A man with a beard and long hair tied back, wearing a blue button-down shirt, is pointing at a tablet held by a woman with dark curly hair wearing a yellow top. They are in an office setting. The background is blurred with some geometric shapes overlaid.

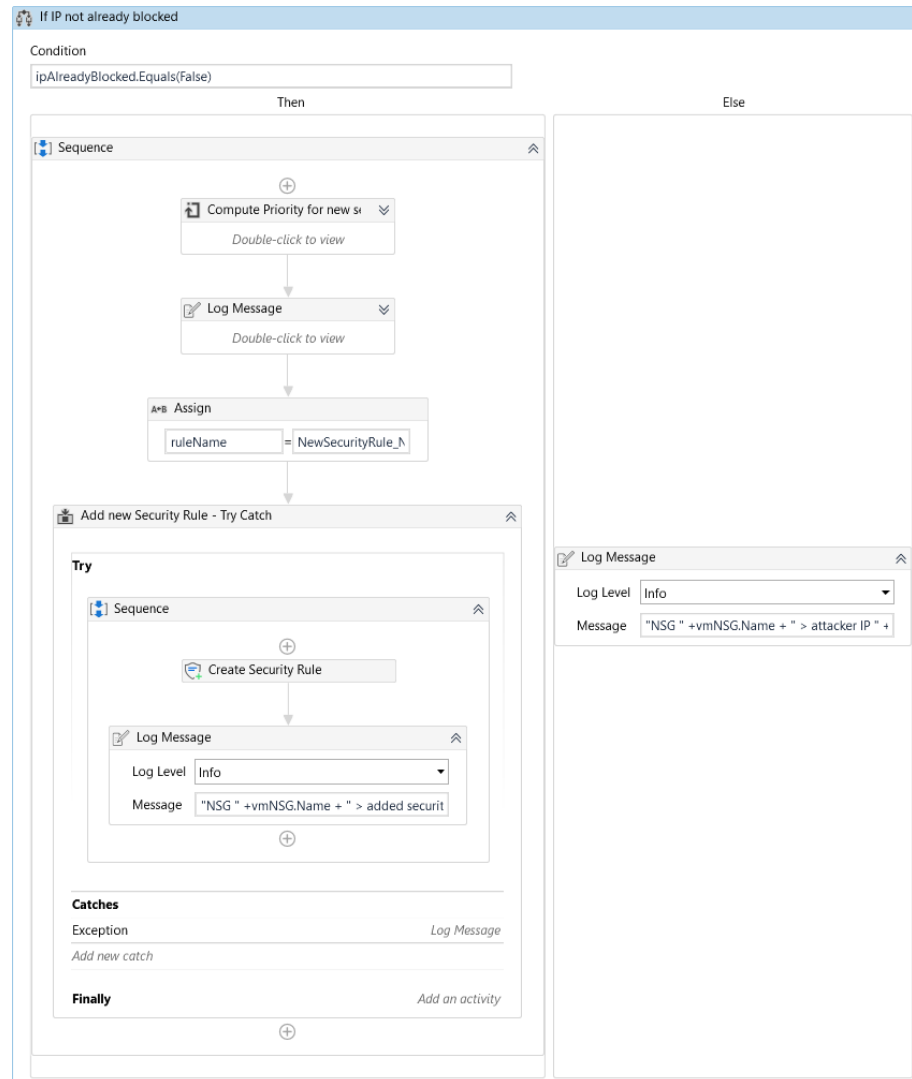
Security Orchestration

powered by IT Automation

Andrei Oros



Security Orchestration with RPA Workflows



Transparent

easy to understand & inspect
workflow business logic

Flexible

easy to update scaling logic with
out-of-the-box drag & drop
UiPath IT Automation activities

Vendor agnostic

Azure, AWS, VMware, Citrix



Security Orchestration RPA Workflows built with out-of-the-box **IT Automation Activities**



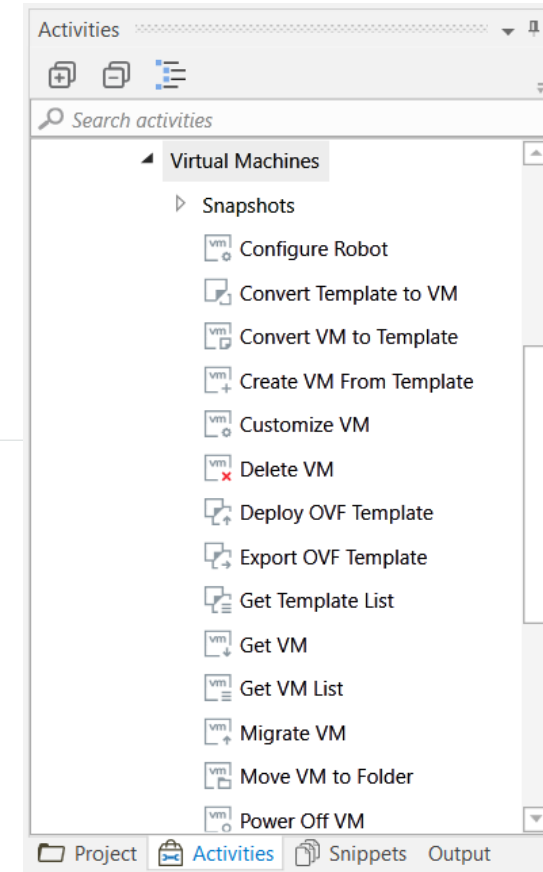
Implementation

- built on top of the official APIs / SDKs provided by the vendors *Microsoft, VMware, Citrix, [..]*
- the activities run in the background, not via the UI

