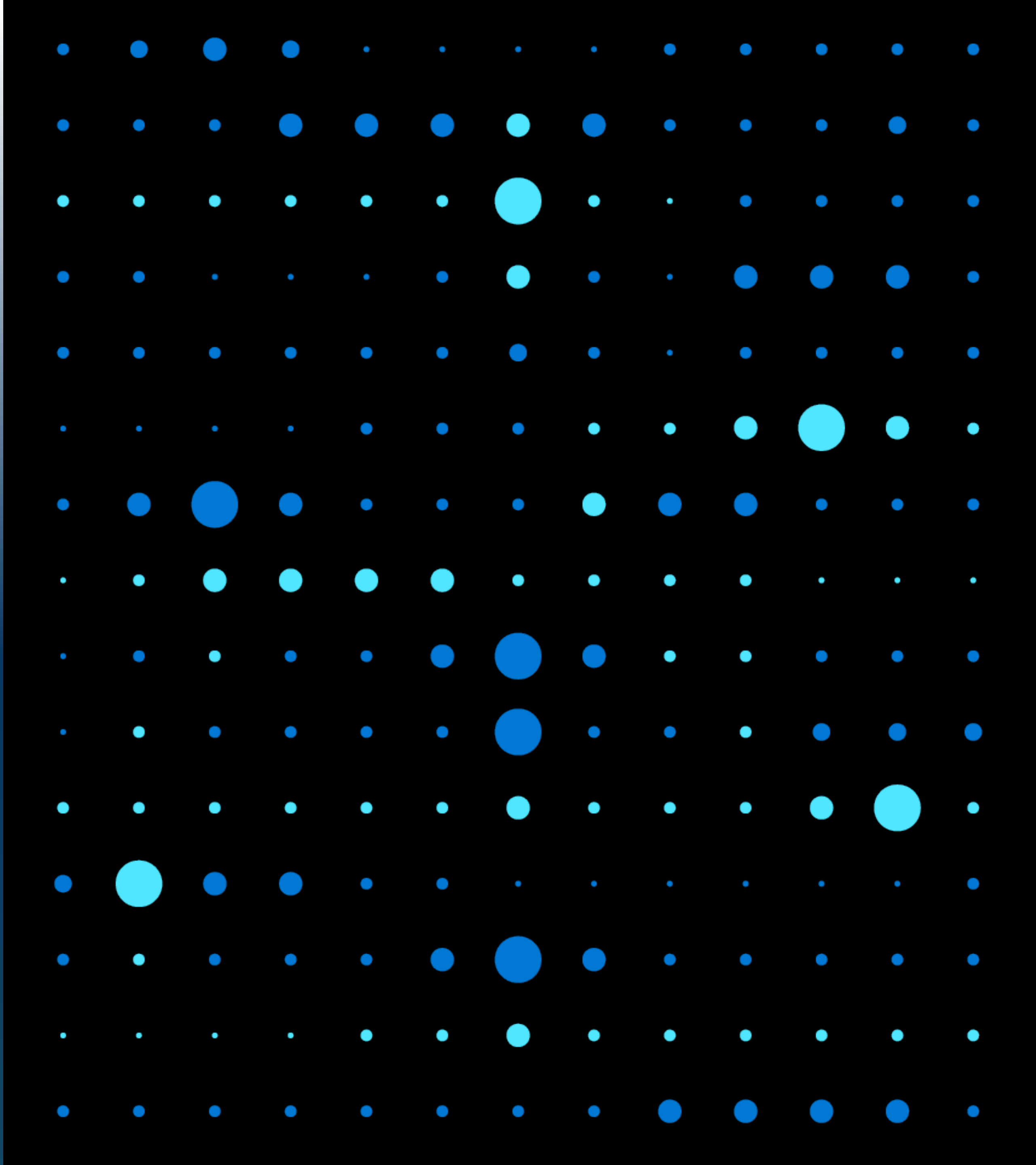
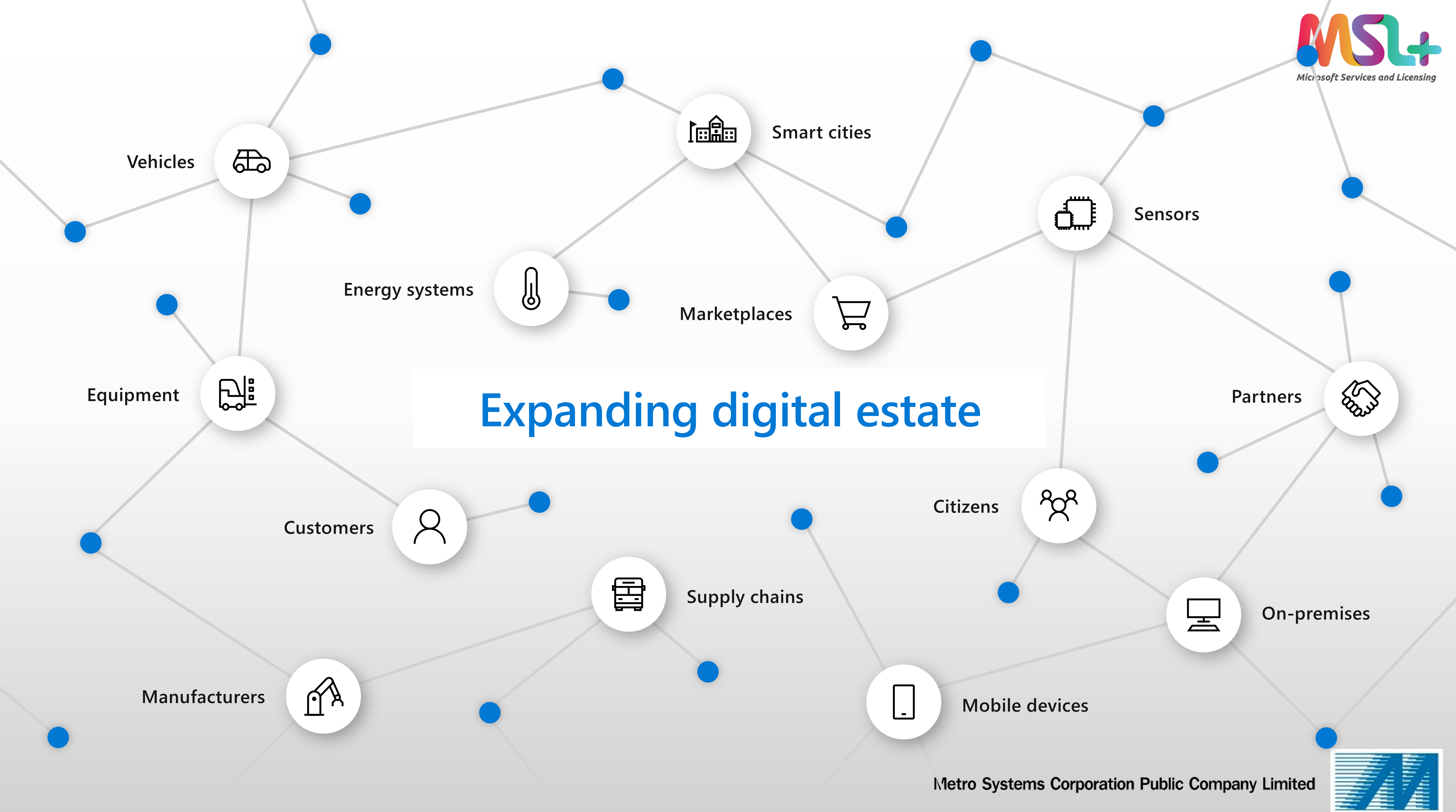
Microsoft Azure

# Modernize your security operations with Azure 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

Sophistication of threats

IT deployment & maintenance

76%
report increasing security data*

44%
of alerts are never investigated

Too many disconnected products

3.5M
unfilled security jobs in 2021

Lack of automation

*ESG: Secur ty Ana yt cs and Operat ons:  ndustry Trends  n the Era of C oud Comput ng 2019

