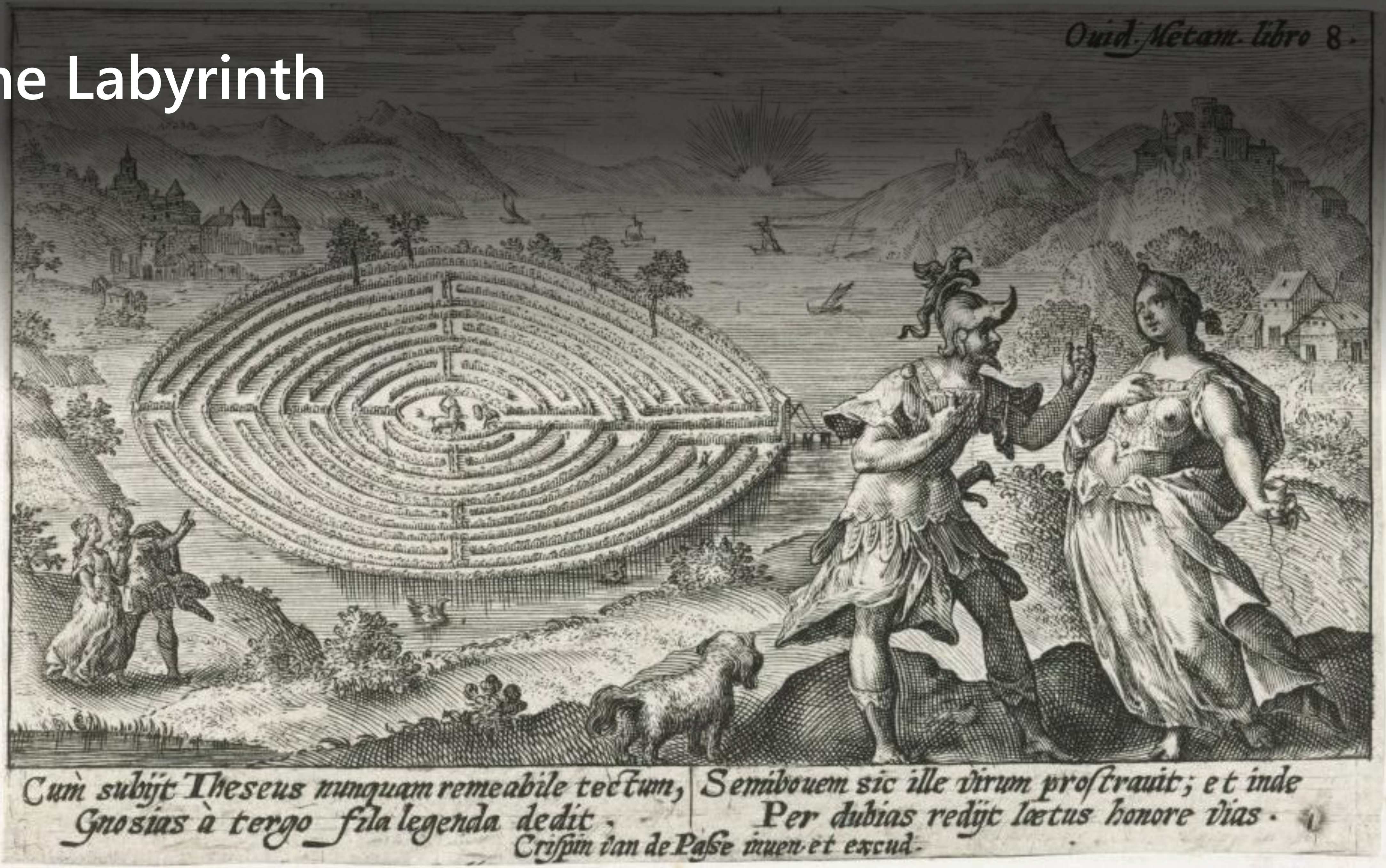
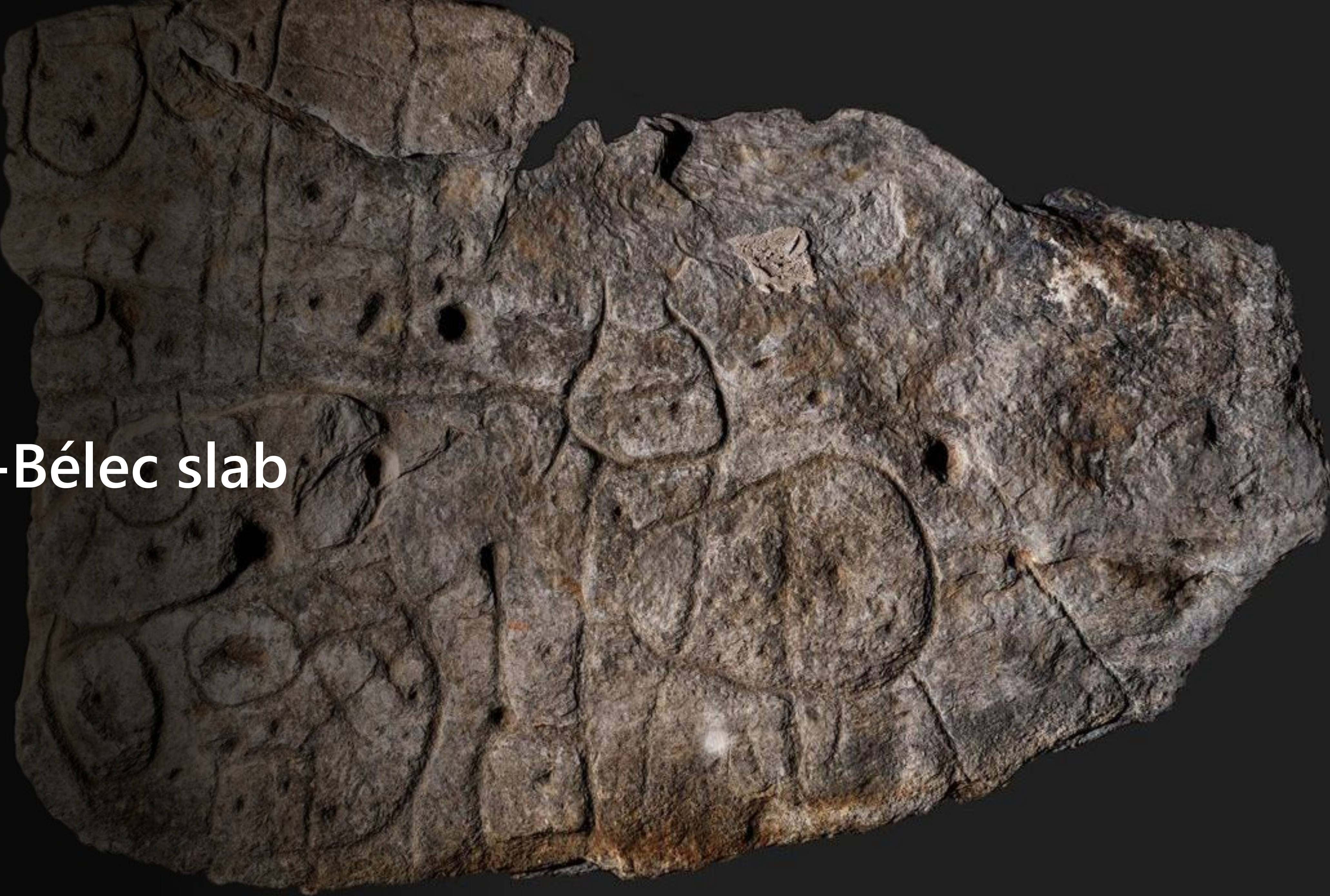
Microsoft Security

