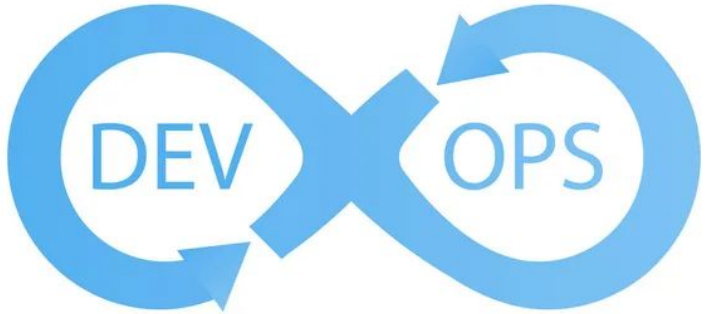

<no/code> automation
For IT Service Desk and Devops
ubility

They work with us

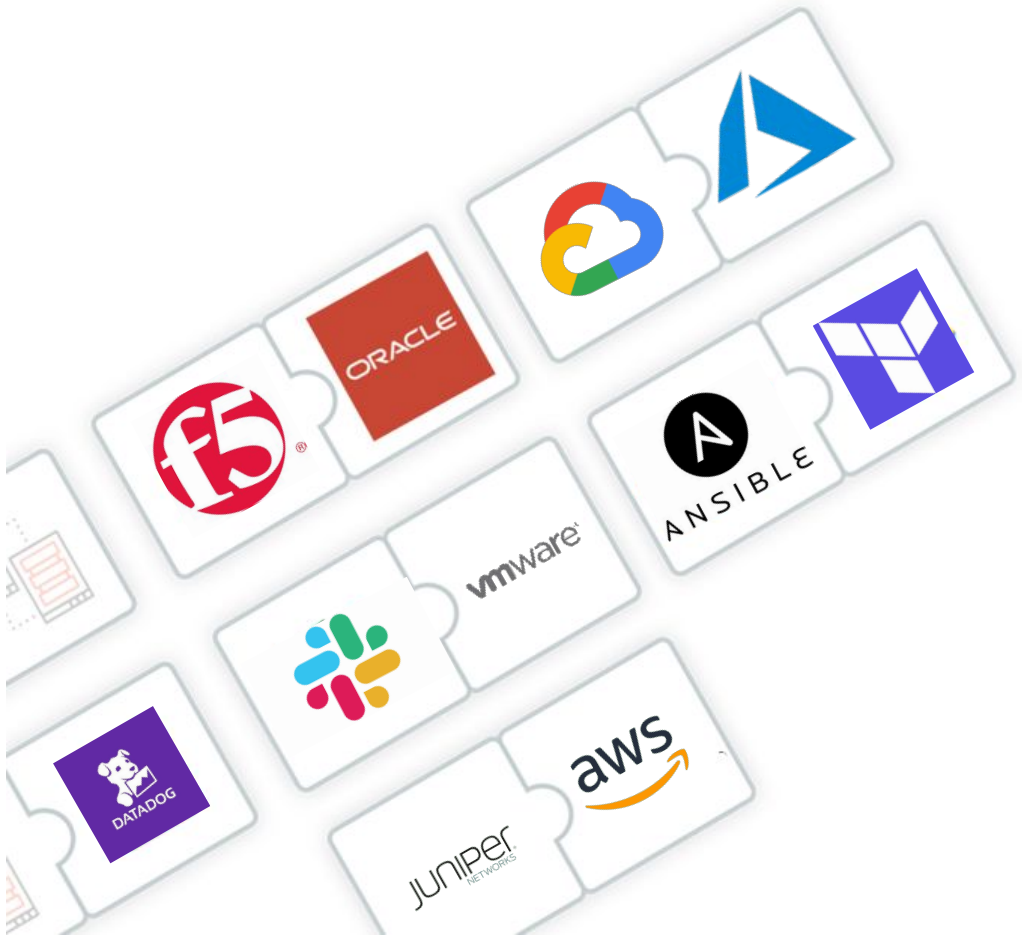
ubility

<no/code> automation – Two use cases

1
IT Service desk & ITOPS



2
DEVOPS & Site Reliability Engineers

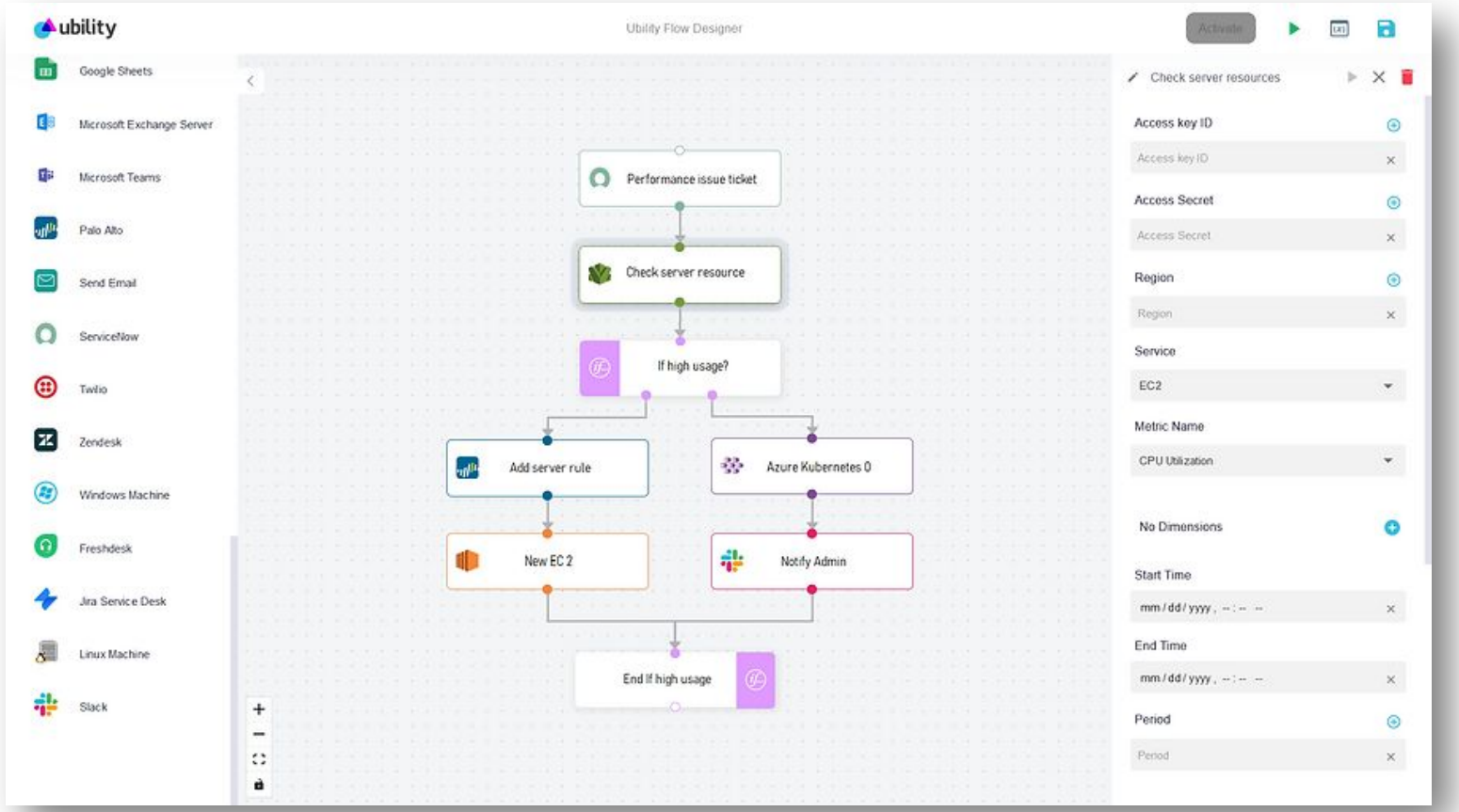


400+ connectors

Interconnect seamlessly and with <no/code> all your Cloud and Devops tools using 1 orchestrator and 1 environment

