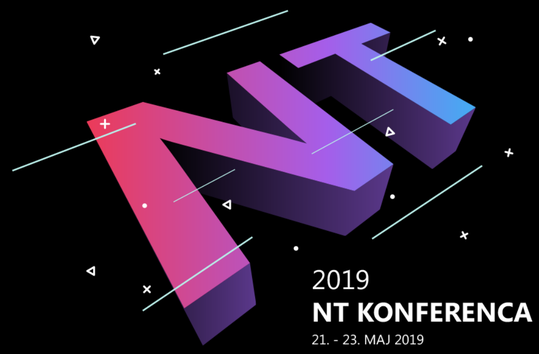
2019

NT KONFERENCA

21. - 23. MAJ 2019

#ntk19



#ntk19

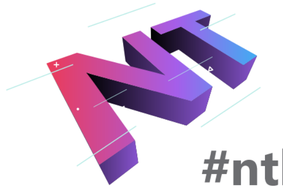
Azure Sentinel - SIEM v oblaku

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

Vehicles

Smart cities

Sensors

Energy systems

Marketplaces

Equipment

Partners

Customers

Citizens

Supply chains

On-premises

Manufacturers

Mobile devices

Traditional SOC Challenges

- High volume of noisy alerts
- IT deployment & maintenance
- Sophistication of threats
- Rising infrastructure costs and upfront investment
- Too many disconnected products
- Lack of automation
- Security skills in short supply

