How is UiPath Automating Cybersecurity Operations?

As they plan for the upcoming year, chief information officers (CIOs) are prioritizing cybersecurity in order to protect their organizations from increasingly sophisticated threats.

Foundry's State of the CIO Study 2022 reports that “throughout the upcoming year, CIOs will focus their time and expertise on security management. 76% anticipate their involvement in cybersecurity to increase over the next year, and 51% say they are currently focused on security management in their role.” The increase in remote work capabilities and penetration of digital solutions during the pandemic have heaped more cybersecurity issues onto the plates of security teams.

Security professionals may currently use various artificial intelligence (AI) applications for IT operations (AIOps) and security operations (SecOps) tools to continuously improve the security posture of their organizations. But, those tools aren't enabling end-to-end security operations automation. On any given day, a cybersecurity engineer may spend a lot of time:

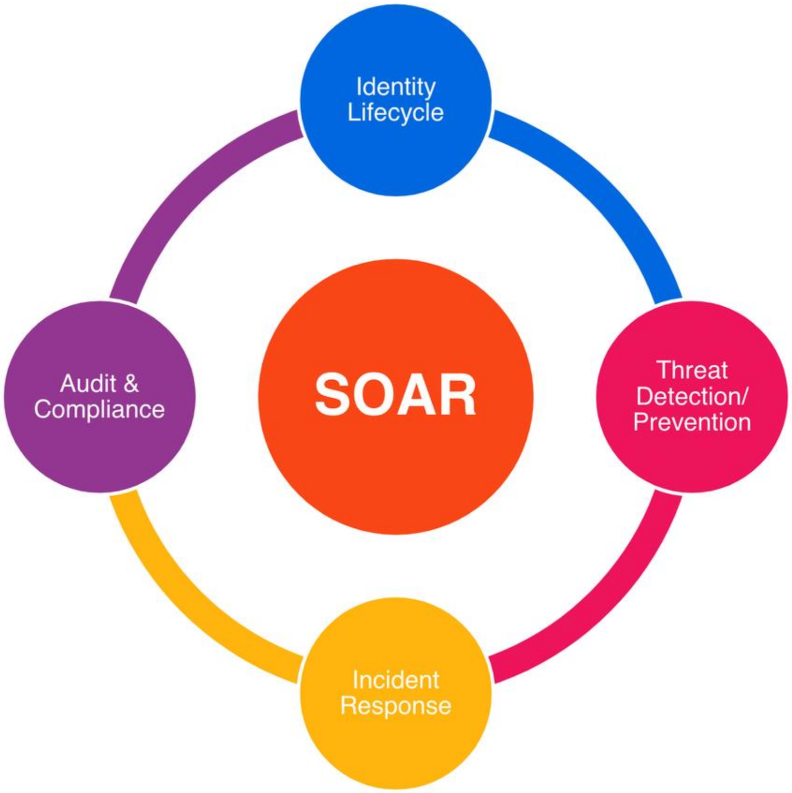
- Defining and enforcing security rules and policies for all areas of the infrastructure/environment
- Scanning for threats, monitoring vulnerabilities, and mitigating attacks
- Performing continuous security audits and tracking access control to critical resources

Alert fatigue continues to be a problem

A team can only handle so many alerts before they start to get missed.

One survey found that “more than one-third of IT security managers and security analysts ignore threat alerts when the queue is full.”

Through IT automation activities, UiPath provides easy-to-use, vendor-agnostic, robust security operations capabilities. This article will explain these capabilities and how they’re enabling full-scale security orchestration, automation, and response (SOAR).

