SwissMicrosoft SECURITY SUMMIT

Common Azure Attacks and Detection Strategies with Microsoft Defender XDR

Complete Research Process

Deniz MUTLU

SwissMicrosoft SECURITY SUMMIT

Hello & Welcome!

My name is Deniz Mutlu

Microsoft Security MVP & MCT

Work At : @ Swiss Post Cybersecurity (Hacknowledge)

Fancy Title : Director Strategic Partner Mgmt | Senior Security Engineer

https://linkedin.com/in/dmutlu

SwissMicrosoft
SECURITY SUMMIT

Thank you to the Sponsors

scopewyse
we are what's next

Ontinue

INGRAM MICRO

EPIC FUSION
BRING IT ALL TOGETHER

Microsoft

water
IT Security & Defense

GRABX

Swiss Post Cybersecurity

techtask

iC CONSULT

Mediawerk

SwissMicrosoft SECURITY SUMMIT

Program of today

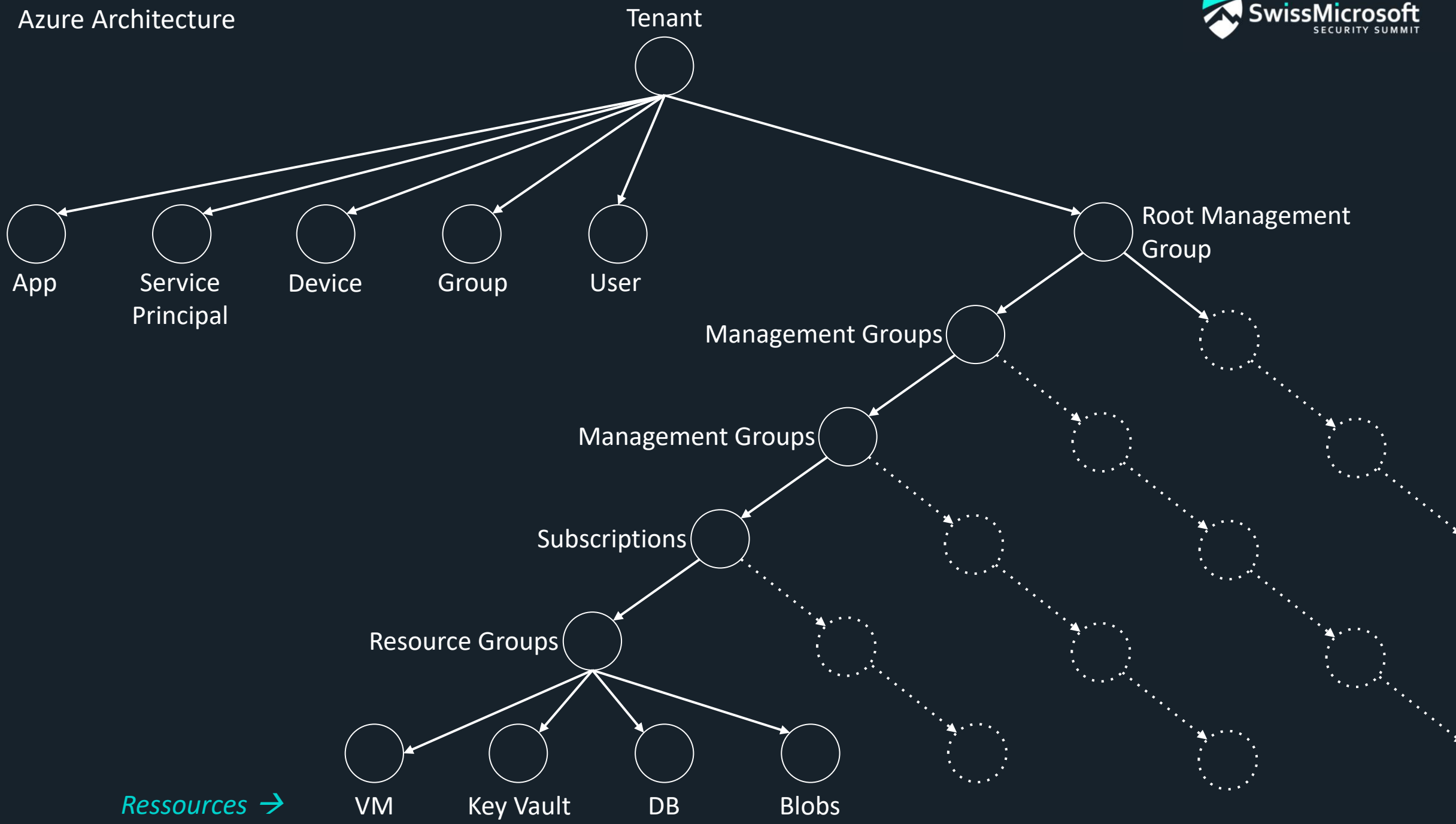
- Introduction
- Azure Fundamentals
- Research process
- Azure Kill Chain & tools for attacks
- Best approach for Detection
- Conclusion

Introduction of Azure Attacks

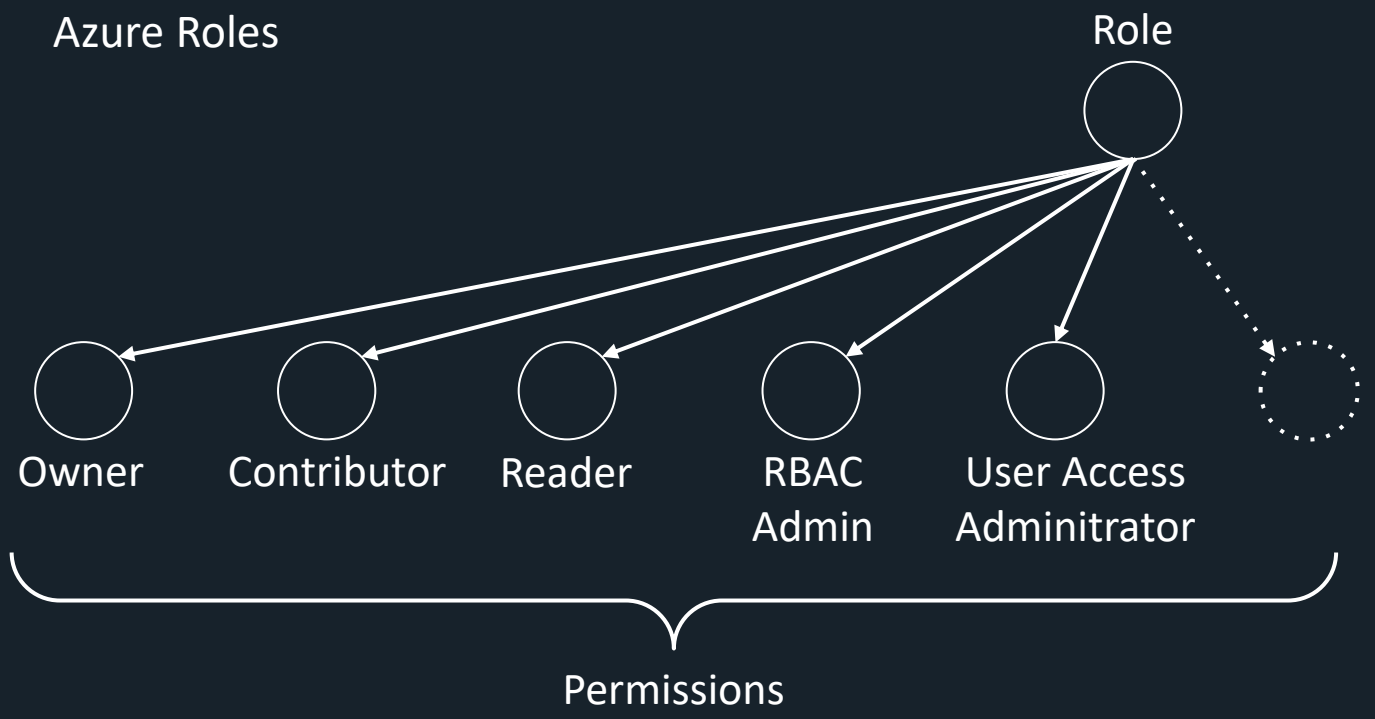
- Microsoft claims 95% of the Fortune 500 companies with Azure*
- Azure has more than 200 products and cloud services*
- New Era of Attacks focusing Azure (AI will help)
- Microsoft said “Think Graph!” (BloodHound also)

*What is Azure—Microsoft Cloud Services | Microsoft Azure

Azure Architecture

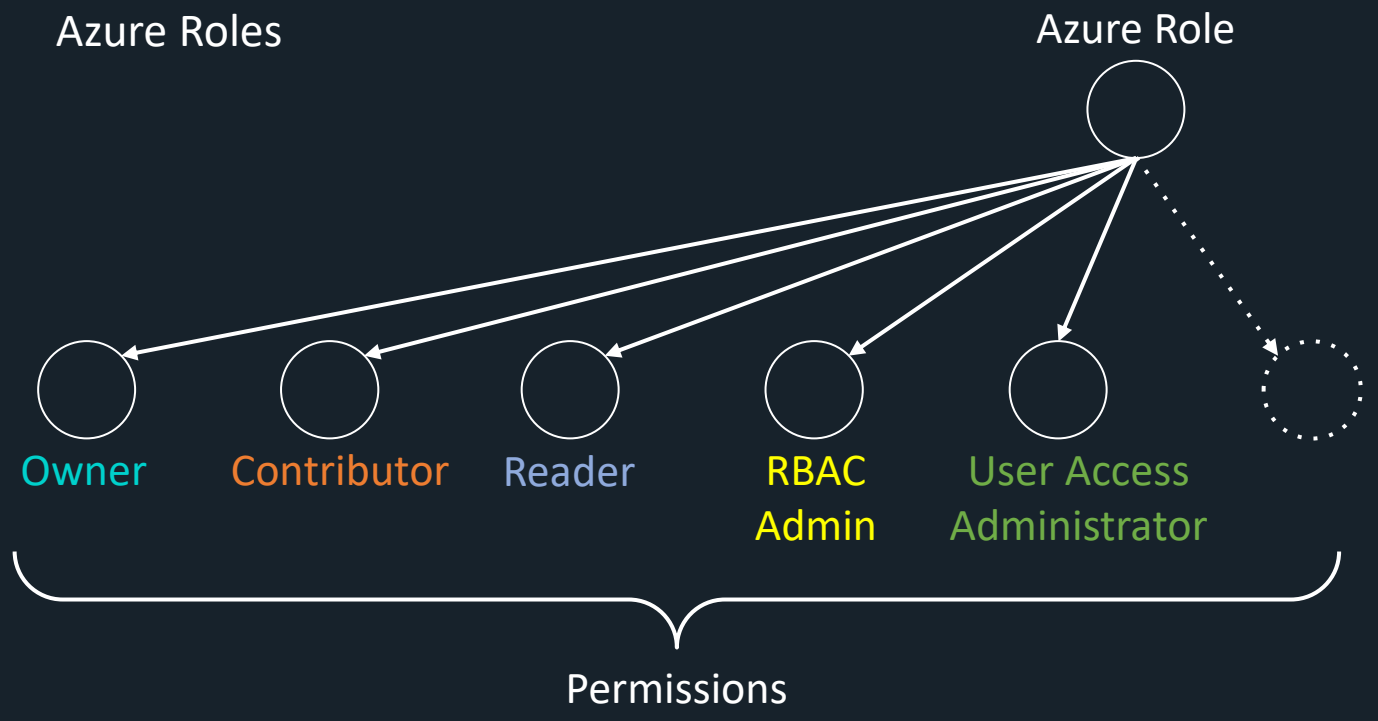


Azure Roles



- *Full access to all resources*
- *Can manage access for other users*
- *View all resources*
- *Can manage access for other users*
- *Can’t manage access using Azure Policy*
- *View all resources*
- *Can Manage access for other users*

Azure Roles



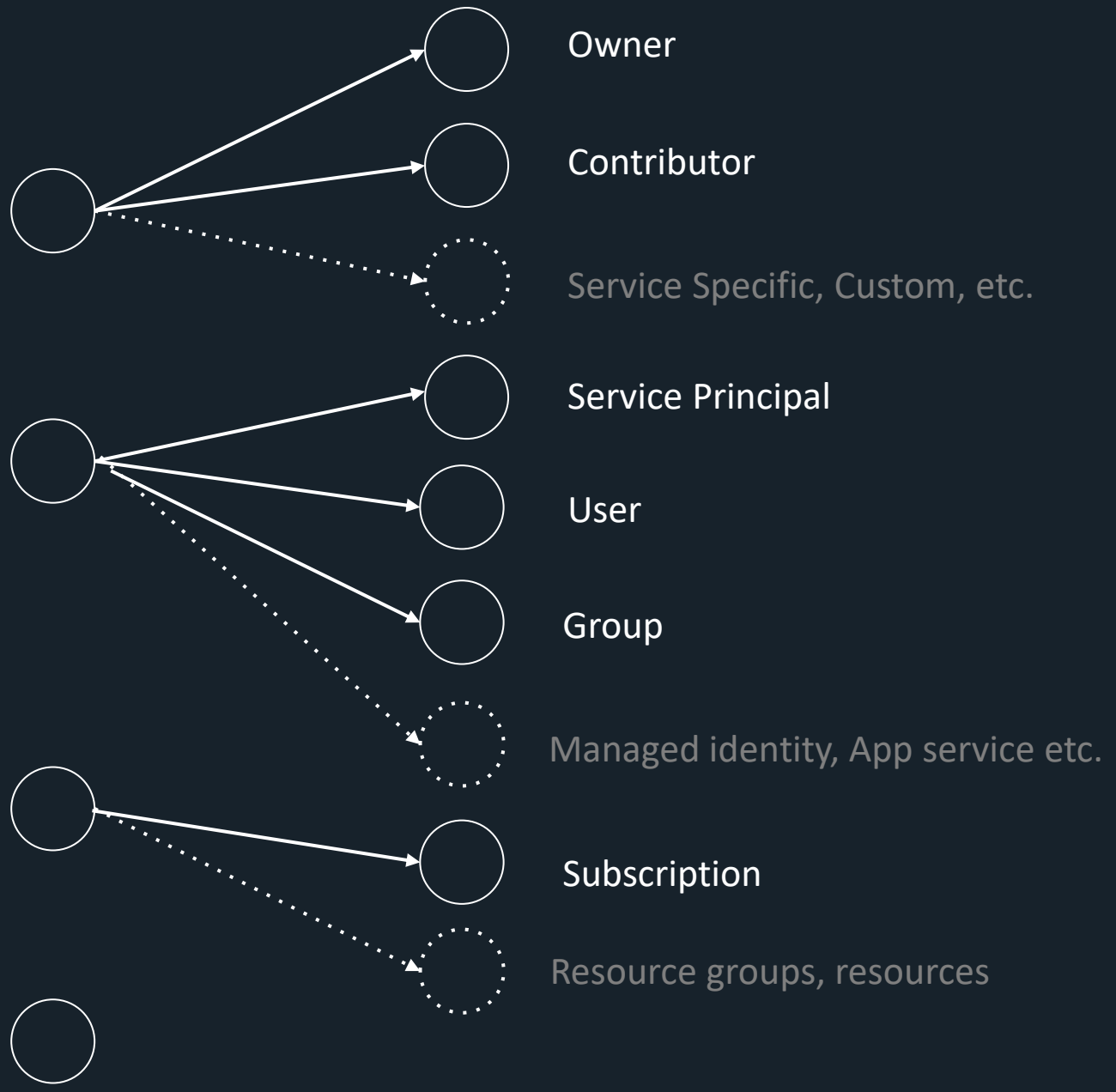
- *Full access to all resources*
- *Can manage access for other users*
- *Full access to all ressources*
- *Cannot manage access*
- *View all resources*
- *Can manage access for other users*
- *Can't manage access using Azure Policy*
- *View all resources*
- *Can Manage access for other users*

Applies to "All resource types"

Azure RBAC has over 120 built-on roles, +400 roles on Azure services, and you can create your own custom roles

List Azure role definitions - Azure RBAC | Microsoft Learn

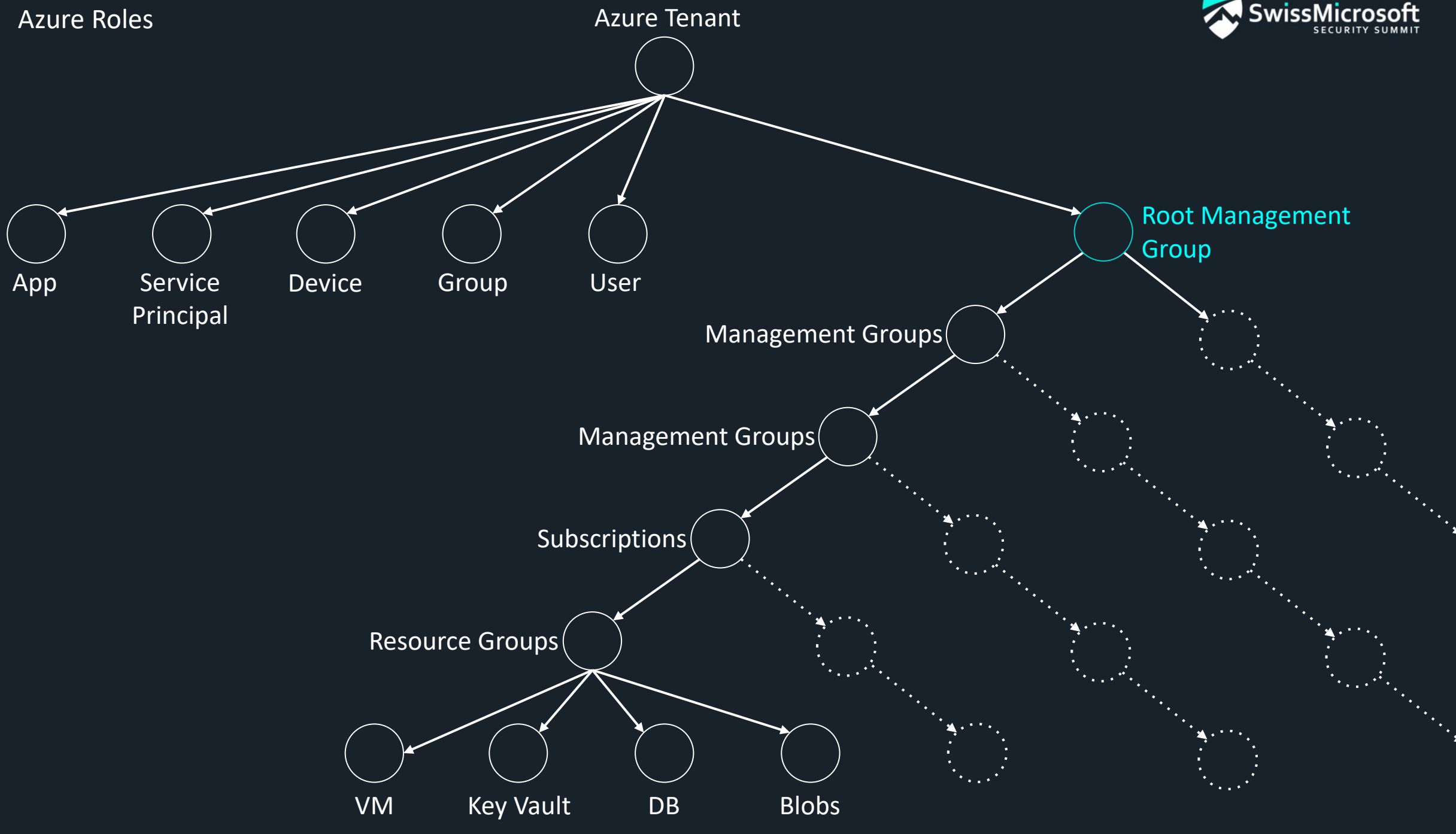
Azure Roles


Role
Owner
Contributor
Service Specific, Custom, etc.
Type
Service Principal
User
Group
Managed identity, App service etc.
Scope
Subscription
Resource groups, resources
Condition

