
# Building a Centralized SOC from the Ground Up

## How a Sweden-Based Financial Institution Launched a 24/7 Threat Monitoring Program

A mid-sized financial institution in Sweden needed a dedicated Security Operations Center (SOC) to combat rising cyber threats and adhere to European compliance mandates. Krish Services Group designed and deployed an end-to-end SOC capability with structured processes, tiered teams, and global coverage.

## CLIENT BACKGROUND

The client is a well established financial services organization based in Sweden, offering retail banking, credit, and fintech products to consumers and small businesses. As the organization scaled digitally, cyber threats and regulatory scrutiny necessitated building a robust, centralized cybersecurity operations program.

## BUSINESS VALUE

**Real-World Incident Containment:**

SOC detected and mitigated a business email compromise from Nigeria in under two hours.

**Policy Reinforcement:**

Strengthened MFA, email protections, and introduced phishing simulations post-incident.

**End-to-End Security Readiness:**

From staffing to automation, the SOC became a foundational control for financial risk management.

## PROBLEMS

- **No Centralized Security Monitoring:** The organization lacked a SOC function to detect, triage, or respond to emerging threats in real time.
- **Escalating Cyber Threats:** Cloud-first and remote work adoption exposed new vulnerabilities across endpoints and emails.
- **Regulatory Compliance Pressure:** EU financial regulations required demonstrable response readiness and incident metrics like MTTR and MTTD.

## SOLUTIONS

- **Multi-Tiered SOC Team Setup:** Deployed Tier 1, 2, and 3 analysts, a SOC manager, and a threat intelligence analyst. Achieved 24/7 support using a follow-the-sun team model.
- **Advanced Security Stack:** Implemented Splunk SIEM, CrowdStrike EDR, and a SOAR platform integrated with threat intel feeds.
- **Process Enablement:** Developed runbooks, KPIs, and maturity assessments for ongoing SOC performance validation.

## TECHNOLOGIES

splunk>

SOAR

CROWDSTRIKE

## Final Perspective

Krish Services Group helped the client transition from fragmented threat handling to a fully operational SOC with measurable KPIs, rapid response, and continuous security improvement.