glueck kanja

HSD

Praxis & Zusammenarbeit

Zusammenarbeit im Managed SOC mit Einblicken in Setup, Monitoring & Incident Response

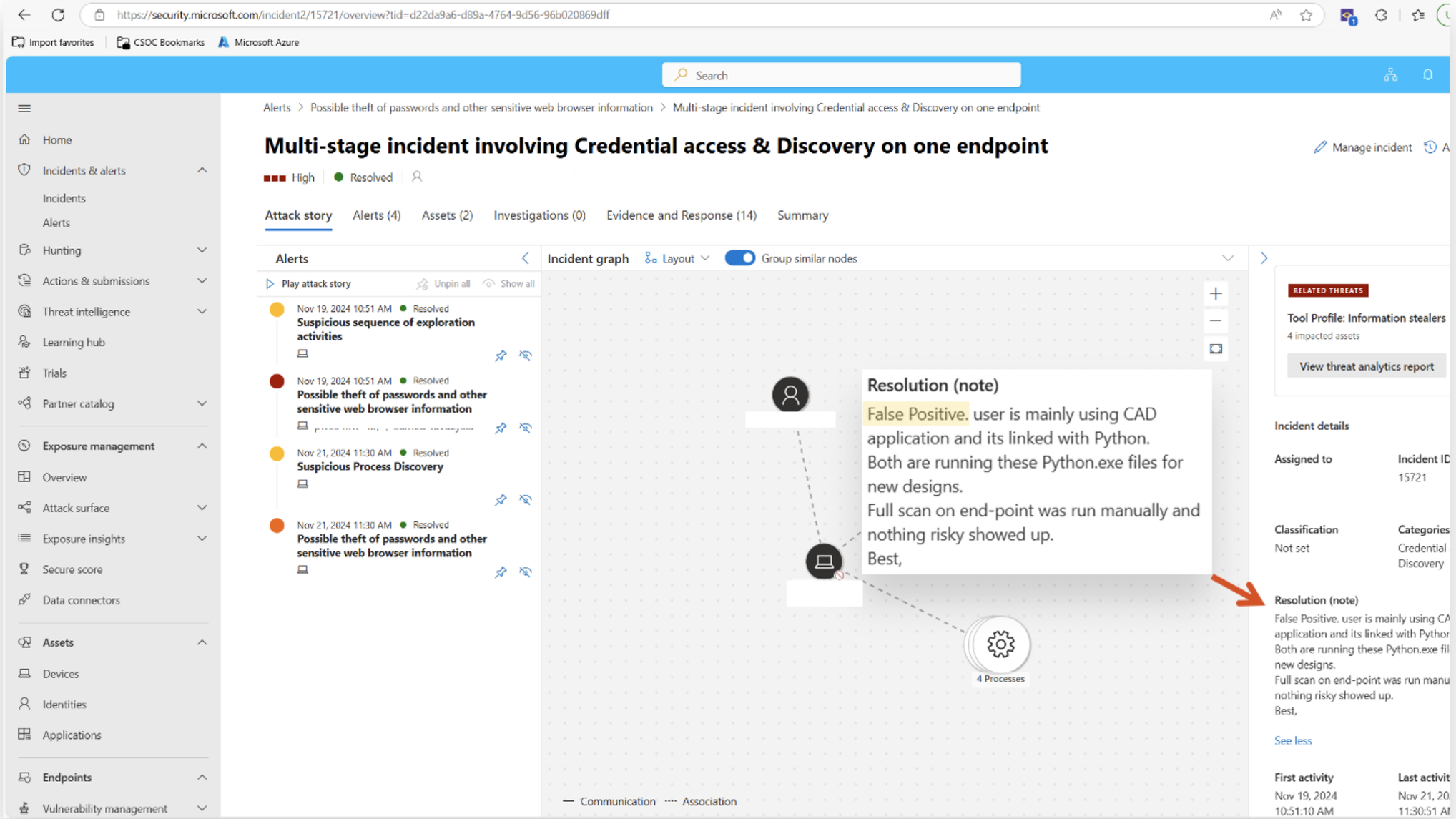
We see your trouble coming.

“Multiple EDR Tools will protect me better than just one.”

Huy @DebugPrivilege · 4h

I've been on multiple IR cases so far and it always shows me. People and process above security products. Organization has 2 EDR installed on their machines, but still breached. Why? No one is responding to these Christmas three alerts 😉 - Hire people, not products.

8 25 95


https://security.microsoft.com/incident2/15721/overview?tid=d22da9a6-d89a-4764-9d56-96b020869dff
Import favorites
CSOC Bookmarks
Microsoft Azure
Search
Alerts > Possible theft of passwords and other sensitive web browser information > Multi-stage incident involving Credential access & Discovery on one endpoint
Multi-stage incident involving Credential access & Discovery on one endpoint
Manage incident
High
Resolved
Attack story
Alerts (4)
Assets (2)
Investigations (0)
Evidence and Response (14)
Summary
Home
Incidents & alerts
Incidents
Alerts
Hunting
Actions & submissions
Threat intelligence
Learning hub
Trials
Partner catalog
Exposure management
Overview
Attack surface
Exposure insights
Secure score
Data connectors
Assets
Devices
Identities
Applications
Endpoints
Vulnerability management
Alerts
Play attack story
Unpin all
Show all
Nov 19, 2024 10:51 AM Resolved
Suspicious sequence of exploration activities
Nov 19, 2024 10:51 AM Resolved
Possible theft of passwords and other sensitive web browser information
Nov 21, 2024 11:30 AM Resolved
Suspicious Process Discovery
Nov 21, 2024 11:30 AM Resolved
Possible theft of passwords and other sensitive web browser information
Incident graph
Layout
Group similar nodes
Resolution (note)
False Positive. user is mainly using CAD application and its linked with Python.
Both are running these Python.exe files for new designs.
Full scan on end-point was run manually and nothing risky showed up.
Best,
4 Processes
Communication
Association
RELATED THREATS
Tool Profile: Information stealers
4 impacted assets
View threat analytics report
Incident details
Assigned to
Incident ID
15721
Classification
Not set
Categories
Credential Discovery
Resolution (note)
False Positive. user is mainly using CA
application and its linked with Pythor
Both are running these Python.exe fil
new designs.
Full scan on end-point was run manu
nothing risky showed up.
Best,
See less
First activity
Nov 19, 2024 10:51:10 AM
Last activit
Nov 21, 20 11:30:51 A

“Never change a running system.”

“I have all those certifications.
We are in a great position!”


WHAT IF I TOLD YOU
THAT HACKERS GIVE A F##K ABOUT
YOUR ISO 27001 CERTIFICATION
imgflip.com

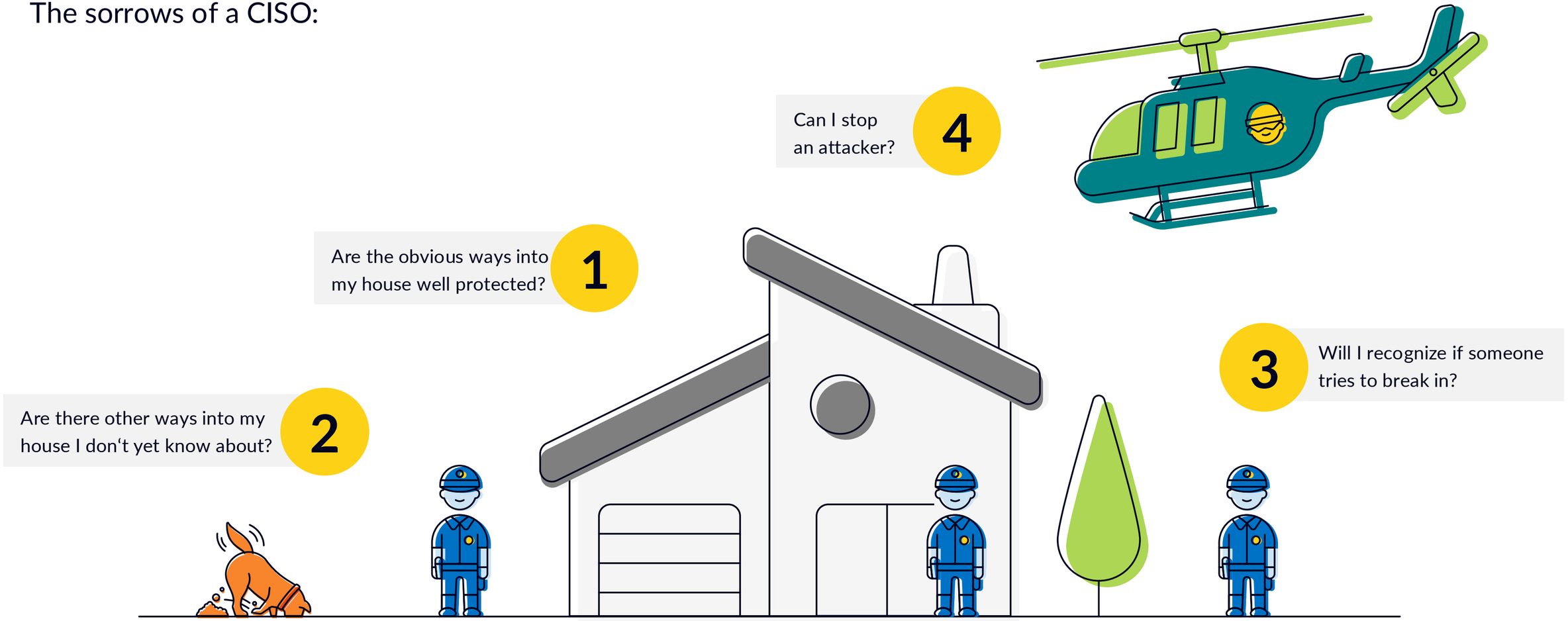
Was hilft?

glueck kanja

HSD

Are we safe enough?

The sorrows of a CISO:



glueck kanja

HSD

Customer Maturity – Are you safe?

1	2	3	4
Are the obvious ways into my house well protected?	Are there other ways into my house I don‘t yet know about?	Will I recognize if someone tries to break in?	Can I stop an attacker?
Security Posture	**Vulnerability Posture**	**Attack Monitoring Capability**	**Incident Response Capability**
Infrastructure Architecture	Vulnerability Monitoring	XDR Monitoring	24/7 IR Resources
As-Is Configuration Quality	External Attack Surface Monitoring	Sentinel Monitoring	Preparation of Emergency Incident
Best Practices Feature Comparison	Pen Testing / Red Teaming	Maintained Detection Repository	Processes

Enterprise Security Status OKR

Are you safe?

Security Posture

Infrastructure Architecture

As-Is Configuration Quality

Best Practices Feature Comparison

Objective	Key Result
Make sure, you know your environment(s). Before you can measure, you need to know what to measure.	Have a detailed overview of your environments and know what to meassure / monitor.
Regular Infrastructure & Configuration Assessments by Experts	Assess infrastructure & configuration: e.g. assess local AD with PingCastle, take results and create roadmap for mitigations. Measure progress. If done make new assessment.
MITRE Defend Alignment https://d3fend.mitre.org, CIS Alignment	Create scoped roadmap to fulfill MITRE Defend Hardening & Isolation Recommendations. Set Goals, measure it.
Vendor Recommendations Alignment	e.g. Microsoft Security Score. Create scoped roadmap and measure progress, SAP Security Best Practices.

glueck kanja

HSD

Enterprise Security Status OKR

Are you safe?

Vulnerability Posture

- Vulnerability Monitoring
- External Attack Surface Monitoring
- Pen Testing / Red Teaming

Objective	Key Result
Monitor Software Vulnerabilities	Measure Vulnerability Monitoring Results e.g., in Dashboards
Monitor External Attack Surface	Measure Vulnerability Monitoring Results e.g., in Dashboards
Do regular Pen Test and Red Teaming Events	List findings and create mitigation plans
Make sure to patch vulnerabilities in time	Meassure MTTP for critical vulnerabilities

glueck kanja

HSD

Enterprise Security Status OKR

Are you safe?

Attack Monitoring Capability	Objective	Key Result
XDR & Sentinel Monitoring	**(Detection Depths)** Measure Detections against MITRE Attack coverage https://attack.mitre.org	Create scoped roadmap for MITRE Attack coverage and measure the implemenation e.g., with a MITRE coverage Heatmap
	(Detection Breadth) Cover entire infrastructure by detections	Inventory your environments. Measure coverage of your detections in these environments e.g., in Dashboards
Holistic Detection Repository (Maintained)	**(Detection Depths)** Do regular Pen Test and Red Teaming Events	List findings and create plans for new or improved detections

glueck kanja

HSD

Enterprise Security Status OKR

Are you safe?

