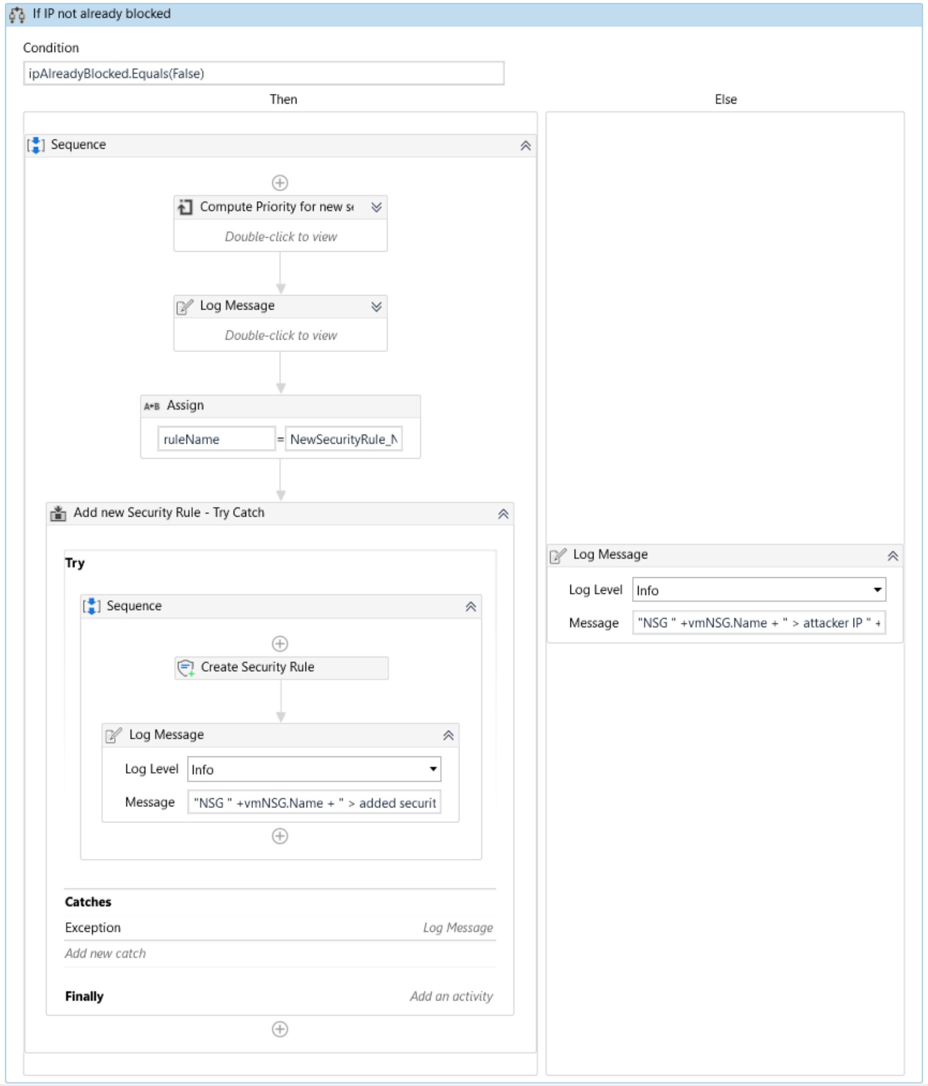
Security Orchestration

powered by **IT Automation**

Andrei Oros

UiPath™

Security Orchestration with RPA Workflows



Condition: ipAlreadyBlocked.Equals(False)

ruleName = NewSecurityRule_N

Log Level: Info

Message: "NSG " +vmNSG.Name + " > added securit

Log Level: Info

Message: "NSG " +vmNSG.Name + " > attacker IP " +

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

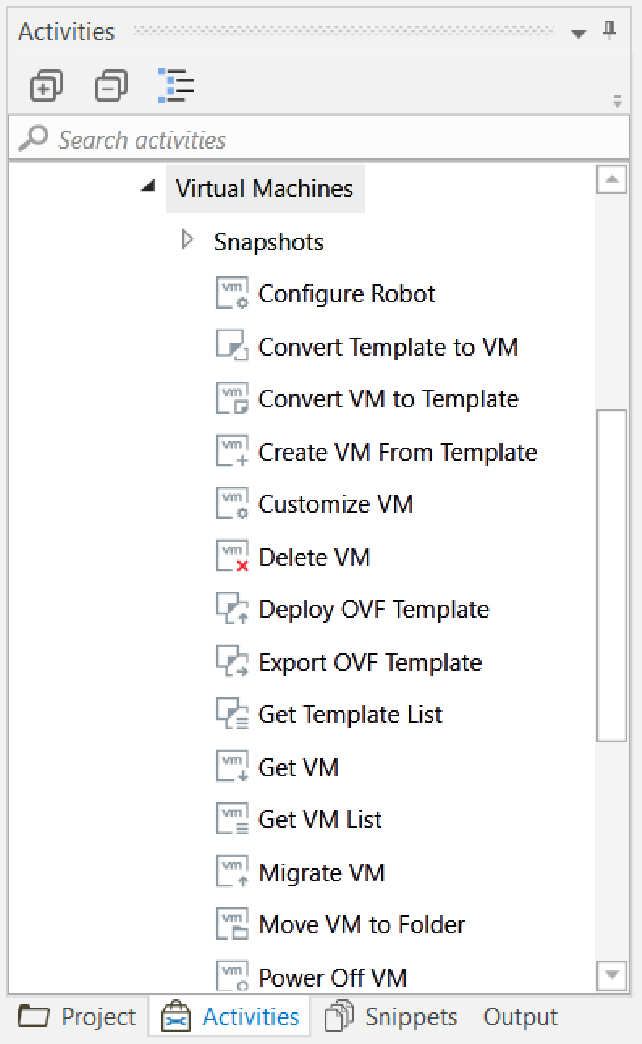
Background running activities built on top of the official SDKs from *Microsoft, Amazon, Citrix, VMware, ..*

Security and Compliance

Developed by UiPath

Published on the official feed (LTS)

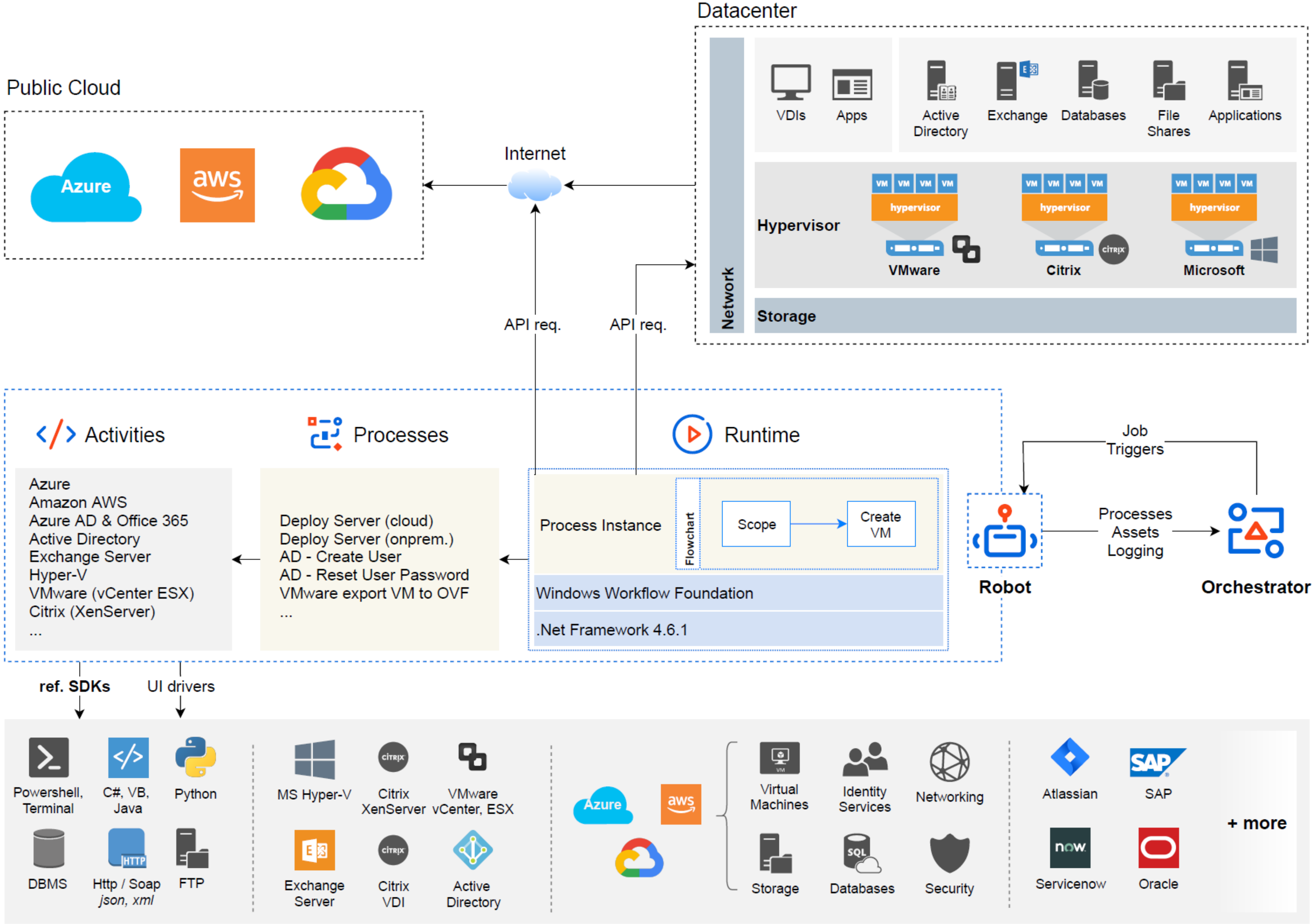
VERACODE
VERIFIED CONTINUOUS


Activities

Search activities

- Virtual Machines
  - Snapshots
  - Configure Robot
  - Convert Template to VM
  - Convert VM to Template
  - Create VM From Template
  - Customize VM
  - Delete VM
  - Deploy OVF Template
  - Export OVF Template
  - Get Template List
  - Get VM
  - Get VM List
  - Migrate VM
  - Move VM to Folder
  - Power Off VM

IT integrations landscape



Public Cloud

Azure

aws

Internet

Datacenter

VDIs

Apps

Active Directory

Exchange

Databases

File Shares

Applications

Hypervisor

VMware

Citrix

Microsoft

Network

Storage

API req.

API req.

Activities

Azure
Amazon AWS
Azure AD & Office 365
Active Directory
Exchange Server
Hyper-V
VMware (vCenter ESX)
Citrix (XenServer)
...

