



Weekly Technical Office Hours for Partners

Remote Work in challenging times

Wednesday, April 22, 2020

The meeting will start at
WEST 11:00 - CET 12:00 – EEST 13:00

Technical Office Hours for WE Microsoft Partners:

Remote Work in challenging times



Agenda

1. Introduction
2. How Azure Sentinel can help to secure remote work
3. Q & A
4. Poll – Proposed topics for next session
5. How to get further help
 - Support channels and options

Our Virtual Team



Jing Liu

Cloud Solution Architect (Azure)



Olivier van der Kruijf

Cloud Solution Architect (Azure)



Stefano Ceruti

Partner Tech. Architect (Teams)



Matteo Malagnino

Cloud Solution Architect (Security)



Philippe Goldstein

Partner Tech. Manager



Sara Canteiro

Partner Tech. Architect (Teams)



Aline Harmand

Partner Tech. Strategist



Jos Verlinde

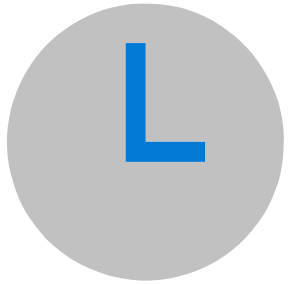
Partner Tech. Architect (Teams)



Toni Willberg

Cloud Solution Architect (Azure)

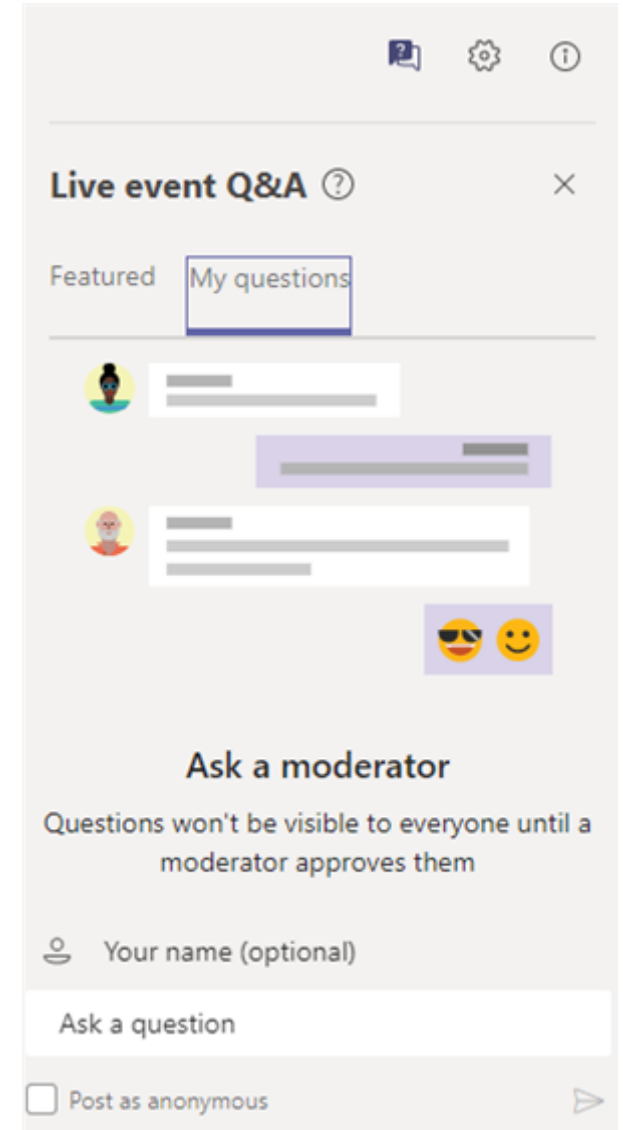
WE Weekly Technical Office Hours – How it works



60 minutes
40 min, presentation
20 min, Q&A



Questions via
chat through
Q&A 



(WEEKLY) Technical Office Hours for WE Microsoft Partners:

Remote Work in challenging times

JOIN
UPCOMING
SESSION



Currently we are receiving a lot of questions from our partners and customers with regards to recommendations and help on working remotely.

To address the **main technical topics** around **working remotely**, Microsoft's Western Europe OCP Technical Team is setting up a series of **Weekly Office Hours for Partners**,

- every **Wednesday** at 12:00 – 13:00 CET (11:00 – 12:00 WEST)
- every **Friday** at 13:00 – 14:00 CET (12:00 – 13:00 WEST)

All sessions will be held in English.

<https://aka.ms/WE-TechOfficeHours>

Next
Session
Details

Upcoming
Sessions

Materials &
Recordings

Other
Resources

Feedback
Form

Wednesdays



Fridays



Don't miss a session;

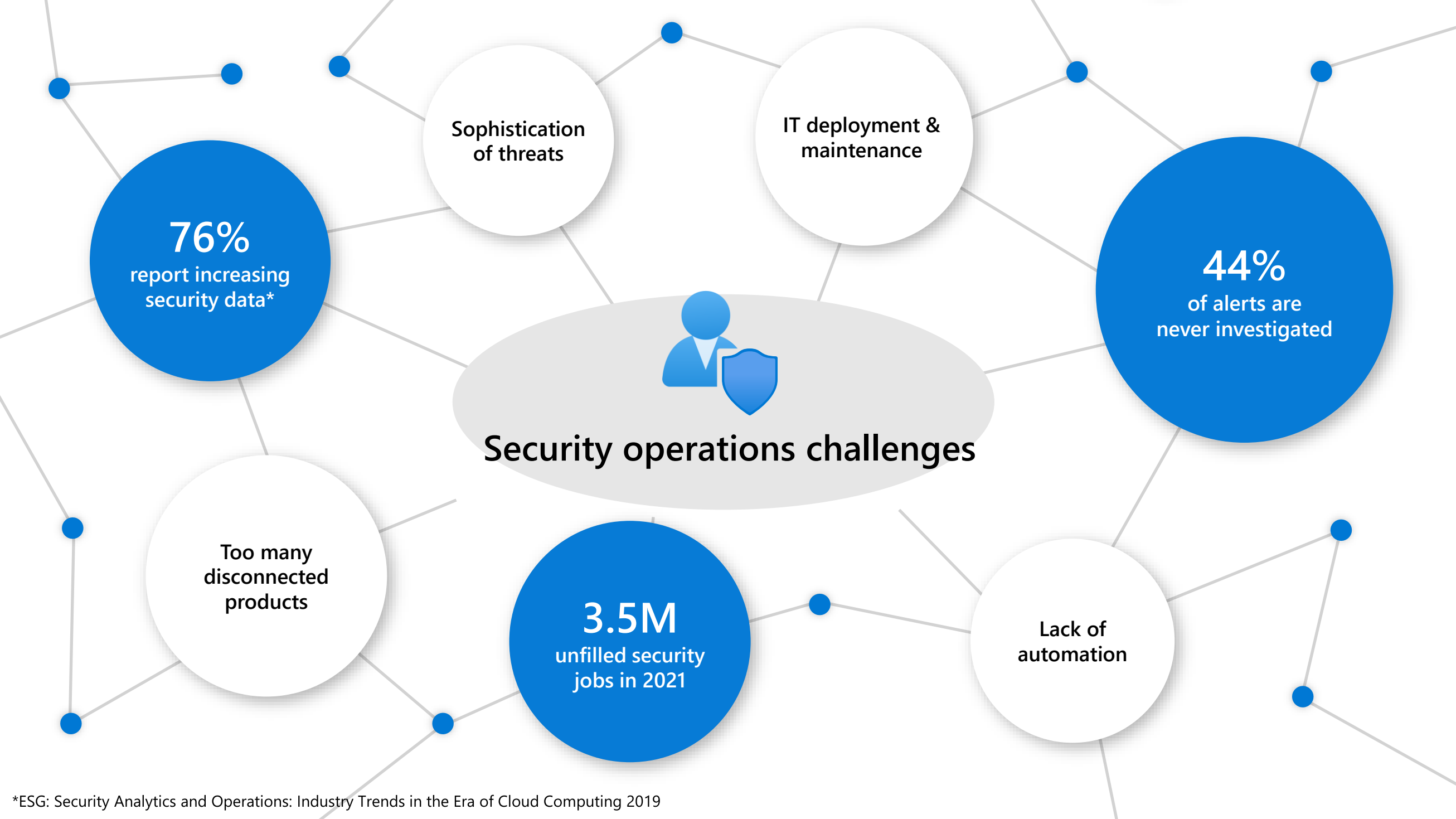
Update your calendar by
using the invites above.