SwissMicrosoft
SECURITY SUMMIT

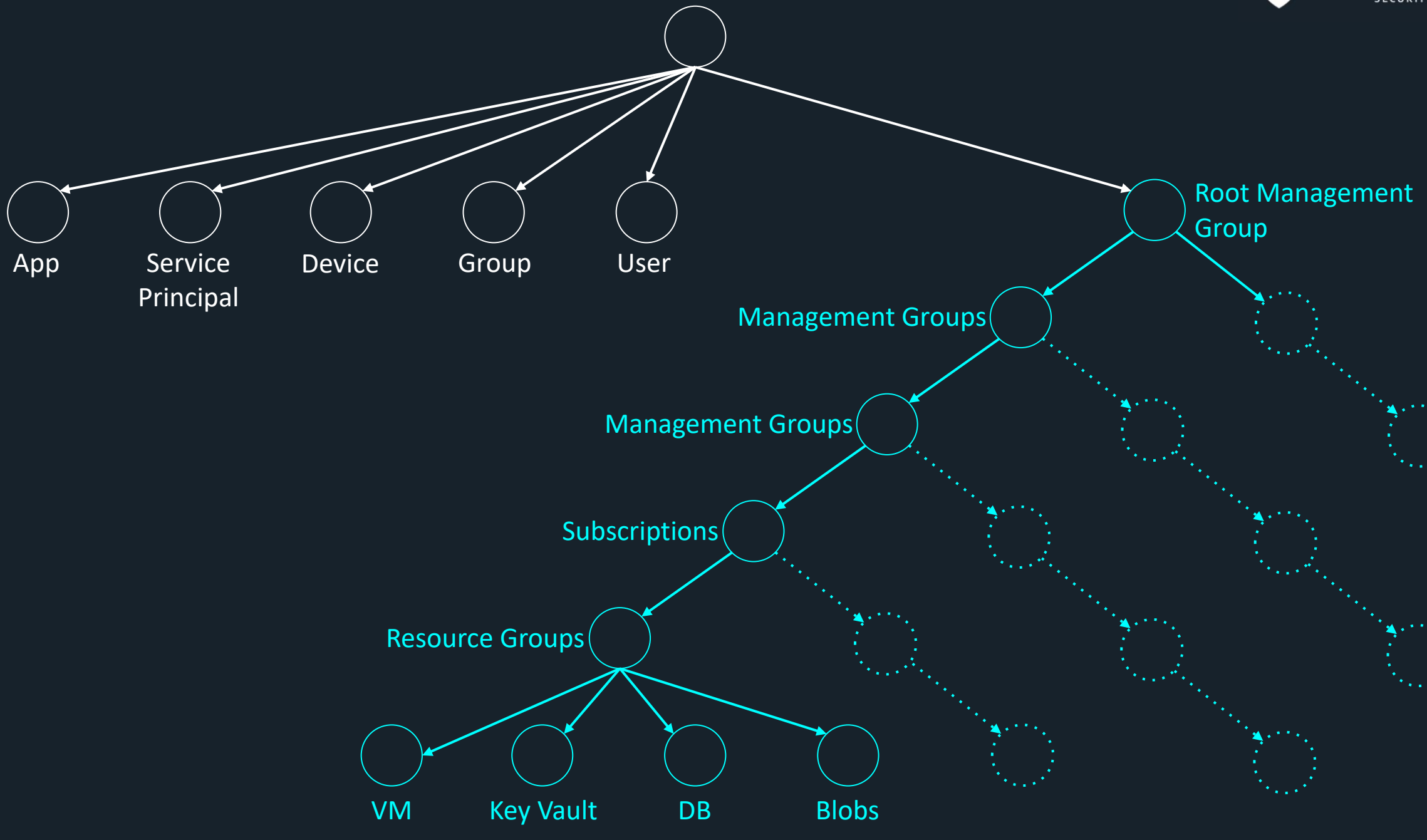
Screenshot Azure Roles

Azure Roles

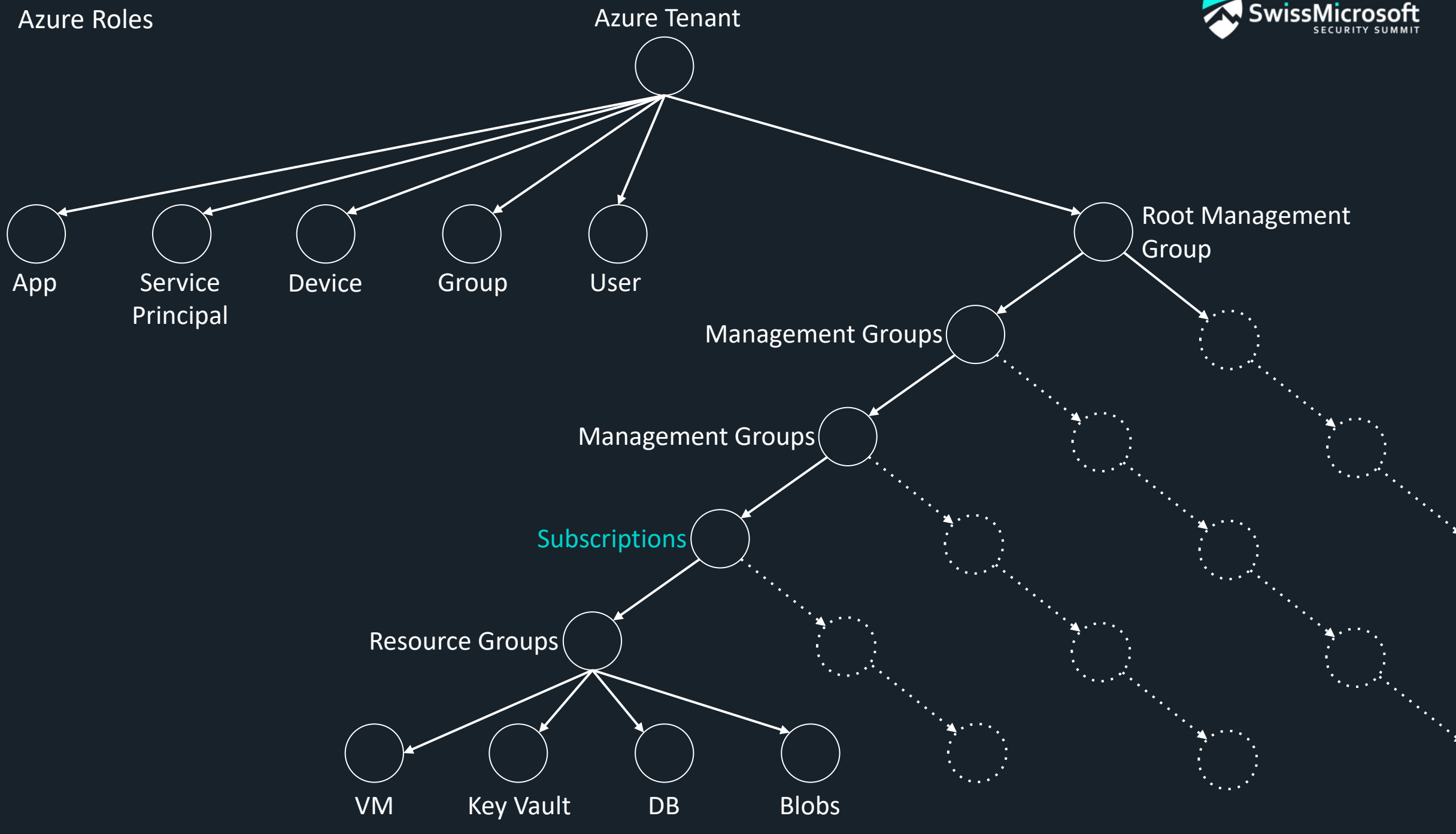


SwissMicrosoft SECURITY SUMMIT

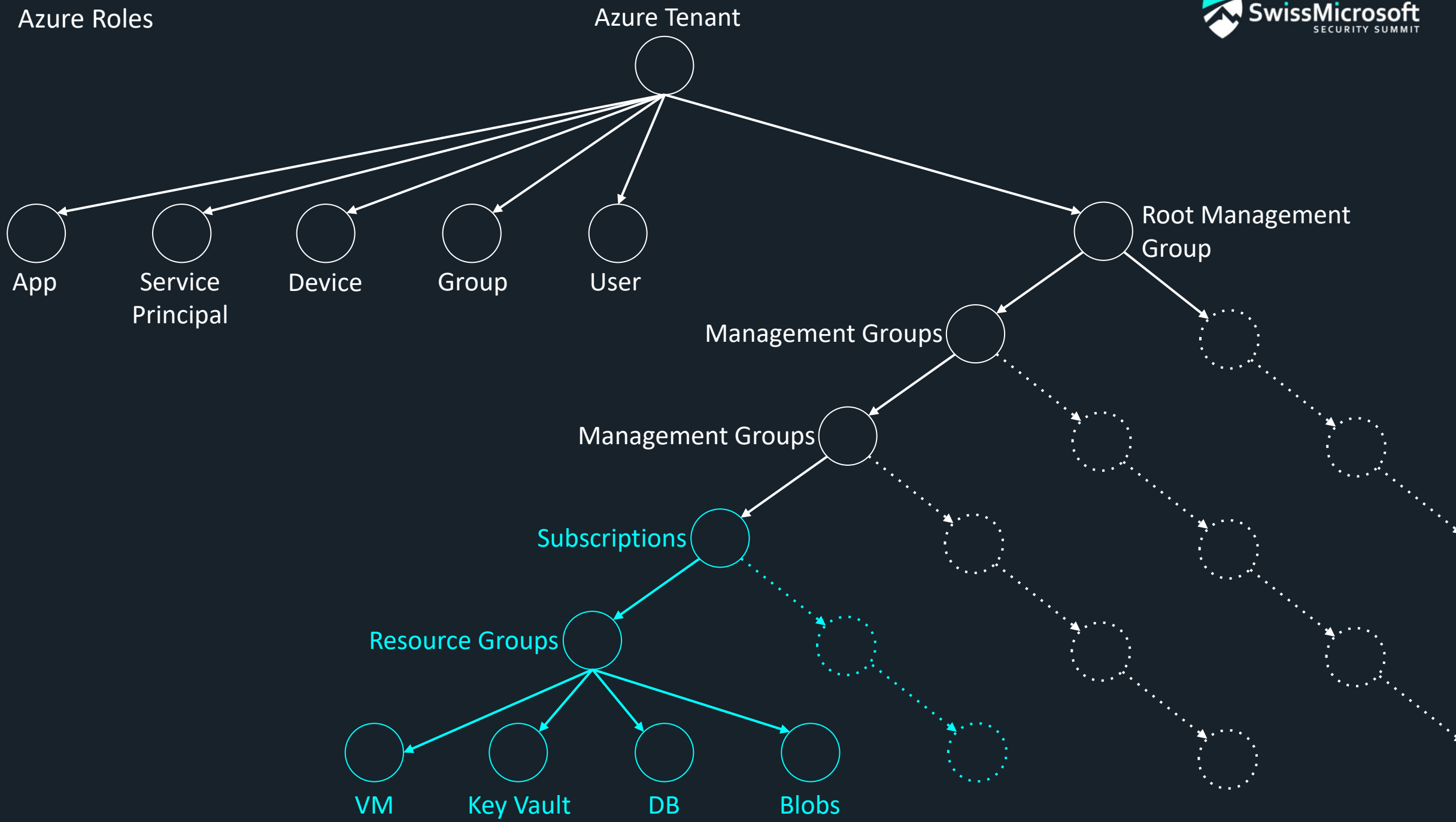
Azure Roles



Azure Roles

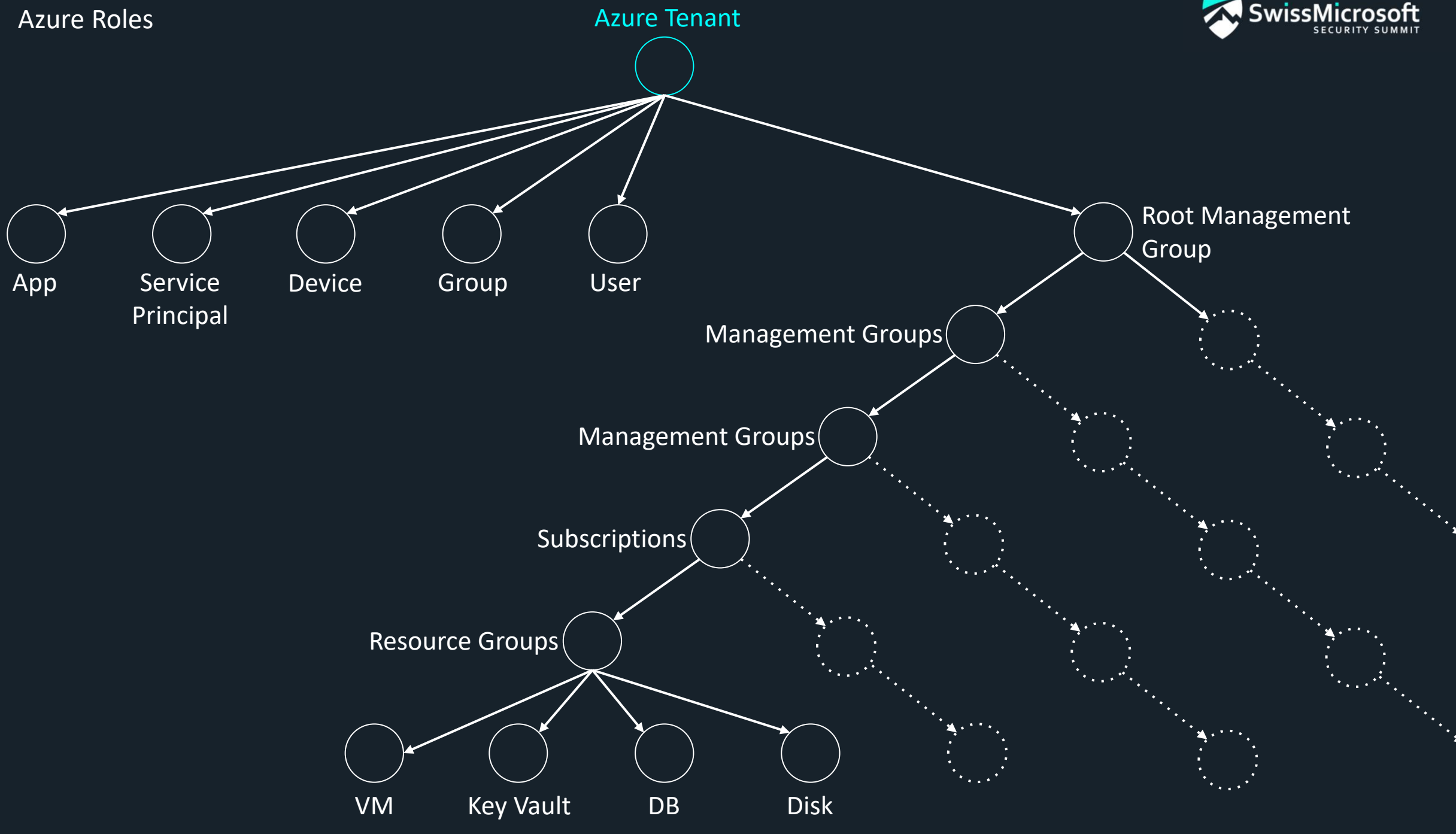


Azure Roles

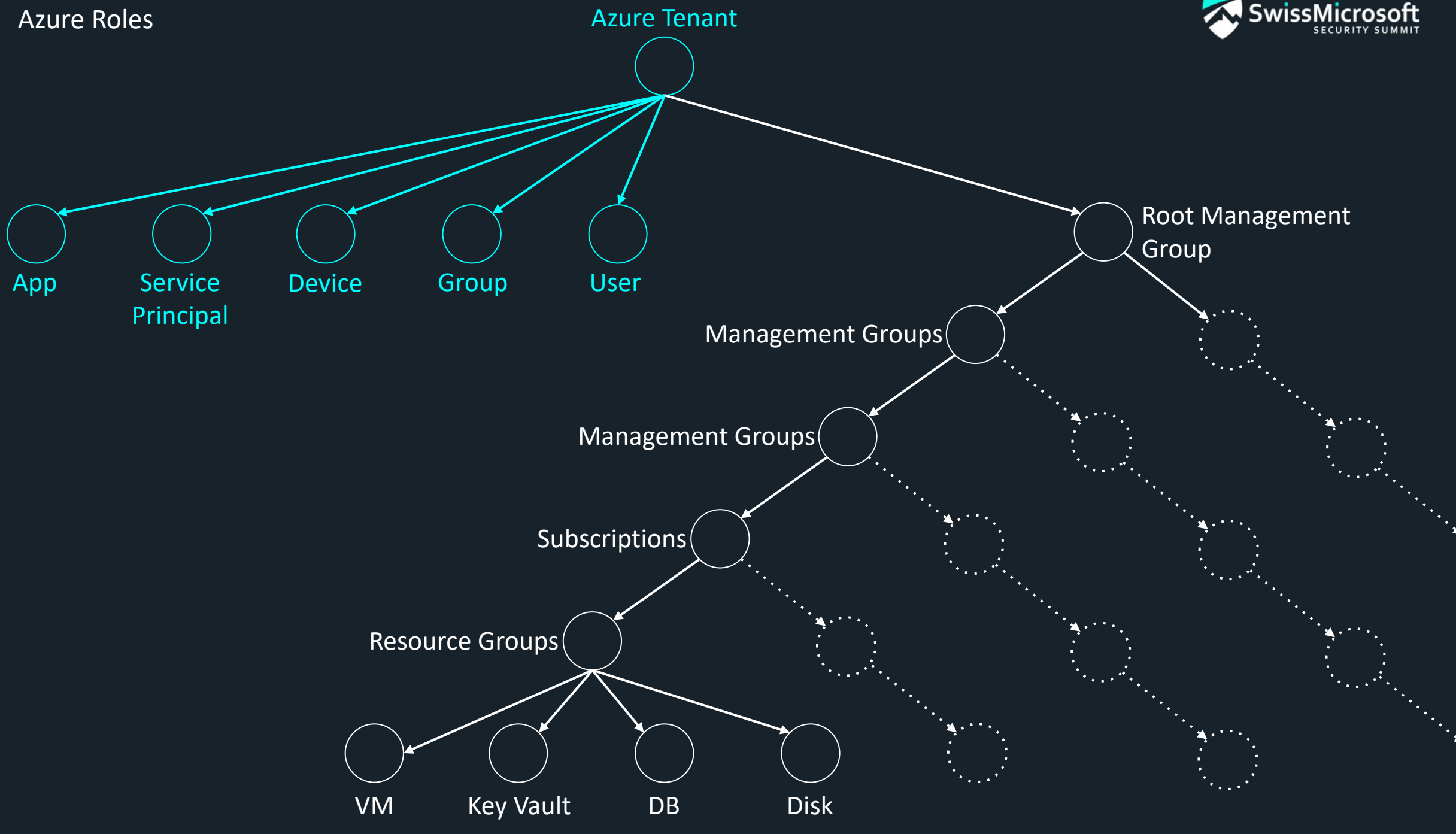


SwissMicrosoft SECURITY SUMMIT

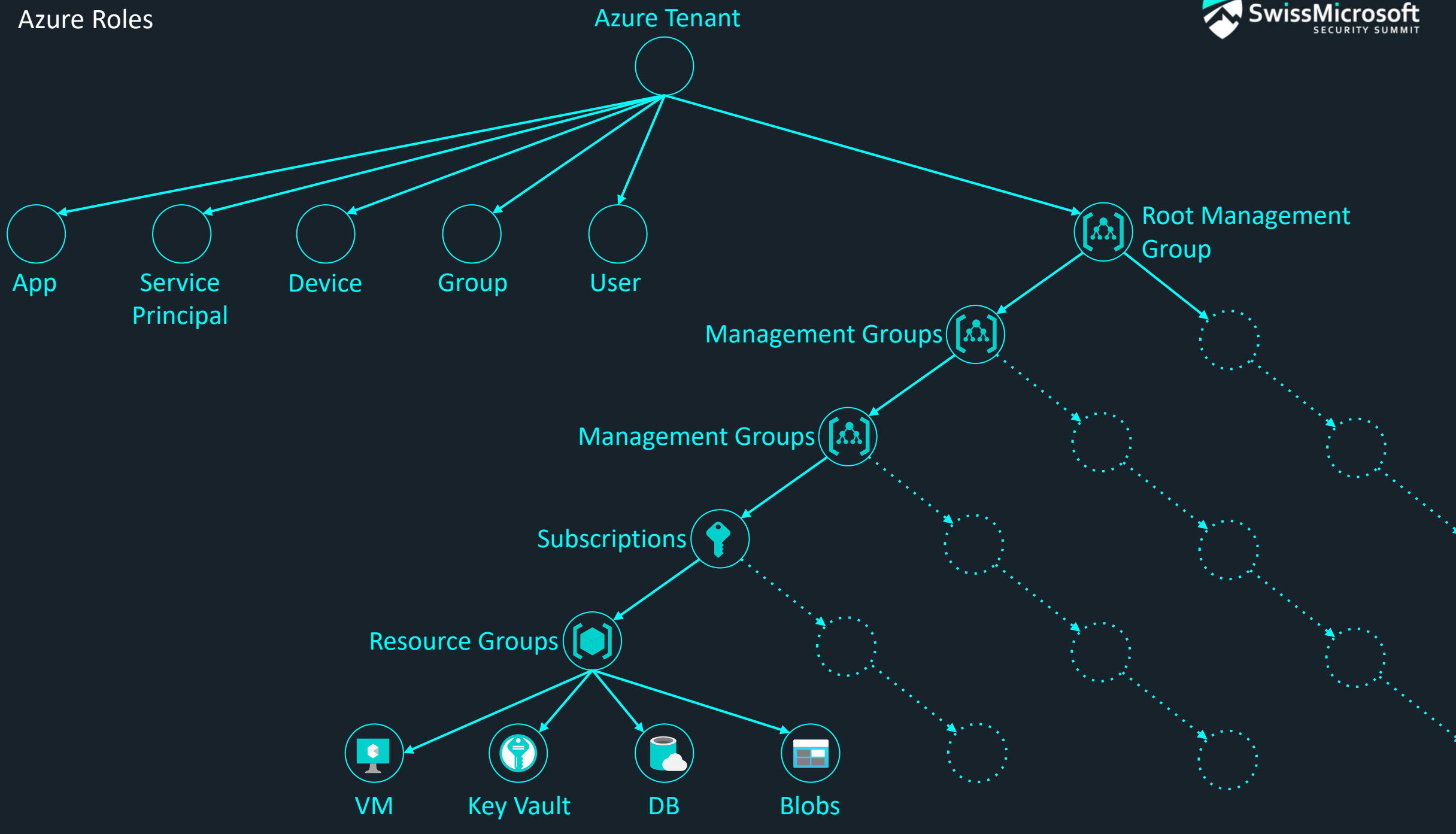
Azure Roles



Azure Roles



Azure Roles


Azure Tenant
App
Service Principal
Device
Group
User
Root Management Group
Management Groups
Management Groups
Subscriptions
Resource Groups
VM
Key Vault
DB
Blobs

Azure Roles

SwissMicrosoft SECURITY SUMMIT

Entra ID
Objects/Principal

User

Group

Service Principal

Managed Identity

HAS

Role Definition

Built-in

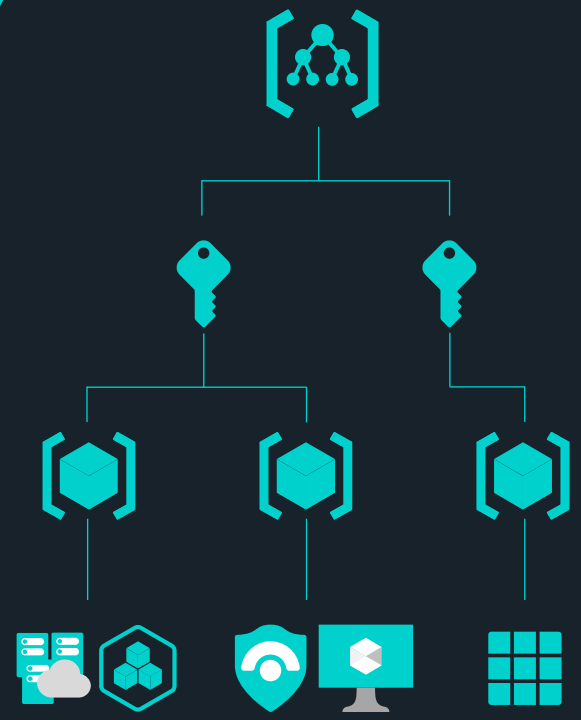
Owner
Contributor
Reader
User Acces Admin
…
Security Reader
VM Contributor
Etc.

