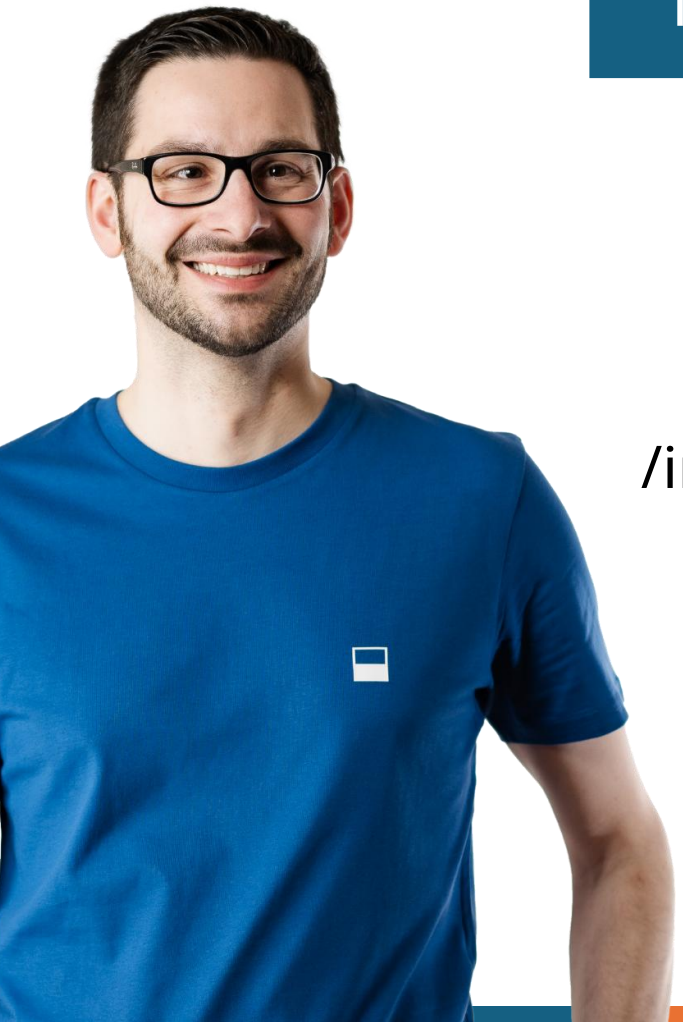
How to build an Entra-ordinary Security Monitoring

Copilot included!

Christopher Brumm,
Thomas Naunheim

Workplace Ninja Summit 2025

About us...



Thomas Naunheim		Chris Brumm
old		very old
Koblenz, Germany		Hamburg, Germany
left-handed		right-handed
@thomas_live		@cbrhh
/in/thomasnaunheim		/in/christopherbrumm
cloud-architekt.net		chris-brumm.com

working at glueckkanja AG
as Cyber Security Architect
Microsoft Identity & Access MVPs
❤️ (punk-rock) music 🤘 and good wine 🍷

Detection Engineering Landscape

Maturity

Data Sources

Detection Engine

Incident Triage and Correlation

Response Engine

Incident/Response Flow

Detection Engineering Landscape

www.wpninjas.eu
#WPNinjaS

Maturity

Data Sources

- WatchLists and Info tables
- UEBA and Behaviors
- Microsoft Entra Diagnostic Logs
- XDR Advanced Hunting Table
- Entra ID Protection / MDI

