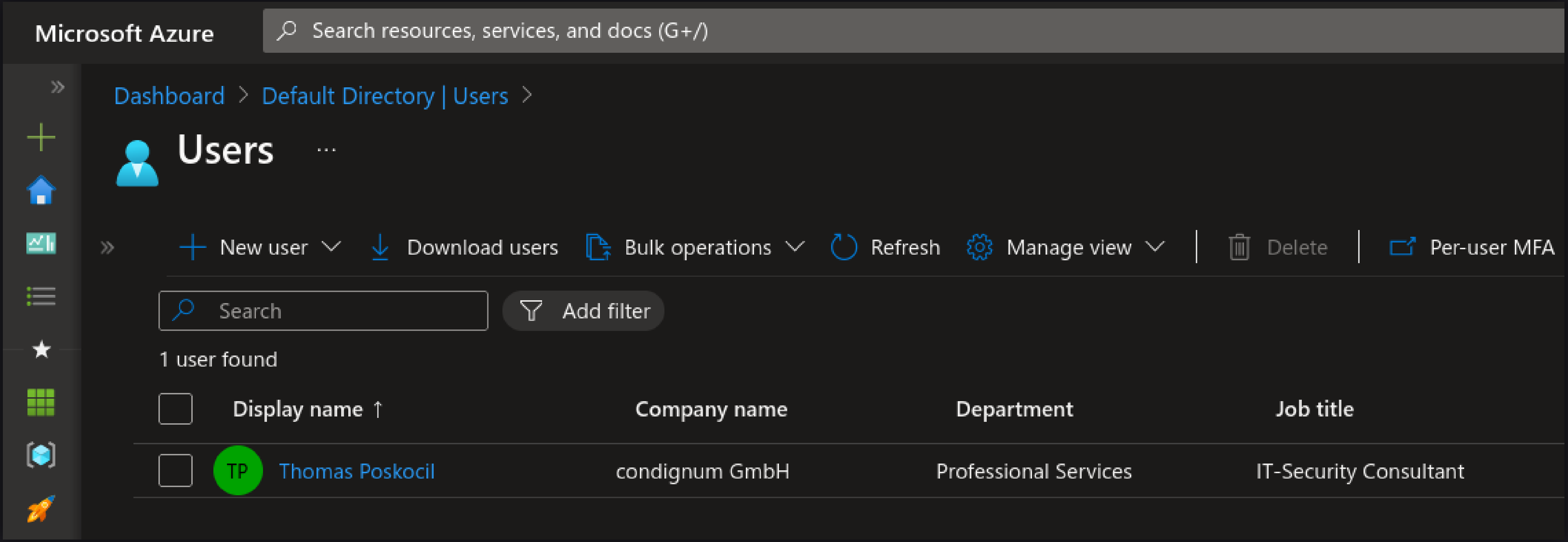
Azure Attack Surfaces

condignum

My User Properties



1 user found

□	Display name ↑	Company name	Department	Job title
□	TP Thomas Poskocil	condignum GmbH	Professional Services	IT-Security Consultant

https://www.condignum.com/

condignum

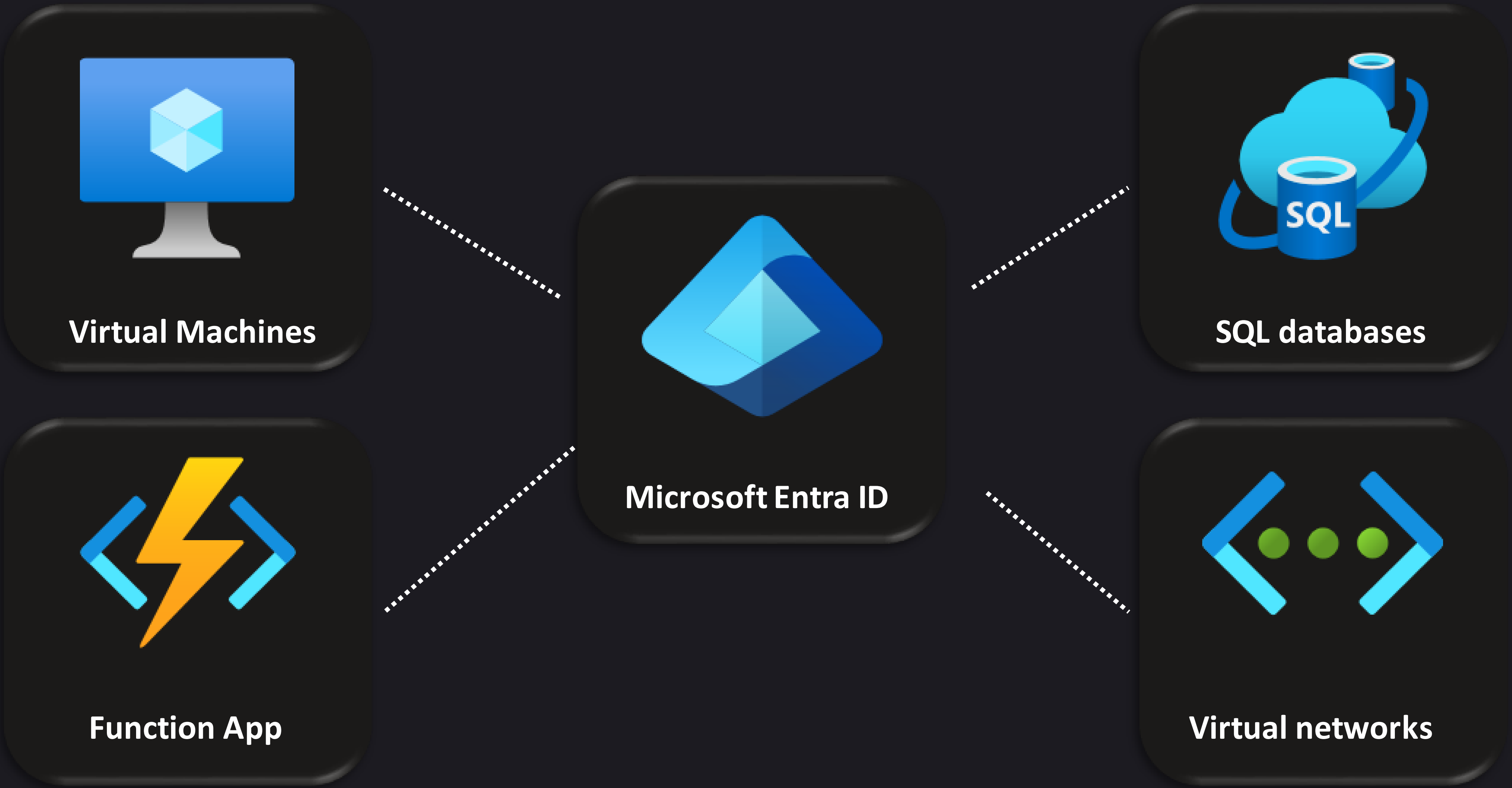
Agenda

- Basics
    - Terminology & Hierarchy
    - Identity & Access Management (Entra ID & RBAC)
- Role-defined Attack Surfaces
    - Common Vectors
    - Attack Surface Reduction
- Takeaways
- Resources & Recommended materials

Terminology & Hierarchy

Azure = Cloud Computing Platform

Azure Services



Virtual Machines

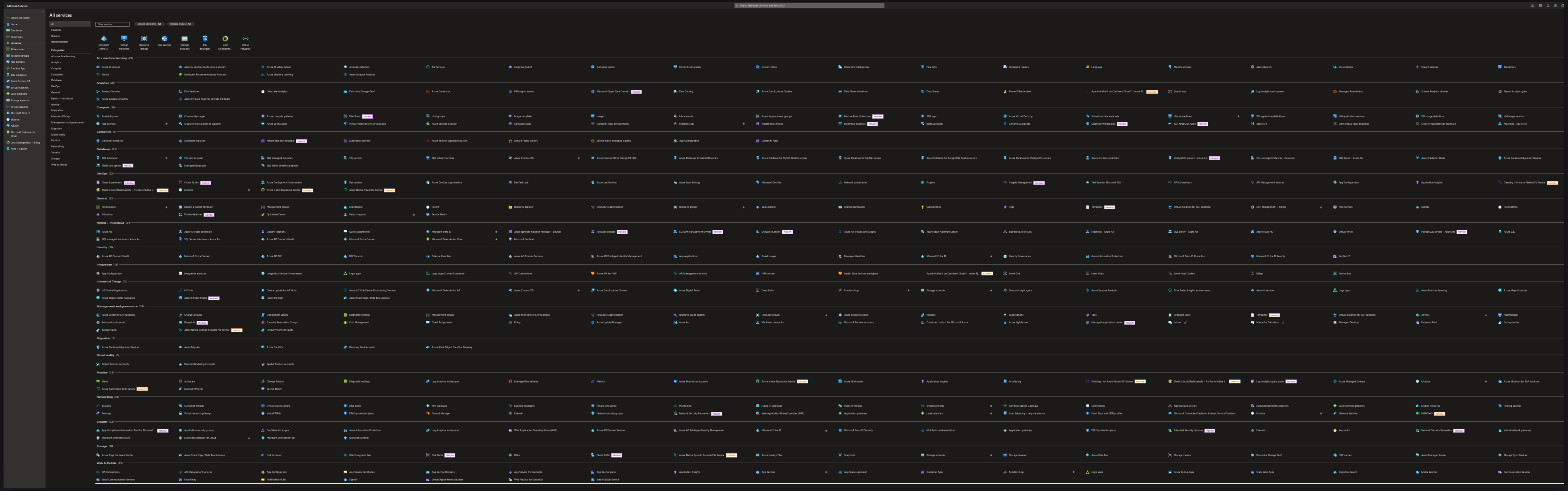
Function App

Microsoft Entra ID

SQL databases

Virtual networks

Azure Services



Microsoft Azure

Search resources, services, and docs (G+/)

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Microsoft Entra ID
- Monitor
- Advisor
- Microsoft Defender for Cloud
- Cost Management + Billing
- Help + support

All services

- All
- Favorites
- Recents
- Recommended

Categories

- AI + machine learning
- Analytics
- Compute
- Containers
- Databases
- DevOps
- General
- Hybrid + multicloud
- Identity
- Integration
- Internet of Things
- Management and governance
- Migration
- Mixed reality
- Monitor
- Networking
- Security
- Storage
- Web & Mobile

Filter services | Service providers : All | Release Status : All

Microsoft Entra ID · Virtual machines · Resource groups · App Services · Storage accounts · SQL databases · Cost Manageme... · Virtual networks

AI + machine learning (22)

Azure AI services · Azure AI services multi-service account · Azure AI Video Indexer · Anomaly detectors · Bot Services · Cognitive Search · Computer vision · Content moderators · Custom vision · Document intelligences · Face APIs · Immersive readers · Language · Metrics advisors · Azure OpenAI · Personalizers · Speech services · Translators
Bonsai · Intelligent Recommendations Accounts · Azure Machine Learning · Azure Synapse Analytics

Analytics (20)

Analysis Services · Data factories · Data Lake Analytics · Data Lake Storage Gen1 · Azure Databricks · HDInsight clusters · Microsoft Graph Data Connect PREVIEW · Data Catalog · Azure Data Explorer Clusters · Data Share Invitations · Data Shares · Power BI Embedded · Apache Kafka® on Confluent Cloud™ - Azure N... PARTNER · Event Hubs · Log Analytics workspaces · Managed Prometheus · Stream Analytics clusters · Stream Analytics jobs
Azure Synapse Analytics · Azure Synapse Analytics (private link hubs)