Processes

Deploy Server (cloud)
Deploy Server (onprem.)
AD - Create User
AD - Reset User Password
VMware export VM to OVF
...

Runtime

Process Instance

Flowchart

Scope

Create VM

Windows Workflow Foundation

.Net Framework 4.6.1

Job Triggers

Robot

Processes
Assets
Logging

Orchestrator

ref. SDKs

UI drivers

Powershell, Terminal

C#, VB, Java

Python

DBMS

Http / Soap
json, xml

FTP

MS Hyper-V

Citrix XenServer

VMware vCenter, ESX

Exchange Server

Citrix VDI

Active Directory

Azure

aws

Virtual Machines

Identity Services

Networking

Storage

Databases

Security

Atlassian

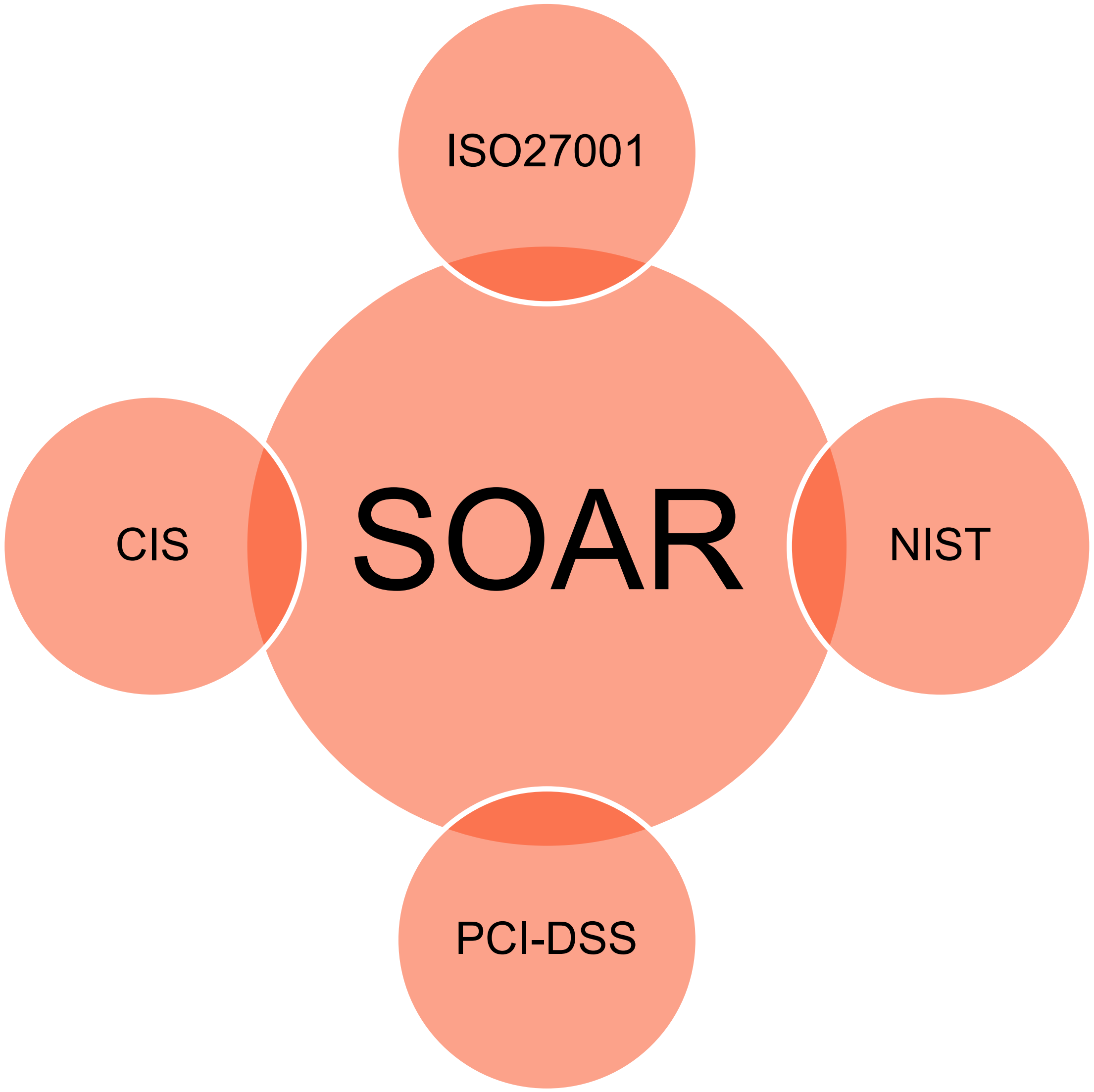
SAP

Servicenow

Oracle

+ more

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)

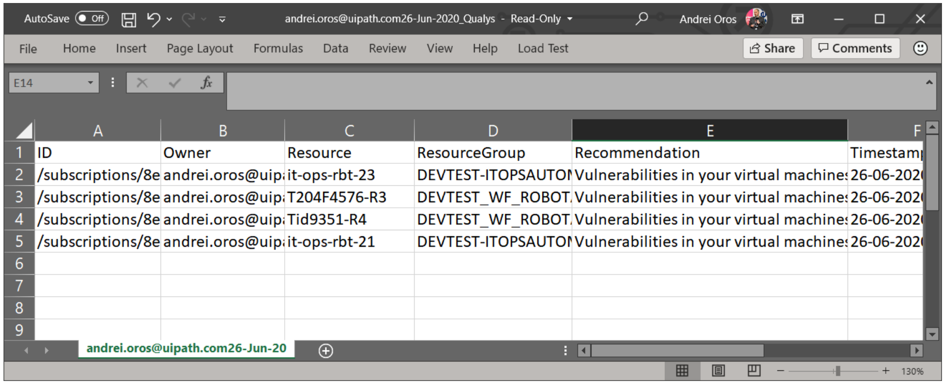
PCI-DSS:

- Regular monitor and test networks (10.6)

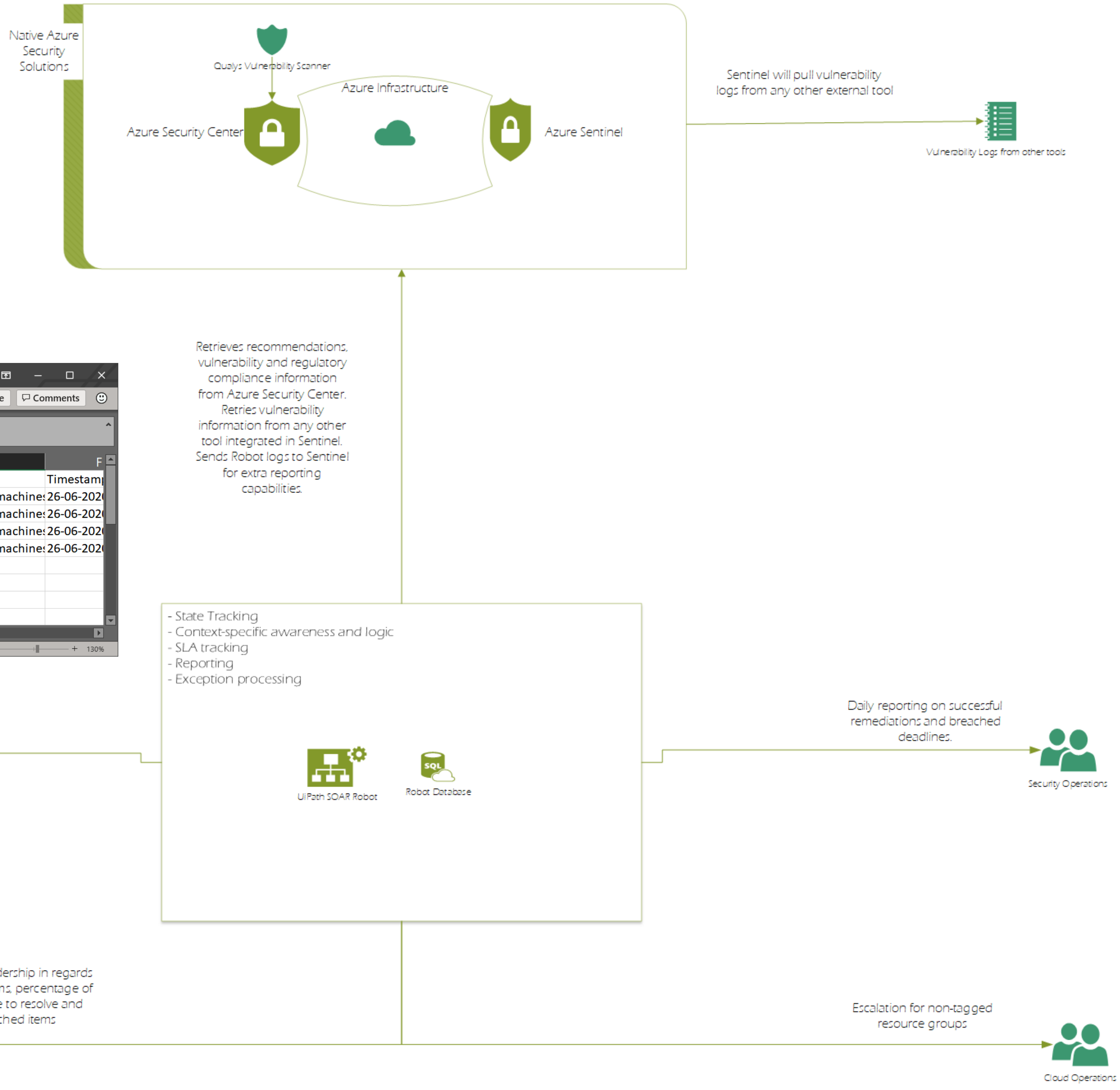
CIS:

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

Cloud Vulnerability Management



	A	B	C	D	E	F
1	ID	Owner	Resource	ResourceGroup	Recommendation	Timestam
2	/subscriptions/8e	andrei.oros@uip	it-ops-rbt-23	DEVTEST-ITOPSAUTON	Vulnerabilities in your virtual machines	26-06-202
3	/subscriptions/8e	andrei.oros@uip	T204F4576-R3	DEVTEST_WF_ROBOT.	Vulnerabilities in your virtual machines	26-06-202
4	/subscriptions/8e	andrei.oros@uip	Tid9351-R4	DEVTEST_WF_ROBOT.	Vulnerabilities in your virtual machines	26-06-202
5	/subscriptions/8e	andrei.oros@uip	it-ops-rbt-21	DEVTEST-ITOPSAUTON	Vulnerabilities in your virtual machines	26-06-202
6						
7						
8						
9						



Sentinel will pull vulnerability logs from any other external tool

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

- State Tracking
- Context-specific awareness and logic
- SLA tracking
- Reporting
- Exception processing