Den Lab Executor
HD ticket reader
VM admins
…

Custom

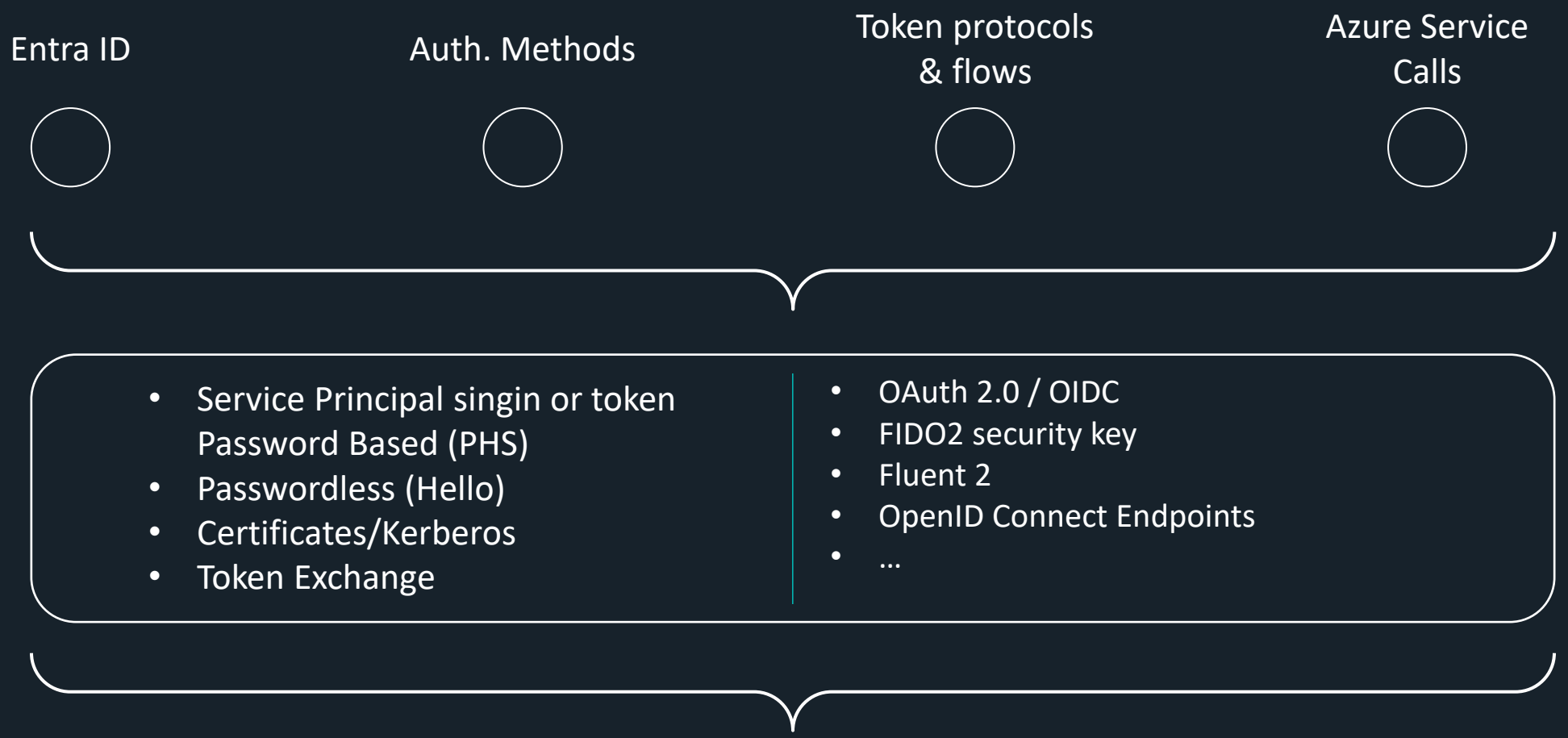
ON

Scope



Azure Authentication

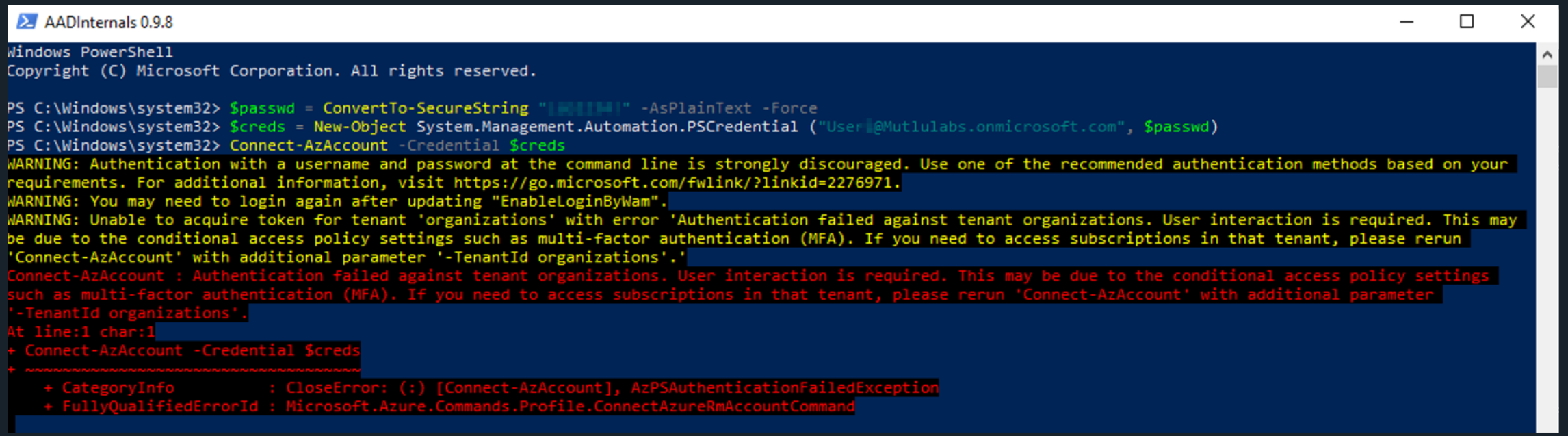
SwissMicrosoft SECURITY SUMMIT

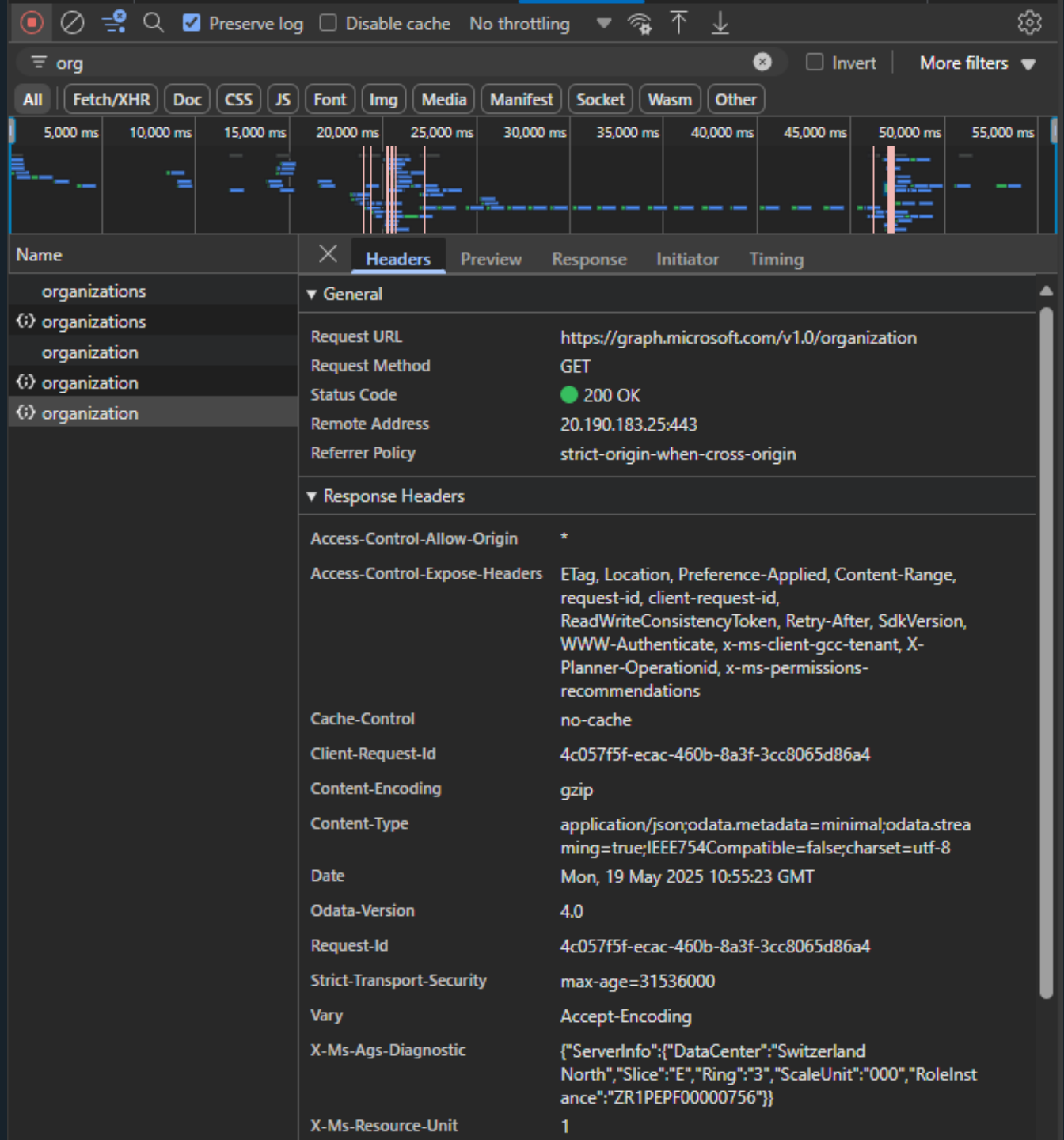


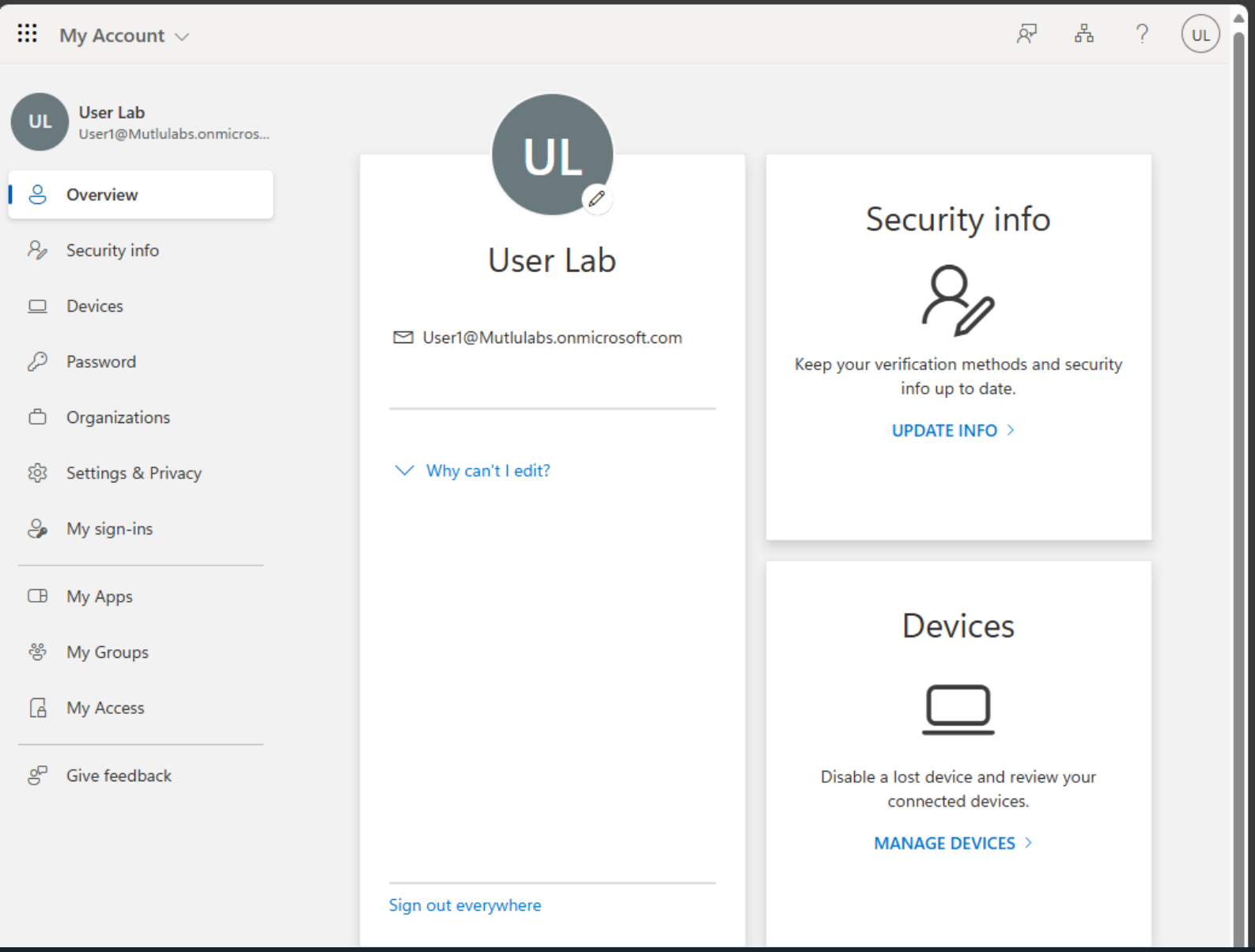
TOKENS (--> Check Thomas N. Slides)

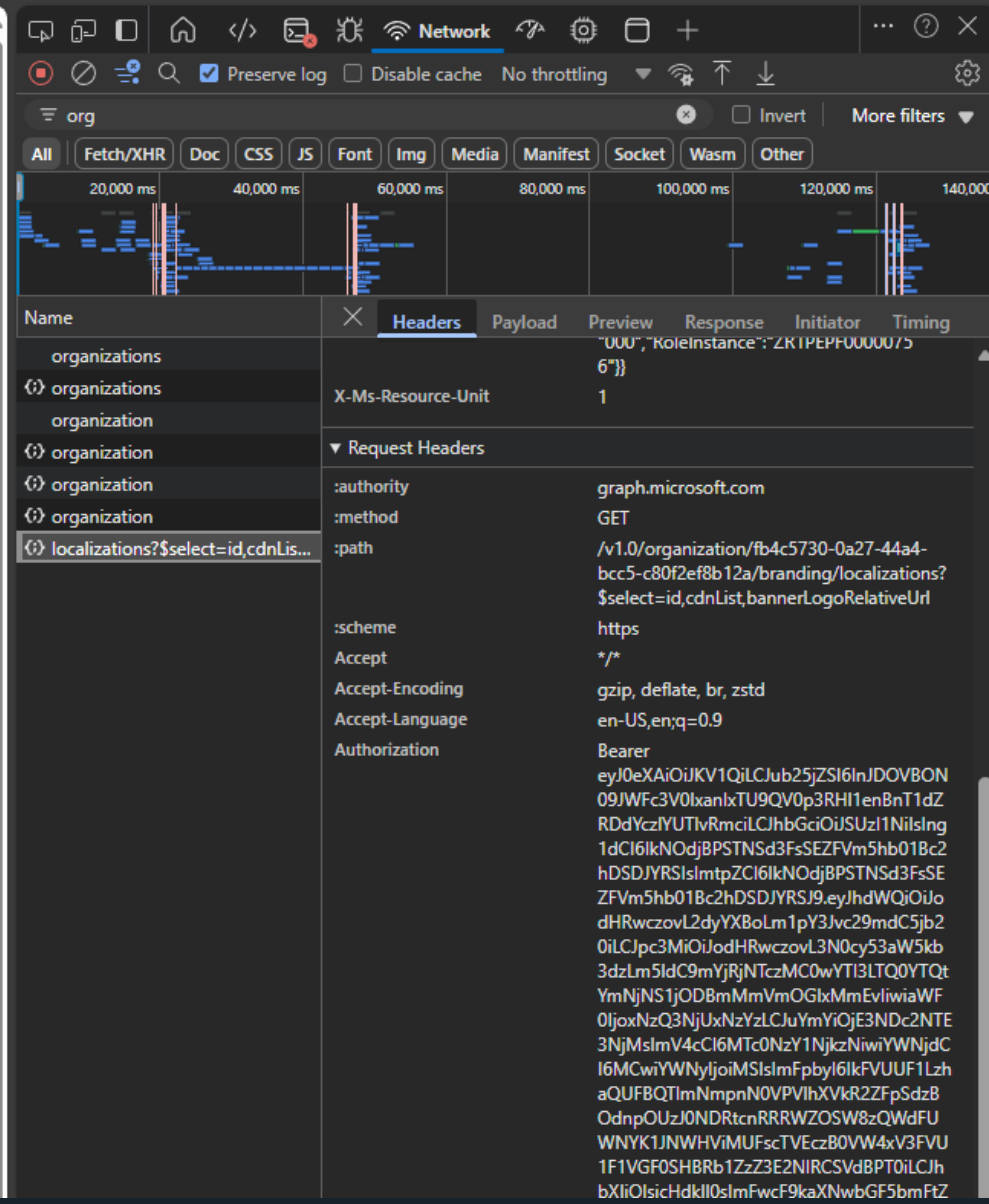
ID Token/Access Token issued by Entra ID (JWS)
Primary Refresh Token (PRT)
Proof-of-Possesion Token (PoP)
Shared Access Signature token (SAS)

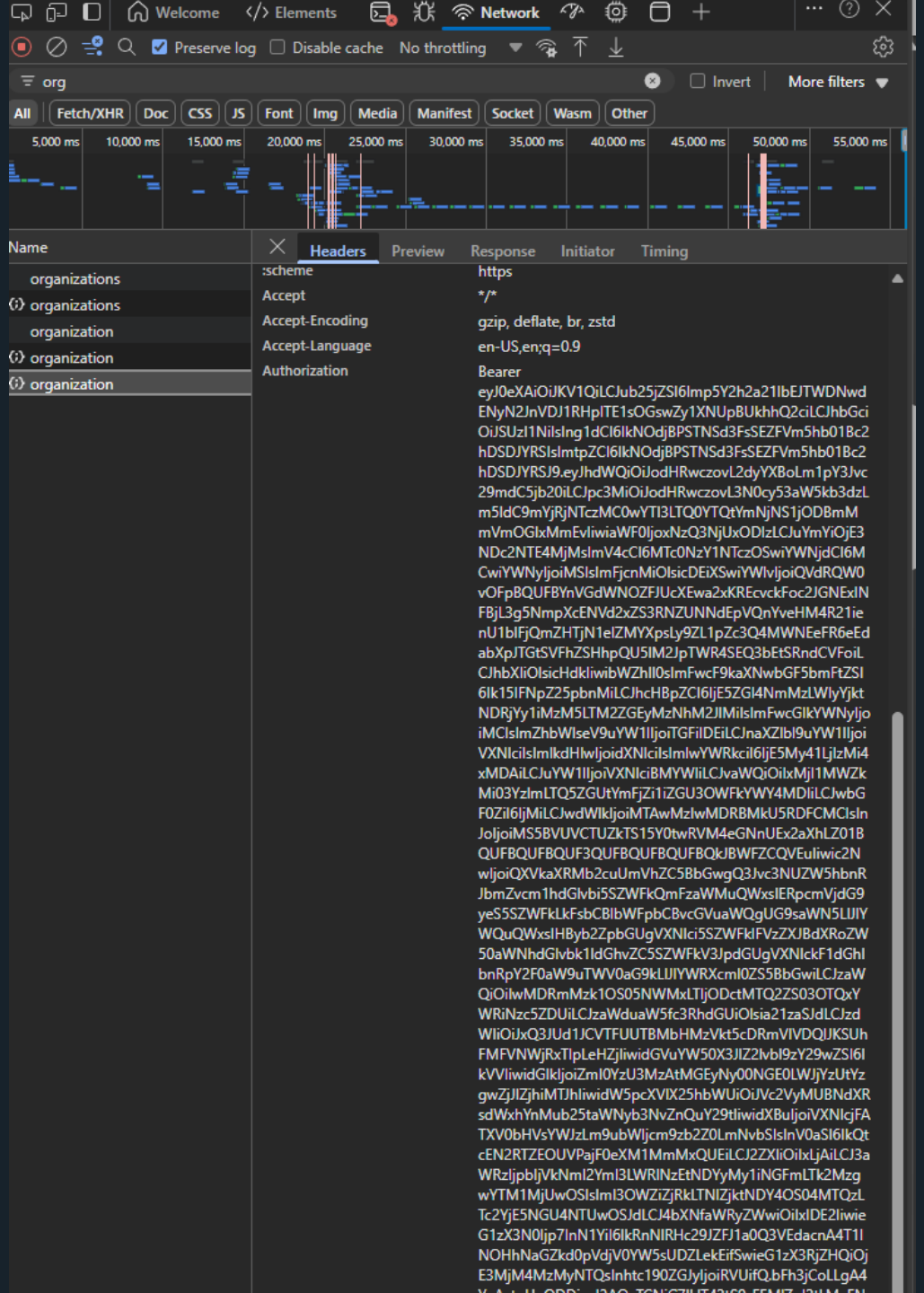
DEMO 1


AADInternals 0.9.8
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> $passwd = ConvertTo-SecureString "[redacted]" -AsPlainText -Force
PS C:\Windows\system32> $creds = New-Object System.Management.Automation.PSCredential ("User[redacted]@Mutlulabs.onmicrosoft.com", $passwd)
PS C:\Windows\system32> Connect-AzAccount -Credential $creds
WARNING: Authentication with a username and password at the command line is strongly discouraged. Use one of the recommended authentication methods based on your requirements. For additional information, visit https://go.microsoft.com/fwlink/?linkid=2276971.
WARNING: You may need to login again after updating "EnableLoginByWam".
WARNING: Unable to acquire token for tenant 'organizations' with error 'Authentication failed against tenant organizations. User interaction is required. This may be due to the conditional access policy settings such as multi-factor authentication (MFA). If you need to access subscriptions in that tenant, please rerun 'Connect-AzAccount' with additional parameter '-TenantId organizations'.'
Connect-AzAccount : Authentication failed against tenant organizations. User interaction is required. This may be due to the conditional access policy settings such as multi-factor authentication (MFA). If you need to access subscriptions in that tenant, please rerun 'Connect-AzAccount' with additional parameter '-TenantId organizations'.
At line:1 char:1
+ Connect-AzAccount -Credential $creds
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo   : CloseError: (:) [Connect-AzAccount], AzPSAuthenticationFailedException
    + FullyQualifiedErrorId : Microsoft.Azure.Commands.Profile.ConnectAzureRmAccountCommand

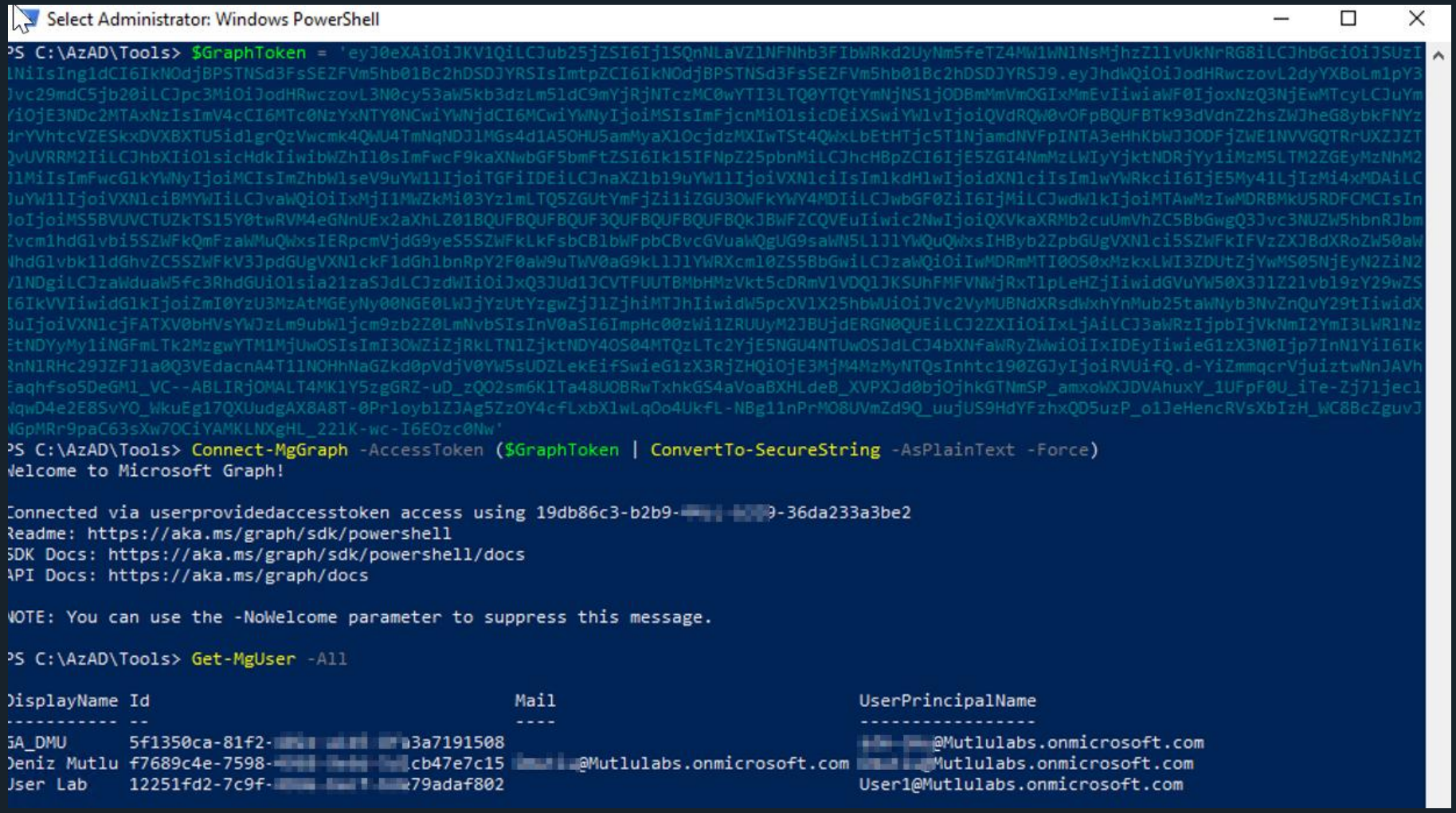



My Account
UL
User Lab
User1@Mutlulabs.onmicros...
Overview
Security info
Devices
Password
Organizations
Settings & Privacy
My sign-ins
My Apps
My Groups
My Access
Give feedback
UL
User Lab
User1@Mutlulabs.onmicrosoft.com
Why can't I edit?
Sign out everywhere
Security info
Keep your verification methods and security info up to date.
UPDATE INFO
Devices
Disable a lost device and review your connected devices.
MANAGE DEVICES


Network
Preserve log
Disable cache
No throttling
org
Invert
More filters
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
Socket
Wasm
Other
20,000 ms
40,000 ms
60,000 ms
80,000 ms
100,000 ms
120,000 ms
Name
organizations
organizations
organization
organization
organization
organization
localizations?$select=id,cdnLis...
Headers
Payload
Preview
Response
Initiator
Timing
X-Ms-Resource-Unit 1
Request Headers
:authority graph.microsoft.com
:method GET
:path /v1.0/organization/fb4c5730-0a27-44a4-bcc5-c80f2ef8b12a/branding/localizations?$select=id,cdnList,bannerLogoRelativeUrl
:scheme https
Accept */*
Accept-Encoding gzip, deflate, br, zstd
Accept-Language en-US,en;q=0.9
Authorization Bearer



SwissMicrosoft SECURITY SUMMIT


Select Administrator: Windows PowerShell
PS C:\AzAD\Tools> $GraphToken = 'eyJ0eXAiOiJKV1QiLCJub25jZSI6Ij1SQnNLaVZlNFNhb3FIbWRkd2UyNm5feTZ4MW1WNlNsMjhzZ1lvUkNrRG8iLCJhbGciOiJSUzI
lNiIsIng1dCI6IkNOdjBPSTNSd3FsSEZFVm5hb01Bc2hDSDJYRSIsImtpZCI6IkNOdjBPSTNSd3FsSEZFVm5hb01Bc2hDSDJYRSJ9.eyJhdWQiOiJodHRwczovL2dyYXBoLm1pY3
Jvc29mdC5jb20iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm51dC9mYjRjNTczMC0wYTI3LTQ0YTQtYmNjNS1jODBmMmVmOGIxMmEvIiwiaWF0IjoxNzQ3NjEwMTcyLCJuYm
YiOjE3NDc2MTAxNzIsImV4cCI6MTc0NzYxNTY0NCwiYWNjdCI6MCwiYWNyIjoiMSIsImFjcnMiOlsicDEiXSwiYWlvIjoiQVdRQW0vOFpBQUFBTk93dVdnZ2hsZWJheG8ybkFNYz
drYVhtcVZESkxDVXBXTU5idlgrQzVwcmk4QWU4TmNqNDJlMGs4d1A5OHU5amMyaXlOcjdzMXIwTSt4QWxLbEtHTjc5T1NjamdNVFpINTA3eHhKbWJJODFjZWE1NVVGQTRrUXZJZT
QvUVRRM2IiLCJhbXIiOlsicHdkIiwibWZhIl0sImFwcF9kaXNwbGF5bmFtZSI6Ik15IFNpZ25pbnMiLCJhcHBpZCI6IjE5ZGI4NmMzLWIyYjktNDRjYy1iMzM5LTM2ZGEyMzNhM2
JlMiIsImFwcGlkYWNyIjoiMCIsImZhbWlseV9uYW1lIjoiTGFiIDEiLCJnaXZlbl9uYW1lIjoiVXNlciIsImlkdHlwIjoidXNlciIsImlwYWRkciI6IjE5My41LjIzMi4xMDAiLC
JuYW1lIjoiVXNlciBMYWIiLCJvaWQiOiIxMjI1MWZkMi03Yz1mLTQ5ZGUtYmFjZi1iZGU3OWFkYWY4MDIiLCJwbGF0ZiI6IjMiLCJwdWlkIjoiMTAwMzIwMDRBMkU5RDFCMCIsIn
JoIjoiMS5BVUVCTUZkTS15Y0twRVM4eGNnUEx2aXhLZ01BQUFBQUFBQUF3QUFBQUFBQUFBQkJBWFZCQVEuIiwic2NwIjoiQXVkaXRMb2cuUmVhZC5BbGwgQ3Jvc3NUZW5hbnRJbm
ZvcmlhdGlvbi5SZWFkQmFzaWMuQWxsIERpcmVjdG9yeS5SZWFkLkFsbCBlbWFpbCBvcGVuaWQgUG9saWN5LlJlYWQuQWxsIHByb2ZpbGUgVXNlci5SZWFkIFVzZXJBdXRoZW50aW
NhdGlvbk1ldGhvZC5SZWFkV3JpdGUgVXNlckF1dGhlbnRpY2F0aW9uTWV0aG9kLlJlYWRXcml0ZS5BbGwiLCJzaWQiOiIwMDRmMTI0OS0xMzkxLWI3ZDUtZjYwMS05NjEyN2ZiN2
VlNDgiLCJzaWduaW5fc3RhdGUiOlsia21zaSJdLCJzdWIiOiJxQ3JUd1JCVTFUUTBMbHMzVkt5cDRmVlVDQ1JKSUhFMFVNWjRxTlpLeHZjIiwidGVuYW50X3J1Z2lvbl9zY29wZS
I6IkVVIiwidGlkIjoiZmI0YzU3MzAtMGEyNy00NGE0LWJjYzUtYzgwZjJlZjhiMTJhIiwidW5pcXVlX25hbWUiOiJVc2VyMUBNdXRsdWxhYnMub25taWNyb3NvZnQuY29tIiwidX
3uIjoiVXNlcjFATXV0bHVsYWJzLm9ubWljcm9zb2Z0LmNvbSIsInV0aSI6ImpHc00zWi1ZRUUyM2JBUjdERGN0QUEiLCJ2ZXIiOiIxLjAiLCJ3aWRzIjpbIjVkNmI2YmI3LWRlNz
EtNDYyMy1iNGFmLTk2MzgwYTM1MjUwOSIsImI3OWZiZjRkLTN1ZjktNDY4OS04MTQzLTc2YjE5NGU4NTUwOSJdLCJ4bXNfaWRyZWwiOiIxIDEyIiwieG1zX3N0Ijp7InN1YiI6Ik
RnN1RHc29JZFJ1a0Q3VEdacnA4T1lNOHhNaGZkd0pVdjV0YW5sUDZLekEifSwieG1zX3RjZHQiOjE3MjM4MzMyNTQsInhtc190ZGJyIjoiRVUifQ.d-YiZmmqcrVjuiztwNnJAVh
Eaqhfso5DeGM1_VC--ABLIRjOMALT4MK1Y5zgGRZ-uD_zQO2sm6K1Ta48UOBRwTxhkGS4aVoaBXHLdeB_XVPXJd0bjOjhkGTNmSP_amxoWXJDVAhuxY_1UFpF0U_iTe-Zj71jec1
WqwD4e2E8SvYO_WkuEg17QXUudgAX8A8T-0PrloyblZJAg5ZzOY4cfLxbXlwLqOo4UkfL-NBg11nPrMO8UVmZd9Q_uujUS9HdYFzhxQD5uzP_o1JeHencRVsXbIzH_WC8BcZguvJ
WGpMRr9paC63sXw7OCiYAMKLNXgHL_221K-wc-I6EOzc0Nw'
PS C:\AzAD\Tools> Connect-MgGraph -AccessToken ($GraphToken | ConvertTo-SecureString -AsPlainText -Force)
Welcome to Microsoft Graph!
Connected via userprovidedaccesstoken access using 19db86c3-b2b9-
-36da233a3be2
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs
NOTE: You can use the -NoWelcome parameter to suppress this message.
PS C:\AzAD\Tools> Get-MgUser -All
DisplayName Id Mail UserPrincipalName
GA_DMU 5f1350ca-81f2- a3a7191508 @Mutlulabs.onmicrosoft.com
Deniz Mutlu f7689c4e-7598- cb47e7c15 @Mutlulabs.onmicrosoft.com
User Lab 12251fd2-7c9f- 79adaf802 User1@Mutlulabs.onmicrosoft.com

```
PS C:\AzAD\Tools> Get-MgUser -All | select UserPrincipalName

UserPrincipalName
-----------------
[redacted]@Mutlulabs.onmicrosoft.com
Dmutlu@Mutlulabs.onmicrosoft.com
User1@Mutlulabs.onmicrosoft.com


PS C:\AzAD\Tools> Get-MgGroup -All

DisplayName           Id                                   MailNickname Description                                                GroupTypes
-----------           --                                   ------------ -----------                                                ---------
All Company           d39c6f38-27bf[redacted]e9640ff237a0 allcompany   This is the default group for everyone in the network {Unified}
Hacknowledge          d8b9a018-f9cd[redacted]d798461bd7c0 Hacknowledge                                                         {Unified}
Lab_AzureAttack_Group fbaed1be-db72[redacted]aa2781c394bd 3b93d323-b                                                           {}


PS C:\AzAD\Tools> $RoleId = (Get-MgDirectoryRole -Filter "DisplayName eq 'Global Administrator'").Id
PS C:\AzAD\Tools> (Get-MgDirectoryRoleMember -DirectoryRoleId $RoleId).AdditionalProperties

Key               Value
---               -----
@odata.type       #microsoft.graph.user
businessPhones    {41795865813}
displayName       Deniz Mutlu
givenName         Deniz
mail              Dmutlu@Mutlulabs.onmicrosoft.com
preferredLanguage en
surname           Mutlu
```

