Rethinking Security Prioritization in Defender: Ranking Security Risk with Tier-Based Risk Score

Morten Knudsen

Microsoft MVP Azure, Security & Security Copilot | Microsoft Certified Trainer

Cloud & Security Architect, freelance

How many security recommendations do we have per device on average each month?

Environment	Recommendations per device (average) *CVEs (missing patches) | Security configuration issues | Exposure recommendations (Defender Secure Score items)*
Well-managed environment	20-50
Average organization	50-150
Poor patching/legacy systems	150-400+

Example:
1000 devices x 80 recommendations/device -> backlog ~**80000 findings**

Changes each month:
5–15% of recommendations **change monthly** (4–12 per device per month)

For 1000 devices -> **4000 – 12000 items/month to review**

Severity Distribution	Amount per device
Critical	2-5
High	5-15
Medium/Low	Majority noise-heavy

The Challenge

- **Hard to keep** up with security recommendations, vulnerabilities, and configuration findings - many findings marked as High or Critical

- **Traditional vulnerability management** often focuses on CVSS scores or severity classifications – challenge:
  - the same vulnerability is evaluated **equally regardless of the asset**
  - **business impact is not considered**
  - **attack chains and relationships** are not identified

- **Which issues should be addressed first?**

From my experience….!
IT deals with **~10–20%** of total findings

Morten Knudsen

- Microsoft MVP Azure, Security & Security Copilot (triple-MVP)
- Freelance cloud & security architect, 2LINKIT
- Sold my 1st company (MindZet) in 2016 – 75 employees

Co-founder

Experts Live Denmark

Lead-organizer
#ELDK2025, #ELDK26

/in/knudsenmorten

@mortenknudsen.net

@knudsenmortendk

aka.ms/morten

mok@mortenknudsen.net

Understanding the Audience

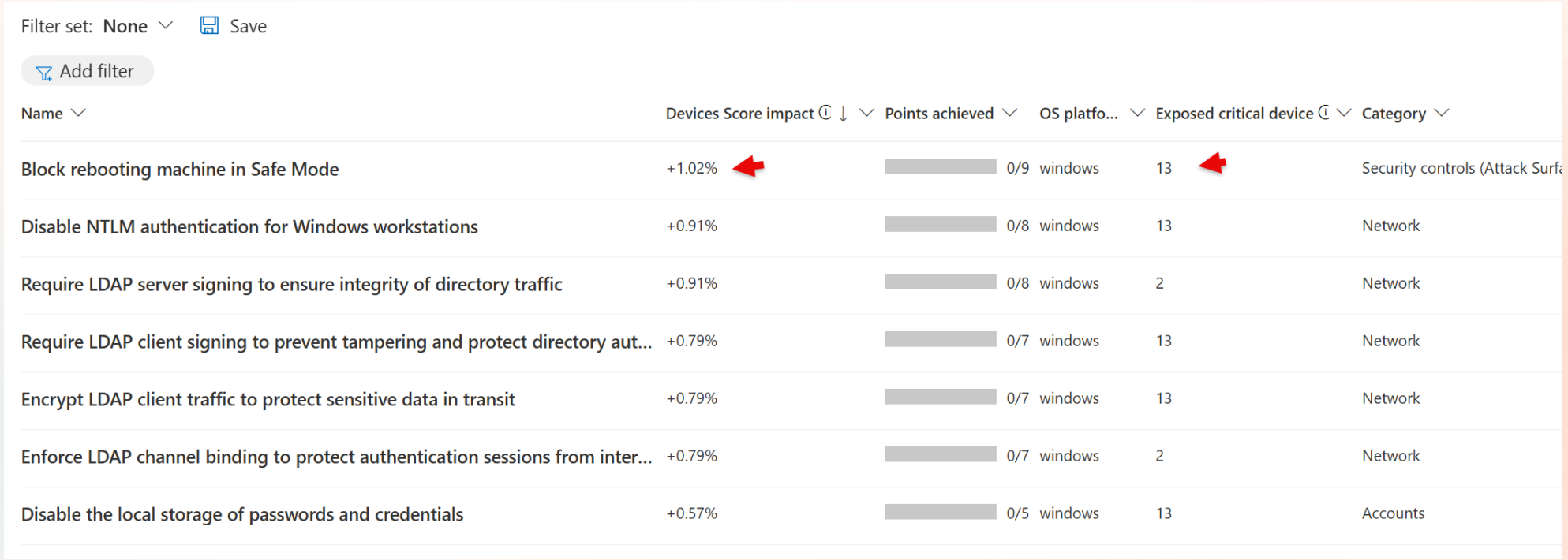
- How many of you work with **implementing** security recommendations every week ?
  - How many of you have a structured approach to prioritize security recommendations, based on business impact ?

- How many of you work with **prioritization** of which recommendations to implement ?
  - How many of you think you are lacking resources to keep up with the many security recommendations ?

Prioritization of Recommendations

Let's be honest: How do we prioritize recommendations today ?

- Sort by Score + Volume ☺
  - Defenders/admins take the easy recommendations first !
  - Often with the highest volume of impacted devices !



Agenda

Seven chapters covering the tier-based risk-scoring model, from theory to implementation.

01

Microsoft Security Posture Management Lifecycle

02

Understanding the Risk-based Prioritization Model

03

Categorizing Security Risks by Severity

04

Classifying Asset Criticality (Endpoint, Identity, Azure)

05

Implementing Asset Criticality Classification

06

Rolling This Out in Your Own Environment

07

Querying ExposureGraph (Appendix)

Goal:
You can test ExposureGraph further

Microsoft Security Posture Management Lifecycle

Free, Community Add-on "SecurityInsight" – Working Closely with Microsoft to improve current thinking

v1 "Secure Score"

- Microsoft Secure Score (M365)
- Azure Secure score (separate solution)
- Recommendations "Consequence"
- No asset prioritization
- Fixed number "overall prevent actions"
- Think as a Defender

v2 "Exposure Management"

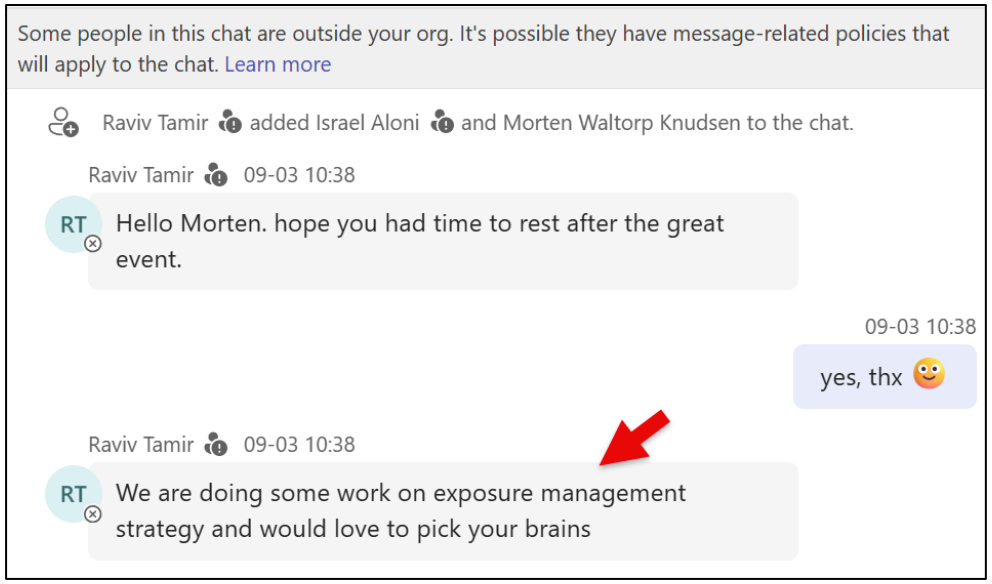
- Initiatives with Individual Scores (Saas, Endpoint, Cloud/Azure, Identity, etc)
- Cloud Secure Score with Risk Factors (preview)
- Attack Paths – "Think as a Hacker"

v2.5 "Risk-based Prioritization"

- Risk Factors in all Recommendations (new)
- Asset criticality w/tagging support incl. exclusions (new)
- Risk Score (new) (Consequence & Probability)
- Compliance & Security frameworks alignments (NIS2, ISO27001, CIS18)
- Better Prioritization (WHAT to focus on, based on Risk Score)
- "API v2" -> ExposureGraph / Azure Resource Graph
- Think as a Hacker & Defender

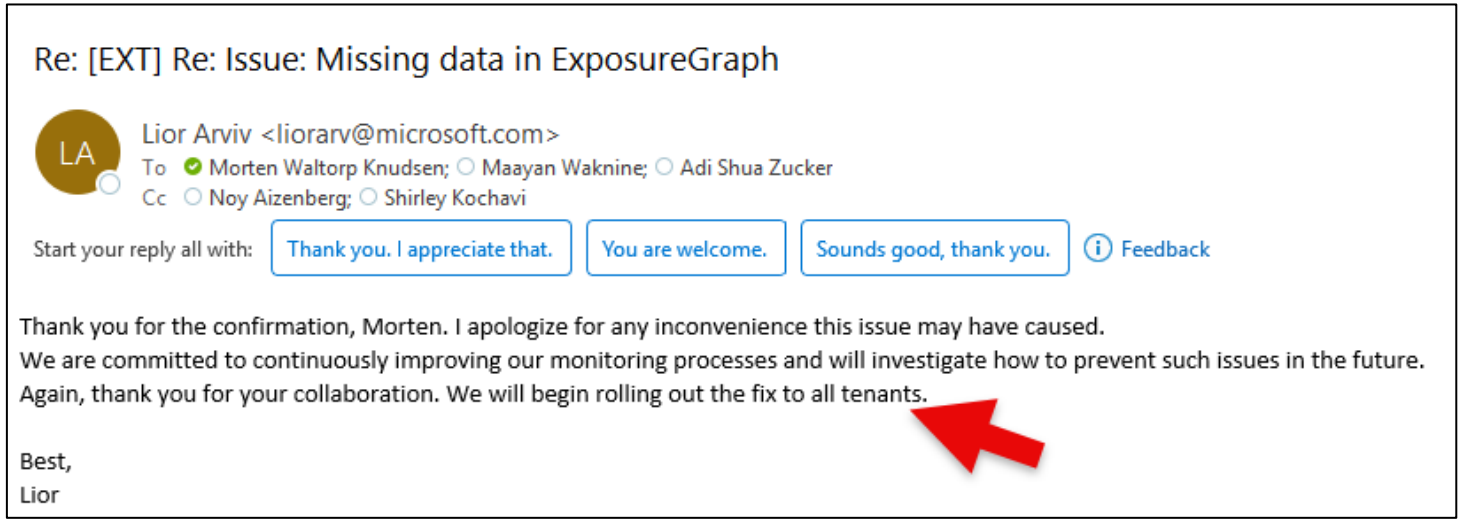
Microsoft Israel (May 2022) | Microsoft Defender Vulnerability Management & Secure Score Principal Group PM

Azure Resource Graph and Azure Resource Management PMs



Microsoft Vice President, Raviv Tamir reaches out to discuss strategy (March 2026)

ExposureGraph PM, Shirley Kochavi, March 2026, Meeting Redmond, USA



I found a critical bug in Graph. Hotfix with node repair deployed to all tenants worldwide (Feb 2026)

Prioritization of Recommendations

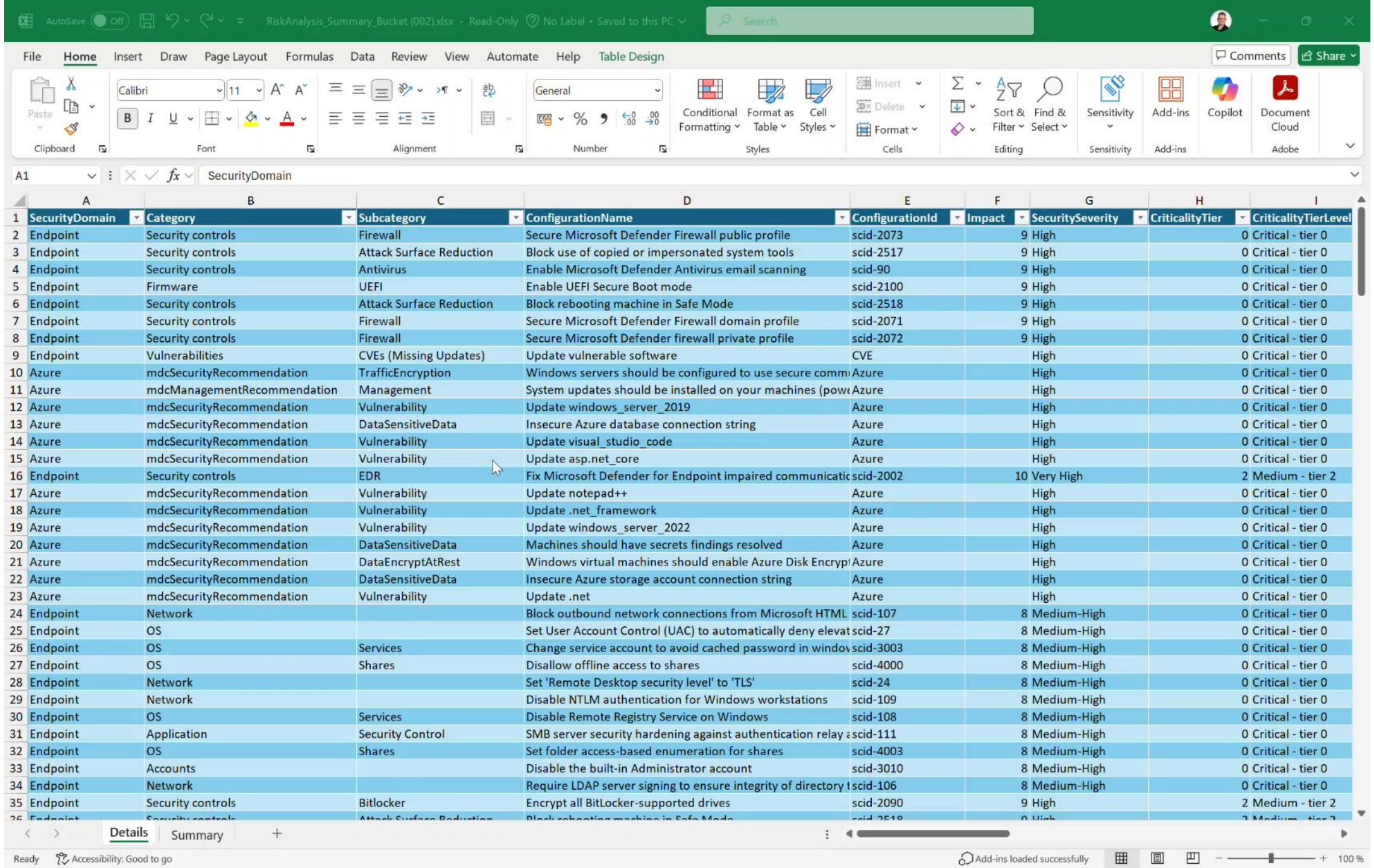
How should we prioritize recommendations instead? (Risk Based approach)

- Goal: **Protect the assets that are most important**
  - DCs, OT env., break-glass accounts, admin devices, service accounts, etc

- **Better prioritization** requires **more dimensions/factors**
  - Severity (Low -> Critical)
  - Asset Criticality (Low -> Critical)
  - Risk Factors:
    - Internet Exposure - Contains Verified Secret - Critical Resource - Lateral Movement - Sensitive Data – LegacyEndOfSupport – ExploitSignals → Vulnerability Exploitkit exist? Yes, choose before others

Demo - Let's see data based on my Risk-based Prioritization model "SecurityInsight"

SecurityDomain	Category	Subcategory	ConfigurationName	ConfigurationId	Impact	SecuritySeverity	CriticalityTier	CriticalityTierLevel	RiskFactor_Consequence	RiskFactor_Probability	RiskFactor_Probability_Detailed	RiskFactor_Probability_DetailedScore	RiskConsequenceScore	RiskProbablityScore	RiskScoreTotal	AssetCount	TotalIssues	ImpactedAssets	CategoryDescription
Endpoint	Security controls	Firewall	Secure Microsoft Defender Firewall domain profile	scid-2071	9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3	3	mgmt1.2linkit.local, dc1.2linkit.local, dc3.2linkit.local	Endpoint protection and attack-surface policies that bloc
Endpoint	Security controls	Firewall	Secure Microsoft Defender firewall private profile	scid-2072	9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3	3	mgmt1.2linkit.local, dc1.2linkit.local, dc3.2linkit.local	Endpoint protection and attack-surface policies that bloc
Endpoint	Security controls	Firewall	Secure Microsoft Defender Firewall public profile	scid-2073	9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3	3	mgmt1.2linkit.local, dc1.2linkit.local, dc3.2linkit.local	Endpoint protection and attack-surface policies that bloc
Endpoint	Security controls	Attack Surface Reduction	Block use of copied or impersonated system tools	scid-2517	9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3	3	mgmt1.2linkit.local, dc1.2linkit.local, dc3.2linkit.local	Endpoint protection and attack-surface policies that bloc
Endpoint	Security controls	Attack Surface Reduction	Block rebooting machine in Safe Mode	scid-2518	9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3	3	mgmt1.2linkit.local, dc1.2linkit.local, dc3.2linkit.local	Endpoint protection and attack-surface policies that bloc
Endpoint	Security controls	Antivirus	Enable Microsoft Defender Antivirus email scanning	scid-90	9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	2	2	mgmt1.2linkit.local, dc3.2linkit.local	Endpoint protection and attack-surface policies that bloc
Endpoint	Security controls	Antivirus	Update Microsoft Defender Antivirus definitions	scid-2011	9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	1	1	dc3.2linkit.local	Endpoint protection and attack-surface policies that bloc
Azure	mdcManagementRecommendation	Management	System updates should be installed on your machines (p	Azure		High	0	Critical - tier 0	0	1	Critical Resource	Critical Resource=1	3	5	15	1	1	dc3.2linkit.local	
Azure	mdcSecurityRecommendation	TrafficEncryption	Windows servers should be configured to use secure cor	Azure		High	0	Critical - tier 0	0	1	Critical Resource	Critical Resource=1	3	5	15	2	2	dc3.2linkit.local, dc1.2linkit.local	
Azure	mdcSecurityRecommer											Critical Resource=1	3	5	15	2	2	mgmt1.2linkit.local, dc3.2linkit.local	
Endpoint	Vulnerabilities											ExploitSignals=0;Internet-Exposed=1;LegacyEndOfSuppo	3	5	15	3	23	mgmt1.2linkit.local, dc3.2linkit.local, dc1.2linkit.local	
Azure	mdcSecurityRecommer											Critical Resource=1;Exposure to the Internet=1	3	4	12	1	1	mgmt1.2linkit.local	
Azure	mdcSecurityRecommer											Critical Resource=1;Exposure to the Internet=1	3	4	12	1	1	mgmt1.2linkit.local	
Azure	mdcSecurityRecommer											Critical Resource=1;Exposure to the Internet=1	3	4	12	1	1	mgmt1.2linkit.local	
Endpoint	Vulnerabilities											ExploitSignals=0;Internet-Exposed=1;LegacyEndOfSuppo	3	4	12	1	30	strv-mok-lt-06	
Azure	mdcSecurityRecommer											Critical Resource=1;Exposure to the Internet=1	3	4	12	3	3	mgmt1.2linkit.local, dc3.2linkit.local, dc1.2linkit.local	
Endpoint	Security controls											Internet-Exposed=1;LegacyEndOfSupport=0	4	3	12	4	4	strv-acw-lt-01, strv-cew-lt-03, heim-new-lt-02, strv-mew	Endpoint protection and attack-surface policies that bloc
Endpoint	Security controls											Internet-Exposed=1;LegacyEndOfSupport=0	3	4	12	1	1	strv-mok-lt-06	Endpoint protection and attack-surface policies that bloc
Endpoint	Network											Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3	3	mgmt1.2linkit.local, dc1.2linkit.local, dc3.2linkit.local	Network security policies that limit attack surface and la
Endpoint	OS											Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3	3	mgmt1.2linkit.local, dc1.2linkit.local, dc3.2linkit.local	Operating system baseline hardening and core protectio
Endpoint	Accounts											Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	1	1	mgmt1.2linkit.local	
Endpoint	Network											Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3	3	mgmt1.2linkit.local, dc1.2linkit.local, dc3.2linkit.local	Network security policies that limit attack surface and la
Endpoint	OS											Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3	3	mgmt1.2linkit.local, dc1.2linkit.local, dc3.2linkit.local	Operating system baseline hardening and core protectio
Endpoint	Network											Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	2	2	dc1.2linkit.local, dc3.2linkit.local	Network security policies that limit attack surface and la
Endpoint	Application											Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	1	1	mgmt1.2linkit.local	Application control and exploit protection to restrict una
Endpoint	OS											Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	1	1	dc1.2linkit.local	Operating system baseline hardening and core protectio
Endpoint	Network											Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3	3	mgmt1.2linkit.local, dc1.2linkit.local, dc3.2linkit.local	Network security policies that limit attack surface and la
Endpoint	Security controls											Internet-Exposed=1;LegacyEndOfSupport=0	3	3	9	13	13	strv-acw-lt-01, strv-cew-lt-03, heim-new-lt-02, strv-mew	Endpoint protection and attack-surface policies that bloc
												Internet-Exposed=1;LegacyEndOfSupport=0	3	3	9	1	1	heim-new-dt-01	Endpoint protection and attack-surface policies that bloc



SecurityDomain	Category	Subcategory	ConfigurationName	ConfigurationId	Impact	SecuritySeverity	CriticalityTier	CriticalityTierLevel
Endpoint	Security controls	Firewall	Secure Microsoft Defender Firewall public profile	scid-2073	9	High	0	Critical - tier 0
Endpoint	Security controls	Attack Surface Reduction	Block use of copied or impersonated system tools	scid-2517	9	High	0	Critical - tier 0
Endpoint	Security controls	Antivirus	Enable Microsoft Defender Antivirus email scanning	scid-90	9	High	0	Critical - tier 0
Endpoint	Firmware	UEFI	Enable UEFI Secure Boot mode	scid-2100	9	High	0	Critical - tier 0
Endpoint	Security controls	Attack Surface Reduction	Block rebooting machine in Safe Mode	scid-2518	9	High	0	Critical - tier 0
Endpoint	Security controls	Firewall	Secure Microsoft Defender Firewall domain profile	scid-2071	9	High	0	Critical - tier 0
Endpoint	Security controls	Firewall	Secure Microsoft Defender firewall private profile	scid-2072	9	High	0	Critical - tier 0
Endpoint	Vulnerabilities	CVEs (Missing Updates)	Update vulnerable software	CVE		High	0	Critical - tier 0
Azure	mdcSecurityRecommendation	TrafficEncryption	Windows servers should be configured to use secure comm	Azure		High	0	Critical - tier 0
Azure	mdcManagementRecommendation	Management	System updates should be installed on your machines (powe	Azure		High	0	Critical - tier 0
Azure	mdcSecurityRecommendation	Vulnerability	Update windows_server_2019	Azure		High	0	Critical - tier 0
Azure	mdcSecurityRecommendation	DataSensitiveData	Insecure Azure database connection string	Azure		High	0	Critical - tier 0
Azure	mdcSecurityRecommendation	Vulnerability	Update visual_studio_code	Azure		High	0	Critical - tier 0
Azure	mdcSecurityRecommendation	Vulnerability	Update asp.net_core	Azure		High	0	Critical - tier 0
Endpoint	Security controls	EDR	Fix Microsoft Defender for Endpoint impaired communicatic	scid-2002	10	Very High	2	Medium - tier 2
Azure	mdcSecurityRecommendation	Vulnerability	Update notepad++	Azure		High	0	Critical - tier 0
Azure	mdcSecurityRecommendation	Vulnerability	Update .net_framework	Azure		High	0	Critical - tier 0
Azure	mdcSecurityRecommendation	Vulnerability	Update windows_server_2022	Azure		High	0	Critical - tier 0
Azure	mdcSecurityRecommendation	DataSensitiveData	Machines should have secrets findings resolved	Azure		High	0	Critical - tier 0
Azure	mdcSecurityRecommendation	DataEncryptAtRest	Windows virtual machines should enable Azure Disk Encrypt	Azure		High	0	Critical - tier 0
Azure	mdcSecurityRecommendation	DataSensitiveData	Insecure Azure storage account connection string	Azure		High	0	Critical - tier 0
Azure	mdcSecurityRecommendation	Vulnerability	Update .net	Azure		High	0	Critical - tier 0
Endpoint	Network		Block outbound network connections from Microsoft HTML	scid-107	8	Medium-High	0	Critical - tier 0
Endpoint	OS		Set User Account Control (UAC) to automatically deny elevat	scid-27	8	Medium-High	0	Critical - tier 0
Endpoint	OS	Services	Change service account to avoid cached password in windov	scid-3003	8	Medium-High	0	Critical - tier 0
Endpoint	OS	Shares	Disallow offline access to shares	scid-4000	8	Medium-High	0	Critical - tier 0
Endpoint	Network		Set 'Remote Desktop security level' to 'TLS'	scid-24	8	Medium-High	0	Critical - tier 0
Endpoint	Network		Disable NTLM authentication for Windows workstations	scid-109	8	Medium-High	0	Critical - tier 0
Endpoint	OS	Services	Disable Remote Registry Service on Windows	scid-108	8	Medium-High	0	Critical - tier 0
Endpoint	Application	Security Control	SMB server security hardening against authentication relay a	scid-111	8	Medium-High	0	Critical - tier 0
Endpoint	OS	Shares	Set folder access-based enumeration for shares	scid-4003	8	Medium-High	0	Critical - tier 0
Endpoint	Accounts		Disable the built-in Administrator account	scid-3010	8	Medium-High	0	Critical - tier 0
Endpoint	Network		Require LDAP server signing to ensure integrity of directory t	scid-106	8	Medium-High	0	Critical - tier 0
Endpoint	Security controls	Bitlocker	Encrypt all BitLocker-supported drives	scid-2090	9	High	2	Medium - tier 2

