

Demystify Microsoft Entra Workload Identities

Thomas Naunheim
Cloud Security Architect
@glueckkanja-gab AG

Workplace Ninja Summit 2022





Platin Sponsor



Gold Sponsor

glueckkanja  gab

baseVISION
SECURE & MODERN WORKPLACE



RECAST SOFTWARE

 LIQUIT

Lenovo

 Snapdragon

Silver and Special Sponsors



LUZERN 
FACEBOOK
DIE STADT. DER SEE. DIE BERGE.

sepago[®]

EPIC  USION


SCAPPMAN

APPMANAGEMENT.COM

2022 | OCTOBER 7
NETHERLANDS

dinext.



Thomas Naunheim

Cloud Security Architect
@glueckkanja-gab AG



@Thomas_Live



cloud-architekt.net





AGENDA

Key takeaways:

- Differences of various workload identity types
- Protection to prevent abuse of non-human identities
- Recommendations on active monitoring with enriched and advanced monitoring

- What are workload identities?
- Different types of workload identities
- Lifecycle and delegated management
- Protection and secure access
- Advanced auditing and monitoring

What are workload identities?





Human and Machine Identities



Human Identities

- Employees
- Partners
- Customers
- Vendors
- Consultants



Machine Identities

Workload Identities

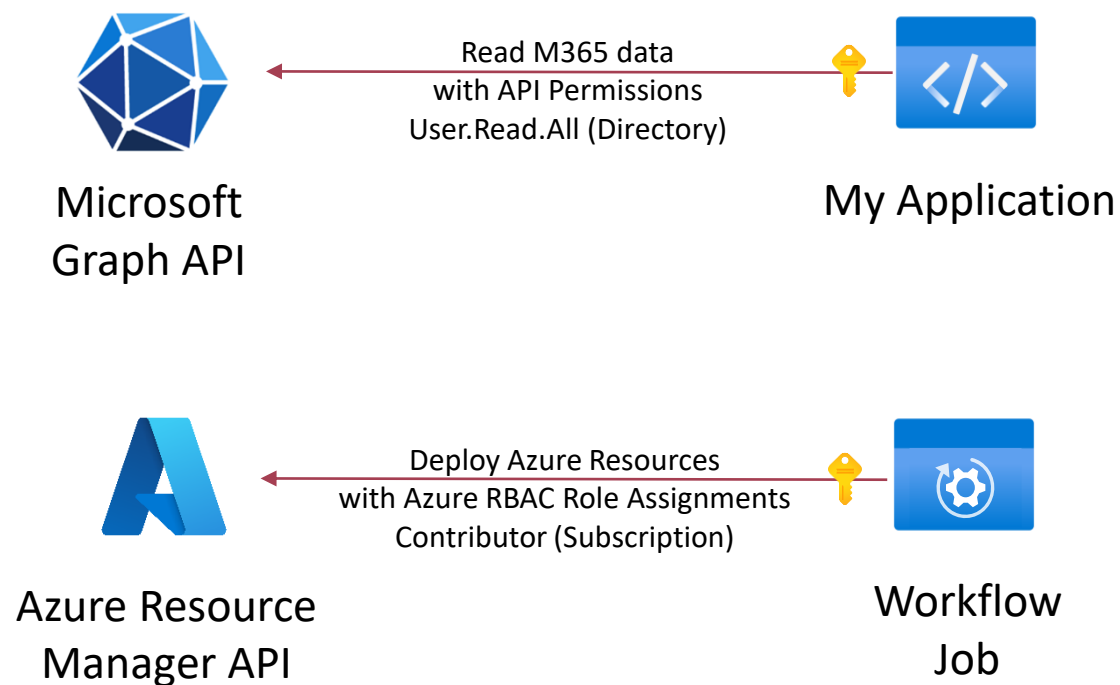
- Containers
- Virtual Machines
- Applications
- Services

