vijilan
IT Security: Enabled

NEXTDEFEND™

FOR END CUSTOMERS

Powered by **CrowdStrike** Falcon Next-Gen SIEM

We Stop Breaches Together with CrowdStrike.

NextDefend™ is an end-to-end managed service built on CrowdStrike Falcon Next-Gen SIEM. Every engagement includes **Onboarding and 24/7 SOC Operations** as the foundation, with **Managed Services available as an optional add-on** — Lite (40 hours) or Standard (80 hours) — for customers that want ongoing engineering capacity. Vijilan's 24/7 global SOC operates the platform, ingests third-party data, hunts across the full data fabric, and coordinates joint remediation. NextDefend works in tandem with Falcon Complete and Adversary OverWatch — extending CrowdStrike protection across cloud, identity, network, and SaaS — and replaces or augments internal IT and end-customer SOC operations.

ROLES & RESPONSIBILITIES MATRIX

24/7 Global SOC	**1 min** Median Time to Contain	**MITRE** ATT&CK Aligned

BUILT FOR HOW YOU BUY.

Every NextDefend engagement includes Onboarding and 24/7 SOC Operations as the foundation. Managed Services — Lite (40 engineer hours) or Standard (80 engineer hours) — is available as an optional add-on for customers that want ongoing engineering capacity for content, parsers, dashboards, and tuning. Customers with strong internal teams often skip Managed Services entirely; customers that want a true co-managed experience add it on.

1. ONBOARDING	2. 24/7 SOC OPERATIONS	3. MANAGED SERVICES(OPTIONAL)
Falcon Next-Gen SIEM tenant build, Falcon integration, third-party data ingest design, parser development, baseline detection content, MITRE ATT&CK mapping, and validated handover.	Round-the-clock monitoring, alert triage, cross-source threat hunting, incident response, joint containment / eradication / recovery, and full post-incident reporting. Included in every engagement.	Ongoing platform management, content evolution, parser maintenance, monthly tuning, and pipeline health. Available as Lite (40 engineer hours) or Standard (80 engineer hours) per annual contract.

THE THREE-PARTY SHARED RESPONSIBILITY MODEL

CrowdStrike provides the platform and Falcon-native protection. Vijilan operates the SOC layer and coordinates joint remediation. The Customer owns business-system recovery and organizational follow-through.

CROWDSTRIKE	VIJILAN SOC	CUSTOMER
Falcon Next-Gen SIEM platform, Charlotte AI, Adversary OverWatch threat hunting on Falcon telemetry, and policy infrastructure. Falcon Complete (where present) provides endpoint-native containment.	24/7 platform operations, third-party ingest, alert triage, cross-source threat hunting, joint containment and eradication, and full post-incident reporting on top of the CrowdStrike platform.	Business systems, change-window approvals, user communications, and recovery execution within business operations. Lessons-learned ownership and organizational follow-through.

PARTNERSHIP & CERTIFICATIONS

Vijilan is an Authorized CrowdStrike Partner and CrowdStrike Powered Service Provider (CPSP), holding the full set of partner designations and Falcon specializations. Our SOC operates under audited corporate compliance, and our engineers carry the CrowdStrike certifications required to operate every layer of the Falcon platform.

CROWDSTRIKE PARTNERSHIP

Authorized Partner
CrowdStrike Powered Service Provider (CPSP)

PARTNER DESIGNATIONS
- MSSP Partner
- Powered Service Provider (PSP)
- Solution Provider / Reseller
- Technology Alliance Partner
- Service Delivery Partner

FALCON SPECIALIZATIONS
- Falcon Next-Gen SIEM
- Falcon Identity
- Falcon Cloud Security

VIJILAN CERTIFICATIONS

CORPORATE COMPLIANCE
- SOC 2 Type 2
- ISO 27001
- PCI DSS
- HIPAA-aligned
- GDPR-aligned
- CMMC

ENGINEER CERTIFICATIONS
- CCFA — Falcon Administrator
- CCFR — Falcon Responder
- CCSE — SIEM Engineer

ROLES & RESPONSIBILITIES MATRIX

This matrix details responsibilities across the three parties for a full NextDefend engagement — Onboarding and 24/7 SOC Operations as the foundation, with optional Managed Services (Lite or Standard). Rows tied specifically to Managed Services apply only when that add-on is selected.