ubility

Drag and drop <no/code> interface



Build, deploy and iterate any automation flow in seconds using our drag and drop <no/code> interface

ubility

Use case 1
For Secops – Devops & SRE

Deploy automation in minutes and experience 70% faster remediation and 50% less incidents

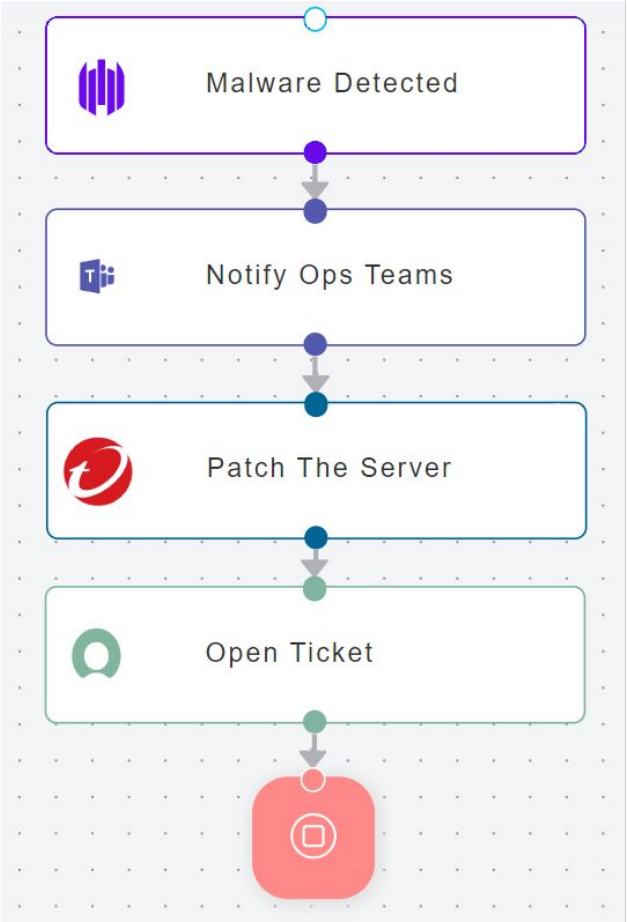
ubility

Security – Automatic Server Patching

Goal – Auto patch a server infected by a malware.

