Tobias Kritten

Defender Security Center – was nun?

Vielen Dank an unsere Sponsoren!

PLATINUM SPONSOR

GOLD SPONSOR

azure geek.io

Cloud (Security) ist meine Leidenschaft

Seit über 15 Jahren helfe ich Unternehmen beim sicheren Einsatz von Microsoft-Technologien: zu Beginn mit meinem eigenen Systemhaus, später durch das Hosting von Exchange, SharePoint- und Microsoft-basierten Applikationen und heute schwerpunktmäßig in der Cloud durch den Einsatz von Microsoft Security-Lösungen und Konzepte wie Azure AD, der Defender-Produktreihe oder Zero Trust.

Cloud Security Portfolio (Auszug)

- Einführung Security-Lösungen (Microsoft Defender for X, Intune, DarkTrace, etc.)
- Durchführung von Security-related Best Practice Workshops und Audits
- Einführung von und Beratung rund um Zero Trust-Konzepte

Cloud Networking Portfolio (Auszug)

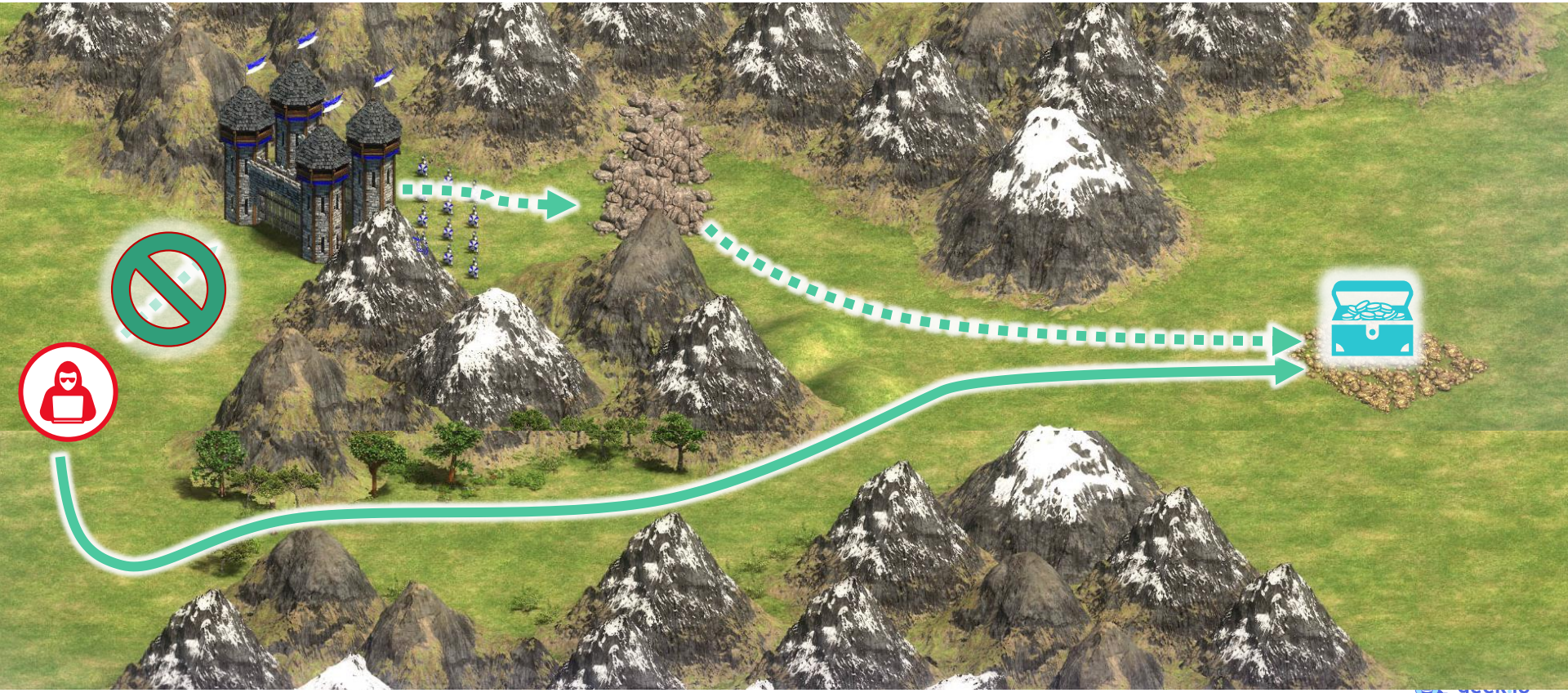
- Integration von Networking-Themen in Cloud-Umgebungen
- Beratung und Problem-Solving in komplexen Networking-Architekturen
- Fokus auf die Integration von Fortinet-Lösungen in Azure-Umgebungen

azure geek.io

Recap

… Angreifer nutzen den Weg des geringsten Widerstand/Kosten!

