SOLUTION BRIEF

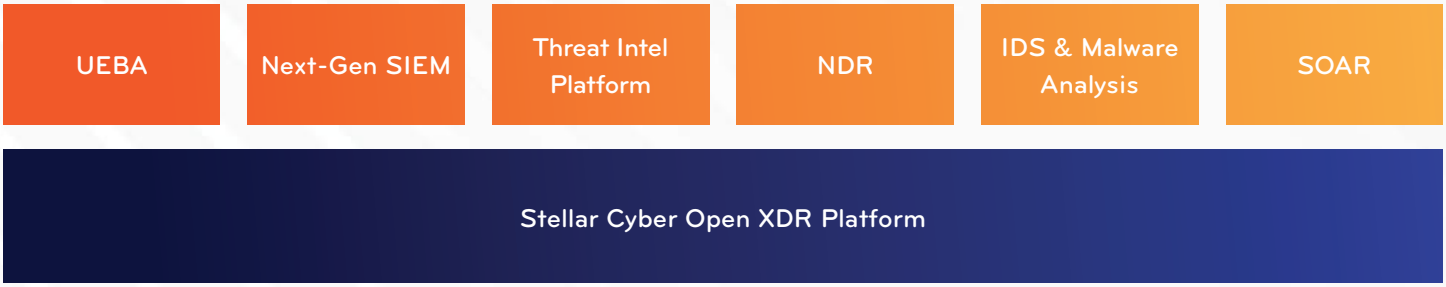
Stellar Cyber for OT Environments

Protect OT and IT Environments with a Single Platform

STELLAR CYBER®

Defending your IT environment from a significant breach is the de facto objective for all security teams, regardless of industry. However, security teams for organizations in specific sectors, such as manufacturing and energy, must go above and beyond this objective and protect an Operational Technology (OT) environment. Typically, these security teams must manage two distinct security stacks to protect these different environments, which increases the complexity and cost of delivering consistent security outcomes that reduce risk. With Stellar Cyber, you can get a single platform and license to simultaneously protect your OT and IT environments.

The Stellar Cyber Open XDR Platform is a threat detection and response platform that works seamlessly with all your existing security tools, natively creating visibility and real-time threat detections in your hard-to-reach OT environments.



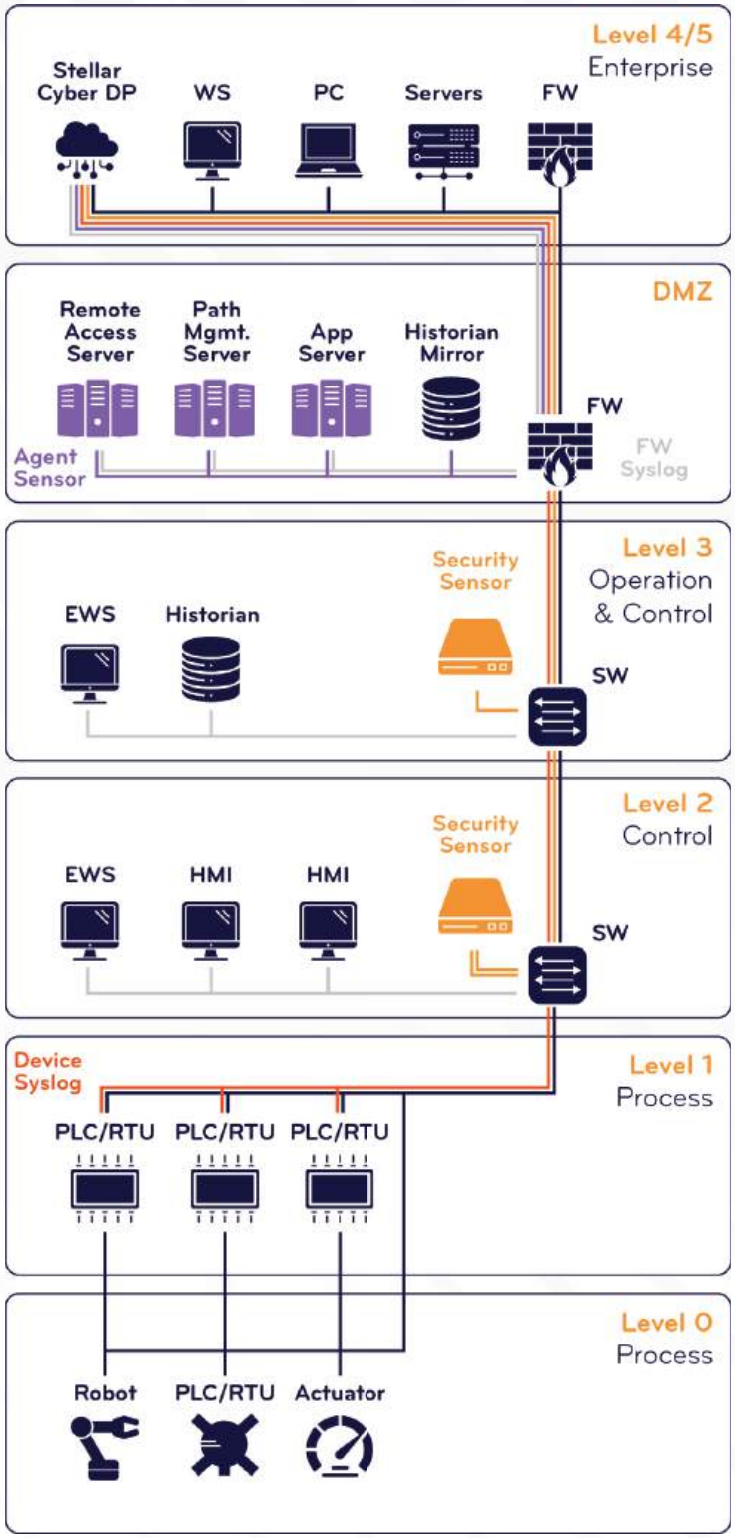
> *Using Stellar Cyber to secure your IT and OT environments means fewer vendors, freeing up your security budget for other uses. With all data and security operations consolidated into a single platform, security analysts' productivity will increase from day one.*

