Automate Incident Detection and Response

Early, accurate alerting so you can respond quickly, with confidence

Today's security teams are facing more complexity than ever before. IT environments are changing rapidly, catalyzed by more cloud infrastructure, increased adoption of SaaS applications, and proliferating data. The threat landscape also continues to evolve, with new threats and attacker groups to watch daily, and the security industry as a whole is largely under-resourced. Security teams must find efficiencies to monitor their widening technology footprint and stay ahead of attackers. Security analysts need threat detection and response technology that works for them (not technology that gives them more work).

InsightIDR, Rapid7's cloud SIEM, addresses the key challenges facing today's security teams by:

- Unifying and normalizing diverse data for visibility across modern networks;
- Providing highly reliable out-of-the-box detections focused on identifying threats early in the attack chain;
- And delivering rich visual investigations and automation to accelerate response times.

Achieve your security goals with efficiency

Unlike legacy approaches to SIEM, InsightIDR was built to remove the burdens of set-up, configuration, and ongoing management that take focus away from actual detection and response. InsightIDR leverages insights and threat intelligence from the Rapid7 community, research department, and our own Managed Detection & Response service to drive intuitive features that enable teams of any size to optimize security operations and further their security posture. Automation workflows in InsightIDR help further enrich investigations, streamline response, and eliminate repetitive, low value work.

"The time from the attacker's first action in an event chain to the initial compromise of an asset is typically measured in minutes. Conversely, the time to discovery is more likely to be months."

— Verizon Data Breach Investigations Report 2019

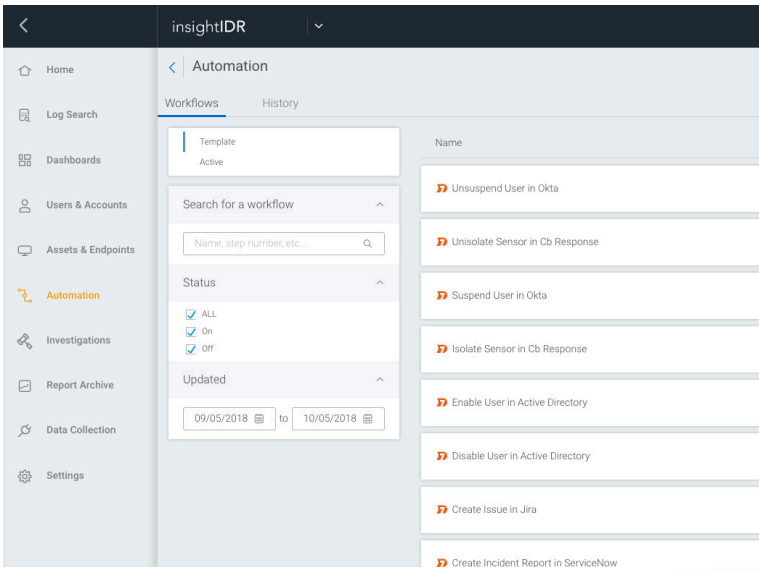

Figure 1: Automation workflows in InsightIDR

Here are four examples of how automation within InsightIDR can help optimize your threat detection and response:

- **Enrich alerts for more threat context:** Add additional information and threat intelligence to alerts to further accelerate investigations. Enrichment workflows help add more context, including IP, hash, or domain lookups from open source plug-ins, or threat intel plug-ins like RecordedFuture.

- **Go from compromise to containment, faster:** Kill malicious process or quarantine infected endpoints from the network via automation actions on the Insight Agent. Take containment actions across Active Directory, Access Management, EDR, and firewall tools. Directly contain threats on the endpoint, network, and user level.

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

- **Trigger responses right off alerts to minimize response time:** With InsightIDR's intuitive user interface, it's easy to create rules to take immediate action on alerts. These actions can be from the automated workflows available natively in InsightIDR, or—for InsightConnect customers—choose any SOAR workflow for further customized and advanced automation.

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.

For modern threat detection and response, automation is a necessary part of the security analyst toolkit.

Learn more about how to accelerate automation adoption and streamline critical processes with InsightIDR and InsightConnect at visit www.rapid7.com.

Support

call +1.866.380.8113

Customer Portal

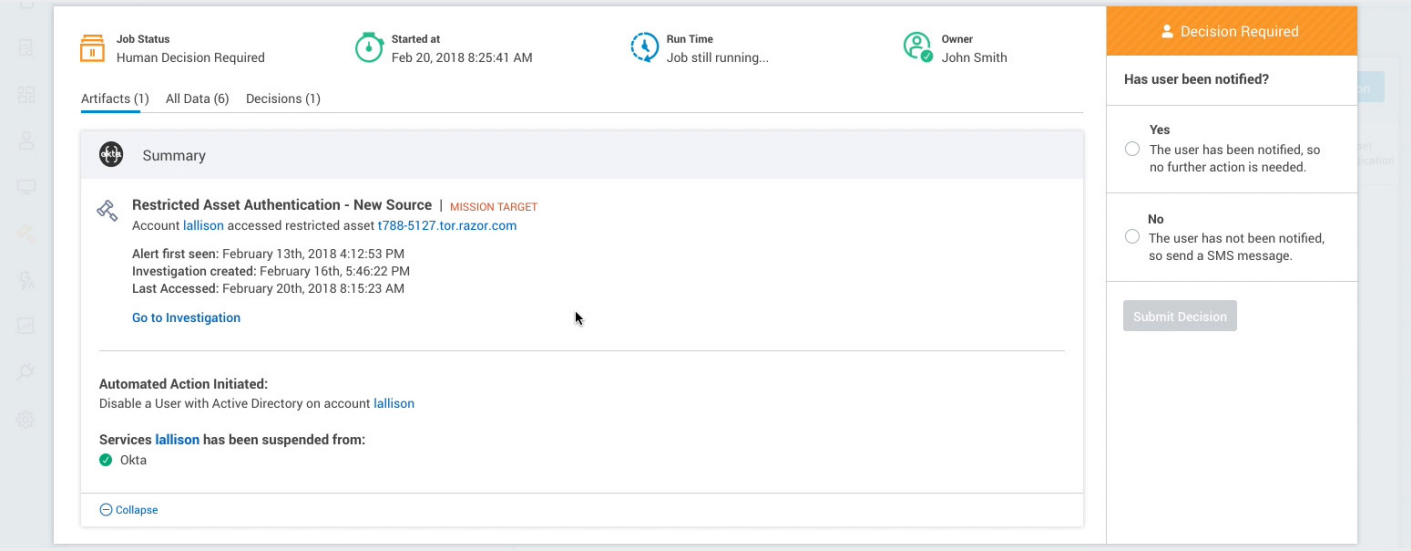

Figure 2: Triggered decision point in InsightIDR