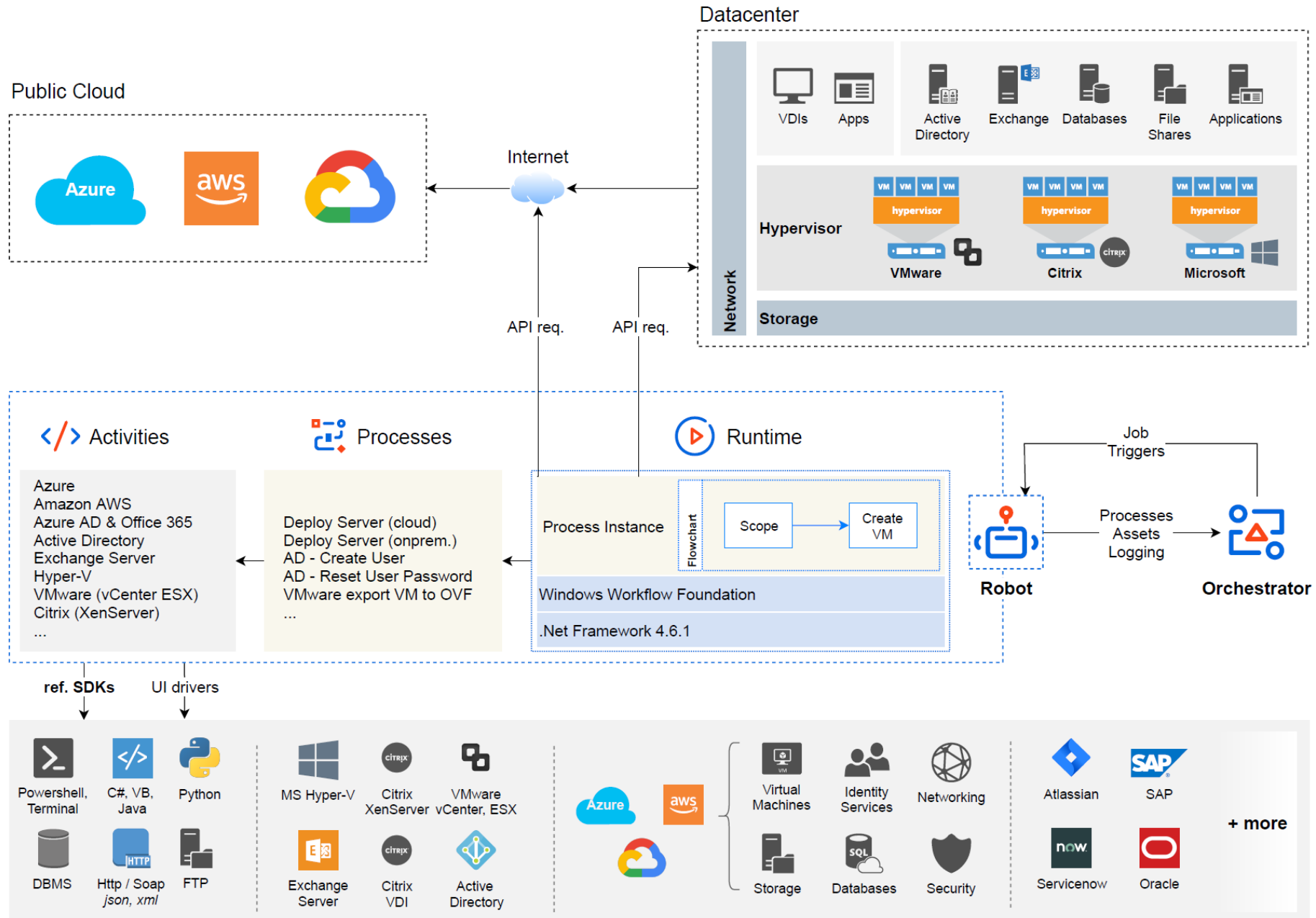


Security. Compliance

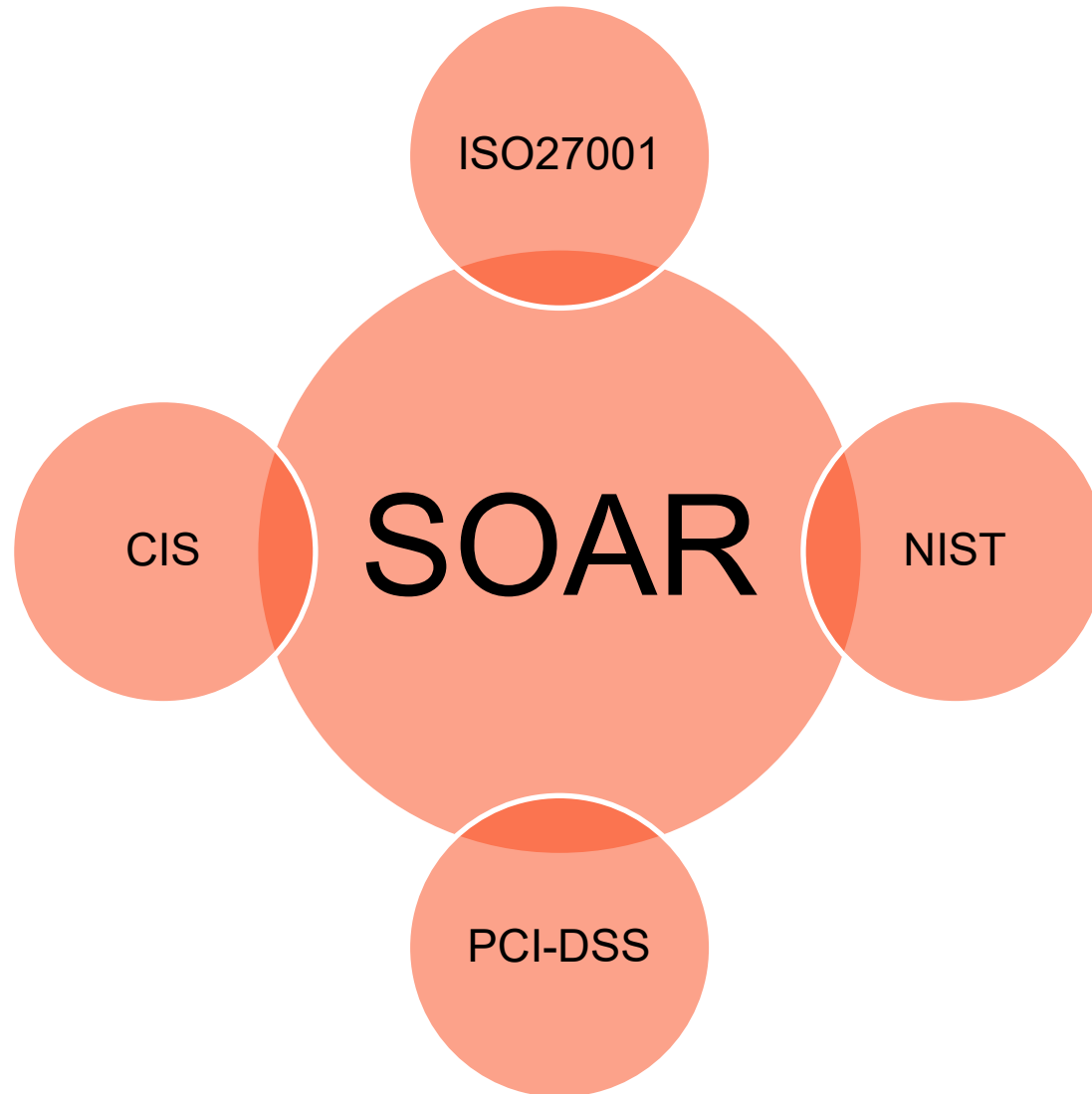
- developed and owned by **UiPath** (*published on the official feed, official maintenance + long term support*)
- scanned and certified with VERACODE and FOSSA



IT integrations landscape



SOAR Certification & Audit



ISO27001:

- 10.6 Network Security Management
- 10.10 Monitoring



NIST:

- Detect:
 - Anomalies and Events (DE.AE2/DE.AE3)
 - Detection Process (DE.DP4/DE.DP5)
- Respond:
 - Response Planning (RS.RP1)
 - Analysis (RS.AN1)
 - Mitigation (RS.MI1/RS.MI2)



PCI-DSS:

- Regular monitor and test networks (10.6)



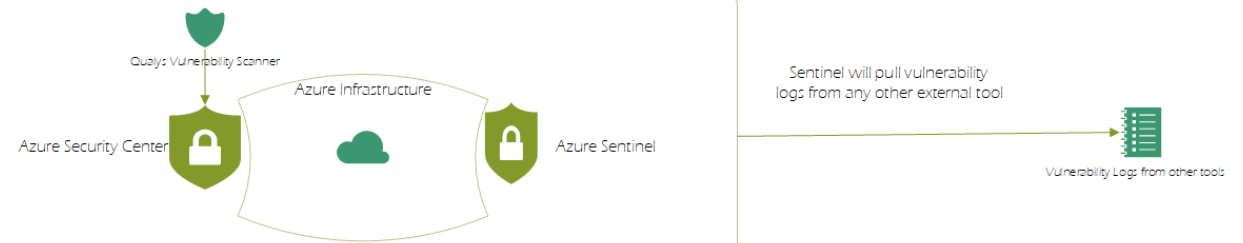
CIS:

- Maintenance, Monitoring and Analysis of Audit Logs (6.6/6.7/6.8)

Cloud Vulnerability Management



Native Azure
Security
Solutions



andrei.oros@uipath.com26-Jun-2020_Qualys - Read-Only

ID	Owner	Resource	ResourceGroup	Recommendation	Timestamp
1	/subscriptions/8e andrei.oros@uip:it-ops-rbt-23	DEVTEST-ITOPSAUTO		Vulnerabilities in your virtual machine:	26-06-2020
2	/subscriptions/8e andrei.oros@uip:T204F4576-R3	DEVTEST_WF_ROBOT		Vulnerabilities in your virtual machine:	26-06-2020
3	/subscriptions/8e andrei.oros@uip:Tid9351-R4	DEVTEST_WF_ROBOT		Vulnerabilities in your virtual machine:	26-06-2020
4	/subscriptions/8e andrei.oros@uip:it-ops-rbt-21	DEVTEST-ITOPSAUTO		Vulnerabilities in your virtual machine:	26-06-2020
5					
6					
7					
8					
9					

andrei.oros@uipath.com26-Jun-20

Retrieves recommendations, vulnerability and regulatory compliance information from Azure Security Center. Retrieves vulnerability information from any other tool integrated in Sentinel. Sends Robot logs to Sentinel for extra reporting capabilities.



Weekly reporting via mail on resources that have vulnerabilities, recommendations and regulatory compliance items with context-specific severity and deadlines



Resource Owner

Daily reporting on successful remediations and breached deadlines.



