A report prepared in partial completion of
The CYBR 7930 Capstone course

Security Operations Program Design

Utsav Patel

December 1st, 2025

Table of Contents

Executive Summary

COMPANY X is a rapidly expanding financial and digital asset services organization that operates in a highly regulated and continuously evolving threat landscape. Since the company is scaling its cloud infrastructure, customer platforms, and third-party integrations, the operational and regulatory risk exposure increases greatly. COMPANY X's current security operations model cannot reliably support the organization's growing business demands or the sophistication of modern cyber threats.

This Security Operations Design Plan provides a strategic and technical blueprint for maturing COMPANY X's cybersecurity capabilities. Using the security services plan with the support of NIST CSF 2.0 and NIST SP 800-35, the plan addresses the core domains required for a resilient security program, including vulnerability management, threat detection and intelligence, detection engineering, incident response, identity and access governance, application security, and disaster recovery. The design emphasizes strong defense protocols, continuous monitoring, and measurable operational processes while aligning with the security services plan designed by the team to ensure consistency and completeness.

The proposed future-state environment includes deployment guidance, training requirements, and key metrics that will help leadership track progress and validate security effectiveness over time. The plan concludes with an outline and introduction to the Master Security Run Book, enabling analysts and engineers to operationalize the program through structured workflows and clear escalation paths. By adopting this design, COMPANY X strengthens its ability to manage risk, improve response readiness, and supports long-term organizational growth.

Problem Statement

COMPANY X has implemented foundational security controls—such as endpoint protection, encryption standards, password management procedures, firewalls, intrusion detection systems, and NIST-aligned system hardening—along with contingency, incident response, disaster recovery, and business continuity plans. While these measures provided adequate protection in a smaller and less complex environment, they no longer meet the demands created by COMPANY X's expanding cloud services, customer-facing systems, and third-party integrations. Legacy controls lack the scalability, automation, and visibility required to support the security needs of a modern financial services organization.

Despite having documented policies and tools, COMPANY X does not operate a unified or continuously monitored security operations function. Logging is fragmented without a centralized SIEM, vulnerability management is limited to patching rather than risk-based scanning, and threat intelligence is not integrated into monitoring or detection workflows. Incident response remains highly manual and lacks structured escalation, forensic capabilities, and automation, while application security and disaster recovery processes do not align with modern cloud environments. These gaps significantly elevate residual risk,

underscoring the need for a redesigned, intelligence-driven security operations model that provides stronger visibility, faster response, and greater resilience as the organization continues to scale.

Scope

The Security Operations Design Plan applies to the entire organization of COMPANY X, covering all business units, cloud environments, production systems, internal applications, and underlying IT infrastructure. It is intended for technical and operational stakeholders who design, implement, and oversee security functions across the enterprise, providing them with guidance to strengthen detection, response, and resilience in alignment with the Security Services Plan. This document is tailored specifically to COMPANY X's business model, technology footprint, and risk profile rather than serving as an industry-wide standard. Its recommendations are based on the firm's current documentation and previously defined security service design, providing direction across a broad set of cybersecurity capabilities.

Because COMPANY X operates as a financial and digital asset management organization, the plan also considers the organization's unique attack surface, including sensitive customer financial data, authentication records, trading information, and operational logs distributed across multiple environments. These assets require the highest level of protection and monitoring, and the plan's scope reflects this criticality. However, it is limited to the systems and processes explicitly documented in the current state; any undocumented integrations, unknown assets, or future architectural changes may necessitate updates to ensure ongoing relevance as COMPANY X evolves.

To demonstrate cost-conscious prioritization, the following table categorizes COMPANY X's data assets by sensitivity and business impact. This helps identify where security resources, monitoring capabilities, and recovery strategies should be concentrated.

