



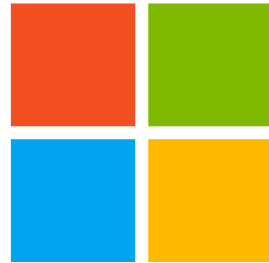
Deploying and Managing Conditional Access at Scale

Thomas Naunheim

#ScottishSummit2022

Thank You to our Sponsors...

Event Sponsor



Microsoft

Platinum Sponsors



the results company



Thank You to our Sponsors...

Gold Sponsors



Data Quality



Event Lunch



Accessibility



Data Analytics



Thomas Naunheim

Cloud Architect
glueckkanja-gab AG



- Azure Identity + Security
- Microsoft MVP
- Co-Organizer Azure Meetup Bonn and Cloud Identity Summit
- Koblenz, Germany



www.cloud-architekt.net



[Thomas_Live](https://twitter.com/Thomas_Live)



[Cloud-Architekt](https://github.com/Cloud-Architekt)



<https://www.linkedin.com/in/thomasnaunheim>



#ScottishSummit2022



Many Thanks to...

glueckkanja  gab



Microsoft
Partner


Gold Application Development
Gold Application Integration
Gold Cloud Platform
Gold Cloud Productivity
Gold Collaboration and Content
Gold Communications
Gold Data Analytics
Gold Datacenter
Gold DevOps
Gold Enterprise Mobility Management
Gold Messaging
Gold Project and Portfolio Management
Gold Security
Gold Small and Midmarket Cloud Solutions
Gold Windows and Devices

Microsoft
Partner


Advanced Specialization
Calling for Microsoft Teams
Advanced Specialization
Identity and Access Management
Advanced Specialization
Meetings and Meeting Rooms
for Microsoft Teams
Advanced Specialization
Microsoft Azure Virtual Desktop
Advanced Specialization
Teamwork Deployment
Advanced Specialization
Threat Protection
Advanced Specialization
Windows Server and SQL Server
Migration to Microsoft Azure

Microsoft
Partner

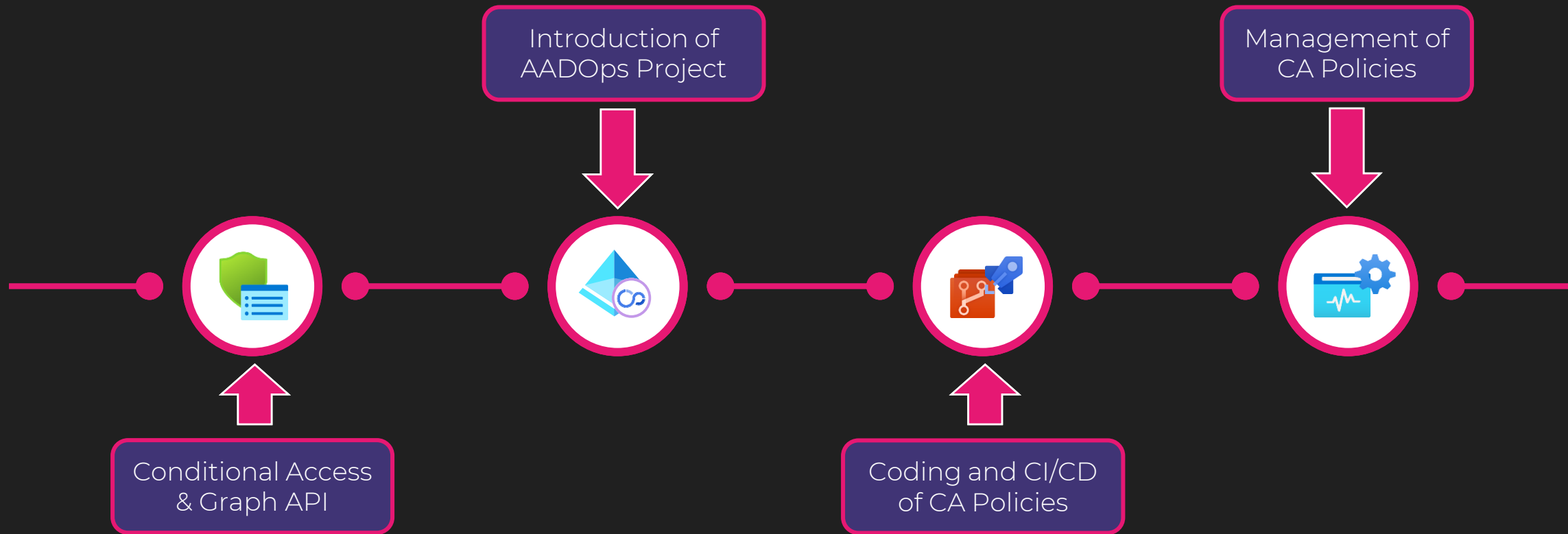

2020 Partner of the Year Finalist
Security and Compliance Award
2019 Partner of the Year Winner
Germany
2019 Partner of the Year Winner
Modern Desktop
2017 Partner of the Year Winner
Enterprise Mobility Award

Microsoft
MISA


Member of
Microsoft Intelligent
Security Association

#ScottishSummit2022

Agenda



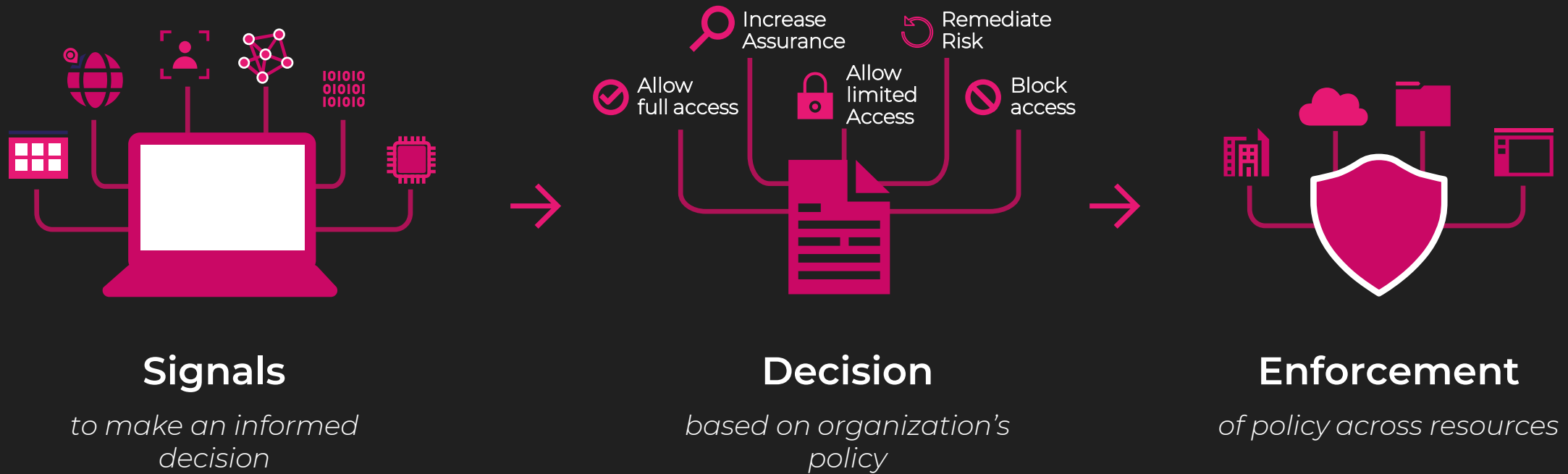


Conditional Access & Microsoft Graph

How to deploy and manage your “Zero Trust Policy Engine” as Code!