Angreifer folgen unseren “geplanten” Angriffs-Szenarien

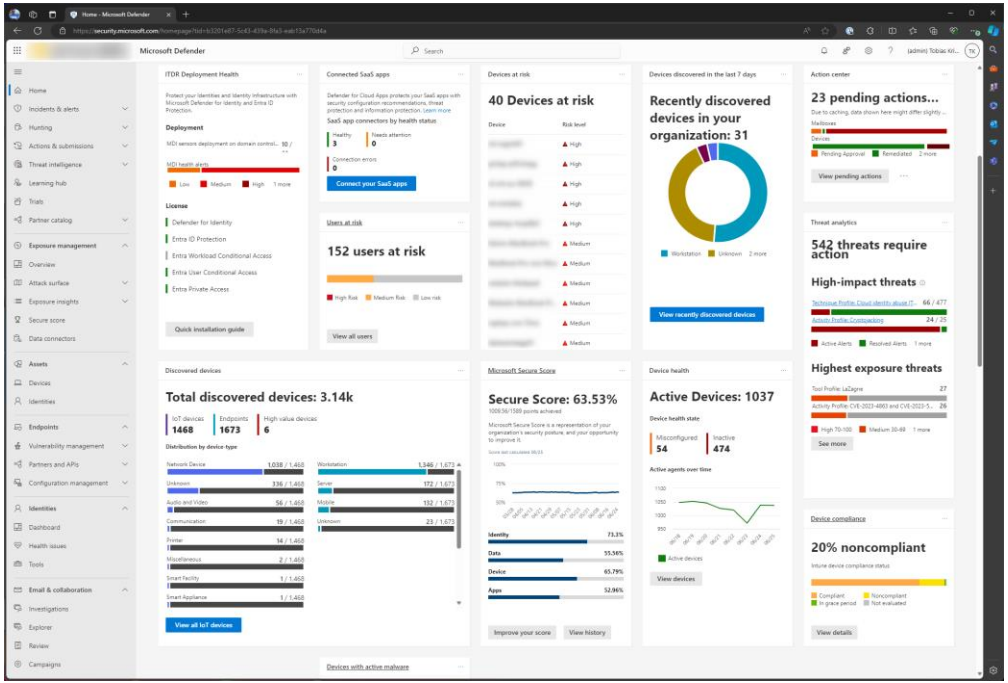


Defender Security Center - Datenquellen

Defender for Office 365

Defender for Endpoint / XDR

Entra ID Identity Protection

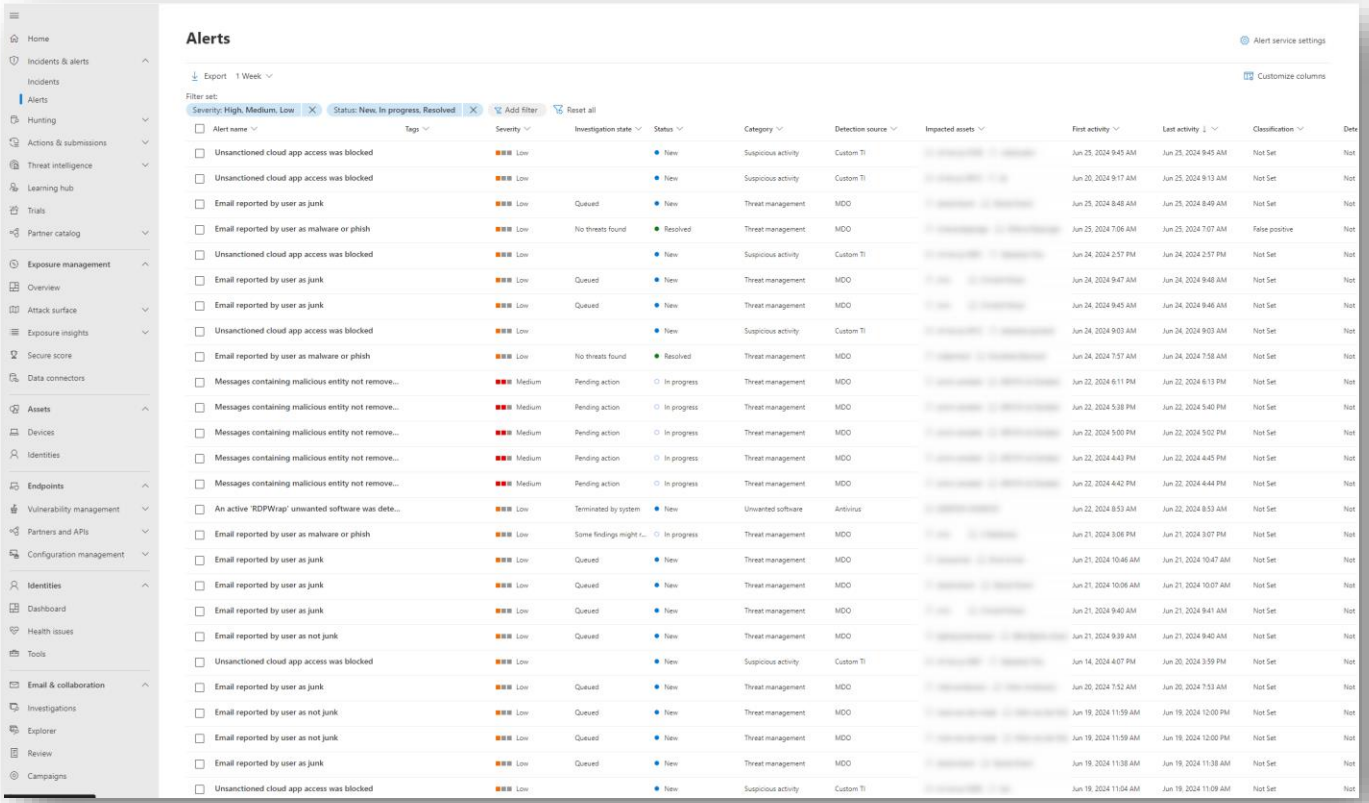


Defender for Identity

Defender for Cloud Apps

