

FALCON ADVERSARY OVERWATCH

24/7 Managed Threat Hunting Powered by AI & Elite Analysts

Stop Advanced Threats Before They Become Breaches

Modern adversaries move fast—often within seconds—using stolen credentials, cloud misconfigurations, and lateral movement across endpoints, identity systems, and cloud environments. Traditional tools can't keep up.

Vijilan, powered by CrowdStrike Falcon Adversary OverWatch, delivers proactive, 24/7 managed threat hunting to detect and stop threats in real time—before damage occurs.

Comprehensive Threat Hunting Coverage

- **Endpoint Threat Hunting** – Detect stealthy malware, living-off-the-land attacks, and persistence techniques
- **Identity Threat Protection** – Monitor credential abuse, account takeover attempts, and insider threats
- **Cloud Threat Detection** – Secure AWS, Azure, and GCP environments from misconfigurations and compromise
- **Extended SIEM Visibility** – Ingest and analyze third-party data (firewalls, VPNs, email, SaaS, IAM)

Powered by Vijilan's 24/7 SOC

With Vijilan, you get more than technology:

- Dedicated threat hunters and SOC analysts
- Real-time alert triage and investigation
- Guided response and containment support
- Proactive threat intelligence and reporting
- Seamless integration with your existing security stack

Why Vijilan + CrowdStrike OverWatch

- Fully Managed (No Internal Resources Required)
- Faster Detection & Response Times
- Reduced Alert Fatigue
- Improved Compliance Readiness (HIPAA, GDPR, SOC 2)
- White-Labeled for MSP & MSSP Delivery

Use Cases

- Detect credential-based cloud intrusions
- Stop ransomware before execution
- Identify insider threats and anomalous behavior
- Correlate multi-domain attacks across endpoint, identity, and cloud
- Gain visibility into stealthy adversaries missed by traditional tools

Get Ahead of Threat Actors

Attackers are faster than ever—your defense needs to be faster.

Partner with Vijilan to gain elite threat hunting, real-time detection, and 24/7 protection—without adding complexity.

What You Get with Vijilan OverWatch



24/7 Proactive Threat Hunting

Our expert SOC analysts continuously hunt for hidden adversaries across your entire attack surface—endpoint, identity, cloud, and network.



Early Threat Detection & Rapid Response

Identify attacker activity early in the kill chain and stop lateral movement before it escalates into a breach.



Full Attack Surface Visibility

Correlate telemetry across endpoints, cloud workloads, identity systems, SaaS apps, and third-party SIEM data for complete visibility.



AI-Driven Detection & Intelligence

Leverage AI-powered analytics and real-time threat intelligence tracking 250+ adversary groups to uncover sophisticated attacks.



Immediate Protection, No Deployment Delays

Start detecting threats instantly—no downtime, no complex setup, no additional overhead.



CONTACT VIJILAN TODAY

Secure your organization with industry-leading managed threat hunting.