

Cybersecurity Operations Service (SOC)

It is a centralized operations service that monitors, analyzes, and manages incident response processes for organizations 24/7. It ensures that CSIRT processes, threat analysis, and incident response operations are handled from a single center.

Cybersecurity Challenges for Organizations

Organizations require continuous monitoring due to advanced threats, ransomware, data leaks, and insider threats. Scattered log structures and manual analysis processes cause critical incidents to be noticed too late. The SOC service analyzes data from different security systems centrally, prioritizes threats, and ensures that swift action is taken.



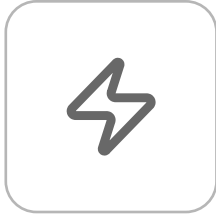
Who can benefit?

- For organizations noticing security incidents late
- For operations teams performing manual log analysis
- For SOC teams struggling with false alarm management
- For organizations requiring 24/7 monitoring and response

Core Principles



Accuracy
False alarm reduction



Fast Response
Swift action on critical events



Continuous Monitoring
24/7 seamless incident tracking



Visibility
Centralized log and event visibility

How Does the SOC Service Work?

The SOC service collects logs from security products within a centralized SIEM infrastructure. Events are analyzed with correlation rules and threat intelligence; critical alarms are prioritized, and incident response processes are managed.

Technical Specifications

Log Collection and Monitoring

- ✓ SIEM analysis across different sources
- ✓ Unified log integration structure
- ✓ Active log continuity tracking
- ✓ Error and accessibility tracking

SIEM and Incident Management

- ✓ Anomaly threat analysis
- ✓ Dynamic threat correlation
- ✓ IP and user visibility
- ✓ Risk-focused alarm optimization

Threat Intelligence

- ✓ Malicious IP and hash tracking
- ✓ Up-to-date IOC integration
- ✓ Custom threat hunting for organizations
- ✓ Attack trend analysis

Reporting and Operations

- ✓ Centralized SOC incident reports
- ✓ SLA-based response tracking
- ✓ Compliance and log support
- ✓ 24/7 SOC operational support