Device Identities

- Mobile devices
- IoT/OT devices
- Desktop computers

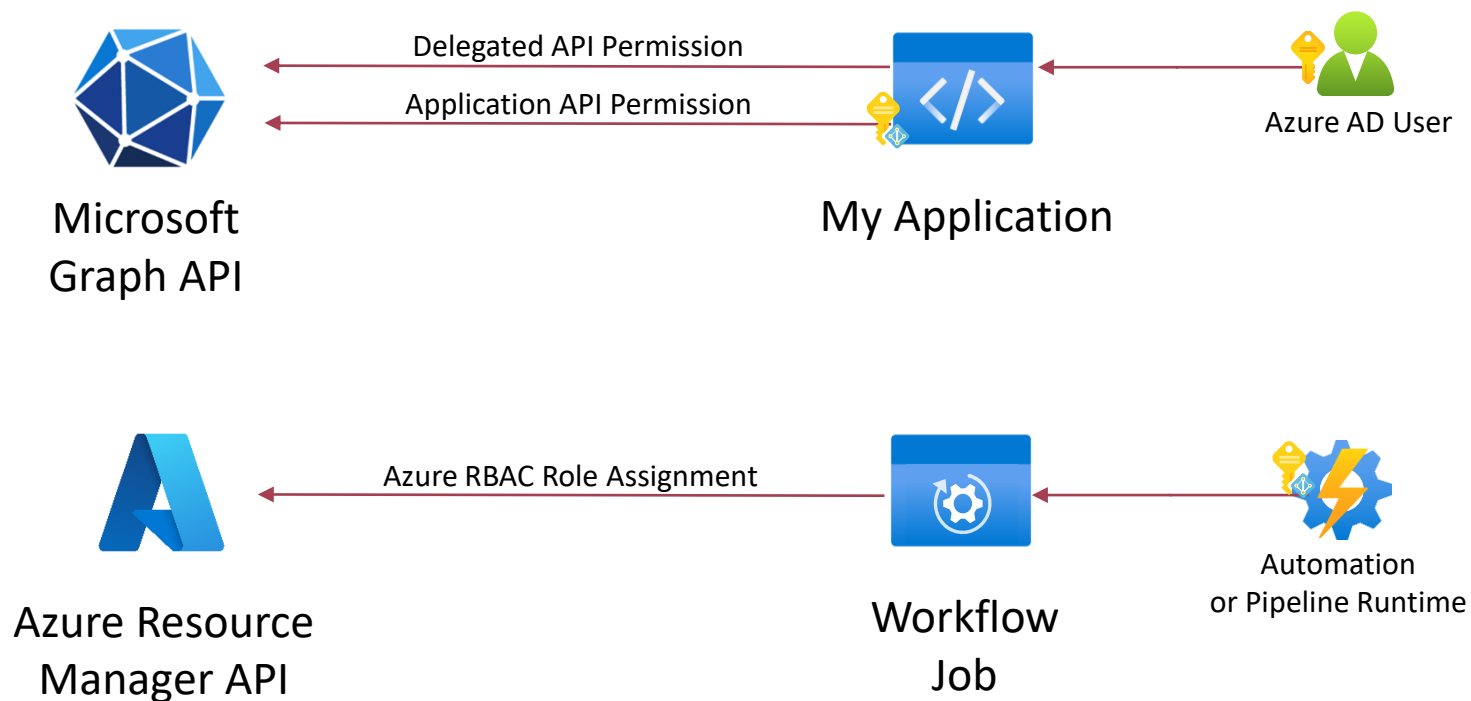


Service-to-Service Interaction





Service-to-Service Interaction

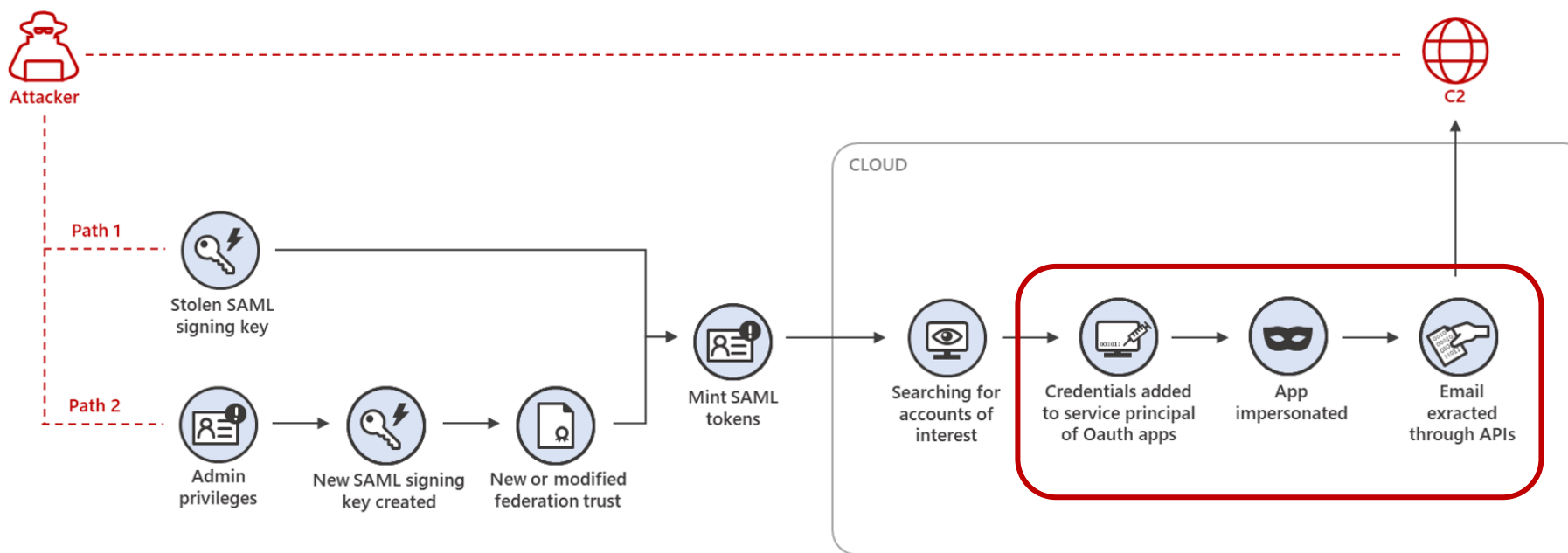




Service Principals in attack paths

SOLORIGATE ATTACK

Stage 3: Hands-on-keyboard attack in the cloud



Types of workload identities

Various options of credentials and integration





Service Principals with Client Secrets

Your Workload Identity

Application Instance



Service Principal
(Enterprise App)

Definition of Application



Application
(App Registration)



API Permissions



Client Secret



App Roles



Properties

Validates Client Secret

Membership



Azure AD
Roles



Group
Membership

API Access

Granted Admin/User
Consent Permissions



User.Read

Defines Required
Delegated/App Permissions

Exposed API
or App Roles
Permissions



Microsoft
Graph

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>

/token
Endpoint

Request
with
Shared
secret

Workload Env.

Shared
Secret



Your
Workload

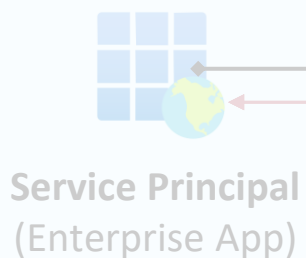
Authentication
Library



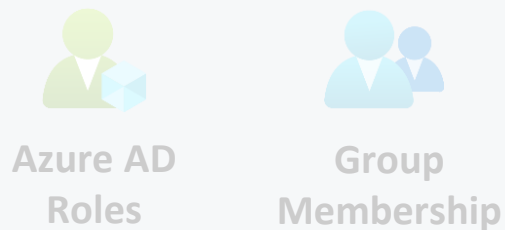
