securonix

STEPTOE & JOHNSON PLLC

INDUSTRY: **LEGAL SERVICES**

LOCATION: **UNITED STATES**

CASE STUDY

From No SIEM to Full Security Visibility: How Steptoe & Johnson Transformed Threat Detection and Compliance

Challenge: Steptoe & Johnson, a national law firm with 18 offices across the U.S., faced increasing security and compliance demands while managing sensitive client data with a lean two-person security team. Without a SIEM solution, they lacked centralized log management, behavioral analytics, and automation capabilities. Their fragmented visibility made correlating security data across disparate tools difficult. To meet rising client security expectations and streamline compliance, they needed a scalable, easy-to-use security platform with built-in analytics and automation.

Solution: Steptoe & Johnson implemented Securonix's Unified Defense SIEM, integrating real-time log aggregation, advanced UEBA for anomaly detection, and SOAR Lite to automate security workflows. This streamlined their security operations, reducing manual workloads and improving compliance reporting. Securonix's scalable architecture enabled seamless onboarding of 15 data sources and the ability to process 65GB of security logs daily, while its threat models reduced false positives.

Benefits

- **Improved Threat Detection & Response:** Reduced time to detect and resolve threats from hours to minutes.
- **Enhanced Compliance:** Automated dashboards cut audit preparation time by 70%.
- **Greater Efficiency:** Centralized visibility and automation eliminated manual processes.
- **Seamless Scalability:** Easily onboarded 15+ data sources without operational disruptions.

Results

- **10 high-priority security alerts** identified weekly.
- **70% reduction** in compliance-related workload..
- **65GB of security logs** processed daily.

"Securonix goes above and beyond. I've worked with vendors in the past that disappeared after implementation, but Securonix provides ongoing support with weekly touchpoints, and their support team ensures that we are never left hanging. Whether onboarding new data sources or scaling up our operations, Securonix makes it seamless. The documentation is always up to date, and ingesting new data sources is effortless. The platform is simple to use, highly scalable, and has dramatically strengthened our security posture.

Securonix has significantly improved our security operations by enhancing compliance reporting, reducing audit preparation time by 70%, and providing seamless scalability to process 65GB of security logs daily across 15 data sources. Continuous fine-tuning of threat detection models has reduced false positives, allowing us to focus on real threats with greater accuracy. With Securonix, we've strengthened our security posture, meeting rising client security expectations while efficiently investigating and responding to an average of 10 high-priority security alerts each week."

– **Tim Thornsberry, Director of Information Security, Steptoe & Johnson**

The Challenge

Steptoe & Johnson PLLC, a national law firm, operates across 18 offices in the U.S. with 800 employees. The firm provides legal services spanning corporate law, energy, real estate, finance, labor, litigation, taxation, and regulatory compliance. With a lean two-person security team led by Director of Information Security, Tim Thornsberry, the firm faced increasing security and compliance demands, particularly around managing and securing sensitive client data, including personally identifiable information (PII) and other legal records. With a lean security team and no log management tool or centralized visibility, they needed a solution that offered ease of use, requiring minimal scripting or syntax knowledge (with SOAR addressing this challenge), and could be maintained by a small team.

Before adopting Securonix, Steptoe & Johnson lacked a Security Information and Event Management (SIEM) solution altogether, leaving them without centralized log management, behavioral analytics, or advanced automation capabilities. Their security team, consisting of just two professionals, had an endpoint security solution for threat detection but otherwise lacked a holistic view of their environment. Without centralized log aggregation, their visibility was fragmented, making correlating security data across disparate tools challenging. Additionally, the firm had no User and Entity Behavior Analytics (UEBA) or Security Orchestration, Automation, and Response (SOAR) capabilities, leaving them unable to efficiently detect and respond to anomalous user activity or automate processes without having to write scripts. With client security expectations rising, Steptoe & Johnson needed a scalable, easy-to-use SIEM with built-in analytics and automation to provide real-time insights, detect threats proactively, reduce manual workloads, and streamline compliance processes.

"Steptoe & Johnson has demonstrated how lean security teams can significantly improve visibility, threat detection, and compliance with the right security platform. By leveraging Securonix's SIEM, UEBA, and SOAR Lite capabilities, they've transformed their security posture, automating critical processes, and enhancing their ability to protect sensitive client data while meeting regulatory requirements."

– **Samer Alami, Chief Customer Officer, Securonix**

Key Challenges

- **Lack of Centralized Security Visibility & Manual Log Management:** Without a SIEM, security data was fragmented across multiple tools, making it difficult to correlate logs, detect threats, and efficiently aggregate and analyze security data on a single pane of glass.
- **Limited Threat Detection Capabilities:** The lack of any UEBA or SOAR functionalities made it difficult to identify and respond to anomalous user activities and automate other tasks.
- **Scalability Limitations:** Lack of a solution capable of efficiently ingesting and processing large volumes of security data, making it difficult to integrate new security tools and data sources without operational disruptions.
- **Compliance and Audit Burdens:** High client security expectations and regulatory requirements necessitated improved security and compliance controls and reporting.
- **Resource Constraints:** A two-person security team required an intuitive and easy-to-manage solution that wouldn't require extensive scripting or maintenance.