Security engineer configures an incident response flow using Ubility flow designer:

1. The flow is triggered when Sentinel one detects a malware on a specific server
2. The flow notifies using MS Teams the security operation engineer to request approval for patching the server.
3. If patching is approved, the flow triggers Trend Micro to patch the server
4. The flow then logs the operation in ServiceNow



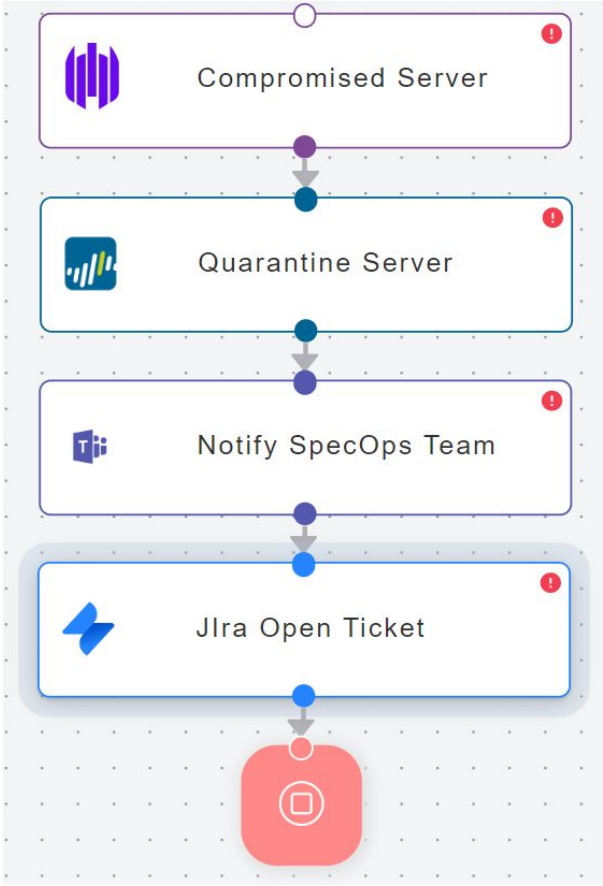
ubility

Security – Automatic Quarantine Server

Goal – Auto Quarantine a compromised Windows server .

Security engineer configures an incident response flow using Ubility flow designer:

1. The flow is triggered when Sentinel one detects that a server is compromised
2. The flow quarantine the server by moving it to a quarantined network on Palo Alto
3. Notify secops team on MS Teams
4. Raise a ticket on Jira



