



NETSPI

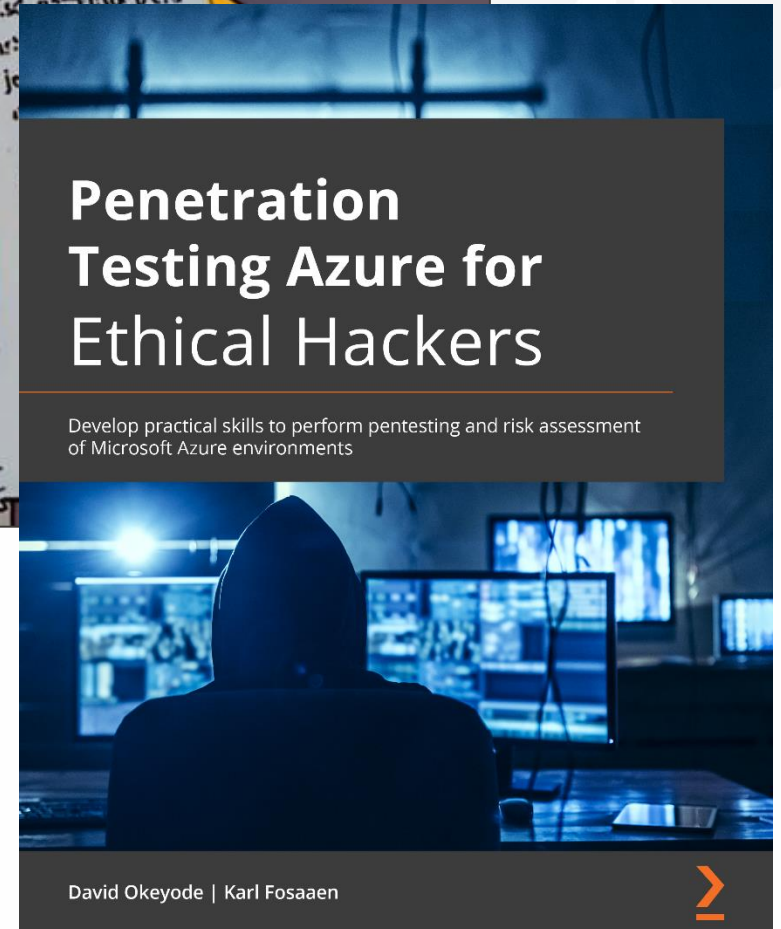
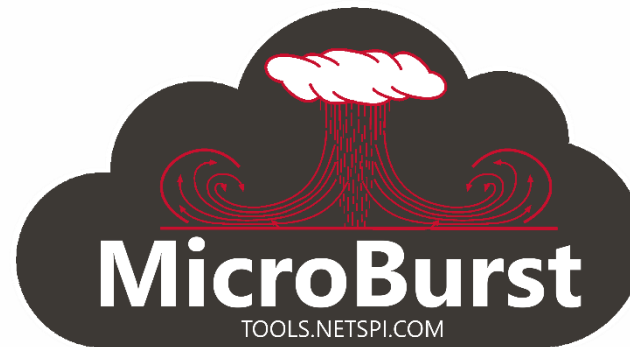
AUTOMATING INSECURITY IN AZURE

Karl Fosaaen

- ◆ Karl Fosaaen
 - ◆ Pen Tester
 - ◆ MicroBurst
 - ◆ Cloud Enthusiast
 - ◆ Private Pilot
 - ◆ Co-Author
 - ◆ Merch Goon



- ◆ <https://github.com/netspi>
- ◆ <https://blog.netspi.com/>
- ◆ Twitter - @kfosaaen



- ◆ Azure AD Tenant
 - ◆ The core of Identity (RBAC / IAM) in Azure
 - ◆ Security Principals
 - Users / Guest Users
 - AD Synced versus Azure Managed
 - Managed Identities
 - System Assigned
 - User Assigned
 - Service Principals
 - Application Accounts
 - ◆ Security Principals are assigned Roles



◆ Subscription Level




- ◆ Owner
- ◆ Contributor
- ◆ Reader

◆ Special/Custom Roles

- ◆ Multi-Level
- ◆ Service Specific
- ◆ Application Specific

◆ Application of Roles

- ◆ Management Group / Child Management Group / Subscription / Resource Group / Resource

		Role			
		Reader	Resource-specific or custom role	Contributor	Owner
Scope	 Subscription	Observers	Users managing resources		Admins
	 Resource group				
	 Resource	Automated processes			

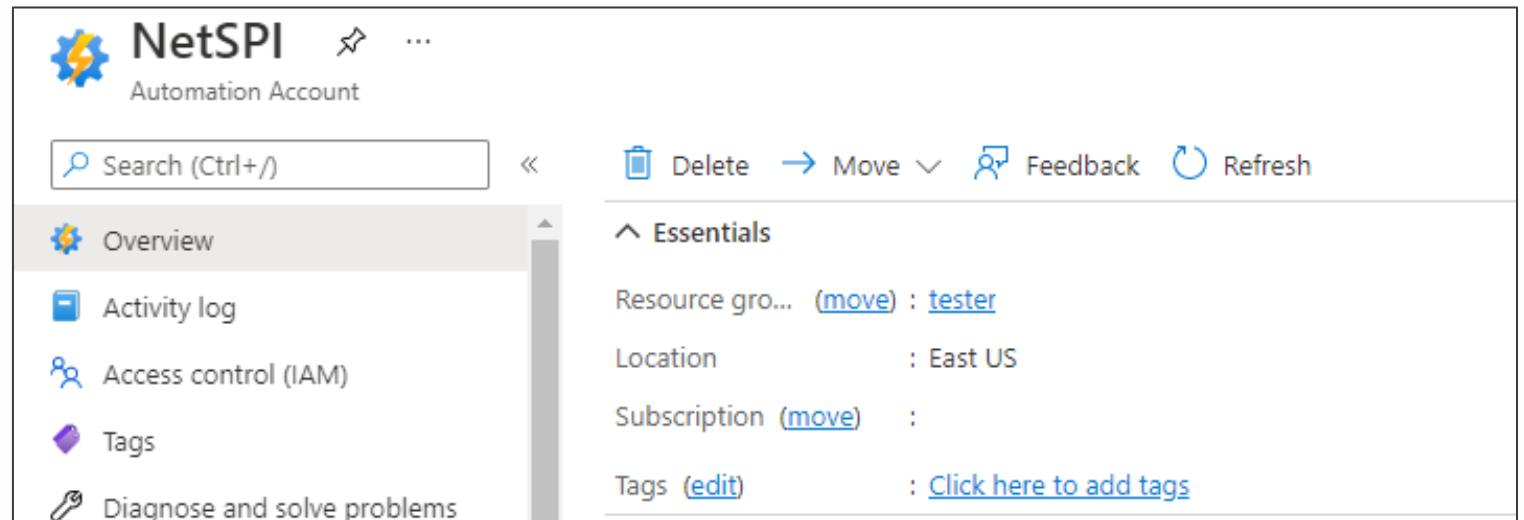
◆ What are Automation Accounts?

