Microsoft

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)

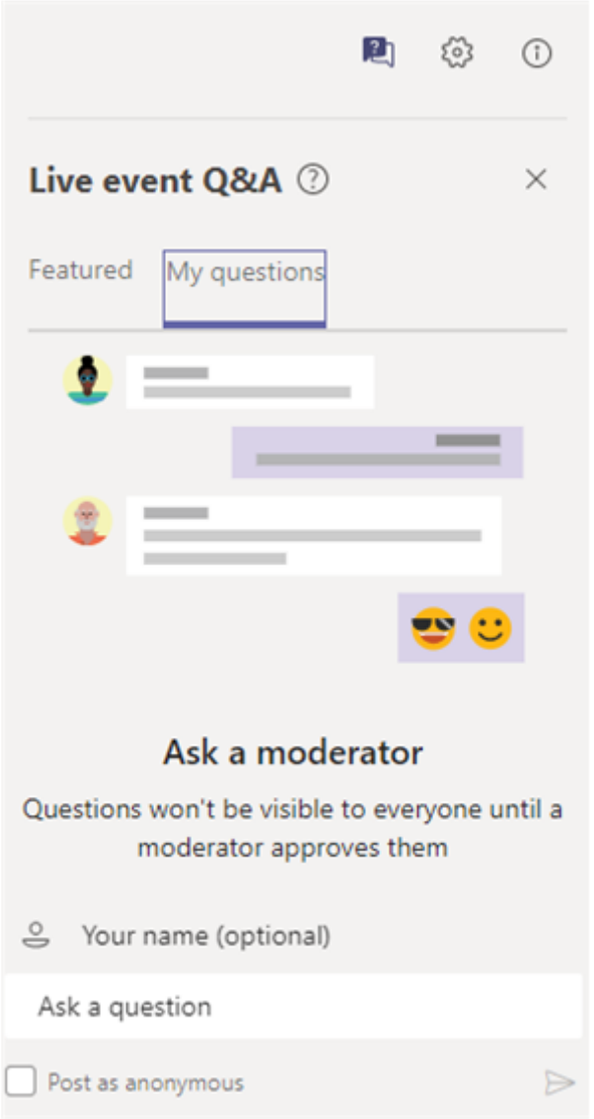
Toni Willberg
Cloud Solution Architect (Azure)

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

Wednesdays

Fridays

Don't miss a session;

Update your calendar by using the invites above.

Next Session Details

Upcoming Sessions

Materials & Recordings

Other Resources

Feedback Form

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

Microsoft

How Azure Sentinel can help to secure remote work

Olivier van der Kruijf
Cloud Solution Architect (Azure)