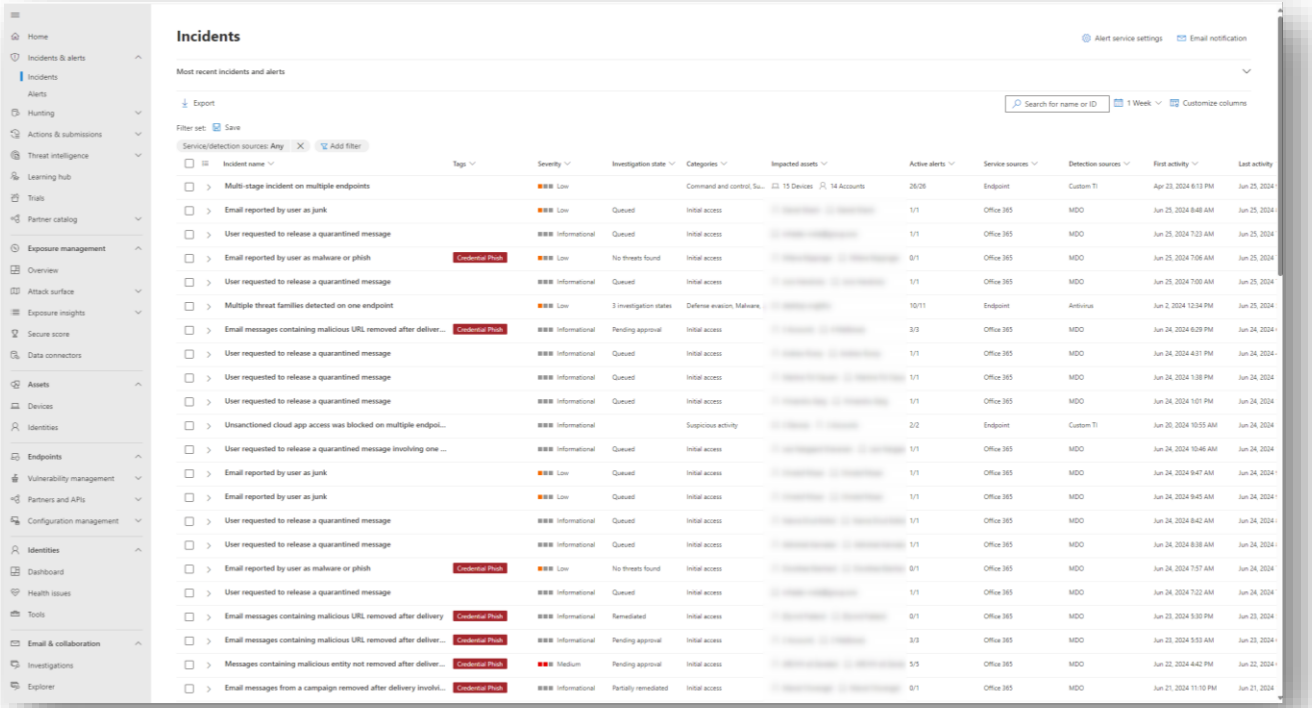
Alerts

- Meldung über ein spezifisches Ereignis
- Entspricht einem “Signal”
- Isolierte Sicht

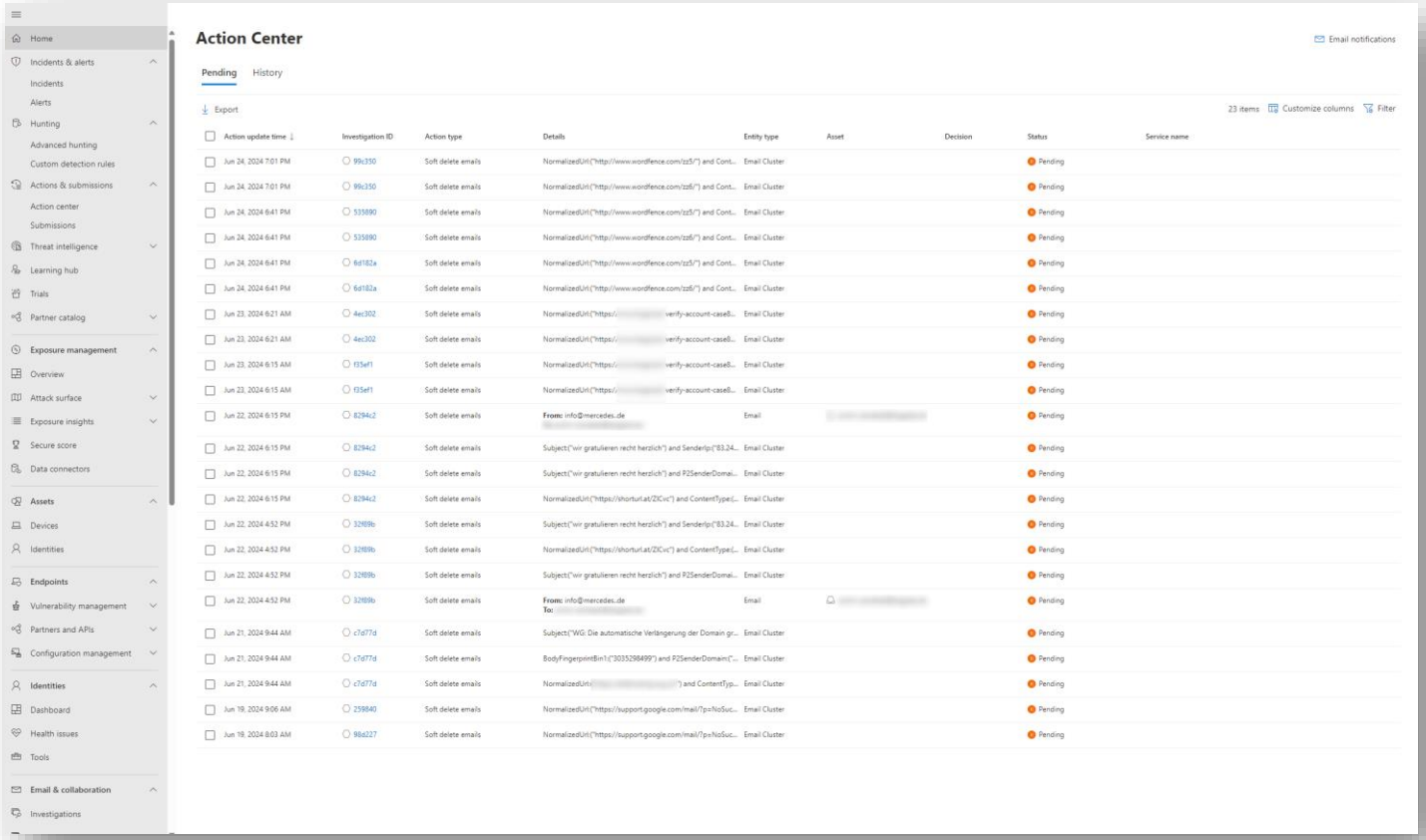


Incidents

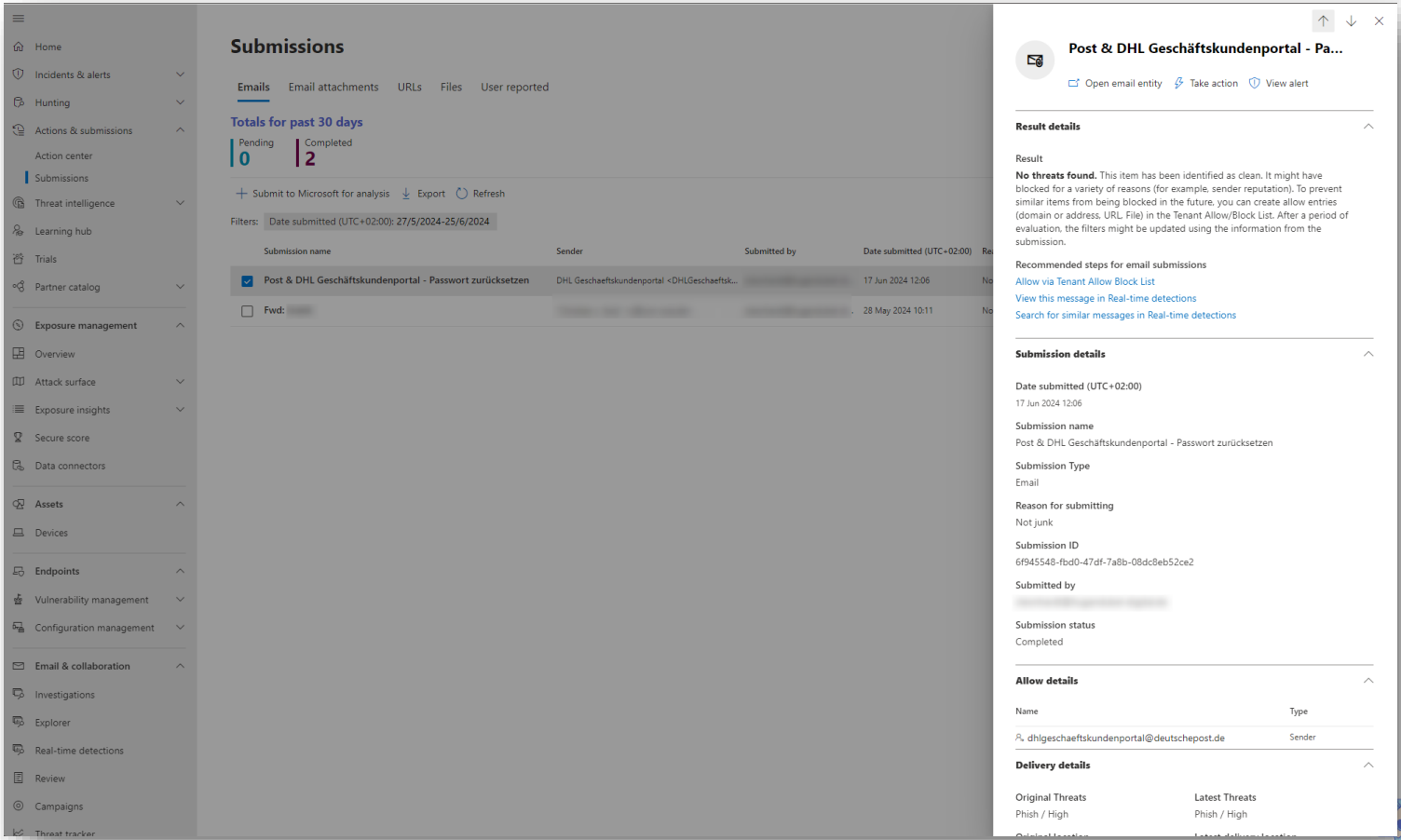
- Sammlung von Alerts zusammenhängender Signals
- Erzählen eine “Story”



