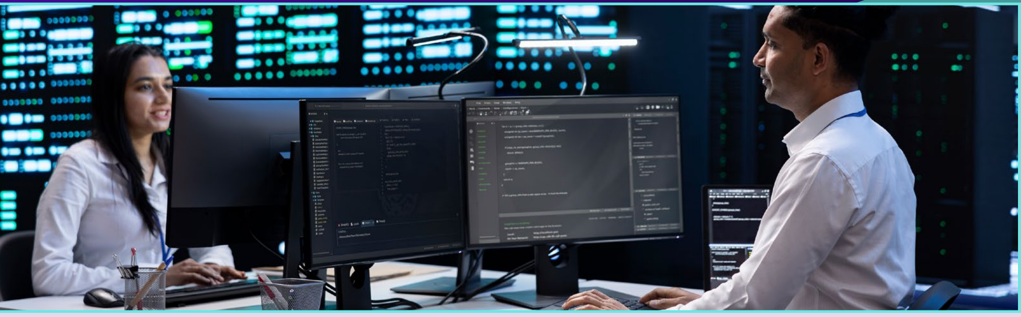
securonix



INDUSTRY:
PROFESSIONAL SERVICES

LOCATION:
GLOBAL

CASE STUDY

Streamlining Cybersecurity Operations: How a Global Services Provider Enhanced Visibility with Securonix

Challenge: A global services provider faced limited visibility, excessive false positives, and insufficient threat detection due to a third-party SIEM that supported only limited data sources. Insider threats and manual detection efforts further hindered security operations.

Solution: The organization implemented Securonix's SIEM with advanced UEBA capabilities, integrating diverse data sources to consolidate telemetry and improve visibility. The solution reduced false positives and streamlined threat detection, leveraging open-source threat intelligence and custom use cases for stronger security.

Benefits

- **Enhanced Visibility:** Unified monitoring of user activity, ensuring real-time detection of threats.
- **Reduced False Positives:** Improved alert accuracy, freeing resources to focus on critical threats.
- **Stronger Threat Detection:** Advanced analytics enabled identification of insider threats and suspicious behavior.
- **Faster Response Times:** Immediate visibility into incidents allowed swift remediation.

Results

Securonix enabled the provider to transform its security posture, achieving enhanced operational efficiency and safeguarding sensitive data across its global environment.

Learn more at securonix.com

The Challenge

Before implementing Securonix, the security team at a major global services provider relied on a third-party SIEM solution that only supported firewall and active directory logs, but was incompatible with other data sources. This limited integration resulted in insufficient visibility across their infrastructure. They also lacked advanced tools like User and Entity Behavior Analytics (UEBA), making it difficult to correlate user behavior across the organization's environment and properly monitor potential threats. The team was also suffering from excessive false positives, which made threat detection and incident response efforts inefficient and hindered their ability to detect sensitive data leaks. These challenges drove the need for a more robust and comprehensive security solution.

As a provider handling sensitive client information with thousands of employees globally, robust security was critical. Before adopting Securonix, their existing SIEM solution offered limited data source integration, lacked the ability to analyze user behavior effectively, and generated an overwhelming number of false positives, which slowed incident response. To address these gaps, they needed a solution that provided advanced analytics, broader visibility, and more efficient threat detection.

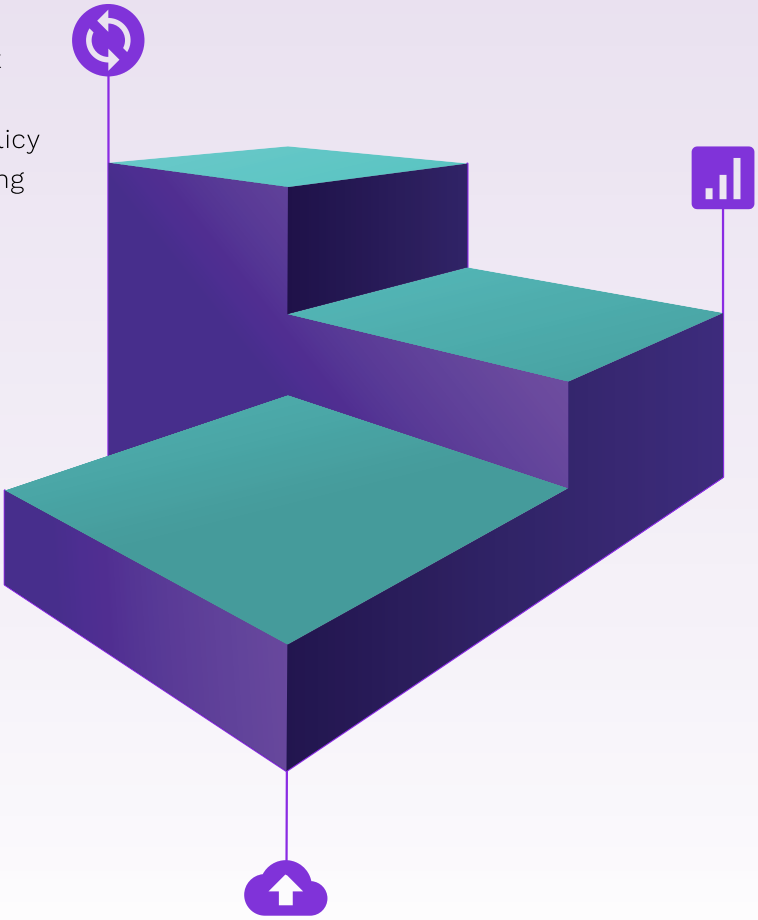
The organization also experienced difficulties with insider threats, including cases in which employees were sending sensitive data to their personal email addresses without adequate detection mechanisms in place. A lack of advanced analytics and data correlation capabilities hindered the company's ability to protect sensitive information and respond quickly to potential incidents.