My Azure Attacks Research Process

SwissMicrosoft SECURITY SUMMIT

Start with the end in mind

I want to understand:

- The fundamental mechanics of the curent Azure Attacks
- How the attacks can compromise the tenants
- How Entra ID can be abused
- How to detect this attacks with Sentinel/Defender XDR

Start with the end in mind

I want to understand:

- The fundamental mechanics of the curent Azure Attacks
- How the attacks can compromise the tenants
- How Entra ID can be abused
- How to detect this attacks with Sentinel/Defender XDR

I want to produce in 2025:

- 2-3 blog posts / 1 talk for others to understand and build on
- Example of tools usage and how to abuse Azure
- Give some Detection guidance / KQL

Start with the end in mind

I want to understand:

- The fundamental mechanics of the current Azure Attacks
- How the attacks can compromise the tenants
- How Entra ID can be abused
- How to detect this attacks with Sentinel/Defender XDR

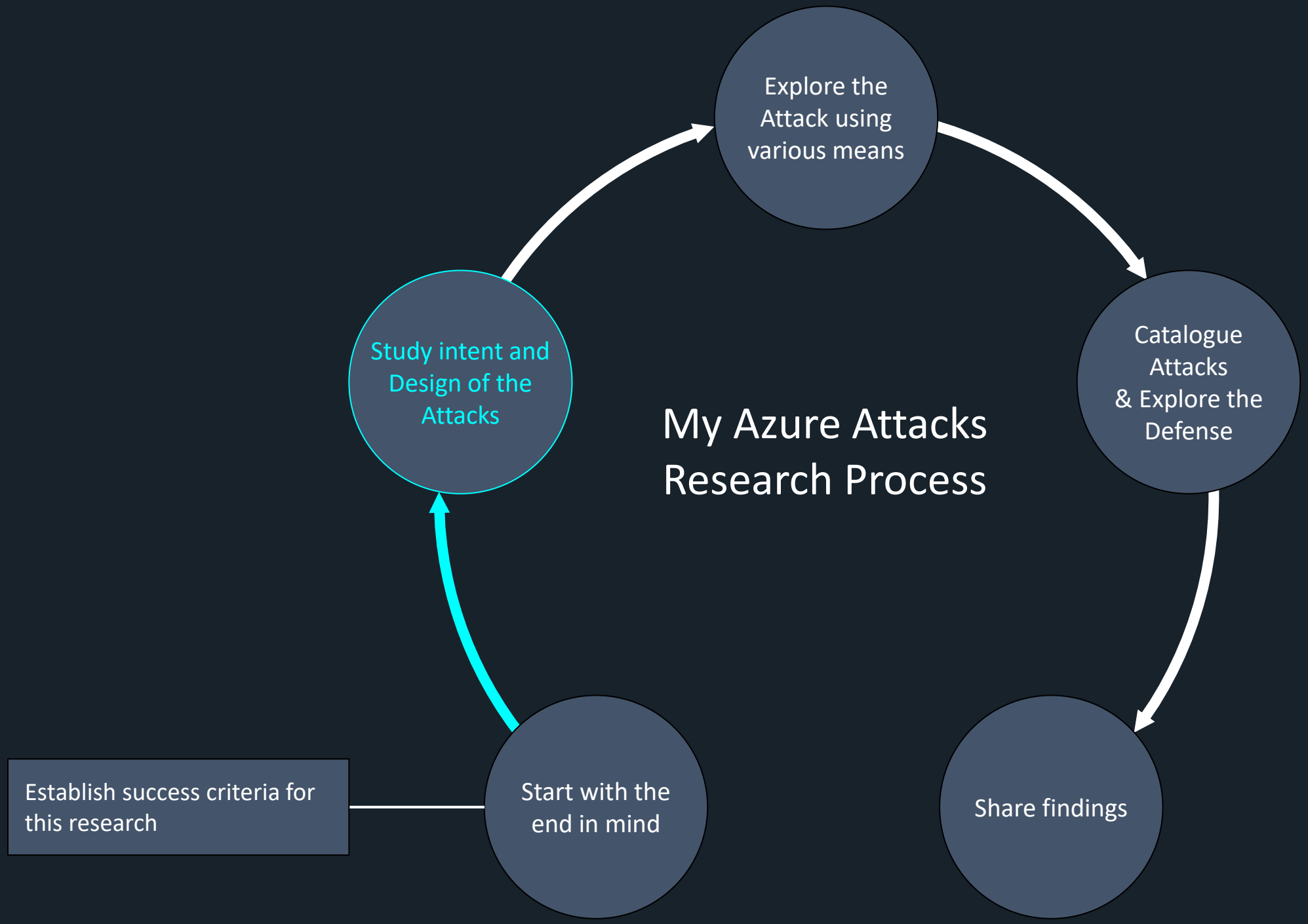
I want to produce in 2025:

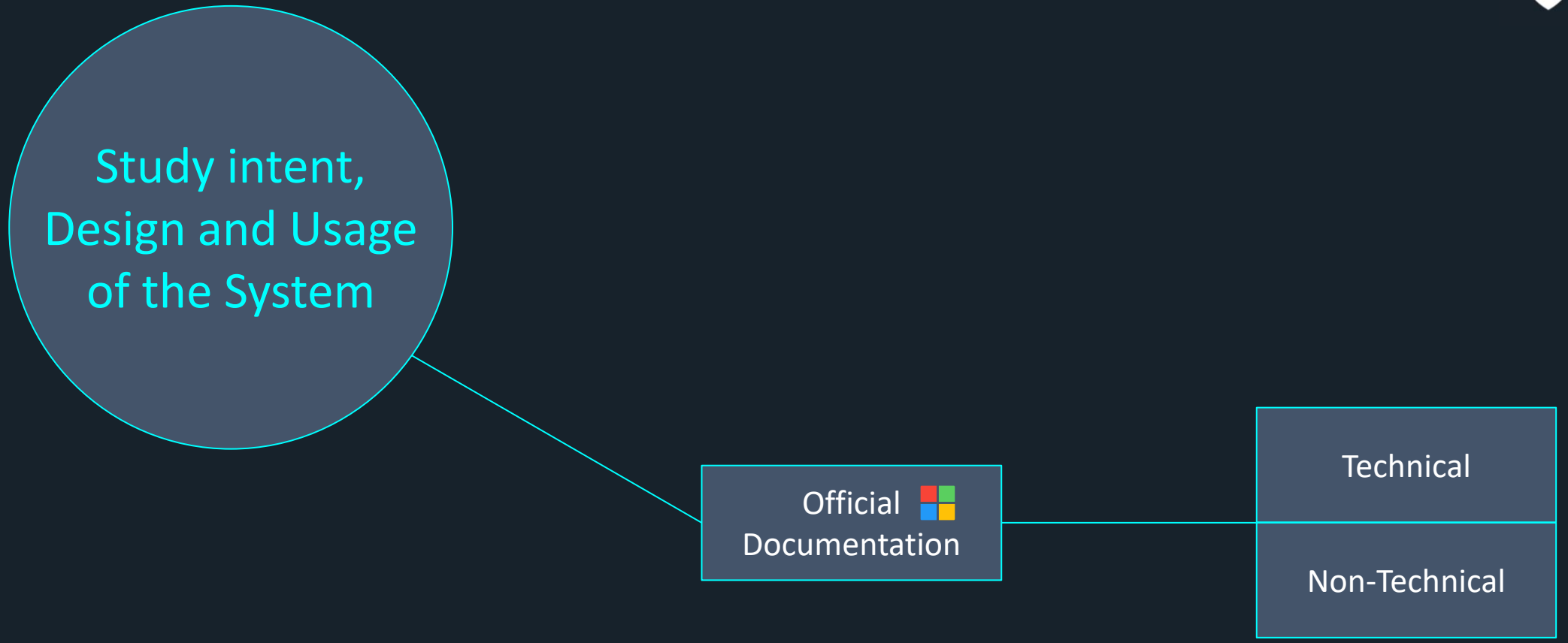
- 2-3 blog posts / 1 talk for others to understand and build on
- Example of tools usage and how to abuse Azure
- Give some Detection guidance / KQL

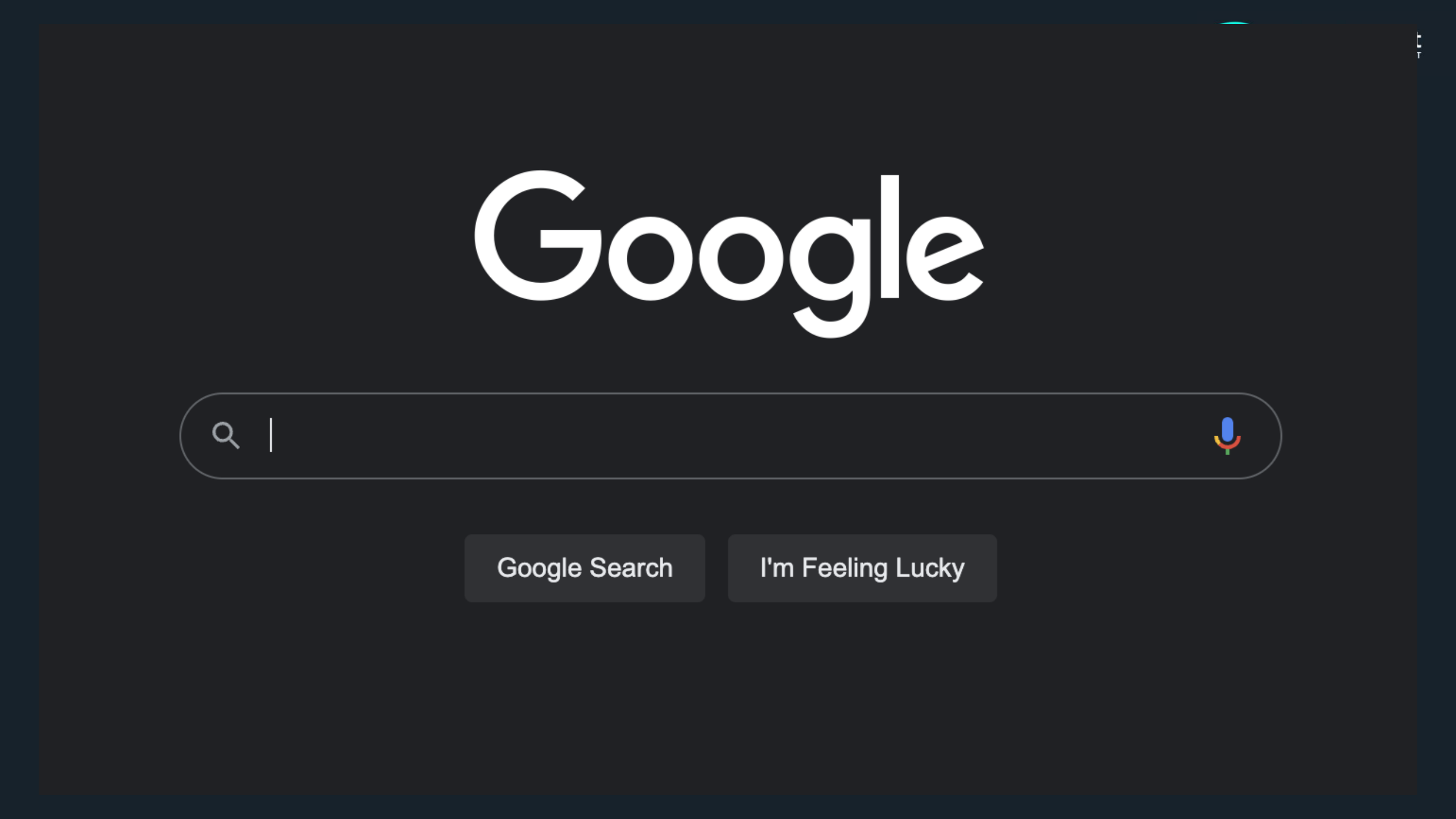
If appropriate for SPCS, I want to prepare for:

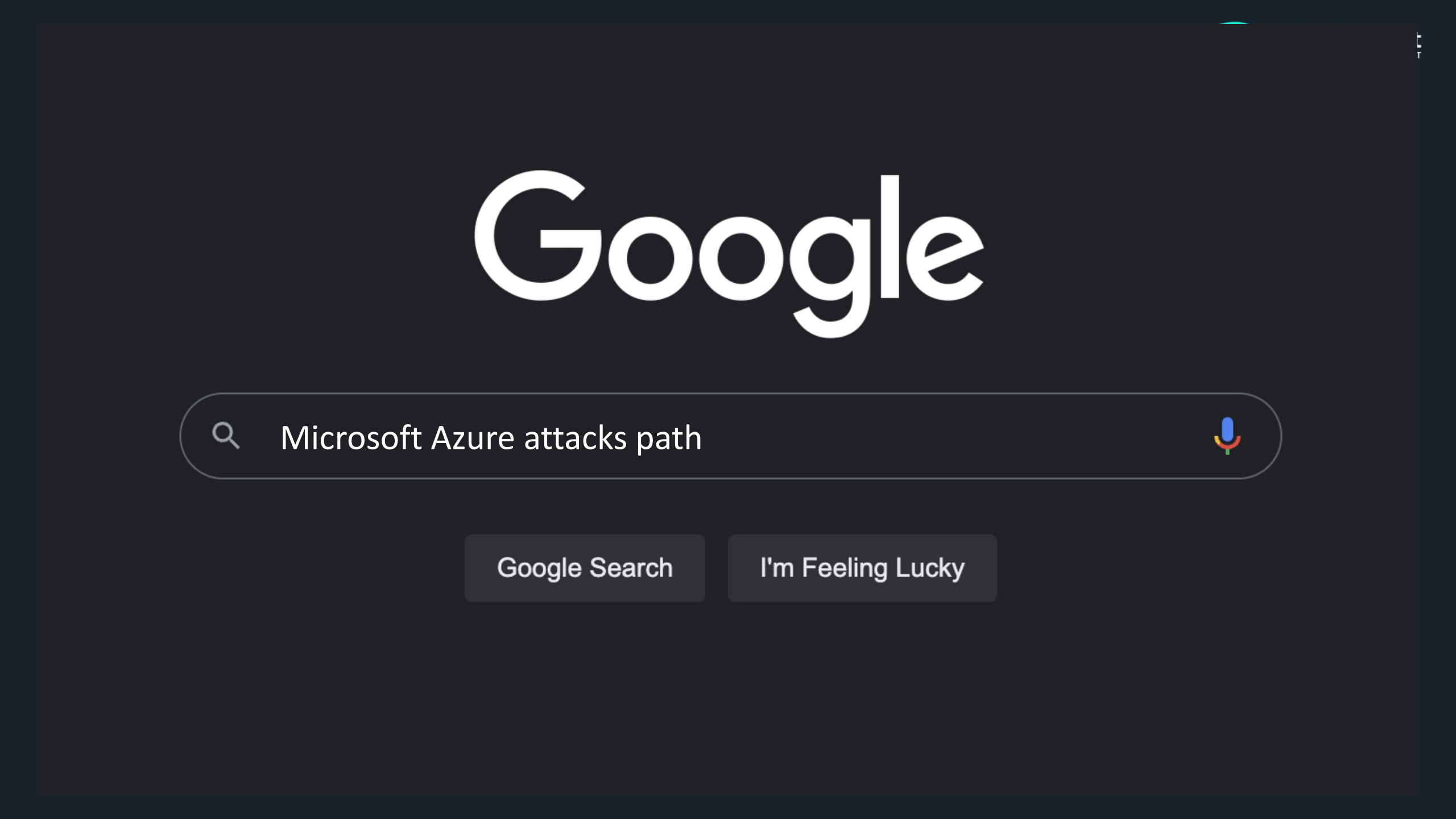
- The impact on the existing SOC Detection
- How to train our teams to investigate this attacks
- What data to collect and ingest, and how to setup An.rules

My Azure Attacks Research Process




Study intent, Design and Usage of the System
Official Documentation
Technical
Non-Technical


Google
Google Search
I'm Feeling Lucky


Google
Microsoft Azure attacks path
Google Search
I'm Feeling Lucky

Types of attacks Azure DDoS Protection mitigate

Article • 03/17/2025 • 7 contributors

Az

Reflection Amplification Attack	Uses a third-party server to amplify the attack traffic towards the target.

- **Protocol attacks**: These attacks render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack. They include SYN flood attacks, reflection attacks, and other protocol attacks. DDoS Protection mitigates these attacks, differentiating between malicious and legitimate traffic, by interacting with the client, and blocking malicious traffic. Common attack types are listed in

Additional resources

Training

Module
Introduction to Azure DDoS Protection - Training

Learn how to guard your Azure services from a denial of service attack using Azure DDoS Protection.

Documentation

Azure DDoS Protection reference architectures

Learn Azure DDoS protection reference architectures.

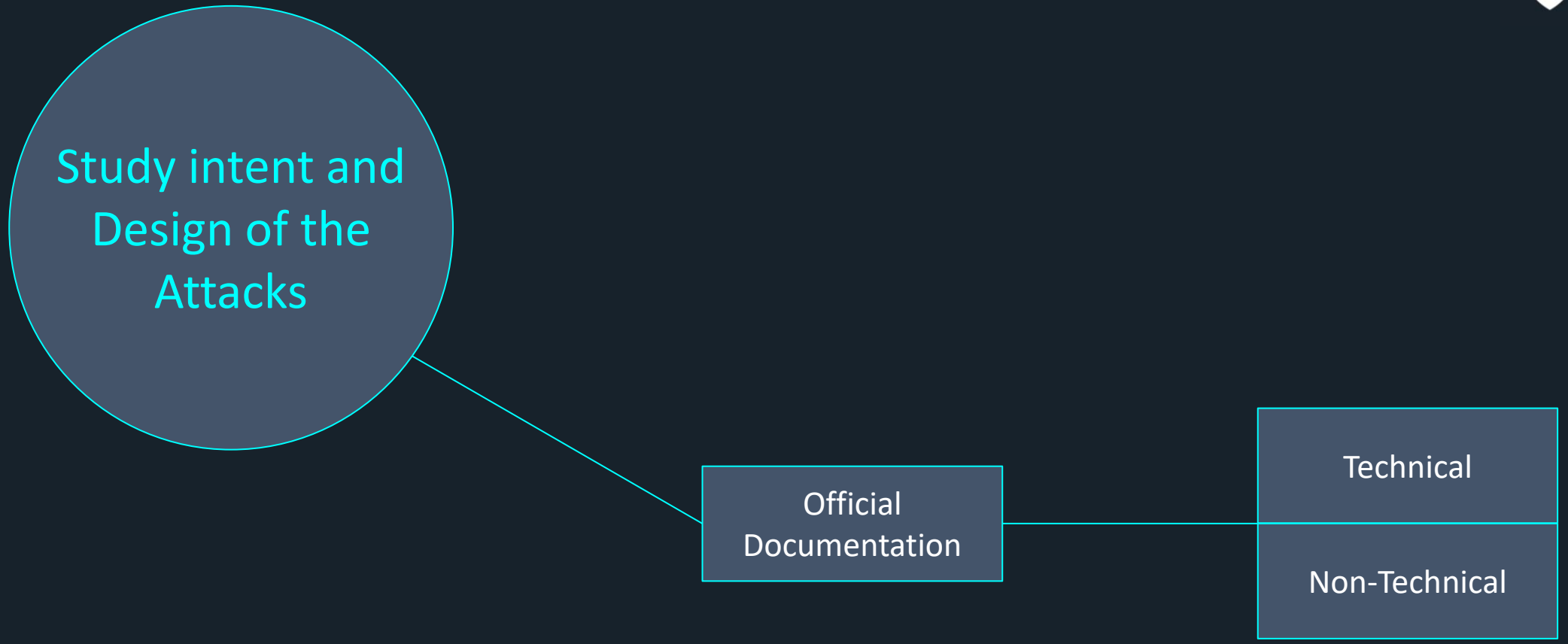
Azure DDoS Protection fundamental best practices

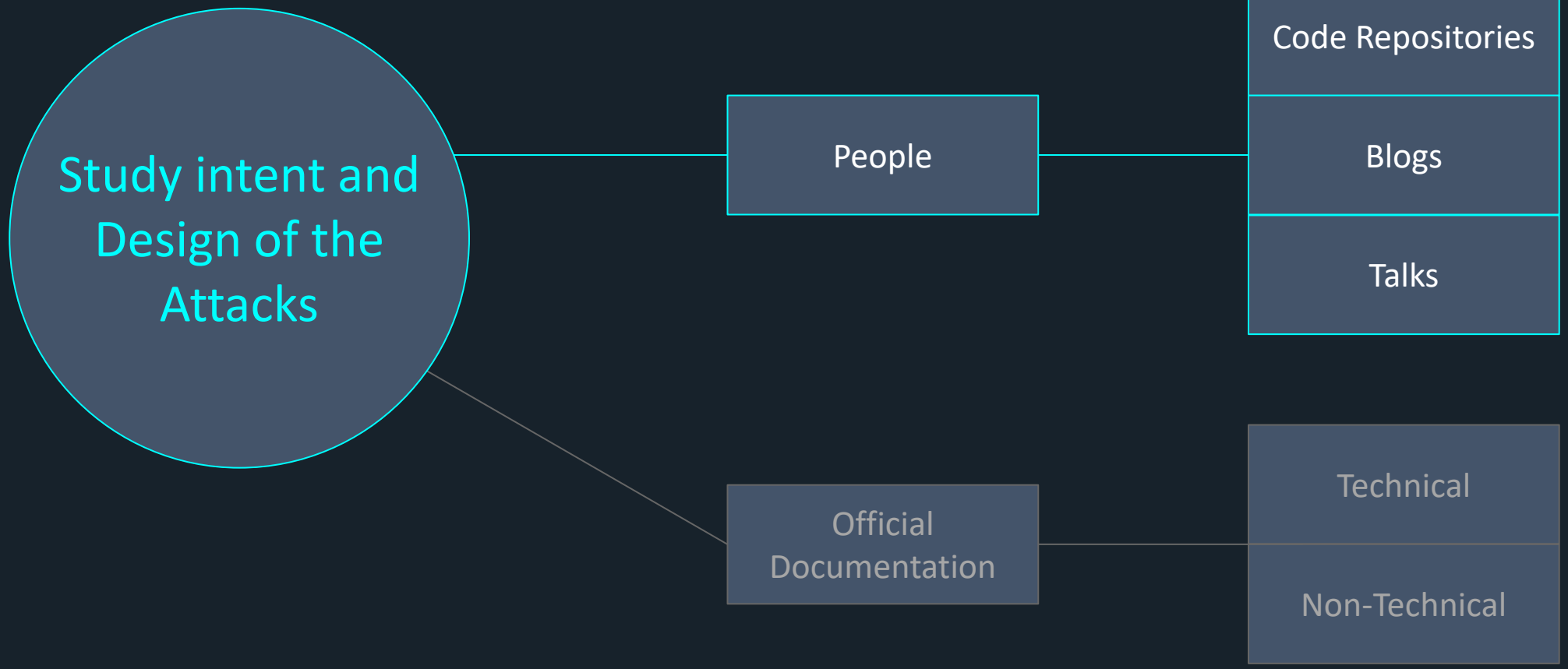
Learn the best security practices using Azure DDoS Protection.