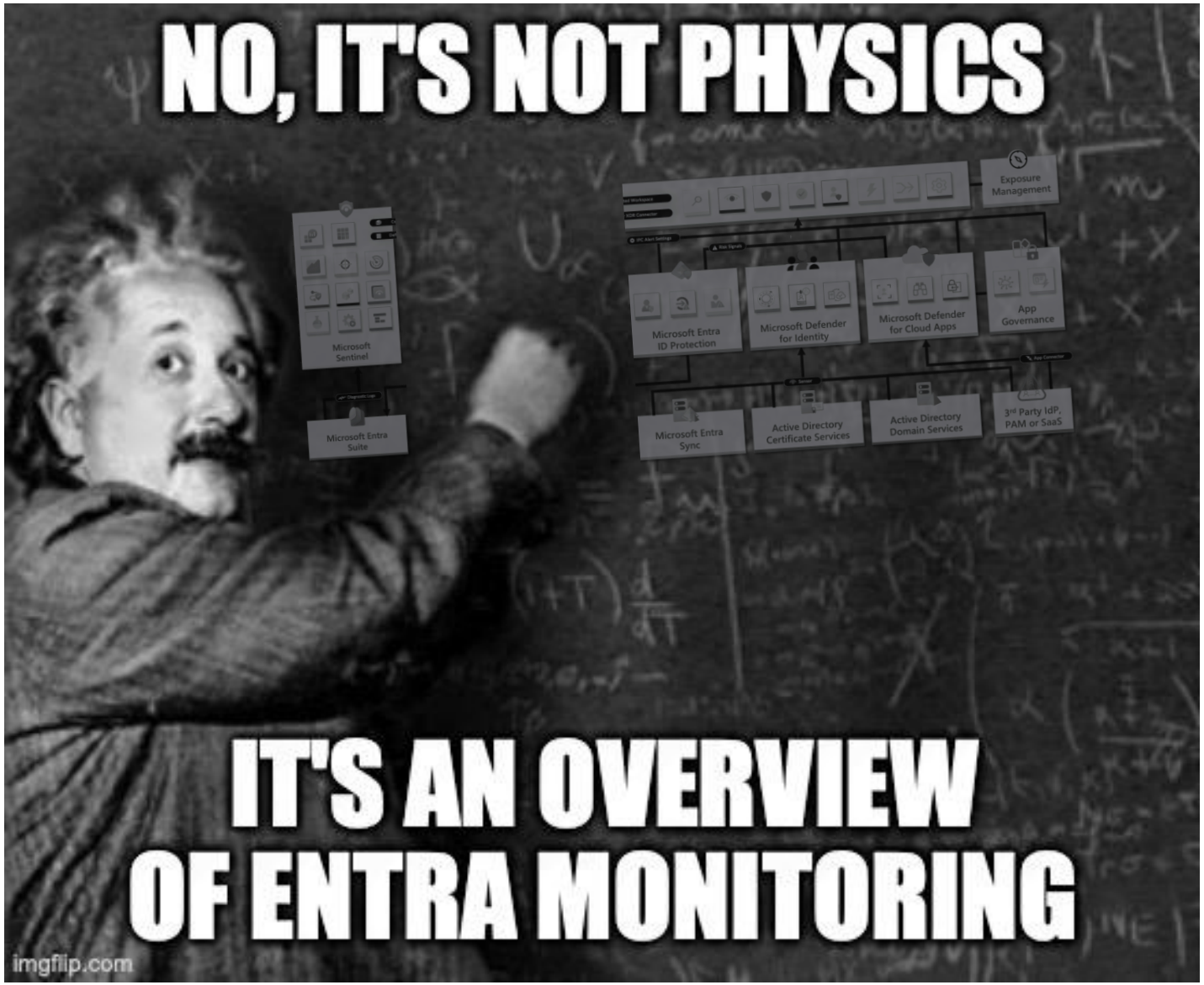
Detection Engine

Incident Triage and Correlation

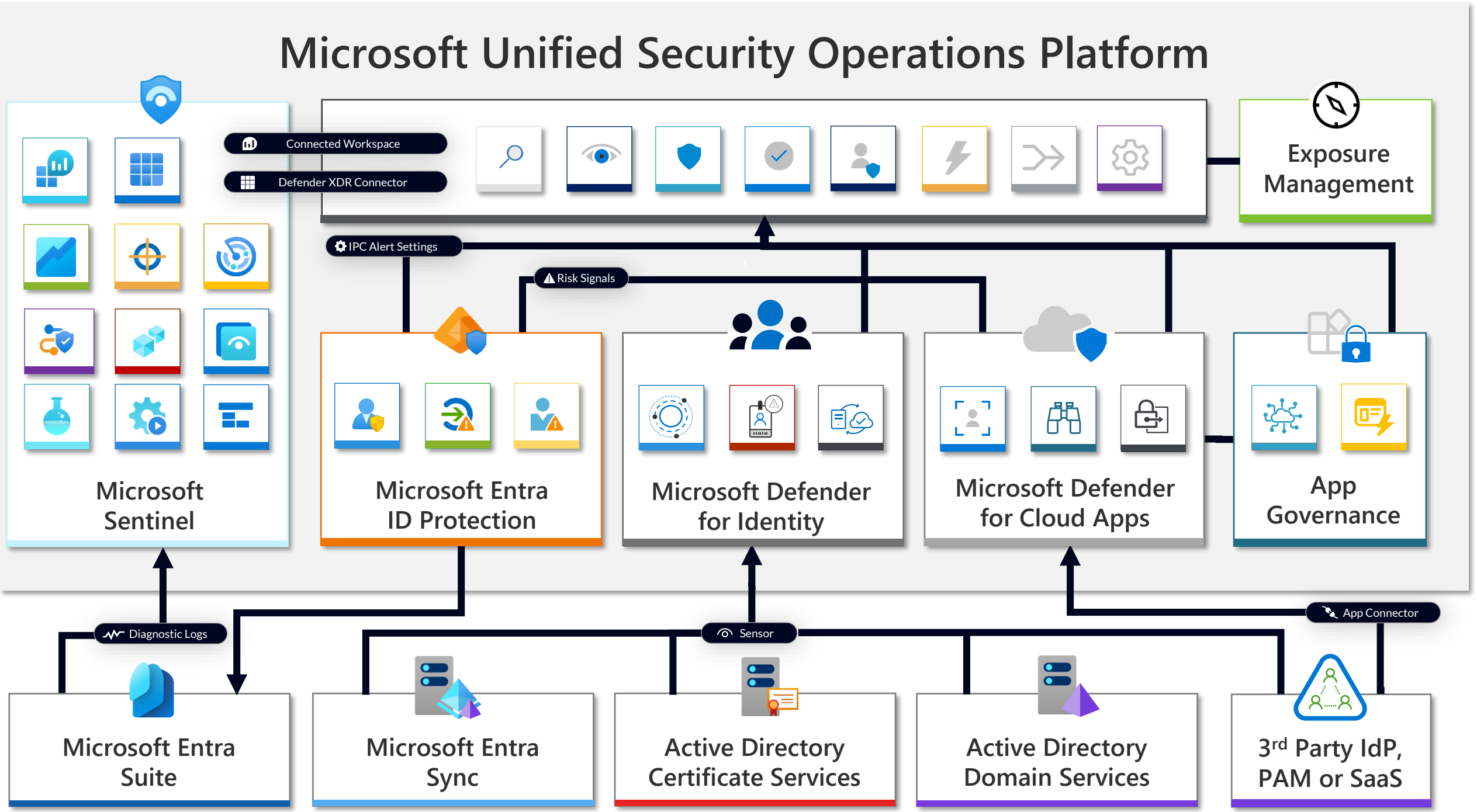
Response Engine

Incident/Response Flow

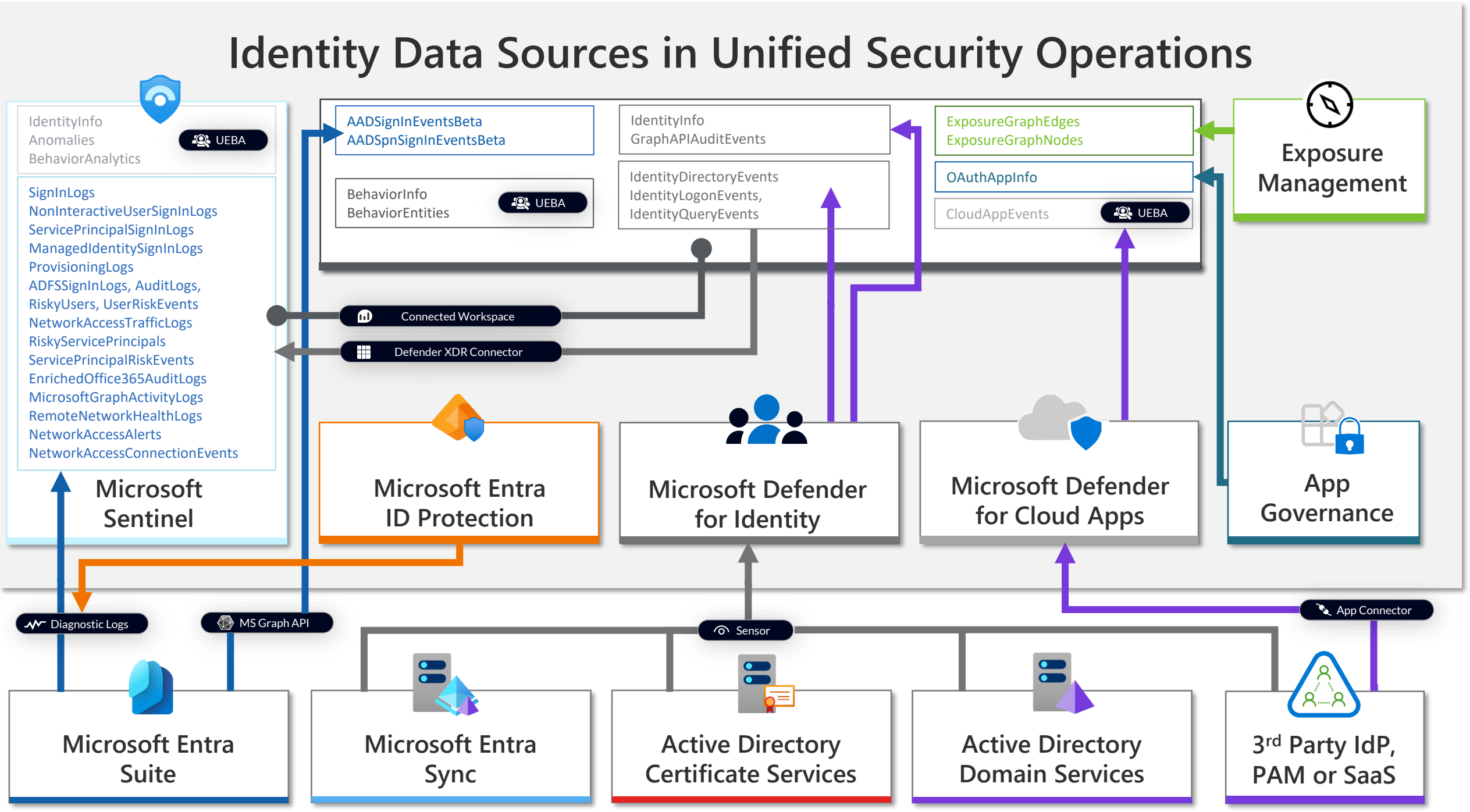
USOP + X = Entra-ordinary SecOps?



Microsoft Unified Security Operations Platform



Identity Data Sources in Unified Security Operations



Which data source for sign-ins?

- **SignInLogs and AADNonInteractiveUserSignInLogs:** Sign-in data from Diagnostic Logs

Run | Time range : Last 24 hours | Show : 1000 results

```
union isfuzzy=true SigninLogs, AADNonInteractiveUserSignInLogs
| extend ConditionalAccessPolicies = coalesce(todynamic(ConditionalAccessPolicies_stri
| extend Status = coalesce(todynamic(Status_string), Status_dynamic)
| extend MfaDetail = coalesce(todynamic(MfaDetail_string), MfaDetail_dynamic)
| extend DeviceDetail = coalesce(todynamic(DeviceDetail_string), DeviceDetail_dynamic)
| extend LocationDetails = coalesce(todynamic(LocationDetails_string), LocationDetails
| extend TokenProtectionStatusDetails = coalesce(todynamic(TokenProtectionStatusDetail
// Remove duplicated columns
| project-away *_dynamic, *_string
```

Results | Chart | Add bookmark

AppDisplayName	ResourceDisplayName	Category
Azure Portal	Azure Resource Manager	NonInteractiveUserSignI
Azure Portal	Azure Portal	NonInteractiveUserSignI
Azure Portal	ADIbizaUX	NonInteractiveUserSignI
Azure Portal	Microsoft Graph	NonInteractiveUserSignI
Azure Purview	ComplianceAuthServer	NonInteractiveUserSignI
Azure Purview	Microsoft Graph	NonInteractiveUserSignI
Azure Purview	Security Copilot API	NonInteractiveUserSignI
Azure Purview	ComplianceAuthServer	NonInteractiveUserSignI
Azure Purview	Microsoft Graph	NonInteractiveUserSignI
Azure Purview	Azure Purview	NonInteractiveUserSignI
Device Management Client	Microsoft Device Management ...	NonInteractiveUserSignI
Device Management Client	Microsoft Device Management ...	NonInteractiveUserSignI

```
imAuthentication()
| where TimeGenerated >ago(7d)
| distinct Application, Dst, Type, EventResult
```

Results | Chart | Add bookmark

Application	Dst	Type	EventResult
		AADNonInteractiveUserSignInL...	Failure
Attestation Service	Attestation Service	AADManagedIdentitySignInLogs	Success
Azure Key Vault	Azure Key Vault	AADManagedIdentitySignInLogs	Success
Azure Monitor Control Service	Azure Monitor Control Service	AADManagedIdentitySignInLogs	Success
Azure Monitor Control Service	Azure Monitor Control Service	AADServicePrincipalSignInLogs	Success
Azure Resource Manager	Azure Resource Manager	AADManagedIdentitySignInLogs	Success
Azure Resource Manager	Azure Resource Manager	AADServicePrincipalSignInLogs	Success
Azure Storage	Azure Storage	AADManagedIdentitySignInLogs	Success
Microsoft Entra AD Synchronization ...	Microsoft Entra AD Synchroniza...	AADServicePrincipalSignInLogs	Success
Microsoft Graph	Microsoft Graph	AADManagedIdentitySignInLogs	Success
Microsoft Graph	Microsoft Graph	AADServicePrincipalSignInLogs	Success
Microsoft Intune API	Microsoft Intune API	AADManagedIdentitySignInLogs	Success
Microsoft.EventHubs	Microsoft.EventHubs	AADManagedIdentitySignInLogs	Success
SCEPman-api	SCEPman-api	AADManagedIdentitySignInLogs	Success
Verifiable Credentials Service Request	Verifiable Credentials Service R...	AADManagedIdentitySignInLogs	Success
WindowsDefenderATP	WindowsDefenderATP	AADManagedIdentitySignInLogs	Success

Which data source for sign-ins?

- **IdentityLogonEvents:** Sign-in data from MDA App Connectors and MDI

Query

```
1  IdentityLogonEvents
2  | where TimeGenerated >ago(365d)
3  | distinct Type, Application, ActionType, LogonType
4  | summarize ActionTypes = array_sort_asc(make_set(ActionType)), LogonTypes = array_sort_asc(make_set(LogonType)) by Application
```

Getting started | Resu

Export | Show

Filters: Add filter

Application

Microsoft 365

Microsoft Azu

Active Directo

App Connectors

App connectors provide you with greater visibility and control over your cloud apps.