#ScottishSummit2022

Zero Trust Policy Engine



Conditional Access (CA) Policy

When this happens...

A user from (group) "Marketing employees" is accessing "Office 365" from a browser on a Windows device from any location and no sign-in risk was detected.

...then do this!

Require a user with strong (multi-factor) authentication and device to be marked as compliant. No session control (CA App Control policies or limited sign-in frequency).

Conditional Access

- id
- displayName
- state

Conditions

- Users, Groups, Apps/Actions
- Identity Risk, Device, Locations and Client Apps

Access Controls

1. Block Access
2. Grant Access
3. Session Controls

Microsoft Graph: "/identity/conditionalAccess/policies"

```
id      : b735629f-49b7-4a5a-8389-f9ae109a3a2d
displayName : Office 365: Require MFA and compliant device
state   : enabled

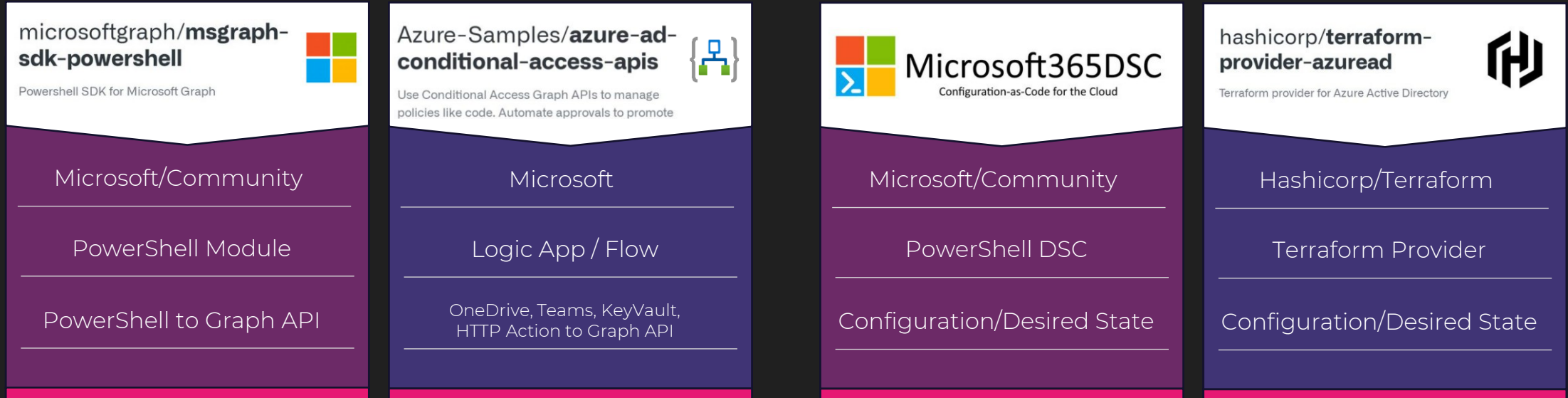
conditions : {
  "users": {...},
  "applications": {...},
  "platforms": {...},
  "locations": {...},
  "signInRiskLevels": [...],
  "clientAppTypes": [...]
}

grantControls: {
  "operator": "OR",
  "builtInControls": [...],
  "customAuthenticationFactors": [],
  "termsOfUse": []
}

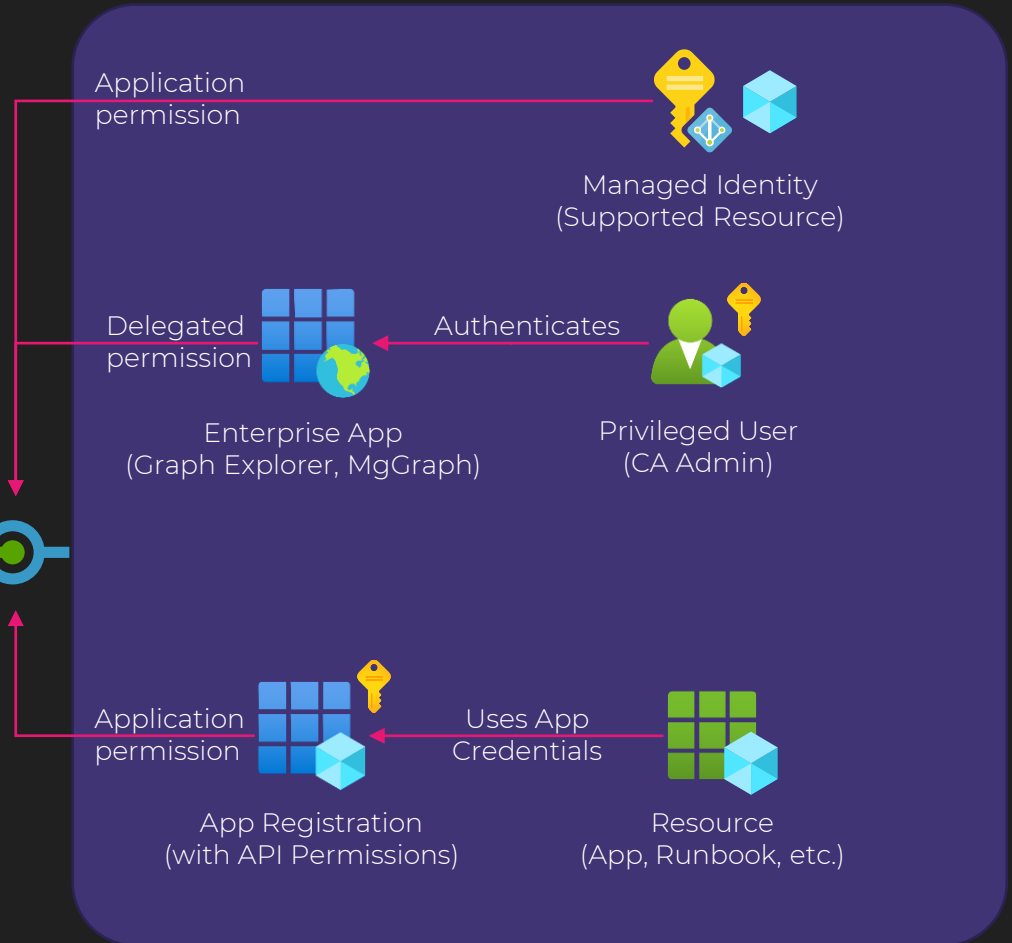
sessionControls: {}
```