Service Principals with Certificate

Your Workload Identity

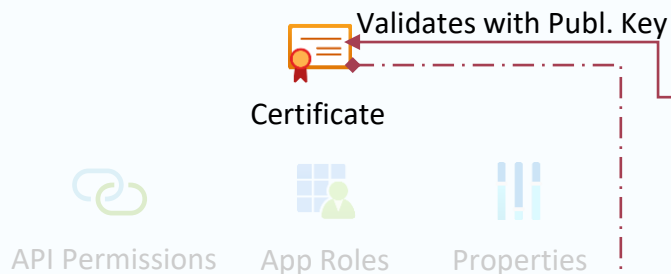
Application Instance



Membership

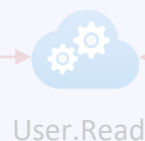


Definition of Application



API Access

Granted Admin/User
Consent Permissions



Exposed API
or App Roles
Permissions



Defines Required
Delegated/App Permissions

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>

**/token
Endpoint**

Request
with signed
JWT
token

Token with
API Scope
& Groups

Workload Env.

Private
/Public Key



**Authentication
Library**

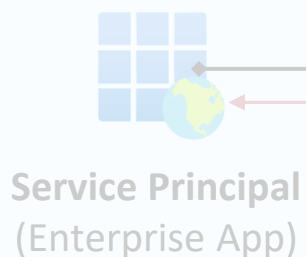
**Your
Workload**



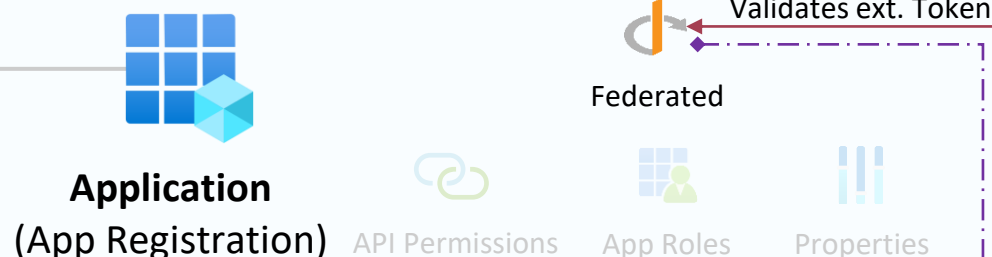
Workload identity federation

Your Workload Identity

Application Instance



Definition of Application

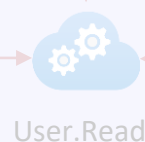


Membership



API Access

Granted Admin/User
Consent Permissions



Exposed API
or App Roles
Permissions



Defines Required
Delegated/App Permissions

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>

**/token
Endpoint**

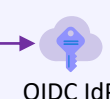
Request
with
Ext. IdP
token

Token with
API Scope
& Groups

Workload Env.