> "Securonix has helped us enrich our data and integrate new data sources to achieve better visibility into our environment and strengthen our security posture. With Securonix, the security team is immediately notified whenever any suspicious activity occurs within the company. For example, alerts are triggered for any kind of encryption, suspicious IP addresses attempting to access the firewalls or any other unusual activities. This allows the security team to identify and respond to potential threats quickly. Thus, whenever Securonix generates an alert, the team recognizes it as a serious issue and can act promptly."
>
> – Security Operations Manager,
> A Leading Global Services Provider

The organization selected Securonix to enhance their security posture. With the help of the Securonix team, they integrated new data sources, which consolidated their organization's diverse telemetry into a single platform, effectively enhancing their visibility and threat detection capabilities. Securonix's advanced UEBA allowed them to track user behavior across their environment, reducing false positives and providing more focused alerts.

The organization achieved several critical benefits with Securonix. They significantly enhanced their visibility across their environment, allowing real-time detection of potential threats and preventing data exfiltration incidents. By fine-tuning alert policies, they reduced false positives, which improved operational efficiency and enabled their security team to focus their time and energy on more pressing activities. Additionally, by leveraging open-source threat intelligence data, they enhanced their threat detection capabilities and built customized use cases, further strengthening their security posture. Securonix also helped them improve incident response times, by providing immediate visibility into policy violations across their environment and enabling the security team to take swift action against suspicious activities.

> "Our customer has truly transformed their security operations by leveraging Securonix's advanced UEBA and comprehensive data integration. Their proactive approach to improving visibility, reducing false positives, and enhancing threat detection showcases their commitment to safeguarding sensitive data while optimizing their security program's operational efficiency."
>
> – Venkat Kotla, Chief Technology Officer, Securonix



Key Challenges

- **Improving Visibility and Adding Additional Data Sources:** The previous SIEM solution was limited to a few data sources, which restricted comprehensive monitoring across the IT infrastructure.
- **Overcoming False Positives and Streamlining Threat Detection Efforts:** The company's prior SIEM solution generated too many false positives and their team spent too much time determining which alerts represented material threats and required investigation. Limited analytics complicated threat detection and hindered their ability to protect sensitive information and respond quickly to incidents. They needed a SIEM solution with advanced, natively integrated UEBA and data correlation capabilities to cut through the noise and improve operational efficiency.
- **Insider Threats and Data Security:** Insider threat detection was also challenging, with employees sending sensitive data to personal email addresses without proper detection mechanisms.

