PRESIDIO® | Case Study

Energy

A Fortune 500 energy firm closed its security blind spots without betting on a single vendor

The Outcome

A leading independent oil and gas producer replaced a failing custom-built SIEM with a hybrid solution pairing Splunk and Exabeam - giving the security team full visibility across Azure and three on-premise data centers, faster threat detection, and automated response workflows, without locking the firm into a single vendor.

How They Got There

Presidio assessed the full IT environment and ran structured proof-of-concept tests on the two strongest SIEM candidates. Splunk proved superior for high-performance log management. Exabeam for behavioral threat detection and ease of management. Rather than choosing, Presidio recommended running both - they integrate cleanly and cover each other's gaps.

Why It Worked

The IT team was treating SIEM selection as a binary decision. Presidio's vendor-agnostic approach reframed the question. Exabeam captures full incident context fast; Splunk pinpoints cause and scope through log correlation. Together they compress detection-to-containment time and both connect to the firm's existing Phantom SOAR platform.

The Situation

A Fortune 500 oil and gas producer operating across three data centers and Azure was running a custom-built open source SIEM that was degrading in performance. When the only developer who understood it planned to leave, the firm decided to transition to an off-the-shelf solution, but the IT team had internal disagreement on which platform was right for their environment.

The Approach

Presidio assembled a security team to assess the firm's full IT environment and existing security tooling, then presented the strengths of multiple SIEM platforms before narrowing to the two strongest: Splunk Core for high-performance logging and Exabeam Advanced Analytics for behavioral analysis. Presidio ran structured proof-of-concept tests on both and recommended deploying them together. Both integrate with the firm's existing Phantom SOAR platform for automated mitigation workflows.

The Result

The energy firm now has full visibility across its Azure environment and all three on-premise data centers. Detection-to-containment time is compressed: Exabeam captures incident context rapidly, Splunk correlates logs to pinpoint cause and scope, and machine learning generates prebuilt incident timelines automatically. The firm is not locked into a single vendor as infrastructure scales.

Hybrid

Splunk + Exabeam - two best-of-breed platforms, one integrated solution

Faster

Threat detection across Azure cloud and 3 on-premise data centers

SOAR

Integrated with Phantom for automated mitigation workflows

Cybersecurity | SIEM | Splunk | Exabeam | Oil & Gas | Threat Detection

PRESIDIO®