Metro Systems Corporation Public Company Limited

Security Operations Team

+

Cloud + Artificial Intelligence

# Azure Sentinel

## SIEM + SOAR

Multi-cloud

Cloud native, any data, any entity

Partnerships

Cloud native

Any data

AI

Automation

Microsoft Services and Licensing

# Modernize your SOC with Azure Sentinel

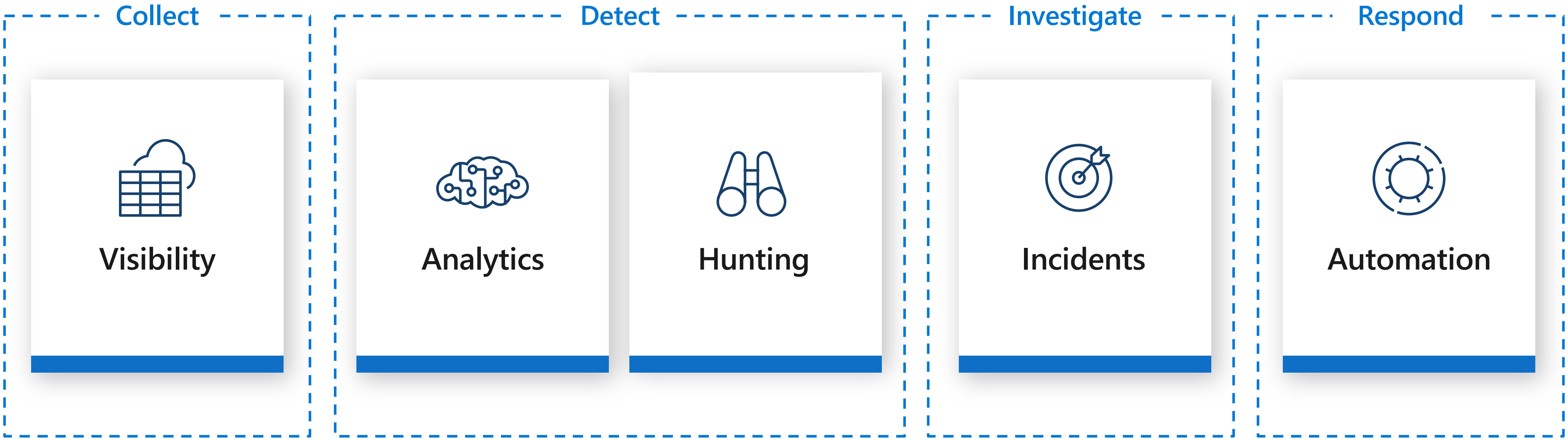
## THE INTELLIGENT, CLOUD-NATIVE SIEM

**Scales to support your growing digital estate**

**Offers improved threat detection**

**Uses AI and automation to increase efficiency**

# End-to-end solution for security operations



Collect

Visibility

Detect

Analytics

Hunting

Investigate

Incidents

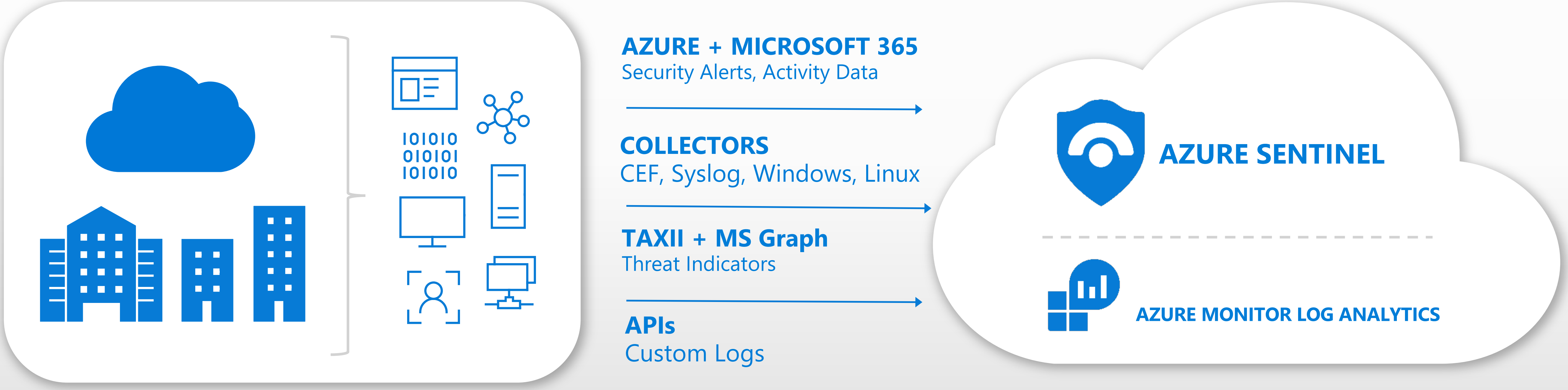
Respond

Automation

Powered by community + backed by Microsoft's security experts

# Visibility

# 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**

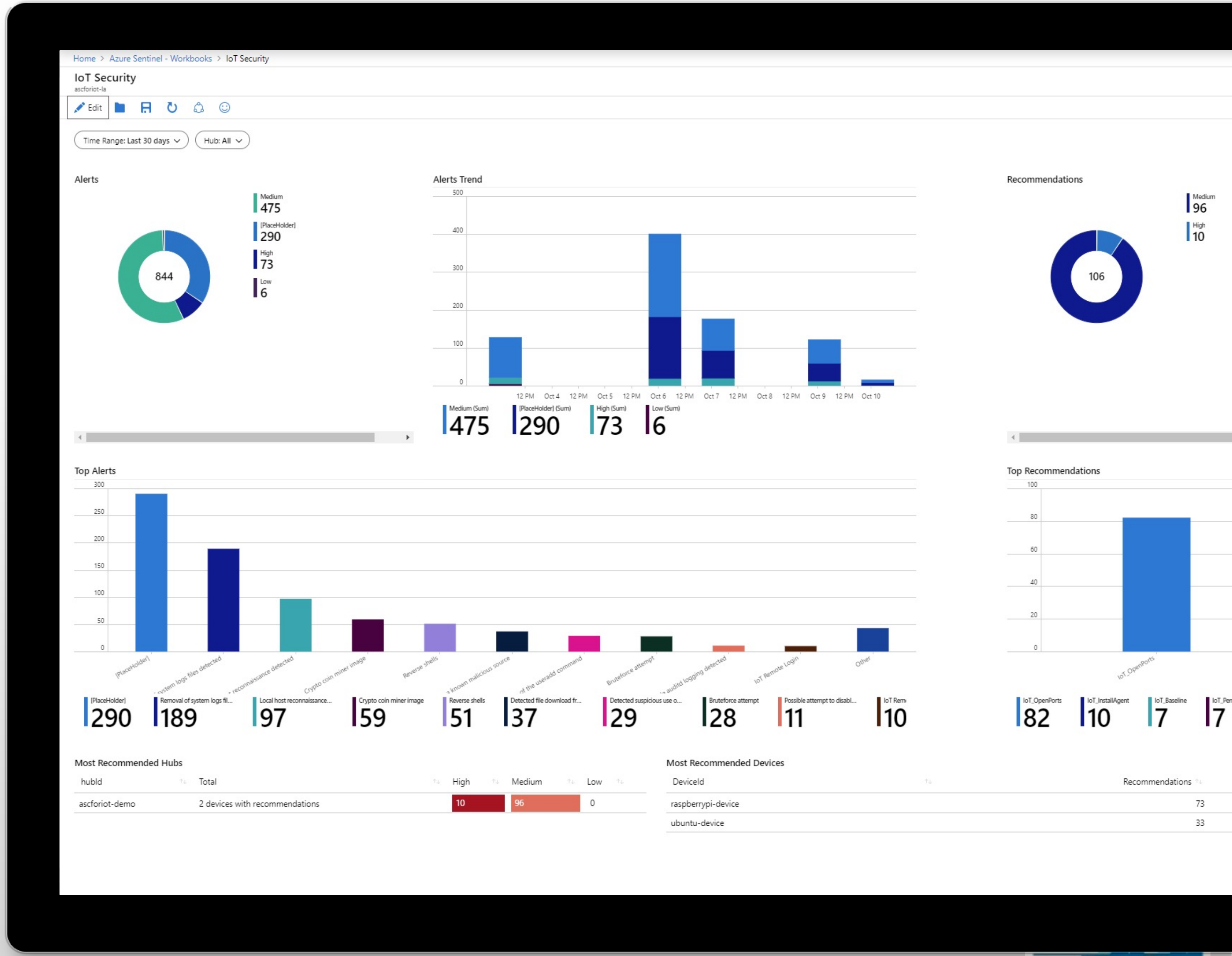
# Get interactive dashboards for powerful insights

## 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



Home > Azure Sentinel - Workbooks > IoT Security

IoT Security
ascforiot-la

Time Range: Last 30 days
Hub: All

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 |

# Analytics

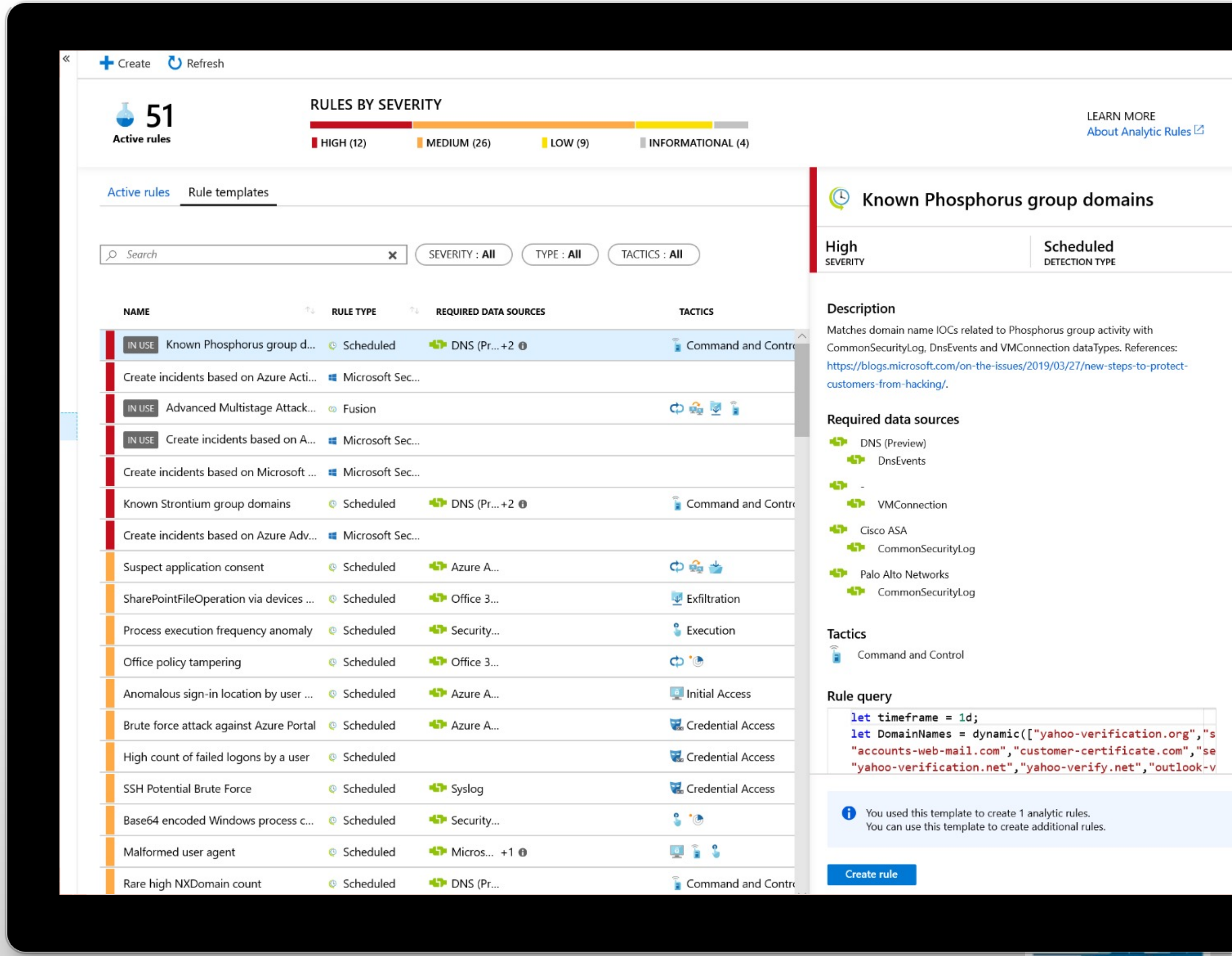
# Leverage extensive library of detections or build your own

## 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 + network data

## 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**

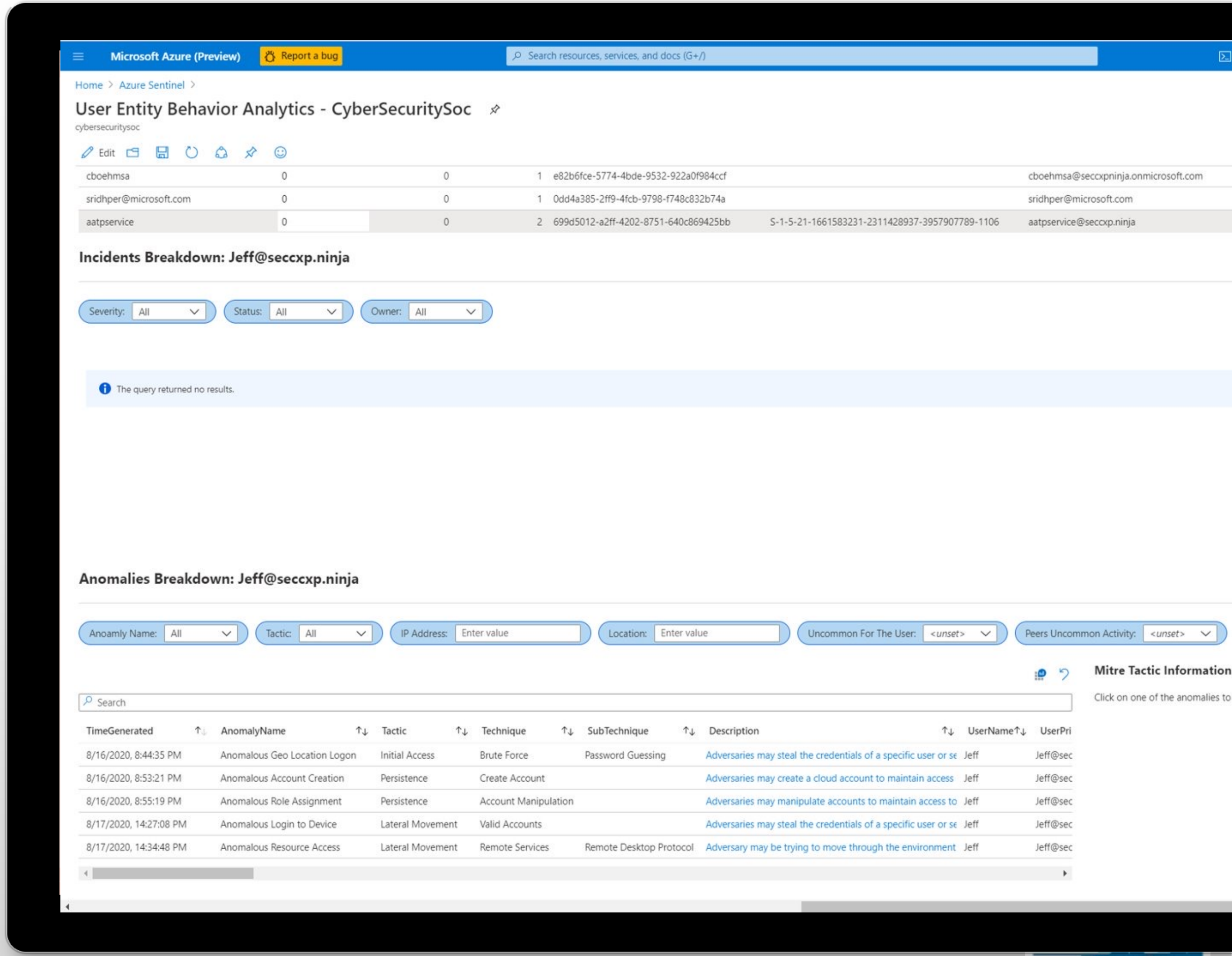
```
let timeframe = 1d;
let DomainNames = dynamic(["yahoo-verification.org","s
"accounts-web-mail.com","customer-certificate.com","se
"yahoo-verification.net","yahoo-verify.net","outlook-v
```

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

# Improve insider and unknown threat detection with User and Entity Behavior Analytics

Use behavioral insights to detect anomalies, understand the relative sensitivity of entities, and evaluate potential impact

Get baseline behavioral profiles of entities across time and peer group horizons


Microsoft Azure (Preview)
Report a bug
Search resources, services, and docs (G+/)
Home > Azure Sentinel >
Edit

User Entity Behavior Analytics - CyberSecuritySoc

cybersecuritysoc

| | | | | | | |
|---|---|---|---|---|---|---|
| cboehmsa | 0 | 0 | 1 | e82b6fce-5774-4bde-9532-922a0f984ccf | | cboehmsa@seccxpninja.onmicrosoft.com |
| sridhper@microsoft.com | 0 | 0 | 1 | 0dd4a385-2ff9-4fcb-9798-f748c832b74a | | sridhper@microsoft.com |
| aatpservice | 0 | 0 | 2 | 699d5012-a2ff-4202-8751-640c869425bb | S-1-5-21-1661583231-2311428937-3957907789-1106 | aatpservice@seccxp.ninja |

**Incidents Breakdown: Jeff@seccxp.ninja**

Severity: All
Status: All
Owner: All

The query returned no results.