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

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

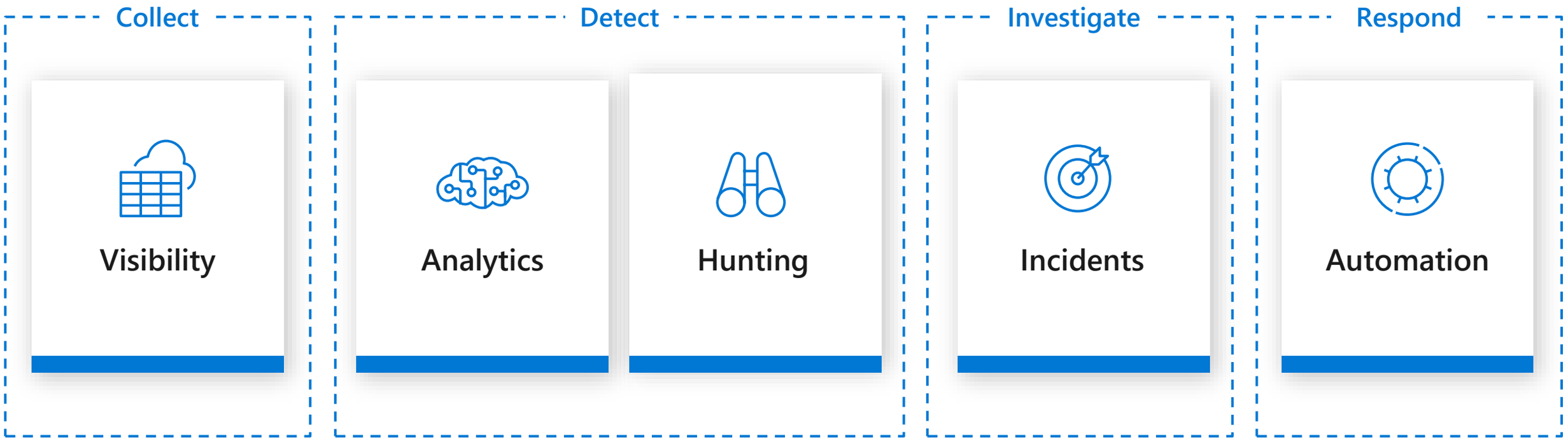
Azure Sentinel

A cloud SIEM

For the Cloud

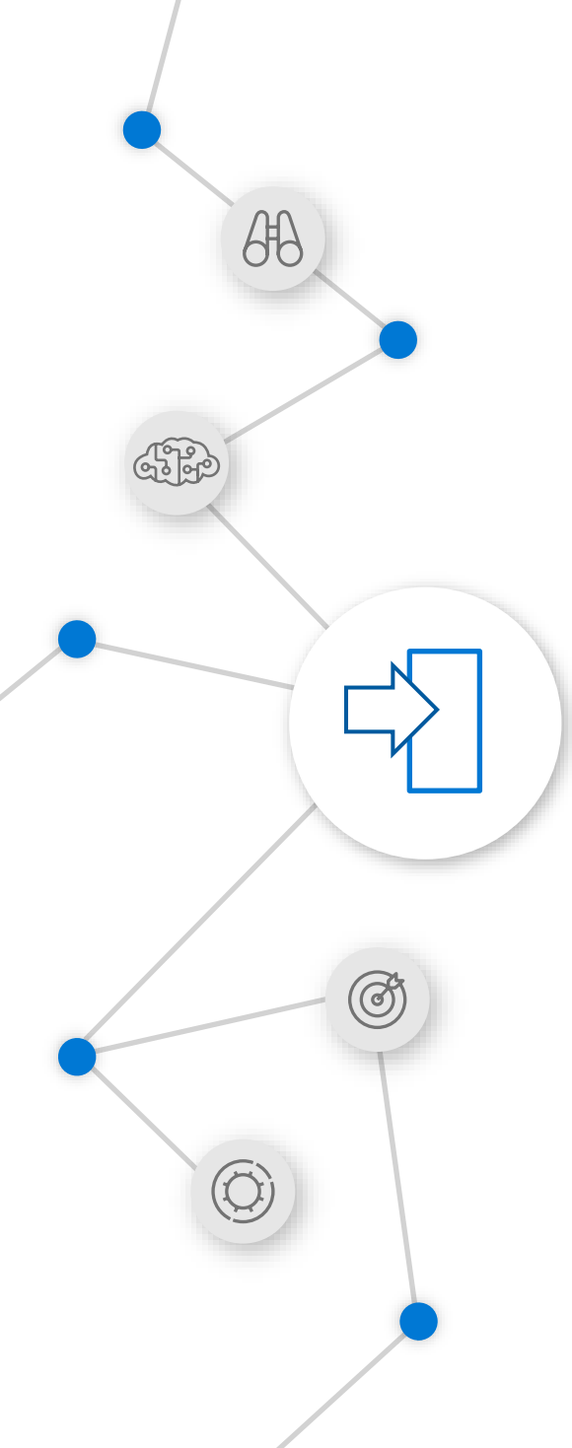
And for on premises

End-to-end solution for security operations



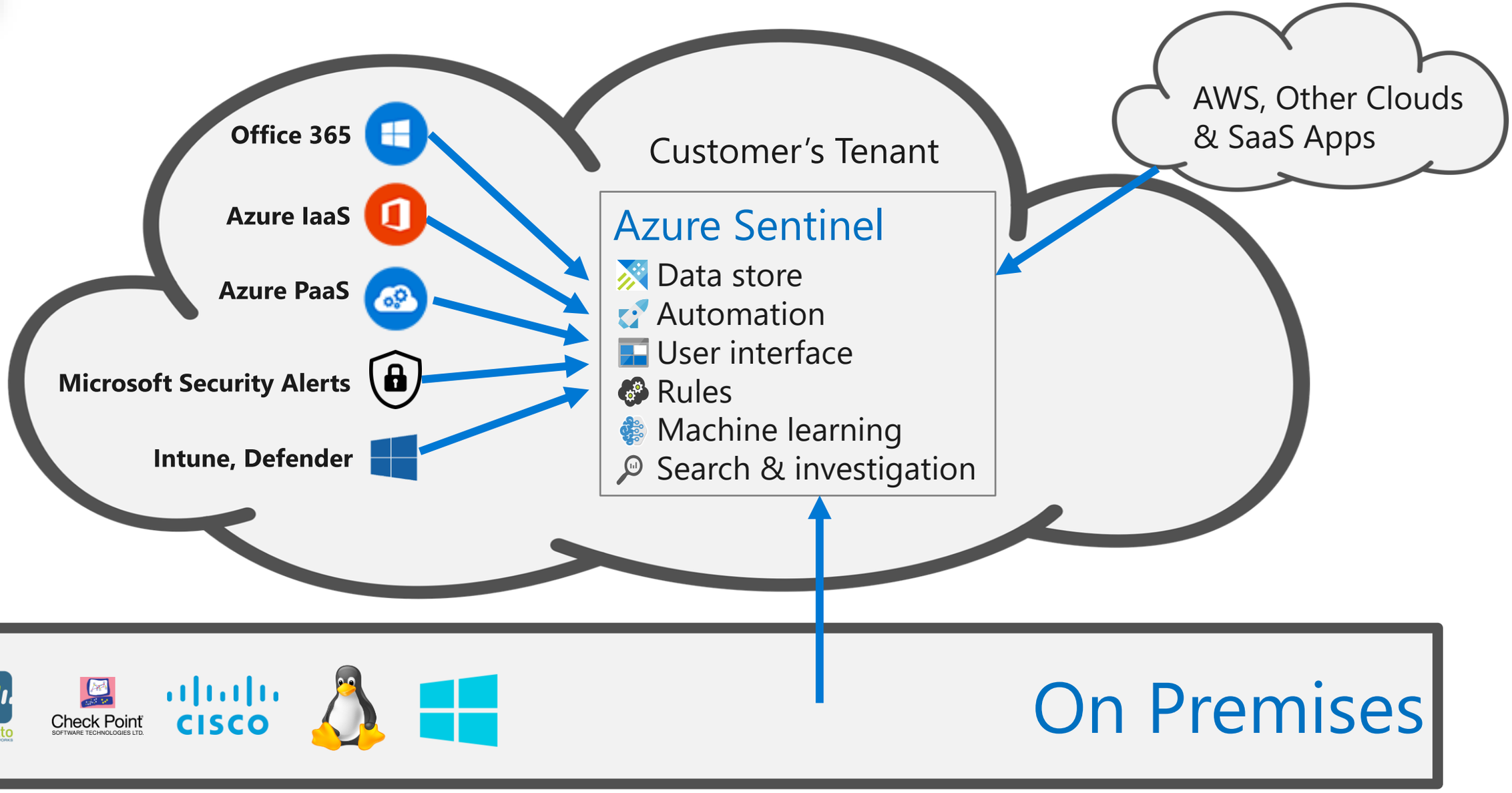
Microsoft Security Advantage

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



Collection

1 Collect security data at cloud scale from any source



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

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

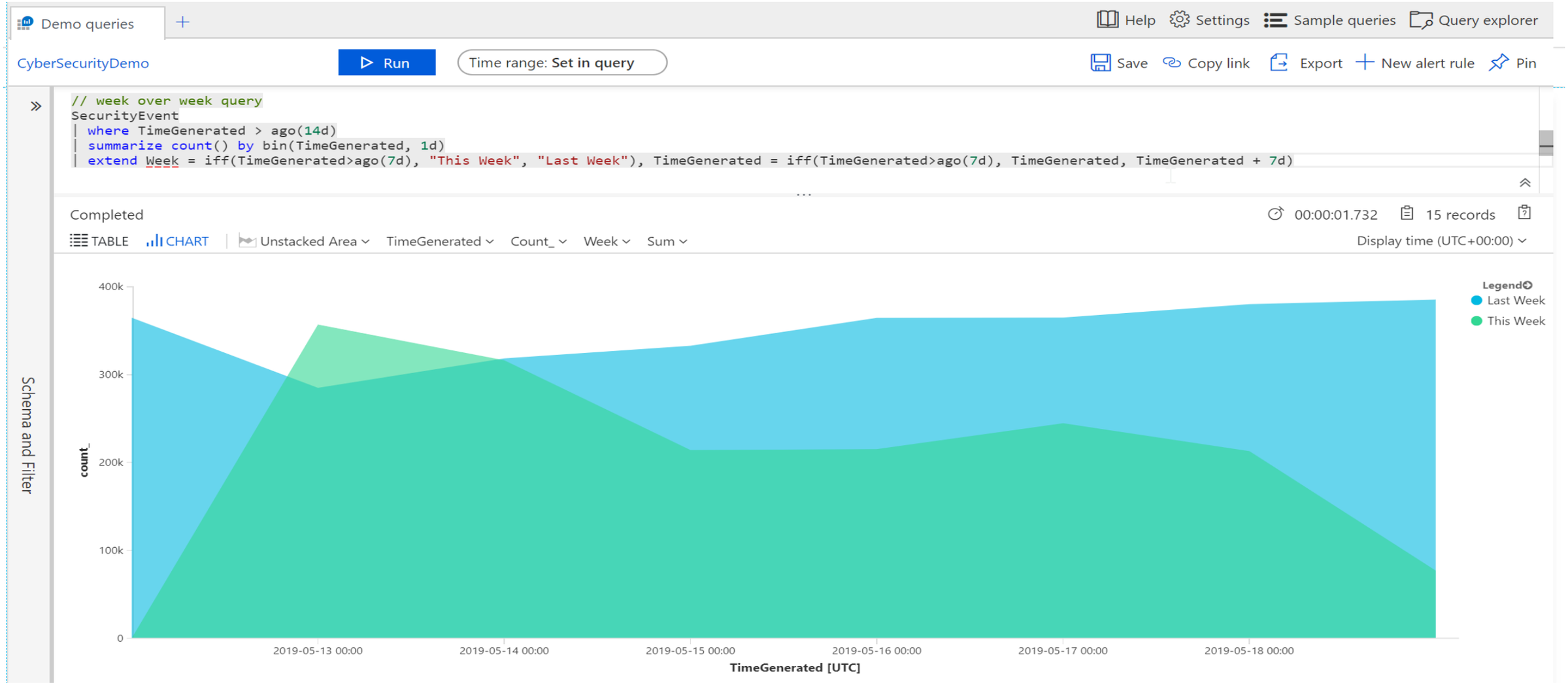
Name	Sign-in Count	Trend	Failure Count	Interrupt Count
US	2.349K		77	67
BE	566		3	8
GB	421		30	24
AU	241		22	65
IL	203		0	5