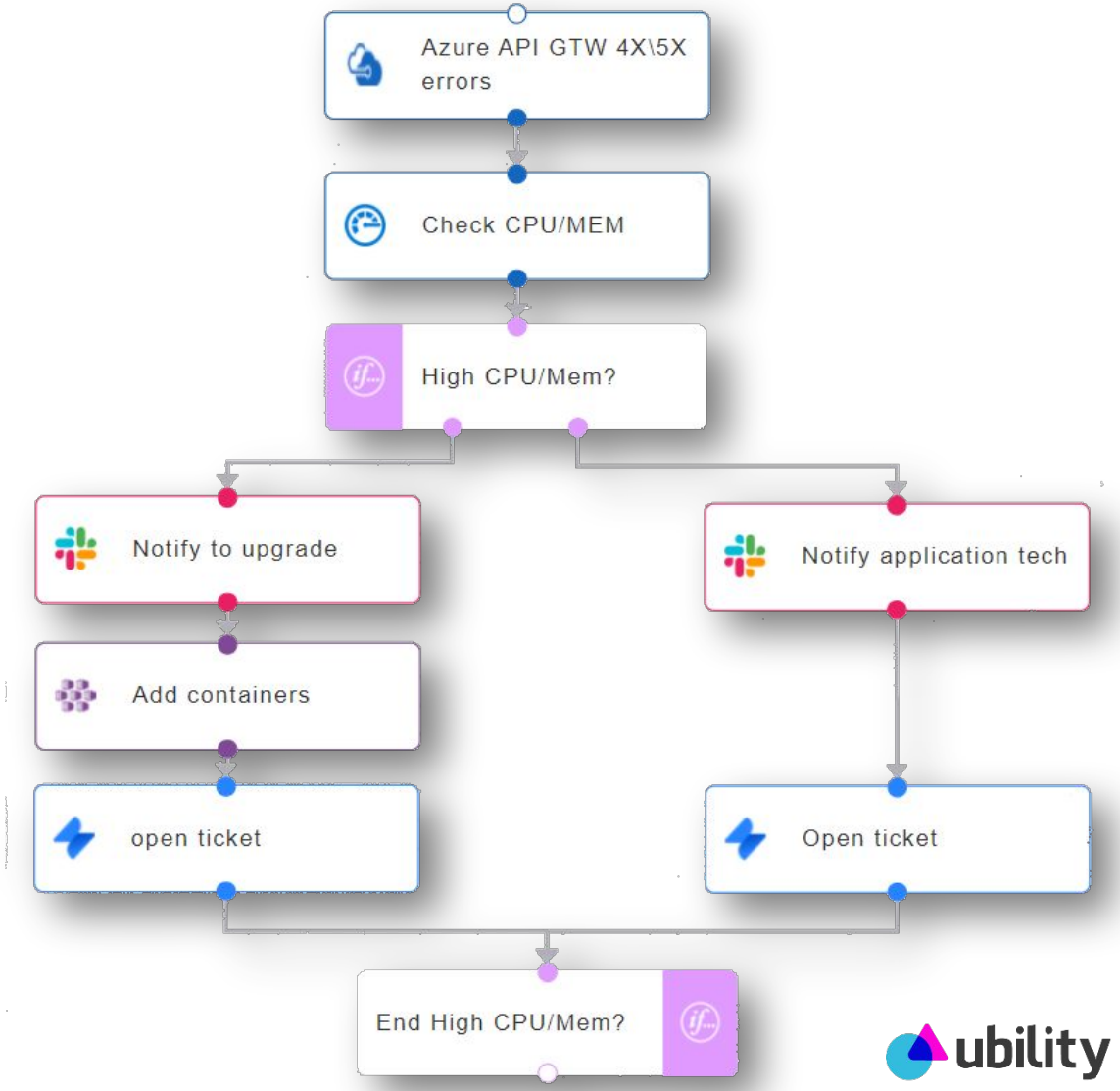
ubility

Automate Incident Response

Goal – Auto response to the performance degradation of an application deployed on Azure.

SRE configures an incident response flow using Ubility flow designer:

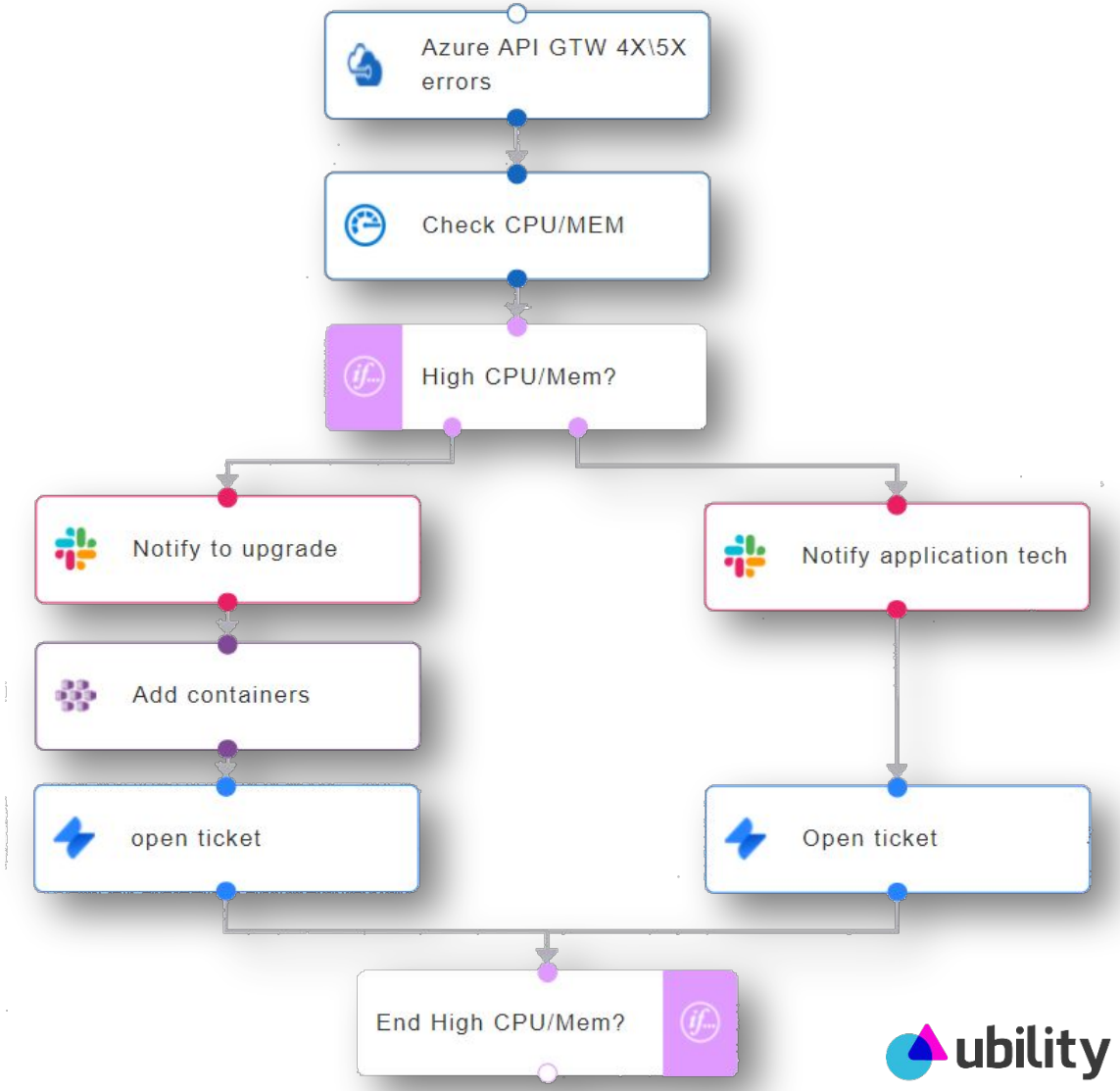
1. The flow is triggered when Azure Monitor raise an alarm of 4xx/5xx errors experienced by the application
2. The flow check automatically using Azure monitor the CPU and Memory of the server running the application



