securonix

INDUSTRY:
INVESTMENT MANAGEMENT & FINANCIAL ADVISORY

LOCATION: **UNITED STATES**

CASE STUDY

Enhancing Security and Operational Efficiency: How an Investment Management and Financial Advisory Company Transformed Its Security Operations with Securonix

Challenge: A leading investment management and financial advisory firm faced significant security challenges, including employees bypassing security controls, unauthorized data transfers, and the absence of a centralized SIEM solution. Without automated log aggregation and event correlation, the firm struggled with inefficient threat detection, prolonged incident response times, and compliance complexities. The organization needed a scalable and intuitive security platform to enhance visibility, streamline operations, and improve overall security posture.

Solution: The firm implemented Securonix to centralize security monitoring, integrate with diverse data sources, and automate threat detection. By leveraging real-time alerting, advanced analytics, and Spotter for compliance management, the organization significantly improved its incident response and operational efficiency. Fine-tuned alerting reduced false positives, allowing analysts to focus on real threats, while compliance workflows were optimized for audit readiness.

Benefits

- **Comprehensive Security Visibility:** Aggregated and analyzed critical logs for full security environment awareness.
- **Reduced False Positives:** Achieved a 40% reduction in unnecessary alerts, enhancing analyst efficiency.
- **Faster Incident Response:** Cut detection-to-resolution times to under 30 minutes.
- **Operational Efficiency Gains:** Reduced security analysts' workload for policy violation reviews by 40-50%.

Results

The organization achieved a 40% reduction in false positives, cut incident response times to under 30 minutes, and decreased analyst workload by 50%.

- **40% fewer** false positives
- Incident response time **under 30 minutes**
- **50% reduction** in analyst workload

Securonix has given us a competitive advantage by sending us alerts without requiring us to check the portal for actionable intelligence, resulting in more efficient operations, time savings, increased visibility, and a more robust overall security posture. We've fine-tuned our instance to ensure critical alerts are prioritized, leading to a 40% reduction in false positives."

– **CISO, A leading investment management and financial advisory company that provides specialized fund administration services to private equity firms**

The Challenge

A leading investment management and financial advisory company that provides specialized fund administration services to private equity and similar investment firms, faced critical security challenges. Employees were frequently bypassing security controls, taking company systems to unauthorized locations, and sending sensitive company data to personal email accounts. The organization lacked a SIEM and therefore had no centralized log aggregation solution for critical applications, making it difficult to detect security incidents or confirm breaches. Prior to adopting Securonix, the firm relied on manual event correlation, resulting in inefficiencies and limited visibility into security threats. The organization needed an intuitive, scalable, and comprehensive SIEM solution to enhance visibility, streamline incident detection and response, and improve operational efficiency.

The firm successfully implemented Securonix to enhance its security operations, leveraging key features such as advanced threat detection, real-time alerting, and scalable log ingestion. By integrating Securonix with diverse data sources, the organization gained complete visibility into its security environment, ensuring critical logs are effectively analyzed. The organization refined its event alerts to reduce false positives by 40%, enabling analysts to devote more time to genuine threats. Additionally, the implementation significantly improved incident response times, reducing detection-to-resolution periods to under 30 minutes. Operational efficiency saw significant gains, with analysts experiencing a 40-50% reduction in workload for reviewing policy violations, allowing them to focus on strategic tasks. Cost savings were also achieved by consolidating security operations into a single platform, eliminating the need for additional tools. Furthermore, Securonix's Spotter streamlined compliance management, making audit readiness more efficient and reducing the time spent on retrieving compliance-related metrics. Through these enhancements, the firm has strengthened its security posture while optimizing resources and costs.

We are proud to be helping our customers strengthen their security operations. Our partnership has empowered them with increased visibility, streamlined incident response, and significant operational efficiencies. By choosing Securonix, our customer has been able to leverage a highly intuitive and effective SIEM solution that meets its security and compliance needs."

– **Stephen Cook, Vice President, Sales – Account Management & Renewals, Securonix**

Key Challenges

- **Lack of Log Aggregation Solution:** The firm faced significant visibility gaps in its security operations due to the absence of a centralized log aggregation system for critical applications. Without this capability, identifying and responding to security events was inefficient and reactive rather than proactive.
- **Security Control Bypass:** Employees were found bypassing security measures and engaging in unauthorized activities, such as transferring sensitive data to personal email accounts. This behavior introduced significant security risks, necessitating a solution that could detect and prevent policy violations in real-time.
- **Inefficient Security Operations:** Without automated event correlation and real-time alerting, security teams relied on manual processes to identify potential threats. This inefficiency slowed incident response times and increased the workload on analysts, highlighting the need for a more streamlined and automated security operations platform.
- **Compliance and Regulatory Challenges:** Ensuring adherence to security policies and regulations was a complex and time-consuming process due to the lack of centralized compliance management. The organization required a solution that could facilitate audit readiness, provide seamless access to compliance-related metrics, and reduce the effort needed for regulatory reporting.