[EXT] Security Insights | Risk Analysis | RiskAnalysis_Summary_Bucket

Summarize

SA svc-automation@2linkit.net
To Morten Waltorp Knudsen

Reply Reply All Forward

sø 05-04-2026 14:39

Archive Never

This message was sent with High importance.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

RiskAnalysis_Summary_Bucket.xlsx
29 KB

Risk Analysis

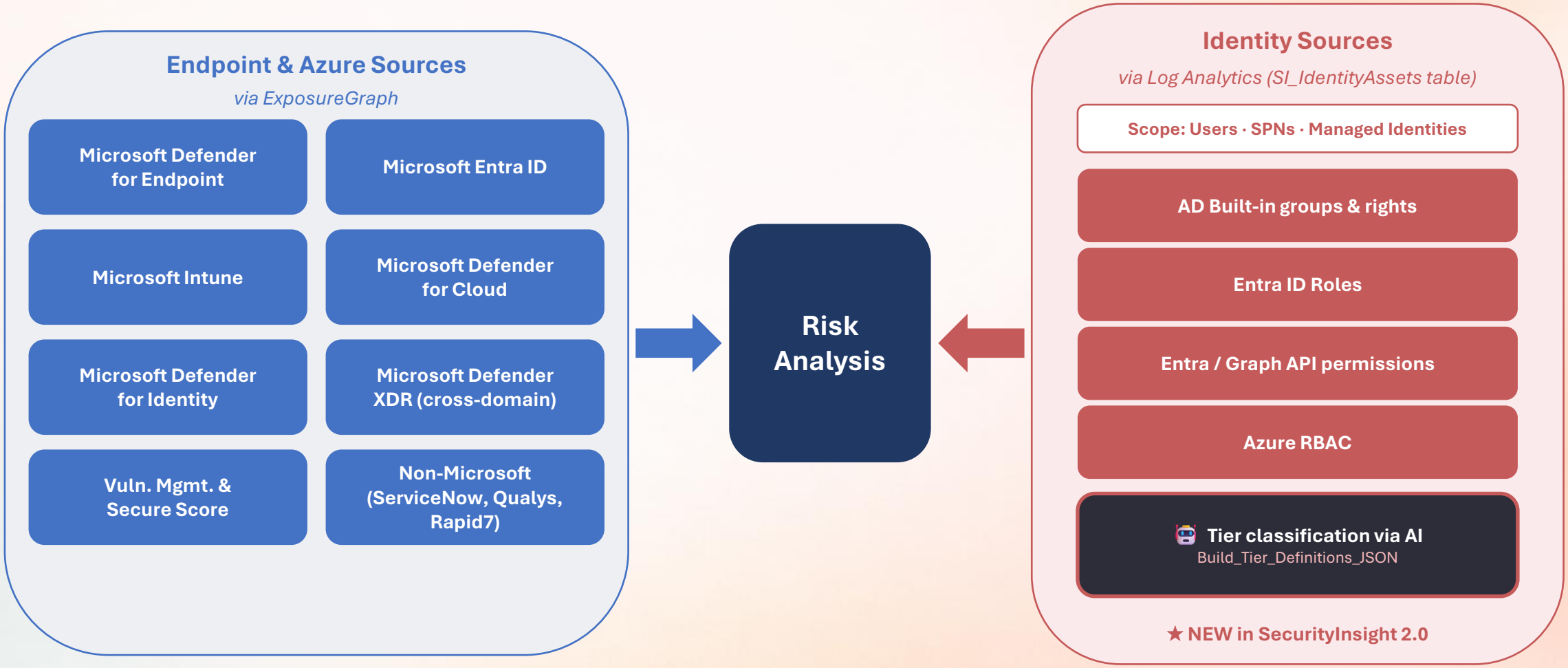
Attached you will find prioritized security risks, ranked by RiskScore.
The Excel file contains full evidence, raw data, and detailed findings per asset (Details sheet).

AI summary (also included in the Excel Summary sheet):

1) Top 25 risky assets:
- 1. mgmt1.2linkit.local | Tier=Critical - tier 0 | MaxRiskScore=15 | RiskScoreTotal=333 | Findings=29 | Domains=Azure, Endpoint
- 2. dc3.2linkit.local | Tier=Critical - tier 0 | MaxRiskScore=15 | RiskScoreTotal=284 | Findings=25 | Domains=Azure, Endpoint
- 3. dc1.2linkit.local | Tier=Critical - tier 0 | MaxRiskScore=15 | RiskScoreTotal=249 | Findings=23 | Domains=Azure, Endpoint
- 4. paw-pxj70zk58z | Tier=Critical - tier 0 | MaxRiskScore=15 | RiskScoreTotal=70 | Findings=8 | Domains=Endpoint
- 5. heim-new-lt-02 | Tier=Medium - tier 2 | MaxRiskScore=12 | RiskScoreTotal=39 | Findings=5 | Domains=Endpoint
- 6. strv-acw-dt-04 | Tier=Medium - tier 2 | MaxRiskScore=12 | RiskScoreTotal=33 | Findings=4 | Domains=Endpoint
- 7. strv-mok-dt-03 | Tier=Medium - tier 2 | MaxRiskScore=9 | RiskScoreTotal=39 | Findings=6 | Domains=Endpoint
- 8. strv-mew-dt-02 | Tier=Medium - tier 2 | MaxRiskScore=9 | RiskScoreTotal=39 | Findings=6 | Domains=Endpoint
- 9. heim-new-dt-01 | Tier=Medium - tier 2 | MaxRiskScore=9 | RiskScoreTotal=36 | Findings=5 | Domains=Endpoint
- 10. strv-cew-lt-03 | Tier=Medium - tier 2 | MaxRiskScore=9 | RiskScoreTotal=33 | Findings=5 | Domains=Endpoint
- 11. dons-ekn-dt-01 | Tier=Medium - tier 2 | MaxRiskScore=9 | RiskScoreTotal=33 | Findings=5 | Domains=Endpoint
- 12. strv-mok-lt-06 | Tier=Medium - tier 2 | MaxRiskScore=9 | RiskScoreTotal=33 | Findings=5 | Domains=Endpoint
- 13. tomsdesktop | Tier=Medium - tier 2 | MaxRiskScore=9 | RiskScoreTotal=33 | Findings=5 | Domains=Endpoint
- 14. usami-tom-lt-01 | Tier=Medium - tier 2 | MaxRiskScore=9 | RiskScoreTotal=27 | Findings=4 | Domains=Endpoint
- 15. strv-mew-lt-02 | Tier=Medium - tier 2 | MaxRiskScore=9 | RiskScoreTotal=27 | Findings=4 | Domains=Endpoint
- 16. dons-ekn-lt-02 | Tier=Medium - tier 2 | MaxRiskScore=9 | RiskScoreTotal=27 | Findings=4 | Domains=Endpoint
- 17. strv-acw-dt-03 | Tier=Medium - tier 2 | MaxRiskScore=9 | RiskScoreTotal=27 | Findings=4 | Domains=Endpoint
- 18. demowin2 | Tier=Low - tier 3 | MaxRiskScore=6 | RiskScoreTotal=12 | Findings=2 | Domains=Azure
- 19. eps-demo-dc1 | Tier=Low - tier 3 | MaxRiskScore=6 | RiskScoreTotal=12 | Findings=2 | Domains=Azure

Sources Feeding Risk Analysis

Endpoint, Azure & Identity



Risk Analysis Queries (126 total)

Area	Count	What's covered
Identity	**104**	MFA gaps, stale/privileged accounts, SPN hygiene, PIM, Break Glass, sign-in anomalies, shadow admins, drift tracking
Endpoints / Devices	**4**	CVE analysis, device recommendations, device vulnerability → lateral movement
Azure	**2**	Azure recommendations (summary + detailed)
Attack Paths	**16**	GitHub→Azure, Public IP→VM, Identity→Privileged Resources, Credential lateral movement, Data sensitivity

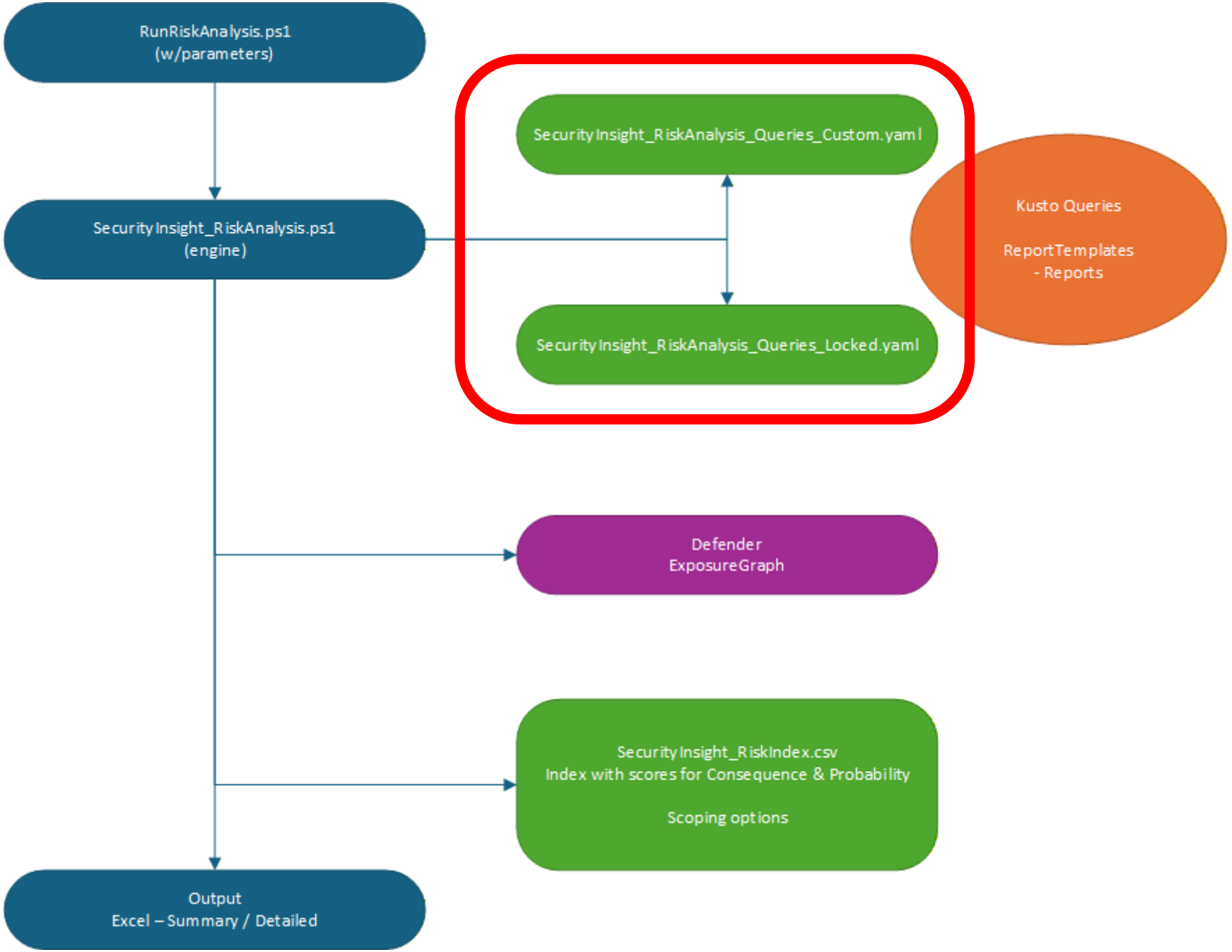
DEMO

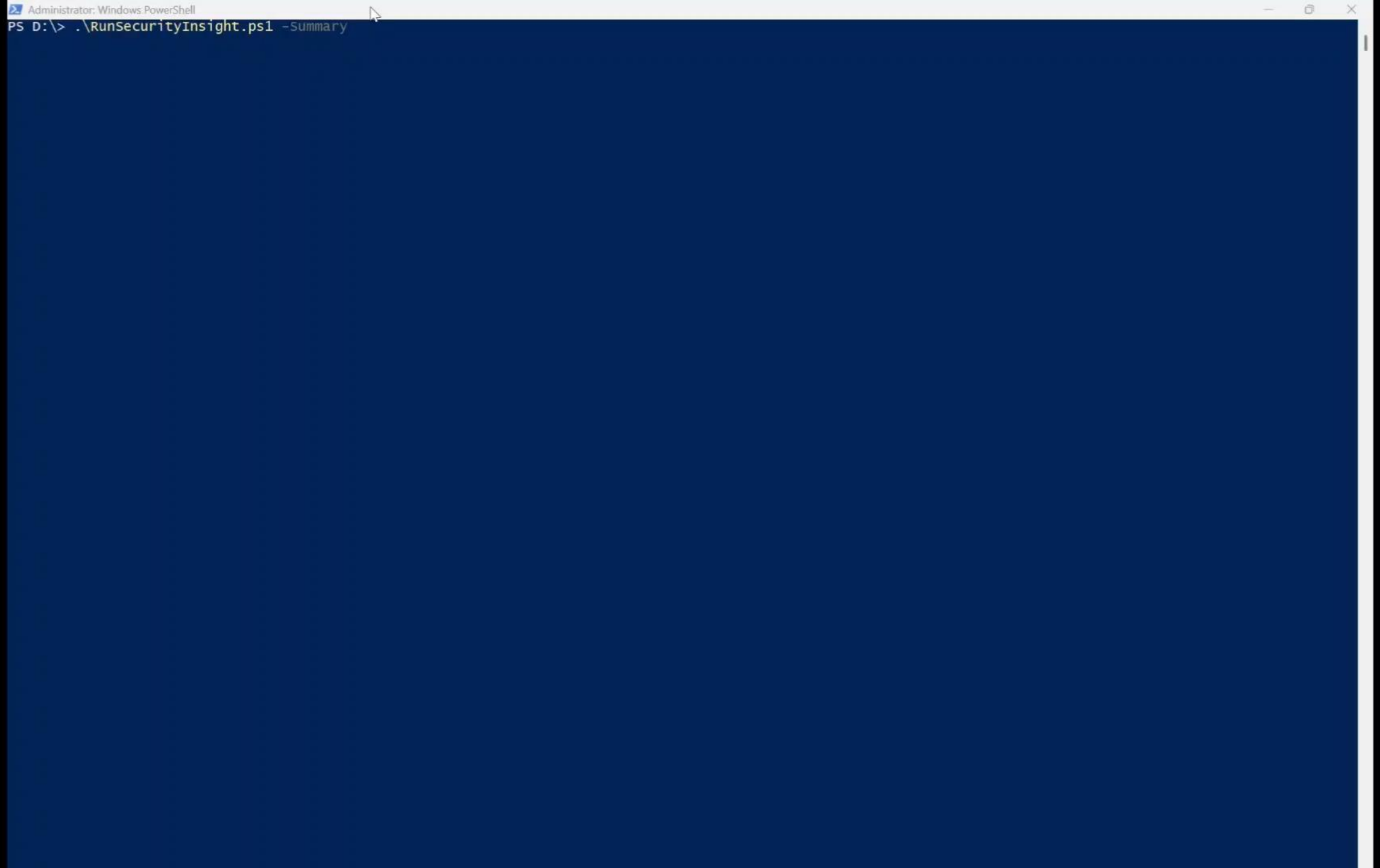
Let’s see query files (YAML)

&

Let’s run the collection

```yaml
Reports:
  - ReportName: Device_Missing_CVEs_Summary_BucketFilter
    ReportPurpose: This report highlights overdue endpoint CVEs older than 40 days, excluding out-of-scope ass
      them using asset criticality, tag-based tiering, and exploit and exposure risk factors to focus remediat
      critical and likely exploitable vulnerabilities.
    SecurityDomain: Endpoint
    CategoryInputName: Category
    SubcategoryInputName: Subcategory
    ConfigurationIdInputName: ConfigurationId
    SecuritySeverityInputName: SecuritySeverity
    CriticalityTierLevelInputName: CriticalityTierLevel
    RiskConsequenceScoreOutputName: RiskConsequenceScore
    RiskProbabilityScoreOutputName: RiskProbablityScore
    RiskScoreOutputName: RiskScoreTotal
    CriticalityTierLevelScope:
    - Critical - tier 0
    - High - tier 1
    - Medium - tier 2
    - Low - tier 3
    SecuritySeverityScope:
    - Very High
    - High
    - Medium-High
    - Medium
    - Low
    OutputPropertyOrder:
    - SecurityDomain
    - Category
    - Subcategory
    - ConfigurationName
    - ConfigurationId
    - Impact
    - SecuritySeverity
    - CriticalityTier
```


RunRiskAnalysis.ps1
(w/parameters)
SecurityInsight_RiskAnalysis.ps1
(engine)
SecurityInsight_RiskAnalysis_Queries_Custom.yaml
SecurityInsight_RiskAnalysis_Queries_Locked.yaml
Kusto Queries
ReportTemplates
- Reports
Defender
ExposureGraph
SecurityInsight_RiskIndex.csv
Index with scores for Consequence & Probability
Scoping options
Output
Excel – Summary / Detailed


Administrator: Windows PowerShell
PS D:\> .\RunSecurityInsight.ps1 -Summary

Download Presentation with all demo’s

https://sharing.mortenknudsen.net/Rethinking-Security-Prioritization-in-Defender-A-Tiered-Risk-Score-Approach-MEM26.pptx

🔢 Understanding the Risk-based Prioritization model

SecuritySeverity (Consequence)

- based on **Impact score in Defender**
- grouped into **Very High, High, Medium-High, Medium, Low**

CriticalityTierLevel (Probability)

- based on **CriticalityLevel in Defender** (if present) – **fallback** to **asset tagging of asset**
- definition is based on **tier-model (Tier-0, Tier-1, Tier-2, Tier-3)**
- grouped into **Critical (tier-0), High (tier-1), Medium (tier-2), Low (tier-3)**

Risk Factors (consequence, probability)

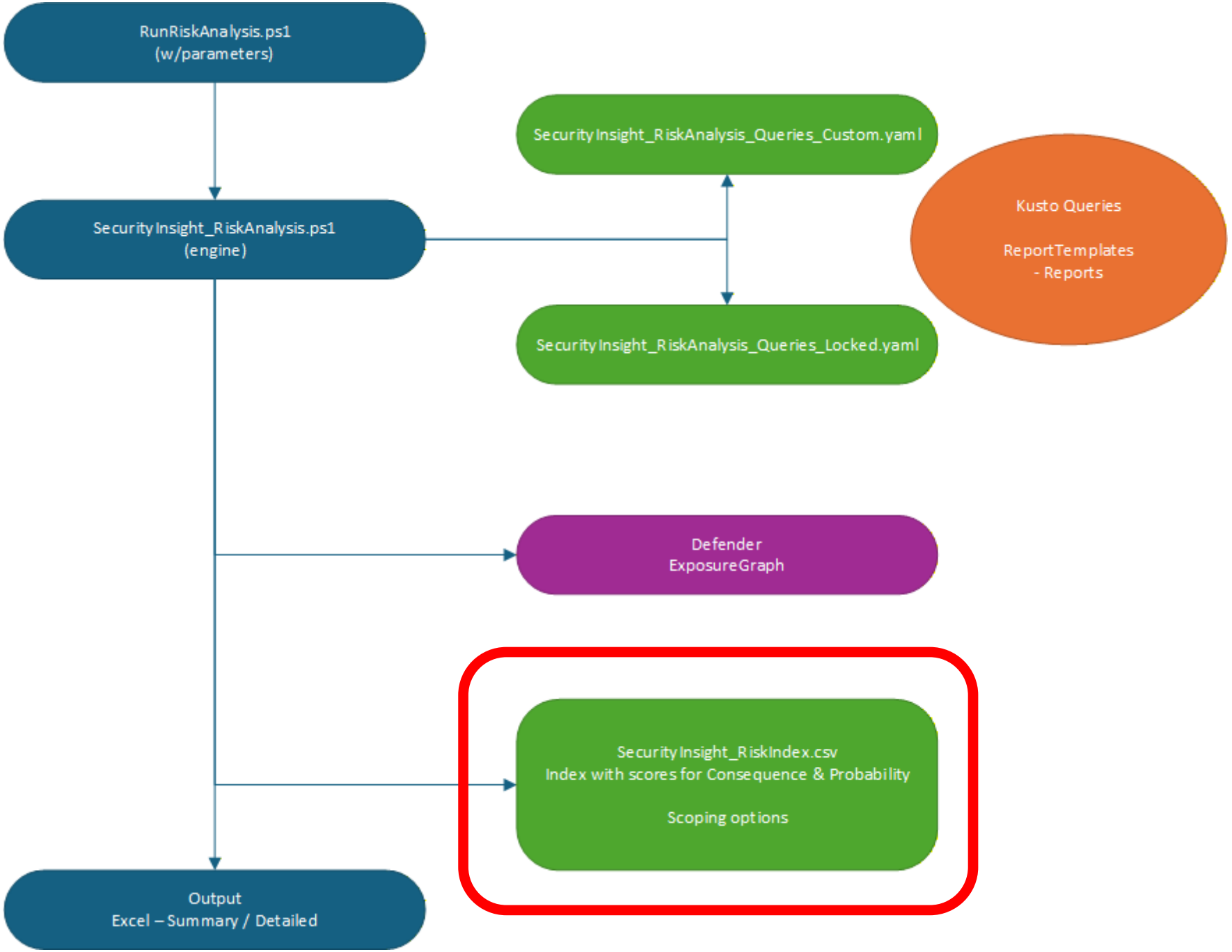
- risk factors could be Internet exposure, Known exploits, Legacy systems
- risk factors increase the score with +1

Risk Index (custom prioritization)

- Scoping on SecurityDomain, Category, SubCategory, ConfigurationId
- Consequence-score (1-5)
- Probability-score (1-5)
- Risk Score