**Anomalies Breakdown: Jeff@seccxp.ninja**

Anoamly Name: All
Tactic: All
IP Address: Enter value
Location: Enter value
Uncommon For The User: <unset>
Peers Uncommon Activity: <unset>

Search

| TimeGenerated | AnomalyName | Tactic | Technique | SubTechnique | Description | UserName | UserPri |
|---|---|---|---|---|---|---|---|
| 8/16/2020, 8:44:35 PM | Anomalous Geo Location Logon | Initial Access | Brute Force | Password Guessing | Adversaries may steal the credentials of a specific user or se | Jeff | Jeff@sec |
| 8/16/2020, 8:53:21 PM | Anomalous Account Creation | Persistence | Create Account | | Adversaries may create a cloud account to maintain access | Jeff | Jeff@sec |
| 8/16/2020, 8:55:19 PM | Anomalous Role Assignment | Persistence | Account Manipulation | | Adversaries may manipulate accounts to maintain access to | Jeff | Jeff@sec |
| 8/17/2020, 14:27:08 PM | Anomalous Login to Device | Lateral Movement | Valid Accounts | | Adversaries may steal the credentials of a specific user or se | Jeff | Jeff@sec |
| 8/17/2020, 14:34:48 PM | Anomalous Resource Access | Lateral Movement | Remote Services | Remote Desktop Protocol | Adversary may be trying to move through the environment | Jeff | Jeff@sec |

**Mitre Tactic Information**

Click on one of the anomalies to

*Powered by the proven Microsoft User and Entity Behavior Analytics (UEBA) engine*

Metro Systems Corporation Public Company Limited

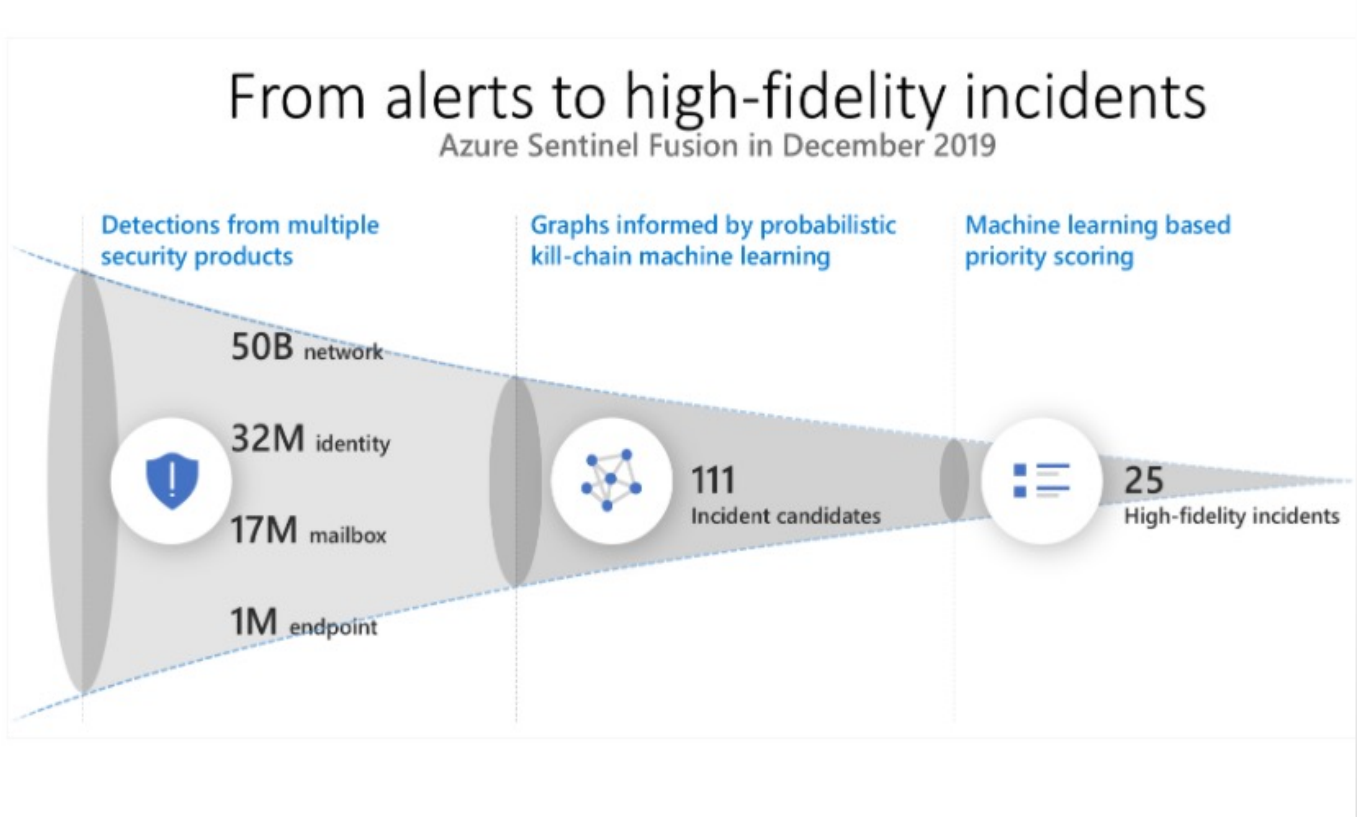
# Tap into the power of ML, increase your catch rate without increasing noise

## 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

- Build ML for your unique needs, leveraging Microsoft’s algorithms and best practices



From alerts to high-fidelity incidents

Azure Sentinel Fusion in December 2019

Detections from multiple security products
Graphs informed by probabilistic kill-chain machine learning
Machine learning based priority scoring
50B network
32M identity
17M mailbox
1M endpoint
111
Incident candidates
25
High-fidelity incidents

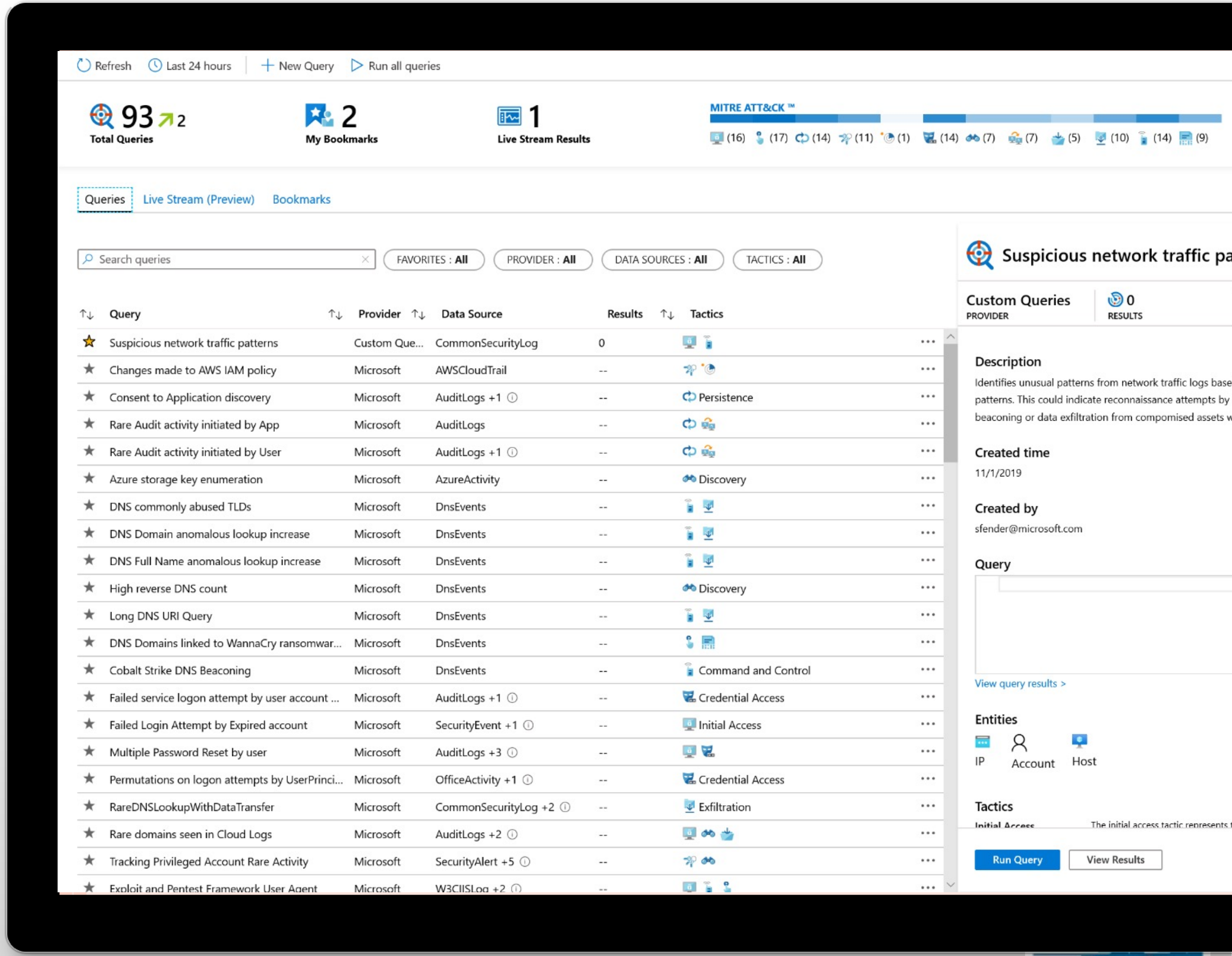
# Hunting

# 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



| | 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

View query results >

Entities

IP Account Host

Tactics

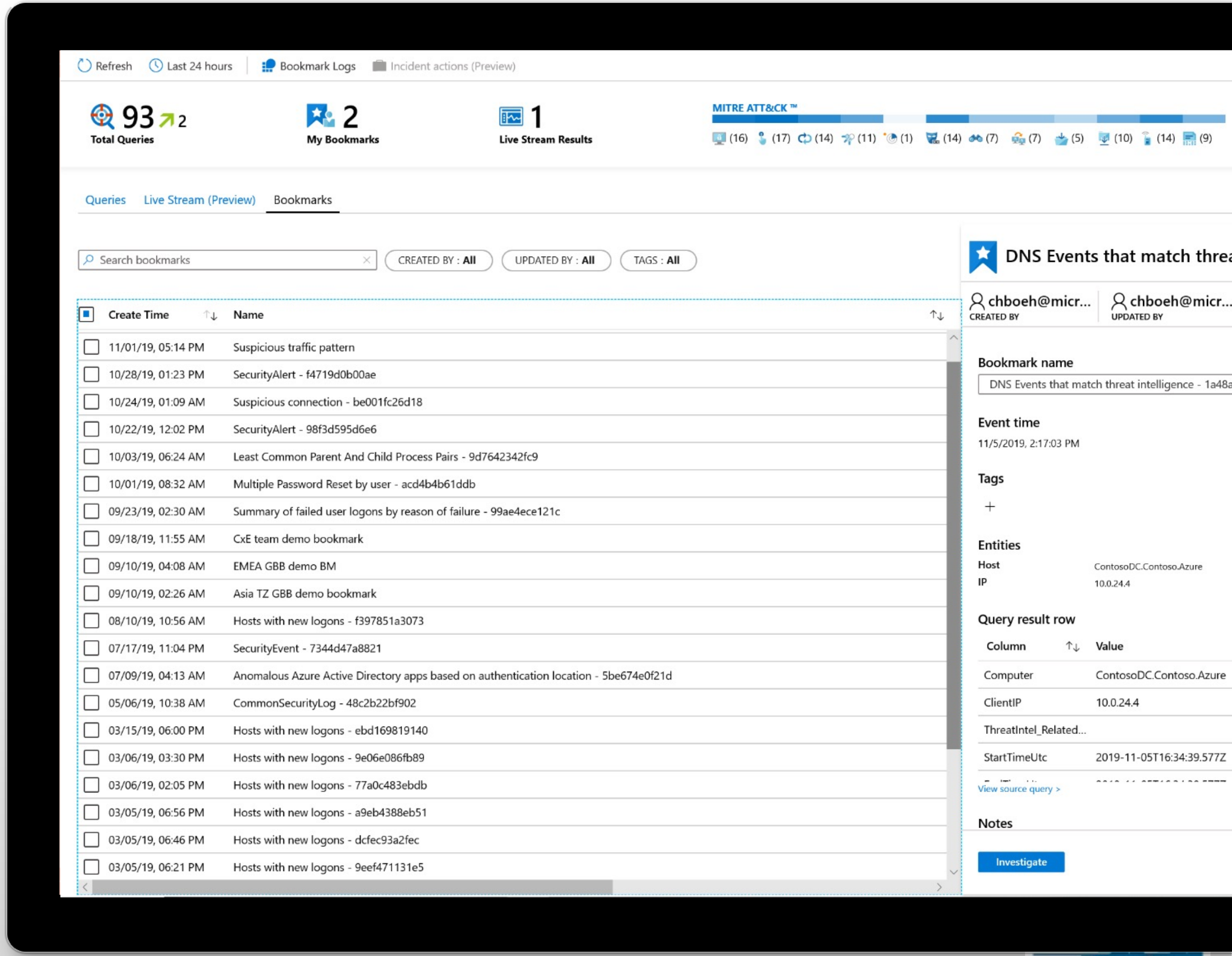
Initial Access The initial access tactic represents t

# 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 |

Notes

# Use Jupyter notebooks for advanced hunting

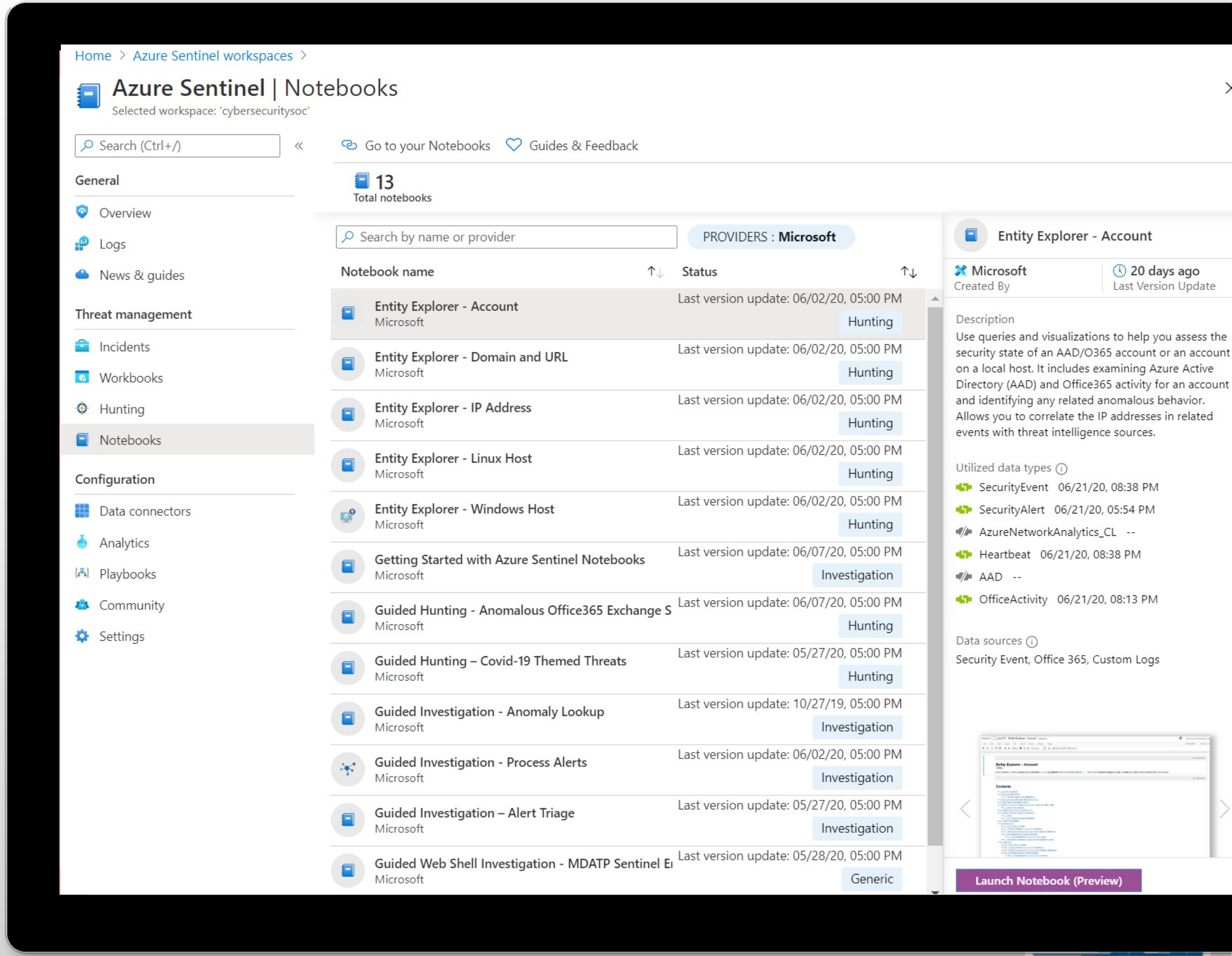
Run in Azure Machine Learning

Use sample templates to help you get started

Save as sharable HTML/JSON

Query Azure Sentinel data and bring in external data sources

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



Home > Azure Sentinel workspaces >

Azure Sentinel | Notebooks

Selected workspace: 'cybersecuritysoc'