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

Resource Owner

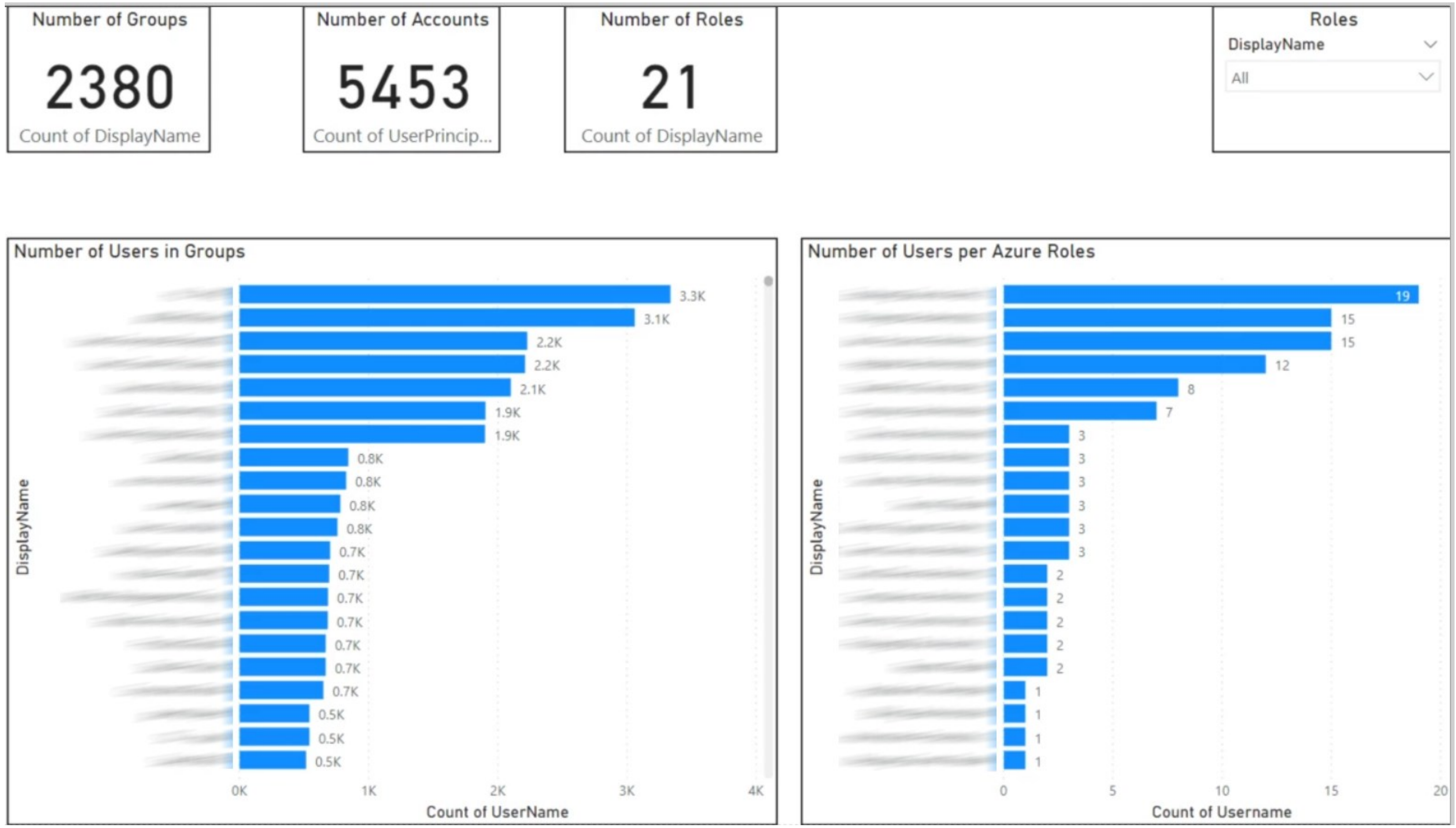
Daily reporting on successful remediations and breached deadlines.

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

Azure AD users groups & roles memberships + resources ownership

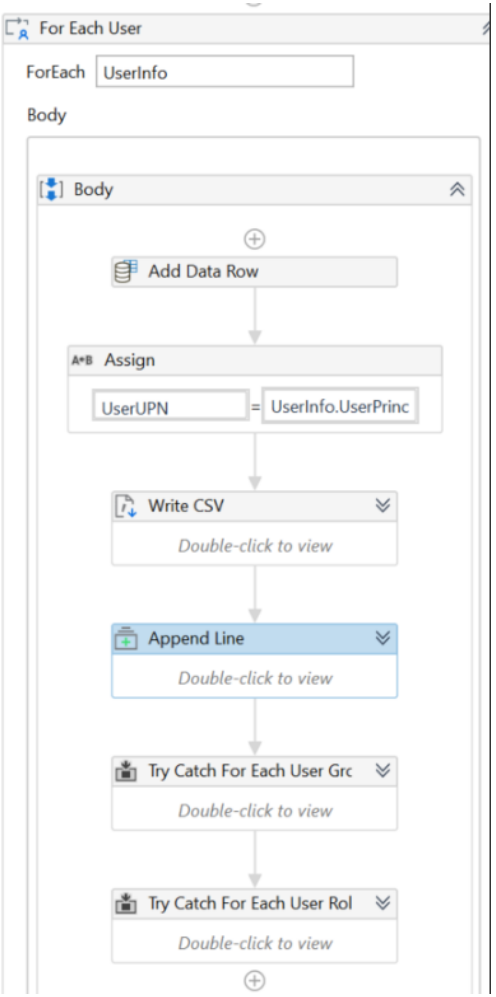


Number of Groups
2380
Count of DisplayName

Number of Accounts
5453
Count of UserPrincip...

Number of Roles
21
Count of DisplayName

Roles
DisplayName
All



For Each User
ForEach UserInfo
Body

Body

Add Data Row

Assign
UserUPN = UserInfo.UserPrinc

Write CSV
Double-click to view

Append Line
Double-click to view

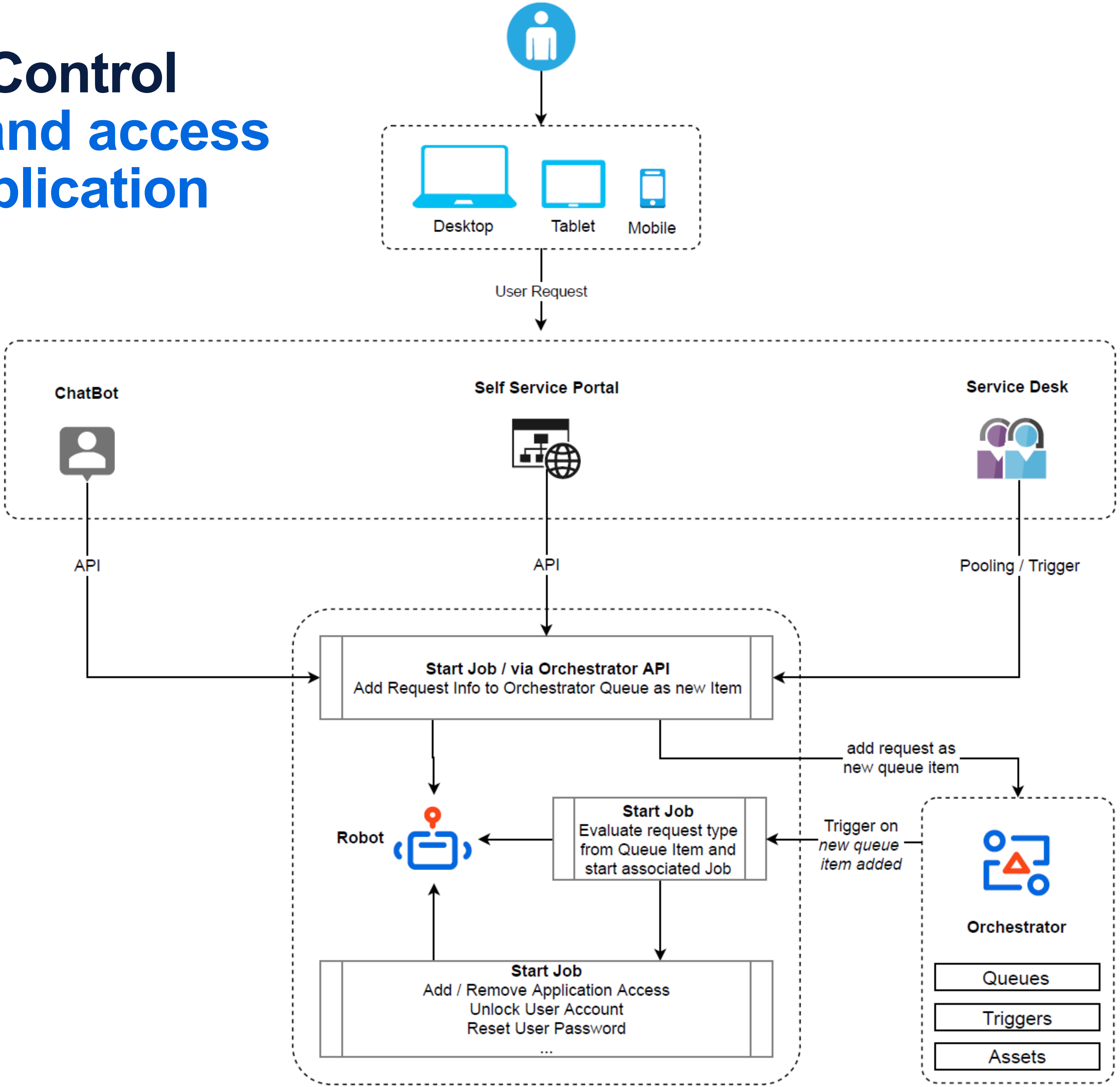
Try Catch For Each User Grc
Double-click to view

Try Catch For Each User Rol
Double-click to view

Access Control

UiPath™

Access Control
on-demand access to an application



Start Job / via Orchestrator API
Add Request Info to Orchestrator Queue as new Item

Start Job
Evaluate request type from Queue Item and start associated Job

Start Job
Add / Remove Application Access
Unlock User Account
Reset User Password
...