◆ Service for automating actions in Azure subscriptions

- Resource Management
- Applying Updates
- Rotating Credentials
- Ensuring Configurations

◆ A great target during a pen test

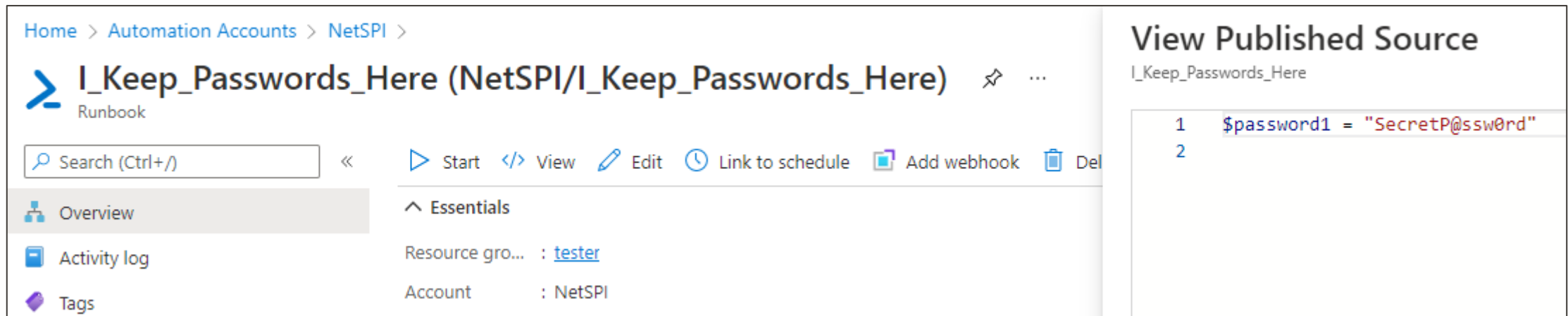
- Credential Access
- Privilege Escalation
- Lateral Movement
- Persistence



◆ Automation Account Components

◆ Runbooks

- PowerShell or Python Scripts
 - Can use custom modules or packages
- Code available to the Reader role
 - Hardcoded credentials in code
- Normally executes within a Microsoft managed container



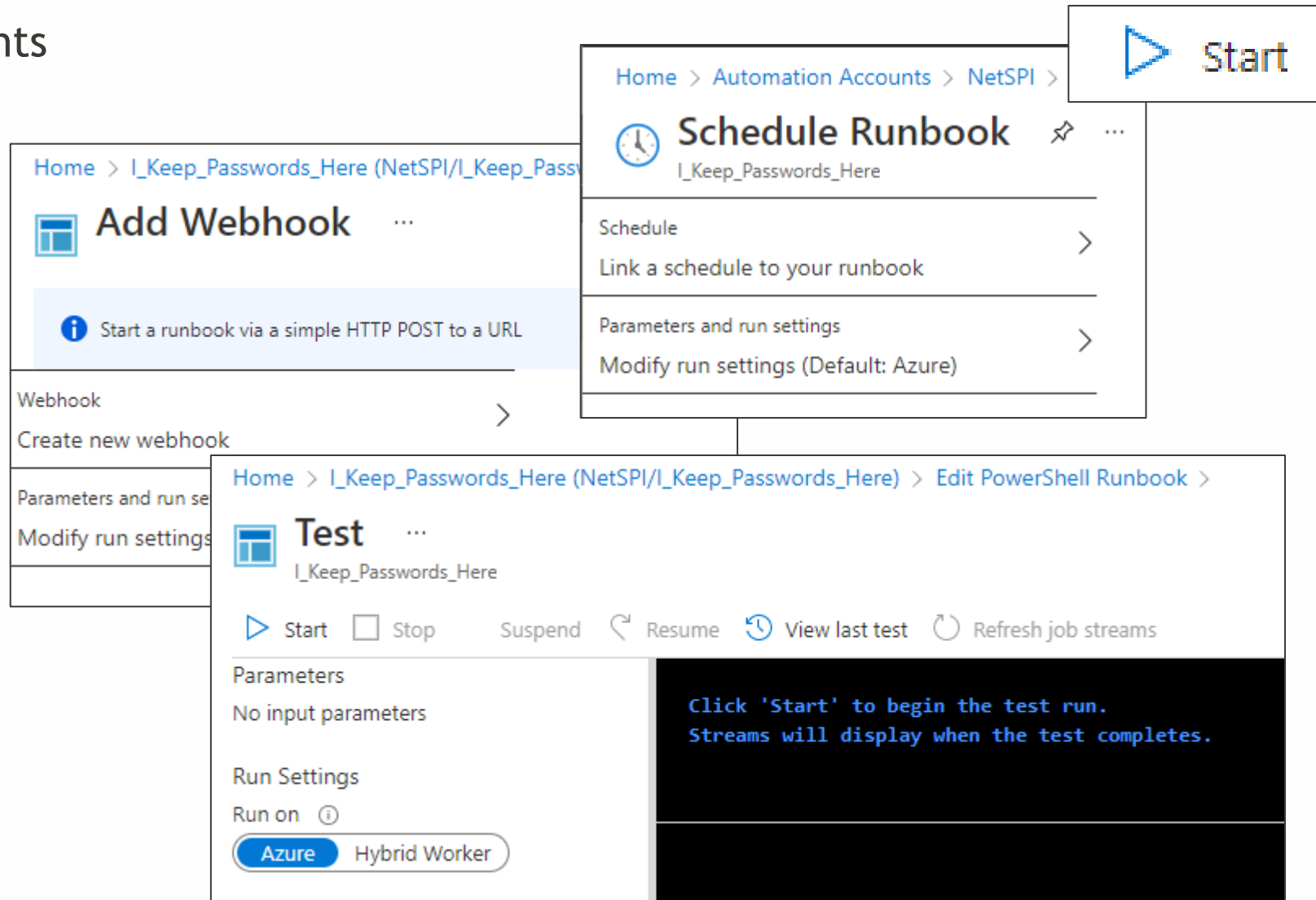
The screenshot displays the Azure Automation portal interface. The breadcrumb navigation shows 'Home > Automation Accounts > NetSPI >'. The main heading is 'I_Keep_Passwords_Here (NetSPI/I_Keep_Passwords_Here) Runbook'. Below the heading is a search bar and a toolbar with icons for Start, View, Edit, Link to schedule, Add webhook, and Delete. A left sidebar contains 'Overview', 'Activity log', and 'Tags'. The 'Essentials' section shows 'Resource group : tester' and 'Account : NetSPI'. The 'View Published Source' panel on the right shows the following code:

```
1 $password1 = "SecretP@ssw0rd"
2
```

