RAPID7 | insightConnect

PLAYBOOK

Security Orchestration and Automation Playbook

| Your practical guide to implementing a SOAR solution

TABLE OF CONTENTS

Introduction

Security orchestration and automation helps teams improve their security posture and create efficiency—without sacrificing control of important security and IT processes. This playbook highlights some of the most common use cases for security orchestration and automation, as well as useful tips on how to get started.

Getting Started with Automation

Before you look for a security orchestration and automation solution, a good place to start is defining the pain points your organization needs to solve. Consider the following:

- Does your security team get too many alerts to handle effectively and in a timely fashion?
- Is your team suffering from symptoms of burnout?
- Do you have trouble hiring and/or retaining security talent?
- Does your team spend an inordinate amount of time gathering and analyzing information?
- Is your mean time to respond to a threat getting worse?

Next, it's important to define your most common use cases, or the tasks your team members spend a lot of time completing. For example, some companies would see immediate benefits by automating the handling of malware incidents because it's the biggest problem area for them. Other companies would benefit by orchestrating threat hunting and data enrichment tasks to better manage an increasing volume of threats and provide more actionable context to the analysts.

Knowing which use cases you can solve for with orchestration and automation—and then prioritizing those that can bring immediate value—will help you narrow down to find the right solution for your fastest time to value. Read on to learn about the most common automation use cases and workflows.

COMMON AUTOMATION USE CASE

Phishing Investigations

Phishing remains the most common attack vector behind successful breaches. However, investigating phishing emails involves time-consuming, manual tasks such as investigating and detonating attachments, checking URLs, or following up on suspicious requests for sensitive information. Orchestration and automation solutions can execute tasks like these behind the scenes while your team works on the rest of your investigation and response, ensuring the situation is handled effectively and efficiently while accelerating response time. Outside of the investigations, you can also build workflows to automate remediation steps for when a phishing email is identified.

- **Scan attachments and URLs**

  Use plugins for safe browsing, sandboxes, and more to contain and investigate suspicious attachments and check suspicious URLs.

- **Workflows to identify threats**

  Leverage workflows to analyze email URLs and file attachments using multiple intelligence sources. Add steps to output reports detailing each indicator identified.

> **According to the Verizon Data Breach Digest, phishing attacks play a role in 92% of security breaches.**

- **Designate decision points**

  After the routine scans and investigations have occurred, configure workflows to trigger a decision point on how best to proceed. Examples include marking as verified phish, automatically posting a message alerting others in your organization to the phishing threat via Slack, and other actions.

SAMPLE WORKFLOW

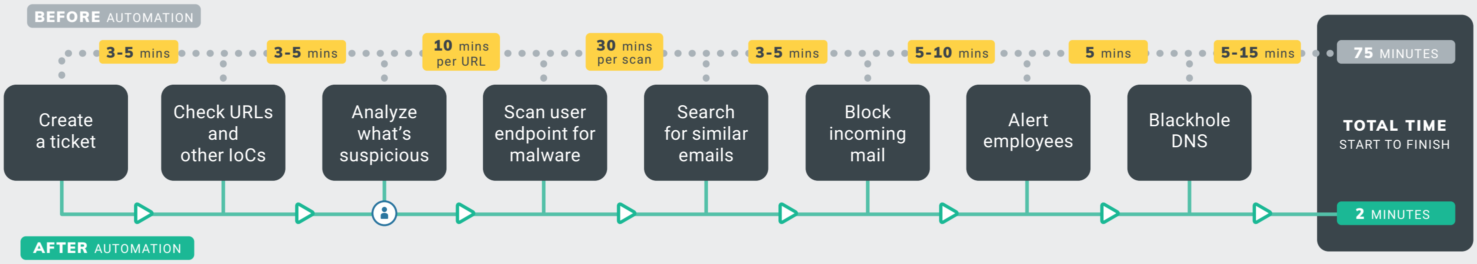
Phishing Investigations

Legend

Before Automation ••••••••••••▶

After Automation ——————▷

Human Decision ⓘ



COMMON AUTOMATION USE CASE

Provisioning and Deprovisioning Users

User permission management is a critical process that all organizations should be able to complete quickly and effectively in order to respond to security threats. The unfortunate reality is that most companies can't keep up. Security orchestration and automation can eliminate the burden of manually managing user accounts in a variety of use cases, from provisioning and deprovisioning users, to remediation in the event of an incident.