Light in the Labyrinth: Breach Path Analysis for Anyone

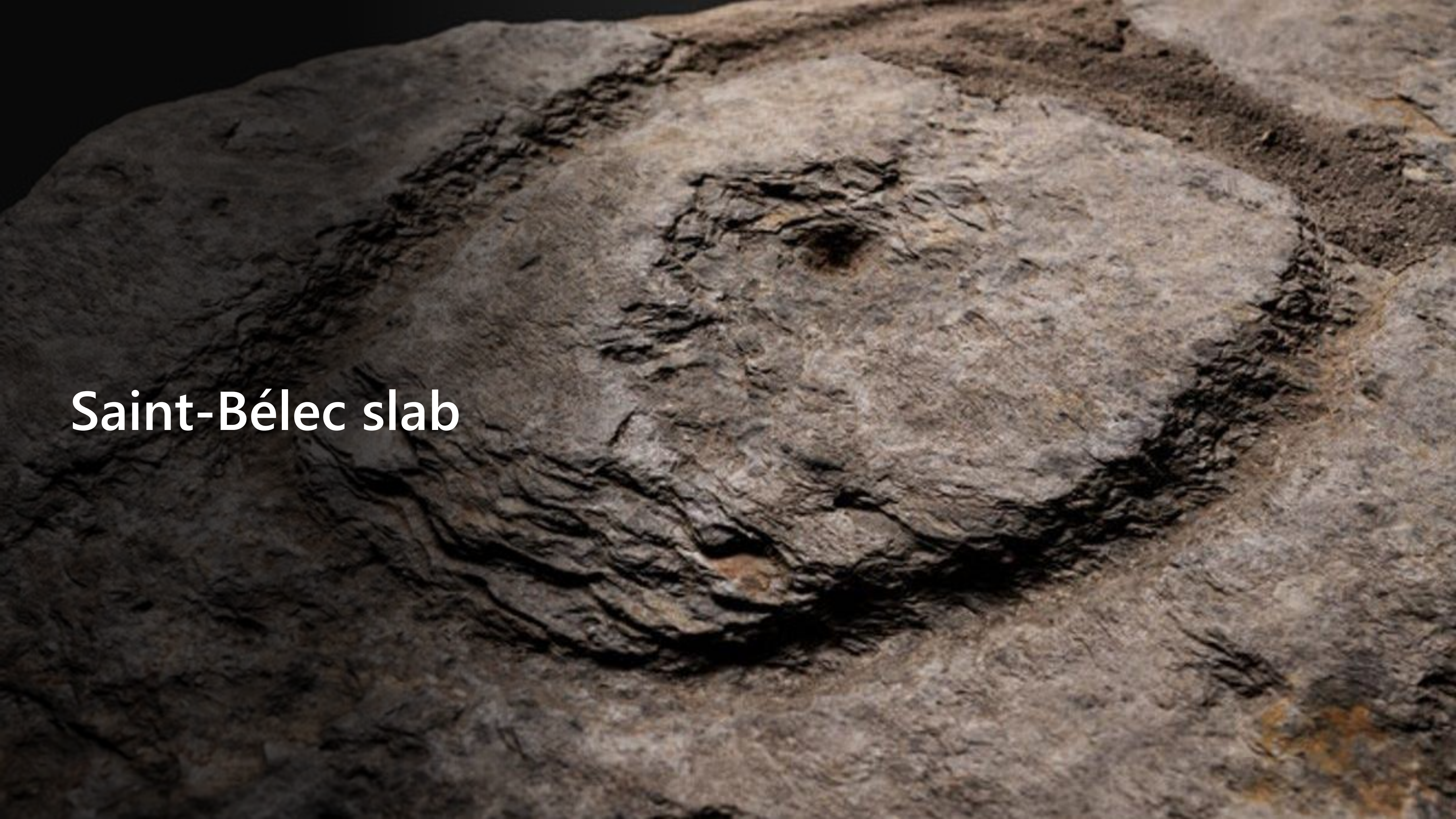
Parker Shelton

The Labyrinth


Ouid. Metam. libro 8.
Cum̀ subijt Theseus nunquam remeabile tectum,
Gnosias à tergo fila legenda dedit.
Semibouem sic ille virum proſtrauit; et inde
Per dubias redijt lætus honore vias.
Criſpin van de Paſſe inuen. et excud.



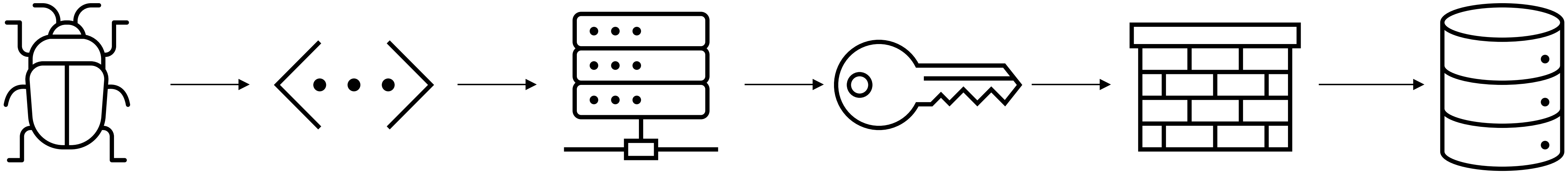
Saint-Bélec slab



Saint-Bélec slab

Universalis Cosmographia

Your Treasure Map



Your Treasure Map

You Need

Inventory

Have a program to collect inventory of users, assets, and permissions.

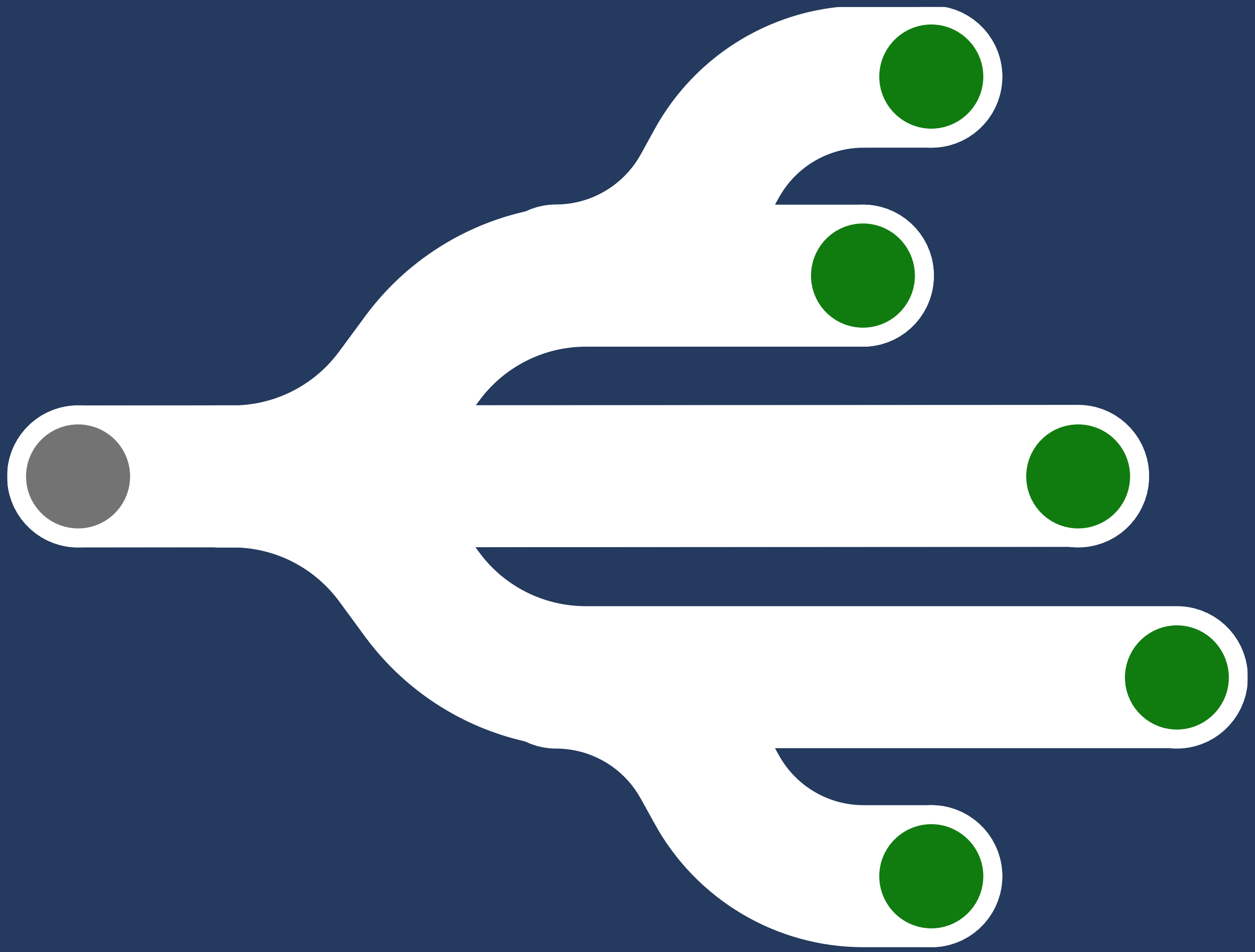
Topological Map

Know the terrain you're defending.

Attacker Mindset

Consider how assets are connected.

Breach Paths



What Are Breach Paths?

A **breach path** is a sequence of steps that a threat actor may use to infiltrate and compromise a network or a system or move laterally or elevate privileges.

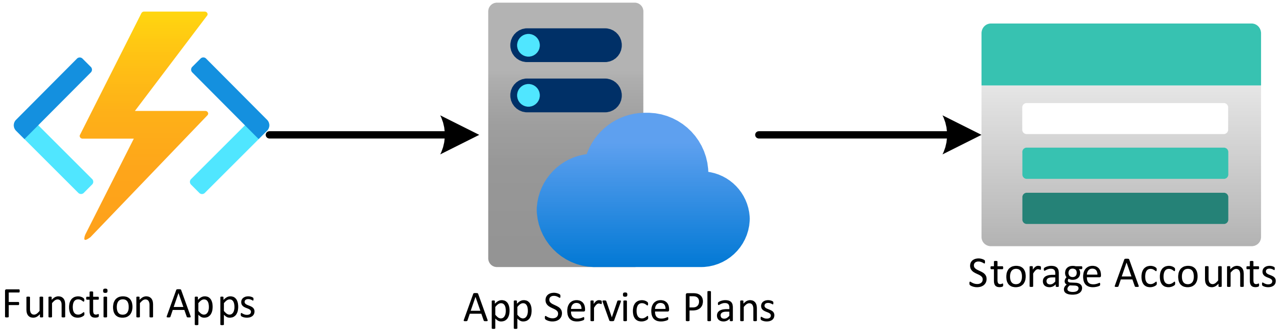
Breach path analysis is a technique to scan the graph of a network or system to identity possible breach paths.