Incident Response Capability

- 24/7 IR Resources
- Preparation of Emergency Incident
- Processes

Objective	Key Result
Make sure all involved parties are available in case of an incident and defined response actions can take place	Evaluate involved parties based on the RACI matrix of the Incident Response process and check their 24/7 availability. Report on the results.
Prepare major environments for an emergency incident	Regularly verify process and report on the results.
Make sure all incident response workflow processes work as expected.	Regularly assess incident workflow (e.g. review Tickets / Incident History) and report on results. Report on Service Delivery (Time to respond & Time to resolution).
Make sure to respond to incidents in time	Meassure MTTR

glueck kanja

Security Services

Preventive Services

Preperation for the worst case in combination with gap analysis

- Active Directory
- Entra ID
- Azure Infrastructure

AzERE

Your Life Net for the worst case: Secure Environment for AD Backup and Recovery

Managed Red Tenant

Managed privileged administration environment

Security Consulting

Deeply skilled experts that help you implement cutting edge security technology

APT Response

Incident Response in case of an Emergency

CSOC

24/7 Managed SOC, based on Microsoft Security Technology

Data Security Services

Prevent sensitive data from traveling into the unknown. Your Purview managed service

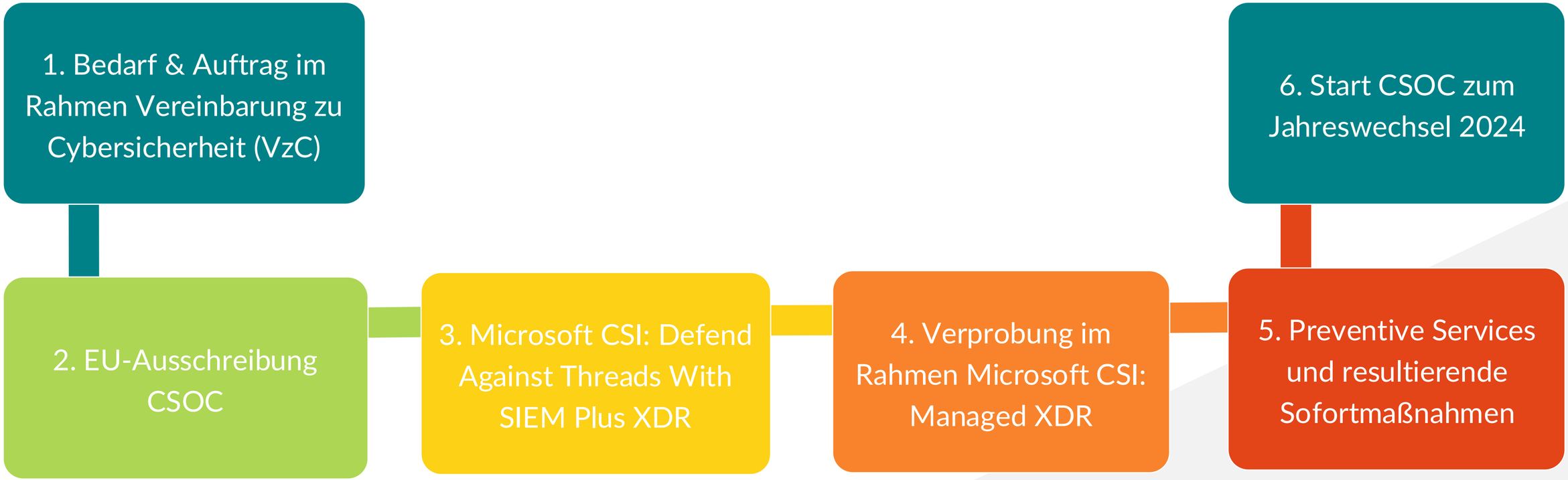
glueck kanja

HSD

Wie haben wir **gemeinsam mit der HSD** auf diese Problematik reagiert?

Kurz: wir haben unseren Managed Service CSOC etabliert

Microsoft Programme & Weg zum Onboarding @HSD



glueck kanja

Our Approach to Modern Security

Implementation

Managed CSOC

CSOC Wide
Microsoft XDR

- Defender for **Endpoint**
- Defender for **Identity**
- Entra ID **Identity Protection**
- Defender for **Office 365**
- Defender for **Cloud Apps**

Defender XDR Custom Detections + Entra ID Sentinel Basic Detections (GK Detection Engineering)

CSOC Deep
Microsoft Sentinel

- **Network Log Interaction** (e.g. Firewalls, Proxy, VPN, OT)
- **Windows Event Logs, Linux, Syslogs**
- **Defender for Cloud**
- **Entra ID Sentinel Advanced Directions**
- **Business Apps** (e.g. Power Platform, Dynamics, SAP)
- **Defender for IoT**
- **Office Activity, Cloud Platform** (Azure, AWS, GCP)**, Cloud Workload**
- **3rd Party Log Interaction** (e.g. Okta, Auth0, Qualys)
- **Self-Managed Threat Intelligence**

GK Detection Engineering

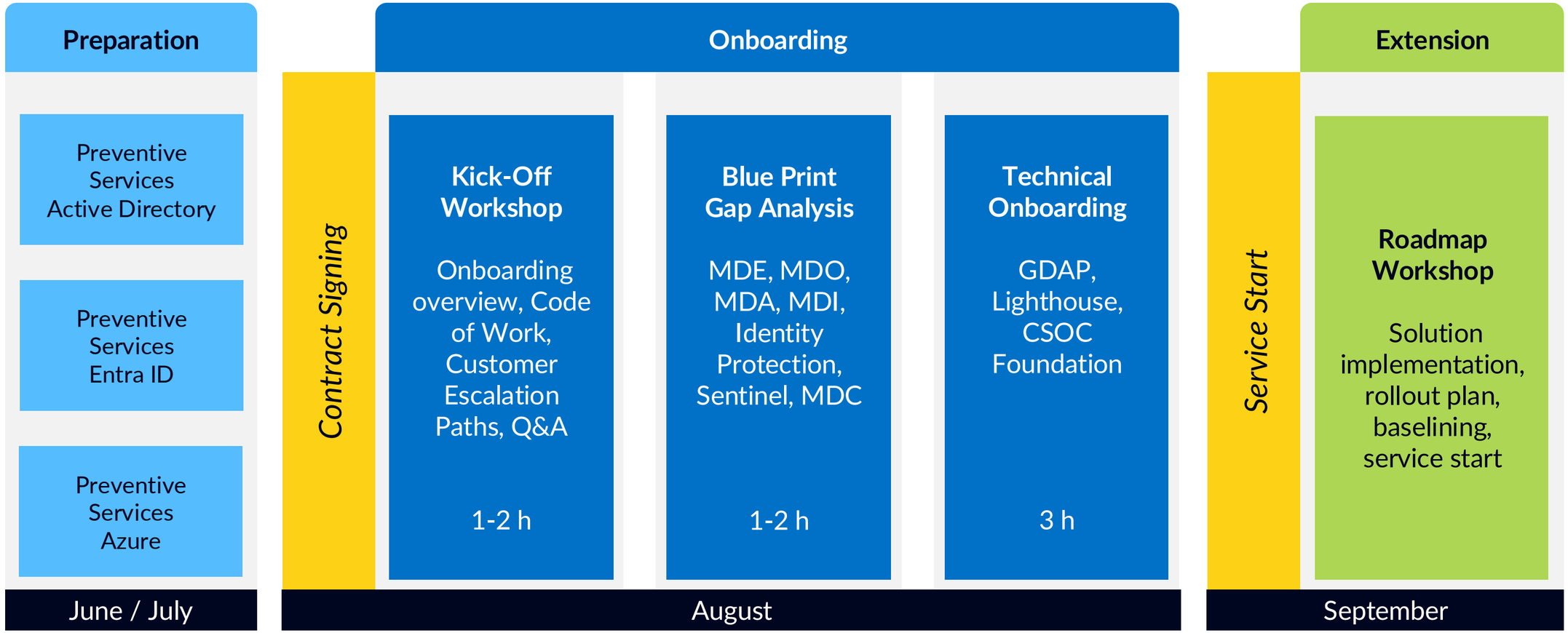
CSOC Foundation
GK Automation

- **CI / CD Deployment**
- **Playbook Manager**
- **Customer Enrichment**

glueck kanja

CSOC Example Roadmap

Get connected quickly and easily



Microsoft Entra ID Assessment

Interview

- Vorbereitetes Interview zu konzeptionellen und prozessualen Themen
- Themen und Fragen in dieser Präsentation

+

Review

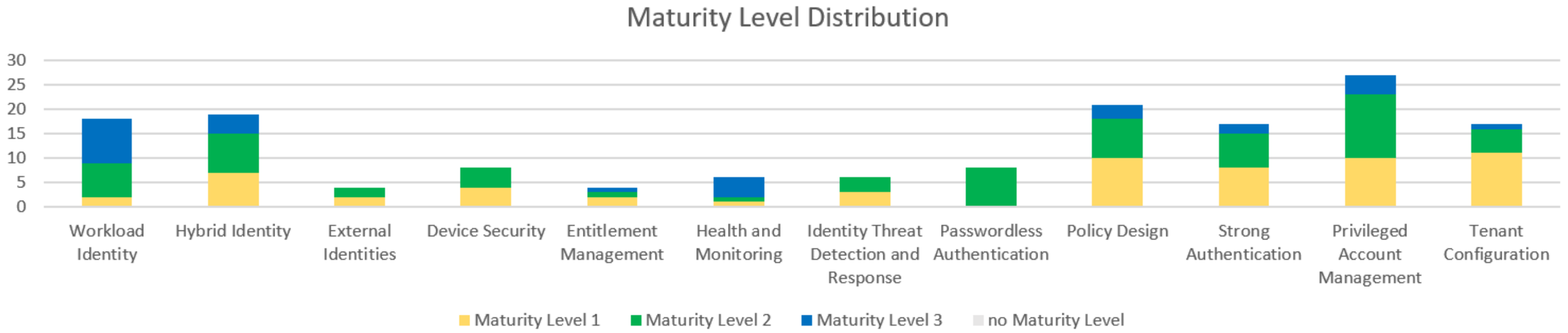
- Detailliertes Review der Cloud Umgebung
- Config Export des Microsoft Entra Connect

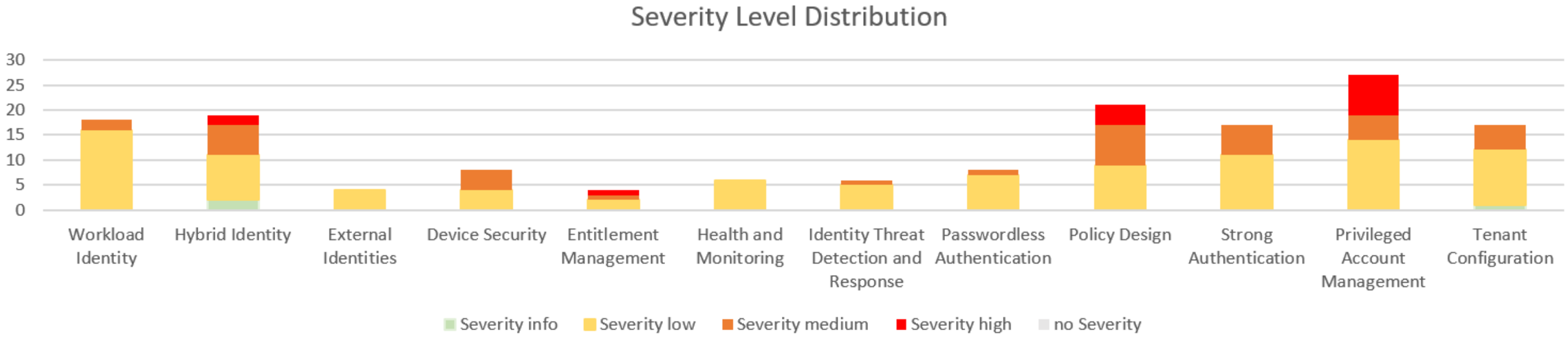
=

Report

- Erstellung von Dokument und Präsentation
- Erläuterung und Diskussion der Ergebnisse und Handlungs-empfehlungen

