EventTracker simplifies SIEM for labor union

Analyst: Javvad Malik

23 Mar, 2015

A large labor organization with 350 staff serving more than 300,000 members across North America was seeking a log management offering that would help it meet government data-security requirements, as well as support its IT team – it needed a platform that would integrate easily with the company's IT environment, as well as meet the regulatory requirements that the company is obliged to comply with. The organization also wanted to work with a vendor that has a managed service element that could augment its internal 12-member IT team.

Early Adopter Snapshot

As a business that undertakes sensitive data exchanges with government agencies, the company needed to adhere to strict government requirements, such as NIST800-53 and the Federal Information Security Management Act. But it also needed a SIEM offering that could be manageable by the existing team of 12 dedicated IT staff. Many offerings were ruled out due to their complexity and the additional staffing requirements they would entail. The final two products came down to Splunk and EventTracker, and EventTracker stuck out as not only being more affordable but also having the services component in SIEM Simplified that would augment the internal team in delivering security.

The 451 Take

Many enterprises have IT departments that are stretched to the limit, so despite needing a SIEM offering, they are unable to take full advantage of the platform because of the resource requirements to both deploy and run it. EventTracker targets such firms with an offering that is not only streamlined, but also has a managed service offering that can help augment struggling IT teams. We see such offerings as key to helping SMBs and enterprises meet their security needs in an efficient manner.

Deployment summary

The labor organization opted for an enterprise-wide deployment from the start by deploying agents on desktops, servers, endpoints and firewalls across its estate of roughly 500 devices, all within the first week of rollout. With regard to deployment, the IT manager said that it was a relatively easy affair, and the company didn't have to spend a lot of time on initial configuration.

About six months after rolling out EventTracker SIEM Simplified, the company hired its first full-time information security staff member, who has since fine-tuned devices, bringing further efficiencies to the platform. Bringing all the data from devices and security tools into SIEM Simplified has allowed the company to detect activity that it says would have previously gone unnoticed. In isolation, suspicious external traffic, accounts added to groups they shouldn't belong to, and logins from unknown geographies might not be true security incidents, but detecting such activtiy has helped the company get a better understanding of its environment and posture.

Company name:
undisclosed
Activities:
Labor union
Head office:
Washington DC
Number of employees:
350
LY revenue:
unknown
LY net income:
unknown
Key suppliers:
EventTracker

Challenges and obstacles

The company says it did not face any major obstacles or technological challenges. When queries were raised, the company was pleased that EventTracker was always open to dialog. This was in sharp contrast to experiences the organization has had in the past with other IT vendors, where the default response to any query or feature request was generally a firm 'no.'

The labor organization did emphasize, however, that any company looking to deploy a SIEM needs to invest the time up front to understand the enterprise environment, its network and where all critical assets are. Without knowing this, a SIEM deployment could easily fail.

Innovation and roadmap

The company is planning to move significant portions of its infrastructure toward Amazon Web

Services. As part of this plan, it has asked EventTracker to look at integrating the Amazon cloud trail, which is something the company says is on its roadmap. Once that is achieved, the organization will look to expand to AWS.