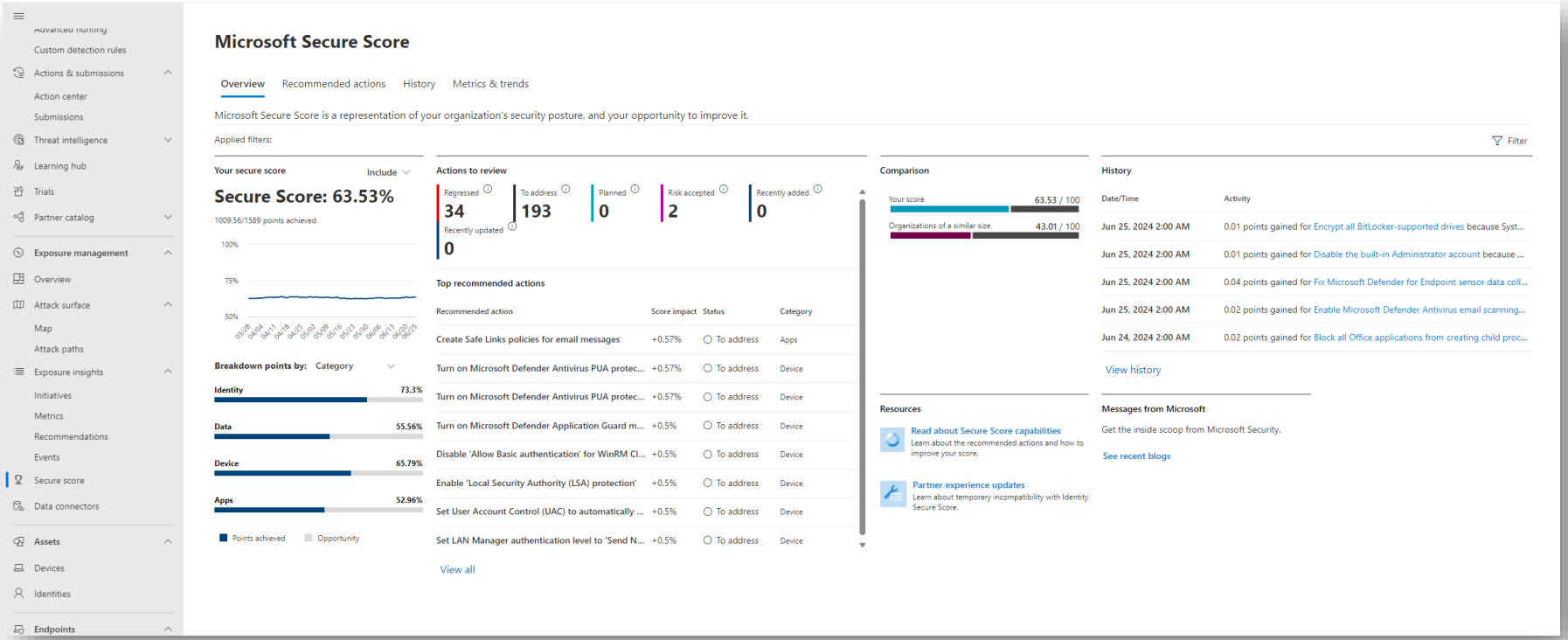
Action Center: Single Pane of Glass



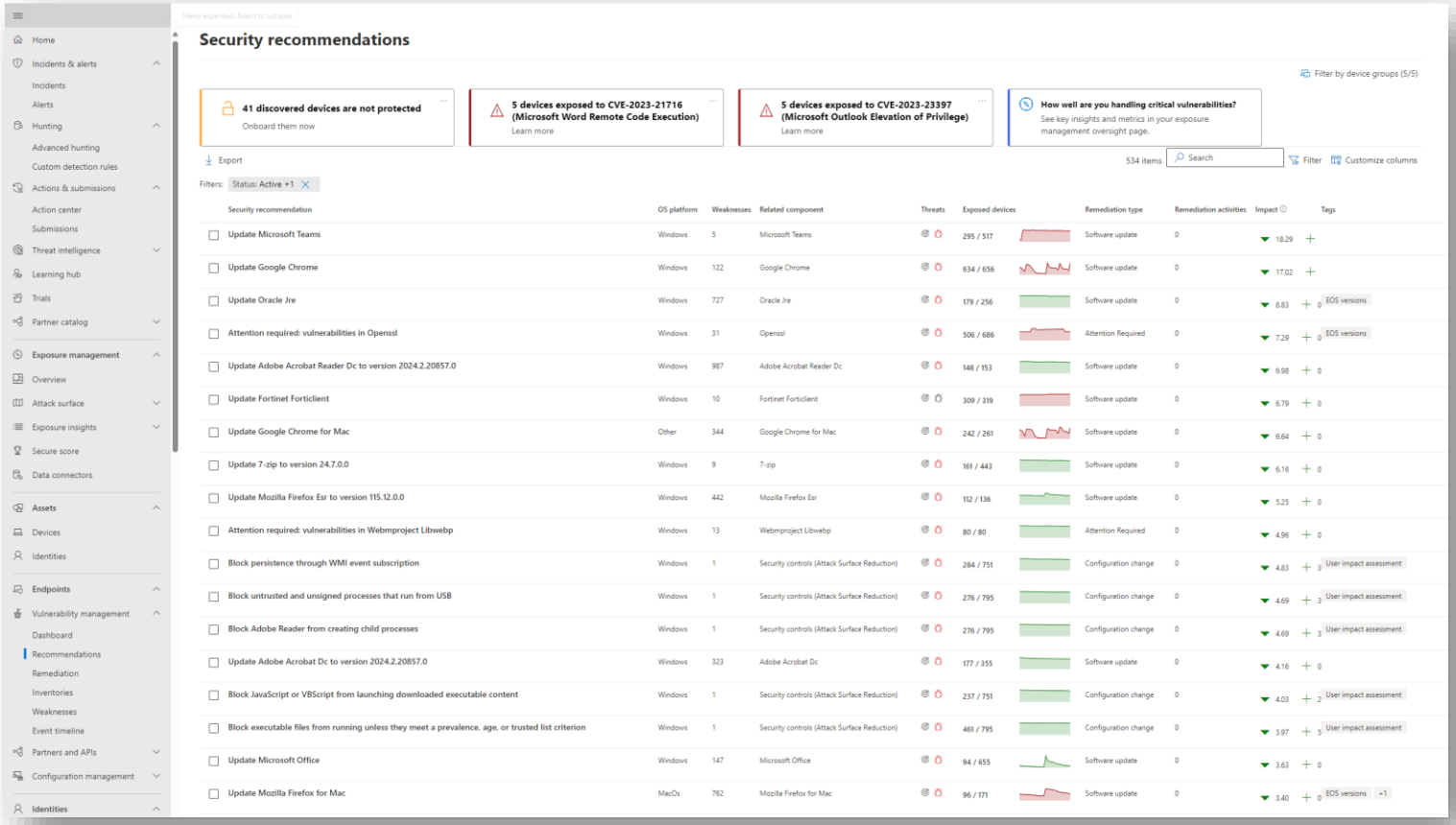
Submissions



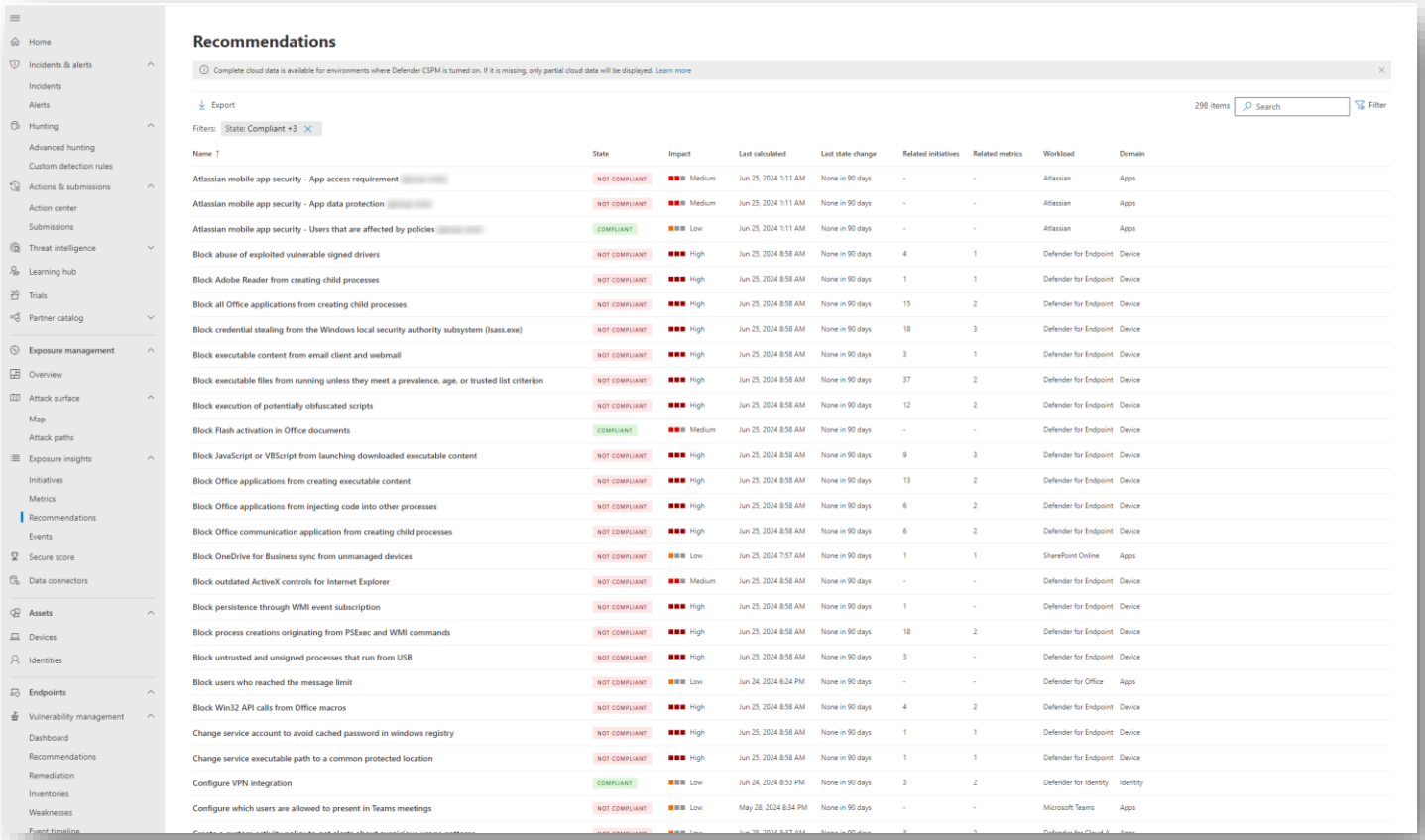
Secure Scores

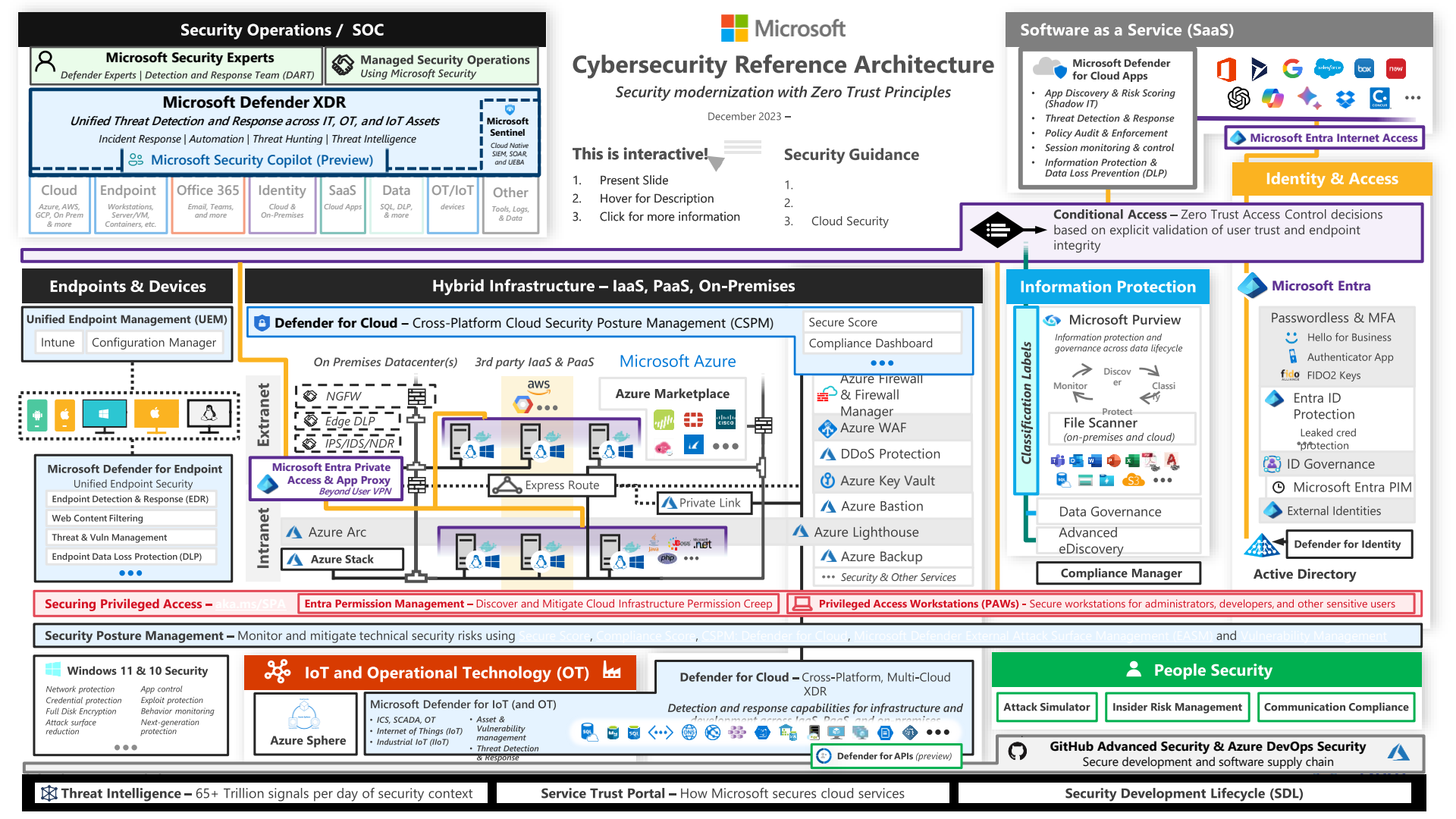


Vulnerability Management - Recommendations



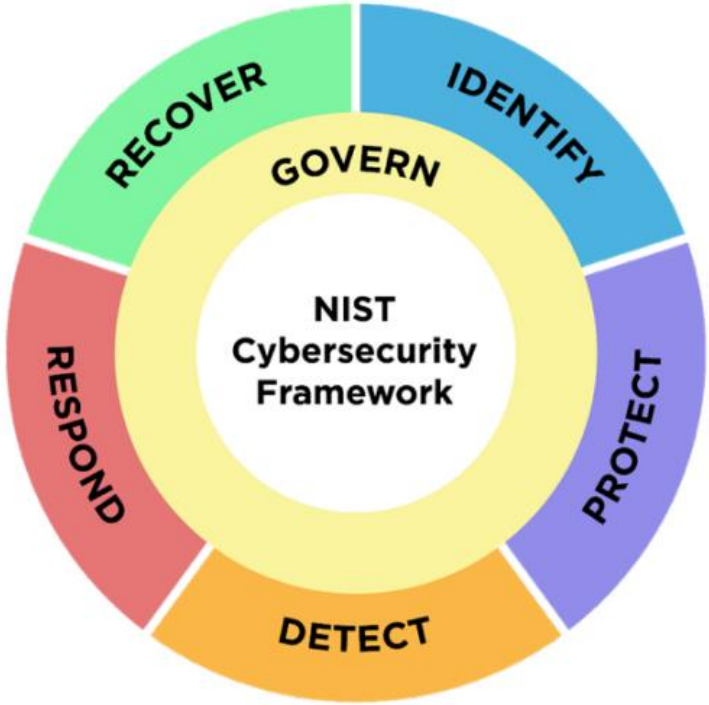
Exposure Management - Recommendations



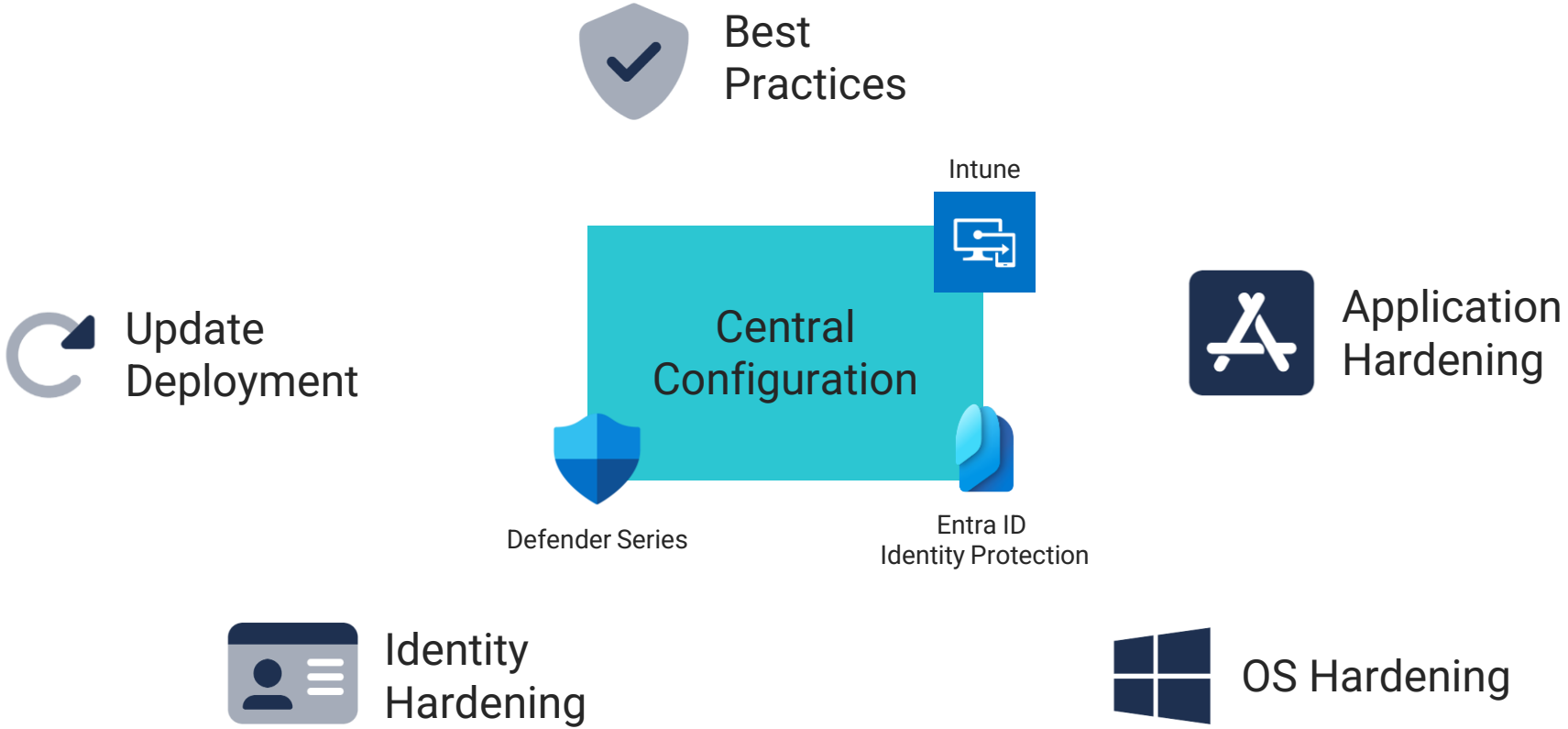

Microsoft
Cybersecurity Reference Architecture
Security modernization with Zero Trust Principles
December 2023 –
This is interactive!
1. Present Slide
2. Hover for Description
3. Click for more information
Security Guidance
1.
2.
3. Cloud Security
Security Operations / SOC
Microsoft Security Experts
Defender Experts | Detection and Response Team (DART)
Managed Security Operations
Using Microsoft Security
Microsoft Defender XDR
Unified Threat Detection and Response across IT, OT, and IoT Assets
Incident Response | Automation | Threat Hunting | Threat Intelligence
Microsoft Security Copilot (Preview)
Microsoft Sentinel
Cloud Native SIEM, SOAR, and UEBA
Cloud
Azure, AWS, GCP, On Prem & more
Endpoint
Workstations, Server/VM, Containers, etc.
Office 365
Email, Teams, and more
Identity
Cloud & On-Premises
SaaS
Cloud Apps
Data
SQL, DLP, & more
OT/IoT
devices
Other
Tools, Logs, & Data
Software as a Service (SaaS)
Microsoft Defender for Cloud Apps
App Discovery & Risk Scoring (Shadow IT)
Threat Detection & Response
Policy Audit & Enforcement
Session monitoring & control
Information Protection & Data Loss Prevention (DLP)
Microsoft Entra Internet Access
Identity & Access
Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity
Endpoints & Devices
Unified Endpoint Management (UEM)
Intune
Configuration Manager
Microsoft Defender for Endpoint
Unified Endpoint Security
Endpoint Detection & Response (EDR)
Web Content Filtering
Threat & Vuln Management
Endpoint Data Loss Protection (DLP)
Hybrid Infrastructure – IaaS, PaaS, On-Premises
Defender for Cloud – Cross-Platform Cloud Security Posture Management (CSPM)
Secure Score
Compliance Dashboard
On Premises Datacenter(s)
3rd party IaaS & PaaS
Microsoft Azure
Extranet
Intranet
NGFW
Edge DLP
IPS/IDS/NDR