Basic filter

Filters: App: **Any** | App category: **Any** | Connected by: **Any**

Connect an app

App	Category	Status	Was connected on
Microsoft 365	Collaboration	Connected	Mar 31, 2021 1:20 PM
Microsoft Azure	Cloud computing platform	Connected	Sep 14, 2020 6:37 PM

Which data source for sign-ins?

- **AADSignInEventsBeta:** Limited set of data from Microsoft Graph API

Run query | Last 3 hours | Save | Share link

Query

```
1  AADSignInEventsBeta
2  | distinct Application, ResourceDisplayName, LogonType, EndpointCall, ErrorCode
```

Getting started | Results | Query history

Export | Show empty columns | 97 items | Search | 00:01.691 | Low

Application	ResourceDisplayName	LogonType	EndpointCall	ErrorCode
Azure Portal	Azure Portal	["nonInteractiveUser"]	OAuth2:Token	0
Azure Portal	Azure Resource Manager	["interactiveUser"]	Login:login	50140
Azure Portal	Azure Resource Manager	["interactiveUser"]	OAuth2:Authorize	0
Azure Portal	ADIbizaUX	["nonInteractiveUser"]	OAuth2:Token	0
Azure Portal	Azure Resource Manager	["interactiveUser"]	Kmsi:kmsi	0
Azure Purview	Security Copilot API	["nonInteractiveUser"]	OAuth2:Token	0
Azure Purview	Azure Purview	["nonInteractiveUser"]	OAuth2:Token	0
Azure Purview	ComplianceAuthServer	["nonInteractiveUser"]	OAuth2:Token	0
Azure Purview	Microsoft Graph	["nonInteractiveUser"]	OAuth2:Token	0
M365 Admin Services	M365 Commerce Mana...	["nonInteractiveUser"]	OAuth2:Token	0
M365 Admin Services	ecvl-assets-aad	["nonInteractiveUser"]	OAuth2:Token	0
Microsoft 365 App Catalo...	Olympus	["nonInteractiveUser"]	OAuth2:Token	0
Microsoft 365 Security an...	Microsoft Office 365 Por...	["nonInteractiveUser"]	OAuth2:Token	0

Selection of data source for detections

Choose right data source and detection engine

- ✓ All required information and details are available?
- ✓ How much latency between event time and ingestion?
- ✓ Which licenses are required?
- ✓ Which pricing model for data ingestion?
- ✓ How long is the retention time for log entries?
- ✓ Can I use NRT or custom enrichment?
- ✓ Lookback and interval options?
- ✓ What are the option for automated response?

Detection Engineering Landscape

www.wpninjas.eu
#WPNinjaS

Maturity

Data Sources

- WatchLists and Info tables
- UEBA and Behaviors
- Microsoft Entra Diagnostic Logs
- XDR Advanced Hunting Table
- Entra ID Protection / MDI

Detection Engine

Incident Triage and Correlation

Response Engine

Incident/Response Flow

Detection Engineering Landscape

www.wpninjas.eu
#WPNinjaS

Maturity

Data Sources

- WatchLists and Info tables
- UEBA and Behaviors
- Microsoft Entra Diagnostic Logs
- XDR Advanced Hunting Table
- Entra ID Protection / MDI

Detection Engine

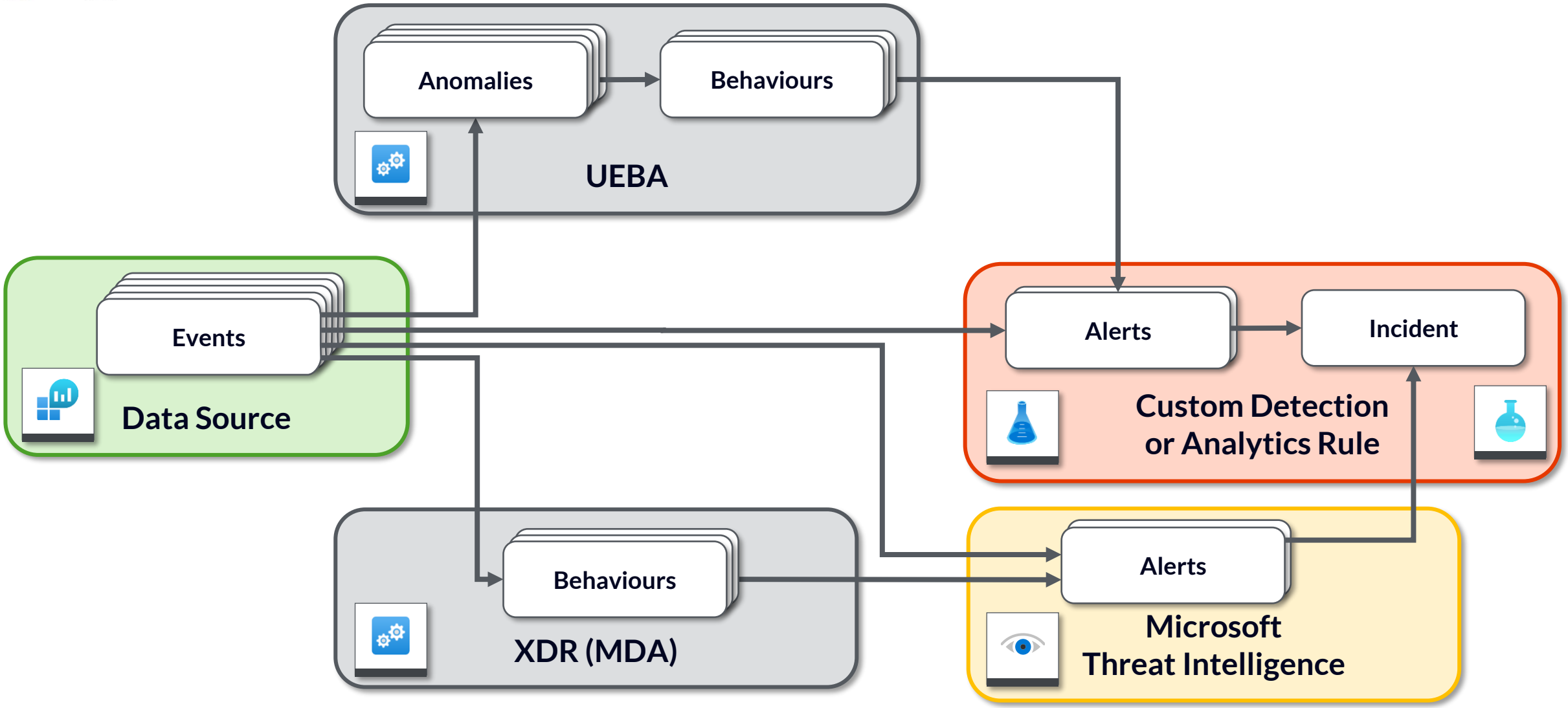
- Analytics Rules
- Custom Detections

Incident Triage and Correlation

Response Engine

Incident/Response Flow

Mysterious ways of incident creation



Behaviors in Defender XDR

www.wpninjas.eu
#WPNinjaS

MDA App Policy

- Activity from infrequent country [Disabled]
  This policy profiles your environment and triggers alerts when activity is detecte...
- Multiple failed login attempts [Disabled]
  This policy profiles your environment and triggers alerts when users perform mul...
- Multiple VM creation activities [Disabled]
  This policy profiles your environment and triggers alerts when users perform mul...
- Multiple Power BI report sharing activities [Disabled]
  This policy profiles your environment and triggers alerts when users perform mul...
- Impossible travel [Disabled]
  This policy profiles your environment and triggers alerts when activities are detec...

Detection

- Suspicious Azure activities related to crypto. mining
- New external user account created by risky user
- Azure AD app registration by risky user
- Risky user created global admin
- Access elevation by risky user
- Risky user added permissions over other mailboxes
- Suspicious role assignment by a risky user
- Unusual activities by AAD Connect sync account

Not meet standard for alerts useful in providing context during an investigation.

Transition to Behaviors and combined detections

Combine Entra ID Protection Alerts + SaaS App Data

Demo: UEBA vs. Behaviors

Capabilities by UEBA and Behaviors table in XDR

Anatomy of an Analytics Rule

www.wpninjas.eu
#WPNinjaS

Infos

Id, name, description, Version , Tags, metadata

Dependencies

requiredDataConnectors
(connectorId, dataTypes)

Alert Attributes

severity

tactics
relevantTechniques

entityMappings,
customDetails

Detection

Query
triggerOperator
triggerThreshold

queryFrequency
queryPeriod
kind

Alert/Incident Creation

createIncident
reopenClosedIncident

suppressionEnabled

Event/Alert Grouping

aggregationKind

enabled
lookbackDuration
matchingMethod
groupByEntities
groupByAlertDetails
groupByCustomDetails

Anatomy of a Custom Detection

Infos

- alertDescription, alertRecommendedAction, guid, ruleName

Dependencies

- N/A

Alert Attributes

- alertSeverity
- alertCategory mitreTechniques
- impactedEntities, customDetails

