PRESIDIO®

CASE STUDY

splunk> | exabeam

Presidio Hybrid SIEM Solution scales security for Fortune 500 energy firm

THE CUSTOMER

Headquartered in the Southwest region of the United States, the client is a Fortune 500 company listed in the S&P 500 Index. They are one of the leading independent oil and natural gas exploration and producers, with a primary focus of onshore operations in the United States. Every day, the energy firm produces approximately 100,000+ barrels of oil, 550+ million cubic feet of natural gas, and 50,000+ barrels of natural gas liquids.

THE CHALLENGE

The energy firm's IT infrastructure runs across three data centers and the Microsoft Azure platform in the cloud. As the infrastructure began to scale, the company's custom open source Security Incident and Event Management (SIEM) solution began to experience degraded performance.

When the developer of the application planned to move into a new role, the client decided to transition away from an open source solution, knowing custom-built SIEMs are more difficult to support. But the IT team had varying perspectives on which off-the-shelf SIEM solution would work best in the energy firm's environment. That's when the team turned to Presidio as its long-time trusted IT partner.

THE APPROACH

Presidio assembled an expert security team to assess the IT infrastructure and other security tools that were already deployed. Presidio then presented the strengths of multiple SIEM platforms that offered best-of-breed solutions.

The Presidio team helped the gas and oil company narrow its choices down to two SIEM solutions—Splunk Core (DataLake) and Exabeam Advanced Analytics—and set up two proofof-concept tests to determine which one would best meet the energy firm's needs. Splunk proved strong for its highperformance logging capabilities, while Exabeam Analytics impressed for its overall security analysis capabilities and ease of management. Given that both solutions offered value for the client, Presidio recommended a hybrid approach: use both solutions.

Integrating the two platforms is easy, and together, they provide all the capabilities the client's IT team required. The gas and oil company also benefited from the ability to eventually integrate both solutions with Phantom, which the IT team uses for Security Orchestration Automation and Response (SOAR).

THE RESULTS

The combination of the Splunk and Exabeam solutions gives the company the ability to reduce the time to detect cyber attacks since the IT team can quickly analyze machine data from the Azure cloud and the three on-premises data centers. With full visibility into malicious threats, the energy firm can also streamline investigations of activities associated with each threat and respond with automated mitigation workflows.

In addition, the company benefits from modern behavioral modeling and analysis powered by machine learning. This combination generates prebuilt timelines to enable the IT team to automatically reconstruct security incidents and a common framework to describe attacker tactics and techniques.

The client was particularly impressed with how quickly Exabeam captured all the contextual data of security incidents, which can then be synchronized with Splunk logs to pinpoint the cause and extent of any security attacks. This, in turn, reduces the amount of time it takes for the IT team to quarantine and mitigate cyberattacks.

By collaborating with Presidio and trusting the technologyagnostic approach, the oil and gas company was able to design and deploy a SIEM solution that meets all its security incident and management needs. The energy firm was also not locked into a single vendor solution that limits the capabilities of the IT team in protecting the firm's digital assets as the IT infrastructure continues to scale.

FOR MORE INFORMATION
CONTACT US AT
INQUIRIES@PRESIDIO.COM