Assessment Findings Summary





glueck kanja

HSD

Two pillars to protect our customers

Lightning-fast responses to your alerts

Simple and ‘to-the-point’ reports – explained in **monthly** Teams meetings

On-Demand Preventive Services Workshops to improve your security posture

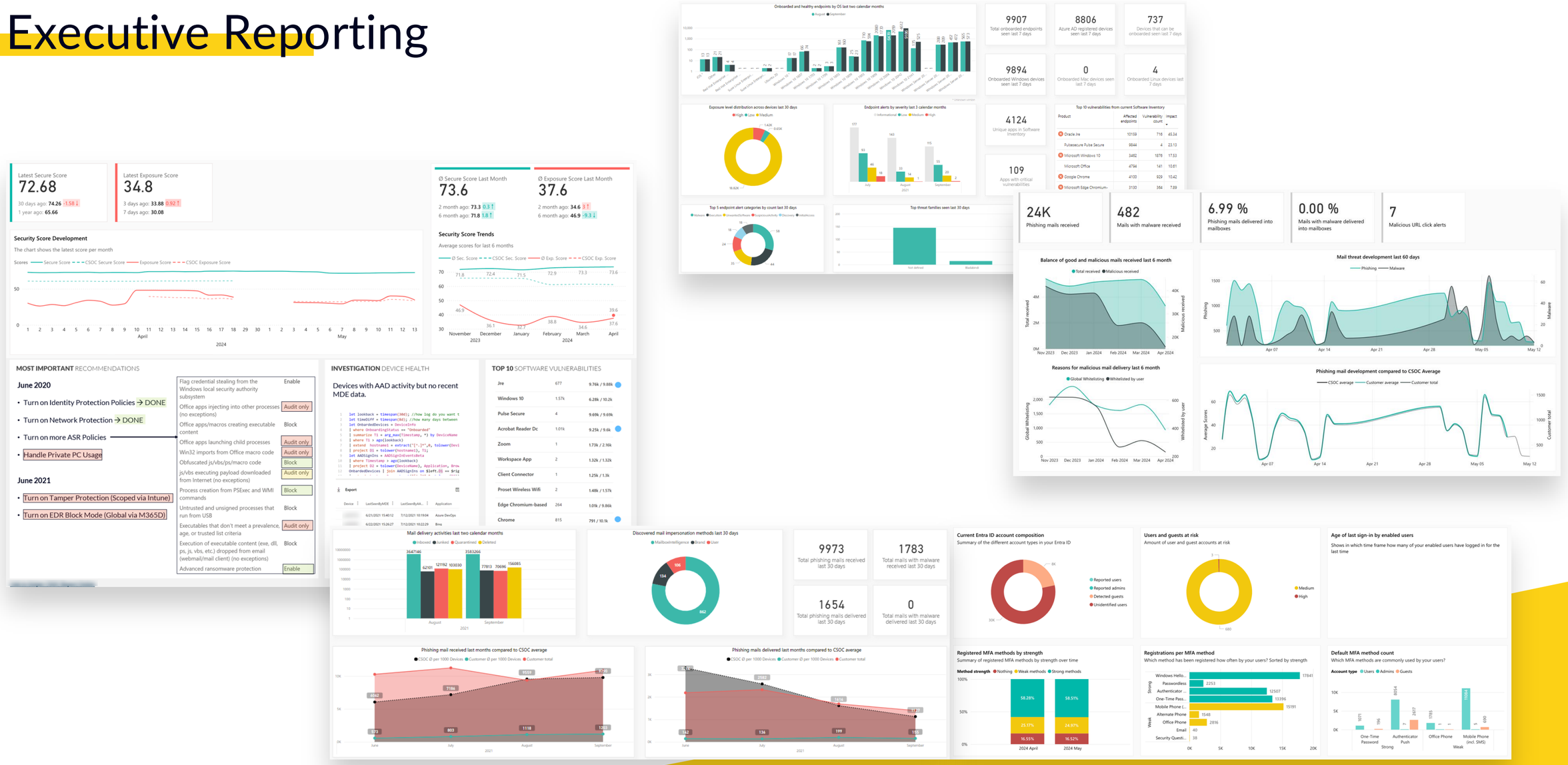
Incident Response

Continuous Improvement

glueck kanja

HSD

Executive Reporting



glueckkanja

HSD

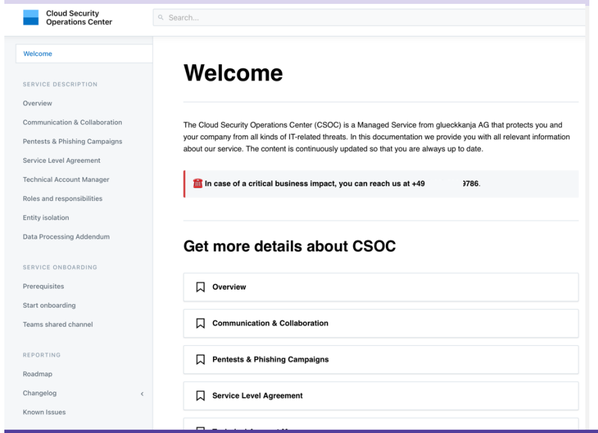
Partnership

Fostering long-term partnerships through exceptional service quality.

Technical Account Manager

Primary Security Analyst

CSOC Customer Docs



Microsoft Teams Shared Channel

Incident Management in Sentinel

- Azure Lighthouse
- GDAP or B2B Permissions
- Security Administrator or Security Operator

CSOC Foundation

No clinging to intellectual property

glueck kanja

HSD

Chronologie des SharePoint-Vorfalls @HSD: Angriff, Reaktion & Maßnahmen

17.07.2025, 09:15 Uhr CEST: ?

Beginn erste Angriffsversuche

17.07.2025, 11:34 Uhr CEST: CSOC

Erste Detektion und Vereitelung durch MDE (Verhaltenserkennung; wurde zunächst CVE-2025-49704 zugeordnet)

17.07.2025, 14:07 Uhr CEST: CSOC

CSOC informiert HSD über Detektion & erfolgreiche Vereitelung > kein direkter Handlungsbedarf, da automatisch mitigiert, noch kein CVE bekannt

19.07.2025: Microsoft

Microsoft veröffentlicht CVE-2025-53770

20.07.2025: Microsoft

Microsoft veröffentlicht CVE-2025-53771

Microsoft veröffentlicht Patch für SP19

20.07.2025, ~ 20:00 Uhr CEST: HSD

Prüfung der Systeme, Abwägung der Kritikalität der Sicherheitslücke und dem möglichen Imageschaden der Organisation durch Kompromittierung oder Abschaltung

glueck kanja

HSD

Chronologie des SharePoint-Vorfalls @HSD: Angriff, Reaktion & Maßnahmen

21.07.2025: HSD & CSOC

Umfangreiche Analyse der Umgebungen > Anzeichen für Kompromittierung

Auslösung APT Response > CSOC

Gemeinsame Abwägung und Rückstufung der Kritikalität von APT Response auf Security Consulting

Erstellung eines gemeinsamen Action Plan mit CSOC

Sicherung & teilweise Isolation der SP-Farmen

Umsetzung der Hersteller Guidance bei SP19 Farm

Eigene Maßnahmen zum Schutz der SP16 Farm implementiert

22.07.2025: HSD

Umsetzung der Hersteller Guidance bei SP16 Farm

Microsoft veröffentlicht Patch für SP16

21.07.2025: Microsoft

Kontinuierliche Überwachung der Umgebung durch CSOC

Wiederherstellung & Prävention nach dem SharePoint-Vorfall @HSD

- Zur vollständigen Wiederherstellung der Systeme wurde die Hersteller Guidance auf beiden SharePoint-Farmen vollständig umgesetzt
- Forensische Arbeiten, weitere Sicherheitsmaßnahmen, u.a. Wechsel sämtlicher in Anwendungsbeziehung genutzter Pass- und Codewörter der SharePoint-Farmen (Service-Accounts, etc.) folgten in den darauffolgenden Tagen
- Erneuerung SP16 Farm auf SPSE geplant
- Abschließende Erkenntnis
  - **keine** Anzeichen auf Abfluss sensibler Daten
  - **keine** Anzeichen auf Ausbreitung des Angriffs auf andere Systeme

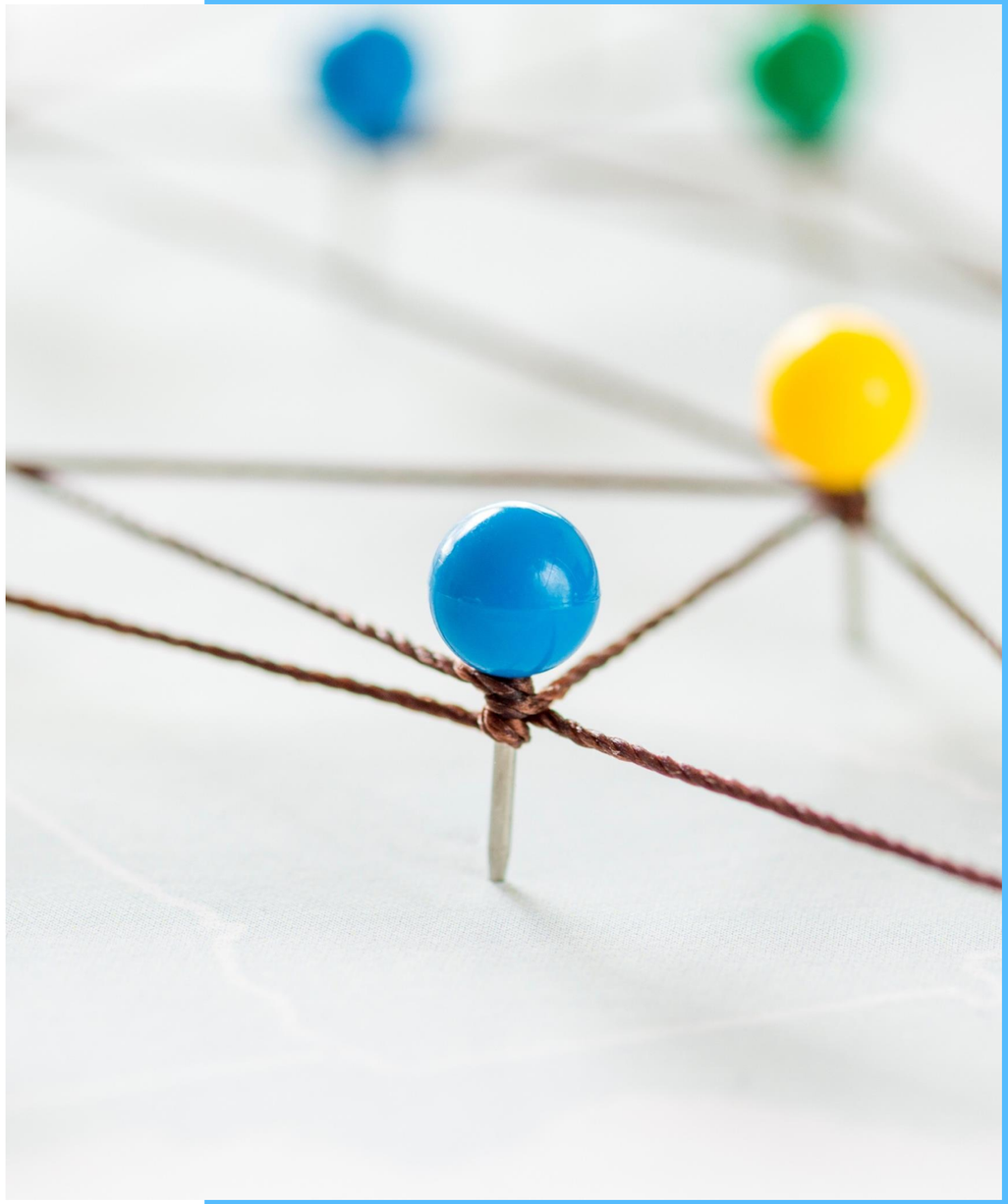
glueck kanja

HSD

Learnings von anderen Hochschulen in NRW

- Der Angriff war ein sogenannter „Spray and Pray“-Angriff, d. h. die HSD war nicht gezielt betroffen; Vielmehr waren alle Hochschulen (und Organisationen) betroffen, die SharePoint ins Internet publishen
- Sämtliche Hochschulen in NRW sind durch Security Operations Center (SOC) abgesichert
  - Das CSOC der HSD hat schnell reagiert und bei der Mitigation umfangreich unterstützt
  - Die SOCs der Hochschulen, welche ein Eigenes betreiben, reagierten verzögert, teilweise war eine Kompromittierung bereits erfolgt *
  - Das Landes-SOC für Hochschulen in NRW hatte bis 23.07.2025 gar nicht auf den Incident reagiert *

*Erkenntnisse aus anderen Hochschulen resultieren aus bilateralen Gesprächen sowie einer durch Netzwerk Informationssicherheit der Hochschulen in NRW (NISHS.NRW) initiierten Austauschrunde zum Exploit am 23.07.2025



glueckkanja

HSD

What didn't work @HSD

- Nicht alle kritischen Systeme waren mit MDE abgesichert
- Nach der Detektion des Angriffs durch das CSOC am 17.07. erfolgte bis zum 20.07. keine HSD-seitige Reaktion; dies Aufgrund einer hohen Abwesenheitsquote in Kombination mit der Unklarheit über die Bedrohungslage auf Seiten der HSD
- Die Ressourcensituation der HSD Campus IT ist nach wie vor angespannt
- Die Geschwindigkeit und Art der Reaktion ist durch die intrinsische Motivation der Beschäftigten geprägt - das ist ein Risiko für die HSD in Kombination mit einer billigenden Inkaufnahme durch die HSD
- Der Incident-Prozess an der HSD muss im Sinne eines QVP einer kontinuierlichen Optimierung unterzogen werden

glueck kanja

HSD

What worked @HSD

- Unser CSOC hat gut funktioniert: Der Angriff wurde schnell detektiert, die Meldewege haben auf Seiten des CSOC funktioniert
- Trotz hoher Abwesenheitsquote (VO, CISO, CISO-Vertretung, Fachadministration) konnte schnell Kontrolle über die Situation gewonnen werden
- Eine längerfristige Downtime, abseits der Wartung aufgr. der Patcheinspielung, konnte verhindert werden
- Die Kommunikation & das Krisenmanagement @HSD hat gut funktioniert
- Die IKM Strategie der HSD ist aufgegangen: Durch die hohe Standardisierung konnten Ausfälle kurzfristig kompensiert werden, da Zugriff auf Vertretungen mit ähnlichen Fähigkeitsprofilen möglich waren

glueck kanja

HSD

Behind the Scenes

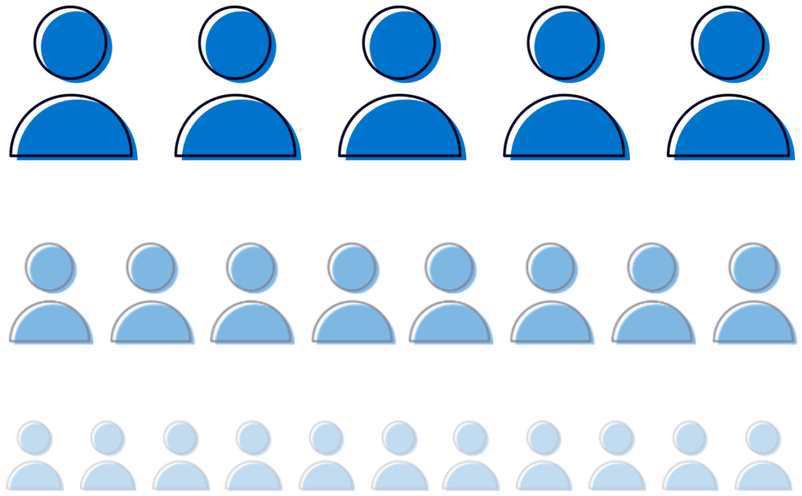
Wie das CSOC arbeitet

glueck kanja

HSD

Deeply Skilled Experts

Other Security Providers Approach



Incident

Customer A

Incident

Customer B

Incident

Customer C

Our Approach

Primary Analyst
Best SMEs on the Market

Incident

Customer A

Primary Analyst
Best SMEs on the Market

Incident

Customer B

Primary Analyst
Best SMEs on the Market

Incident

Customer C

- Long-term, personal relationship
- Knowledge of customer specifics
- One face to the customer throughout the whole incident handling process

