On The Radar: Stellar Cyber offers XDR with built-in traffic analysis, SIEM, and automated response

Integration with SOAR platforms provides more advanced features

Publication Date: 20 Mar 2020 | Product code: INT005-000099

Rik Turner

Summary

Catalyst

Stellar Cyber develops technology for detecting and responding to threats across multiple domains of enterprise infrastructure such as endpoint, network, and cloud. Omdia refers to this type of technology as XDR, with component parts for endpoint (EDR) and network (NDR, which is also referred to as network traffic analysis, or NTA), though detection and response for cloud is not currently referred to as CDR.

Stellar Cyber calls its Starlight product an “Open-XDR” platform to highlight its ability to ingest data from any source within a corporate infrastructure and take remedial action via any enforcement point.

Key messages

- Stellar Cyber’s Starlight platform collects data from multiple on-premises and cloud assets, enriches it with its own threat intel, then puts it through its detection mechanisms.
- The inclusion of deception technology and NTA/NDR in the platform is a clear differentiator. Built-in user and entity behavior analysis (UEBA) gives broader insight into what it observes in a customer’s environment.
- Stellar Cyber’s primary focus is on the enterprise (1,000–20,000 employees), with a channel play with managed services providers (MSPs) for smaller organizations, for which reason it has security incident and event management (SIEM) and some automated response capabilities built in.
- It also partners with vendors of firewalls (Check Point), vulnerability management (Tenable), and automated response for more advanced orchestration functionality in adjacent areas.

Omdia view

XDR is an expanding segment, and the openness of Stellar Cyber’s platform bodes well for its market potential. The breadth of its offering, including UEBA, NTA, SIEM, and automated response, makes it particularly relevant for XDR projects.

Recommendations for enterprises

Why put Stellar Cyber on your radar?

Stellar Cyber has brought together a comprehensive set of capabilities in its XDR platform that its competitors either do not yet have or have had to acquire to add in. Its combination of NTA, SIEM, and automated response is not common among SIEM or XDR players: it is particularly useful in helping to understand attacker behavior and can thus turbocharge the threat investigation and threat hunting that the Starlight platform enables.

Starlight is currently available for deployment on premises, in public clouds, and with managed services environments. It is microservices based, with its data processor able to sit on containers,

virtual machines (VMs), or bare metal, and a future software-as-a-service (SaaS) version will further extend Stellar Cyber's market reach.

Highlights

Omdia has in the past classified Stellar Cyber as a challenger in the SIEM market, but the vendor's own positioning puts it into the more dynamic segment of XDR. Its Open-XDR branding goes further, highlighting Starlight's ability to draw on data from any source and to enforce policy and remediation through any security tool available (firewalls, CASB, DLP, NAC, and so on) from any vendor. The company also includes as core functions within XDR both UEBA and NTA, where it uses machine learning (ML) to model user behaviors or anomalies in the user traffic patterns.

The vendor's reluctance to be considered a SIEM vendor is understandable given the somewhat fusty image such technology has acquired in recent years, not to mention SIEM's association with notions of costliness and complexity. That said, Starlight certainly performs all the necessary SIEM functions, namely

- collection: deploying agent sensors, network sensors, security sensors, and deception sensors across a customer's infrastructure to send logs, packets, and files into Starlight, where they are correlated and enriched with context in a process the company calls Interflow
- detection: running advanced ML algorithms on the improved data set in order to detect higher-fidelity security events
- investigation: leveraging the fact that Interflow fuses contextual data into packet and log records so that security analysts have a single record to scrutinize when trying to prove that a detection is accurate and actionable
- response: delivering a variety of response actions once security events have been detected and found actionable by investigation. The system can generate email or Slack alerts; send PDF reports; submit data to security orchestration, automation, and response (SOAR) tools such as Demisto and Phantom Cyber; or instruct firewalls, either manually or automatically, to take appropriate response actions such as blocking an IP address or redirecting a user to a captive portal for further authentication.

Of course, traditional SIEMs do not extend into response, which is the main reason that the SOAR sector emerged in the first place. It is also why leading SOAR vendors have been acquired: Resilient by IBM (which offers the QRadar SIEM); Phantom by another SIEM major, Splunk; and Demisto by Palo Alto Networks, which does not have a SIEM but which has overt ambitions in security management, expressed in its Cortex XDR offering. Indeed, Omdia would argue that XDR is the future of SIEM, either as its evolution or as its replacement.