Compute (36)

Availability sets · Community images · Azure compute galleries · Disk Pools PREVIEW · Host groups · Image templates · Images · Lab accounts · Proximity placement groups · Restore Point Collections PREVIEW · SSH keys · Azure Virtual Desktop · Virtual machine scale sets · Virtual machines ★ · VM application definitions · VM application versions · VM image definitions · VM image versions
App Services ★ · Cloud services (extended support) · Azure Spring Apps · Virtual Instances for SAP solutions · Azure VMware Solution · Container Apps · Container Apps Environments · Function App ★ · Kubernetes services · BareMetal Instances PREVIEW · Batch accounts · Genomics accounts · Quantum Workspaces PREVIEW · SAP HANA on Azure PREVIEW · Azure Arc · Citrix Virtual Apps Essentials · Citrix Virtual Desktops Essentials · Machines - Azure Arc

Containers (9)

Container instances · Container registries · Kubernetes fleet manager PREVIEW · Kubernetes services · Azure Red Hat OpenShift clusters · Service Fabric clusters · Service Fabric managed clusters · App Configuration · Container Apps

Databases (21)

SQL databases ★ · SQL elastic pools · SQL managed instances · SQL servers · SQL virtual machines · Azure Cosmos DB ★ · Azure Cosmos DB for MongoDB (RU) · Azure Database for MariaDB servers · Azure Database for MySQL flexible servers · Azure Database for MySQL servers · Azure Database for PostgreSQL flexible servers · Azure Database for PostgreSQL servers · Azure Arc data controllers · PostgreSQL servers – Azure Arc PREVIEW · SQL managed instances - Azure Arc · SQL Server - Azure Arc · Azure Cache for Redis · Azure Database Migration Services
Elastic Job agents PREVIEW · Managed databases · SQL Server stretch databases

DevOps (22)

Chaos Experiments PREVIEW · Chaos Studio PREVIEW · Azure Deployment Environments · Dev centers · Azure DevOps organizations · DevTest Labs · Azure Lab Services · Azure Load Testing · Microsoft Dev Box · Network connections · Projects · Targets Management PREVIEW · Test Base for Microsoft 365 · API Connections · API Management services · App Configuration · Application Insights · Datadog - An Azure Native ISV Service PARTNER
Elastic Cloud (Elasticsearch) – An Azure Native I... PARTNER · Monitor ★ · Azure Native Dynatrace Service PARTNER · Azure Native New Relic Service PARTNER

General (23)

All resources ★ · Deploy a custom template · Management groups · Marketplace · Recent · Resource Explorer · Resource Graph Explorer · Resource groups ★ · SaaS (classic) · Shared dashboards · Subscriptions · Tags · Templates PREVIEW · Virtual Instances for SAP solutions · Cost Management + Billing ★ · Free services · Quotas · Reservations
Education · Preview features PREVIEW · Quickstart Center · Help + support ★ · Service Health

Hybrid + multicloud (24)

Azure Arc · Azure Arc data controllers · Custom locations · Guest Assignments · Microsoft Entra ID ★ · Azure Network Function Manager – Devices · Resource bridges PREVIEW · SCVMM management servers PREVIEW · VMware vCenters PREVIEW · Azure Arc Private Link Scopes · Azure Edge Hardware Center · ExpressRoute circuits · Machines - Azure Arc · SQL Server - Azure Arc · Azure Stack HCI · Virtual WANs · PostgreSQL servers – Azure Arc PREVIEW · Azure SQL
SQL managed instances - Azure Arc · SQL Server databases - Azure Arc · Azure AD Connect Health · Microsoft Entra Connect · Microsoft Defender for Cloud ★ · Microsoft Sentinel

Identity (16)

Azure AD Connect Health · Microsoft Entra Connect · Azure AD B2C · B2C Tenants · External Identities · Azure AD Domain Services · Azure AD Privileged Identity Management · App registrations · Guest Usages · Managed Identities · Microsoft Entra ID ★ · Identity Governance · Azure Information Protection · Microsoft Entra ID Protection · Microsoft Entra ID Security · Verified ID

Integration (16)

App Configuration · Integration accounts · Integration Service Environments · Logic apps · Logic Apps Custom Connector · API Connections · Azure API for FHIR · API Management services · FHIR service · Health Data Services workspace · Apache Kafka® on Confluent Cloud™ - Azure N... PARTNER · Event Grid · Event Hubs · Event Hubs Clusters · Relays · Service Bus

Internet of Things (22)

IoT Central Applications · IoT Hub · Device Update for IoT Hubs · Azure IoT Hub Device Provisioning Services · Microsoft Defender for IoT · Azure Cosmos DB ★ · Azure Data Explorer Clusters · Azure Digital Twins · Event Hubs · Function App ★ · Storage accounts ★ · Stream Analytics jobs · Azure Synapse Analytics · Time Series Insights environments · Azure AI services · Logic apps · Azure Machine Learning · Azure Maps Accounts
Azure Maps Creator Resources · Azure Percept Studio PREVIEW · Power Platform · Azure Stack Edge / Data Box Gateway

Management and governance (39)

Azure Center for SAP solutions · Change Analysis · Deployment Scripts · Diagnostic settings · Management groups · Azure Monitors for SAP solutions · Resource Graph Explorer · Resource Graph queries · Resource groups ★ · Azure Resource Mover · Rollouts · Subscriptions · Tags · Template specs · Templates PREVIEW · Virtual Instances for SAP solutions · Advisor ★ · Automanage
Automation Accounts · Blueprints PREVIEW · Capacity Reservation Groups · Cost Management · Guest Assignments · Policy · Azure Update Manager · Azure Arc · Machines - Azure Arc · Microsoft Purview accounts · Customer Lockbox for Microsoft Azure · Azure Lighthouse · Managed applications center PREVIEW · Intune ↗ · Intune for Education ↗ · Managed Desktop · Universal Print · Backup center
Backup vaults · Azure Native Qumulo Scalable File Service PARTNER · Recovery Services vaults

Migration (5)

Azure Database Migration Services · Azure Migrate · Azure Data Box · Recovery Services vaults · Azure Stack Edge / Data Box Gateway

Mixed reality (3)

Object Anchors Accounts · Remote Rendering Accounts · Spatial Anchors Accounts

Monitor (21)

Alerts · Autoscale · Change Analysis · Diagnostic settings · Log Analytics workspaces · Managed Prometheus · Metrics · Azure Monitor workspaces · Azure Native Dynatrace Service PARTNER · Azure Workbooks · Application Insights · Activity log · Datadog - An Azure Native ISV Service PARTNER · Elastic Cloud (Elasticsearch) – An Azure Native I... PARTNER · Log Analytics query packs PREVIEW · Azure Managed Grafana · Monitor ★ · Azure Monitors for SAP solutions
Azure Native New Relic Service PARTNER · Network Watcher · Service Health

Networking (35)

Bastions · Custom IP Prefixes · DNS private resolvers · DNS zones · NAT gateways · Network managers · Private DNS zones · Private Link · Public IP addresses · Public IP Prefixes · Virtual networks ★ · Communications Gateways · Connections · ExpressRoute circuits · ExpressRoute traffic collectors · Local network gateways · Mobile Networks · Peering Services
Peerings · Virtual network gateways · Virtual WANs · DDoS protection plans · Firewall Manager · Firewalls · Network security groups · Network Security Perimeters PREVIEW · Web Application Firewall policies (WAF) · Application gateways · Load balancers ★ · Load balancing - help me choose · Front Door and CDN profiles · Microsoft Connected Cache for Internet Service Providers · Monitor ★ · Network Watcher · NGINXaaS PARTNER

Security (22)

App Compliance Automation Tool for Microsoft ... PREVIEW · Application security groups · Confidential Ledgers · Azure Information Protection · Log Analytics workspaces · Web Application Firewall policies (WAF) · Azure AD Domain Services · Azure AD Privileged Identity Management · Microsoft Entra ID ★ · Microsoft Entra ID Security · Multifactor authentication · Application gateways · DDoS protection plans · Extended Security Updates PREVIEW · Firewalls · Key vaults · Network Security Perimeters PREVIEW · Virtual network gateways
Microsoft Defender EASM · Microsoft Defender for Cloud ★ · Microsoft Defender for IoT · Microsoft Sentinel

Storage (18)

Azure Edge Hardware Center · Azure Stack Edge / Data Box Gateway · Disk Accesses · Disk Encryption Sets · Disk Pools PREVIEW · Disks · Elastic SANs PREVIEW · Azure Native Qumulo Scalable File Service PARTNER · Azure NetApp Files · Snapshots · Storage accounts ★ · Storage browser · Azure Data Box · Storage movers · Data Lake Storage Gen1 · HPC caches · Azure Managed Lustre · Storage Sync Services

Web & Mobile (25)

API Connections · API Management services · App Configuration · App Service Certificates · App Service Domains · App Service Environments · App Service plans · Application Insights · App Services ★ · App Spaces (preview) · Container Apps · Function App ★ · Logic apps · Azure Spring Apps · Static Web Apps · Cognitive Search · Media Services · Communication Services
Email Communication Services · Fluid Relay · Notification Hubs · SignalR · Virtual Appointments Builder · Web PubSub for Socket.IO · Web PubSub Service

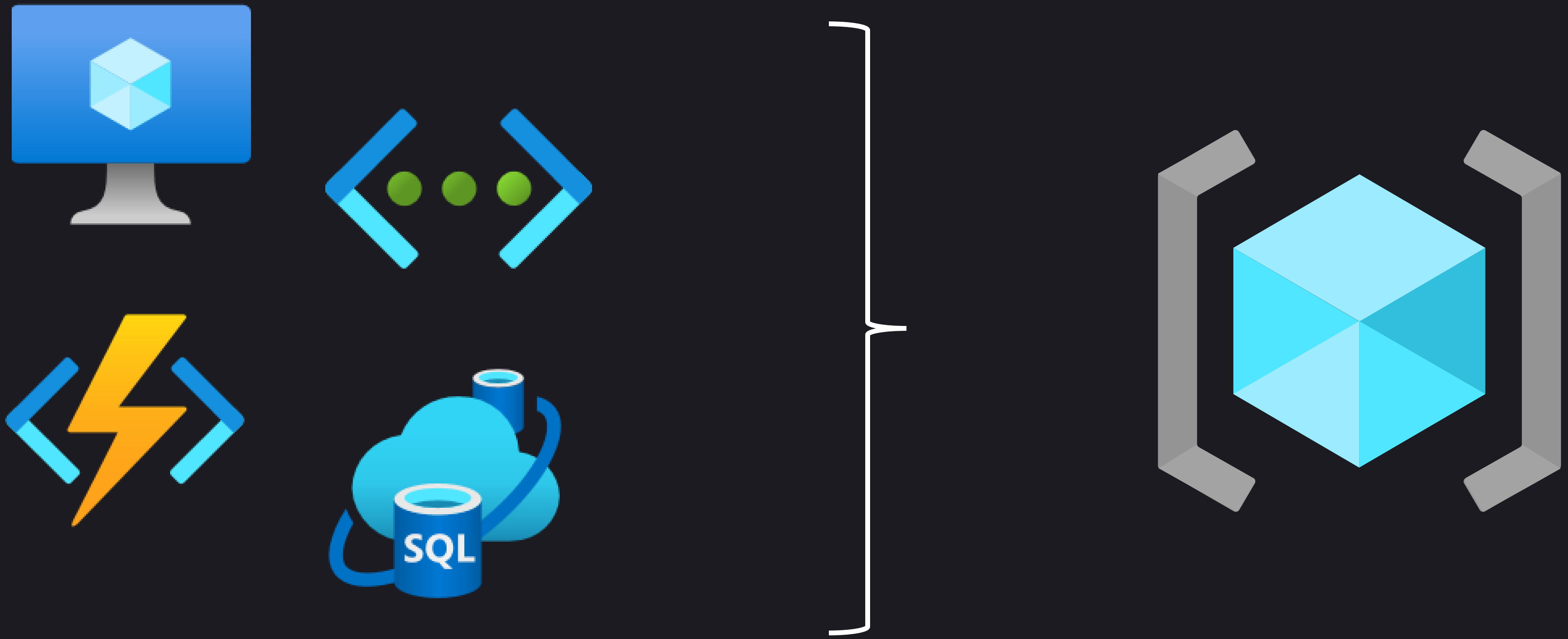
https://portal.azure.com/#allservices/category/All

condignum

Resources & Grouping

Resource
(actual instance of a service)