Detection

- queryText
- frequency

Alert/Incident Creation

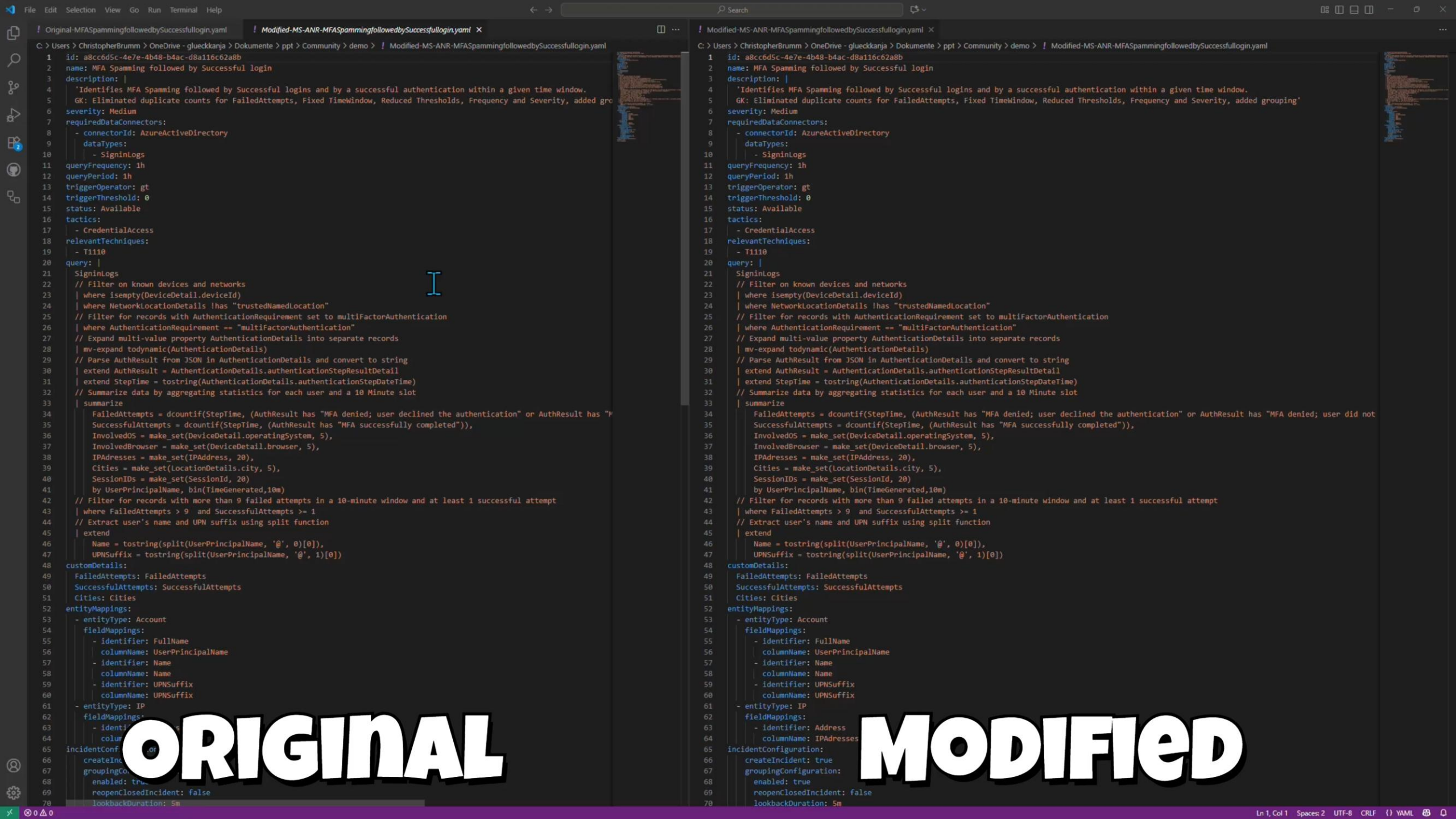
- isEnabled
- alertTitle

Event/Alert Grouping

- N/A

Demo: …

Examples of noisy (default) analytic rule templates from Content Hub and how to optimize them


ORIGINAL
MODIFIED

Example: MFASpammingfollowedbySuccessfullogin.yaml

Prompt:

Please summarize the difference of both files as a table. Focus on what is used for summarize and the Failed/Success Counts in the query and include also the Incident and Event Grouping and Entities, CustomDetails, frequency and severity

Summary:

The modified version improves deduplication of attempts, uses a longer time window, lowers thresholds, adds incident/event grouping, includes custom details, and reduces frequency and severity. It also changes entity mapping for IPs to a set and adds grouping by Account for incidents.

Aspect	Original	Modified
Summarize Logic	Aggregates by UserPrincipalName, IPAddress, State, City, Region and computes min/max times for window.	Aggregates by UserPrincipalName and 10-minute time bins. Collects sets of OS, browser, IPs, cities, session IDs.
Failed Count	FailedAttempts = countif(AuthResult == "...") (simple count of failed MFA attempts)	FailedAttempts = dcountif(StepTime, ...) (distinct count of failed MFA attempts by step time)
Success Count	SuccessfulAttempts = countif(AuthResult == "...") (simple count of successful MFA)	SuccessfulAttempts = dcountif(StepTime, ...) (distinct count of successful MFA by step time)
Thresholds	FailedAttempts > 10 in <= 5m window, SuccessfulAttempts >= 1	FailedAttempts > 9 in 10m window, SuccessfulAttempts >= 1
Frequency/Period	queryFrequency: 1d, queryPeriod: 1d	queryFrequency: 1h, queryPeriod: 1h
Severity	High	Medium
Incident Grouping	Not present	Present: Groups by Account, 5m lookback, no reopen, selected matching
Event Grouping	Not present	aggregationKind: AlertPerResult
Entities	Account (FullName, Name, UPNSuffix), IP (Address)	Account (FullName, Name, UPNSuffix), IP (IPAdresses)
Custom Details	Not present	FailedAttempts, SuccessfulAttempts, Cities

Building Detections is easy!

www.wpninjas.eu
#WPNinjaS

ATT&CK®

Threat Intelligence Research

Field Experience

Purple Teaming

New Rules

SME **SME** **SME**

Data Source **Data Source** **Data Source**

Detection Engineering

Test / PoC

Production Requirements

F/P Reduction

Enrichment

Playbooks

Detection Engineering Landscape

www.wpninjas.eu
#WPNinjaS

Maturity

Data Sources

- WatchLists and Info tables
- UEBA and Behaviors
- Microsoft Entra Diagnostic Logs
- XDR Advanced Hunting Table
- Entra ID Protection / MDI

Detection Engine

- Analytics Rules
- Custom Detections

Incident Triage and Correlation

Response Engine

Incident/Response Flow

Detection Engineering Landscape

www.wpninjas.eu
#WPNinjaS

Maturity

Data Sources

- WatchLists and Info tables
- UEBA and Behaviors
- Microsoft Entra Diagnostic Logs
- XDR Advanced Hunting Table
- Entra ID Protection / MDI

Detection Engine

- Analytics Rules
- Custom Detections

Incident Triage and Correlation

- Custom Enrichment Engine
- Custom Correlation Engine
- XDR Correlation Engine

Response Engine

Incident/Response Flow

Microsoft Sentinel Fusion

www.wpninjas.eu
#WPNinjaS

Dashboard > Microsoft Sentinel | Incidents >

Preview: Possible multistage attack activities detected by Fusion

Incident number 4518

Refresh | Delete incident | Logs | Tasks | Activity log

High
Severity

New
Status

Unassigned
Owner

Overview | Entities

Workspace name
lab-la-4d3e5b65-8a52-4b2f-bf5c-d1620c700136

Description
This Fusion incident triggered by our machine learning model correlates anomalous signals and suspicious activities that are potentially associated with multistage attacks on User: thomas@cloud-architekt.net. We recommend that you investigate all alerts and/or anomalies included in this incident to understand the full chain of attack and take immediate actions to remediate.
Some alerts in this Fusion incident are converted from anomalies. You can view details in the Anomalies table using the following query:
View anomalies in Log Analytics

For more information about this detection, please visit https://aka.ms/SentinelFusion

Incident timeline

Search

Add filter

Nov 14 10:06:21 — Mail.Read Permissions Grante... — Me... | Detected by Micro... | Ta...

Nov 14 07:12:56 — Anomalous Azure operations — Infor... | Detected by M... | Ta...

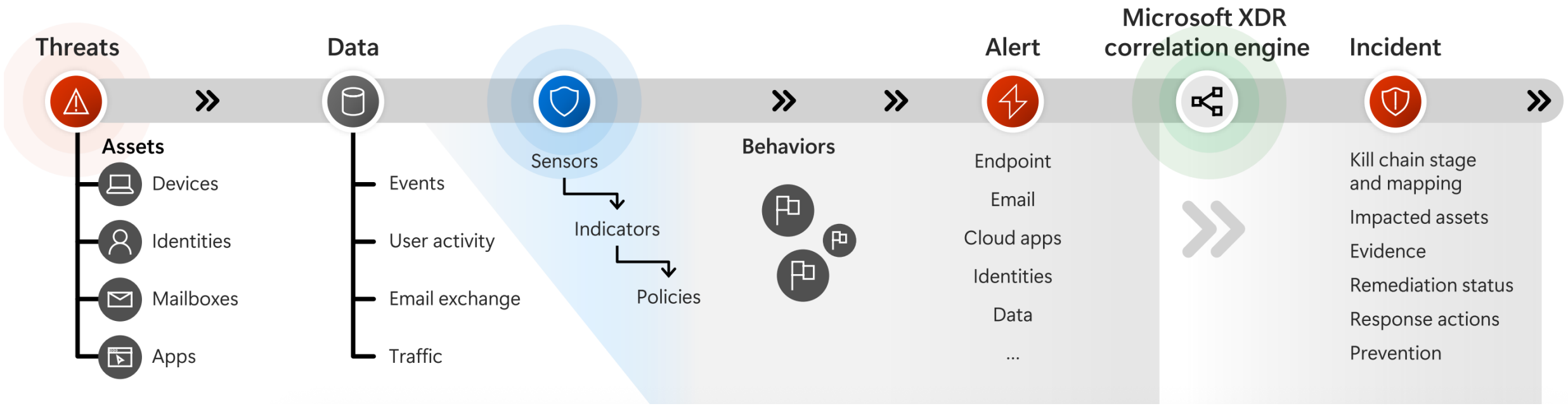
Nov 12 11:45:28 — Changes to Application Owner... — M... | Detected by Mi... | Ta...

