RAPID7

carahsoft.

InsightIDR Dashboards And Reporting

Thank you for downloading this Rapid7 product brief. Carahsoft is the distributor for Rapid7 Cybersecurity solutions available via GSA, ITES-SW2, NASA SEWP V, and other contract vehicles.

To learn how to take the next step toward acquiring Rapid7's solutions, please check out the following resources and information:

For additional resources:
carah.io/Rapid7Resources

For upcoming events:
carah.io/Rapid7Events

For additional Rapid7 solutions:
carah.io/Rapid7Solutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Rapid7@carahsoft.com
888-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/Rapid7Contracts

InsightIDR Dashboards and Reporting

Create sophisticated reports with ease with pre-built dashboards and intuitive customization.

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:

- Complicated query-writing and arduous chart-building make creating sophisticated visuals and reports a challenge.

- Audit processes can derail employees and take staff away from critical security work to prepare reports and compliance documentation.

- Tailoring dashboards for different audiences or use cases is time-consuming and makes it difficult to demonstrate security progress.

"

The user interface is very clean and customizable so you can see what is most important to you. The evidence provided (raw data) is easily searched and aids in the remediation effort.

Director of Information Technology, Gas & Utilities Medium Enterprise via Gartner Peer Insights

Instantly actionable insights with pre-built dashboards and cards

In today's security climate, time is the SOC's most precious resource. Reliable security, monitoring, and compliance dashboards are a critical component of SOC success, but spending time writing queries and perfecting charts and graphs can distract from more urgent and impactful priorities. With InsightIDR, teams have access to over 45 dashboards out-of-the-box, spanning use cases

such as viewing internal and perimeter Enhanced Network Traffic Analysis data, exporting firewall configuration reports to satisfy compliance requirements, and achieving a consolidated view of your multi-cloud environment. With input from our own global MDR SOC, these dashboards are built with a focus on driving faster decision-making and relevant, contextual insights.

Analysts can also leverage this pre-built content as a springboard for customizing their own reports. InsightIDR provides multiple query modes and methods for creating data visualizations — so whether you are more comfortable with loose keyword search, working in our intuitive query language, or simply clicking on charts to narrow down results — every analyst can operate as an expert, regardless of their prior SIEM experience.

Audit-ready in just a few clicks

All customers have access to 13 months of searchable data storage by default, to search across normalized events, anomalies, and indicators of compromise. Whether your need is compliance, hunting, or longer-term forensics, your data is always live and ready to go when you are. Our pre-built compliance dashboards span many critical frameworks, including:

- HIPAA
- ISO 27001
- CIS
- PCI DSS

Create and share reports seamlessly right from the dashboard, and export for broader stakeholders in either PDF or interactive HTML files. New dashboards are constantly being created and added to our ever-growing library.

"

Unifying many systems into Rapid7 InsightIDR had helped us greatly reduce the time of investigations and threat hunting, as well help us as a healthcare provider monitor and meet many security criteria by HIPAA.

Jose Torres, IT Security Engineer, Hospital Oncologico Dr. Isaac Gonzalez Martinez via TechValidate

Provide visibility into critical security metrics and SOC progress

The ability to visualize key performance indicators and team productivity are critical for Security and Risk leaders to demonstrate progress and tell the story of the SOC with data. InsightIDR enables both leaders and analysts to quickly build impactful reports for any audience — whether that's the board, company leaders, or your peers across DevSecOps. Quickly gain visibility into your security team's performance and the overall threat trends facing your organization displayed in a single, powerful dashboard. With the Security Operations Activity dashboard, quickly visualize team KPIs and security progress, including:

- analysis of your security team's investigation activity;
- which alert types are triggered the most to inform prevention priorities;
- the part of the attack chain that is the most targeted to better understand where defenses may be lacking;
- movement in critical security metrics - like MTTR.

With pre-built content and intuitive dashboards and reporting in InsightIDR, teams unify diverse data sets into cohesive, actionable insights and accelerate decision making. InsightIDR removes the distractions and streamlines critical security reporting, so your team can focus on what matters most.