Resource Group
(logical grouping of resources)

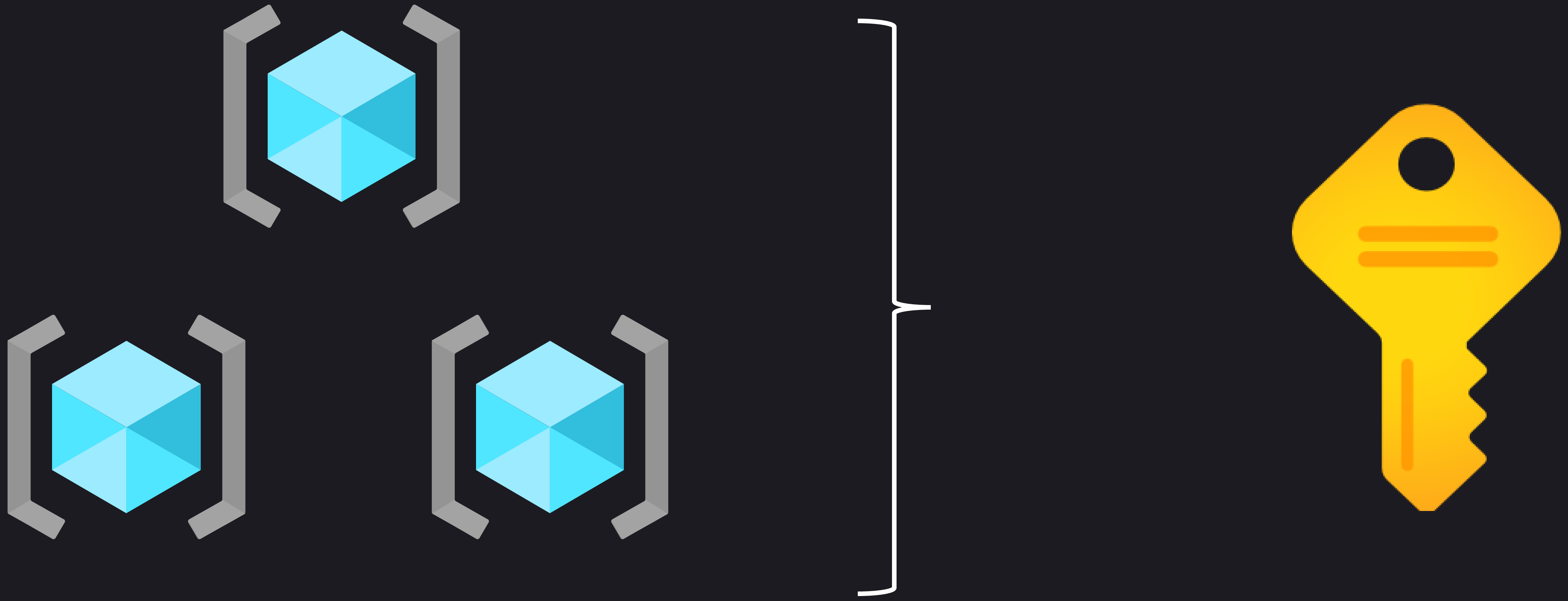


$ubscriptions

Resource Groups

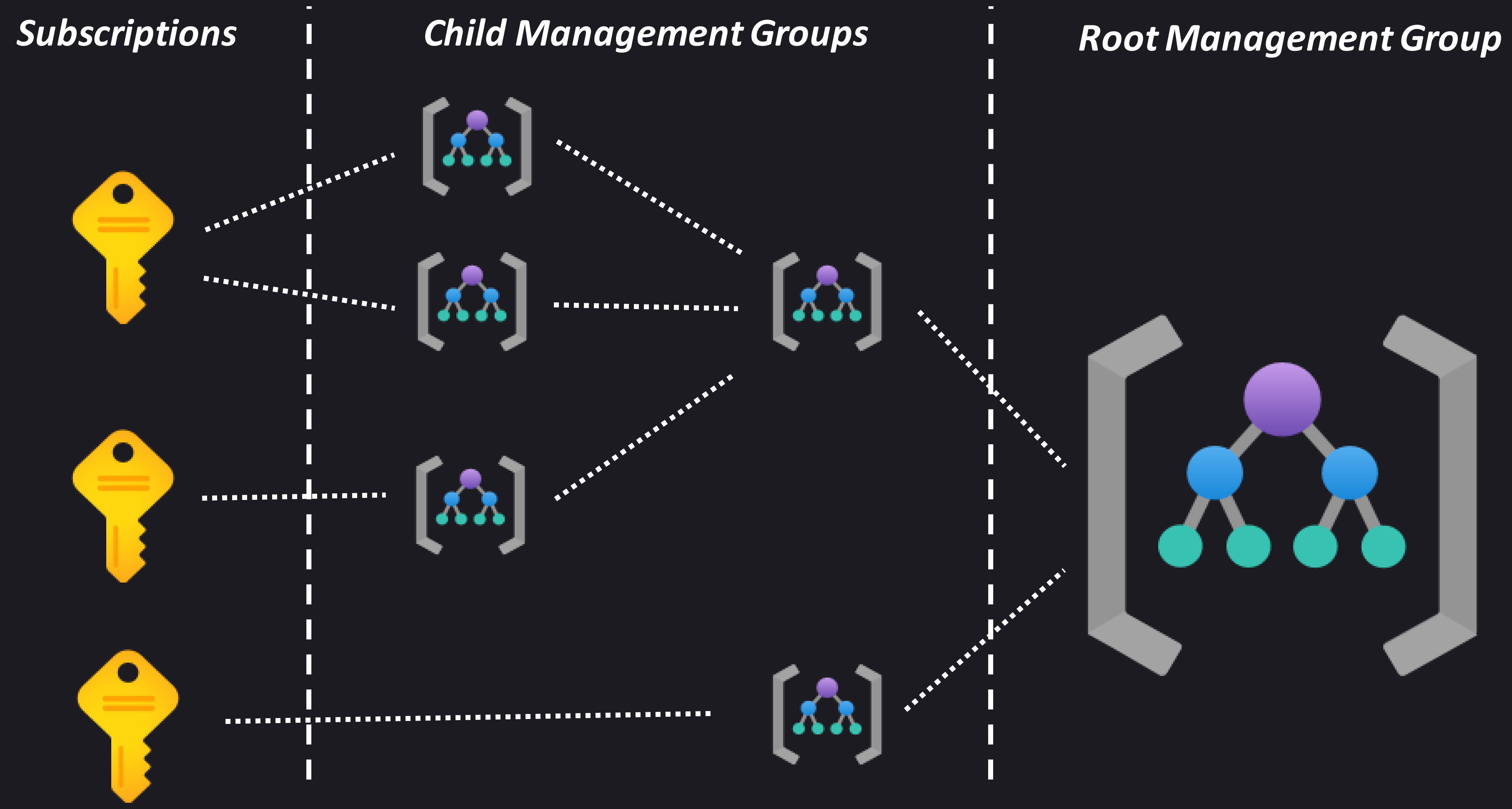
Subscription

(logical payment container)



Management Groups

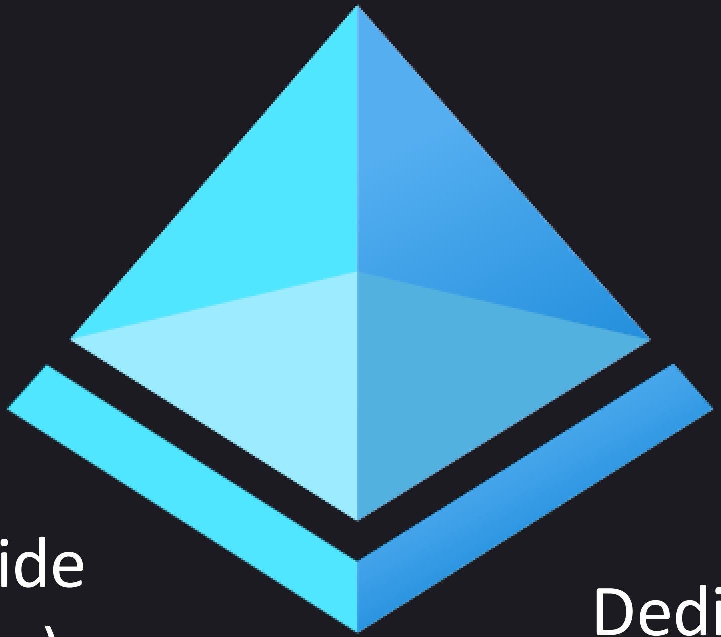
Containers for subscriptions
(not enabled by default)