CA Configuration As Code

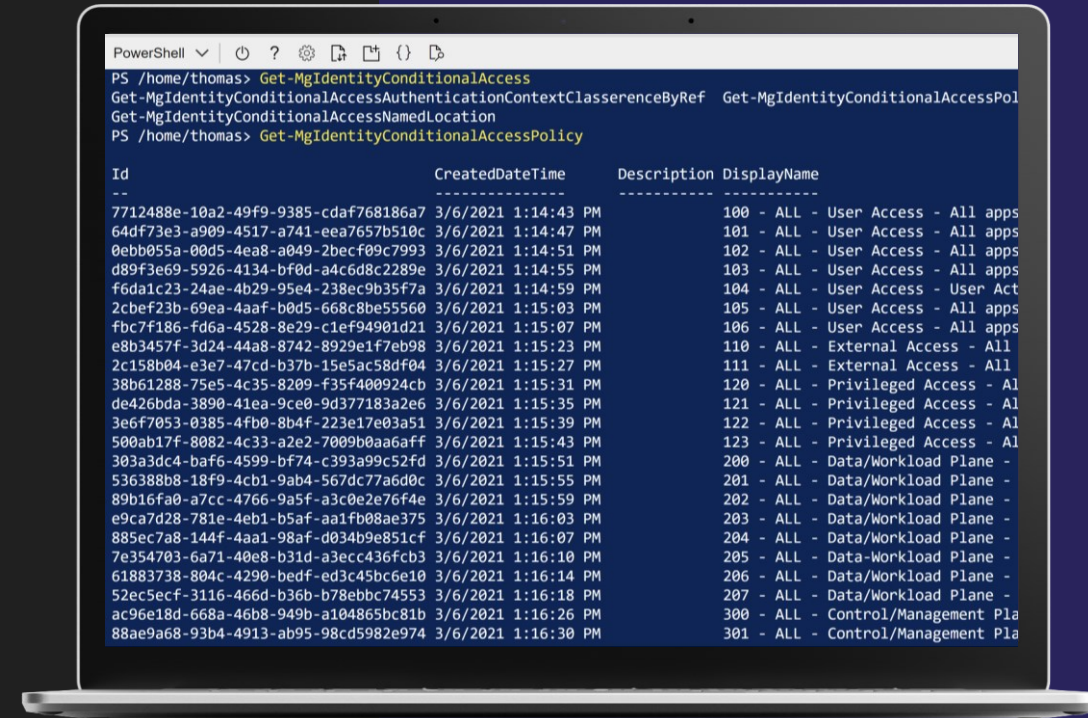


Microsoft Graph API Access



Demo Graph API

- Microsoft Graph SDK PowerShell Module
- Logic App Sample from Microsoft (Ignite)



```
PowerShell
PS /home/thomas> Get-MgIdentityConditionalAccess
Get-MgIdentityConditionalAccessAuthenticationContextClasserenceByRef Get-MgIdentityConditionalAccessPol
Get-MgIdentityConditionalAccessNamedLocation
PS /home/thomas> Get-MgIdentityConditionalAccessPolicy
```

Id	CreatedDateTime	Description	DisplayName
7712488e-10a2-49f9-9385-cdaf768186a7	3/6/2021 1:14:43 PM		100 - ALL - User Access - All apps
64df73e3-a909-4517-a741-eea7657b510c	3/6/2021 1:14:47 PM		101 - ALL - User Access - All apps
0ebb055a-00d5-4ea8-a049-2becf09c7993	3/6/2021 1:14:51 PM		102 - ALL - User Access - All apps
d89f3e69-5926-4134-bf0d-a4c6d8c2289e	3/6/2021 1:14:55 PM		103 - ALL - User Access - All apps
f6da1c23-24ae-4b29-95e4-238ec9b35f7a	3/6/2021 1:14:59 PM		104 - ALL - User Access - User Act
2cbef23b-69ea-4aaf-b0d5-668c8be55560	3/6/2021 1:15:03 PM		105 - ALL - User Access - All apps
fb7f186-fd6a-4528-8e29-c1ef94901d21	3/6/2021 1:15:07 PM		106 - ALL - User Access - All apps
e8b3457f-3d24-44a8-8742-8929e1f7eb98	3/6/2021 1:15:23 PM		110 - ALL - External Access - All
2c158b04-e3e7-47cd-b37b-15e5ac58df04	3/6/2021 1:15:27 PM		111 - ALL - External Access - All
38b61288-75e5-4c35-8209-f35f400924cb	3/6/2021 1:15:31 PM		120 - ALL - Privileged Access - A1
de426bda-3890-41ea-9ce0-9d377183a2e6	3/6/2021 1:15:35 PM		121 - ALL - Privileged Access - A1
3e6f7053-0385-4fb0-8b4f-223e17e03a51	3/6/2021 1:15:39 PM		122 - ALL - Privileged Access - A1
500ab17f-8082-4c33-a2e2-7009b0aa6aff	3/6/2021 1:15:43 PM		123 - ALL - Privileged Access - A1
303a3dc4-baf6-4599-bf74-c393a99c52fd	3/6/2021 1:15:51 PM		200 - ALL - Data/Workload Plane -
536388b8-18f9-4cb1-9ab4-567dc77a6d0c	3/6/2021 1:15:55 PM		201 - ALL - Data/Workload Plane -
89b16fa0-a7cc-4766-9a5f-a3c0e2e76f4e	3/6/2021 1:15:59 PM		202 - ALL - Data/Workload Plane -
e9ca7d28-781e-4eb1-b5af-aa1fb08ae375	3/6/2021 1:16:03 PM		203 - ALL - Data/Workload Plane -
885ec7a8-144f-4aa1-98af-d034b9e851cf	3/6/2021 1:16:07 PM		204 - ALL - Data/Workload Plane -
7e354703-6a71-40e8-b31d-a3ecc436fcb3	3/6/2021 1:16:10 PM		205 - ALL - Data/Workload Plane -
61883738-804c-4290-bedf-ed3c45bc6e10	3/6/2021 1:16:14 PM		206 - ALL - Data/Workload Plane -
52ec5ecf-3116-466d-b36b-b78ebbc74553	3/6/2021 1:16:18 PM		207 - ALL - Data/Workload Plane -
ac96e18d-668a-46b8-949b-a104865bc81b	3/6/2021 1:16:26 PM		300 - ALL - Control/Management Pla
88ae9a68-93b4-4913-ab95-98cd5982e974	3/6/2021 1:16:30 PM		301 - ALL - Control/Management Pla

CA Scripts & Templates

Fortigi/
ConditionalAccess 

Fortigi

Scripts, GUID Convert

PowerShell


DanielChronlund/
DCToolbox 

Tools for Microsoft cloud fans

Daniel Chronlund

Module, Templates, Report

PowerShell

AlexFilipin/
ConditionalAccess 

Alex Filipin

Scripts, Templates

PowerShell



Introduction of "AADOps" project

Manage your Conditional Access Policies in DevOps-style!