Other Examples for Credential harvesting scenarios

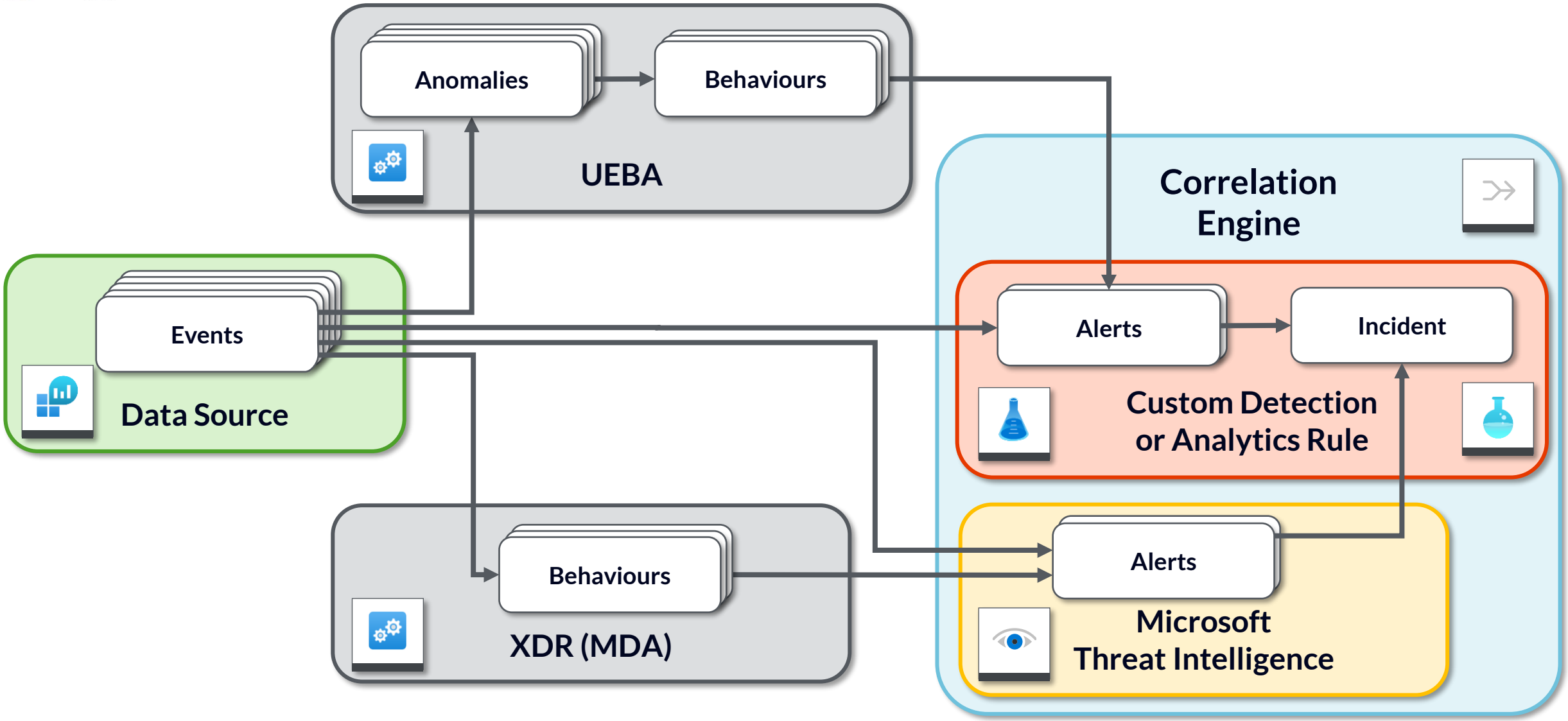
- Impossible travel to atypical locations leading to malicious credential theft tool execution
- Sign-in event from an unfamiliar location leading to malicious credential theft tool execution
- Sign-in event from an anonymous IP address leading to malicious credential theft tool execution
- Sign-in event from user with leaked credentials leading to malicious credential theft tool execution

XDR Correlation Engine

www.wpninjas.eu
#WPNinjaS



Levels


Anomalies
Behaviours
UEBA
Correlation Engine
Events
Data Source
Alerts
Incident
Custom Detection or Analytics Rule
Behaviours
XDR (MDA)
Alerts
Microsoft Threat Intelligence

Improve focus on incidents

www.wpninjas.eu
#WPNinjaS

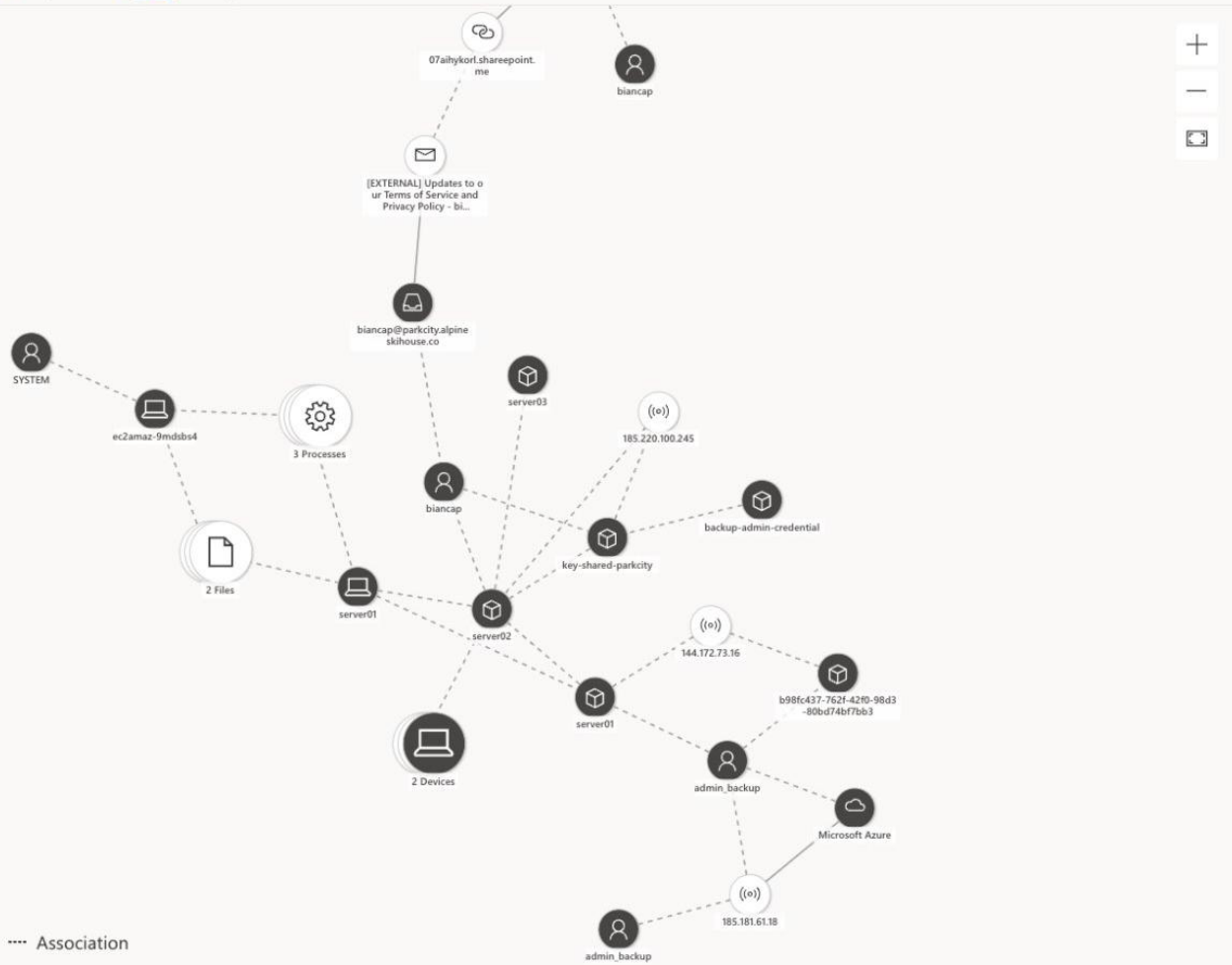
Attack story | Recommended actions (38) | Alerts (10) | Assets (15) | Investigations (2) | Evidence and Response (19) | Summary | Similar incidents

Alerts

0/10 Active alerts | Unpin all | Show all

- Oct 24, 2023 6:47 PM ● Resolved
  Suspicious URL clicked
  parkcity-win11h.parkcity.alpineskihouse.co
  biancap
- Oct 24, 2023 6:50 PM ● Resolved
  A potentially malicious URL click was detected
  Bianca Pisani | Bianca Pisani
- Oct 24, 2023 7:21 PM ● Resolved
  Azure Resource Manager operation from suspicious proxy IP address
  4 Cloud Resources
- Oct 24, 2023 7:21 PM ● Resolved
  Access from a TOR exit node to a key vault
  2 Cloud Resources
- Oct 24, 2023 11:58 PM ● Resolved
  Malicious IP address
  Backup Admin (parkcity)
- Oct 25, 2023 12:03 AM ● Resolved
  Activity from a Tor IP address
  Backup Admin (Parkcity)
- Oct 25, 2023 12:19 AM ● Resolved
  Suspicious elevate access operation (Preview)
  b98fc437-762f-42f0-98d3-80bd74bf7bb3
- Oct 25, 2023 12:24 AM ● Resolved
  Azure Resource Manager operation

