fortium partners

Case Study

Transforming Cybersecurity: From Fragmentation to Measurable Risk Reduction

Client Profile

- Industry: Enterprise Software - Data Analytics and Cybersecurity
- Annual Revenue: ~ $3B - $4B
- Employees: 7,000 - 9,000
- Headquarters: West Coast, USA

The Challenge

Modern cybersecurity programs are defined not by the number of tools deployed but by how effectively they are operationalized to deliver visibility, detection, and rapid containment. This case study details how Fortium Partners helped a $3B-$4B Enterprise Software firm eliminate fragmentation to achieve over $1.2M in savings and a 75% reduction in attacker dwell time.

The organization's fragmented environment created unacceptable financial waste and elevated its exposure to material cyber and regulatory risks. This failure was compounded by cultural friction and inaccurate reporting, making the security program a business liability rather than a strategic asset.

Key challenges:

- **Fragmented visibility** across security tools, limiting correlation of threats across endpoints, identity, cloud, and email
- **High cost with low return** from a legacy XDR/SIEM platform due to escalating ingestion fees and limited automation
- **SOC maturity gaps,** including alert fatigue, manual processes, and inconsistent incident documentation
- **Staffing misalignment and skill gaps,** leading to slower triage, inconsistent execution, and limited capacity for advanced threats
- **Inaccurate patching visibility** caused by false positives and OS misreporting, creating confusion and wasted effort
- **Cultural friction** between IT and Security teams, slowing decision-making and weakening accountability
- **Increasing regulatory pressure,** requiring stronger governance, documentation, and audit-ready evidence

These issues resulted in reduced detection confidence, slower containment, and elevated enterprise risk.

The Solutions

To address these challenges, a multi-dimensional transformation was executed across technology, operations, governance, and culture. The client engaged Fortium Partners as the Fractional CISO to execute a transformation across six key pillars.

1. **Technology Modernization**
   - Replaced the legacy XDR/SIEM (Extended Detection and Response/Security Information and Event Management) platform, achieving over $1M in cost savings over three years
   - Implemented a unified XDR model with managed 24×7 SOC support (Security Operations Center), increasing detection coverage and containment speed by over 50%
2. **Operational Maturity**
   - Rebuilt the vulnerability management program with risk-tiered prioritization, consistent remediation workflows, and weekly and bi-weekly reporting cadences
3. **Identity and Email Security Enhancements**
   - Implemented OAuth (Open Authorization) governance controls and token revocation playbooks
   - Strengthened phishing defenses and reduced exposure to credential-based and identity-driven attacks
4. **Governance and Accountability**
   - Established cross-functional governance structures, including weekly vulnerability review sessions and monthly cybersecurity risk meetings
   - Defined escalation paths, control ownership, and delivered board-ready dashboards with clear risk visibility
5. **Workforce and Skill Alignment**
   - Deployed a managed XDR/EDR and SOC capability with expert 24×7 monitoring
   - Realigned IT and Security responsibilities and delivered targeted coaching to improve investigation quality and operational discipline
6. **Patching and Reporting Transformation**
   - Rebuilt patching workflows with a single source of truth
   - Eliminated false positives, introduced tiered remediation SLAs (Service Level Agreements), and restored confidence through consistent reporting

The Results

Fortium Partners' engagement delivered over $1.2M in cost savings and a 75% improvement in detection and containment capability, reducing attacker dwell time. The organization accelerated remediation, strengthened 24×7 threat detection and response, and improved audit readiness and governance with clear accountability. Operationally, it achieved faster triage, higher-quality investigations, and stronger IT and Security alignment. Patching and vulnerability management were stabilized through improved visibility and faster remediation, reducing overall cyber, operational, and regulatory risk.