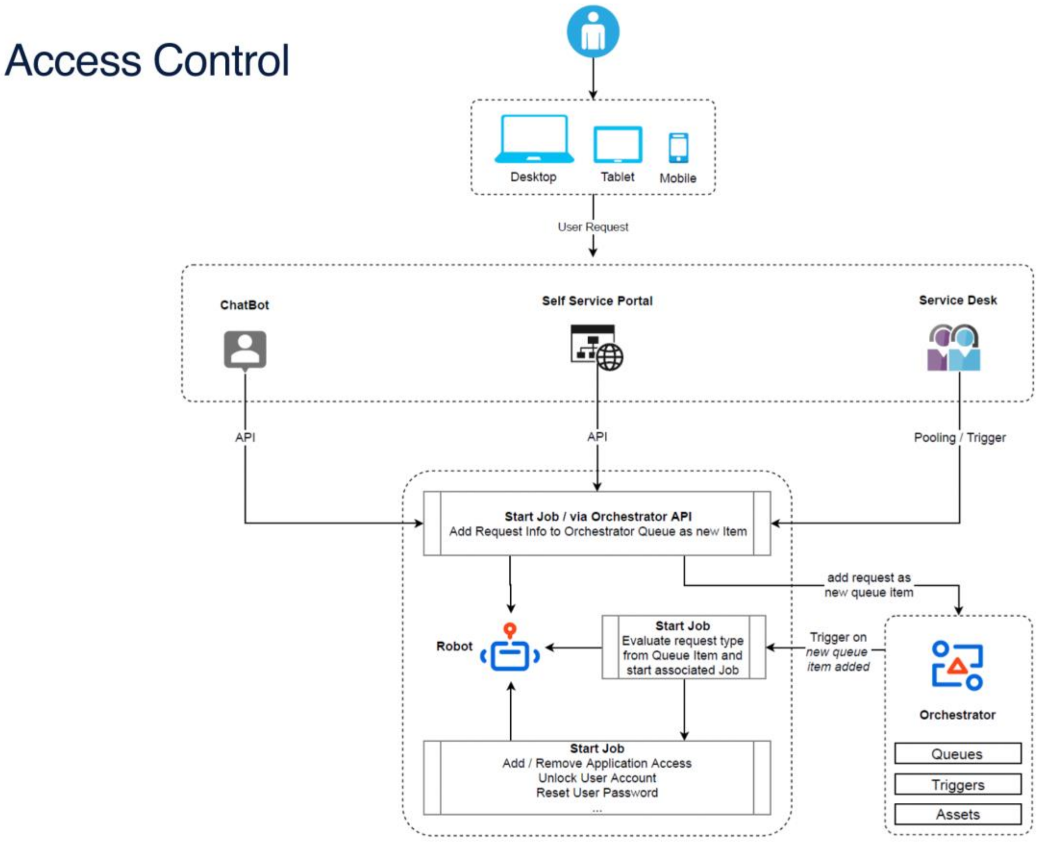


Identity lifecycle

Within most companies, IT analysts manage user profiles, roles, and employee access controls. Some of their activities may include user provisioning, adding/removing application access, resetting user passwords, and unlocking user accounts.

UiPath has user interface (UI) automation and API integration with major identity access management (IAM) tools, such as Microsoft Azure AD, to automate identity management activities like the ones described above.

Combined with UI and API capabilities expanding to the service management area, a UiPath Robot can also monitor IT service management (ITSM) tickets. The robot can start jobs based on the defined trigger, perform necessary user management actions, update the ITSM ticket, and inform the user about the resolution.


Access Control
Desktop
Tablet
Mobile
User Request
ChatBot
Self Service Portal
Service Desk
API
API
Pooling / Trigger
Start Job / via Orchestrator API
Add Request Info to Orchestrator Queue as new Item
add request as new queue item
Robot
Start Job
Evaluate request type from Queue Item and start associated Job
Trigger on new queue item added
Orchestrator
Start Job
Add / Remove Application Access
Unlock User Account
Reset User Password
...
Queues
Triggers
Assets

Threat detection and prevention

Another key focus for security professionals is detection and prevention activities. Per a recent IBM study, “organizations with a ‘fully deployed’ security automation strategy had an average breach cost of $2.90 million – whereas those with no automation experienced more than double that cost at $6.71 million.”

UiPath extends the security automation capabilities of existing security operation tools. Using event-driven automation capabilities, a UiPath Robot can be triggered from the endpoint detection and response (EDR), extended detection and response (XDR), security information and event management (SIEM), or other security monitoring tools to perform remediation actions.

As security monitoring tools identify an indicator of compromise (IoC), the tools may not have the ability to perform actions on network systems such as firewalls due to missing API integration or routing issues. In these cases, the security analyst needs to manually perform actions such as blocking IP addresses in firewall systems.

Similarly, security analyzers may perform firewall rules assessments but not be able to disable or delete firewall or network address translation (NAT) rules and NAT objects. A UiPath Robot can perform these manual actions using UI and API capabilities for any product due to our vendor-agnostic automation abilities.