13
Total notebooks

Search by name or provider

PROVIDERS : **Microsoft**

| Notebook name | Status |
|---|---|
| Entity Explorer - Account<br>Microsoft | Last version update: 06/02/20, 05:00 PM<br>Hunting |
| Entity Explorer - Domain and URL<br>Microsoft | Last version update: 06/02/20, 05:00 PM<br>Hunting |
| Entity Explorer - IP Address<br>Microsoft | Last version update: 06/02/20, 05:00 PM<br>Hunting |
| Entity Explorer - Linux Host<br>Microsoft | Last version update: 06/02/20, 05:00 PM<br>Hunting |
| Entity Explorer - Windows Host<br>Microsoft | Last version update: 06/02/20, 05:00 PM<br>Hunting |
| Getting Started with Azure Sentinel Notebooks<br>Microsoft | Last version update: 06/07/20, 05:00 PM<br>Investigation |
| Guided Hunting - Anomalous Office365 Exchange S<br>Microsoft | Last version update: 06/07/20, 05:00 PM<br>Hunting |
| Guided Hunting – Covid-19 Themed Threats<br>Microsoft | Last version update: 05/27/20, 05:00 PM<br>Hunting |
| Guided Investigation - Anomaly Lookup<br>Microsoft | Last version update: 10/27/19, 05:00 PM<br>Investigation |
| Guided Investigation - Process Alerts<br>Microsoft | Last version update: 06/02/20, 05:00 PM<br>Investigation |
| Guided Investigation – Alert Triage<br>Microsoft | Last version update: 05/27/20, 05:00 PM<br>Investigation |
| Guided Web Shell Investigation - MDATP Sentinel E<br>Microsoft | Last version update: 05/28/20, 05:00 PM<br>Generic |

Entity Explorer - Account

Microsoft
Created By

20 days ago
Last Version Update

Description

Use queries and visualizations to help you assess the security state of an AAD/O365 account or an account on a local host. It includes examining Azure Active Directory (AAD) and Office365 activity for an account and identifying any related anomalous behavior. Allows you to correlate the IP addresses in related events with threat intelligence sources.

Utilized data types

SecurityEvent 06/21/20, 08:38 PM
SecurityAlert 06/21/20, 05:54 PM
AzureNetworkAnalytics_CL --
Heartbeat 06/21/20, 08:38 PM
AAD --
OfficeActivity 06/21/20, 08:13 PM

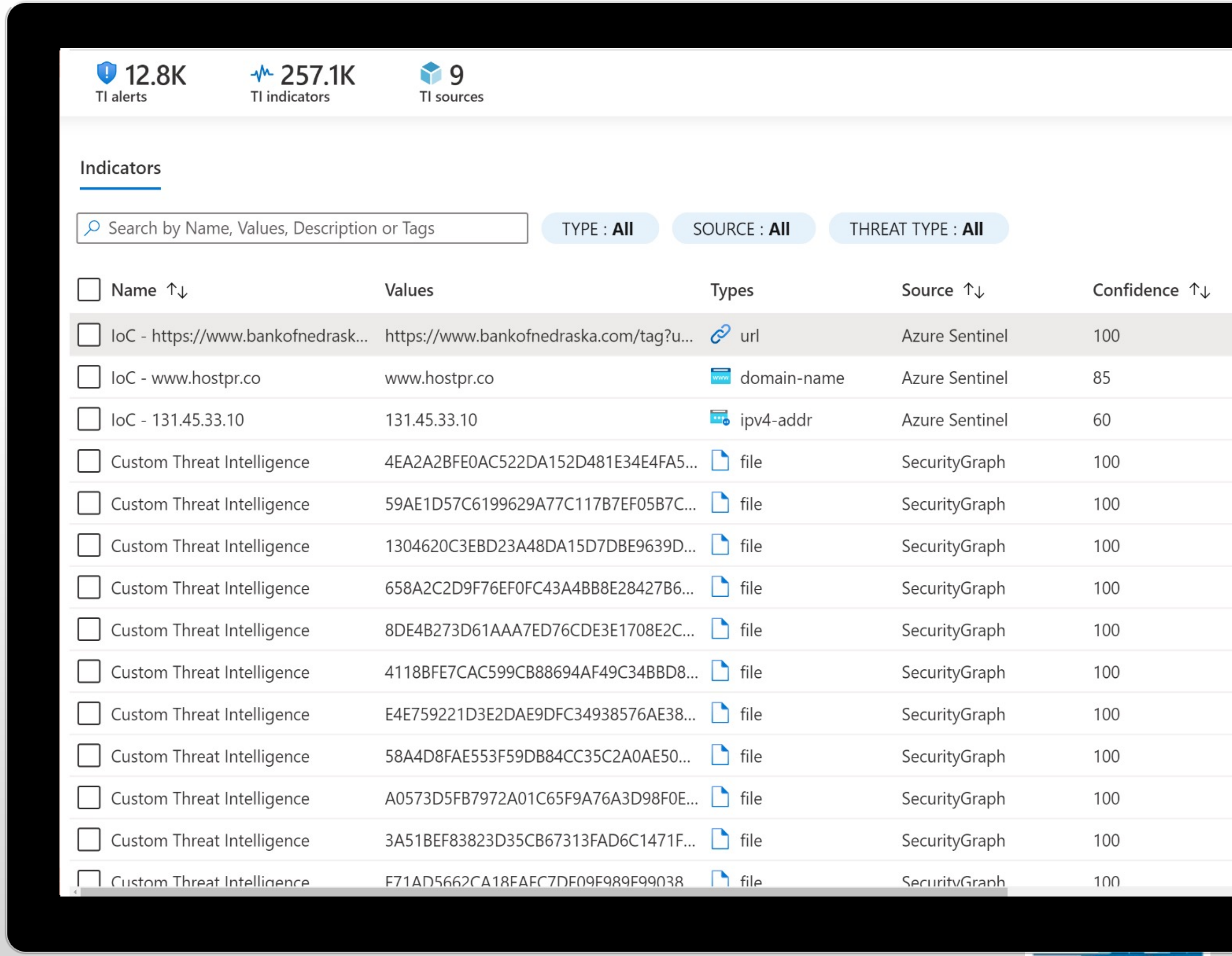
Data sources

Security Event, Office 365, Custom Logs

# Intelligence

# Monitor and manage threat intelligence

- Create, view, search, filter, sort, and tag all your threat indicators in a single pane
- Use alert metrics to help understand top threats targeting your organization
- Use automation playbooks for leading threat intelligence providers to enrich alerts



12.8K TI alerts

257.1K TI indicators

9 TI sources

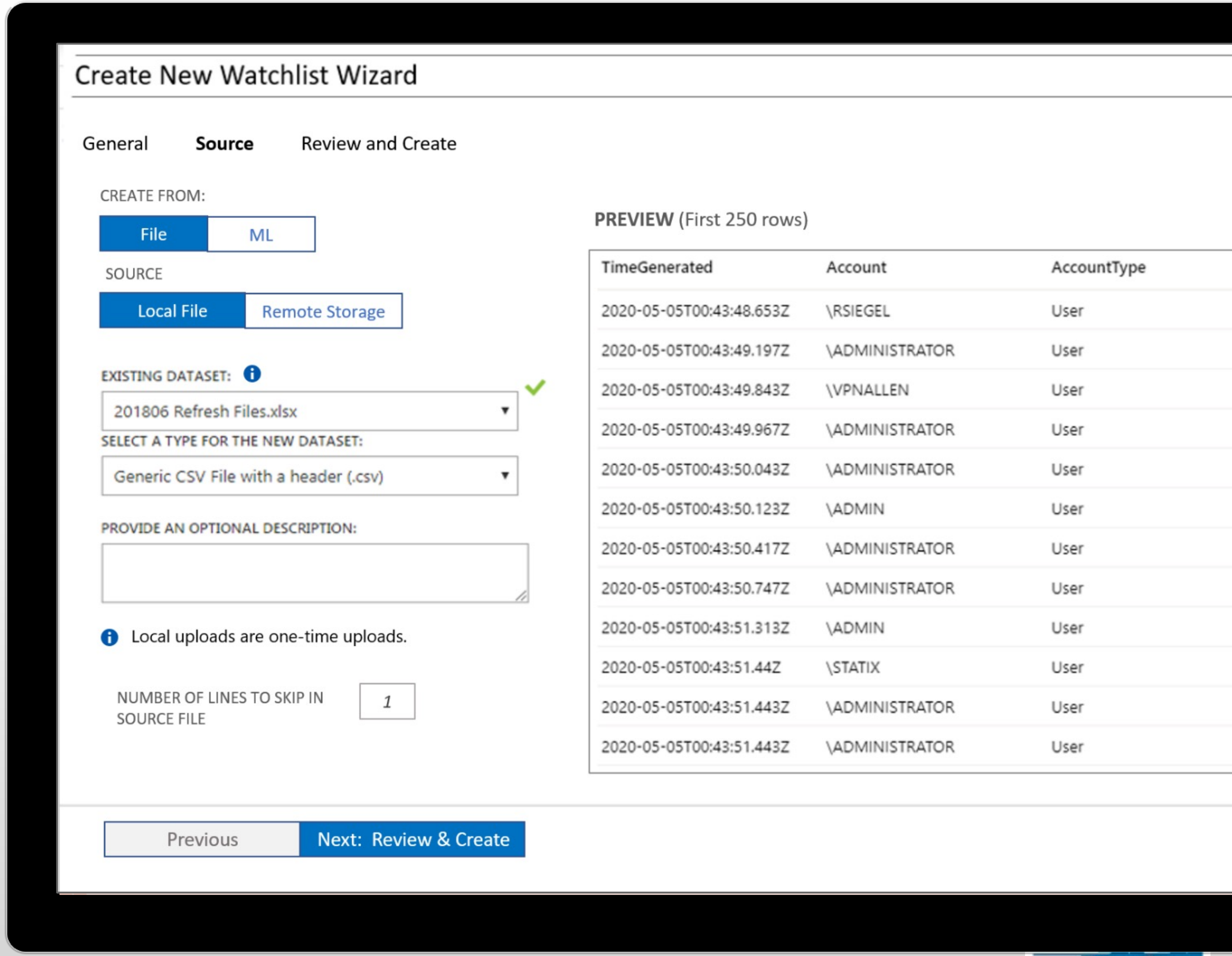
Indicators

Search by Name, Values, Description or Tags

| □ Name ↑↓ | Values | Types | Source ↑↓ | Confidence ↑↓ |
|---|---|---|---|---|
| □ IoC - https://www.bankofnedrask... | https://www.bankofnedraska.com/tag?u... | url | Azure Sentinel | 100 |
| □ IoC - www.hostpr.co | www.hostpr.co | domain-name | Azure Sentinel | 85 |
| □ IoC - 131.45.33.10 | 131.45.33.10 | ipv4-addr | Azure Sentinel | 60 |
| □ Custom Threat Intelligence | 4EA2A2BFE0AC522DA152D481E34E4FA5... | file | SecurityGraph | 100 |
| □ Custom Threat Intelligence | 59AE1D57C6199629A77C117B7EF05B7C... | file | SecurityGraph | 100 |
| □ Custom Threat Intelligence | 1304620C3EBD23A48DA15D7DBE9639D... | file | SecurityGraph | 100 |
| □ Custom Threat Intelligence | 658A2C2D9F76EF0FC43A4BB8E28427B6... | file | SecurityGraph | 100 |
| □ Custom Threat Intelligence | 8DE4B273D61AAA7ED76CDE3E1708E2C... | file | SecurityGraph | 100 |
| □ Custom Threat Intelligence | 4118BFE7CAC599CB88694AF49C34BBD8... | file | SecurityGraph | 100 |
| □ Custom Threat Intelligence | E4E759221D3E2DAE9DFC34938576AE38... | file | SecurityGraph | 100 |
| □ Custom Threat Intelligence | 58A4D8FAE553F59DB84CC35C2A0AE50... | file | SecurityGraph | 100 |
| □ Custom Threat Intelligence | A0573D5FB7972A01C65F9A76A3D98F0E... | file | SecurityGraph | 100 |
| □ Custom Threat Intelligence | 3A51BEF83823D35CB67313FAD6C1471F... | file | SecurityGraph | 100 |
| □ Custom Threat Intelligence | F71AD5662CA18FAFC7DF09F989F99038 | file | SecurityGraph | 100 |

# Use Watchlists to integrate business insights

- Create collections of data for threat hunting and detection (e.g. restricted IPs, trusted systems, critical assets, risky users, vulnerable hosts)
- Incorporate watchlists into analytic rules, hunting queries, workbooks, and more  - create allow/deny lists, add context, and add enrichments
- Upload a CSV file, create automation playbooks upload



Create New Watchlist Wizard

CREATE FROM: File | ML

SOURCE: Local File | Remote Storage

EXISTING DATASET: 201806 Refresh Files.xlsx

SELECT A TYPE FOR THE NEW DATASET: Generic CSV File with a header (.csv)

PROVIDE AN OPTIONAL DESCRIPTION:

Local uploads are one-time uploads.