ubility

Automate Incident Response

3. If the CPU/Memory is high, notify through Slack the SRE engineer in charge of the performance issues
4. The notification encloses the detail information of the CPU/Memory asking the SRE to upgrade the Kubernetes cluster.
5. SRE clicks on the button of upgrade in the Slack message
6. The flow upgrade automatically AKS and open a ticket on Jira including all the details.



ubility

Automate Security Response

Goal – Auto quarantine malware infected VM

SRE configures a security response flow using Ubility flow designer:

1. The flow is triggered when AWS Cloudwatch raises an alarm reporting a malware detected on a EC2 VM
2. The flow locks the EC2 VM
3. The flow moves the VM to a Quarantine VPC
4. Notify through Slack the security team to start the investigation process

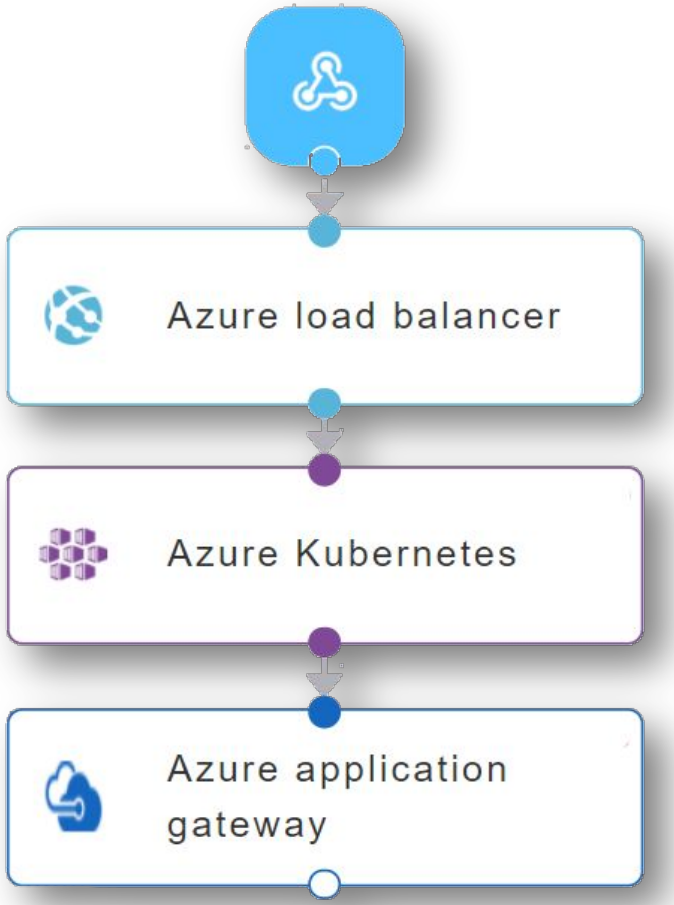
ubility

Infrastructure as <no/code>

Goal: Automatically deploy and configure an Azure cluster made of an Azure load balancer, AKS and an Azure APP GW

SRE configures au automation flow that:

1. Is triggered via a webhook (to be connected to Jira, Servicenow, etc.)
2. Launch and configure an Azure load balancer
3. Launch an AKS with the needed containers
4. Launch and configure an Azure Application gateway.



