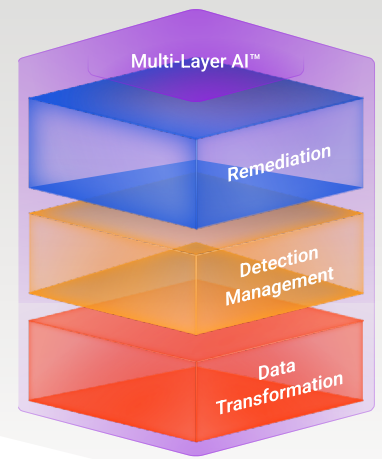


Identity Threat Detection and Response (ITDR)



Connect identity activity to the full attack chain - investigate faster and move to containment from the same workflow.

Stellar Cyber turns identity activity into a complete attack story by correlating it with endpoint, network, cloud, SaaS, OT, and security telemetry. The goal is not to replace IAM, MFA, PAM, or identity governance, but to connect those controls to detection, investigation, and response.

Why this matters

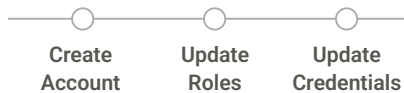
A suspicious login is only the starting point. The decisive question is what the identity does next - whether it moves laterally, changes privileges, touches sensitive assets, or becomes part of a larger attack.

Full Attack-Chain Context for Identity Threats

IAM

Identity and Access Management

Who gets an account, and what it may do.

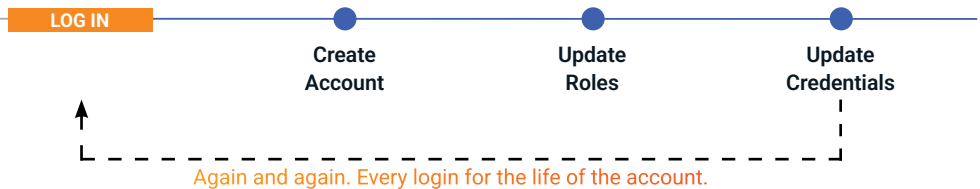


IAM decides who should get access. It cannot tell you when that access is being used by someone else.

ITDR

Identity Threat and Response

What that account actively does once it is in.



How Stellar Cyber Detects It

Detection Rules

Known attack techniques, mapped to MITRE ATTACK.

Machine Learning (UEBA)

A per-user baseline, so "not like itself" becomes measurable

Your Identity Vendors

Vendors identity alerts, correlated with ours.

**"Authentication proves someone had the right credentials.
It does not prove the right person was using them."**

1. Connect the Identity Signal

Ingest identity telemetry from Active Directory, Microsoft Entra ID, Okta, LDAP, and other supported sources - then correlate it with endpoint, network, cloud, SaaS, OT, and security activity inside one case.

2. Detect Valid-Account Abuse

Use UEBA to surface impossible travel, MFA spraying, brute-force attempts, unusual access, privilege misuse, out-of-scope logins, and abnormal data movement.

3. Follow What Happens Next

Connect suspicious identity activity to pass-the-hash, golden-ticket activity, privilege escalation, unusual internal movement, and subsequent lateral movement.

4. Keep the Evidence Together

Show the user, device, network activity, privilege changes, and resulting behavior in one investigation instead of forcing analysts to manually stitch together separate alerts.

From Identity Detection to Containment

Stellar Cyber keeps detection, investigation, triage, and response connected so analysts can move from suspicious behavior to action without another point product or investigation console.

Detect in Context

- Correlate identity events with endpoint, network, cloud, SaaS, OT, and security telemetry.
- Use UEBA to prioritize unusual identity behavior and identity-linked risk.
- Evaluate what an identity does after authentication - not only whether authentication succeeded.

Investigate and Triage

- Place identity alerts in case timelines with supporting evidence.
- Follow the user, device, network activity, privilege changes, and lateral movement together.
- Use automated triage to reduce manual correlation and focus analysts on explainable cases.

Respond and Contain

- Disable compromised users and expire active sessions through supported integrations.
- Isolate affected endpoints.
- Trigger SOAR, ITSM, firewall, and security-tool workflows through low-code or automated playbooks.

Built for the Team You Already Have

- Works with Microsoft, Okta, Google, EDR, firewall, cloud, network, and other security systems
- Supports hybrid identity environments and agentless identity-log ingestion
- Brings identity into the investigation console analysts already use

Built for Teams That Need to Move Faster

- Multi-tenant architecture and role-based governance help keep security data controlled and separated as AI use expands
- Identity-to-network correlation extends visibility beyond endpoint alerts
- Automated triage and response workflows help analysts move faster from suspicious behavior to containment

THE OUTCOME

Turn identity signals into a complete attack story - then move from investigation to containment in the same workflow.