Microsoft Entra Private Access & App Proxy
Beyond User VPN
Express Route
Private Link
Azure Arc
Azure Stack
Azure Marketplace
Azure Firewall & Firewall Manager
Azure WAF
DDoS Protection
Azure Key Vault
Azure Bastion
Azure Lighthouse
Azure Backup
Security & Other Services
Information Protection
Classification Labels
Microsoft Purview
Information protection and governance across data lifecycle
Monitor
Discover
Classify
Protect
File Scanner
(on-premises and cloud)
Data Governance
Advanced eDiscovery
Compliance Manager
Microsoft Entra
Passwordless & MFA
Hello for Business
Authenticator App
FIDO2 Keys
Entra ID Protection
Leaked cred protection
ID Governance
Microsoft Entra PIM
External Identities
Defender for Identity
Active Directory
Securing Privileged Access – aka.ms/SPA
Entra Permission Management – Discover and Mitigate Cloud Infrastructure Permission Creep
Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users
Security Posture Management – Monitor and mitigate technical security risks using Secure Score, Compliance Score, CSPM, Defender for Cloud, Microsoft Defender External Attack Surface Management (EASM) and Vulnerability Management
Windows 11 & 10 Security
Network protection
Credential protection
Full Disk Encryption
Attack surface reduction
App control
Exploit protection
Behavior monitoring
Next-generation protection
IoT and Operational Technology (OT)
Azure Sphere
Microsoft Defender for IoT (and OT)
ICS, SCADA, OT
Internet of Things (IoT)
Industrial IoT (IIoT)
Asset & Vulnerability management
Threat Detection & Response
Defender for Cloud – Cross-Platform, Multi-Cloud XDR
Detection and response capabilities for infrastructure and development across IaaS, PaaS, and on-premises
Defender for APIs (preview)
People Security
Attack Simulator
Insider Risk Management
Communication Compliance
GitHub Advanced Security & Azure DevOps Security
Secure development and software supply chain
Threat Intelligence – 65+ Trillion signals per day of security context
Service Trust Portal – How Microsoft secures cloud services
Security Development Lifecycle (SDL)

… und jetzt?!

Pragmatische IT-Security-Strategie für SMB



Dimension “Configuration”



Dimension “Operations”

