TekStream's Managed Detection and Response Service Secures Client Data and Lowers Annual Fees

splunk>partner+

2022 AMER Cloud Partner of the Year
- 2021 Global Professional Services
- 2021 AMER Professional Services

allied global marketing

Location: Los Angeles, CA

Industry: Marketing

Products/Services: Full-service integrated marketing agency working with the world's largest entertainment, consumer, and lifestyle brands.

Employees: 200-500

Business Challenge

As a global media buying powerhouse, Allied Global Marketing provides integrated marketing services for some of the world's largest brands. Typically, these brands require stringent contractual provisions on data privacy and security. Failure to meet these requirements could result in multi-million-dollar fines, and the loss of $100M+ clients.

Allied Global's legacy security monitoring and response system was unable to keep up with the exponentially increasing complexity of their IT environment. They needed to rapidly enhance their security posture to protect their corporate and their clients' data, and to remain in compliance with their contractual responsibilities.

Allied Global selected Splunk for its best-in-class security monitoring and management of their digital platforms. Since their staff had limited Splunk experience, Allied Global engaged TekStream Solutions, a managed security company with deep Splunk expertise, to help them configure their Splunk environment, establish best practices, and train their internal team to best utilize their new tools.

"TekStream didn't show up with a cookie-cutter process. They took the time to understand our specific needs and develop a custom solution. Through their guidance and training, we were able to improve our Splunk ROI and build a team of internal subject matter experts."

— Brian Weir,
SVP Information Technology
Allied Global

Key Pain Points

Current security monitoring tools were inadequate for their revolving IT environment

Current IT support partner was not an expert in Splunk and was inflexible in their managed support offering

The internal team had limited experience and confidence with Splunk

Risk of overpaying their Splunk usage license due to inefficient data ingestion

How we fixed it:

TekStream implemented an approach to maximize Allied Global Marketing's Splunk investment while ensuring the company's security posture was constantly being evaluated and improved across three critical security measurements (Visibility, Fidelity, and Automation). TekStream then developed a custom Splunk implementation plan built around Allied Global's specific business needs and expectations. This helped ensure Allied Global received the exact monitoring and incident detection they needed from the solution.

The TekStream team leveraged their 360° understanding of Allied Global's business and identified key opportunities to lower Allied Global's annual Splunk fees by streamlining its data ingestion. **This resulted in a saving of $75,000 per year in licensing fees.**

A robust training regimen provided Allied Global's internal security team the necessary skills to best use Splunk to monitor and detect abnormal behavior. TekStream continues to work hand-in-hand with Allied Global's team to expand their internal Splunk capabilities for improving their security and incident detection, response, remediation, and future prevention.

Not only has this training helped maximize the Allied Global team's understanding of Splunk, it has also helped them better serve their clients and reduce the risk of data breaches. Together, the internal staff and TekStream work cohesively to keep the company's global operations secure and operating efficiently.

Key Successes:

✓ TekStream established an operational model that delivered immediate increases in security posture and contractual compliance.

✓ TekStream identified $75,000 in annual Splunk licensing saving by better rationalizing their data ingestion.

✓ TekStream provided greater visibility, fidelity, and automation through custom dashboards that called out false positives and applied automation to identify what needed a response.

✓ Through robust training, TekStream improved Allied Global's internal team's confidence in utilizing Splunk to meet the security needs of their operations.

splunk>partner+

Technology Involved

- TekStream MDR
- Splunk Enterprise with InfoSec
- Security Essentials