Hey, This landing page is actually a PowerPoint. Click through to see the next slides.

How Azure Sentinel can help to secure remote work



Olivier van der Kruijf
Cloud Solution Architect (Azure)



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

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



Security
Operations Team



Cloud + Artificial Intelligence

Azure Sentinel



A cloud SIEM

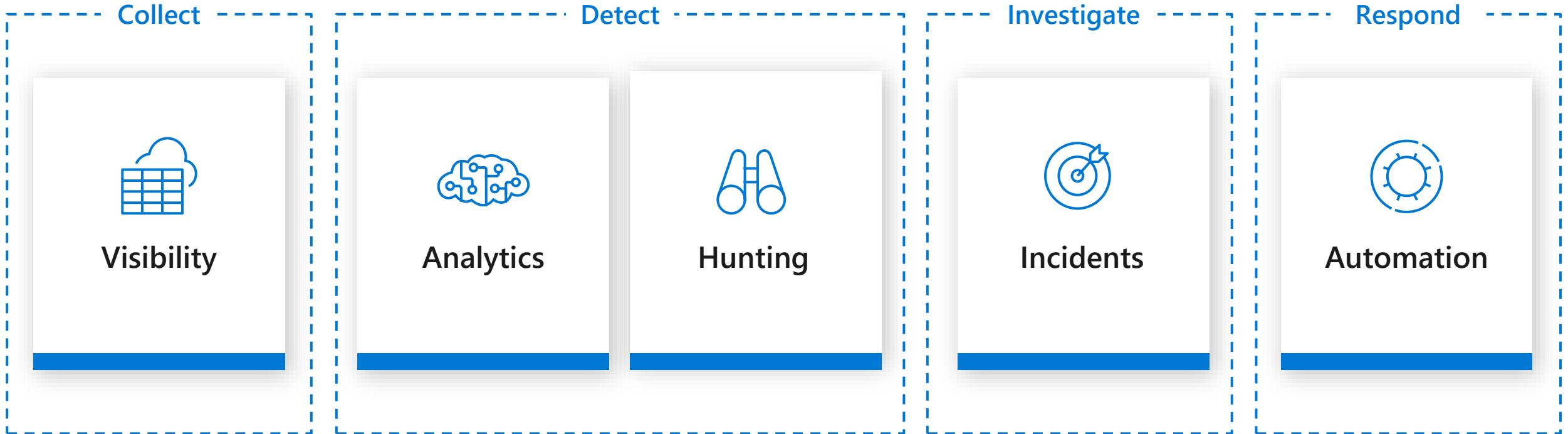


For the Cloud



And for on premises

End-to-end solution for security operations



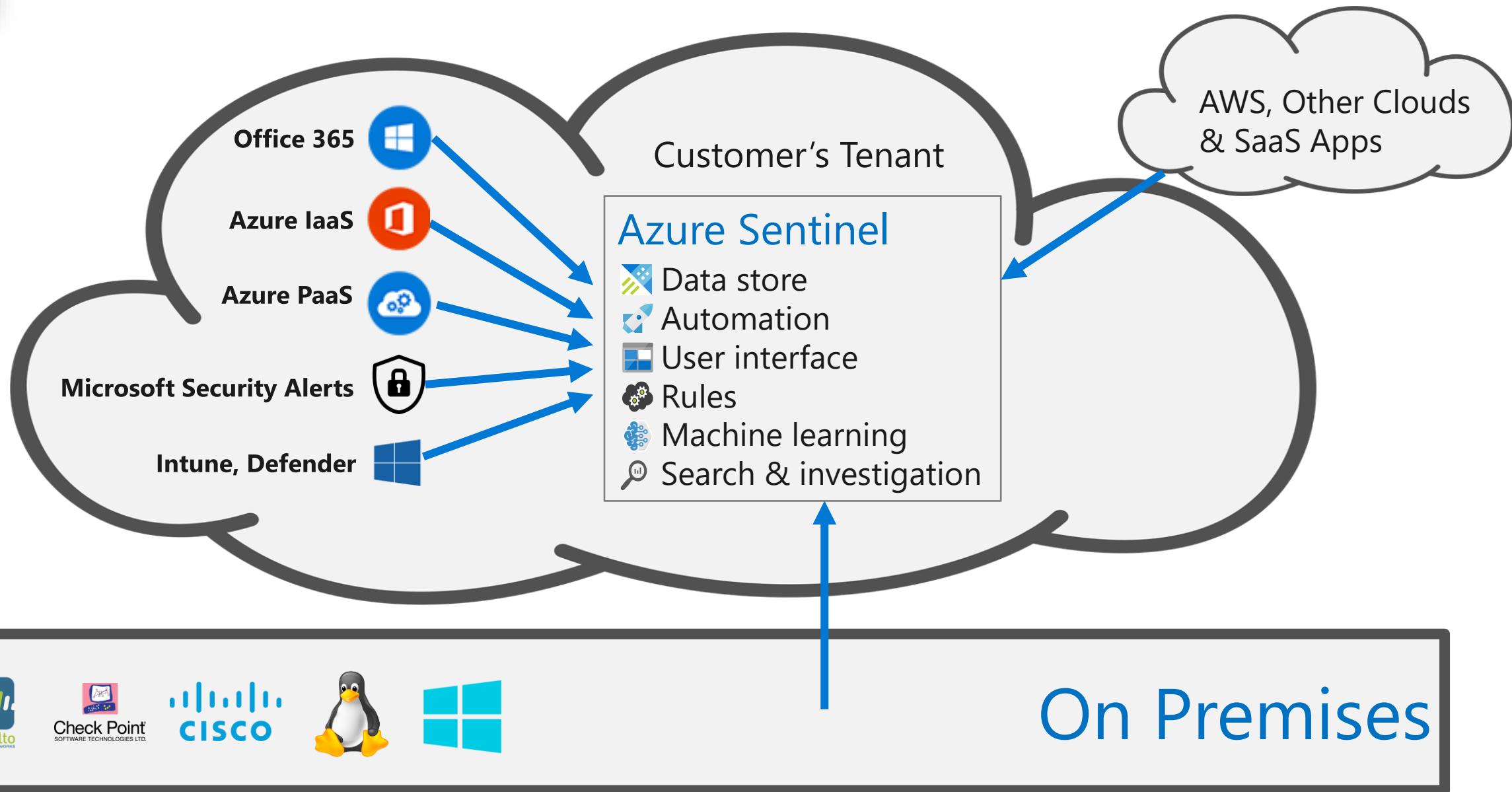
Microsoft Security Advantage

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





1 Collect security data at cloud scale from any source





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



Workbooks: interactive dashboarding

Sign-in Analysis



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

Sign-ins by Location

🔍 Search

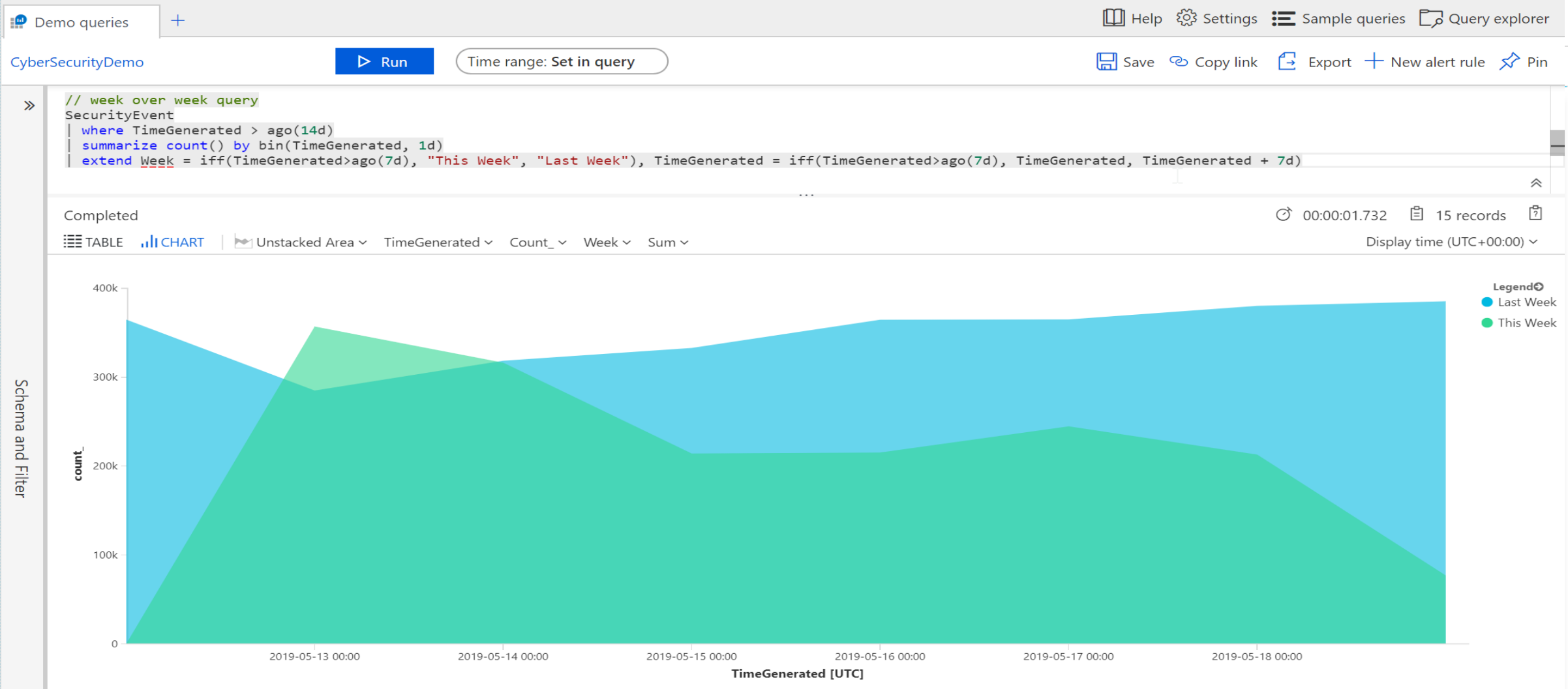
Name	Sign-in Count	Trend	Failure Count	Interrupt Count
▶ US	2.349K		77	67
▶ BE	566		3	8
▶ GB	421		30	24
▶ AU	241		22	65
▶ IL	203		0	5

Location Sign-in details

🔍 Search

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

Chart search results





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

The screenshot displays the Microsoft Sentinel 'Active rules' interface. At the top, there's a '51 Active rules' indicator and a 'RULES BY SEVERITY' bar chart showing counts for HIGH (12), MEDIUM (26), LOW (9), and INFORMATIONAL (4). Below this, a search bar and filters for SEVERITY, TYPE, and TACTICS are visible. The main table lists various rules, with 'Known Phosphorus group domains' selected. The right-hand pane provides details for this rule, including its description, required data sources, tactics, and the KQL query used for detection.

NAME	RULE TYPE	REQUIRED DATA SOURCES	TACTICS
Known Phosphorus group domains	Scheduled	DNS (Pr...+2)	Command and Control
Create incidents based on Azure Acti...	Microsoft Sec...		
Advanced Multistage Attack...	Fusion		
Create incidents based on A...	Microsoft Sec...		
Create incidents based on Microsoft ...	Microsoft Sec...		
Known Strontium group domains	Scheduled	DNS (Pr...+2)	Command and Control
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 Control