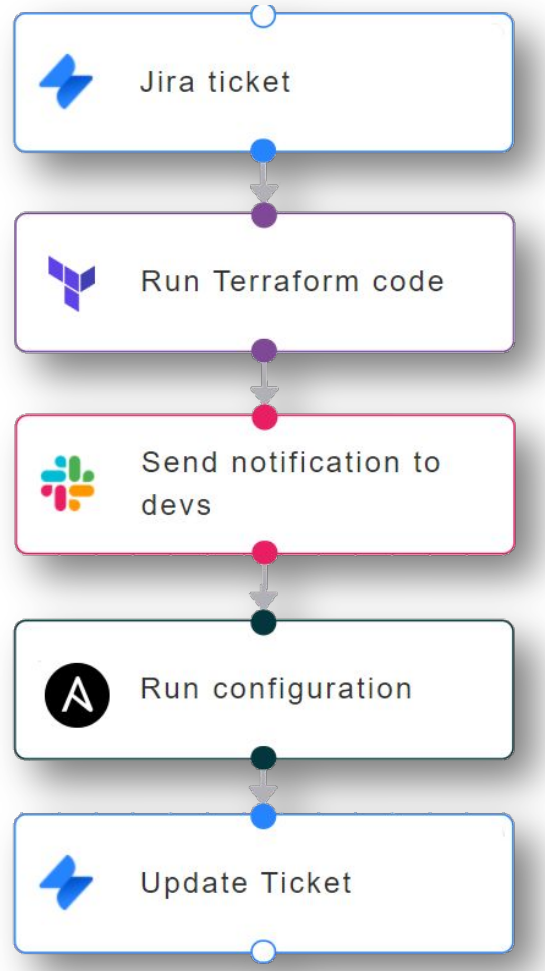
ubility

Interconnect & Leverage your existing automations

Goal: Interconnect seamlessly your automation scripts using our drag & drop interface

SRE creates a workflow that:

1. Run from Jira a Terraform code
2. Send notification to Slack when the code is successful
3. Use the Terraform result as input to Ansible configuration script
4. Update the Jira ticket when flow is ended



ubility

Use case 2
IT Service Desk & ITOPS

Automate and remediate 60% of your incident and service requests

ubility

How Abu Dhabi Islamic Bank is automating 80% of its IT service desk using our AI Platform

As one of the biggest banks in UAE, ADIB was looking for a platform to automate the IT support for his **8000+** employees.