condignum

Entra Tenant

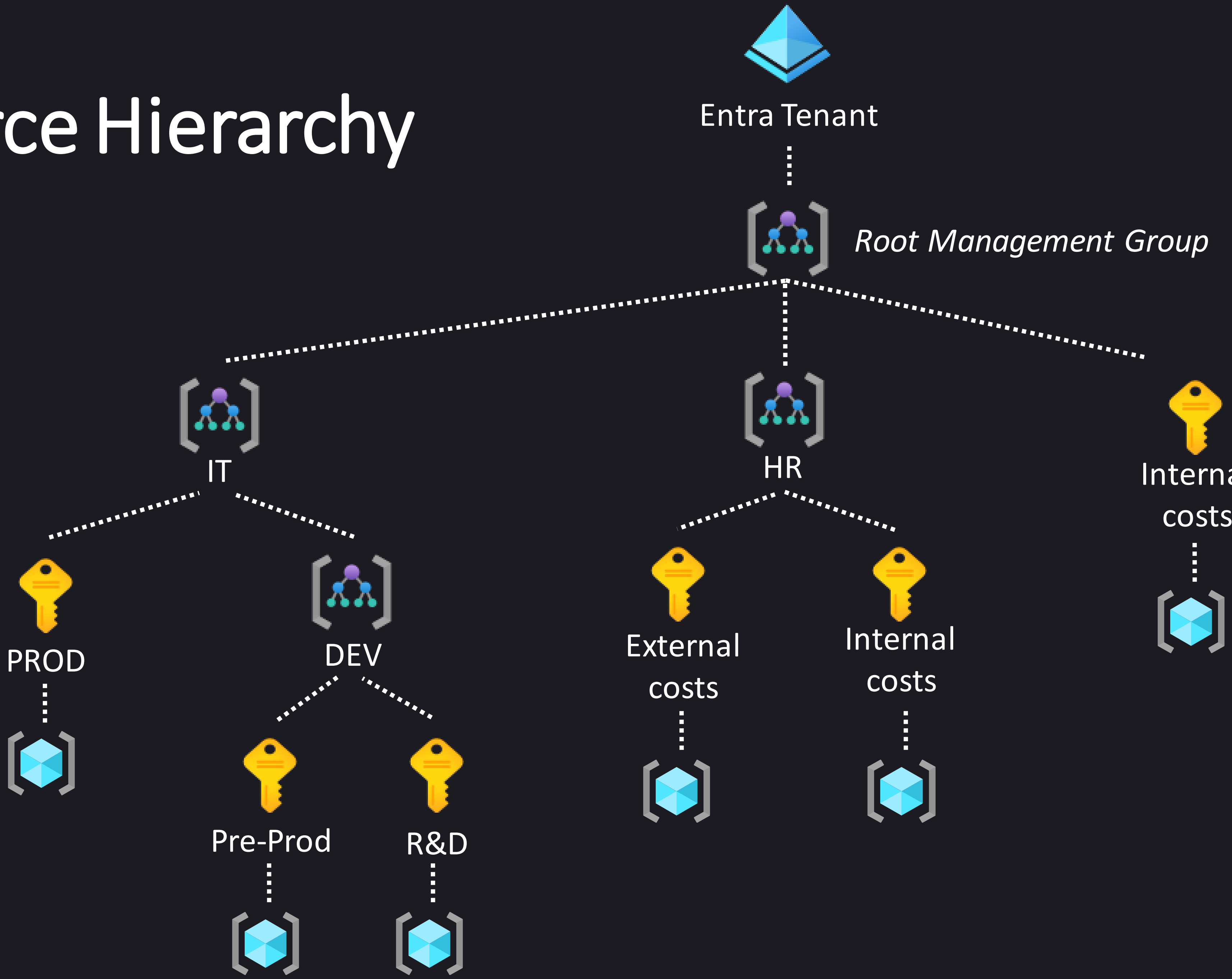
Represents an organization



Maintains all assets inside (users, subscriptions, ...)

Dedicated Entra ID instance

Resource Hierarchy



condignum

Identity & Access Management

Entra ID & RBAC

condignum

Entra ID (~~Azure AD~~)

Identity & **Access** Management Service
(handles authentication)

Unique instance
per tenant

Used by multiple
Microsoft cloud platforms

There is no directory

Security Principals

Identity objects in **Entra ID** requesting access to Azure services

- **User**
- **Group**
- **Service Principal**
- **Managed Identity**

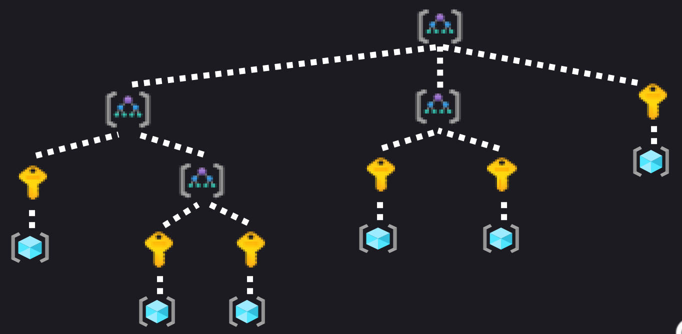
Roles

Entra Roles

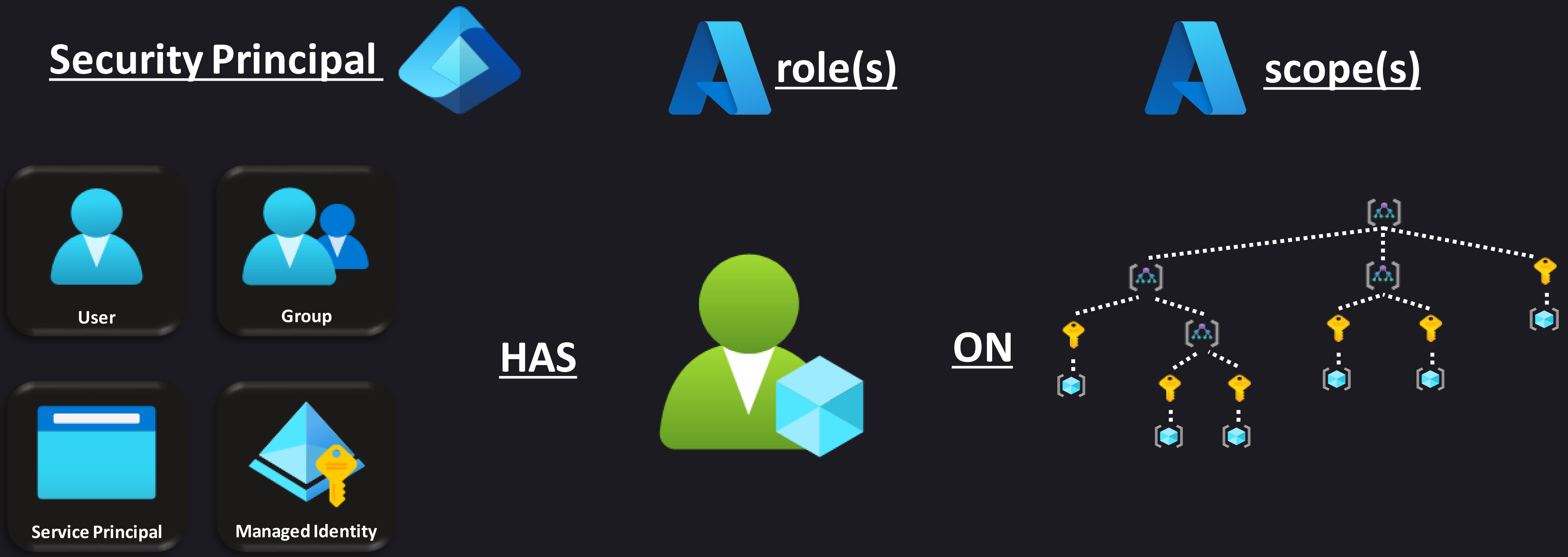
Manages access to Entra resources (Adding / Editing Users)

Azure Roles

Manages access to Azure resources



Role-Based Access Control (RBAC)