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", "se  
accounts-web-mail.com", "customer-certificate.com", "se  
yahoo-verification.net", "yahoo-verify.net", "outlook-v
```

Create rule

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

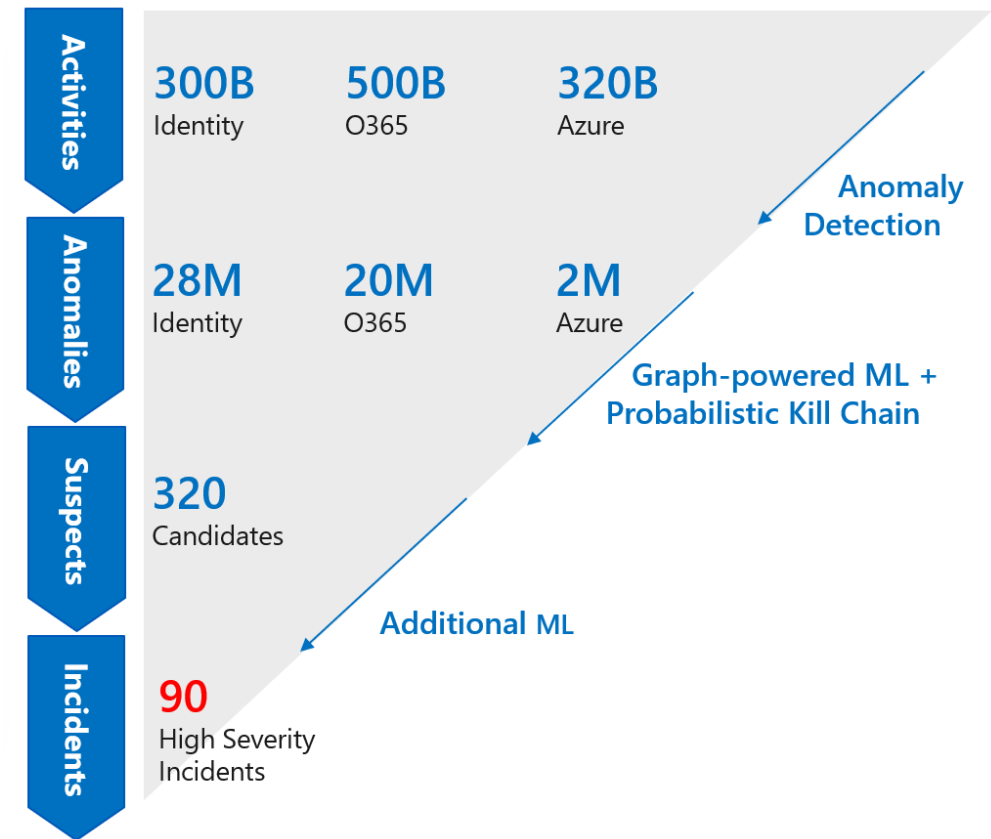
Use built-in models – no ML experience required

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)





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

Integrate with your ticketing system

The screenshot displays a security incident management interface. At the top, there are summary cards for '42 OPEN INCIDENTS', '42 NEW INCIDENTS', and '0 IN PROGRESS'. A bar chart titled 'Open Incidents By Severity' shows the distribution: CRITICAL (0), HIGH (5), MEDIUM (28), LOW (6), and INFORMATIONAL (3). Below this is a search bar and filters for severity, status, and product name. A table lists 42 incidents, with the first incident selected. The right sidebar provides details for the selected incident, including its title, severity, status, owner, and a list of related entities.

INCIDENT ID	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

GetCaierAgency 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)

Write a comment

Investigate (Now available!) | View full details

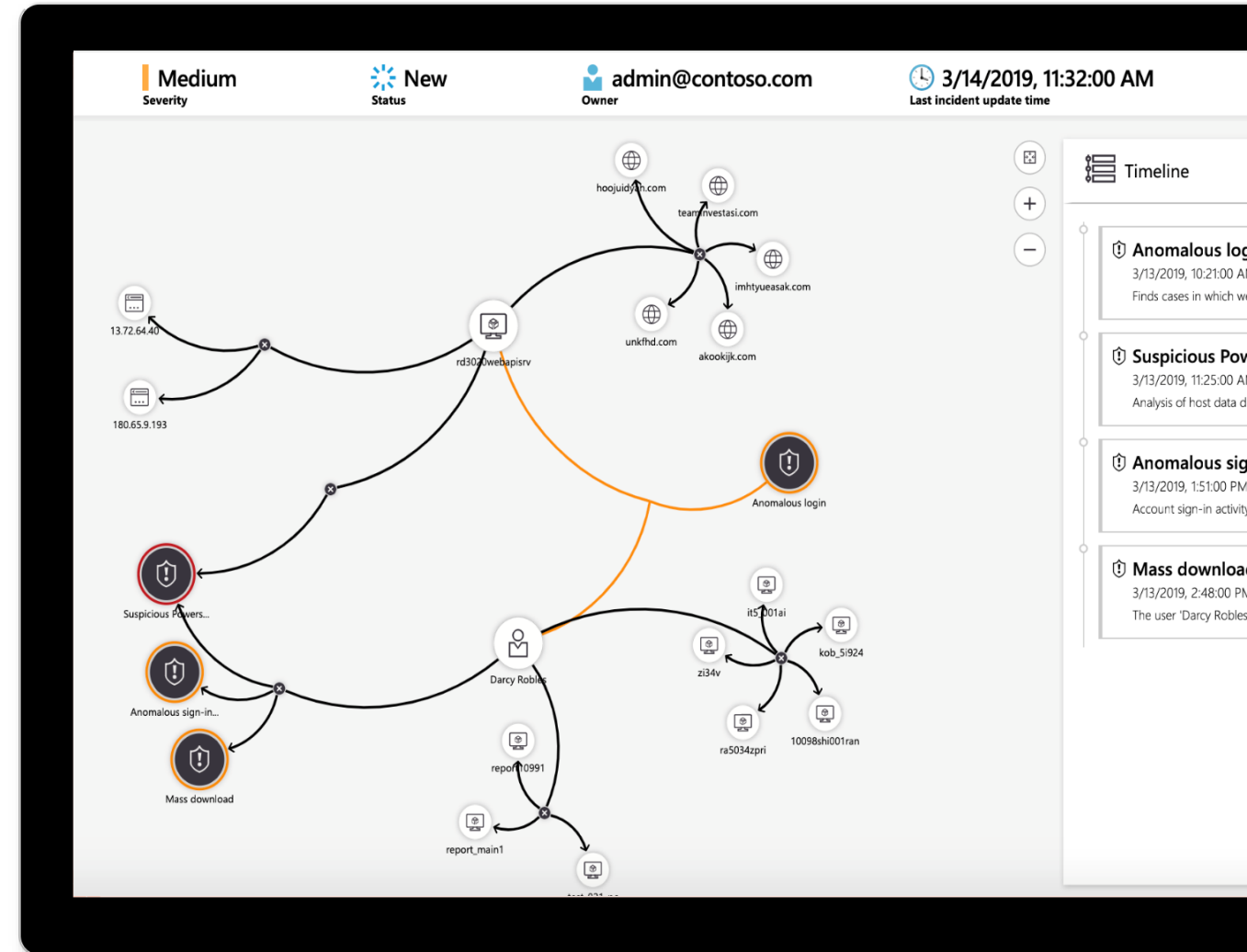
6 Visualize the entire attack to determine scope and impact

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

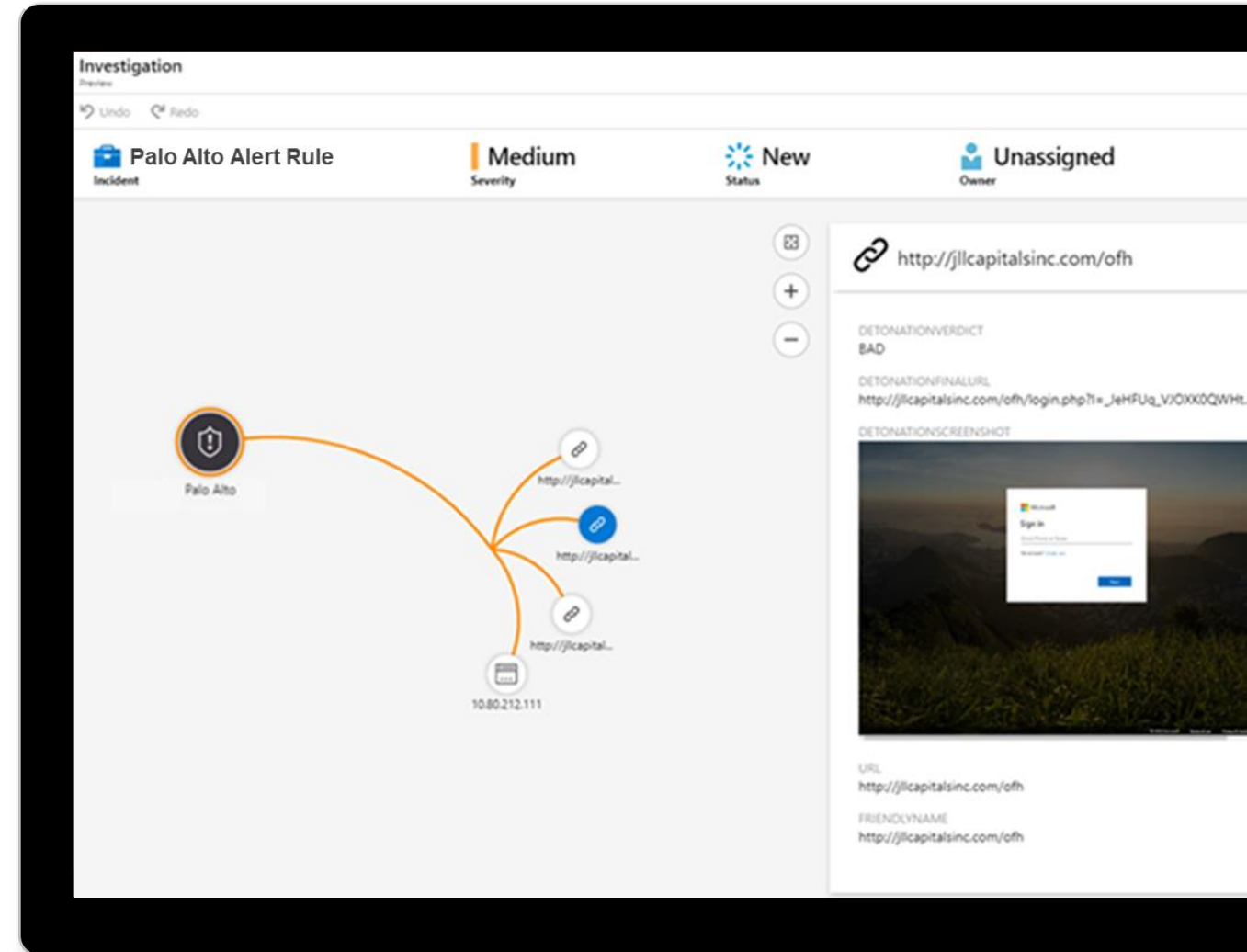


7 Gain deeper insight with built-in automated detonation

Configure URL Entities in analytics rules

Automatically trigger URL detonation

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



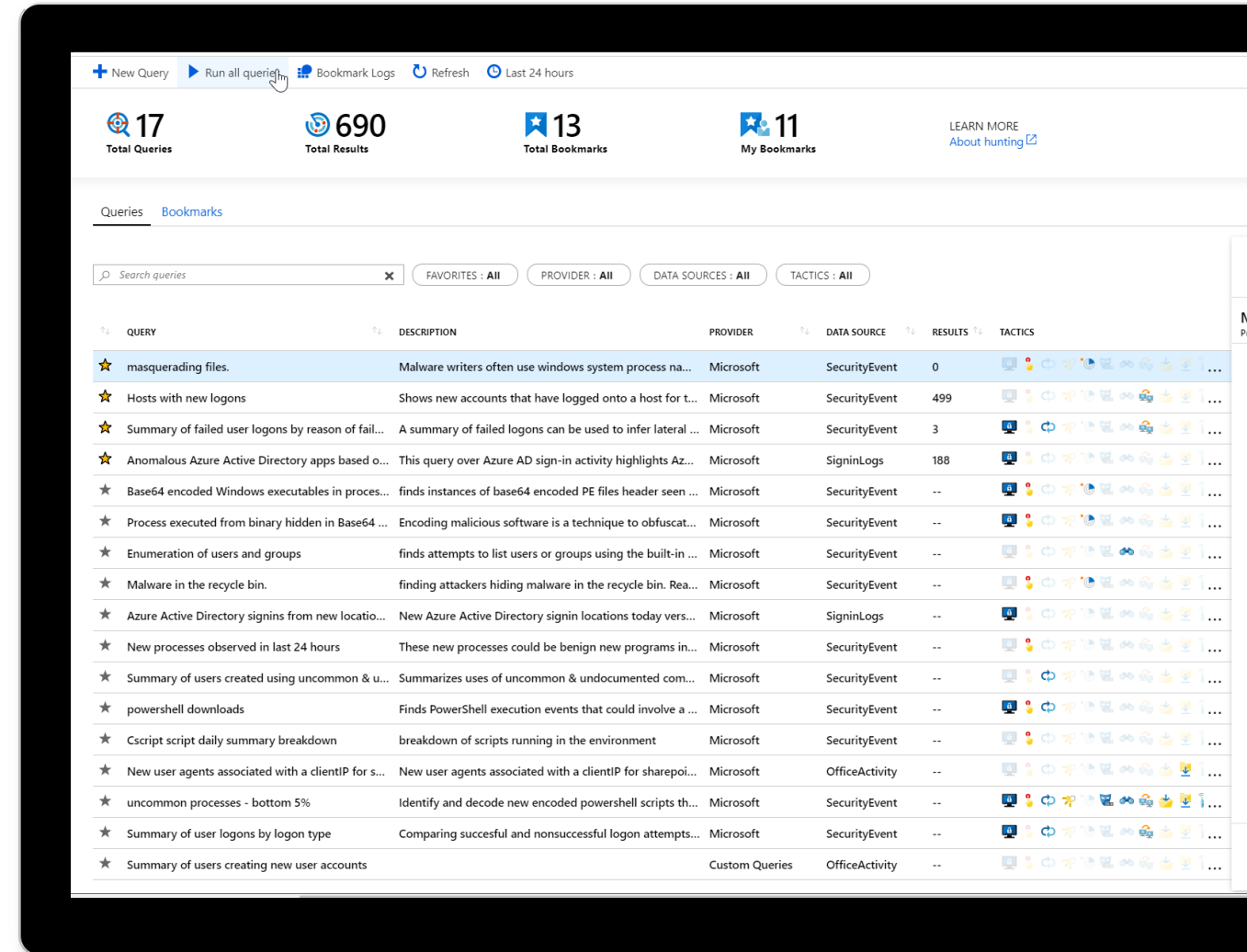


8 Start hunting over security data with fast, flexible queries

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

Customize and create your own hunting queries using KQL

Integrate hunting and investigations



9

Explore data sets

