

Stellar Cyber MSP to MSSP Fast Track Program

Working with Stellar Cyber and our versatile MSSP partners can put you on the fast track to delivering best-in-class security services.

The Customer Security Question

Managed Service Providers (MSPs) customers understand that securing their environments is paramount. To that end, they seek partners that can handle their routine IT management and deliver the security services their internal teams cannot. In the past, when customers posed this security question to their MSPs, most did not have a good answer.

That all changed with the introduction of the Stellar Cyber Open XDR Platform adopted by some of the world's most profitable Managed Security Service Providers (MSSPs). With the Open XDR Platform, MSSPs can deliver a wide range of security services from a single solution without adding expensive security analyst resources or increasing their capital expenditures. With Stellar Cyber, MSSPs can now offer their security services to end customers and MSPs alike. With the Stellar Cyber MSP to MSSP Fast Track Program, you can answer "Yes" to your customer's security question today.

How it Works

If you are like most MSPs, you have limited security expertise in-house due to the nature of the services you deliver. Given this reality, you are unlikely to deploy, manage, and use the Open XDR Platform with your existing team. In this scenario, Stellar Cyber recommends you partner with a particular class of MSSP that focuses on providing security services through an MSP. These MSSPs, known as Master MSSPs, do not sell their services directly

to end customers. Instead, they exclusively work with MSPs like you, "white-labeling" their security services, enabling you to position these security services as your own.

Daily, the Master MSSPs security operations team investigates threats surfaced by the Stellar Cyber Open XDR Platform and, if necessary, determines the response actions required to mitigate the risk associated with the identified threat. The MSSP team then sends you the response actions for your delivery team to implement or take the actions themselves. The choice is yours.

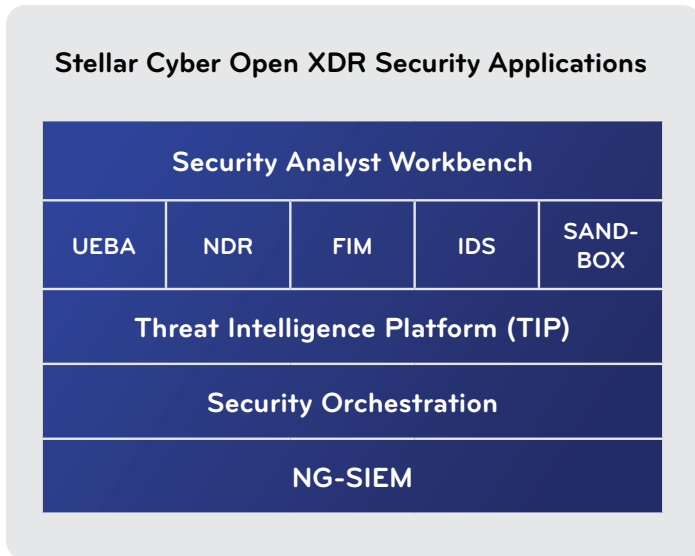
Benefits


- Introduce security services to your customers today.
- No need to add security experts to your internal team.
- There is no need to invest millions of dollars in the required HW/SW to build your SOC.
- Learn how an MSSP delivers security services so that if you want to provide the services yourself in the future, you will have a headstart.


The Stellar Cyber Open XDR Platform


The Stellar Cyber Open XDR platform delivers many core security technologies that MSP customers need to secure their environment. The Open XDR platform automatically collects and analyzes data from any security, IT, and productivity tool to identify potential threats in real-time.


Unlike “closed” XDR solutions that are extensions of a vendor’s endpoint detection and response (EDR) product and only work with the vendor’s specific EDR product, Stellar Cyber’s “Bring your Own EDR” approach works with any EDR product, enabling security service delivery to the broadest range of end customers possible. The platform includes all the security applications below under an all-in single license, eliminating surprise fees and upcharges typical of other security platforms.





Security Analyst Workbench:
 The analyst workbench is an intuitive user interface where all activities occur. Analysts can dive into the details of any case from the workbench, perform fast threat-hunting, initiate response actions, and more.


User and Entity Behavior Analytics (UEBA):
 Baselines users and entity behaviors, automatically identifying behaviors outside the norms as potential security risks.


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 IT and OT network threats.


File Integrity Monitoring (FIM):
 Monitors critical files you tag across Microsoft Windows and Linux environments and generates alerts when unauthorized changes are detected.

Intrusion Detection System (IDS):
 Monitors network traffic for suspicious activity based on known attack signatures.

Sandbox:
 Suspicious files detonate automatically and safely to determine if they have malicious intent.

Threat Intelligence Platform (TIP):
 Data from third-party threat intelligence sources are automatically ingested and associated with related alerts and suspicious activities to give security analysts the context they need to understand the impact of threats.

Security Orchestration:
 Respond to cyber threats using pre-defined playbooks, ensuring consistent security outcomes.

Next-Generation SIEM (Next-Gen SIEM):
 Collects and automatically normalizes data from any source to optimize search and threat-hunting functions, with the added benefit of making data audit-ready for compliance purposes.

Say “Yes” Today

Each day you answer “No” to your customer’s security question brings them one day closer to finding an MSP that can say “Yes”. The Stellar Cyber MSP to MSSP Fast Track Program mitigates the threat of customer attrition, making it easy to maintain your existing customers and add new ones. Visit stellarcyber.ai and set up an introductory meeting with one of our MSP to MSSP consultants to begin your journey today.