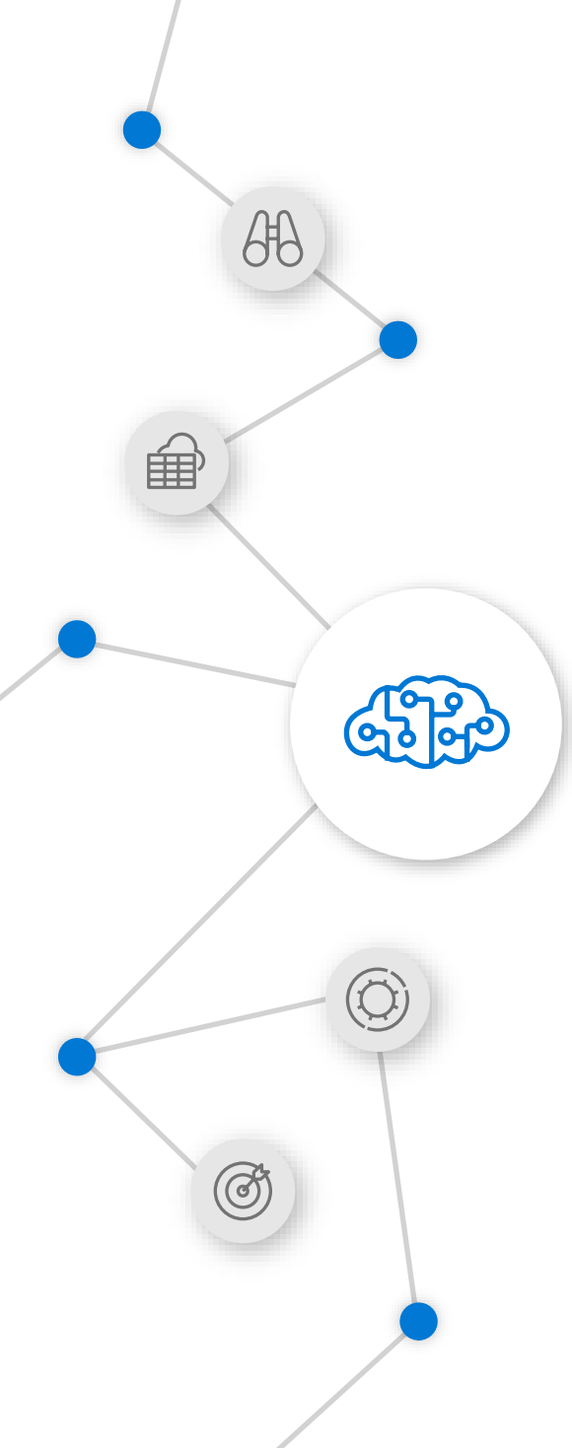
Location Sign-in details

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

Chart search results





Analytics

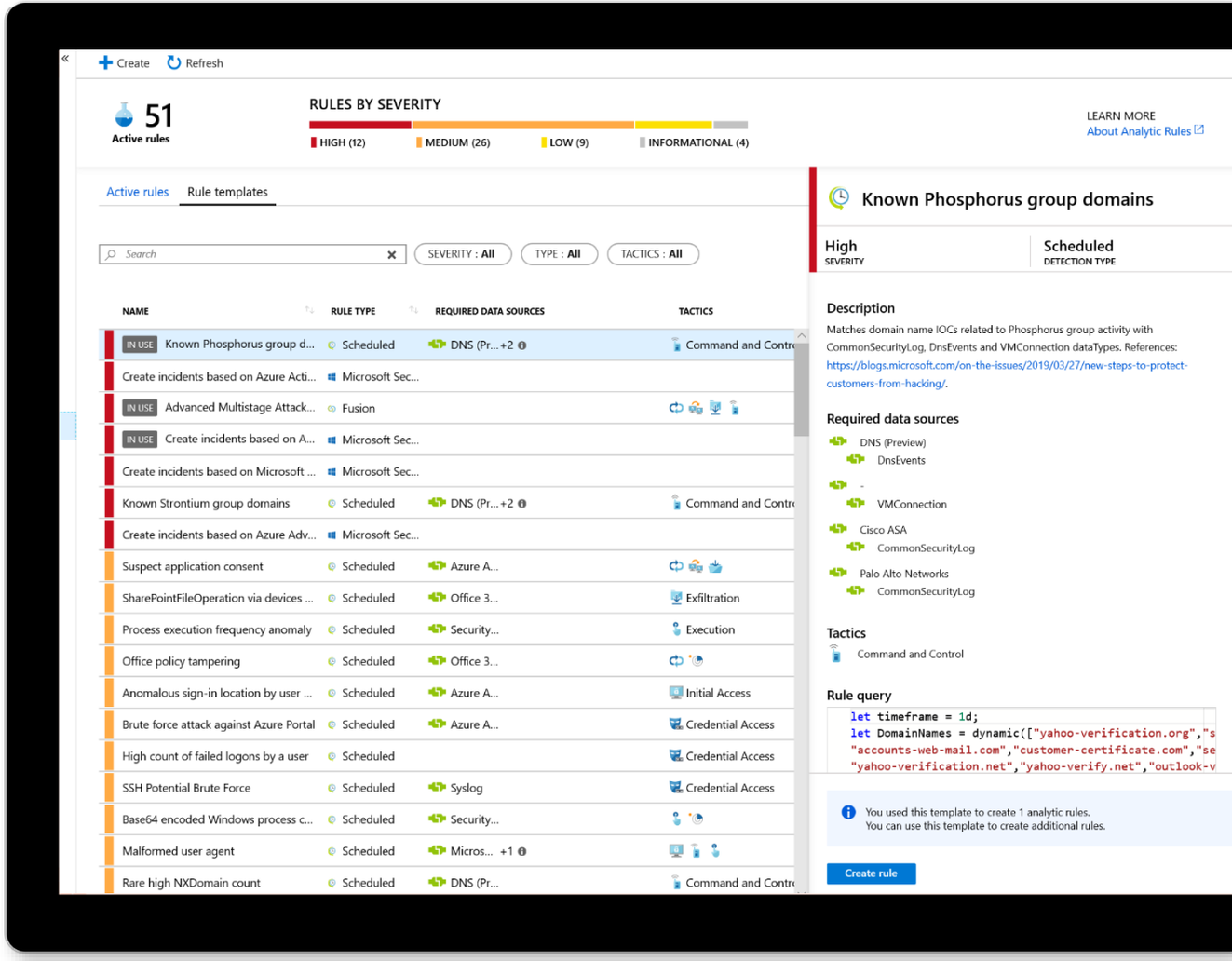
3 Leverage analytics to detect threats

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

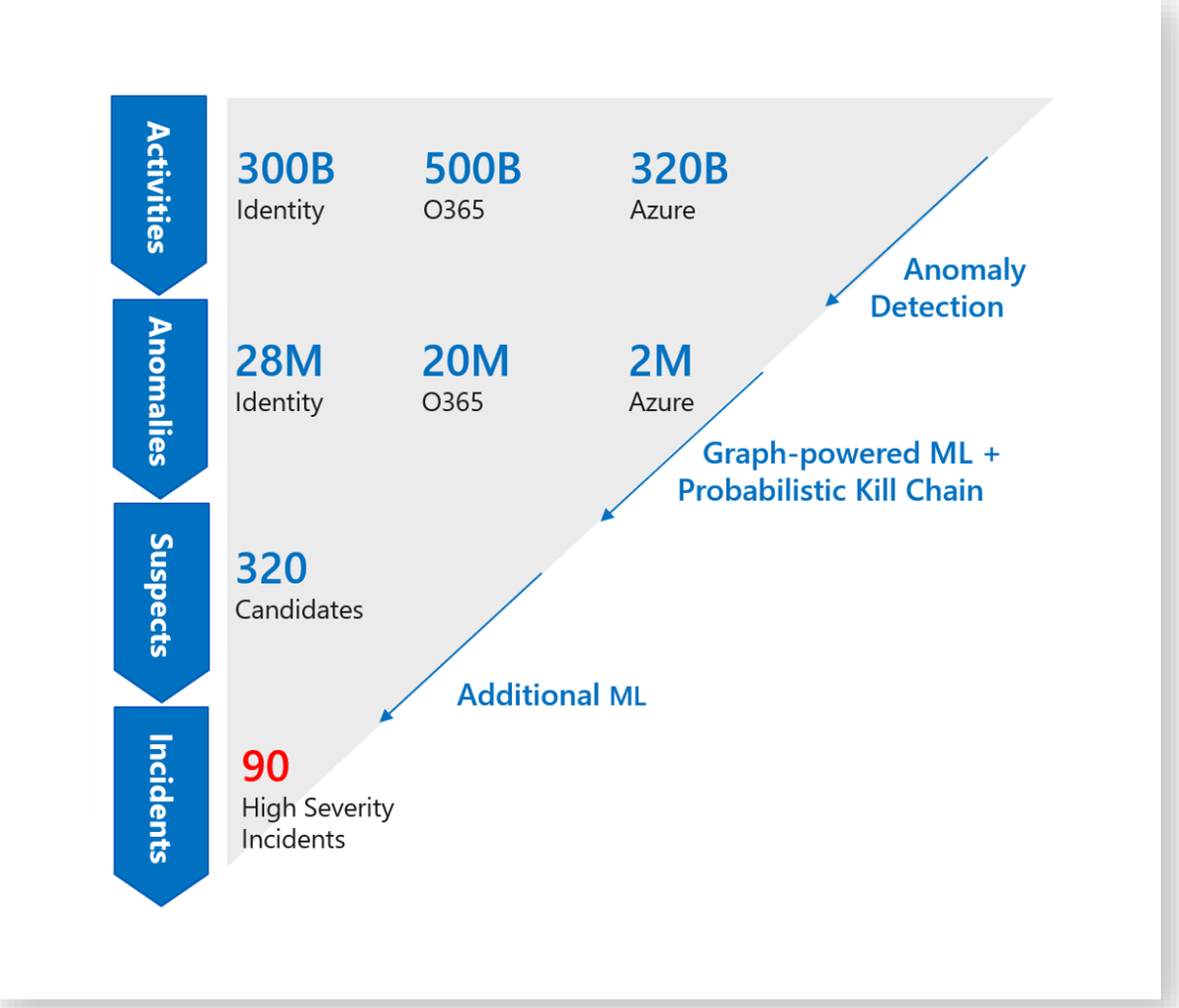


