RAPID7

SOLUTION GUIDE

Optimize Security Operations with Automation

A guide to automating SOC tasks and increasing efficiency with the Rapid7 Insight cloud

TABLE OF CONTENTS

Automation on the Insight Cloud

We've built automation into the core of our offerings, so you can work more effectively

As security teams continue to evolve, adapt, and innovate at a rapid rate, the struggle to balance increasing workloads with limited resources, complex ecosystems, and rising threats has never been greater. Security orchestration and automation helps teams improve their security posture and create efficiency—without sacrificing control of important security and IT processes.

To work more efficiently, accelerate your security processes, and automate your most important use cases, we offer a suite of solutions on the Rapid7 Insight cloud:

InsightConnect

Our standalone orchestration and automation solution accelerates and streamlines time-intensive processes—with little to no code. With 290+ 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 their expertise when it's most critical.

InsightIDR

Our threat-focused SIEM solution includes built-in automation workflows for containment, such as quarantining assets and disabling users; ticketing integrations for streamlined incident response processes between teams; and investigation enrichment.

"62% of enterprise security decision makers report not having enough security staff, while 65% state that finding employees with the right skills is a challenge."

— Forrester, "Breakout Vendors: Security Automation and Orchestration"

Overview: In-Product vs. Standalone Automation Capabilities

For the past several years, we've been hard at work building the Rapid7 Insight cloud, which provides visibility through unified data collection, analytics, and automation for all of our Insight products. When it comes to security orchestration and automation (SOAR), we've leveraged the technology in different ways across our portfolio for maximum impact for our customers. The SOAR technology that powers our standalone solution, InsightConnect, allows users to build and customize workflows as much or as little as they'd like. We've also incorporated pieces of that technology into products like InsightIDR to help customers accelerate their existing operations.

The tables in this document will clarify the differences between the automation capabilities of InsightConnect versus those built into InsightIDR, so you can make the best decision for your organization.

In-Product Workflows vs. InsightConnect

	IN-PRODUCT WORKFLOWS (INSIGHTIDR)	INSIGHTCONNECT
Use cases	A core set of pre-defined use cases	Can accommodate a variety of security operations and IT use cases, including use cases unique to your organization
Customizability	Logic is pre-determined to meet specific business processes and integrations	Fully customizable logic that can accommodate a variety of use cases to match your business processes
Supported integrations	A core set of use cases leveraging specific third-party integrations, or plugins	A growing library of 290+ plugins to connect your tools, plus a software development kit (SDK) if you want to build or customize your own plugins
Flexibility	All workflows must be "triggered" from InsightIDR events	Can orchestrate any piece of your technology stack, including third-party SIEMs and VM solutions, and extends automation capabilities in InsightVM and InsightIDR

See it in action:

