[EMA™ CASE STUDY]

Using Securonix Analytics and Next-Gen SIEM to Improve Security Operations in Healthcare and Pharmaceuticals

Written by David Monahan, Enterprise Management Associates
Q4 2018

EMA™

Using Securonix Analytics and Next-Gen SIEM to Improve Security Operations in Healthcare and Pharmaceuticals

EXECUTIVE SUMMARY

Healthcare records are the most valuable personally identifiable information and a constant target for information thieves. Pharmaceutical thefts are growing at an alarming rate[1]. For a global healthcare provider and pharmaceutical distributor, it seems to be the perfect storm ready to sink their ship. However, the Chief Data Protection Officer (CDPO) recognized that combating these threats required a change in approach to help his team work smarter not harder, so he began looking for a new way to collect, consolidate, and analyze the available data, providing context to turn data into valuable telemetry. This paper identifies some of the problems he faces and how he is addressing teams to come to a decision to use Securonix to protect his organization and the millions of people that depend on him to keep the information safe.

THE PROBLEMS

First, getting to where he is today was a multi-year process with several turns necessary and at times, those turns were unexpected. When the current CDPO assumed the role, the company was using a managed security services provider (MSSP) to support security operations. However, he felt that the provider was not meeting his needs from both a delivery and a value perspective. Insufficient visibility, lack of reporting into the issues they were facing on a daily basis, and an inability to step outside of their box to help him identify and deal with new and adapting threatscapes forced him to begin looking for a means of bringing security operations back in-house.

His first challenge was that his MSSP was limited in the types of data the tools could absorb. He felt this limitation significantly hampered the team's ability to identify some threats, convert events into incidents, and ultimately prioritize the work appropriately. He needed to bring together more types of information and combine them in a way that created usable intelligence for the full visibility he wanted.

His second challenge was determining, if he brought this back in-house, whether he could support the additional work with his existing team. Adding the analysis and incident triage that was being done by the MSSP could put significant strain on his existing staff. "Security resources are difficult to come by, so even though we expected to have some budget to work with in the transition, increasing the team size was not necessarily a viable option," he said.

The CDPO knew he would need a sustainable, flexible platform to sustain the broad logging intelligence he wanted to collect. That platform also needed to maintain solid analytics on that information and do it in a timely manner, with high confidence that the incident alerts that were brought to the forefront were accurate and properly prioritized to be worked first. He felt he also needed to move into a more proactive mode. He wanted to get to a point where the information and analytics could help him predict security gaps, so he could address them before they were exploited.

Being in the healthcare and pharmaceutical businesses, the CDPO also had compliance at the top of his mind. Whatever solution he selected would have to be able to support the organization in maintaining compliance and producing the necessary reporting for the required audits.

He was all-in on moving forward. To improve his chances of success in the requirements creation phase, he went to the point of engaging an outside analyst firm and data scientists from other corporate divisions to help him identify the right requirements. After creating line-item requirements, he ruled out most of the traditional SIEM vendors because he felt each had their various limitations such as lack of scalability, inability to integrate some forms of asset data and others. Lack of support for big data ruled out a number of SIEM vendors that had data type and ingestion rate scalability limitations. For others, it was a limited or no cloud delivery option, and

[1] Pharmaceutical Theft: a Growing Problem

most had a requirement for the creation and maintenance of correlation rules and policies. They also had the need to know what he was looking for, so detection would work, indicating that their true analytics capabilities were lacking.

After a three-month process gathering requirements and validation, the CDPO kicked off the proof of concept phase where he presented his requirements and, based on responses, invited select vendors to participate. During the POC, each vendor displayed various strengths, but one vendor met more of his requirements out-of-the-box than the others.

SECURONIX VALUE PROPOSITION

Securonix was able to support the ingestion and processing of the wide array of data. Its big data architecture was able to meet the ingestion and processing scale they needed. Its analytics were also able to reduce the volume of alerts by combining the seemingly separate events into far fewer real and actionable incidents without burdening his team with any manual correlation and filtering activities. He said, "Admittedly, this was not magic and required a little tuning at the beginning, but that was more from the need to adjust to poor data quality coming from the non-IT systems we were also receiving data from and other data quality issues brought by multiple acquisitions in a short period of time."

Once the tuning process was completed, the quality of the incidents drove a reduction in the analyst investigation time, thereby accelerating the incident response. That improvement, along with higher-quality alerts and fewer overall incidents, created an avenue for his team to provide more visible and value-added support in other parts of the business, improving the perception of his team within the business. "Securonix reduced our false positive rate by 70 percent. It also reduced our incident response SLA by 98 percent. We went from two days to 30 minutes!"

"SECURONIX REDUCED OUR FALSE POSITIVE RATE BY 70 PERCENT. IT ALSO REDUCED OUR INCIDENT RESPONSE SLA BY 98 PERCENT. WE WENT FROM TWO DAYS TO 30 MINUTES!"

3783.111518