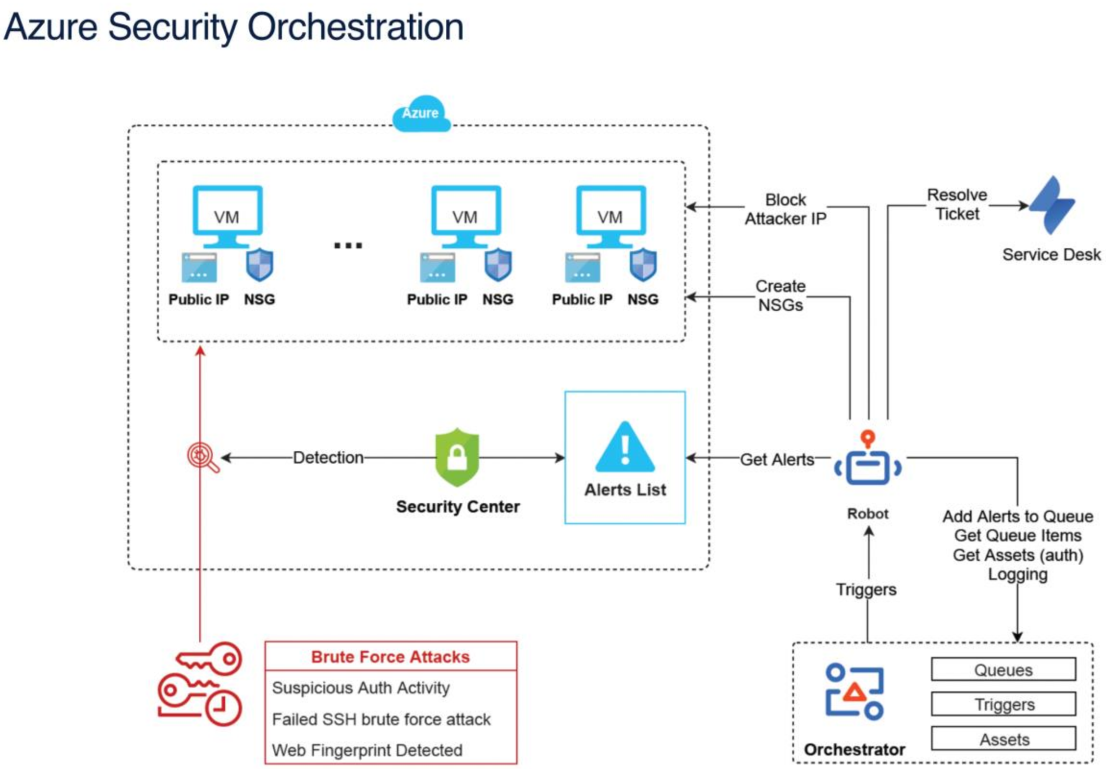
What about email phishing?

Our robots can automatically quarantine email threads and trigger remediation actions. Some of the threat detection and prevention areas that can be automated using UiPath are:

- Detection controls
- Potential threat triage
- Automated remediation

- Vulnerability management
- Endpoint protection

We’re using such automations internally to manage brute force attack alerts generated from sources like Azure Security Orchestration. We're also blocking more than 20,000 brute force attacks every year using our own automations.

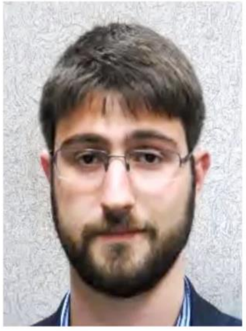


Azure Security Orchestration

UiPath can help automate processes that touch multiple systems. For example, in the demo video below, UiPath opens tickets for top system vulnerabilities. The robot utilizes four enterprise systems—Tableau, Tenable, ServiceNow, and SharePoint—to complete the process.

Cyber Top 100

Lewis Bell
Pre-Sales Engineer



Incident response

Even the best organizational tools that detect and prevent security threats aren't foolproof. Security incidents happen frequently, and incident response management is the true test of a security team's robustness.

Timing is of the essence in case of any breach. The aforementioned IBM study validates that investments in incident response activities reduce breach costs, saying “companies with an incident response team that also tested their incident response plan had an average breach cost of $3.25 million, while those that had neither in place experienced an average cost of $5.71 million (representing a 54.9% difference.)”