Security
Operations Team

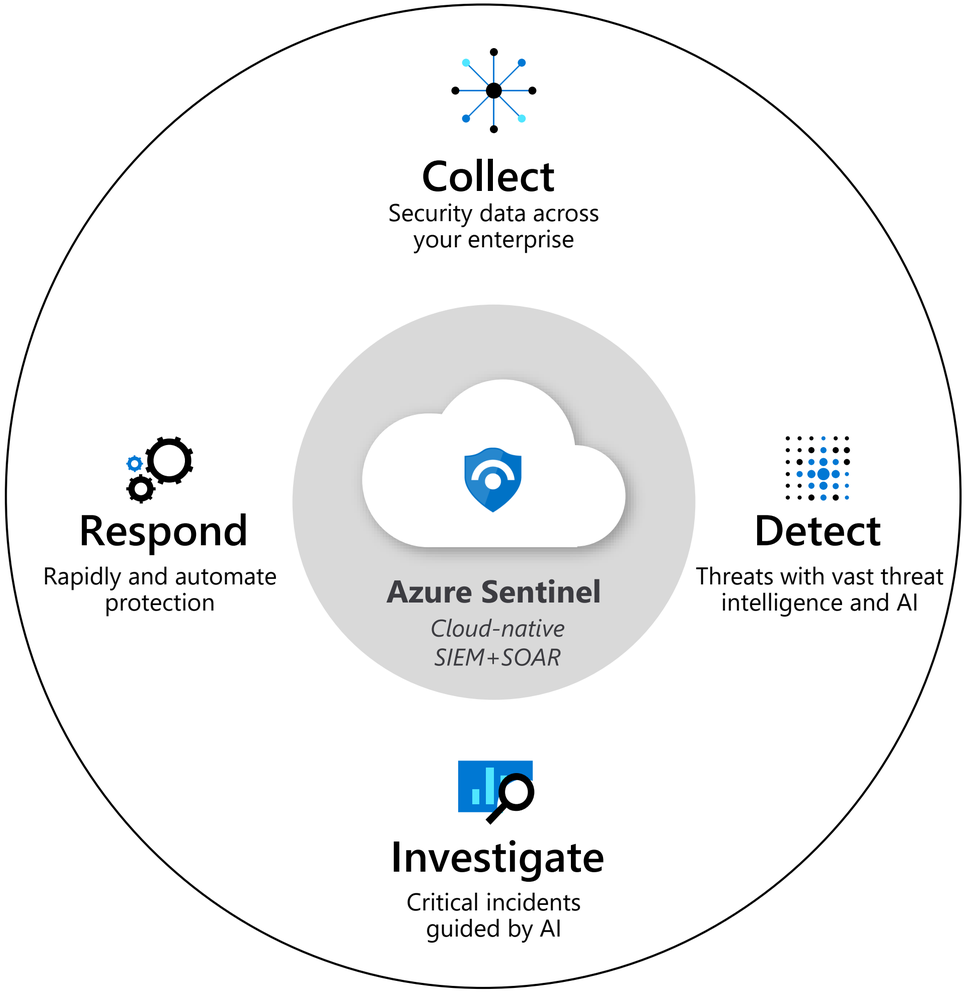
+

Cloud + Artificial Intelligence

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

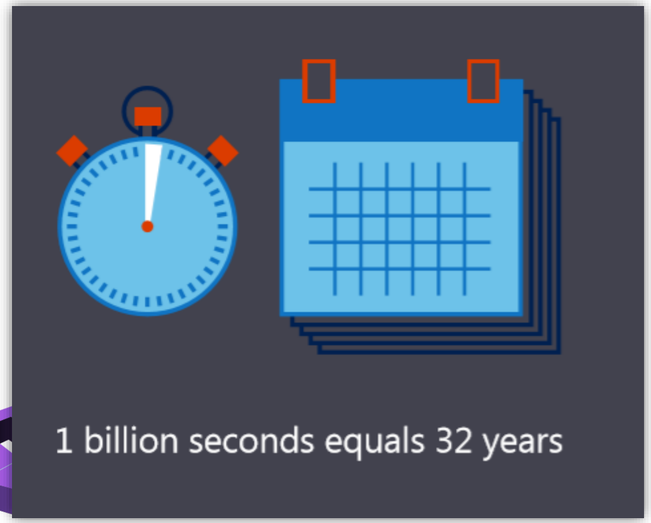
- $1B annual investment in cybersecurity
- 3500+ global security experts
- Trillions of diverse signals for unparalleled intelligence

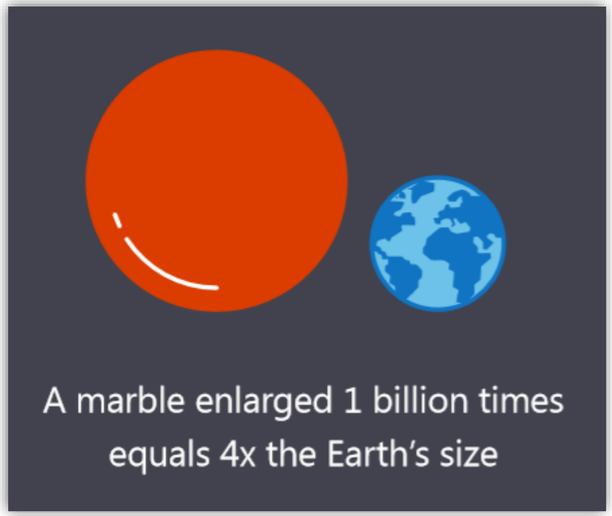
#ntk19

Security in Billions ($1B)

