CHAOSSEARCH

SOLUTION BRIEF

THE CHAOSSEARCH DATA LAKE PLATFORM

# Scalable Log Analytics for Security Operations and Threat Hunting

## CHALLENGE

### Traditional Log Management Systems Don't Meet the Needs of Today's Secops Teams

SecOps teams rely on access to massive data sets from a wide range of sources to effectively identify and mitigate threats. In addition, they also need longer data retention to defend against advanced persistent threats (APTs) and meet new regulatory and compliance mandates.

However, the volume and variety of log data has demonstrated that traditional log management systems and SIEMs cannot efficiently scale. SecOps teams are forced to make risky tradeoffs between the breadth of captured data and how long they can retain it. This tradeoff can result in vulnerabilities that nefarious actors are more than happy to exploit.

The need for quantity and quality of log data made available to the SecOps team has exposed the shortcomings of SIEMs and traditional log management tools at scale:

#### Limited Data Retention

APTs can span 200 days or more. And anomaly detection requires an historical baseline. But SecOps teams are often forced to make trade-offs in log retention due to the high cost and unreliability of storing log data at scale.

#### Data Movement and Lack Of Data Ownership and Controls

The mix of on-premises and cloud infrastructure complicates log and data ownership and controls. Moving data in and out of central storage into analytics platforms and back is not only costly, it can break chain of custody and compliance mandates for data controls.

#### No Single Source of Truth

With log data captured and stored in multiple systems, organizations lack a single source of truth. Threat hunters need access to data sources that gives them visibility into host and network activities as well as telemetry data collected by security infrastructure.

#### High Storage Costs

A SIEM serves a critical function, but they are not designed to store large volumes of log data for long periods of time. Without centralized log management, relying on your SIEM for long-term retention increases storage and license fees.

## A BETTER APPROACH TO THREAT HUNTING

Imagine sending all your data to your cloud environment in its native format—no parsing or schema changes. ChaosSearch indexes all data as-is, without transformation, while auto-detecting native schemas. With cost effective unlimited retention for all sources of security telemetry, you have the ability to analyze the lifecycle of all threats and their origins.

## SCALABLE LOG ANALYTICS FOR SECURITY OPERATIONS AND THREAT HUNTING

### Scalable Log Analytics for Application Troubleshooting and DevOps Efficiency

ChaosSearch enables customers to Know Better™, activating the data lake for analytics. Unlike traditional log management and SIEM tools, ChaosSearch indexes all log data in your cloud object storage, as-is, without the need for any data transformation or data movement.

ChaosSearch complements the best-of-breed functionality of SIEM tools with centralized log management that enhances threat hunting and compliance efforts. SecOps teams can deploy ChaosSearch in parallel with a SIEM, can split log data with the SIEM, or can simply ingest the log data from the SIEM. With a SIEM and ChaosSearch, organizations can more efficiently ingest and index a wide variety of data types from a wide variety of sources at speed. They can also add more data sources without needing to re-extract, transform and load (ETL) data.

#### Unlimited Data Retention

ChaosSearch treats your cloud object storage (AWS/S3, GCP/CS) as first-class citizens allowing unlimited retention and scalability at much lower cost. ChaosSearch gives SecOps teams the capability to proactively fight long tail intrusions including advanced persistent threats as well as retain more data for compliance reporting and audits.

#### A Single Source of Truth

Whether deployed with a SIEM or standalone, ChaosSearch centralizes all logs from CDNs, edge devices, network and core infrastructure, as well as your cybersecurity tools to better respond to more persistent attacks, tighter regulations and compliance mandates. And built-in alerts let you set thresholds to tag and automate response to threats in near real time.

#### No Data Movement

ChaosSearch indexes the data in your cloud environment while auto-detecting native data schemas—no complex pipelines, no data transformation, or parsing on ingest. You also retain complete control over your data with full RBAC and all security controls, durability, and reliability of a cloud service.

#### Dramatically Reduce Costs

With a virtually unlimited total capacity, you can maintain long-term data retention, avoiding the painful "cost vs. retention" tradeoffs prevalent with SIEM tools. You'll reduce your storage costs, minimize duplicate data, and reduce SIEM license costs.

**SIEM tools are a critical part of maintaining your security posture on premises and in the cloud. ChaosSearch complements SIEM platforms by optimizing log coverage so SecOps teams can incorporate more data sources, retain data indefinitely, and enhance their threat hunting capabilities and compliance reporting.**

**SecOps teams often turn to IT and DevOps teams to gain access to more log data during a security event or audit. Those teams often rely on an Elasticsearch stack, either on-premises or hosted in the cloud. ChaosSearch commonly replaces the Elasticsearch stack, yielding massive cost-performance improvements (up to 80% TCO savings), without any data movement or behavior change needed from end users.**

> *"Deploying ChaosSearch alongside Splunk, this new system extends the company's data retention periods from weeks to years—enabling trend analyses over longer periods of time. With this capability, the company can better adapt to rapidly shifting shopper behaviors, complex data privacy laws, and security requirements."*
>
> **European Fintech Provider**

## ABOUT CHAOSSEARCH

ChaosSearch empowers data-driven businesses like Blackboard, Equifax, and Klarna to Know Better™, delivering data insights at scale while fulfilling the true promise of data lake economics. The ChaosSearch Data Lake Platform indexes a customer's cloud data, rendering it fully searchable and enabling data analytics at scale with massive reductions of time, cost and complexity. The Boston-based company raised $40M Series B in December 2020 and is hiring to support its hyper growth.

**For more information, visit ChaosSearch.io or follow us on Twitter @ChaosSearch and LinkedIn.**

info@chaossearch.com | www.chaossearch.io