Access Control
on-demand access to a server

User requests access to a server via the Assistant

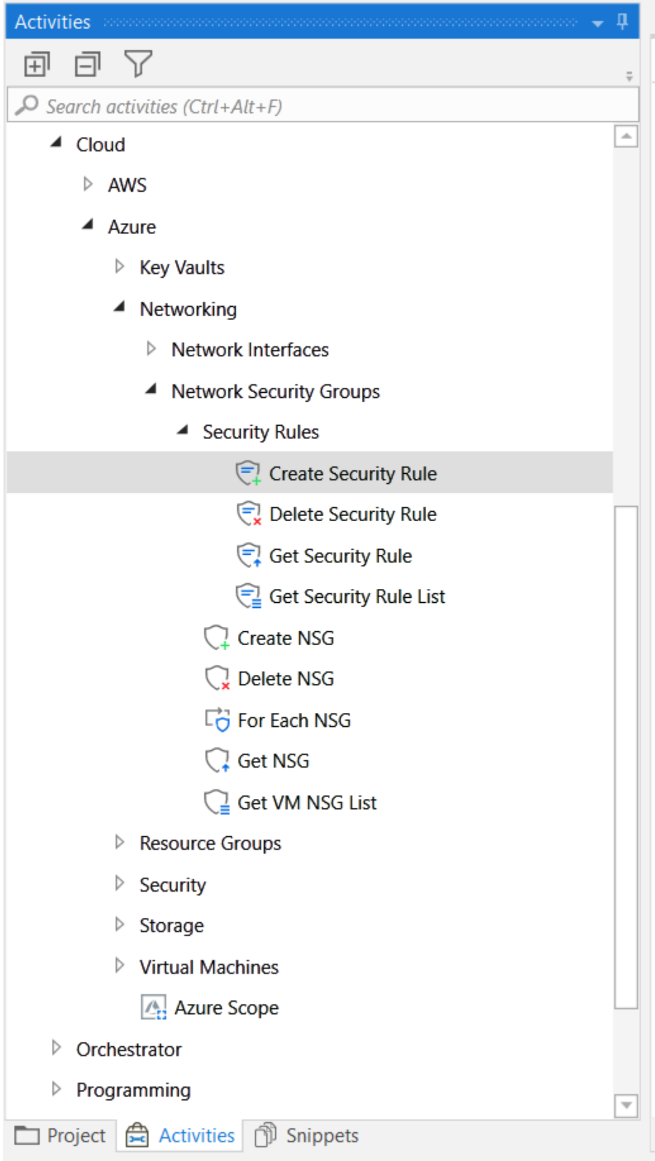
Approve Task sent to IT
Job is persisted
IT approves
Job resumes execution

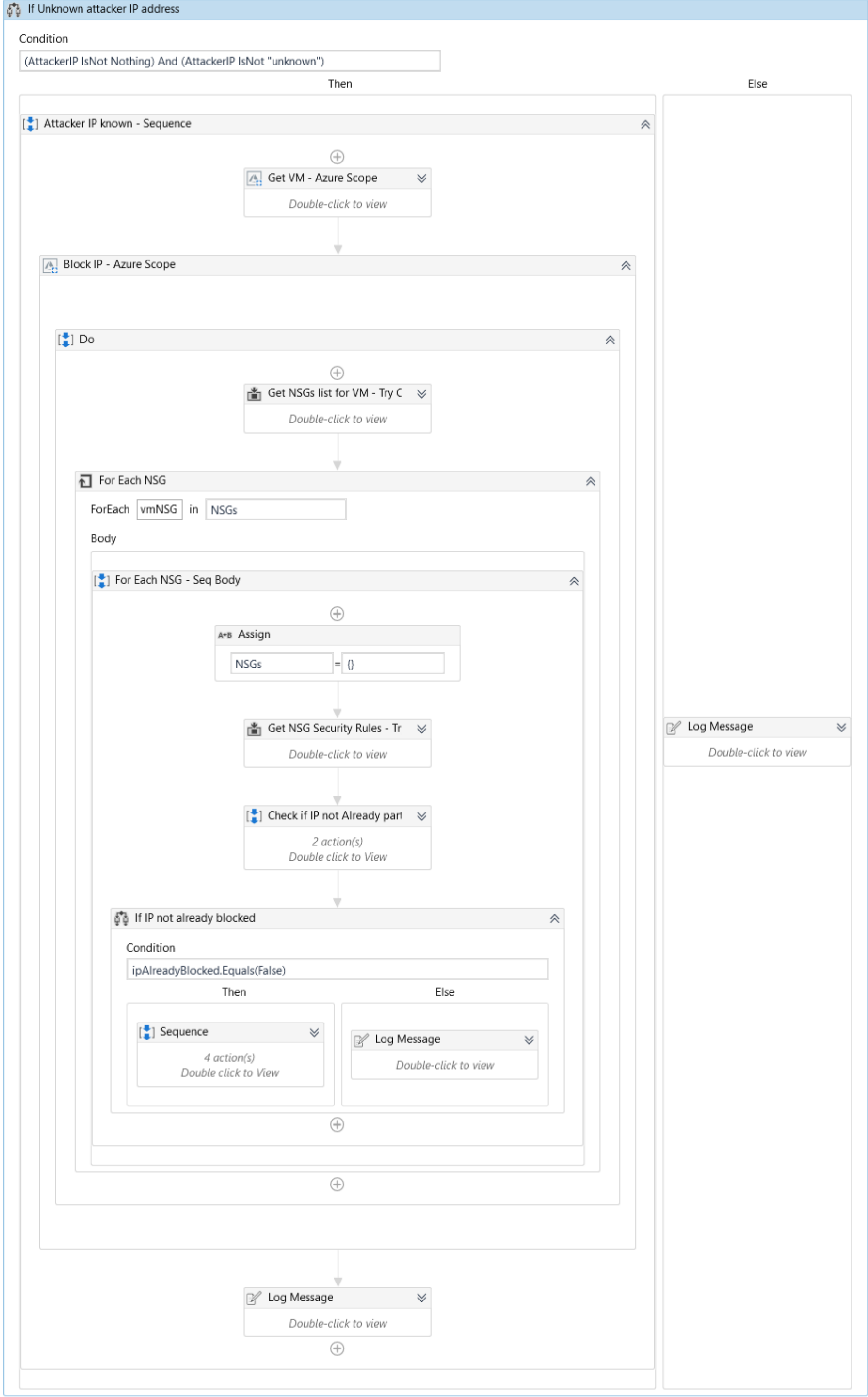
Temporary access is granted to the user’s IP via a security rule

Job is persisted X time

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

UiPath™





Condition
(AttackerIP IsNot Nothing) And (AttackerIP IsNot "unknown")

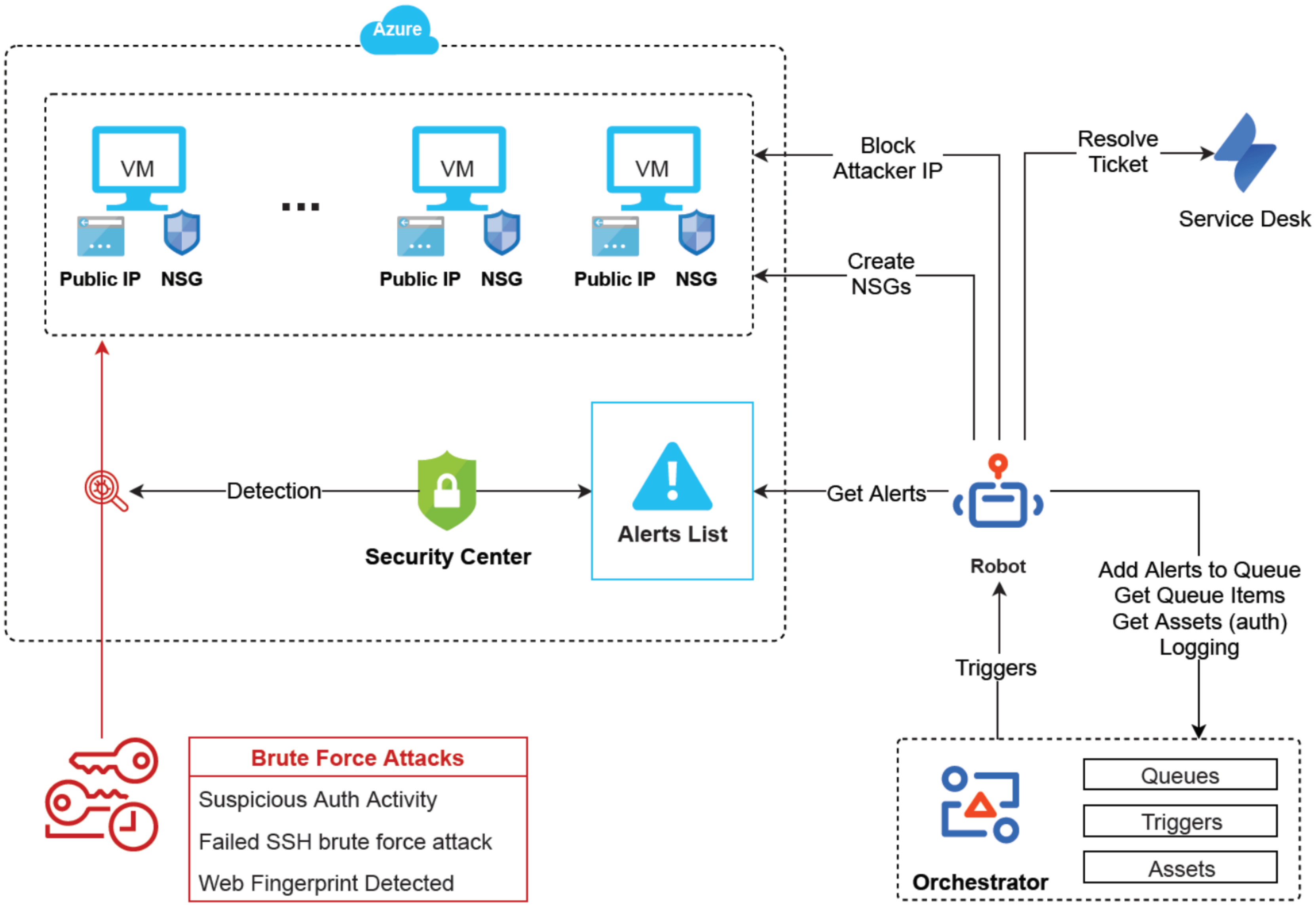
ForEach vmNSG in NSGs

NSGs = {}

Condition
ipAlreadyBlocked.Equals(False)