Threat actors may move laterally within a network or elevate their privileges to gain access to critical systems. You want to know how before they do it.

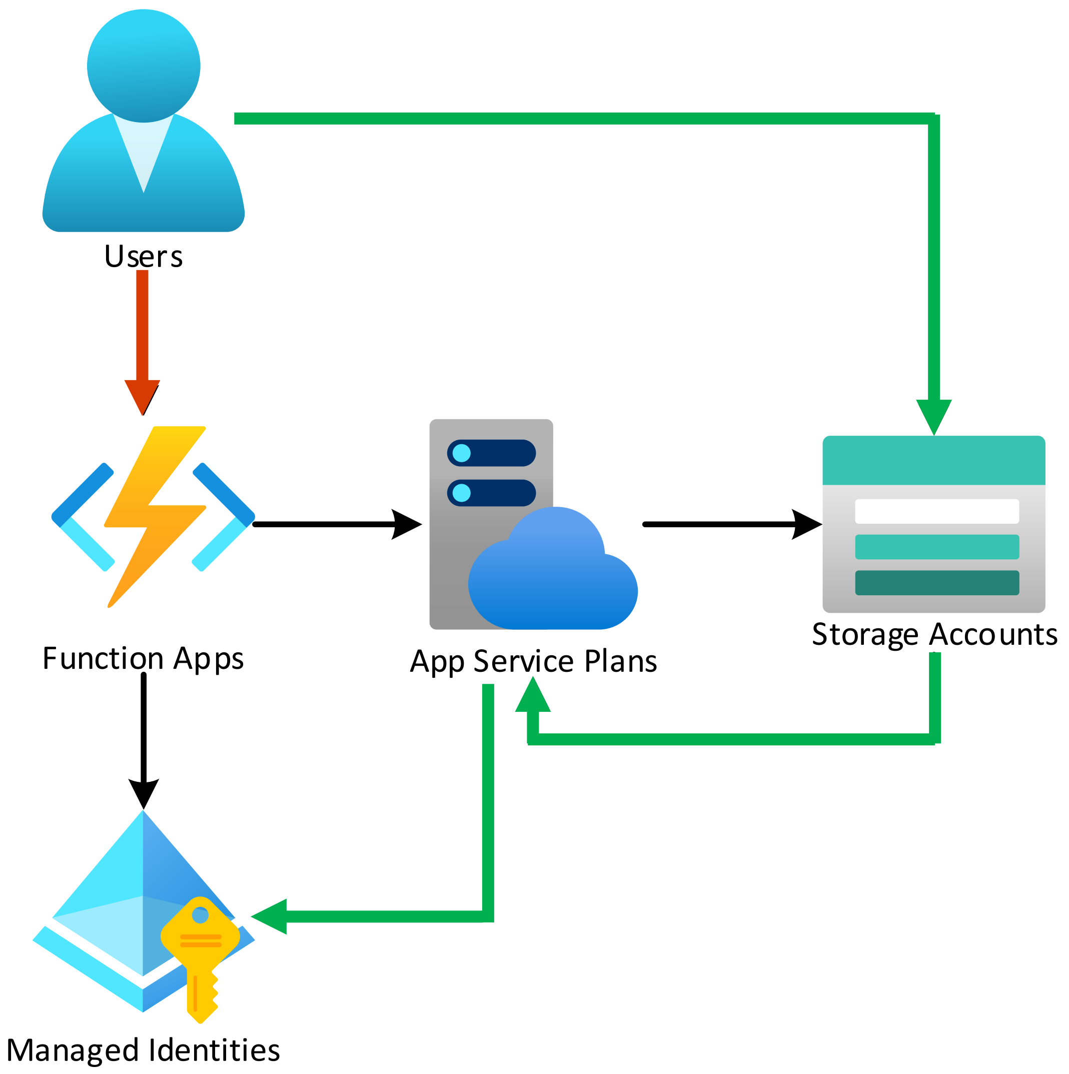
Breach Path: Storage Account Privilege Escalation

“Azure Functions use storage for several purposes. Azure Functions code may be stored in the account specified.”

“Important data, such as function code, access keys, and other important service-related data, can be persisted in the storage account. You must carefully manage access to the storage accounts used by function apps.”



Breach Path: Storage Account Privilege Escalation

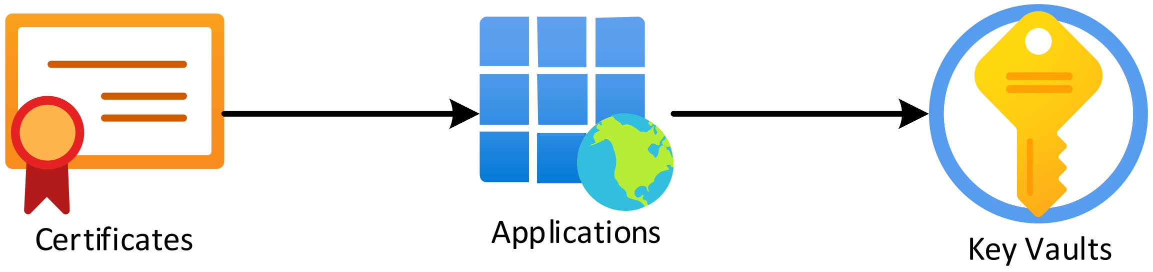


NetSPI's research highlighted the risks associated with write access to storage accounts in Azure, which can lead to **privilege escalation** on Azure App Services and Functions.

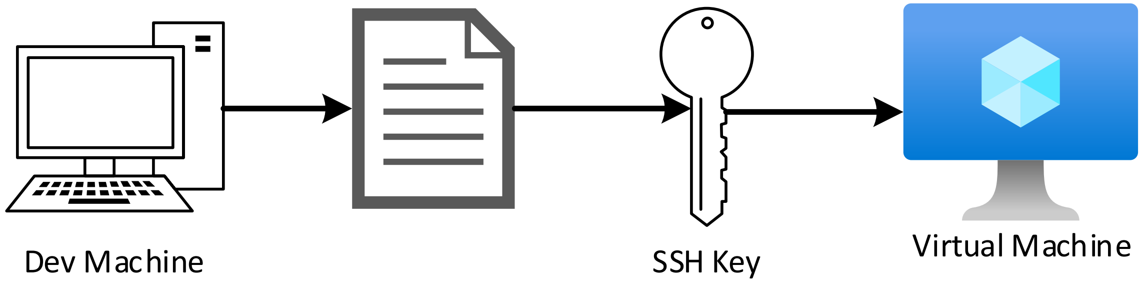
Compromising a storage account can lead to compromise of any identities associated with the Azure App Service.

Breach Path: Leaked Credentials

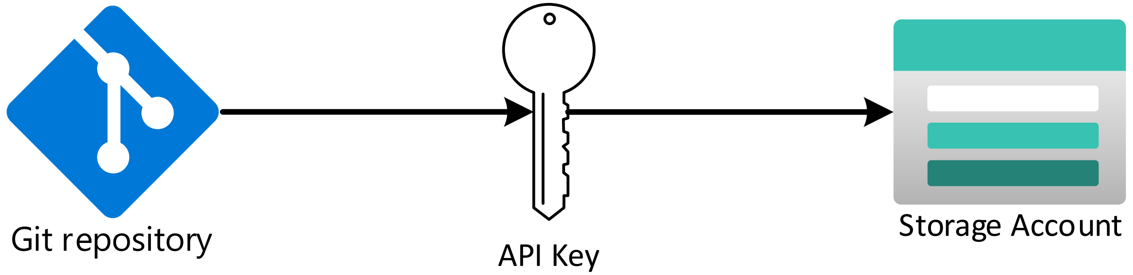
X509 client certificates on developer machines can lead to lateral movement and privilege escalation if a threat actor dumps other identity credentials in key management systems.