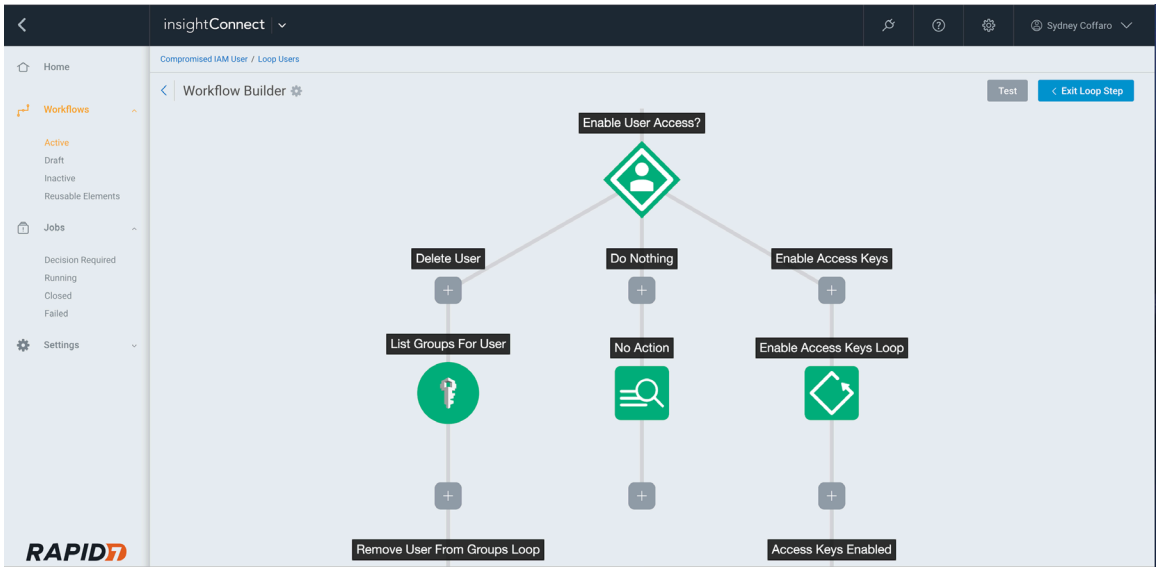


Figure 1: Using the Workflow Builder in InsightConnect to enable user access.

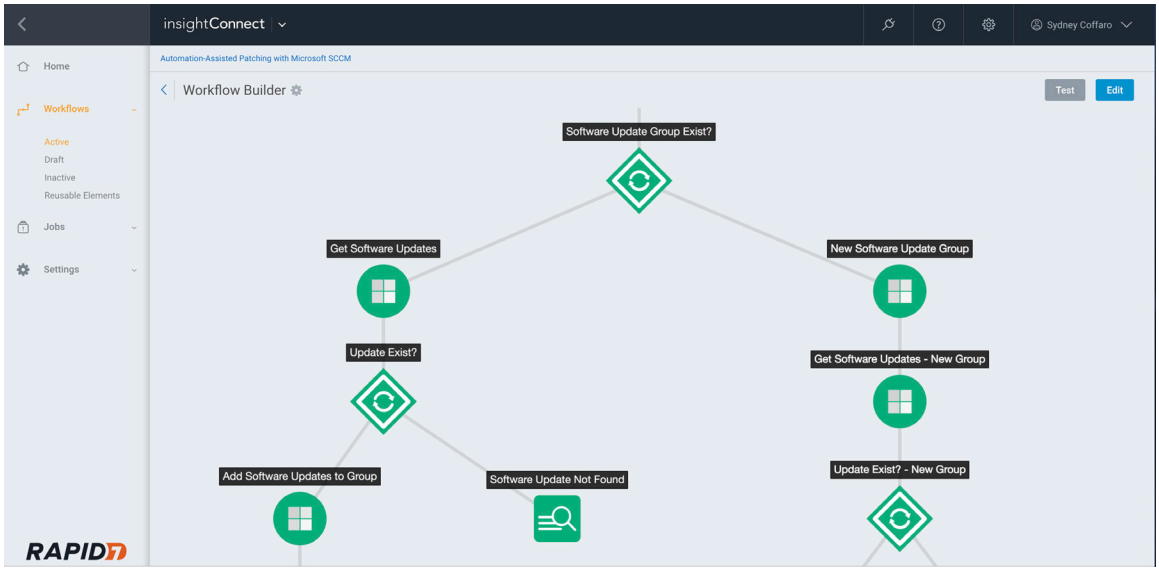


Figure 2: Using the Workflow Builder in InsightConnect to automate software updates.

Want to see what else is possible with InsightConnect automation?

Request a demo at www.rapid7.com/see-insightconnect.

Automation for Incident Detection and Response

InsightIDR vs. InsightConnect

USE CASE	WHEN TO USE BUILT-IN PRODUCT FUNCTIONALITY	WHEN TO PURCHASE INSIGHTCONNECT
User containment	If you need to suspend a user in Okta, or disable a user in Active Directory. AND If you want to trigger this off of an alert from within InsightIDR.	...If you need to support disabling user accounts on alternative identity providers, such as Duo or Google. ... If you need to perform custom logic in Okta or Active Directory to contain a user (e.g. move to a quarantine group). ... If you need to add additional approval steps before you perform user containment. ... If you need to create tickets, or perform other actions as part of your user containment workflow. ... If you need to trigger user containment automatically, or from third-party solutions other than InsightIDR.
Endpoint containment	If you want to perform endpoint containment on an asset in an InsightIDR investigation using Carbon Black Protect's isolate sensor, or with the Insight Agent. AND If you want to trigger this off of an alert from within InsightIDR.	... If you want to perform containment in a different way (by isolating using a firewall or a different third-party endpoint solution), or using a different Carbon Black capability. ... If you need to add additional approval steps before you perform endpoint containment. ... If you need to create tickets, or perform other actions as part of your user containment workflow. ... If you want to trigger endpoint containment automatically, or from third-party solutions other than InsightIDR.