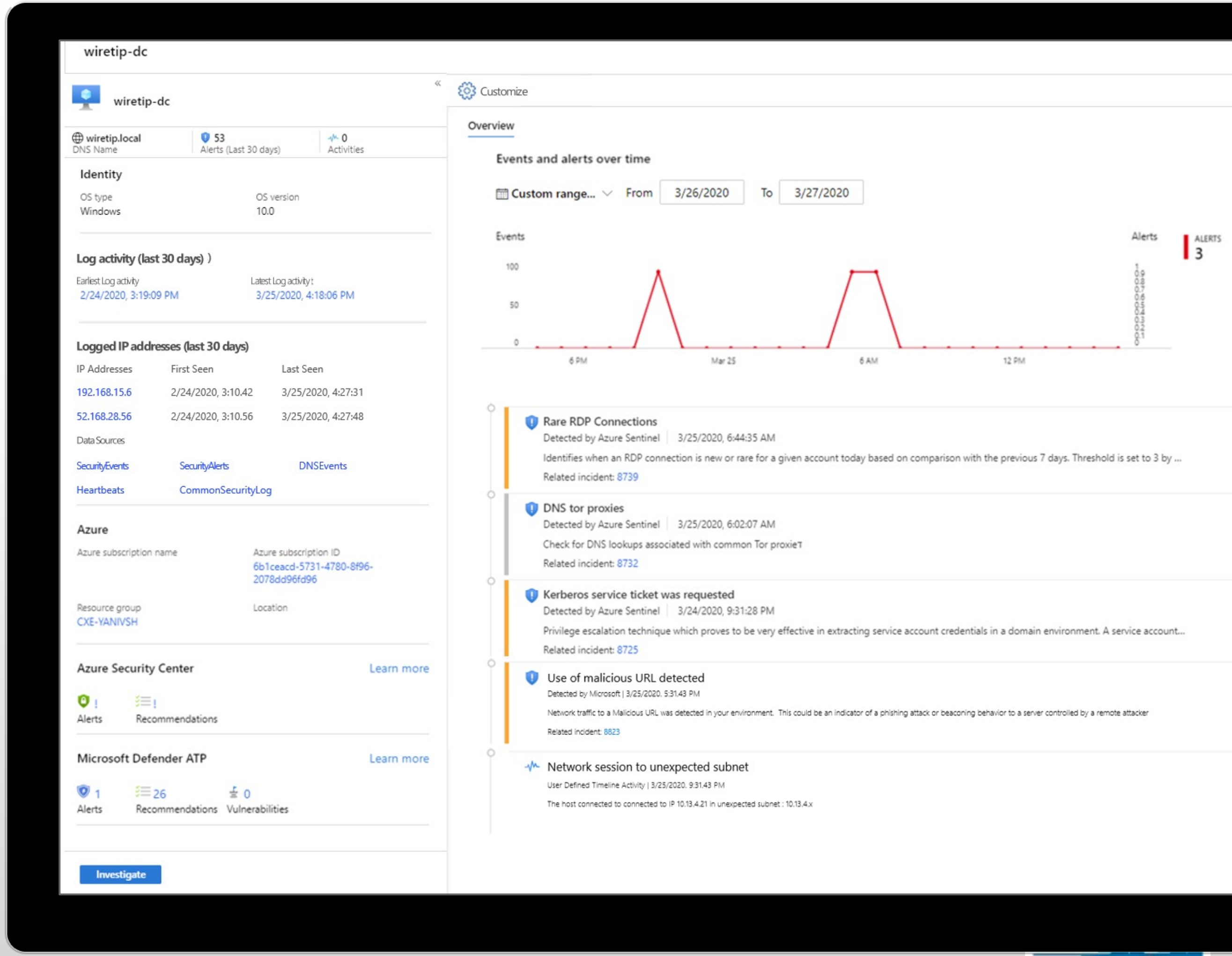
NUMBER OF LINES TO SKIP IN SOURCE FILE: 1

**PREVIEW** (First 250 rows)

| TimeGenerated | Account | AccountType |
|---|---|---|
| 2020-05-05T00:43:48.653Z | \RSIEGEL | User |
| 2020-05-05T00:43:49.197Z | \ADMINISTRATOR | User |
| 2020-05-05T00:43:49.843Z | \VPNALLEN | User |
| 2020-05-05T00:43:49.967Z | \ADMINISTRATOR | User |
| 2020-05-05T00:43:50.043Z | \ADMINISTRATOR | User |
| 2020-05-05T00:43:50.123Z | \ADMIN | User |
| 2020-05-05T00:43:50.417Z | \ADMINISTRATOR | User |
| 2020-05-05T00:43:50.747Z | \ADMINISTRATOR | User |
| 2020-05-05T00:43:51.313Z | \ADMIN | User |
| 2020-05-05T00:43:51.44Z | \STATIX | User |
| 2020-05-05T00:43:51.443Z | \ADMINISTRATOR | User |
| 2020-05-05T00:43:51.443Z | \ADMINISTRATOR | User |

# Access unified insights with entity profiles

- Get a complete view of a host or user by bringing together data from multiple sources, including UEBA
- View timeline information across the most relevant data sources
- Use Insights to quickly identify activities of interest
- Customize timeline to tune results and add other data sources
- Link directly to M365 and Azure Defender where relevant for more information



wiretip-dc

wiretip-dc

| | | |
|---|---|---|
| wiretip.local<br>DNS Name | 53<br>Alerts (Last 30 days) | 0<br>Activities |

Identity

| | |
|---|---|
| OS type<br>Windows | OS version<br>10.0 |

Log activity (last 30 days) )

| | |
|---|---|
| Earliest Log activity<br>2/24/2020, 3:19:09 PM | Latest Log activity t<br>3/25/2020, 4:18:06 PM |

Logged IP addresses (last 30 days)

| IP Addresses | First Seen | Last Seen |
|---|---|---|
| 192.168.15.6 | 2/24/2020, 3:10.42 | 3/25/2020, 4:27:31 |
| 52.168.28.56 | 2/24/2020, 3:10.56 | 3/25/2020, 4:27:48 |

Data Sources

SecurityEvents SecurityAlerts DNSEvents
Heartbeats CommonSecurityLog

Azure

| | |
|---|---|
| Azure subscription name | Azure subscription ID<br>6b1ceacd-5731-4780-8f96-2078dd96fd96 |
| Resource group<br>CXE-YANIVSH | Location |

Azure Security Center

| | |
|---|---|
| ! | ! |
| Alerts | Recommendations |

Microsoft Defender ATP

| | | |
|---|---|---|
| 1 | 26 | 0 |
| Alerts | Recommendations | Vulnerabilities |

Events and alerts over time

Custom range... From 3/26/2020 To 3/27/2020

Rare RDP Connections
Detected by Azure Sentinel | 3/25/2020, 6:44:35 AM
Identifies when an RDP connection is new or rare for a given account today based on comparison with the previous 7 days. Threshold is set to 3 by ...
Related incident: 8739

DNS tor proxies
Detected by Azure Sentinel | 3/25/2020, 6:02:07 AM
Check for DNS lookups associated with common Tor proxieٵ
Related incident: 8732

Kerberos service ticket was requested
Detected by Azure Sentinel | 3/24/2020, 9:31:28 PM
Privilege escalation technique which proves to be very effective in extracting service account credentials in a domain environment. A service account...
Related incident: 8725

Use of malicious URL detected
Detected by Microsoft | 3/25/2020. 5:31.43 PM
Network traffic to a Malicious URL was detected in your environment. This could be an indicator of a phishing attack or beaconing behavior to a server controlled by a remote attacker
Related incident: 8823

Network session to unexpected subnet
User Defined Timeline Activity | 3/25/2020. 9.31.43 PM
The host connected to connected to IP 10.13.4.21 in unexpected subnet : 10.13.4.x

# Incidents

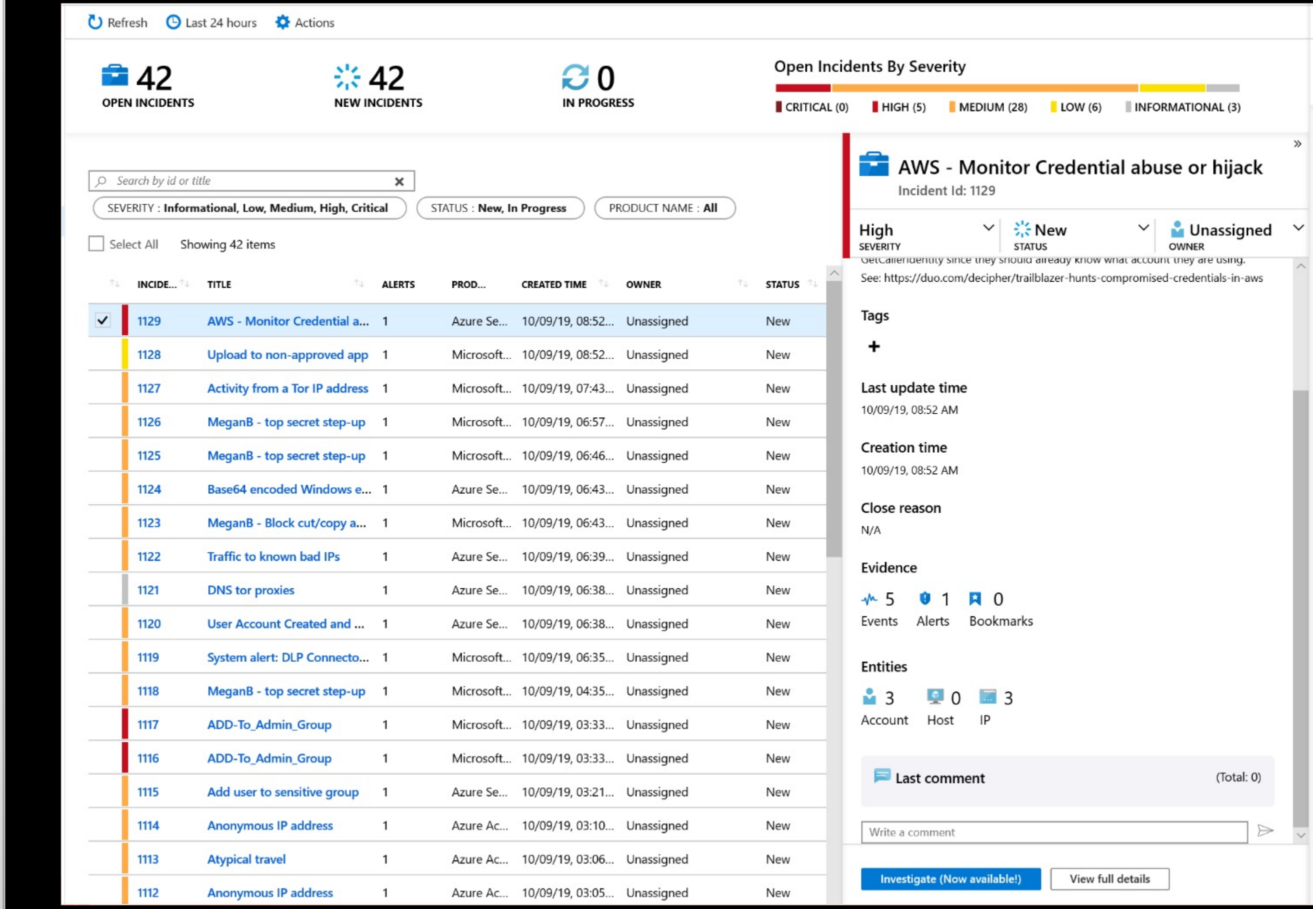
# Start and track investigations from prioritized, actionable security incidents