Security Operations

Monthly reporting to leadership in regards to open items, closed items, percentage of closed items, mean time to resolve and owners with breached items



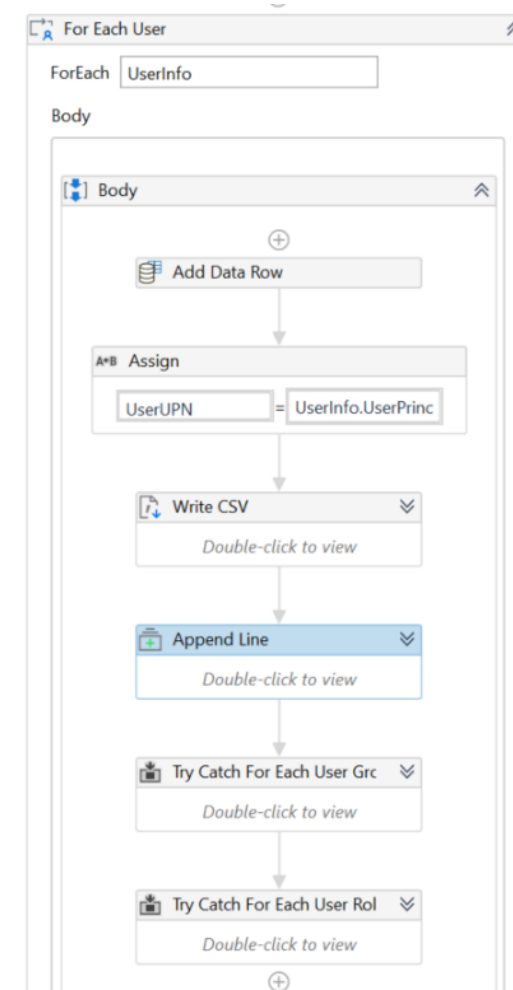
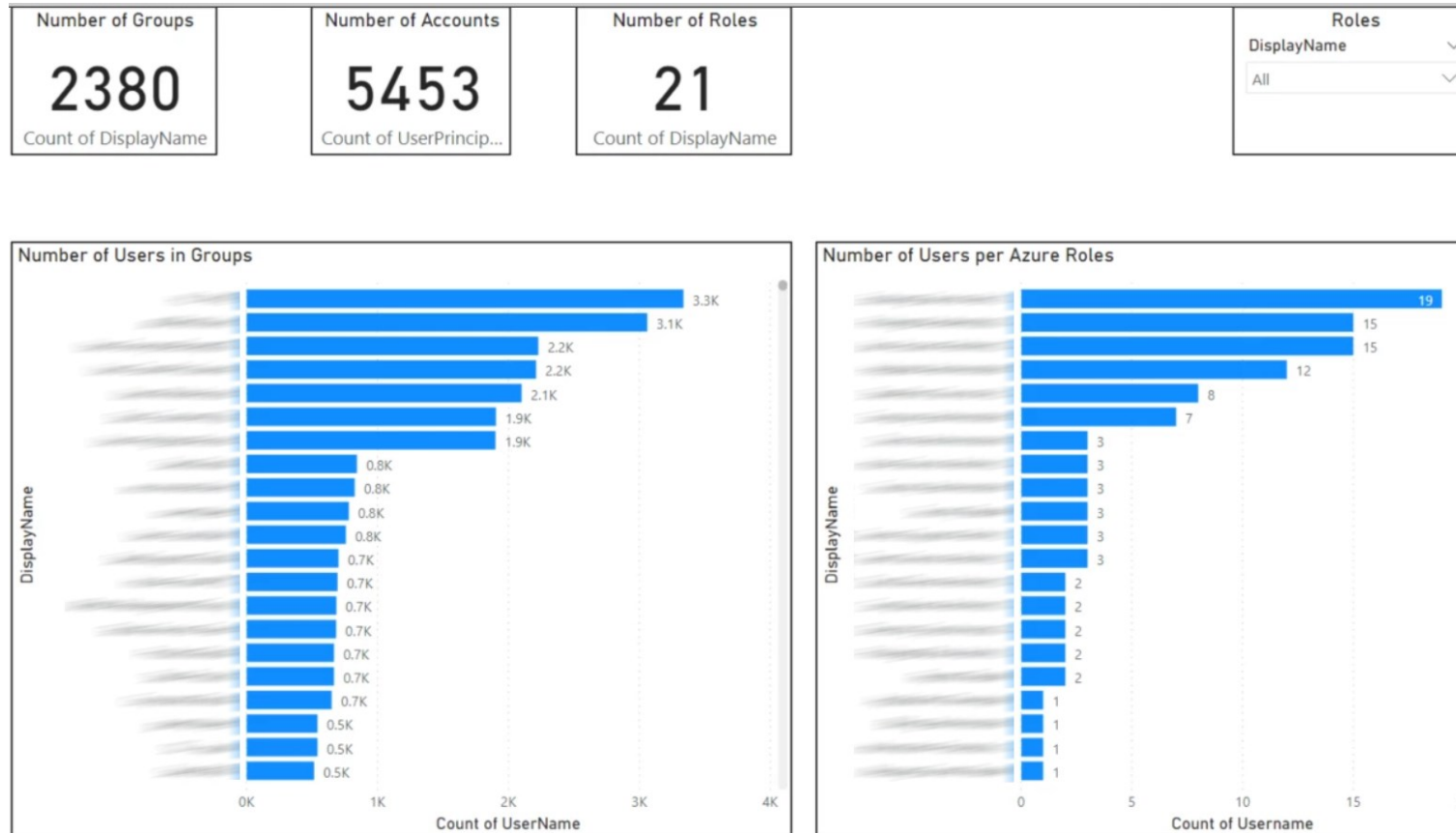
Leadership