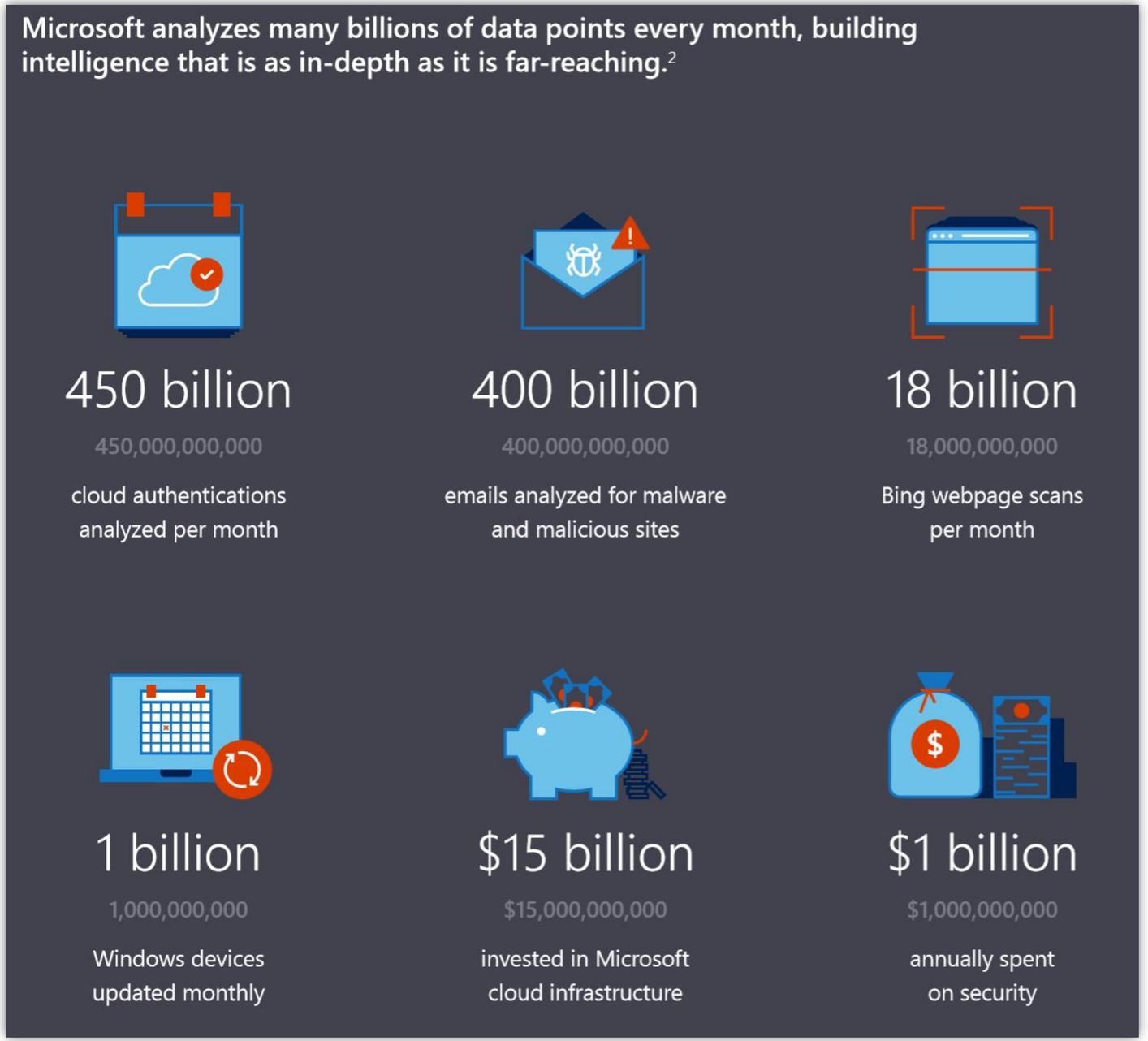
Big data is transforming how security experts defend against cyberattacks—and Microsoft is leading the way. Our global reach generates billions of data points that help us diagnose attacks, reverse engineer advanced threat techniques, and apply intelligence to strengthen your security.

Just how much is 1 billion?





Security in Billions ($1B)