## 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)

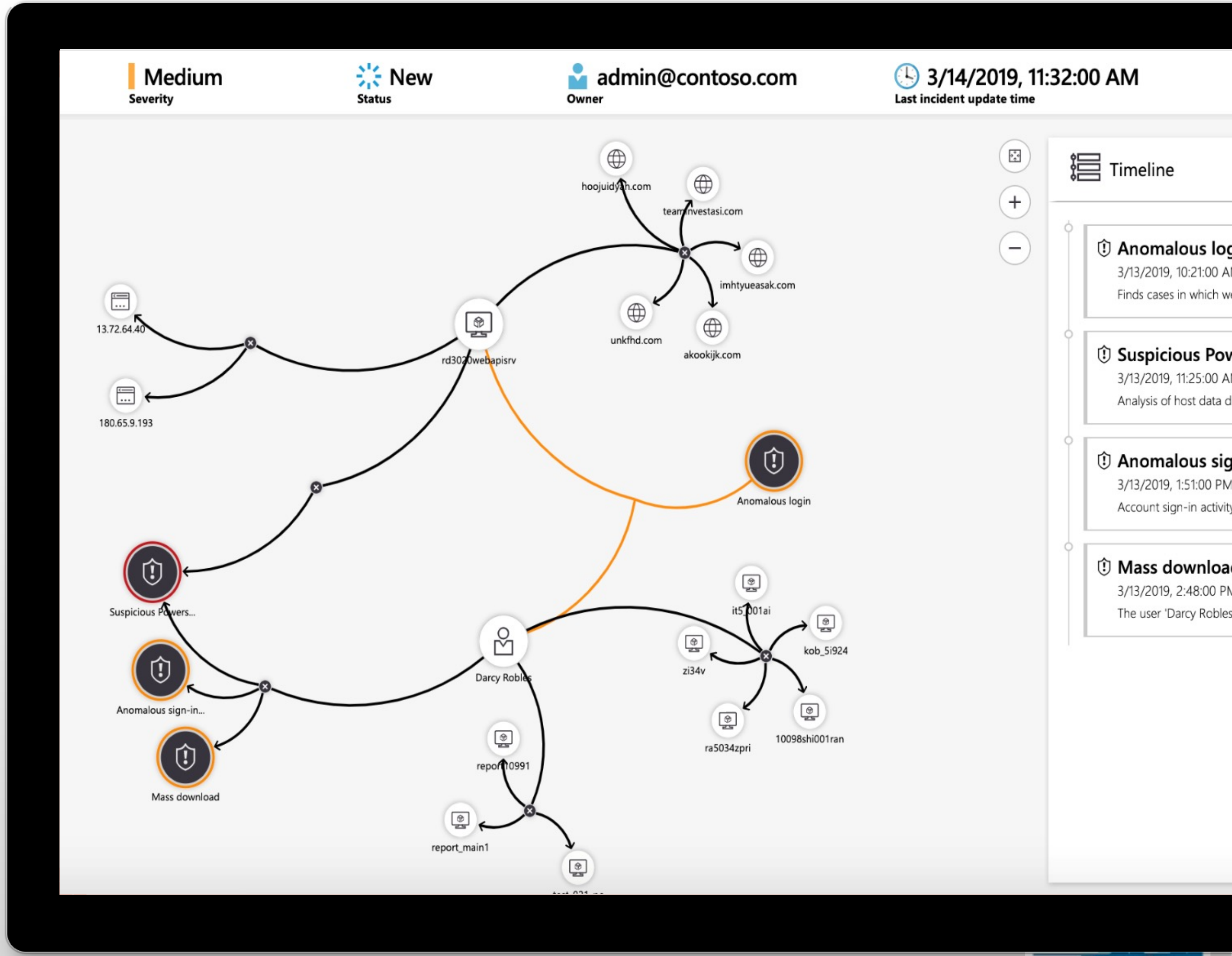
# Visualize the entire attack to determine scope and impact

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 Pov
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

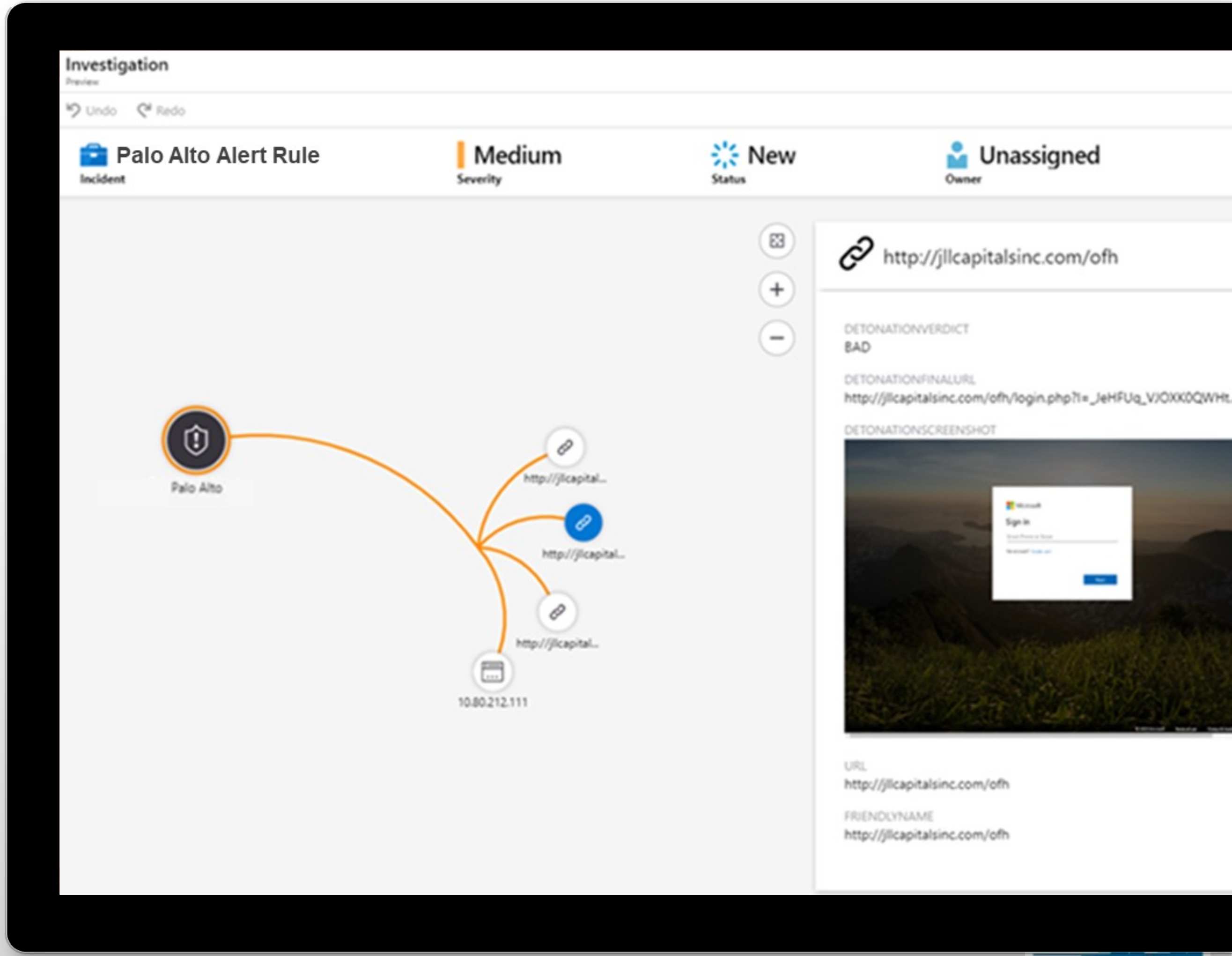
Mass downloa
3/13/2019, 2:48:00 PM
The user 'Darcy Robles

# 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)



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

# Automation

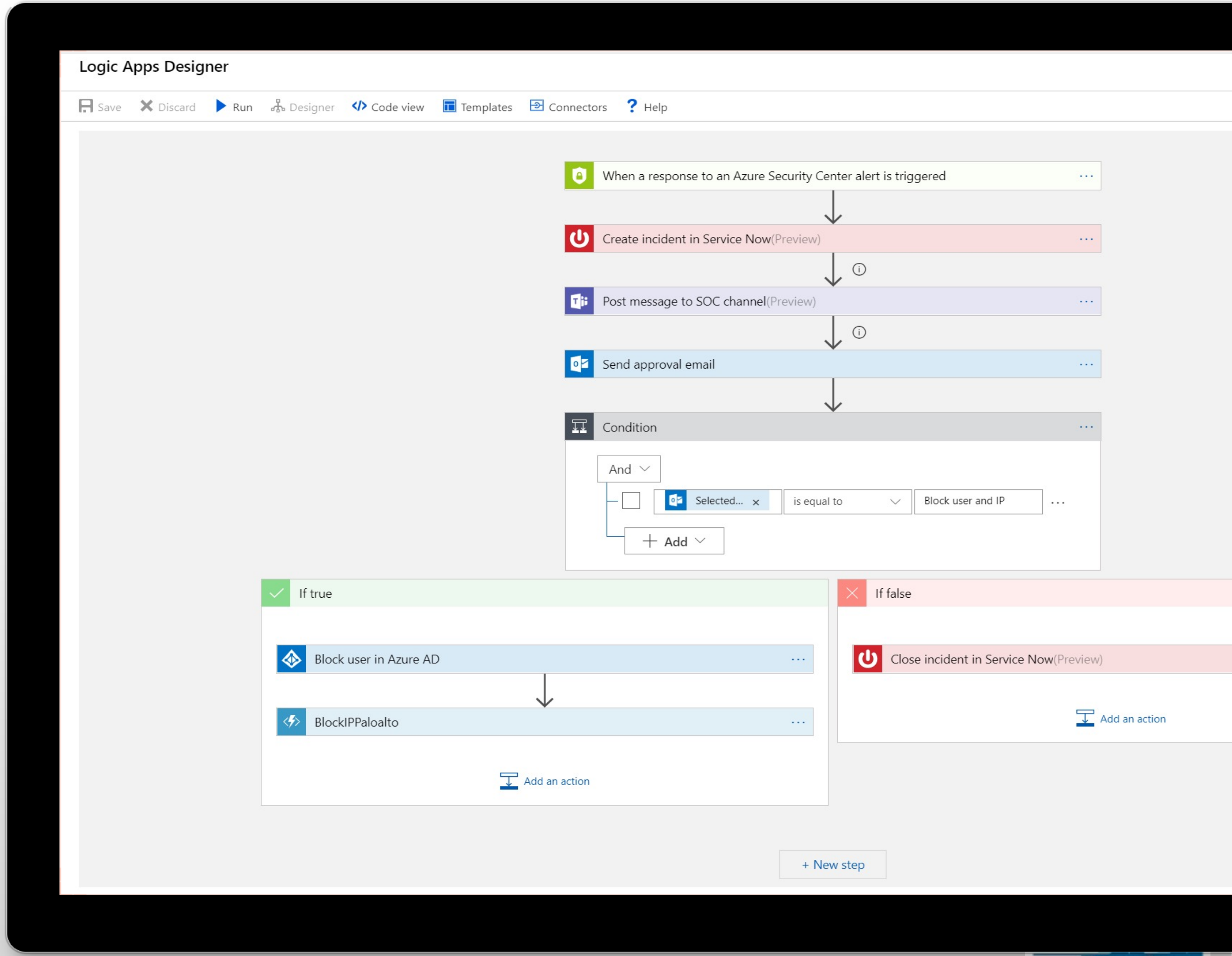
# Automate and orchestrate security operations using integrated Azure Logic Apps

**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**



Logic Apps Designer

When a response to an Azure Security Center 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

BlockIPPaloalto

Add an action

If false

Close incident in Service Now(Preview)

Add an action

+ New step

# 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

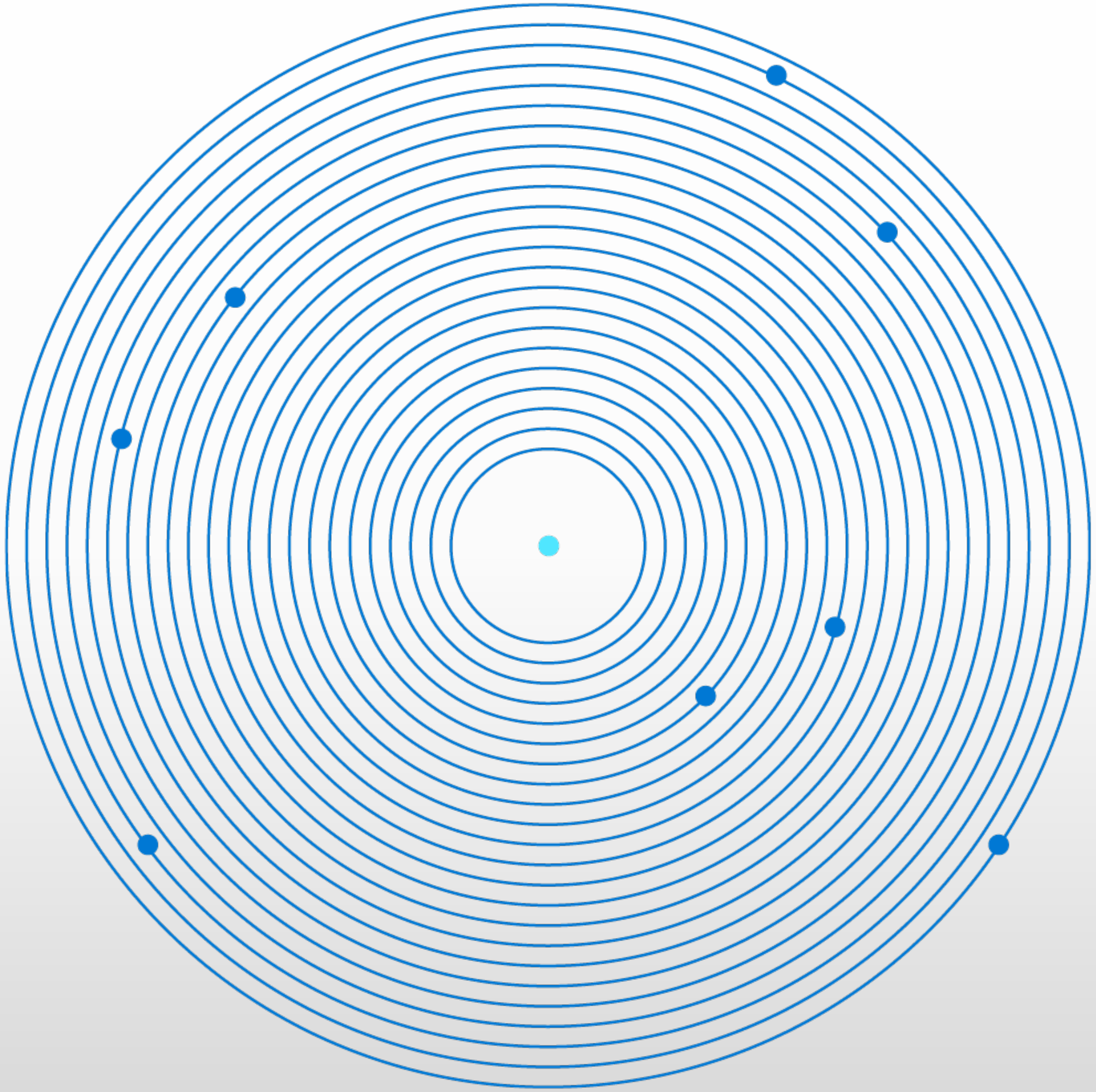
Trigger Conditional Access

Isolate Machine

Microsoft Azure

Microsoft Services and Licensing

# Demo



Metro Systems Corporation Public Company Limited

# Product Roadmap

## Data Collection

Additional data connectors

Collection methods and pipelines

Normalization

Filtering

## Analytics + Intelligence

Anomaly detections

MITRE ATT&CK coverage

MS Threat Intelligence

Near real-time detections

## Automation

Alert/Incident grouping and triage

Automation rules

Additional automation playbooks

## Enterprise/Partner Ready

Cross-workspace, cross-tenant

Management (RBAC, APIs, ..)