**Your
Workload**



Establish Trust relationship



Multi-Tenant App

Customer / Resource Tenant

Application Instance



Create SP
from App

**Service Principal
(Enterprise App)**

Membership



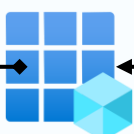
**Azure AD
Roles**



**Group
Membership**

Your Azure AD / Home Tenant

Definition of Application



**Application
(App Registration)**

Certificate

Client Secret

Federated

API Permissions

App Roles

Properties

API Access

Granted Admin/User
Consent Permissions

User.Read

Exposed API
or App Roles
Permissions



**Microsoft
Graph**

Microsoft Identity Platform

<https://login.microsoftonline.com/common>

**/token
Endpoint**

Request with
Cred. Token with
API Scope
& Groups

**/admin
consent**

Redirect for
admin user

Workload Env.



**Your
Workload**

Auth. Library



Demo: Federated Credentials

www.wpninjas.eu

- Abuse and replay of token from Federated Workload (GitHub Actions)





System-Assigned Managed Identity

Your Workload Identity

Application Instance



Service Principal
(Enterprise App)



API
Permissions

Management of Identity

Managed Identity Resource Provider
(MSRP)



Certificate

issues certificates
and rolling secrets

Membership



Azure AD
Roles



Group
Membership

API Access

Granted Admin/User
Consent Permissions



User.Read

Exposed API
or App Roles
Permissions



Microsoft
Graph

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>



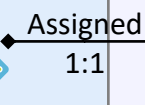
/token
Endpoint

Token with API Scope & Groups

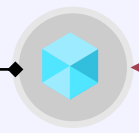
Request with signed JWT token

Azure Managed Resource

**Managed
Identity**
(System)



Assigned
1:1



**Your
Workload**

**Azure Instance
Metadata Service (IMDS)**

[http://169.254.169.254/
metadata/identity](http://169.254.169.254/metadata/identity)

Request
token locally

/token
Endpoint





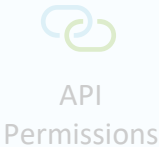
User-Assigned Managed Identity

Your Workload Identity

Application Instance



Service Principal
(Enterprise App)



Membership



Azure AD
Roles



Group
Membership

Management of Identity

Managed Identity Resource Provider
(MSRP)

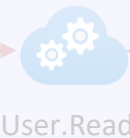


Certificate

issues certificates
and rolling secrets

API Access

Granted Admin/User
Consent Permissions



User.Read

Exposed API
or App Roles
Permissions



Microsoft
Graph

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>

Request with signed JWT token/
Token with API Scope & Groups

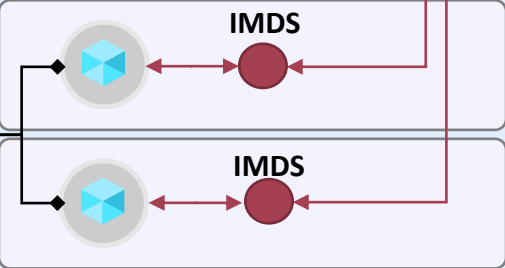


/token
Endpoint

Azure Managed Resource

Managed
Identity
(User)

Assigned
1:N



Your
Workloads



Demo: Managed Identities




www.wpninjas.eu

- Managed Identities - Behind the scene
- User-Assigned Identities and relation to Resource





Types of workload identities

	 Service Principal (Key- or Certificate)	 Service Principal (Federated Credentials)	 Managed Identity (System/User Assign.)
Supported Use Case	No limitation	Limited to supported Workloads (outside of Azure)	Limited to supported Workloads (Azure-managed Resources)
Security Boundary	Single- or multi-tenant	Single- or multi-tenant	Single-tenant*
Relation to Workload	Unassigned	Assigned to Issuer/Entity	Assigned to Resource(s) System (1:1), User (N:1)
Workload Environment	Everywhere	Supported OIDC Federated IdP	Azure- and Azure Arc-enabled resources
Token Lifetime / Cache	1h (Default), 24h (CAE)	less than or equal to 1h	24h (<u>Cache per resource URI</u>)