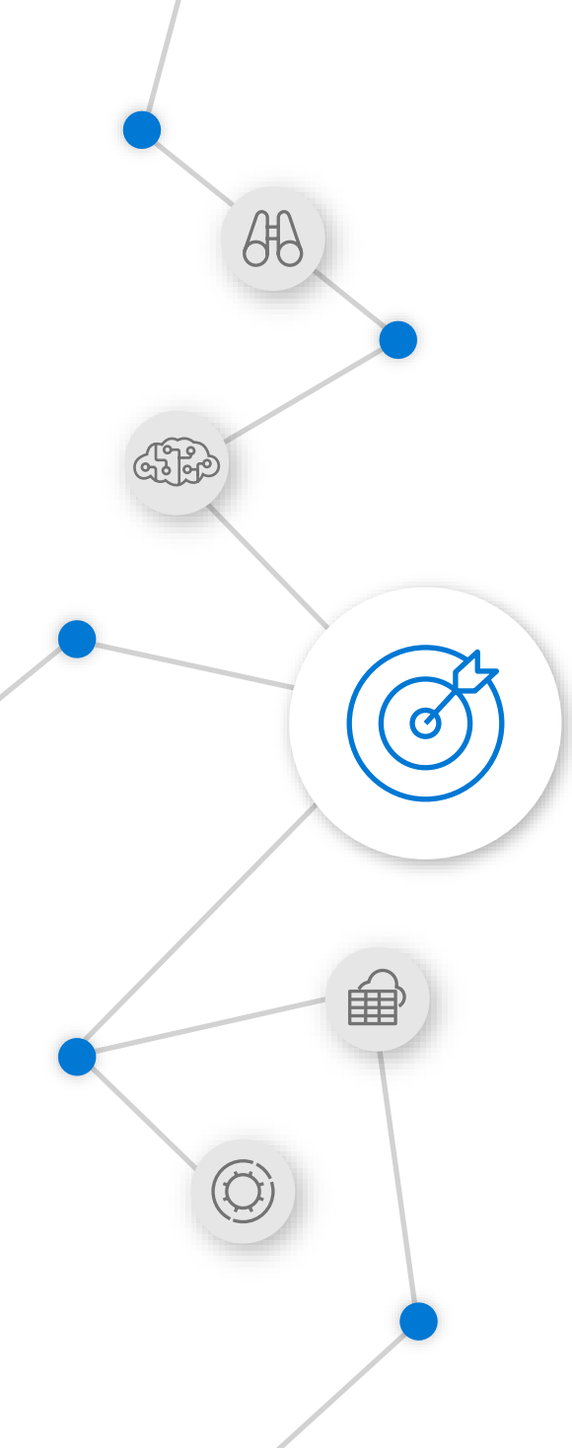
4 Tap into the power of ML increase your catch rate without increasing noise

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

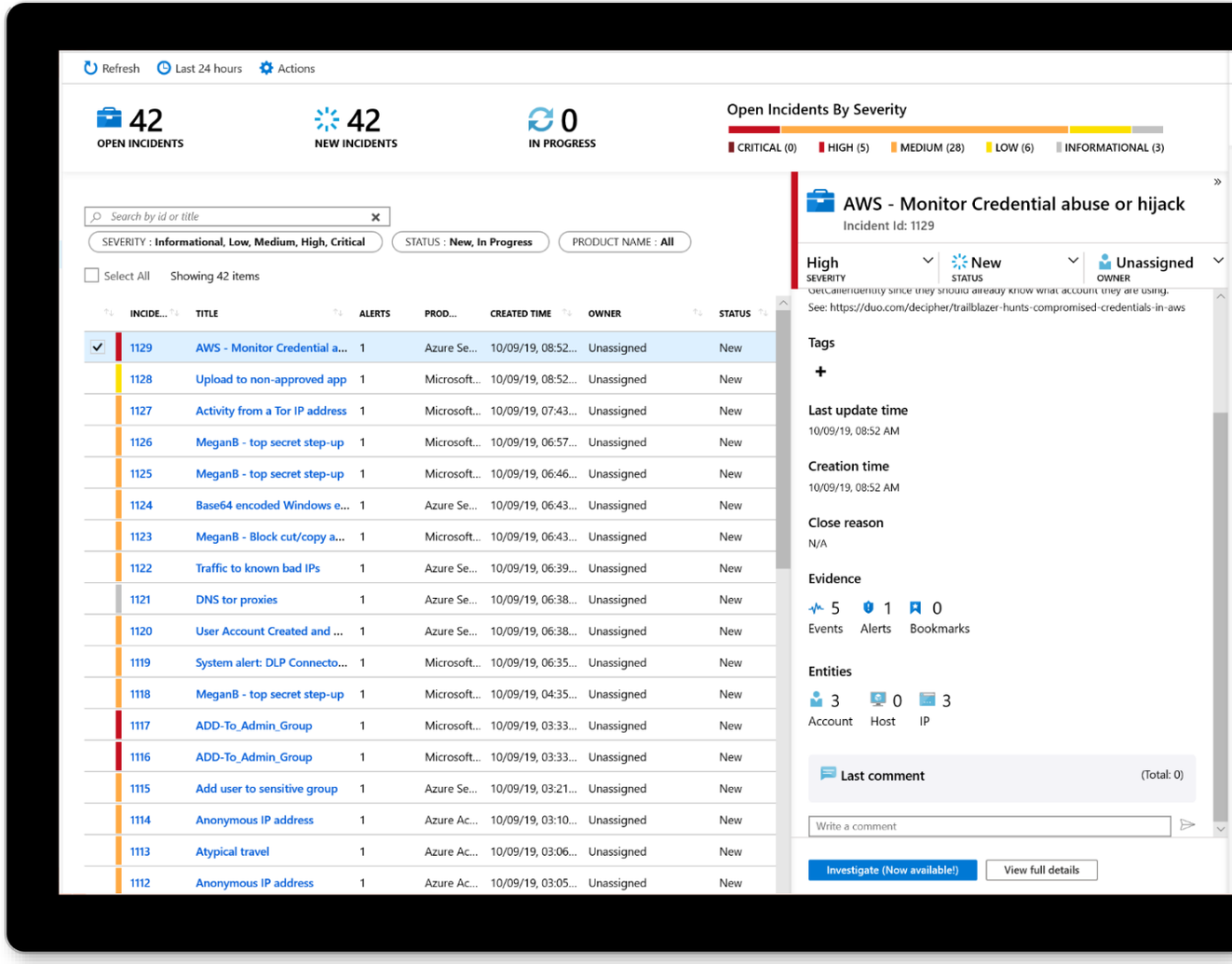
5 Start and track investigations from prioritized, actionable security incidents