Brute Force Attacks
Azure

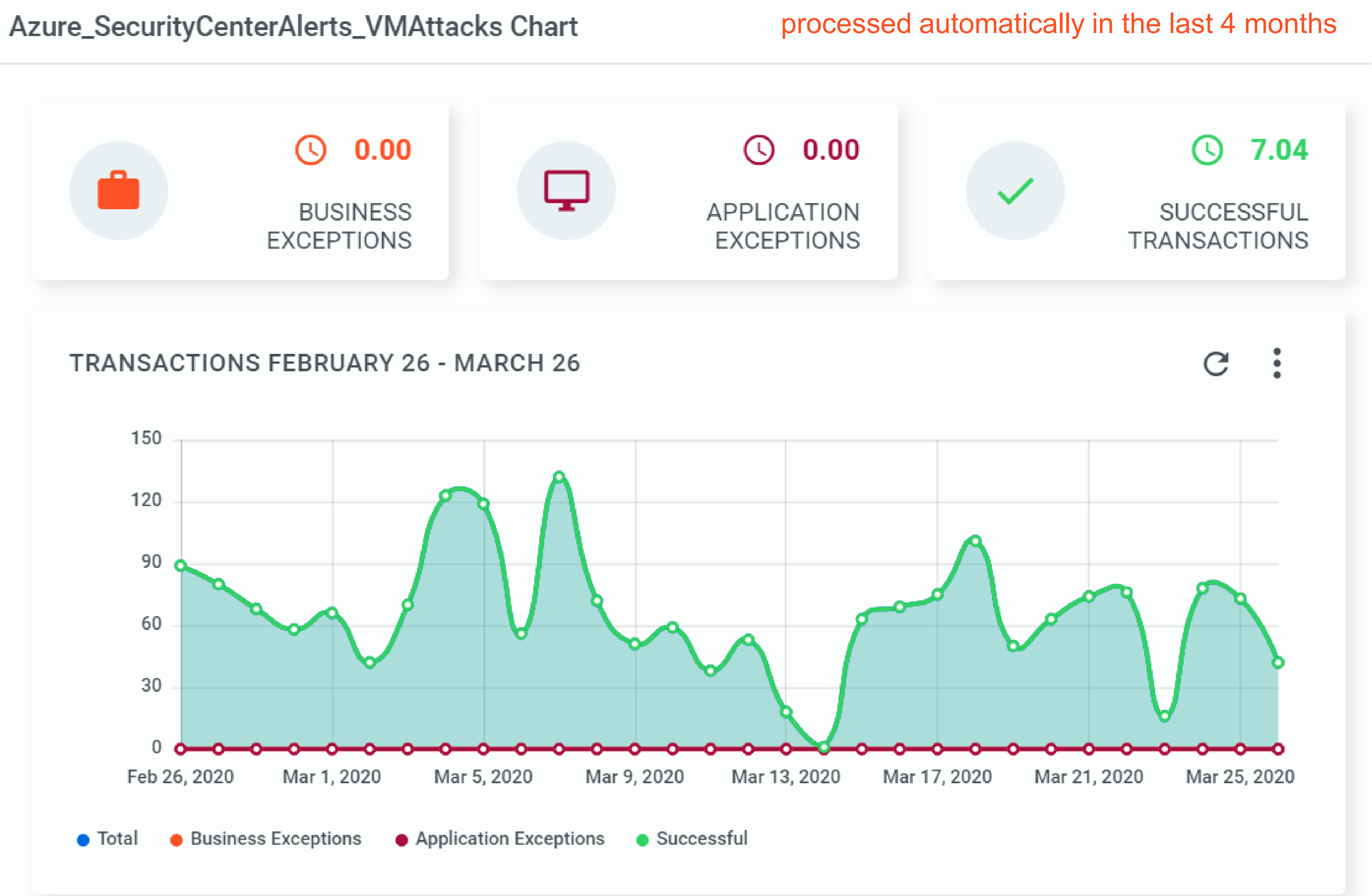
Azure Security Orchestration



Trusted by UiPath

10500+ attacks

processed automatically in the last 4 months



Azure_SecurityCenterAlerts_VMAttacks Chart

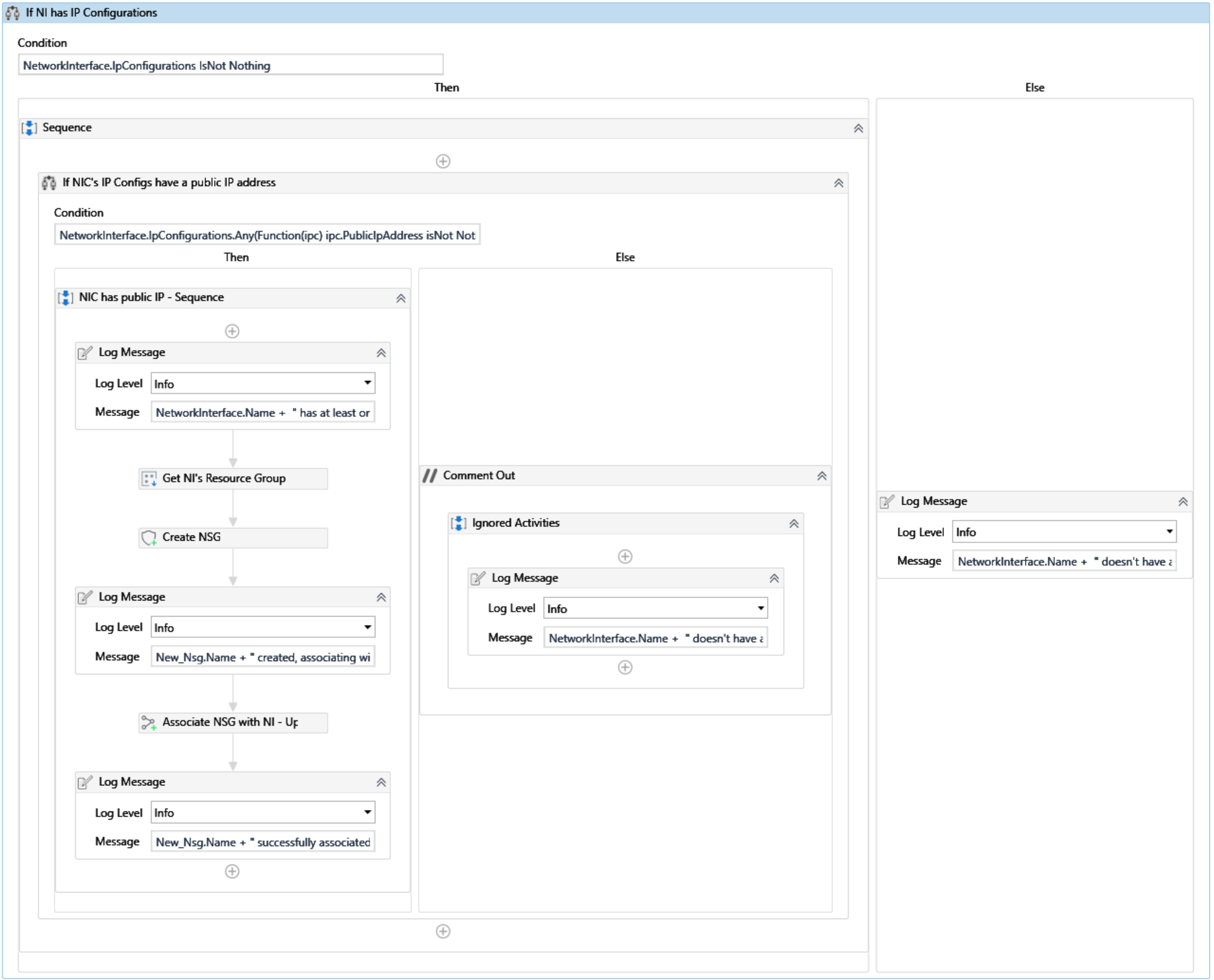
0.00
BUSINESS EXCEPTIONS

0.00
APPLICATION EXCEPTIONS

7.04
SUCCESSFUL TRANSACTIONS

TRANSACTIONS FEBRUARY 26 - MARCH 26

Create NSGs for NIs without one



If NI has IP Configurations

Condition: NetworkInterface.IpConfigurations IsNot Nothing

Then

Sequence

If NIC's IP Configs have a public IP address

Condition: NetworkInterface.IpConfigurations.Any(Function(ipc) ipc.PublicIpAddress isNot Not

Then

NIC has public IP - Sequence

Log Message
Log Level: Info
Message: NetworkInterface.Name + " has at least or

Get NI's Resource Group

Create NSG

Log Message
Log Level: Info
Message: New_Nsg.Name + " created, associating wi

Associate NSG with NI - Up

Log Message
Log Level: Info
Message: New_Nsg.Name + " successfully associated

Else

Comment Out

Ignored Activities

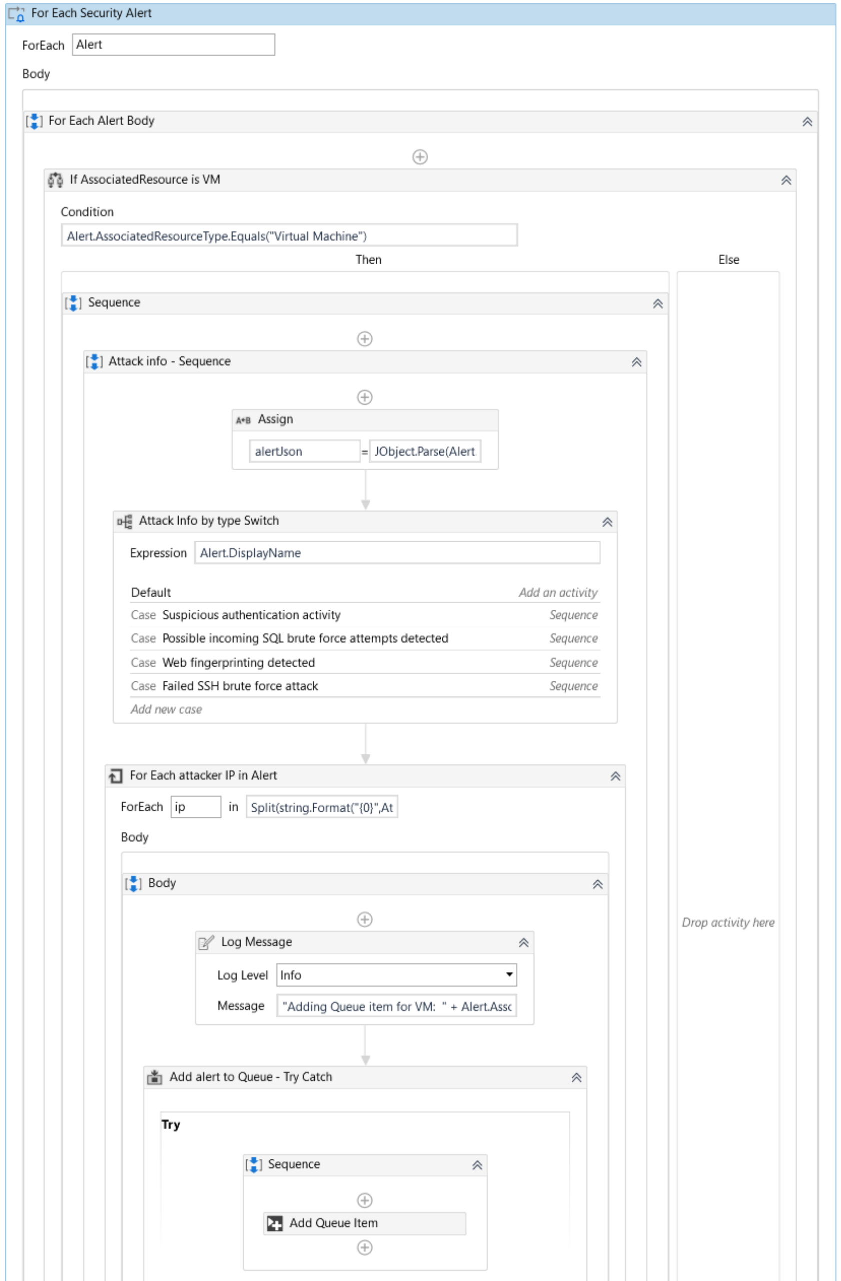
Log Message
Log Level: Info
Message: NetworkInterface.Name + " doesn't have a