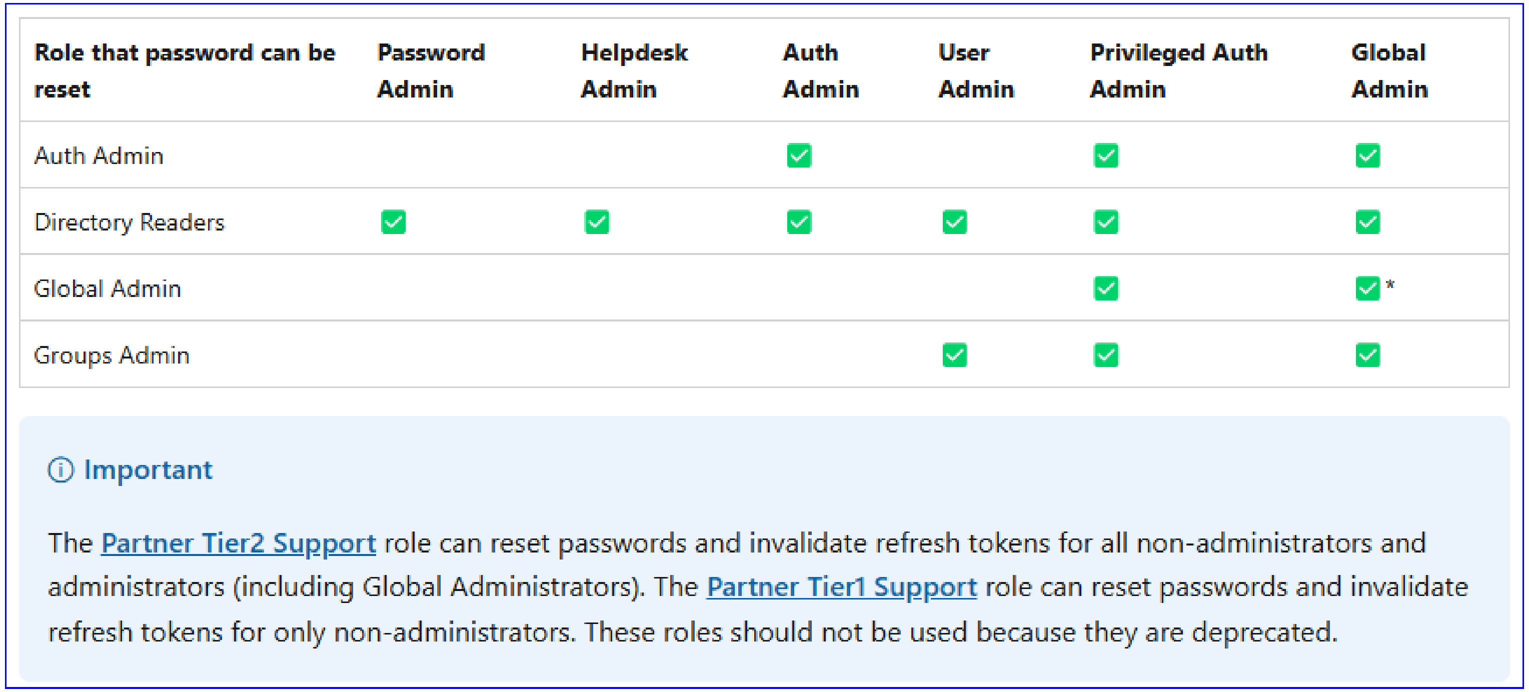
SSH keys stored on developer machines can grant access to cloud resources.



API keys checked into git repositories can grant access to cloud resources.



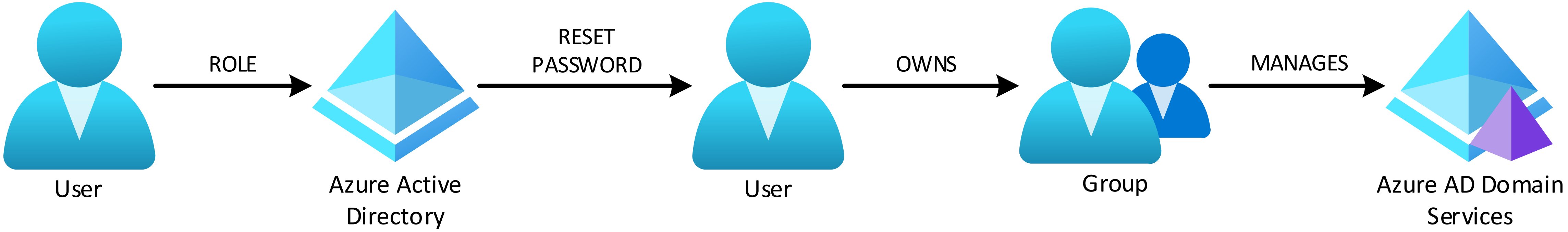
Breach Path: Entra Support Roles



Role that password can be reset	Password Admin	Helpdesk Admin	Auth Admin	User Admin	Privileged Auth Admin	Global Admin
Auth Admin			☑		☑	☑
Directory Readers	☑	☑	☑	☑	☑	☑
Global Admin					☑	☑*
Groups Admin				☑	☑	☑

ⓘ **Important**

The Partner Tier2 Support role can reset passwords and invalidate refresh tokens for all non-administrators and administrators (including Global Administrators). The Partner Tier1 Support role can reset passwords and invalidate refresh tokens for only non-administrators. These roles should not be used because they are deprecated.



