STELLAR CYBER®

DATA SHEET

Identity Threat Detection & Response (ITDR)

Protect the New Perimeter: Detect Identity Threats Before They Become Breaches.

Identity is the new frontline in cybersecurity: According to Verizon's 2024 DBIR, 70% of breaches began with compromised credentials, and SecurityToday.com reports that 22% of confirmed breaches in 2025 were the result of account compromise—making identity-based threats the most prevalent and persistent attack vector facing organizations today.

Key Use Cases Driving the Need for **Identity Threat Detection and Response (ITDR)**

As identity becomes a primary attack surface in today's threat landscape, organizations are increasingly turning to ITDR to detect and mitigate credential-based attacks. Common use cases where ITDR plays a critical role include:

- **Compromised User Accounts:** Detecting unusual access patterns or privilege misuse that may indicate lateral movement or credential abuse.
- **Account Takeover via Impossible Travel:** Identifying login anomalies, such as geographically impossible access attempts, that signal potential account compromise.
- **Insider Data Exfiltration:** Monitoring privileged user behavior to flag large or unusual data transfers that may suggest malicious insider activity.

Unify, Detect, & Remediate Identity Attacks Across Any Environment

Built into the Stellar Cyber Open and Unified SecOps platform—no agents, no silos, no extra charge.

Identity Is the #1 Attack Vector. We Make It the Center of Detection and Response.

Stellar Cyber brings identity security into sharp focus with ITDR embedded directly into its Open and Unified AI-powered SecOps platform. As attackers exploit credentials to move laterally, escalate privileges, and bypass defenses, your SOC needs full identity visibility—not another standalone tool.

Whether it's Active Directory, Microsoft Entra ID (Azure AD), or Okta, Stellar Cyber unifies identity telemetry with endpoint, network, and cloud signals to detect threats early and respond decisively.

- ✓ **No extra agents**
- ✓ **Deployed in minutes**
- ✓ **Full-stack context, real-time response**

The Identity Security Challenge

Security teams face overwhelming complexity:

- Analysts are forced to swivel between IAM, SIEM, and EDR consoles.
- Credential-based threats like MFA spray, lateral movement, and privilege escalation bypass point solutions.
- Identity attack surfaces continue to grow across SaaS, cloud, and hybrid infrastructure.
- Siloed tools lead to alert fatigue and blind spots.

70% of breaches begin with compromised credentials – Verizon DBIR 2024

22% of confirmed breaches in 2025 started with account compromise – SecurityToday.com

Teams need full identity context, AI-powered detection, and fast response—without adding complexity.

How Stellar Cyber's ITDR Works

Stellar Cyber puts identity at the core of the threat story:

Ingests logs from Active Directory, Entra ID, Okta, LDAP, and more—no agents required.

Uses Multi-Layer AI™ and UEBA to detect behavioral anomalies like impossible logins, privilege abuse, and lateral movement.

Correlates identity events with signals from endpoints, networks, cloud, SaaS, and OT in a unified case timeline.

Launches one-click containment actions like disabling accounts, expiring sessions, and isolating hosts—right from the console.

No extra license. No tool sprawl. Just smarter identity defense that works on day one.

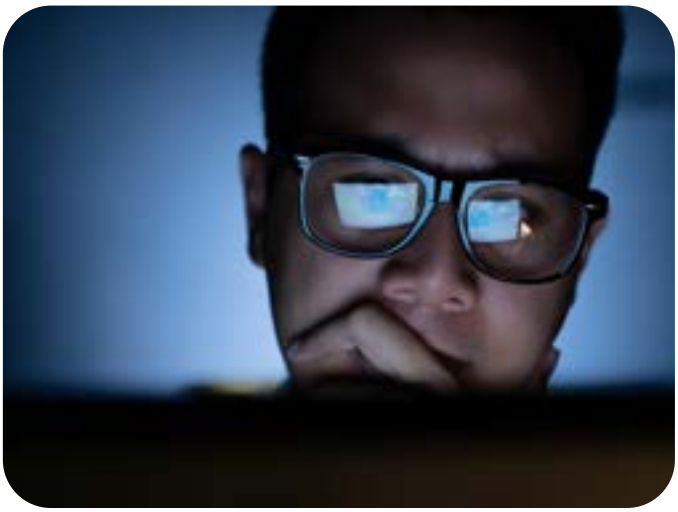
Key ITDR Capabilities

Real-Time Identity Attack Detection

- Active Directory, Entra ID & Okta log collection
- MFA spray, geo-velocity spikes, out-of-scope logins
- Tracks IAM policy changes, GPO edits, and MFA reconfigurations