- Deep knowledge and experience at the front
- Continuous improvement of automation processes & use cases
- Well-rehearsed team

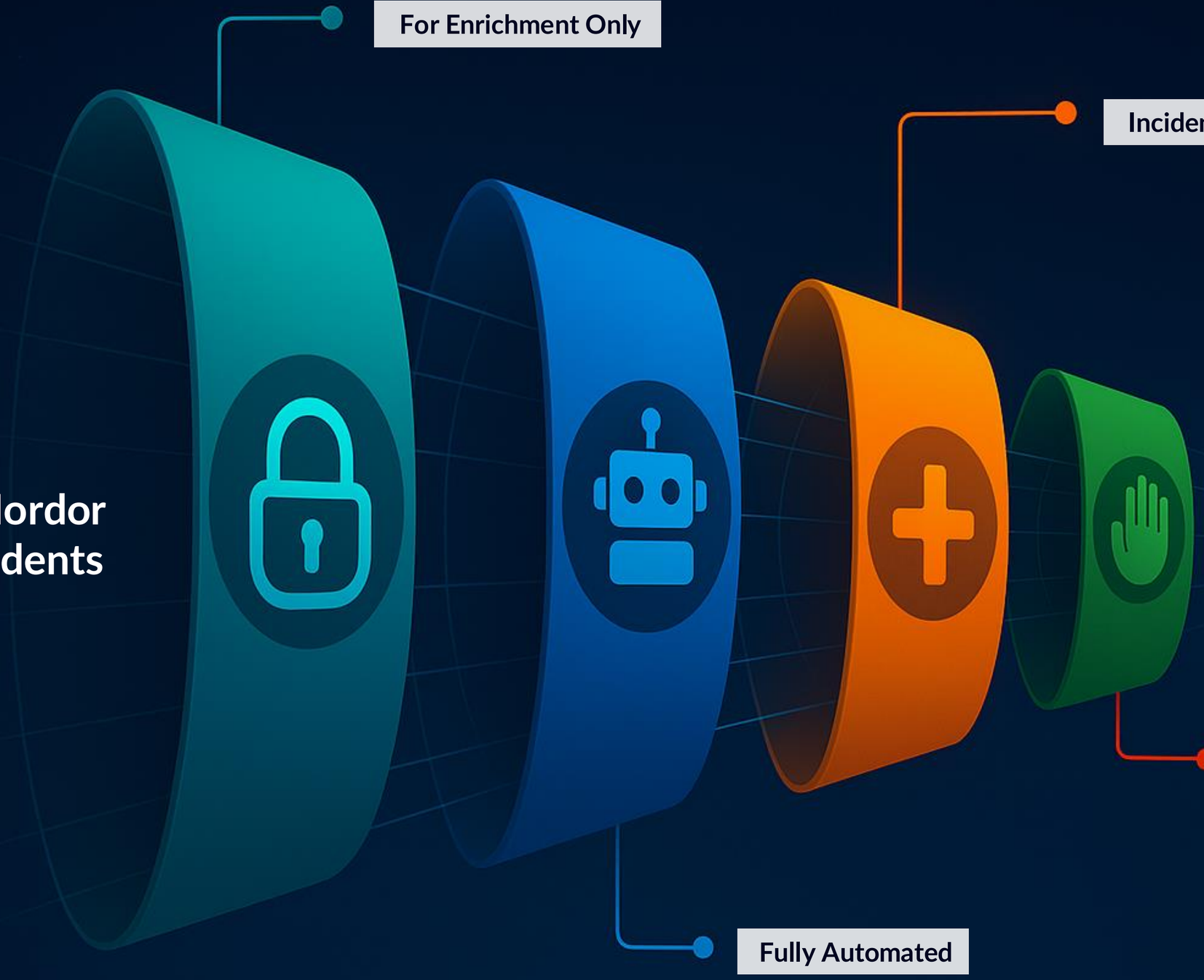
glueck kanja

CSOC

HSD

120K Incidents / Month

The Mordor of Incidents



Our Principles

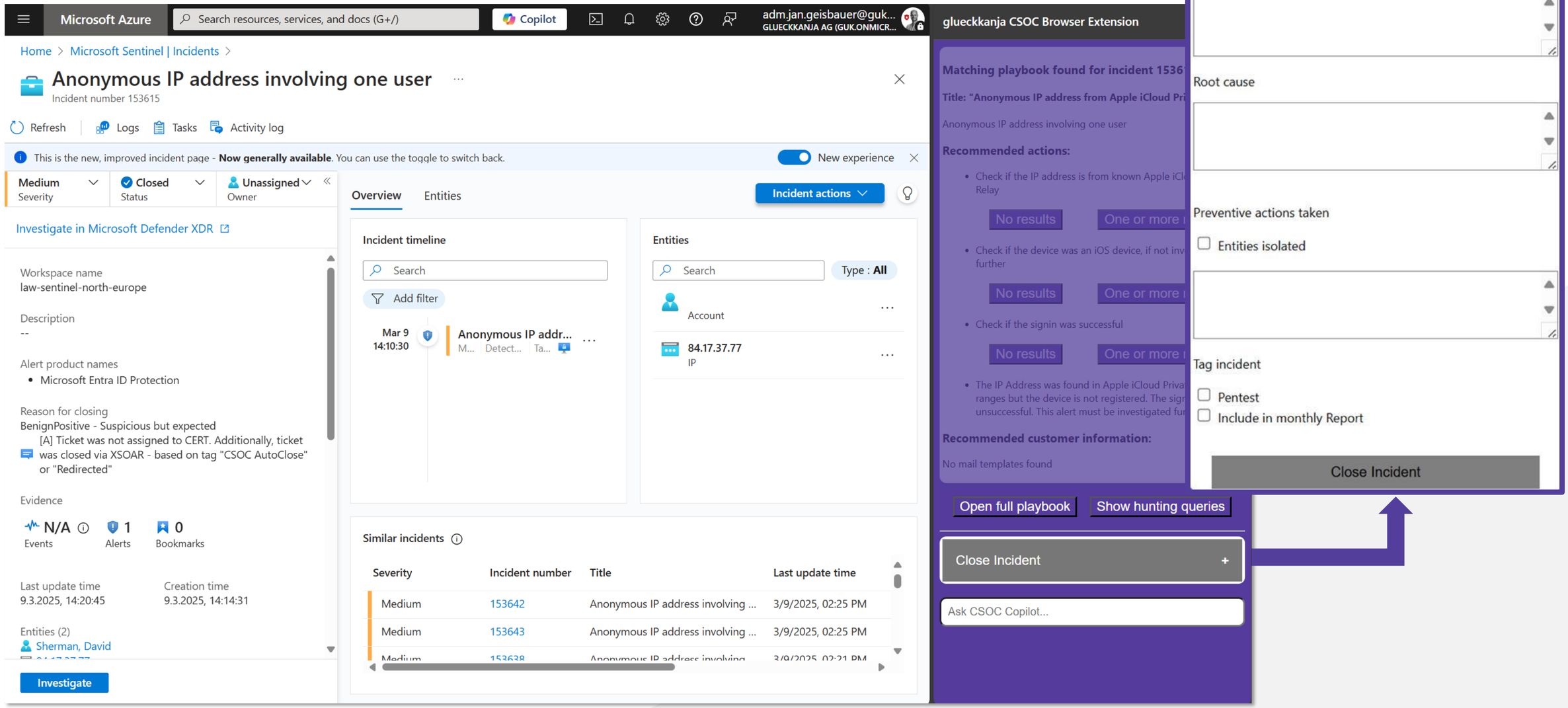
We only want to handle incidents manually that cannot yet be handled automatically.

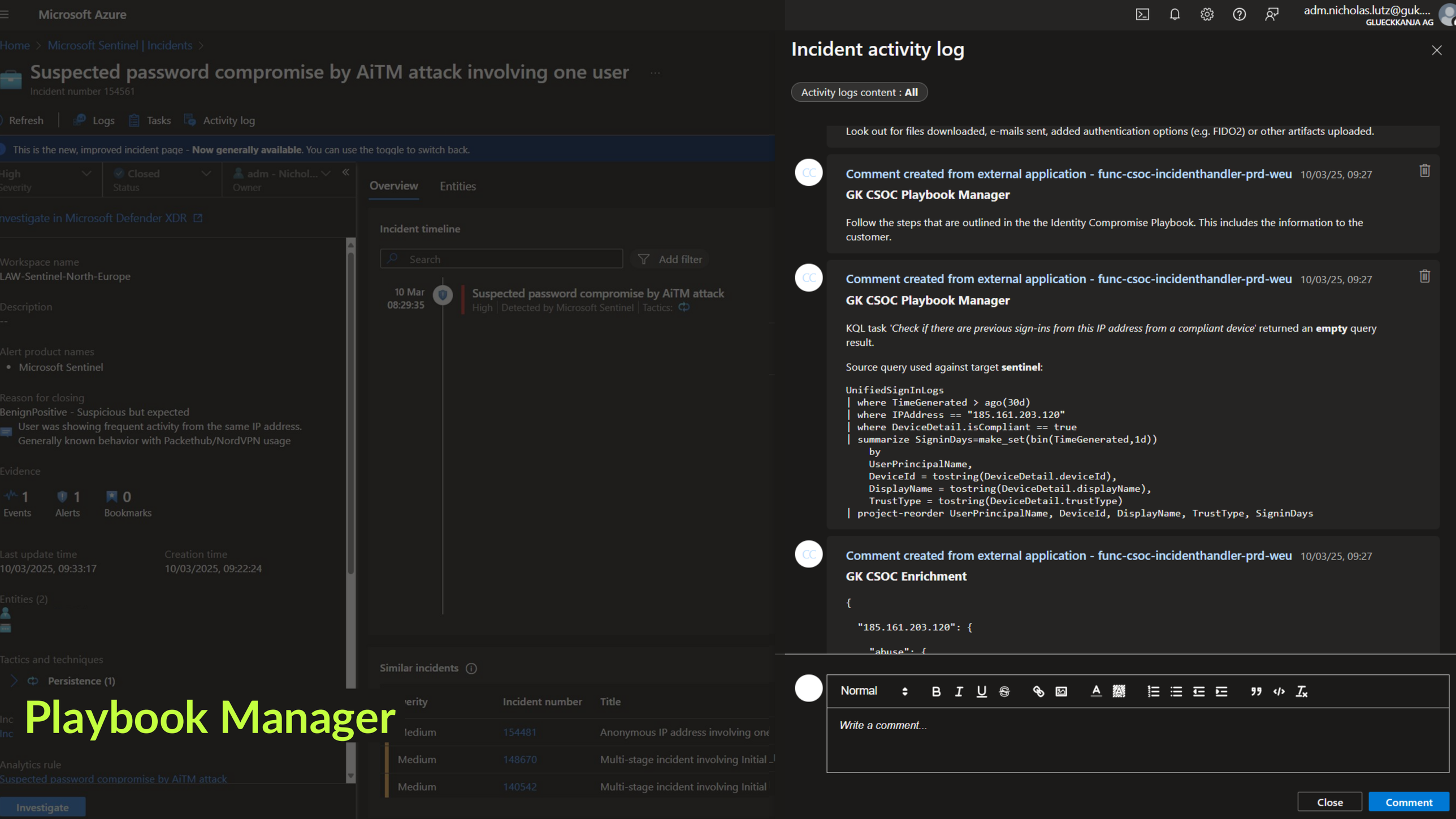
With each incident we either handle manually or automatically, we want to add value to the process.

