CASE STUDY Security operations build | SOC AND SIEM | FINANCIAL SERVICES

A 24/7 SOC for a Swedish financial firm
Email attack contained in 2 hours.

A mid-sized financial institution in Sweden faced rising cyber risk and stricter European rules. We designed and deployed a full **Security Operations Center** with tiered analysts, defined processes and **continuous monitoring**.

CLIENT: A MID-SIZED FINANCIAL SERVICES FIRM IN SWEDEN

CONTAINMENT

2 HRS

A business email compromise detected and contained within 2 hours

COVERAGE

24/7

Round-the-clock monitoring with a follow-the-sun model

ANALYST TIERS

3

Tiered teams for triage, incident response and threat hunting

CLIENT BACKGROUND

The client is an **established financial services organization in Sweden**. It offers retail banking, credit and fintech solutions to consumers and small businesses.

As digital adoption grew, the attack surface expanded and regulators expected more. To protect customer data and keep trust, the firm needed a central security operations model aligned with European compliance standards.

BEFORE
Fragmented threat handling
No central monitoring or formal incident process

→

AFTER
A fully operational SOC
24/7 monitoring, runbooks and measurable KPIs

THE CHALLENGE

No central security monitoring
Without a SOC, real-time detection, alert triage and coordinated response were limited.

A growing threat landscape
Cloud adoption and remote work raised exposure across endpoints, identities and email.

Stricter regulatory expectations
European financial rules called for measurable incident metrics and audit-ready processes.

No formal incident response
There was no defined process for handling and escalating security incidents.

No automated workflows
Security tasks ran by hand, which slowed detection and response.

Customer trust at stake
The firm had to protect customer data to keep the trust of consumers and small businesses.

WHAT WE DELIVERED

01 **Tiered SOC team** — TIER 1 TO 3
Triage, incident response and threat hunting tiers, with a SOC manager and threat intel analyst.

02 **24/7 coverage** — 24/7
A follow-the-sun model with international support keeps monitoring running around the clock.

03 **Integrated security stack** — SIEM · EDR
SIEM, EDR, SOAR automation and threat intelligence feeds for better correlation.

04 **Runbooks, escalation paths and KPIs** — MTTD · MTTR
Runbooks plus metrics such as mean time to detect and mean time to respond.

05 **SOC maturity testing** — EXERCISES
Regular exercises and maturity assessments keep operations repeatable and improving.

06 **Post-incident hardening** — MFA
Stronger MFA, Conditional Access and email policies, plus phishing simulations.

RESULTS

2HRS — **Email compromise contained**
A business email compromise was contained within 2 hours, limiting impact.

24/7 — **Continuous monitoring**
Global tiered coverage speeds escalation and keeps handling consistent.

Stronger security policies
Better MFA, email security and awareness cut the risk of repeat incidents.

Enterprise-wide readiness
The SOC became a core control for threat response and financial risk management.

Incident in focus. Unusual executive login caught, account reset, malicious forwarding rules found, contained in 2 hours.

TECHNOLOGIES USED

Splunk (SIEM) · CrowdStrike (EDR) · SOAR · Threat intel feeds · Conditional Access

FINAL PERSPECTIVE

Krish helped the client move from **fragmented threat handling to a fully operational SOC**, with measurable KPIs, rapid response and continuous improvement.

Building or maturing a SOC?

Talk to a Krish security engineer.

krishservicesgroup.com/contact-us
+1 (813) 494-4015

Read this case study online: krishservicesgroup.com/case-study/end-to-end-soc-for-a-mid-sized-european-firm/