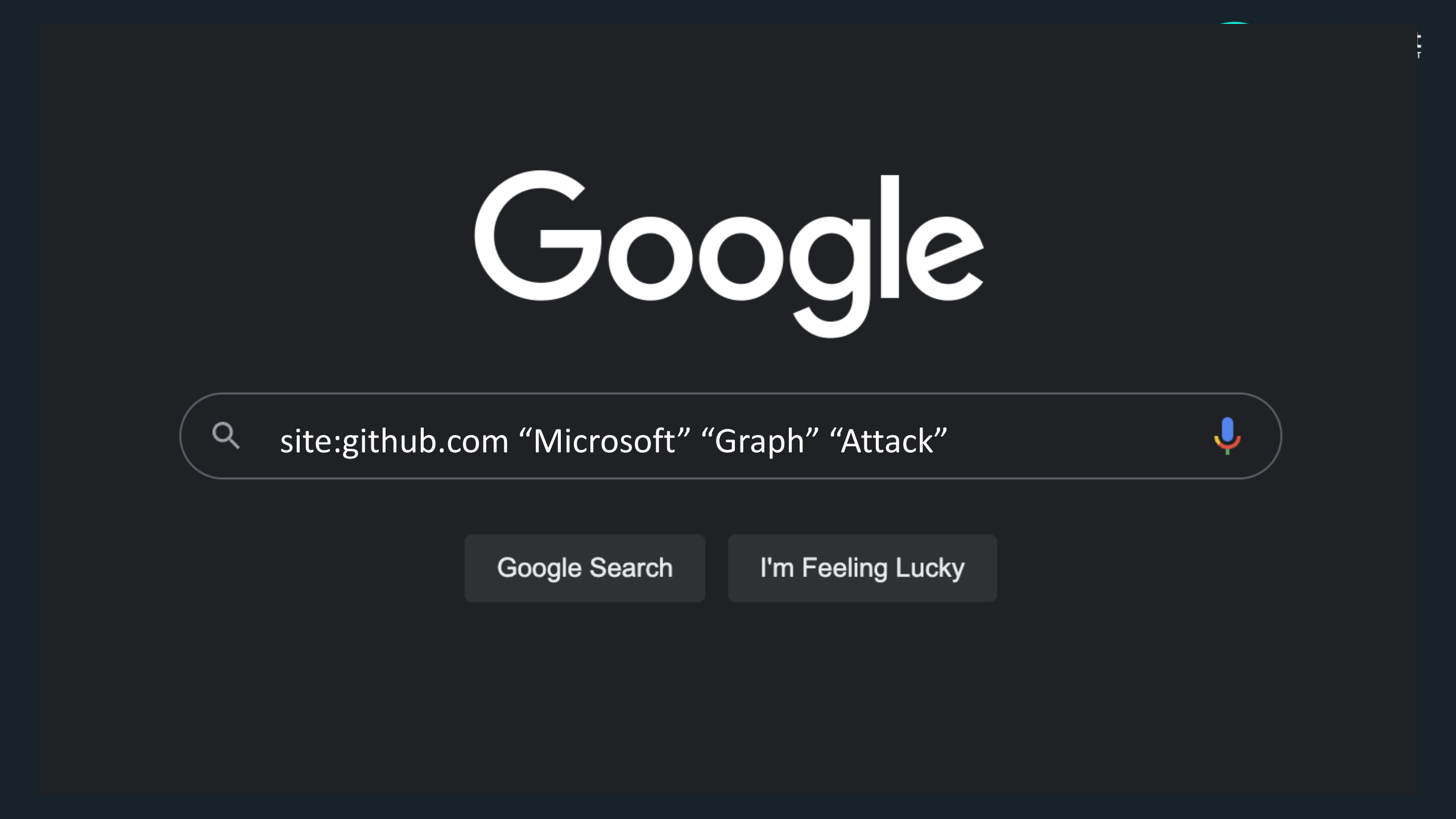
Azure DDoS Protection features

Learn Azure DDoS Protection features

Show 4 more


Study intent and Design of the Attacks
Official Documentation
Technical
Non-Technical


Study intent and Design of the Attacks
People
Code Repositories
Blogs
Talks
Official Documentation
Technical
Non-Technical


Google
site:github.com “Microsoft” “Graph” “Attack”
Google Search
I'm Feeling Lucky

SwissMicrosoft SECURITY SUMMIT

AADInternals

AADInternals is PowerShell module for administering Azure AD and Office 365

For details, please visit https://aadinternals.com/aadinternals

Installation

Run the following PowerShell command to install

```
Install-Module AADInternals
```

MicroBurst

TOOLS.NETSPI.COM

GraphRunner

Do service principals dream of electric sheep?

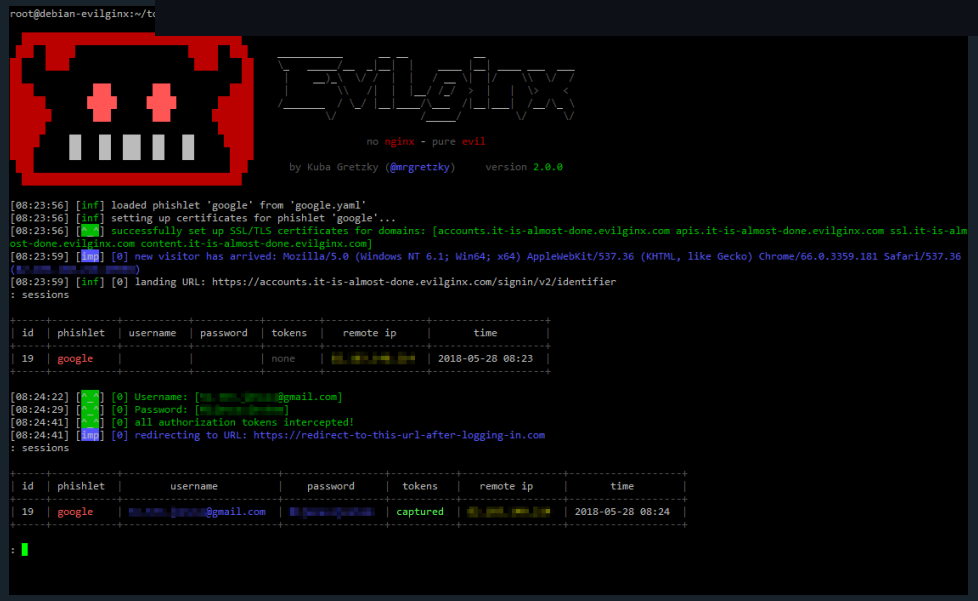
AzureHound

The BloodHound data collector for Microsoft Azure

build failing | release v2.4.1 | downloads 160k | documentation

ROADtools

STORMSPOTTER

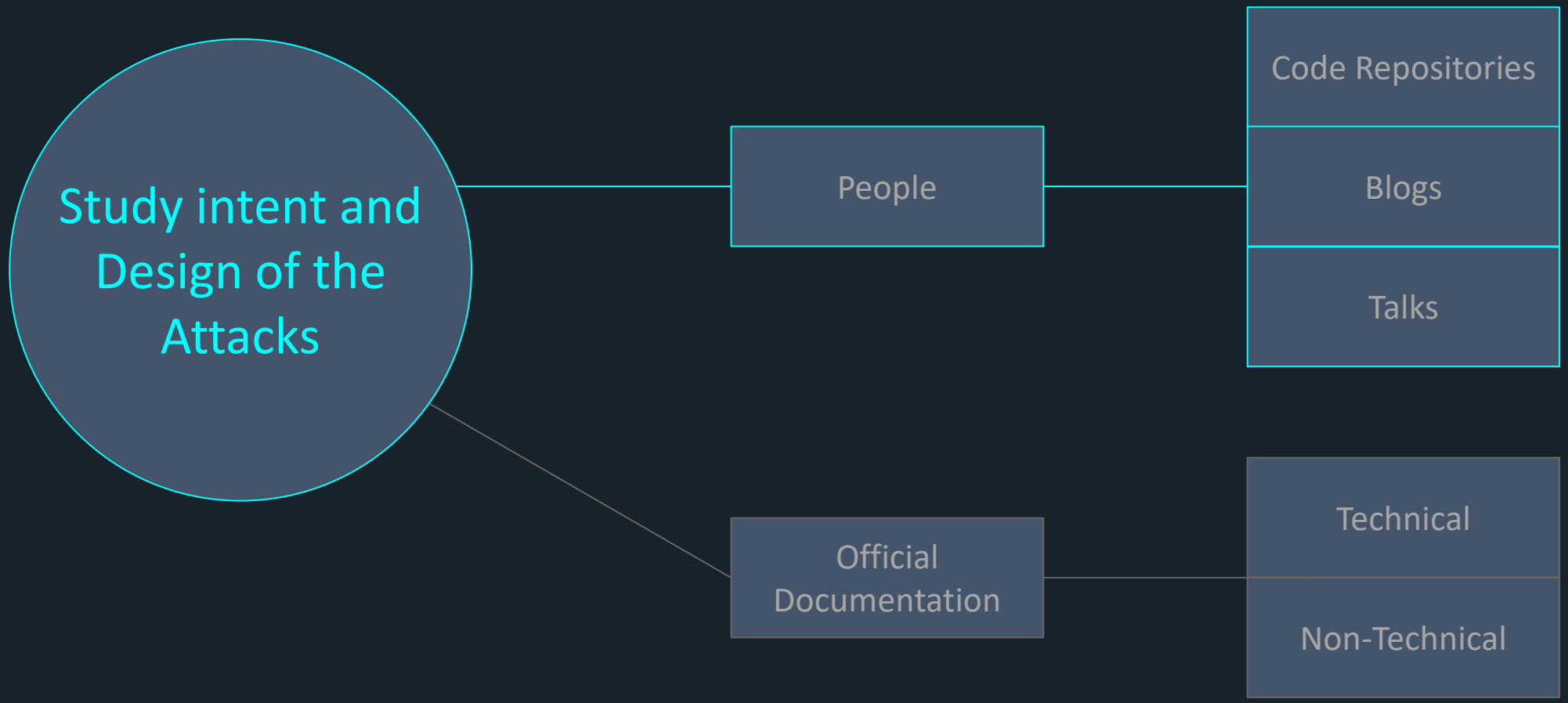


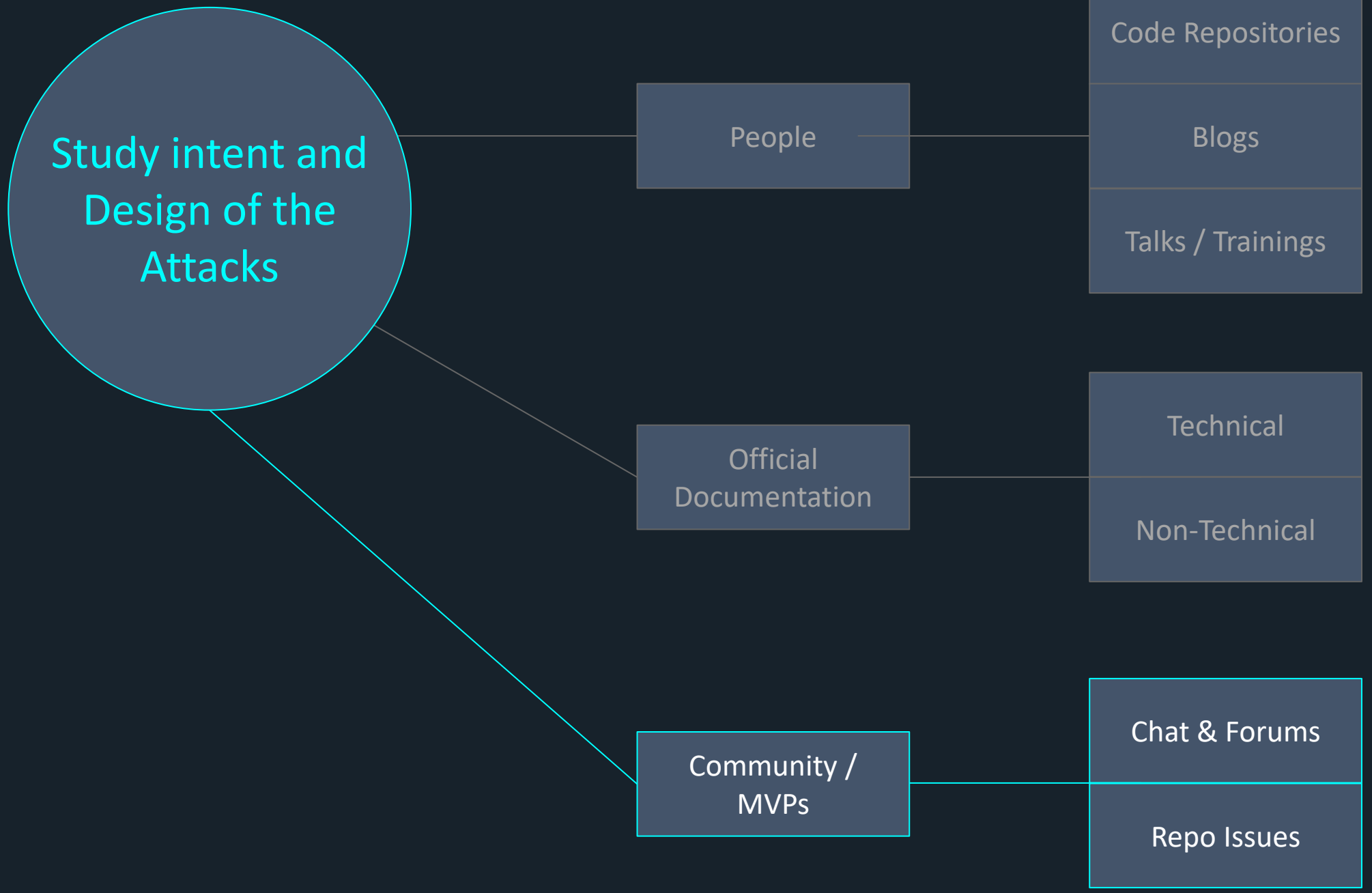
MSOLSpray

A password spraying tool for Microsoft Online accounts (Azure/ l is valid, if MFA is enabled on the account, if a tenant doesn't exist, if a user doe the account is disabled.

BE VERY CAREFUL NOT TO LOCKOUT ACCOUNTS!

CLOUD Katana


Study intent and Design of the Attacks
People
Code Repositories
Blogs
Talks
Official Documentation
Technical
Non-Technical


Study intent and Design of the Attacks
People
Code Repositories
Blogs
Talks / Trainings
Official Documentation
Technical
Non-Technical
Community / MVPs
Chat & Forums
Repo Issues

SwissMicrosoft SECURITY SUMMIT

Exploring Azure Cloud Attack Vectors In 2024 — Compromising Sensitive Storage Account Containers

Frank Kyazze · Follow · 10 min read · Jun 30, 2024

4

Hey there, friends! Ever felt like taking a day off from the usual grind and diving into the exhilarating world of Azure attack vectors? Well, buckle up, because today we're going on a joyride through the cloud!

Picture this: it's 2024, and the digital landscape is buzzing with opportunities and threats. Our mission? To explore Scenario 1 of the Azure attack vectors from the wonderful folks at XM Cyber, armed with nothing but our wits, an Azure tenant, Terraform (version 1.0.9 or above, please!), the trusty Azure CLI, and a user account with Owner permissions on Subscription and Global

From Azure AD to Active Directory (via Azure Unanticipated Attack Path

MAY 27 2020

By Sean Metcalf in Cloud Security, Microsoft Security, TheCloud

For most of 2019, I was digging into Office 365 and Azure AD and looking at features as part of the of the new Trimarc Microsoft Cloud Security Assessment which focuses on improving customer M 365 and Azure AD security posture. As I went through each of them, I found one that was very int

In May 2020, I presented some Microsoft Office 365 & Azure Active Directory security topics in a Webcast called "Securing Office 365 and Azure AD: Protect Your Tenant" and included the attack in this article that takes advantage of a little known feature.

While Azure leverages Azure Active Directory for some things, Azure AD roles don't directly affec Azure RBAC) typically. This article details a known configuration (at least to those who have dug ir configuration options) where it's possible for a Global Administrator (aka Company Administrator Directory to gain control of Azure through a tenant option. This is "by design" as a "break-glass" (e option that can be used to (re)gain Azure admin rights if such access is lost.
In this post I explore the danger associated with this option how it is currently configured (as of M

The key takeaway here is that if you don't carefully protect and control Global Administrator role associated accounts, you could lose positive control of systems hosted in all Azure subscriptions a 365 service data.

Note:
Most of the research around this issue was performed during August 2019 through December 2019 and Microsoft may have incorporated cha

Attack Scenario:
In this scenario, Acme has an on-pren a Service (IAAS) as an additional data their "cloud datacenter"). Acme IT loc administration to the VMs hosting th

Acme signed up for Office 365 and st

Cloud Security, Application security, API security

Attackers evade detection by leveraging Microsoft Graph API

May 3, 2024 · Share

By Steve Zurier

(Adobe Stock)

Attackers were observed evading detection by leveraging the Microsoft Graph API used by developers to access resources on Microsoft cloud services.

In a May 2 blog post, Symantec researchers said attackers are drawn to Graph API because they believe that executing their activities on known entities such as widely used Microsoft

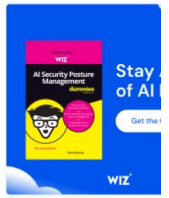
Hackers Increasingly Abusing Microsoft Graph API for Stealthy Malware Communications

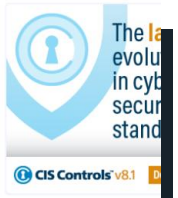
May 03, 2024 · Ravie Lakshmanan · Cloud Security / Threat Intelligence

Threat actors have been increasingly weaponizing Microsoft Graph API for malicious purposes with the aim of evading detection.

This is done to "facilitate communications with command-and-control (C&C) infrastructure hosted on Microsoft cloud services," the Symantec Threat Hunter Team, part of Broadcom, said in a report shared with The Hacker News.

Since January 2022, multiple nation-state-aligned hacking groups have been observed using Microsoft Graph API for C&C. This includes threat actors tracked as APT28, REF2924, Red Stinger, Fleg, APT29,





— Trending News

Play Ransomware E
Windows CVE-2025-

Community Alert: Ongoing Azure At Phishing and Cloud ATO

SHARE WITH YO

FEBRUARY 12, 2024 | THE PROOFPOINT CLOUD SECURITY RESPONSE TEAM

Over the past weeks, Proofpoint researchers have been monitoring an ongoing **cloud account takeover** campaign impacting dozens of Microsoft Azure environments and **hundreds of user accounts**, including senior executives. This post serves as a community warning regarding the Azure attack and offers suggestions that affected organiz implement to protect themselves from it.

What are we seeing?

In late November 2023, Proofpoint researchers detected a new malicious campaign affecting Microsoft Azure's cloud security, integrating **credential phishing** and cloud ac (**ATO**) techniques. As part of this campaign, which is still active, threat actors target users with individualized phishing lures within shared documents. For example, some w documents include embedded links to "View document" which, in turn, redirect users to a malicious **phishing** webpage upon clicking the URL.

Threat actors seemingly direct their focus toward a wide range of individuals holding diverse titles across different organizations, impacting hundreds of users globally. The base encompasses a wide spectrum of positions, with frequent targets including Sales Directors, Account Managers, and Finance Managers. Individuals holding executive as "Vice President, Operations", "Chief Financial Officer & Treasurer" and "President & CEO" were also among those targeted. The varied selection of targeted roles indicate strategy by threat actors, aiming to compromise accounts with various levels of access to valuable resources and responsibilities across organizational functions.

ck Paths

cluded in Azure Azure AD Entra ID PowerShell Security Sentinel KQL
18 words · 25 minutes

aining a secure environment is hard. And with every technology or product added to your s more complicated. Microsoft Azure as a cloud environment is no exception to this rule and ices and features that get added every year it just gets more complicated even if you did not cause keeping your IT assets secure is important as you move to the cloud, it is important to actices to avoid and which attack scenarios are out there.

I want to shed some light on known attack paths in an Azure environment. The attacks are no relied on public research from other IT security professionals while writing this article. Like ctive Directory I thought it is important to make this information as easily accessible as ow different services and permissions can lead to a vulnerable environment is key and having n in one place is a good start.

s help to ease some of the complexity, I based my overview of the different attack paths on

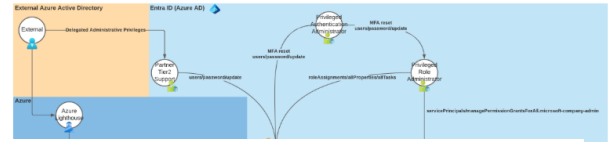
nformation included in the published work for each attack path, I limited my writeup to a bri and you will have to read the original articles for the nitty-gritty details and in-depth 't want to just replicate the original authors work, but create a starting point for everybody o nd the information I was looking for, I included a more detailed description in this article.

tacks are not just academic in nature, but are used by attackers in the real world.

Note

If provided, all hunting queries will be based on PowerShell or Kusto/KQL queries. For the latter you will have to forward you Azure and Entra ID (Azure AD) activity to a Log Analytics workspace. This workspace, in most cases, does not have to be Microsoft Sentinel enabled to execute the queries, but I try to optimize them for usage in Sentinel.

Map



Microsoft Graph API Emerges as a Top Attacker Tool to Plot Data Theft

Weaponizing Microsoft's own services for command-and-control is simple and costless, and it helps attackers better avoid detection.

Nate Nelson, Contributing Writer · May 2, 2024 · 3 Min Read

SOURCE: ROBERT K CHIN STOREFRONTS VIA ALAMY STOCK PHOTO

Related Content Sponsored by snyk

RESOURCES · TWITTER

Whitepaper: DevSecOps is dead...or is it?
Many organizations still find it challenging to effectively implement and meaningfully integrate security into rapid, agile DevOps practices. Dive into Snyk's six pillars for success and how we arrived here in the first place.

Zero to hero: A blueprint for establishing a security champions program
Security champions programs are a proven method for scaling security across large development teams. Snyk met with security leaders around the globe to compile the ultimate blueprint to building, implementing, and scaling a security champions program.

ChatGPT o3

What's on your mind today?