Escalation for non-tagged resource groups



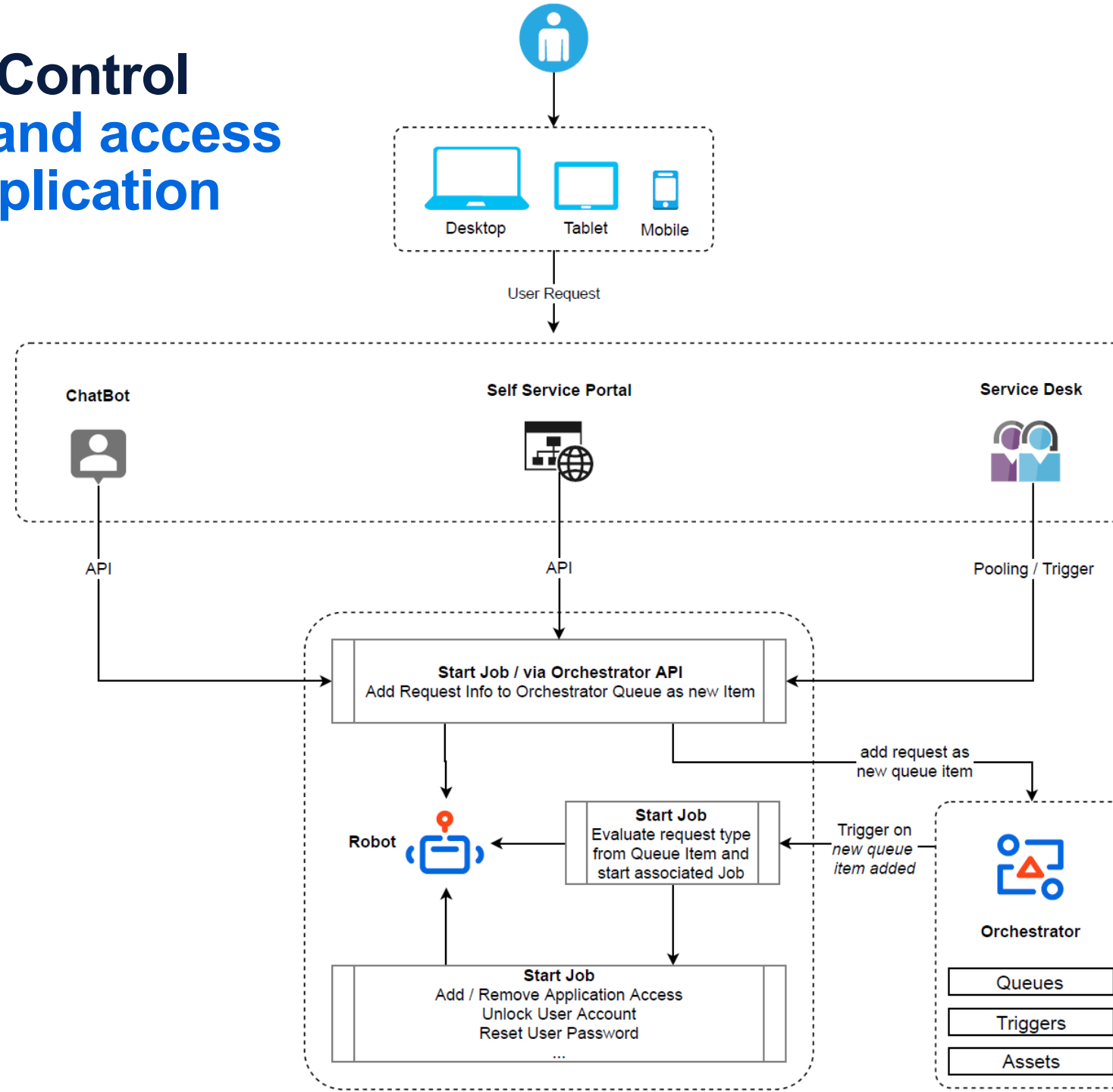
Cloud Operations

Azure AD users groups & roles memberships + resources ownership



Access Control

Access Control on-demand access to an application



Access Control on-demand access to a server

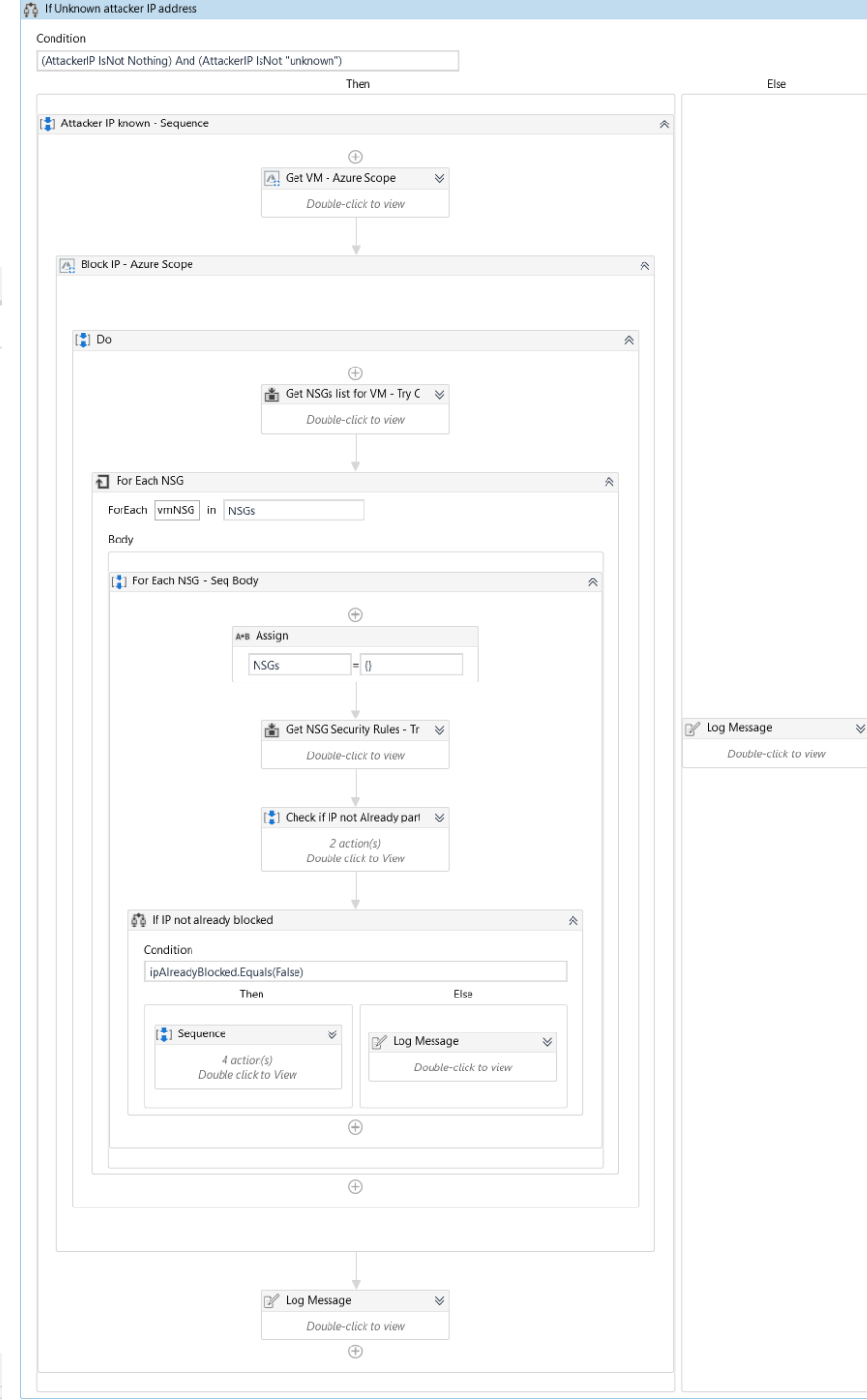
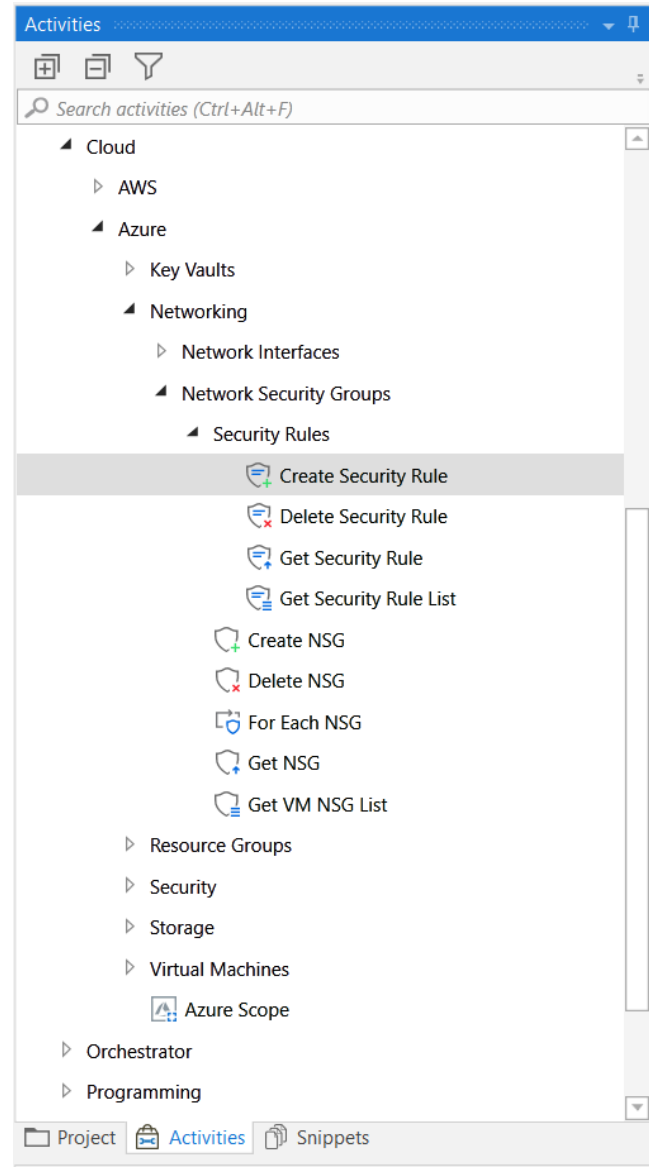
User requests access to a server via the Assistant