#ntk19

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

Integrated toolset for rapid threat remediation

Microsoft Threat Protection

Breadth
- *Unified Alert Queue*
- *Customized Alerts*

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

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

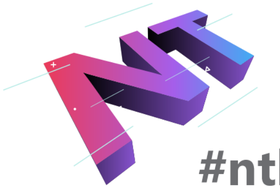
Investigate

Critical incidents guided by AI

Respond

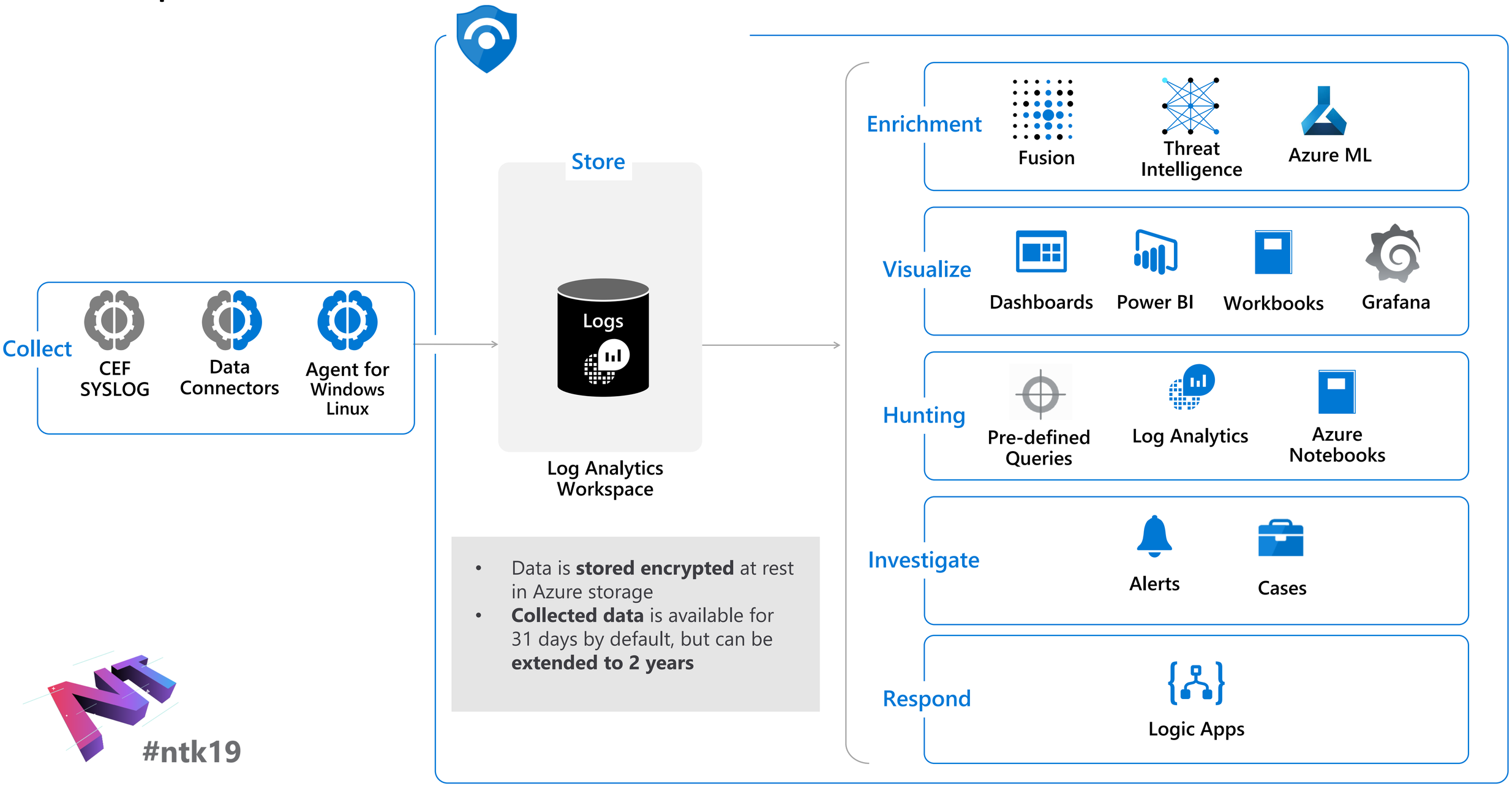
Rapidly and automate protection

Automate



#ntk19

Components of Azure Sentinel

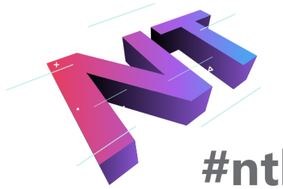


- Data is **stored encrypted** at rest in Azure storage
- **Collected data** is available for 31 days by default, but can be **extended to 2 years**