#ScottishSummit2022

DevOps for Conditional Access



Change Management

- Documentation of policy requirements and changes
- Planning, versioning (incl. backup/restore) and tracking policy changes
- Integration of "Quality Gates" and "Approval Workflows"



Ring- / Multi-Tenant (Staged) Deploy

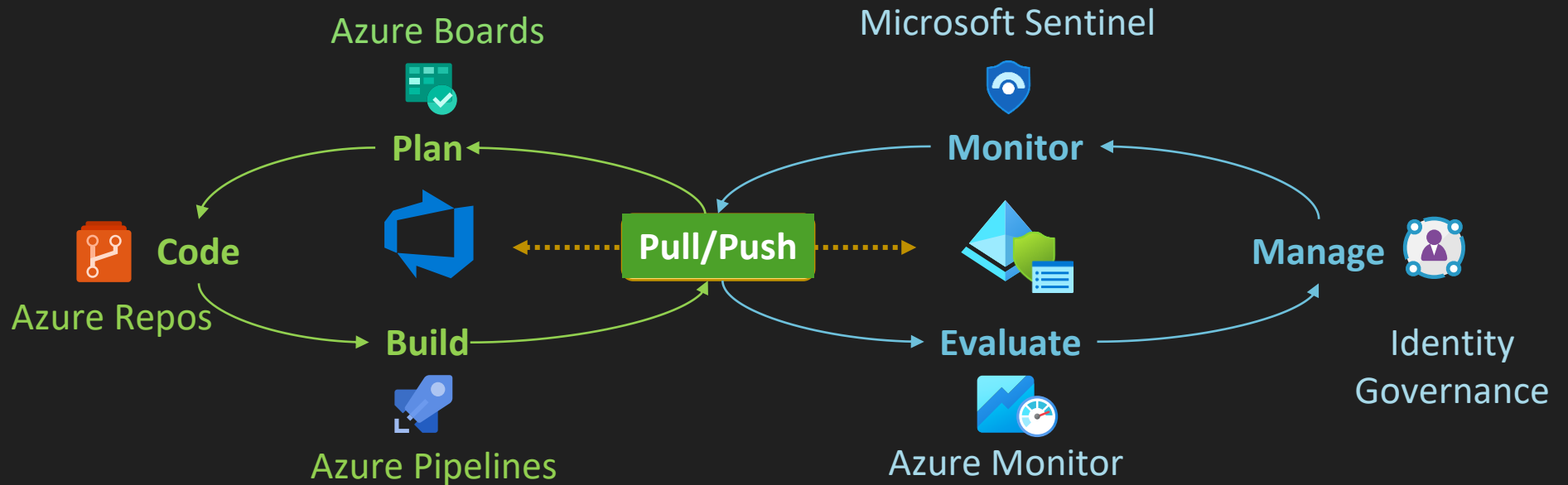
- Deploy policy configuration across various target groups or tenants
- Using templates for **standardized policy sets**
- **Reduced roll-out risks** by automated and staged deployment
- Reduced costs by automated deployment (Managed Service Provider)



Policy-As-Code and Governance

- Reduced role assignments to "Conditional Access Administrator"
- Comparison and "full visibility" of deployed policies (and changes)
- Roll-out of contingency plan and resilient access controls (in case of MFA disruption or emergency access)

DevOps for Conditional Access!



Flexibility of Core Components



Git Repository



PowerShell Core



YAML Pipeline

Demo Secure DevOps

- Layered Managed Identities
- Isolated and hardened Self-Hosted Pipeline Agents

```

werShell
/home/thomas> Get-MgIdentityConditionalAccess
t-MgIdentityConditionalAccessAuthenticationContextClasserenceByRef Get-MgIdentityConditionalAccess
t-MgIdentityConditionalAccessNamedLocation
/home/thomas> Get-MgIdentityConditionalAccessPolicy

```

	CreatedDateTime	Description	DisplayName
12488e-10a2-49f9-9385-cdaf768186a7	3/6/2021 1:14:43 PM	100 - ALL - User Access - All a	
df73e3-a909-4517-a741-eea7657b510c	3/6/2021 1:14:47 PM	101 - ALL - User Access - All a	
bb055a-00d5-4ea8-a049-2becf09c7993	3/6/2021 1:14:51 PM	102 - ALL - User Access - All a	
9f3e69-5926-4134-bf0d-a4c6d8c2289e	3/6/2021 1:14:55 PM	103 - ALL - User Access - All a	
da1c23-24ae-4b29-95e4-238ec9b35f7a	3/6/2021 1:14:59 PM	104 - ALL - User Access - User	
bef23b-69ea-4aaf-b0d5-668c8be55560	3/6/2021 1:15:03 PM	105 - ALL - User Access - All a	
c7f186-fd6a-4528-8e29-c1ef94901d21	3/6/2021 1:15:07 PM	106 - ALL - User Access - All a	
b3457f-3d24-44a8-8742-8929e1f7eb98	3/6/2021 1:15:23 PM	110 - ALL - External Access - A	
158b04-e3e7-47cd-b37b-15e5ac58df04	3/6/2021 1:15:27 PM	111 - ALL - External Access - A	
b61288-75e5-4c35-8209-f35f400924cb	3/6/2021 1:15:31 PM	120 - ALL - Privileged Access -	
426bda-3890-41ea-9ce0-9d377183a2e6	3/6/2021 1:15:35 PM	121 - ALL - Privileged Access -	
6f7053-0385-4fb0-8b4f-223e17e03a51	3/6/2021 1:15:39 PM	122 - ALL - Privileged Access -	
0ab17f-8082-4c33-a2e2-7009b0aa6aff	3/6/2021 1:15:43 PM	123 - ALL - Privileged Access -	
3a3dc4-baf6-4599-bf74-c393a99c52fd	3/6/2021 1:15:51 PM	200 - ALL - Data/Workload Plane	
6388b8-18f9-4cb1-9ab4-567dc77a6d0c	3/6/2021 1:15:55 PM	201 - ALL - Data/Workload Plane	
b16fa0-a7cc-4766-9a5f-a3c0e2e76f4e	3/6/2021 1:15:59 PM	202 - ALL - Data/Workload Plane	
ca7d28-781e-4eb1-b5af-aa1fb08ae375	3/6/2021 1:16:03 PM	203 - ALL - Data/Workload Plane	
5ec7a8-144f-4aa1-98af-d034b9e851cf	3/6/2021 1:16:07 PM	204 - ALL - Data/Workload Plane	
354703-6a71-40e8-b31d-a3ecc436fcb3	3/6/2021 1:16:10 PM	205 - ALL - Data/Workload Plane	
883738-804c-4290-bedf-ed3c45bc6e10	3/6/2021 1:16:14 PM	206 - ALL - Data/Workload Plane	
ec5ecf-3116-466d-b36b-b78ebbc74553	3/6/2021 1:16:18 PM	207 - ALL - Data/Workload Plane	
96e18d-668a-46b8-949b-a104865bc81b	3/6/2021 1:16:26 PM	300 - ALL - Control/Management	
ae9a68-93b4-4913-ab95-98cd5982e974	3/6/2021 1:16:30 PM	301 - ALL - Control/Management	

