



2019

NT KONFERENCA

21. - 23. MAJ 2019

#ntk19



#ntk19

Azure Sentinel - SIEM v oblaku

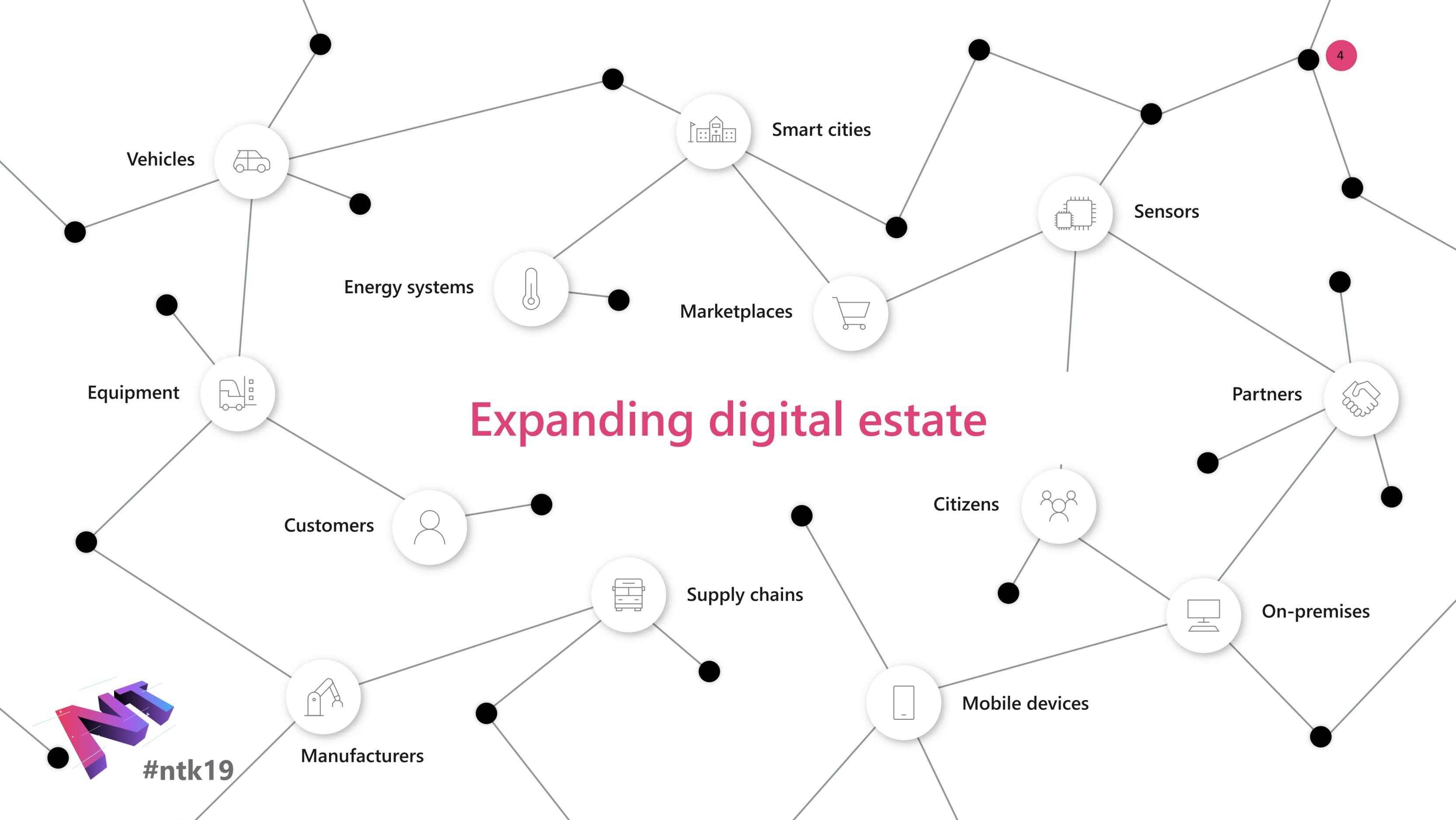
Gregor Šuster

Senior Consultant, Microsoft

Agenda

- Kaj je Azure Sentinel?
- Kako se rešitev pozicionira sklopu ostalih Microsoftovih varnostnih rešitev?
- Kakšne so funkcionalnosti produkta in kako ga lahko preiskusimo danes?