- **Provisioning new accounts**

  Different employees require different access levels to various tools and systems within your organization. Easily orchestrate tools such as Okta or Active Directory together, and kick off automation regarding designated user accounts.

- **Deprovisioning departing employees**

  No matter the reason why an employee is leaving, it's a security best practice to remove access to their account as quickly as possible. When an employee leaves, security and IT teams can immediately deactivate the account via a single automated workflow.

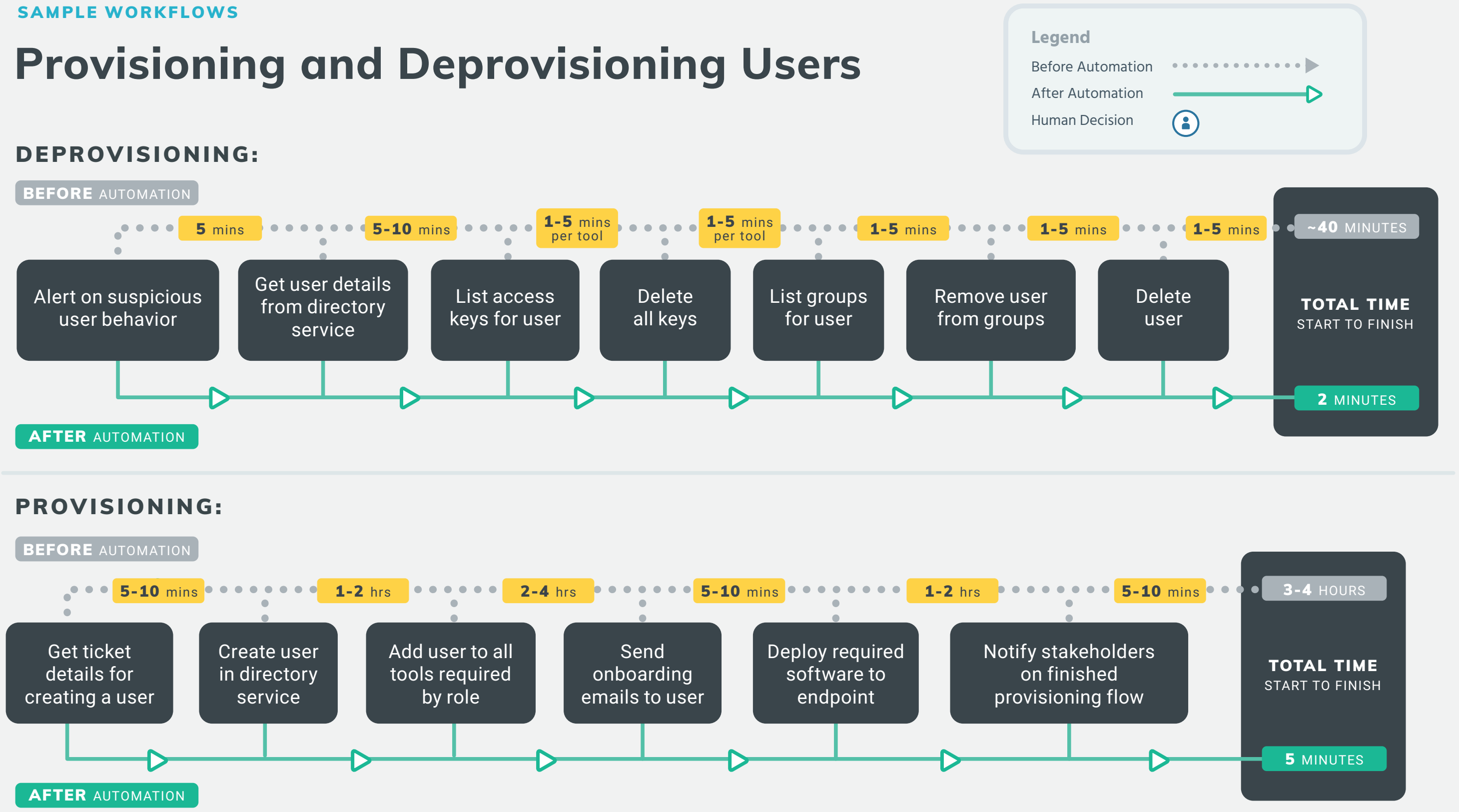
- **Shutting the [access] doors**

  User accounts are commonly exploited in phishing attacks. In the event of an incident, automatically deprovision affected user accounts, remove user access from key systems, and revoke permissions as needed until the threat is contained.

POPULAR PLUG-INS: AWS IAM, AD/LDAP, Okta, Duo, JIRA, GitHub, Workday

SAMPLE WORKFLOWS

Provisioning and Deprovisioning Users



Legend

Before Automation ••••••••▶

After Automation ——▷

Human Decision 👤

DEPROVISIONING:

BEFORE AUTOMATION

Alert on suspicious user behavior → 5 mins → Get user details from directory service → 5-10 mins → List access keys for user → 1-5 mins per tool → Delete all keys → 1-5 mins per tool → List groups for user → 1-5 mins → Remove user from groups → 1-5 mins → Delete user → 1-5 mins → ~40 MINUTES

AFTER AUTOMATION → 2 MINUTES

TOTAL TIME START TO FINISH

PROVISIONING:

BEFORE AUTOMATION

Get ticket details for creating a user → 5-10 mins → Create user in directory service → 1-2 hrs → Add user to all tools required by role → 2-4 hrs → Send onboarding emails to user → 5-10 mins → Deploy required software to endpoint → 1-2 hrs → Notify stakeholders on finished provisioning flow → 5-10 mins → 3-4 HOURS

AFTER AUTOMATION → 5 MINUTES

TOTAL TIME START TO FINISH

COMMON AUTOMATION USE CASE

Malware Containment

Security teams are bogged down by an overabundance of ransomware, viruses, spyware, and more. Automate the investigation and containment of malware before it does significant damage to your network.

- **Identify malicious activity**

  When dealing with malware, it's important to know the signs to look for and how to stop malware in a timely manner to reduce the spread of infection. Automate processes to identify indicators like misspelled process names or abnormal log activity.

- **Investigate the threat**

  When malware is detected, leverage workflows to analyze it using plugins from today's leading malware analysis solutions and common sandbox tools, such as Cuckoo. You'll be able to investigate malicious files in a safe space, before they get into your network.