◆ Automation Account Components

◆ Runbook Execution

- Run as a Job
 - Very visible in logs
- Schedule to Run
 - Persistence option
- Trigger with Webhook
 - Persistence option
 - Can accept parameters
 - Command Injection Potential
- Run in Test Pane
 - Less noise in the logs

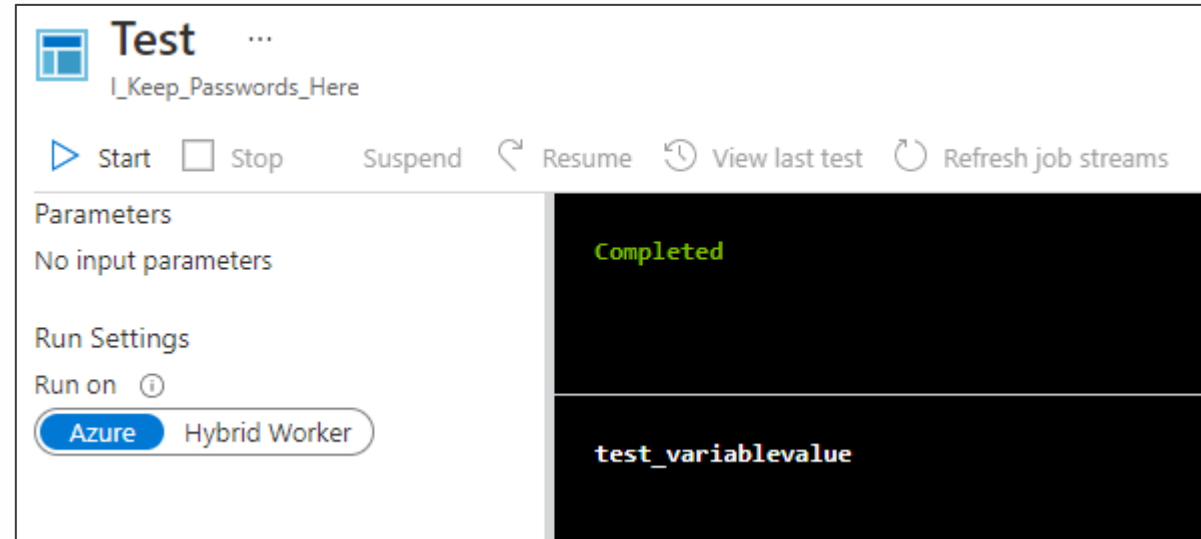


The screenshot displays the Azure Automation Accounts interface. At the top right, there is a 'Start' button. Below it, the 'Schedule Runbook' panel is visible, showing the breadcrumb 'Home > Automation Accounts > NetSPI >' and the runbook name 'I_Keep_Passwords_Here'. The panel includes a 'Schedule' section with the instruction 'Link a schedule to your runbook' and a 'Parameters and run settings' section with the instruction 'Modify run settings (Default: Azure)'. Below this, the 'Test' panel is shown, with the breadcrumb 'Home > I_Keep_Passwords_Here (NetSPI/I_Keep_Passwords_Here) > Edit PowerShell Runbook >'. The 'Test' panel features a 'Test' button and a 'Start' button. Below the buttons, there are sections for 'Parameters' (No input parameters) and 'Run Settings' (Run on: Azure, Hybrid Worker). A black box on the right side of the 'Test' panel contains the text: 'Click 'Start' to begin the test run. Streams will display when the test completes.'

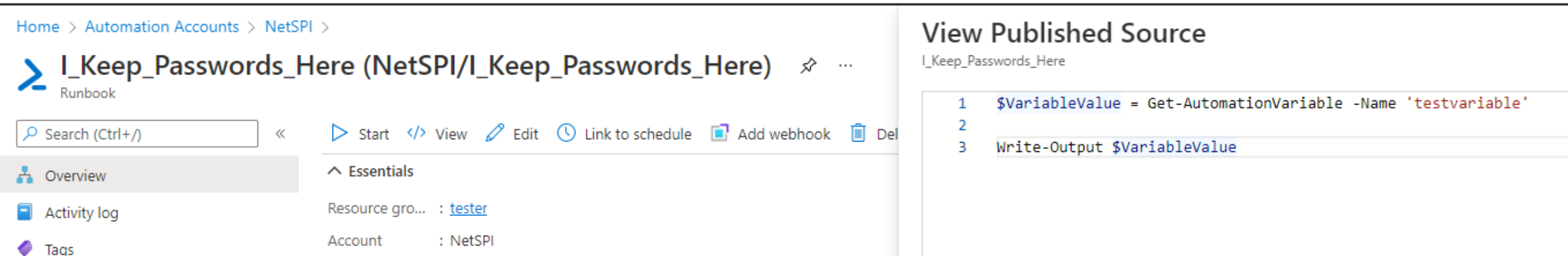
◆ Automation Account Components

◆ Variables

- Stores commonly used variable values
- Often contains credentials or keys
- Easy to cast to outputs for extraction
- Available to the Reader role
 - *Unless they're encrypted



The screenshot shows the 'Test' interface for a runbook named 'I_Keep_Passwords_Here'. The test has been completed successfully, as indicated by the green 'Completed' status. The output of the test is 'test_variablevalue'. The interface includes controls for Start, Stop, Suspend, Resume, View last test, and Refresh job streams. The Parameters section shows 'No input parameters'. The Run Settings section shows the test is running on 'Azure Hybrid Worker'.