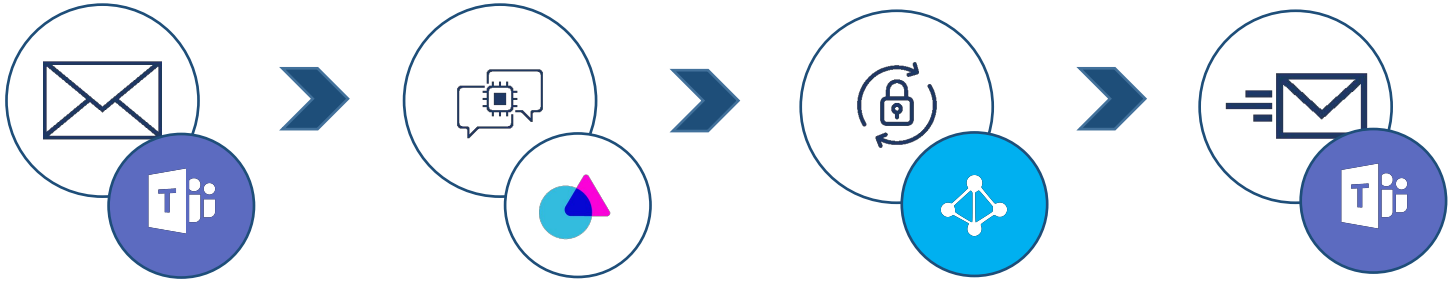
The platform should be able to

Solve IT issues without any human intervention

Rolling out new automations **quickly** and **easily**

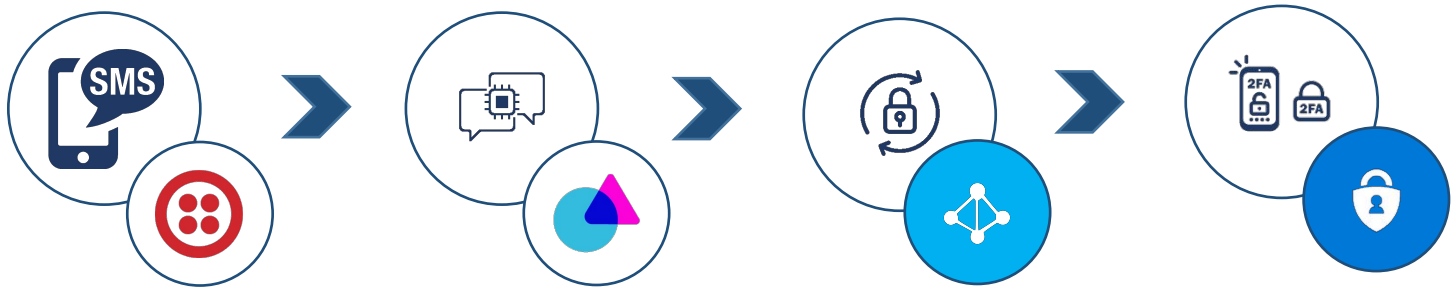
ubility

Unlock Password



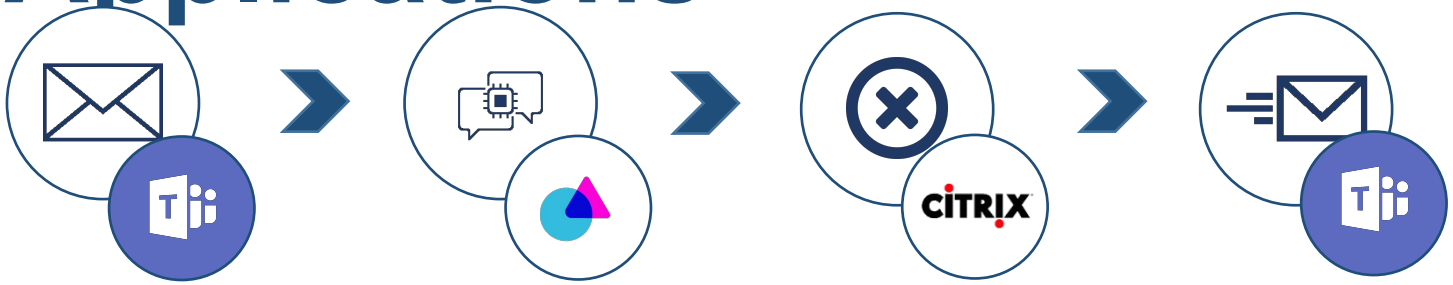
1. User sends a request through Microsoft Teams to unlock his password.
2. ***Ubibot NLP*** triggers ***UbiRPA*** unlock password automation process.
3. ***UbiRPA*** connects to Active Directory and unlock user's password.
4. The user get notified via Teams that his password was unlocked.

Password Reset



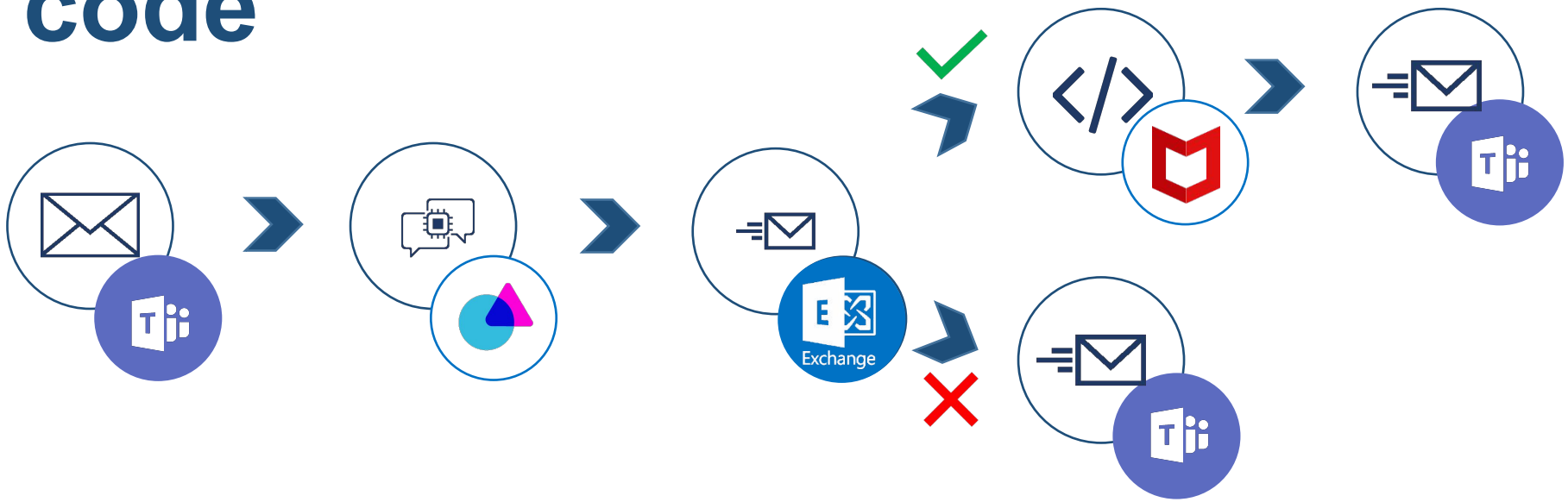
1. ***UbiRPA*** process connects to Twilio to receive password reset messages from employees registered phone numbers.
2. ***Ubibot*** NLP triggers reset password process.
3. ***UbiRPA*** connects to Azure Active Directory and initiate the Self Service Password Reset service.
4. The user is then notified through Microsoft Authenticator to perform a 2 factor authentication to complete the password reset process.