User

ROLE

Azure Active Directory

RESET PASSWORD

User

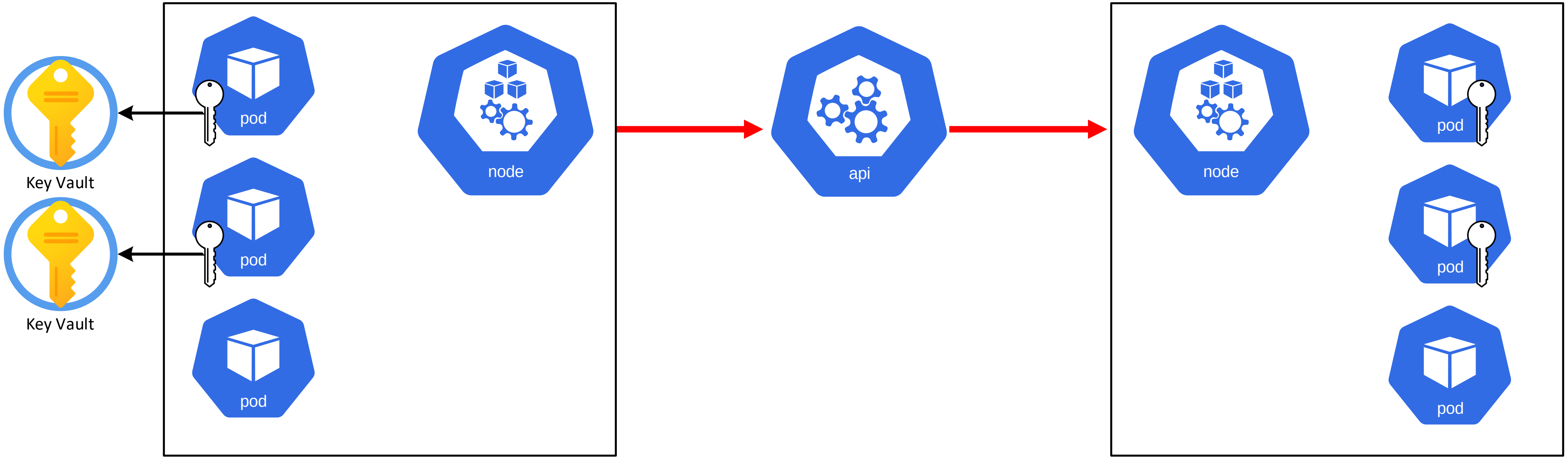
OWNS

Group

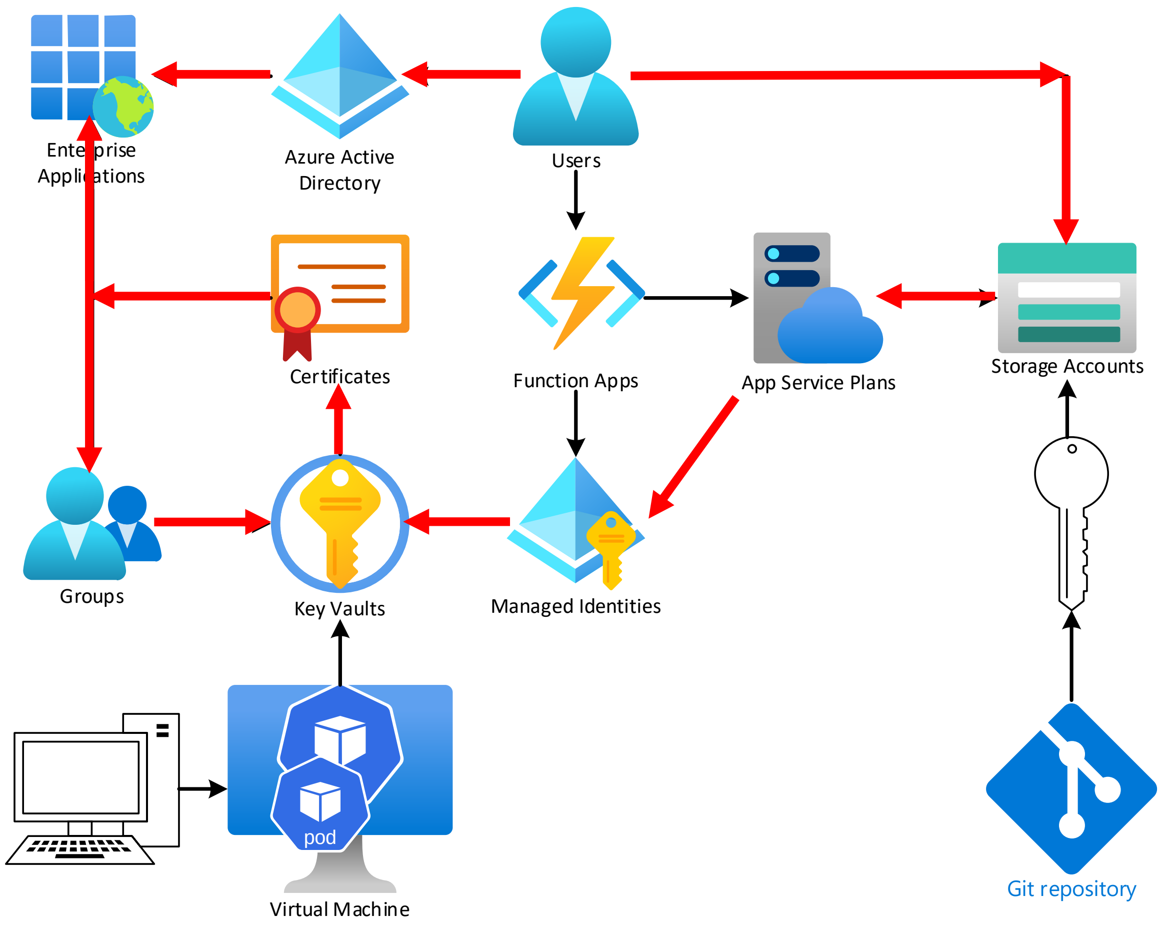
MANAGES

Azure AD Domain Services

Breach Path: Container Escapes



Paths Come Together In a Graph



Graphs visualize collections of paths.

This is the multiverse of possibilities, not actual threat actor activity.

Security graphs help **blue teams** detect security risks that need to be mitigated.

Security graphs help **red teams** understand where they are and the path to their objective.

Build or Buy a Graph?

Cloud Security Posture Management, Exposure Management, and Attack Path management tools exist!

You may have **unique business needs** such as proprietary services or solutions.

You may have **regulatory requirements** or security concerns limiting third-party access.

You can use the following engineer concepts to understand how some of these products work or evaluate vendor fit.

Architecting a Security Graph

Architecting a Security Graph

Inventory

Labels

Data Movement

Data Storage

Queries

UI

Computation

Architecting a Security Graph

Inventory

Labels

Data Movement

Data Storage

Queries

UI

Computation

You Need Inventory

Inventory

Cloud

Identity

Secrets

And More!

You Need Cloud Inventory

Inventory

Cloud

Identity

Secrets

And More!

You Need Identity Inventory

Inventory

Cloud

Identity

Secrets

And More!

You Need Secret Inventory

Inventory

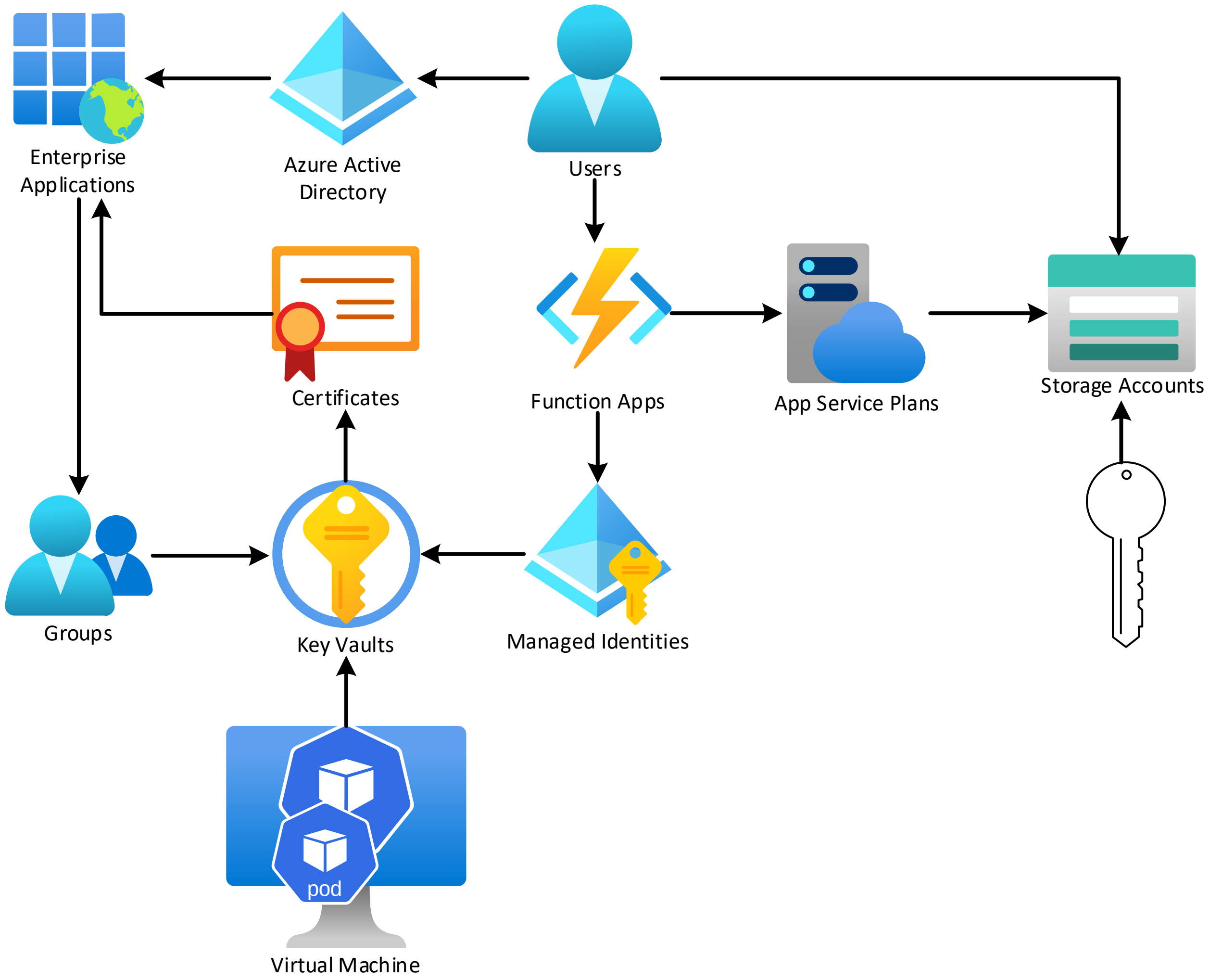
Cloud

Identity

Secrets

And More!

You Need Inventory



You (Probably) Need More Inventory

Inventory

Cloud

Identity

Secrets

And More!

Your Inventory Will Be Incomplete

All maps are wrong; some are useful.

Adversaries are not limited by how you **think** systems and objects are connected.

Maps get **better over time** through exploration. Don't let perfect be the enemy of good.

Architecting a Security Graph

Inventory

Labels

Data Movement

Data Storage

Queries

UI

Computation

You Need Labels

Graphs have nodes and edges that need labels. This is an **ontology**.

Triple = Subject – Verb – Object

The **Resource Description Framework** (RDF) gives subjects, predicates, and objects types and RDF Schema (RDFS) adds classes.

Web Ontology Language (OWL) adds semantics such as transitivity or equality of different relationships.

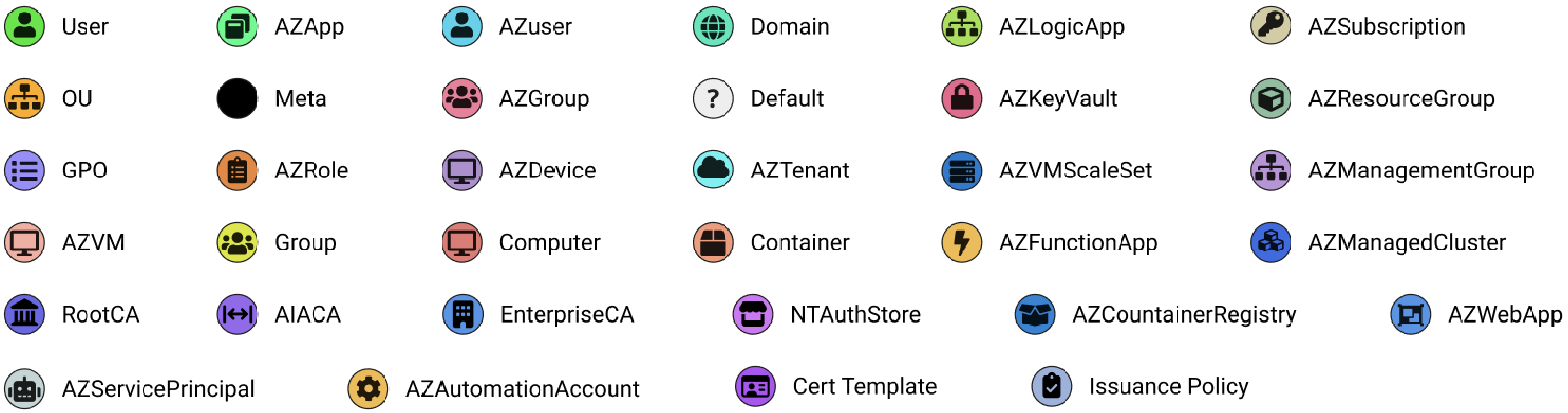
Subject	Predicate	Object
Alex	Pets	Buffalo
Buffalo	Eat	Grass
Buffalo	Buffalo	Buffalo

```
<rdf:Description about="http://contoso/book/1">
  <si:title>The Cat in the Hat</si:title>
  <si:author>Dr. Seuss</si:author>
</rdf:Description>
```

```
<owl:Class rdf:ID="WineGrape">
  <rdfs:subClassOf rdf:resource="&food;Grape" />
</owl:Class>
<WineGrape rdf:ID="CabernetSauvignonGrape" />
```

You Can Borrow An Ontology

Studying existing ontologies, like BloodHound, provides insight into effective graph models.