Alert &
Incident
Management

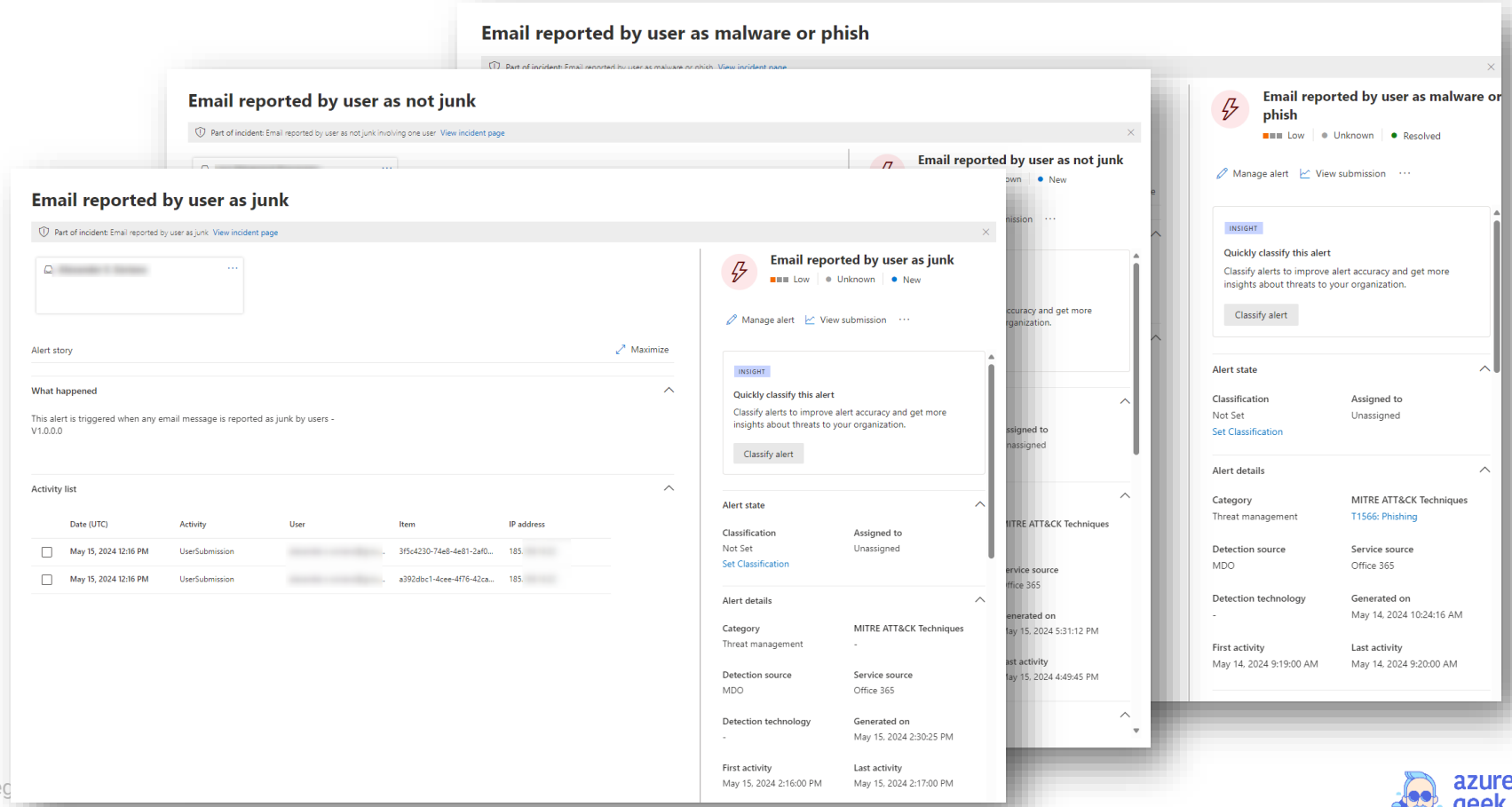
Security
Operations
Platform

Defender Security
Center

Vulnerability
Monitoring

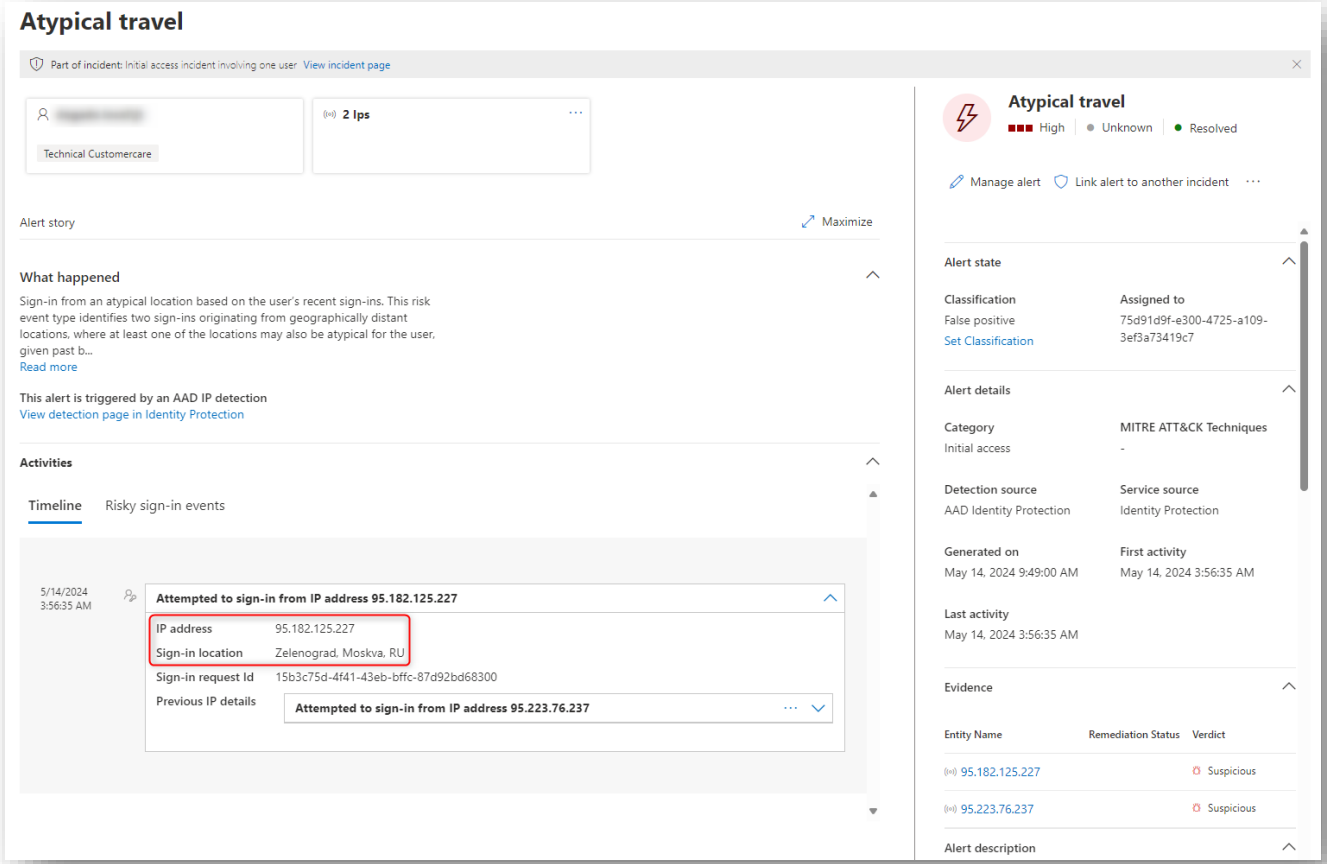
Gängige Alerts & Incidents

E-Mail reported as junk / not junk / malware / phish

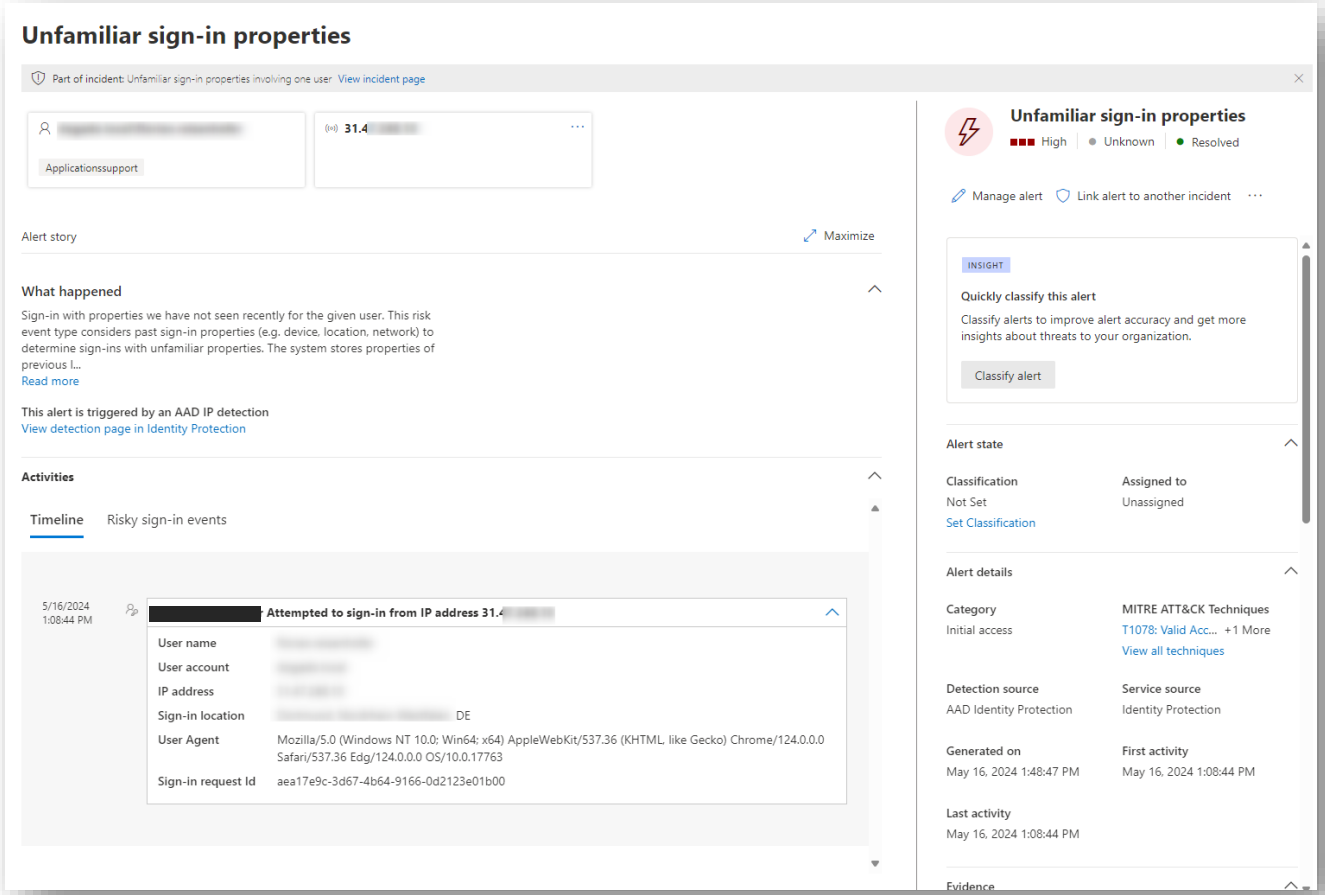