Roles & Responsibilities	CrowdStrike	Vijilan SOC	Customer
Onboarding & Planning			
Provide CrowdStrike Falcon Next-Gen SIEM platform and tenant	✓		
Procure Falcon Next-Gen SIEM licensing (direct, via VAR, or via Vijilan)			✓
Conduct Solution Architecture Workshop and scoping		✓	✓
Provide environment inventory, log source list, and access credentials			✓
Configure NGSIEM tenant and base platform settings	✓	✓	
Design and build third-party data ingestion pipelines (Cribl, syslog, API)		✓	
Develop custom parsers for non-standard or proprietary data sources		✓	
Approve change windows for production data source onboarding			✓
Deploy baseline correlation rules, dashboards, and detection content		✓	
Map detection coverage to MITRE ATT&CK framework		✓	
Conduct Day 7 Service Excellence call (operating model, escalation, cadence)		✓	✓

Roles & Responsibilities	CrowdStrike	Vijilan SOC	Customer
Steady State — Platform Operations			
Maintain Falcon Next-Gen SIEM platform availability	✓		
Monitor data pipeline health and ingestion volume		✓	
Maintain and tune custom parsers as source schemas evolve		✓	
Manage NGSIEM ingest cost optimization (Cribl routing, sampling, tiering)		✓	✓
Onboard additional data sources as customer environment expands		✓	✓
Notify Vijilan SOC of new data sources or environment changes			✓

Roles & Responsibilities	CrowdStrike	Vijilan SOC	Customer
24/7 SOC Operations —Monitoring & Triage			
Provide 24/7/365 monitoring across Falcon and third-party data		✓	
AI-native detection via Charlotte AI on Falcon platform	✓		
Tier 1 alert triage, enrichment, and false-positive suppression		✓	
Tier 2 investigation and cross-source correlation		✓	
Escalate confirmed incidents per agreed escalation matrix		✓	
Acknowledge and act on Vijilan escalations within agreed SLA			✓

Roles & Responsibilities	CrowdStrike	Vijilan SOC	Customer
Cross-Source Threat Hunting			
Adversary OverWatch — elite hunting on Falcon endpoint telemetry	✓		
Hypothesis-driven hunts across third-party data (identity, cloud, SaaS, network)		✓	
Ad-hoc hunts within 48 hours of CrowdStrike Intel critical bulletins		✓	
Cross-source pivot hunts (endpoint → identity → cloud → SaaS chains)		✓	
Hunt reports with hypothesis, queries, and findings (positive and negative)		✓	
Feed hunt findings back into detection engineering content cycle		✓	
Containment— Joint Effort			
Endpoint isolation and process termination via Falcon (where Falcon Complete present)	✓		
Endpoint containment via Falcon RTR (where Falcon Complete not present)		✓	
Identity containment — disable accounts, force re-auth via Entra/Okta API		✓	
Network containment — firewall, email gateway, proxy API actions		✓	
Cloud containment — IAM revocation, resource isolation via cloud APIs		✓	✓
Approve emergency containment actions outside pre-authorized scope			✓
Coordinate user-facing communications during active containment			✓

Roles & Responsibilities	CrowdStrike	Vijilan SOC	Customer
Eradication— Joint Effort			
Malicious artifact removal on Falcon-protected endpoints (Falcon Complete)	✓		
Remove malicious artifacts via API across third-party systems		✓	
Develop and deploy new detection content to prevent recurrence		✓	
Patch vulnerable systems and applications			✓
Rotate credentials, revoke OAuth grants, reset secrets in business apps		✓	✓
Threat intelligence enrichment and IOC pivoting		✓	
Recovery— Joint Effort			
Endpoint health validation and full system restoration (Falcon Complete)	✓		
Validate clean state across all monitored data sources		✓	
Restore business operations and re-enable user access			✓
Tune detection content based on incident learnings		✓	
Stakeholder and end-user communications			✓

Roles & Responsibilities	CrowdStrike	Vijilan SOC	Customer
Post-Incident & Reporting			
Provide full post-incident report and root cause analysis		✓	
Deliver monthly SOC performance and cadence reporting		✓	
Apply organizational lessons learned and policy updates			✓
Quarterly business review with detection coverage and roadmap		✓	✓

KEY COMMITMENTS

WORKS IN TANDEM

NextDefend complements Falcon Complete and Adversary OverWatch — it does not replace them. Falcon protects the endpoint. NextDefend extends protection across cloud, identity, network, and SaaS through Falcon Next-Gen SIEM.

REPLACES OR AUGMENTS

NextDefend replaces or augments internal IT and end-customer SOC operations. Whether you have no SOC, a partial SOC, or a 9-to-5 SOC, NextDefend provides the 24/7 coverage and cross-source hunting your environment requires.

JOINT REMEDIATION

Vijilan acts on every system we have API access to — endpoint, identity, cloud, network, SaaS. Where we cannot act — your business systems, your change windows, your users — we hand you a runbook and stay on the call until you are recovered.

FLEXIBLE COMMERCIAL MODEL

Every engagement includes Onboarding and 24/7 SOC Operations. Managed Services is an optional add-on — Lite (40 engineer hours) or Standard (80 hours) — for customers that want ongoing engineering capacity. Customers with strong internal teams skip it; customers wanting a true co-managed experience add it on.

NEXTDEFEND ™

Powered by **CrowdStrike** Falcon Next-Gen SIEM

We Stop Breaches Together with CrowdStrike.

vijilan IT Security: Enabled