Key Features Utilized

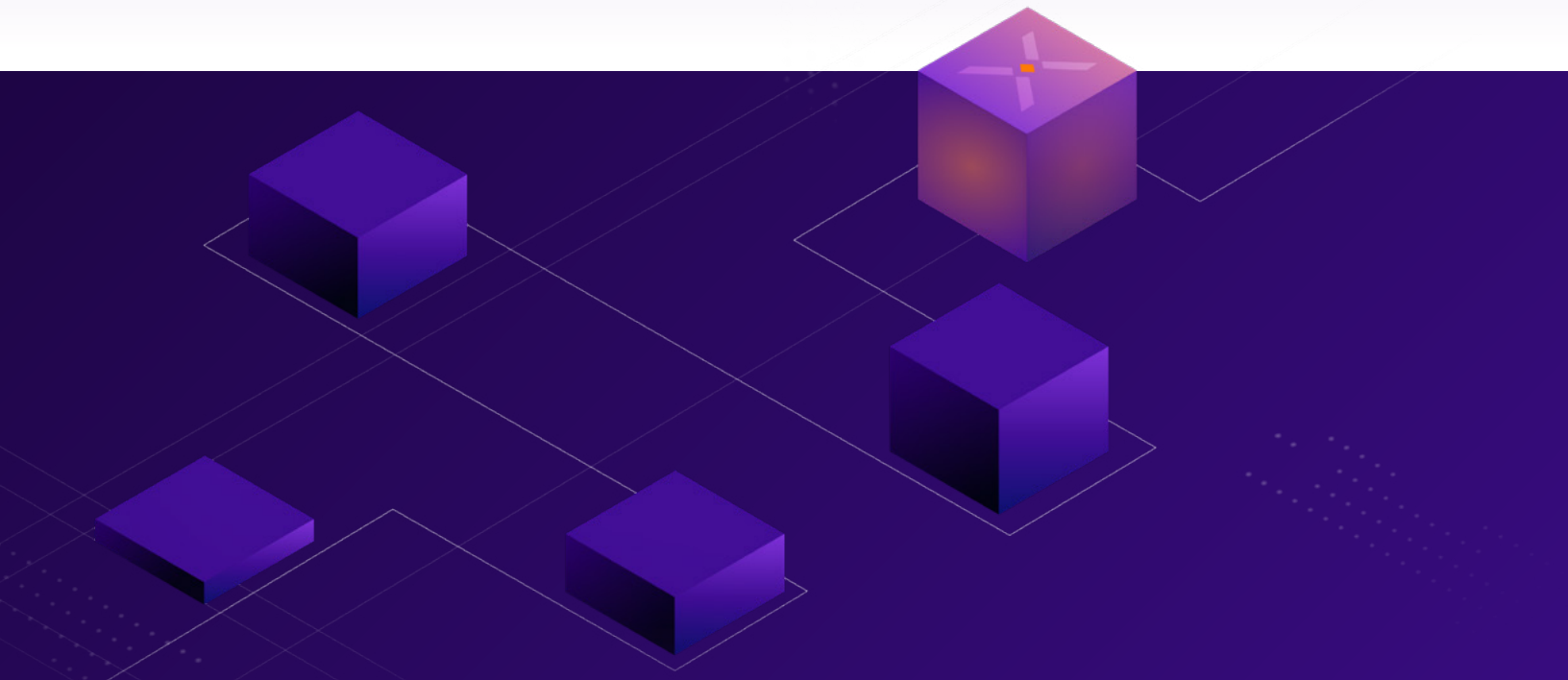
- **Securonix SIEM:** Provided centralized log aggregation, real-time threat detection, and streamlined compliance reporting.
- **User and Entity Behavior Analytics (UEBA):** Enabled advanced anomaly detection to identify suspicious user behaviors across systems.
- **SOAR Lite:** Automated manual security workflows, reducing the workload on the security team.
- **Scalable Data Ingestion:** Enabled easy integration of new security tools and data sources without operational disruptions.
- **Threat Models & Kill Chain Analysis:** Improved detection accuracy by correlating disparate security events into actionable intelligence.
- **Compliance Dashboards and Reporting:** Simplified regulatory reporting, reducing audit-related workload.

Benefits

- **Improved Threat Detection & Response:** Reduced time to detect and resolve threats from hours to minutes by aggregating logs and applying UEBA analytics.
- **Increased Operational Efficiency:** Securonix's automation and centralized visibility eliminated manual processes, significantly reducing the security team's workload.
- **Stronger Compliance & Reporting:** Automated dashboards and compliance reporting capabilities enable quick report generation, decreasing audit preparation time by 70%.
- **Seamless Scalability:** Allowed seamless onboarding of 15 different data sources, processing approximately 65GB of security logs daily.
- **Reduced False Positives:** Continuous fine-tuning of threat detection models reduced false positives and improved alert accuracy.
- **Strengthened Security Posture:** Securonix strengthened Steptoe & Johnson's ability to meet rising client security expectations and regulatory requirements while enabling them to investigate and respond to an average of 10 high-priority security alerts weekly, improving overall security effectiveness.

Conclusion:

Since adopting Securonix, Steptoe & Johnson has significantly improved its security operations, transitioning from no SIEM to a fully integrated, advanced security platform. The firm now benefits from enhanced visibility, automated security processes, and improved compliance management, allowing its small security team to operate efficiently. As they continue to refine their deployment, Securonix remains a trusted partner in their evolving security strategy.



About Steptoe & Johnson

Steptoe & Johnson is a national law firm with more than a century of experience in the areas of business, energy, labor & employment, and litigation. The firm has over 400 attorneys and other professionals practicing in 18 offices in Colorado, Kentucky, Ohio, Oklahoma, Pennsylvania, Texas, and West Virginia. focused on business, energy, labor & employment, and litigation. The firm is committed to protecting sensitive client data and maintaining industry-leading security and compliance standards. Visit and connect with us on X and LinkedIn.

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