Can you resume this pages on key points

SwissMicrosoft SECURITY SUMMIT

Blog Posts	Interesting	Community/MVP	Tools
1. Azure Attack Path (6)	9. ROADrecon (5)	https://danielchronlund.com/2022/01/07/the-attackers-guide-to-az	https://github.com/Gerenios/AADInternals
https://cloudbrothers.info/en/azure-attack-paths/	https://github.com/dirkjanm/ROADtools#rc	https://aadinternals.com/post/prt/	GitHub - LMGsec/o365creeper: Python script that performs email address validation against Office 365 without s
https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/operationalizing-a	https://dirkjanm.io/roadrecon-explore-you	https://aadinternals.com/post/just-looking/	https://github.com/NetSPI/MicroBurst
https://sofblocks.github.io/azure-attack-paths/	https://www.youtube.com/watch?v=oHt-Pl	https://aadinternals.com/aadkillchain/	GitHub - dafthack/MSOLSpray: A password spraying tool for Microsoft Online accounts (Azure/O365). The script I
https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-attack-path	https://posts.specterops.io/visualizing-azur	https://cloudbrothers.info/en/azure-attack-paths/	Issues · ustayready/fireprox
https://posts.specterops.io/intune-attack-paths-part-1-4ad1882c1811	https://thedfirreport.com/2023/12/20/roadi	https://cloudbrothers.info/en/prem-global-admin-password-reset/	GitHub - kgretzky/evilginx2: Standalone man-in-the-middle attack framework used for phishing login credentials
https://argos-security.io/2023/11/18/discovering-attack-paths-in-microsoft-azure-for-enhanced-security/		https://jeffreyappel.nl/aitm-mfa-phishing-attacks-in-combination-	GitHub - dirkjanm/ROADtools: A collection of Azure AD/Entra tools for offensive and defensive security purpose
cloudbrothers.info	8. Azure Persistence (6)	https://www.verboon.info/2020/05/meet-the-new-microsoft-defe	GitHub - Azure/Stormspotter: Azure Red Team tool for graphing Azure and Azure Active Directory objects
TECHCOMMUNITY.MICROSOFT.COM	https://posts.specterops.io/azure-ad-persis	https://dirteam.com/sander/2021/08/10/two-new-azure-ad-connec	GitHub - SpecterOps/AzureHound: Azure Data Exporter for BloodHound
Sofblocks	https://www.mandiant.com/resources/blog	https://samilamppu.com/2022/03/22/introduction-of-azure-ad-atta	GitHub - Azure/Stormspotter: Azure Red Team tool for graphing Azure and Azure Active Directory objects
Microsoft Learn	https://rhysida2.com/azure-automation-acc	https://securecloud.blog/2022/05/05/cross-tenant-attacks-via-mult	GitHub - Azure/Stormspotter: Azure Red Team tool for graphing Azure and Azure Active Directory objects
Posts By SpecterOps Team Members	https://outflank.nl/blog/2024/02/27/malicic	https://www.karlots.com/blog/azure-audit-logs	GitHub - mdsecactivebreach/o365-attack-toolkit: A toolkit to attack Office365
blog.pwnedlabs.io	https://labs.nccgroup.com/2023/09/10/pers	https://www.dsinternals.com/en/how-azure-active-directory-conn	Home - PingCastle
argos-security.io	https://github.com/RhinoSecurityLabs/clou	https://cqureacademy.com/hacks/pass-the-prt-attack	Monkey365
		https://derkvanderwoude.medium.com/pass-the-prt-attack-and-de	GitHub - silverhack/monkey365: Monkey365 provides a tool for security consultants to easily conduct not only M
2. Azure Attack (6)	13. PRT / Pass-the-PRT Attack (5)	https://practical365.com/use-azure-ad-admin-consent-requests-to-	GitHub - cammurray/orca: The Microsoft Defender for Office 365 Recommended Configuration Analyzer (ORCA)
https://blog.pwnedlabs.io/mapping-attack-surface-for-azure-initial-access	https://posts.specterops.io/pass-the-prt-st	https://dirteam.com/sander/2021/08/10/two-new-azure-ad-connec	https://github.com/cisagov/ScubaGear
https://www.netspi.com/blog/technical/cloud-penetration-testing/15-ways-to-hack-azure	https://andyrobbins.com/primary-refresh-t	https://merill.net/2019/11/password_hash_sync_and_staged_rollou	microsoft-graph-docs-contrib/api-reference/beta/resources/attacksimulationroot.md at main · microsoftgraph/
https://www.wiz.io/blog/chaosdb-critical-azure-vulnerability	https://www.mandiant.com/resources/toke	https://jeffreyappel.nl/protecting-against-password-spray-attacks-	microsoft-graph-docs-contrib/api-reference/v1.0/api/attacksimulationroot-list-simulationautomations.md at m
https://www.microsoft.com/en-us/security/blog/2024/01/18/defending-against-modern-c	https://github.com/Gerenios/AADInternals,	https://samilamppu.com/2022/03/22/introduction-of-azure-ad-atta	https://github.com/microsoft/CloudKatana
https://www.mandiant.com/resources/blog/from-on-prem-to-azuread-takeover	https://www.microsoft.com/security/blog/2024/05/07/defending-against-prt-token-theft/		
https://unit42.paloaltonetworks.com/top-azure-threats-2024/			
	14. Azure MFA Bypass (5)		
3. Graph API Attack (6)	https://www.secureworks.com/blog/bypassing-azure-mfa-legacy-auth		
https://dirkjanm.io/abusing-azure-ad-graph-api/	https://research.nccgroup.com/2024/01/10/mfa-bypass-techniques-office-365/		
https://posts.specterops.io/graph-api-privilege-escalation-in-azure-7b2cb14c4e44	https://learn.microsoft.com/en-us/entra/fundamentals/legacy-authentication-block		
https://labs.nccgroup.com/2024/02/05/office-365-and-microsoft-graph-api-exploitation/	https://www.proofpoint.com/us/blog/threat-insight/phishing-kits-bypass-azure-mfa		
https://github.com/samccann/GraphRunner	https://www.withsecure.com/en/resources/mfa-fatigue-attacks-in-entra-id		
https://www.microsoft.com/security/blog/2022/04/20/illicit-consent-grant-attacks-graph-api/			
https://www.f-secure.com/en/resources/insights/exploiting-microsoft-graph-api			
4. Azure Pentest (6)			
https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-pentesting-101-part-1/			
https://rhinosecuritylabs.com/azure/hacking-azure-pentesters-guide/			
https://www.blackhillsinfosec.com/azure-ad-pentest-cheat-sheet/			
https://github.com/microsoft/CloudKatana			
https://book.hacktricks.xyz/cloud-security/azure-methodology			
https://media.defcon.org/DEF%20CON%2031/DEF%20CON%2031%20presentations/DEF%20CON%2031%20-%20Speaker%20-%20Hacking%20Azure%20from%20the%20Cloud.pdf			
5. AzureHound / BloodHound (6)			
https://github.com/BloodHoundAD/AzureHound			
https://posts.specterops.io/introducing-azurehound-5b2bcb1fa813			
https://posts.specterops.io/azurehound-community-edition-release-2024-1d9be3a2f113			
https://bloodhound.readthedocs.io/en/latest/data-collection/azurehound.html			
https://cptofevil.com/posts/using-azurehound-for-red-teaming/			
https://www.youtube.com/watch?v=Y0P_MSTXB1c			
6. Secure Azure (6)			
https://learn.microsoft.com/en-us/azure/security/fundamentals/best-practices			

SwissMicrosoft SECURITY SUMMIT

Phishing

MS GRAPH

MFA Bypass

Enumeration

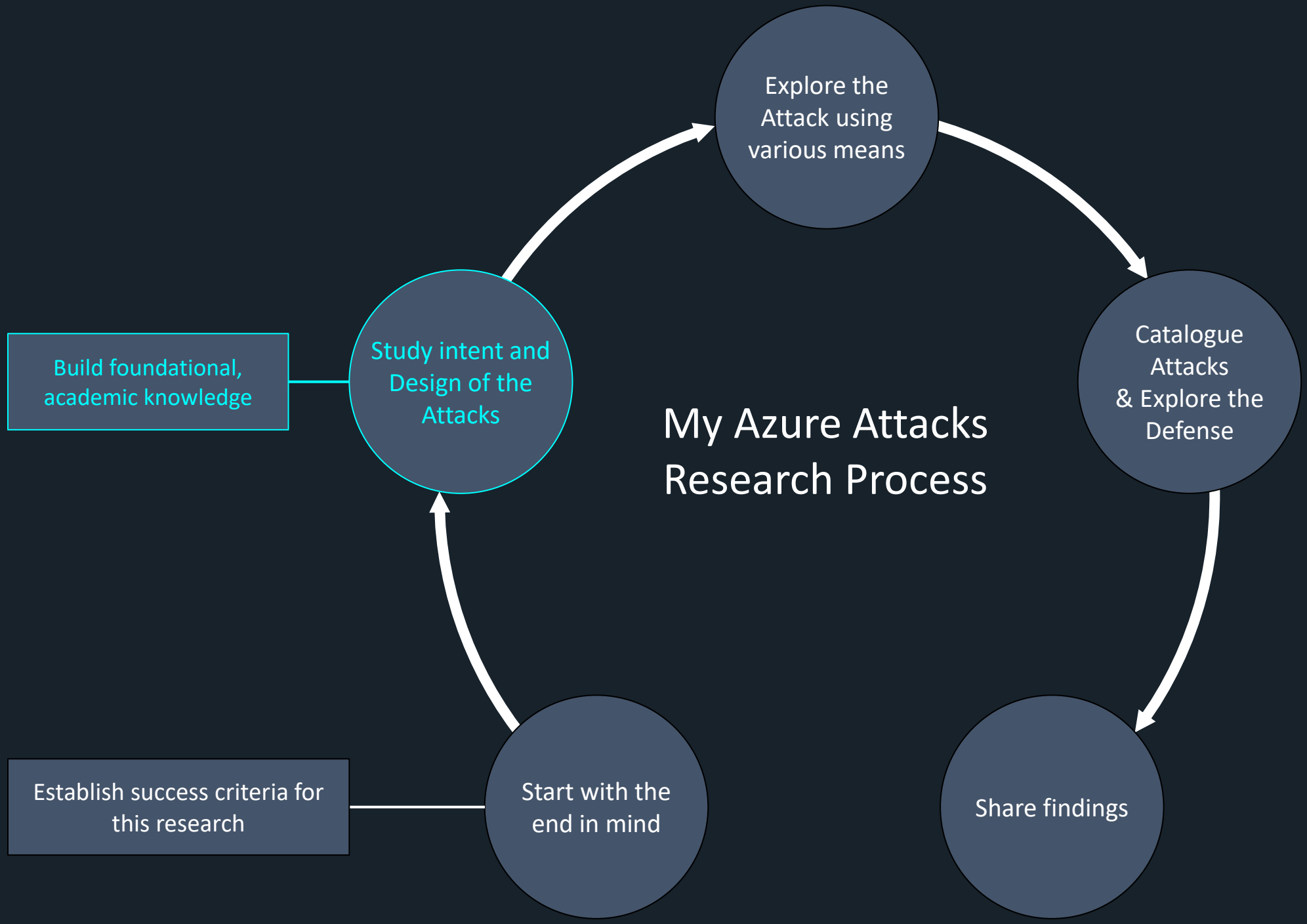
TOKEN

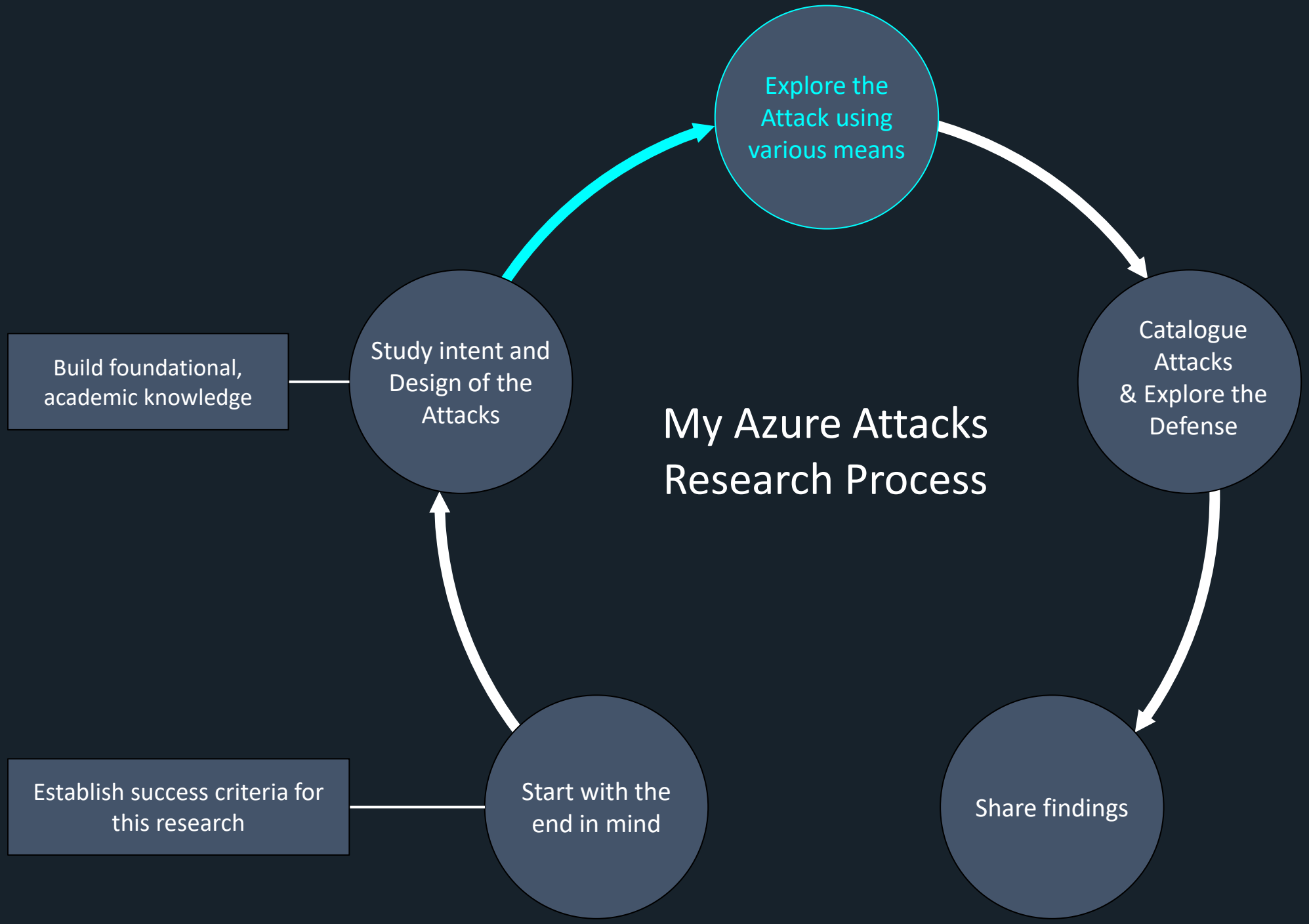
PRT

Illicit consent grant

AzureHound

My Azure Attacks Research Process



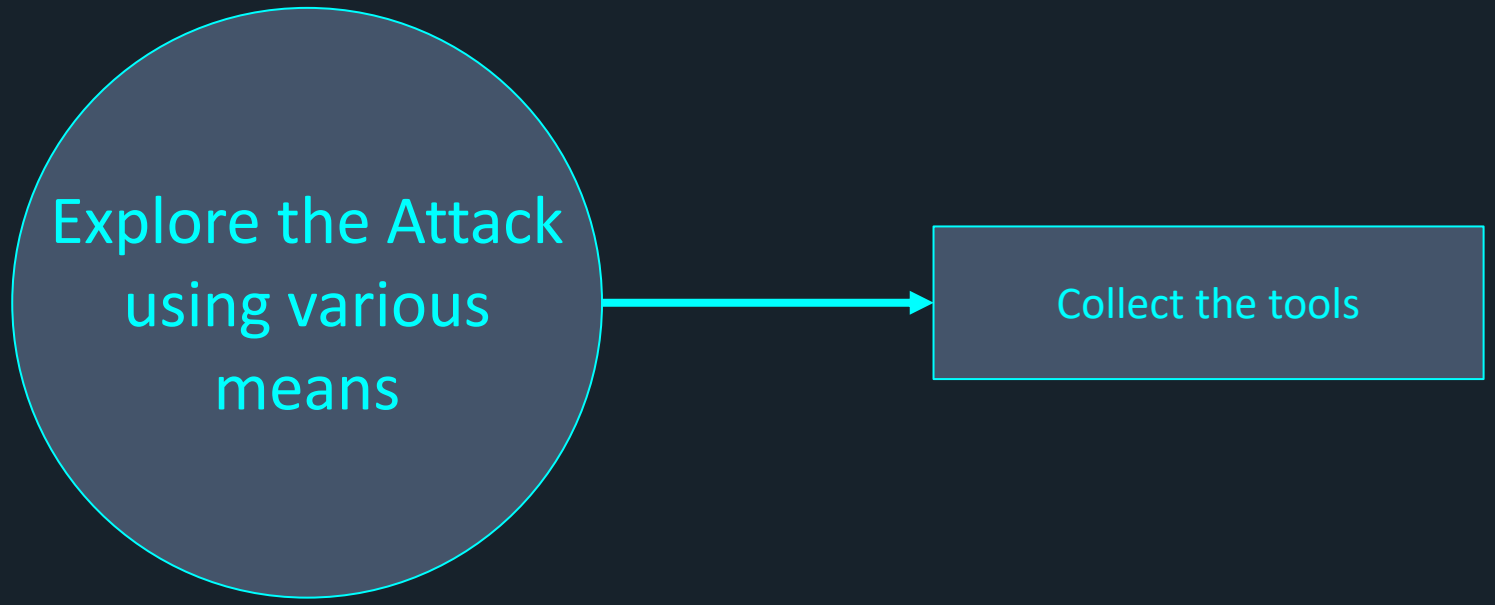

Explore the Attack using various means
Catalogue Attacks & Explore the Defense
Share findings
Start with the end in mind
Establish success criteria for this research
Study intent and Design of the Attacks
Build foundational, academic knowledge
My Azure Attacks Research Process

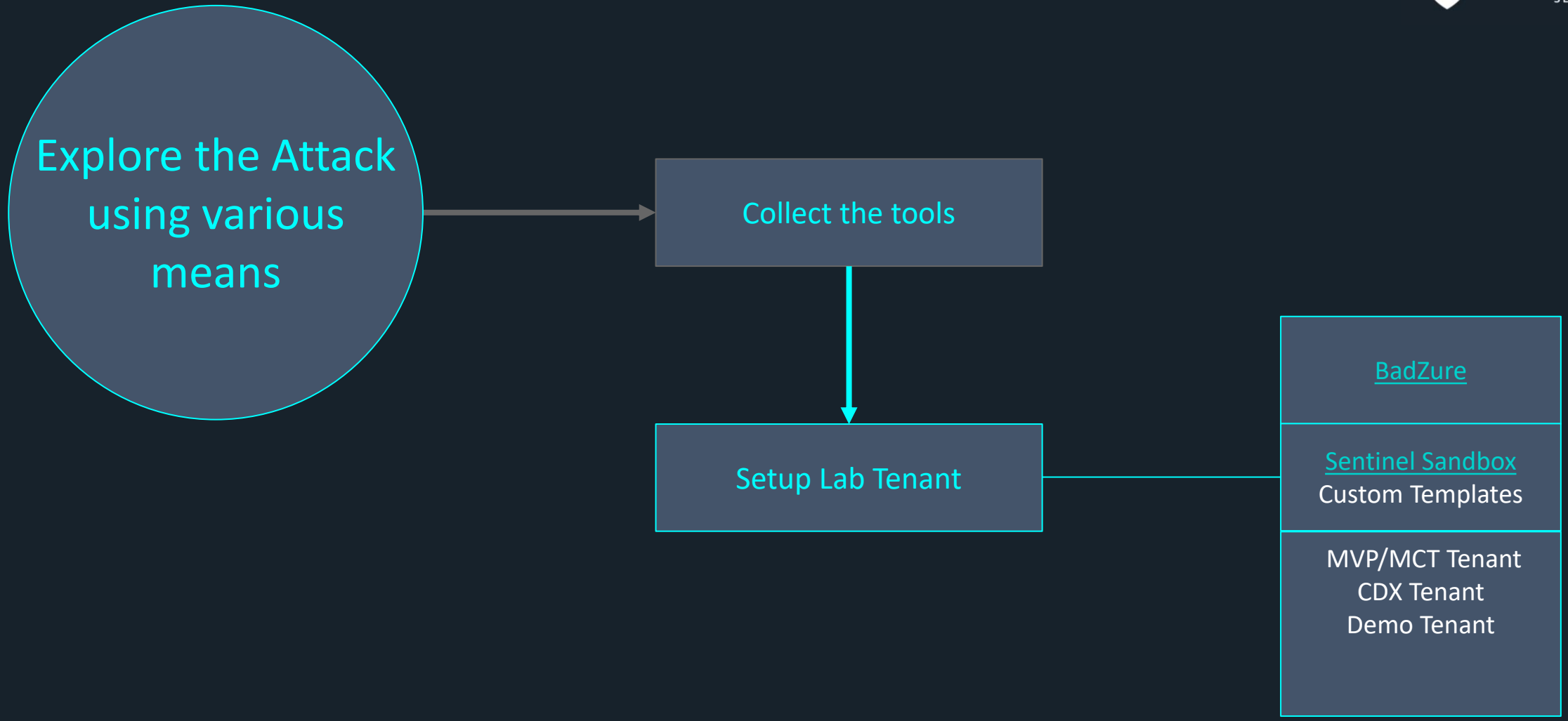
You must go beyond the documentation.

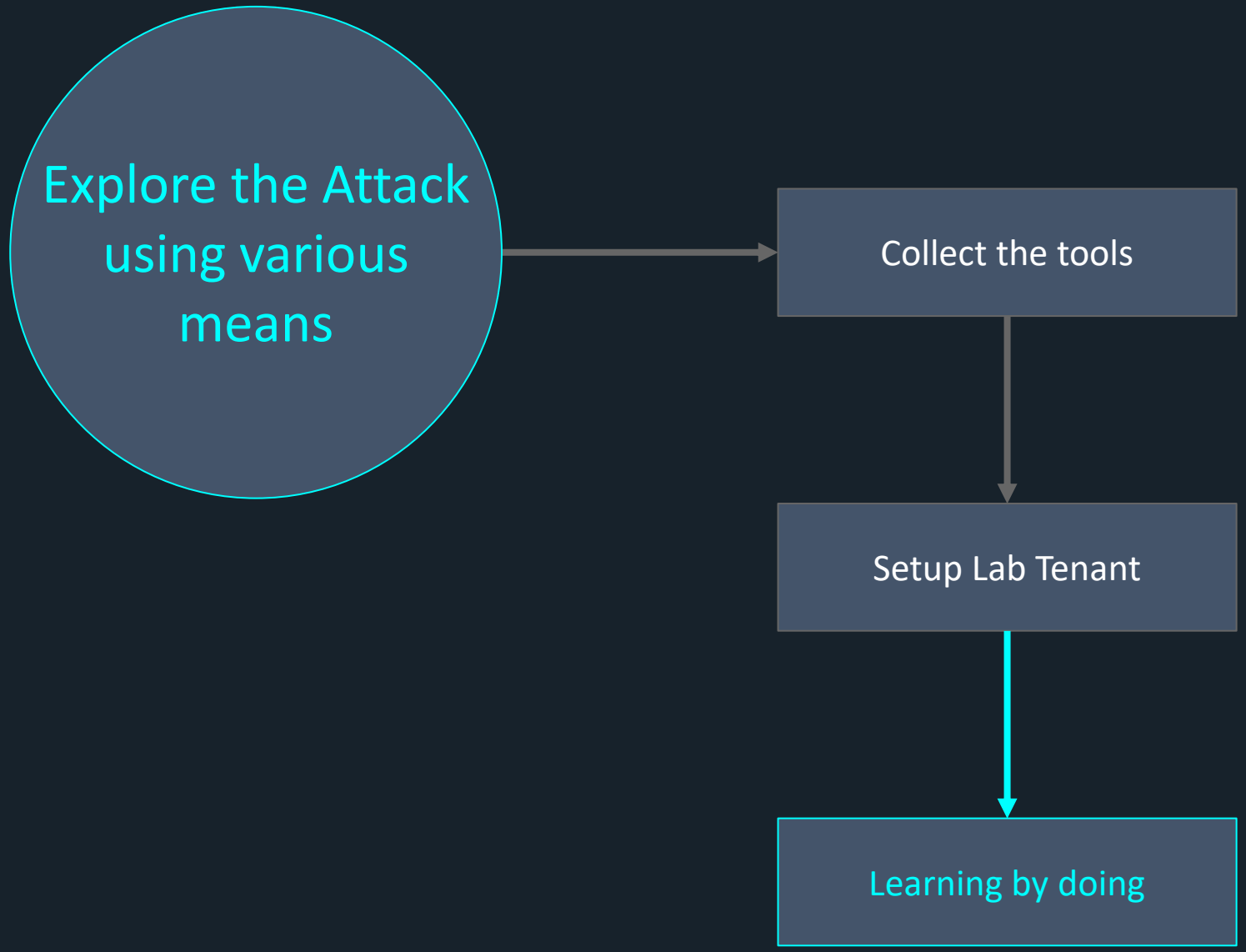
- These Attacks are interconnected in undocumented and non-public ways
- Documentation often doesn’t keep up with changes
- Tooling based only on documentation is almost always inaccurate, unreliable tooling.