Search using free text or fields

Tabulate your data

Visualize query results

Automatically detect and plot anomalies in data



10

Use Jupyter notebooks for advanced hunting

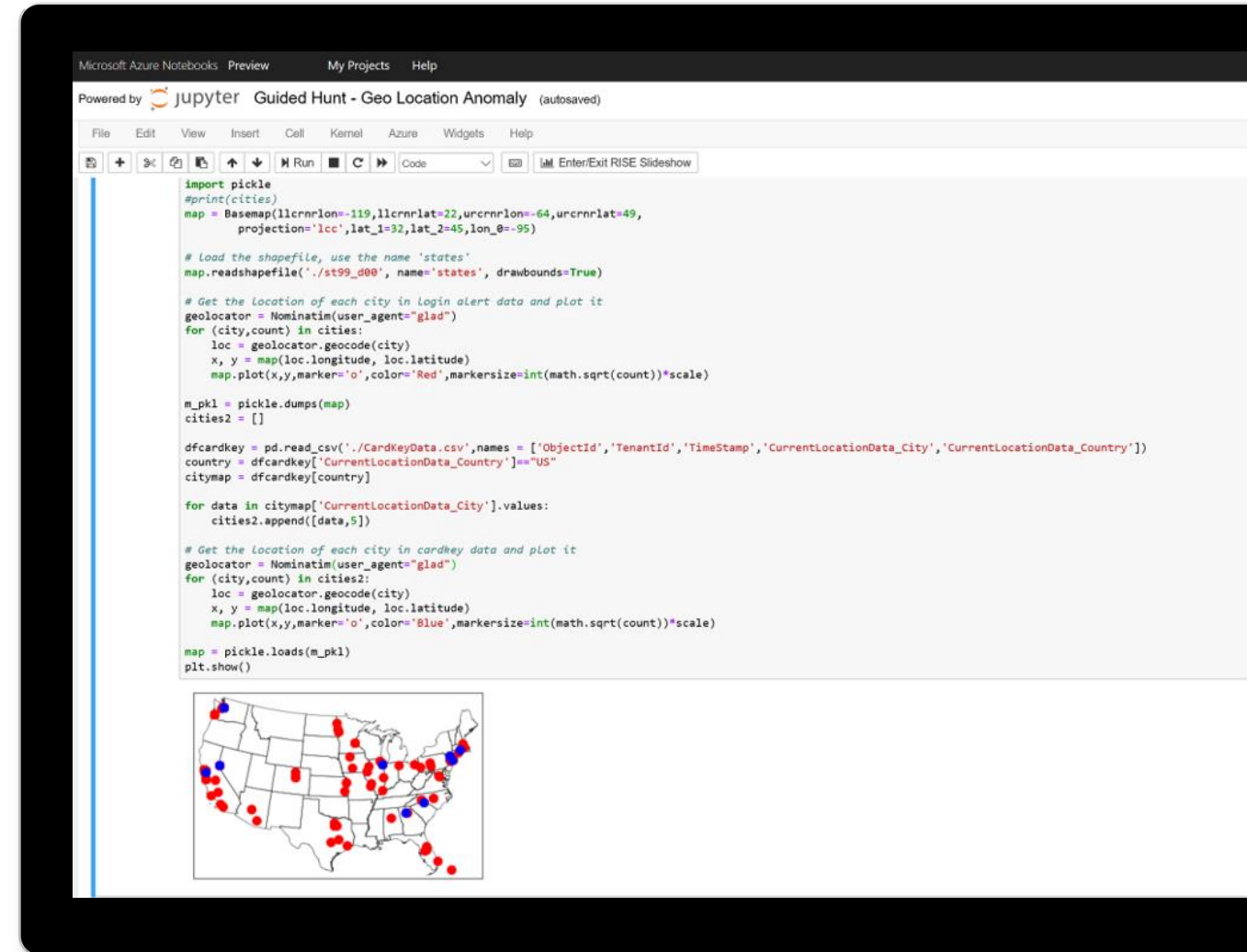
Run in the Azure cloud

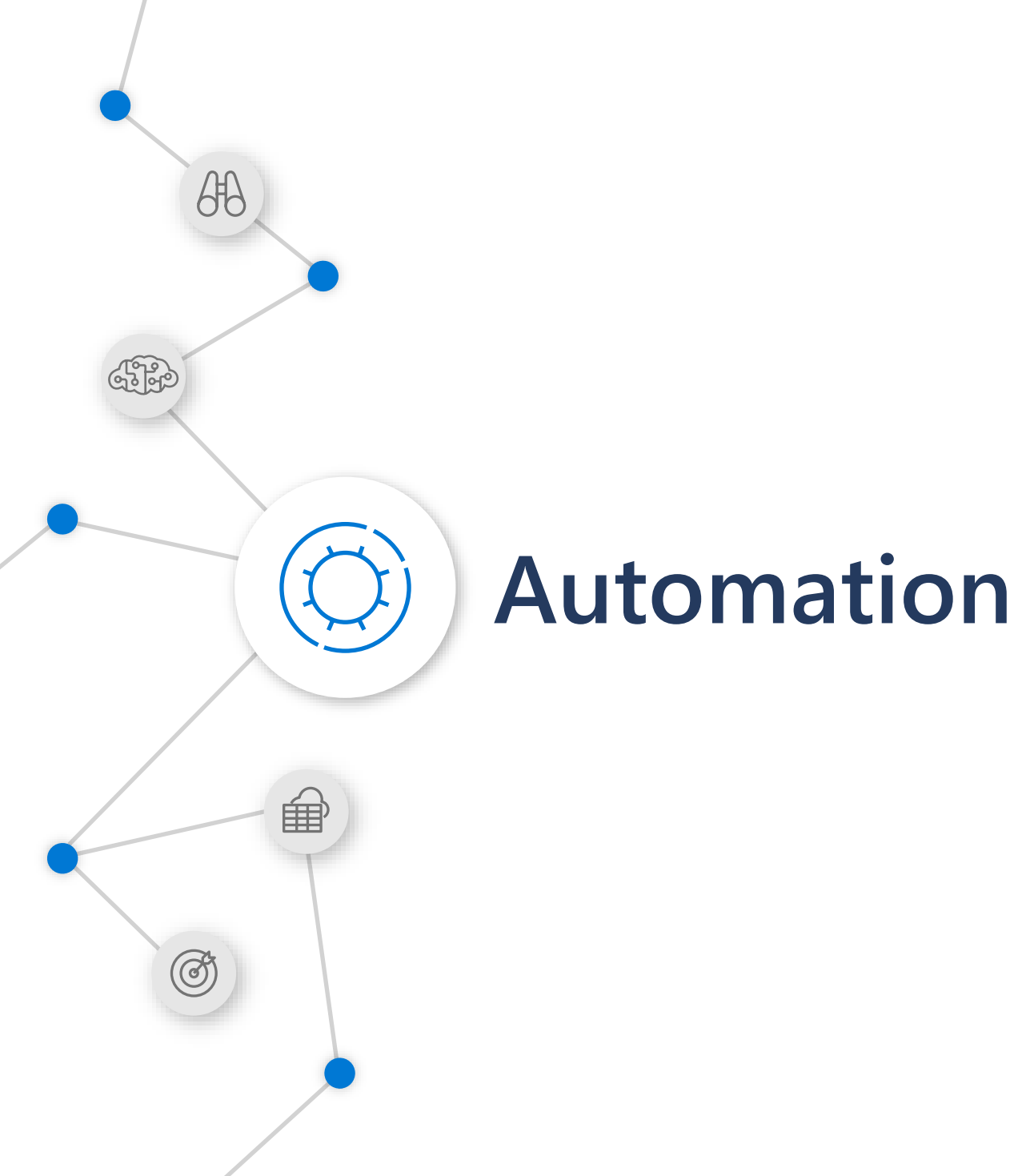
Save as sharable HTML/JSON

Query Azure Sentinel data

Bring external data sources

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





11

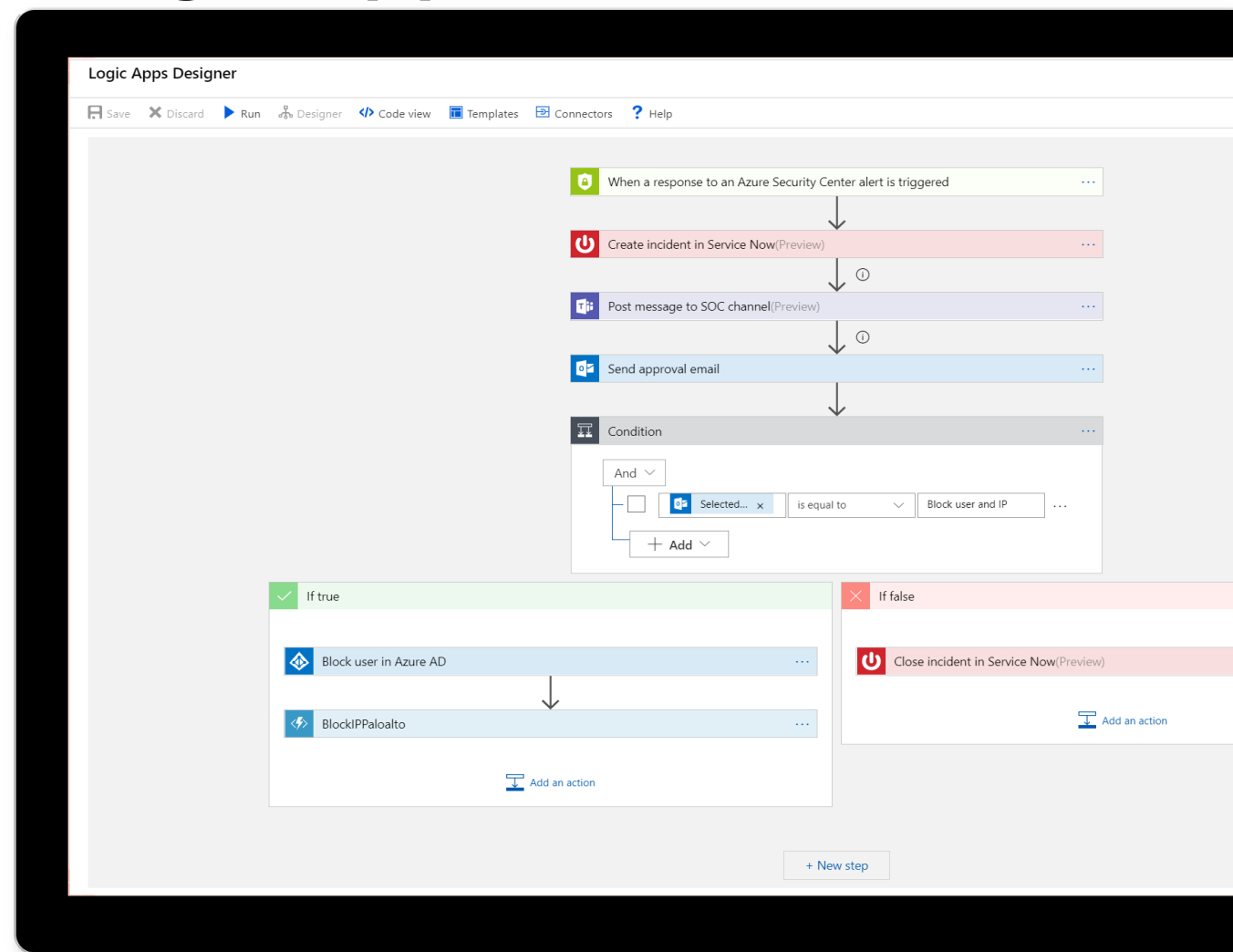
Automate and orchestrate security operations using integrated Azure Logic Apps

Build automated and scalable playbooks that integrate across tools

Choose from a library of samples

Create your own playbooks using 200+ built-in connectors

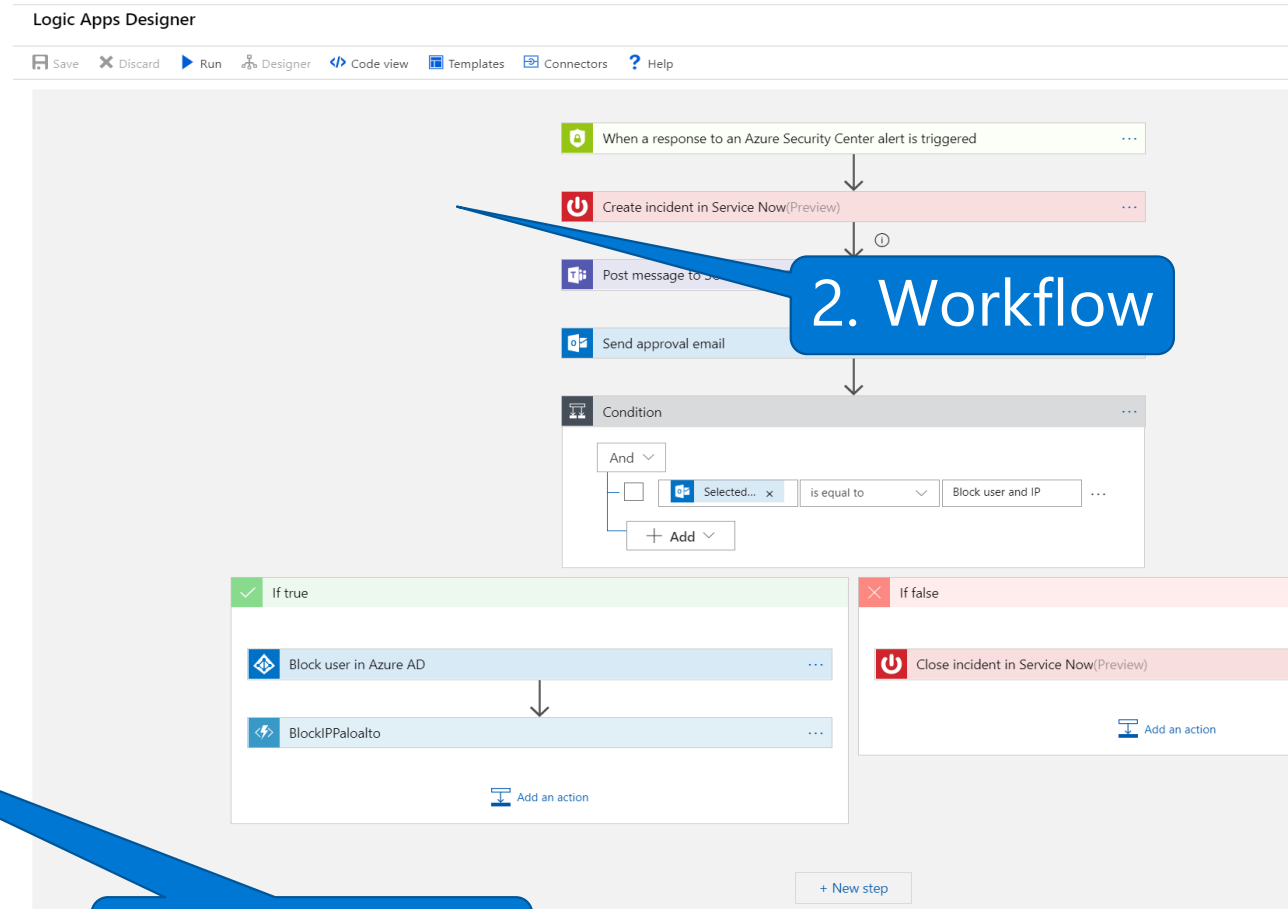
Trigger a playbook from an alert or incident investigation



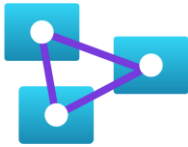
1. Integration

2. Workflow

3. Response



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

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>

Open Q & A

Please ask any question in the Q&A

We will read your questions and answer them in this meeting , or a next meeting.



Poll



Which Topics should we cover next?

Planned Sessions	Main Topics
Wednesday, April 22, 2020	How Azure Sentinel can help to secure remote work
Friday, April 24, 2020	Secure Remote Work: threats, scenarios and best practices
Wednesday, April 29, 2020	Teams for Education
Friday, May 01, 2020	Bank holiday
Wednesday, May 06, 2020	Teams for Healthcare

- 1) Power Platform (how to leverage, deep dive on Crisis Communication App,...)
- 2) Information Protection
- 3) Any Other Suggestions?

Feedback Form

- Feedback on sessions
- Topic suggestions

Please take 1 minute to fill the survey and help us improve!



or <https://aka.ms/WE-TechOfficeHoursSurvey>

Partner Support Resources

WE Weekly Technical Office Hours

- **Goal:** address the main technical topics around working remotely and leveraging Microsoft technology (incl. Teams, Security, Power Platform, Windows Virtual Desktop...)