Else

Log Message
Log Level: Info
Message: NetworkInterface.Name + " doesn't have a

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



For Each Security Alert

ForEach Alert

Body

For Each Alert Body

If AssociatedResource is VM

Condition

Alert.AssociatedResourceType.Equals("Virtual Machine")

Then

Else

Sequence

Attack info - Sequence

Assign

alertJson = JObject.Parse(Alert

Attack Info by type Switch

Expression Alert.DisplayName

Default	Add an activity
Case Suspicious authentication activity	Sequence
Case Possible incoming SQL brute force attempts detected	Sequence
Case Web fingerprinting detected	Sequence
Case Failed SSH brute force attack	Sequence
Add new case	

For Each attacker IP in Alert

ForEach ip in Split(string.Format("{0}",At

Body

Body

Log Message

Log Level Info

Message "Adding Queue item for VM: " + Alert.Assc

Add alert to Queue - Try Catch

Try

Sequence

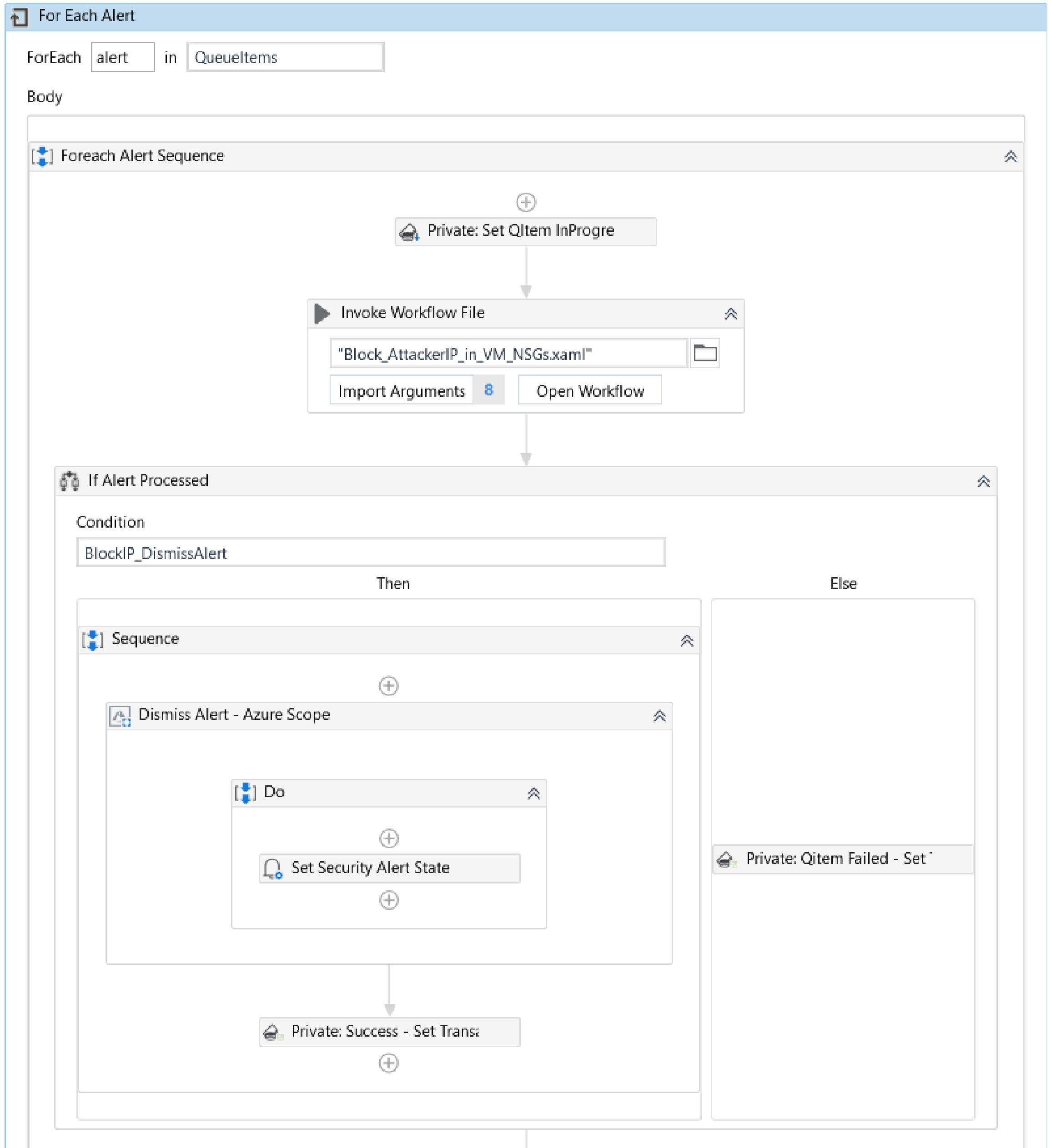
Add Queue Item

Drop activity here

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



ForEach alert in QueueItems

"Block_AttackerIP_in_VM_NSGs.xaml"