Use incident to collect related alerts, events, and bookmarks

Manage assignments and track status

Add tags and comments

Integrate with your ticketing system



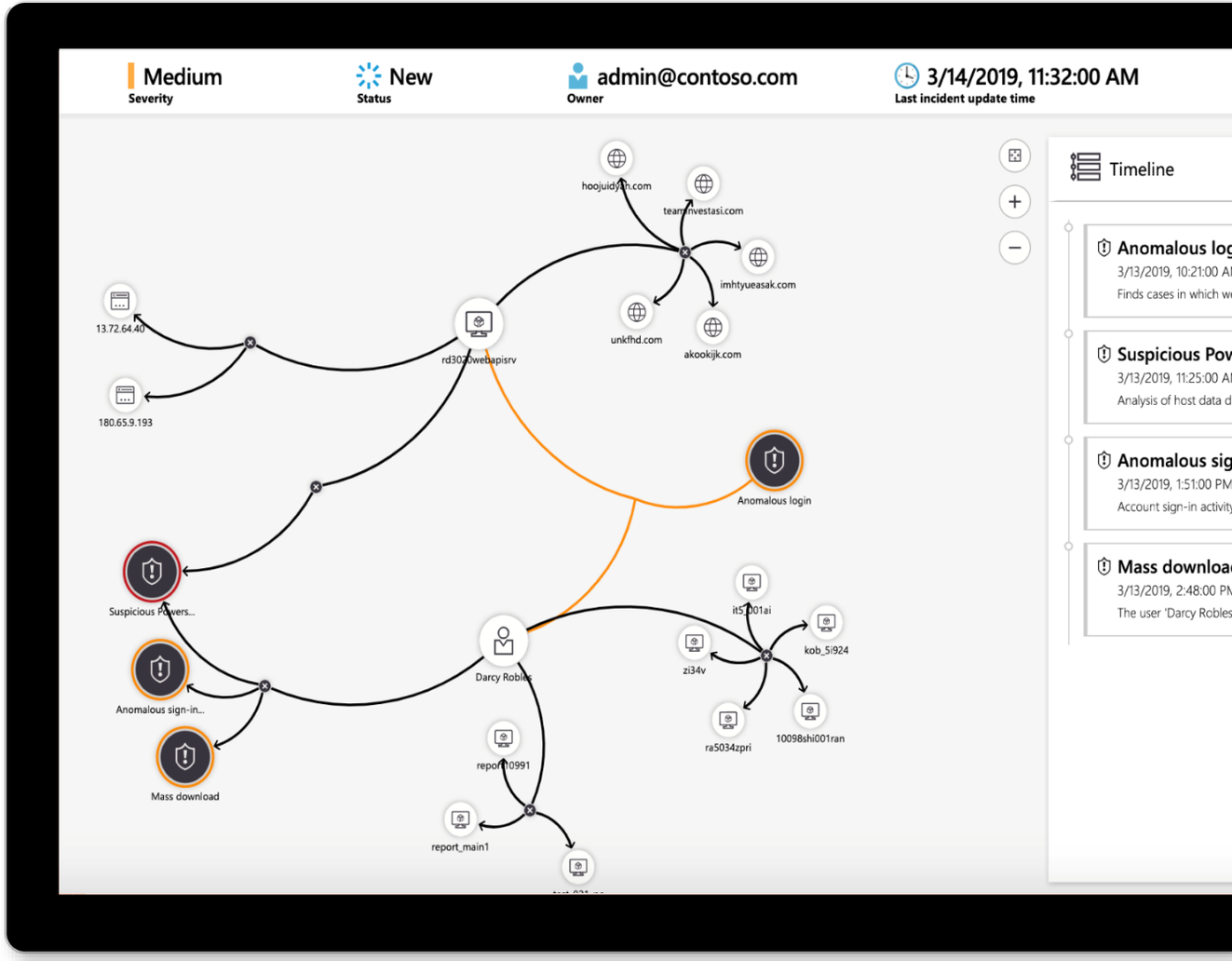
6 Visualize the entire attack to determine scope and impact