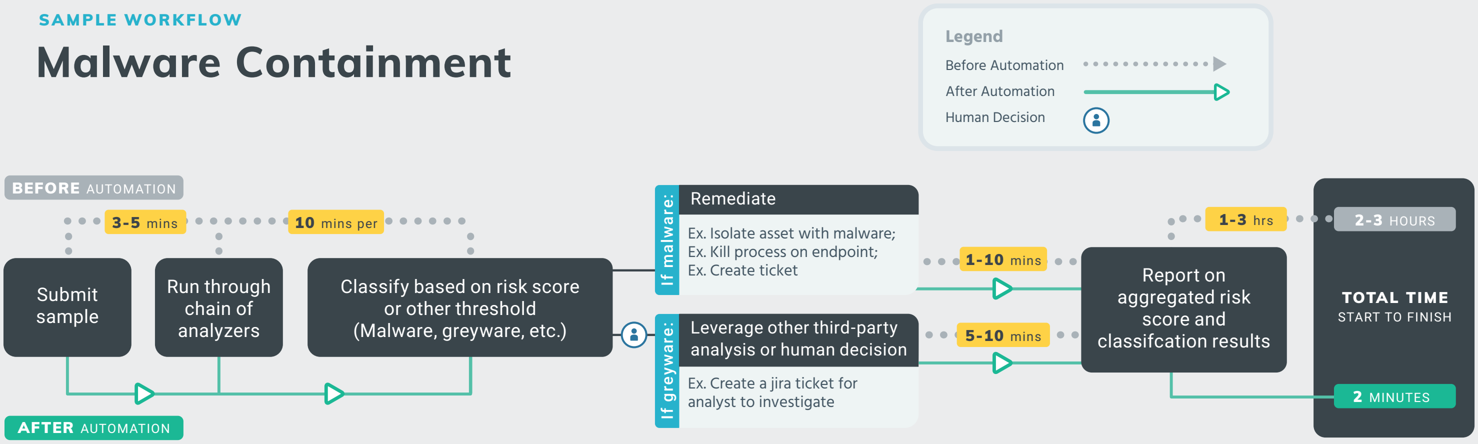
- **Containment and removal**

  All malware will require some type of containment/removal action. Leverage automation to identify the affected users and assets, leaving decision points for security practitioners to remove the necessary user accounts, isolate the malware, or disconnect machines from the network.

POPULAR PLUG-INS: VirusTotal, Hybrid Analysis, Cuckoo, Palo Alto Wildfire, VMRay, Cortex, JIRA

SAMPLE WORKFLOW

Malware Containment


Legend
Before Automation
After Automation
Human Decision
BEFORE AUTOMATION
3-5 mins
10 mins per
Submit sample
Run through chain of analyzers
Classify based on risk score or other threshold (Malware, greyware, etc.)
If malware:
Remediate
Ex. Isolate asset with malware;
Ex. Kill process on endpoint;
Ex. Create ticket
If greyware:
Leverage other third-party analysis or human decision
Ex. Create a jira ticket for analyst to investigate
1-10 mins
5-10 mins
Report on aggregated risk score and classifcation results
1-3 hrs
2-3 HOURS
TOTAL TIME
START TO FINISH
2 MINUTES
AFTER AUTOMATION

COMMON AUTOMATION USE CASE

Alert Enrichment

The SOC at an enterprise-level organization owns an average of 75 different security tools. Bouncing between tools when SIEM alerts roll in every day is mind-numbing work that disguises the value of Tier 1 analysts. Orchestration and automation solutions can help you accelerate detection by enriching the quality of the security alerts you receive and automatically weeding out many false positives, giving your team more time and greater context to tackle the actual threats.

- **Leave the heavy-lifting to the machines**

  Today's security teams are receiving an average of 12,000 security alerts per day. With your security tools automatically gathering and compiling relevant context about a security event, your team can switch their focus to analysis and response instead of spending exorbitant amounts of time manually collecting data.

- **Reduce the noise**

  Alert fatigue is real. Optimize your operations by automating your most repetitive tasks. The result? False positives are vetted out quicker and threats are dealt with faster through automation of enrichment tasks, investigation, and more.

> **44% of security alerts go uninvestigated due to the overwhelming amount of information received by security analysts.**
>
> Source: Cisco