The screenshot shows the 'View Published Source' interface for the runbook 'I_Keep_Passwords_Here'. The source code is displayed as follows:

```

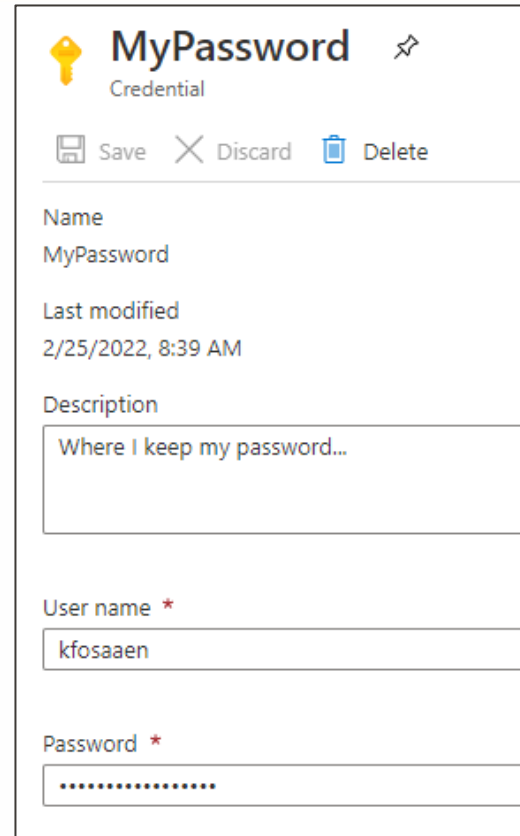
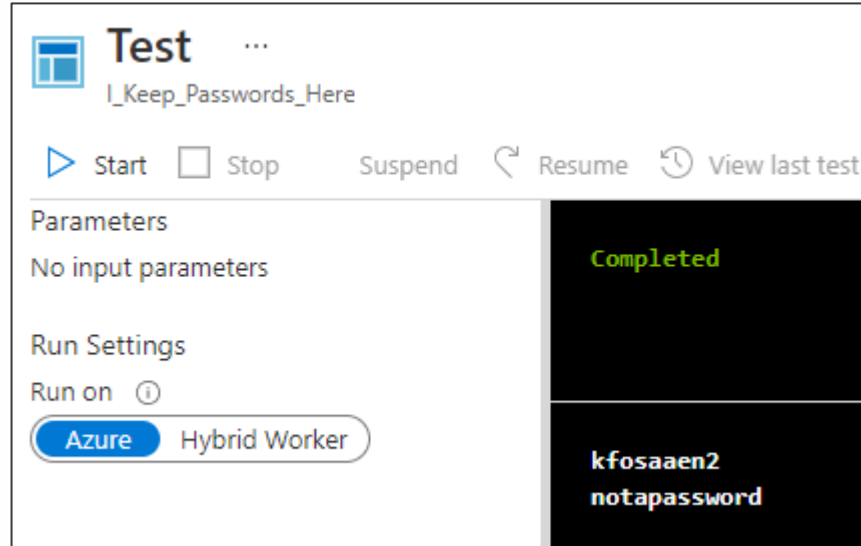
1 $VariableValue = Get-AutomationVariable -Name 'testvariable'
2
3 Write-Output $VariableValue
    
```

The interface also shows the breadcrumb 'Home > Automation Accounts > NetSPI >' and the runbook name 'I_Keep_Passwords_Here (NetSPI/I_Keep_Passwords_Here)'. The left sidebar includes 'Overview', 'Activity log', and 'Tags'. The top navigation bar includes 'Start', 'View', 'Edit', 'Link to schedule', 'Add webhook', and 'Del'. The 'Essentials' section shows 'Resource gro... : tester' and 'Account : NetSPI'.

◆ Automation Account Components

◆ Platform Credential Options

- “Credentials”
 - Username and Password combination
 - AAD credentials
 - Domain or Local credentials for VMs
 - Easy to cast to outputs for extraction
 - Key Vaults are the safer option



Home > Automation Accounts > NetSPI >

I_Keep_Passwords_Here (NetSPI/I_Keep_Passwords_Here) ...

Runbook

Search (Ctrl+/) << Start </> View Edit Link to schedule Add webhook Del

Overview

Activity log

Essentials

Resource gro... : [tester](#)

View Published Source

I_Keep_Passwords_Here

```
1 $credValue = Get-AutomationPSCredential -Name 'extractMe'  
2 Write-Output $credValue.Username  
3 Write-Output $credValue.GetNetworkCredential().Password
```

◆ Automation Account Components

◆ Platform Credential Options



- “Run as” Accounts / “Connections”
 - Older Method
 - Relies on App Registration
 - Uses Certificates for Authentication
 - Granted “Contributor” role on the subscription by default



View Published Source

I_Keep_Passwords_Here

```
1 $RunAsCert = Get-AutomationCertificate -Name 'AzureRunAsCertificate'  
2 $certPath = Join-Path $env:temp AzureRunAsCertificate.pfx  
3 $Cert = $RunAsCert.Export('pfx','Password4theCert')  
4 Set-Content -Value $Cert -Path $certPath -Force -Encoding Byte  
5 $base64string = [Convert]::ToBase64String([IO.File]::ReadAllBytes($certPath))  
6 Write-Output $base64string
```


Home > Automation Accounts > NetSPI >

 **Azure Run As Account** 
Properties

 Renew certificate  Delete

Azure Active Directory Application ⓘ

Display Name

NetSPI_sQKdofkT0iNsNEZUUyv+nAsNo... 

Certificate ⓘ

Name

AzureRunAsCertificate





Expiration

10/7/2022, 5:00 PM

Thumbprint

 **Test** ...

I_Keep_Passwords_Here

 Start Stop Suspend  Resume  View last test  Refresh job streams

Parameters

No input parameters

Run Settings

Run on ⓘ

Azure Hybrid Worker

Activity-level tracing

This configuration is available only for graphical runbooks.