User AZApp AZuser Domain AZLogicApp AZSubscription

OU Meta AZGroup Default AZKeyVault AZResourceGroup

GPO AZRole AZDevice AZTenant AZVMScaleSet AZManagementGroup

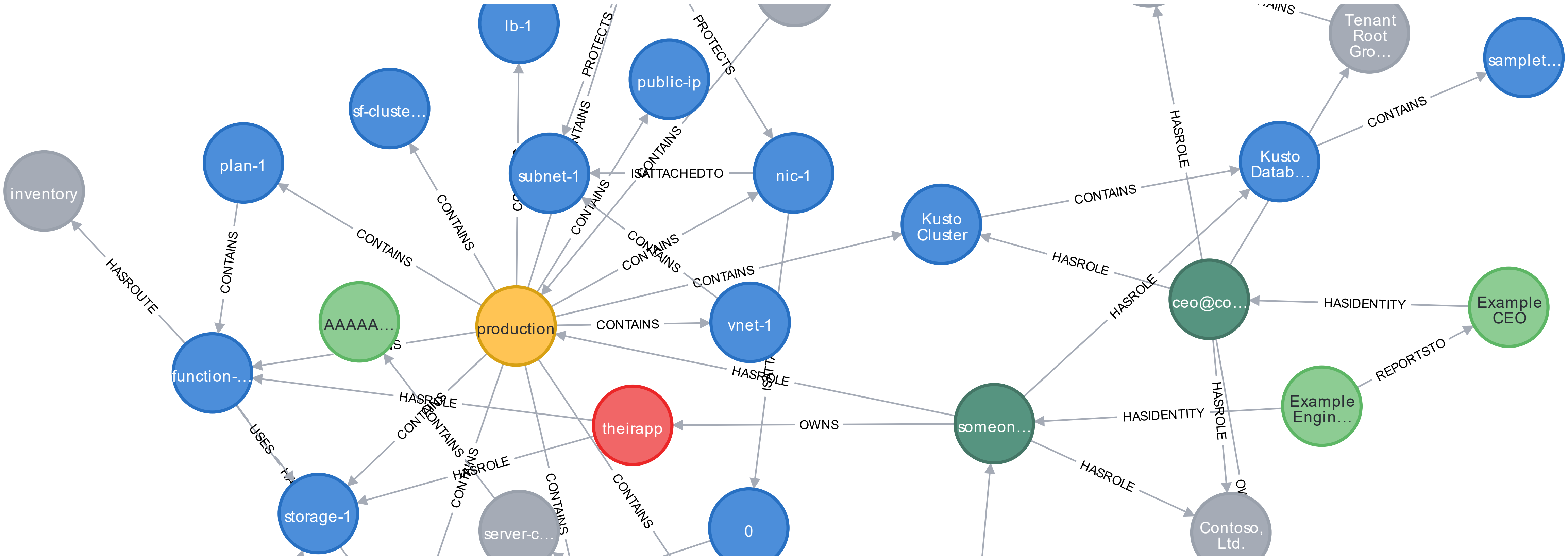
AZVM Group Computer Container AZFunctionApp AZManagedCluster

RootCA AIACA EnterpriseCA NTAuthStore AZCountainerRegistry AZWebApp

AZServicePrincipal AZAutomationAccount Cert Template Issuance Policy

We Have An Ontology You Could Explore

You can explore a sample ontology we've published inspired by our internal tooling at:
https://github.com/microsoft/security-graph-schemas



Architecting a Security Graph

Inventory

Labels

Data Movement

Data Storage

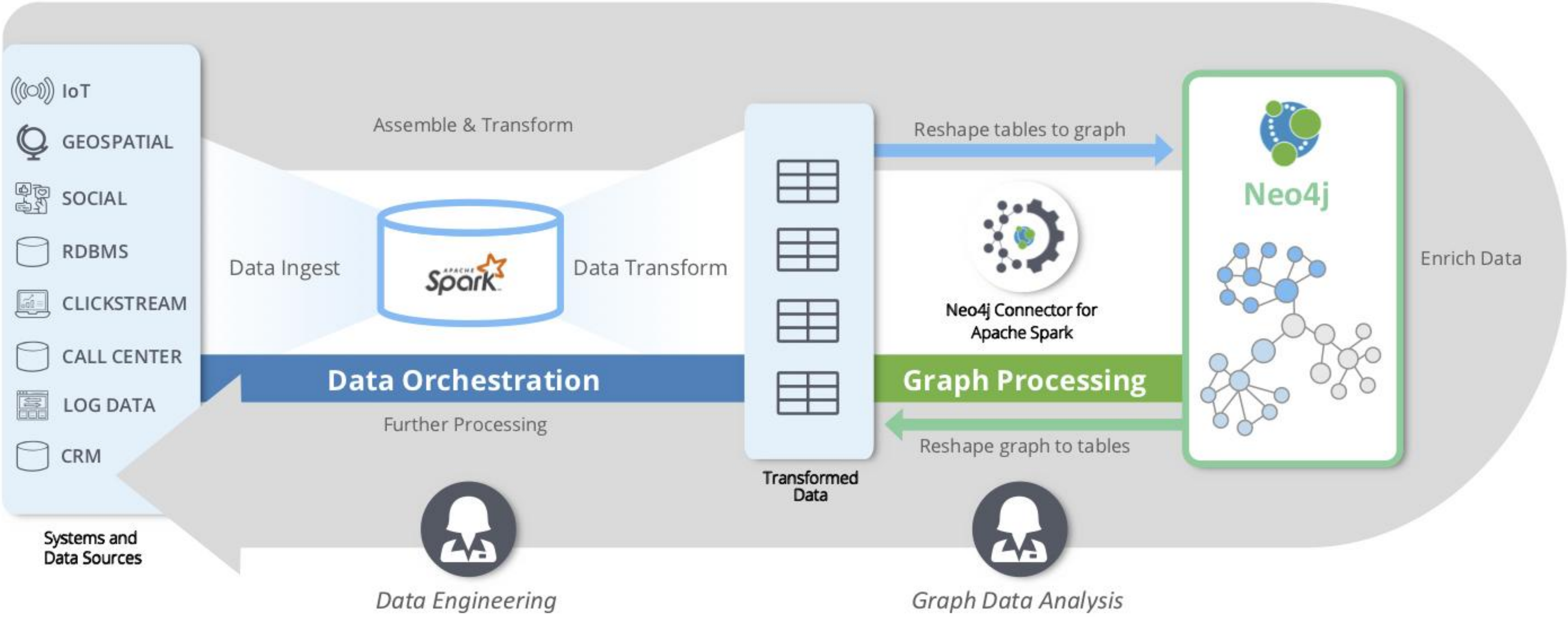
Queries

UI

Computation

You Need To Move Data Around

You need ETL processes to transform relational data into a graph-friendly triple representation.



Architecting a Security Graph

Inventory

Labels

Data Movement

Graph Storage

Queries

UI

Computation

You (May) Need Graph Storage

Your ETL processes could write nodes and edges into a relational database so you could fake traversals with joins.

Other tools can perform graph analytics on top of relational data.

Kusto Graph Operators

Kusto's new make-graph and graph-match operators can analyze relational data in graph form.

Gremlin on CosmosDB

Gremlin queries can now be executed against CosmosDB NoSQL data, enabling graph analytics.