Expanding digital estate





Traditional SOC Challenges

Sophistication of threats

High volume of noisy alerts

IT deployment & maintenance

Rising infrastructure costs and upfront investment

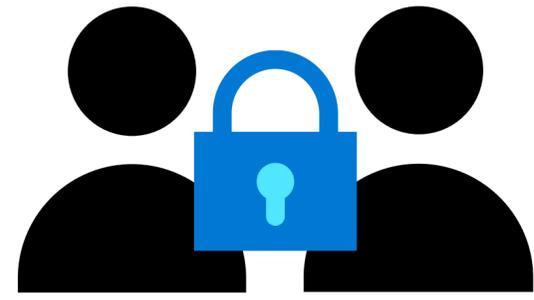
Too many disconnected products

Lack of automation

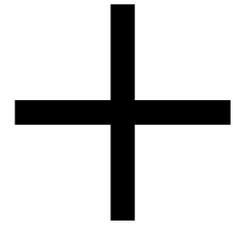
Security skills in short supply

#ntk19

5



Security Operations Team



Cloud + Artificial Intelligence

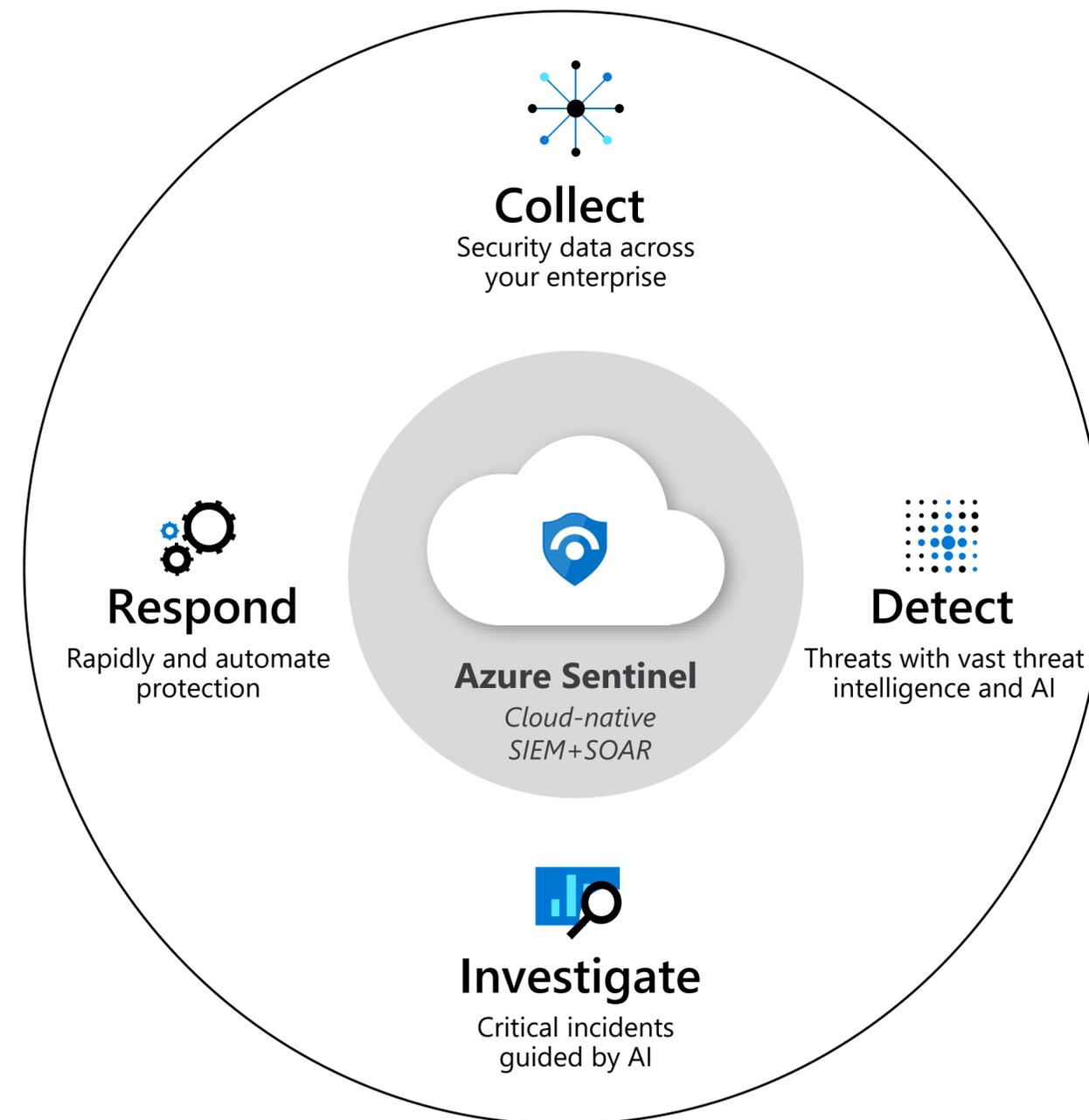


#ntk19

Introducing Microsoft Azure Sentinel

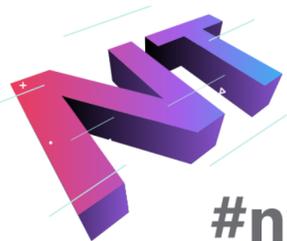
Cloud-native SIEM for intelligent security analytics for your entire enterprise

