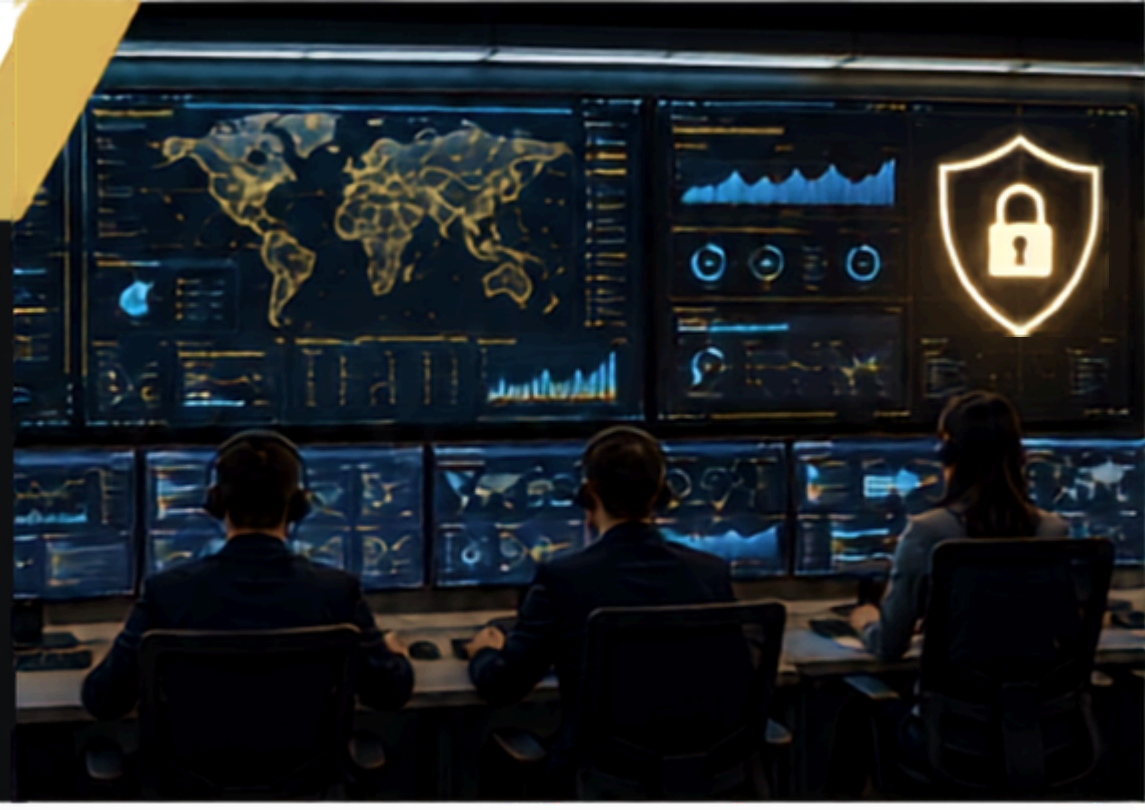
FLINT
Empowering Through Experience

CASE STUDY

# Managed Cyber Defense & Intelligence - Telecom SOC, Dubai

*50,000+ assets. 2,000+ alerts a week. One SOC that cannot blink.*



## CLIENT
Cisco's enterprise customer, Dubai, UAE

## SECTOR
Telecom / Enterprise ICT

## SERVICE
Managed SOC operations, cyber defense & intelligence

## THE ENVIRONMENT
Cisco needed a trusted, highly specialized Managed Security Services Partner to operate and mature a mission-critical Security Operations Center for one of its major Dubai customers. The scale of the environment set the bar:

- **50,000+** monitored assets
- **2,000+** alerts per week
- **150+** security applications
- **24×7** operations

Those 150+ applications spanned SIEM, Soar, EDR, NDR, TIP, IAM, VTM and more - a stack that had to be run as one coherent defense, not a collection of consoles.

## THE MANDATE
Elevate cyber-defense maturity and deliver 24×7 incident readiness, sharper threat visibility and strict SLA adherence across every domain — real-time monitoring and incident response, cyber-infrastructure operations, DevOps, IAM governance, vulnerability and threat-exposure management, and security change reviews — all without interrupting operations.

## WHAT FLINT RAN
Flint took the end-to-Cyber Defense & Intelligence program for a full year, across the operational, analytical and strategic layers of the SOC - L1/L2 at 24*7 and L3 in business hours with on-call:

Security monitoring & Incident Response- **Proactive detection, triage, IOC analysis, incident handling and threat-intelligence enrichment.**

DFIR & DevOps — SIEM/Soar optimization, log-source onboarding, security automation, patching, use case engineering and content modernization.

Identity & access management - access governance, UAM ticket execution, access reviews and audit-ready reporting.

Vulnerability & threat management - scanning, prioritization, remediation guidance and risk escalation to cut high-risk exposure.

Operational change reviews - firewall assessments, configuration audits, infra change reviews, capacity planning and documentation.

### THE NUMBERS THAT MATTER

Performance was held to defined SLAs across the program:

| METRIC | SLA ACHIEVED |
|---|---|
| P1 Incident detection | ≤ 15 minus |
| P1 Incident resolution | ≤ 75 minutes |
| IAM service levels | 95–97% |
| Content / onboarding SLA | 99% |
| Vulnerability (VTM) SLA | Met across all severity categories |

## THE RESULT
Cisco's customer reached a highly resilient security operations environment — stronger threat detection, faster remediation cycles and robust governance maturity, with alert fatigue actively reduced rather than tolerated. SOC operations in Dubai ran uninterrupted across the year, reinforcing trust and establishing a scalable framework for future cyber-defense initiatives across the region.

## AI-DRIVEN MANAGED SERVICES
At SOC scale - 50,000+ assets and 2,000+ weekly alerts - AI is decisive: Flint applies it to cut alert noise, automate triage and surface the signals that matter, enabling smarter, faster decisions without adding analyst headcount

Al Rashid Center, 4th Floor King Saud Road, Al Murabba Riyadh 12612, Saudi Arabia

www.flint-international.me