Approve Task sent to IT
Job is persisted
IT approves
Job resumes execution

Temporary access is granted to the user's IP via a security rule

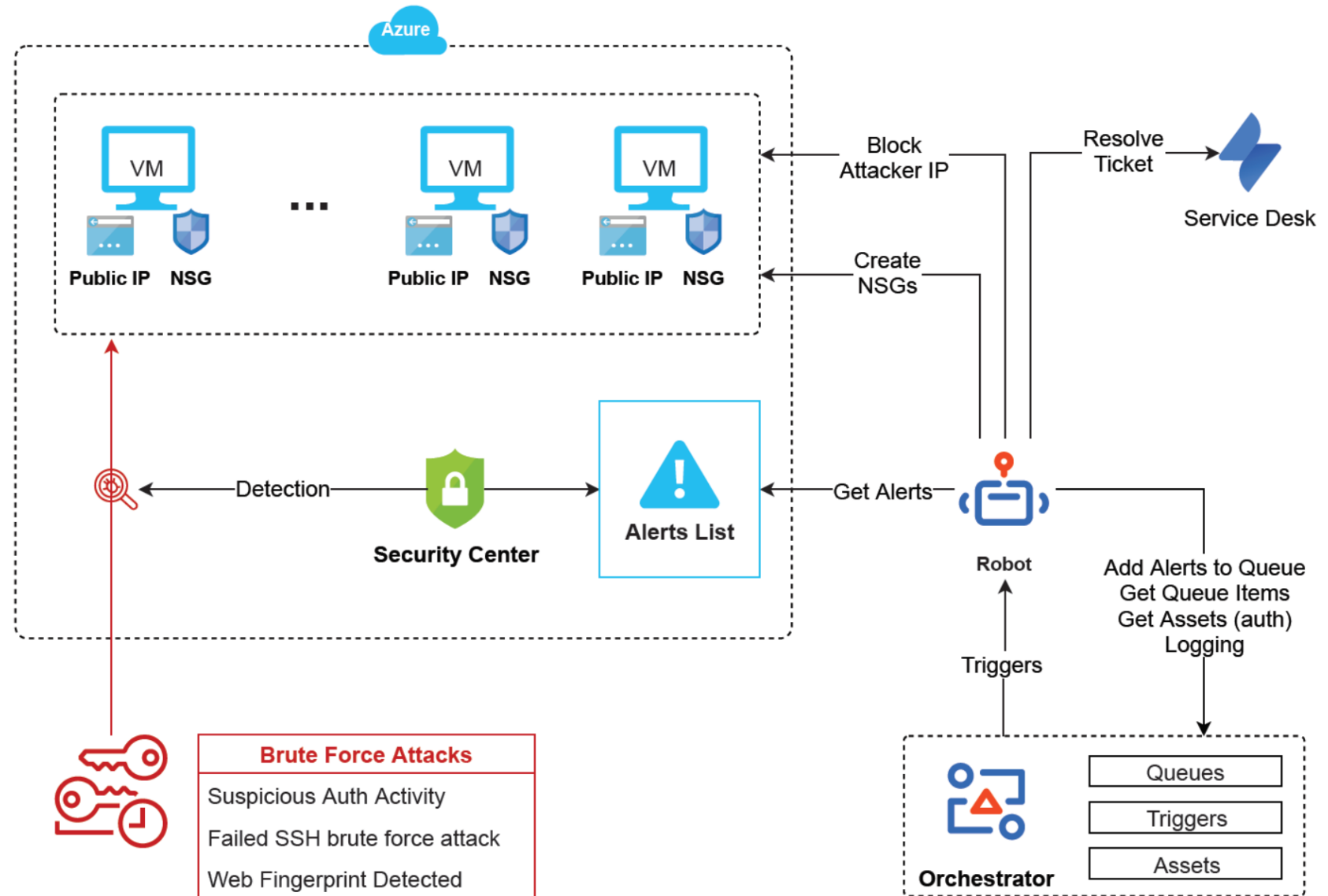
Job is persisted X time

Job is un-persisted after X time and the user's access is revoked



Brute Force Attacks Azure

Azure Security Orchestration



10500+ attacks

processed automatically in the last 4 months

Azure_SecurityCenterAlerts_VMAccounts Chart



0.00

BUSINESS
EXCEPTIONS



0.00

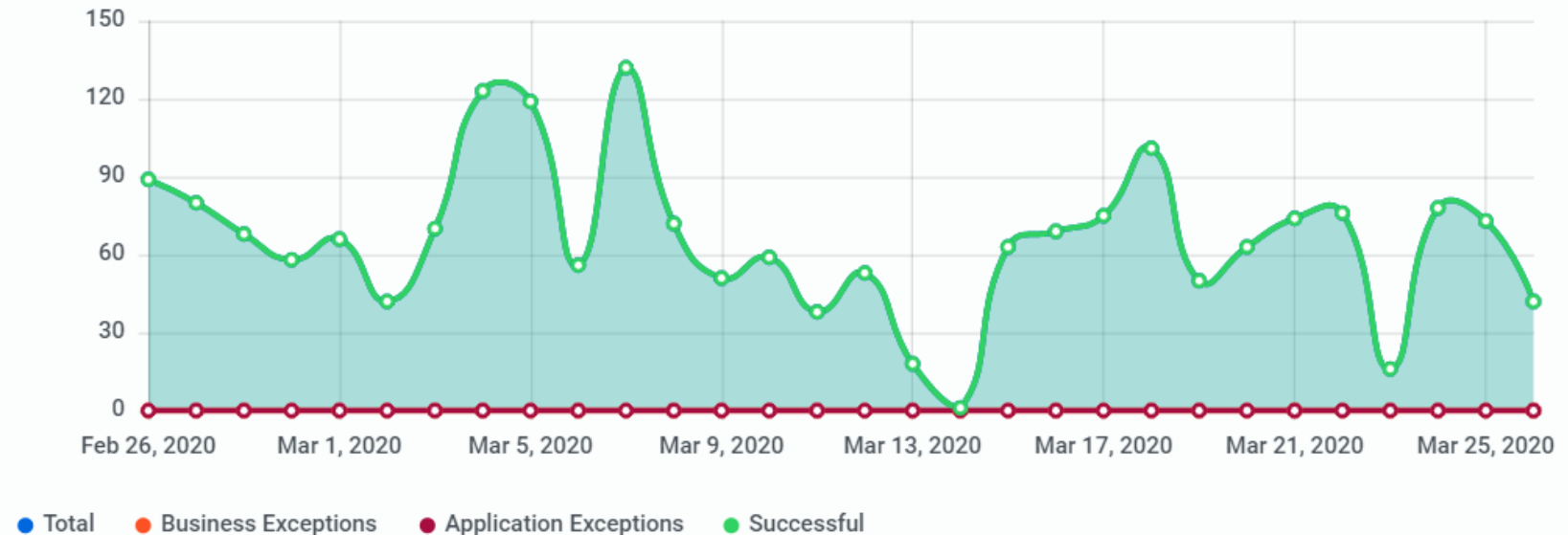
APPLICATION
EXCEPTIONS



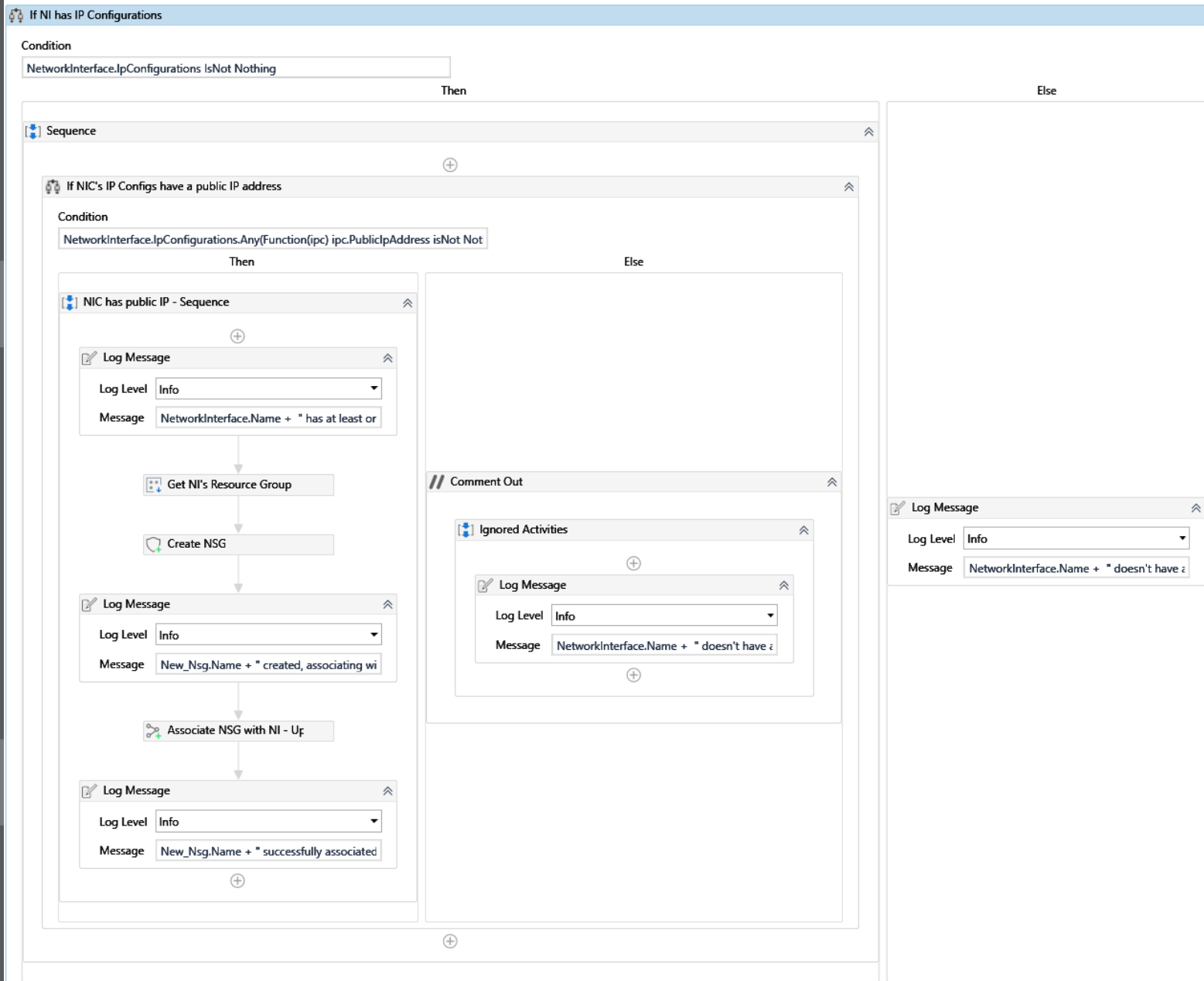
7.04

SUCCESSFUL
TRANSACTIONS

TRANSACTIONS FEBRUARY 26 - MARCH 26