Geo footprint

Add-on marketplace

**Better together integration with Microsoft 365 and Azure Defender.**

Microsoft Services and Licensing

# 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

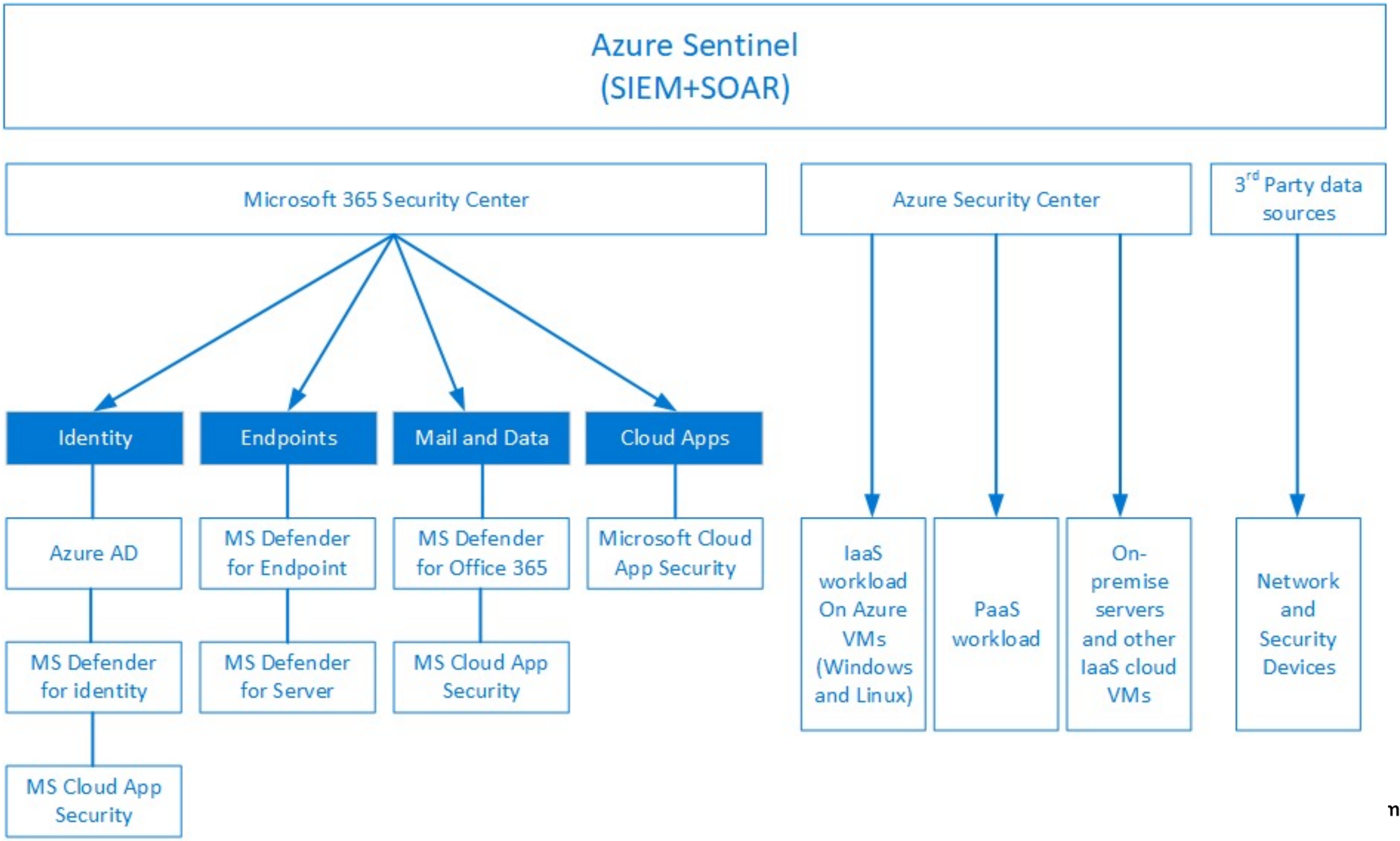
Microsoft Azure

MSL+

Microsoft Services and Licensing

# Thank you.

Metro Systems Corporation Public Company Limited



Azure Sentinel
(SIEM+SOAR)

Microsoft 365 Security Center

Identity

Azure AD

MS Defender for identity

MS Cloud App Security

Endpoints

MS Defender for Endpoint

MS Defender for Server

Mail and Data

MS Defender for Office 365

MS Cloud App Security

Cloud Apps

Microsoft Cloud App Security

Azure Security Center

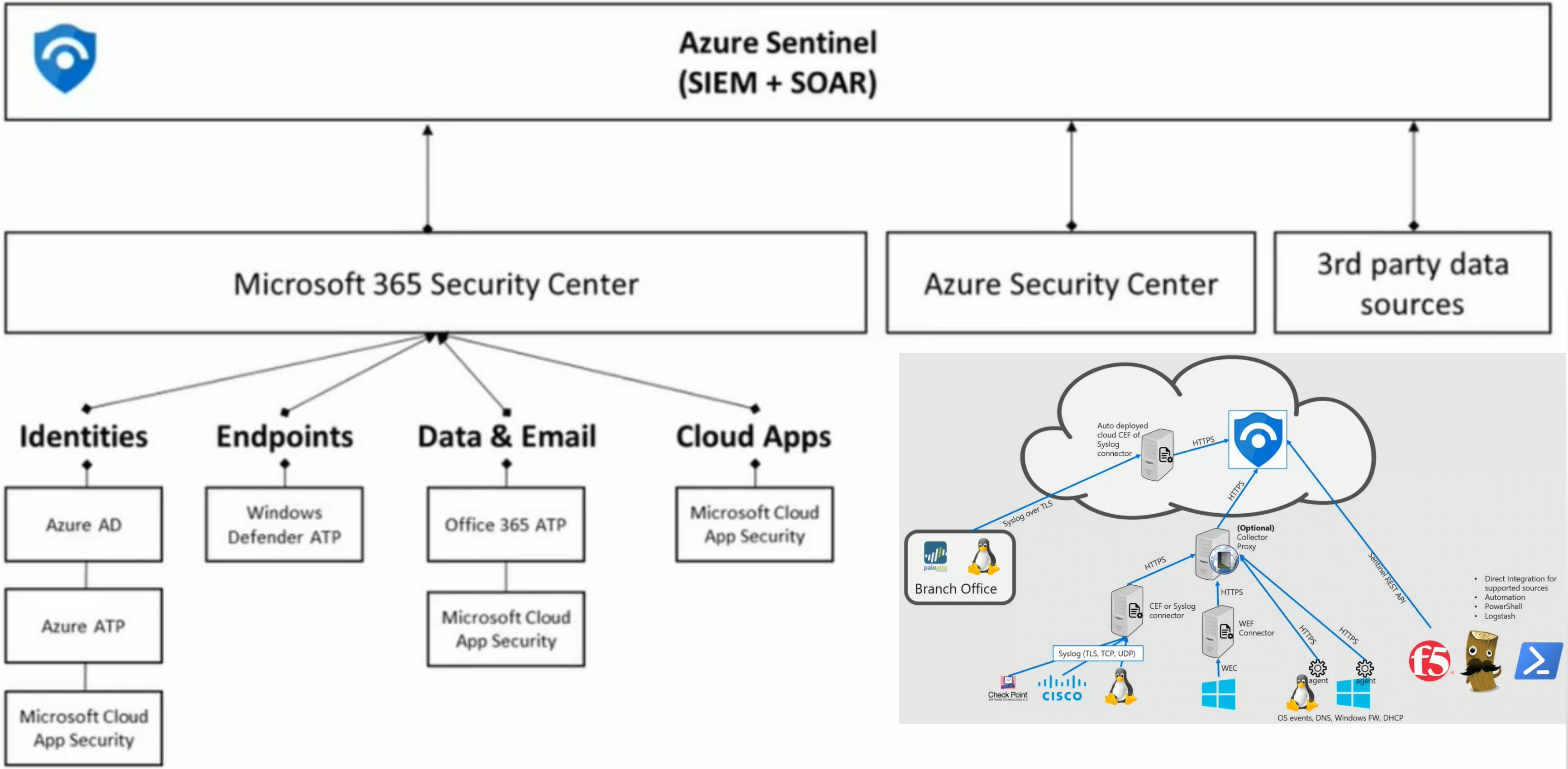
IaaS workload On Azure VMs (Windows and Linux)

PaaS workload

On-premise servers and other IaaS cloud VMs

3rd Party data sources

Network and Security Devices



Azure Sentinel
(SIEM + SOAR)

Microsoft 365 Security Center

Azure Security Center

3rd party data sources

Identities

Azure AD

Azure ATP

Microsoft Cloud App Security

Endpoints

Windows Defender ATP

Data & Email

Office 365 ATP

Microsoft Cloud App Security

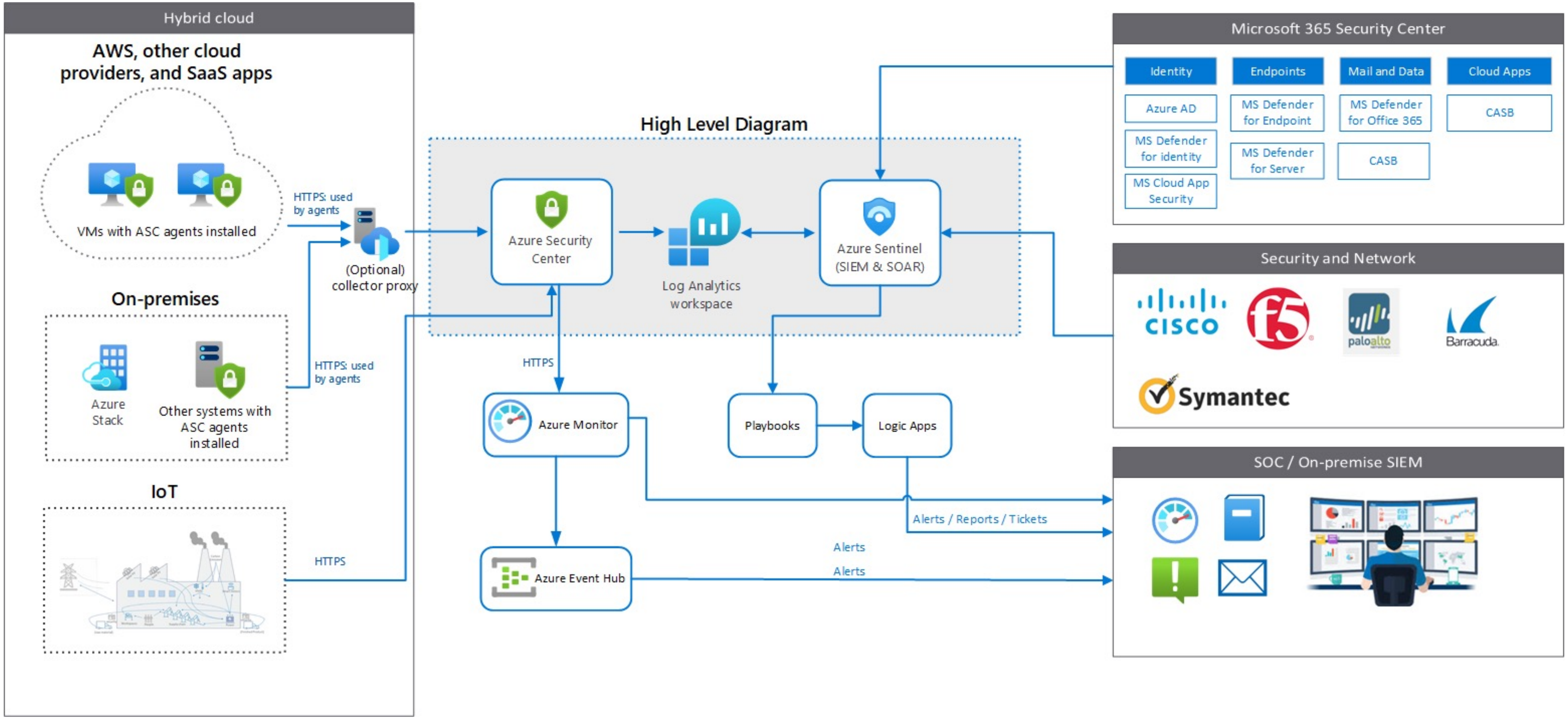
Cloud Apps

Microsoft Cloud App Security

- Direct Integration for supported sources
- Automation
- PowerShell
- Logstash

# High Level Diagram

Microsoft Services and Licensing



Hybrid cloud

AWS, other cloud providers, and SaaS apps

VMs with ASC agents installed

HTTPS: used by agents

(Optional) collector proxy

On-premises

Azure Stack

Other systems with ASC agents installed

HTTPS: used by agents

IoT

HTTPS

High Level Diagram

Azure Security Center

Log Analytics workspace

Azure Sentinel (SIEM & SOAR)