- Weekly Sessions – aka.ms/WE-TechOfficeHours
 - **Wednesdays** at **12:00 – 13:00 CET** (11:00 – 12:00 WEST, 13:00 – 14:00 EEST)
 - **Fridays** at **13:00 – 14:00 CET** (12:00 – 13:00 WEST, 14:00 – 15:00 EEST)
- Hosted and moderated by **experts** on these topics, from **WE OCP Technical Team**, **EMEA Partner Tech Services** and **Corp Engineering Team**

<https://aka.ms/WE-TechOfficeHours-Materials>

Get help now

- Check out the [Technical Support Options](https://support.microsoft.com/en-us/help/4020188/technical-support-for-microsoft-partners) for Microsoft Partners
<https://support.microsoft.com/en-us/help/4020188/technical-support-for-microsoft-partners>
- If you have a **dedicated Partner Development Manager / Partner Technology Strategist** – reach out to them [directly](#) with your query
- If you do not have a dedicated Partner Development Manager / Partner Technology Strategist, and you need **guidance on a specific customer scenario** (pre-sales technical or deployment assistance) – make use of your [advisory hours](#) and reach out to [Partner Technical Services](#)

New "Secure Remote Work workshop" available

As a part of the "Microsoft 365 Partner Accelerators" this one-day workshop is designed to help customers **rapidly deploy remote work scenarios** to:

- empower employees to stay connected,
- while maintaining **security & control**.

Secure Remote Work Workshop phases



Preparation

Define scope, identify stakeholders, and gather information about current environment and workloads to be enabled or optimized for remote work



Design

Determine the identity, Microsoft Teams, Office 365, and Security requirements to deploy remote work scenarios securely



Deployment plan

Develop a joint deployment plan, including timelines and next actions

Learn more: aka.ms/RemoteWorkWorkshop

- **Targeted audience:** partners in the Teams and Security space
- **When:** April 23, 2020 , 17:00-18:00 CET