#ntk19

Demo #1

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



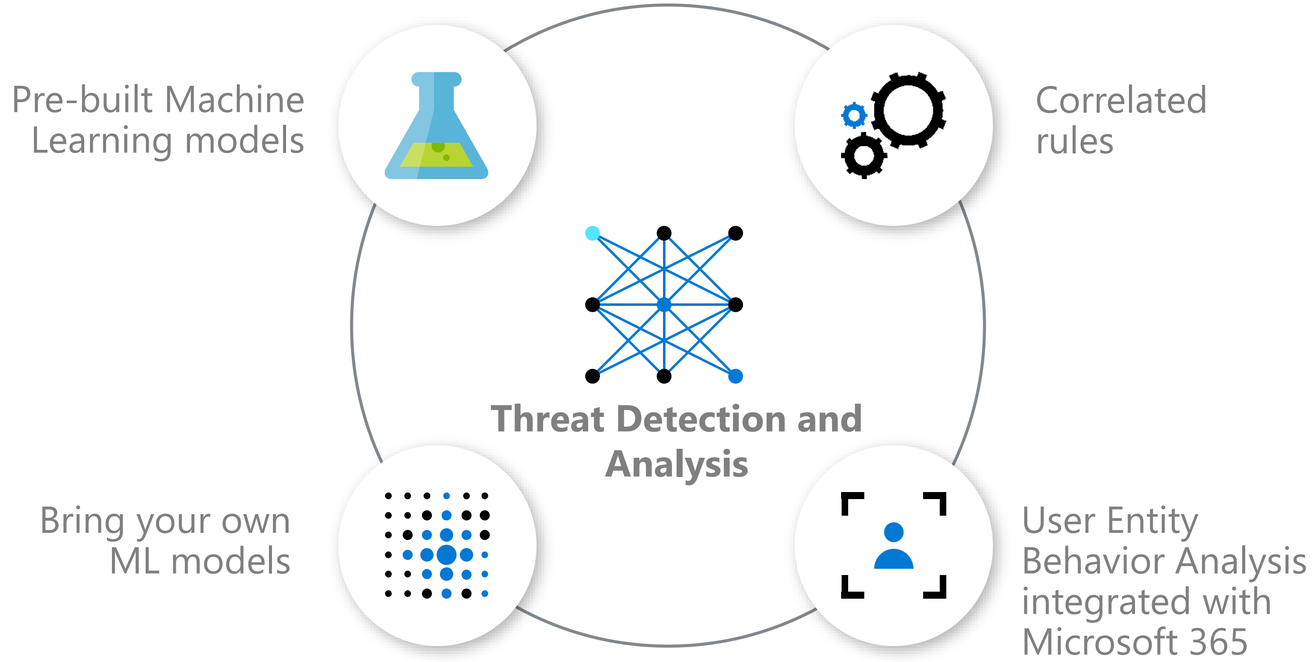
Detect threats and analyze security data quickly with AI

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

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

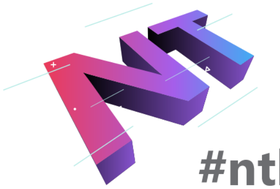
Insights based on vast **Microsoft threat intelligence** and your own TI