HTTPS

Azure Monitor

Azure Event Hub

Playbooks

Logic Apps

Alerts / Reports / Tickets

Alerts

Alerts

Microsoft 365 Security Center

| Identity | Endpoints | Mail and Data | Cloud Apps |
|---|---|---|---|
| Azure AD | MS Defender for Endpoint | MS Defender for Office 365 | CASB |
| MS Defender for identity | MS Defender for Server | CASB | |
| MS Cloud App Security | | | |

Security and Network

cisco

f5

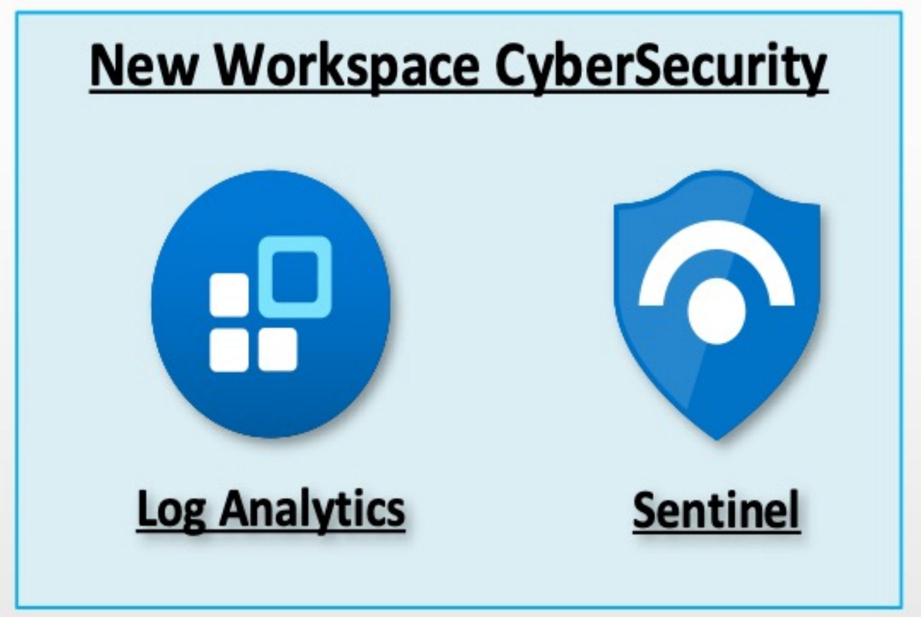
paloalto

Barracuda

Symantec

SOC / On-premise SIEM

# Centralized management Design



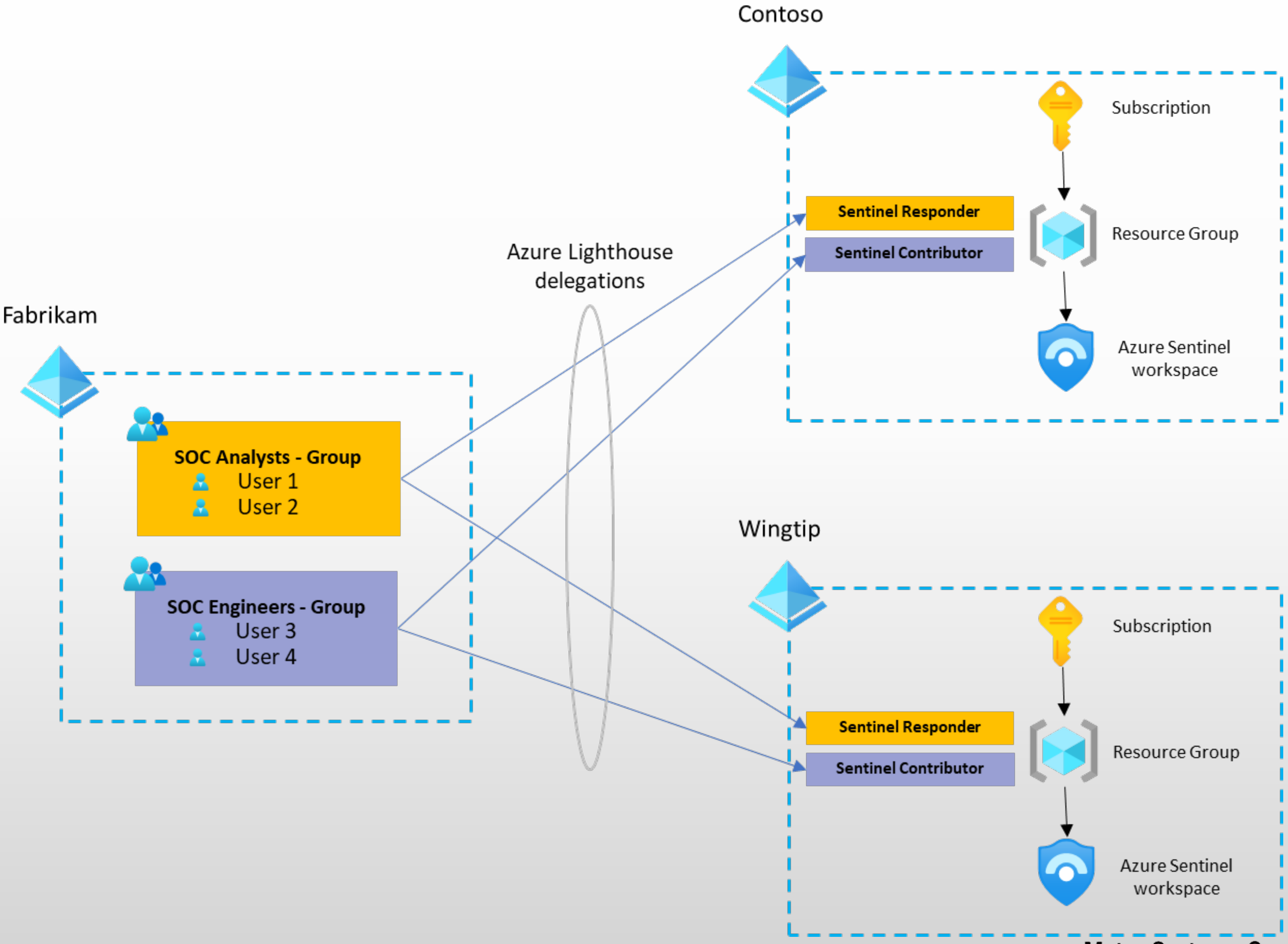
Design:

- Single log analytic and Sentinel and to be separated operational and security log (if require)
- Log Analytics workspace to Azure Sentinel connection is 1-to-1
- Data from multiple workspaces, resource  groups, subscriptions, tenants will be sent to 1 Log Analytics workspace
- Manage subscription via Azure lighthouse

Key concern:

- All inbound (ingress) data transfers to Azure data centers from, for example, on-premises resources or other clouds, are free. However, Azure outbound (egress) data transfers from one Azure region to another Azure region, incur charges
- All outbound traffic between regions is being charged

# Azure Lighthouse – Managed Service



Metro Systems Corporation Public Company Limited

# Use Cases

| No | Connector | Use case | Description: |
|---|---|---|---|
| 1 | Azure Active Directory | Malicious administrative activity / brute force | An incidents of this type indicate that an anomalous number of administrative activities were performed in a single session following a suspicious Azure AD sign-in from the same account. This also indicates that an account with administrative privileges may have been compromised.<br>The permutations of suspicious Azure AD sign-in alerts with the suspicious cloud app administrative activity alert are:<br>• Impossible travel to an atypical location<br>• Sign-in event from an unfamiliar<br>• Sign-in event from an infected device leading to suspicious<br>• Sign-in event from an anonymous IP address<br>• Sign-in event from user with leaked credentials |

**Data connector sources:** Microsoft Cloud App Security, Azure Active Directory Identity Protection

# Use Cases

| No | Connector | Use case | Description: |
|---|---|---|---|
| 2 | AAD, O365, Azure Activity, M365 Defender and Azure Security center | Event, alert and automation open incident ticket in ServiceNow | Take an incidents /alert from connector. The objective is to visualize and get analysis of what's happening on customer environment. |

**Data connector sources:** Microsoft 365 Defender family

# Use Cases

| No | Connector | Use case | Description: |
|---|---|---|---|
| 3 | MDI and MDE | Suspicious PowerShell command line following suspicious sign-in | The incidents of this type indicate that a user executed potentially malicious PowerShell commands following a suspicious sign-in to an Azure AD account. This provides a high-confidence indication that the account noted in the alert description has been compromised and further malicious actions were taken. Attackers often leverage PowerShell to execute malicious payloads in memory without leaving artifacts on the disk, in order to avoid detection by disk-based security mechanisms such as virus scanners. The permutations of suspicious Azure AD sign-in alerts with the suspicious PowerShell command alert are:<br>•Impossible travel to atypical locations leading to suspicious PowerShell command line<br>•Sign-in event from an unfamiliar location leading to suspicious PowerShell command line<br>•Sign-in event from an infected device leading to suspicious PowerShell command line<br>•Sign-in event from an anonymous IP address leading to suspicious PowerShell command line<br>•Sign-in event from user with leaked credentials leading to suspicious PowerShell command line |

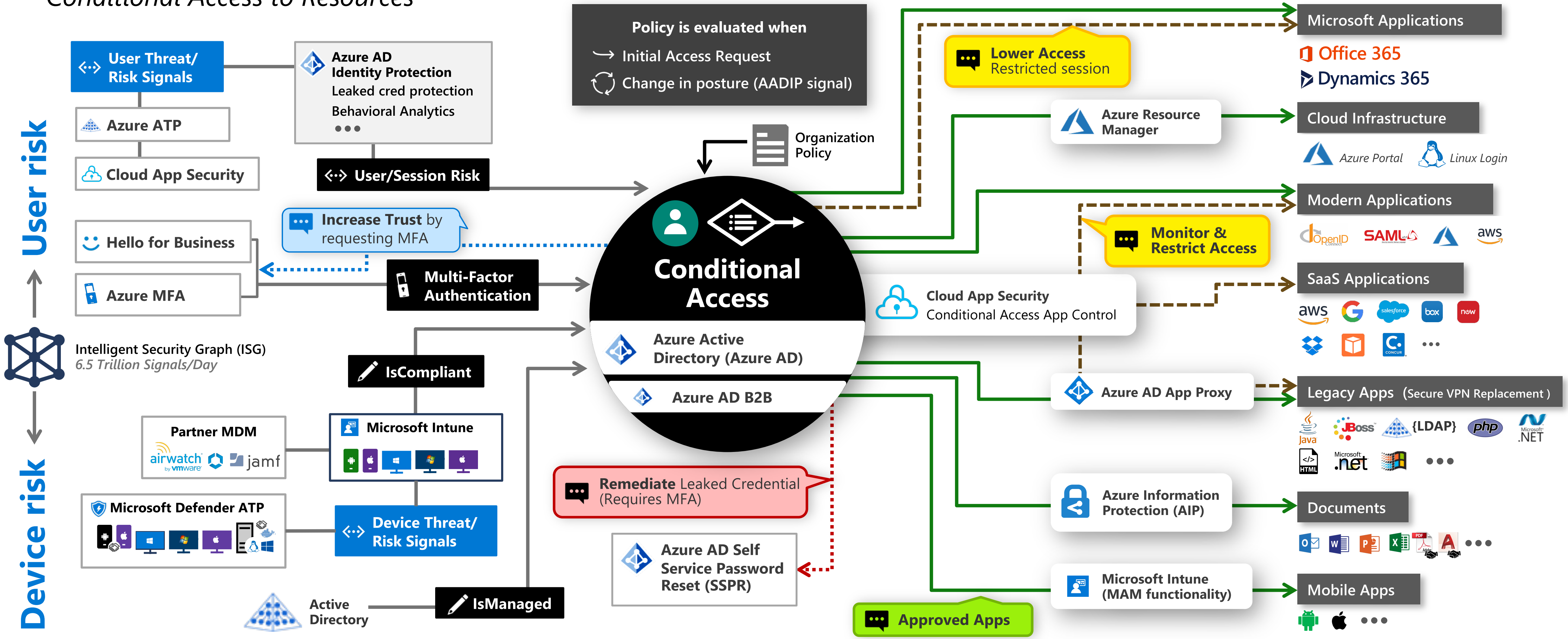
**Data connector sources:** Azure Active Directory Identity Protection, Microsoft Defender for Endpoint (formerly MDATP)

# Zero Trust User Access

*Conditional Access to Resources*

**Legend**

- Full access
- Limited access
- Risk Mitigation
- Remediation Path



User risk

Device risk

User Threat/ Risk Signals

Azure ATP

Cloud App Security

Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
•••

User/Session Risk

Hello for Business

Azure MFA

Increase Trust by requesting MFA

Multi-Factor Authentication

Intelligent Security Graph (ISG)
*6.5 Trillion Signals/Day*

IsCompliant

Partner MDM
airwatch by vmware
jamf

Microsoft Intune

Microsoft Defender ATP

Device Threat/ Risk Signals

Active Directory

IsManaged

Policy is evaluated when
Initial Access Request
Change in posture (AADIP signal)

Organization Policy

Conditional Access

Azure Active Directory (Azure AD)

Azure AD B2B

Remediate Leaked Credential (Requires MFA)

Azure AD Self Service Password Reset (SSPR)

Lower Access
Restricted session

Azure Resource Manager

Monitor & Restrict Access

Cloud App Security
Conditional Access App Control

Azure AD App Proxy

Azure Information Protection (AIP)

Microsoft Intune (MAM functionality)

Approved Apps

Microsoft Applications
Office 365
Dynamics 365

Cloud Infrastructure
*Azure Portal*
*Linux Login*

Modern Applications
OpenID
SAML
aws

SaaS Applications
aws
salesforce
box
now
CONCUR
•••

Legacy Apps (Secure VPN Replacement )
Java
JBoss
{LDAP}
php
.NET
HTML
Microsoft .net
•••

Documents
•••

Mobile Apps
•••

**Signal**
to make an informed decision

**Decision**
based on organizational policy

**Enforcement**
of policy across resources

Q
A