- **How to register:** register at this link <https://aka.ms/M365v256PAL-Register>

Secure Remote Work Workshop funding

Partner funding is available for eligible partners and customers. Funding is designed to enable partners to deliver rapid deployment & adoption engagements to assist customers with business continuity.



\$2500
per engagement

Customer Requirements

- **Existing Office/M365 customers:**
> 1000 Exchange Online qualified entitlements
- **Non-Office 365 customers:**
> 1000 PC Install Base

Program Dates

- **First day to nominate customers:**
April 16, 2020

Partner Requirements

- Co-sell Ready or Fast Track Ready
- SSPA Compliant

Proof of Execution

- Customer Satisfaction Survey
- Partner Findings Survey
- Deployment Plan

Funding Available

- Up to \$2,500 for completion of the workshop

Partners should ***nominate*** customers here: aka.ms/SecureRemoteWorkWorkshop

Virtual End-to-End Microsoft Security Bootcamp



Virtual End-to-End Microsoft Security Bootcamp

April 28 – 30



We're excited to invite you to our three half days security bootcamp with our Engineering experts to learn more about **Microsoft Security solutions**. This training focuses on providing practice leads, security architects, and consultants **a deeper understanding of the capabilities within the Microsoft Security stack**.

- **Targeted audience:** individuals who have fundamental technical skills in security and want to expand their security practices and increase their expertise in Microsoft Security solutions,
- **When:** April 28-30, 2020
- **Registration and agenda:** [Link](https://learning.eventbuilder.com/SecurityBootcamp) <https://learning.eventbuilder.com/SecurityBootcamp>

Microsoft Teams Virtual Calling and Meetings Bootcamp



We are excited to invite you to a five half-days virtual technical bootcamp with subject matter experts from Microsoft where you'll learn the landscape of **Teams architecture, governance, and manageability** with special tech focus on Meetings and Teams Room.