Citrix Stuck Applications



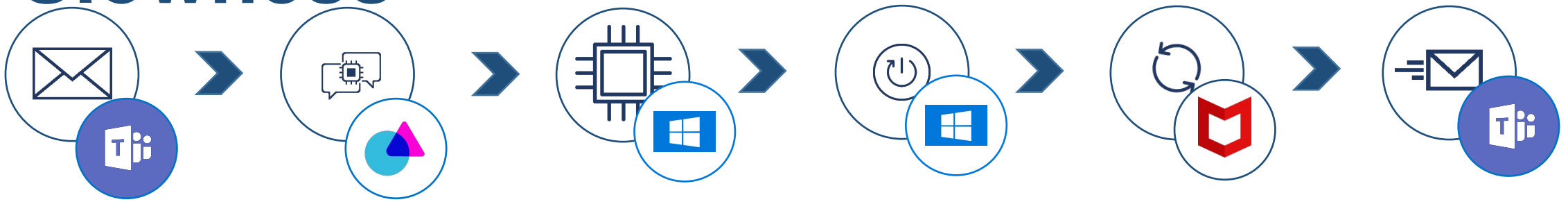
1. User getting his applications stuck in Citrix, sends a request through Microsoft Teams.
2. ***Ubibot*** NLP triggers the Citrix troubleshooting process on **UbiRPA**.
3. ***UbiRPA*** connects Citrix Director and log off all running application for the specific user.
4. The user is then notified through Teams to check is his issue is solved.

DLP release code



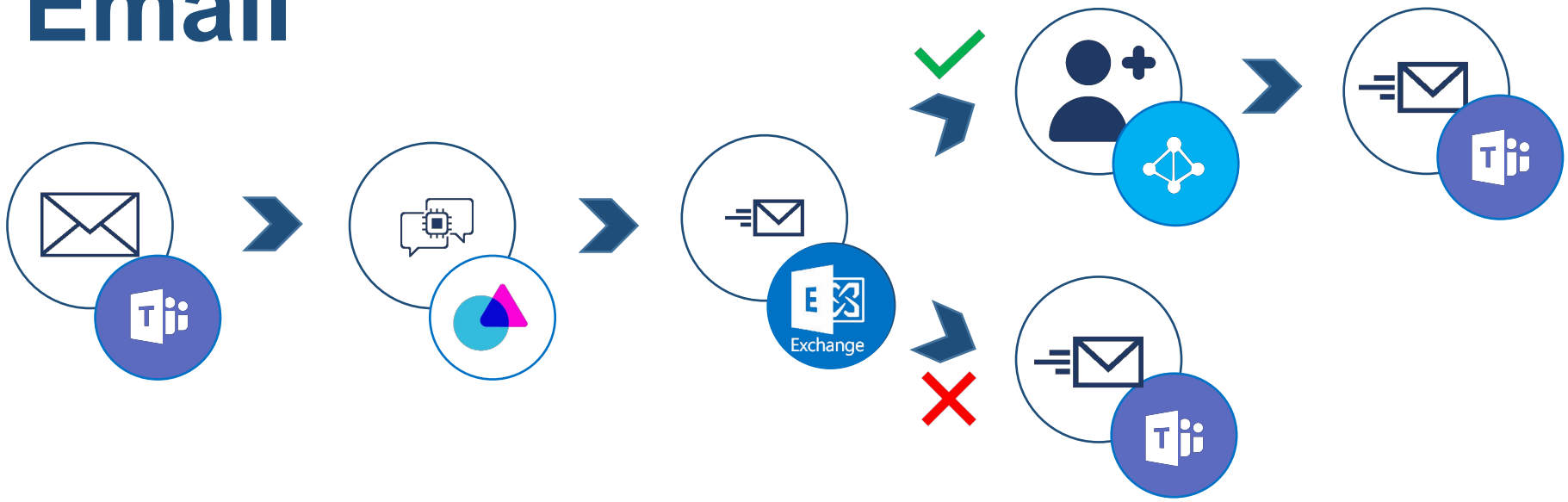
1. User sends a DLP release code through Microsoft Teams.
2. ***Ubibot*** NLP triggers the DLP release code process on **UbiRPA**.
3. ***UbiRPA*** sends an email to the user's manager requesting approval for DLP code.
4. If manager approves the request, ***UbiRPA*** connects to Mcaffe EPO and get a DLP code for the user.
5. DLP code shared with user via Teams.

PC Slowness



1. User experiencing slowness on his corporate PC, sends a request through Microsoft Teams.
2. ***Ubibot*** NLP triggers the PC slowness process on **UbiRPA**.
3. ***UbiRPA*** connects to PC and check the CPU & memory. If high, restart PC.
4. Otherwise run Mcafee antivirus automatically.
5. user informed via Teams.

Creating a Distribution Email



1. A request is sent from Teams for a new E-mail account to be created.
2. Ubibot NLP picks it up and requests manager approval via Email.
3. If accepted a distribution email is created on Exchange.