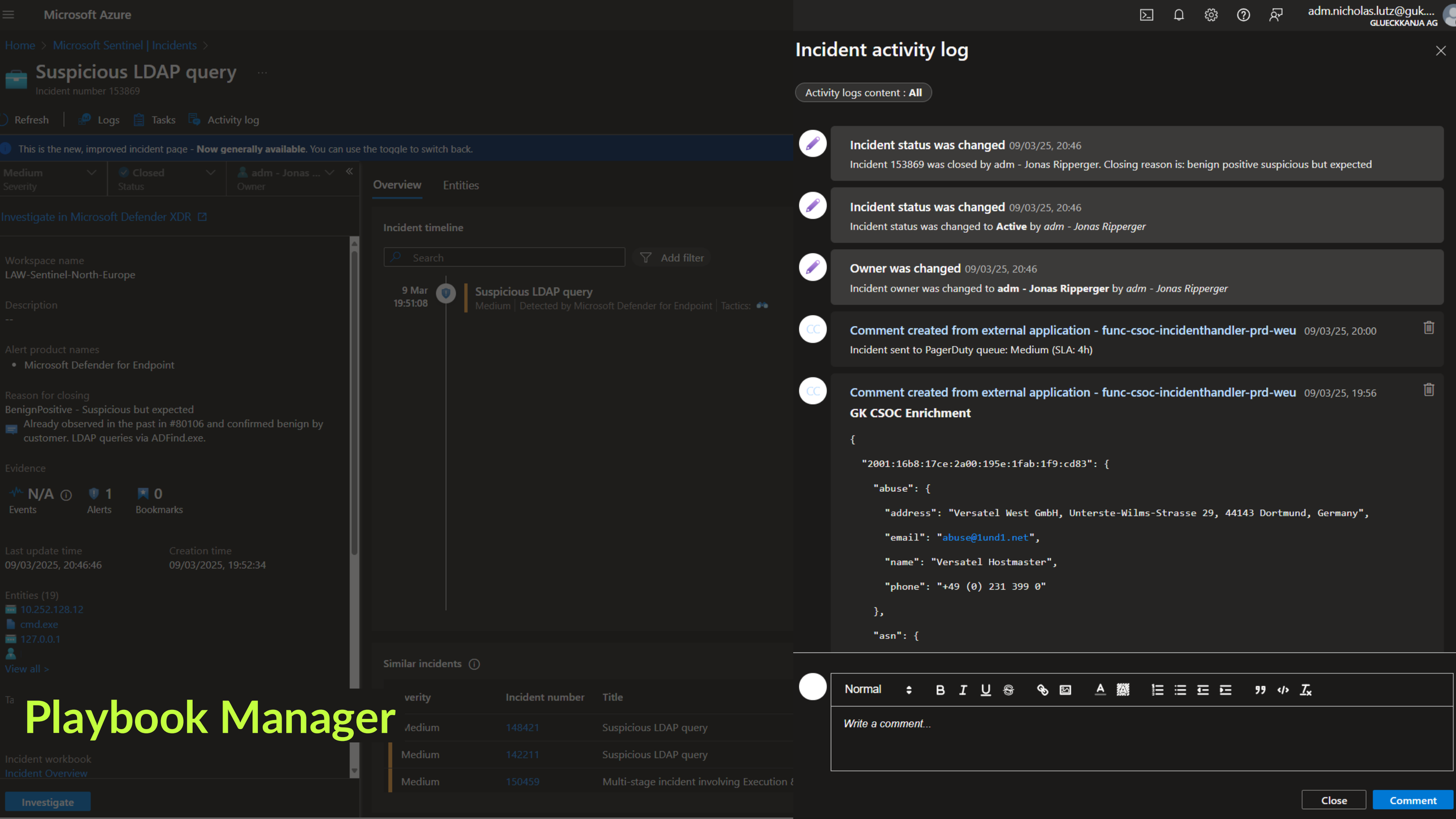
glueck kanja

glueckkanja

CSOC Browser Extension



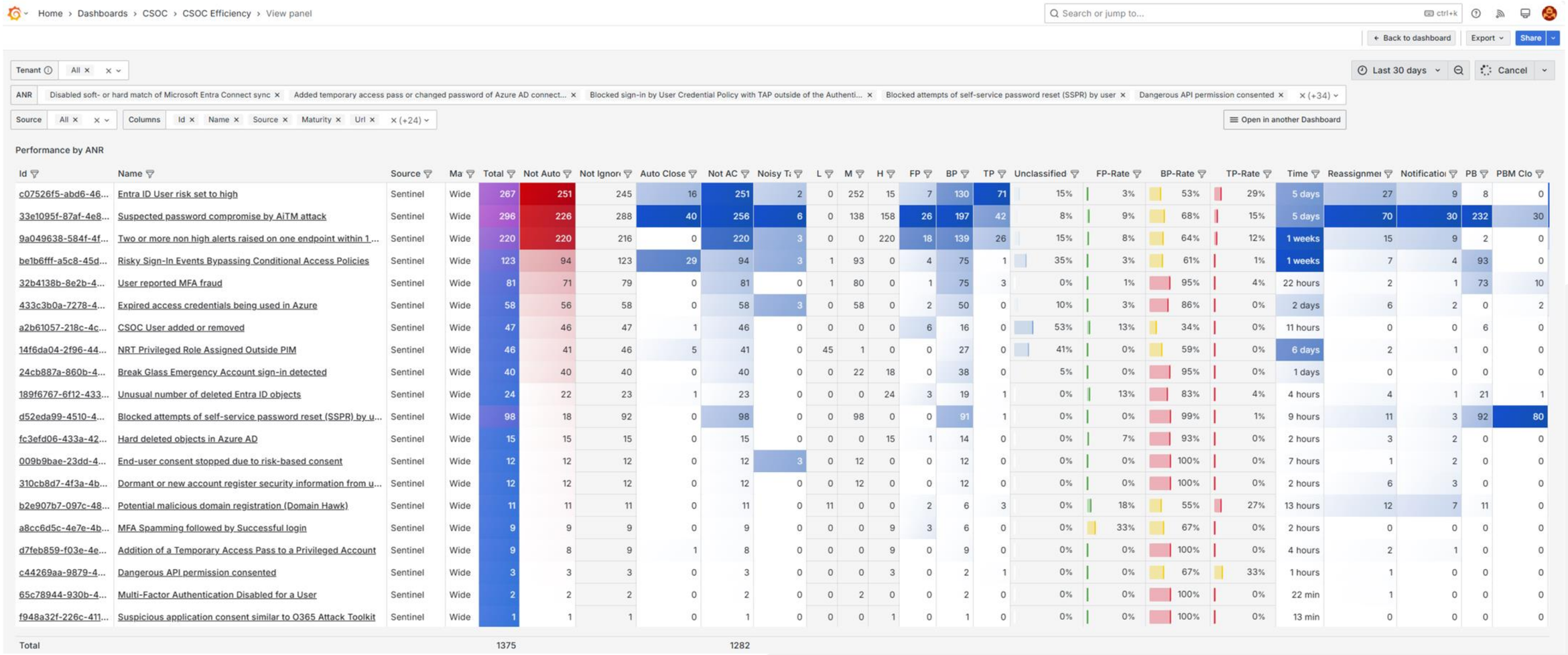

Microsoft Azure
adm.nicholas.lutz@guk....
GLUECKKANJA AG
Home > Microsoft Sentinel | Incidents >
Suspected password compromise by AiTM attack involving one user
Incident number 154561
Refresh
Logs
Tasks
Activity log
This is the new, improved incident page - Now generally available. You can use the toggle to switch back.
High
Severity
Closed
Status
adm - Nichol...
Owner
Investigate in Microsoft Defender XDR
Workspace name
LAW-Sentinel-North-Europe
Description
--
Alert product names
Microsoft Sentinel
Reason for closing
BenignPositive - Suspicious but expected
User was showing frequent activity from the same IP address.
Generally known behavior with Packethub/NordVPN usage
Evidence
1
Events
1
Alerts
0
Bookmarks
Last update time
10/03/2025, 09:33:17
Creation time
10/03/2025, 09:22:24
Entities (2)
Tactics and techniques
Persistence (1)
Analytics rule
Suspected password compromise by AiTM attack
Investigate
Overview
Entities
Incident timeline
Search
Add filter
10 Mar
08:29:35
Suspected password compromise by AiTM attack
High | Detected by Microsoft Sentinel | Tactics:
Similar incidents
Incident number
Title
Medium
154481
Anonymous IP address involving one
Medium
148670
Multi-stage incident involving Initial
Medium
140542
Multi-stage incident involving Initial
Incident activity log
Activity logs content : All
Look out for files downloaded, e-mails sent, added authentication options (e.g. FIDO2) or other artifacts uploaded.
Comment created from external application - func-csoc-incidenthandler-prd-weu 10/03/25, 09:27
GK CSOC Playbook Manager
Follow the steps that are outlined in the the Identity Compromise Playbook. This includes the information to the customer.
Comment created from external application - func-csoc-incidenthandler-prd-weu 10/03/25, 09:27
GK CSOC Playbook Manager
KQL task 'Check if there are previous sign-ins from this IP address from a compliant device' returned an empty query result.
Source query used against target sentinel:
UnifiedSignInLogs
| where TimeGenerated > ago(30d)
| where IPAddress == "185.161.203.120"
| where DeviceDetail.isCompliant == true
| summarize SigninDays=make_set(bin(TimeGenerated,1d))
by
UserPrincipalName,
DeviceId = tostring(DeviceDetail.deviceId),
DisplayName = tostring(DeviceDetail.displayName),
TrustType = tostring(DeviceDetail.trustType)
| project-reorder UserPrincipalName, DeviceId, DisplayName, TrustType, SigninDays
Comment created from external application - func-csoc-incidenthandler-prd-weu 10/03/25, 09:27
GK CSOC Enrichment
{
"185.161.203.120": {
"abuse": {
Normal
Write a comment...
Close
Comment
Playbook Manager


Microsoft Azure
adm.nicholas.lutz@guk....
GLUECKKANJA AG
Home > Microsoft Sentinel | Incidents >
Suspicious LDAP query
Incident number 153869
Refresh
Logs
Tasks
Activity log
This is the new, improved incident page - Now generally available. You can use the toggle to switch back.
Medium
Severity
Closed
Status
adm - Jonas ...
Owner
Investigate in Microsoft Defender XDR
Workspace name
LAW-Sentinel-North-Europe
Description
--
Alert product names
Microsoft Defender for Endpoint
Reason for closing
BenignPositive - Suspicious but expected
Already observed in the past in #80106 and confirmed benign by customer. LDAP queries via ADFind.exe.
Evidence
N/A
Events
1
Alerts
0
Bookmarks
Last update time
09/03/2025, 20:46:46
Creation time
09/03/2025, 19:52:34
Entities (19)
10.252.128.12
cmd.exe
127.0.0.1
View all >
Incident workbook
Incident Overview
Investigate
Overview
Entities
Incident timeline
Search
Add filter
9 Mar
19:51:08
Suspicious LDAP query
Medium | Detected by Microsoft Defender for Endpoint | Tactics:
Similar incidents
verity
Incident number
Title
Medium
148421
Suspicious LDAP query
Medium
142211
Suspicious LDAP query
Medium
150459
Multi-stage incident involving Execution
Incident activity log
Activity logs content : All
Incident status was changed 09/03/25, 20:46
Incident 153869 was closed by adm - Jonas Ripperger. Closing reason is: benign positive suspicious but expected
Incident status was changed 09/03/25, 20:46
Incident status was changed to Active by adm - Jonas Ripperger
Owner was changed 09/03/25, 20:46
Incident owner was changed to adm - Jonas Ripperger by adm - Jonas Ripperger
Comment created from external application - func-csoc-incidenthandler-prd-weu 09/03/25, 20:00
Incident sent to PagerDuty queue: Medium (SLA: 4h)
Comment created from external application - func-csoc-incidenthandler-prd-weu 09/03/25, 19:56
GK CSOC Enrichment
{
"2001:16b8:17ce:2a00:195e:1fab:1f9:cd83": {
"abuse": {
"address": "Versatel West GmbH, Unterste-Wilms-Strasse 29, 44143 Dortmund, Germany",
"email": "abuse@1und1.net",
"name": "Versatel Hostmaster",
"phone": "+49 (0) 231 399 0"
},
"asn": {
Normal
Write a comment...
Close
Comment
Playbook Manager