Impact	SecuritySeverity	CriticalityTier	CriticalityTierLevel	RiskFactor_Consequence	RiskFactor_Probability	RiskFactor_Probability_Detailed	RiskFactor_Probability_DetailedScore	RiskConsequenceScore	RiskProbablityScore	RiskScoreTotal	AssetCount
10	Very High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	4	5	20	1
9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	[illegible]	[illegible]	[illegible]	3
9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3
9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3
9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3
9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	4
9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	2
10	Very High	2	Medium - tier 2	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	5	3	15	1
	High	0	Critical - tier 0	0	1	Critical Resource	Critical Resource=1	3	5	15	1
	High	0	Critical - tier 0	0	1	Critical Resource	Critical Resource=1	3	5	15	2
	High	0	Critical - tier 0	0	1	Internet-Exposed	ExploitSignals=0;Internet-Exposed=1;LegacyEndOfSupp	3	5	15	3
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	1
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	1
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	3
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	1
10	Very High	2	Medium - tier 2	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	4	3	12	3
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	4
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	1
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	2
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	2
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	1

	A	B	C	D	E	F	G	H
1	SecurityDomain	Category	Subcategory	AssetName	AssetLabel	ConfigurationName	ConfigurationId	Impact
2	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-59200	CVE	
3	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54099	CVE	
4	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-59278	CVE	
5	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54112	CVE	
6	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-55696	CVE	
7	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-49734	CVE	
8	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-59205	CVE	
9	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54918	CVE	
10	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54110	CVE	
11	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-53801	CVE	
12	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54111	CVE	
13	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54110	CVE	
14	Endpoint	Vulnerabilities	CVEs (Missing Updates)	paw-pxj70zk58z	microsoft.compute/virtualmachines	CVE-2024-12797	CVE	
15	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54918	CVE	
16	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc1.2linkit.local	microsoft.compute/virtualmachines	CVE-2023-40031	CVE	
17	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54894	CVE	
18	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-59254	CVE	
19	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-53801	CVE	
20	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-53154	CVE	
21	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54916	CVE	
22	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-59191	CVE	
23	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-59275	CVE	
24	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2023-31096	CVE	
25	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2024-43590	CVE	
26	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2023-31096	CVE	
27	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54916	CVE	
28	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54895	CVE	
29	Endpoint	Vulnerabilities	CVEs (Missing Updates)	mgmt1.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-53152	CVE	
30	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-54913	CVE	
31	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-59277	CVE	
32	Endpoint	Vulnerabilities	CVEs (Missing Updates)	dc3.2linkit.local	microsoft.compute/virtualmachines	CVE-2025-58714	CVE	
33	Endpoint	Security controls	Attack Surface Reduction	dc3.2linkit.local	microsoft.compute/virtualmachines	Block rebooting machine in Safe Mode	scid-2518	
34	Endpoint	Security controls	Firewall	mgmt1.2linkit.local	microsoft.compute/virtualmachines	Secure Microsoft Defender firewall private profile	scid-2072	
35	Endpoint	Security controls	Firewall	mgmt1.2linkit.local	microsoft.compute/virtualmachines	Secure Microsoft Defender Firewall public profile	scid-2073	
36	Endpoint	Security controls	Antivirus	mgmt1.2linkit.local	microsoft.compute/virtualmachines	Enable Microsoft Defender Antivirus email scanning	scid-90	
37	Azure	mdcManagementRecommendation	Management	dc3.2linkit.local	microsoft.compute/virtualmachines	System updates should be installed on your machines (powe	Azure	
38	Endpoint	Security controls	Antivirus	dc3.2linkit.local	microsoft.compute/virtualmachines	Enable Microsoft Defender Antivirus email scanning	scid-90	
39	Azure	mdcSecurityRecommendation	DataEncryptAtRest	dc1.2linkit.local	microsoft.compute/virtualmachines	Windows virtual machines should enable Azure Disk Encrypt	Azure	


RunRiskAnalysis.ps1
(w/parameters)
SecurityInsight_RiskAnalysis.ps1
(engine)
SecurityInsight_RiskAnalysis_Queries_Custom.yaml
SecurityInsight_RiskAnalysis_Queries_Locked.yaml
Kusto Queries
ReportTemplates
- Reports
Defender
ExposureGraph
SecurityInsight_RiskIndex.csv
Index with scores for Consequence & Probability
Scoping options
Output
Excel – Summary / Detailed

	A	B	C	D	E	F	G	H	I
1	SecurityDomain	Category	SubCategory	ConfigurationId	SecuritySeverity	RiskConsequenceScore_SecuritySeverity	CriticalityTierLevel	RiskProbablityScore_CriticialityTierLevel	Comments
2					Very High	4	Critical - tier 0	4	
3					Very High	4	High - tier 1	3	
4					Very High	4	Medium - tier 2	2	
5					Very High	4	Low - tier 3	1	
6					High	3	Critical - tier 0	4	
7					High	3	High - tier 1	3	
8					High	3	Medium - tier 2	2	
9					High	3	Low - tier 3	1	
10					Medium-High	2	Critical - tier 0	4	
11					Medium-High	2	High - tier 1	3	
12					Medium-High	2	Medium - tier 2	2	
13					Medium-High	2	Low - tier 3	1	
14					Medium	1	Low - tier 3	1	
15					Medium	1	Low - tier 3	1	
16					Medium	1	Low - tier 3	1	
17					Medium	1	Low - tier 3	1	
18					Low	1	Critical - tier 0	4	
19					Low	1	High - tier 1	3	
20					Low	1	Medium - tier 2	2	
21					Low	1	Low - tier 3	1	
22	Endpoint				Very High	4	Critical - tier 0	4	
23	Endpoint				Very High	4	High - tier 1	3	
24	Endpoint				Very High	4	Medium - tier 2	2	
25	Endpoint				Very High	4	Low - tier 3	1	
26	Endpoint				High	3	Critical - tier 0	4	
27	Endpoint				High	3	High - tier 1	3	
28	Endpoint				High	3	Medium - tier 2	2	
29	Endpoint				High	3	Low - tier 3	1	
30	Endpoint				Medium-High	2	Critical - tier 0	4	
31	Endpoint				Medium-High	2	High - tier 1	3	
32	Endpoint				Medium-High	2	Medium - tier 2	2	
33	Endpoint				Medium-High	2	Low - tier 3	1	
34	Endpoint				Medium	1	Low - tier 3	1	
35	Endpoint				Medium	1	Low - tier 3	1	

How we categorize a Security Recommendation into Severity?

Consequence Classifications

Severity Prioritization | Risk Score Definitions

Defender Score	Risk Impact	Attack Impact
10	Very High	**Absence of this control gives attackers an immediate and decisive advantage.** Either a critical attack path is left fully exposed, or a single exploitation leads directly to full environment compromise with no further steps required.
9	High	This control addresses **weaknesses that are actively weaponized in the wild by ransomware operators, credential theft campaigns, and advanced persistent threat actors**. Exploitation is well-documented, tooling is widely available, and remediation should be treated as urgent.
8	Medium-High	This control is a **foundational hardening measure that meaningfully shrinks the attack surface and disrupts common lateral movement techniques** While not immediately catastrophic if missing, its absence creates conditions that attackers routinely chain together to escalate privileges or move laterally.
5-7	Medium	This control reflects **established security best practice and reduces exposure to known attack patterns**. Exploitation is possible but less consistent, typically requiring specific environmental conditions or attacker patience. Prioritize after higher-severity items are addressed.
1-4	Low	This control contributes to **security hygiene and long-term posture improvement**. Missing controls in this range are unlikely to be directly targeted but may marginally increase the cost or noise for an attacker operating in the environment.

SecuritySeverity
(Consequence)

- based on **Impact score in Defender**
- grouped into **Very High, High, Medium-High, Medium, Low**

Impact	SecuritySeverity	CriticalityTie	CriticalityTierLevel	RiskFactor_Consequence	RiskFactor_Probability	RiskFactor_Probability_Detailed	RiskFactor_Probability_DetailedScore	RiskConsequenceScore	RiskProbablityScore	RiskScoreTotal	AssetCount
10	Very High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	4	5	20	1
9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	[illegible]	[illegible]	[illegible]	3
9	High	0	Critical - tier 0	0	[illegible]	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3
9	High	0	Critical - tier 0	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3
9	High	0	Critical - tier 0	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3
9	High	0	Critical - tier 0	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	4
9	High	0	Critical - tier 0	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	2
10	Very High	2	Medium - tier 2	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	5	3	15	1
	High	0	Critical - tier 0	0	1	Critical Resource	Critical Resource=1	3	5	15	1
	High	0	Critical - tier 0	0	1	Critical Resource	Critical Resource=1	3	5	15	2
	High	0	Critical - tier 0	0	1	nternet-Exposed	ExploitSignals=0;Internet-Exposed=1;LegacyEndOfSuppo	3	5	15	3
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	1
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	1
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	3
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	1
10	Very High	2	Medium - tier 2	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	4	3	12	3
8	Medium-High	0	Critical - tier 0	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	4
8	Medium-High	0	Critical - tier 0	0	[illegible]	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	1
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	2
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	2
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	1

How we classify Criticality for Assets like Endpoint / Device | Identity | Cloud (Azure)?

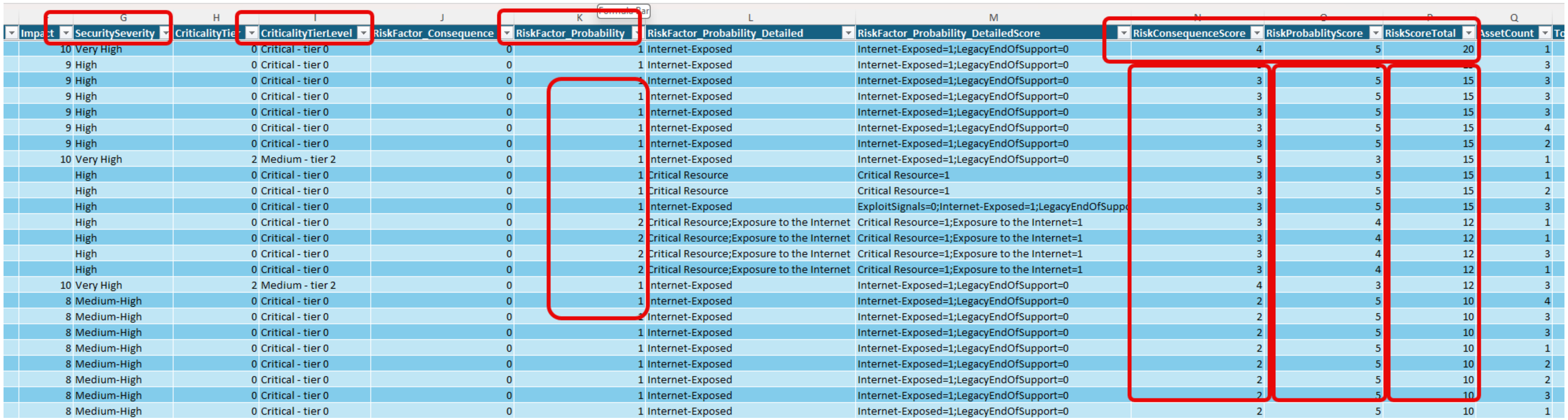
Probability (Likelihood) Classifications

Criticality Prioritization | Risk Score Definitions

Criticality Level	Attack Impact	Defender Terms
Critical (Tier-0)	**Immediate full environment compromise if taken** Compromise of a Domain Controller, krbtgt account, or Global Administrator yields unrestricted control over every identity, credential, and resource in the environment. An attacker can forge Kerberos tickets, replicate the entire AD database, assign any Entra role, and persist indefinitely without detection. Recovery requires full forest rebuild.	**Portal:** Very High - tier 0 **API:** 0
High (Tier-1)	**High impact, one or two pivots to full compromise** Compromise of an Exchange server, Authentication Administrator, or jump server provides credential material, token abuse opportunities, or lateral movement paths that lead to tier 0 within one or two steps. An attacker can reset MFA, intercept authentication flows, abuse unconstrained delegation, or exploit ADCS misconfigurations to escalate without direct access to tier 0 assets.	**Portal:** High - tier 1 **API:** 1
Medium (Tier-2)	**Significant workload impact, conditional path to escalation** Compromise of a file server, developer workstation, or SharePoint environment enables mass data exfiltration, credential harvesting from application configs, and abuse of scoped service accounts. Escalation to tier 0 is possible but requires chaining multiple weaknesses such as finding reused credentials, misconfigured delegation, or an over-permissioned service principal.	**Portal:** Medium - tier 2 **API:** 2
Low (Tier-3)	**Low blast radius, limited lateral movement potential** Compromise of a standard employee workstation, guest PC, or read-only service account yields limited immediate value. An attacker gains a foothold for phishing, internal reconnaissance, or credential capture via keylogging, but cannot directly access sensitive systems or escalate without exploiting additional misconfigurations elsewhere in the environment.	**Portal:** Low - tier 3 **API:** 3

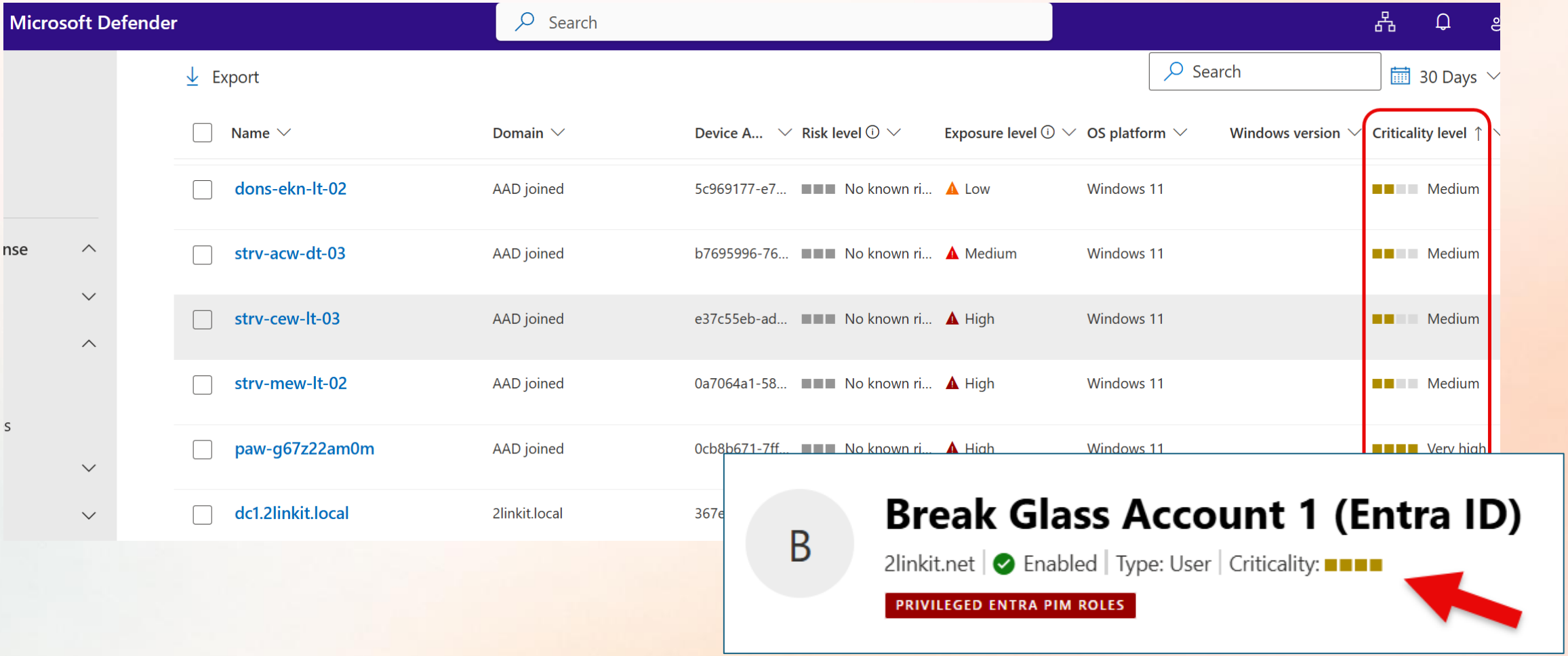
CriticalityTierLevel (Probability)

- based on **CriticalityLevel in Defender** (if present) – **fallback** to **asset tagging of asset**
- definition is based on **tier-model (Tier-0, Tier-1, Tier-2, Tier-3)**
- grouped into **Critical (tier-0), High (tier-1), Medium (tier-2), Low (tier-3)**



Impact	SecuritySeverity	CriticalityTie	CriticalityTierLevel	RiskFactor_Consequence	RiskFactor_Probability	RiskFactor_Probability_Detailed	RiskFactor_Probability_DetailedScore	RiskConsequenceScore	RiskProbablityScore	RiskScoreTotal	AssetCount
10	Very High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	4	5	20	1
9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	[illegible]	[illegible]	[illegible]	3
9	High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3
9	High	0	Critical - tier 0	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3
9	High	0	Critical - tier 0	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	3
9	High	0	Critical - tier 0	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	4
9	High	0	Critical - tier 0	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	3	5	15	2
10	Very High	2	Medium - tier 2	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	5	3	15	1
	High	0	Critical - tier 0	0	1	Critical Resource	Critical Resource=1	3	5	15	1
	High	0	Critical - tier 0	0	1	Critical Resource	Critical Resource=1	3	5	15	2
	High	0	Critical - tier 0	0	1	nternet-Exposed	ExploitSignals=0;Internet-Exposed=1;LegacyEndOfSupp	3	5	15	3
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	1
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	1
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	3
	High	0	Critical - tier 0	0	2	Critical Resource;Exposure to the Internet	Critical Resource=1;Exposure to the Internet=1	3	4	12	1
10	Very High	2	Medium - tier 2	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	4	3	12	3
8	Medium-High	0	Critical - tier 0	0	1	nternet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	4
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	1
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	2
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	2
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	3
8	Medium-High	0	Critical - tier 0	0	1	Internet-Exposed	Internet-Exposed=1;LegacyEndOfSupport=0	2	5	10	1

Criticality Examples

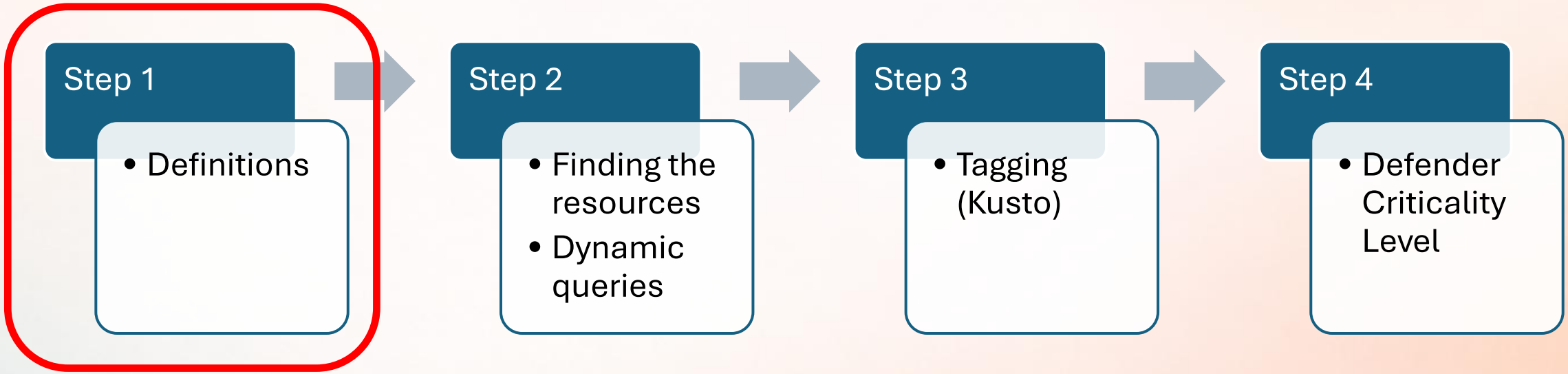


Implementing Asset Criticality Classification

Endpoint, Azure & Identity

Asset Criticality Classifications

Implementation Steps – Endpoint, Azure & Identity



Disclaimer: The asset criticality classifications and attacker-centric tiering presented here are based on my own professional judgment and experience working with identity, endpoint, and cloud security environments. Actual tier assignments may vary depending on each organization's specific architecture, hybrid connectivity model, existing compensating controls, risk tolerance, regulatory requirements, and operational priorities. Classifications should be used as a strategic prioritization framework, not as a definitive or exhaustive measure of asset risk.

Identity Asset Criticality Classification – Tier-0

Criticality Level	Typical Assets		
Critical (tier-0) *Immediate full environment compromise if taken*	Cloud - Entra ID Roles: * Global Administrator accounts * Privileged Authentication Administrator * Privileged Role Administrator * Directory Synchronization Service Accounts * Break-glass Emergency Access Accounts * Directory Writers Azure: * Privileged Credential Vault Root Access	Cloud - Entra ID Services: * Conditional Access and Identity Governance core policies AD: * Domain Admins * Enterprise Admins * Schema Admins	AD (continued): * Administrators (Built-in) * Key Admins / Crypto Admins * Cert Publishers * Group Policy Creator Owners * Incoming Forest Trust Builders * Protected Users Group * Privileged Kerberos delegation accounts

Identity Asset Criticality Classification – Tier-1 (Part 1)

Criticality Level	Typical Assets		
High (tier-1) *Fast-Track Takeover (Abusable Privileges)*	**Cloud – Entra ID Roles:** * Authentication Administrator * Hybrid Identity Administrator * Exchange Administrator * Application Administrator * Cloud App Administrator * Security Administrator * Intune Administrator * Identity Governance Administrator * Helpdesk Administrator (targeting admins) * Password Administrator (targeting admins) * Azure DevOps Administrator * Windows 365 Administrator	**Application Permissions (Graph/API):** * Application.ReadWrite.All * Mail.ReadWrite (app, all users) * User.ReadWrite.All * Group.ReadWrite.All * Sites.FullControl.All * DeviceManagement*.ReadWrite.All * Policy.ReadWrite.ConditionalAccess * Policy.ReadWrite.PermissionGrant * EntitlementManagement.ReadWrite.All * UserAuthenticationMethod.ReadWrite.All * AccessReview.ReadWrite.All * Organization.ReadWrite.All	**Azure Built-in Roles:** * Owner (sub or RG) * User Access Admin (sub scope) * Key Vault Administrator * AKS Cluster Admin * VM Contributor * Automation Account Contributor * Logic App Contributor **Azure Permissions:** * Contributor on Key Vault (access policy model) * Storage Account Contributor * Azure Arc onboarding rights * Defender for Cloud admin * IMDS token theft via VM access

Identity Asset Criticality Classification – Tier-1 (Part 2)

Criticality Level	Typical Assets		
High (tier-1) *Fast-Track Takeover (Abusable Privileges)*	**AD Built-in Groups:** * Account Operators * Backup Operators * Server Operators * Print Operators **AD Permissions:** * GPO edit rights on Tier-0 OUs * AdminSDHolder write access * msDS-KeyCredentialLink write * WriteOwner / WriteDACL on domain root * GenericAll on Tier-0 groups * AllExtendedRights on domain root * ForceChangePassword on admin accounts	**AD Permissions (continued):** * Manage CA (AD CS) * Certificate enrollment agents * ESC1–ESC8 vulnerable cert templates * SeBackupPrivilege / SeRestorePrivilege * SeTakeOwnershipPrivilege * SeDebugPrivilege / SeImpersonatePrivilege on DC * Unconstrained delegation accounts * Shadow Credentials write on admin accounts * SID History injection rights * GPO link rights on Tier-0 OUs	**Accounts:** * Entra Connect service account * Service principals with T0 Graph permissions * Admin-consented OAuth apps (T1 perms) * AD CS enrollment agent accounts * SAs with unconstrained delegation * Accounts with GenericAll on Tier-0 objects * Federated identity credentials on high-priv apps * Managed identities as Owner / UAA at sub scope * Azure Automation Run-As accounts * Service principals with secrets in shared Key Vaults