- **Targeted audience:** Individuals responsible for Teams practice development and those willing to sharpen their tech expertise with Microsoft Teams Calling
- **When:** May 4-6, 11&13, 2020
- **Registration and agenda:** [Link](https://learning.eventbuilder.com/CallingAndMeetingsBootcamp) <https://learning.eventbuilder.com/CallingAndMeetingsBootcamp>

Other Partner Resources

- **Best practices and discussion for remote work**
 - [Best practices](#), based on Microsoft internal learnings
 - (new) [Microsoft Tech Community](#) forum for discussing / sharing best practices
- **Enabling Microsoft Teams**
 - We recommend that partners lead with the [CSP Trial](#). See details in our [news article](#).
 - For customers who **don't align to the CSP Trial**, partners can get access to the **Office 365 E1 Trial** for them.
Go to [Partner Center Support](#) and click on *CSP > Cannot find an offer in the catalog*.
- **Resources for Education Partners**
 - Check out the [EDU Partner Flash on Yammer](#)
 - [Office 365 A1](#) – **Free** versions to **all educational institutions**: unlimited chat, built-in group and one-on-one audio or video calling, 10 GB of team file storage, and 2 GB of personal file storage per user. You also get real-time collaboration with the Office apps for web, including Word, Excel, PowerPoint, and OneNote. No restrictions for # of users.
 - [Microsoft Teams for Free](#) (**Individuals** and **IT roll-out** – in Office 365 A1 above): unlimited chat, built-in group and one-on-one audio or video calling, 10 GB of team file storage, and 2 GB of personal file storage per user.
 - [Minecraft: Education Edition](#): We've extended access to Minecraft: Education Edition to all free and paid O365 Education accounts through the end of June 2020 and published a [M:EE remote learning toolkit](#) with links to >100 Minecraft lessons and STEM curriculum.

Thank You!

