CASE STUDY

AmerisourceBergen Uses Securonix Next-Gen SIEM to Reduce Risk

The Challenge: Protect Against Internal and External Threats

- Build a robust, flexible, open, and affordable platform to be the core of their cybersecurity capabilities.
- Gather and store every piece of log intelligence generated within the company.
- Improve security operations center (SOC) analysts' abilities to detect, mitigate, and respond to cyber threats.
- Use analytics to improve and drive decision making – threat detection, hunting, investigation, and response.

The Solution: Massive Data, Extensive Analytics, Reduced Manual Effort

Cybersecurity leadership evaluated several products including Splunk and IBM QRadar and ended up choosing Securonix Next-Gen SIEM for its scalability and machine learning-based analytics. Securonix Next-Gen SIEM:

- Increases operational efficiency with a single, unified platform for monitoring, detection, response, and remediation.
- Provides anomaly-based threat detection for monitoring in depth.
- Improves analyst efficiency through a user-centric platform, usability, and automation.
- Uses threat chains and models to create a meaningful representation of advanced threats, which reduces time to triage.

The Securonix platform is used by AmerisourceBergen as a central security monitoring solution to mitigate the risk posed by external threats as well as insiders. AmerisourceBergen does this by using Securonix in their SOC to ingest data from over 100 devices with over 100 billion events, while ensuring near real-time ingestion. They also have close to 100 different indicators running on the Securonix platform, performing behavioral and event rarity detection.

The Business Impact:

Reduced Insider Threat Risks

In order to reduce the risk of insider threats, analysts use Securonix to look for nefarious activities caused by complacent, ignorant, and—most importantly—malicious insiders. For analysts to be able to effectively respond to insider threats, they need as much information as possible up front, so they have the context needed to act on a case. This organization accomplishes that by bringing both technical (email, proxy, DLP, etc.) and non-technical (HR, etc.) data into the Securonix platform so that the data is available for investigations.

The results have been significant. In one month, out of 500 insider threat incidents, around 400 (80%) were closed after further investigation identified infected endpoints and malicious internal actors. Ongoing investigations are being reviewed by senior analysts and provide the organization with an overview of the risk level to which they are exposed. More importantly, it has assisted in the identification of corrective measures – such as users who require education on cyber hygiene, revoking rouge access privileges, and closing unnecessary network routes.

Company Profile

AmerisourceBergen is one of the world's largest pharmaceutical distributors. They are based in the United States and have over 150 global offices in more than 50 countries worldwide. It was founded over 100 years ago and as of 2019 is ranked #12 in the Fortune 500.

Reduced Reputational and Financial Risks

In order to detect and respond to external threats, analysts at this organization monitor the organization's servers, networks, and endpoints for any malicious activity across the various stages of an advanced persistent threat. Using entity behavioral analytics, infected machines that are beaconing or making suspicious connections to external sites are detected and removed from the network, preventing an attack from advancing further. This helps reduce reputational and financial risks that could be caused by an external attack that resulted in the theft of business-critical information or disruption of the organization's critical services. This also reduces confidentiality and integrity risks that could be caused by the theft of critical data by malicious insiders. The business impacts or benefits of proactively monitoring enterprise systems and people provides both tangible and intangible benefits.

Securonix's kill chain view has been quickly adopted by the SOC to identify threats in various stages of progression, which helps them associate a threat with a risk level. The sooner a threat is identified, the easier it is to mitigate or destroy it before any significant damage occurs. For example, port scan activity from at least 60 different external addresses is detected by Securonix in a week. This is used to identify bad firewall rules and address them before a malicious external actor can use the weakness to gain access to the network and steal confidential data.

Improved Regulatory Compliance

This organization uses the Securonix platform as a security data lake to collect and analyze logs from a variety of data sources. The use cases implemented include detecting data compromise attempts, malware infections, and account misuse. These use cases support compliance efforts including the United States' Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and the European Union's General Data Protection Regulation (GDPR).

A major concern for this organization is the storage and retrieval of data over a large period of time for compliance – which may span several years. The Securonix data lake allows them to parse any log data, enrich, store, and make it searchable through the Securonix Spotter interface. While their current deployment limits this storage to between six months and a year, it can easily be scaled up with additional hardware, or through a cloud service like Amazon Web Services (AWS). The open source data model embraced by Securonix also allows other applications to store or consume the same data downstream.

Improved User Experience

Besides solving core security problems, Securonix works closely with this organization's end users and analysts to determine how to enhance the end user experience better overall. This improves analysts' efficiency as they respond to, and keep up with, the ever-growing types of threats faced; ultimately leading to better risk mitigation for the enterprise.

One such example is a single pane of glass view, where the analyst only needs to look at one screen to conclude their investigation instead of switching between multiple screens. Previously, analysts had to switch between screens to look at security alerts from an endpoint solution, endpoint details from a CMDB repository, and additional tools for third-party intelligence. This switching can take anywhere from several minutes to several hours depending on the complexity of the investigation, and cycling through multiple screens can frustrate analysts. Securonix has integrated with several infrastructure and security solutions and has developed connectors to pull all the necessary details into the Securonix interface. This way, the end user can have quick access to the information they need with minimal distraction.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.