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

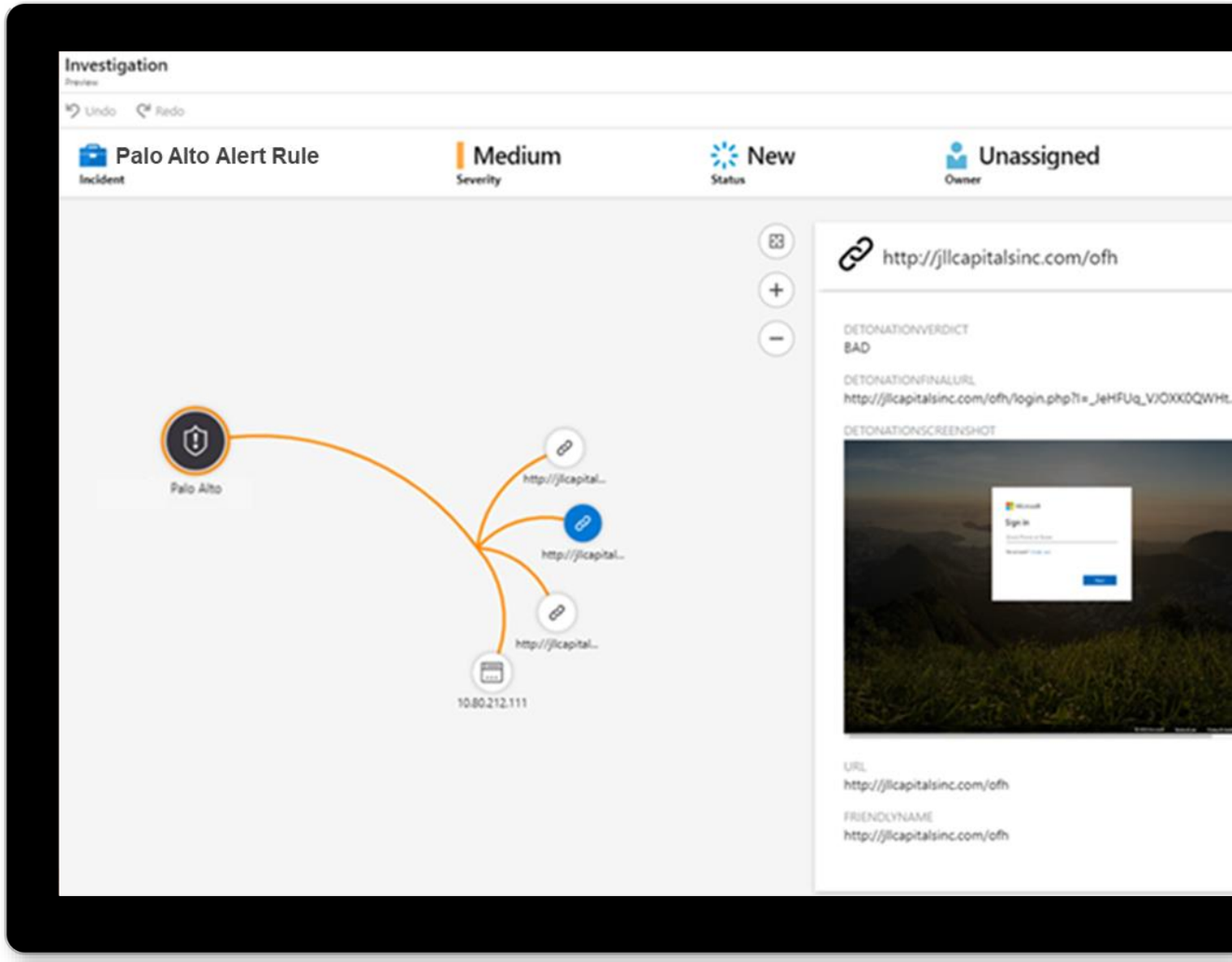


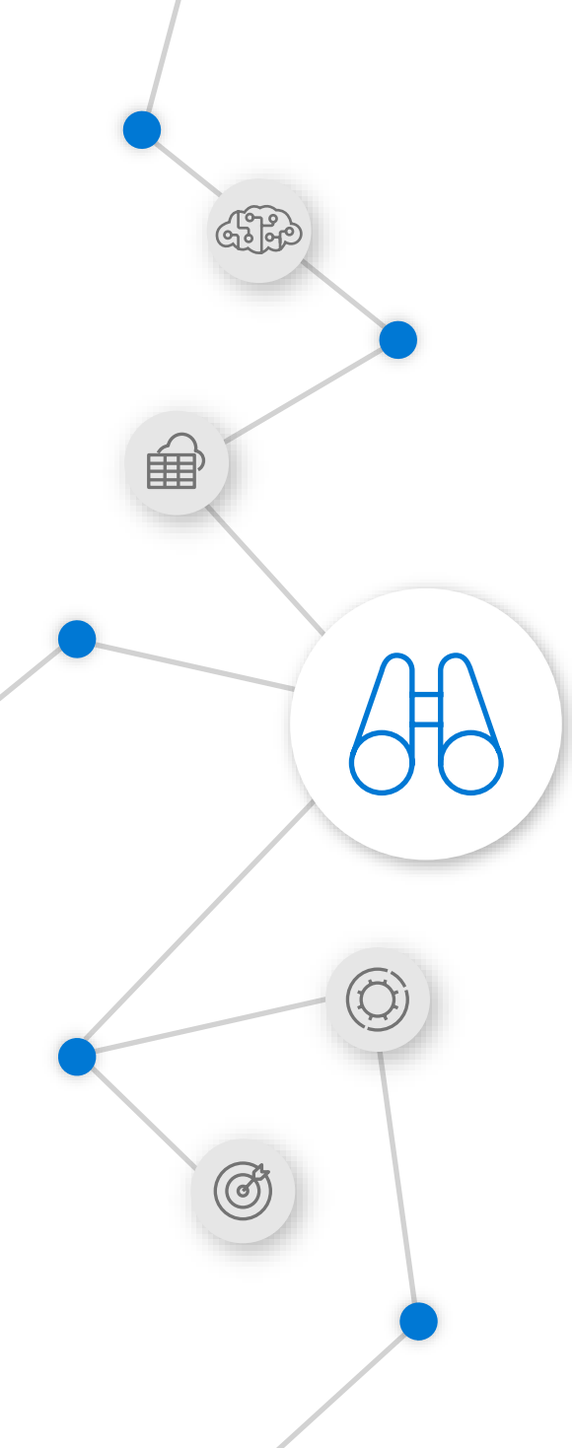
7 Gain deeper insight with built-in automated detonation