glueck kanja

HSD

Tool driven detection optimization

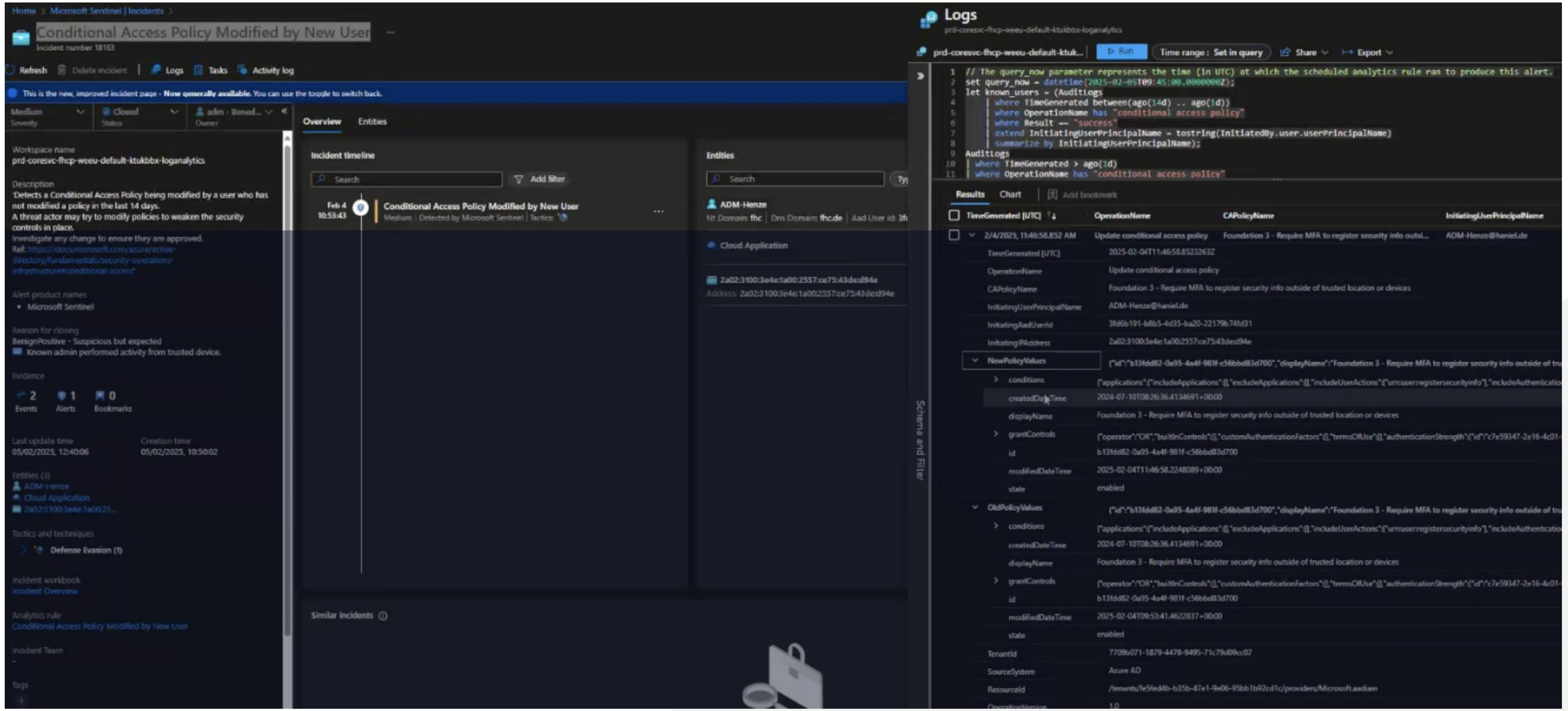


Id	Name	Source	Ma	Total	Not Auto	Not Ignor	Auto Close	Not AC	Noisy T	L	M	H	FP	BP	TP	Unclassified	FP-Rate	BP-Rate	TP-Rate	Time	Reassignme	Notificatio	PB	PBM Clo
c07526f5-abd6-46...	Entra ID User risk set to high	Sentinel	Wide	267	251	245	16	251	2	0	252	15	7	130	71	15%	3%	53%	29%	5 days	27	9	8	0
33e1095f-87af-4e8...	Suspected password compromise by AiTM attack	Sentinel	Wide	296	226	288	40	256	6	0	138	158	26	197	42	8%	9%	68%	15%	5 days	70	30	232	30
9a049638-584f-4f...	Two or more non high alerts raised on one endpoint within 1 ...	Sentinel	Wide	220	220	216	0	220	3	0	0	220	18	139	26	15%	8%	64%	12%	1 weeks	15	9	2	0
be1b6fff-a5c8-45d...	Risky Sign-In Events Bypassing Conditional Access Policies	Sentinel	Wide	123	94	123	29	94	3	1	93	0	4	75	1	35%	3%	61%	1%	1 weeks	7	4	93	0
32b4138b-8e2b-4...	User reported MFA fraud	Sentinel	Wide	81	71	79	0	81	0	1	80	0	1	75	3	0%	1%	95%	4%	22 hours	2	1	73	10
433c3b0a-7278-4...	Expired access credentials being used in Azure	Sentinel	Wide	58	56	58	0	58	3	0	58	0	2	50	0	10%	3%	86%	0%	2 days	6	2	0	2
a2b61057-218c-4c...	CSOC User added or removed	Sentinel	Wide	47	46	47	1	46	0	0	0	0	6	16	0	53%	13%	34%	0%	11 hours	0	0	6	0
14f6da04-2f96-44...	NRT Privileged Role Assigned Outside PIM	Sentinel	Wide	46	41	46	5	41	0	45	1	0	0	27	0	41%	0%	59%	0%	6 days	2	1	0	0
24cb887a-860b-4...	Break Glass Emergency Account sign-in detected	Sentinel	Wide	40	40	40	0	40	0	0	22	18	0	38	0	5%	0%	95%	0%	1 days	0	0	0	0
189f6767-6f12-433...	Unusual number of deleted Entra ID objects	Sentinel	Wide	24	22	23	1	23	0	0	0	24	3	19	1	0%	13%	83%	4%	4 hours	4	1	21	1
d52eda99-4510-4...	Blocked attempts of self-service password reset (SSPR) by u...	Sentinel	Wide	98	18	92	0	98	0	0	98	0	0	91	1	0%	0%	99%	1%	9 hours	11	3	92	80
fc3efd06-433a-42...	Hard deleted objects in Azure AD	Sentinel	Wide	15	15	15	0	15	0	0	0	15	1	14	0	0%	7%	93%	0%	2 hours	3	2	0	0
009b9bae-23dd-4...	End-user consent stopped due to risk-based consent	Sentinel	Wide	12	12	12	0	12	3	0	12	0	0	12	0	0%	0%	100%	0%	7 hours	1	2	0	0
310cb8d7-4f3a-4b...	Dormant or new account register security information from u...	Sentinel	Wide	12	12	12	0	12	0	0	12	0	0	12	0	0%	0%	100%	0%	2 hours	6	3	0	0
b2e907b7-097c-48...	Potential malicious domain registration (Domain Hawk)	Sentinel	Wide	11	11	11	0	11	0	11	0	0	2	6	3	0%	18%	55%	27%	13 hours	12	7	11	0
a8cc6d5c-4e7e-4b...	MFA Spamming followed by Successful login	Sentinel	Wide	9	9	9	0	9	0	0	0	9	3	6	0	0%	33%	67%	0%	2 hours	0	0	0	0
d7feb859-f03e-4e...	Addition of a Temporary Access Pass to a Privileged Account	Sentinel	Wide	9	8	9	1	8	0	0	0	9	0	9	0	0%	0%	100%	0%	4 hours	2	1	0	0
c44269aa-9879-4...	Dangerous API permission consented	Sentinel	Wide	3	3	3	0	3	0	0	0	3	0	2	1	0%	0%	67%	33%	1 hours	1	0	0	0
65c78944-930b-4...	Multi-Factor Authentication Disabled for a User	Sentinel	Wide	2	2	2	0	2	0	0	2	0	0	2	0	0%	0%	100%	0%	22 min	1	0	0	0
f948a32f-226c-411...	Suspicious application consent similar to O365 Attack Toolkit	Sentinel	Wide	1	1	1	0	1	0	0	0	1	0	1	0	0%	0%	100%	0%	13 min	0	0	0	0
Total				1375				1282																

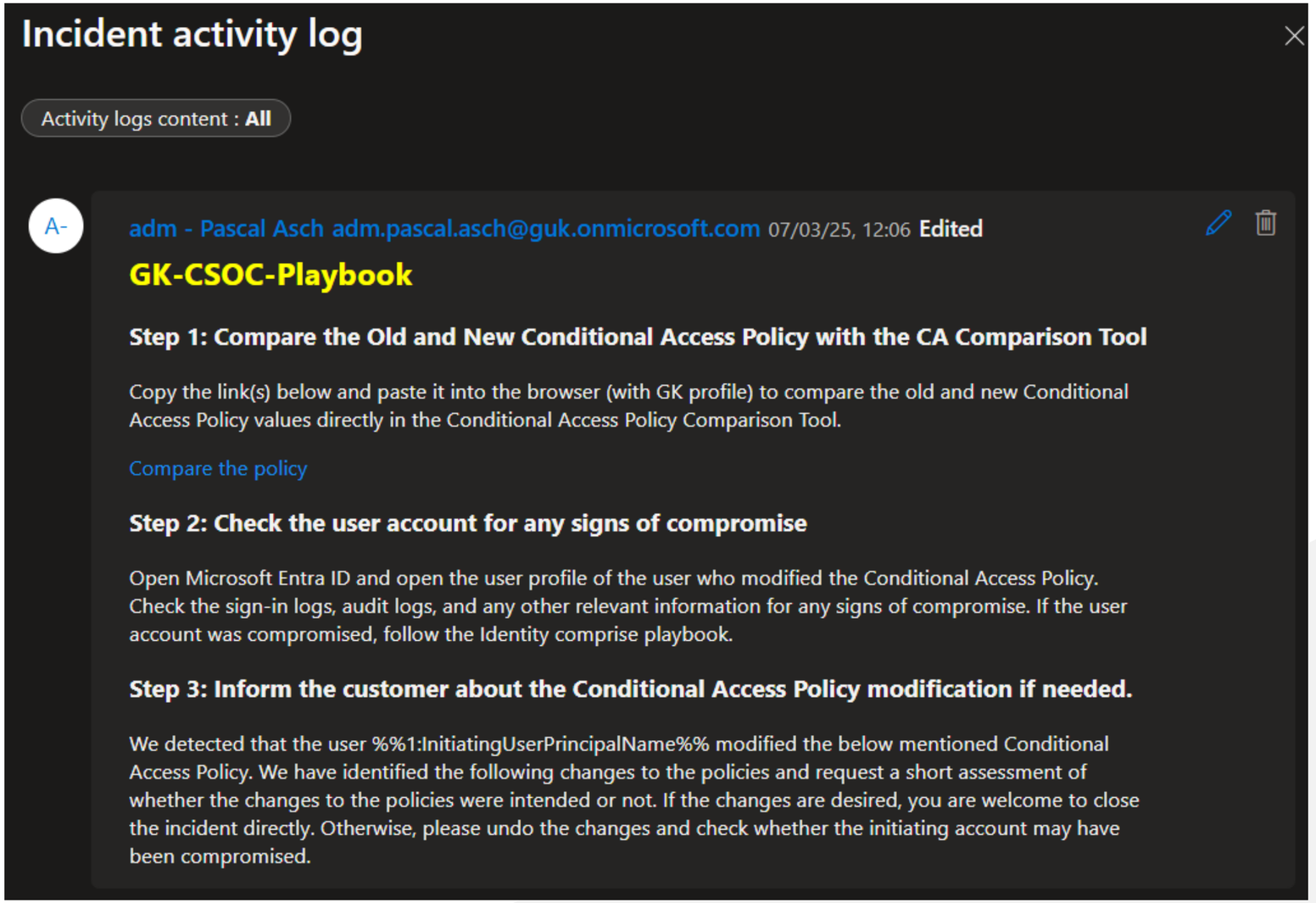
Daily Brown Bag Meetings

- Squads are browsing through the SOC Efficiency Dashboard
- Analysts bring up noisy incidents / improvement ideas
- Automation / Enhancement takes place
  - New Playbooks
  - New Detections / Improved Detections
  - New Manual Approaches
  - New Tools

Conditional Access Policy Modified by New User



Playbook Manager Output



HSD

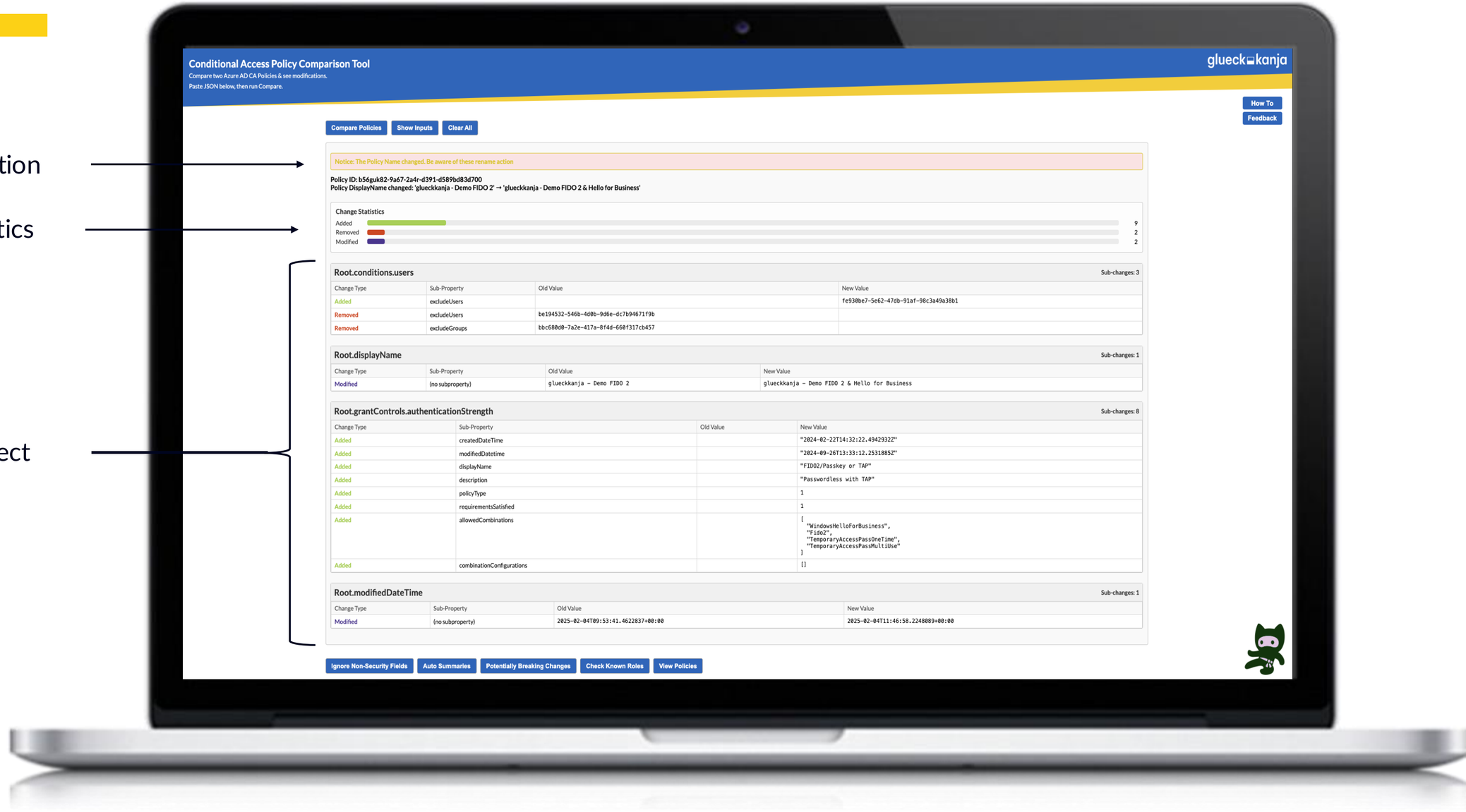
Workflow

Analysis

Basic information

Change statistics

Changes are easy to detect



Workflow

Check Known Roles

Ignore Non-Security Fields | Auto Summaries | Potentially Breaking Changes | Check Known Roles | View Policies

