LogicHub Managed SIEM

The Capabilities You Need at 1/5th the Cost

Why LogicHub Managed SIEM?

It's time to rethink your approach to SIEM. Traditional platform-based SIEM solutions are built on 20 year old technology, and even most cloud-based solutions are held back by inefficient, outdated architectures.

If you don't already have a SIEM, now you can do it without worrying about the typical operational problems that may have derailed a deployment in the past.

LogicHub delivers:

Automated Alert Triage

Intelligent Decision Automation analyzes and triages SIEM alerts to eliminate 95% or more of the false positives that overwhelm traditional SIEMs.

High Performance Search

A search-optimized format data layer delivers rapid access and ad hoc investigations. Long term data can be easily pulled into the search-optimized tier at any time, but you only pay for what you use.

The LogicHub Advantage

- All the SIEM capabilities you need for 1/5th the cost
  - Pay only for the storage you need
  - Minimal operating overhead
- Automated deep threat detection
- Intelligent decision automation to eliminate false positives
- Modern storage architecture based on logical data usage
  - Near term data layer optimized for analyst search
  - Long term data layer optimized for machine-based analytics
  - Easily move data between storage layers as needed

Affordable Enterprise Scalability

A long term data store operates at a fraction of the cost, and is machine optimized for automated detection playbooks to deliver continuous value without blowing up your budget.

Deep Threat Detection

Automated detection playbooks analyze all data at machine speeds, accurately identifying true threats faster, without the high positive rates typically associated with SIEM alerts.

Machine Automated Threat Hunting

Automated threat hunting playbooks continuously search through long term storage, optimized for machine based analysis, for hidden threats that would otherwise go undetected.

Modern Data Architecture

Combining the high performance search capabilities of Spark with the low cost scalability of Amazon S3 buckets delivers the right data retention at a fraction of the cost of traditional SIEM.

LogicHub Managed SIEM delivers all of the compliance and security capabilities you're looking for in a SIEM, at a fraction of the cost of traditional platforms and cloud-based services. With a modern architecture built on Spark and S3, it delivers 24x7 guaranteed collection and monitoring of all your log data, while significantly reducing your overhead and licensing costs.

A New Data Architecture That Works for You

SIEM is the cornerstone of any enterprise security stack. Whether it's for compliance, internal auditing, or advanced correlation and threat detection, almost every security operations team needs to collect, monitor, and analyze log data. But as the volume of data has exploded and retention requirements continue, the high cost of storage alone has increasingly made SIEM excessively expensive.

LogicHub's cloud-native SIEM platform uses the high performance capabilities of Spark and low cost S3 buckets to deliver scalable log collection and retention that stores data in whatever format is optimal for your specific needs. A search-optimized datastore allows you to rapidly find whatever data you need, for immediate forensic investigations. For everything else, a long-term, machine-optimized data lake stores your data in the most cost effective way, without limiting deep threat detection or threat hunting capabilities. And it's simple to move data between tiers whenever you need to.

Key Components

Modern Storage Architecture

- Data optimized by need
  - 30 days near term search optimized (default)
  - 1 year long term machine optimized (default)
  - Easily move data between storage tiers as needed
- Guaranteed, 24/7 collection for compliance
- Secure, multi-tenant environment

Deep Threat Detection

- 24x7 monitoring and advanced analytics
- >95% reduction in false postitives
- Automated, continuous threat hunting
- Confirmed cases with complete event context

No Operating Overhead

- Fully managed setup and administration
- Expert-defined and configured deep threat detection rules
- Cost effective, cloud native infrastructure
- Seemless integration with the LogicHub MDR service

To learn more about the LogicHub SOAR+ platform visit: logichub.com/SOAR

LogicHub

301 N Whisman Rd Mountain View, CA 94043
info@logichub.com • tel 650- 262-3756
logichub.com