Incident graph | Layout | Group similar nodes



Multi-stage incident involving Initial access & Credential access including Ransomware on multiple endpoints reported by multiple sources

High | Resolved

Ransomware | Credential Phish | 20231025 | +1

Manage incident

RECOMMENDATIONS

Phishing Incident response playbook

View phishing investigation and response recommended steps for this incident

Open phishing playbook

RECOMMENDATIONS

Ransomware Incident response playbook

View ransomware investigation and response recommended steps for this incident

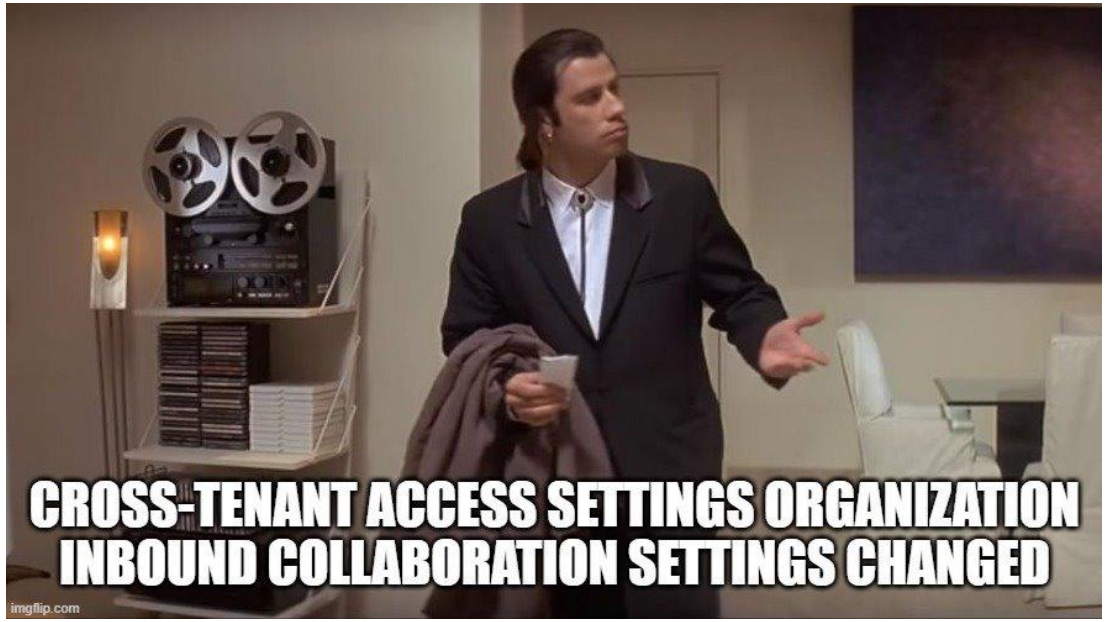
Open ransomware playbook

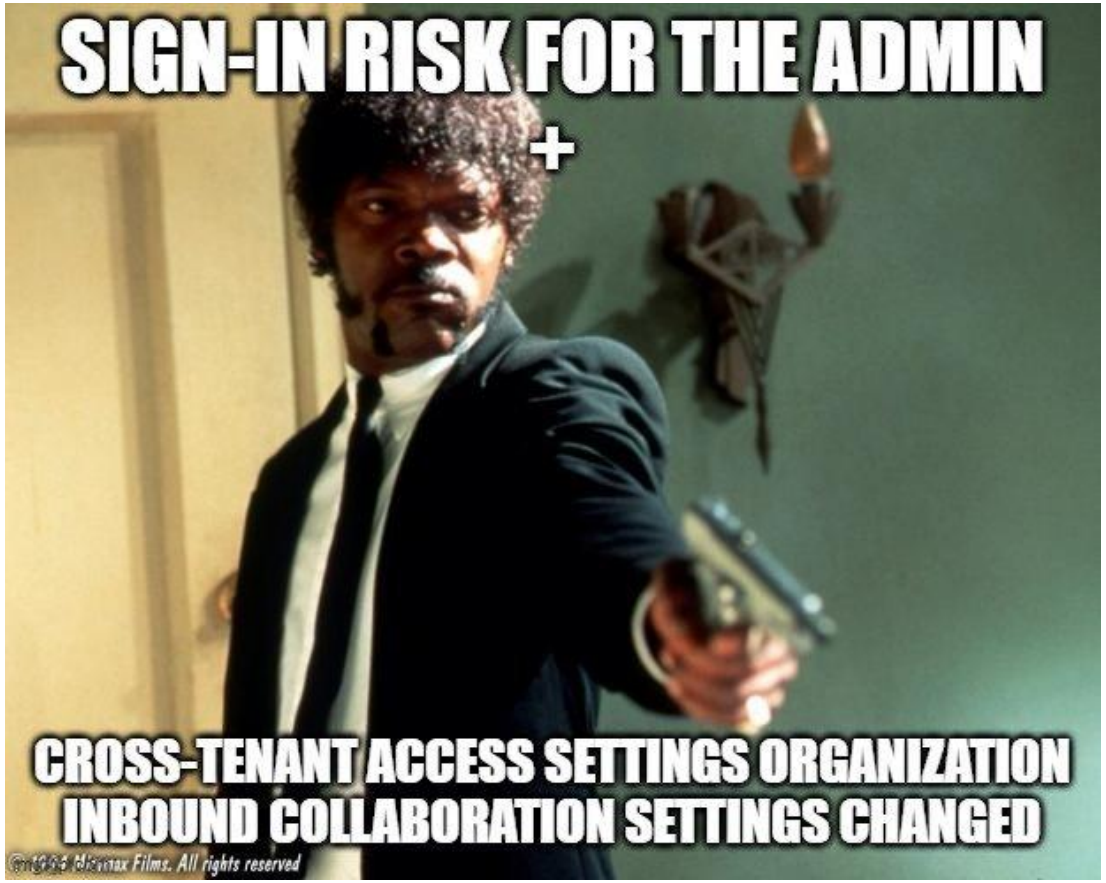
The Mordor of Incidents

Correct entity and MITRE mapping	Pre-requisite for any triage and correlation activity
Behaviors or alert	Downgrade Incidents to Alerts Change Severity to Informational Single alert leads into high-fidelity incidents
Entity enrichment	Evidence or relation to similar/related incidents identify impact (blast radius) or relation to an attack story

Scenario- and context-based alerts and incidents

Scenario- and context-based approach





Integration of custom enrichment

www.wpninjas.eu
#WPNinjaS

Incidents > User account compromise identified from a known attack pattern (attack disruption)

User account compromise identified from a known attack pattern (attack disruption)

High | Active | Unassigned | Attack Disruption | CSOC Notify

Attention! Attack disruption initiated a disable user action on a compromised account. For more details, select the Assets > Users tab or go to the Action center.

Attack story | Alerts (42) | Assets (24) | Investigations (0) | Evidence and Response (17) | Summary

Alerts

Play attack story | Unpin all | Show all

Mar 4, 2025 5:30 AM • New
First access credential added to Application or Service Principal where no credential was present
Thomas Naunheim

Mar 4, 2025 5:30 AM • New
Secret added to high privileged application
Thomas Naun... | EntraOps-Clo...

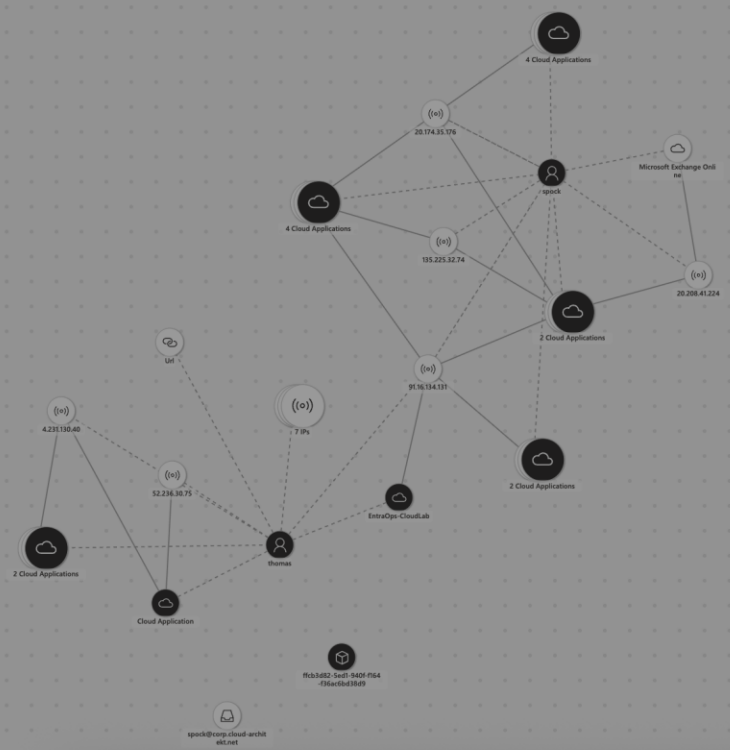
Mar 4, 2025 5:41 AM • New
CloudLab Conditional Access: Add member to group sug_AAD.CA.Exclusion.EmergencyAccessAccounts outside of IG/EM and AADOps
Thomas Naunheim

