STELLAR CYBER®

Solution Brief - Identity Threat Detection & Response

Identity Has Changed. Your Tools Need to Work Together.

Connect the tools you already trust.
Reveal the attack between them.

Strong Tools. Separate Signals.

Your identity, access, application and vulnerability tools already do important work.
The next question is: **What do their signals reveal together?**

IAM, MFA, privilege management and identity hygiene remain essential. So do your access controls, application defenses and vulnerability scanners. But an attacker using valid credentials can leave clues across these systems without any one signal revealing the broader attack.

AI agents, bots and service accounts add identities to monitor, making connected evidence essential.

The SecOps Question is Changing

From “What did one tool detect?” to “What do our tools reveal together?”

ITDR Brings Your Existing Tools Together

Stellar Cyber Identity Threat Detection and Response (ITDR) connects identity activity with evidence from your existing secure access service edge (SASE), security service edge (SSE), vulnerability, web application firewall (WAF) and endpoint tools: SIEM correlates broadly; ITDR adds identity-specific context.

- **SASE/SSE:** Combine Zscaler web/firewall logs, Cato Networks events or Netskope activity with Entra ID or Okta sign-ins and endpoint evidence to investigate what followed apparently legitimate access.
- **Vulnerability:** Add Tenable, Qualys or Rapid7 findings to determine whether assets linked to suspicious identity activity have known vulnerabilities and deserve higher priority.
- **WAF:** Connect Barracuda WAF, Cloudflare or AWS WAF events with identity, application and endpoint evidence to investigate whether an exploit attempt became a broader compromise.
- **Endpoint and network:** Correlate CrowdStrike or Microsoft Defender for Endpoint alerts with DNS, firewall and network detections to follow possible lateral movement or data exfiltration.

The goal is not more identity alerts.

It is to reveal attack patterns that signals viewed separately can miss.

Stellar Cyber Makes Identity Part of the Attack Story

Stellar Cyber brings ITDR directly into the SecOps Platform, not another silo. **Multi-Layer AI** connects related detections into cases; identity, access, application, endpoint, network and vulnerability context

Connected Signals	Full Attack-Chain Context	Exposure-Aware Prioritization	Coordinated Response
Identity + SASE/SSE	**Application + network**	**Vulnerable assets**	**Supported actions**

Stellar Cyber Case Analysis connects identities with related hosts, processes, services and URLs. Analysts investigate the attack instead of reconstructing it across consoles.

From Connected Signals to Confident Action

Consider a possible attack: Barracuda WAF records an exploit attempt against a server Qualys identifies as vulnerable. Microsoft Defender for Endpoint flags suspicious server activity; Entra ID and Cato events help trace related account use. Connected evidence helps analysts investigate whether the attempt became a compromise and spread. XDR can correlate telemetry; here, identity is a first-class signal.

Detect • Investigate and Triage • Respond and Contain

Stellar Cyber brings related evidence into the investigation so analysts can validate the threat and act through supported integrations. With Microsoft Entra ID, actions include disabling users and revoking sign-in sessions. Netskope response templates support user quarantine and destination blocking. Available actions depend on product, version, permissions and configuration.

Better Context. Better Analyst Outcomes.

Connecting tools should reduce analyst work, not add another queue. Stellar Cyber reports **2–4 hours of** human triage per alert versus **1 minute 15 seconds** with Agentic Auto Triage. At Stellar Cyber, ITDR, SIEM, NDR and UEBA share one workflow.

Platform-wide results show the potential analyst benefit; these are not ITDR-specific measurements:

99.7%
AI-human verdict agreement

19 min
Returned per analyst hour

1 min 15 sec
Agentic triage per alert vs. 2–4 hours for a human

Customer trials spanning 124 trial-days and 138,475 real security alerts reported 99.7% agreement between Agentic Auto Triage and human analyst verdicts. Automation returned approximately 19 minutes per analyst hour; 64% of adjudicated alerts were closed as false positives.

For a lean enterprise SOC, the outcome is less time reconciling separate alerts and more time investigating meaningful risk, without simply adding headcount.

Identity is part of that operating model, not another console. Bring access, identity, WAF, endpoint, network and vulnerability evidence into one detection, investigation and response workflow.

Start With Your Tools. Build for What Comes Next.

Today, Stellar Cyber ITDR connects human identity activity with the wider security environment. Your existing tools keep doing their jobs; the SOC gains the context to investigate what happens between them.

As human and machine identities increasingly work side by side, extend this approach through supported telemetry. Connect identity, activity and exposure before deciding how to respond.

Keep Your Tools. Connect Their Signals. Act On the Attack.

Stellar Cyber connects identity to the full attack story so your SOC can see what matters and act faster. Start with the SASE/SSE, identity, WAF, endpoint and vulnerability tools you already use.

* Triage times are Stellar Cyber-reported per-alert figures. Agreement and analyst-capacity metrics reflect Agentic Auto Triage customer trials. Results are platform-wide, not ITDR-specific performance measurements.