* access to Azure Resources from onboarded subscriptions via Azure Lighthouse

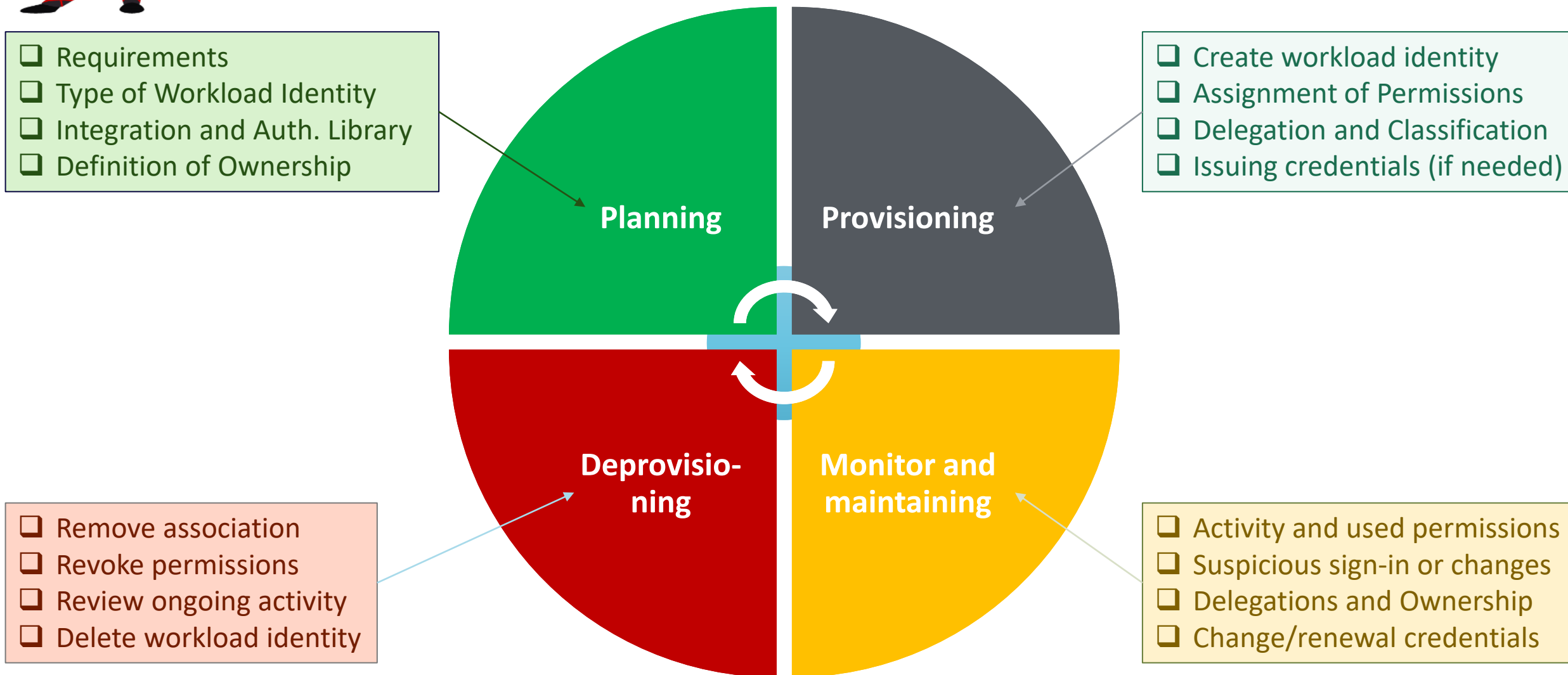
Lifecycle and delegated management

Governance process for non-human identities








Lifecycle process





Types of workload identities

www.wpninjas.eu

	 Service Principal (Key- or Certificate)	 Service Principal (Federated Credentials)	 Managed Identity (System/User Assign.)
Supported Use Case	No limitation	Limited to supported Workloads	Limited to supported Workloads (Azure-managed Resources)
Relation to Workload	Unassigned	Assigned to Issuer/Entity	Assigned to Resource(s) System (1:1), User (N:1)
Workload Environment	Everywhere	Supported OIDC Federated IdP	Azure- and Azure Arc-enabled resources
Lifecycle management	Managed by Admin	Managed by Admin	System: Shared Lifecycle with Resource, User: Independent, Managed by Admin
Delegated Management	Application/Enterprise App Owner Azure AD Role (Directory, Object)		Enterprise App Owner, Azure AD Role Azure RBAC Role/Resource Owner
Built-in recovery from deletions	Soft deleted		Not Available



Demo: Delegation and Management

www.wpninjas.eu

- Default Permissions and Custom Roles for Delegated Management
- App Management Policies
- Classification of Workload Identities