Mar 4, 2025 5:51 AM • New
Suspicious inbox manipulation rule
Spock | 4 Applications

Mar 4, 2025 5:53 AM • New
CloudLab Conditional Access: Spock has access to Microsoft Account Controls V2 without satisfying any policy
Spock | 2 Applications

Mar 4, 2025 6:03 AM • New

Incident graph | Layout | Group similar nodes



Activity log

Status changed from "Active" to "In Progress"
May 28, 2025 8:02 AM

Incident was assigned
May 28, 2025 8:02 AM

func
May 27, 2025 1:41 PM

GK CSOC

Not all affected file entities are in 'Prevented' stat or entities are classified as "hacktool". This alert must be investigated further.

func
May 27, 2025 1:41 PM

GK CSOC

KQL query *'List which files are not in 'Prevented' state'* returned:

HostName	RemediationState	RemediationDate	FolderP
5xn	Active	5/27/2025 11:22:52 AM	C:\User

Normal | B I U S | Add comment

Save

Build your own Correlation logic

Sources

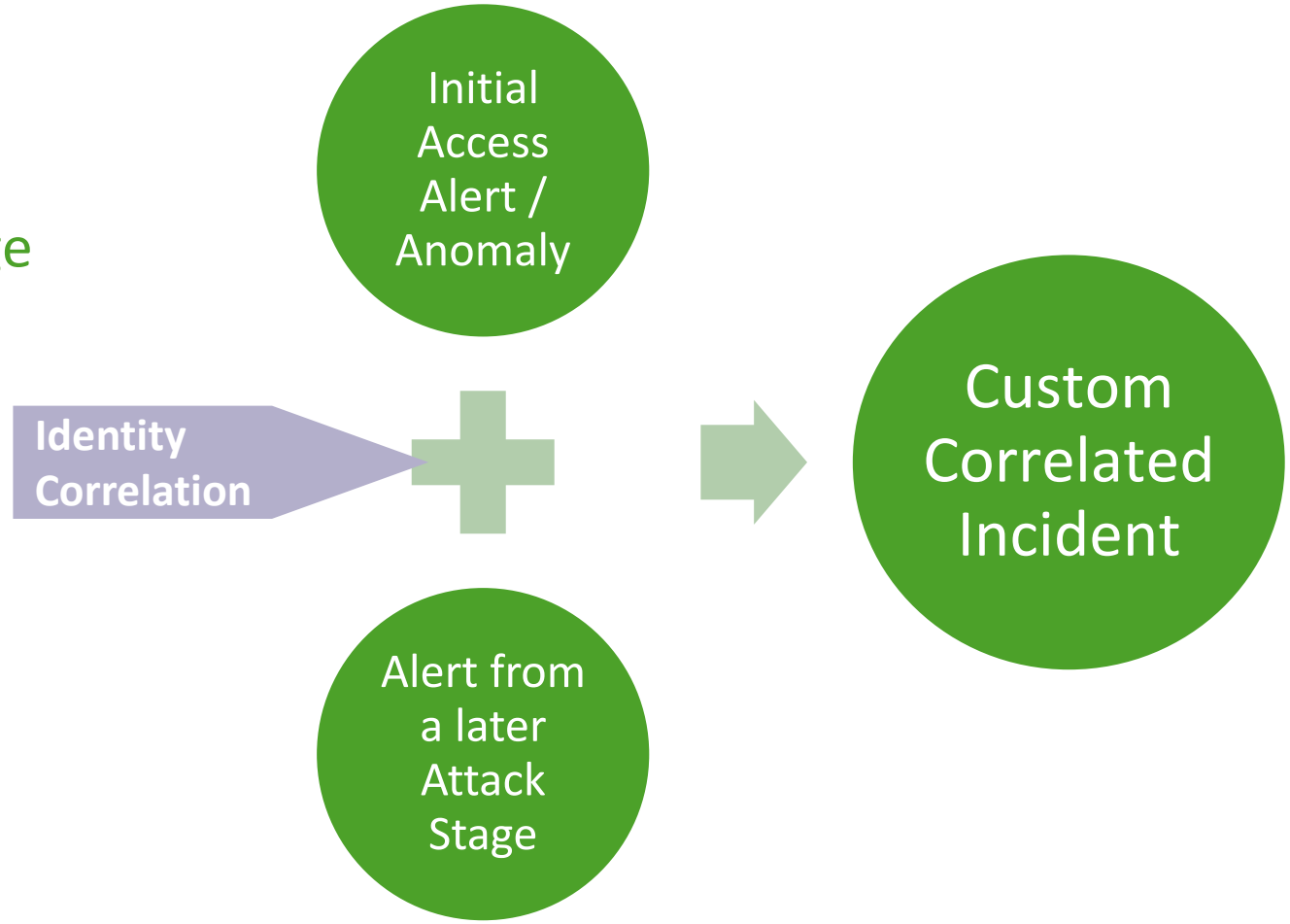
Incidents

- Correlated incidents with high-fidelity alerts which includes scoped attack stage by M&TRE techniques and tactics

ML-based data sources with raw data

- All Identity Protection risks
- BehaviourAnalytics Entry with high InvestigationPriority

Logic



Build your own Correlation logic

www.wpninjas.eu
#WPNinjaS

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot

Home > Microsoft Sentinel | Incidents >

[GK Fusion] Unusual Entra Conditional Access Failures followed by Authentication Method Changed for Privil...

Incident number 21813

Refresh | Delete incident | Logs | Tasks | Activity log

Medium Severity | Closed Status | [redacted] Owner

Workspace name [redacted]

Description
GK: Fusion to correlate enrichment alerts as multi-stage attack or suspicious activity across various MITRE TTPs

Alert product names
- Microsoft Sentinel

Reason for closing [redacted]

Evidence

N/A Events | 1 Alerts | 0 Bookmarks

Last update time
20/08/2025, 16:43:55

Creation time
20/08/2025, 14:04:25

Investigate

Overview | Entities | Incident actions

Incident timeline

Search | Add filter

Aug 20 13:13:27 [GK Fusion] Unusual Entra Conditional ...
Medi... | Detected by Microsoft Se... | Tacti...

Entities

Search | Type : All

[redacted] Account

Similar incidents

No similar incidents to display

Demo: …

Custom function to gather entity details from various sources (UnifiedIdentityInfo)

Detection Engineering Landscape

www.wpninjas.eu
#WPNinjaS

Maturity

Data Sources

- WatchLists and Info tables
- UEBA and Behaviors
- Microsoft Entra Diagnostic Logs
- XDR Advanced Hunting Table
- Entra ID Protection / MDI

Detection Engine

- Analytics Rules
- Custom Detections

Incident Triage and Correlation

- Custom Enrichment Engine
- Custom Correlation Engine
- XDR Correlation Engine

Response Engine

Incident/Response Flow

Detection Engineering Landscape

www.wpninjas.eu
#WPNinjaS

Maturity

Data Sources

- WatchLists and Info tables
- UEBA and Behaviors
- Microsoft Entra Diagnostic Logs
- XDR Advanced Hunting Table
- Entra ID Protection / MDI

Detection Engine

- Analytics Rules
- Custom Detections

Incident Triage and Correlation

- Custom Enrichment Engine
- Custom Correlation Engine
- XDR Correlation Engine

Response Engine

- Custom SOAR Engine
- Sentinel Playbooks
- XDR Automations
- Risk-based CA

Incident/Response Flow

Attack disruption

www.wpninjas.eu
#WPNinjaS

Attack disruption disables the OAuth app preventing further lateral movement

Defender XDR alert:
"Activity from a password-spray associated IP address"

Defender XDR alert:
"User added or updated a suspicious OAuth app"

Microsoft Defender XDR alert:
"Suspicious Microsoft Entra ID app creation"

Microsoft Defender XDR alerts:
"Suspicious inbound connector created that allow unsecured emails from external sender IP addresses",

"New transport rule removing antispam header",

"Suspicious inbound connector and transport rule created to remove sender email headers"

Attacker

2023-06-06 9:45AM — Attacker compromises admin account through password spraying

2023-06-06 10:00AM — Attacker creates an application with known bad redirect URL and high permissions to manage Exchange Online settings

