

Tips and Tricks from a baseVISION Security Engineer

Loris Ambrozzo / Sponsor Session baseVISION AG



*Workplace Ninja
Summit 2024*



Thank you Sponsors

www.wpninjas.eu

#WPNinjaS

Diamond Sponsor



Microsoft

Gold Sponsors



Platinum Sponsors



PATCH MY PC



RECAST SOFTWARE



Silver Sponsors



UMB creating time®



EPIC FUSION
BRING IT ALL TOGETHER





About Loris Ambrozzo

www.wpninjas.eu
#WPNinjaS

Focus

Senior Security Engineer @baseVISION

From

Switzerland

My Blog



github.com/lorisAmbrozzo



Certifications

BSc in Business Information Technology

Hobbies

Sport (Running, Hiking)

Contact

linkedin.com/in/lorisambrozzo/
x.com/LorisAmbrozzo





Agenda

www.wpninjas.eu
#WPNinjaS

Key takeaways:

- Tips and tricks in the area of security automation in Microsoft Azure

- Daily work @baseVISION
- Introduction Azure Automation
- Azure Automation Tips and Tricks
- Example Use Cases
- Closing

Daily work @baseVISION





Daily work @baseVISION

www.wpninjas.eu
#WPNinjaS

- Senior Security Engineer
- baseVISION focus on Secure and Modern Endpoint Management
- Focus on Identity, Endpoint Security and Cloud Security Topics



Microsoft Entra



Microsoft Defender XDR



Microsoft Sentinel

Introduction Azure Automation





Introduction Azure Automation

www.wpninjas.eu

#WPNinjaS

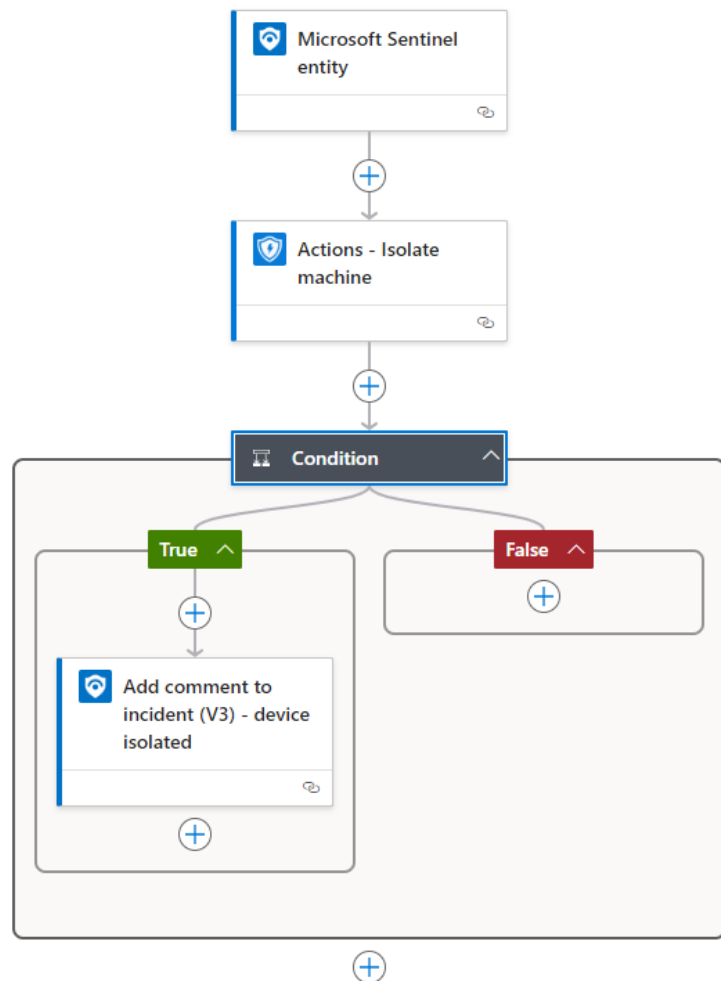
- Talking about Automation in Azure Environments there are main solution (Azure Resources)
 - Azure Logic Apps
 - Azure Automation Accounts
 - Azure Function Apps

Azure Automation Account	Azure Logic App
• “Normal Coding” • Build code by writing scripts (Powershell / Python) • Access the PowerShell Gallery and import custom modules • Execute code in the cloud and/or hybrid environment	• No-Code / Low-Code Platform • Build code with a designer • Many custom connectors available • First party (Azure, Microsoft 365) • Third Party (e.g. Zendesk, Virus Total) • Execute code only in the cloud