Protection and secure access

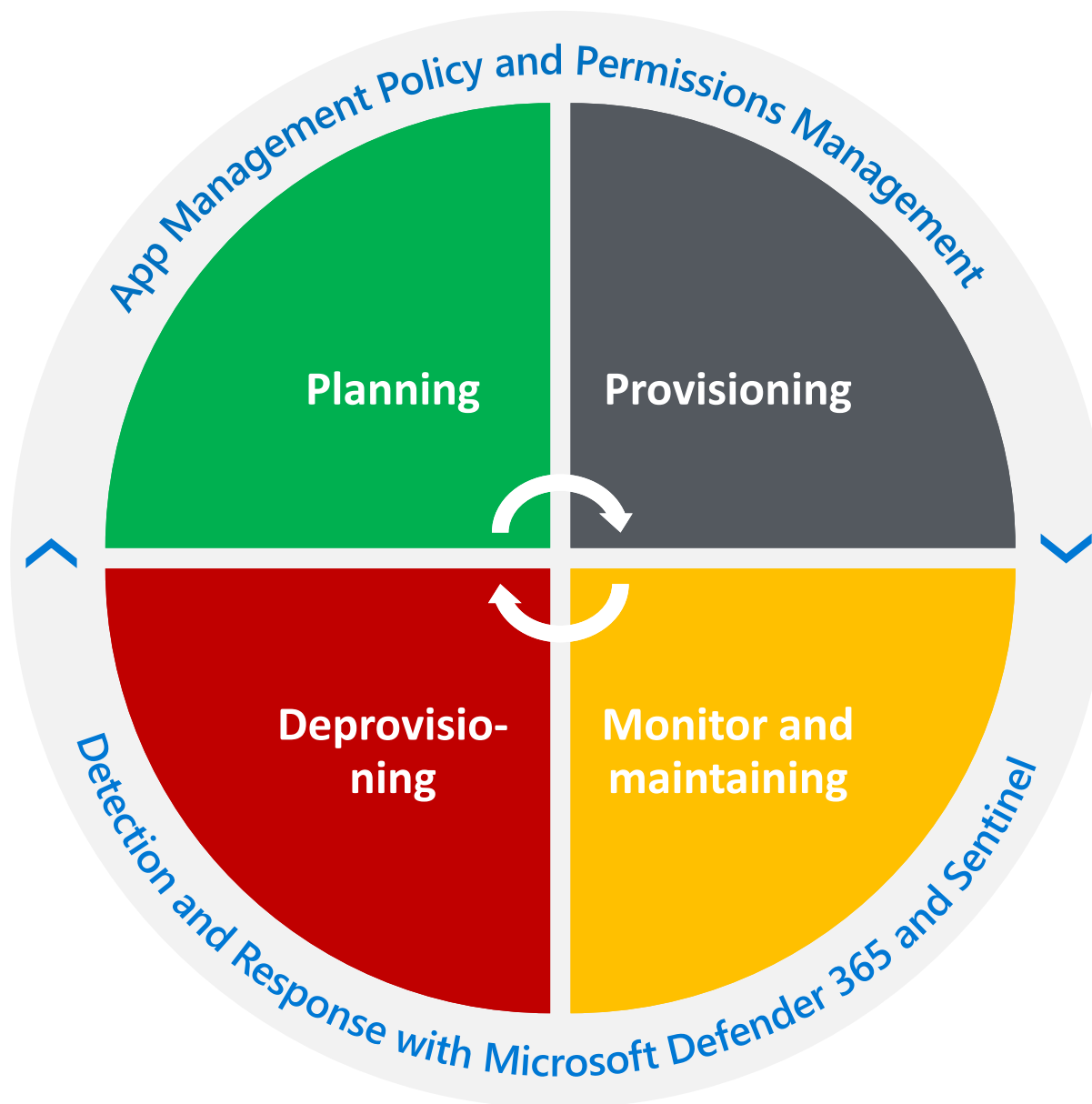
Integrated threat intelligence and security features





Workload Identity Governance & Security

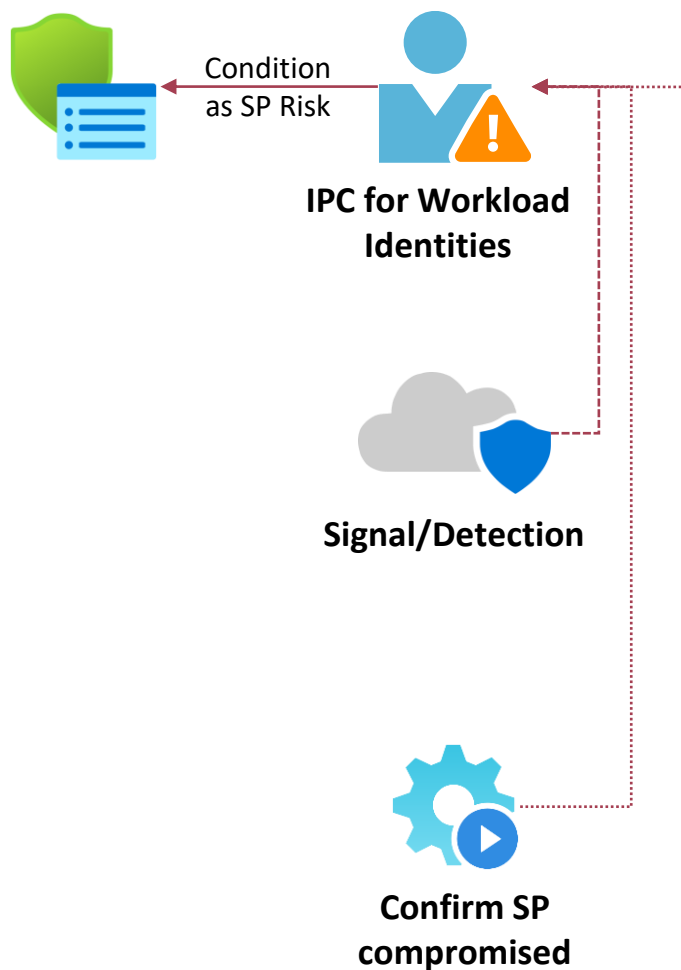
www.wpninjas.eu





Threat Intelligence and Integration in CA

www.wpninjas.eu



Azure AD Identity Protection (IPC)

