securonix

GLP

CASE STUDY

GLP Optimizes Security with Securonix SOAR & ATS

CASE STUDY

GLP Optimizes Security with Securonix SOAR & ATS

About GLP

GLP is a leading global business builder, owner, developer and operator of logistics real estate, data centers, renewable energy, and related technologies. GLP's deep expertise and operational insights allow it to build and scale high-quality businesses and create value for its customers. GLP owns and operates assets and businesses in 17 countries across Asia, Europe and the Americas. GLP Capital Partners, a global alternative asset manager, is the exclusive investment and asset manager of GLP. To learn more about GLP, visit **www.glp.com/global**.

The Challenge: GLP's SOC team faced the challenge of managing a complex, globally distributed security environment while maximizing resources. Manual tasks like threat hunting, ticket creation and incident response consumed valuable analyst time, reducing their capacity to perform other value-added tasks to effectively monitor and protect their network.

GLP, a leading global logistics real estate developer and operator, navigates the complex world of interconnected logistics supply chains. Their vast network spans diverse locations and requires robust security measures to protect sensitive data and ensure operational continuity. As cyber threats evolve, maintaining a secure environment becomes paramount.

Although GLP had already adopted Securonix as their SIEM solution, they were not leveraging its full potential as the platform's initial configuration was not optimized for GLP's specific environment and use cases. The GLP security team worked with Securonix engineering and threat content teams to craft effective security policies and maximize data ingestion from various sources to achieve comprehensive visibility.

Through a collaborative effort, the Securonix team worked closely with GLP to refine configurations, train analysts on advanced use cases, and optimize data intake. This enhanced utilization of the Securonix platform significantly improved GLP's security posture.

The introduction of Securonix Autonomous Threat Sweeper (ATS) and Security Orchestration, Automation, and Response (SOAR) further improved GLP's security operations. ATS streamlined threat detection by automating threat intelligence sweeps, eliminating manual tasks, generating detailed reports and freeing up analyst time for investigation and hunting. SOAR's automation capabilities significantly reduced manual workflows associated with incident response, leading to cost savings and improved efficiency. Analysts were empowered to focus on strategic tasks like threat triage and investigation, maximizing their expertise and effectiveness.

"The automation features in Securonix SOAR have significantly reduced the workload for my team and we've seen a 40% reduction in weekly tickets. This allows us to focus more on analysis and investigation."

– Ji Cheng Zhu
CISO, GLP

"By leveraging automation and AI-driven capabilities, GLP witnessed a remarkable reduction in total cost of ownership, freeing up resources for strategic investments. The frictionless analyst experience has empowered their team to tackle complex security challenges with ease, fostering a more agile and proactive approach. Our partnership has not only fortified their cyber defenses but also elevated their operational efficiency, positioning GLP for sustained success in today's dynamic threat landscape."

– Ajay Biyani
VP Sales, Securonix

Key Challenges

- **Managing Complexity and Reducing Manual Workload:** GLP's SOC team faced the challenge of managing a complex security environment with limited resources. Manual tasks like threat hunting, ticket creation and incident response consumed valuable analyst time, reducing their capacity to perform other value-added tasks to effectively monitor and protect their network.
- **Keeping Pace with Evolving Threats:** The evolving threat landscape demanded a more proactive approach to security. GLP's SOC team needed a solution that could not only detect known threats but also identify sophisticated zero-day attacks.
- **Improving Visibility and Streamlining Workflows:** Limited visibility across their IT infrastructure made it difficult for the GLP SOC team to identify and respond to security incidents efficiently. They needed a solution that could provide a centralized view of their security posture and streamline workflows.

Key Features Utilized

- **Securonix SOAR:** Automated ticket generation and consolidation significantly reduced manual workload, lowering weekly tickets by 40%, freeing up valuable analyst time for deeper threat investigation.
- **Securonix OpenAI Integration:** Integration between Securonix SOAR & OpenAI facilitated rapid investigations via AI on any incidents observed in the environment and improved the analyst Threat Detection and Incident Response (TDIR) experience.
- **Securonix Autonomous Threat Sweeper (ATS):** Automated threat intelligence sweeps eliminated manual tasks and provided automatic reports, saving time and resources.

Benefits

- **Improved Efficiency:** SOAR's automation streamlined incident response workflows, reducing manual effort and accelerating response times.
- **Enhanced Threat Detection:** ATS proactively identified potential threats and IOCs, improving overall security posture.
- **Increased Analyst Productivity:** Automation freed up analysts for critical threat investigation and analysis.
- **Stronger Partnership:** Bi-weekly communication and ongoing support solidified a collaborative relationship with Securonix.

By leveraging Securonix's advanced features and fostering a strong partnership with customer support, GLP achieved significant improvements in security efficiency, threat detection, and analyst productivity. Their commitment to continuous improvement positions them well to stay ahead of evolving threats in the future.

About Securonix

Securonix is leading the evolution of SIEM for today's hybrid cloud, data-driven enterprises. Securonix Unified Defense SIEM provides organizations with the first and only content-driven threat detection, investigation, and response (TDIR) solution built with a highly scalable data cloud and a unified experience from the analyst to the CISO. The innovative cloud-native solution enables organizations to scale up their security operations and keep up with evolving threats.

For more information visit securonix.com