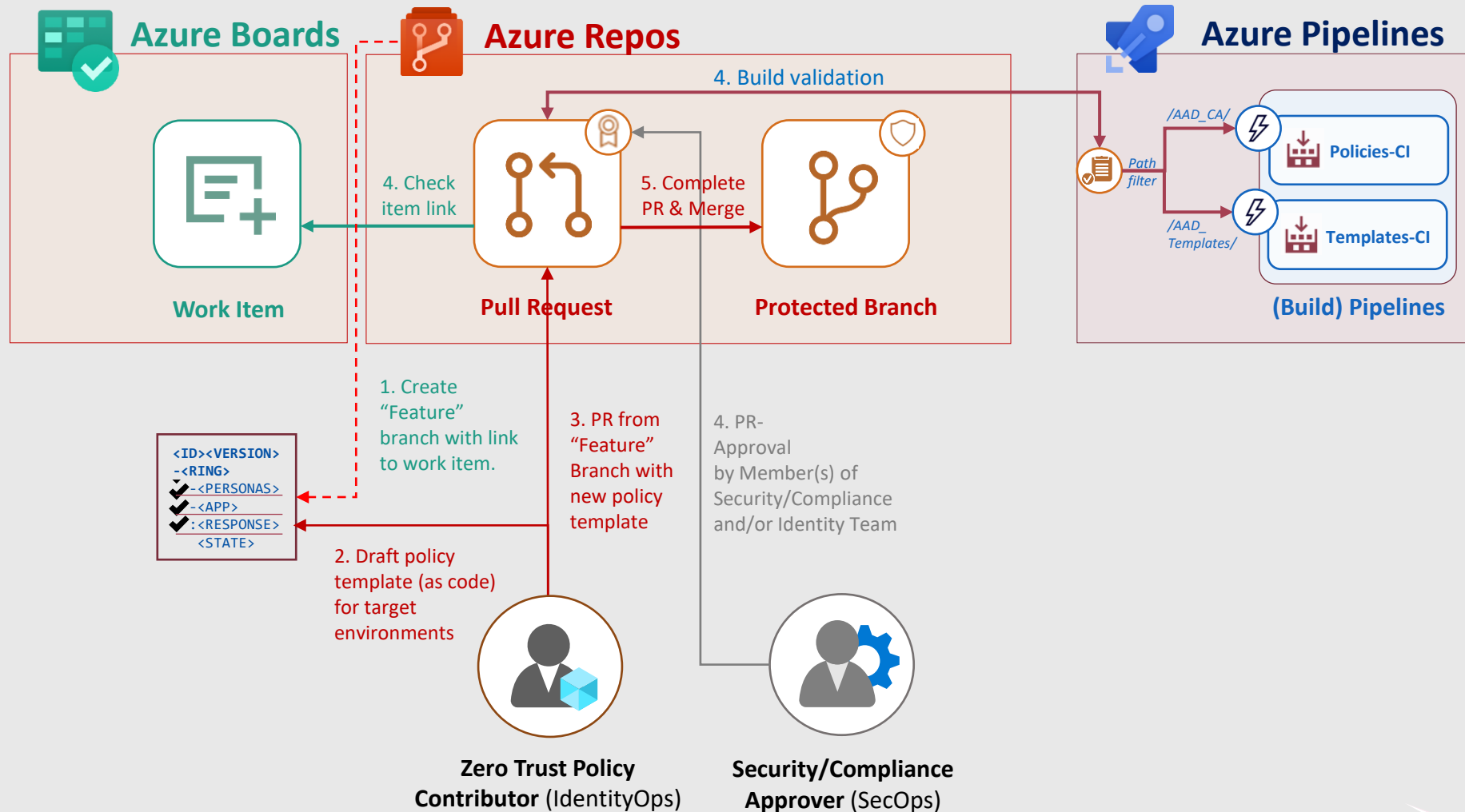


Coding and CI/CD of CA Policies

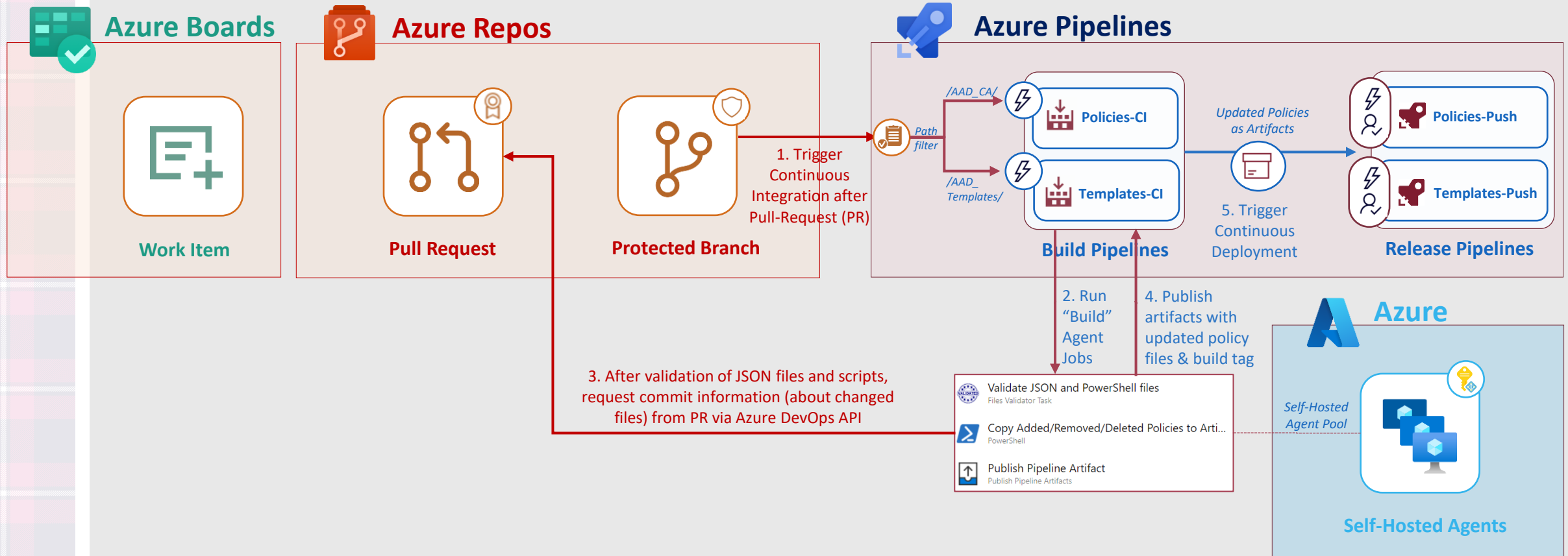
Safe and staged deployment of policies and templates at Scale!

