THREATRESPOND OVERVIEW & POSITIONING

ThreatRespond is Vijilan's vendor-agnostic, 24/7 detection and alerting solution, designed for MSPs that need round-the-clock visibility, validated threat insights, and expert escalation — all without handing over remediation control. It is powered by our cloud-native SIEM and integrated detection ecosystem.

How It Works

ThreatRespond includes access to Vijilan's cloud-based SIEM, the Vijilan Information Security Hub (ViSH), hosted securely on AWS in the US. On-premise environments are connected via the Threat Sensor — a lightweight log collection appliance that parses, normalizes, and securely ships logs to ViSH. There, logs are enriched and correlated using threat intelligence feeds from global leaders like CrowdStrike, as well as our proprietary detection content.

Detection & Escalation Workflow

Logs are collected via Threat Sensor from on-prem environments (e.g., firewalls, AD, servers, etc.)

Data is enriched and analyzed in ViSH using detection use cases and threat intelligence

When suspicious activity is detected, a ticket is generated and routed to our 24/7 SOC

Vijilan SOC Analysts review, triage, and validate alerts; false positives are closed immediately

Escalations are sent to our Incident Response Team (IRT) for deeper investigation

If required, the IRT activates a communication plan to alert MSP partners for action

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

Key Benefits

- Complete 24/7 monitoring without needing to replace your security stack
- Alerts are triaged and validated by humans, not just AI
- Access to a cloud-native SIEM (ViSH) with threat enrichment
- Vendor-agnostic: works with any firewall, endpoint, SIEM, or cloud system
- Full integration with PSA systems for ticket delivery

Optional Add-On: Falcon EDR/XDR Licensing & Management

MSPs who wish to deploy Falcon EDR/XDR can purchase licenses through Vijilan under ThreatRespond. Vijilan will deploy, manage, and monitor the Falcon agent while maintaining full alert visibility and triage.

Ideal for

- MSPs who already have tools but need expert monitoring and alert validation
- Partners who want to offer advanced detection under their own brand
- Organizations transitioning to a managed SIEM model without full MDR
- MSPs needing SOC 2-aligned, US-based 24/7 monitoring for compliance and reporting

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