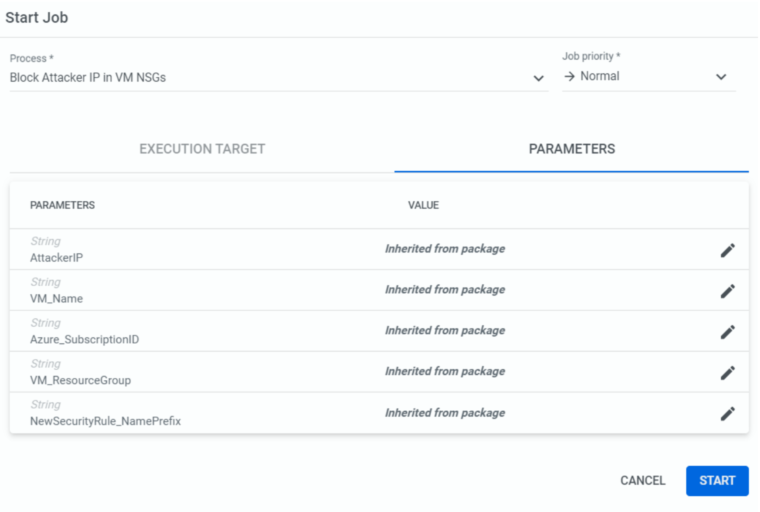
Condition
BlockIP_DismissAlert

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

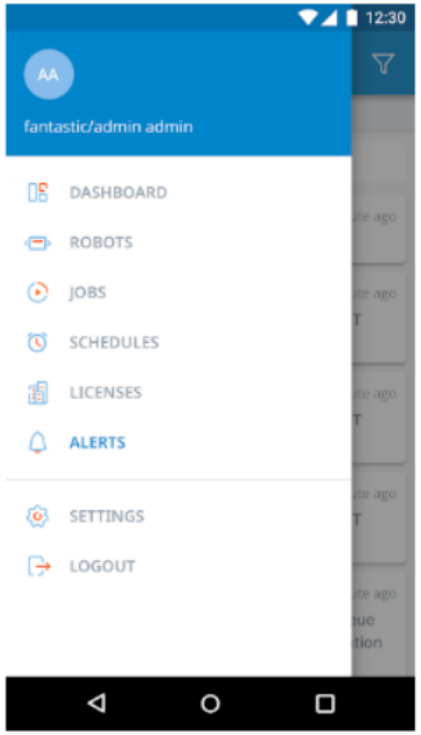
Process *
Block Attacker IP in VM NSGs

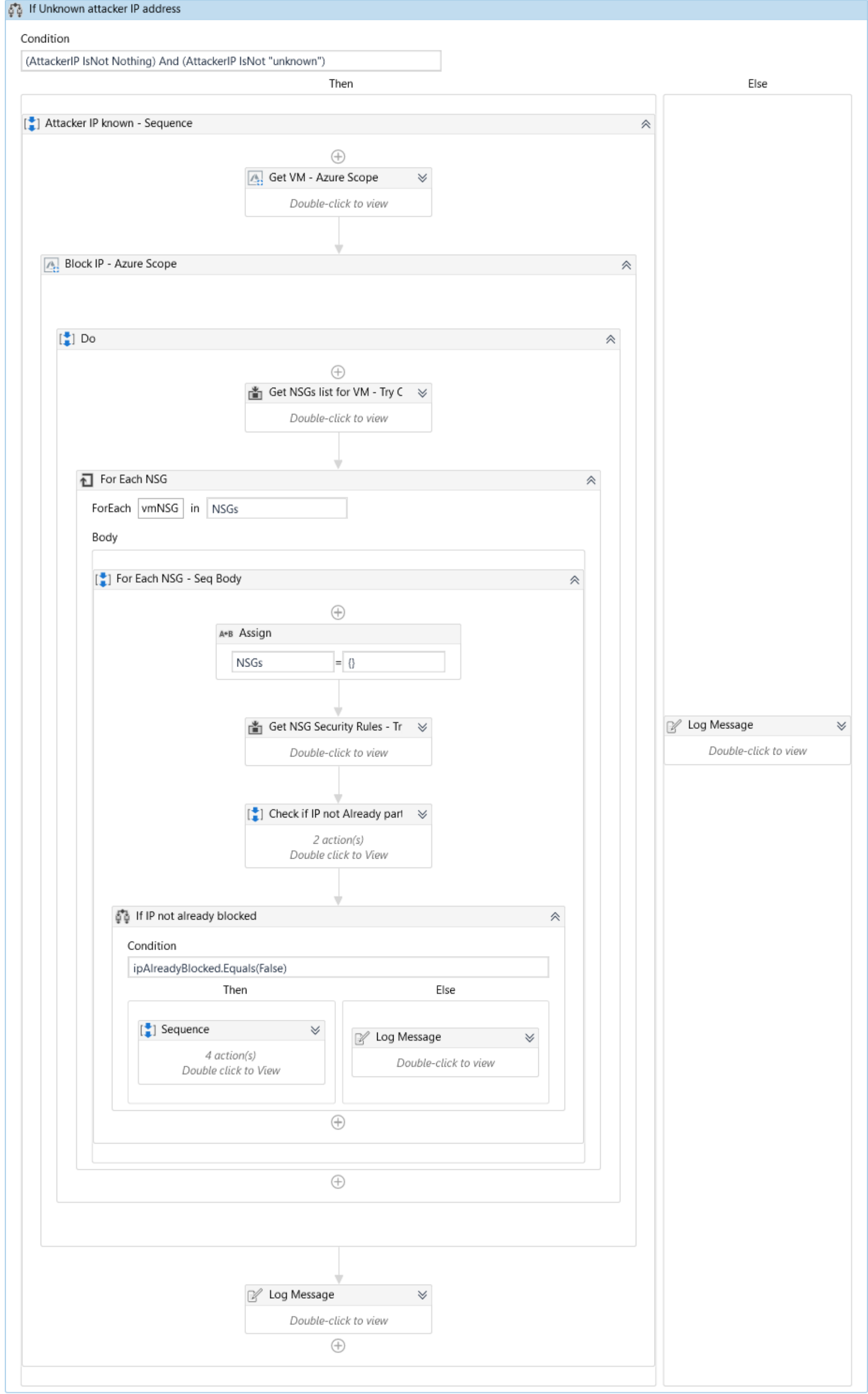
Job priority *
→ Normal

EXECUTION TARGET | PARAMETERS

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





If Unknown attacker IP address

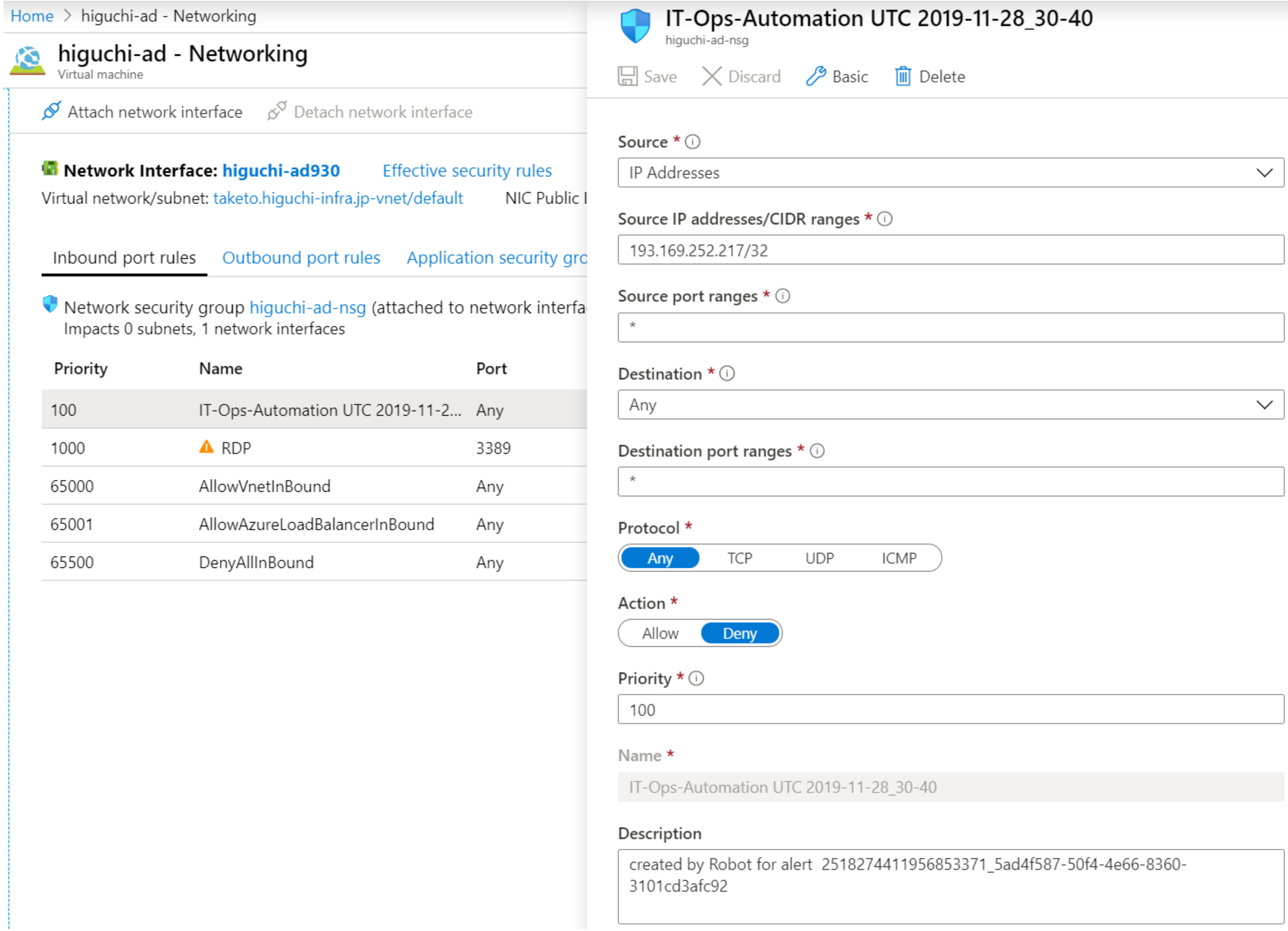
Condition: (AttackerIP IsNot Nothing) And (AttackerIP IsNot "unknown")

ForEach vmNSG in NSGs

Assign: NSGs = {}

Condition: ipAlreadyBlocked.Equals(False)

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

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

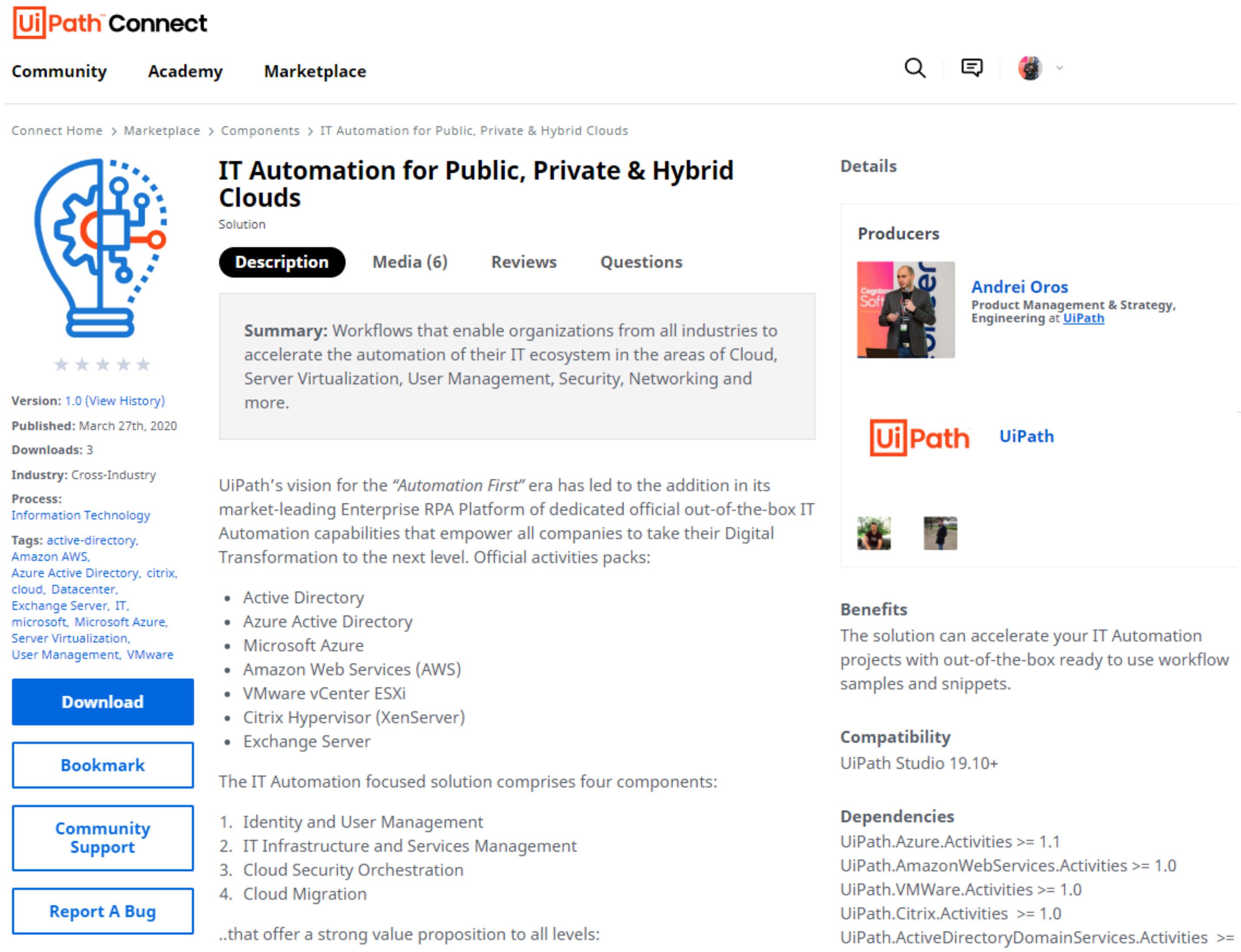
Action *
Allow [✓ Deny]

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



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

IT Automation for Public, Private & Hybrid Clouds

Solution

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:

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

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

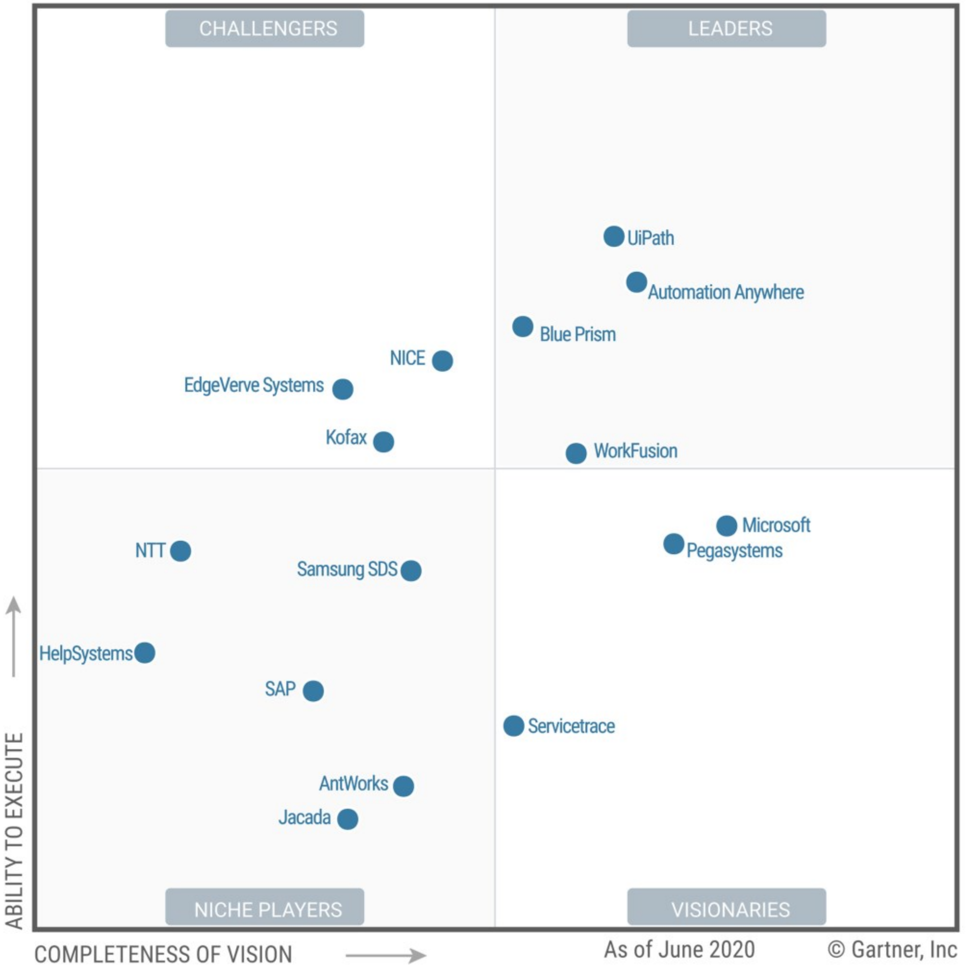
UiPath™

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."**

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.

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

A Forrester Wave Leader

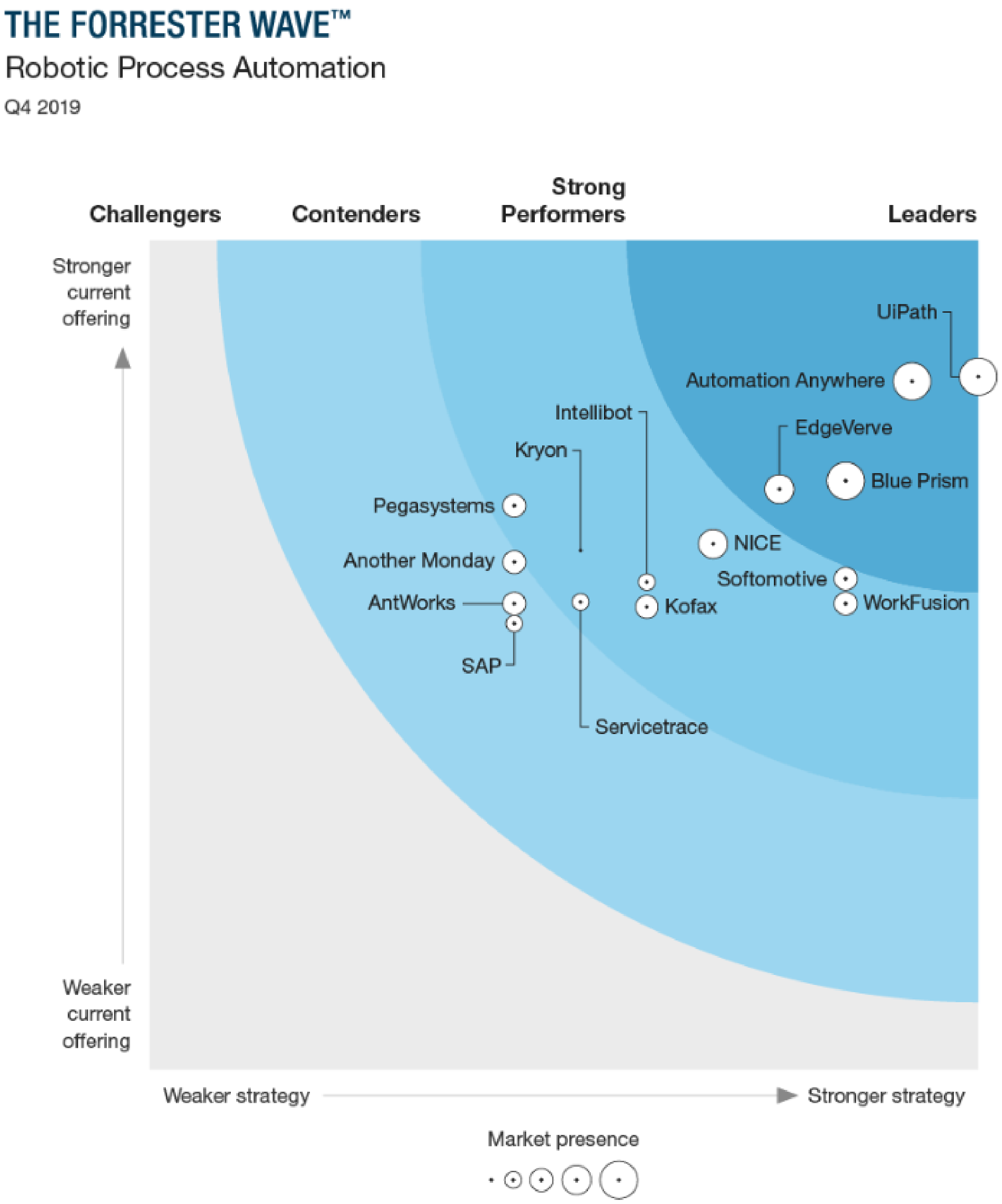
Highest Scores in Current Offering, and Highest Possible Scores in Strategy and Market Presence

“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

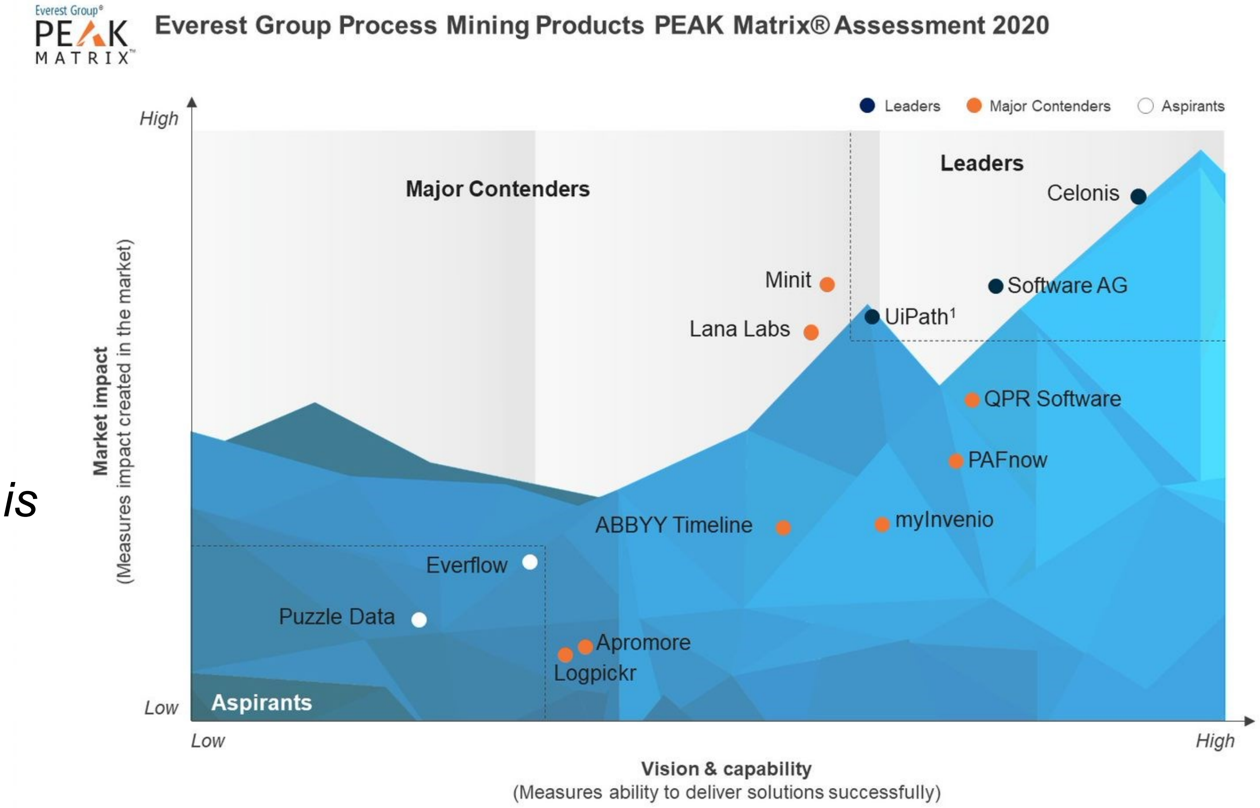


A Process Mining Leader

Everest Group PEAK Matrix® for Process Mining Technology Vendors 2020

Everest Group
PEAK MATRIX®
LEADER 2020
PROCESS MINING PRODUCTS

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



1 UiPath Process Mining (formerly ProcessGold)

Full report: https://www.uipath.com/hubfs/Reports/Everest_Group_PEAK_Matrix_for_Process_Mining_Products_2020_Focus_on_UiPath.pdf

UiPath™

Business Partner Ecosystem Spans Globally and Locally

Global	Americas	Japan	EMEA	India	Asia Pacific
accenture	Atos	CTC Challenging Tomorrow's Changes	Capgemini	Cognizant	Bb Blackbook.ai
EY	HURON	PERSOL パーソル プロセス＆テクノロジー	CGI	KGiSL	INNOVIOR
Cognizant	perspecta	accenture	sopra steria	NIIT	KDDI KDDI China
IBM	TATA CONSULTANCY SERVICES	iSiD IT Solution Innovator	itelligence NTT DATA Business Solutions	RPATech –automating intelligence–	posco
Deloitte.	Infosys®	TIS TIS INTEC Group	TATA CONSULTANCY SERVICES	Tech Mahindra	ncs making IT happen
pwc					
KPMG					

600+ business partners that help with the implementation of RPA

Thank you

andrei.oros@uipath.com

UiPath™