#ScottishSummit2022

AADOps Planning & Coding

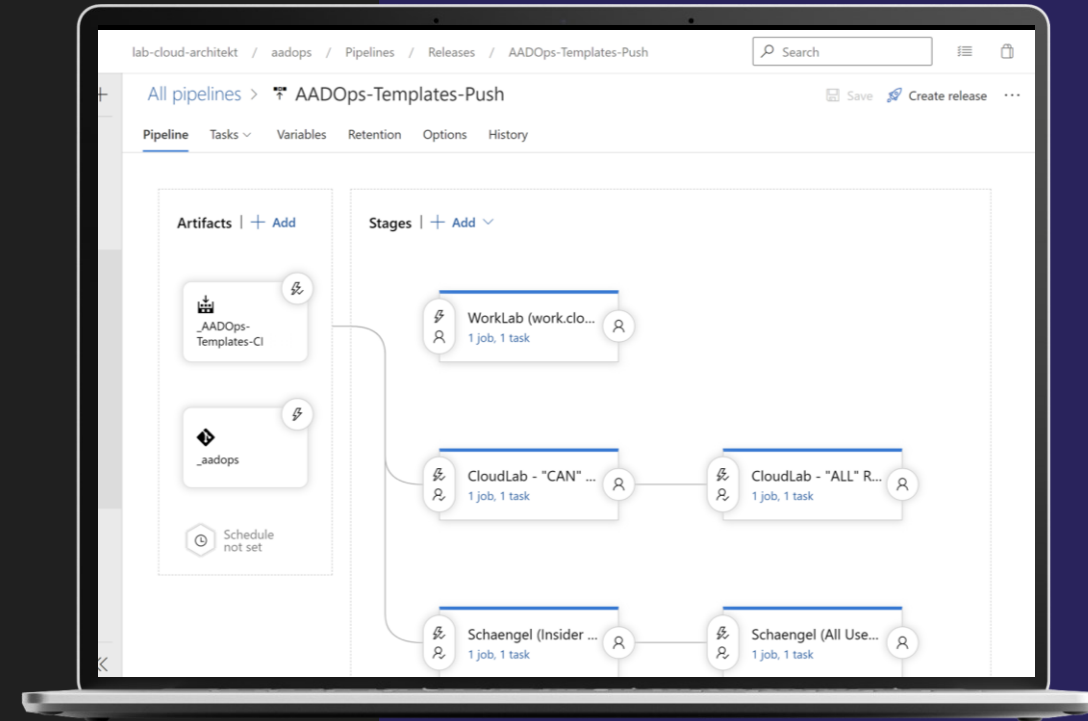


AADOps Build Policies (CI)



Demo Pull/Push and CI

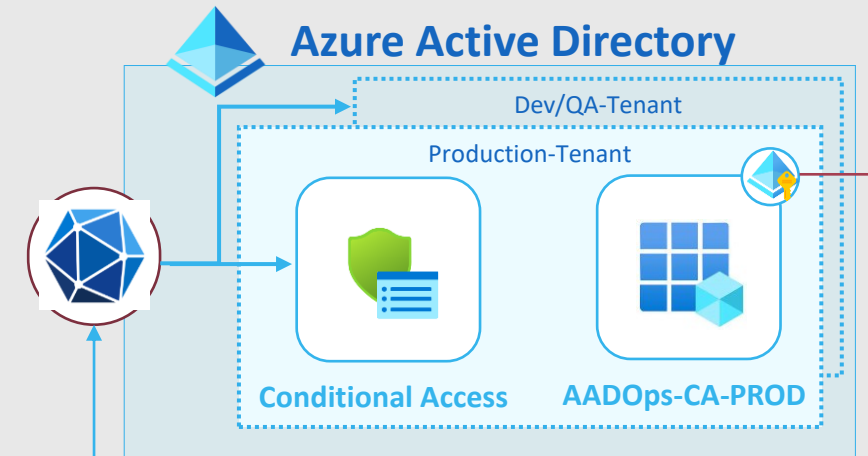
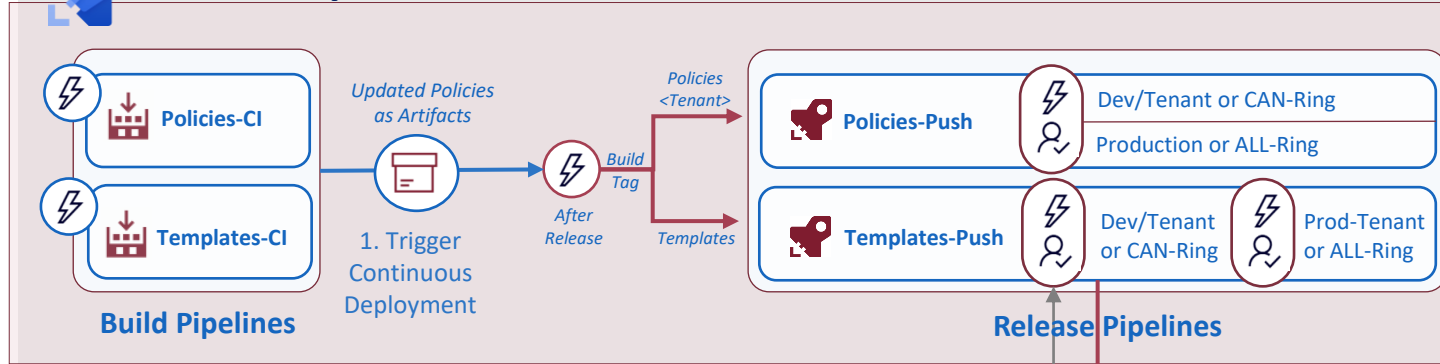
- Pull-Pipeline
- Inclusion between “GUI” and “DevOps” style AAD admin
- Validation of JSON
- Work Item Links