Unified XDR Context

- Identity data fused with all other telemetry in a single Case
- No switching consoles or copying alerts



Automated Response & Remediation

- Disable users, expire sessions, isolate endpoints
- Integrate with SOAR, ITSM, and firewall tools
- Open API and low-code playbooks

Lateral Movement Containment

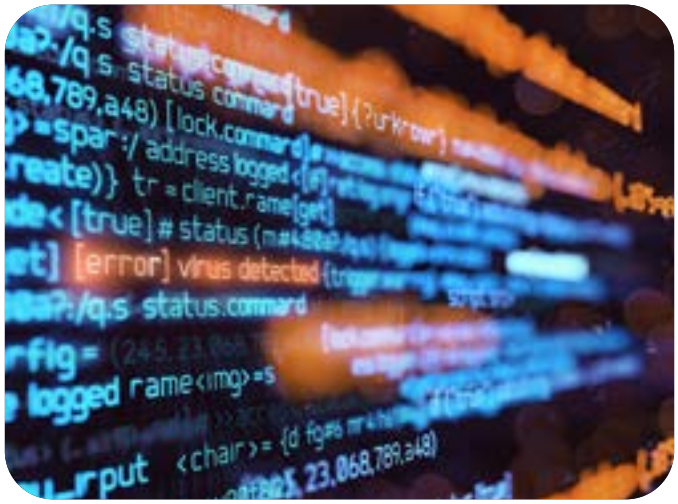
- Detects pass-the-hash and golden-ticket attacks
- Locks compromised accounts and enforces segmentation

Identity Threat Surface Monitoring

- Scores every user and service account
- Flags stale accounts, risky permissions, and dormant identities
- Feeds posture gaps into live detection

Threat Intelligence Enrichment

- STIX/TAXII, MISP, and commercial feeds enrich user and machine IOCs
- Correlates risk across identity, network, and cloud



MSSP-Ready

- True multi-tenancy with tenant-level dashboards, RBAC, and onboarding
- Cross-tenant intel sharing and SLA support

Business Benefits

- **Stop Credential-Based Attacks Fast**
  Shrink attacker dwell time with early detection and automated containment.
- **No Extra Tools or Costs**
  ITDR is built into Stellar Cyber's Open XDR—no additional modules or licensing.

  Faster Compliance & Audit Readiness
  PCI DSS, HIPAA, SOC 2, ISO 27001—mapped right out of the box.
- **Accelerated Investigations**
  Unified, story-driven timeline cuts MTTR by correlating identity, endpoint, and network.
- **Day-One Value**
  Deploys in under an hour. Delivers high-fidelity identity findings within 24 hours.
- **Vendor-Agnostic and Future-Proof**
  Works with Microsoft, Okta, CrowdStrike, Zscaler, and more—no rip-and-replace.

See Identity Attacks Coming. Know How to Defend. Act Decisively.

Start your journey to a leaner, smarter, identity-aware SOC with Stellar Cyber ITDR.

Request a Demo or see the platform in action today.

By shining a bright light on the darkest corners of security operations, Stellar Cyber empowers organizations to see incoming attacks, know how to fight them, and act decisively – protecting what matters most. Stellar Cyber's award-winning open security operations platform includes NG SIEM, NDR, Open XDR, and Multi-Layer AI™ under one license. With almost 1/3 of the top 250 MSSPs and over 14,000 customers worldwide, Stellar Cyber is one of the most trusted leaders in security operations. Learn more at https://stellarcyber.ai/.