RAPID7

SOLUTION BRIEF

Accelerating Incident Response: Leveraging InsightConnect with InsightIDR

Streamline how your team prioritizes, investigates, and responds to threats.

Security teams face a skills shortage, a continuously expanding attack surface, too many hard-to-prioritize alerts, unintegrated security tools, slow investigations, inconsistent response procedures, and general analyst burnout. That's a lot. While there is no magic solution for these challenges, security orchestration, automation, and response (SOAR) systems can help.

When combined with InsightIDR, Rapid7 InsightConnect provides targeted automation that enables better alert prioritization, streamlining of repetitive processes, and investigation acceleration. It also helps you resolve incidents more efficiently by leveraging existing IT and security tools. You don't have an infinite supply of security professionals, so why not use automation to level up the expertise you do have?

> “
>
> ***The only reason I can run a 24/7 SOC with three people is because of InsightIDR and InsightConnect***
>
> Auden Group

Key benefits of using InsightConnect with InsightIDR

✓ Easily develop and deploy tailored automations that leverage 300+ pre-built integrations and a streamlined workflow interface.

✓ Reduce MTTR by automating tedious or time-sensitive investigation-and-response tasks.

✓ Ensure process consistency by incorporating automation into response playbooks.

✓ Maximize analyst productivity: Free them up from tedious, manual tasks.

✓ Integrate core security and IT technologies to minimize portal fatigue and leverage your existing processes.

✓ Improve collaboration by pushing tasks to other IT and security stakeholders via their preferred channels (ChatOps, email, and ITSM).

InsightConnect enables your team to automate key elements of incident response:

- Get 24/7/365 incident response.
- Trigger response playbooks directly from InsightIDR investigations or alerts.
- Consistently define alert priority and filter out low-priority/ false-positive alerts.
- Enrich alerts and investigations with threat intelligence.
- Define alert pathways to external tools like PagerDuty, Slack, and Microsoft Teams.
- Collaborate on incident response activities through ChatOps and ITSM integrations.
- Speed ad-hoc investigations and threat hunting by leveraging preconfigured automation actions – Quick Actions – within InsightConnect or InsightIDR.
- Contain active threats by leveraging security endpoints, firewalls, web gateways, secure email gateways, and other security controls.

Improved efficiency and efficacy with InsightConnect-based incident-response automations

Incident Response Requirements	Example InsightConnect Workflow	Sample Integrations
Enrich alerts with threat intelligence	Update InsightIDR threat with new indicators of compromise (IOCs) from Rapid7's Threat Command. When Threat Command generates an alert, InsightConnect will automatically parse the alert and extract the domains, IP addresses, URLs and file hashes. It will then upload them into the chosen InsightIDR Threat.	Recorded Future RAPID7 ANOMALI VirusTotal
Leverage existing communication and ticketing systems	Create an incident in ServiceNow from Slack. If your team is collaborating on and handling incidents in Slack, you can send the information you need to ServiceNow in a matter of seconds.	servicenow Jira zendesk pagerduty T ivanti cherwell bmc
Block active threats at the network or endpoint	Block host with Check Point Firewall from Slack. This workflow blocks/ unblocks a specific host in Check Point via Slack commands, and reports status information back to Slack.	Carbon Black. CHECK POINT RAPID7 SOPHOS SONICWALL FORTINET cybereason CISCO CROWDSTRIKE paloalto SentinelOne zscaler
Suspend user accounts, force password resets, block/remove phishing emails	Block domain account in Active Directory from an InsightIDR UBA alert. This workflow disables a domain user account from an InsightIDR Brute Force–UBA alert.	okta DUO Active Directory proofpoint mimecast E Office 365

insightCloudSec | insightIDR | ThreatCommand | insightVM

insightAppSec | insightConnect | Security Services

To learn more or start a free trial, visit
https://www.rapid7.com/products/insightconnect/try/

Support

Customer Portal | Call +1.866.380.8113