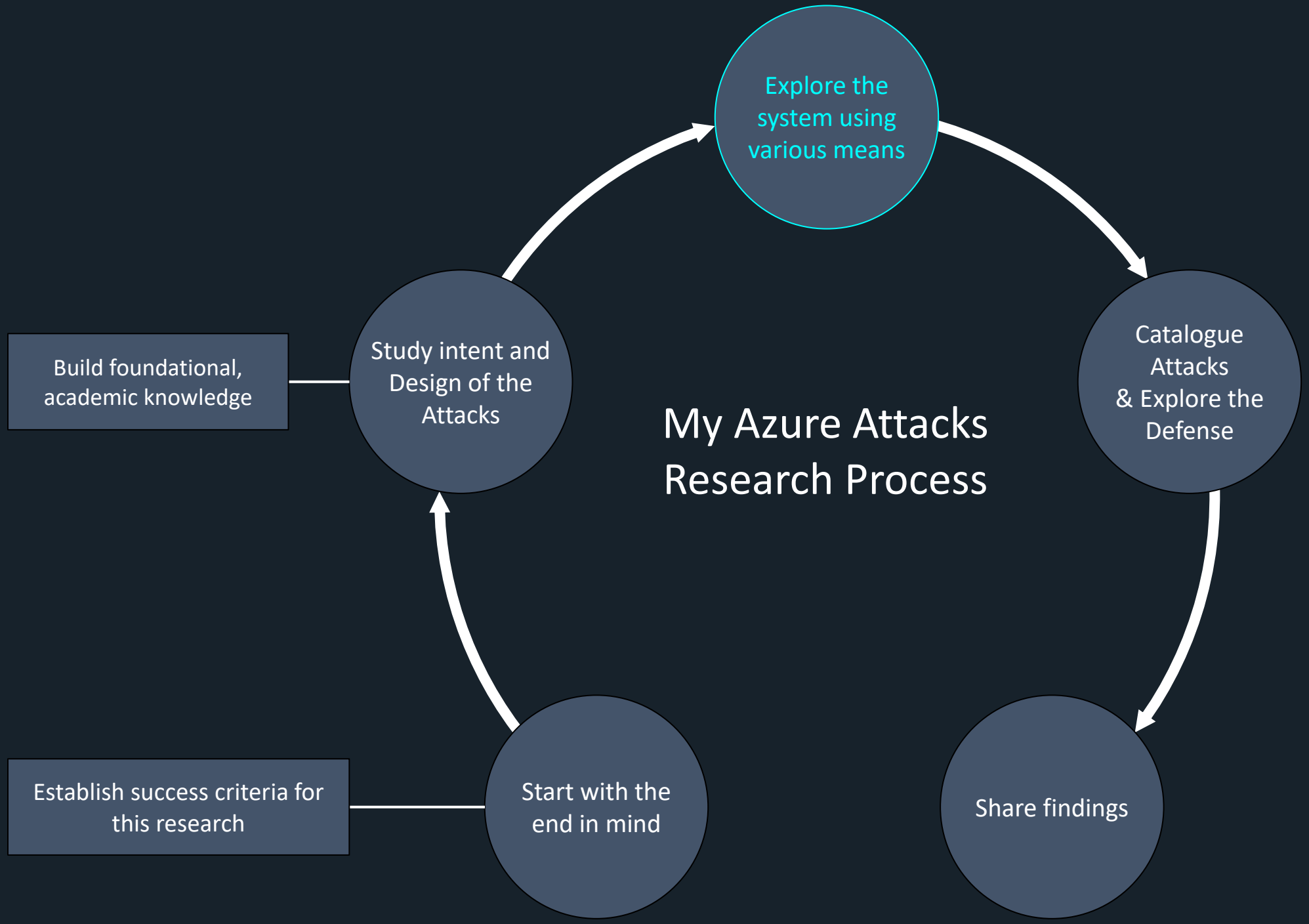
SwissMicrosoft
SECURITY SUMMIT

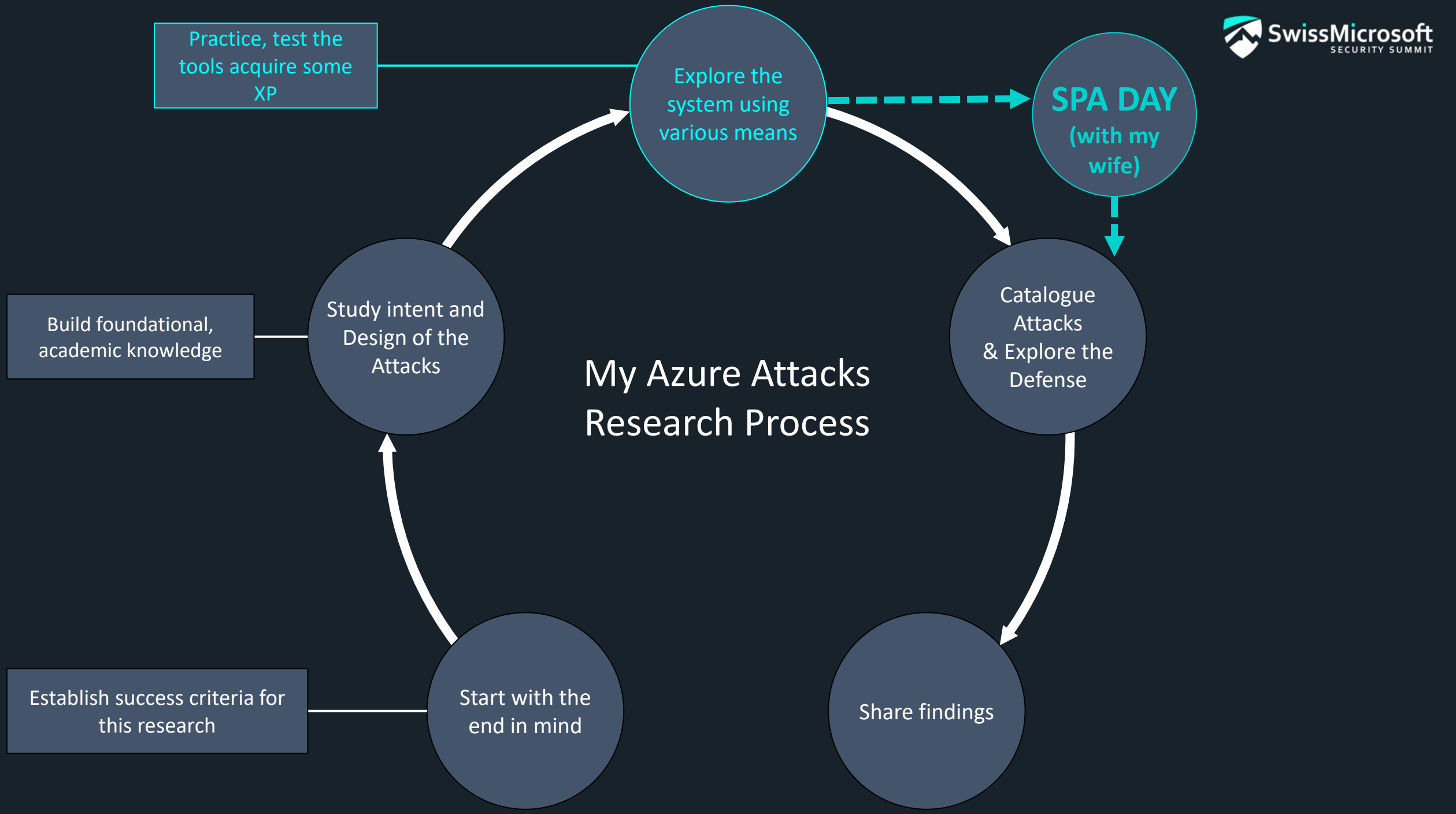
Explore the Attack using various means

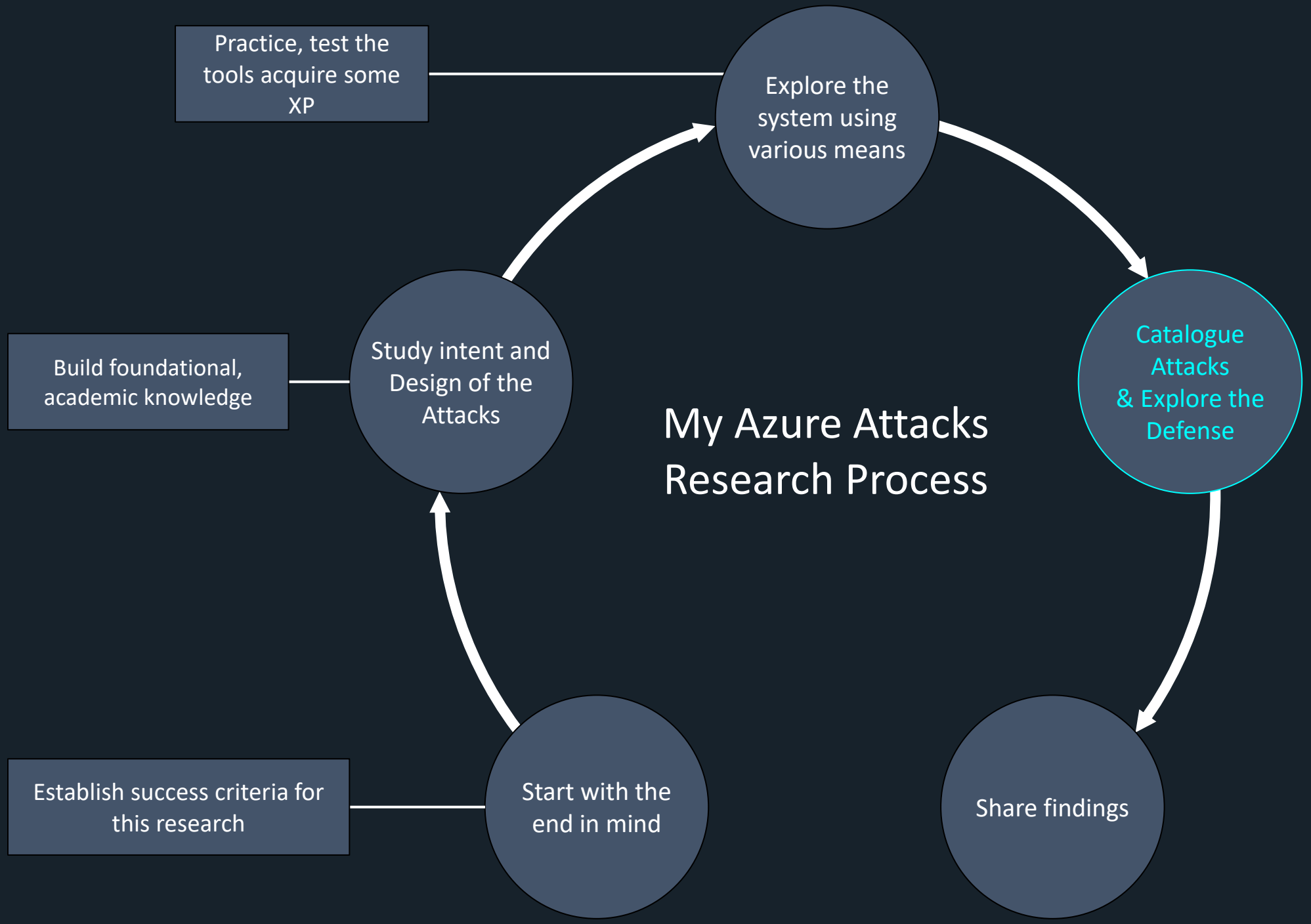

Explore the Attack using various means
Collect the tools

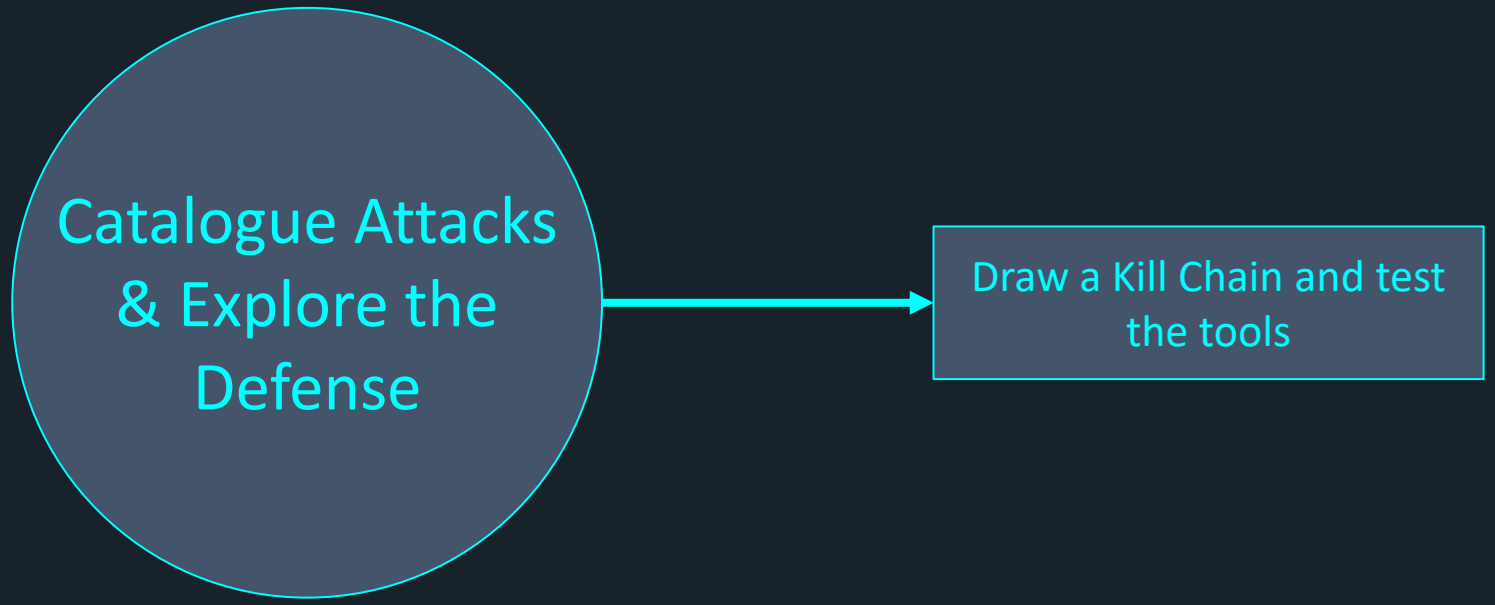

Explore the Attack using various means
Collect the tools
Setup Lab Tenant
BadZure
Sentinel Sandbox
Custom Templates
MVP/MCT Tenant
CDX Tenant
Demo Tenant

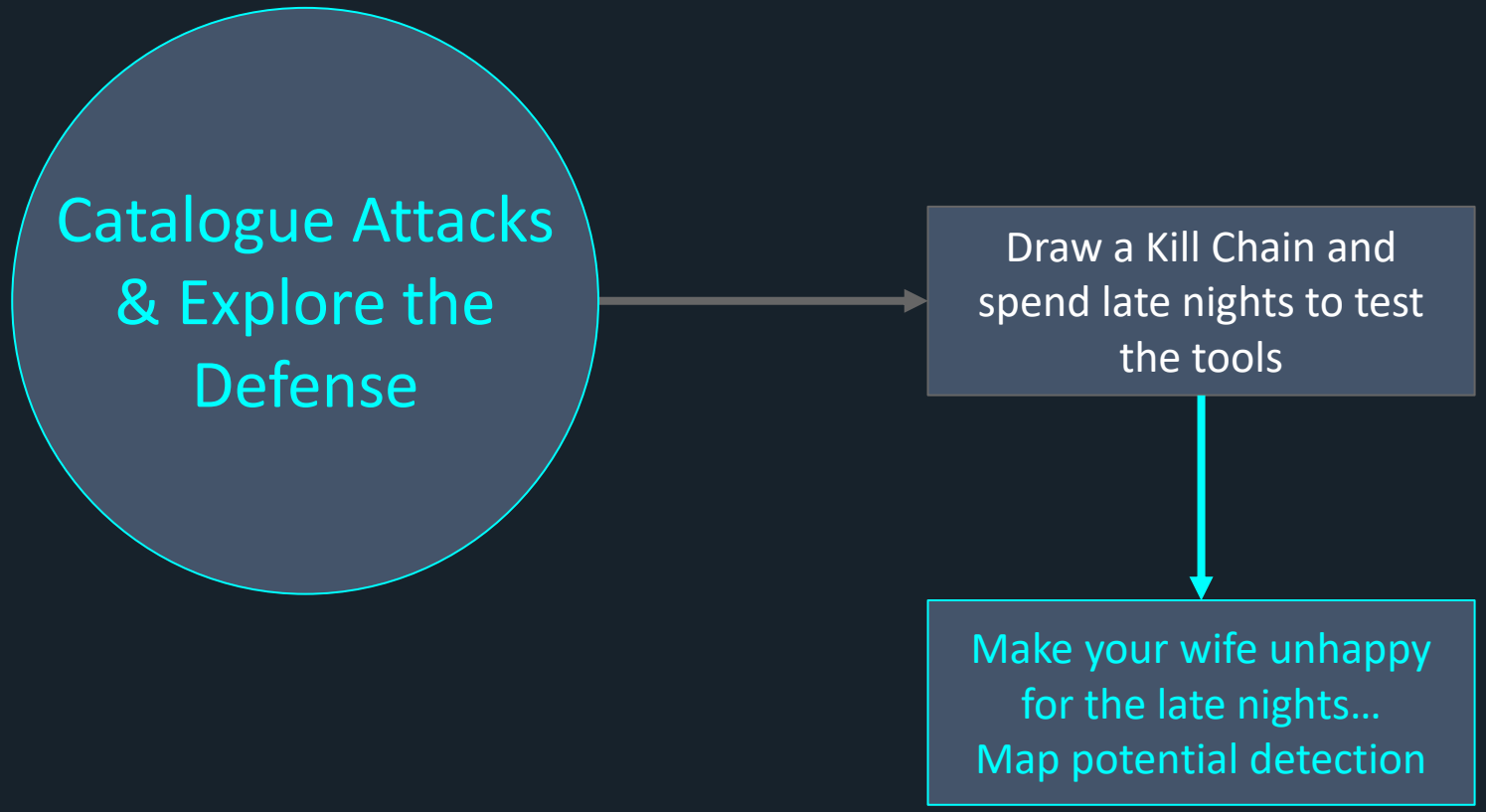

Explore the Attack using various means
Collect the tools
Setup Lab Tenant
Learning by doing

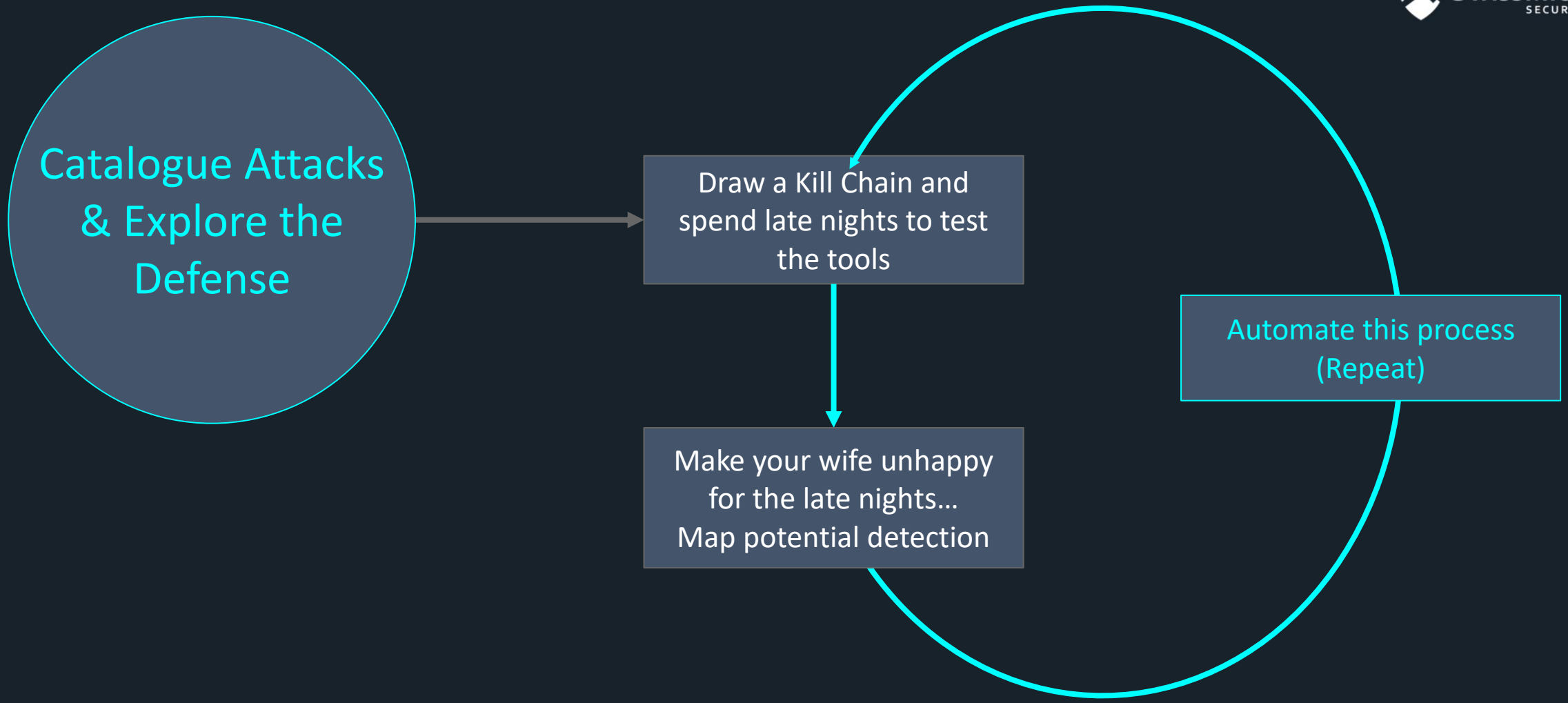

Explore the system using various means
Catalogue Attacks & Explore the Defense
Share findings
Start with the end in mind
Establish success criteria for this research
Study intent and Design of the Attacks
Build foundational, academic knowledge
My Azure Attacks Research Process


SwissMicrosoft
SECURITY SUMMIT
Practice, test the tools acquire some XP
Explore the system using various means
SPA DAY (with my wife)
Catalogue Attacks & Explore the Defense
Share findings
Start with the end in mind
Establish success criteria for this research
Study intent and Design of the Attacks
Build foundational, academic knowledge
My Azure Attacks Research Process


Practice, test the tools acquire some XP
Explore the system using various means
Catalogue Attacks & Explore the Defense
Share findings
Start with the end in mind
Establish success criteria for this research
Study intent and Design of the Attacks
Build foundational, academic knowledge
My Azure Attacks Research Process

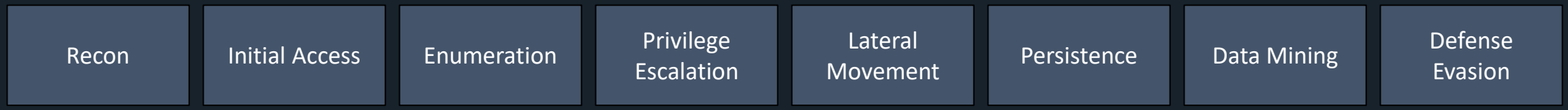

Catalogue Attacks & Explore the Defense
Draw a Kill Chain and test the tools


Catalogue Attacks & Explore the Defense
Draw a Kill Chain and spend late nights to test the tools
Make your wife unhappy for the late nights…
Map potential detection


Catalogue Attacks & Explore the Defense
Draw a Kill Chain and spend late nights to test the tools
Make your wife unhappy for the late nights…
Map potential detection
Automate this process (Repeat)

SwissMicrosoft SECURITY SUMMIT

Azure Attack Kill Chain



Azure Attack Kill Chain

Recon	Initial Access	Enumeration	Privilege Escalation	Lateral Movement	Persistence	Data Mining	Defense Evasion

- Azure Tenant usage
- Tenant ID
- Tenant Name
- Auth. Type (Federation or not)
- Domains
- Azure Services used
- Email Ids

- AADInternals (https://github.com/Gerenios/AADInternals) → used for multiple attacks against Azure Entra ID
- O365creeper (https://github.com/LMGsec/o365creeper) → check if an email ID belongs to a tenant
- MicroBurst (https://github.com/NetSPI/MicroBurst) → useful tool for security assessment of Azure

SwissMicrosoft SECURITY SUMMIT

Azure Attack Kill Chain

Recon	Initial Access	Enumeration	Privilege Escalation	Lateral Movement	Persistence	Data Mining	Defense Evasion

- Password Spraying
- Brute Force

Clearly noisy techniques easy to detect

Password spray attack can be done against different API endpoints, Azure Tenant Graph, Microsoft Graph, Office 365 Reporting webservice etc.

- MSOLSpray (https://github.com/dafthack/MSOLSpray) → used for password spray against the accounts that we discovered
- Fireprox (https://github.com/ustayready/fireprox) → to rotate source IP address on auth request
- Evilginx3 (https://github.com/kgretzky/evilginx2) → for phishing attacks
  - (acts as a relay/man-in-the-middle between the legit web page and the target user, pure beauty tool ;))

Azure Attack Kill Chain

Recon	Initial Access	Enumeration	Privilege Escalation	Lateral Movement	Persistence	Data Mining	Defense Evasion

A normal user account has many interesting permissions in Entra ID!