- Limitless cloud speed and scale
- Bring your Office 365 data for Free
- Easy integration with your existing tools
- Faster threat protection with AI by your side



Microsoft Security Advantage

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



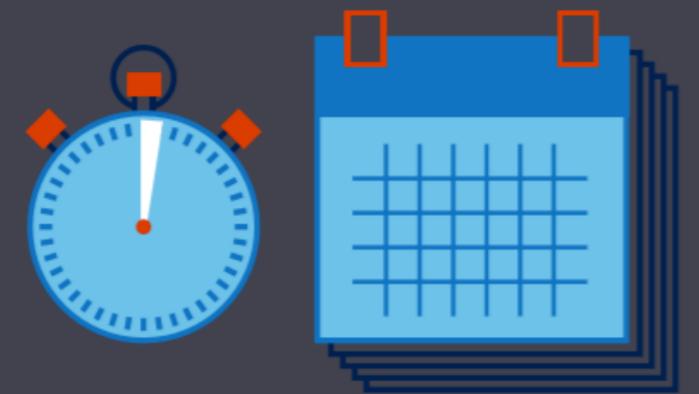
#ntk19



Security in Billions (\$1B)

Big data is transforming how security experts defend against cyberattacks—and Microsoft is leading the way. Our global reach generates billions of data points that help us diagnose attacks, reverse engineer advanced threat techniques, and apply intelligence to strengthen your security.

Just how much is 1 billion?