Reduce alert fatigue by up to 90%



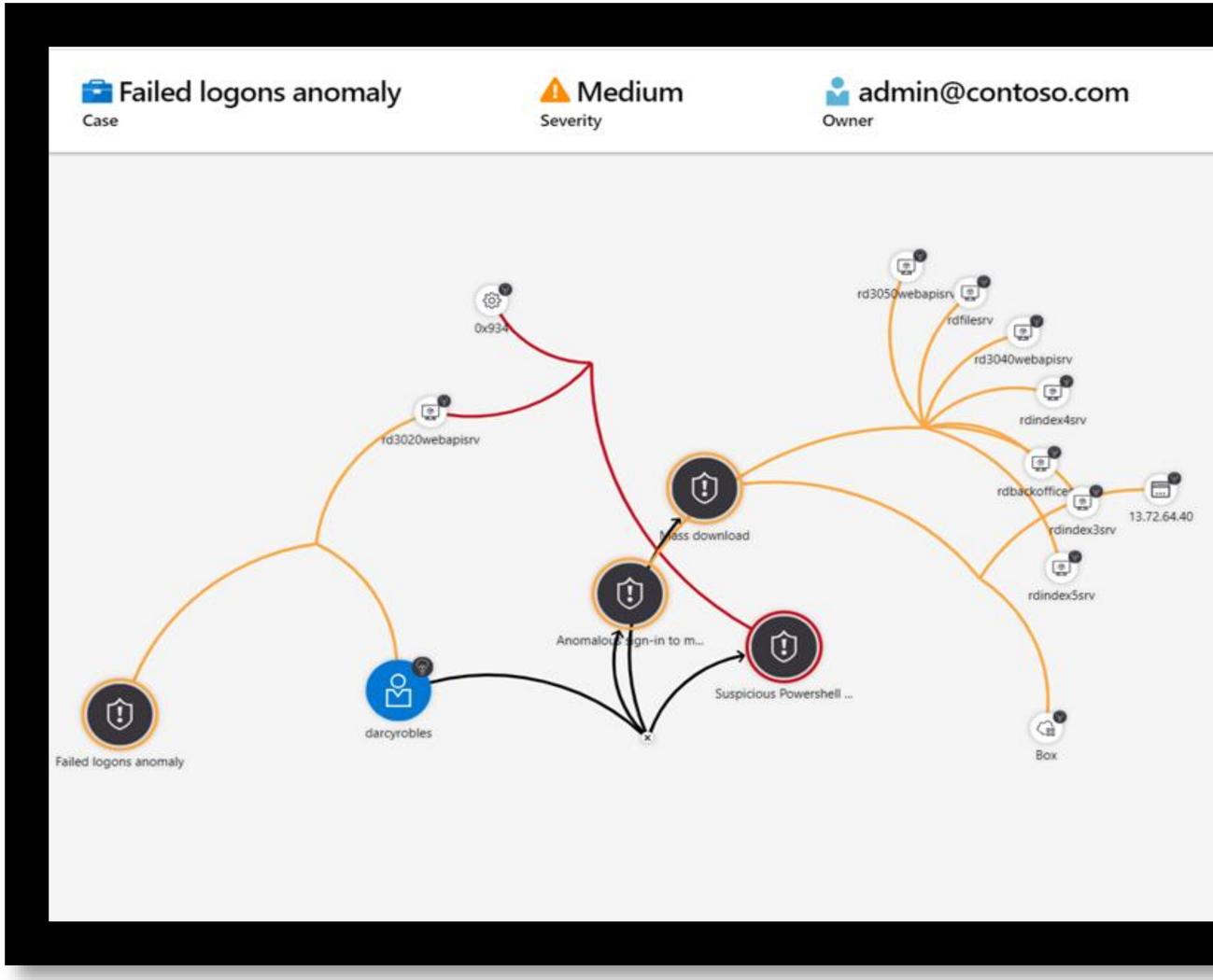
Demo #2

- Exploring Logs in Query Explorer
- Dashboards



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

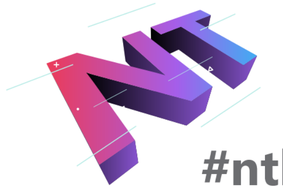
- Get prioritized alerts and **automated expert guidance**
- **Visualize** the entire attack and its impact
- Hunt for suspicious activities using **pre-built queries and Azure Notebooks**