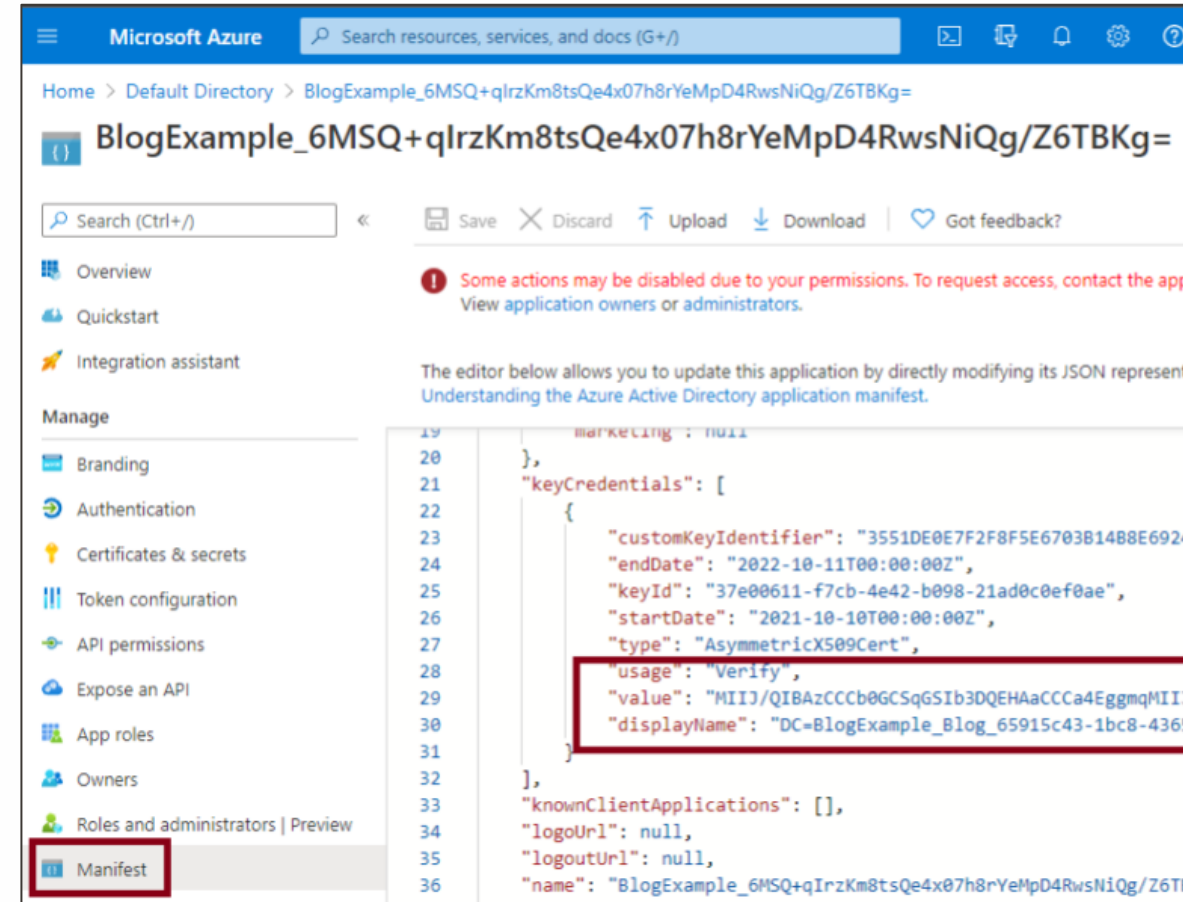
Completed

MIIKMwIBAzCCe8GCSqGSIb3DQEHAaCCeAEggncMIIJ2DCCB
t0i+f9s2TsJIowrt1N7Tak+ZfPeoi6C+rcgtjp+hCS4uDvb8a
hR3Aw7RSANfvOJRS951Mhn+yJPCukwiTlHgrxs0GvWRNiR1oF
jVx9x8+7YAcBTtDGJV6DDFi7hjw0Lv5/X6Csvq1009NNHRsXn
ru0YFTbBYTN2ZAB2CyT2DwuCeQkOP9xUiaVj6enhIa+ocEnN
b1T0GyELOeSPdKsxnLazpkrGbhmqL7Cy8uMukMo2wUzkbks2
ftNMZmqnoGdzh8RQ3Le589UYAmNtt0Egihct0EaIhVax+A4v

