panther

Security Data Lake Search, No SQL Required

The industry's first analyst-grade search experience with the efficiency and performance benefits of modern data lakes

Traditional solutions make critical high-volume log sources too costly and unwieldy to ingest and search at scale. This leads to fragmented investigations that can't match the speed and complexity of cloud security threats.

Panther's Security Data Lake Search redefines investigation workflows for cloud security. Teams can harness the full potential of mission-critical cloud logs for investigations, with cost-effective deployment options. Fast queries on multiple log sources drive complex search workflows across threat vectors, delivering an intuitive, powerful search experience for all skill levels.

zapier

"The search experience combined with the security data lake lets me immediately find, display, and correlate events across multiple sources, like AWS Cloudtrail and our Custom Logs, without having to resort to complex SQL statements."

MICHAEL KUCHERA
TEAM LEAD FOR SECURITY DETECTION AND RESPONSE, ZAPIER

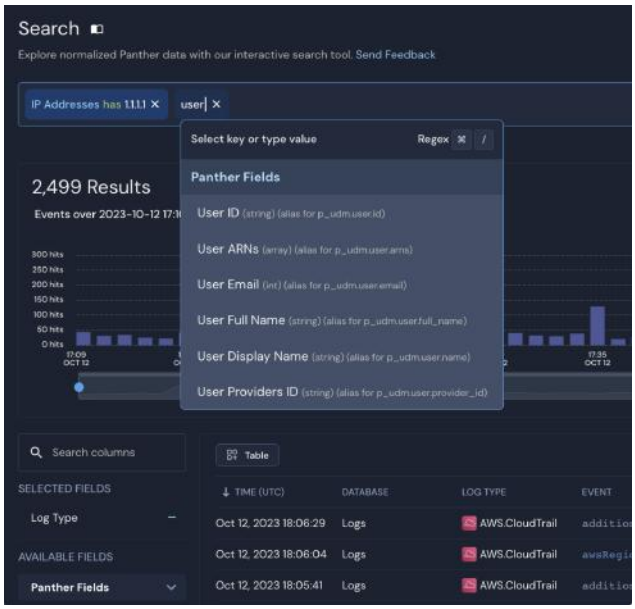
- No need for SQL. Build queries with an intuitive no-code UX
- Unparalleled search performance across long term hot data storage
- Comprehensive cross-log search results across all log types in your data lake
- Quickly query security logs, without knowing their structure beforehand

A Powerful, Intuitive Search Hub

- Unified search experience for fast, efficient investigation workflows
- No-code, click-to-build queries deliver cross log results
- Support for substring and wildcard searches

Enhanced Results Table

- Comprehensive visibility of events across log types
- Easily pivot based on results in view
- Flexible tables with ability to add/remove columns
- Support for investigations on potentially correlated events



Panther Overcomes Other Tools' Search Limitations

PANTHER	OTHER TOOLS
✓ SQL-free search complex yet intuitive queries	✗ Knowledge of SQL or SPL required
✓ Cross-log search results for powerful correlation insights	✗ One log type per query limits insights into more nuanced attacks
✓ One year of hot data storage for faster search results	✗ Limited hot data storage, expensive cold storage
✓ Paired with dectection-as-code for high-fidelity incident response workflows	✗ No modern detection-as-code features, limiting incident response effectiveness

SEE HOW PANTHER DRIVES FAST, EFFECTIVE INVESTIGATIONS

Request a Demo