- Azure AD Threat Intelligence *
- Suspicious Sign-ins *
- Leaked Credentials (from GitHub) *

Microsoft Defender for Cloud Apps (MDA)

- Unusual addition of credentials to an OAuth app*
- Unusual ISP for an OAuth app
- ...

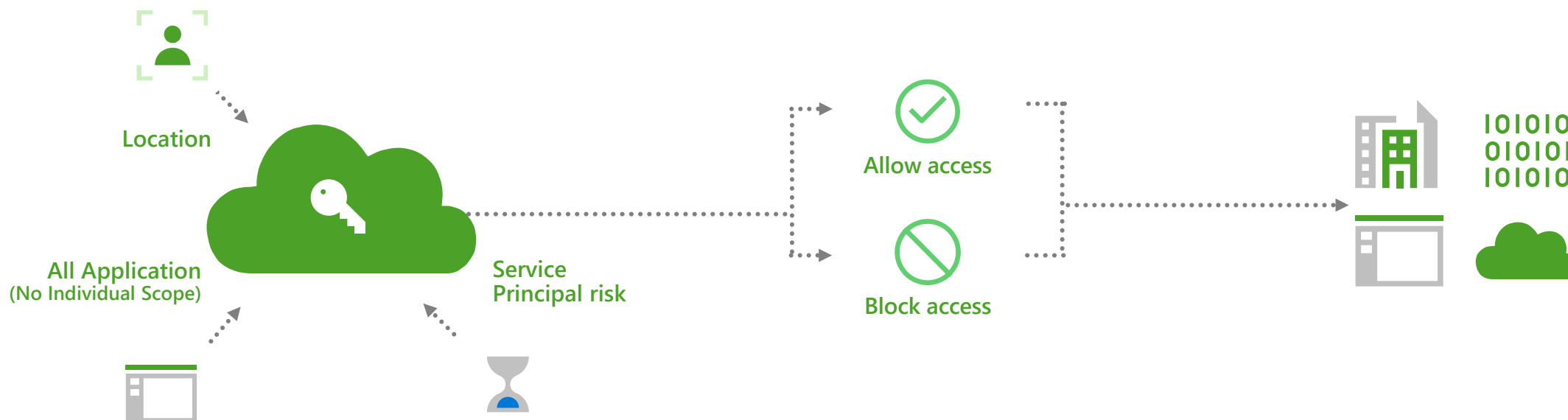
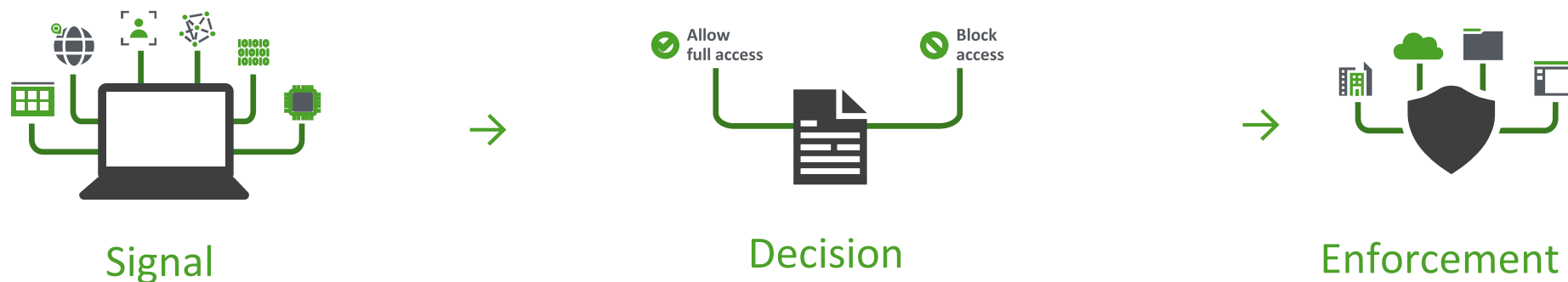
Microsoft Sentinel Analytics Rules (Custom Detections)

- Service Principal Authentication Attempt from New Country
- Federated Credential has been created for GitHub entity outside of organization
- ...