Data Type	Associated Risks	Priority Level
Customer Financial Data (account information, transaction logs, digital asset records)	Data breach, regulatory violation, identity theft, financial fraud	High
Authentication & Access Data (password hashes, MFA tokens, admin credentials)	Account takeover, privilege escalation, insider threat	High
Application Source Code & Dev Assets	Exploitation of vulnerabilities, IP theft, supply-chain compromise	High

Data Type	Associated Risks	Priority Level
Backup & Recovery Data	Ransomware impact, unrecoverable data loss, operational downtime	High
Internal Business Records (operations data, project files, internal documentation)	Unauthorized disclosure, integrity loss	Medium
HR Data (employee records, payroll, benefits)	Privacy violations, identity fraud	Medium
General IT Logs (system logs, firewall logs, operational metrics)	Loss of forensic visibility, delayed detection	Medium
Public Website Content	Defacement, availability impact, brand damage	Low – But High for availability/brand
Marketing and Public Communications	Misinformation, reputational damage	Low

Current Security Operations

This section describes the existing security operations and control mechanisms currently implemented at COMPANY X (COMPANY X). Although the organization has deployed a number of foundational security technologies and documented procedures, these capabilities operate independently and do not yet form an integrated or continuously monitored Security Operations function. The following subsections outline the current control areas in place based on the case study and omnibus documentation.

Endpoint Security Controls

COMPANY X has deployed antimalware solutions across all corporate-owned endpoints to protect against malicious software, unauthorized access, and tampering. The antimalware platform detects and quarantines harmful files, blocks suspicious macros, and prevents users from accessing known malicious web links. These endpoint protections support baseline operational security but operate primarily as standalone tools without centralized analytics or behavioral monitoring.

Data Protection & Encryption Standards

COMPANY X maintains established encryption standards to protect sensitive data in alignment with federal regulatory requirements and industry expectations. The approved encryption algorithms include DES, Blowfish, RSA, RC5, PGP, and IDEA, which are applied across various systems to safeguard confidential customer and operational data. These standards are foundational for data protection but are not yet tied into a broader data governance or classification framework.

Identity & Credential Management

A documented password management procedure governs credential resets, distribution, and auditing. The Technical Support Center (TSC) handles all employee password reset requests and retains audit logs for one year, ensuring accountability for credential changes. While this provides a basic identity management process, the overall identity lifecycle—including provisioning, de-provisioning, and least-privilege enforcement—remains largely manual and decentralized.

Network Perimeter Security

COMPANY X maintains an established perimeter defense architecture that includes enterprise firewalls and a segmented Demilitarized Zone (DMZ). Public-facing services are hosted in the DMZ, separated from internal resources using firewalls configured according to least-access principles. The Network Support Organization manages all firewall devices and applies configuration updates based on department needs and operational requirements. This architecture provides foundational segmentation but lacks advanced monitoring or automated policy enforcement.

Intrusion Detection & Monitoring

Intrusion Detection Systems (IDS) are deployed both at the network perimeter and between the DMZ and internal networks. IDS signatures are updated every two weeks to ensure coverage against known threats. Alerts triggered by the IDS or anomalies observed by administrators must be reported to the IT security office within one hour, and significant incidents involving customer or financial data loss are

escalated to senior leadership within seven days. IDS logs are retained for one year. However, all IDS monitoring occurs at the device level—there is no central SIEM platform to correlate alerts across different systems.

System Hardening & Patch Management

COMPANY X configures all servers, workstations, and laptops according to NIST-recommended security baselines. Operating system updates are deployed using the Software Update Server (SUS), ensuring consistent application of patches across the enterprise. All system changes—including upgrades and configuration adjustments—must be approved through the formal change management process and recorded with timestamps in the change management database. While patching is reliable, vulnerability scanning and remediation are not yet integrated into a continuous, risk-based workflow.

Contingency, Incident Response, and Disaster Recovery Planning

The organization maintains documented Contingency Plans, an Incident Response Plan (IRP), and a Disaster Recovery/Business Continuity Plan (DR/BCP). These documents outline procedures, roles, responsibilities, incident categories, escalation paths, and reporting requirements for various types of security and operational events. Although well-documented, these plans function as compliance artifacts and are not yet supported by automated workflows, integrated tooling, or a dedicated security operations team responsible for real-time coordination.