Security Principal

User

Group

Service Principal

Managed Identity

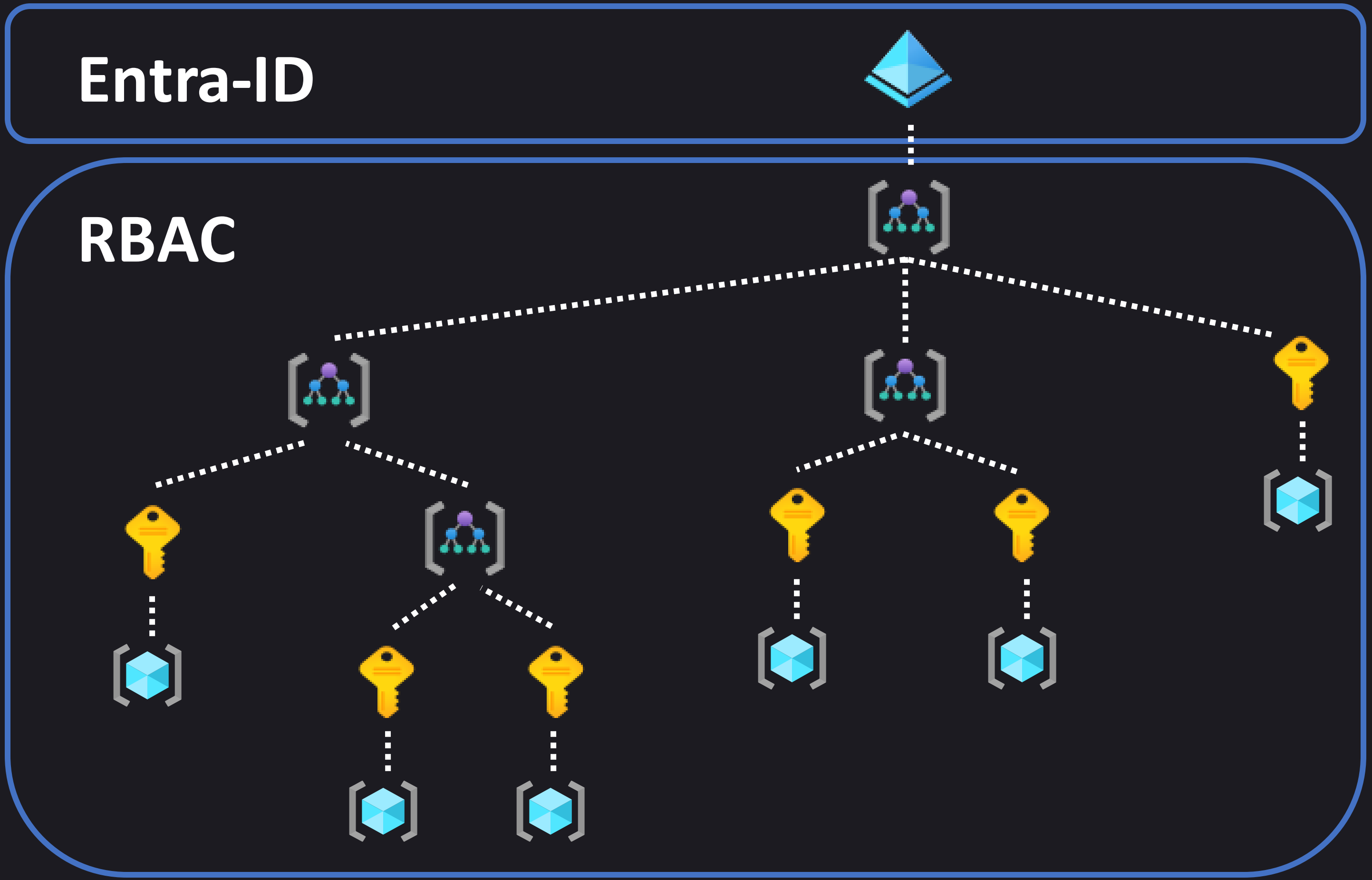
HAS

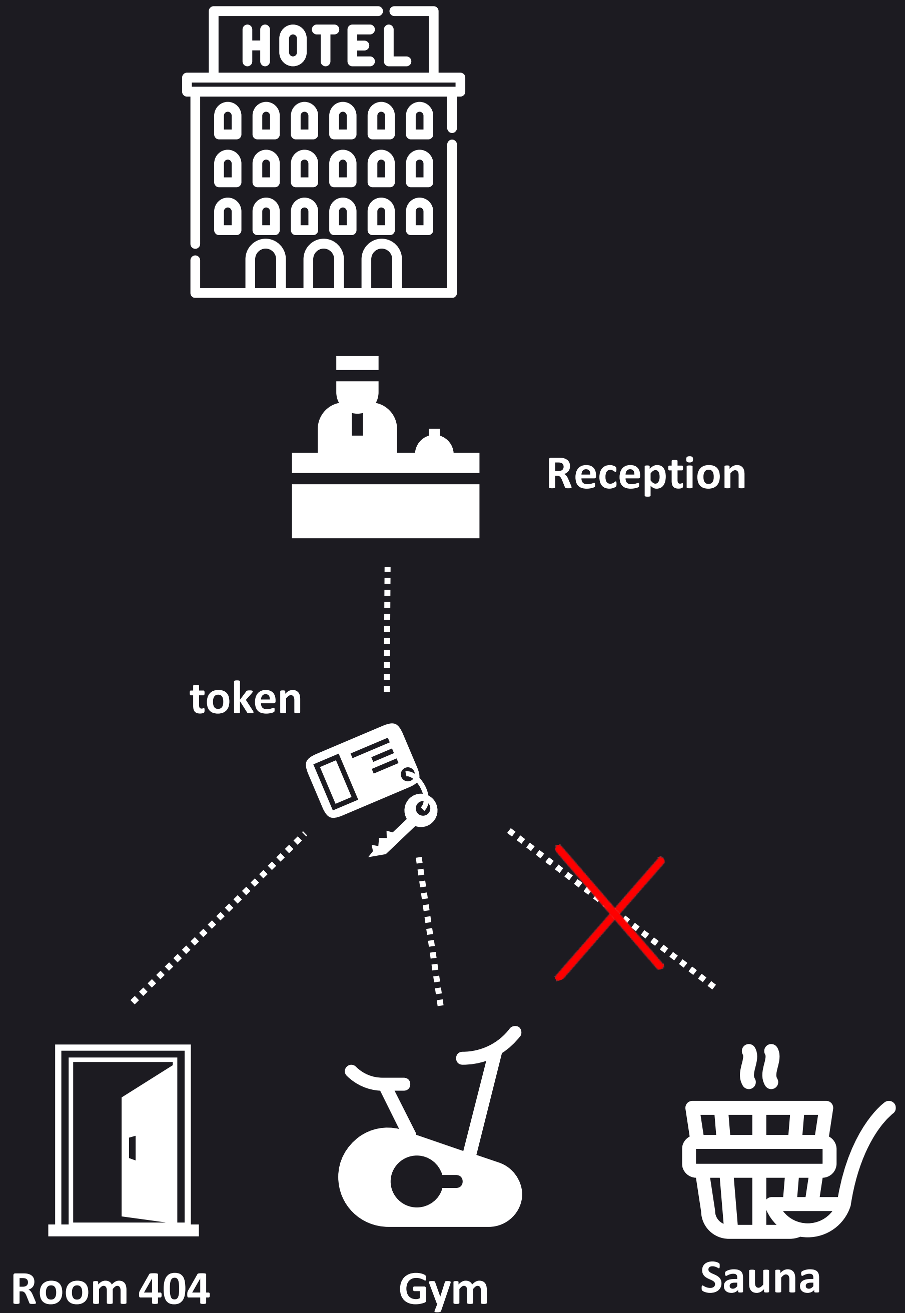
role(s)

ON

scope(s)

Hotel



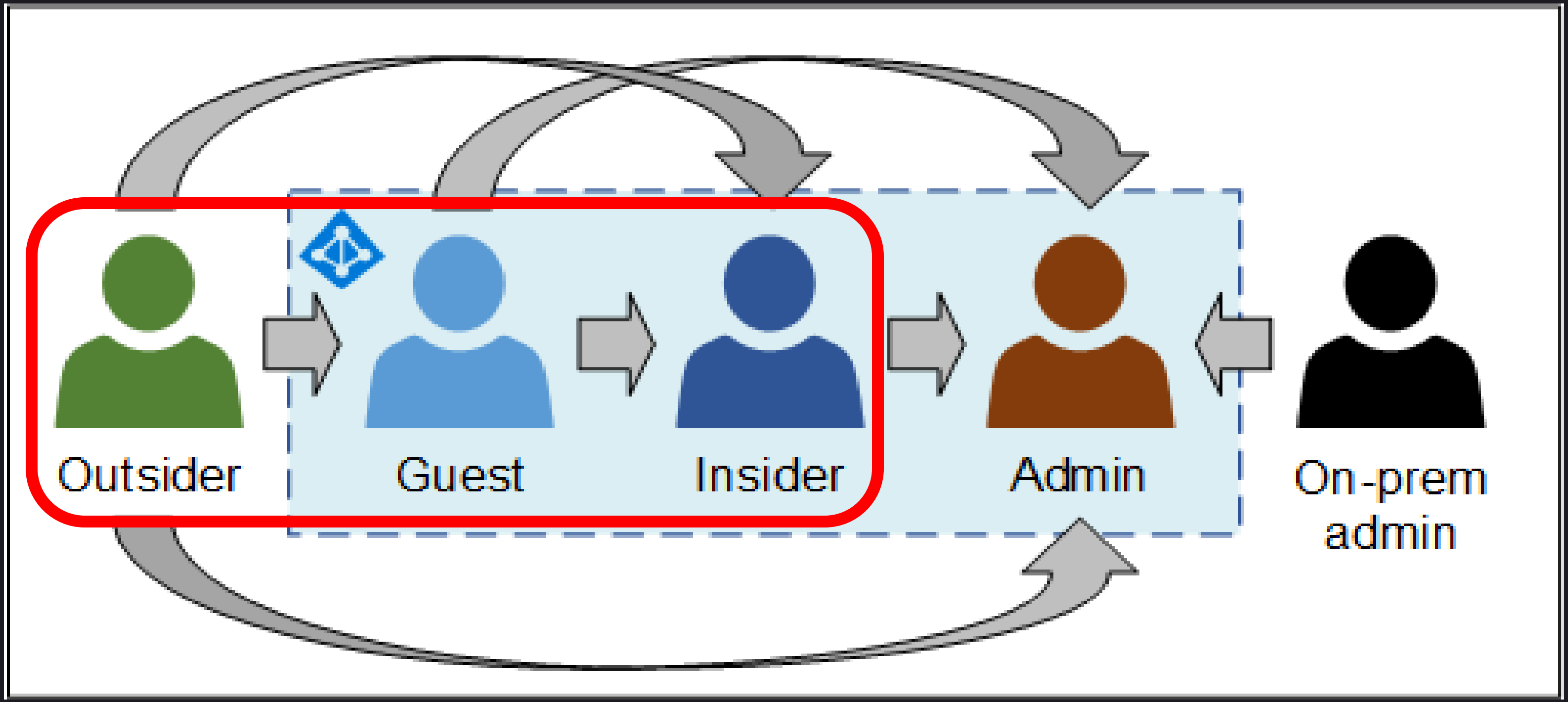


condignum

Role-defined Attack Surfaces

condignum

Kill Chain Roles



© Dr Nestori Syynimaa

https://aadinternals.com/

OUTSIDER – Generic Attack Surfaces

Overly exposed resources

Vulnerable resources
(App Service or Function App Abuse)

Insecure data storage

Malware/Credential
Phishing

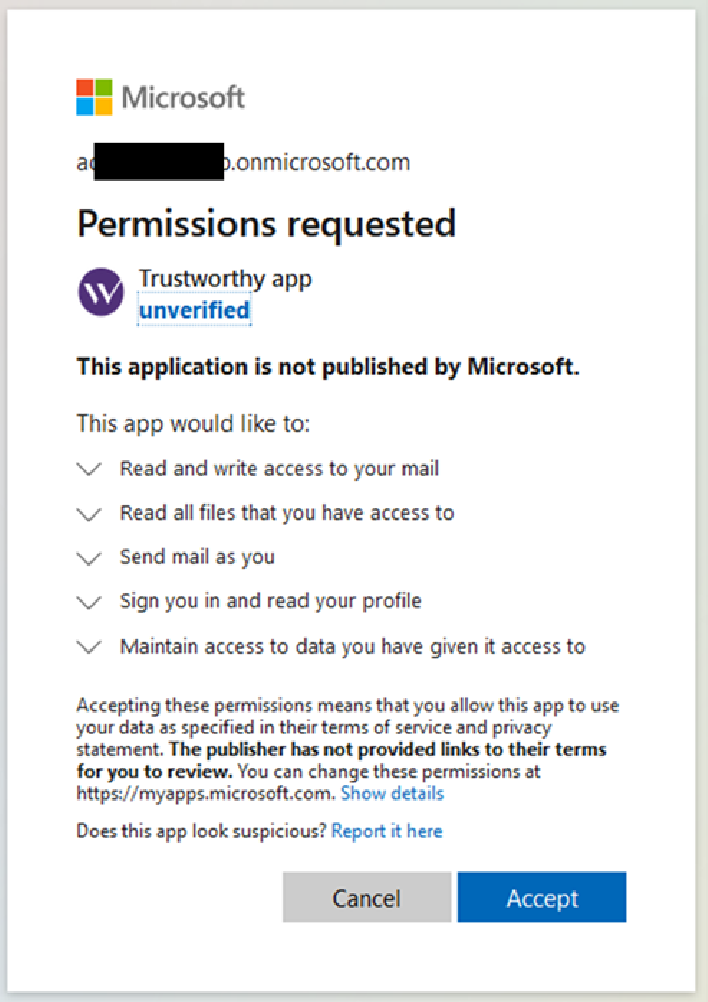
Weak credentials

OUTSIDER – Illicit Consent Grant

ATTACKER

Registered app with a set of non-admin permissions

Application's Service Principal is able to act on victim's behalf & query the APIs



Microsoft

a[redacted].onmicrosoft.com

Permissions requested

Trustworthy app
unverified

This application is not published by Microsoft.

This app would like to:

- Read and write access to your mail
- Read all files that you have access to
- Send mail as you
- Sign you in and read your profile
- Maintain access to data you have given it access to

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

VICTIM

User receives a phishing mail with a link & accepts

Users are allowed by default to consent

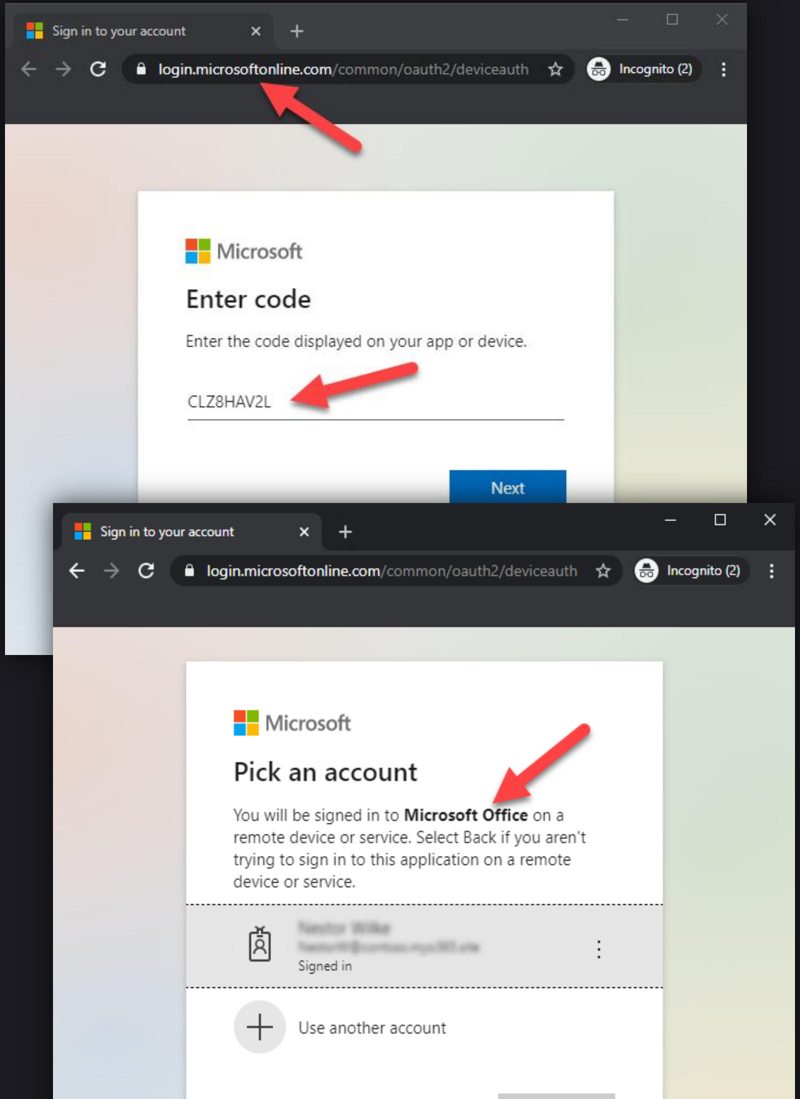
OUTSIDER – Device Code Authentication

Used for logging in to devices with limited controls (Xbox, Kiosk terminals)

ATTACKER

Requests the code

Sends verification link & code



Sign in to your account

login.microsoftonline.com/common/oauth2/deviceauth

Incognito (2)

Microsoft

Enter code

Enter the code displayed on your app or device.