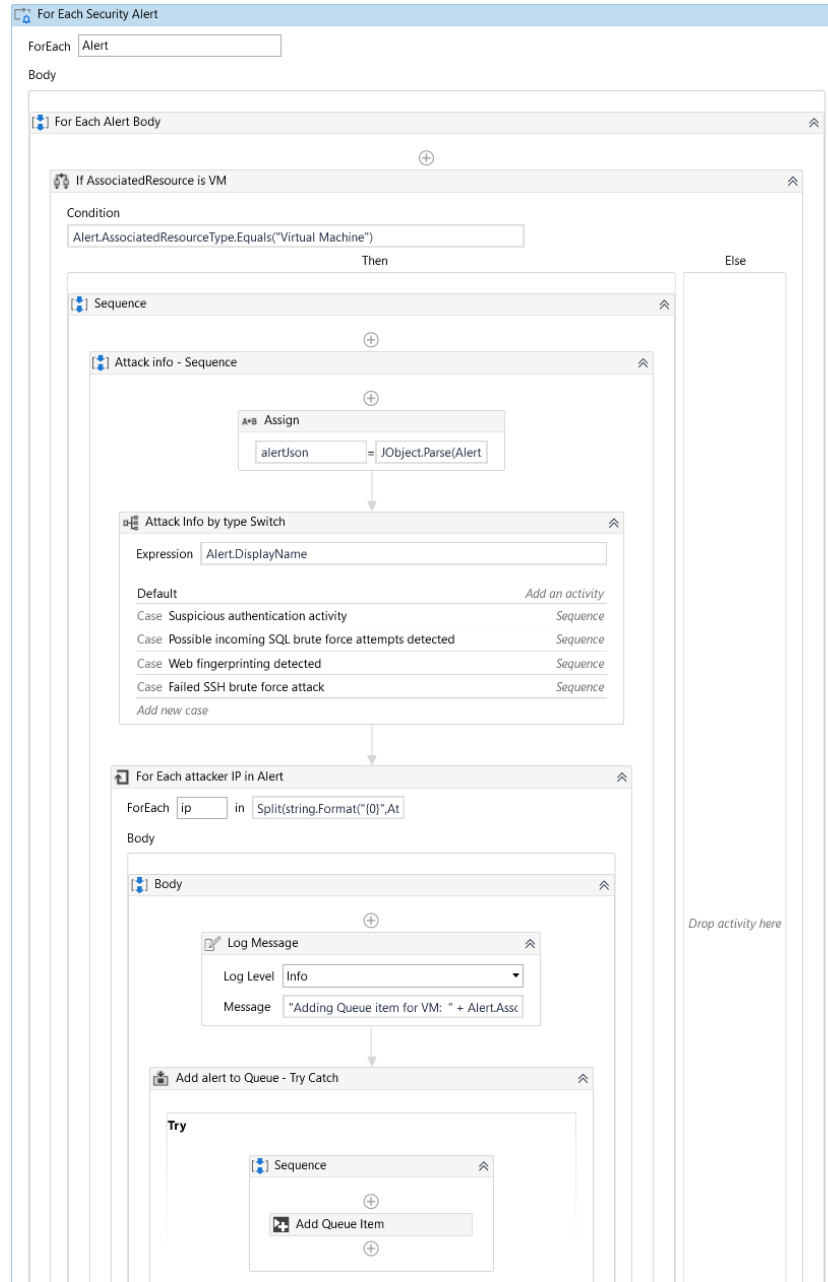


Create NSGs for NIs without one



Create Network Security Groups for all the Network Interfaces that have public IP addresses in their IP Configurations and don't have an associated NSG.

Get Alerts from Azure Security Center

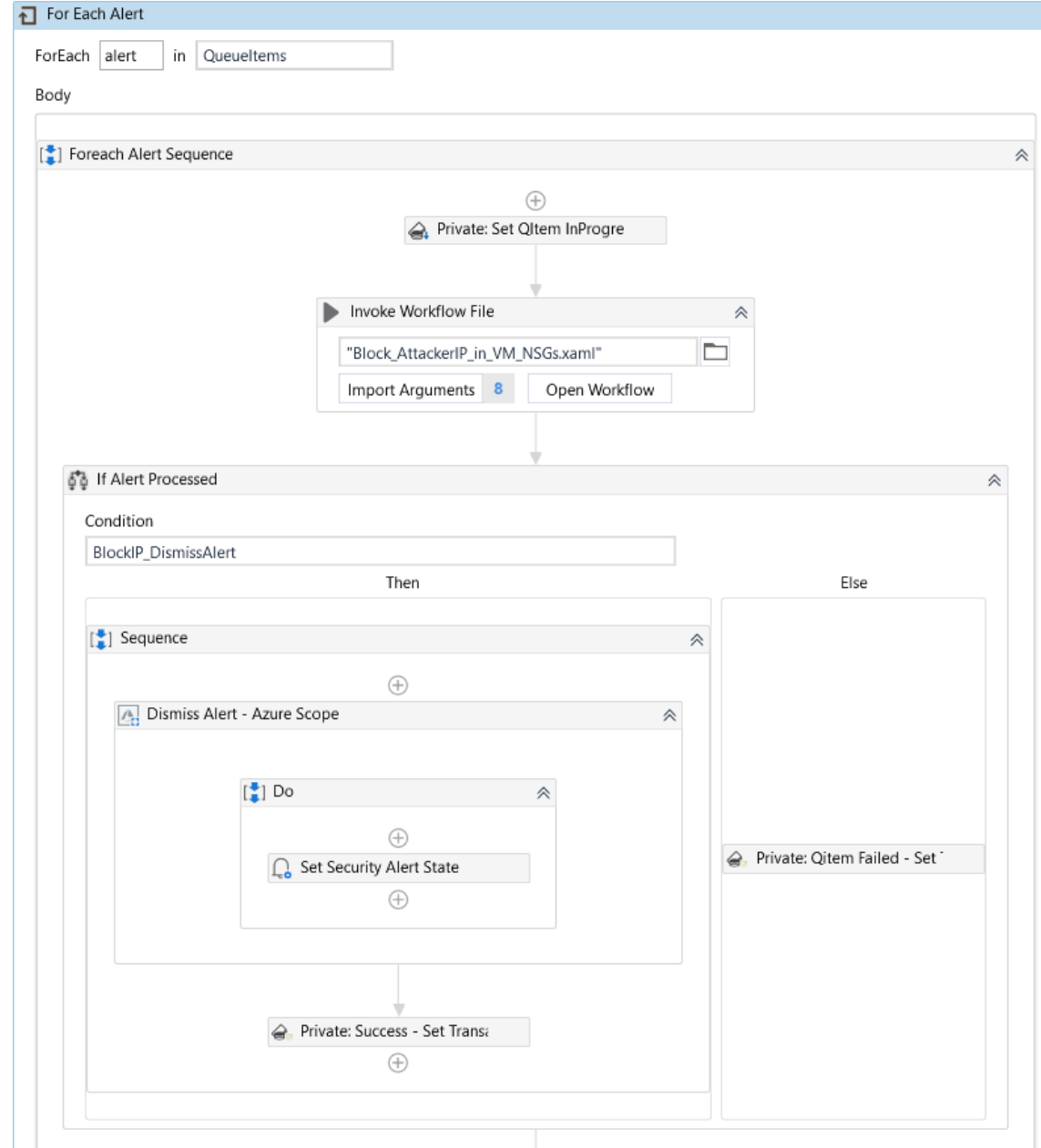


Get all the Azure Security Center Alerts associated with Brute Force Attacks on Virtual Machines with public IPs

Add a Queue Item for each Alert with the info required to block the Attacker IP

- VM Name & Resource Group
- Attacker IP
- Azure info (subscription, location)

Process Alerts



Get all Queue Items from the associated Orchestration queue.