Identity Asset Criticality Classification – Tier-2

Criticality Level	Typical Assets		
Medium (tier-2) *Conditional Takeover (Needs Chaining / Misconfig)*	**Cloud – Entra ID Roles:** * User Administrator * Groups Administrator * Conditional Access Administrator * SharePoint Administrator * Teams Administrator * Lifecycle Workflows Administrator **Application Permissions (Graph/API):** * Mail.Read (app, all users) * Calendars.ReadWrite * Files.ReadWrite.All * AuditLog.Read.All * IdentityRiskyUser.ReadWrite.All * DeviceManagementConfiguration.ReadWrite.All	**Azure Built-in Roles:** * Network Contributor * Log Analytics Contributor * Automation Operator * Azure DevOps stakeholder * AKS Cluster User **Azure Permissions:** * Contributor on single non-sensitive RG * Storage Blob Data Reader (scoped) * Log Analytics Reader / Monitoring Reader * Security Reader (Defender for Cloud) * Managed Identity on low-privilege workload * Service principal scoped to single RG	**AD Built-in Groups:** * DNS Admins **AD Permissions:** * OU-scoped write ACLs * LAPS read rights * Constrained delegation (msDS-AllowedToDelegateTo) * RBCD write rights * Kerberoastable high-privilege SAs **Accounts:** * SPs scoped to a single workload * Admin-consented OAuth apps with scoped perms * Automation accounts with limited RBAC * ADO service connections to single subscription

Identity Asset Criticality Classification – Tier-3

Criticality Level	Typical Assets		
Low (tier-3) *Low Blast Radius, Limited Lateral Movement*	**Cloud – Entra ID Roles:** * Global Reader * Security Reader * Reports Reader * Message Center Reader * Usage Summary Reports Reader * Directory Readers * Guest User (default) **Application Permissions (Graph/API):** * User.Read (delegated) * Mail.Read (delegated, self) * Calendars.Read (delegated) * Directory.Read.All * AuditLog.Read.All (delegated) * IdentityRiskEvent.Read.All	**Azure Built-in Roles:** * Reader (sub or RG) * Billing Reader * Cost Management Reader * Tag Contributor * Azure DevOps Basic user (no pipeline access) **Azure Permissions:** * Storage Blob Data Reader (scoped, non-sensitive) * Managed Identity with Reader only * Service principal with Reader on isolated RG	**AD Built-in Groups:** * Domain Users (default) * Read-only DC (RODC) **AD Permissions:** * Scoped helpdesk OU read * GenericRead on non-priv objects **Accounts:** * Standard user accounts * Guest accounts * Read-only service accounts * Managed identities with no RBAC assignments * Expired or disabled service principals

Endpoint Asset Criticality Classification – Tier-0

Criticality Level	Typical Assets		
Critical (Tier-0)	**Core Identity Infrastructure:** * Domain Controllers (primary & RODC) * AD Certificate Services (root & subordinate CA) * Entra Connect / AD Connect servers * Federation servers (AD FS primary) * HSM-attached servers (root CA keys)	**Privileged Management:** * PAWs used by Tier-0 admins * Backup servers with DC / CA data * Monitoring servers with domain agents * KMS with domain credential store * vCenter / SCVMM managing Tier-0 hypervisors * Hypervisor hosts running Tier-0 VMs	**Network & OT:** * Core routers (BGP / MPLS backbone) * Core switches spanning all VLANs * Firewall clusters (perimeter & segmentation) * Out-of-band mgmt (iDRAC, iLO, IPMI) * SD-WAN controllers, load balancers * BMS / physical security w/ domain integration

Endpoint Asset Criticality Classification – Tier-1

Criticality Level	Typical Assets		
High (Tier-1)	**Servers & Services:** * Exchange servers * MFA / RADIUS servers * PKI subordinate CA servers * DNS servers (non-DC hosted) * AD FS proxy servers	**Privileged Management:** * PAWs used by Tier-1 admins * Jump servers / bastion hosts * SIEM & EDR management servers * SCCM / MECM primary site servers * HashiCorp Vault, Azure Key Vault (private endpoints) * WSUS / patch mgmt, PIM approval servers * Azure Arc-connected servers with high-priv MI	**Network & Client:** * NAC servers, VPN concentrators * Wireless LAN controllers * Proxy servers (SSL inspection) * RADIUS / TACACS+ authentication servers * Citrix ADC / F5 BIG-IP remote access * IT staff workstations (helpdesk, sysadmin, SOC analyst) * SCADA / ICS servers (non-Tier-0 adjacent)

Endpoint Asset Criticality Classification – Tier-2

Criticality Level	Typical Assets		
Medium (Tier-2)	**Servers & Applications:** * File servers * SharePoint servers * SQL servers (sensitive databases) * Citrix / RDS session hosts * Web apps with Entra-integrated auth * API gateway servers * Teams on-prem / Skype for Business	**Mgmt & Business Systems:** * HR & identity lifecycle servers * Internal certificate RA servers * ITSM servers (ServiceNow, Jira) * Log aggregation servers * DevOps / CI-CD build agents * Kubernetes worker nodes * Hypervisor hosts running Tier-2 VMs	**Network:** * Access-layer switches (user VLANs) * Managed wireless access points * Network monitoring appliances (read-only) * Standalone DHCP servers (non-domain) * Content filtering / web proxy appliances

Endpoint Asset Criticality Classification – Tier-3

Criticality Level	Typical Assets		
Low (Tier-3)	**Client Devices** • Standard user workstations • Standard user laptops • BYOD devices (unmanaged) • Shared / kiosk devices (low-privilege)	**Lab / Test / Dev** • Test and lab machines • Isolated / air-gapped workstations • Training / classroom PCs • Non-production VM hosts (isolated)	**Network / Peripherals / IoT** • Guest network devices • Network-attached printers (no domain integration) • IoT sensors without domain integration • Consumer-grade Wi-Fi APs (guest) • Digital signage endpoints

Cloud (Azure) Asset Criticality Classification – Tier-0

Criticality Level	Typical Assets		
Critical (Tier-0) *Total cloud takeover*	**Azure Built-in Roles (Root / Tenant)** • Owner — root management group • User Access Administrator — root MG • Owner — tenant root subscription • Contributor + blueprint assign (root MG) • Managed Identity Contributor (root scope)	**Identity & Control Plane** • Global Administrator (Entra ID) • Privileged Role Administrator • Hybrid Identity Administrator • Partner / GDAP Delegated Admin • Break-glass emergency access accounts • Service principals — Directory.ReadWrite.All • Service principals — RoleManagement.ReadWrite.Directory	**Critical Azure Resources** • Key Vaults storing Tier-0 private keys / HSM • Azure AD Connect sync VMs • AD FS / Federation servers in Azure • Root management groups • Lighthouse delegations to external tenants • Cross-tenant access policies (admin) • Confidential VMs running AD DS (Tier-0)

Cloud (Azure) Asset Criticality Classification – Tier-1

Criticality Level	Typical Assets		
High (Tier-1) *Fast-track escalation*	**Azure Built-in Roles (Subscription)** • Owner — workload subscription • User Access Administrator — subscription • Key Vault Administrator (non-root) • AKS Cluster Admin • VM Contributor / Automation Contributor • Logic App Contributor • Storage Account Contributor (Entra-integrated)	**Workload Identities & Permissions** • Managed Identities — Owner at subscription • Managed Identity Operator (on high-priv MIs) • Service principals with client secrets in Key Vault • Azure DevOps project admin with T1 service connection • Azure Arc onboarding (Connected Machine Agent) • Application.ReadWrite.All (Graph app permission) • Policy.ReadWrite.ConditionalAccess	**Critical Azure Resources** • Production Key Vaults (non-root keys) • Azure Automation accounts • Shared image galleries / custom images • Private DNS zones • Azure Firewall / Application Gateway • Sentinel / SIEM workspaces • PIM approval workflow infrastructure

Cloud (Azure) Asset Criticality Classification – Tier-2

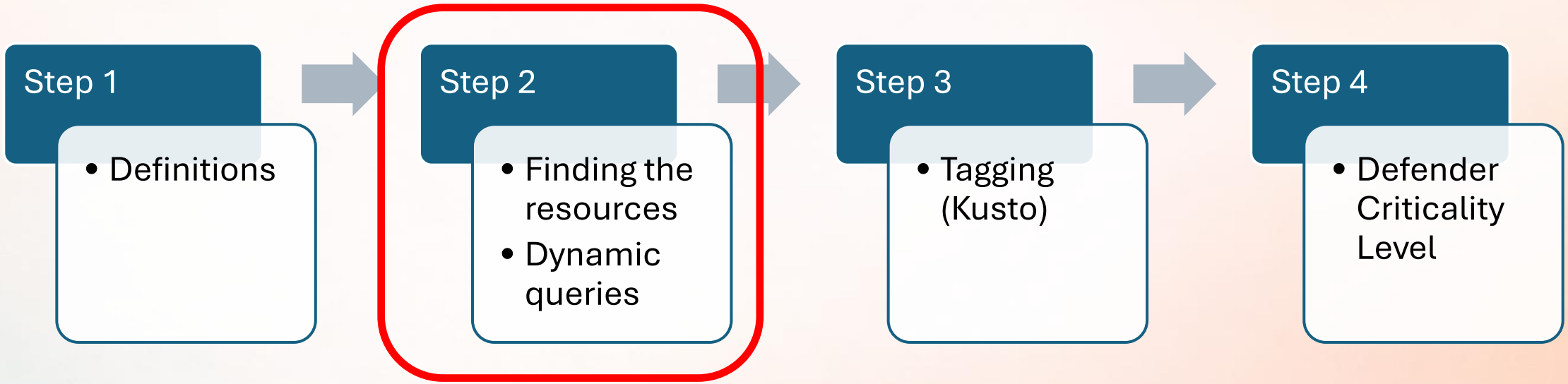
Criticality Level	Typical Assets		
Medium (Tier-2) *Workload impact, conditional escalation*	**Azure Built-in Roles (Workload Scope)** • Contributor — single resource group • Network Contributor • Log Analytics Contributor • Monitor Reader • Security Reader (Defender for Cloud) • AKS Cluster User • Automation Operator	**Workload Identities & Permissions** • Managed identities scoped to workload • Service principals scoped to single RG • Azure DevOps service connections (scoped) • Storage Blob Data Reader (non-sensitive) • Storage Blob Data Contributor (non-sensitive) • OAuth apps with scoped permissions	**Workload Azure Resources** • Application resource groups • Non-production Key Vaults • Workload storage accounts • App Service plans / Web Apps • Non-critical SQL databases • Log Analytics workspaces (workload) • AKS workload clusters

Cloud (Azure) Asset Criticality Classification – Tier-3

Criticality Level	Typical Assets		
Low (Tier-3) *Low blast radius, limited lateral movement*	**Azure Built-in Roles (Read / Isolated)** • Reader — subscription or resource group • Billing Reader • Cost Management Reader • Tag Contributor • Azure DevOps Basic user (no pipeline)	**Low-Privilege Identities** • Managed identities with Reader only • Service principals with Reader on isolated RG • Expired or disabled service principals • Guest users (default scope) • OAuth apps — delegated self-scope (User.Read, Mail.Read)	**Isolated Azure Resources** • Dev / test resource groups • Sandbox subscriptions • Demo storage accounts • Storage Blob Data Reader (isolated, non-sensitive) • Decommissioned workload RGs • Evaluation / PoC environments

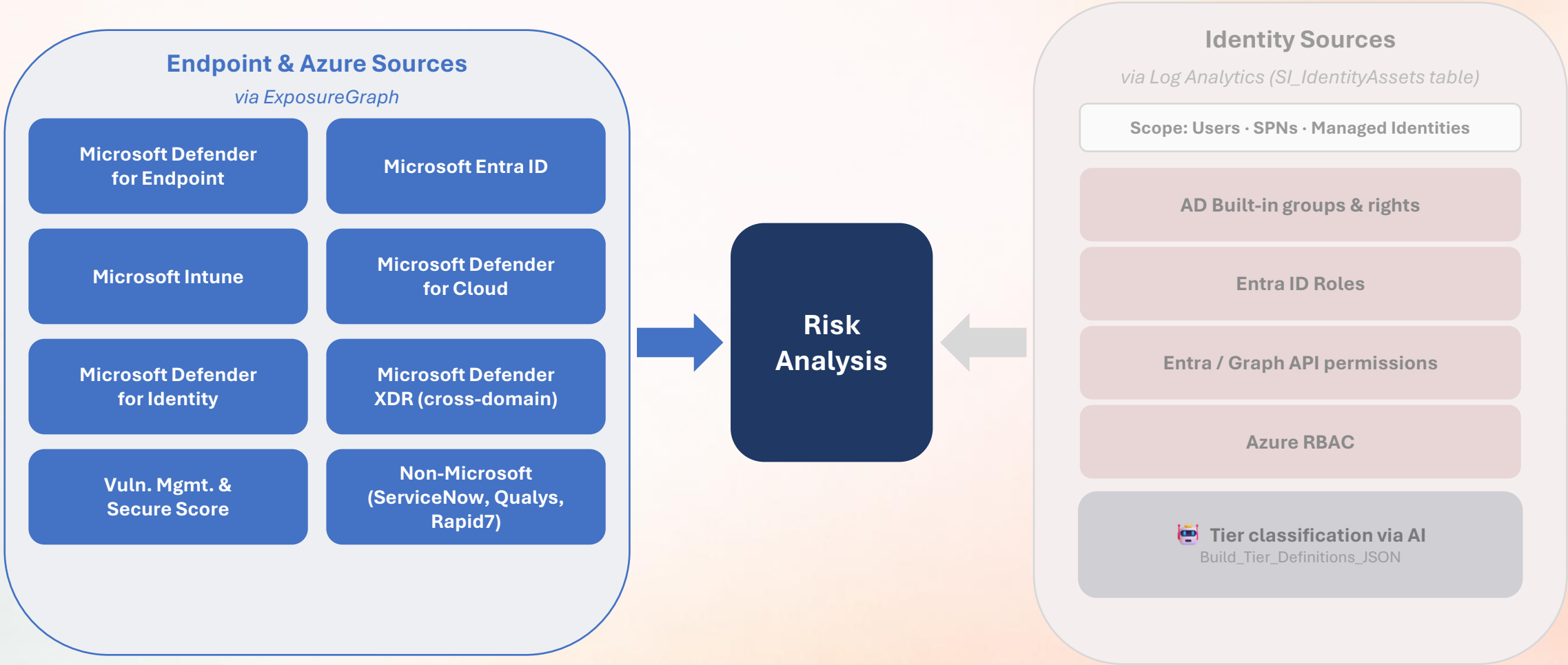
Asset Criticality Classifications

Implementation Steps – Endpoint & Azure



Sources Feeding Risk Analysis

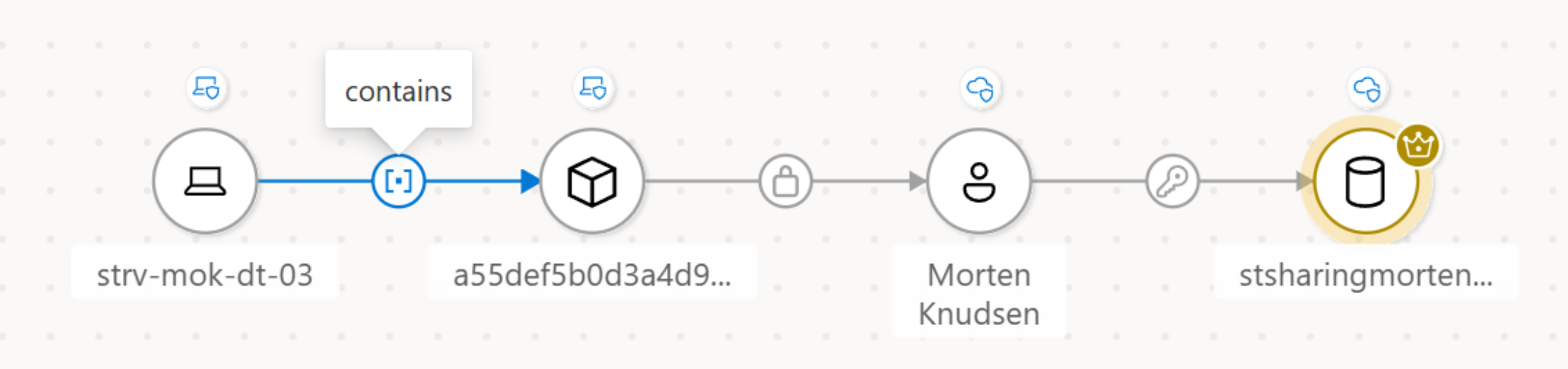
Endpoint & Azure via ExposureGraph



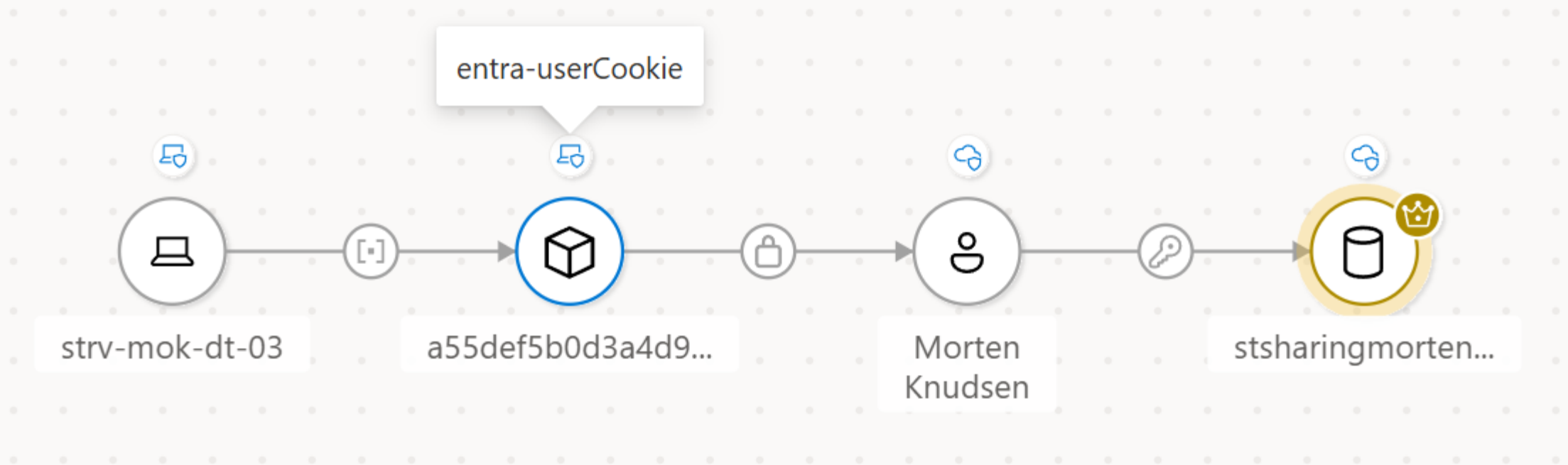
Why Graph is Better than APIs!

- **Defenders** thinks in **Lists (APIs)**
  - "What vulnerabilities exist?"
- **Attackers** thinks in **Graphs**
  - "Which vulnerabilities could actually lead to a critical system being compromised?"
  - Find a way to elevate as admin and take ownership
- Why Graph is better than APIs ?
  - Hunting challenge -> Humans cannot correlate all the lists and keep up with all relationships
- A **graph model** allows security platforms to:
  - **Map relationships between assets**
  - **Identify possible attack paths**
  - **Detect lateral movement opportunities**
  - **Prioritize exposures that could lead to high-impact compromise**

