Case Study:

GLOBAL INSURANCE PROVIDER

Industry: Global Insurance & Risk Management

Company Size: Enterprise

Headquarters: North America, with numerous global locations

Products: Gurucul UEBA (User and Entity Behavior Analytics) and Gurucul Next-Gen SIEM

The Organization

This Fortune 500 insurance provider delivers risk management solutions across various industries, offering specialized coverage options such as property, auto, casualty, device protection and financial assurance. Operating in 20+ countries, the company focuses on digital transformation and security resilience to protect its vast enterprise data environment.

Project Goals:

- Replace Exabeam SIEM with a modern, stable and scalable security analytics platform.
- Ensure new SIEM replacement runs efficiently on the company's existing Snowflake data lake for enterprise-scale security monitoring with seamless data integration.
- Utilize behavioral analytics and UEBA models for high-value detections.
- Overcome challenges related to query performance, data ingestion, and operational inefficiencies.
- Enable flexible rule creation, automated workflows, and seamless data management.

Customer Results

Replaced unreliable Exabeam solution with Gurucul's Next-Gen SIEM and UEBA in a unified platform, fully integrated with Snowflake, their data lake of choice, to deliver real-time threat detection, reduced false positives, and streamlined security operations with enhanced performance and scalability.

Outcomes

- **Replaced Exabeam with Gurucul Next-Gen SIEM with advanced security analytics.**
- **Streamlined security operations through Gurucul's automation and AI-driven detection models with model-chaining, contextual insights and dynamic risk-scoring.**
- **Created data pipeline optimization and fast migration to Snowflake's data lake with easy integration and operability.**
- **By using Gurucul UEBA they were able to ingest all relevant security—regardless of format, source, or IT estate—and present contextualized analysis on a single, unified platform reducing operations efforts.**
- **Gurucul brought stability to the environment allowing the company to scale faster.**

The Challenge

This global leader in insurance and risk management has a worldwide presence with 13,000+ employees and brings in over $11 billion in revenue. The company faced mounting challenges with its security operations. Its existing SIEM solution, Exabeam, failed to meet performance benchmarks and lacked the flexibility to integrate seamlessly with their Snowflake data lake.

Gurucul

Why Gurucul?

Fast Migration – Gurucul quickly migrated Exabeam rules to Gurucul models using the rule migration app.

Gurucul's Next-Gen SIEM with Snowflake – Successful SIEM migration to Gurucul Next-Gen SIEM using Snowflake data lake at full enterprise scale with full feature parity.

Advanced Behavioral Analytics – Gurucul's AI and ML-driven detection models enhanced threat identification creating high-value detections which enabled faster response times with confidence.

Flexible & Scalable Architecture – Supported large-scale data ingestion without performance bottlenecks.

Real-Time Threat Detection – Gurucul delivered immediate alerts upon data ingestion (1-2 minutes response time) for faster query results, successfully exceeding stringent customer benchmarks.

Operational Efficiency & Cost Reduction – Gurucul reduced storage costs while increasing security efficiency through automation.

Replaced Exabeam with Gurucul Next-Gen SIEM and UEBA

With Exabeam they faced numerous challenges including limited performance and scalability with delayed threat detection and response. As the company expanded its security operations, Exabeam struggled to keep up. Exabeam had a lack of integration and automation that led to problems utilizing their centralized Snowflake data lake. That created bottlenecks that led to slow queries and inefficient data retrievals causing delays in investigations. Exabeam was not meeting their rigorous security benchmarks.

They needed a solution that could scale with their growing data demands while delivering real-time, accurate threat detection. Gurucul's high-performance Next-Gen SIEM provided the scalability and radical clarity required to ingest and decipher large data volumes without compromising performance benchmarks enabling streamlined security operations while seamlessly integrating with Snowflake. With UEBA-driven behavioral anomaly detection and contextual insights, the company could generate dynamic risk scores, effectively identifying real threats while minimizing false positives. This significantly improved analyst efficiency, allowing them to focus on genuine security risks instead of wasting time on irrelevant alerts.