◆ Automation Account Components

◆ Platform Credential Options

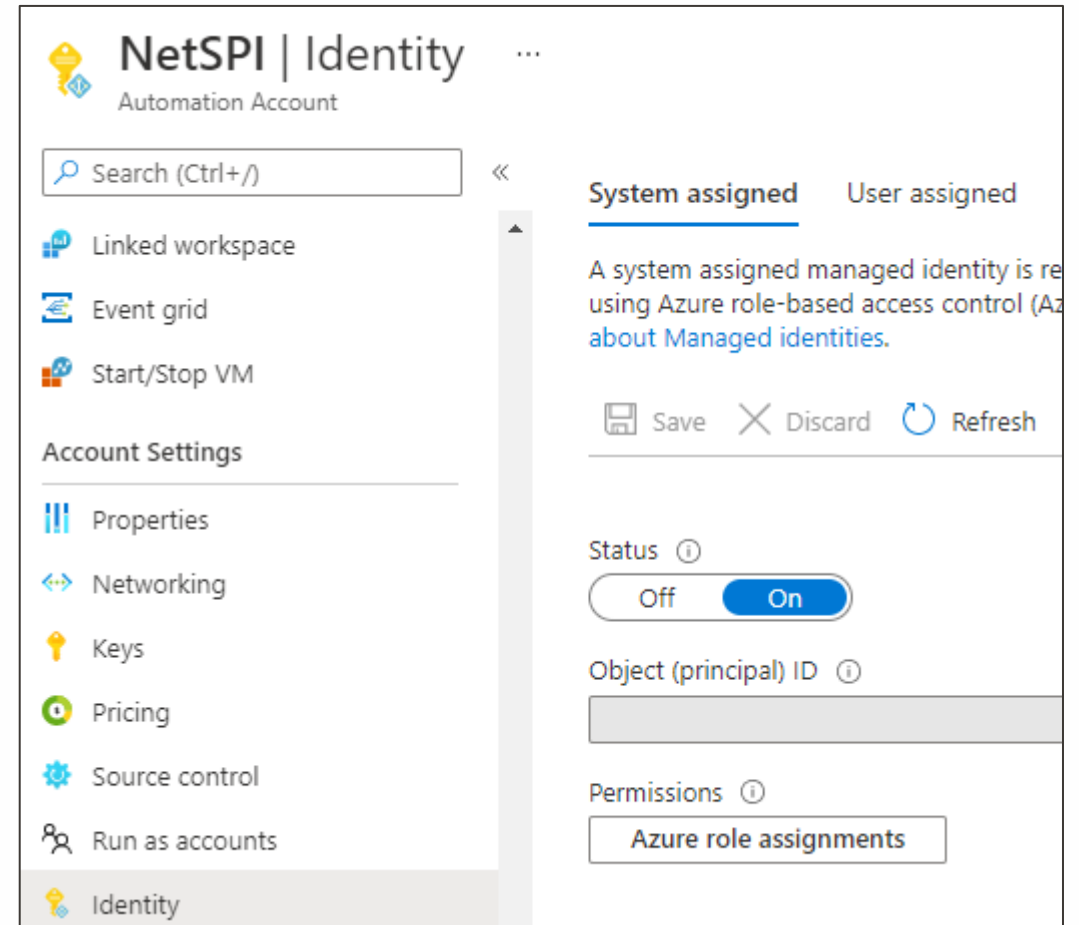
- “Run as” Account Credential Exposure
 - “CredManifest” (CVE-2021-42306) Vulnerability
 - Exposed PFX files in the App Registration Manifest files
 - Affected Services:
 - Automation Accounts
 - Azure Migrate
 - Azure Site Recovery
- Applies to AAD users with ability to read App Registrations
 - Most cases, all users could read this data
 - Domain user -> Subscription Contributor
 - At a minimum...



◆ Automation Account Components

◆ Platform Credential Options

- Managed Identities
 - System assigned vs. User assigned
 - Generates tokens for temporary access
 - Uses localhost Managed Service Identity (MSI) endpoint
 - Safer alternative to “Run as” accounts
- Extracting Tokens
 - Make a request to the MSI endpoint
 - Write to Job Output
 - Exfiltrate via POST request



The screenshot shows the 'NetSPI | Identity' page for an 'Automation Account'. The left sidebar contains a navigation menu with the following items: 'Linked workspace', 'Event grid', 'Start/Stop VM', 'Account Settings', 'Properties', 'Networking', 'Keys', 'Pricing', 'Source control', 'Run as accounts', and 'Identity' (which is currently selected). The main content area is titled 'System assigned' and 'User assigned'. Below this, there is a description: 'A system assigned managed identity is re using Azure role-based access control (Az about Managed identities)'. There are three buttons: 'Save', 'Discard', and 'Refresh'. The 'Status' section shows a toggle switch set to 'On'. Below that, the 'Object (principal) ID' field is empty. The 'Permissions' section shows a button labeled 'Azure role assignments'.

◆ Automation Account Components

◆ Platform Credential Options

- Managed Identities
 - “AutoWarp” Vulnerability
 - Cross-tenant isolation issue
 - MSI endpoint listening on high number port (40,000+)
 - Shared container space / lack of container isolation
 - Generate tokens for managed identities in other tenants

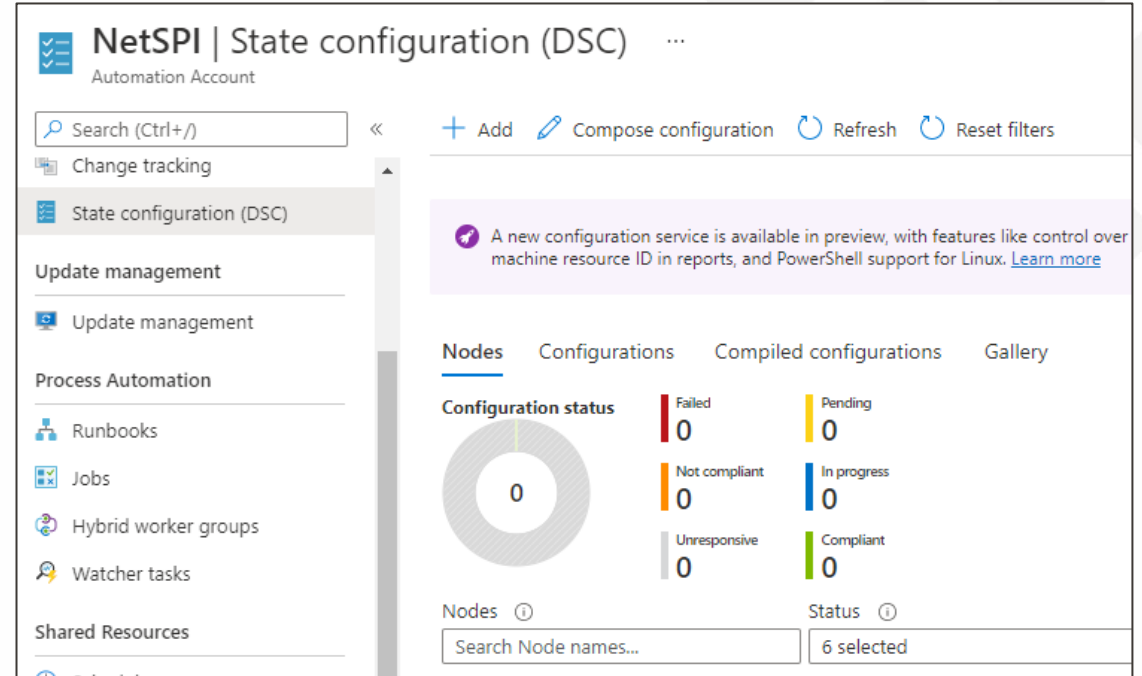
◆ Blog:

<https://orca.security/resources/blog/autowarp-microsoft-azure-automation-service-vulnerability/>