Changed Roles

Change Type	Role ID	Role Name	Path
Added	fe930be7-5e62-47db-91af-98c3a49a38b1	User Administrator	Root.conditions.users

All Recognized Roles (Old & New)

Role ID	Role Name	Found In	Paths
fe930be7-5e62-47db-91af-98c3a49a38b1	User Administrator	New Policy	New: Root.conditions.users.excludeUsers[0]

Detect Roles in the policy

Easy readable role name

Shows the location

glueckkanja

Workflow

Auto Summaries

Ignore Non-Security Fields | Auto Summaries | Potentially Breaking Changes | Check Known Roles | View Policies

We have detected **13** changes in this Conditional Access Policy. The modification of this policy was done at 2025-02-04T11:46:58.2248089+00:00.

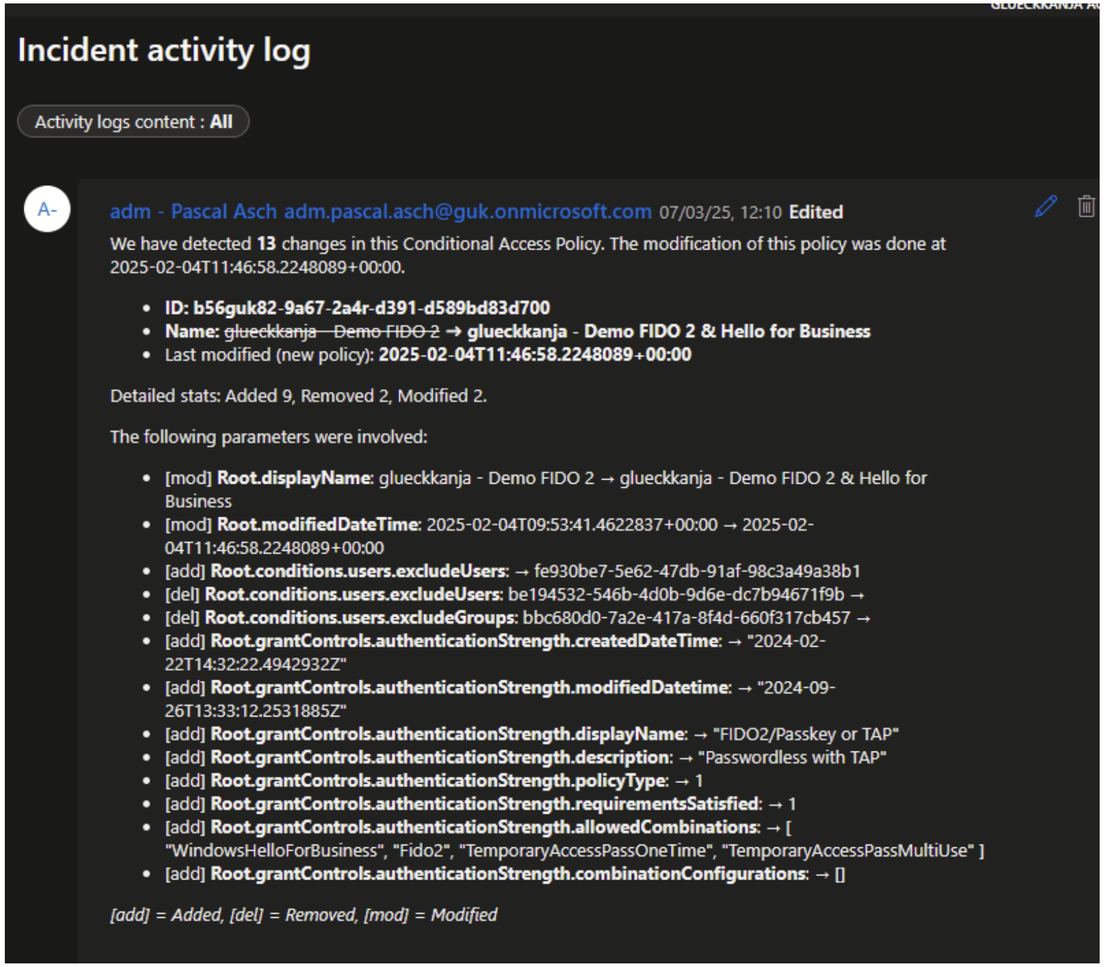
- **ID: b56guk82-9a67-2a4r-d391-d589bd83d700**
- **Name:** ~~glueckkanja - Demo FIDO 2~~ **→ glueckkanja - Demo FIDO 2 & Hello for Business**
- Last modified (new policy): **2025-02-04T11:46:58.2248089+00:00**

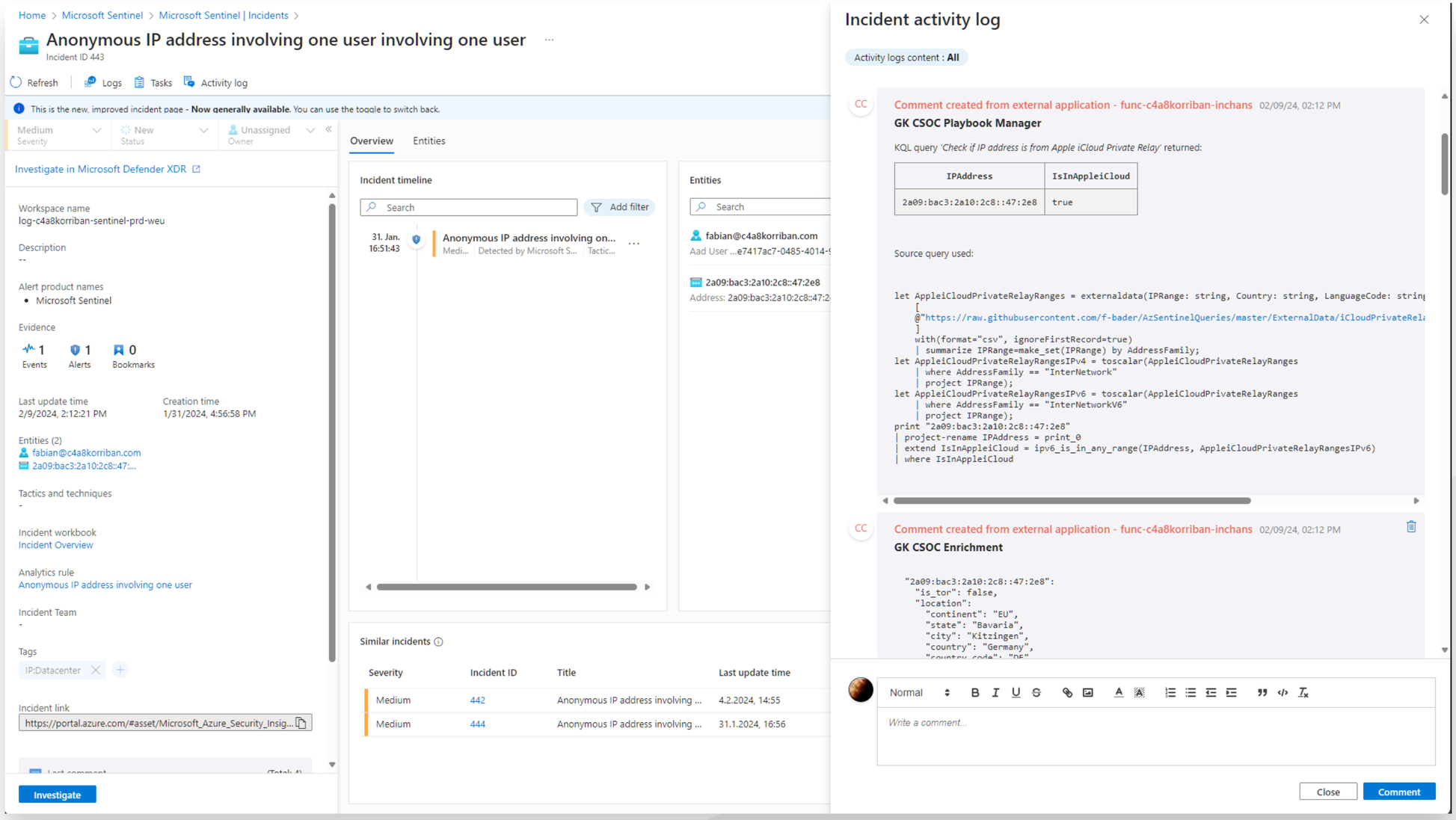
Detailed stats: Added 9, Removed 2, Modified 2.
The following parameters were involved:

- [mod] **Root.displayName**: ~~glueckkanja - Demo FIDO 2~~ → glueckkanja - Demo FIDO 2 & Hello for Business
- [mod] **Root.modifiedDateTime**: ~~2025-02-04T09:53:41.4622837+00:00~~ → 2025-02-04T11:46:58.2248089+00:00
- [add] **Root.conditions.users.excludeUsers**: → fe930be7-5e62-47db-91af-98c3a49a38b1
- [del] **Root.conditions.users.excludeUsers**: ~~be194532-546b-4d0b-9d6e-dc7b94671f9b~~ →
- [del] **Root.conditions.users.excludeGroups**: ~~bbc680d0-7a2e-417a-8f4d-660f317cb457~~ →
- [add] **Root.grantControls.authenticationStrength.createdDateTime**: → "2024-02-22T14:32:22.4942932Z"
- [add] **Root.grantControls.authenticationStrength.modifiedDatetime**: → "2024-09-26T13:33:12.2531885Z"
- [add] **Root.grantControls.authenticationStrength.displayName**: → "FIDO2/Passkey or TAP"
- [add] **Root.grantControls.authenticationStrength.description**: → "Passwordless with TAP"
- [add] **Root.grantControls.authenticationStrength.policyType**: → 1
- [add] **Root.grantControls.authenticationStrength.requirementsSatisfied**: → 1
- [add] **Root.grantControls.authenticationStrength.allowedCombinations**: → ["WindowsHelloForBusiness", "Fido2", "TemporaryAccessPassOneTime", "TemporaryAccessPassMultiUse"]
- [add] **Root.grantControls.authenticationStrength.combinationConfigurations**: → []

[add] = Added, [del] = Removed, [mod] = Modified

Copy to Sentinel




Home > Microsoft Sentinel > Microsoft Sentinel | Incidents >
Anonymous IP address involving one user involving one user
Incident ID 443
Refresh
Logs
Tasks
Activity log
This is the new, improved incident page - Now generally available. You can use the toggle to switch back.
Medium
Severity
New
Status
Unassigned
Owner
Investigate in Microsoft Defender XDR
Workspace name
log-c4a8korriban-sentinel-prd-weu
Description
--
Alert product names
Microsoft Sentinel
Evidence
1
Events
1
Alerts
0
Bookmarks
Last update time
2/9/2024, 2:12:21 PM
Creation time
1/31/2024, 4:56:58 PM
Entities (2)
fabian@c4a8korriban.com
2a09:bac3:2a10:2c8::47:...
Tactics and techniques
-
Incident workbook
Incident Overview
Analytics rule
Anonymous IP address involving one user
Incident Team
-
Tags
IP:Datacenter
Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insig...
Investigate
Overview
Entities
Incident timeline
Search
Add filter
31. Jan.
16:51:43
Anonymous IP address involving on...
Medi...
Detected by Microsoft S...
Tactic...
Entities
Search
fabian@c4a8korriban.com
Aad User ...e7417ac7-0485-4014-
2a09:bac3:2a10:2c8::47:2e8
Address: 2a09:bac3:2a10:2c8::47:2
Similar incidents
Severity
Incident ID
Title
Last update time
Medium
442
Anonymous IP address involving ...
4.2.2024, 14:55
Medium
444
Anonymous IP address involving ...
31.1.2024, 16:56
Incident activity log
Activity logs content : All
CC
Comment created from external application - func-c4a8korriban-inchans
02/09/24, 02:12 PM
GK CSOC Playbook Manager
KQL query 'Check if IP address is from Apple iCloud Private Relay' returned:
IPAddress
IsInAppleiCloud
2a09:bac3:2a10:2c8::47:2e8
true
Source query used:
let AppleiCloudPrivateRelayRanges = externaldata(IPRange: string, Country: string, LanguageCode: string
[
@"https://raw.githubusercontent.com/f-bader/AzSentinelQueries/master/ExternalData/iCloudPrivateRela
]
with(format="csv", ignoreFirstRecord=true)
| summarize IPRange=make_set(IPRange) by AddressFamily;
let AppleiCloudPrivateRelayRangesIPv4 = toscalar(AppleiCloudPrivateRelayRanges
| where AddressFamily == "InterNetwork"
| project IPRange);
let AppleiCloudPrivateRelayRangesIPv6 = toscalar(AppleiCloudPrivateRelayRanges
| where AddressFamily == "InterNetworkV6"
| project IPRange);
print "2a09:bac3:2a10:2c8::47:2e8"
| project-rename IPAddress = print_0
| extend IsInAppleiCloud = ipv6_is_in_any_range(IPAddress, AppleiCloudPrivateRelayRangesIPv6)
| where IsInAppleiCloud
CC
Comment created from external application - func-c4a8korriban-inchans
02/09/24, 02:12 PM
GK CSOC Enrichment
"2a09:bac3:2a10:2c8::47:2e8":
"is_tor": false,
"location":
"continent": "EU",
"state": "Bavaria",
"city": "Kitzingen",
"country": "Germany",
Normal
Write a comment...
Close
Comment

glueckkanja

HSD

Threat & Vulnerability Management

- Based on Defender for Endpoint
- Ad-hoc Recommendations for new **critical** vulnerabilities
  - Through notification, member-only newsletter & monthly reports