Introduction Azure Automation

www.wpninjas.eu
#WPNinjaS



Edit PowerShell Runbook

Entra-ExpiringAppRegistration

Save Publish Revert to published Test pane Edit in VS Code Feedback

RUNBOOKS ASSETS

```
48 )
49
50 begin {
51     # set runtime date
52     $now = Get-Date
53
54     try {
55         # Connect to Microsoft Graph
56         # $null = Connect-MgGraph -Scopes 'Application.Read.All' -NoWelcome -ErrorAct
57         Connect-MgGraph -Identity
58     }
59     catch {
60         Write-Warning "Could not connect to Microsoft Graph. Please make sure you ha
61         break
62     }
63
64     # create an empty list to store the result
65     $result = [System.Collections.Generic.List[PSCustomObject]]::new()
66
67
68     process {
69         $applications = Get-MgApplication -all
70         Write-Warning "found $($applications.Count) applications"
71         foreach ($application in $applications) {
72             # get application owner infomration
73             $Owner = Get-MgApplicationOwner -ApplicationId $application.Id
74             $Username = $Owner.AdditionalProperties.userPrincipalName -join ';'
75         }
76     }
77 }
```

Azure Automation Tips and Tricks





Azure Automation Tips and Tricks

www.wpninjas.eu
#WPNinjaS

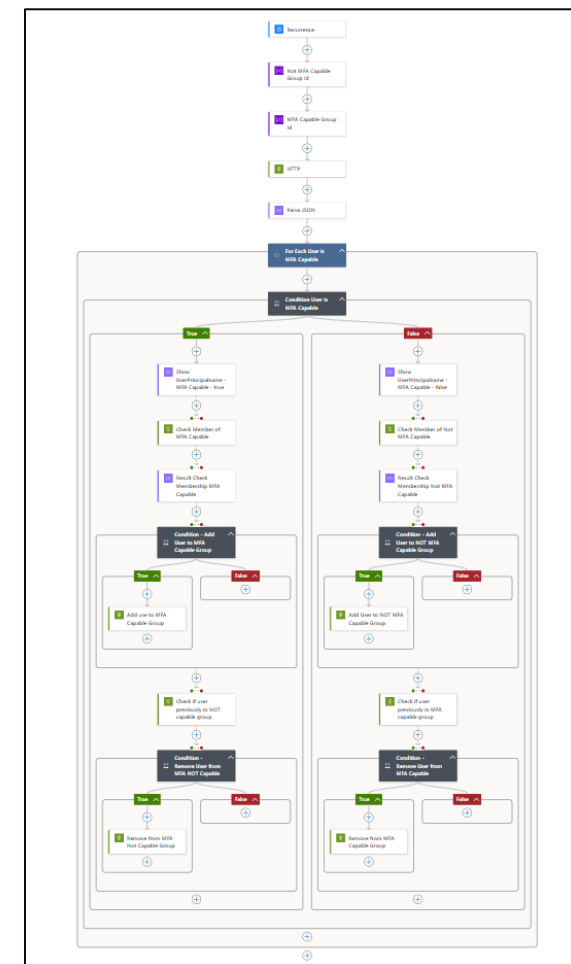
1. Build complex logic → Use Azure Automation accounts where possible to save runtime

Azure Logic App duration (6 Minutes)

Get started <u>Runs history</u> Trigger history Metrics				
Resubmit Add filter Specify the run identifier to open monitor view directly				
Identifier	Status	Start time (Local Time)	Duration	
08584848528860298579695963675CU16	✓ Succeeded	26/05/2024, 10:06:39 pm	5.44 Minutes	
08584849392862504157725966543CU82	✓ Succeeded	25/05/2024, 10:06:39 pm	5.3 Minutes	
08584850256866694410122535524CU82	✓ Succeeded	24/05/2024, 10:06:38 pm	4.66 Minutes	
08584851120858939410814378979CU206	✓ Succeeded	23/05/2024, 10:06:39 pm	5.56 Minutes	

Azure Automation Account duration (1 minutes script duration)

^ Essentials			
Id	: 30c7a4a1-69b4-42f3-8d83-22a3c18cdb27	Created	: 23/08/2024, 10:00:09 am
Status	: Completed	Last Update	: 23/08/2024, 10:03:46 am
Ran on	: Azure	Runbook	: UpdateEntraGroupMFACapability
Ran As	: User	Source snapshot	: View source snapshot
Input Output Errors Warnings All Logs Exception			