Intended Security Operations

The future-state Security Operations environment for COMPANY X (COMPANY X) is designed to transition the organization from a collection of foundational, standalone controls toward a centralized, intelligence-driven, and fully integrated security capability. This architecture aligns with NIST CSF 2.0, NIST SP 800-35, and the operational requirements defined in the Security Services Plan. The objective is to enable real-time visibility, rapid detection and response, automated control enforcement, and measurable risk reduction across every part of COMPANY X's technology ecosystem. The following subsections outline the core components of the intended design.

Centralized Threat Detection and Security Monitoring

At the core of the future-state architecture is a Security Information and Event Management (SIEM) platform capable of aggregating logs from firewalls, IDS, cloud environments, endpoints, applications, authentication systems, and critical servers. Unlike the current environment—where logs are stored independently—the SIEM will correlate events, identify anomalies, and alert analysts in real time. Integration with cloud-native telemetry (e.g., Azure logging) and threat intelligence feeds will improve detection fidelity, reduce false positives, and ensure visibility across hybrid environments. The SIEM will serve as the central hub of COMPANY X's detection and response program.

Enhanced Endpoint Detection and Response (EDR)

To strengthen COMPANY X's endpoint security posture, the existing antimalware platform will be upgraded to a modern Endpoint Detection and Response (EDR) solution. EDR will provide behavioral monitoring, automated containment, investigation capabilities, and forensic data collection. This

enables rapid identification of ransomware activity, credential theft, unauthorized lateral movement, and abnormal system behavior. EDR will feed directly into the SIEM, ensuring unified visibility and coordinated alerting across the environment.

Vulnerability Management and Continuous Scanning

The future-state design replaces periodic, patch-focused practices with a continuous, risk-based Vulnerability Management (VM) program. A dedicated VM platform will scan servers, endpoints, containers, and cloud resources on a scheduled and event-driven basis. Findings will be prioritized using CVSS scores aligned with COMPANY X's data classification model, ensuring high-risk assets—such as customer financial systems and authentication infrastructure—receive priority remediation. Integrated dashboards will allow leadership and engineers to track remediation timelines and operational risk exposure.

Threat Intelligence Integration

COMPANY X will adopt a formal Threat Intelligence (TI) capability to identify emerging vulnerabilities, threat actor behaviors, and relevant compromise indicators. Threat intelligence sources—including vendor feeds, ISACs, and public advisories—will feed into the SIEM and detection engineering workflows. This enables predictive defense, timely alert tuning, and proactive threat hunting activities. COMPANY X will use this capability to anticipate attacks targeting financial services organizations, cloud workloads, and identity infrastructure.

Detection Engineering Lifecycle

To operate effective alerting, COMPANY X will establish a Detection Engineering function responsible for creating, tuning, and maintaining detection logic within the SIEM and EDR. All detection rules will follow a documented lifecycle: development → testing → production → versioning → periodic review. This ensures high-fidelity alerts, reduces noise, and provides consistent operational coverage. Detection engineering will also leverage TI insights to design new detections that address emerging attacker techniques.

Incident Response Modernization

While COMPANY X already maintains documented incident response procedures, the future-state design advances these into a fully operationalized Incident Response (IR) program with centralized and coordinated execution. The new model introduces a centralized incident queue within the SIEM, clearly defined triage and escalation roles (Tier 1, Tier 2, Tier 3/Forensics), and automated enrichment processes such as WHOIS lookups, IP reputation checks, and hash analysis to accelerate investigations. The program also integrates with an Incident Management System (IMS) to improve tracking, uses playbook-driven workflows to standardize containment and recovery actions, and establishes defined communication channels for legal, executive, and compliance teams. Additionally, forensic tooling will support root-cause analysis and evidence preservation, enabling rapid, well-structured responses that protect business continuity and support regulatory obligations.