AADOps Deploy Templates



Azure Pipelines



2. Pre-Deployment Approval
by Member(s) of
Identity Team

3. Run
Agent
Jobs

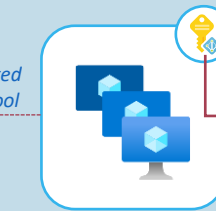
4. Microsoft Graph API
Calls to target (staging)
environment

Push-AADOpsConditionalAccess
 PowerShell

- ✓ **Download Artifacts**
- ✓ **MSI/KeyVault Access**
- ✓ **Create Exclusion Groups**
- ✓ **Replacement of Variables**
 - ✓ Ring/Stage
 - ✓ Version
- ✓ **Create/update policies**

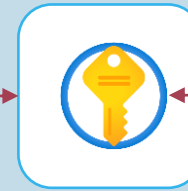


Self-Hosted
Agent Pool



Self-Hosted Agents

Using MSI
to get secrets
from KeyVault



Azure KeyVault

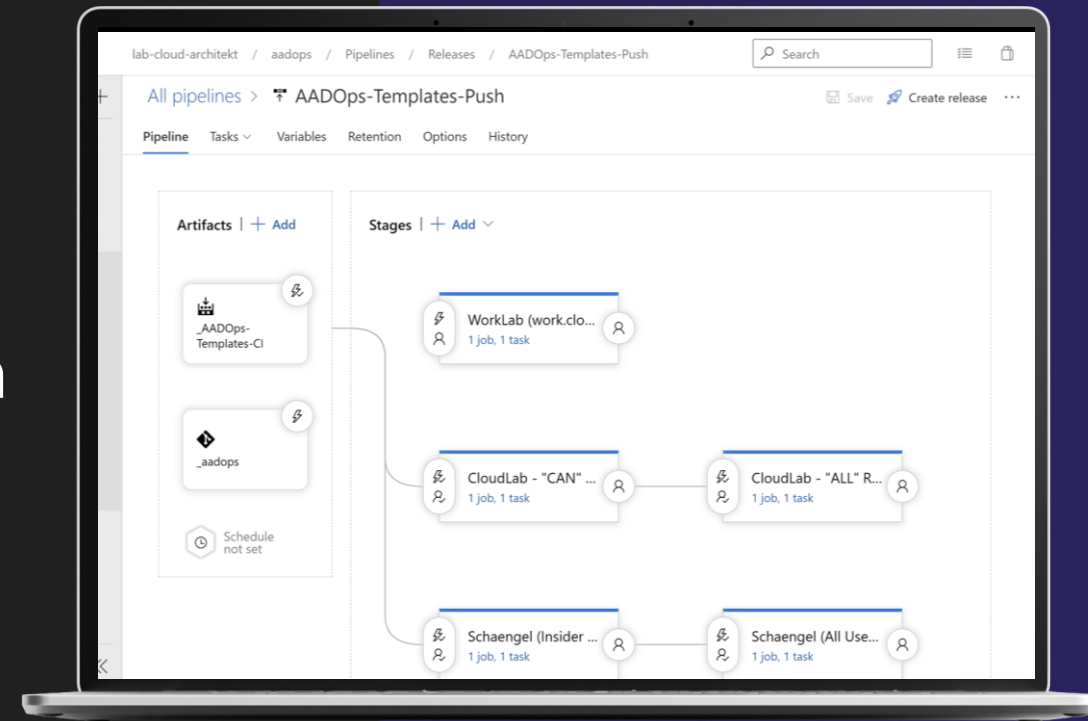
Secrets or certificate of Service Principal with required
application permissions to Microsoft Graph API



AAD Tenant/Service
Owner (IdentityOps)

Demo CA Templates

- Continuous Deployment
- Staging of CA Templates
- Tracking Deployment Stage in Work Items





Operationalization of CA Management

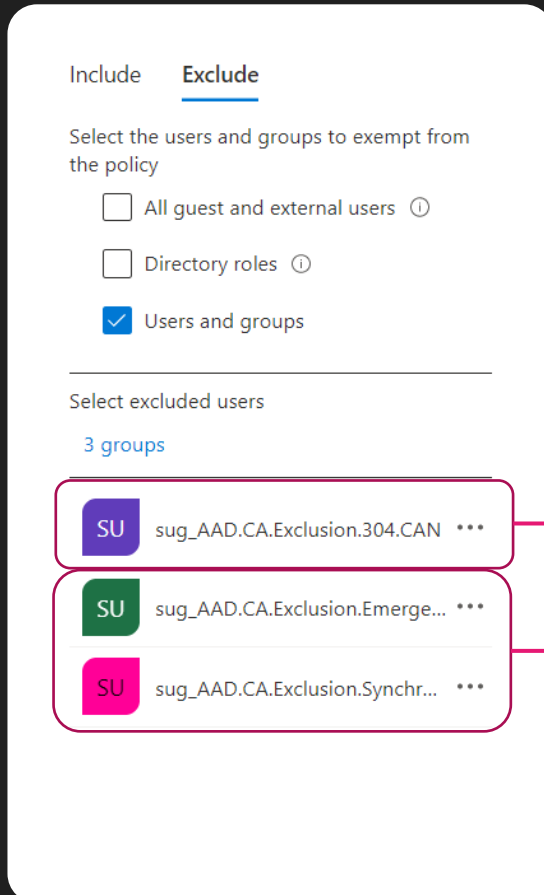
Automated and monitored management of Policy lifecycle!

#ScottishSummit2022

Conditional Access Exclusions

General approach:

- Exclusion by (Cloud-only) Security Group
- Privileged Role Assignable Group for Protection?
- Review of Excluded Groups (Azure AD access reviews)
- Monitoring of Exclusion Group

A screenshot of the Azure AD Conditional Access Exclusions configuration page. The "Exclude" tab is selected. Under "Select the users and groups to exempt from the policy", the "Users and groups" option is checked. Under "Select excluded users", three groups are listed: "sug_AAD.CA.Exclusion.304.CAN", "sug_AAD.CA.Exclusion.Emerge...", and "sug_AAD.CA.Exclusion.Synchr...". Each group entry has a colored icon (purple, green, and pink respectively) and a "SU" label. Red arrows point from the first and third group entries to the "Use Case A" and "Use Case B" sections respectively.