Enrichment	If you want to enrich investigations with open source or supported threat intelligence feeds. AND If you want to trigger this off of specific alert types from within InsightIDR.	... If you want to submit a file or hash for sandbox analysis with Hybrid Analysis, Cuckoo, Team Cymru, Recorded Future, or other solutions. ... If you want to notify team members of response decisions with Slack, Microsoft teams, or Pagerduty. ... If you want to check suspicious URLs against phishing intelligence tools like PhishTan, VirusTotal, or OpenPhish. ... If you want to check an IP's geo location, malicious reputation, or registry date against tools like WhoIs, AbuseIPDB, or Recorded Future.
Ticketing	If you want to create a ticket in Jira or ServiceNow from an InsightIDR investigation with a pre-built message body format. AND If you want to trigger this off of an alert from within InsightIDR.	…. If you want to create a ticket using The Hive, Trello, or other solutions. … If you want to customize the body of the ticket based on the contents of the alert. … If you want to transition the ticket state or have it track changes to an investigation.

Looking for even more advanced automation capabilities?
Get started with InsightConnect to unlock fully customizable workflows and use cases.

See it in action:

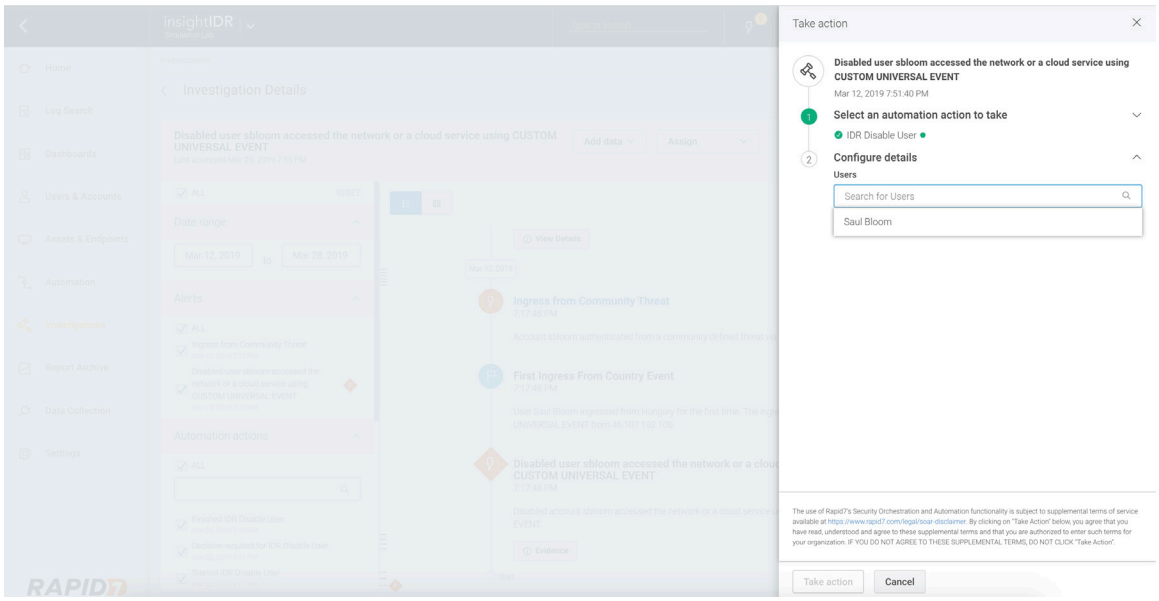


Figure 1: Easily take action from an investigation to create tickets or contain threats at the user, endpoint, or network level.