Key Features Utilized

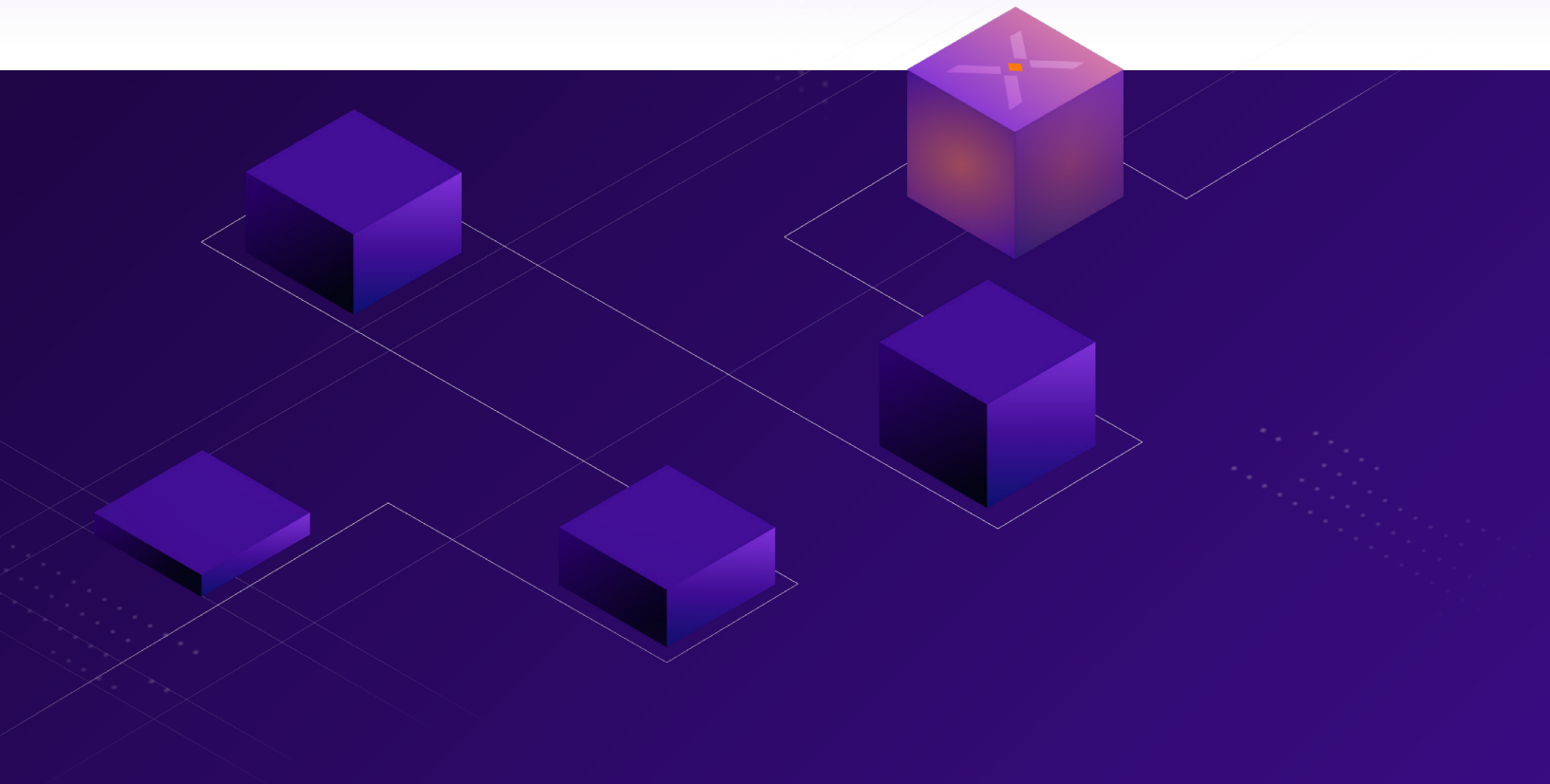
- **SIEM Platform:** Leveraged for advanced threat detection, enabling proactive identification and mitigation of security threats.
- **Real-Time Alerting:** Automated notifications and alerts ensure rapid response to potential security incidents, minimizing risks.
- **Intuitive Dashboards:** Customizable dashboards offer clear visualization of security events and trends, enhancing situational awareness.
- **Spotter Search:** Facilitates streamlined threat hunting and compliance management, enhancing overall security posture.
- **Scalable Log Ingestion:** Designed to accommodate diverse security data sources, including integrations with cloud-based security solutions from virtual environments.

Benefits

- **Enhanced Threat Visibility:** The organization now has complete visibility into its security environment, ensuring all critical application logs are aggregated and analyzed.
- **Reduced False Positives:** Fine-tuning their Securonix instance resulted in a 40% reduction in false positives, allowing analysts to focus more on real threats.
- **Improved Incident Response Time:** The average time from detection to resolution has been reduced to less than 30 minutes.
- **Operational Efficiency Gains:** The workload of security analysts reviewing policy violations has been reduced by 40-50%, enabling them to focus on higher-value tasks.
- **Cost Savings:** By consolidating security operations into a single platform, the organization has reduced the total cost of ownership and eliminated the need for additional security tools.
- **Compliance and Audit Readiness:** Spotter's advanced search capabilities enable the easy retrieval of compliance-related metrics, resulting in significant time savings in audit management.

Conclusion:

Since implementing Securonix, the organization has transformed its security operations by enhancing threat detection and streamlining incident response. The firm now benefits from a centralized, automated security monitoring platform that reduces operational burden while improving visibility and compliance. With Securonix's scalable and user-friendly SIEM solution, the company has achieved greater efficiency, security, and cost savings. Moving forward, the organization continues to leverage Securonix to optimize security operations and maintain a proactive approach to threat management.



About the Customer

The customer is an investment management and financial advisory firm specializing in fund administration services for private equity and similar investment firms. The company provides accounting, reporting, and compliance support, enabling investment funds to streamline their operational infrastructure and investor communications.

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.

securonix