◆ Automation Account Components

◆ Desired State Configurations

- Used for managing system configurations
 - Domain joining
 - Running processes
 - Applying updates
- Can be used for persistence / command execution
 - Ensure X process is running
 - If not, download exe and run it
- Pivot to on-prem (ARC) systems
- Can be a sneaky way to execute a Runbook
 - Configuration compilation happens in your Automation Account container



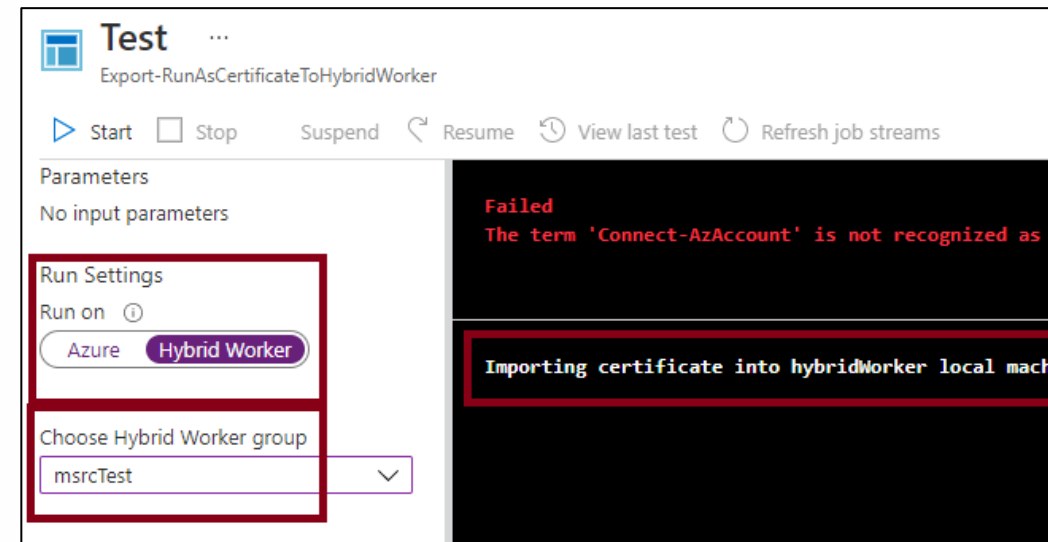
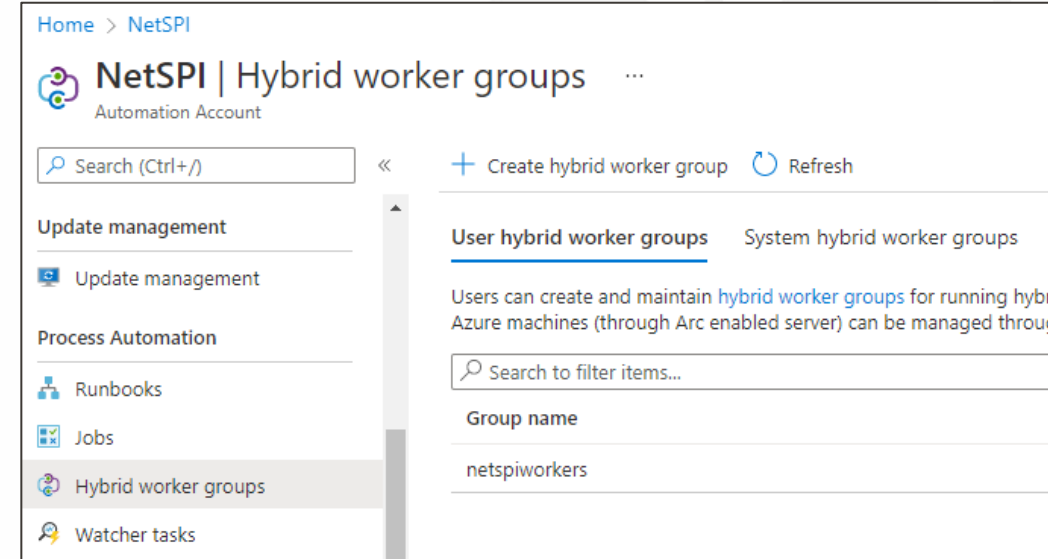
The screenshot displays the NetSPI State configuration (DSC) interface. The top navigation bar includes a search box, a list of actions (Add, Compose configuration, Refresh, Reset filters), and a sidebar menu with options like Change tracking, State configuration (DSC), Update management, Process Automation, and Shared Resources. The main content area features a notification about a new configuration service and a 'Configuration status' section with a donut chart showing 0 nodes in various states: Failed, Pending, Not compliant, In progress, Unresponsive, and Compliant. Below this, there are search boxes for 'Nodes' and 'Status', with '6 selected' nodes indicated.

<https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-persistence-with-desired-state-configurations/>

◆ Automation Account Components

◆ Hybrid Workers

- External systems that can be used to run Automation Runbooks
 - Greater CPU/RAM/Disk capacity
- Requires “Run as” certificate to be installed for Authentication
- Any user with local admin can extract the certificate
- Multiple Azure roles can execute commands (as system) on VMs
 - Virtual Machine Contributor
 - Virtual Machine Administrator Login
 - Virtual Machine User Login
 - Azure Connected Machine Onboarding
 - Azure Connected Machine Resource Administrator
 - Log Analytics Contributor



