from a library of samples

Create your own playbooks using 200+ built-in connectors

Trigger a playbook from an alert or incident investigation



Example playbooks

Incident Management

Assign an Incident to an Analyst

Open a Ticket (ServiceNow/Jira)

Keep Incident Status in Sync

Post in a Teams or Slack Channel

Enrichment + Investigation

Lookup Geo for an IP

Trigger Defender ATP Investigation

Send Validation Email to User

Remediation

Block an IP Address

Block User Access

Trigger Conditional Access

Isolate Machine

Sentinel demo

Take actions today—Get started with Azure Sentinel

Start
Microsoft Azure trial

Create Azure Sentinel
instance

Connect
data sources

To learn more, visit https://aka.ms/AzureSentinel

Festive Tech Calendar 2020

Ed Baker
@edbaker1965