- Read all users, Groups, Applications, Devices, Roles, Subscriptions, and their public properties
- Create Security groups
- Read non-hidden Group memberships
- Add guests to Owned groups
- Create new application
- Invite Guests
- Add up to 50 devices to Azure

- MSGraph (PowerShell module) → used for managing Entra ID and other M365 services, API wrapper for MSGraph API
  - Install-Module Microsoft.Graph
- RoadRecon (https://github.com/dirkjanm/ROADtools) → Powerful tool for enumerating Entra ID environments
- StormSpotter (https://github.com/Azure/Stormspotter) → tool from Microsoft for creating attack graphs of Azure resources
- BloodHound/AzureHound (https://github.com/BloodHoundAD/AzureHound) → supports Azure / Entra ID to map attack paths
- O365 Attack toolkit (https://github.com/mdsecactivebreach/o365-attack-toolkit) → abuse the consent grant settings

SwissMicrosoft
SECURITY SUMMIT

DEMO 2

Azure Attack Kill Chain

Recon	Initial Access	Enumeration	Privilege Escalation	Lateral Movement	Persistence	Data Mining	Defense Evasion

Automation Account abuse
Key Vault
Arm Templates
Function App

- Az PowerShell / Az CLI (Get-AzAutomationAccount, Get-AzDeployment)-
- AADInternals (Invoke-AADIntAddAADAppSecret
- StormSpotter & AzureHound to visualise escalation paths
  CloudKatana playbooks for Key Vault

Azure Attack Kill Chain

Recon	Initial Access	Enumeration	Privilege Escalation	Lateral Movement	Persistence	Data Mining	Defense Evasion

- Azure VMs Abuse (script insertion)
- Azure VMs (User Data Abuse)
- Entra ID Devices (Entra join, Entra registration or Entra hybrid join abuse)
- PRT (Primary Refresh Token) / Pass-the-PRT
- Intune → Cloud to On-Prem (execute PowerShell scripts on an enrolled Windows device)
- Dynamic Groups
- Application Proxy
- Hybrd Identity -> Entra Connect / Cloud Sync
  Password Hass Sync Abuse

- ROADtoken / roadtx (PRT extraction & replay)
- Mimikatz (sekurlsa::cloudap)
- Endpoint Manager portal automation or Invoke-DeviceManagementScript
- AADInternals (ConvertTo-AADIntBackdoor, PTAspy)

Azure Attack Kill Chain

Recon	Initial Access	Enumeration	Privilege Escalation	Lateral Movement	Persistence	Data Mining	Defense Evasion

- Trusted Domain
- Token Signing Certificate
- Storage Account Access Keys
- Applications and Service Principals
- Illicit Consent Grant
- Azure VMs and NSGs
- Custom Entra ID Roles
- Deployment Modification
- AzureAdSSACC – On-Prem to Cloud
  - Password/key of the AZUREADSSOACC never changes

- AzADAppSecret.ps1
- AADInternals (Open-AADIntOffice365Portal, New-AADIntADFSSelfSignedCertificates)
- AzCopy / Storage Explorer for key abuse
- …

Azure Attack Kill Chain

Recon	Initial Access	Enumeration	Privilege Escalation	Lateral Movement	Persistence	Data Mining	Defense Evasion

- Public / mis-scoped Storage Blobs – code & credential dumps
- Key Vault secret dumps after escalation
- Graph API – enumerate mail, Teams chats, SharePoint once tokens obtained

- Token replay from compliant location
- **Modify/clear Log Analytics retention** to 0 days
- Rename or hide Runbooks
- Access Defender Portal
- Abuse “Exclude service principals from MFA”

- MicroBurst (Invoke-EnumerateAzureBlobs, Invoke-EnumerateAzureSubDomains)
- Az CLI / az keyvault secret download
- GraphRunner / ROADrecon for bulk Graph pulls

- CloudKatana to simulate and test detection gaps

SwissMicrosoft SECURITY SUMMIT

Program of today

- Introduction
- Azure Fundamentals
- Research process
- Azure Kill Chain & tools for attacks
- Best approach for Detection
- Conclusion

SwissMicrosoft SECURITY SUMMIT

Defense Strategy

Fundamentals

Awareness

Trainings

Patching / Baselines

Microsoft offering

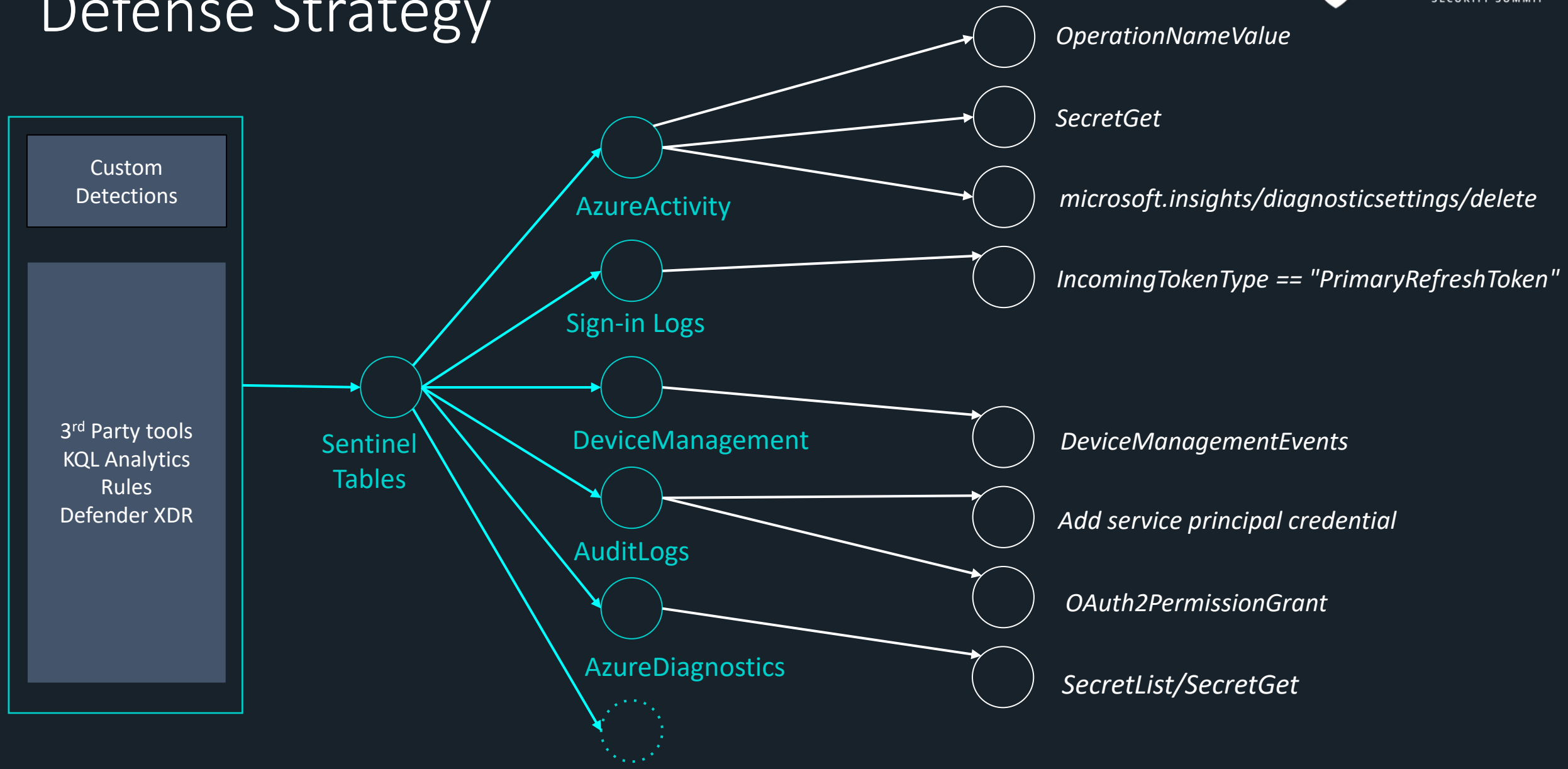
Microsoft Products ($)

Security Best Practices
Azure Security Fundamentals
Cloud Security Benchmark
Defender for Cloud
Secure Score
Secure Identity
Secure Apps and data with Entra ID
Mechanism
MFA
Conditionnal Access / Policies
Exposure Managagement

Custom Detections

3rd Party tools
KQL Analytics Rules
Defender XDR

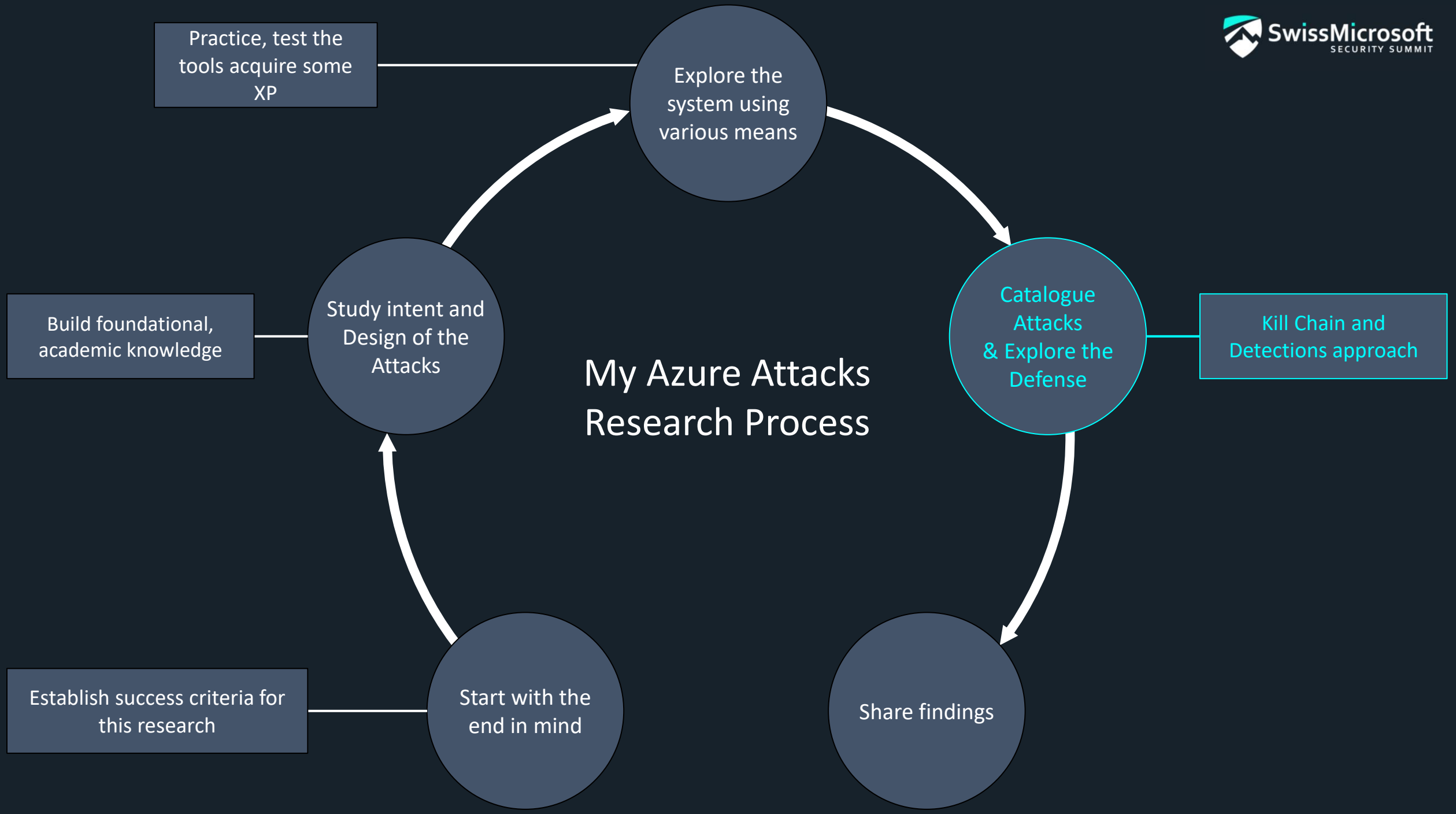
Defense Strategy

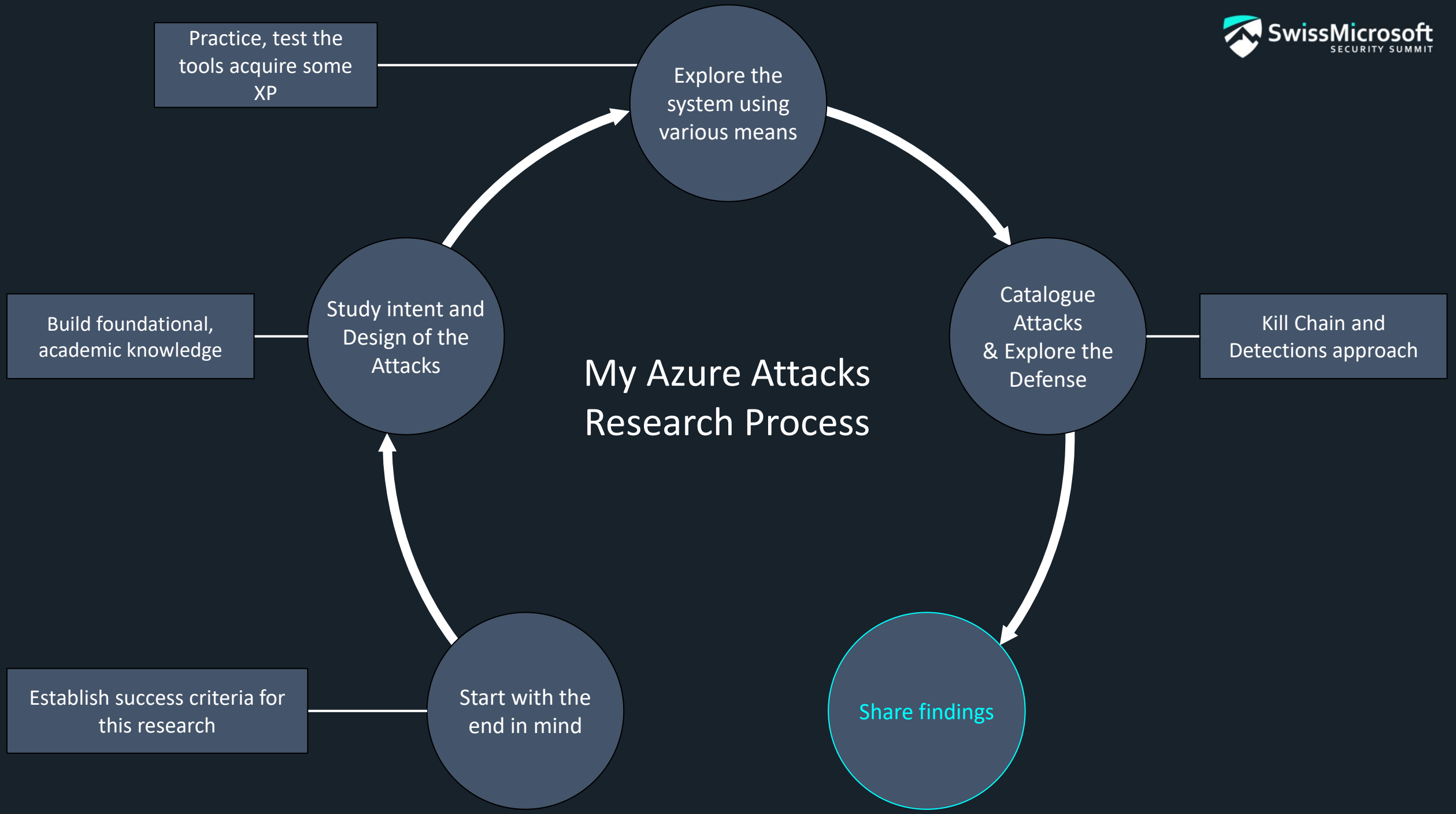


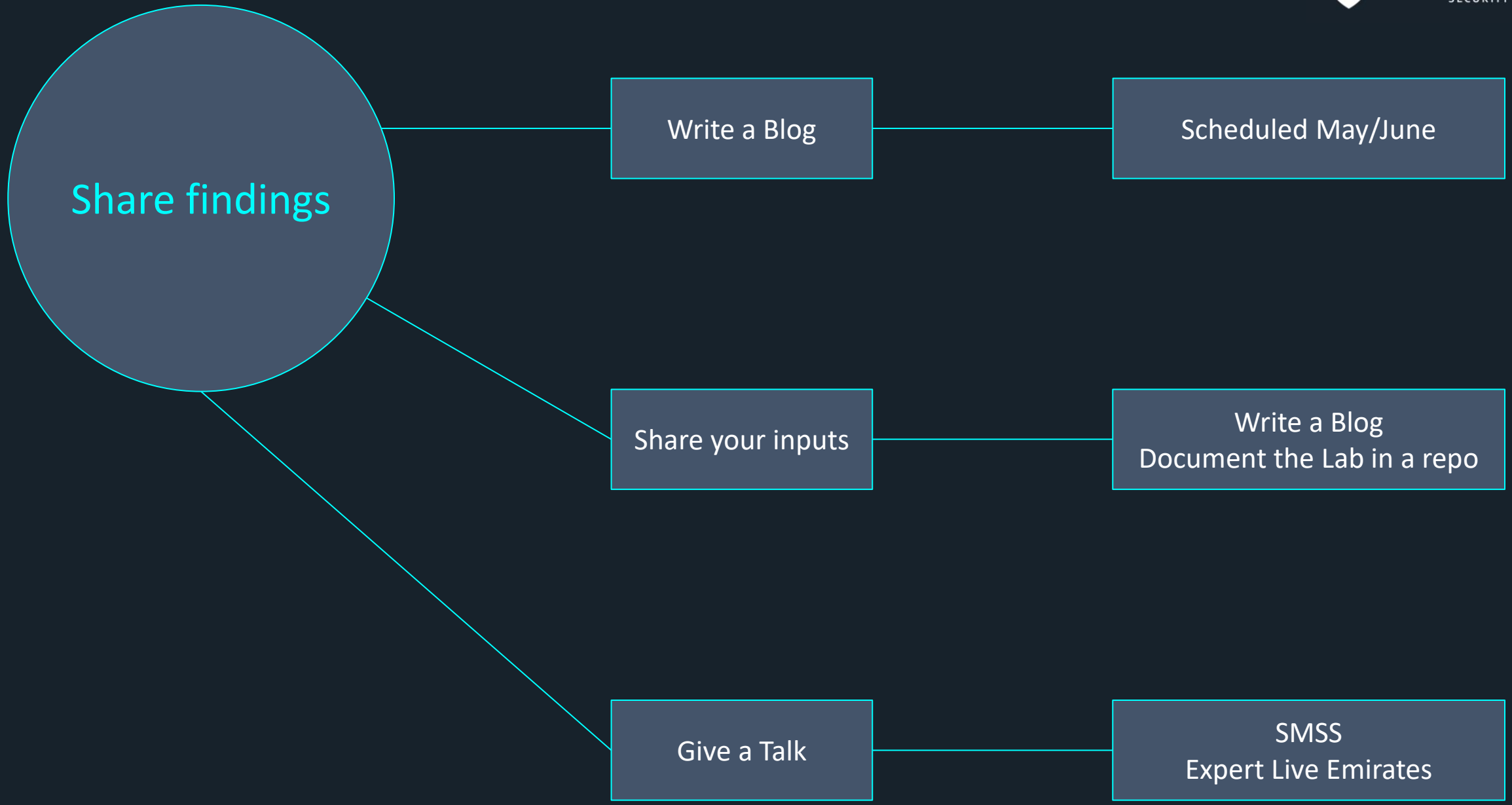
Detection Approach weapons available

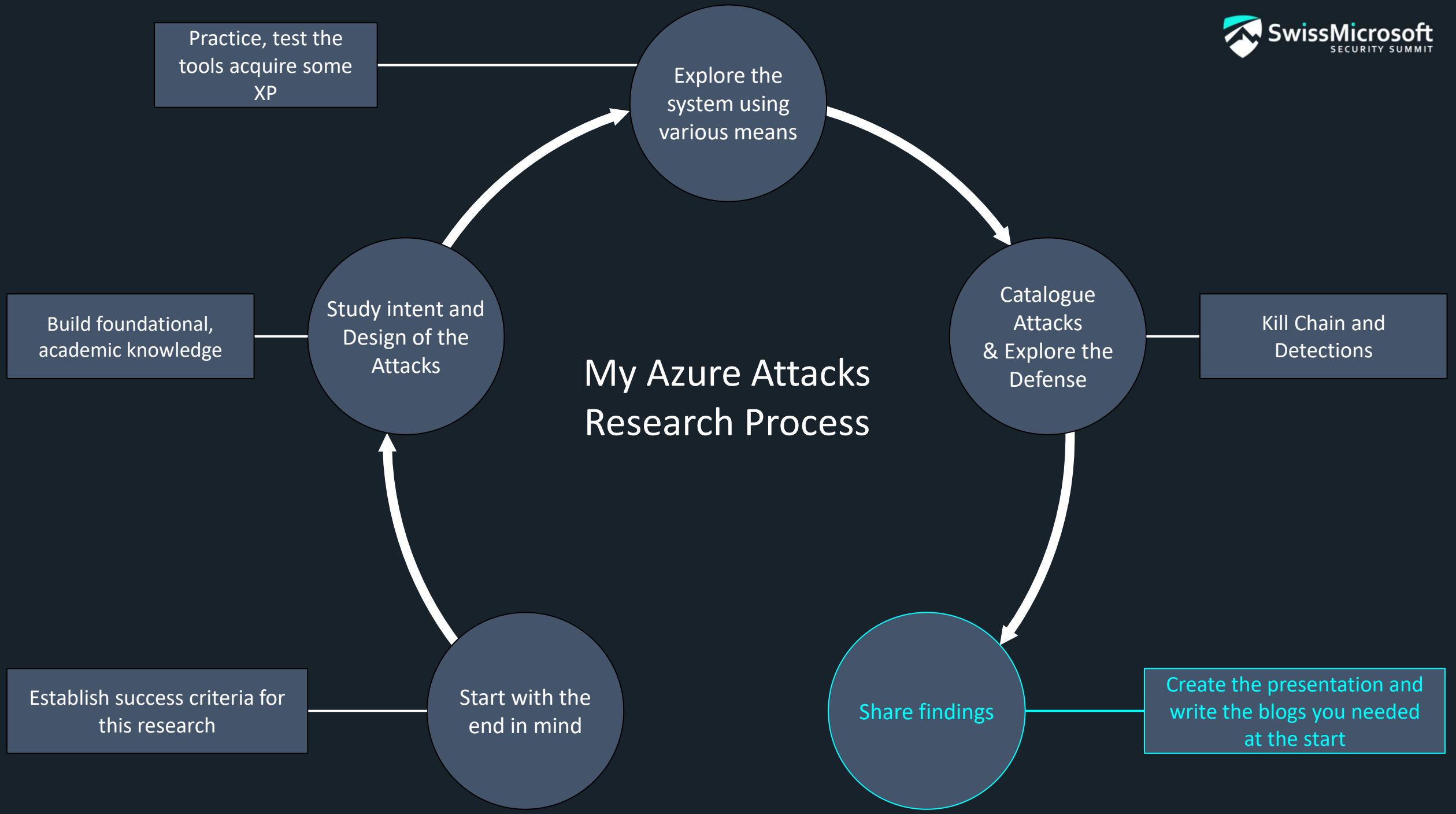
- From Hunting the tools to detection (Analytics rule)
- Fusion in XDR (MDC, MDE, etc…) mapping on same identity
- Playbooks (disable a service principal, key vault access etc..)

It’s a long process, rely on existing solutions, share with the community, and automate what you can.


Practice, test the tools acquire some XP
Explore the system using various means
Catalogue Attacks & Explore the Defense
Kill Chain and Detections approach
Share findings
Start with the end in mind
Establish success criteria for this research
Study intent and Design of the Attacks
Build foundational, academic knowledge
My Azure Attacks Research Process


Practice, test the tools acquire some XP
Explore the system using various means
Catalogue Attacks & Explore the Defense
Kill Chain and Detections approach
Share findings
Start with the end in mind
Establish success criteria for this research
Study intent and Design of the Attacks
Build foundational, academic knowledge
My Azure Attacks Research Process


Share findings
Write a Blog
Scheduled May/June
Share your inputs
Write a Blog
Document the Lab in a repo
Give a Talk
SMSS
Expert Live Emirates


SwissMicrosoft
SECURITY SUMMIT
Practice, test the tools acquire some XP
Explore the system using various means
Catalogue Attacks & Explore the Defense
Kill Chain and Detections
Share findings
Create the presentation and write the blogs you needed at the start
Start with the end in mind
Establish success criteria for this research
Study intent and Design of the Attacks
Build foundational, academic knowledge
My Azure Attacks Research Process

Start with the end in mind

I want to understand:

- The fundamental mechanics of the current Azure Attacks
- How the attacks can compromise the tenants
- How Entra ID can be abused
- How to detect this attacks with Sentinel/Defender XDR

I want to produce in 2025:

- 2-3 blog posts / 1 talk for others to understand and build on
- Example of tools usage and how to abuse Azure
- Give some Detection guidance / KQL

If appropriate for SPCS, I want to prepare for:

- The impact on the existing SOC Detection
- How to train our teams to investigate this attacks
- What data to collect and ingest, and how to setup An.rules

Start with the end in mind

Status after 7 months…

I want to understand:

- ☑ The fundamental mechanics of the current Azure Attacks
- ☑ How the attacks can compromise the tenants
- ☑ How Entra ID can be abused
- ☑ How to detect this attacks with Sentinel/Defender XDR

I want to produce in 2025:

- ☑ 2-3 blog posts / 1 talk for others to understand and build on
- ☑ Example of tools usage and how to abuse Azure
- 🚧 Give some Detection guidance / KQL

If appropriate for SPCS, I want to prepare for:

- ☑ The impact on the existing SOC Detection
- 🚧 How to train our teams to investigate this attacks
- 🚧 What data to collect and ingest, and how to setup A.rules

SwissMicrosoft SECURITY SUMMIT

Program of today

- Introduction
- Azure Fundamentals
- Research process
- Azure Kill Chain & tools for attacks
- Best approach for Detection
- Conclusion

Conclusion

- We cannot protect what we can't see or we don’t know!
- There has never been a better time than right now to get involved in Azure attack/Defense research. Think Purple
- You have in these slides enough tools to test during days!

SwissMicrosoft SECURITY SUMMIT

Follow These MVP/People on X

@fabian_bader | Fabian Bader
https://cloudbrothers.info/en/

@BertJanCyber | Bert-Jan
https://kqlquery.com/

@DrAzureAD | Dr. Nestori Syynimaa
AADInternals.com

@castello_johnny | Gianni Castaldi
https://www.kustoking.com/

@Thomas Naunheim | Thomas Naunheim
https://www.cloud-architekt.net/

Some Trainings

Home - CQURE Academy

SEC541: Cloud Security Threat Detection | SANS Institute

PEN-300: Advanced Penetration Testing Certification | OffSec

SwissMicrosoft SECURITY SUMMIT

Bookmark these pages

https://aadinternals.com/

https://goodworkaround.com/

https://www.azadvertizer.net/

https://thomasvanlaere.com/

https://m365maps.com/matrix.htm

https://msportals.io/?search=

https://www.thelazyadministrator.com

SwissMicrosoft SECURITY SUMMIT

Mentions & Sources

- My wife, for her understanding and support, especially during my late-night sessions in front of the computer
- Andy Robbins, co-creator of BloodHound, for inspiring the process
- Nikhil Mittal and the Altered Security Community on Discord for their insights and collaboration
- Al Schneiter & org Team, MVP Security, for the invitation for this event

Thank you & stay safe!

- Github repo for the tools & Demos

GitHub - DenMutlu/AzureATK: Azure Audit Toolkit is a process using Tools, process, docs to audit and review security configuration on Azure Tenant