CLZ8HAV2L

Next

Sign in to your account

login.microsoftonline.com/common/oauth2/deviceauth

Incognito (2)

Microsoft

Pick an account

You will be signed in to **Microsoft Office** on a remote device or service. Select Back if you aren't trying to sign in to this application on a remote device or service.

[redacted]

Signed in

Use another account

VICTIM

Opens the link & enters the code - that's it

<u>Legitimate Microsoft Domain</u>

<u>No consent is requested</u>

<u>Device code expires after 15 minutes</u>

condignum

OUTSIDER – Blob Storage Hunting

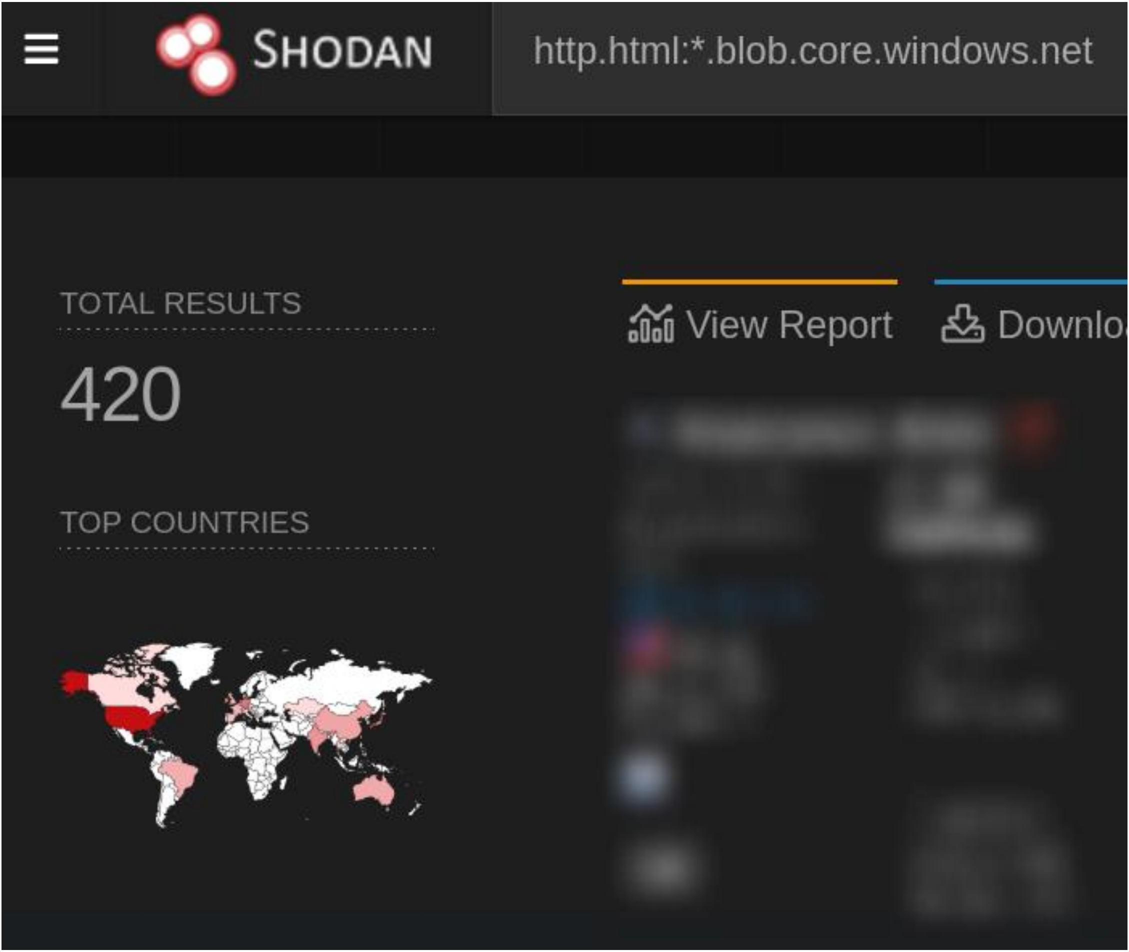
Equivalent of a S3 bucket in AWS

Stores unstructured data (files, videos, ...)

Per default not publicly accessible

Might expose unwanted data (Credentials, DBs, Backups, ...)