Include **Exclude**

Select the users and groups to exempt from the policy

☐ All guest and external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Select excluded users

3 groups

SU	sug_AAD.CA.Exclusion.304.CAN	***
SU	sug_AAD.CA.Exclusion.Emerge...	***
SU	sug_AAD.CA.Exclusion.Synchr...	***

Use Case A: Individual or wide scoped

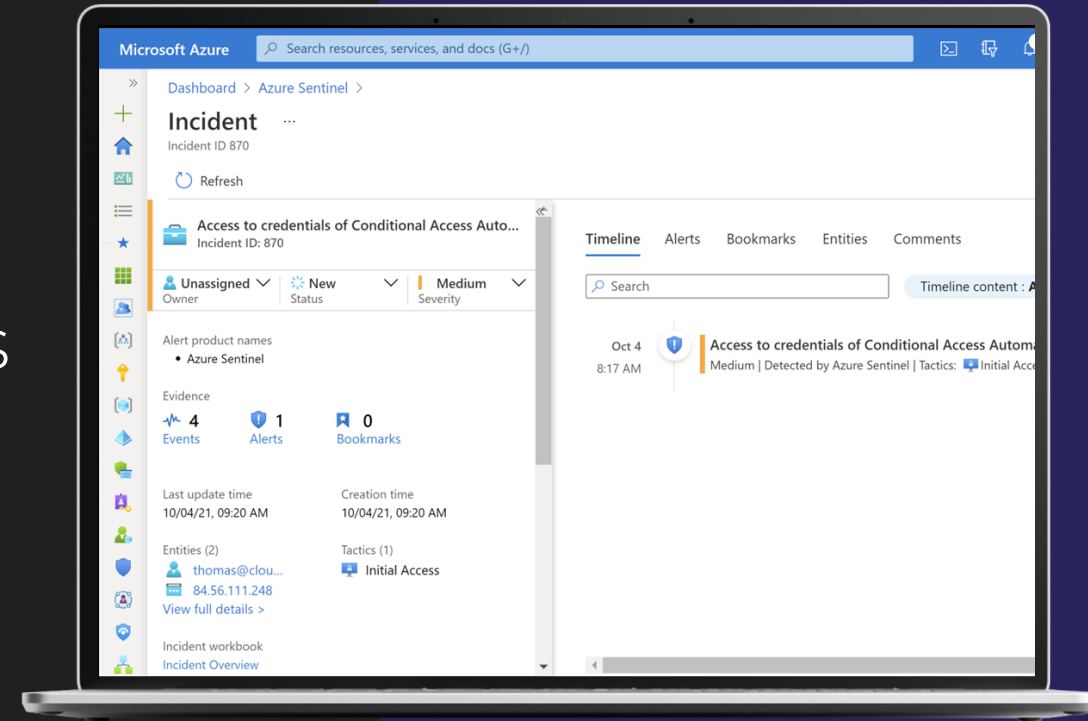
- Temporary or limited Exclusion
- Exclusion for each policy (or group of policies)
- Exclusion after approval process, assignment as Access Package

Use Case B: Break Glass or Sync Account

- Permanent Exclusion
- Assignment to certain account type, strictly monitored

Demo CA Governance

- Exclusion Management with Azure AD Identity Governance
- Microsoft Sentinel Incidents as work items in AADOPs
- Operational Insights of Conditional Access policies



Conditional Access Monitoring



Operational Insights

Azure AD Insights and Workbooks:

- Analyses and Visualizations to understand impact of Conditional Access Policies and gaps in your environment
- Coverage of apps, users and locations



Auditing

Azure AD Audit Logs:

- Changes on CA Policies
- Changes on Target/Exclusion Groups
- State change (Deactivated, Report-only, Activated)

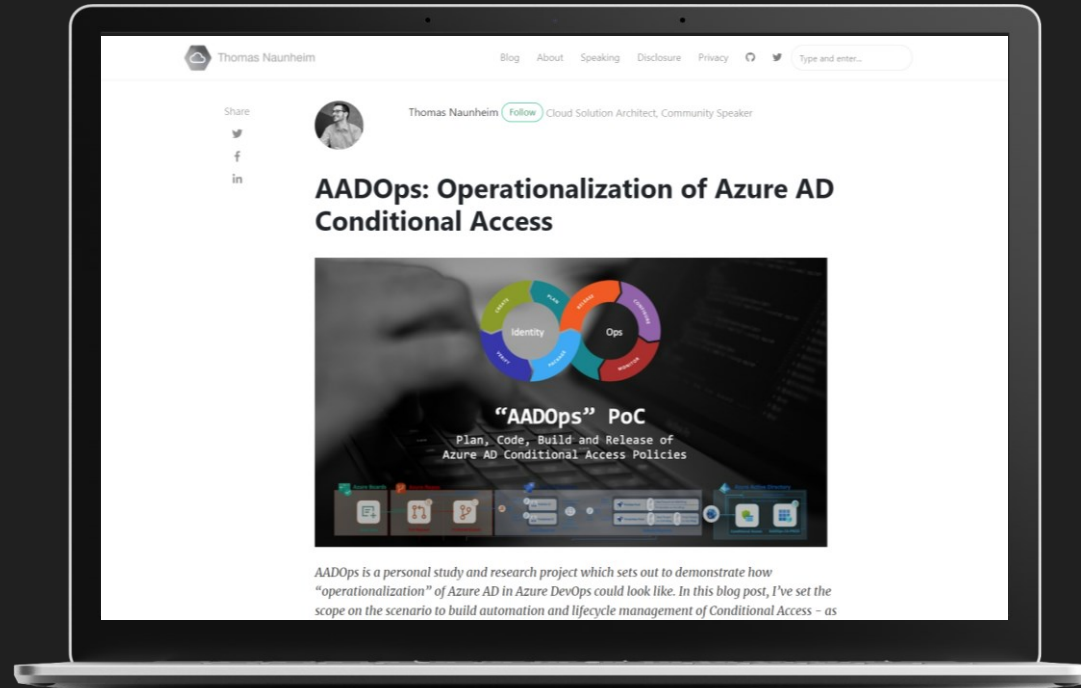


Security Insights

Microsoft Sentinel:

- Attempt to bypass conditional access rule in Azure AD
- Correlation of data from Azure DevOps and Azure Audit Logs (detection of changes outside of automated process)

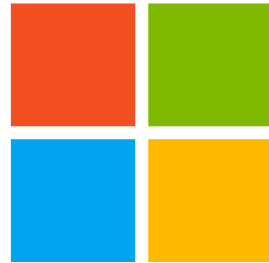
Learn more about AADOps



AADOps: Operationalization
of Azure AD Conditional Access
[Cloud-Architekt.net](https://cloud-architekt.net)

Thank You to our Sponsors...

Event Sponsor



Microsoft

Platinum Sponsors



the results company



Thank You to our Sponsors...

Gold Sponsors



Data Quality



Event Lunch



Accessibility



Data Analytics



Q&A | Thank You!



www.cloud-architekt.net



Thomas_Live



Cloud-Architekt



<https://www.linkedin.com/in/thomasnaunheim>

#ScottishSummit2022