Spanner Graph Capabilities

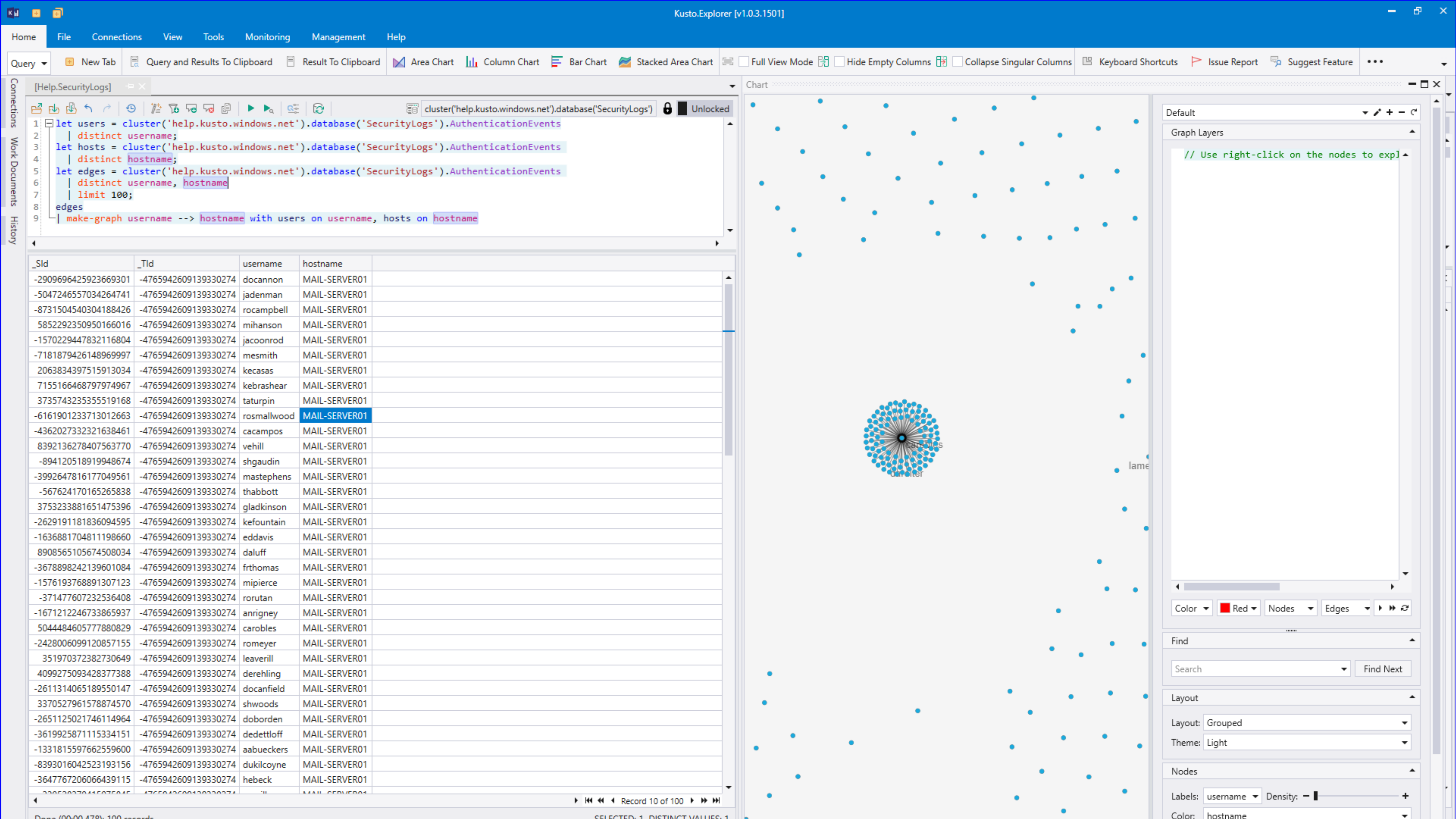
Spanner now supports Spanner Graph, allowing graph analytics on top of its relational database.

No ETL Solutions

Offerings like PuppyGraph reduce ETL with federated queries against diverse data stores.

Commercial Graph Databases

- Neo4J
- AWS Neptune
- TinkerPop
- TigerGraph
- Memgraph



cluster('help.kusto.windows.net').database('SecurityLogs')

```
let users = cluster('help.kusto.windows.net').database('SecurityLogs').AuthenticationEvents
   | distinct username;
let hosts = cluster('help.kusto.windows.net').database('SecurityLogs').AuthenticationEvents
   | distinct hostname;
let edges = cluster('help.kusto.windows.net').database('SecurityLogs').AuthenticationEvents
   | distinct username, hostname
   | limit 100;
edges
| make-graph username --> hostname with users on username, hosts on hostname
```

_SId	_TId	username	hostname
-2909696425923669301	-4765942609139330274	docannon	MAIL-SERVER01
-5047246557034264741	-4765942609139330274	jadenman	MAIL-SERVER01
-8731504540304188426	-4765942609139330274	rocampbell	MAIL-SERVER01
5852292350950166016	-4765942609139330274	mihanson	MAIL-SERVER01
-1570229447832116804	-4765942609139330274	jacoonrod	MAIL-SERVER01
-7181879426148969997	-4765942609139330274	mesmith	MAIL-SERVER01
2063834397515913034	-4765942609139330274	kecasas	MAIL-SERVER01
7155166468797974967	-4765942609139330274	kebrashear	MAIL-SERVER01
3735743235355519168	-4765942609139330274	taturpin	MAIL-SERVER01
-6161901233713012663	-4765942609139330274	rosmallwood	MAIL-SERVER01
-4362027332321638461	-4765942609139330274	cacampos	MAIL-SERVER01
8392136278407563770	-4765942609139330274	vehill	MAIL-SERVER01
-894120518919948674	-4765942609139330274	shgaudin	MAIL-SERVER01
-3992647816177049561	-4765942609139330274	mastephens	MAIL-SERVER01
-567624170165265838	-4765942609139330274	thabbott	MAIL-SERVER01
3753233881651475396	-4765942609139330274	gladkinson	MAIL-SERVER01
-2629191181836094595	-4765942609139330274	kefountain	MAIL-SERVER01
-1636881704811198660	-4765942609139330274	eddavis	MAIL-SERVER01
8908565105674508034	-4765942609139330274	daluff	MAIL-SERVER01
-3678898242139601084	-4765942609139330274	frthomas	MAIL-SERVER01
-1576193768891307123	-4765942609139330274	mipierce	MAIL-SERVER01
-371477607232536408	-4765942609139330274	rorutan	MAIL-SERVER01
-1671212246733865937	-4765942609139330274	anrigney	MAIL-SERVER01
5044484605777880829	-4765942609139330274	carobles	MAIL-SERVER01
-2428006099120857155	-4765942609139330274	romeyer	MAIL-SERVER01
351970372382730649	-4765942609139330274	leaverill	MAIL-SERVER01
4099275093428377388	-4765942609139330274	derehling	MAIL-SERVER01
-2611314065189550147	-4765942609139330274	docanfield	MAIL-SERVER01
3370527961578874570	-4765942609139330274	shwoods	MAIL-SERVER01
-2651125021746114964	-4765942609139330274	doborden	MAIL-SERVER01
-3619925871115334151	-4765942609139330274	dedettloff	MAIL-SERVER01
-1331815597662559600	-4765942609139330274	aabueckers	MAIL-SERVER01
-8393016042523193156	-4765942609139330274	dukilcoyne	MAIL-SERVER01
-3647767206066439115	-4765942609139330274	hebeck	MAIL-SERVER01

Record 10 of 100

Done (00:00.478): 100 records

SELECTED: 1, DISTINCT VALUES: 1

```
// Use right-click on the nodes to expl
```

Layout: Grouped

Theme: Light

Labels: username

Color: hostname

You (May) Need Graph Storage

Your ETL processes could write nodes and edges into a relational database so you could fake traversals with joins.

Other tools can perform graph analytics on top of relational data.

Kusto Graph Operators

Kusto's new make-graph and graph-match operators can analyze relational data in graph form.

Gremlin on CosmosDB

Gremlin queries can now be executed against CosmosDB NoSQL data, enabling graph analytics.

Spanner Graph Capabilities

Spanner now supports Spanner Graph, allowing graph analytics on top of its relational database.

No ETL Solutions

Offerings like PuppyGraph reduce ETL with federated queries against diverse data stores.

Commercial/OSS Graph Databases

- Neo4J
- AWS Neptune
- TinkerPop
- TigerGraph
- Memgraph

Architecting a Security Graph

Inventory

Labels

Data Movement

Graph Storage

Queries

UI

Computation

You Need Graph Queries

Cypher

Proprietary query language from Neo4j.

OpenCypher

Open-source language specification adopted by multiple vendors.

GQL

ISO standard language specification completed in 2024.

Gremlin

Functional data-flow language under the Apache umbrella.