* Built-in detection source and signal in Identity Protection for Workload Identities



CA Policies for Workload Identities





Demo: Protection and secure access

www.wpninjas.eu




- Conditional Access and Identity Protection for Workload Identities
- Detection and Response with Microsoft Sentinel
- Access Review with MDA App Governance and Entra Permissions Management





Types of workload identities

www.wpninjas.eu

	 Service Principal (Key- or Certificate)	 Service Principal (Federated Credentials)	 Managed Identity (System/User Assign.)
Supported Use Case	No limitation	Limited to supported Workloads	Limited to supported Workloads (Azure-managed Resources)
Security Boundary	Single- or multi-tenant	Single- or multi-tenant	Single-tenant*
Relation to Workload	Unassigned	Assigned to Issuer/Entity	Assigned to Resource(s) System (1:1), User (N:1)
Workload Environment	Everywhere	Supported OIDC Federated IdP	Azure- and Azure Arc-enabled resources
Lifecycle management	Managed by Admin	Managed by Admin	System: Shared Lifecycle with Resource, User: Independent, Managed by Admin
Delegated Management	Application/Enterprise App Owner Azure AD Role (Directory, Object)		Enterprise App Owner, Azure AD Role Azure RBAC Role/Resource Owner
Security Dependencies	Secure storing of credentials, Protection of App Reg/SP object	Security of Federated Workload/IdP, Protection of App Reg/SP object	Security and restricted management of Azure Resource(s) and SP object
Restrict token acquisition	Conditional Access (Single Tenant only), CAE support		Not Available
Detection for Identity Attacks	Identity Protection, Sign-in logs	Identity Protection, Correlation between AAD and Trusted IdP AuthN/AuthZ logs	Limited Sign-in logs

Advanced auditing and monitoring

Context enriched detections in DevOps environments





Automated Classification

Classification of Action and Scope

```
[
  {
    "EAMTierLevelName": "ControlPlane",
    "EAMTierLevelTagValue": "0",
    "TierLevelDefinition": [
      {
        "Category": "Microsoft.Azure",
        "Service": "Management",
        "RoleAssignmentScopeName": [
          "/",
          "/providers/Microsoft.Management/managementGroups/36955ea9-c98e-
          /providers/Microsoft.Management/managementGroups/lab",
          "/providers/Microsoft.Management/managementGroups/lab-platform",
          "/providers/Microsoft.Management/managementGroups/lab-saezone"
        ],
        "RoleDefinitionActions": [
          "Microsoft.Authorization/*",
          "*"
        ]
      }
    ]
  }
]
```

Classified Privileged Access of Workload Identity

```
{
  "ObjectId": "4fbc88a-18b5-42cf-82ac-30ca6d4f6919",
  "ObjectType": "ServicePrincipal",
  "ObjectDisplayName": "azops-msi",
  "Classification": [
    {
      "AdminTierLevel": "0",
      "AdminTierLevelName": "ControlPlane",
      "Service": "Management"
    }
  ],
  "RoleAssignments": [
    {
      "RoleAssignmentId": "/providers/Microsoft.Authorization/roleAssignments/a308c801",
      "RoleAssignmentScope": "/",
      "RoleAssignmentType": "Direct",
      "PIMManagedRole": "False",
      "PIMAssignmentType": "Permanent",
      "RoleDefinitionName": "Owner",
      "RoleDefinitionId": "8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
      "ObjectId": "4fbc88a-18b5-42cf-82ac-30ca6d4f6919",
      "ObjectDisplayName": "azops-msi",
      "ObjectType": "ServicePrincipal",
      "Classification": [
        {
          "AdminTierLevel": "0",
          "AdminTierLevelName": "ControlPlane",
          "Service": "Management",
          "TaggedBy": "JSONwithAction"
        }
      ]
    }
  ]
}
```



Demo: Advanced auditing & monitoring

www.wpninjas.eu

- Classification of privileged Service Principals
- Advanced Analytics Rules with enriched and classified data
- Track and monitor workload identities “as Code” with “AzADServicePrincipalInsights”





Workload Identities

Summary | Take Aways



Consider secure implementation of authentication library, storing credentials and token caching
Avoid long-term credentials and verify security of trusted entities for Workload Identity Federation
Implement application management policy to govern credential issuing



Implement an application and lifecycle management
Consider Azure AD roles and ownership with permissions on application/service principal objects
Classify your application to detect privilege escalation paths and sensitivity of workload identity



Apply Conditional Access Policies for Service Principals and monitor risk detection
Monitor used/unused permissions and activity (IP address and type of access) after AuthN/AuthZ
Implement playbooks to automate response on suspicious sign-in or activity of service principals




Deploy rule templates for Service Principals in Microsoft Sentinel
Monitor trusted entities/IdP (for Federated Credentials) and resources with assigned MSI particularly
Review and integrate enriched data (from [AzGovViz](#) and [AzADServicePrincipalInsights](#) by Julian Hayward)



Questions?

www.wpninjas.eu

Meet me at
glueckkanja  **gab**
sponsor booth on 1st Floor

Contact me



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



Thomas@Naunheim.net



Thank You



Workplace Ninja Summit 2022