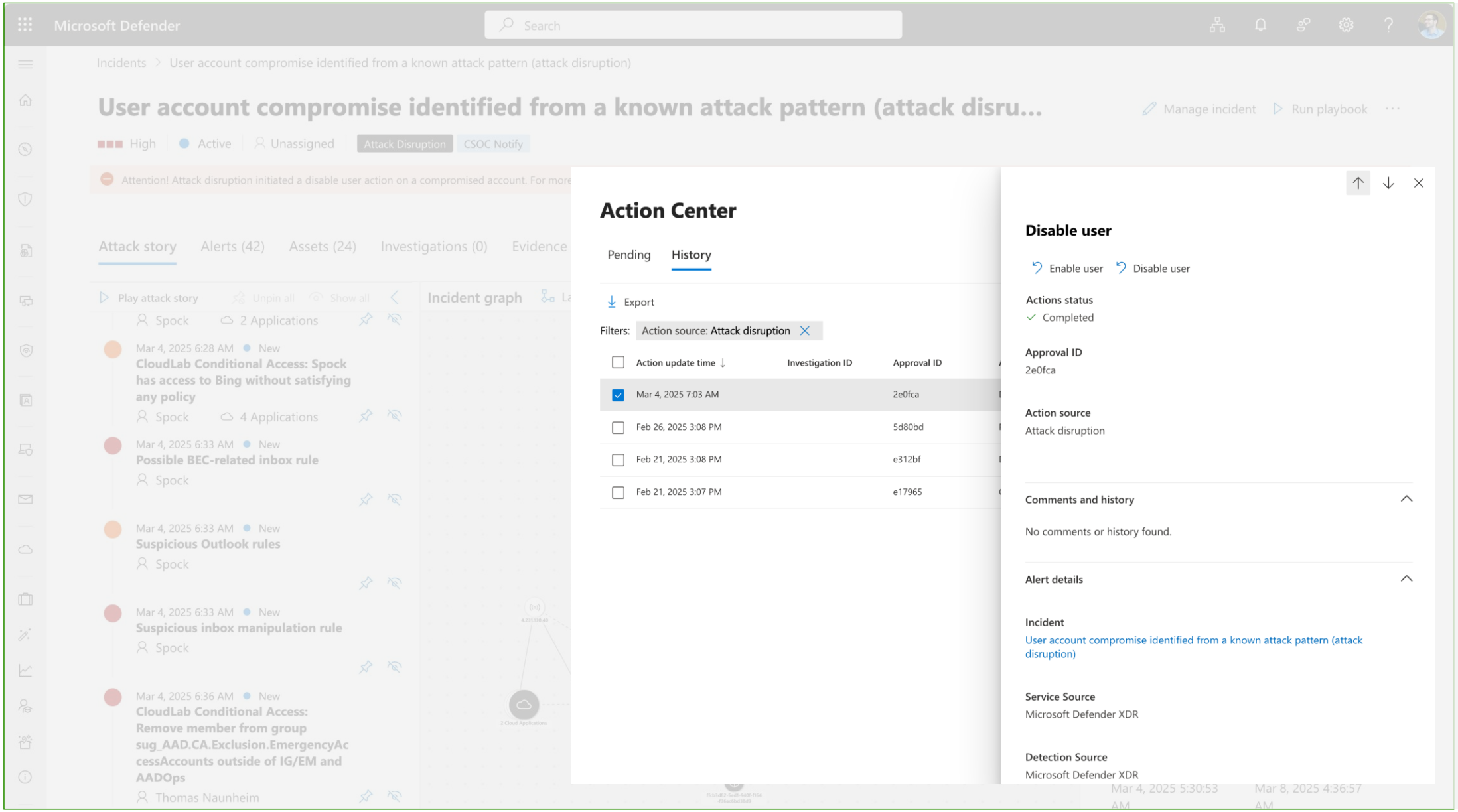
2023-06-06 10:05AM — Attacker assigns global and Exchange admin roles to application

2023-06-07 8:35PM — Attacker then uses this app to create malicious Exchange connectors and transport rules to evade spam filtering and allow spamming in the tenant

2023-06-12 9:35 PM — Attacker begins spamming the tenant

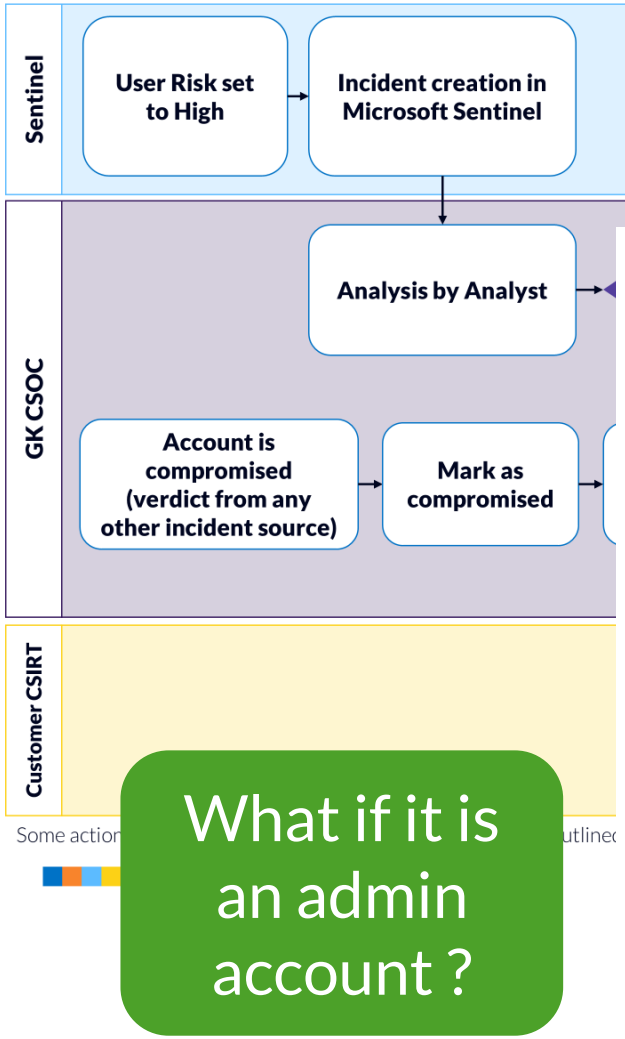
Example of Attack Disruption

www.wpninjas.eu
#WPNinjaS

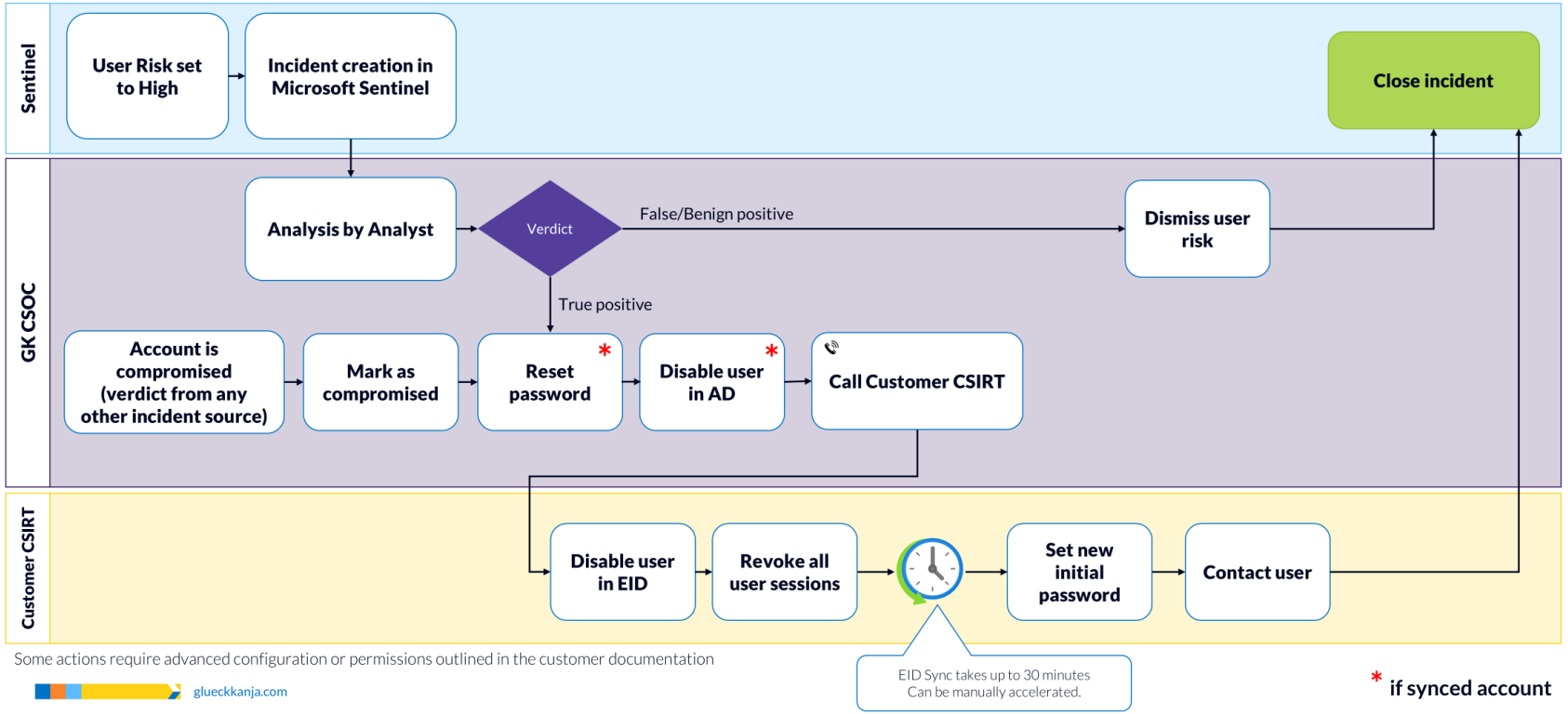


Containment | identity compromise process

www.wpninjas.eu
#WPNinjaS



What if it is an admin account ?



Detection Engineering Landscape

www.wpninjas.eu
#WPNinjaS

Maturity

Data Sources

- WatchLists and Info tables
- UEBA and Behaviors
- Microsoft Entra Diagnostic Logs
- XDR Advanced Hunting Table
- Entra ID Protection / MDI

Detection Engine

- Analytics Rules
- Custom Detections

Incident Triage and Correlation

- Custom Enrichment Engine
- Custom Correlation Engine
- XDR Correlation Engine

Response Engine

- Custom SOAR Engine
- Sentinel Playbooks
- XDR Automations
- Risk-based CA

Incident/Response Flow

www.wpninjas.eu
#WPNinjaS

We love Feedback

https://wpninjas25.sched.com/

Great Session!

Okay Session!

Not so okay Session!

Workplace Ninja Summit 2025

Thank You