TOP 10 SOFTWARE VULNERABILITIES

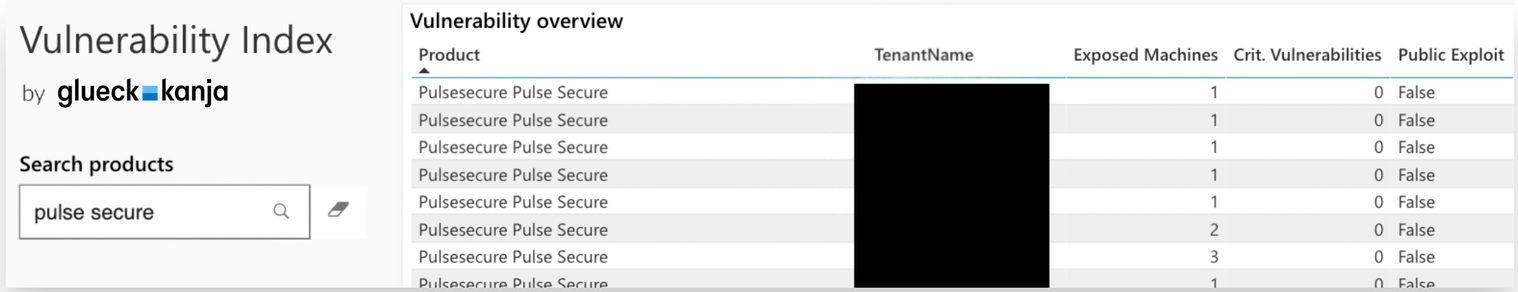
Product	Machines	Vulnerabilities	Impact
Google Chrome	1809	891	12.09
Microsoft Edge Chromium-based	431	236	2.88
Microsoft Windows 10	191	1118	2.24
Cisco Ios	116	201	1.62
Zoom	290	3	1.43
Apache Log4j	172	7	1.42
Microsoft Office	182	52	1.22
Oracle Jre	117	605	0.85
Openbsd Openssh	88	50	0.77
Microsoft .NET Framework	109	6	0.63

Public Exploit

Windows Hyper-V Elevation of Privilege Vulnerability

CSOC Severity

- Critical (Now)
- High (4 Weeks)
- Medium (8 Weeks)

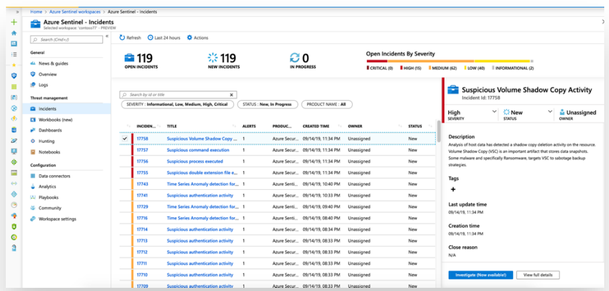


glueck kanja

HSD

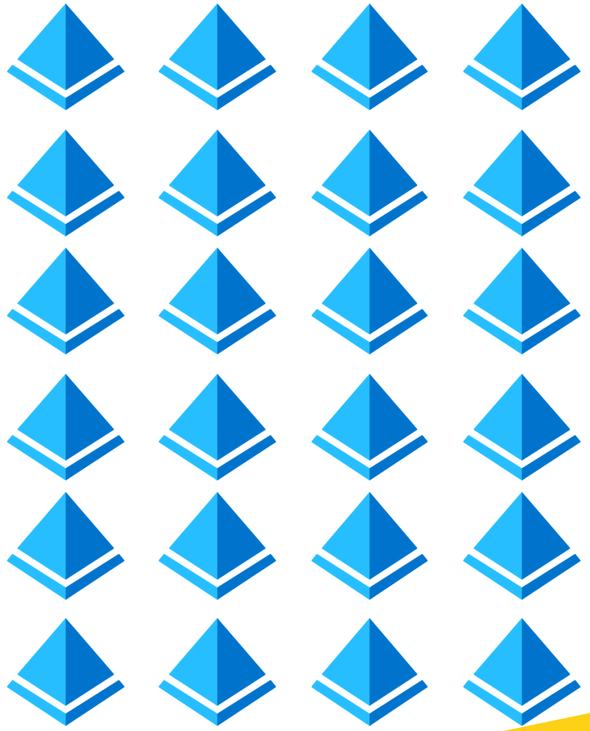
Threat Intelligence – Global Insights

Incident IOCs from Customer Tenant



GK Threat Research

All Customer Tenants

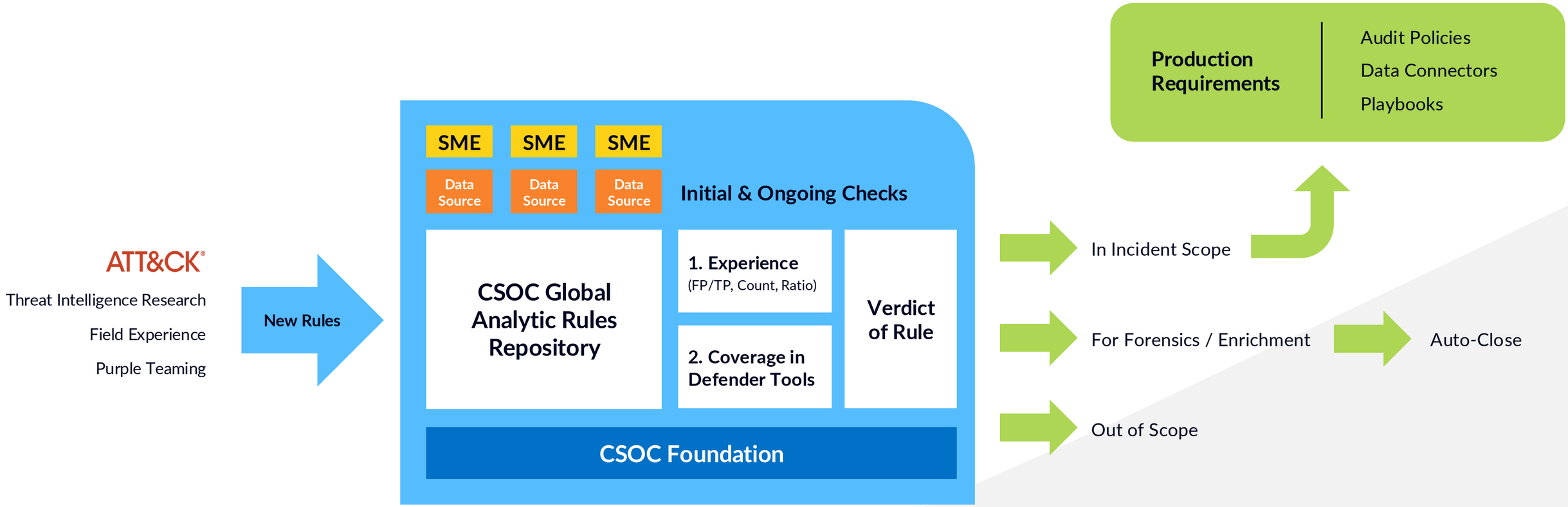


CSOC Foundation

glueck kanja

HSD

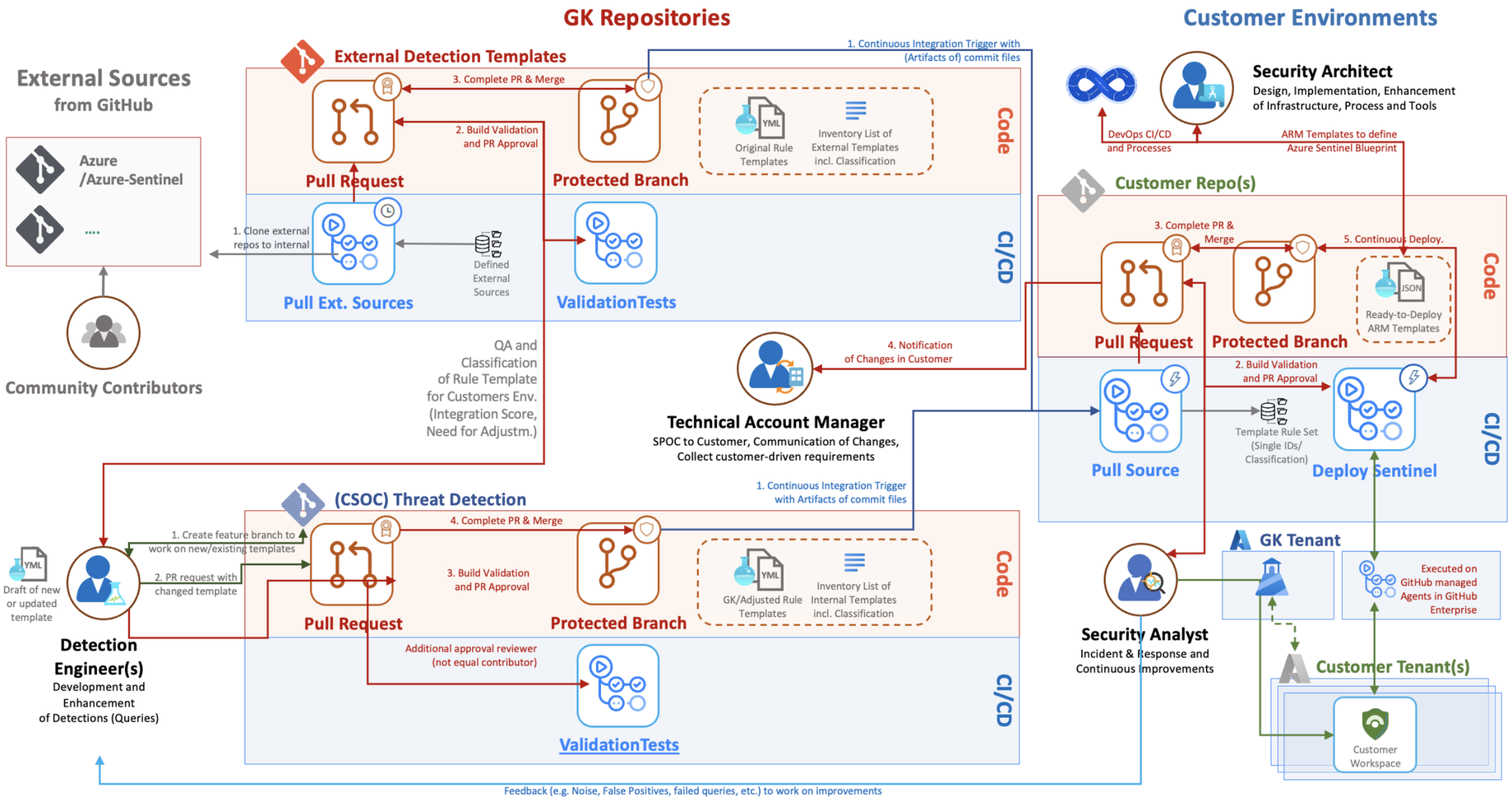
Advanced Detection Lifecycle



glueck kanja

HSD

CSOC Foundation



glueck kanja

HSD

Highly Secure Working Environment

Preventing Supply-Chain Attacks

Customer Environment

CSOC Admin Accounts can only logon to customer resources from PAW - CA Device Filter, **coming soon**.

Azure Lighthouse, GDAP & MTO

CSOC Red Tenant

CSOC Admins login via FIDO2 only

GK CSOC PAW

- Restricted Web Access
- Application Control (App-Locker)
- No Local Admin Access
- TPM, VBS, Code Integrity, Secure Boot
- XDR & SIEM Monitoring
- Strict Separation of Duties
- Dedicated PW Management

Stricly Restricted Data Transfer and Sharing Capabilities

GK Office Tenant

glueck kanja

HSD

Zusammengefasste Perspektive der HSD

glueckkanja gab

Thank you.
Open Questions?

Contact me via LinkedIn:
https://www.linkedin.com/in/JanGeisbauer