Configure URL Entities in analytics rules

Automatically trigger URL detonation

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





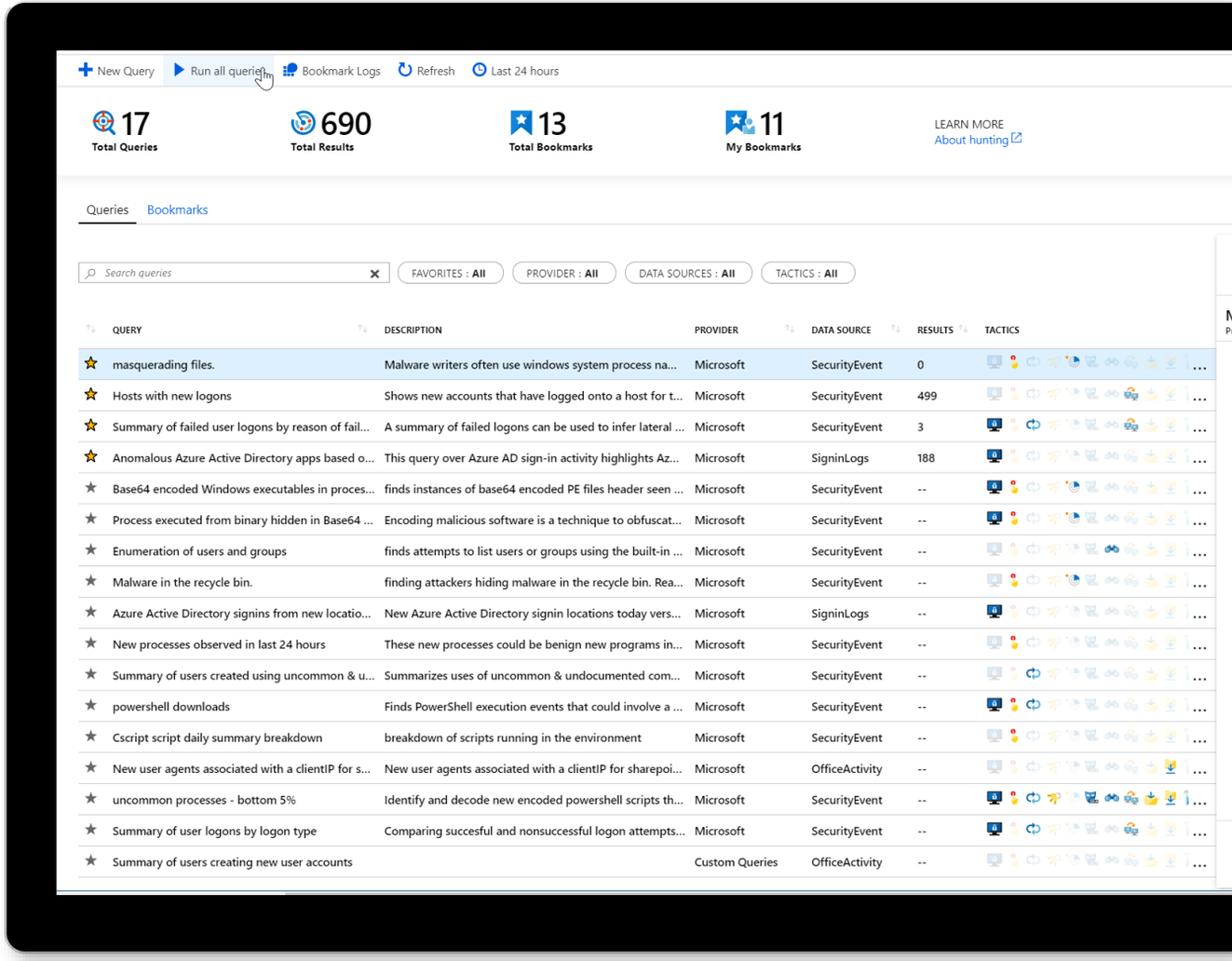
Hunting

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



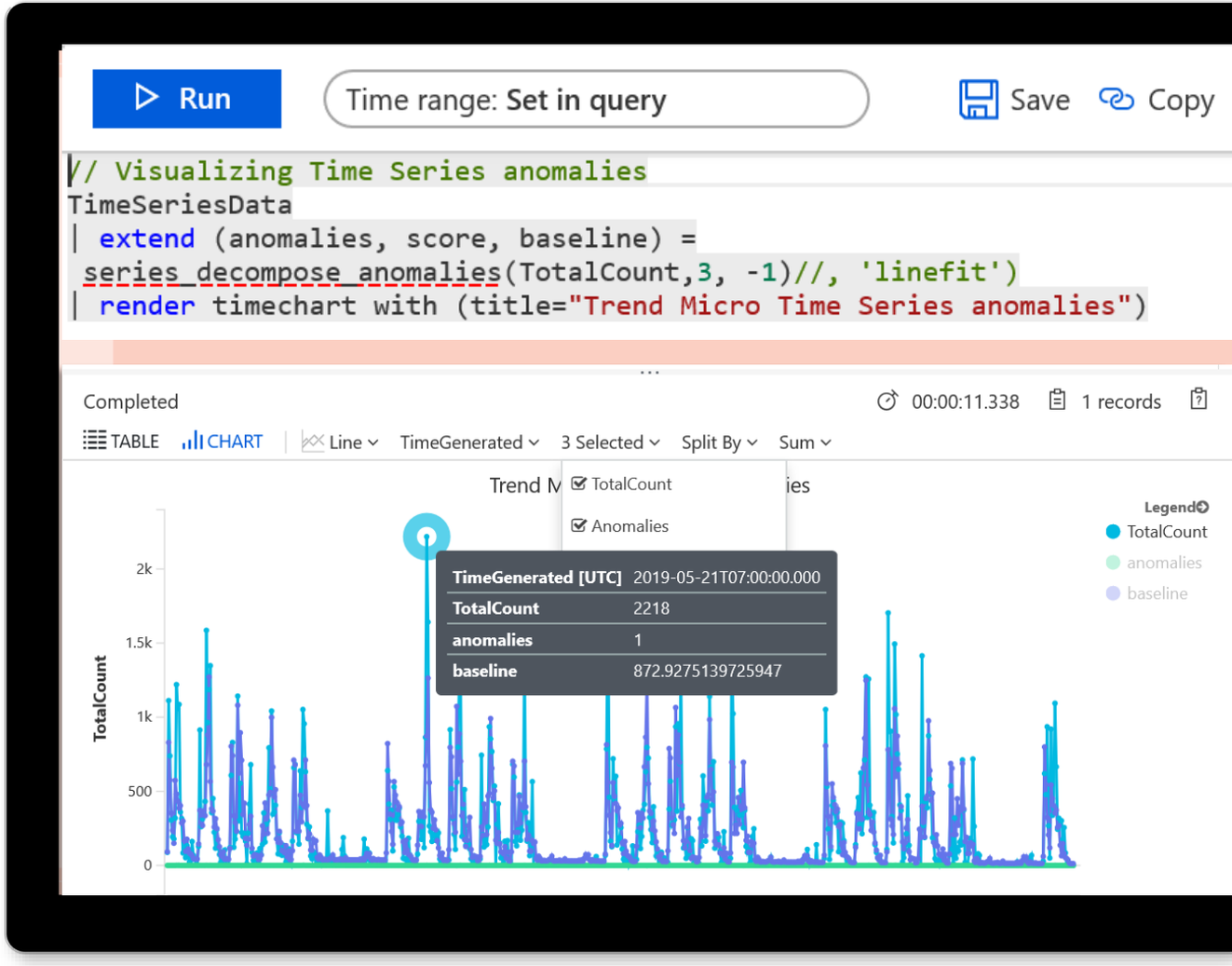
9 Explore data sets

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

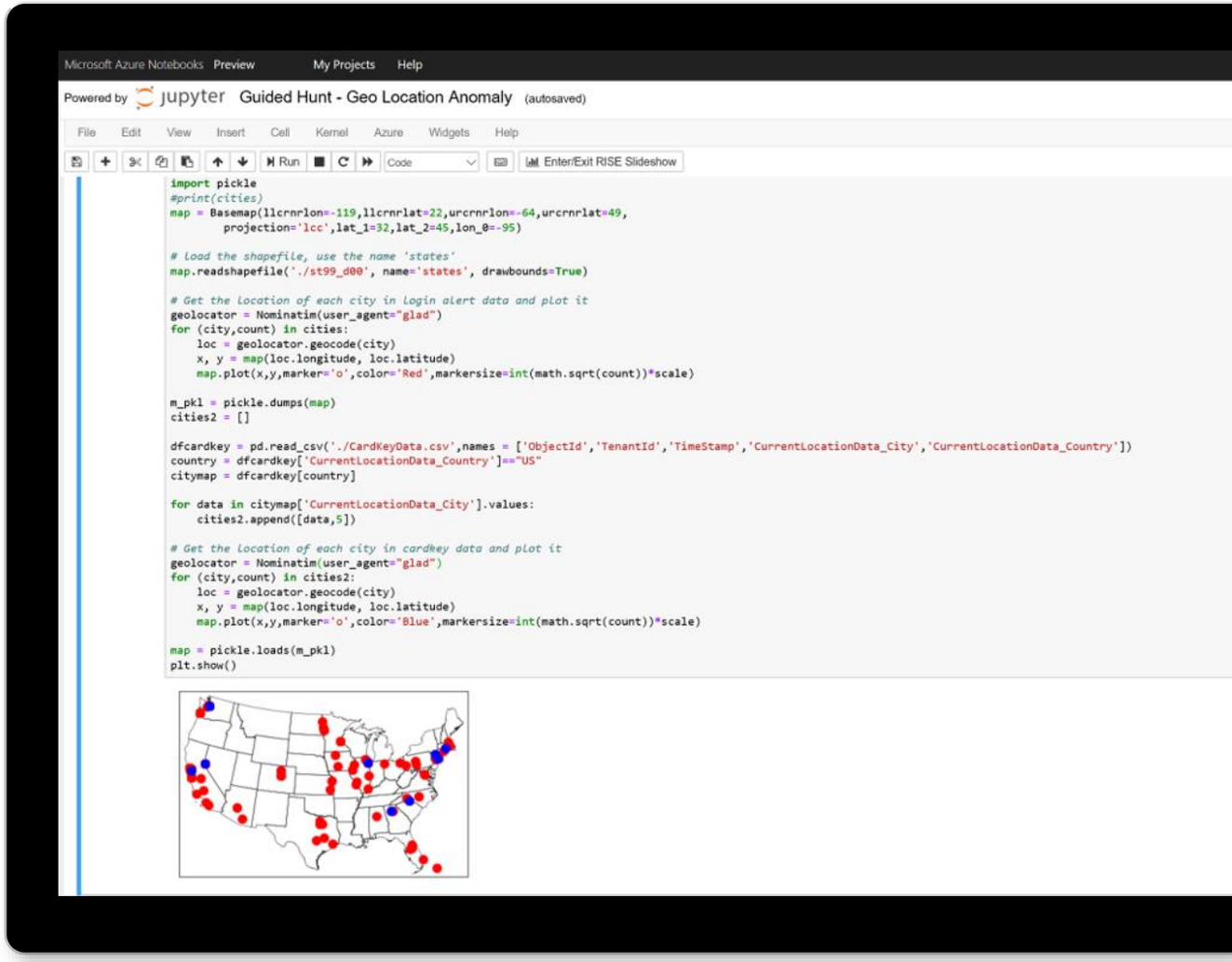
Run in the Azure cloud

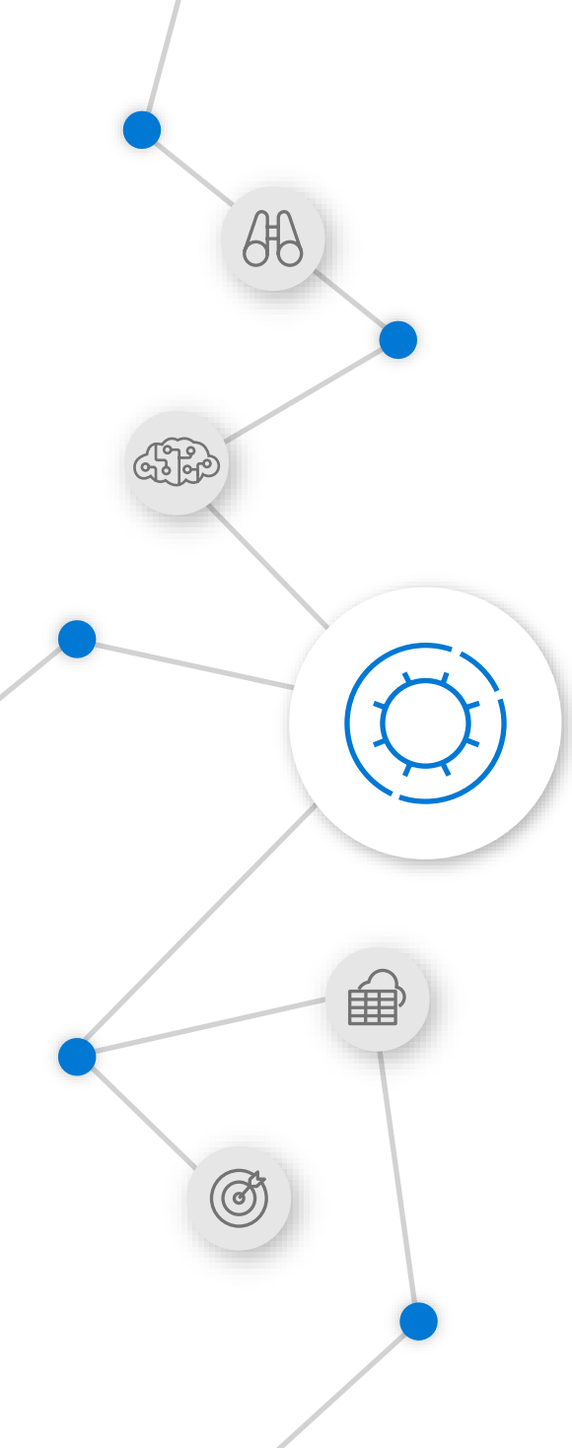
Save as sharable HTML/JSON

Query Azure Sentinel data

Bring external data sources

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





Automation

11

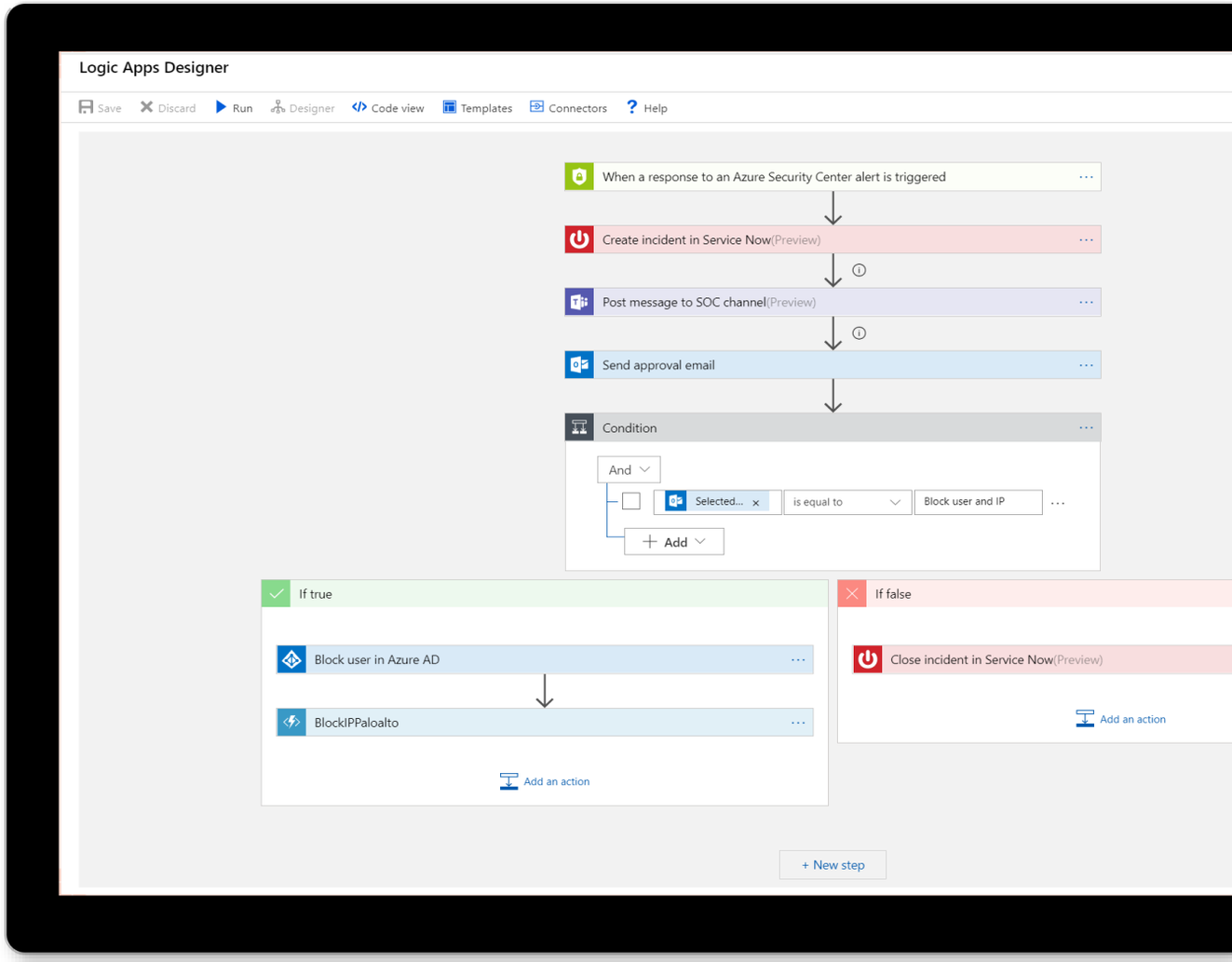
Automate and orchestrate security operations using integrated Azure Logic Apps

