516.281.2200
www.vandis.com
1 Albertson Avenue
Albertson, NY 11507

GLOBAL ADVERTISING COMPANY TURNS TO VANDIS' MANAGED SOC FOR BETTER NETWORK VISIBILITY, SECURITY, AND ANALYTICS

Challenge:

A global advertising technology company needed a security solution that could support their complex environment. At the time, they had 2,500 servers running in AWS with seven forms of authentication. In addition, they were currently collecting logs from various in-house customer applications including G-Suite, Microsoft 365, and other SaaS enterprise applications. The difficulty of correlating these authentications along with the need for several custom parsed logs required a flexible and customizable solution.

At the time, the team was using four different open source logging and monitoring applications, which created information silos, duplicated work efforts, and increased cloud consumption and manpower costs. With different platforms and multiple data points for each user, it would take the team a long time to identify the source of an attack and act accordingly, putting the organization at risk. Scale and cost issues were threatening the organization's ability to maintain their monitoring platforms.

The organization was looking fora single SIEM platform that could correlate all their data, perform user behavior analytics, and accommodate their custom log formats. As they did not have the staff to constantly adjust alerts within their environment or create custom parcers, they were also seeking on-going assistance in managing the solution. As a fully cloud-based operation, they also needed to consider both the upfront and ongoing cost of the solution.

Solution:

Because of the existing relationship with Vandis, this company consulted Vandis' engineering team to find a solution that would best fit their needs. Vandis recommended our Managed SOC solution, which combines a SIEM solution with ongoing SOC team analysis to manage and optimize moving forward. Vandis' Managed SOC solution is not only available at a lower OpEx cost than other solutions, it eliminated the need for hefty front-end parcing work upfront.

This option provided the behavior analytics, stability, and turnkey alert management that the organization was looking for. When compared to other solutions, Vandis Managed SOC was the only product that could solve the organization's NOC and SOC needs in a single platform.

The Vandis team wrote custom parsers to accommodate the organization's custom log formats, implemented the SOC solution, and assumed management of the environment. The Vandis team also created relevant alerting thresholds for security and operation performance issues. Lastly, custom dashboards were built to provide the client and the Vandis SOC team full visibility into the environment.

516.281.2200
www.vandis.com
1 Albertson Avenue
Albertson, NY 11507

Results:

This organization now has full security visibility into their environment and confidence that the Vandis SOC team will be alerting and threat hunting on known anomalies. They are now seeing correlations over a massive data set that they can easily search and create their own dashboards for. These dashboards will allow them to better understand their AWS and CarbonBlack data.

The company is also now equipped to increase their rate of migration to AWS, since they can do so knowing that their expanding cloud environment will be receiving the same level of security monitoring as their premise network. Their alerts and rules have already made them aware of key security risks, like abnormal employee behavior. With continuous, active dialogue between the Vandis SOC team and the organization's team where they ask questions, discuss potential risks, and get guidance from the Vandis team about new alerts and dashboards, this organization can feel confident in their decision of selecting Vandis' Managed SOC solution.