MANAGED SOC SERVICE OVERVIEW

THREATREMEDIATE™ 24/7 SECURITY OPERATIONS CENTER

THE CHALLENGE

Building an in-house SOC costs $2-5M annually and takes 12-18 months to operationalize. Even then, staffing a 24/7 operation requires 8-12 analysts—talent that's increasingly impossible to find and retain.

The reality:

- 3.5 million cybersecurity positions remain unfilled globally
- Average SOC analyst tenure is just 18–24 months
- Most attacks happen 24/7—your team works 9–5

THE VIJILAN APPROACH

Our Certified Security Operations Center becomes an extension of your team. We provide 24/7/365 monitoring, triage, and response—staffed by expert analysts who know your environment.

SOC CAPABILITIES

Monitoring & Detection

- Real-time log analysis across all sources
- Behavioral anomaly detection
- Correlation across endpoint, identity, and network
- Custom detection rules for your environment

RESPONSE & CONTAINMENT

- Automated playbook execution
- Manual intervention for complex threats
- Host isolation and process termination
- Account lockout and password reset coordination

INVESTIGATION & TRIAGE

- Severity classification (P1-P4)
- Root cause analysis
- Attack timeline reconstruction
- Indicator of Compromise (IOC) extraction

REPORTING & COMMUNICATION

- Real-time portal access
- Instant notification (email, SMS, phone)
- Post-incident reports
- Compliance-ready documentation

SOC CERTIFICATIONS & COMPLIANCE

Our SOC maintains the highest industry certifications:

Certification	Description
ISO 27001	Information Security Management
SOC 2 Type 2	Security, Availability, Confidentiality
GDPR Compliant	EU Data Protection
HIPAA Compliant	Healthcare Data Security

ANALYST TEAM

Our analysts aren't entry-level—they're battle-tested experts:

Certifications Required:
- GCIA (GIAC Certified Intrusion Analyst)
- GCIH (GIAC Certified Incident Handler)
- OSCP (Offensive Security Certified Professional)
- CrowdStrike Certified Falcon Administrator

Average Experience: 7+ years in security operations

Continuous Training: Monthly threat briefings, annual certification renewals

vijilan.com
info@vijilan.com
+1 (954) 334-9988

INCIDENT RESPONSE WORKFLOW

EXECUTE

TRIAGE (Tier 1)
Analyst reviews within SLA

INVESTIGATE (Tier 2)
Scope, impact, root cause

RESPOND (Tier 3)
Contain, isolate, remediate

REPORT
Document, notify, improve

TECHNOLOGY STACK

Our SOC is built on industry-leading platforms:

Primary Platform: CrowdStrike Falcon
- LogScale (Next-Gen SIEM)
- Falcon Insight (EDR/XDR)
- Falcon Identity (ITDR)
- Falcon Spotlight (Exposure)

Data Pipeline: Cribl
- Log routing and enrichment
- 40-60% cost reduction
- Universal log compatibility

Network Visibility: Corelight
- Zeek-based network detection
- Full packet metadata
- Encrypted traffic analysis

SERVICE LEVELS

Metric	Essentials	Premium
Coverage	24/7/365	24/7/365
Initial Response	30 minutes	15 minutes
Escalation to Analyst	60 minutes	30 minutes
Incident Acknowledgment	4 hours	1 hour
Post-Incident Report	5 business days	24 hours
Threat Hunting	Monthly	Continuous
Dedicated Analyst		✓

COMMUNICATION & ESCALATION

Real-Time Alerts:
- Email notification (immediate)
- SMS for critical (P1) incidents
- Phone call for confirmed breaches

Regular Reporting:
- Daily digest (optional)
- Weekly executive summary
- Monthly business review
- Quarterly strategic review

Escalation Path:
1. SOC Analyst → Your IT/Security Team
2. SOC Manager → Your Security Leadership
3. VP Security Operations → Your CISO/Executive Team

ONBOARDING TIMELINE

Phase	Duration	Activities
Discovery	Week 1	Environment review, stakeholder interviews
Integration	Week 2	Log source connection, agent deployment
Tuning	Weeks 3–4	Baseline establishment, false positive reduction
Go-Live	Week 5	Full monitoring activation
Optimization	Ongoing	Continuous improvement, threat hunting

YOUR TEAM CAN'T BE EVERYWHERE. OURS IS.

Get 24/7 threat detection, investigation, and expert response—without building a SOC from scratch.

vijilan
IT Security: Enabled

vijilan.com
info@vijilan.com
+1 (954) 334-9988

AICPA SOC
ISO 27001
A-LIGN