Build automated and scalable playbooks that integrate across tools

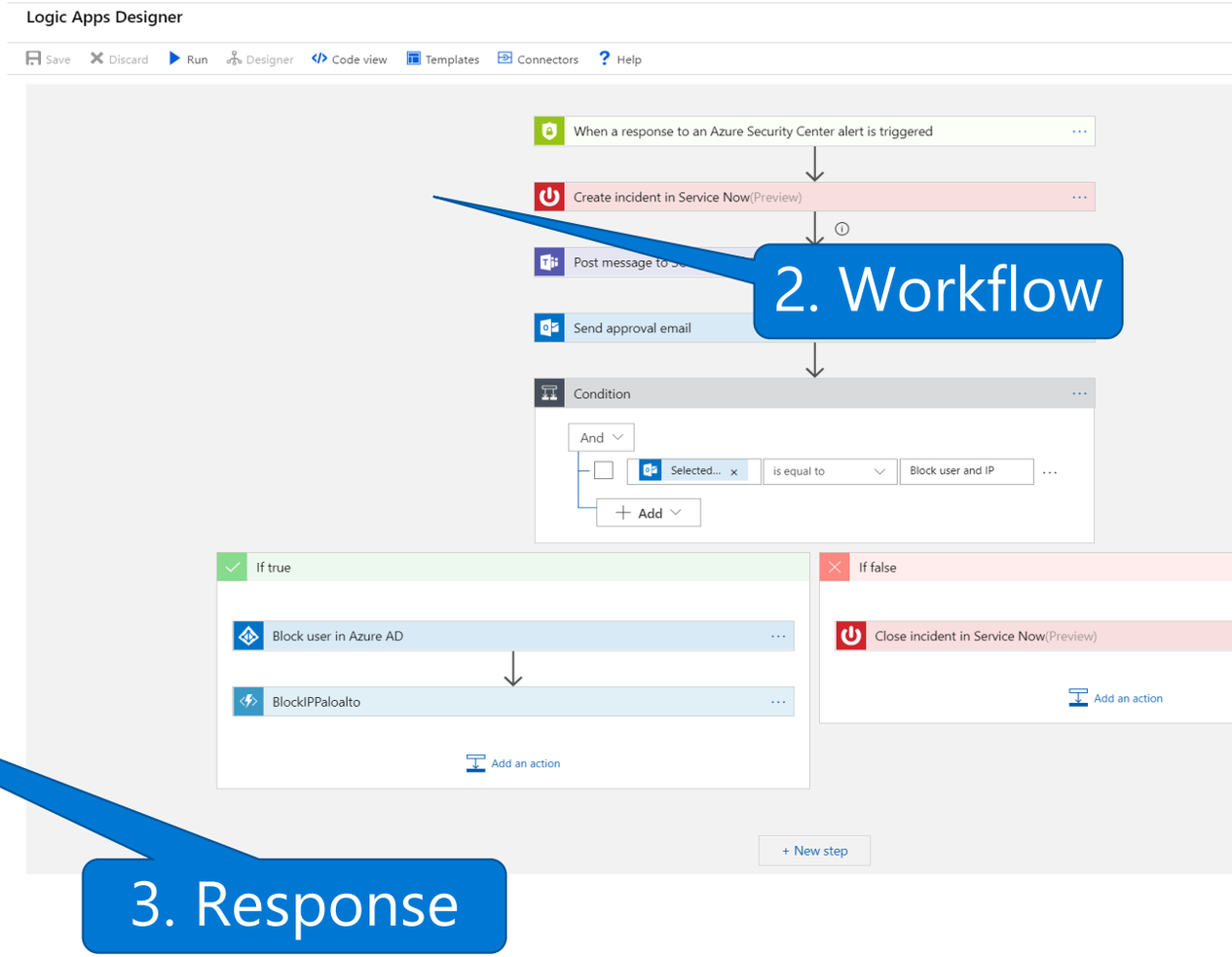
Choose from a library of samples

Create your own playbooks using 200+ built-in connectors

Trigger a playbook from an alert or incident investigation



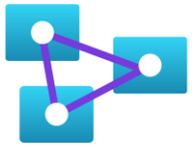
1. Integration



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 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.**

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

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

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 Teems 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

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.

Microsoft

Thank You!