Seamless Integration with Snowflake's Data Lake

The Exabeam solution had storage issues. Gurucul's REVEAL platform is data lake agnostic and works with any data storage. By leveraging Gurucul and Snowflake's easy integration, the company was able to eliminate redundant data storage by leveraging Snowflake's centralized location ensuring that data is not duplicated. This allowed for optimized ingestion and the ability to leverage out-of-the-box pipelines to ensure faster data processing, filtering and enrichment through a unified and integrated user interface (UI) significantly reducing investigation times while helping to maintain the company's demanding performance requirements.

By eliminating the need for a proprietary data lake, Gurucul significantly reduced storage costs for the company. Additionally, with Gurucul's federated search, the company could query data across both hot and cold storage without the need for rehydration, ensuring faster access to historical data while optimizing costs.

Reduced False Positives In Real Time

Exabeam's SIEM was cumbersome and time-consuming, creating too many false positives that overwhelmed analysts, inhibiting their ability to identify actual threats. Gurucul's AI-driven behavioral-based threat detection models with machine learning and real-time analytics reduced false positives while prioritizing high-risk alerts. This allowed the company to reduce response times from hours to minutes, significantly reducing time to detection for analysts. Gurucul's

> Reduced response times from hours to minutes

customizable detection rules and unique model chaining feature allowed the company to tailor security models to its specific use cases, enhancing overall threat detection accuracy.

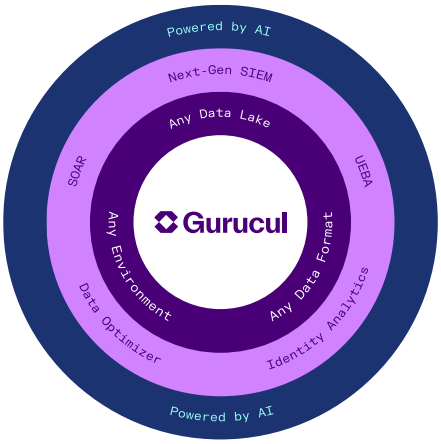
Stable and Predictable Security Operations

Exabeam often caused disruptions that negatively impacted workflows with unexpected ad-hoc configuration changes that were made without adequate notification, leading to system instability. The company was not enabled to create new models to satisfy custom use cases on Exabeam. They liked that Gurucul's solution is fully customizable to any use case today or that might emerge in the future. That coupled with a general lack of timely and quality support from Exabeam, the company decided to look for the modern solution they found in Gurucul.

Security Analytics Beyond Expectations

Gurucul enabled this Fortune 500 insurance provider to replace its legacy SIEM with a modern, scalable security analytics platform, seamlessly integrating with Snowflake to enhance security operations. By leveraging AI-driven behavioral analytics and UEBA, the company achieved real-time threat detection, significantly reducing false positives and improving analyst efficiency. Gurucul's optimized data pipelines streamlined ingestion, query performance, and operational workflows, ensuring stability and predictability in security operations.

Additionally, the platform accelerated rule migration, reduced investigation times, and lowered storage costs by eliminating redundant data duplication. With Gurucul, the organization strengthened its security posture while achieving cost savings and operational efficiency.



In summary, migrating to Gurucul's unified security analytics platform REVEAL transforms security operations with proactive threat detection, intelligent automation, and easy integrations. Gurucul's AI-powered security analytics platform integrates seamlessly with existing IT environments both on-prem and cloud, ingesting structured and unstructured big data from any source. Advanced correlation, risk scoring, and automated response mechanisms empower organizations to proactively detect and mitigate security risks. The platform's open architecture supports dynamic scaling, ensuring adaptability to evolving threats while maintaining operational efficiency.

About Gurucul

Gurucul is the only cost-optimized security analytics company founded in data science that delivers radical clarity about cyber risk. Our REVEAL security analytics platform analyzes enterprise data at scale using machine learning and artificial intelligence. Instead of useless alerts, you get real-time, actionable information about true threats and their associated risk. The platform is open, flexible and cloud native. It conforms to your business requirements so you don't have to compromise. Our technology has earned us recognition from leading industry analysts as the most Visionary platform and an Overall leader in product, market and innovation. Our solutions are used by Global 1000 enterprises and government agencies to minimize their cybersecurity risk. To learn more, visit Gurucul.com and follow us on LinkedIn and Twitter.

Gurucul | 222 North Pacific Coast Highway, Suite 1310 | El Segundo, CA 90245 | 213-259-8472 | sales@gurucul.com |