GQL

```
GRAPH Entra
MATCH (g:Group {impact: "high")-[:Contains]->(u:User {intern: TRUE})
RETURN g.name, COUNT(*) AS num_interns
ORDER BY num_interns
```

Gremlin

```
entra.V('impact','high').outE('contains').inV().has('intern',true).name
```

Architecting a Security Graph

Inventory

Labels

Data Movement

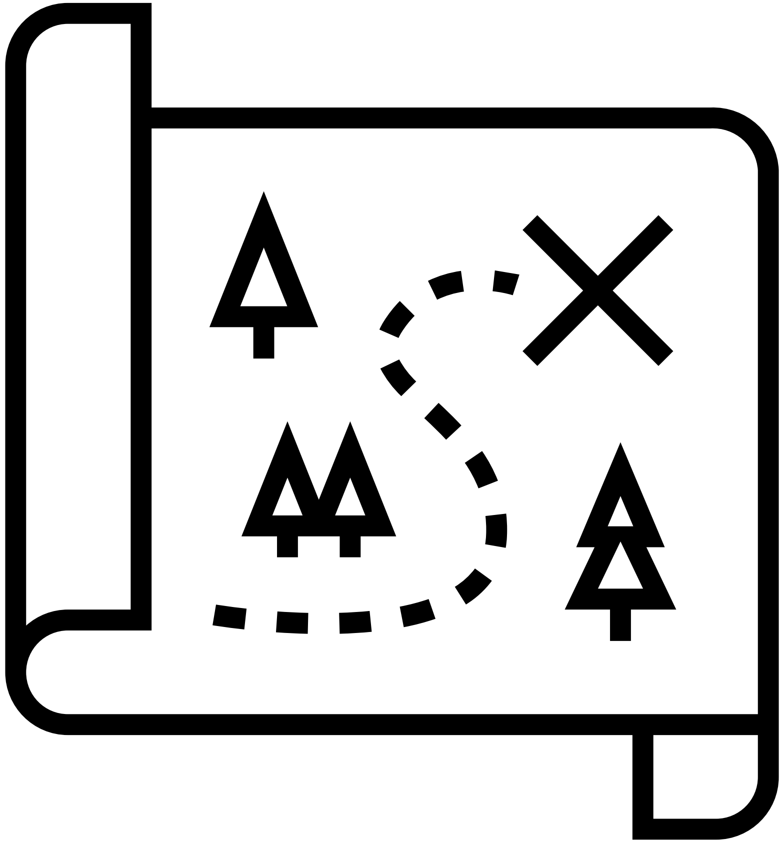
Graph Storage

Queries

UI

Computation

You Need a Graph UI



Explore the effectiveness of your queries.

Render **pictures** from your queries for effective risk communication with leadership.

Support the **red team**, helping them understand the next set of steps to take to compromise a target.

Architecting a Security Graph

Inventory

Labels

Data Movement

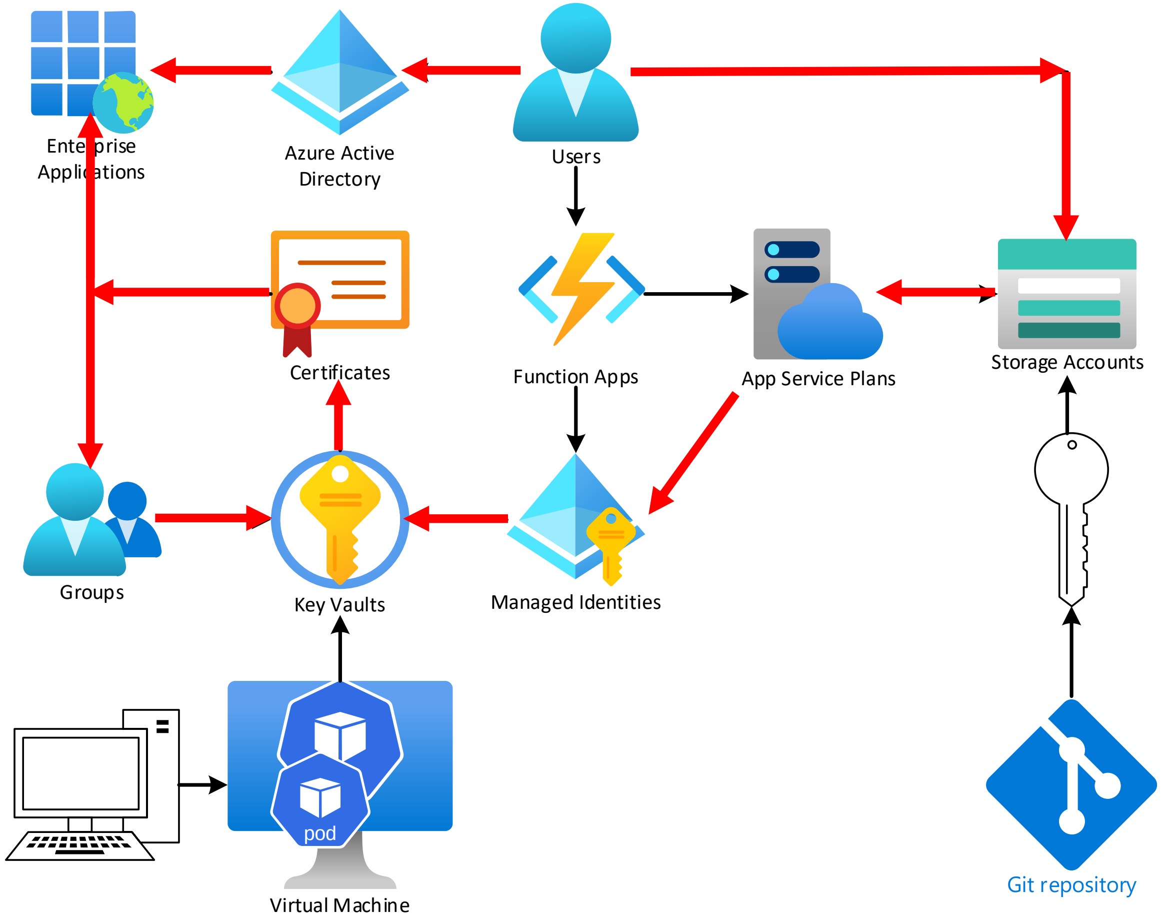
Graph Storage

Queries

UI

Computation

You Need Graph Computation



Reuse the same ETL process you picked earlier to continuously analyze the graph.

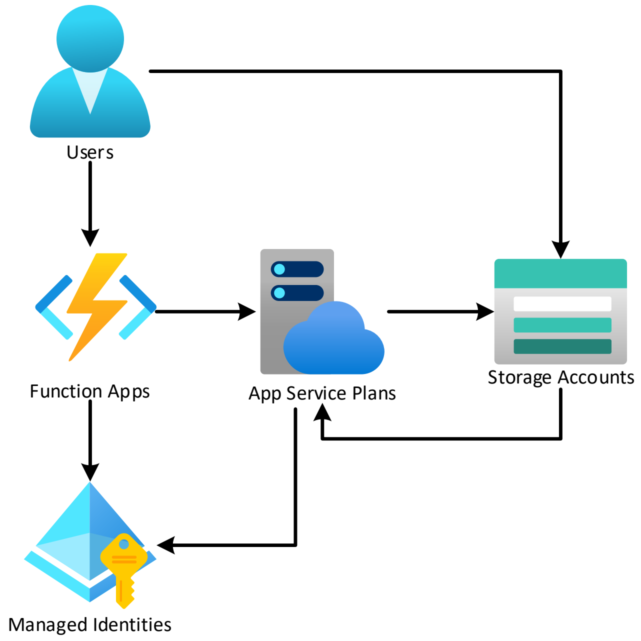
Encode Tactics, Techniques, and Procedures (TTPs) as **query fragments**.

Combine query fragments to create breach path queries to discover risks.

Store results for historical trending.

This supports **blue team** risk identification and risk mitigation.

Finding Vulns With Graphs



Graph Nodes and Edges:

1. (:USER)-[:HASROLE]->(:STORAGEACCOUNT)
2. (:FUNCTIONAPP)-[:USES]->(:STORAGEACCOUNT)
3. (:FUNCTIONAPP)-[:HASIDENTITY]->(:AADOBJECT)
4. (:AADOBJECT)-[:HASROLE]->(:KEYVAULT)

Fragments:

1. MATCH (u:USER)-[:HASROLE {role: “write”}]->(s:STORAGEACCOUNT)<-[:USES]-(f:FUNCTIONAPP)-[:HASIDENTITY]->(:AADOBJECT)
   WHERE NOT EXISTS ((u)-[:HASROLE {role: “write”}]->(f))
2. MATCH (: AADOBJECT) –[:HASROLE role: “write”}]->(:KEYVAULT)

Additional Work

BSides Seattle 2025

How Attackers (or Red Teamers) Navigate Azure Using Key Vault Lateral Movement

Christiano Bianchet

Microsoft Red Team

BSides Dublin 2025

One Bug, Two Bug, Red Bug, Blue Bug

Lea Snyder and Patrick Fitzgerald

Microsoft Entra

Your Treasure Map

You Need

Inventory

Have a program to collect inventory of users, assets, and permissions.

Topological Map

Know the terrain you’re defending.

Attacker Mindset

Consider how assets are connected.

Microsoft Security

Light in the Labyrinth: Breach Path Analysis for Anyone

Parker Shelton

Credits

“Theseus and Ariadne in front of the labyrinth (Metamorphoses)” by Crispijn de Passe the Elder via The Rijksmuseum, Netherlands

Saint Belec Slab © Denis Gliksman, Inrap. Licensed under https://creativecommons.org/licenses/by-nc-nd/4.0/deed.fr

Waldseemuller map 2 - Waldseemüller map via Wikipedia (Public Domain)

“A flat black and white vector icon of a map where part of the terrain is covered by a dark cloud representing fog of war” by Bing Designer

Introducing the Neo4j Connector for Apache Spark via Neo4j