Why Logz.io Cloud SIEM?

Agile SIEM for modern security teams, built on a scalable and secure SaaS platform

Your organization needs a SIEM delivering advanced threat analysis and investigation with less complexity and cost. Logz.io Cloud SIEM meets the needs of the current security environment, addressing slow investigation, time-consuming management and understaffed SOC teams. Logz.io believes SIEM requires a unique model—from product features, to customer support, to licensing and storage. You'll get:

- Fast querying
- Multidimensional detection
- Deep customizable security content
- Unparalleled customer support

Monitor and investigate threats across the full-expanse of your cloud environment—with no performance degradation, regardless of data volumes. Logz.io removes SIEM management pain.

How Logz.io Cloud SIEM extends your team

Parsing as a service

Automatically parses logs shipped from many platforms, services, containers, servers for faster onboarding.

Content as a service

SIEM experts help write custom rules to reduce false positives and enable precision analysis for continuous improvement.

Data & Storage Optimization

Hands-on guidance and technical capabilities that highlight and ensure ongoing cost efficiency for adaptive cost control.

Faster Onboarding → Continuous Improvement → Adaptive Cost Control

Supported Customer Journey

Phase 1:
Logz.io Cloud SIEM account configured by your Customer Success Engineer

Phase 2:
Simply and quickly ship your data from any source at any scale, from the cloud or on-prem

Phase 3:
See immediate value within minutes, as data starts populating the SIEM

Phase 4:
Review and query data using hundreds of detection rules and curated dashboards

Phase 5:
Get advice from Logz.io security experts at no extra cost to optimize your SIEM deployment

logz.io

The Logz.io Difference - Targeted and Effective SIEM

Before, organizations with massive data volumes and limited time & expertise faced increased risk and perpetually high complexity & exposure.

With Logz.io Cloud SIEM, that transforms thanks to the following:

Data Prioritization

Supervised ML separates critical data from noise

Tailored Analysis

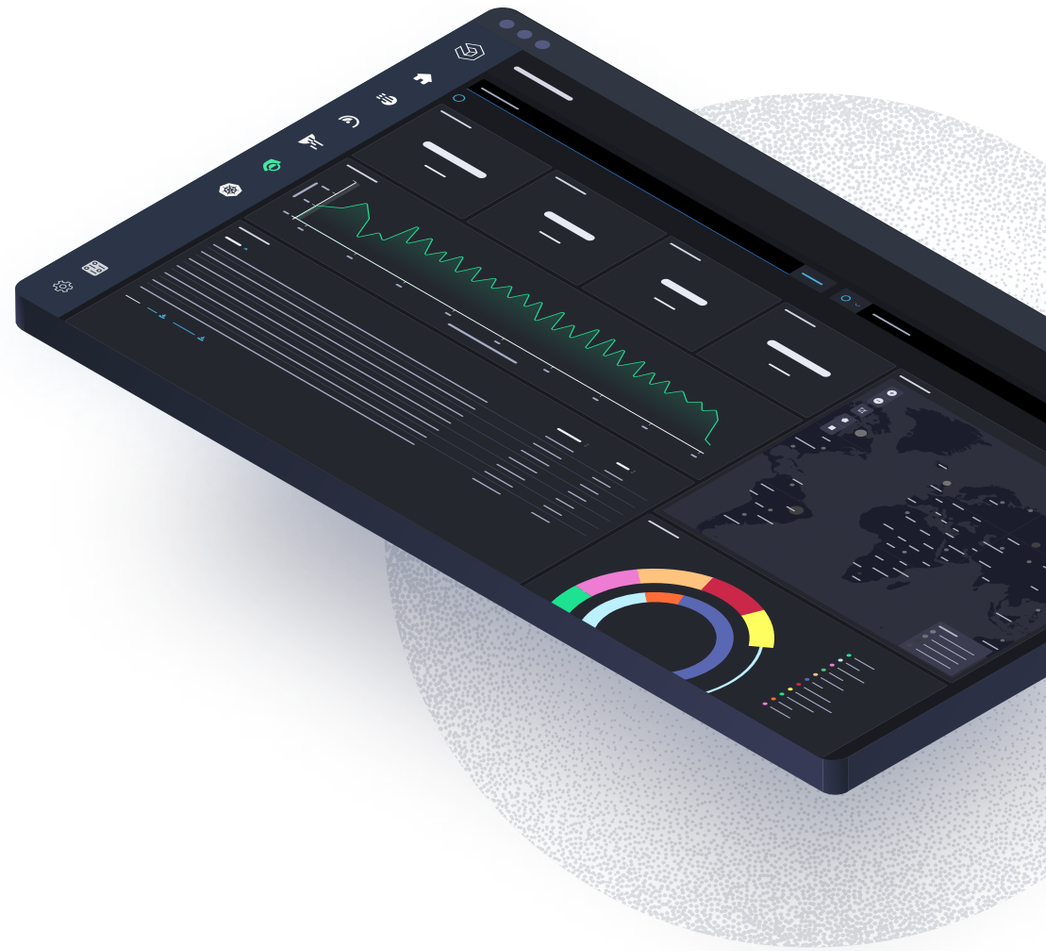
Custom & onboard rules, queries & dashboards

Curated Intelligence

Combining leading & custom threat intel feeds

Archive + Restore

Tiered data retention & availability



Enabling Technologies

Dynamic Lookups:

Maintain dynamic lists for use in alerting through advanced querying of external systems and correlation with log detections.

Data Enrichment & Workflow:

Using Event Management workflows, investigate, remediate and close every event faster with increased efficiency.

Cost-Effective Architecture:

Use intelligent ingestion pipeline to filter and correlate data. Smart storage architecture automatically moves data between tiers for fast queries over longer time periods.

Your Data Is Safe