Attack Surface Areas Covered by Stellar Cyber

Attack Surface Area	Purdue Level	Category	Stellar Cyber Components Deployed	Detection Techniques Employed
SCADA Networks	0, 1, 2, 3	OT	Passive use of Stellar Cyber Security Sensors, Integration with any existing OT telemetry source	• DPI Engine understands 50+ SCADA protocols • NDR identifies anomalous communication paths • Custom security rules to detect non-standard protocol use or non-standard communication paths • IDS detects active exploits • Malware Sandbox detects the presence of malware on the network • OT asset visibility (MES, HMI, PLC, RTU, etc.) via asset discovery • Active Directory connector for dedicated OT domains
SCADA / IT DMZ	3, 5	OT / IT	Stellar Cyber Server Sensors	• Streamline collection of security and audit logs from Windows and Linux servers acting as the DMZ • Collect telemetry from firewalls and other network DMZ devices • Hundreds of out-of-the-box detections, Machine Learning and rule-based, detecting malicious files, lateral movement
Enterprise IT Networks (Identity, Cloud, Endpoints, Email)	4, 5	IT	Stellar Cyber Security Sensors, Stellar Cyber Server Sensors, 3rd party integrations	• Generate telemetry (network flow, DPI), collect telemetry (log forwarding, audit logs), and edge detections (IDS, Malware Sandbox) via Stellar Cyber Sensors • Hundreds of out-of-the-box detections, Machine Learning and rule-based, detecting malicious files, lateral movement, anomalous access, and more
All	1, 2, 3, 4, 5	OT / IT	Incident Correlation	• Correlation of detections, regardless of their attack surface source - OT or IT - into a single Incident for efficient, comprehensive threat detection

Deployment Model

Stellar Cyber's Sensors and 3rd Party Integrations are deployed throughout an organization to achieve complete coverage across all OT and IT environments.



Stellar Cyber Open XDR Capabilities

- **User and Entity Behavior Analysis (UEBA):** Automatically identifies anomalous and suspicious behaviors to eliminate potential security threats other security controls miss.
- **Next-Generation SIEM (Next-Gen SIEM):** Collect and automatically normalize log data from any data source to optimize search and threat-hunting functions, making data audit-ready for compliance purposes.
- **Threat Intel Platform (TIP):** Third-party threat intel sources can easily be integrated into the platform and used to enrich any alert to provide appropriate context.
- **Network Detection and Response (NDR):** Combines raw packet collection with NGFW, logs, Netflow, and IPFix from physical or virtual switches, containers, servers, and public clouds to identify network threats.
- **IDS & Malware Analysis:** Suspicious files detonate automatically and safely to determine if they have malicious intent.
- **Security Orchestration and Response (SOAR):** Respond to cyber threats using pre-defined playbooks, ensuring consistent security outcomes.

Enablement Included

- **For MSSPs:** We train your SOC team to use the platform and your sales team to sell the platform effectively.
- **For Enterprises:** We train your administrators and analysts to use the platform as effectively as possible.

Stellar Cyber Open XDR platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments. With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering a 20X improvement in MTTD and an 8X improvement in MTTR. The company is based in Silicon Valley. For more information, contact www.stellarcyber.ai.