azure geek.io

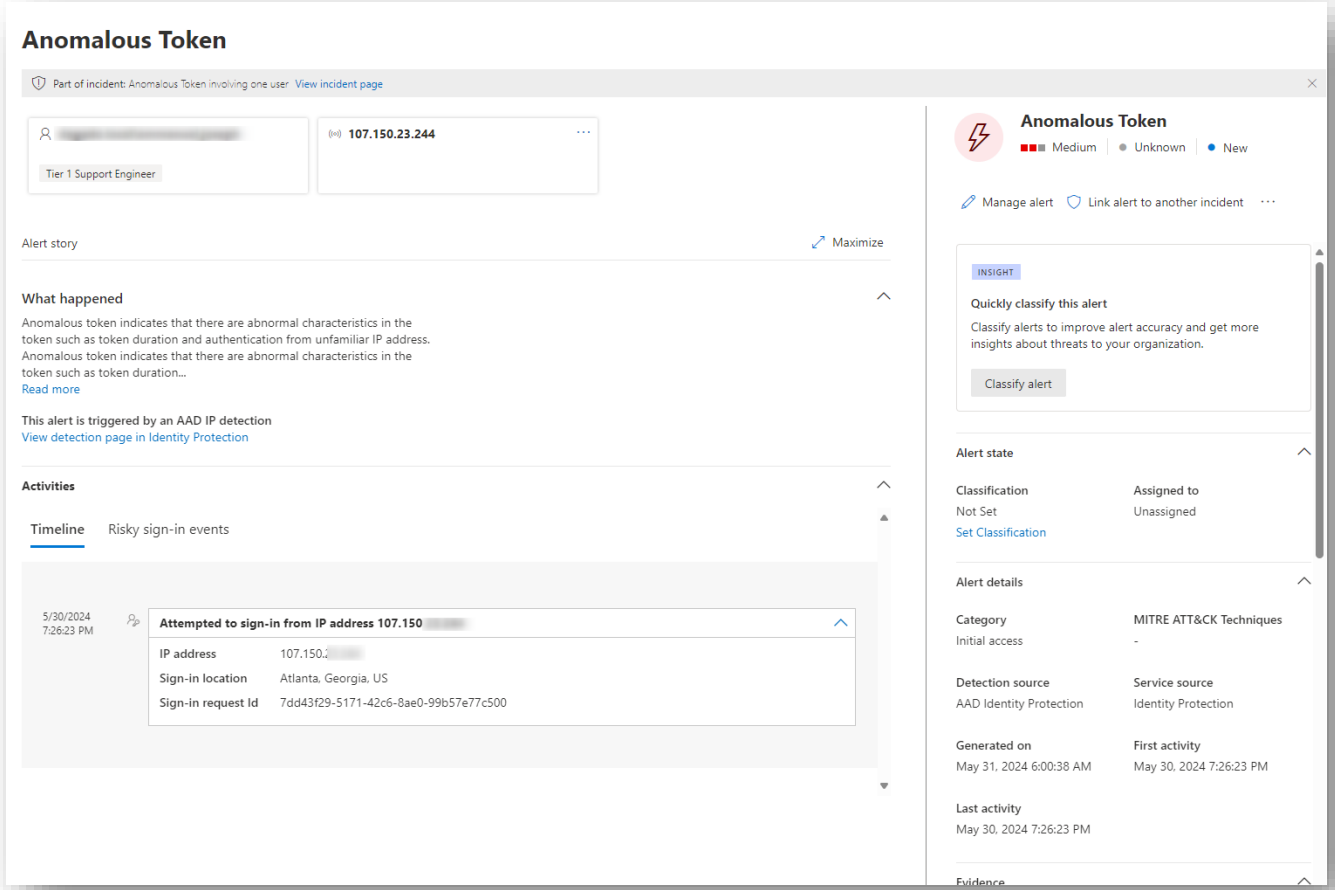
Atypical Travel



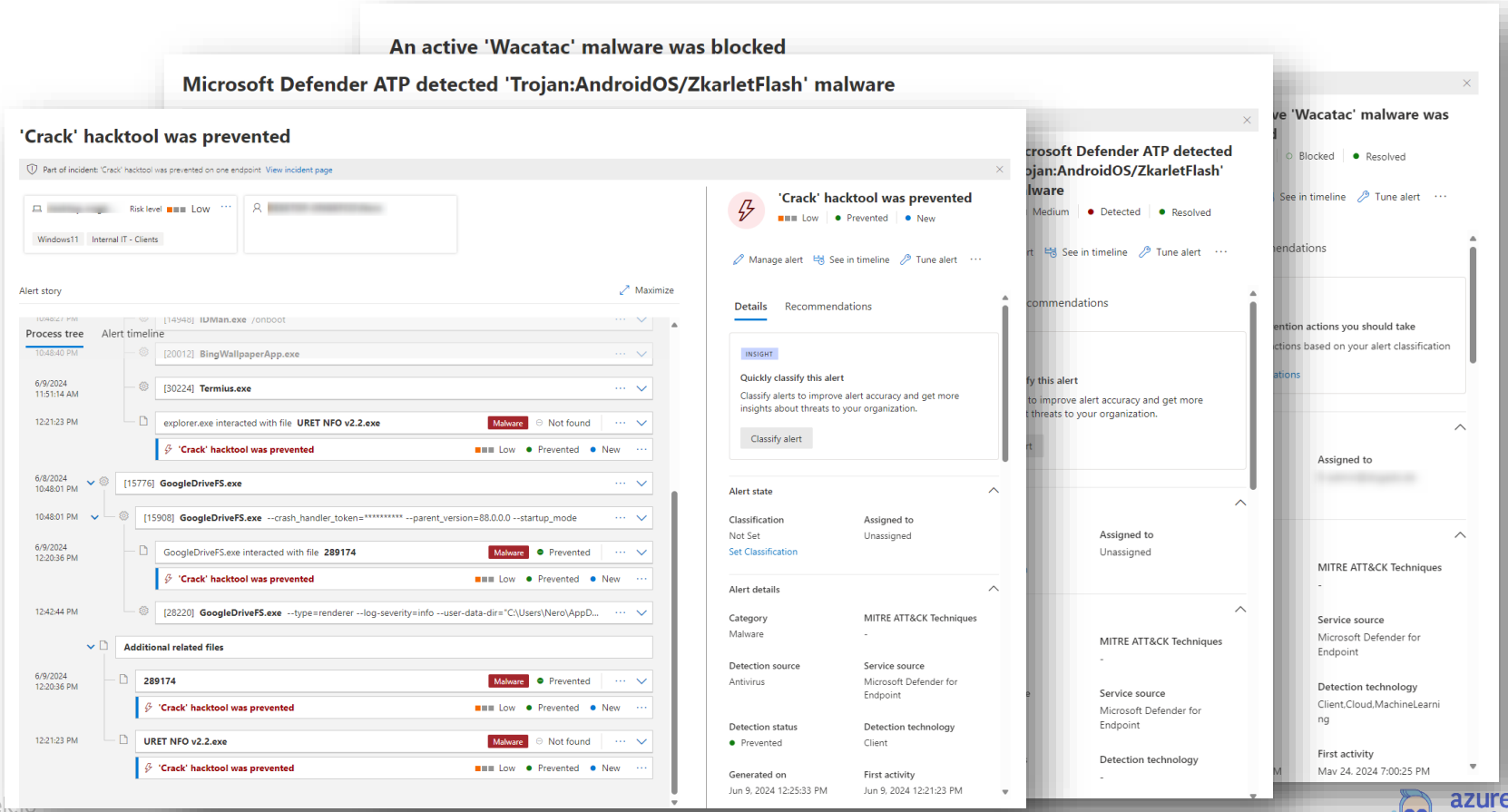
Unfamiliar sign-in properties



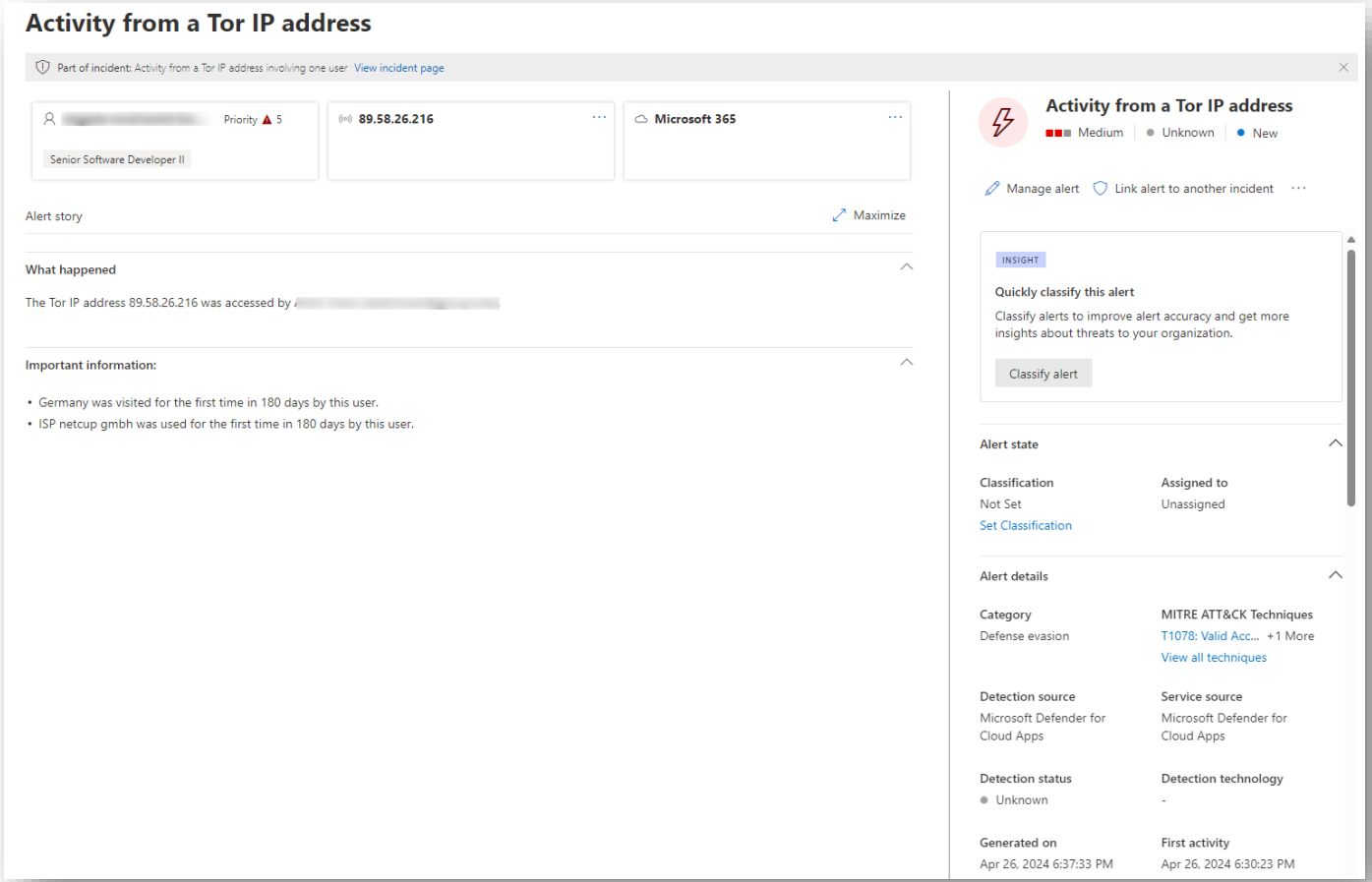
Anomalous Token



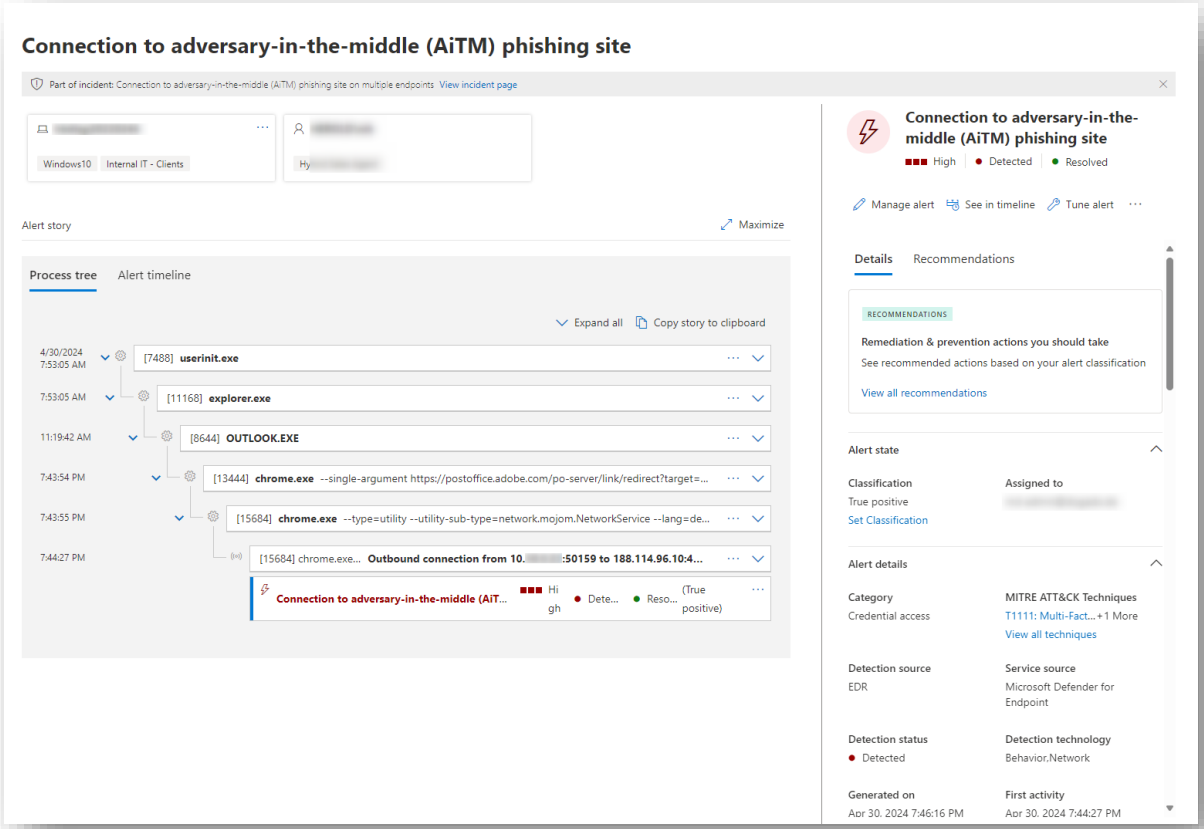
Malware was blocker / hacktool was prevented