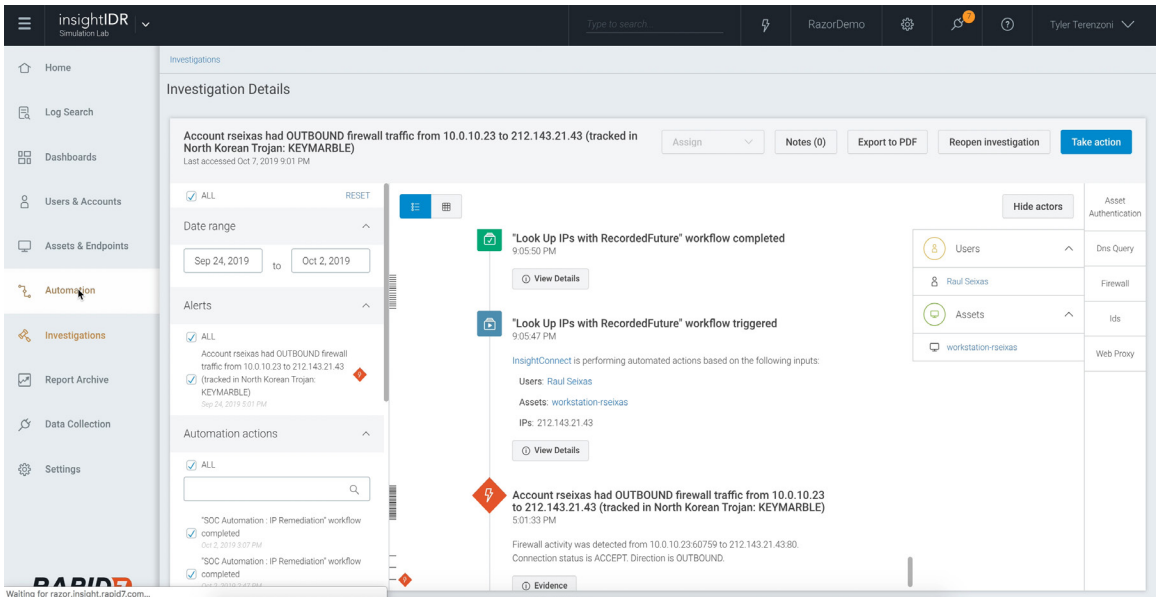


Figure 2: All automated steps are reflected in the Timeline, including decisions made manually by analysts to mitigate risk.

Want to learn more about automation in InsightIDR?

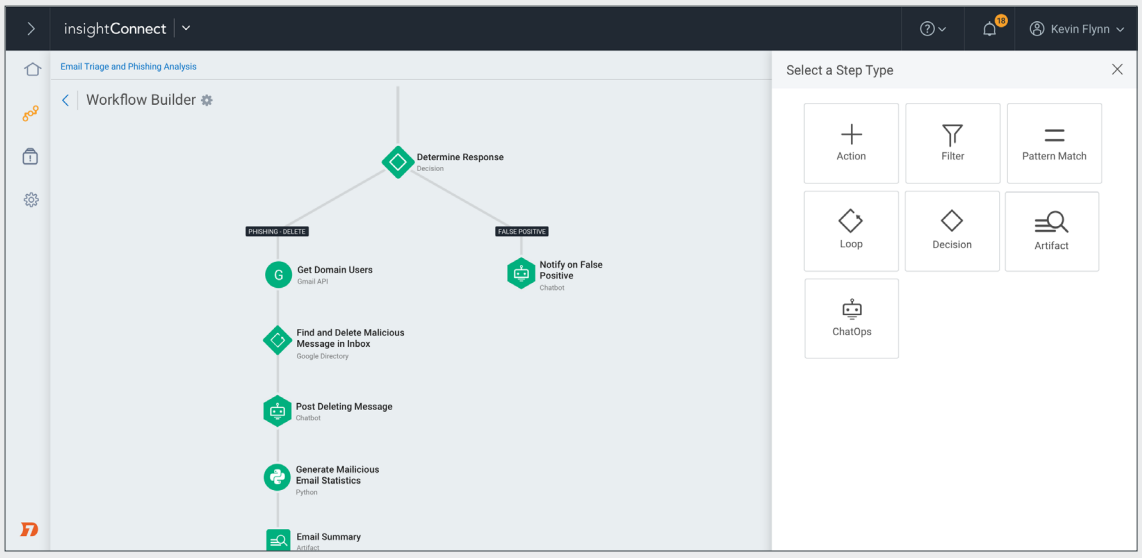
Start your free trial at www.rapid7.com/try/insightidr.

Conclusion

You've seen how much time and money security orchestration and automation can save you. And while you could add both of these concepts with custom development, using an orchestration and automation solution will bring value and demonstrate ROI at a considerably faster and more effective rate. This is where InsightConnect comes in.

InsightConnect is the orchestration and automation layer for SecOps, to help you orchestrate and automate your security tools and tasks faster than ever before. Easily connect your tools and automate all your security processes, without writing a single line of code. Save time and money, all while increasing productivity, efficiency, and accuracy.

To learn more or request a demo, visit:
rapid7.com/insightconnect



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.