PHOENIXCYBER

CASE STUDY

Phoenix Cyber Reduces Alert Noise by 100+ Alerts Per Hour with Security Automation for Leading MSSP

THE CHALLENGE

An industry-leading managed security service provider (MSSP) was encountering compounding operational challenges with their security automation platform that was impacting system reliability and eroding user confidence. Corrupted platform instances caused by library component failures disrupted workflows and introduced instability across the environment. At the same time, poor coding practices were generating excessive alert noise, overwhelming analysts, and reducing overall efficiency.

Additional issues further slowed operations. Inaccurate and delayed reporting was frustrating for end users who depended on timely and reliable insights. UI bugs, memory constraints, and ingestion limitations restricted incident processing to email-based workflows, which limited scalability and increased response times. Collectively, these challenges constrained performance, delayed incident resolution, and put the overall security automation platform's stability at risk for the MSSP.

THE PHOENIX CYBER SOLUTION

Phoenix Cyber combined its technical expertise with strategic enablement and partnered closely with the MSSP to restore stability and optimize performance across the security automation platform. The engagement began with targeted recovery efforts to safely restore corrupted instances without data loss. To reduce future downtime, Phoenix Cyber developed an API wrapper that accelerated instance wipes and redeployment, significantly improving recovery speed during critical events.

The team addressed infrastructure troubleshooting, including Docker and Kubernetes configurations. They coordinated directly with the platform's support team to address UI and memory corners and restored reporting accuracy and smoother operations.

As part of the project, Phoenix Cyber led a major ingestion upgrade, transitioning the service provider from email-based ingestion to JSON-based ingestion, resulting in increased processing capacity. Additional improvements included eliminating infinite

PHOENIXCYBER

CASE STUDY

loops, introducing trigger-based automation, redesigning the application interface for improved usability and streamlined workflows, and delivering comprehensive platform training to the internal team to support long-term operational independence.

THE BENEFITS

The engagement delivered clear, measurable improvements across performance, efficiency, and customer satisfaction.

Incident throughput increased by five times following the migration from email-based ingestion to JSON-based ingestion, enabling faster response and greater operational scale. Eliminating infinite loops and implementing trigger-based automation reduced alert noise conservatively by over 100 alerts per hour, allowing analysts to focus on higher-value work rather than repetitive troubleshooting. API-driven redeployment and faster recovery processes minimized downtime and improved overall business continuity.

Enhancements streamlined operations and reporting accuracy was restored. Comprehensive platform training empowered the service provider to operate more independently, reducing reliance on external support and strengthening long-term sustainability. The success of the engagement resulted in strong customer satisfaction and deep appreciation for the Phoenix Cyber team's security automation services.

CONTACT US AT **SALES@PHOENIXCYBER.COM**