AWN CyberSOC Log Search

Log Search for Arctic Wolf's AWN CyberSOC™ service brings IT organizations improved visibility into their operational and cybersecurity posture. Log Search lets AWN CyberSOC customers query log data ingested by the service so they can better answer operational and security questions and achieve greater understanding into key aspects of their organization. An add-on to the AWN CyberSOC threat detection and response service, AWN CyberSOC Log Search enables you to query your log data from not only on-premises systems, but cloud SaaS and IaaS sources as well.

Log Search Unlocks New Insights

The intuitive AWN CyberSOC Log Search interface permits you to quickly harvest operational and security insights by searching your accumulated log data. It also provides pre-defined queries that function as templates for common searches. Its dynamic histogram of search results allows you to view data "hotspots." What's more, Log Search enables you to download query results for further analysis using your own toolset.

Discover answers to common IT issues, including:

Operational Questions

- Validate IT configuration changes
- Use login information to answer employee productivity questions
- Determine if a user has been locked out of their account
- Find out who is using Pandora.com (or other specific URLs)
- O365
  - What login failures have occured?
  - Was email sent to a user?
  - Terminated employee activity

Technical Questions

- Investigate failed login attempts (AD log information or O365)
- Search operational information needed for audits
- Locate a change event—firewall, router, AD GPO, or any other log source
- Verify that a firewall is denying or allowing a connection
- Validate users logging into servers or that servers are being used

Improve IT Operations with Log Search

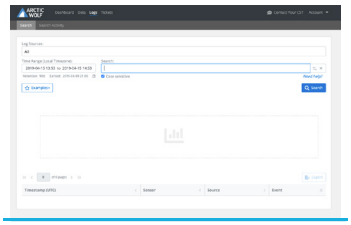
Improve IT staff productivity

- Intuitive interface answers questions quickly
- Pre-defined queries simplify searching
- Single, unified log repository to answer operational and security questions

Log Sources :

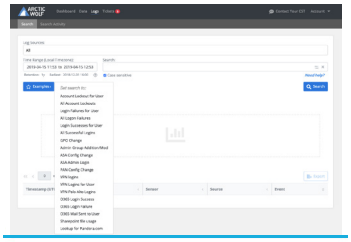
- All on-premises security and operational log data
- Cloud SaaS and IaaS data

Log Search: Simplicity Enables Quick Answers



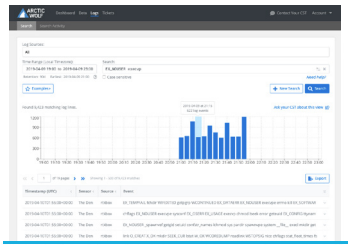
Intuitive Log Search Interface

Simple interface enables users to quickly use log search tool.



Query Examples Speed Answers

Example templates for frequent searches facilitates rapid searching of data to harvest insights from operational log information.



Histogram Summary Shows Hotspots

Search results include a histogram summary to understand data hotspots.

The Industry's Fiercest SOC-as-a-Service

A security operations center (SOC) is the most essential element of modern security. But a SOC is expensive to build, complicated to manage, and far beyond the reach of most small to midsize enterprises. So, many take the easy route and invest in new point security products, which is no guarantee of better protection. The cloud-based AWN CyberSOC™ service provides comprehensive 24x7 monitoring of both your on-premises network infrastructure and your cloud-native SaaS and IaaS applications. AWN CyberSOC™ services are anchored by Concierge Security™ teams who provide custom threat hunting, alerting, and reporting. Arctic Wolf's purpose-built, cloud-based service offers 24×7 monitoring, risk management, threat detection, and response.

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com