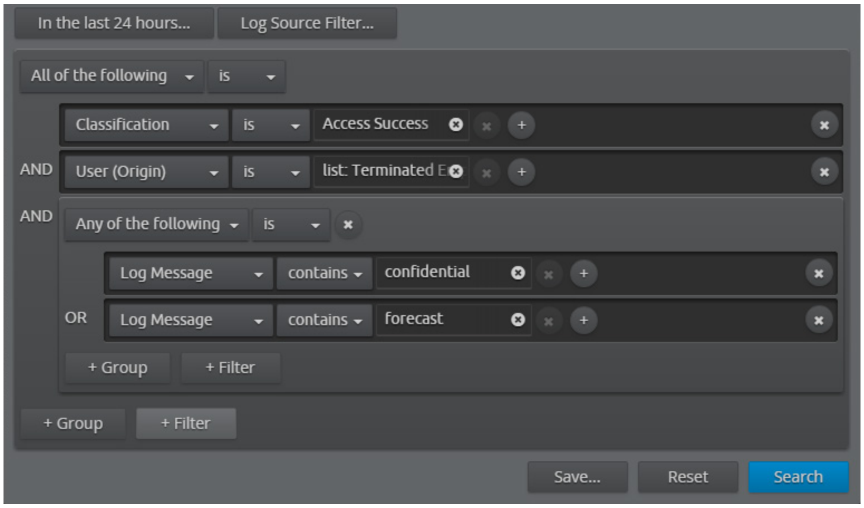
PRODUCT OVERVIEW

Precision Search

LogRhythm®
The Security Intelligence Company



All of the following is

Classification is Access Success

AND User (Origin) is list: Terminated E

AND Any of the following is

Log Message contains confidential

OR Log Message contains forecast

Advanced cyber-attacks are designed to bypass traditional security measures and some inevitably succeed. Rapid incident detection and response is critical for finding and stopping attacks before they cause serious damage. Most organizations, however, struggle to identify relevant event information due to the massive amounts of data generated by their environments.

Security analysts require immediate access to all of the context surrounding an attack. They need to rapidly find and understand data where context doesn't exist in order to quickly qualify threats, understand scope, and determine root cause.

LogRhythm Search expedites incident detection and response through faster analysis and deeper understanding of critical event details. An intuitive web console designed for security workflows simplifies search through a single, easy-to-use interface that delivers a powerful combination of contextualized and unstructured Search. A highly-performant Elasticsearch indexing tier delivers immediate and precise results at any scale.

Unified Search Interface

- Integrated Contextualized and Unstructured Search
  - Faster searches with relevant event context
  - Common interface for all Search types

Unstructured Search

- Search raw data from any source
- Keyword search across full text
- Search results automatically include structured metadata when available

Contextualized Search

- Higher precision results
  - Faster query building
  - Validated search syntax
- Automatic field population
- Clear and logical data presentation

Intuitive, Advanced Search Builder

- Simple interface
  - Streamlined creation of complex searches
  - Low learning curve
- Requires minimal understanding of indexing tier
- Integrated list capability for more precise results

Clustering

- Distributed Search across multiple nodes
  - Faster Search speeds
  - Larger data sets
- Information assurance through active/active failover
- Distributed indexing for real-time results

Machine Data Intelligence

- Event contextualization prebuilt for over 750 sources
- Comprehensive, logical event taxonomy with clearly worded metadata
  - Improved search accuracy
  - Rapid event understanding

Use Cases

- **Unstructured Search** can be used when the query parameters aren't clearly defined. A partial text string identified in a PCAP may be tied to a user account or a hostname. Using unstructured search to investigate the text string simplifies forensic analysis, while results that include processed logs are still returned in a structured format with all relevant metadata for greater context and usability.
- **Contextualized Search** for specific events automatically populates query parameter based on keystrokes for greater precision and eliminating failed investigations resulting from incorrect search strings. Integrated list management adds even greater precision. For example, when looking for forensic details surrounding an inbound attack, a blacklist of known bad IPs from a threat intelligence feed can be quickly added to search criteria, limiting results to show only relevant suspicious traffic.
- **Hybrid Contextualized and Unstructured Search** in a single interface makes investigations on the latest Indicators of Compromise (IOCs) faster. Unstructured Search can find a command and control executable across random registry hives. Adding contextual fields like the Destination IP and activity classification to the same search returns results faster and with greater precision.