PHOENIXCYBER

CASE STUDY

Phoenix Cyber Helps an MSSP Migrate 70+ Clients to a Security Automation Platform Under Fixed Deadline

THE CHALLENGE

A leading managed security service provider (MSSP) focused on critical infrastructure and regulated industries needed to transition over 70 clients onto Swimlane, a SOC automation solution, under a steep, inflexible deadline before the expiration of an existing contract. The migration needed to occur without disrupting current SOC operations, while integrating with newly developed API services that were still being built during the project.

Compounding the challenge, the project operated under strict GDPR and EU regulatory constraints. Phoenix Cyber had no access to live customer data and limited availability of reliable mock data for testing. The APIs required for ingestion and automation were evolving in parallel with the migration effort, leaving critical data fields undefined until late in the process. Despite these constraints, the MSSP required a production-ready, scalable solution that would support both immediate operational needs and future growth.

THE PHOENIX CYBER SOLUTION

Phoenix Cyber began by analyzing the existing environment despite having limited direct visibility into current systems. To bridge information gaps, the team relied heavily on proven SOAR best practices, structured interviews with stakeholders, and detailed design workshops to capture functional and operational requirements.

Without direct API testing, the engineers mocked APIs using available documentation and scaffolded systems with fields still unknown, enabling parallel progress while the vendor's APIs matured.

Phoenix Cyber designed and implemented APIs guided by vendor specifications and the constrained information available for data mocking. The solution delivered a scalable, agile, centralized reporting system that gives SOC analysts a single-pane-of-glass across all clients by consolidating data into a master tenant. This master tenant supports global daily operations and reporting, with drill-down to client-specific details when needed. This helps to balance enterprise-wide visibility with per-client control.

PHOENIXCYBER

CASE STUDY

Phoenix Cyber provided technical account management (TAM) and went beyond standard delivery by conducting architecture reviews and design planning. The team anticipated future phases and influenced priorities toward provisioning to ensure long-term scalability and readiness.

SERVICES PROVIDED

- Technical Account Management (TAM) services throughout the engagement
- Architecture reviews and SOAR design planning
- API design and mock development to enable parallel build and testing
- Scalable tenant and data model design to support multi-client SOC operations
- Forward-looking planning to anticipate future phases and influence provisioning priorities
- Strategic guidance to ensure long-term scalability, readiness, and operational resilience

THE BENEFITS

The engagement delivered immediate operational stability while laying the foundation for scalable, compliant SOC automation across a rapidly growing client base, including the following benefits:

- Centralized visibility for SOC analysts: A single, unified view across all clients via the master tenant, improving operational awareness and coordination.
- Operational scalability: Architecture reviews and provisioning recommendations made with future growth in mind, positioning the company for subsequent phases without redesign.
- Risk-managed delivery under constraints: Mocked APIs and iterative design enabled progress despite the absence of live data and evolving vendor services.

Complex migrations often stall when data cannot be accessed for testing. This project demonstrates how structured discovery, API mocking, and future-proof architecture recommendations can keep critical timelines intact while delivering enterprise-grade visibility across many client environments.

Phoenix Cyber helped the MSSP turn a high-risk, time-constrained migration into a scalable foundation for modern SOC operations.

Phoenix Cyber *is a leading cybersecurity services company providing security engineering, operations, and technical cybersecurity expertise to federal agencies and enterprsies determined to mitigate risk and safeguard their business.*