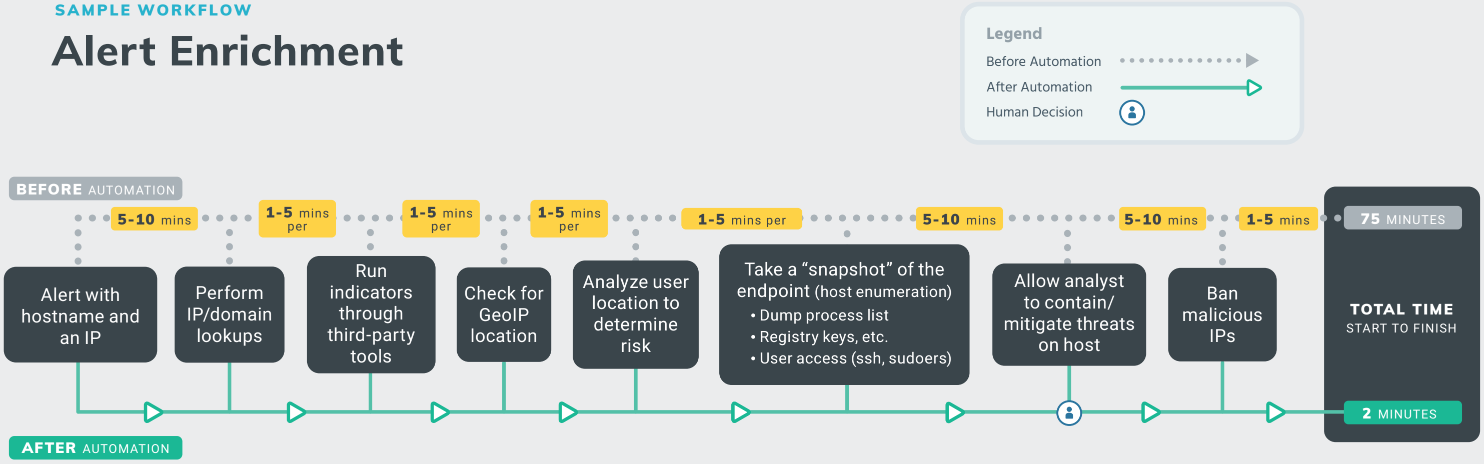
- **Intel to act efficiently**

  Automatically enrich your security alerts with important information, such as geo-IP lookups, domain analysis, malware detonation, and more. Orchestrate your favorite threat intelligence platforms, or use a variety of free and open source tools to ensure your team is equipped with the context they need to take action.

POPULAR PLUG-INS: WhoIS, AbuseIPDB, DomainTools, FreeGeoIP, GeoIP2 Precision, Snort Labs IP Reputation, Powershell, Python

SAMPLE WORKFLOW

Alert Enrichment



Legend
Before Automation
After Automation
Human Decision

BEFORE AUTOMATION

5-10 mins · 1-5 mins per · 1-5 mins per · 1-5 mins per · 1-5 mins per · 5-10 mins · 5-10 mins · 1-5 mins

Alert with hostname and an IP

Perform IP/domain lookups

Run indicators through third-party tools

Check for GeoIP location

Analyze user location to determine risk

Take a "snapshot" of the endpoint (host enumeration)
- Dump process list
- Registry keys, etc.
- User access (ssh, sudoers)

Allow analyst to contain/ mitigate threats on host

Ban malicious IPs

75 MINUTES

TOTAL TIME
START TO FINISH

2 MINUTES

AFTER AUTOMATION

COMMON AUTOMATION USE CASE

ChatOps: Distributed Alerting

For today's modern SOC, time is paramount when it comes to KPIs. Teams are always striving to reduce the time between security alert generation and resolution to a theoretical null. First popularized by the security team at Slack, a Distributed Alerting strategy avoids alert fatigue and staffing issues in the SOC by immediately bringing up alerts into the Slack instance of the person who generated it. Augmented with multi-factor authentication (MFA), analysts spend less time dealing with multiple alerts and more time triaging true positives due to a better signal-to-noise ratio.

- **Streamline business operations**

  Trigger actions to push comments to solutions like JIRA or Slack. With your security ecosystem set up to deliver alerts, incident notifications, and other data via your existing tools, security operations become more streamlined, collaborative, and efficient.

- **Two-way flow of information**

  Automation can deliver alerts that come in from your security tools straight into your chat applications and delegate tasks back to other connected tools, making communication and case management bi-directional.

- **Go mobile**

  Take your work on the go. ChatOps integrations allow your team to maintain maximum uptime without having to be physically present in the SOC to keep your organization safe.