1 billion seconds equals 32 years



1 billion people equals the population of 117 New York cities



A marble enlarged 1 billion times equals 4x the Earth's size



Security in Billions (\$1B)



Microsoft analyzes many billions of data points every month, building intelligence that is as in-depth as it is far-reaching.²



450 billion

450,000,000,000

cloud authentications
analyzed per month



400 billion

400,000,000,000

emails analyzed for malware
and malicious sites



18 billion

18,000,000,000

Bing webpage scans
per month



1 billion

1,000,000,000

Windows devices
updated monthly



\$15 billion

\$15,000,000,000

invested in Microsoft
cloud infrastructure



\$1 billion

\$1,000,000,000

annually spent
on security

⁽²⁾ "7 Steps to a Holistic Security Strategy," 2017, Microsoft

Integrated toolset for rapid threat remediation

Microsoft Threat Protection

Cloud Native SIEM + SOAR - Azure Sentinel (Preview)
Built on Azure Monitor, Logic Apps, and Microsoft's UEBA/ML Technology

Microsoft Security Center



ENDPOINT

Windows Defender ATP
Endpoint Detection & Response (EDR)



IDENTITY

Azure ATP + Azure AD
Identity Protection



SaaS

Office 365 Advanced
Threat Protection (ATP)
+ Cloud App Security



AZURE

Azure Security
Center



NETWORK



SERVERS



OTHER

3rd party and Microsoft Logs and Tools

Breadth

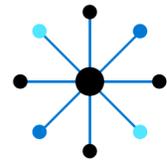
- *Unified Alert Queue*
- *Customized Alerts*

Depth

- *High quality alerts*
- *End to end investigation and remediation*



Core Azure Sentinel Capabilities



Collect

Security data across your enterprise



Detect

Threats with vast threat intelligence



Investigate

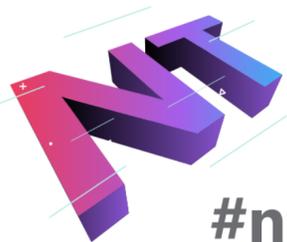
Critical incidents guided by AI



Respond

Rapidly and automate protection

Automate



#ntk19

Components of Azure Sentinel



Collect

- CEF SYSLOG
- Data Connectors
- Agent for Windows Linux

Store

Log Analytics Workspace

- Data is **stored encrypted** at rest in Azure storage
- **Collected data** is available for 31 days by default, but can be **extended to 2 years**

Enrichment

Fusion

Threat Intelligence

Azure ML

Visualize

Dashboards

Power BI

Workbooks

Grafana

Hunting

Pre-defined Queries

Log Analytics

Azure Notebooks

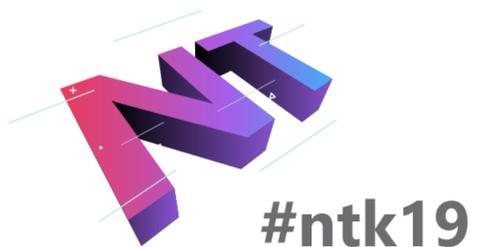
Investigate

Alerts

Cases

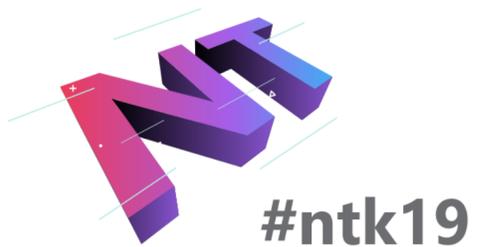
Respond

Logic Apps



Demo #1

- Core components of Azure Sentinel
- Configuring connectors for information/events/log collection



Detect threats and analyze security data quickly with AI

ML models based on **decades of Microsoft security experience and learnings**

Millions of signals filtered to few **correlated and prioritized incidents**

Insights based on vast **Microsoft threat intelligence** and your own TI

Reduce alert fatigue by up to 90%

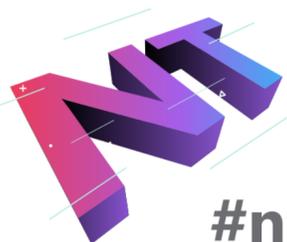
Pre-built Machine Learning models



Correlated rules

Bring your own ML models

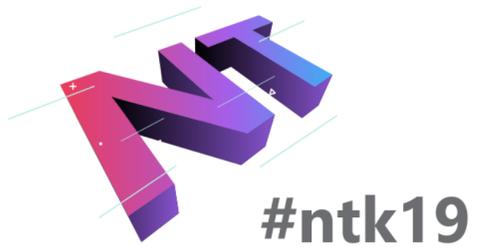
User Entity Behavior Analysis integrated with Microsoft 365



