

# Even faster MTTR is possible: Pair InsightConnect with MDR

Simplify the implementation of your MDR Findings Report recommendations and automate responses for InsightIDR and 3rd party security alerts with InsightConnect.

Partnering with an MDR provider is an important step in addressing the security talent, expertise, and resource constraints that impact your team. But being able to detect and respond in today's world is only half the battle. The other factor is time - how fast can you respond, remediate, and recover?

When every second counts, you need a way to ensure your incident response processes are as effective and efficient as they can be. Security orchestration, automation, and response (SOAR) systems, like InsightConnect, can help your team quickly take recommended actions in your MDR Findings Report. In addition, InsightConnect can further address incidents initially triaged by MDR Active Response by automating blocklist updates, user access changes, or password resets.

And if you set up custom alerts within InsightIDR or need to configure workflows for your other 3rd-party security alerts, InsightConnect can help your team save time by automating notification, enrichment, mitigation and remediation actions.

The bottom line is that by complementing your MDR service with InsightConnect, the Rapid7 SOAR extends the capabilities of Active Response while improving your ability to respond and move faster from risk to remediation.








## Key Benefits of Using InsightConnect with Rapid7 MDR Service

- ✓ Reduce MTTR by automating repetitive, manual remediation steps
- ✓ Automate responses to custom InsightIDR and third-party security system alerts
- ✓ Build automation playbooks to consistently respond to critical threats
- ✓ Improve incident response efficiency so your team works smarter and more strategically
- ✓ Integrate core security and IT technologies to minimize portal fatigue and leverage your existing processes
- ✓ Integrate communication channels like ChatOps and email to push notifications and tasks to other IT stakeholders or users via their preferred channels

InsightConnect workflows enable your team to automate many types of responses:

- Quarantine endpoints for third-party and custom InsightIDR alerts
- Contain users for third-party and custom InsightIDR alerts
- Remove phishing emails and block senders/URLs
- Execute approval chains
- Enrich investigations with threat intelligence
- Block IPs and domains
- Update file hash blocklists
- Create and manage IT tickets

InsightConnect automation powers faster remediation and mitigation of MDR Findings Report recommendations

Typical Recommendation in your MDR Findings Report	Example InsightConnect Workflow	Sample of Supporting Integrations
Rebuild affected systems from known-good baseline images	Open a high-priority ticket in your ITSM to rebuild the system.	
Block malicious domains at firewalls, proxies, and DNS servers	Update block policies based on the list of confirmed malicious domains provided by the MDR SOC.	 
Block malicious IP addresses at firewalls, proxies, and DNS servers	Update block policies based on the list of confirmed malicious IPs provided by the MDR SOC.	
Quarantine endpoint from the network	If configured, Rapid7 MDR will use Active Response to contain the endpoint using the Rapid7 Insight Agent. You can also set up InsightConnect workflows to contain endpoints using the Insight Agent or another EDR agent. Also to respond to third-party or custom InsightIDR alerts not monitored by the MDR SOC.	 
Lock affected user accounts	If configured, Rapid7 MDR will use Active Response to contain the user account. You can also set up InsightConnect workflows to lock user accounts initiated by third-party or custom InsightIDR alerts not monitored by the MDR SOC.	 
Force password resets for affected accounts	Automatically reset passwords of compromised user accounts after they are disabled by Active Response. You can also set up InsightConnect workflows to reset passwords for accounts from third-party or custom InsightIDR alerts not monitored by the MDR SOC.	

**“We use the MDR SOC with InsightConnect to develop several triggers and responses so that if certain attributes happen, the SOC and I know to take action. I just click on the response, and it isolates a system or disables a user. It’s already integrated with InsightConnect, so I know what’s going to work.”**

Tony Hamil, Sr. Security Engineer at Hillwood Development

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