Identity & Access Management (IAM) and Provisioning Controls

To strengthen identity governance and reduce credential-related risk, the future-state design deploys a centralized IAM platform that automates provisioning and de-provisioning, enforces Role-Based Access Control (RBAC), and ensures least-privilege access across all systems. Multi-Factor Authentication (MFA) will be applied consistently throughout the environment, while Privileged Access Management (PAM) controls will secure administrative and high-value accounts. Together, these capabilities provide tighter control over identity lifecycle management, reduce the likelihood of unauthorized access, and improve alignment with financial sector regulatory requirements.

Application Security and Secure Development

To secure COMPANY X's software development lifecycle, the future-state environment integrates Application Security (AppSec) practices directly into development and deployment workflows. This includes the use of Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Software Composition Analysis (SCA) to identify code vulnerabilities and risks introduced through third-party components. Developers will follow structured secure code review procedures, conduct dependency vulnerability checks, and rely on hardened build pipelines to prevent insecure configurations from reaching production. By embedding these capabilities early in the development cycle, COMPANY X reduces the risk of releasing vulnerable software and strengthens application resilience across the enterprise.

Disaster Recovery and Business Resilience

COMPANY X's Disaster Recovery and Business Continuity capabilities will be strengthened through clearly defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), automated backup validation processes, and enhanced cloud failover mechanisms. The organization will conduct regular disaster recovery simulation exercises to validate procedures and ensure readiness, while implementing tiered service resilience requirements to prioritize mission-critical systems. These enhancements improve COMPANY X's ability to maintain operations during cyber incidents, system outages, or infrastructure failures, ensuring the business can recover quickly and reliably.

Integration with Security Service Plan

All future-state security capabilities are fully aligned with the Security Services Plan, ensuring every operational function maps directly to a documented service and its defined goals. This includes SIEM and monitoring operations, EDR and endpoint protection, IAM and access controls, threat intelligence processing, vulnerability management, incident response, data loss prevention and Zero Trust segmentation, disaster recovery and business continuity, and governance, risk, and compliance workflows. By aligning technical capabilities with the service model, COMPANY X creates a unified, cohesive blueprint for long-term security maturity and ensures operational consistency across all project deliverables.

Budget

Implementation costs for these security operations are incurred despite the occurrence of actual security events and might be either direct or indirect costs. Below shows the estimated cost for implementation.

SECURITY OPERATION	COST ESTIMATE	TOTAL PER SECURITY OPERATION
CENTRALIZED THREAT DETECTION & SECURITY MONITORING		
SIEM PLATFORM LICENSING	$80,000	
LOG STORAGE & RETENTION (1 YEAR)	$25,000	
PROFESSIONAL SERVICES (SIEM ONBOARDING)	$12,000	
STAFF TRAINING & CERTIFICATION	$4,000	**$121,000**
ENHANCED ENDPOINT DETECTION & RESPONSE		
EDR SOLUTION LICENSING	$60,000	
DEPLOYMENT & CONFIGURATION SERVICES	$8,000	
EDR TRAINING & ANALYST ENABLEMENT	$3,000	**$71,000**
VULNERABILITY MANAGEMENT & CONTINUOUS SCANNING		
VM PLATFORM SUBSCRIPTION	$35,000	
PROFESSIONAL SERVICES (RISK PRIORITIZATION SETUP)	$7,000	
SCANNING ENGINE DEPLOYMENT	$4,000	
VM TRAINING	$2,500	**$48,500**
THREAT INTELLIGENCE INTEGRATION		
THREAT INTELLIGENCE FEED SUBSCRIPTION	$30,000	
THREAT INTEL PLATFORM (OPTIONAL)	$15,000	
TI TOOLS INTEGRATION	$3,000	
TI CERTIFICATION/ TRAINING	$1,500	**$49,500**
DETECTION ENGINEERING LIFECYCLE		
DETECTION ENGINEERING TOOLKIT	$15,000	
PROFESSIONAL SERVICES	$10,000	
TRAINING	$3,000	**$28,000**
INCIDENT RESPONSE & FORENSICS		
INCIDENT MANAGEMENT SYSTEM	$20,000	
IR RETAINER SERVICE	$15,000	
ANNUAL IR TABLETOP EXERCISES	$8,000	
FORENSIC TOOLING & IMAGE STORAGE	$15,000	
IR TRAINING & CERTIFICATIONS	$5,000	**$63,000**
IDENTITY & ACCESS MANAGEMENT & PROVISIONING		
IAM PLATFORM LICENSING	$65,000	
PAM MODULE LICENSING	$20,000	
PROFESSIONAL SERVICES	$12,000	
IAM TRAINING	$5,000	**$102,000**
APPLICATION SECURITY & SECURE DEVELOPMENT		
SAST/ DAST TOOLING	$30,000	