◆ Automation Account Components

◆ Hybrid Workers

- Undocumented APIs are used by the agent for tasking
 - Could be abused to access stored credentials and “Run as” certificates
- Escalation from Reader to Contributor
 - Ability to read Automation Account enrollment key
 - Self enroll your own Hybrid Worker
 - Get token and request “Run as” certificate
 - Authenticate as the “Run as” account
- Remediated by Microsoft
- Subscription Reader can no longer read AA keys

```
1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=utf-8
3 Server: Microsoft-IIS/10.0
4 x-ms-request-id: f5c068f8-5884-4841-9ef7-a0213c7ba96e
5 X-Powered-By: ASP.NET
6 Date: Fri, 05 Nov 2021 21:13:33 GMT
7 Content-Length: 3599
8
9
10 {
11   "value": [
12     {
13       "name": "AzureRunAsCertificate",
14       "value": "MIIJ9wIBAzCCBcGCSqGSIb3DQEHAAcCCAgEggmkMIIJoDCCFi
15       5BgkrBgEAYI3EQExbB5qAE0AaQBJAHIAbwBzAG8AZgBOACAARQBuaGgAYQ
16       "isExportable": true,
17       "description": null,
18       "thumbprint": "BDD023EC342FE04CC1C0613499F9FF63111631BB",
19       "expiryTime": "2022-10-08T00:00:00+00:00"
20     }
21   ]
22 }
```

```
GET /automationAccounts/1c65a02c-1d72-45c6-967c-0ab3dec1fc97/certificates?api-version=1.0&vmResourceId=
=
/subscriptions/d[redacted]b2/resourceGroups/tester/providers/Microsoft.Compute/
virtualMachines/HybridBlogTesting HTTP/1.1
Host: 1c65a02c-1d72-45c6-967c-0ab3dec1fc97.jrds.eus.azure-automation.net
Accept: application/json
Content-Type: application/json
Authorization: Bearer eyJ0eX
BjQ0g[redacted]
vc3Rz[redacted]
iI6MT[redacted]
kIjoi[redacted]
2luZG[redacted]
iYjRm[redacted]
UEuIiw[redacted]
tNT
Oi8
SiZ
cG1
Mud
MC1
1BQ
LWE
```


◆ Remediated Privilege Escalation Path

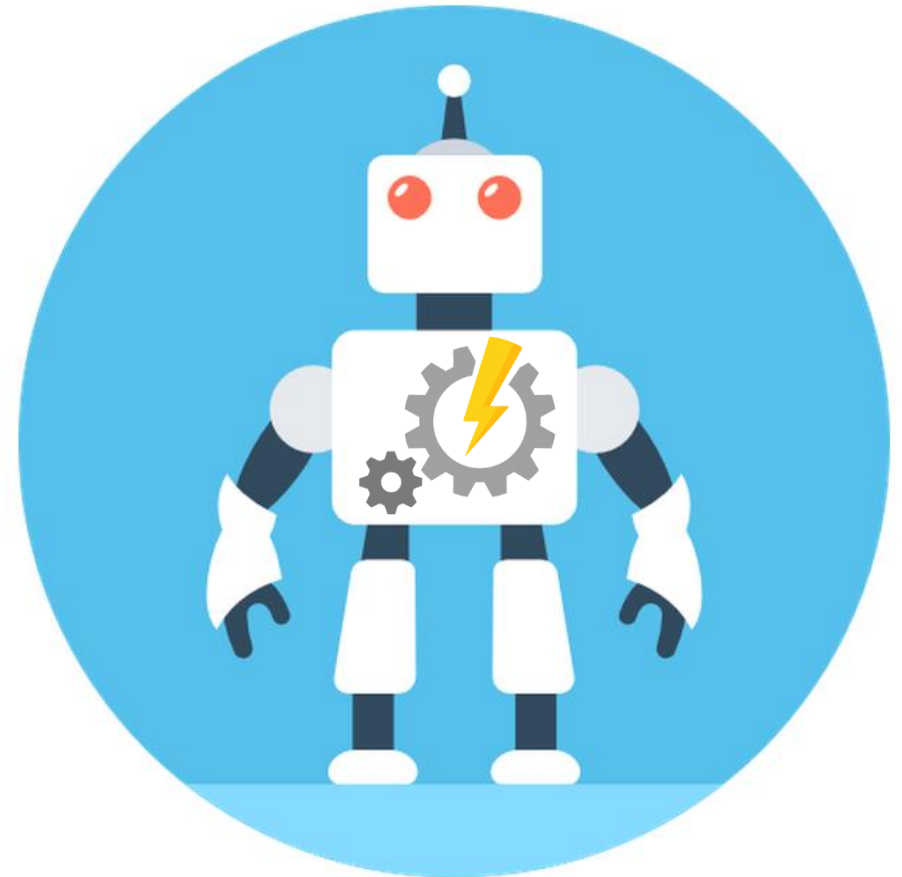
◆ Log Analytics Contributor Role

- Initially allowed * permissions on Automation Accounts
- Use Log Analytics Contributor role to export the “Run as” certificate
- Use the exported certificate to login as a Contributor (slightly more privileges)

```
1  {
2      "id": "/providers/Microsoft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-94a3-d43ce8d16293",
3      "properties": {
4          "roleName": "Log Analytics Contributor",
5          "description": "Log Analytics Contributor can read all monitoring data and edit monitoring settings.",
6          "assignableScopes": [
7              "/"
8          ],
9          "permissions": [
10             {
11                 "actions": [
12                     "**/read",
13                     "Microsoft.Automation/automationAccounts/*",
14                     "Microsoft.ClassicCompute/virtualMachines/extensions/*",
15                     "Microsoft.ClassicStorage/storageAccounts/listKeys/action",
16                     "Microsoft.Compute/virtualMachines/extensions/*",
```

◆ Automation Accounts Conclusions

- ◆ Can be useful
 - Automates many of the tasks in an Azure environment
 - Security improvements are being made
- ◆ Can be dangerous
 - Often misconfigured
 - Can expose credentials
 - Can allow for privilege escalation
- ◆ Potential target during an Azure Pentest?
 - Absolutely



Questions?

- ◆ MicroBurst GitHub - <https://github.com/NetSPI/MicroBurst>
- ◆ NetSPI Blog - <https://www.netspi.com/blog/technical/>
- ◆ Automation Account Blogs:
 - ◆ <https://www.netspi.com/blog/technical/cloud-penetration-testing/encrypting-password-data-in-get-azpasswords/>
 - ◆ <https://www.netspi.com/blog/technical/cloud-penetration-testing/maintaining-azure-persistence-via-automation-accounts/>
 - ◆ <https://www.netspi.com/blog/technical/cloud-penetration-testing/exporting-azure-runas-certificates/>
 - ◆ <https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-automation-accounts-key-stores/>
 - ◆ <https://www.netspi.com/blog/technical/cloud-penetration-testing/escalating-azure-privileges-with-the-log-analystics-contributor-role/>
 - ◆ <https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-cloud-vulnerability-credmanifest/>
- ◆ Twitter - @kfosaaen





MINNEAPOLIS | NEW YORK | PORTLAND | DENVER | DALLAS

<https://www.netspi.com>

 <https://www.facebook.com/netspi>
 @NetSPI

<https://www.slideshare.net/NetSPI>