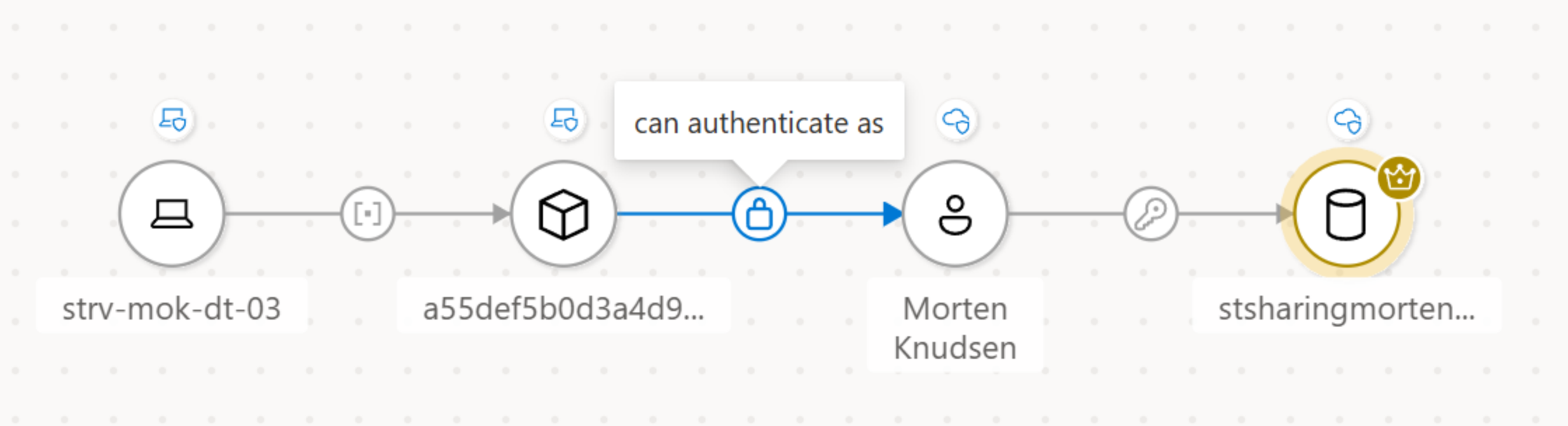
Example of Attack Path



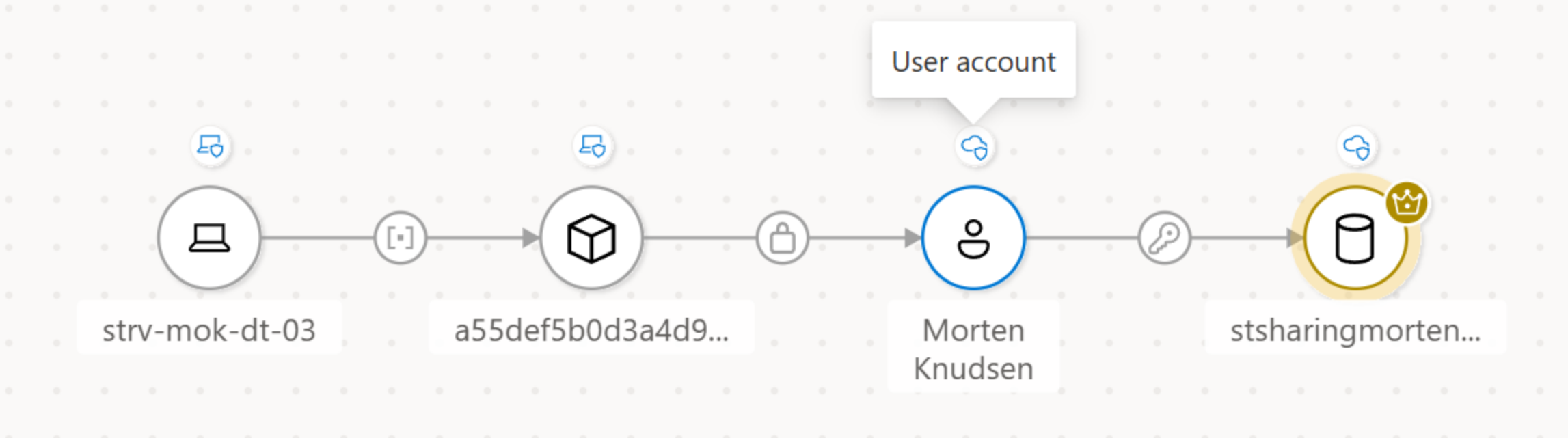
Example of Attack Path



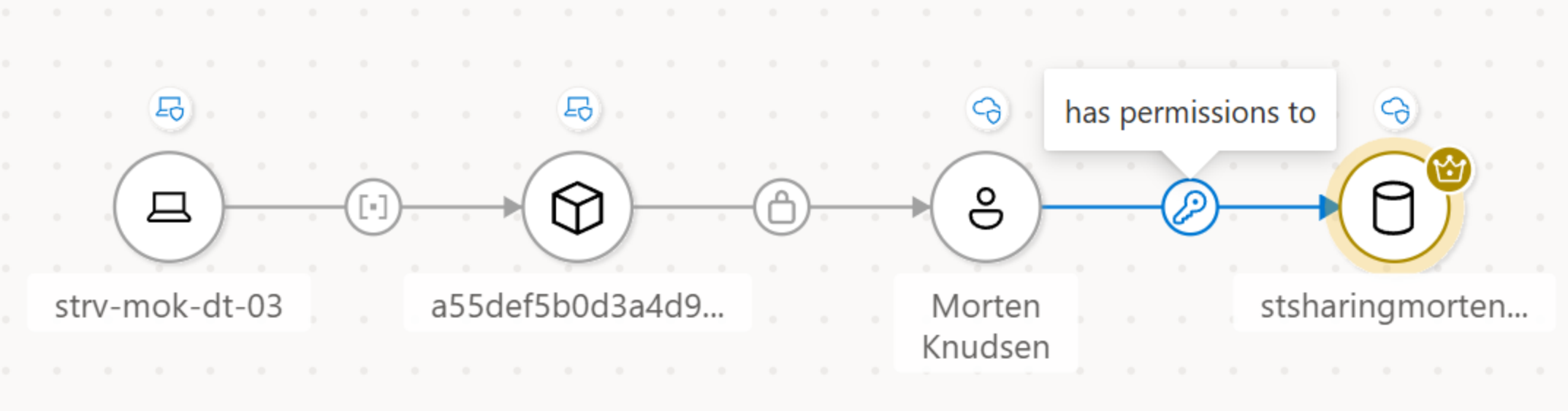
Example of Attack Path



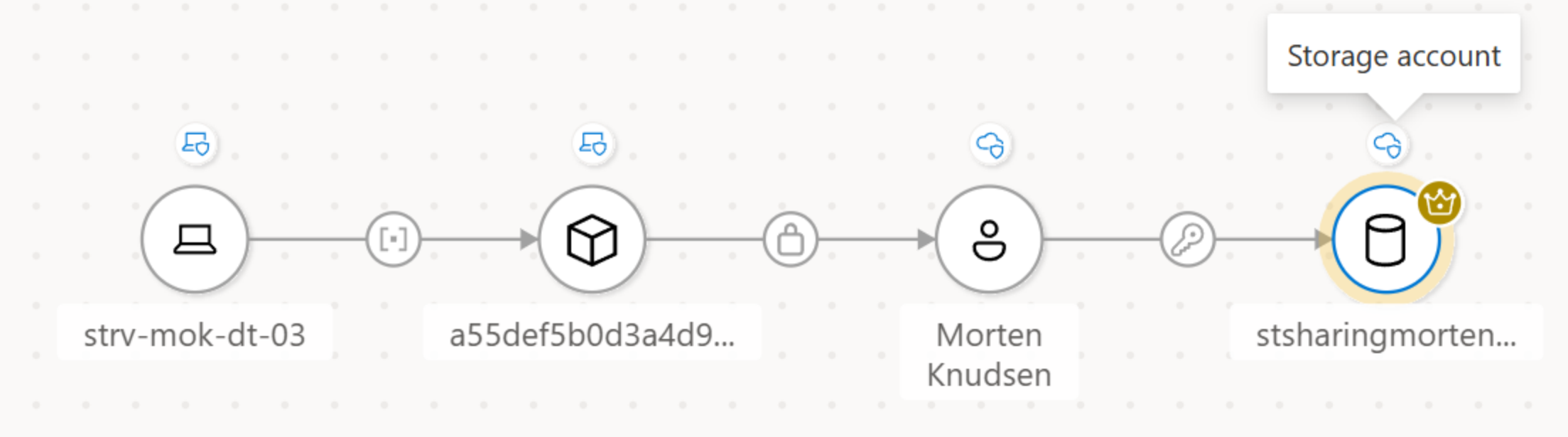
Example of Attack Path



Example of Attack Path



Example of Attack Path

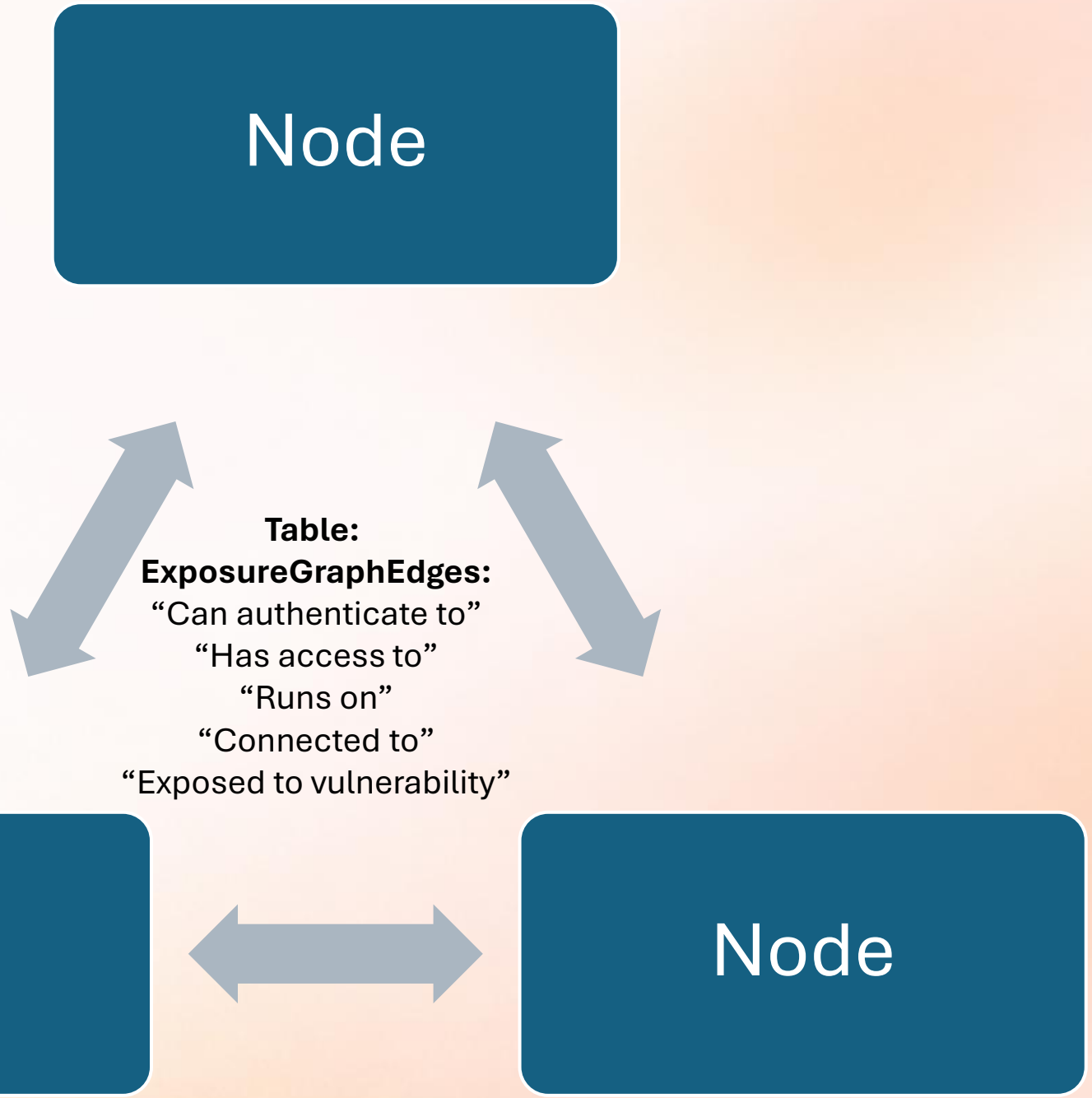


ExposureGraph

"API v2" - Index

Table: ExposureGraphNodes (normalized sources):

Devices
Users / identities
Groups
Cloud resources (VMs, storage, containers)
Applications / services



Advanced hunting

New query* | New query | New query*

Query | Run query

```
ExposureGraphNodes
| distinct NodeLabel
```

Results | Query history | Getting started

Export | Show empty columns

Filters: Add filter

NodeLabel
baseModel
Cve
serviceprincipal
device
microsoft.compute/virtualmachines/extensions
user
endpointAiAgent
managedidentity
microsoft.sql/servers
entra-userCookie
Microsoft Entra OAuth App
microsoft.network/virtualnetworks/subnets
resourcegroups
group
mdcSecurityRecommendation
mdcAuditingRecommendation
mdcManagementRecommendation
mde-healthFinding

2LINKIT Microsoft Defender

Home

Exposure management

Investigation & response

Incidents & alerts

Hunting

Advanced hunting

Custom detection rules

Actions & submissions

Partner catalog

Threat intelligence

Assets

Microsoft Sentinel

Identities

Endpoints

Email & collaboration

Cloud apps

Cloud security

Advanced hunting

New query* | New query | New query*

Query | Run query

```
ExposureGraphEdges
| distinct EdgeLabel
```

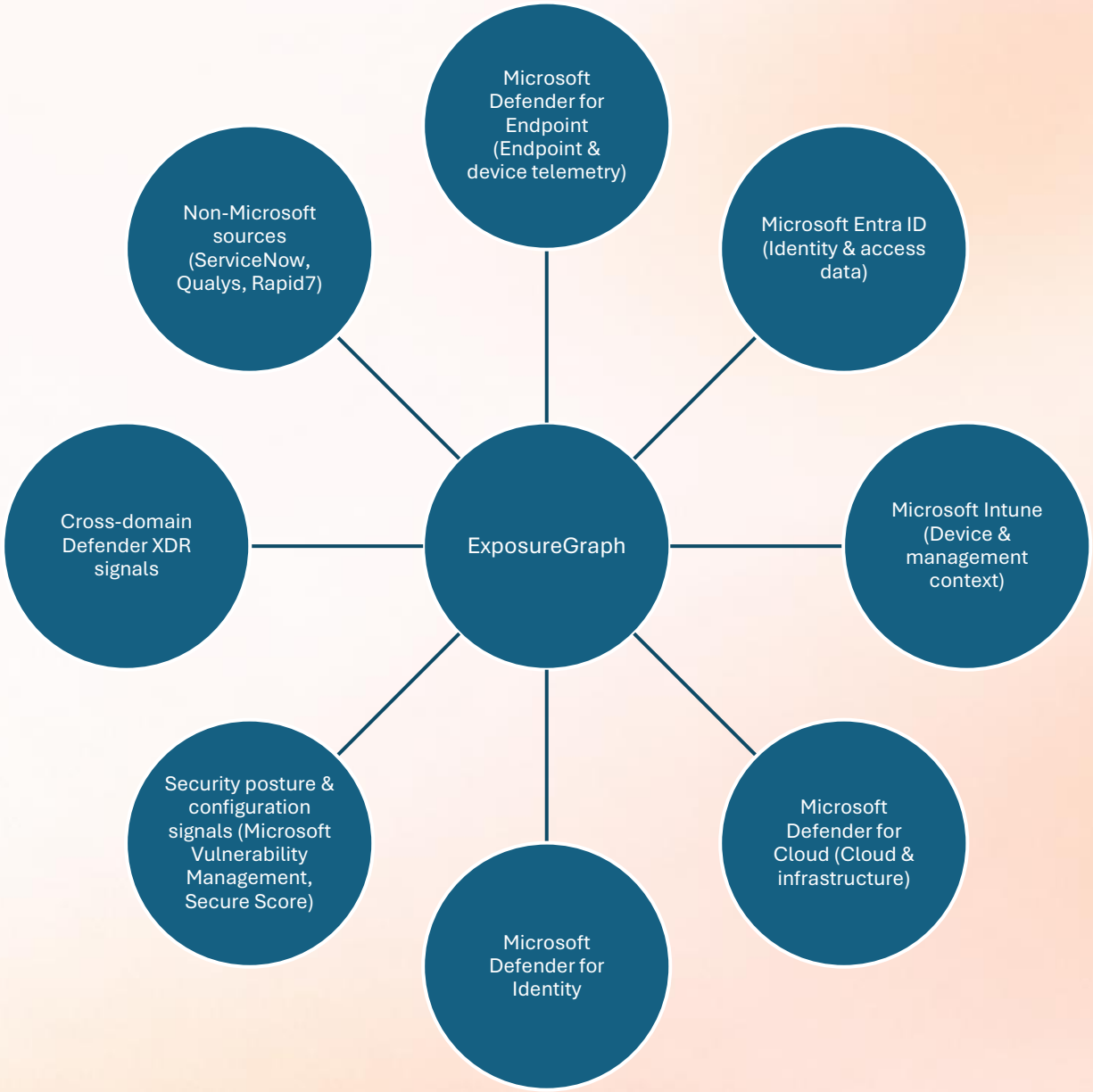
Results | Query history | Getting started

Export | Show empty columns

Filters: Add filter

EdgeLabel
contains
affecting
has role on
has credentials of
has permissions to
can authenticate as
routes traffic to
member of
frequently logged in
can authenticate to
defined in
defines
can impersonate as
runs on

ExposureGraph Data sources



Find all DC & DNS resources

```
ExposureGraphNodes
| where NodeLabel has "device"
   or NodeLabel has "microsoft.compute/virtualmachines"
   or NodeLabel has "microsoft.hybridcompute/machines"
| extend rawData = todynamic(NodeProperties).rawData
| where tobool(rawData.isExcluded) == false
| where tostring(rawData.deviceType) == "Server"
| where tolower(tostring(rawData.onboardingStatus)) == "onboarded"
| project NodeId, NodeName, NodeLabel, rawData, EntityIds
| extend
    confidenceHigh = iff(isnull(rawData.criticalityConfidenceHigh), dynamic([]), todynamic(rawData.criticalityConfidenceHigh)),
    confidenceLow  = iff(isnull(rawData.criticalityConfidenceLow),  dynamic([]), todynamic(rawData.criticalityConfidenceLow))
| extend
    DetectedRoles  = strcat_array(array_concat(confidenceHigh, confidenceLow), ";")
| where DetectedRoles has "DomainController"
    or DetectedRoles has "Dns"
```

Find all DC & DNS resources

```
ExposureGraphNodes
| where NodeLabel has "device"
    or NodeLabel has "microsoft.compute/virtualmachines"
    or NodeLabel has "microsoft.hybridcompute/machines"
| extend rawData = todynamic(NodeProperties).rawData
| where tobool(rawData.isExcluded) == false
| where tostring(rawData.deviceType) == "Server"
| where tolower(tostring(rawData.onboardingStatus)) == "onboarded"
| project NodeId, NodeName, NodeLabel, rawData, EntityIds
| extend
    confidenceHigh = iff(isnull(rawData.criticalityConfidenceHigh), dynamic([]), todynamic(rawData.criticalityConfidenceHigh)),
    confidenceLow  = iff(isnull(rawData.criticalityConfidenceLow),  dynamic([]), todynamic(rawData.criticalityConfidenceLow))
| extend
    DetectedRoles  = strcat_array(array_concat(confidenceHigh, confidenceLow), ";")
| where DetectedRoles has "DomainController"
    or DetectedRoles has "Dns"
```

Find all DC & DNS resources

```
ExposureGraphNodes
| where NodeLabel has "device"
    or NodeLabel has "microsoft.compute/virtualmachines"
    or NodeLabel has "microsoft.hybridcompute/machines"
| extend rawData = todynamic(NodeProperties).rawData
| where tobool(rawData.isExcluded) == false
| where tostring(rawData.deviceType) == "Server"
| where tolower(tostring(rawData.onboardingStatus)) == "onboarded"
| project NodeId, NodeName, NodeLabel, rawData, EntityIds
| extend
  confidenceHigh = iff(isnull(rawData.criticalityConfidenceHigh), dynamic([]), todynamic(rawData.criticalityConfidenceHigh)),
  confidenceLow  = iff(isnull(rawData.criticalityConfidenceLow),  dynamic([]), todynamic(rawData.criticalityConfidenceLow))
| extend
  DetectedRoles  = strcat_array(array_concat(confidenceHigh, confidenceLow), ";")
| where DetectedRoles has "DomainController"
    or DetectedRoles has "Dns"
```

Find all DC & DNS resources

```
ExposureGraphNodes
| where NodeLabel has "device"
    or NodeLabel has "microsoft.compute/virtualmachines"
    or NodeLabel has "microsoft.hybridcompute/machines"
| extend rawData = todynamic(NodeProperties).rawData
| where tobool(rawData.isExcluded) == false
| where tostring(rawData.deviceType) == "Server"
| where tolower(tostring(rawData.onboardingStatus)) == "onboarded"
| project NodeId, NodeName, NodeLabel, rawData, EntityIds
| extend
    confidenceHigh = iff(isnull(rawData.criticalityConfidenceHigh), dynamic([]), todynamic(rawData.criticalityConfidenceHigh)),
    confidenceLow  = iff(isnull(rawData.criticalityConfidenceLow),  dynamic([]), todynamic(rawData.criticalityConfidenceLow))
| extend
    DetectedRoles  = strcat_array(array_concat(confidenceHigh, confidenceLow), ";")
| where DetectedRoles has "DomainController"
   or DetectedRoles has "Dns"
```

```
| where DetectedRoles has "ActiveDirectoryCertificateServicesServer"
```

Updating ExposureGraph

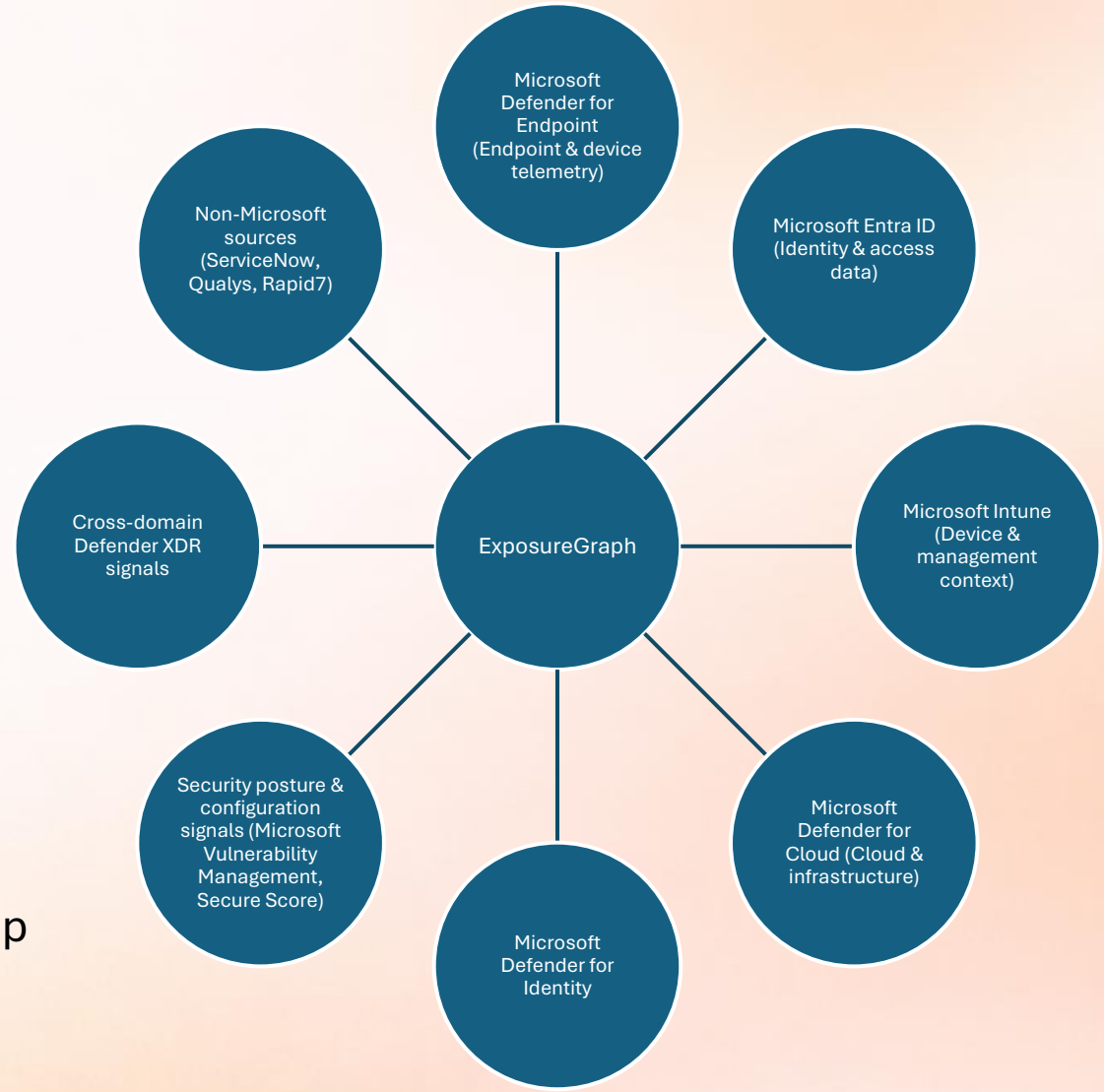
Goal: near-real time data !