#ntk19

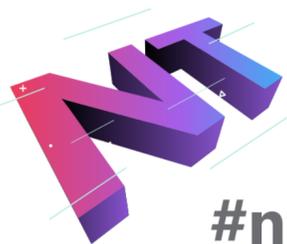
Demo #2

- Exploring Logs in Query Explorer
- Dashboards

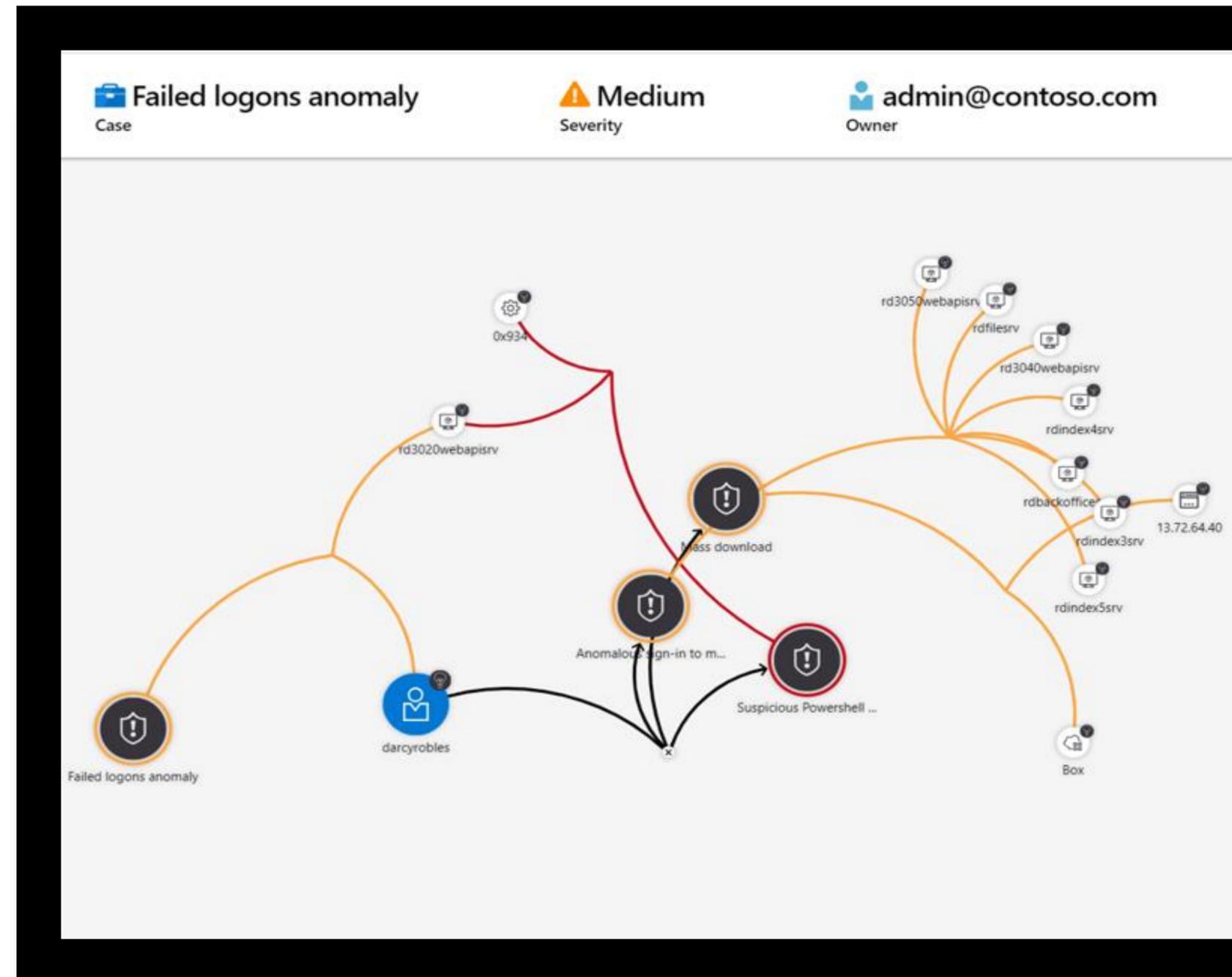


Investigate threats with AI and hunt suspicious activities at scale, tapping into years of cybersecurity work at Microsoft

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

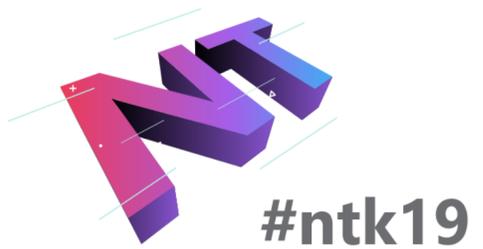


#ntk19

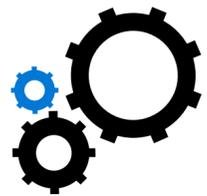


Demo #3

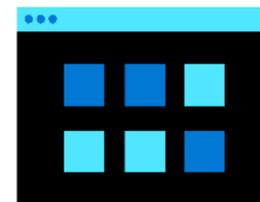
- Cases and investigations



Respond rapidly with built-in orchestration and automation



Build automated and scalable playbooks that integrate across tools



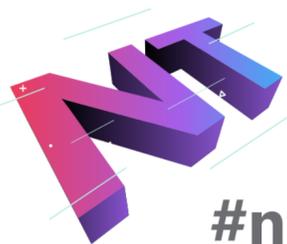
Azure Logic Apps



Security Products

Ticketing Systems
(ServiceNow)

Additional tools



#ntk19

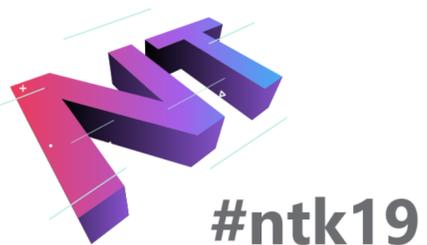
Demo #4

- Threat detection, investigation and response

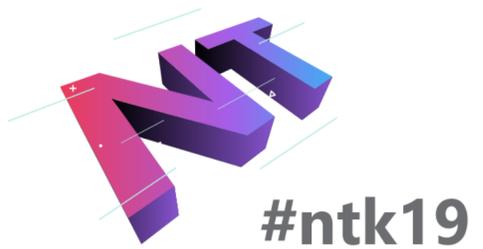
The screenshot displays the Microsoft Azure Logic Apps Designer interface. The workflow is titled "Logic Apps Designer" and is located within the "Alert playbooks" section. The workflow starts with a trigger: "When a response to an Azure Security Center alert is triggered". This is followed by a sequence of actions: "Create incident in Service Now(Preview)", "Post message to SOC channel(Preview)", and "Send approval email". A condition step follows, with the logic: "And" (Selected... x is equal to Block user and IP). The workflow then branches into two paths: "If true" and "If false". The "If true" path contains two actions: "Block user in Azure AD" and "BlockIPPalto". The "If false" path contains one action: "Close incident in Service Now(Preview)". The interface includes a search bar at the top, navigation links, and various toolbars for saving, running, and adding new steps.

Summary

- Cloud-native SIEM for intelligent security analytics for your entire enterprise
- The service is currently in Public Preview → Go and test it!
- To learn more, visit <https://aka.ms/AzureSentinel>



Additional questions?





2019

NT KONFERENCA

21. - 23. MAJ 2019

#ntk19