THREATREMEDIATE 24/7 RESILIENT SOC & SIEM

Vijilan's ThreatRemediate platform offers a comprehensive Security Operations Center (SOC) and Security Information and Event Management (SIEM) solution, providing both monitoring and active threat containment. Our U.S.-based SOC operates around the clock to ensure real-time detection and response to every incident

Business Impact

- Reduce incident response time with proactive, automated containment
- Lower SIEM costs using index-free log ingestion and efficient storage
- Achieve continuous compliance with audit-ready log retention and reporting
- Enhance visibility across endpoints, network, cloud, and identity sources
- Empower MSPs and clients via multi-tenant, white-labeled portal access

Key Capabilities

Firewall IP blocking, email domain restrictions, endpoint isolation, user account disablement, and MFA enforcement

CrowdStrike Falcon LogScale + Cribl for high-performance ingestion, normalization, and storage

Corelight Zeek & Suricata integrations for deep network and endpoint monitoring

Analytics to detect lateral movement and privilege misuse in real time

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

Use Cases

- Automatically block malicious traffic and quarantine endpoints at first indication
- Disable compromised user accounts and enforce dynamic MFA in minutes
- Seamlessly integrate alerts and incidents into ConnectWise, Zendesk, Jira, ServiceNow, and more
- Deliver branded dashboards and compliance reports to MSP clients via a multi-tenant portal

Compliance Alignment

- HIPAA: Continuous monitoring, audit-ready log retention, and access controls
- PCI DSS v4.0: Secure log collection, monitoring, and forensic readiness
- CMMC 2.0: Evidence-based incident response and containment workflows
- NIST 800-53: SI-4 (Continuous Monitoring), AU-2 (Audit Events), IR-5 (Incident Monitoring)
- ISO Standards: Comprehensive SOC operations aligned to global best practices

Part of the ThreatRemediate Ecosystem

Falcon Identity
Link user behavior with threat telemetry

Falcon Exposure Management
Prioritize and remediate vulnerabilities

Falcon Discover
Monitor device and application changes in real time

Falcon LogScale
Ingest SOC data into SIEM for advanced analytics

Falcon Resilient SOC
24/7 containment, escalation, and response from Vijilan

Falcon EDR/XDR
Correlate exposures with endpoint activity

vijilan
IT Security: Enabled
vijilan.com
info@vijilan.com
+1 (954) 334-9988