Azure Resource Graph:
Asset -> Control Plane – Transaction – near real-time
Rebuild every 24 hour

ExposureGraph:
Signals (alerts, events) arrive near real-time
Asset inventory are synced (master/slave)

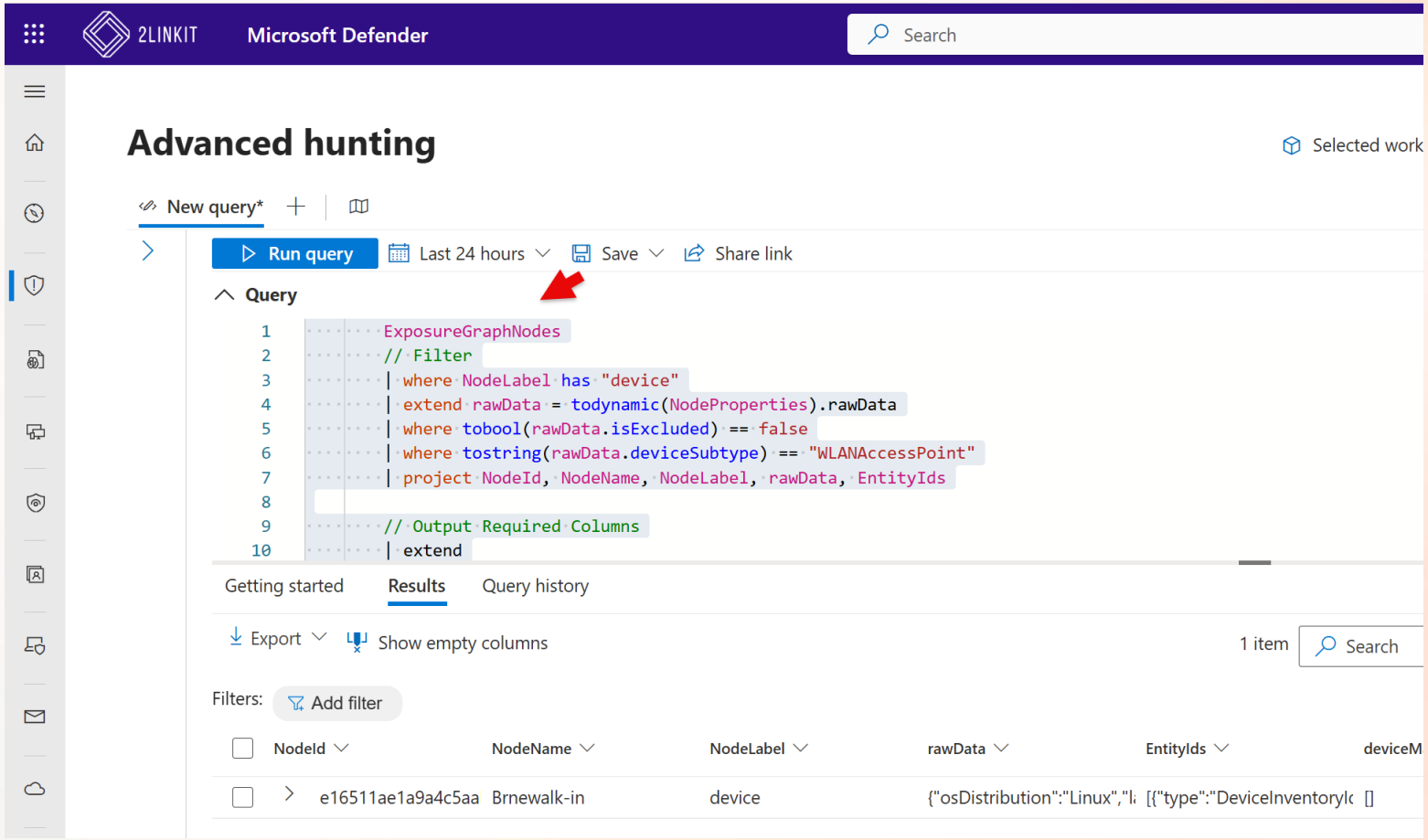
Graph normalization + relationship
Delay: ~24-72 hours

Challenge: Frequency, re-design architecture speed-up



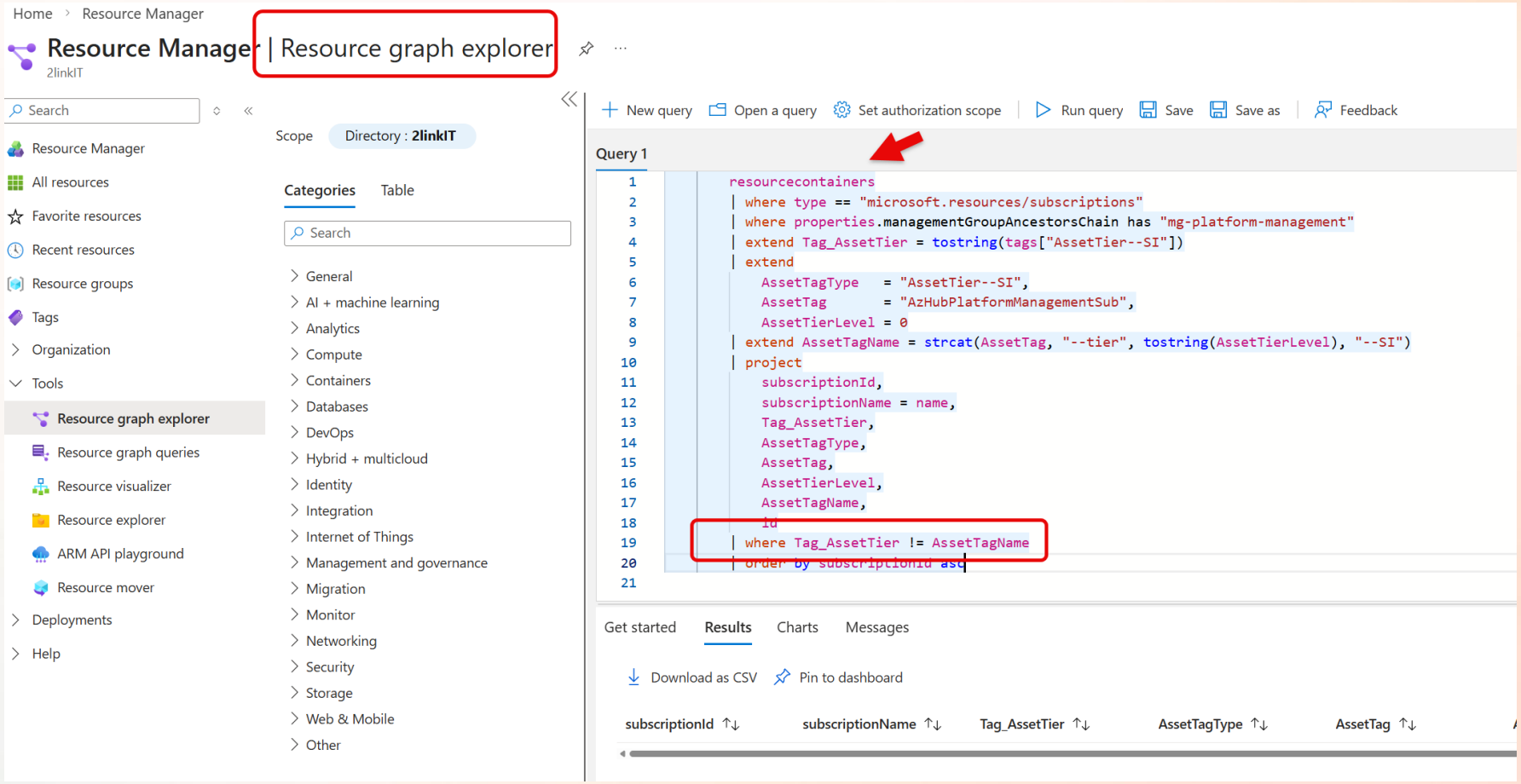
Testing Queries

Defender



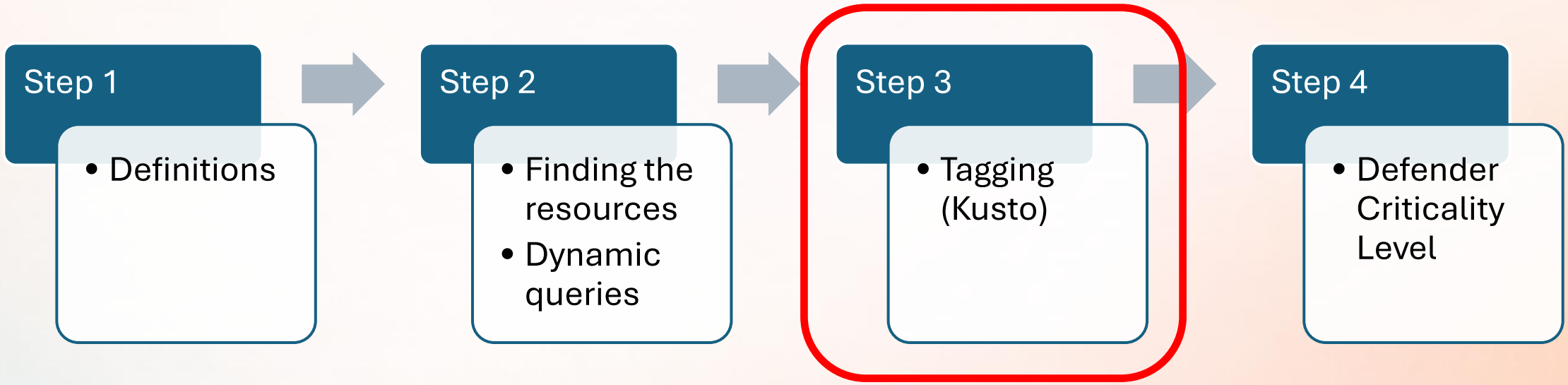
Testing Queries

Azure

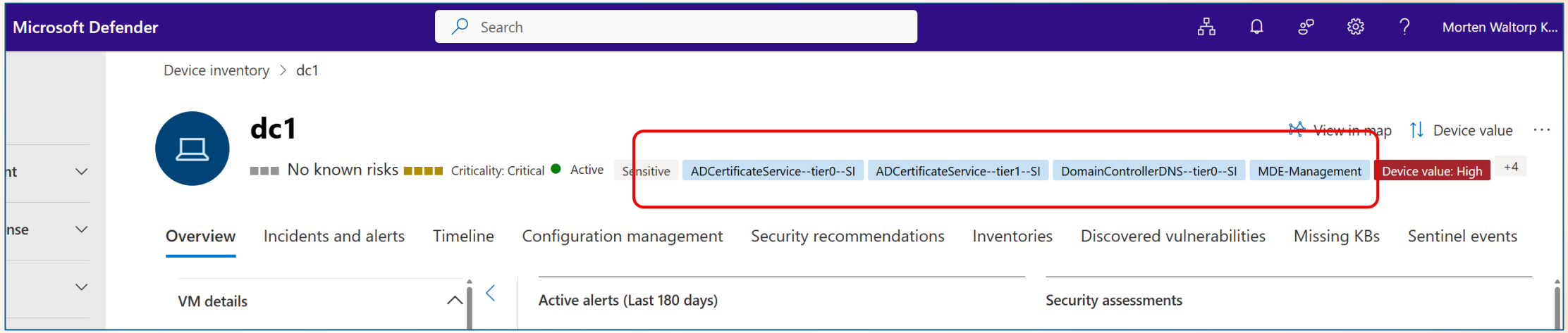


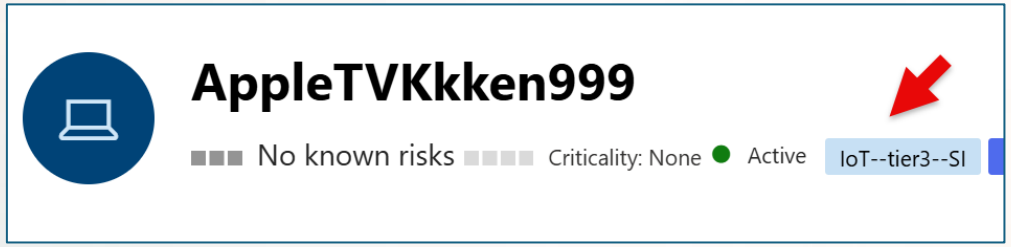
Asset Criticality Classifications

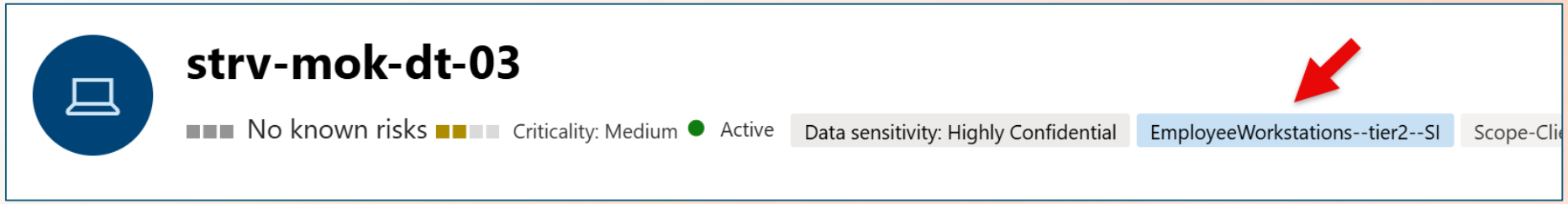
Implementation Steps



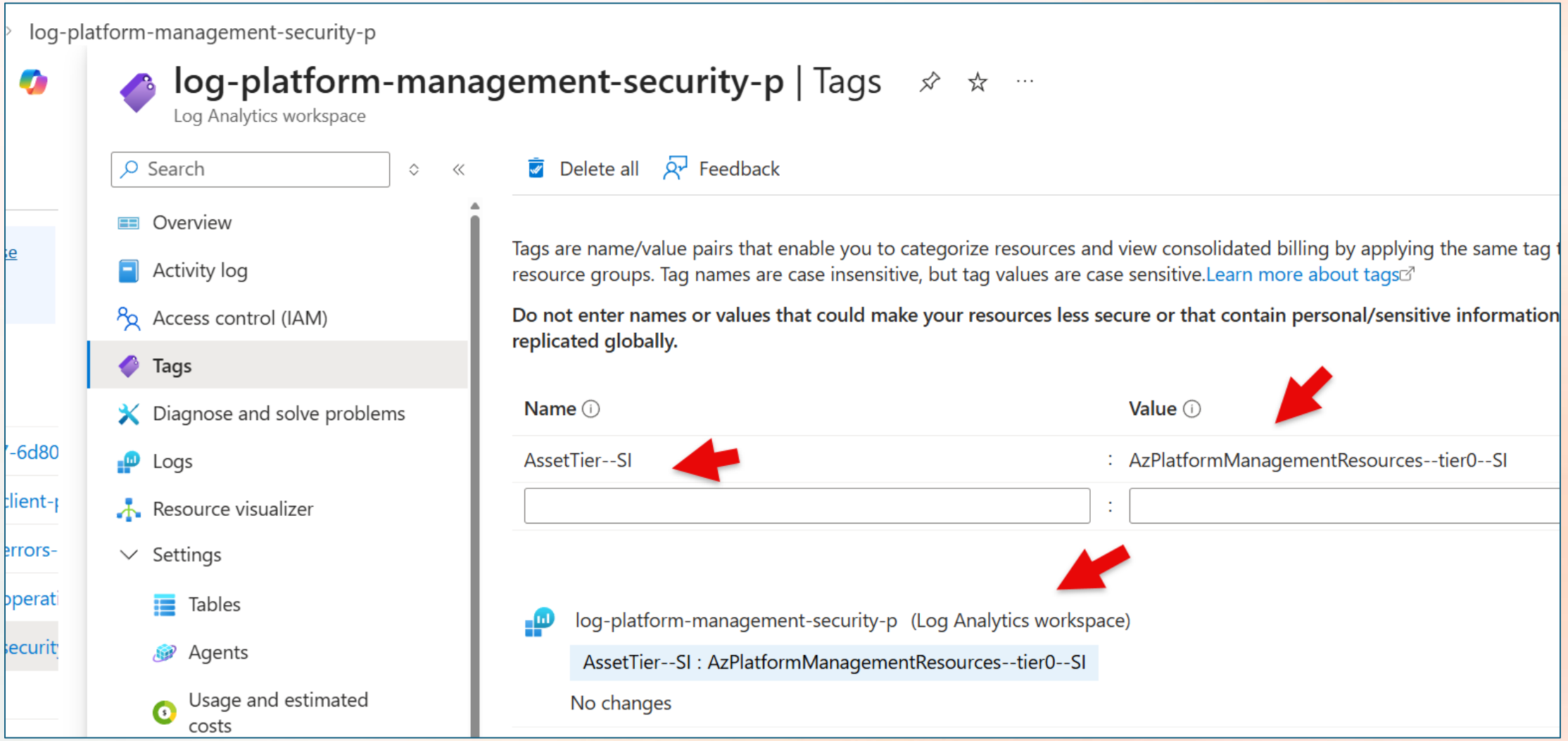
Tagging Example (Defender)







Tagging Example (Azure)



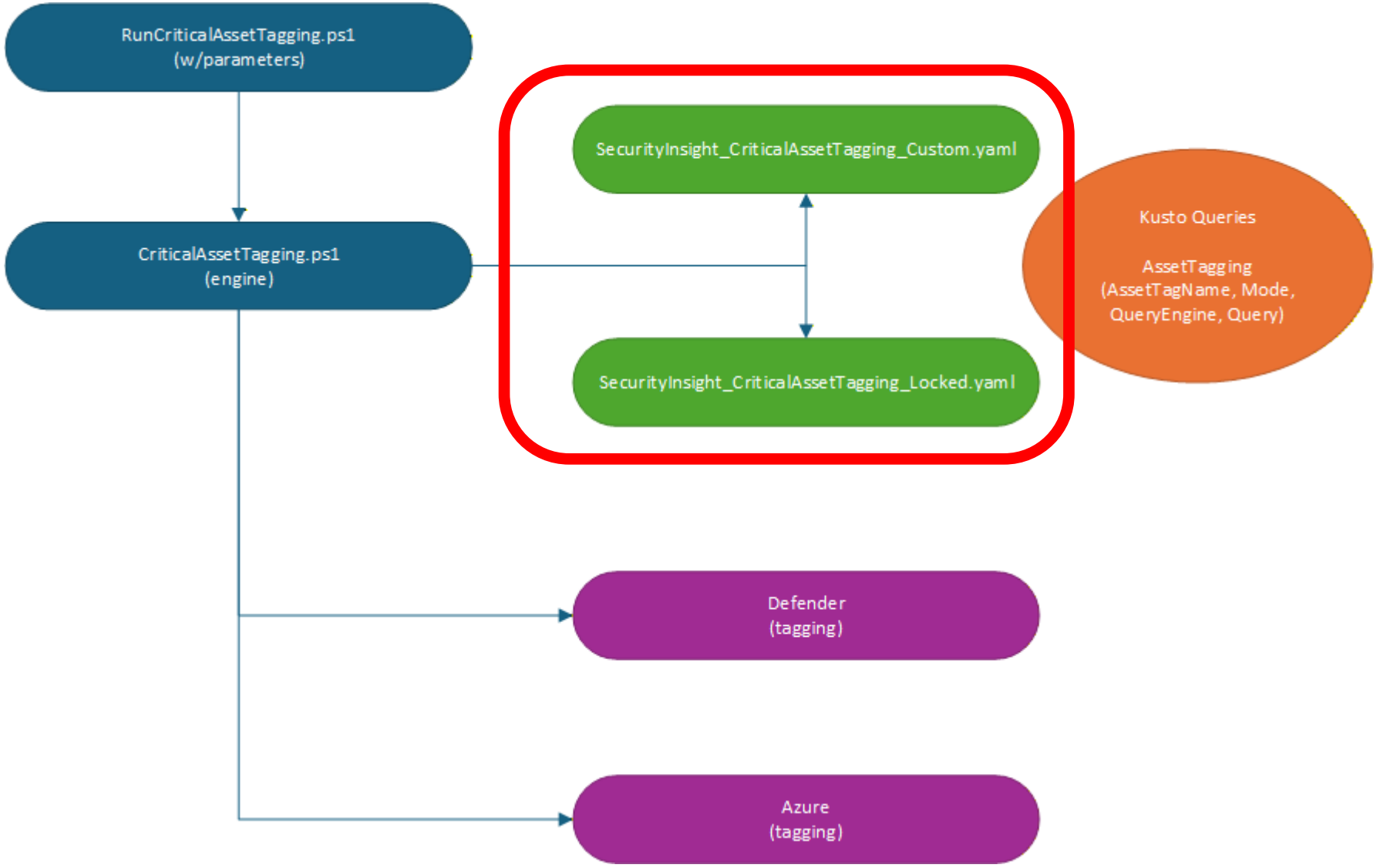
Asset Tags (180 total)

Critical asset coverage across identity, cloud, and endpoint

Area	Count	What's covered
Identity	**24**	Entra/AD roles, SPNs, service accounts, Break Glass, krbtgt, sync accounts
Azure	**72**	VMs, storage, networking, Key Vault, AKS, DevOps, Arc, Stack HCI, Automation, subscriptions
Endpoints / Servers	**46**	Domain Controllers, AD CS, Entra Sync, PAWs, workstations, jump servers, hypervisors, backup/patch/security mgmt servers
Network	**14**	Backbone switches/routers, WLAN, SD-WAN, SSL inspection, access/distribution switches, VoIP
IoT / OT	**7**	Domain-integrated OT, industrial OT, office IoT, consumer IoT
Other	**17**	Kiosk/shared terminals, BYOD, developer machines, SOC workstations, misc


Administrator: Windows PowerShell
PS D:\>

Flow
Asset Tagging

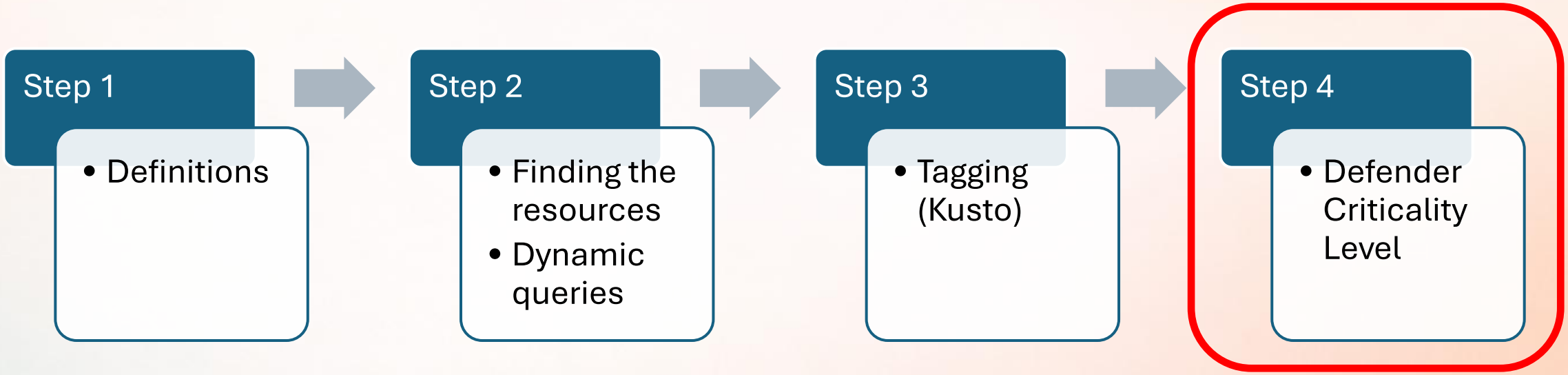


```yaml
AssetTagging:
  - AssetTagName: AzHubPlatformManagementSub--tier0--SI
    Mode: Test
    QueryEngine: AzureResourceGraph
    Query:
      - |
        resourcecontainers
        | where type == "microsoft.resources/subscriptions"
        | where properties.managementGroupAncestorsChain has "mg-platform-management"
        | extend Tag_AssetTier = tostring(tags["AssetTier--SI"])
        | extend
            AssetTagType   = "AssetTier--SI",
            AssetTag       = "AzHubPlatformManagementSub",
            AssetTierLevel = 0
        | extend AssetTagName = strcat(AssetTag, "--tier", tostring(AssetTierLevel), "--SI")
        | project
            subscriptionId,
            subscriptionName = name,
            Tag_AssetTier,
            AssetTagType,
            AssetTag,
            AssetTierLevel,
            AssetTagName,
            id
        | where Tag_AssetTier != AssetTagName
        | order by subscriptionId asc


  - AssetTagName: AzHubPlatformManagementResources--tier0--SI
    Mode: Test
    QueryEngine: AzureResourceGraph
    Query:
      - |
        resources
        | join kind=inner (
```

```
AssetTagging:
  - AssetTagName: DomainControllerDNS--tier0--SI
    Mode: Prod
    QueryEngine: DefenderGraph
    Query:
      - |
        ExposureGraphNodes

        // Filter
        | where NodeLabel has "device"
           or NodeLabel has "microsoft.compute/virtualmachines"
           or NodeLabel has "microsoft.hybridcompute/machines"

        | extend rawData = todynamic(NodeProperties).rawData
        | where tobool(rawData.isExcluded) == false
        | where tostring(rawData.deviceType) == "Server"
        | where tolower(tostring(rawData.onboardingStatus)) == "onboarded"
        | project NodeId, NodeName, NodeLabel, rawData, EntityIds
        | extend
            confidenceHigh = iff(isnull(rawData.criticalityConfidenceHigh), dynamic([]), todynamic(rawData.criticalityConfidenceHigh)),
            confidenceLow  = iff(isnull(rawData.criticalityConfidenceLow),  dynamic([]), todynamic(rawData.criticalityConfidenceLow))
        | extend
            DetectedRoles  = strcat_array(array_concat(confidenceHigh, confidenceLow), ";"),
            osPlatform     = tostring(rawData.osPlatform),
            osVersion      = tostring(rawData.osVersion),
            onboardingStatus = tostring(rawData.onboardingStatus)

        | where DetectedRoles has "DomainController"
            or DetectedRoles has "Dns"

        // Output Required Columns
        | extend
            deviceManualTags = iff(isnull(rawData.deviceManualTags), dynamic([]), todynamic(rawData.deviceManualTags)),
            deviceDynamicTags = iff(isnull(rawData.deviceDynamicTags), dynamic([]), todynamic(rawData.deviceDynamicTags)),
            tags = iff(isnull(rawData.tags.tags), dynamic([]), todynamic(rawData.tags.tags))
        | extend
            AssetTags  = strcat_array(array_concat(deviceManualTags, deviceDynamicTags), ";")
        | extend entityIds_dyn = todynamic(EntityIds)
        | mv-apply e = entityIds_dyn on (
            summarize
                DeviceInventoryId = anyif(tostring(e.id), tostring(e.type) == "DeviceInventoryId"),
                SenseDeviceId     = anyif(tostring(e.id), tostring(e.type) == "SenseDeviceId"),
                AzureResourceId   = make_list_if(tostring(e.id), tostring(e.type) == "AzureResourceId")
        )
        | extend AzureResourceId = strcat_array(AzureResourceId, ";")
```

