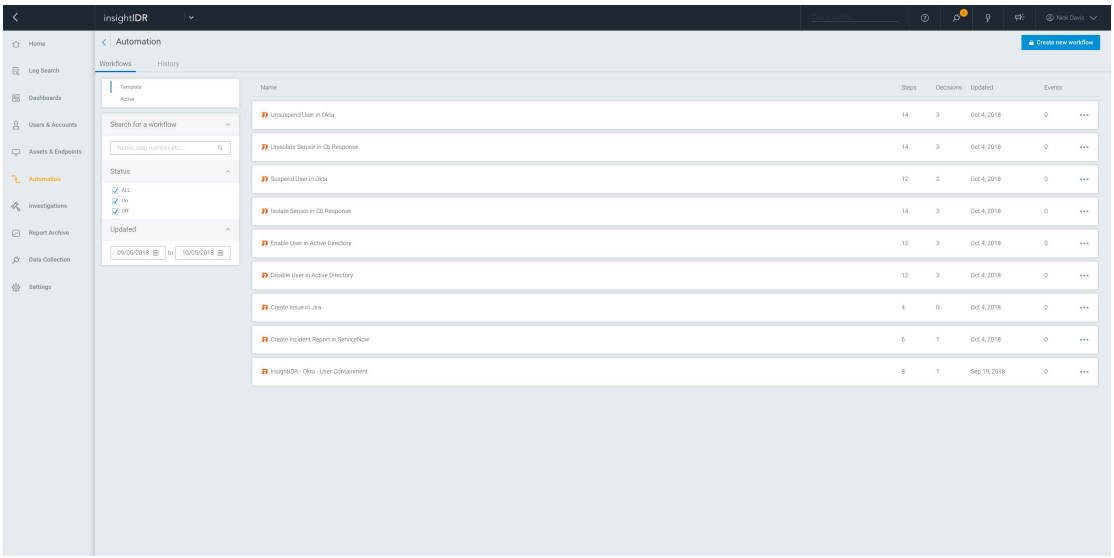
SOLUTION BRIEF

Automate Incident Detection and Response

Take action on alerts quicker and more effectively

Even the most adept teams with the best-in-class detection tools are looking for ways to increase efficiency when responding to security threats. Imagine if you could make your detection and response program work better and faster, with more visibility and control. With the right threat detection technologies, it's possible to gain visibility across your entire environment, detect attackers with analytics, and automate response. The result? Meaningful alerts with relevant context, combined with the power to directly contain threats. Now pair that with orchestration and automation, and you'll conserve manpower for what humans do best: analyzing threats and adversaries, making informed response decisions, and embarking on strategic initiatives to reduce risk.

Figure 1: Automation workflows in InsightIDR



Achieve your security goals with efficiency

InsightIDR helps you detect and respond to all of the top attack vectors behind breaches: phishing, malware, and the use of stolen credentials. Unlike legacy approaches to SIEM and threat detection, InsightIDR was built from the ground up to help you automate as much as possible across the incident response lifecycle. Just like our global SOCs, which monitor hundreds of organizations, and the InsightIDR customer community, your team can escape the drudgery of managing a growing mountain of log data and pivoting to yet another tool just for simple answers.

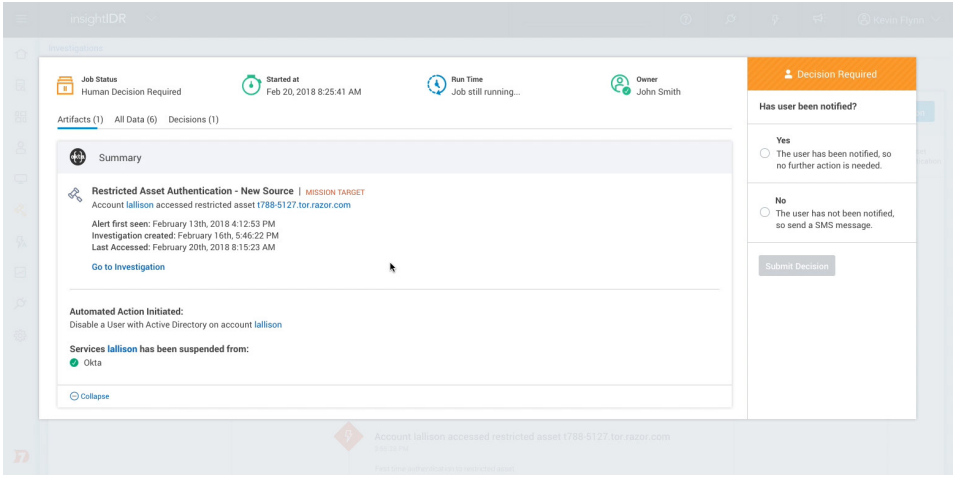
Here are three examples of how automation within InsightIDR can arm you with visibility, detection, and options for response.

Go from compromise to containment, faster: Save time and lower risk when responding to incidents. When investigating threats in InsightIDR, you not only get important context, but you can immediately take steps to contain a threat. With the included Insight Agent, you can kill malicious processes or quarantine infected endpoints from the network. You can also use InsightIDR to take containment actions across Active Directory, Access Management, EDR, and firewall tools. You'll have the power to directly contain threats on an endpoint, network, and user level.

Detect and contain compromised user accounts: Compromised credentials and lateral movement consistently show up as stealthy underlying behaviors behind breaches. With InsightIDR, you'll be able to detect stealthy malicious behaviors across the entire MITRE ATT&CK framework. Unlike tools that focus on signatures on the endpoint, InsightIDR integrates with Active Directory and leading cloud services to apply User Behavior Analytics to authentications across your environment. Once you identify a compromised user account or endpoint in InsightIDR, you can take direct action to contain the threat. Containment actions include deprovisioning a user, resetting a password, killing a malicious process, quarantining an asset, and more.

Slot into existing response workflows with IT: For any type of alert created or managed by InsightIDR, you can automatically create a corresponding ticket or case in tools like JIRA and ServiceNow. Paired with our native case management features, this ensures that for any alert, the right team members are notified and empowered to take action.

Figure 2: Triggered decision point in InsightIDR



About InsightIDR

Rapid7 InsightIDR leverages attacker analytics to detect intruder activity earlier in the attack chain, cutting down false positives and days' worth of work for security professionals. It hunts for actions indicative of compromised credentials, spots lateral movement across assets, detects malware, and sets traps for intruders.

To see what else automation can do for you, visit www.rapid7.com/insightconnect

READY TO GET STARTED?

To learn more about automation in Rapid7 InsightIDR, or to start a free trial, visit:

www.rapid7.com/insightidr