UEBA

In this context, it is also worth noting that Starlight has built-in UEBA, in which it uses ML to model the behavior not only of people in an organization but also of assets such as files (where they reside, who normally accesses them, whether they are normally downloaded or copied, etc.).

UEBA was another shortcoming of traditional SIEMs, so much so that SIEM and XDR vendors have acquired companies in this segment:

- Splunk bought Caspida (2015).

- Palo Alto Networks acquired LightCyber and Forcepoint bought RedOwl (2017).
- Fortinet bought enSilo (2019).

Meanwhile, at least two UEBA vendors, namely Exabeam and Securonix, have themselves expanded to compete head-on in the SIEM market.

NTA/NDR

Another differentiator for Starlight is its NTA capabilities. Omdia has tracked this area of technology, which is still largely the preserve of standalone vendors. We see it as a capability that should be integrated into broader security platforms, however, so its inclusion in Stellar Cyber's arsenal is a welcome feature in our estimation.

Background

Stellar Cyber was founded in 2015 as Accaella Technology and was renamed first as Aella Data, subsequently settling on its current name. Its founders are CEO Changming Liu, who had previously founded WLAN vendor Aerohive and took it public in eight years and had been a distinguished engineer at Juniper, and its senior VP of engineering, Aimei Wei, a veteran of companies such as Cisco, Ciena, and Nortel as well as a string of startups.

The company has raised $14.7m in two rounds of venture funding, most recently announcing a Series A round in February 2019 led by Valley Capital Partners and an A+ round in March 2020 led by SIG, taking its total raised so far to $21.8m.

Current position

Machine learning

Stellar Cyber leverages three types of ML:

- supervised ML (where the algorithms are trained by humans before going into production), which it uses to reduce the number of alerts generated by the intrusion detection it applies to incoming data, thus reducing the noise an intrusion detection system (IDS) normally provokes
- unsupervised ML (where the algorithms learn for themselves in the production environment), which it uses to model what constitutes normal traffic so as to alert on anomalies
- deep learning (which leverages neural networks), used to detect some specific cases such as DNS tunneling and domain generation algorithms (DGAs), which are embedded in some types of malware to large quantities of domain names to serve as rendezvous points for command-and-control servers.

Built-in automated response

While Stellar Cyber positions itself in XDR, it acknowledges that its automatic response capabilities can be seen as SOAR, even though it partners with dedicated SOAR vendors for more advanced functions. In terms of its own automated response capabilities, Stellar Cyber has partnerships with Check Point (in the firewall market) and Tenable (in vulnerability management), writing specific enforcement functionality such as shutting off a particular attacking IP address or issuing a ServiceNow ticket.

Meanwhile, its SOAR integrations are with specialists Demisto, Phantom, and Swimlane. While Stellar Cyber's RESTful API approach enables many SOAR vendors to work with Starlight, with Demisto and Phantom it has gone further, enabling its playbooks to be available on their platforms.

SaaS is still to come

The vendor currently does not offer its technology in SaaS mode. That said, it is already working on enabling the data lake into which it stores all the information it collects to reside in a public or private cloud or within MSPs' infrastructures as well as on customers' premises. It has several MSPs offering managed detection and response (MDR) services and customers who use the platform as SOC-as-a-service by leveraging its multitenancy and role-based access control (RBAC). The development of a SaaS offering should not prove too challenging, since architecturally the technology is microservices based and already supports two levels of multitenancy, that is, for both the end customers and service provider partners.

Data sheet

Key facts

Table 1: Data sheet: Stellar Cyber

Product name	Starlight Open-XDR Security Platform	**Product classification**	XDR platform
Version number	Current release is 3.5.1	**Release date**	4Q18
Industries covered	All	**Geographies covered**	Global
Relevant company sizes	Enterprise	**Licensing options**	One-, three-, and five-year subscriptions
URL	stellarcyber.ai	**Routes to market**	Resellers, distributors, MSSPs
Company headquarters	Santa Clara, CA, US	**Number of employees**	<100

Source: Omdia

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

Beyond SIEM: Where Security Management Needs to Go Next, INT005-000034 (September 2019)

Google Cloud Security can go beyond GCP with Anthos, INT005-000074 (January 2020)

Microsoft's Expanded Horizons in Security, INT003-000345 (April 2019)

Ovum Market Radar: Deception Technology, INT003-000317 (January 2019)

Ovum Market Radar: Threat Intelligence Platforms, INT003-000291 (December 2018)

Platform Plays and the Future of Security Management, INT005-000023 (August 2019)

"Is SIEM dead or just on life support?" INT003-000135 (April 2018)

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@omdia.com

Omdia Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com