Here are some activities that your security team can automate as part of incident response:

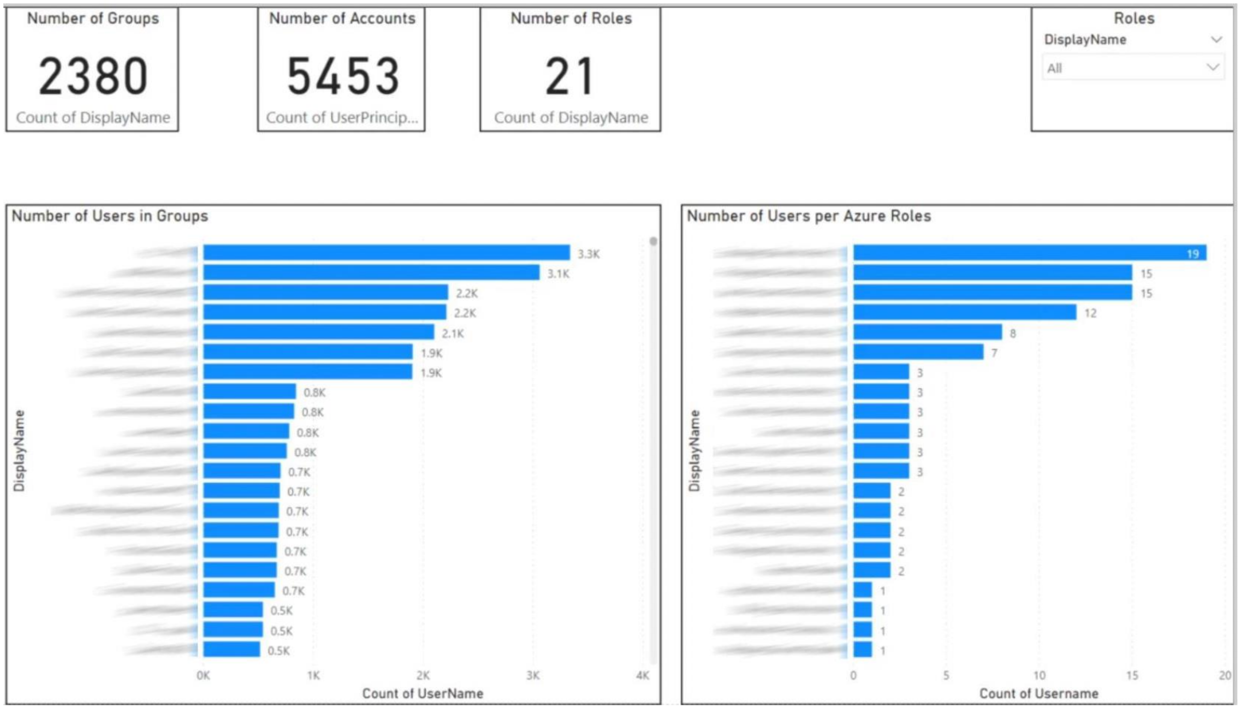
- Delete or quarantine suspicious malware-infected files
- Perform a geolocation lookup on a given IP address
- Search for files on a particular endpoint
- Block a URL on perimeter devices
- Quarantine a device from the network
- Retrieve information about any compromised users

These activities help accelerate remediation as well as standardize incident response processes.

Audit and compliance

All organizations must perform various audits and ensure compliance against industry standards such as SOX, HIPAA, and GDPR. As part of an audit, teams need to collect evidence, map information, and perform controls testing and assessment. You can automate many of these activities, especially related to IT general control, by:

- Pulling a list of all AD users by groups, role memberships, and resource ownerships
- Validating separation of duties across application development and deployment processes



We don't just help with audits—our robots can also monitor compliance needs. Instead of waiting until annual auditing activities, robots can proactively stop any control failures and alert respective managers.

UiPath Robot can automatically notify you in case of any compliance violations. For example, usage of health information that could identify a person (known as protected healthcare information), is not permitted or authorized under the privacy rule of HIPAA compliance. This reduces the risk of simple errors or oversights derailing compliance efforts.

UiPath automation platform also helps with internal reporting mechanisms. Stakeholders can gather necessary information, generate comprehensive reports, and disseminate those documents to appropriate parties quicker and easier than before.

We're using robots internally for SOX compliance testing and evidence collections through multiple automations, including over 2,000 license reconciliations. We're also providing audit evidence to assess the completeness, accuracy, and existence of the more than 1,000 invoices recorded in our NetSuite system.