#ntk19

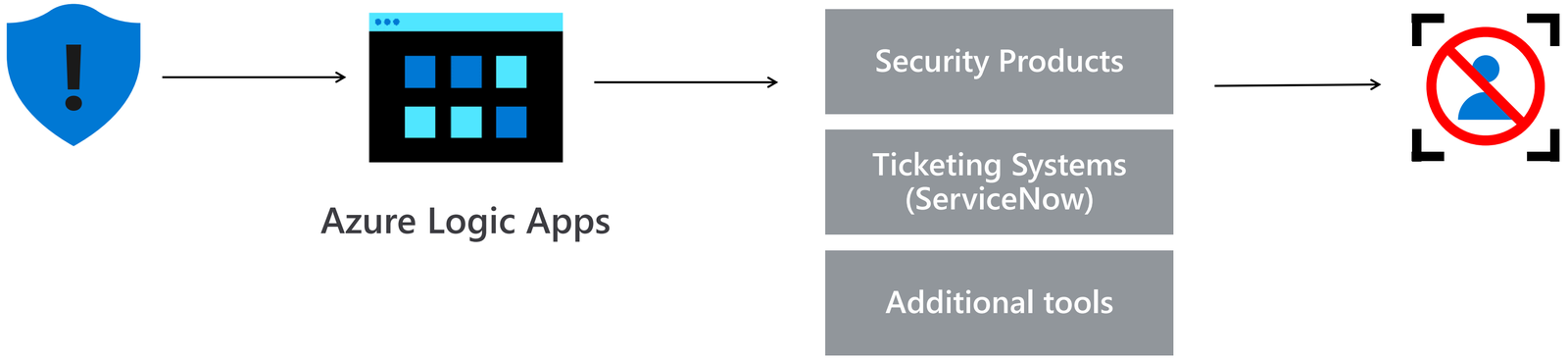
Demo #3

- Cases and investigations



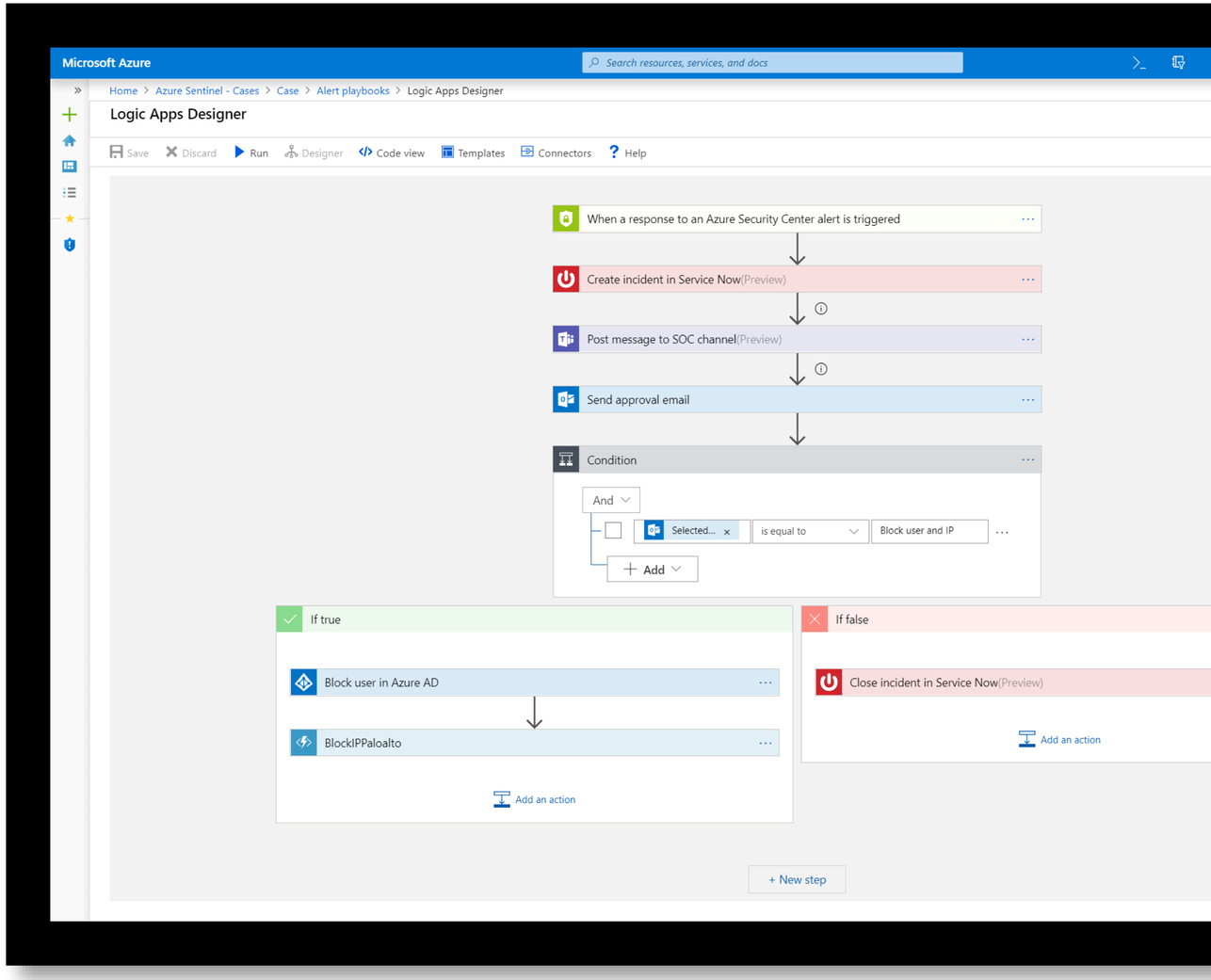
Respond rapidly with built-in orchestration and automation

Build automated and scalable playbooks that integrate across tools



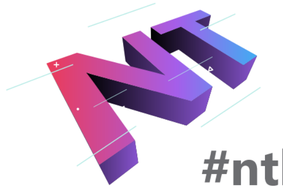
Demo #4

- Threat detection, investigation and response

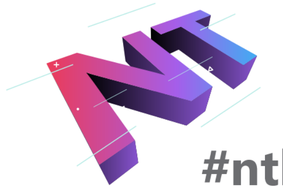


Summary

- 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