Activity from TOR IP

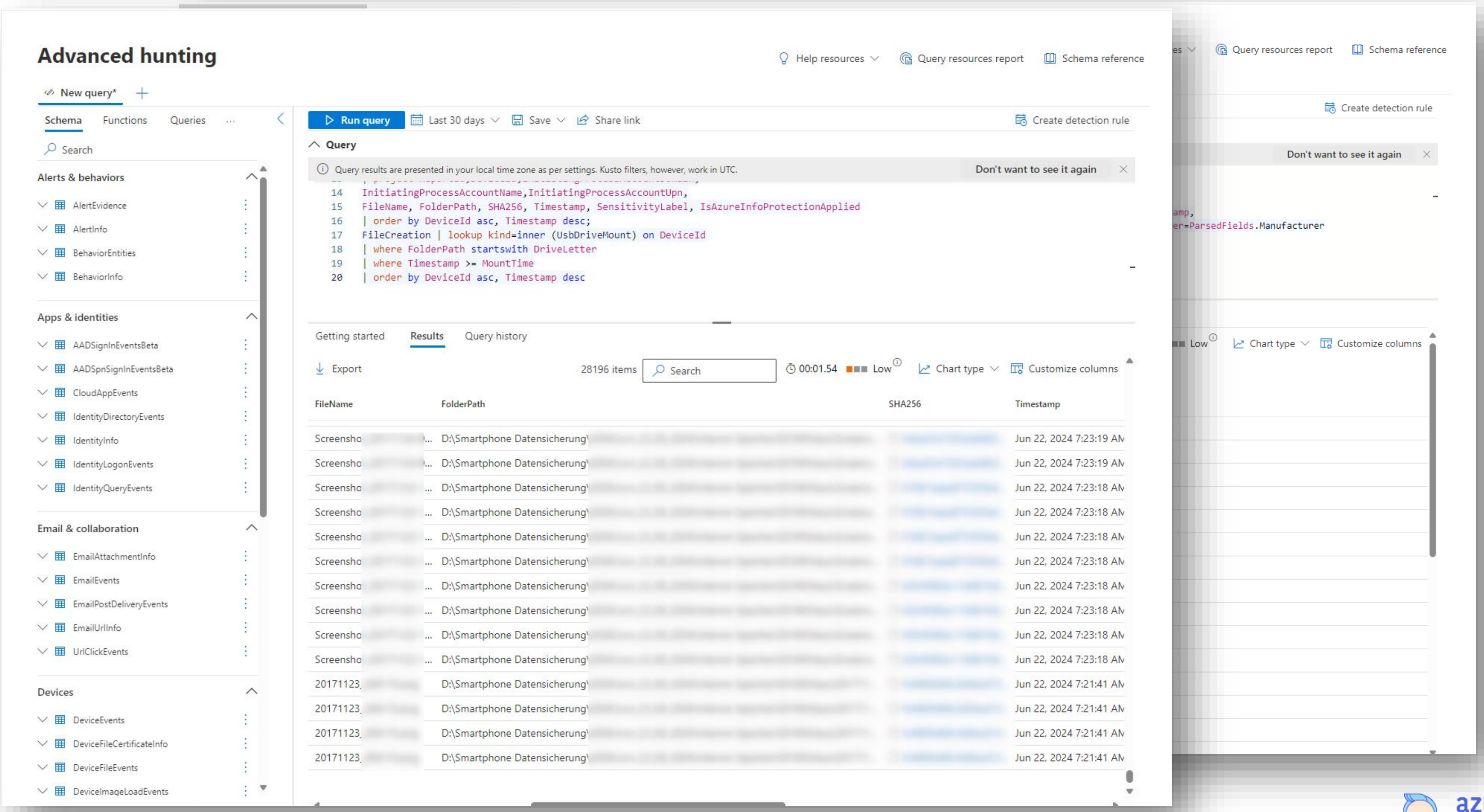


Connection to adversary-in-the-middle Phishing Site



Kritische Alerts: AD CS Attack tool, DPAPI, etc.

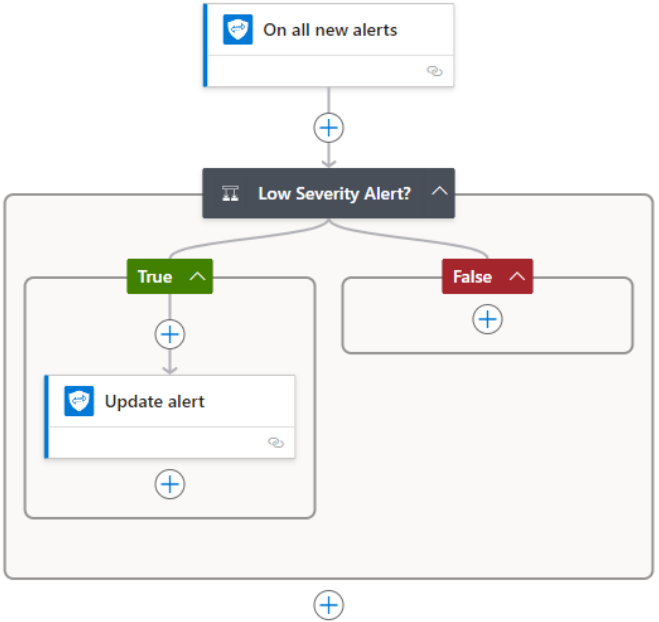
Advanced Hunting - USB



Automatisierung

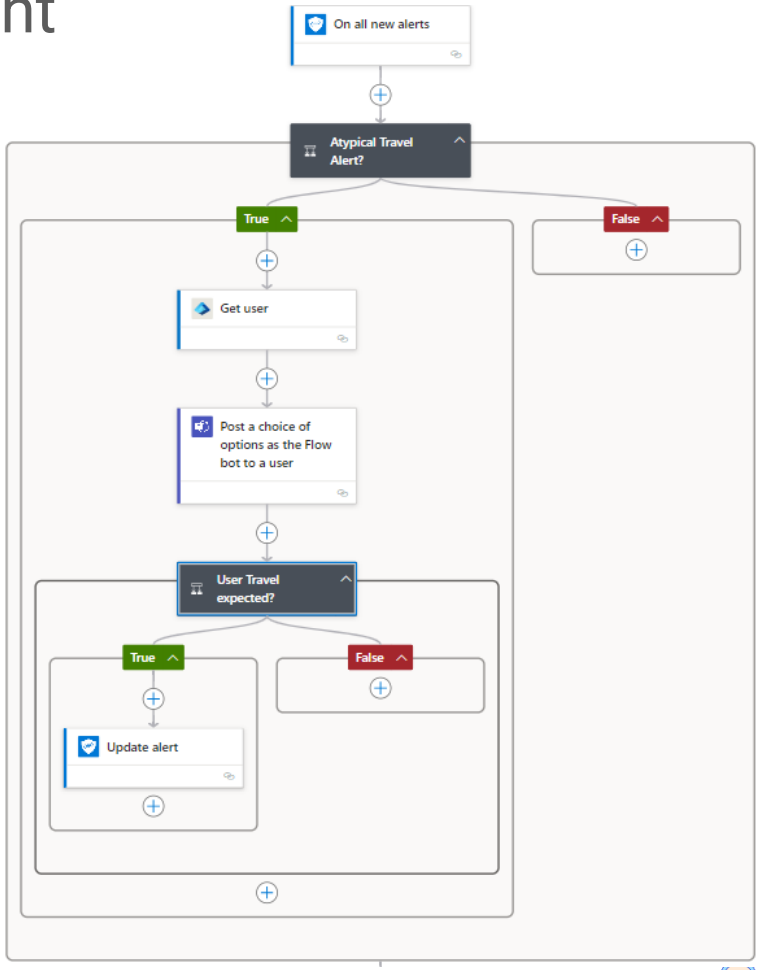
Auto Close für Informational Messages

- Trigger: neuer Alert
- Bedingung: Alert von Severity “Informational”
- Aktion: Alert schließen



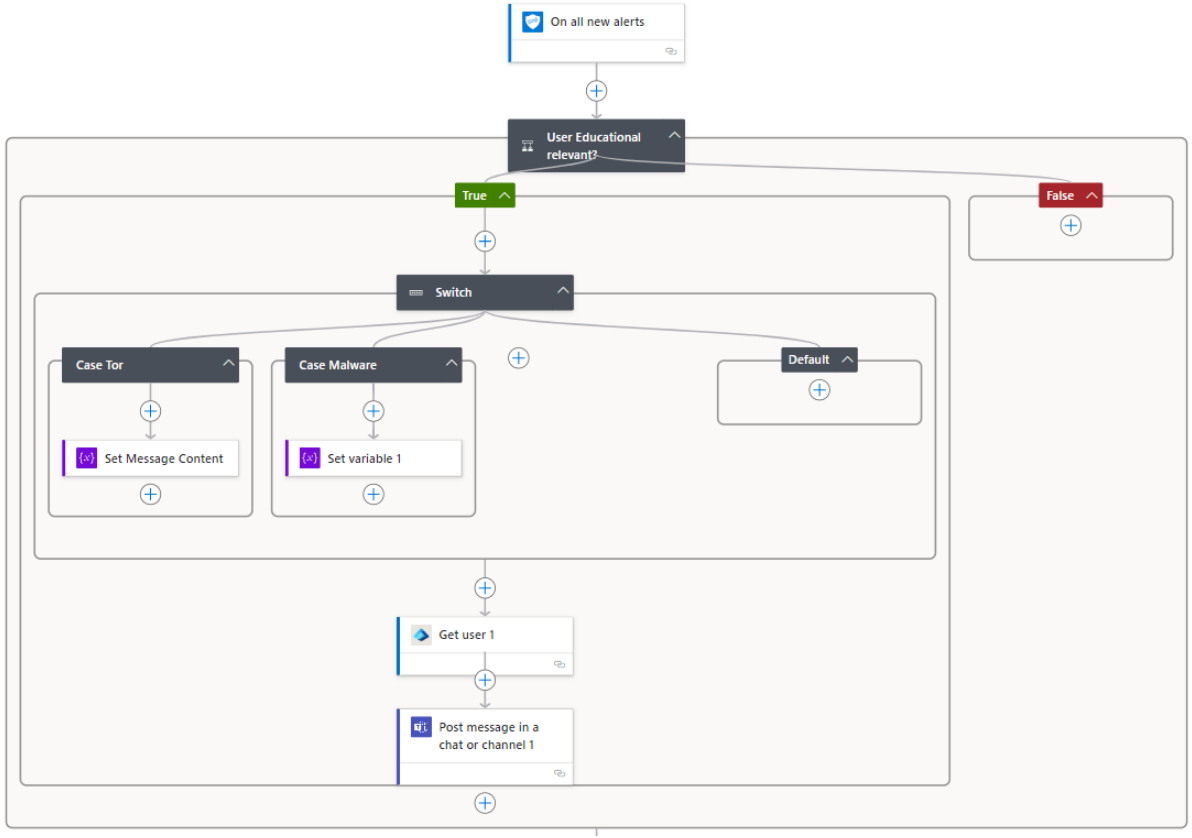
Atypical Travel – Teams-Nachricht an Manager

- Trigger: neuer Alert
- Bedingung: Alert vom Typ atypical Travel
- Aktionen:
  - Nutzer aus Entra ID abrufen
  - Manager fragen, ob Nutzer wirklich im Land
  - Alert ggf. schließen



Phishing / Tor-Nutzung / Unwanted Software: Info an User

- Trigger: neuer Alert
- Bedingung: diverse Alert-Typen
- Aktion: Nutzer per Teams über Erkennung informieren und bitten, Aktion zukünftig zu unterlassen



Vielen Dank für eurer Interesse! Fragen?

Gerne stehe ich bei Fragen, Ideen und zur Diskussion zur Verfügung

Austria – Wien
Germany – NRW

+49 151 116 18 108

tk@cloudguard.net

azuregeek.io