Solve Security Problems More Efficiently

RIVERSAFE
INTEGRITY, INNOVATION, IMPACT

SCENARIO:

The customer wants to better operationalize Exabeam in the SOC, including improving processes for event management, taking events from triage to resolution, and optimizing their Exabeam deployment.

SOLUTION:

By working with SOC L3 analysts through investigations of Exabeam events, RiverSafe aligns Exabeam end-to-end across the customer's security operations. They can establish best practices for threat hunting and for use of Exabeam for security analytics.

WHAT PAST CUSTOMERS HAVE ACHIEVED:

- Documented Exabeam best practices for threat hunting and incident response.
- Applied knowledge to actively conduct investigations and generate usable data.
- Understood Exabeam's role within their technology ecosystem.
- Drove the improvement of data quality for ingested sources

exabeam

RIVERSAFE'S OPTIMIZATION SERVICES

- **ASSESS** existing SOC processes against goals and objectives.
- **REVIEW** Exabeam behavioral models and the quality of log data being ingested.
- **ANALYZE** for gaps and identified areas for improvement across both technology and processes.
- **IMPROVE** technology and processes by creating a number of remediation categories: event validation, noise reduction, search optimization.

WHAT'S THE ESTIMATED LEVEL OF EFFORT?

- Duration of 12 weeks
- 2 staff: security operations personnel and 1 manager for oversight
- Customer support team contribute approximately 20-25% of their time, including a SOC manager and part-time support by analysts.