Key Features Utilized

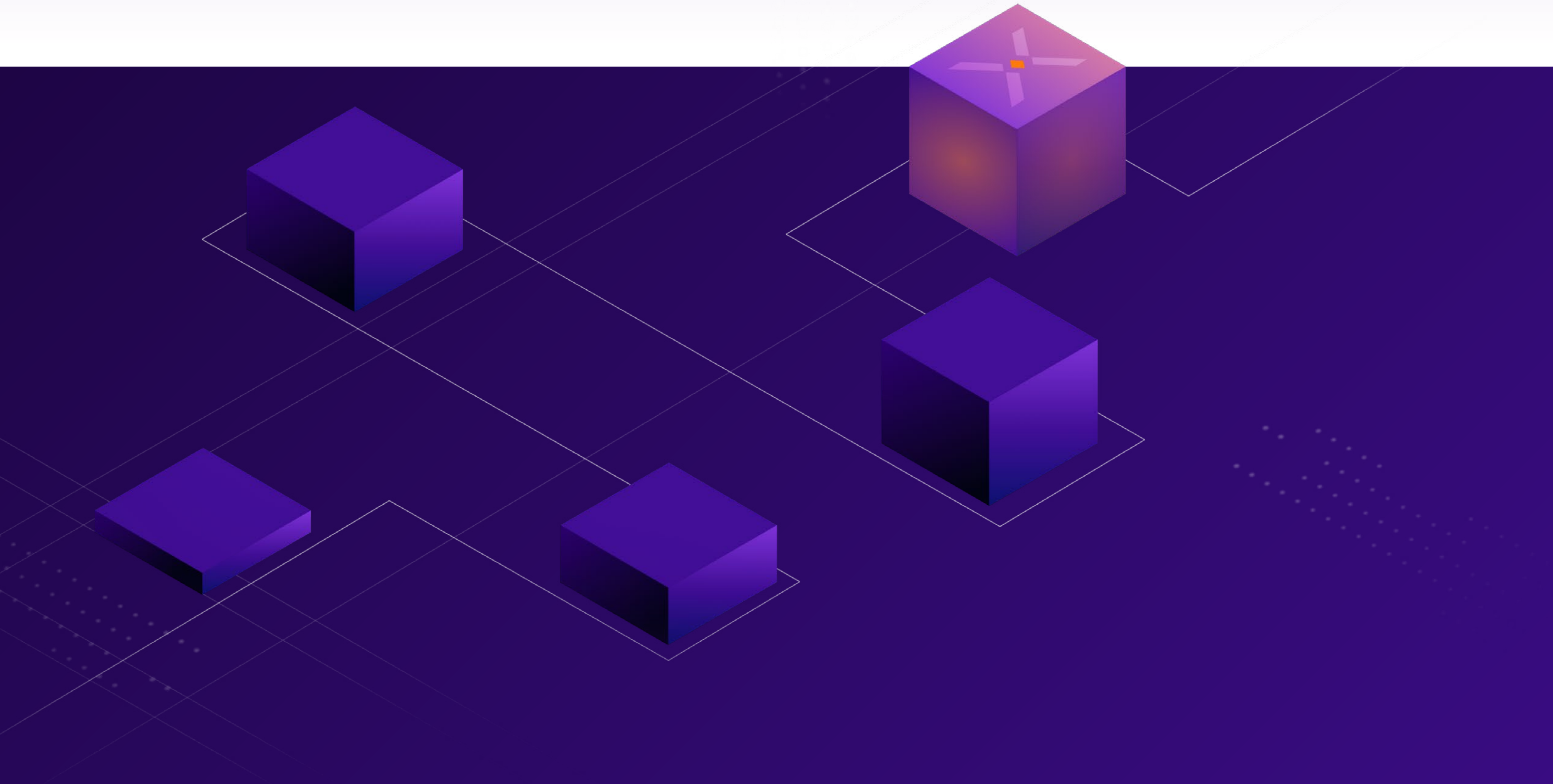
- **Comprehensive Data Source Integration:** With Securonix, the company added new data sources, providing greater telemetry across their environment. This enriched their threat detection capabilities by consolidating data from diverse sources into a single platform.
- **Advanced UEBA for Threat Detection:** Securonix's UEBA capabilities allowed the security team to correlate user behavior from disparate data sources across their environment. This helped reduce false positives and gave the security team more focused alerts.

Benefits

- **Enhanced Visibility and Security Posture:** The company improved their visibility across their environment, ensuring the security team was aware of potential threats in real-time. Securonix's comprehensive data integration and advanced UEBA enabled it to detect suspicious user behaviors and prevent data exfiltration incidents, such as employees sending sensitive data to personal accounts.
- **Improved Operational Efficiency:** By fine-tuning alert policies, the company reduced false positives, leading to more efficient security operations. This allowed their security team to focus on genuine threats, immediately addressing violations that required action.
- **Better Threat Detection:** Integrating open-source threat intelligence data enhanced the company's ability to detect threats and allowed them to build customized use cases, increasing the overall efficiency of their security measures.
- **Faster Incident Response:** Securonix's ability to detect and create alerts for policy violations enabled the team to act swiftly in the case of any suspicious behavior. Whether it was detecting unauthorized access attempts or encryptions, Securonix provided immediate visibility, allowing the team to jump into action.

Conclusion:

Securonix has played a crucial role in transforming the organization's security operations, enabling them to gain comprehensive visibility into their environment and drastically improve their response to potential threats. With the integration of more data sources, advanced UEBA, and enhanced threat detection capabilities, the company has strengthened its security posture and ensured the protection of sensitive data across the organization.



About Securonix

Securonix is pushing forward its mission to secure the world by staying ahead of cyber threats, reinforcing all layers of its platform with AI capabilities. Securonix Unified Defense SIEM provides organizations with the first and only AI-reinforced solution built with a cybersecurity mesh architecture on a highly scalable data cloud. The innovative cloud-native solution is enhanced by Securonix EON to deliver a frictionless CyberOps experience and enables organizations to scale up their security operations and keep up with evolving threats. For more information, visit securonix.com, or follow us on LinkedIn and X.