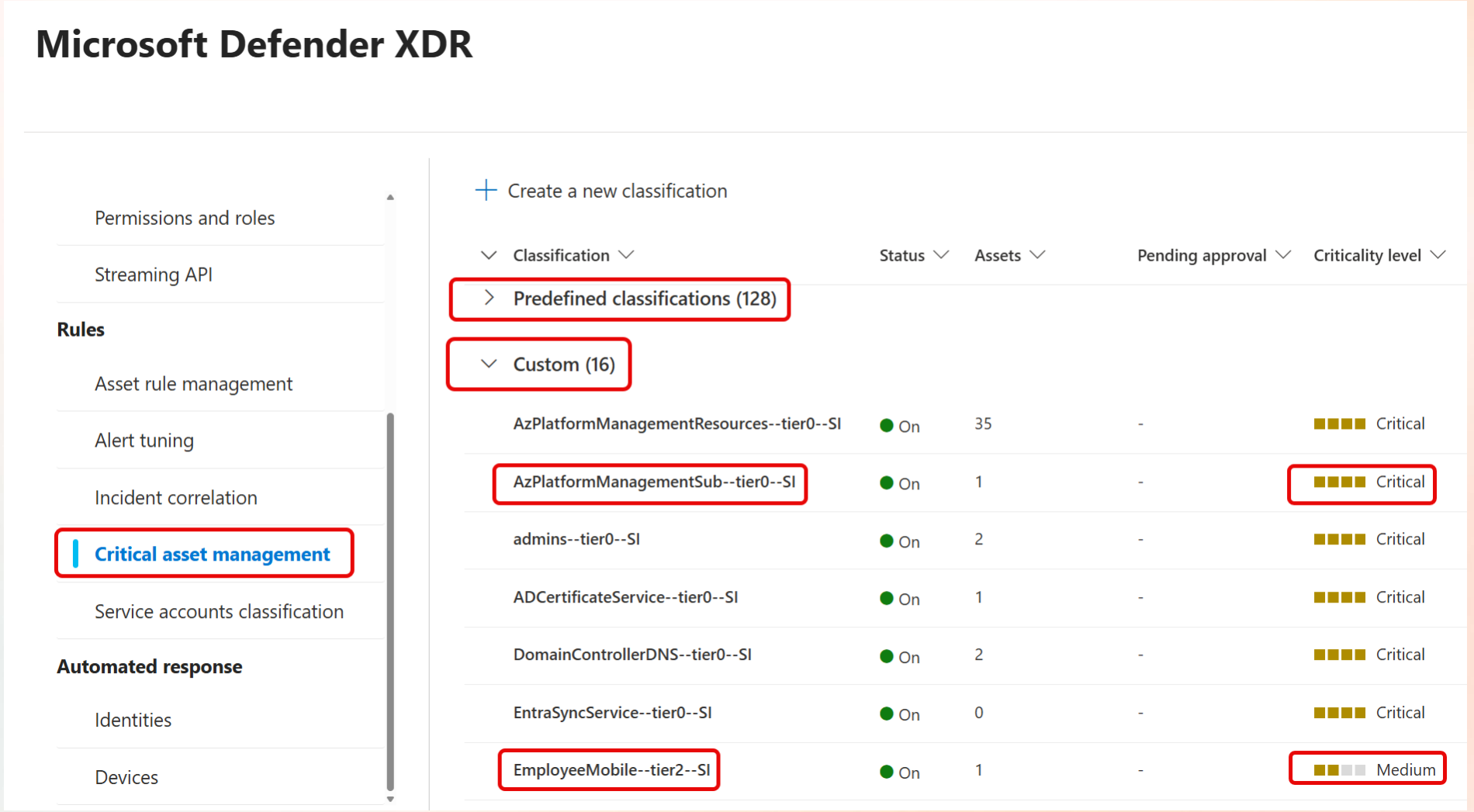
Asset Criticality Classifications

Implementation Steps – Endpoint & Azure



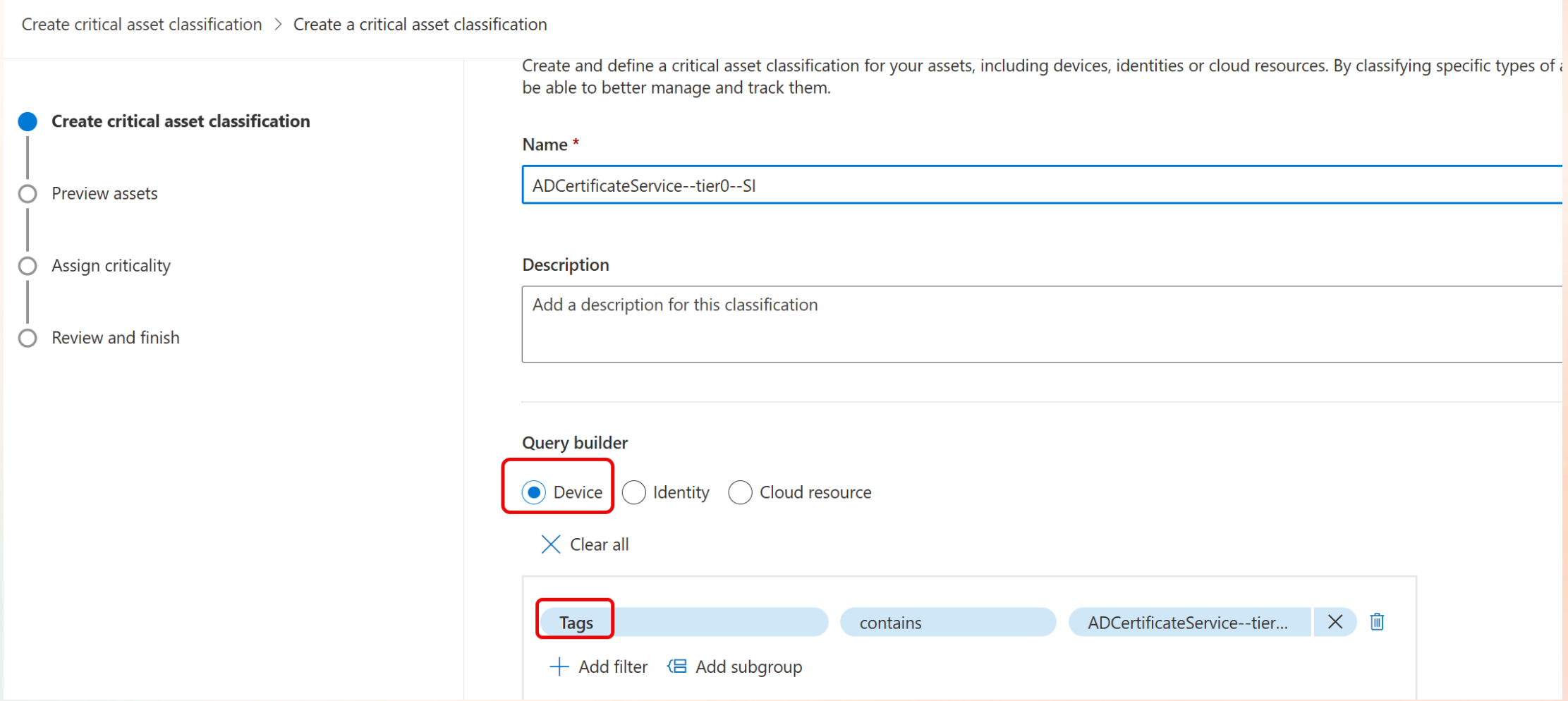
Criticality Level Tagging | Defender

Custom Classifications



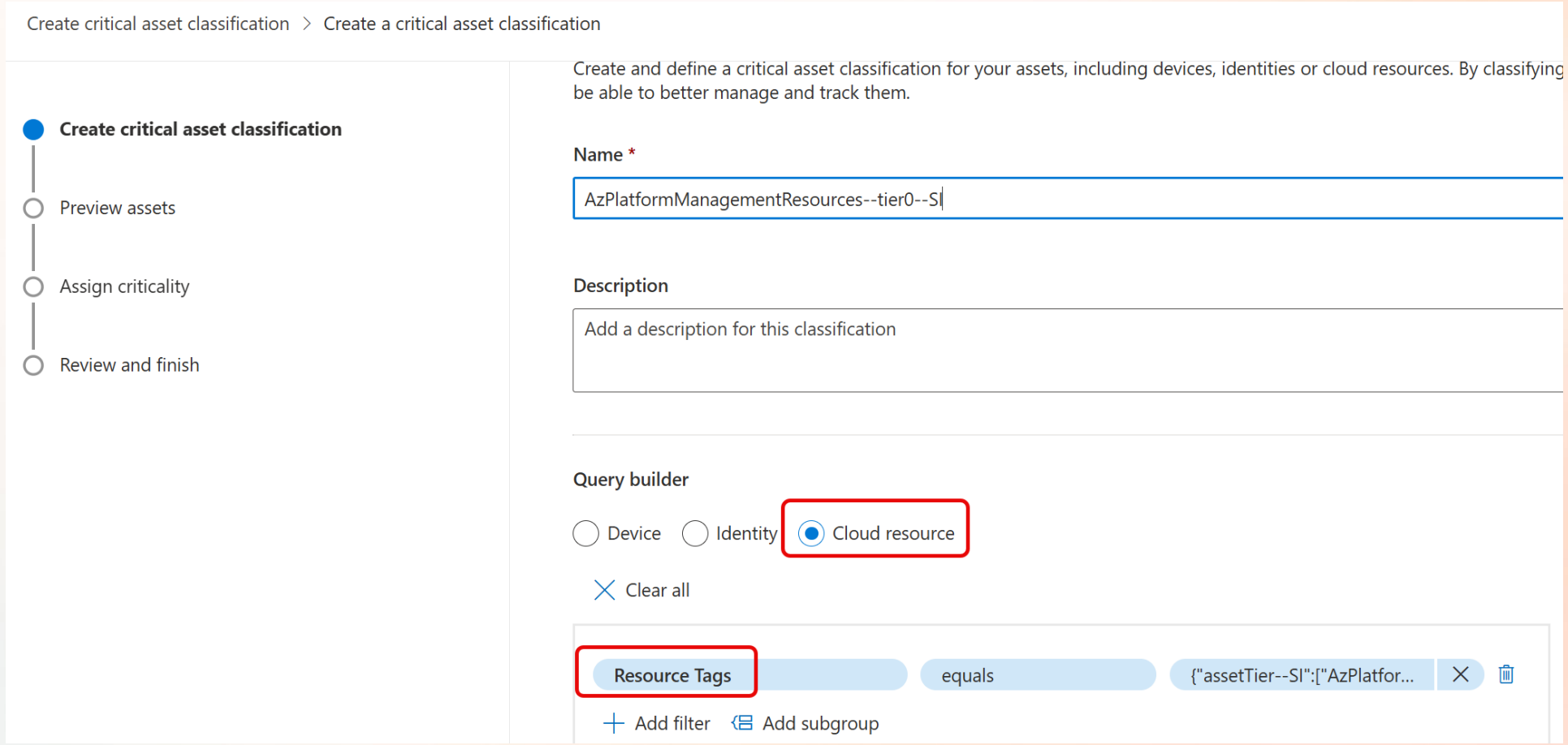
Criticality Level Tagging | Defender

Device



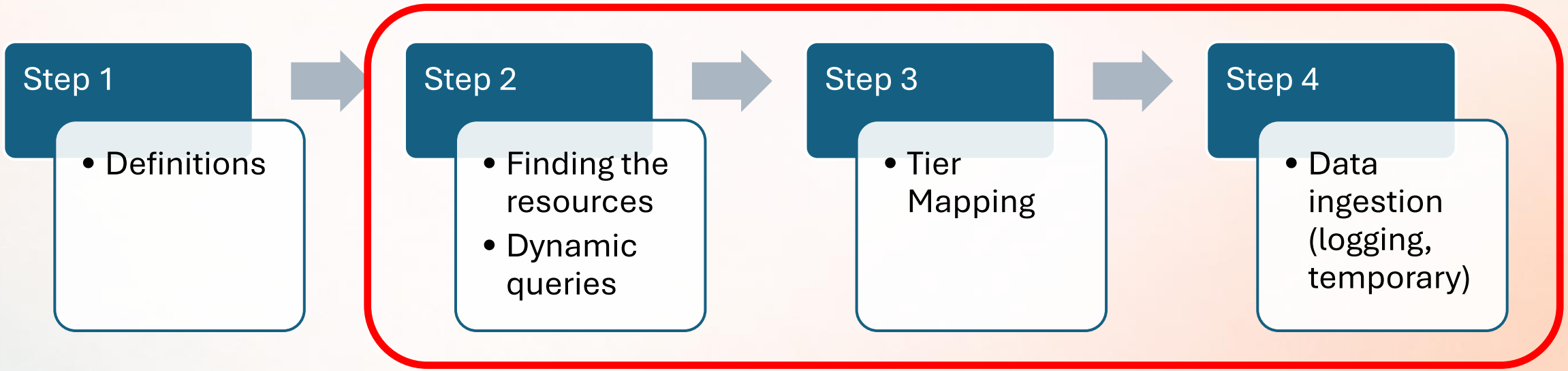
Criticality Level Tagging | Defender

Cloud Resource (Azure)



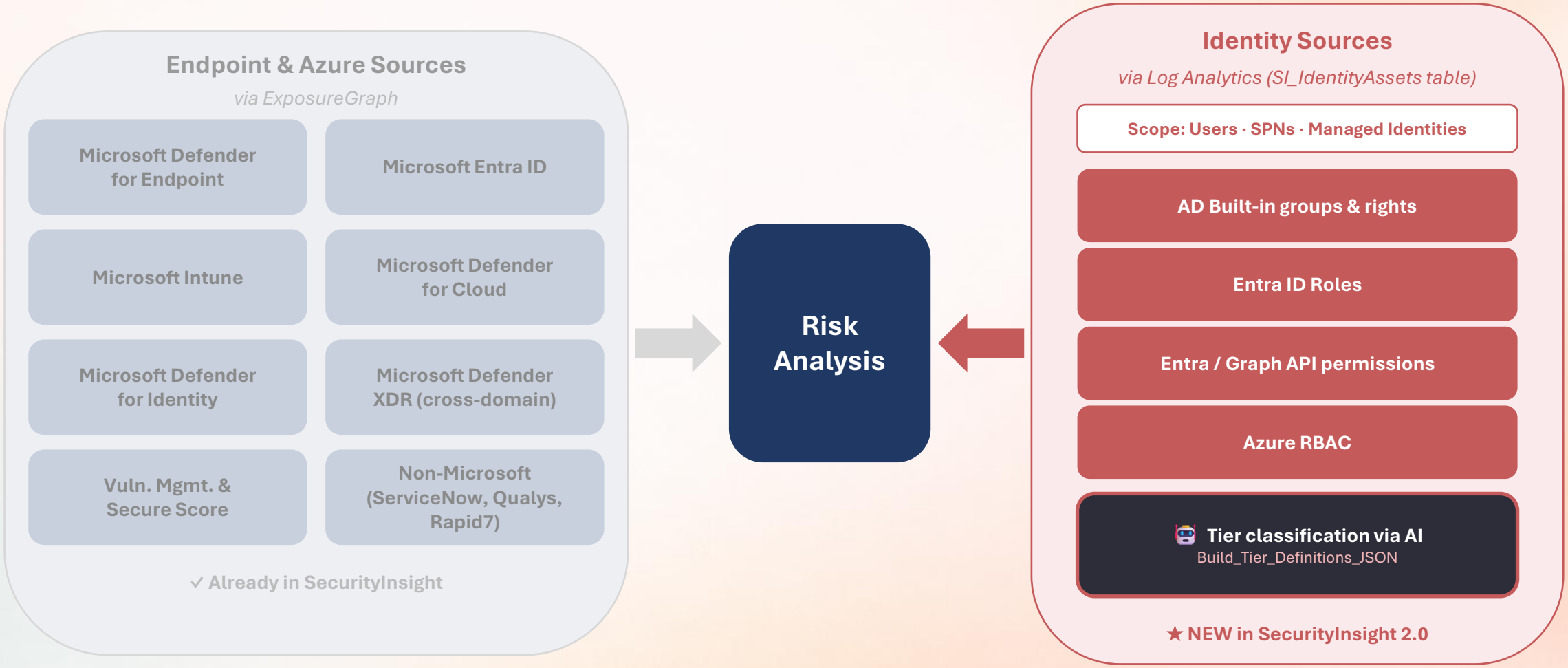
Asset Criticality Classifications

Implementation Steps – Identity

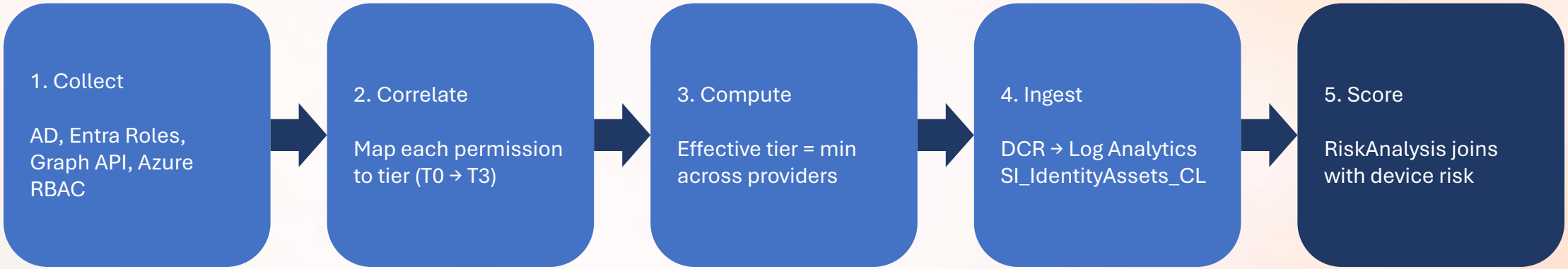


Sources Feeding Risk Analysis

New: Identity via Log Analytics



The Identity Risk Pipeline



Pipeline stored temporarily in Log Analytics via Data Collection Rule

Scope
Every identity in the tenant — users, service principals, managed identities.

Cadence
Daily — separate from the monthly tier-catalogue builder.

How the AI Tier Catalogue Gets Built

Build_Tier_Definitions_JSON_File.ps1

STEP 1

COLLECT

Built-in permissions behind every role across AD, Entra, Graph, and Azure RBAC.

STEP 2

ASSEMBLE

Permission manifest per role — what the role actually lets an attacker do.

STEP 3

EVALUATE

Azure OpenAI rates each manifest against the SecurityInsight rubric (T0 → T3).

STEP 4

WRITE

Aggregate into SecurityInsight_IdentityTiering.json — consumed by the collector.

⏱️ **Cadence**

Weekly — or on demand when Microsoft publishes notable role changes.

📦 **Fallback**

Platform-shipped sample (DATA\SecurityInsight_IdentityTiering.json) used until

100+ New Queries Detect Identity Drift

Identity becomes a first-class citizen in RiskAnalysis

100+

new identity
KQL queries
detecting drift

Privilege Drift

Identities that crossed into a higher tier since last snapshot — new GA, new T0 scope on a service principal.

Permission Sprawl

Accumulated Graph scopes and Azure RBAC over time — effective permissions exceeding intended role.

Stale Tier-0

Inactive or dormant identities that still hold Tier-0 permissions across AD, Entra, Graph, or Azure.

Shadow SPs & MIs

Service principals and managed identities with privileged scopes that don't appear in any governance review.

How can you implement this in your environment ?

How can you implement this in your environment ?

- Github:
  - https://github.com/KnudsenMorten/SecurityInsight

- Quick-link:
  - **securityinsight.mortenknudsen.net**
    (url forward to Github repo)

TESTING OF V2 IN PROGRESS !!!!
Expect to release later in May 2026
I will announce on LinkedIn

Check out files & documentation now !!
Please wait .... lots of commits !