Can be found in website sources, with google dorks or listen on shodan



condignum

OUTSIDER – Attack Surface Reduction

Strong password policy & enable MFA for all users

Awareness

Minimal infrastructure exposure

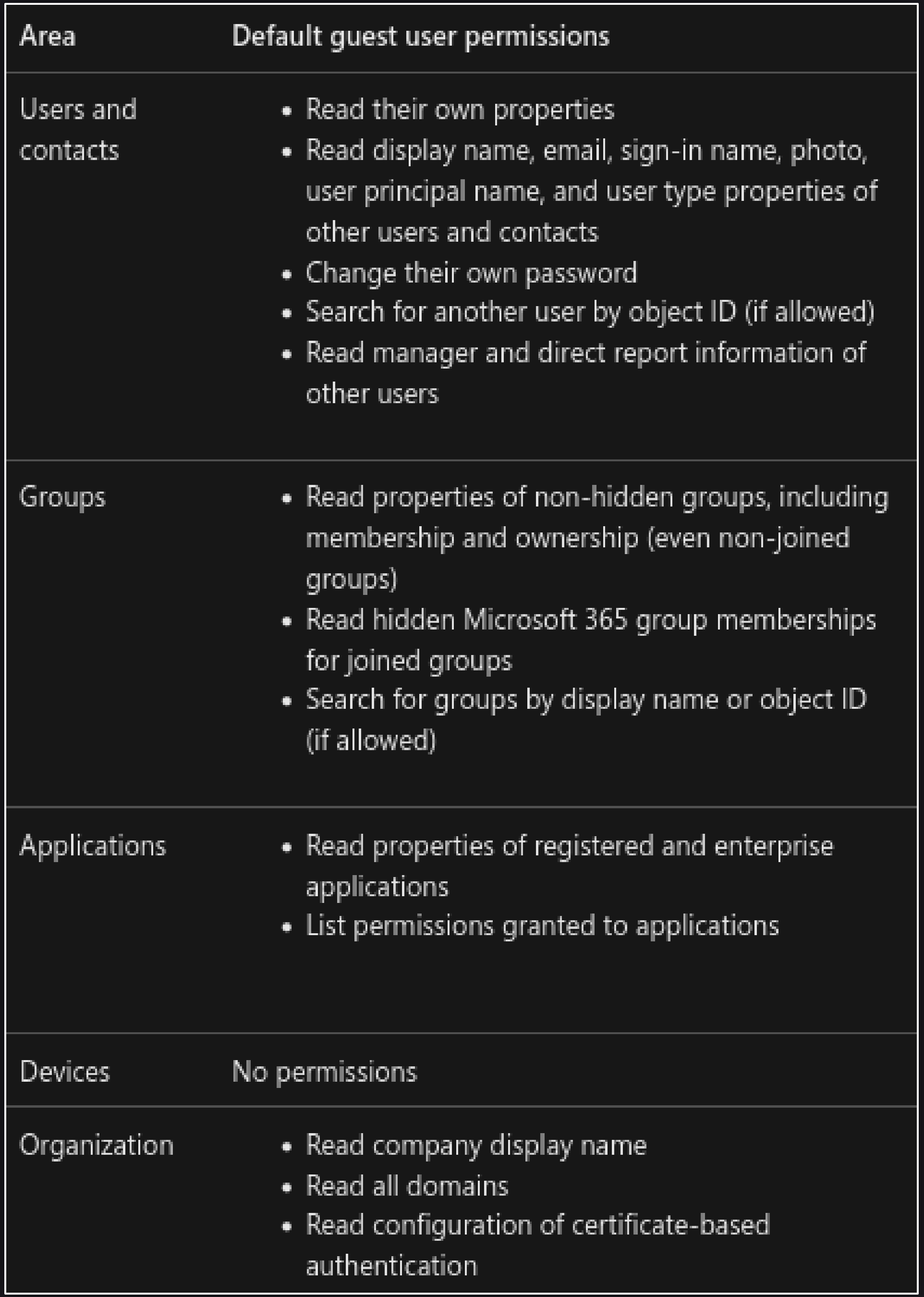
Do not allow user consent

(limited) Logging & Alert Rules

Proper Patch-Management

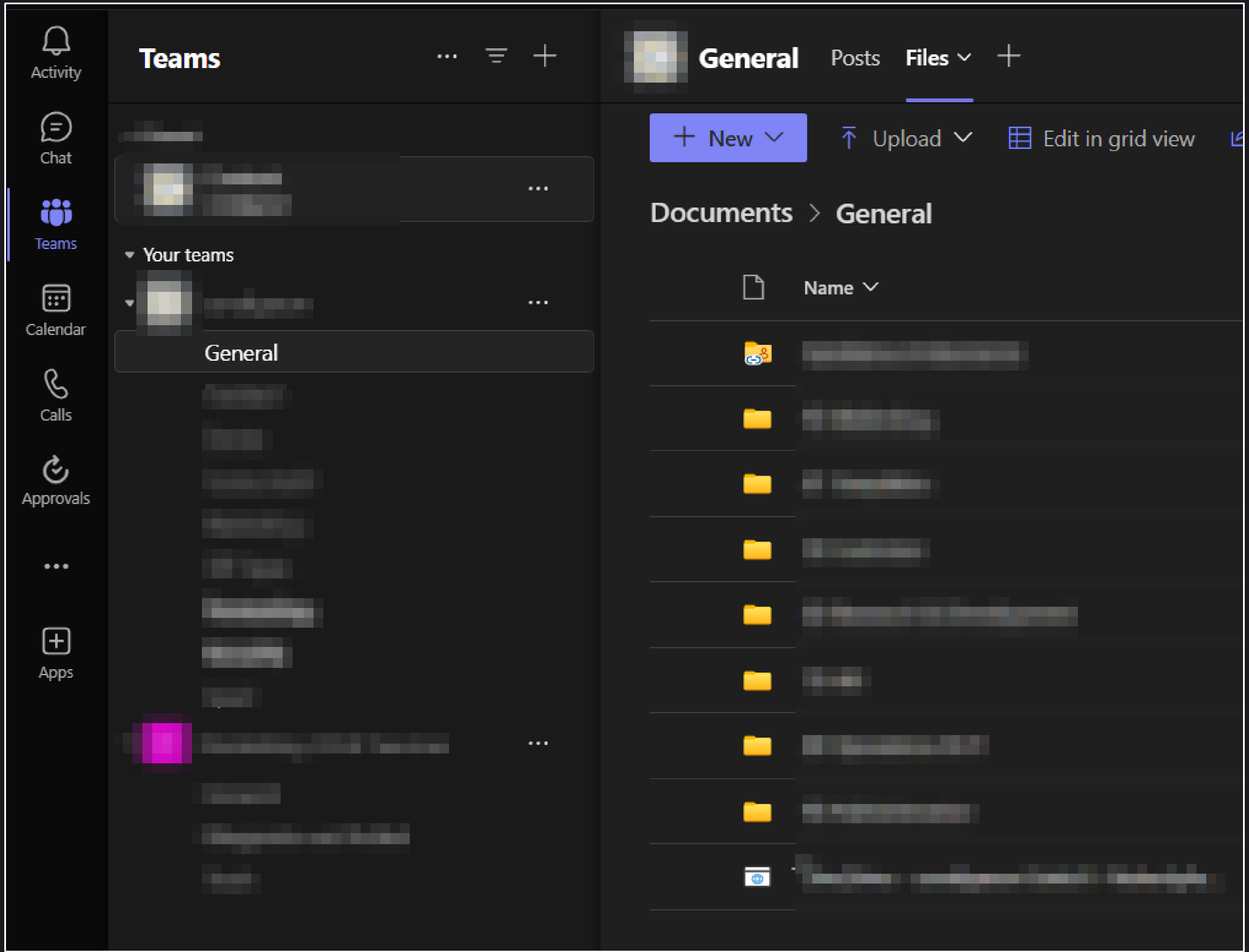
GUEST – Permissions

READ-ONLY
access by default



Area	Default guest user permissions
Users and contacts	• Read their own properties • Read display name, email, sign-in name, photo, user principal name, and user type properties of other users and contacts • Change their own password • Search for another user by object ID (if allowed) • Read manager and direct report information of other users
Groups	• Read properties of non-hidden groups, including membership and ownership (even non-joined groups) • Read hidden Microsoft 365 group memberships for joined groups • Search for groups by display name or object ID (if allowed)
Applications	• Read properties of registered and enterprise applications • List permissions granted to applications
Devices	No permissions
Organization	• Read company display name • Read all domains • Read configuration of certificate-based authentication

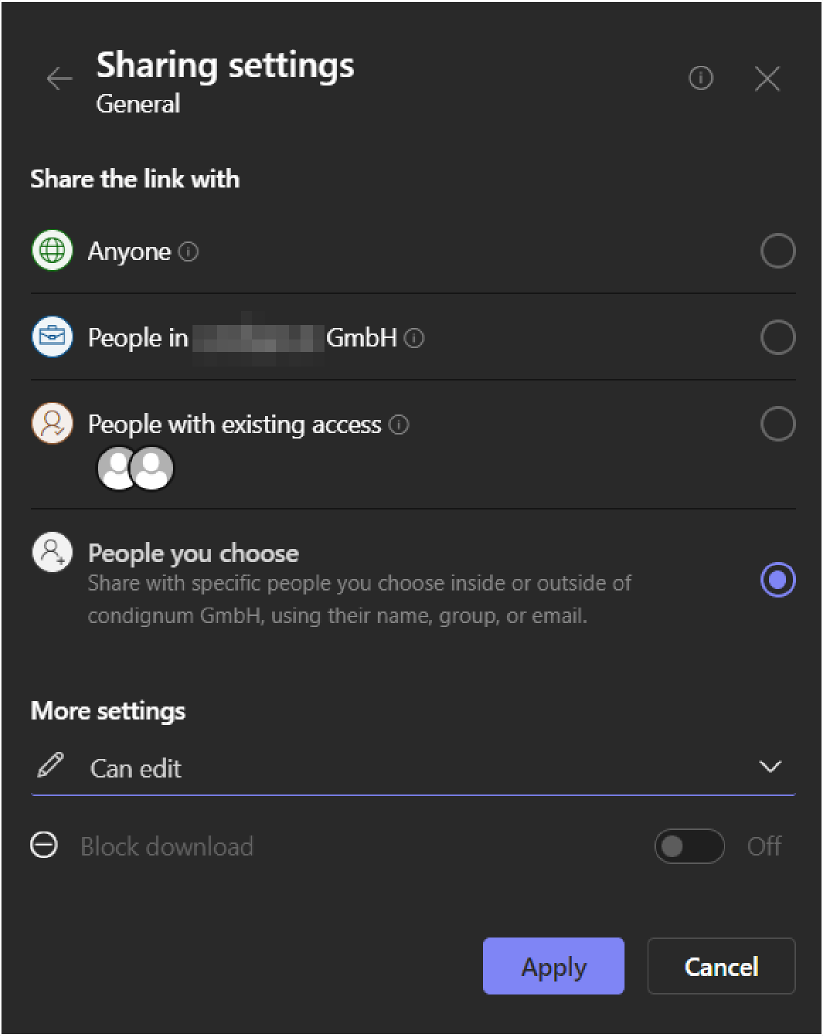
GUEST – Public Teams



Self-join

View & share data

GUEST – Unrestricted File Share



Sharing settings

General

Share the link with

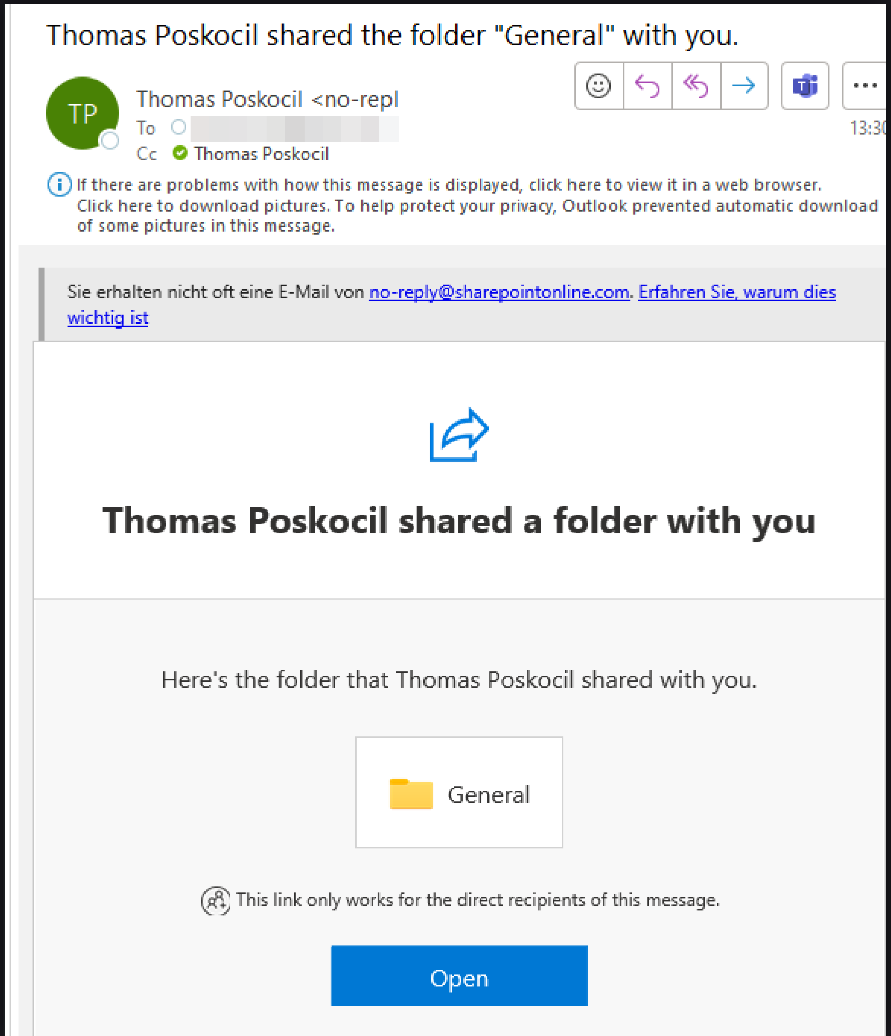
- Anyone ⓘ ○
- People in [redacted] GmbH ⓘ ○
- People with existing access ⓘ ○
- People you choose ●
  Share with specific people you choose inside or outside of condignum GmbH, using their name, group, or email.

More settings

Can edit

Block download Off

Apply | Cancel



Thomas Poskocil shared the folder "General" with you.

Thomas Poskocil <no-repl

To [redacted]

Cc Thomas Poskocil

13:3

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Sie erhalten nicht oft eine E-Mail von no-reply@sharepointonline.com. Erfahren Sie, warum dies wichtig ist

Thomas Poskocil shared a folder with you

Here's the folder that Thomas Poskocil shared with you.

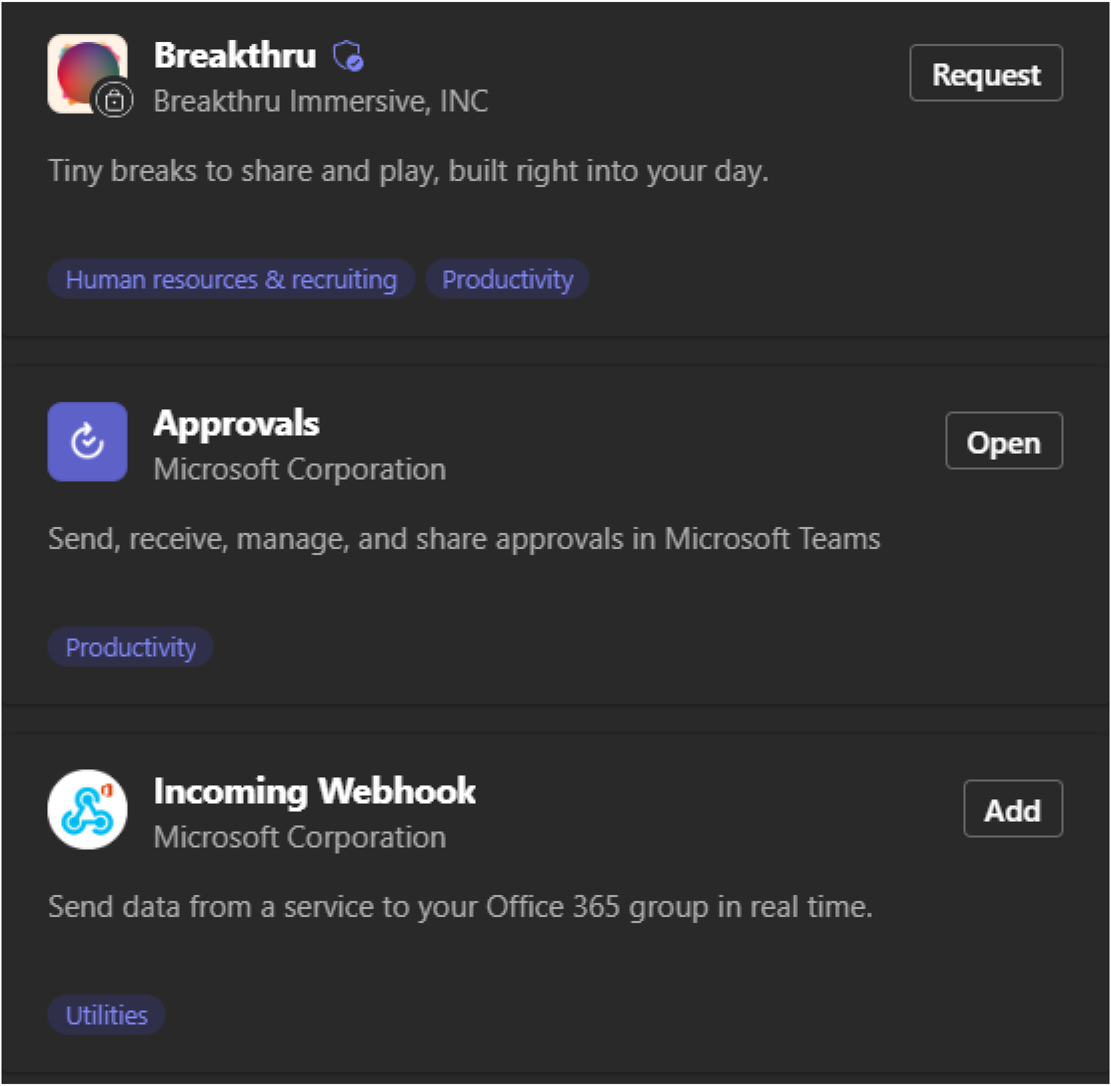
General

This link only works for the direct recipients of this message.