For each Alert item, block the Attacker IP in all the Network Security Groups that are associated with the Attacked Virtual Machine:

- adds a security rule in each NSG to deny all connections on all ports for the specified attacker IP address

On Demand Block IP

Start the process via an Orchestrator Job with the web or mobile app and block the specified attacker IP's access to the input Virtual Machine:

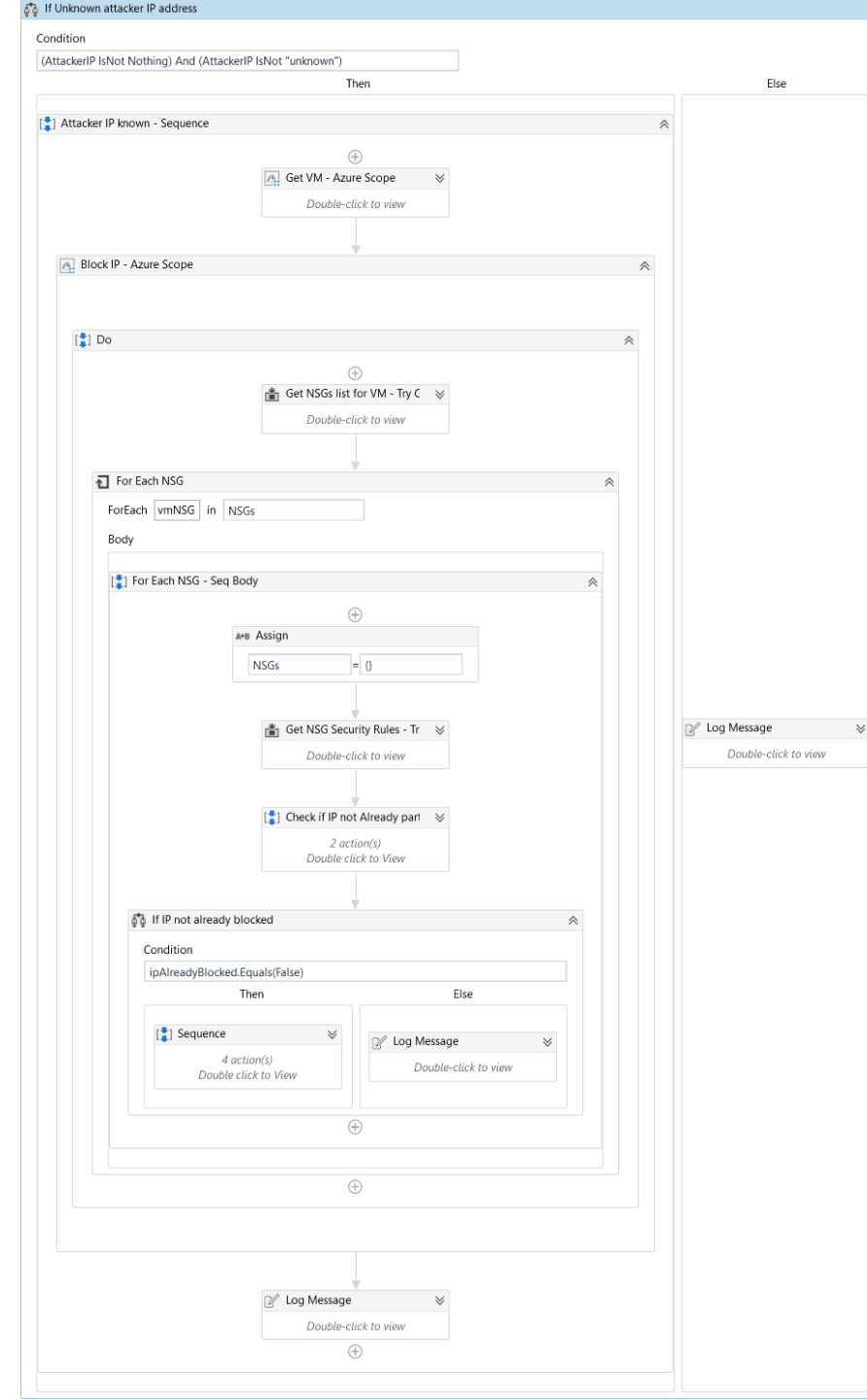
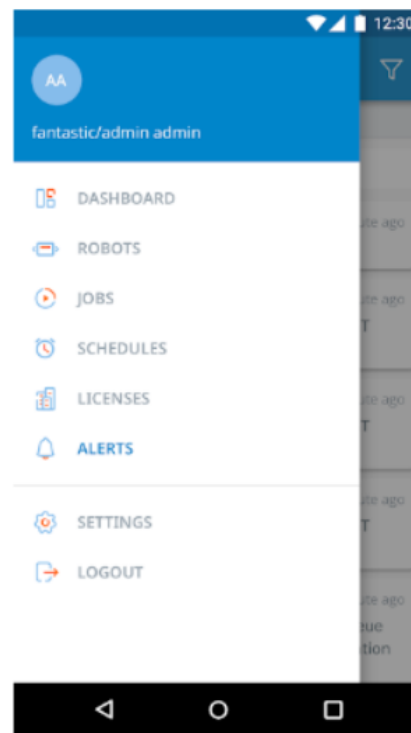
Start Job

Process *
Block Attacker IP in VM NSGs

Job priority *
→ Normal

EXECUTION TARGET	PARAMETERS												
	<table><thead><tr><th>PARAMETERS</th><th>VALUE</th></tr></thead><tbody><tr><td>String AttackerIP</td><td>Inherited from package</td></tr><tr><td>String VM_Name</td><td>Inherited from package</td></tr><tr><td>String Azure_SubscriptionID</td><td>Inherited from package</td></tr><tr><td>String VM_ResourceGroup</td><td>Inherited from package</td></tr><tr><td>String NewSecurityRule_NamePrefix</td><td>Inherited from package</td></tr></tbody></table>	PARAMETERS	VALUE	String AttackerIP	Inherited from package	String VM_Name	Inherited from package	String Azure_SubscriptionID	Inherited from package	String VM_ResourceGroup	Inherited from package	String NewSecurityRule_NamePrefix	Inherited from package
PARAMETERS	VALUE												
String AttackerIP	Inherited from package												
String VM_Name	Inherited from package												
String Azure_SubscriptionID	Inherited from package												
String VM_ResourceGroup	Inherited from package												
String NewSecurityRule_NamePrefix	Inherited from package												


CANCEL START




Demo




[Home](#) > [higuchi-ad - Networking](#)


 **higuchi-ad - Networking**
Virtual machine


[Attach network interface](#) [Detach network interface](#)





 **Network Interface: higuchi-ad930** [Effective security rules](#)
Virtual network/subnet: [taketo.higuchi-infra.jp-vnet/default](#) NIC Public I

[Inbound port rules](#) [Outbound port rules](#) [Application security gro](#)

 Network security group [higuchi-ad-nsg](#) (attached to network interfa
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port
100	IT-Ops-Automation UTC 2019-11-2...	Any
1000	 RDP	3389
65000	AllowVnetInBound	Any
65001	AllowAzureLoadBalancerInBound	Any
65500	DenyAllInBound	Any

 **IT-Ops-Automation UTC 2019-11-28_30-40**
higuchi-ad-nsg

 Save  Discard  Basic  Delete

Source * ⓘ
IP Addresses

Source IP addresses/CIDR ranges * ⓘ
193.169.252.217/32

Source port ranges * ⓘ
*

Destination * ⓘ
Any

Destination port ranges * ⓘ
*

Protocol *
Any TCP UDP ICMP

Action *
Allow Deny

Priority * ⓘ
100

Name *
IT-Ops-Automation UTC 2019-11-28_30-40

Description
created by Robot for alert 2518274411956853371_5ad4f587-50f4-4e66-8360-3101cd3afc92

IT Automation for Public, Private & Hybrid Clouds



Community Academy Marketplace



Connect Home > Marketplace > Components > IT Automation for Public, Private & Hybrid Clouds



Version: 1.0 (View History)

Published: March 27th, 2020

Downloads: 3

Industry: Cross-Industry

Process:
Information Technology

Tags: active-directory,
Amazon AWS,
Azure Active Directory, citrix,
cloud, Datacenter,
Exchange Server, IT,
microsoft, Microsoft Azure,
Server Virtualization,
User Management, VMware

Download

Bookmark

Community
Support

Report A Bug

IT Automation for Public, Private & Hybrid Clouds

Solution

Description

Media (6)

Reviews

Questions

Summary: Workflows that enable organizations from all industries to accelerate the automation of their IT ecosystem in the areas of Cloud, Server Virtualization, User Management, Security, Networking and more.

UiPath's vision for the "Automation First" era has led to the addition in its market-leading Enterprise RPA Platform of dedicated official out-of-the-box IT Automation capabilities that empower all companies to take their Digital Transformation to the next level. Official activities packs:

- Active Directory
- Azure Active Directory
- Microsoft Azure
- Amazon Web Services (AWS)
- VMware vCenter ESXi
- Citrix Hypervisor (XenServer)
- Exchange Server

The IT Automation focused solution comprises four components:

1. Identity and User Management
2. IT Infrastructure and Services Management
3. Cloud Security Orchestration
4. Cloud Migration

..that offer a strong value proposition to all levels:

Details

Producers



Andrei Oros
Product Management & Strategy,
Engineering at [UiPath](#)



UiPath



Benefits

The solution can accelerate your IT Automation projects with out-of-the-box ready to use workflow samples and snippets.

