RAPID7

SOLUTION BRIEF

Find Insights Faster

Powerful and Efficient Log Search with InsightIDR

You connect event sources across your environment, we do the rest

InsightIDR normalizes, attributes, enriches, analyzes, and unifies data from diverse event sources to make it easier to search your logs, make connections between them, and to understand what they're telling you. With a cloud-native, scalable log storage system at the core and a transparent, asset-based pricing model, you and your team can focus on collecting all of the relevant security data you need—no more trade offs or compromises.

Query log data and build custom detections in easy, intuitive search language

InsightIDR ties your entire environment together across search, dashboards, and detections with our powerful search language: Log Entry Query Language (LEQL).

With our LEQL search language you can run queries and functions across all of your data, no matter the source, and extract hidden data within your logs. Whether your data is structured and normalized or unstructured, you have the flexibility to have your data how you need it.

Key customer benefits:

- ✓ 13 months of readily searchable data by default
- ✓ Run queries across all your data, no matter the source with our unified search language
- ✓ Uplevel your investigation with automatically enriched log events
- ✓ Visualize your data with dozens of pre-built dashboards, or customize your own

Unlock fast, long-term-searchable log storage: 13 months by default

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.

Hunt and investigate like an elite SOC

Improve hunting and investigation capabilities with InsightIDR's timeline of enriched log events. All your data is automatically parsed to remove the noise and leave you with actionable telemetry. You can also extract log data that is most relevant to you with a Custom Parsing

Tool. Long-term log storage means you can search through months of raw data to bring context to events when you need it the most — like while investigating an attack that may have started months ago and is now coming to light.

Explore and visualize robust data sets with just a few clicks

Search your data how you want and when you need it.

- Explore your logs using LEQL, which supports keyword, key/value, and RegEx searches
- Group by multiple fields in your log searches for a more detailed view into your data
- Leverage pre-built cards and dashboards from our Dashboard Library, or create your own visualizations that best capture the dynamics of your network

Access your data faster

InsightIDR normalizes and enriches log data upon ingestion and prior to storage. They are then stored in log sets that are defined by an established structure or schema. This means your searches will be fast and not require re-indexing or hydrating your log data. If a need arises you can jump right in, query the data using the established schema, and start seeing results within seconds.

> **InsightIDR has really impressed me with how easy it is to use and set up. The alerting and the log search tools are fantastic as well**
>
> | Infrastructure Administrator via Gartner Peer Insights

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

To learn more or start a free trial, visit
www.rapid7.com/insightidr

Support

Customer Portal | Call +1.866.380.8113