Open

condignum

GUEST – Untrusted Apps



Tiny breaks to share and play, built right into your day.

Send, receive, manage, and share approvals in Microsoft Teams

Send data from a service to your Office 365 group in real time.

GUEST – Attack Surface Reduction

Create app permission policies for Teams

Users should only create private teams

Restrict File-Sharing to **Users** with existing access only

Very restrictive Guest roles (need-to-know)

Establish conditional access policies

INSIDER – Default Permissions

Invite Guests

Create new applications

Add up to 50 devices to Azure

Create Security Groups

INSIDER – Dynamic Group Memberships

Rules to automatically join groups

Can be an efficient access control

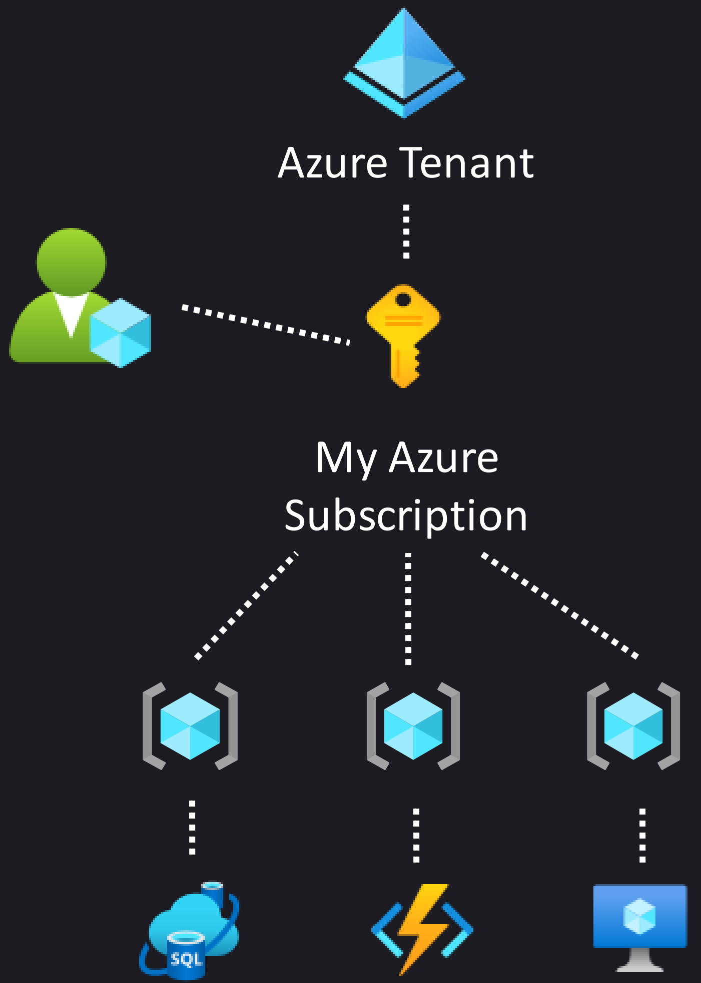
Memberships are updated in "real-time"

Designed to reduce Group management efforts

INSIDER – Insecure Azure Role Configuration

Overly permissive roles

Lack of Segmentation



condignum

INSIDER – Attack Surface Reduction

Properly segment your resources

Follow a multi-tenant approach

Users should only create private teams

Fine tune your dynamic group membership rules

Follow the **least-privilege** & **kneed-to-know** principles, when **defining & assigning** roles

Takeaways

Focus on permissions & access controls (role definition & assignment)

Don't trust default settings

Azure will not protect you from service vulnerabilities

Everything compromised might have an identity

condignum

Resources

Images & Icons:

- https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/geographies-hero?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=2880&qlt=100&fit=constrain
- https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/products-hero?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=2880&qlt=100&fit=constrain
- https://learn.microsoft.com/en-us/azure/architecture/icons/
- https://www.svgrepo.com/
- https://www.riskinsight-wavestone.com/wp-content/uploads/2023/03/Imagebis.png
- https://aadinternals.com/images/posts/killchain.png
- https://aadinternals.com/post/phishing/

Recommended material

Free hosted hands-on trainings (mini CTFs)

- https://azure.enterprisesecurity.io/
- https://dartctf.enterprisesecurity.io/

Mini Training Ranges (self-hosted)

- https://github.com/ine-labs/AzureGoat
- https://github.com/mandiant/Azure_Workshop
- https://github.com/XMCyber/XMGoat

Book + Labs ($)

- https://github.com/PacktPublishing/Penetration-Testing-Azure-for-Ethical-Hackers

Trainings ($$$)

- https://training.xintra.org/attacking-and-defending-azure-m365
- https://www.alteredsecurity.com/azure-basic
- https://www.netspi.com/training/dark-side-ops-azure-cloud-pentesting/
- https://cloudbreach.io/

Penetration Testing Information

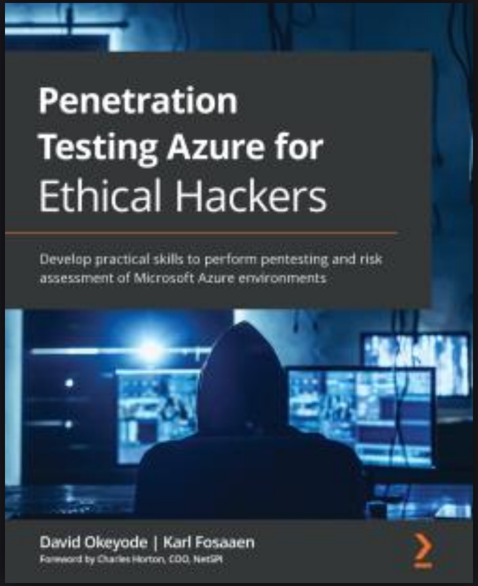
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20Azure%20Pentest.md
- https://www.cobalt.io/blog/azure-ad-pentesting-fundamentals
- https://github.com/Kyuu-Ji/Awesome-Azure-Pentest

Further readings

- https://csandker.io/2022/10/19/Untangling-Azure-Permissions.html
- https://csandker.io/2022/11/10/Untangling-Azure-II-Privileged-Access.html
- https://posts.specterops.io/azure-privilege-escalation-via-azure-api-permissions-abuse-74aee1006f48
- https://aadinternals.com/post/

Follow them for up2date information

- https://twitter.com/nikhil_mitt
- https://twitter.com/DrAzureAD
- https://twitter.com/DirectoryRanger
- https://twitter.com/XintraOrg
- https://twitter.com/0xcsandker
- https://twitter.com/_wald0

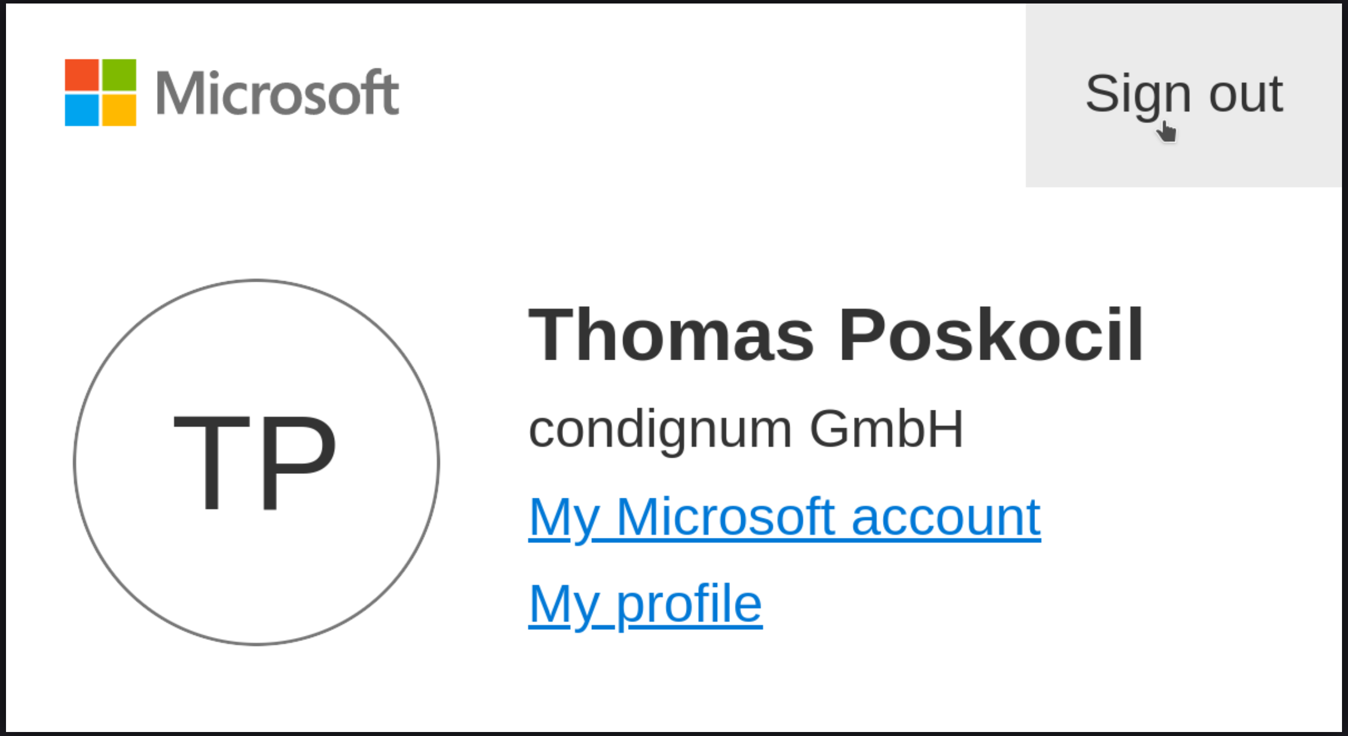


Penetration Testing Azure for Ethical Hackers

Develop practical skills to perform pentesting and risk assessment of Microsoft Azure environments

David Okeyode | Karl Fosaaen
Foreword by Charles Horton, COO, NetSPI

*Focus on the **ROLES** an attacker gained access to,*
rather than which resources were compromised



Thomas Poskocil

condignum GmbH

My Microsoft account

My profile