Azure Automation Tips and Tricks

www.wpninjas.eu
#WPNinjaS

2. Build complex logic → Use Azure Automation accounts where possible to save money

Azure Logic App (Consumption Plan)

- Costs per **action** (basically every step) (4000 actions free)
- CHF 0.000033 / per call



Total (CHF) ⓘ	Average
CHF 21.10 ↓ 2%	CHF 0.68 / day

Azure Automation Account

- Costs per job **run time** (500 minutes free per month)
- CHF 0.002/minute



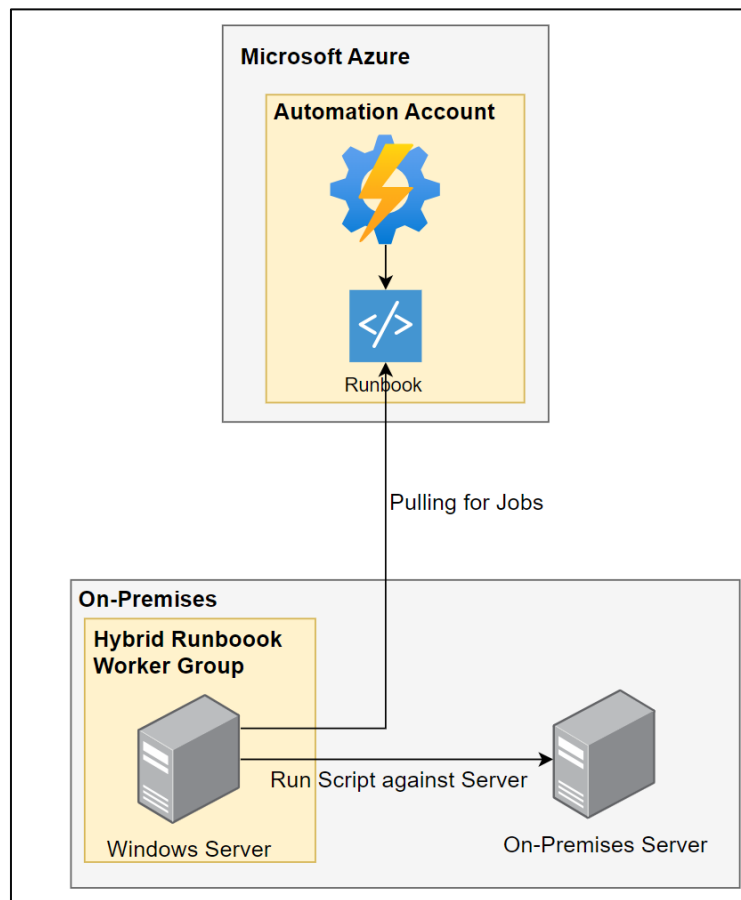
Total (CHF) ⓘ	Average
CHF 0.03	<CHF 0.01 / day



Azure Automation Tips and Tricks

www.wpninjas.eu
#WPNinjaS

3. Use Azure Automation accounts when you need to automate tasks on-premises from the cloud





Azure Automation Tips and Tricks

www.wpninjas.eu
#WPNinjaS

4. I use Logic Apps when I need to implement...

- Simple and Non-Complex Tasks
- Logic needs to be triggered e.g. based on a Microsoft Sentinel incident, Web-Hook
- Integration with First and 3rd party applications

Add a trigger

Sentinel

Runtime

Select a runtime

Action type

Triggers

☒ Group by Connector

 Microsoft Sentinel

See more

Microsoft Sentinel entity

Preview

Trigger

Microsoft Sentinel alert

Preview

Trigger

Microsoft Sentinel incident

Preview

Trigger

Example Use Cases





Example Use Cases

www.wpninjas.eu
#WPNinjaS

- **Azure Automation Account Use Cases**

- Add every Entra User based on a criteria to a specific group
- Send an E-Mail with all Expired App Registration Secrets / Certificates
- Update Entra Conditional Access Named Location
- Stale Device Clean Up in Entra ID

- **Azure Logic Apps Use Cases**

- Revoke Sign In Session from a User
- Disable / Enable User in Entra ID
- Isolate a specific device in Defender for Endpoint
- Create Custom Indicator in Defender for Endpoint
- Inform Security Team via Microsoft Teams / E-Mail



Thank You



*Workplace Ninja
Summit 2024*



We love Feedback

<https://wpninjas24.sched.com/>



Great Session!



Okay Session!



Not so okay Session!



Workplace Ninja
Summit 2024