SECURITY OPERATION	COST ESTIMATE	TOTAL PER SECURITY OPERATION
SOFTWARE COMPOSITION ANALYSIS	$12,000	
DEVSECOPS PIPELINE INTEGRATION	$6,000	
DEVELOPER SECURITY TRAINING	$3,000	**$51,000**
DISASTER RECOVERY & BUSINESS RESILIENCE		
BACKUP & RECOVERY SYSTEM UPGRADE	$20,000	
SECONDARY DATA CENTER/ CLOUD FAILOVER	$25,000	
DR SIMULATION EXERCISES	$5,000	
DR TRAINING & WORKSHOPS	$2,500	**$52,500**
GOVERNANCE, RISK, & METRICS		
GOVERNANCE & RISK PLATFORM	$25,000	
COMPLIANCE AUTOMATION TOOLS	$10,000	
KPI/KRI DASHBOARDING	$6,000	
GRC TRAINING	$2,500	**$43,500**
TOTAL SECURITY OPERATION COST		**$580,000**

Improvement Program

COMPANY X's security operations design is designed to guide the organization from its current state of fragmented baseline controls toward a fully integrated, intelligence-driven environment. The program prioritizes visibility, automation, and resilience, ensuring that each improvement step aligns with both business priorities and the services outlined in the Security Services Plan. Early phrases focus on establishing a centralized point of security that addresses the most immediate operational risks and creates the foundation needed for higher-order capabilities. Subsequent phrases will emphasize deeper integration between systems, management, and security throughout the development process.

As the program matures, COMPANY X will transition into a proactive security posture supported by threat intelligence, detection engineering, and continuous performance measurement. Resilience initiatives will strengthen business continuity and reduce operational downtime during incidents. Each phase of the improvement program increases COMPANY X's security maturity while ensuring cost-efficient investment, proper sequencing of technical deployments, and alignment with regulatory expectations. This staged approach delivers sustainable progress toward a SOC model that supports real-time monitoring, rapid response, and measurable risk reduction.

As mentioned previously, these security operations will span over three years. Below is an improvement program:

Security Operation	Owner	Target Start Date	Target Completion Date
Year 1 – Foundation Buildout			
Centralized Threat Detection & Monitoring	SOC Director	<MM/DD/YYYY>	<MM/DD/YYYY>
Enhanced Endpoint Detection & Response	SOC Director	<MM/DD/YYYY>	<MM/DD/YYYY>
Vulnerability Management & Continuous Scanning	SOC Director	<MM/DD/YYYY>	<MM/DD/YYYY>
Threat Intelligence Integration	CTI Director	<MM/DD/YYYY>	<MM/DD/YYYY>
Year 2 – Response Maturity & Identity Controls			
Incident Response Modernization	IR & Contingency Director	<MM/DD/YYYY>	<MM/DD/YYYY>
Detection Engineering Lifecycle	DFIR Director	<MM/DD/YYYY>	<MM/DD/YYYY>
Identity & Access Management	IAM Director	<MM/DD/YYYY>	<MM/DD/YYYY>
Application Security & Secure Development	CTO	<MM/DD/YYYY>	<MM/DD/YYYY>
Year 3 – Resilience, Governance & Optimization			
Disaster Recovery & Business Resilience	IR & Contingency Director	<MM/DD/YYYY>	<MM/DD/YYYY>
Governance, Metrics, & Reporting	CISO	<MM/DD/YYYY>	<MM/DD/YYYY>

