RAPID7

SOLUTION BRIEF

Detections Methodology in InsightIDR

Stay ahead of threats with curated, high-fidelity detections

InsightIDR—Rapid7's cloud-native SIEM and XDR—delivers highly efficient, accelerated detection and response. Teams work smarter and faster with InsightIDR's frictionless SaaS deployment experience, hyper intuitive interface, robust out-of-the-box detections, and actionable automation.

Key SOC Challenges

- **Overwhelming noise and false positives** distract from real threats
- **Too little context + talent shortages** = teams don't know what to do next
- **Resource gap** means team don't have time to curate threat intelligence and create detections content themselves

When it comes to these challenges, InsightIDR can help—we have you covered with a sane default configuration, robust detection tuning options, as well as our advanced knowledge of the threat landscape thanks to our open source community research projects, our MDR and service engagements, and external threat intelligence.

Expertly Vetted Detections You Can Trust

Comprehensive coverage across all types of attacks

With a variety of detection types—User Behavior Analytics (UBA), Attacker Behavior Analytics (ABA), and custom detections—you're covered against it all, from lateral movement to unique attacker behaviors and everything in between. In addition to behavior based threats, InsightIDR also has coverage for IOCs for the most comprehensive and enduring detection coverage.

A curated Detection Library of expertly vetted detections

Leveraging insights and intelligence from our open source community research projects, our Threat Intelligence and Detection Engineering (TIDE) team continuously collaborates with our Incident Response/Managed Detection and Response (MDR) service to develop and enhance our detection library in catching real world attacks. The TIDE team writes detections as soon as they see new techniques being used by attackers, which means all customers immediately get the most up-to-date threat intel, no configuration needed.

Once written, these detections are vetted immediately in the field by our MDR SOC to ensure they drive low-noise and only alert on real potential threats.

> **Rapid7 InsightIDR has been a wonderful tool that gives us insight into our user behaviors, as well as clearly alerting us to potential threats that exist in our network. Our team has become more efficient with fewer false positives and improved investigation times.**
>
> Josh Petrucka,
>
> Security Analyst, Conexus Credit Union via TechValidate

Detections mapped to the MITRE ATT&CK framework

Our MITRE ATT&CK Matrix view maps detection rules to MITRE tactics and techniques commonly used by attackers, enabling you to see where you have coverage with Rapid7's out-of-the-box detection rules for common attacker use cases.

Key Customer Outcomes

Stay ahead of emergent threats	Every time an analyst creates an alert it takes work. At Rapid7 we want to save you time and advance your security posture—which is where our Detections Library comes in. Curated and managed by our MDR SOC team, you can rest assured that you'll only be alerted to behaviors that are worthy of human review so that you can make the most out of your limited time and focus on the threats that really matter.
Identify advanced attacker behaviors	To add another layer to our threat intelligence, we've integrated Rapid7's Threat Command Threat Library into InsightIDR to give more visibility into new indicators of compromise (IOC's), and continued strength around signal-to-noise. All IOC's related to Threat Actors tracked in Threat Command are automatically applied to customer data sent to InsightIDR, which means you automatically get current and future coverage as new ones are found by the research team.
Detect intruder compromise, insider threats, and risky behavior	InsightIDR uses machine learning to baseline user behavior in your environment, making it easy to spot when something's awry (like stolen credentials or someone's logging in from multiple countries at the same time).
Customize detections to suit your unique environment	While we focus on creating a curated, high fidelity library of detections, we know each environment has its unique challenges—which is why our ABA detections are robustly tuneable. You're also able to get more granular and create custom detections, as well as customize which UBA directions you have turned on so that your alerting aligns with your environment.

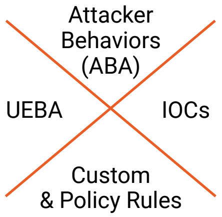
> **"InsightIDR provided value to us on Day-1. We didn't have to write long lists of rules or tweak hundreds of settings in order to get security alerts from our operating environment. Better still, the signal-to-noise ratio of the alerts is great; little-to-no false positives.**
>
> Philip Daly,
>
> VP Infrastructure and
> Information Security,
> Carlton One Engagement
> via TechValidate

InsightIDR Detections Methodology

External & Unique Rapid7 Community Threat Intel

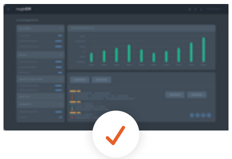
Full Environment Coverage

Known & Unknown Threats



Vetted by MDR SOC Experts: Superior Signal-to-Noise

Always Up-to-Date Detections Content Creation Service



PRODUCTS

insightCloudSec | insightIDR | Threat Command

insightVM | insightAppSec | insightConnect

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

SUPPORT

Customer Portal | Call +1.866.380.8113

RAPID7