RAPID7 | insightIDR

CYBERSEC SOLUTIONS

PRODUCT BRIEF

Detect faster, respond smarter, secure everywhere.

InsightIDR delivers the freedom to focus on what matters most.

InsightIDR—Rapid7's next-gen 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 Security Team Challenges

- **Attack surface is constantly changing** and many solutions don't scale
- **Resource constrained teams are outmatched** by the fast moving threat landscape and noisy alerts
- **Most solutions are hard to stand up** and time consuming to maintain
- **Accurate, timely response to threats is hard** and often unattainable for security teams

InsightIDR addresses all of these challenges as it works to **unify** and transform relevant security data from across a customer's modern environment to tie together disparate data, **detect** real threats early in the attack chain, and provide security teams with high context, actionable insights and automation to **respond** to threats fast.

UNIFY: With leading next-gen SIEM at the core, it's big data collection without big work

InsightIDR provides complete coverage with a native endpoint agent, network sensors, collectors, and APIs to streamline security operations and levels up outcomes.

- **Lightweight software-based collection technologies**
  Correlate, attribute, and enrich diverse datasets into a single, harmonious picture
- **Fast, flexible log search**
  Analysts of any skill-level can quickly visualize and process complex data
- **13-month data retention**
  Normalized and readily searchable data at your fingertips
- **Actionable reporting**
  Be audit-ready always with pre-built dashboards and intuitive, custom report builders

DETECT: Unique intelligence plus expert vetting mean early threat detection you can trust

InsightIDR has a robust library of high-fidelity detections spanning attacker behavior-based (Attacker Behavior Analytics) detections as well as User Behavior Analytics detections, covering both known and unknown threats.

- **Embedded, curated threat intelligence**
  Get high-signal, low-noise from intelligence across Rapid7's open source community research projects, MDR and service engagements, and external threat intelligence powered by Rapid7's Threat Command
- **MITRE ATT&CK mapping**
  Users have a full matrix view and searchability, with filters on tactic, technique, and advanced persistent threat (APT) group
- **Expertly vetted alerts you can trust**
  Rapid7's global MDR SOC experts use InsightIDR, giving us a rare feedback loop and deep understanding of the user experience
- **Intuitive rule creation**
  Zero in on policy violations and unique threats with wizard-style UIs that guide you through custom log parsers and rule creation

RESPOND: Analysts respond faster and more confidently with playbooks and automation

When an attack is underway, every second counts. InsightIDR eliminates distractions and context switching, and drives fast, automated responses to stop attackers early in the attack chain.

- **Detailed events and investigations**
  InsightIDR's attribution engine tracks users and assets as they move around the network, auto-enriching every log line
- **Correlation across diverse telemetry**
  Get a single investigation timeline for each alert, streamlining workflow with all the details of an attack in one place
- **Expert response recommendations**
  Each alert comes with recommended actions from our global MDR SOC and Rapid7 Velociraptor's digital forensics and incident response playbooks
- **One-click response and automation**
  With embedded containment workflows or seamless integration with Rapid7 InsightConnect SOAR workflows, orchestrated response just a click away

> ***Rapid7 InsightIDR vastly improved the visibility of our network, endpoints, and weak spots. We now have the ability to respond to threats we didn't see before we had InsightIDR.***
>
> **Robert Middleton**
> Network Administrator CU4SD via TechValidate

insightCloudSec | insightIDR | ThreatCommand | insightVM
insightAppSec | insightConnect | Security Services

Contact Cybersec Solutions to learn more and start a free trial

Tel: 01494 936696 | Email: info@cybersec.solutions | Web: www.cybersec.solutions