Love to connect with you ☺
Morten Knudsen

/in/knudsenmorten

@mortenknudsen.net

@knudsenmortendk

aka.ms/morten

mok@mortenknudsen.net

Thank You ☺

Appendix next slides

Querying ExposureGraph

Demo 1-11

Querying ExposureGraph

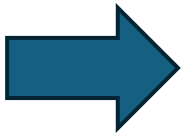
- Demo 1: What asset types exist in our exposure graph
- Demo 2: List endpoints and their criticality (asset posture view)
- Demo 3: What edge labels exist
- Demo 4: Show relationship between node types
- Demo 5: Pick one asset and show its immediate neighbors
- Demo 6: Find all “finding” nodes and their affected assets
- Demo 7: Internet exposure risk factor
- Demo 8: Internet-facing assets
- Demo 9: Assets impacted by the same finding
- Demo 10: Show all Edges for a specific user
- Demo 11: Excluded assets hygiene check

Demo 1: What asset types exist in our exposure graph

Show what kinds of objects the graph contains (endpoints, identities, cloud resources, apps, etc.) and how many of each.

```
ExposureGraphNodes
| summarize NodeCount = count() by NodeLabel
| order by NodeCount desc
```

Process:
1) Query nodes
2) Use NodeLabel to group into “types”



NodeLabel	NodeCount
mdcSecurityRecommendation	484350
Cve	342818
group	3402
serviceprincipal	1018
baseModel	979
managedidentity	553
Microsoft Entra OAuth App	236
mdcManagementRecommendation	209
mdcAuditingRecommendation	88
resourcegroups	78
user	71
device	54
microsoft.compute/virtualmachines/exten:	40
mde-healthFinding	27
githubrepository	26

Demo 2: List endpoints and their criticality (asset posture view)

Show “asset context” enrichment: criticality levels and rule-based criticality (if populated), plus basic asset identification.

```
ExposureGraphNodes
| where tostring(NodeProperties.rawData.deviceCategory) == "Endpoint"
| extend CriticalityLevel = toint(coalesce(
    tostring(NodeProperties.criticalityLevelProps[0].criticalityLevel),
    tostring(NodeProperties.rawData.criticalityLevel.criticalityLevel),
    tostring(NodeProperties.criticalityLevel.criticalityLevel)
))
| extend RuleBasedCriticality = toint(coalesce(
    tostring(NodeProperties.criticalityLevelProps[0].ruleBasedCriticalityLevel),
    tostring(NodeProperties.rawData.criticalityLevel.ruleBasedCriticalityLevel),
    tostring(NodeProperties.criticalityLevel.ruleBasedCriticalityLevel)
))
| project NodeId, AssetName=NodeName, NodeLabel, CriticalityLevel, RuleBasedCriticality, NodeProperties
| order by CriticalityLevel asc
```

Process:
1) Filter to endpoint assets (many tenants store this in rawData.deviceCategory)
2) Extract criticality fields from the possible locations
3) Sort by most critical first

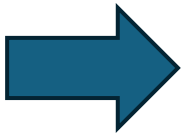
NodeId	AssetName	NodeLabel	CriticalityLevel	RuleBasedCriticality	NodeProperties
f95d2e35601544b9b0c7125d77ca4c	eps-demo-byod	microsoft.compute/virtualmachines			{"rawData":{"deviceRole":[],"lastSeen":"2026-04
230f7bc7524b4ecc9ba429a27a9846	eps-demo-dc1	microsoft.compute/virtualmachines			{"rawData":{"deviceCategory":"Endpoint","devic
885afcb1c4f147b78b3c1c7378e0bd	demowin2	microsoft.compute/virtualmachines			{"rawData":{"deviceSubtype":"Server","isHybrid
7fae4100b5a241df8ea4bd227a35d9	eps-demo-whfb	microsoft.compute/virtualmachines			{"rawData":{"deviceType":"Workstation","isCust
6fa35b325acc445ca8b04a3ae400bc		device			{"rawData":{"osVersion":"6.0","firstSeenByInven
fd176dca37f247e8a81c3642d499ba	MACBOOKAIR-2A42	device			{"rawData":{"deviceCategory":"Endpoint","devic
1fe344af097b474e9dbf1eac39f734c	dc1.2linkit.local	microsoft.compute/virtualmachines	0	0	{"rawData":{"tags":{"tags":{"Environment":"PRO
f601b610bc88400baf86becda53f39	dc3.2linkit.local	microsoft.compute/virtualmachines	0	0	{"rawData":{"tags":{"tags":{"Environment":"PRO
7d4f6d2ec54b426ea8e4e95f8e3578	mgmt1.2linkit.local	microsoft.compute/virtualmachines	0	0	{"rawData":{"tags":{"tags":{"Environment":"PRO
cd9b95e12ac849dfb1ae93d3675c1e	strv-mok-dt-03	device	1	1	{"rawData":{"deviceCategory":"Endpoint","devic
69e43cfad61c4f9e883f0e40303aa36	strv-cew-lt-03	device	2	2	{"rawData":{"isCustomerFacing":true,"deviceTyp
9be56ff4cdf94f15b298562eb4b02f7	niels_Android	device	2	2	{"rawData":{"isCustomerFacing":true,"deviceTyp
585e4d2679e346178a7866452e40fc	heim-new-lt-02	device	2	2	{"rawData":{"isCustomerFacing":true,"deviceTyp
b24a984cdc9b40d5948013fa60c79e	strv-mew-lt-02	device	2	2	{"rawData":{"deviceCategory":"Endpoint","devic
fe32fb6232354f8b8e7c63e946876ce	dons-ekn-lt-02	device	2	2	{"rawData":{"isCustomerFacing":true,"deviceTyp

Demo 3: What edge labels exist

Show how the graph connects objects by showing the edge label relationship taxonomy

```
ExposureGraphEdges
| summarize EdgeCount = count() by EdgeLabel
| order by EdgeCount desc
```

Process:
1) Query edges
2) Group by EdgeLabel



EdgeLabel	EdgeCount
affecting	4939
has permissions to	1414
member of	1373
has role on	1018
can authenticate as	239
contains	226
can authenticate to	40
routes traffic to	38
can impersonate as	32
has credentials of	15
frequently logged in by	12
runs on	7
defined in	1
defines	1

Demo 4: Show relationship between node types

Show a relationship heat map like Endpoint → Identity, Identity → App, CloudResource → Finding, etc. (type-to-type map)

```
let Nodes = ExposureGraphNodes | project NodeId, NodeLabel, NodeName;
ExposureGraphEdges
| join kind=inner (Nodes) on $left.SourceNodeId == $right.NodeId
| extend SourceLabel = NodeLabel, SourceName = NodeName
| join kind=inner (Nodes) on $left.TargetNodeId == $right.NodeId
| extend TargetLabel = NodeLabel, TargetName = NodeName
| summarize EdgeCount=count() by SourceLabel, EdgeLabel, TargetLabel
| order by EdgeCount desc
```

Process:
1) Join edges to nodes twice (source and target)
2) Summarize by SourceLabel → EdgeLabel → TargetLabel

SourceLabel	EdgeLabel	TargetLabel	EdgeCount
Cve	affecting	Cve	4764
user	member of	user	1250
group	has role on	group	807
managedidentity	has permissions to	managedidentity	675
serviceprincipal	has permissions to	serviceprincipal	647
Microsoft Entra OAuth App	can authenticate as	Microsoft Entra OAuth App	214
managedidentity	has role on	managedidentity	105
group	member of	group	103
mdcSecurityRecommendation	affecting	mdcSecurityRecommendation	94
user	has permissions to	user	90
subscriptions	contains	subscriptions	78
resourcegroups	contains	resourcegroups	65
user	has role on	user	63
aadSecurityRecommendation	affecting	aadSecurityRecommendation	51
serviceprincipal	has role on	serviceprincipal	42

Demo 5:
Pick one asset and show its immediate neighbors

Show neighbors to a single asset (neighbors = identities, apps, findings, resources)

```
let assetSearch = "mgmt1.2linkit.local";
let Nodes = ExposureGraphNodes | project NodeId, NodeLabel, NodeName;
let Asset = Nodes | where NodeName has assetSearch | take 1;
let AssetId = toscalar(Asset | project NodeId);


ExposureGraphEdges
| where SourceNodeId == AssetId or TargetNodeId == AssetId
| extend NeighborId = iif(SourceNodeId == AssetId, TargetNodeId, SourceNodeId)
| join kind=leftouter (Nodes) on $left.NeighborId == $right.NodeId
| project AssetId, EdgeLabel, NeighborLabel=NodeLabel, NeighborName=NodeName, NeighborId
| order by NeighborLabel asc, NeighborName asc
```

Process:
1) Pick an asset name (or NodeId)
2) Get all edges where it's source or target
3) Join to nodes to show neighbor names/types

AssetId	EdgeLabel	NeighborLabel	NeighborName	NeighborId
7d4f6d2ec54b426ea	affecting	Cve	CVE-2026-25188	930771d7576244fca53bd545447781l4
7d4f6d2ec54b426ea	affecting	Cve	CVE-2026-25189	cacd4ecd686b4da785e30bc8e652662c
7d4f6d2ec54b426ea	affecting	Cve	CVE-2026-25190	7733441bef6c4b1bbe36897c3969a9d6
7d4f6d2ec54b426ea	affecting	Cve	CVE-2026-25926	4da106be14154c808548d2b8835c1e48
7d4f6d2ec54b426ea	affecting	Cve	CVE-2026-26111	3c0423f4f8b7470990969ddbb9a3488a
7d4f6d2ec54b426ea	affecting	Cve	CVE-2026-26128	1b5ace65cc67409a8094ed595452a3c0
7d4f6d2ec54b426ea	affecting	Cve	CVE-2026-26130	1c5cd19f3daa4641ac4034c0567ff4aa
7d4f6d2ec54b426ea	affecting	Cve	CVE-2026-26132	ec9673866975416dba9377bcfbc29064
7d4f6d2ec54b426ea	contains	azure-active-directory-user-credentials	1cf7e0aab6ac02f53037913631665a1	c525c8b0781a41759a40549cad44c47c
7d4f6d2ec54b426ea	contains	azure-database-connection-string	2dea1a426b0e0f029d00ecd5653670	7e0ea16a5b7948378b1066752e49d927
7d4f6d2ec54b426ea	contains	azure-storage-connection-string	419367600c6bb171e43c2acae0cc1bc	acec3f1aa73e4c338de46b1937621c7d
7d4f6d2ec54b426ea	contains	azure-storage-connection-string	609fce4dccdc9046f9baa8b14cd2896	8428e789d2ca4018be9c88a8226e7483
7d4f6d2ec54b426ea	contains	azure-storage-shared-access-signature	162cbca5843ab8132f7b0456117f155	64e1c467908a4ca092ddc13497b3fba6
7d4f6d2ec54b426ea	contains	azure-storage-shared-access-signature	34f1d038fa6012652d919f802a62ab2	138971078d534290ada3f1ecd4feadbd
7d4f6d2ec54b426ea	contains	azure-storage-shared-access-signature	7bbda8c3aac90af89db737ac43e0b92	b09b5e82db0d4211a34c1d555ec39fb8
7d4f6d2ec54b426ea	contains	azure-storage-shared-access-signature	f10b773933564c945da87ec7ef8dc57	c4cc64865ac84ddd9169a1dff84ca54e

Demo 6: Find all “finding” nodes and their affected assets

Show that findings are nodes and they connect to impacted assets via edges (often “affecting…”)

```
let Findings =
   ExposureGraphNodes
   | where tostring(Categories) has "finding"
   | project FindingNodeId=NodeId, FindingName=NodeName, FindingLabel=NodeLabel;

let Nodes = ExposureGraphNodes | project NodeId, NodeName, NodeLabel;

ExposureGraphEdges
| where tostring(EdgeLabel) has "affecting"
| join kind=inner (Findings) on $left.SourceNodeId == $right.FindingNodeId
| join kind=inner (Nodes) on $left.TargetNodeId == $right.NodeId
| summarize ImpactedAssets=dcount(NodeId) by FindingName, FindingLabel
| order by ImpactedAssets desc
```

Process:
1) Identify findings (Categories contains “finding”)
2) Join to edges labeled affecting
3) Join targets/sources to get impacted assets
4) Summarize counts

FindingName	FindingLabel	ImpactedAssets
SigninRiskPolicy	aadSecurityRecommendat	28
MfaRegistrationV2	aadSecurityRecommendat	15
CVE-2025-68160	Cve	14
CVE-2026-22795	Cve	14
CVE-2025-69419	Cve	14
CVE-2025-9230	Cve	14
CVE-2025-69420	Cve	14
CVE-2026-22796	Cve	14
CVE-2025-69421	Cve	14
CVE-2025-15467	Cve	14
CVE-2025-15468	Cve	13
CVE-2025-66199	Cve	13
CVE-2025-9231	Cve	13
CVE-2025-9232	Cve	12
CVE-2024-9143	Cve	10

Demo 7:
Internet exposure risk factor

Demonstrate that edges can carry risk metadata (riskLevel, riskFactors) - >
Risk is not just on a device, it’s on relationships !!

```
let Nodes = ExposureGraphNodes | project NodeId, NodeName, NodeLabel;


ExposureGraphEdges
| extend EdgeProps = column_ifexists("EdgeProperties", dynamic({}))
| extend RiskLevel = tostring(EdgeProps.rawData.risk.riskLevel)
| extend RiskFactors = tostring(EdgeProps.rawData.risk.riskFactors)
| where RiskFactors has "Exposure to the Internet" or tolower(RiskLevel) == "critical"
| join kind=leftouter (Nodes) on $left.SourceNodeId == $right.NodeId
| extend SourceName=NodeName, SourceLabel=NodeLabel
| join kind=leftouter (Nodes) on $left.TargetNodeId == $right.NodeId
| extend TargetName=NodeName, TargetLabel=NodeLabel
| project EdgeLabel, RiskLevel, RiskFactors, SourceLabel, SourceName, TargetLabel, TargetName
| order by RiskLevel desc
```

Process:
1) Start from edges
2) Pull EdgeProperties.rawData.risk.*
3) Filter on “Exposure to the Internet”
4) Show which assets are affected

Filters: Add filter

EdgeLabel	RiskLevel	RiskFactors	SourceLabel	SourceName	TargetLabel	TargetName
affecting	Medium	["Exposure to the Internet'	mdcSecurityRecommenda	[Enable if required] Storage accounts should	mdcSecurityRecommenda	[Enable if required] Storag
affecting	Medium	["Exposure to the Internet'	mdcSecurityRecommenda	Virtual machines and virtual machine scale s	mdcSecurityRecommenda	Virtual machines and virtu
affecting	Medium	["Exposure to the Internet'	mdcSecurityRecommenda	Windows virtual machines should enable Az	mdcSecurityRecommenda	Windows virtual machines
affecting	Medium	["Exposure to the Internet'	mdcSecurityRecommenda	Managed identity should be enabled on we	mdcSecurityRecommenda	Managed identity should b
affecting	Medium	["Exposure to the Internet'	mdcSecurityRecommenda	[Enable if required] Storage accounts should	mdcSecurityRecommenda	[Enable if required] Storag
affecting	Low	["Exposure to the Internet'	mdcSecurityRecommenda	[Enable if required] Microsoft Foundry resou	mdcSecurityRecommenda	[Enable if required] Micros
affecting	Low	["Exposure to the Internet'	mdcSecurityRecommenda	Microsoft Foundry resources should restrict	mdcSecurityRecommenda	Microsoft Foundry resourc
affecting	Low	["Exposure to the Internet'	mdcSecurityRecommenda	Access to storage accounts with firewall and	mdcSecurityRecommenda	Access to storage account
affecting	Low	["Exposure to the Internet'	mdcSecurityRecommenda	Microsoft Foundry resources should use Azu	mdcSecurityRecommenda	Microsoft Foundry resourc
affecting	Low	["Exposure to the Internet'	mdcSecurityRecommenda	Microsoft Foundry resources should use Azu	mdcSecurityRecommenda	Microsoft Foundry resourc
affecting	Low	["Exposure to the Internet'	mdcSecurityRecommenda	Storage accounts should restrict network ac	mdcSecurityRecommenda	Storage accounts should r
affecting	Low	["Exposure to the Internet'	mdcSecurityRecommenda	Microsoft Foundry resources should use Azu	mdcSecurityRecommenda	Microsoft Foundry resourc
affecting	Low	["Exposure to the Internet'	mdcAuditingRecommenda	Diagnostic logs in Microsoft Foundry resour	mdcAuditingRecommenda	Diagnostic logs in Microsc
affecting	Low	["Exposure to the Internet'	mdcAuditingRecommenda	Diagnostic logs in Microsoft Foundry resour	mdcAuditingRecommenda	Diagnostic logs in Microsc
affecting	Low	["Exposure to the Internet'	mdcAuditingRecommenda	Diagnostic logs in Microsoft Foundry resour	mdcAuditingRecommenda	Diagnostic logs in Microsc

Demo 8: Internet-facing assets

(Customer-facing)

Show how you can segment assets by business impact flags like customer-facing and then look at their top exposures.

```
let CustomerFacingAssets =
    ExposureGraphNodes
    | extend IsCustomerFacing = tobool(coalesce(NodeProperties.rawData.isCustomerFacing, NodeProperties.raw.isCustomerFacing))
    | where IsCustomerFacing == true
    | project AssetNodeId=NodeId, AssetName=NodeName, AssetLabel=NodeLabel;

let Nodes = ExposureGraphNodes | project NodeId, NodeName, NodeLabel;

ExposureGraphEdges
| extend EdgeProps = column_ifexists("EdgeProperties", dynamic({}))
| extend RiskLevel = tostring(EdgeProps.rawData.risk.riskLevel)
| join kind=inner (CustomerFacingAssets) on $left.SourceNodeId == $right.AssetNodeId
| join kind=leftouter (Nodes) on $left.TargetNodeId == $right.NodeId
| summarize EdgeCount=count(), CriticalEdges=countif(tolower(RiskLevel) in ("critical","very high"))
    by AssetName, AssetLabel, EdgeLabel, TargetLabel=NodeLabel
| order by CriticalEdges desc, EdgeCount desc
```

Process:
1) Filter nodes to assets where isCustomerFacing = true
2) Join to edges and risk metadata
3) Rank the “most risky customer-facing relationships”

AssetName	AssetLabel	EdgeLabel	TargetLabel	EdgeCount	CriticalEdges
dc1.2linkit.local	microsoft.compute/virtuali	contains	azure-app-configuration-k	5	0
mgmt1.2linkit.local	microsoft.compute/virtuali	contains	azure-storage-shared-acce	4	0
strv-mok-dt-03	device	contains	entra-userCookie	3	0
strv-acw-dt-03	device	contains	entra-userCookie	2	0
strv-mok-lt-06	device	has credentials of	user	2	0
strv-mok-lt-06	device	contains	entra-userCookie	2	0
mgmt1.2linkit.local	microsoft.compute/virtuali	contains	azure-storage-connection	2	0
dons-ekn-dt-01	device	contains	entra-userCookie	2	0
dc1.2linkit.local	microsoft.compute/virtuali	can authenticate as	managedidentity	1	0
dons-ekn-lt-02	device	has credentials of	user	1	0
dons-ekn-lt-02	device	frequently logged in by	user	1	0
dons-ekn-dt-01	device	has credentials of	user	1	0
mgmt1.2linkit.local	microsoft.compute/virtuali	contains	azure-database-connectio	1	0
strv-acw-dt-04	device	has credentials of	user	1	0
strv-acw-dt-04	device	frequently logged in by	user	1	0

Demo 9: Assets impacted by the same finding

Show shared exposure clusters: “this one finding impacts these assets”

```
let Nodes = ExposureGraphNodes | project NodeId, NodeName, NodeLabel, Categories;
let Findings =
    Nodes
    | where tostring(Categories) has "finding"
    | project FindingId=NodeId, FindingName=NodeName;

let Assets =
    Nodes
    | where NodeLabel !has "finding"
    | project AssetId=NodeId, AssetName=NodeName, AssetLabel=NodeLabel;

let AffectingEdges =
    ExposureGraphEdges
    | where tostring(EdgeLabel) has "affecting"
    | project SourceNodeId, TargetNodeId, EdgeLabel;

AffectingEdges
| join kind=inner (Findings) on $left.SourceNodeId == $right.FindingId
| join kind=inner (Assets) on $left.TargetNodeId == $right.AssetId
| summarize AssetCount=dcount(AssetId), ImpactedAssets=make_set(AssetName) by FindingName
| order by AssetCount desc
```

Filters: Add filter

FindingName	AssetCount	ImpactedAssets
SigninRiskPolicy	28	["LogicApp Connector Service Account, Azure WestEurope [DEMO]","svc-backup-keepit","F
MfaRegistrationV2	15	["LogicApp Connector Service Account, Azure WestEurope [DEMO]","Morten Knudsen (Ma
CVE-2025-69419	14	["strv-mew-lt-02","usami-tom-lt-01","strv-mok-lt-06","strv-mok-dt-03","tomsdesktop","doı
CVE-2025-69420	14	["strv-mew-lt-02","usami-tom-lt-01","strv-mok-lt-06","strv-mok-dt-03","tomsdesktop","doı
CVE-2025-69421	14	["strv-mew-lt-02","usami-tom-lt-01","strv-mok-lt-06","strv-mok-dt-03","tomsdesktop","doı
CVE-2025-15467	14	["strv-mew-lt-02","usami-tom-lt-01","strv-mok-lt-06","strv-mok-dt-03","tomsdesktop","doı
CVE-2025-68160	14	["strv-mew-lt-02","usami-tom-lt-01","strv-mok-lt-06","strv-mok-dt-03","tomsdesktop","doı
CVE-2026-22795	14	["strv-mew-lt-02","usami-tom-lt-01","strv-mok-lt-06","strv-mok-dt-03","tomsdesktop","doı
CVE-2025-9230	14	["strv-mew-lt-02","usami-tom-lt-01","strv-mok-lt-06","strv-mok-dt-03","tomsdesktop","doı
CVE-2026-22796	14	["strv-mew-lt-02","usami-tom-lt-01","strv-mok-lt-06","strv-mok-dt-03","tomsdesktop","doı
CVE-2025-66199	13	["strv-mew-lt-02","usami-tom-lt-01","strv-mok-lt-06","strv-mok-dt-03","tomsdesktop","doı
CVE-2025-9231	13	["strv-mew-lt-02","usami-tom-lt-01","strv-mok-lt-06","strv-mok-dt-03","tomsdesktop","doı

Demo 10:
Show all Edges for a specific user

Can Authenticate As
Can Authenticate To
Frequently Logged in By
Can Impersonate As
Has Role On
Has Credentials Of
MemberOf

```
let userUPN = "caroline@waltorp.dk";
let userNodeId =
    ExposureGraphNodes
    | where NodeLabel == "user"
    | extend p = todynamic(NodeProperties)
    | where tostring(p.rawData.accountUpn) =~ userUPN
    | project NodeId
    | take 1;


ExposureGraphEdges
| where SourceNodeId in (userNodeId) or TargetNodeId in (userNodeId)
| sort by EdgeLabel asc
```

EdgeLabel	SourceNodeId	SourceNodeName	SourceNodeLabel	SourceNodeCatego...	TargetNodeId	TargetNodeName	TargetNodeLabel	TargetNodeCategories
can authenticate as	29322e0919e64318a5a9f2	a5d6a2881db2ddfddf40e3	entra-userCookie	["cookies","secret"]	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","environmentCloud","identities","identity","user_account"]
can authenticate to	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","envi	69e43cfad61c4f9e883f0e4	strv-cew-lt-03	device	["compute","device","physical_device"]
can impersonate as	6a9d29318bf54dc199a61d	623256f8-5e9d-4b6e-a7bc	serviceprincipal	["application_identity","en	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","environmentCloud","identities","identity","user_account"]
can impersonate as	0a79d5f361894fe0aa7fa3a	468d666b-eb27-4702-936	serviceprincipal	["application_identity","en	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","environmentCloud","identities","identity","user_account"]
can impersonate as	095ecf84fcb7465ca94fdf9f	48c72940-ab0e-4ac6-b9fe	serviceprincipal	["application_identity","en	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","environmentCloud","identities","identity","user_account"]
can impersonate as	d71ea0af0773471ea2609f	e4d9397a-4581-4c4b-9dd	serviceprincipal	["application_identity","en	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","environmentCloud","identities","identity","user_account"]
can impersonate as	7c77123c5eb840f9ac3e78	7c0a0d12-af69-4102-a552	serviceprincipal	["application_identity","en	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","environmentCloud","identities","identity","user_account"]
frequently logged in by	69e43cfad61c4f9e883f0e4	strv-cew-lt-03	device	["compute","device","phys	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","environmentCloud","identities","identity","user_account"]
has credentials of	69e43cfad61c4f9e883f0e4	strv-cew-lt-03	device	["compute","device","phys	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","environmentCloud","identities","identity","user_account"]
has credentials of	83a9db5ed32246128507a	strv-mok-lt-06	device	["compute","device","phys	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","environmentCloud","identities","identity","user_account"]
has permissions to	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","envi	465e0127aac5495194cc83	Windows Azure Active Directory	Microsoft Entra OAuth App	["application_identity","identities","identity"]
has permissions to	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","envi	f66ecc7e3d2f434b9ae156	Office 365 Exchange Online	Microsoft Entra OAuth App	["application_identity","identities","identity"]
has permissions to	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","envi	0b9459787ce54d2c83a81	Microsoft Graph	Microsoft Entra OAuth App	["application_identity","identities","identity"]
has role on	5bc780aef54d4eb0a2a953	Enterprise Key Admins	group	["environmentAzure","envi	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","environmentCloud","identities","identity","user_account"]
has role on	762ad8b42cfe4db3bf64b2	Enterprise Admins	group	["environmentAzure","envi	6c932f8b47b24be28e9712	Caroline Waltorp	user	["environmentAzure","environmentCloud","identities","identity","user_account"]

Demo 11: Excluded assets hygiene check

Show governance: which assets are excluded, and what you might be missing because of it.

```
ExposureGraphNodes
| extend IsExcluded = tobool(coalesce(NodeProperties.rawData.isExcluded, NodeProperties.raw.isExcluded))
| where IsExcluded == true
| summarize ExcludedCount=count() by NodeLabel
| order by ExcludedCount desc
```

```
ExposureGraphNodes
| extend IsExcluded = tobool(coalesce(NodeProperties.rawData.isExcluded, NodeProperties.raw.isExcluded))
| extend NoderawData = todynamic(NodeProperties).rawData
| extend
   deviceManualTags  = iff(isnull(NoderawData.deviceManualTags),  dynamic([]), todynamic(NoderawData.deviceManualTags)),
   deviceDynamicTags = iff(isnull(NoderawData.deviceDynamicTags), dynamic([]), todynamic(NoderawData.deviceDynamicTags)),
   tags              = iff(isnull(NoderawData.tags.tags),       dynamic([]), todynamic(NoderawData.tags.tags))
| extend _AllTags = array_concat(array_concat(deviceManualTags, deviceDynamicTags), tags)
| extend AssetTags = strcat_array(_AllTags, ";")
| extend _TierTags = extract_all(@"([^;]*--tier[0-3]--SI[^;]*)", AssetTags)
| extend AssetTierByTag = strcat_array(array_sort_asc(coalesce(_TierTags, dynamic([]))), ";")
| extend NodeAssetTags = _AllTags
| where (AssetTags has "--Excluded--SI") or (IsExcluded == true)
```