SAMPLE WORKFLOW

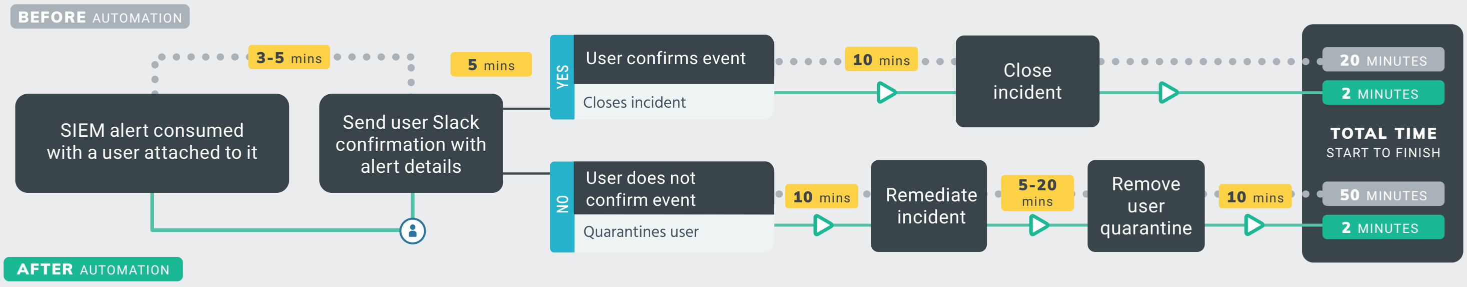
ChatOps: Distributed Alerting

Legend

Before Automation ⋯▷

After Automation —▷

Human Decision ⓘ



COMMON AUTOMATION USE CASE

Threat Hunting

Threat hunting is time consuming and demands a highly technical skill set that most organizations, for better or worse, have to consider a luxury. According to a recent SANS Institute study, only 31% of organizations have staff dedicated to hunting threats. But being proactive in this area can enable your analysts to better uncover and defend against complex advanced persistent threats (APTs)—the attacks that are almost guaranteed to succeed and that, with a massive dwell time, allow attackers to wreak widespread havoc. Lower the barrier to hunting and bolster your team's ability to compete with today's most-capable adversaries by automating processes around identifying suspicious malware, domain, and other indicators.

- **Operationalize disparate data sets**

  Hunting is not just time-intensive; it's also unbounded. The more data sets you are able to analyze, the more thorough your proactive search for compromise will be. With orchestration, you can easily add additional tools to your data set without adding substantial time to your hunt cycle.

- **Automate repeatable tasks**

  By automating the ongoing tasks associated with threat hunting, such as recurring scans, your team will have more time to do what they do best: finding and thwarting the bad guys. Bring team members into this process strategically for maximum efficiency.

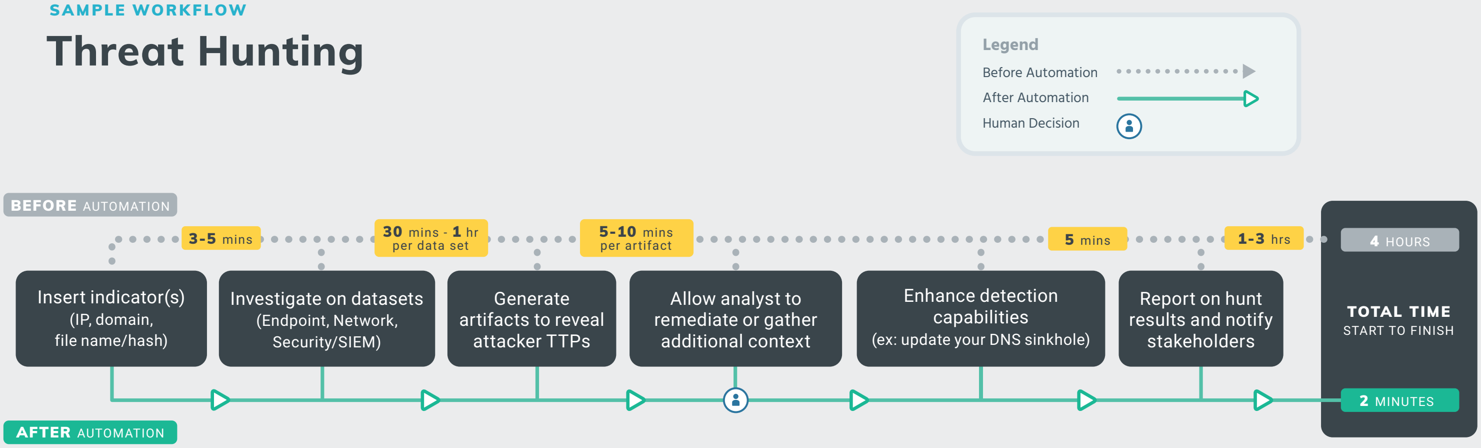
Cybercriminals spend an average of 191 days inside a network before being discovered.*

- **Notify and respond faster**

  Create and kick off designated response workflows based on the type of threat you've discovered. This ensures that you follow proper protocol, your stakeholders are notified as quickly as possible, and that everyone works from the same set of data for a complete end-to-end investigation.