Compatibility

UiPath Studio 19.10+

Dependencies

UiPath.Azure.Activities >= 1.1
UiPath.AmazonWebServices.Activities >= 1.0
UiPath.VMWare.Activities >= 1.0
UiPath.Citrix.Activities >= 1.0
UiPath.ActiveDirectoryDomainServices.Activities >=



Get it from
Connect



Get it from
**Microsoft Azure
Marketplace**



Get it from
**Microsoft
AppSource**



<https://connect.uipath.com/marketplace/components/it-automation-for-public-private-and-hybrid-clouds>

About UiPath



A Leader in the 2020 Gartner Magic Quadrant for Robotic Process Automation

For the second consecutive year, UiPath is placed highest for its ability to execute

*“In the second year of this Magic Quadrant, the bar has been raised for market viability, relevance, growth, revenue and how vendors set the vision for their RPA offerings in a fluid market.”**

* Source: Gartner, “Magic Quadrant for Robotic Process Automation,” Saikat Ray, Arthur Villa, Cathy Tornbohm, Naved Rashid, Melanie Alexander, July 27, 2020



Magic Quadrant for Robotic Process Automation



Source: Gartner (July 2020)

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from UiPath. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



A Forrester Wave Leader

Highest Scores in Current Offering, and Highest Possible Scores in Strategy and Market Presence

“References report that UiPath will go the extra mile to meet a client's need and cite the transparent and innovation culture as a plus.

They also applaud the low cost of getting started, the well-organized partner channel, overall product stability, and strong security.”

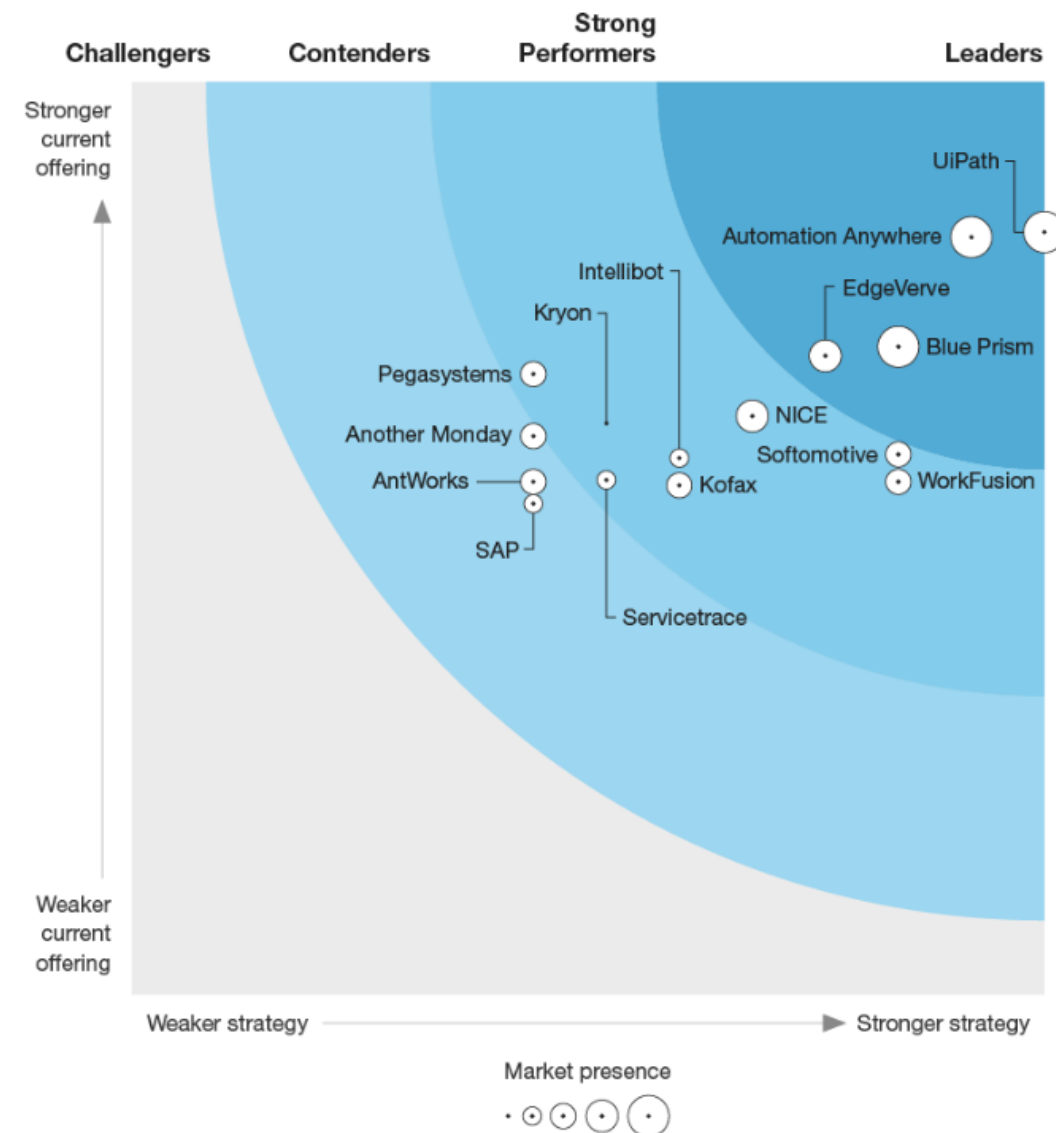
Source: ForresterWave™:RoboticProcessAutomation,Q42019

FIGURE 1 Forrester Wave™: Robotic Process Automation, Q4 2019

THE FORRESTER WAVE™

Robotic Process Automation

Q4 2019



A Process Mining Leader

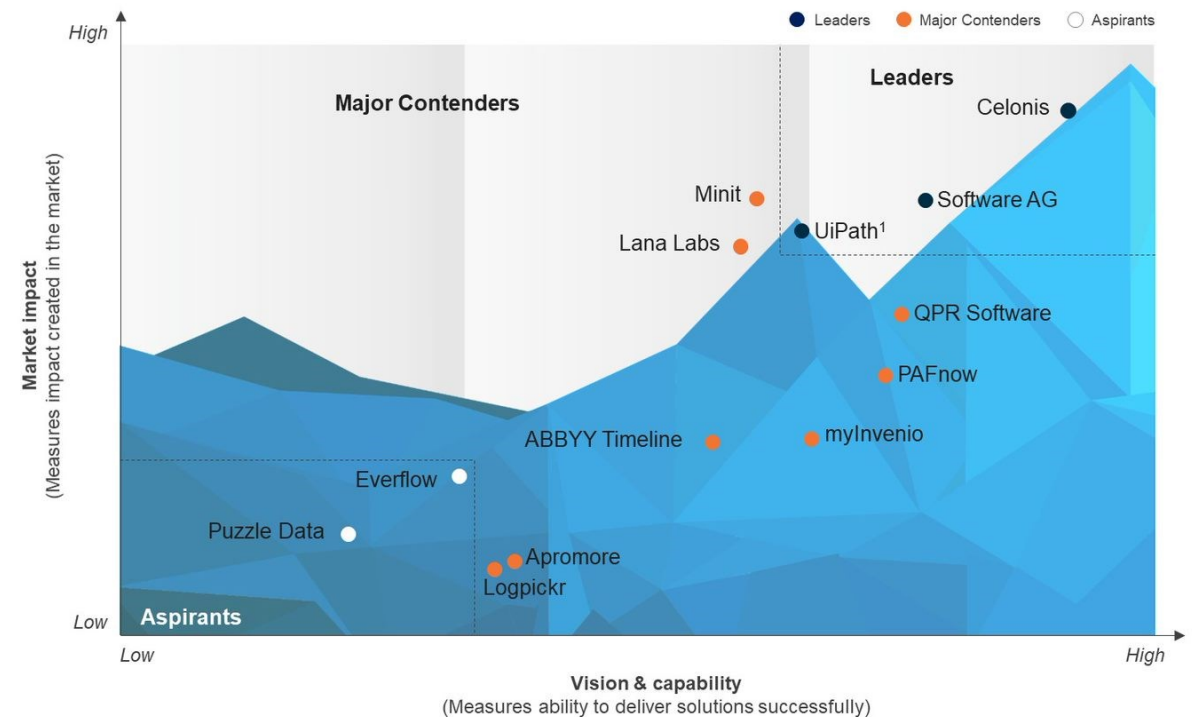
Everest Group PEAK Matrix® for Process Mining Technology Vendors 2020



"[...] its product development strategy is now more focused toward helping enterprises discover automation use cases and accelerate their automation journeys."



Everest Group Process Mining Products PEAK Matrix® Assessment 2020



1. UiPath Process Mining (formerly ProcessGold)

Business Partner Ecosystem Spans Globally and Locally

Global	Americas	Japan	EMEA	India	Asia Pacific
      	    	    	    	    	    

600+ business partners that help with the implementation of RPA



Thank you

andrei.oros@uipath.com

