MANAGED ITDR SERVICE OVERVIEW

THREATREMEDIATE™ IDENTITY THREAT DETECTION & RESPONSE

THE CHALLENGE

80% of breaches involve compromised credentials. Attackers don't break in—they log in. Yet most organizations still treat identity as an IT problem, not a security problem.

The reality:

- Credentials are the #1 attack vector
- Average organization has 10x more service accounts than employees
- Active Directory is 20+ years old and riddled with misconfigurations
- Traditional MFA doesn't stop pass-the-hash or token theft

THE VIJILAN APPROACH

ThreatRemediate ITDR protects the identity layer—where modern attacks actually happen. We monitor Active Directory, Entra ID, and cloud identities in real-time, detecting and stopping credential-based attacks before they escalate.

PLATFORM: CROWDSTRIKE FALCON IDENTITY

Our platform detects identity-based threats such as Active Directory attacks (Kerberoasting, Golden Ticket, DCSync), unusual login behavior, and lateral movement, while protecting cloud identities across Entra ID, Okta, and federated systems.

We also improve identity hygiene by identifying stale accounts, excessive privileges, unused service accounts, and weak password policies. As part of a Zero Trust foundation, we provide real-time identity risk scoring, enable conditional access, uncover MFA enforcement gaps, and detect shadow admin accounts that may go unnoticed.

Success Metrics

Within 90 days, organizations typically see a 50%+ reduction in identity attack surface, gain 100% visibility into service accounts, achieve an 80% reduction in shadow admin accounts, and experience zero successful credential-based attacks.

WHAT'S INCLUDED

Capability	Description
AD Security Monitoring	Real-time detection of AD attacks and misconfigurations
Entra ID Protection	Cloud identity threat detection for Microsoft 365
Lateral Movement Detection	Catch attackers moving through your network
Credential Theft Prevention	Stop pass-the-hash, Kerberoasting, DCSync
Identity Hygiene	Find and fix risky configurations
Zero Trust Enablement	Risk-based conditional access recommendations

HOW IT WORKS

MONITOR
Continuous visibility into AD, Entra ID, Okta

DETECT
AI + behavioral analytics identify threats

ANALYZE
SOC analysts investigate identity incidents

RESPOND
Lock accounts, reset creds, block access

HARDEN
Fix misconfigurations, reduce attack surface

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

AICPA SOC · ISO 27001 · A-LIGN

COMPLIANCE SUPPORT

Our solution helps organizations meet identity and access-related requirements across key frameworks, including HIPAA (§164.312(d)), PCI DSS v4.0 (Requirements 7 & 8), CMMC 2.0 (IA.2.078, IA.2.079, AC.2.005), NIST 800-53 (IA-2, IA-4, IA-5, AC-2), and SOC 2 (CC6.1–CC6.3).

INTEGRATIONS

Our platform integrates seamlessly with leading tools across your security stack, including identity providers like Microsoft Active Directory, Microsoft Entra ID (Azure AD), Okta, and Ping Identity; SIEM/SOAR platforms such as CrowdStrike LogScale, Microsoft Sentinel, and Splunk; and endpoint solutions like CrowdStrike Falcon and Microsoft Defender.

THREATS WE DETECT & STOP

Our platform detects and stops a wide range of credential-based attacks, including Pass-the-Hash (using stolen NTLM hashes), Kerberoasting (extracting service account credentials), Golden Ticket (forged Kerberos tickets), DCSync (Active Directory replication abuse), and Silver Ticket attacks. We also identify password spraying, credential stuffing, and token theft using advanced techniques such as behavioral analytics, protocol anomaly detection, API and session monitoring, and threat intelligence.

DEPLOYMENT

Metric	Value
Time to Deploy	24-48 hours
AD Integration	Lightweight connector, no agents on DCs
Entra ID Integration	API-based, read-only permissions
Performance Impact	Negligible
First Hygiene Report	Within 72 hours

IDENTITY HYGIENE REPORT

Within 72 hours of deployment, you receive a detailed report covering:

- Account Inventory: Total user and service accounts, identification of stale or inactive accounts, and accounts without MFA.
- Privilege Analysis: Count of Domain Admins, detection of shadow admins, over-privileged service accounts, and risky nested group memberships.
- Configuration Risks: Exposure to Kerberos vulnerabilities, LDAP signing status, password policy weaknesses, and use of legacy protocols.
- Recommendations: Actionable remediation steps, quick wins vs. long-term priorities, and guidance toward a Zero Trust security model.

WHY VIJILAN FOR IDENTITY

Differentiator	Vijilan	Traditional IAM
Focus	Threat Detection	Access Management
AD Attack Detection	Real-time	None
Lateral Movement	Tracked	Invisible
Response	Active (lock, reset)	Manual
Service Accounts	Discovered & monitored	Often unknown
Zero Trust	Enabled	Checkbox

SERVICE TIERS

Feature	Essentials	Premium
AD Attack Detection	✓	✓
Entra ID Protection	✓	✓
Lateral Movement Detection	✓	✓
Identity Hygiene Assessment	Quarterly	Continuous
Risk-Based Alerts	✓	✓
Incident Response	Guided	Full Remediation
Zero Trust Roadmap	-	✓
Dedicated Identity Analyst	-	✓
Executive Reporting	Monthly	Weekly

EXPERIENCE REAL-TIME IDENTITY THREAT DETECTION.

Stay Ahead of Identity-Based Attacks with Real-Time Detection and Response.

vijilan
IT Security. Enabled.

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

AICPA SOC
ISO 27001
A-LIGN