SAMPLE WORKFLOW

Threat Hunting


Legend
Before Automation
After Automation
Human Decision
BEFORE AUTOMATION
3-5 mins
30 mins - 1 hr per data set
5-10 mins per artifact
5 mins
1-3 hrs
Insert indicator(s) (IP, domain, file name/hash)
Investigate on datasets (Endpoint, Network, Security/SIEM)
Generate artifacts to reveal attacker TTPs
Allow analyst to remediate or gather additional context
Enhance detection capabilities (ex: update your DNS sinkhole)
Report on hunt results and notify stakeholders
4 HOURS
TOTAL TIME
START TO FINISH
2 MINUTES
AFTER AUTOMATION

*source: https://securityintelligence.com/a-beginners-guide-to-threat-hunting

COMMON AUTOMATION USE CASE

Patching and Remediation

Security teams today face more vulnerabilities in their environment than they can realistically remediate on their own. The result? A mounting backlog, piling up to a point where issues start slipping through the cracks, leaving you more vulnerable if certain actions aren't taken in a timely manner. A SOAR solution should integrate with your existing tools to orchestrate vulnerability management processes from notification to remediation, so you can ensure critical issues are being addressed with every security advisory that comes in—while keeping human decision points where most critical. Automate actions to scan, find patches, verify remediation, and more.

- **Monitor advisory lists**

  Coordinating vendor vulnerability response used to be a manual process requiring multiple stakeholders. With an automation solution, you can build workflows to automatically monitor advisory lists via RSS feed plugins, and set up decisions and action points as needed.

- **Notify stakeholders**

  When a vulnerability needs to be addressed, automatically trigger the creation of service tickets via integrations with leading solutions like JIRA and ServiceNow.

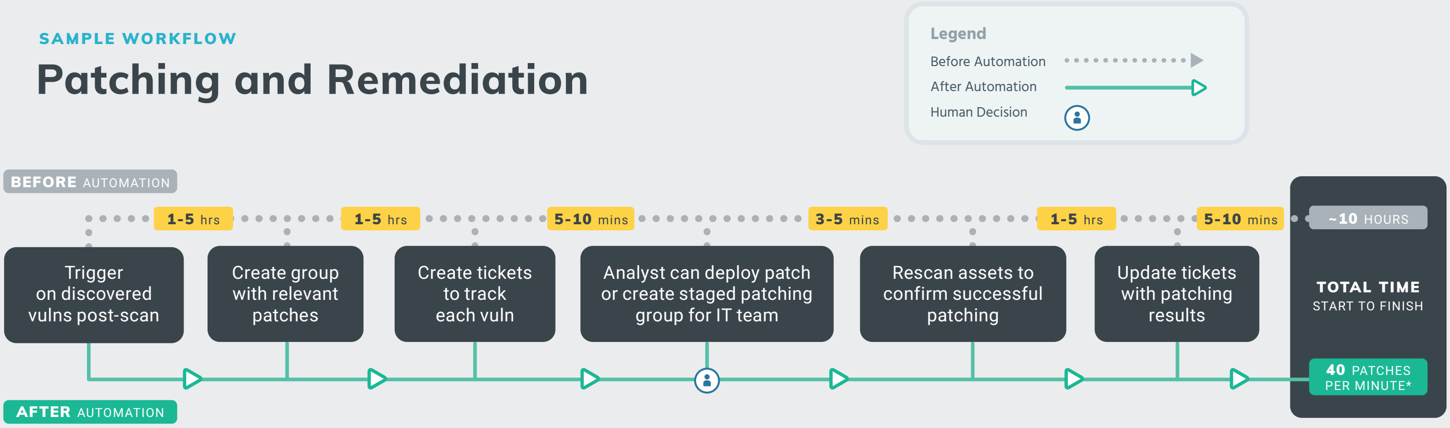
- **Meet compliance drivers**

  Wrangling all stakeholders and ensuring necessary tasks happen within an SLA timeframe is a time-consuming project in itself. Automation enables you to respond efficiently and within required timeframes, ensuring vulnerabilities don't fall through the cracks.