Security Operation	Owner	Target Start Date	Target Completion Date
Security Architecture Enhancements	Steve Smith - CTO	<MM/DD/YYYY>	<MM/DD/YYYY>
Physical & Environmental Security	Melissa Stark – Assistant Operations Officer	<MM/DD/YYYY>	<MM/DD/YYYY>

Master Security Run Book

The master security runbook provides an outline of operations that engineers and administrators will perform for each security operation.

Centralized Threat Detection & Security Monitoring (SIEM)

- SIEM Daily Monitoring Checklist
- Log Source Onboarding Procedures
- Alert Severity Definitions
- Escalation Triggers for High-Fidelity Alerts
- SIEM Dashboard Review Standards

Enhanced Endpoint Detection & Response (EDR)

- Endpoint Enrollment Procedures
- EDR Alert Triage Workflow
- Auto-Isolation Procedures
- Malware Containment Playbook
- EDR Threat Artifact Collection

Vulnerability Management & Continuous Scanning

- Weekly Scan Scheduling
- Asset Criticality Assignment
- Vulnerability Triage & Prioritization
- Patch Verification Workflow
- Critical Vulnerability Escalation Procedures

Threat Intelligence Operations

- Threat Intel Feed Processing
- Indicator Validation & Relevance Scoring
- IOC/IOA Distribution into SIEM & EDR
- TI-Driven Threat Hunting Procedures
- Weekly TI Summary for Leadership

Detection Engineering Lifecycle

- Rule Development & Versioning
- Pre-Deployment Testing Checklist
- Alert Quality Assurance (False Positives/Negatives)
- Monthly Detection Review Cycle
- Documentation Requirements for Rules

Incident Response Modernization

- Incident Classification Matrix (Low → Critical)

- Initial Containment Procedures
- Root Cause Analysis Workflow
- IR Communication Protocols (IT, Legal, Compliance, Execs)
- Post-Incident Review Template

Identity & Access Management (IAM)

- Access Request Workflow (RBAC)
- Privileged Access Approval Process
- Emergency Access Procedures
- User De-Provisioning Checklist
- Quarterly Access Review Playbook

Application Security & Secure Development

- SAST/DAST Execution Workflow
- Secure Code Review Checklist
- CI/CD Integration Steps
- Vulnerability Fix Verification
- AppSec Reporting Requirements

Disaster Recovery & Business Resilience

- DR Activation Criteria
- Failover Execution Procedures
- Backup Validation Checklist
- RTO/RPO Tracking Workflow
- DR Exercise Playbook

Governance, Metrics & Reporting

- KPI/KRI Measurement Model
- Weekly SOC Metrics Review
- Monthly Security Leadership Briefing
- Quarterly Policy & Control Review
- MSRB Maintenance & Update Schedule

Conclusion

The Security Operations Design Plan provides COMPANY X with a clear, modern, and actionable blueprint for maturing its security capabilities into an integrated, intelligence-driven operational model. By transitioning from fragmented baseline controls to a coordinated set of capabilities, COMPANY X establishes the foundation for sustained risk reduction, regulatory alignment, and operational reliability. This plan not only outlines the future state architecture but also defines the phased improvement path and operational run-book structure necessary to support consistent execution. As COMPANY X continues to evolve, this design provides a scalable framework that can adapt to new threats, technologies, and business priorities while ensuring a measurable increase in security maturity and organizational resilience.

Reference

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework 2.0. https://www.nist.gov/cyberframework

Scarfone, K., & Smith, M. (2003). Guide to Information Technology Security Services (NIST SP 800 35). National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-35/final