POPULAR PLUG-INS: Microsoft SCCM, IBM BigFix, Metasploit, JIRA, ServiceNow

SAMPLE WORKFLOW

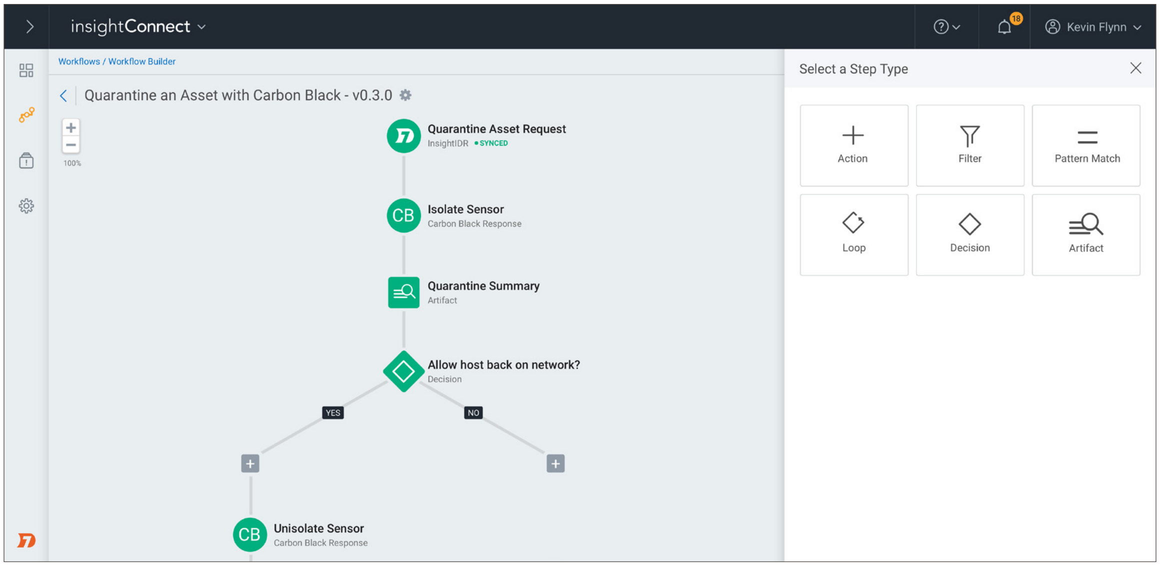
Patching and Remediation


Legend
Before Automation
After Automation
Human Decision
BEFORE AUTOMATION
1-5 hrs
1-5 hrs
5-10 mins
3-5 mins
1-5 hrs
5-10 mins
~10 HOURS
Trigger on discovered vulns post-scan
Create group with relevant patches
Create tickets to track each vuln
Analyst can deploy patch or create staged patching group for IT team
Rescan assets to confirm successful patching
Update tickets with patching results
TOTAL TIME START TO FINISH
40 PATCHES PER MINUTE*
AFTER AUTOMATION

*Based on current testing of environments with low asset counts and high volume of patch IDs.

Simplify Your Security with InsightConnect

InsightConnect is a security orchestration and automation solution that enables your team to accelerate and streamline time-intensive processes with little to no code. With 270+ plugins to connect your tools and easily customizable connect-and-go workflows, you'll free up your team to tackle other challenges, while still leveraging human decision points when it's most critical. With significant time savings and productivity gains across overall security operations, you'll go from overwhelmed to operating at maximum efficiency in no time.



Want to learn more about Rapid7 automation?

Check out our Automation Solution Brief.

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our website, check out our blog, or follow us on Twitter.