Publication date:
20 May 2021
Author:
Rik Turner, Principal Analyst, Emerging Technologies

Splunk buys TruSTAR to beef up its threat intelligence management capabilities

Brought to you by Informa Tech

Table of Contents :

Omdia view

Summary

Data analytics heavyweight Splunk has announced the acquisition of TruSTAR, a vendor that enables organizations to manage both their internal and their external threat intelligence. The move underscores Splunk's growing presence in the world of SecOps and provides a further argument for customers to use its technology to organize and analyze their security information then move to remedial actions based on the insights they glean from that process.

Splunk was led into security by its customers

Splunk's raison d'être since its foundation in 2003 has been to enable enterprises to search, monitor, and analyze machine-generated big data via a web-style interface, making IT information management a logical first sector for its application.

It realized within a few years, however, that security had become a primary use case for its technology, and it has been in the market with a security-specific product, Splunk Enterprise Security, since 2014. That platform competes in the security incident and event management (SIEM) market, where it has steadily grown its presence to overshadow some of the erstwhile market leaders such as ArcSight (now part of Micro Focus).

Splunk has also invested to keep the product relevant in the changing SIEM market in recent years, adding a user and entity behavioral analysis (UEBA) capability via the acquisition of Caspida in 2015 and security orchestration, automation, and response (SOAR) by buying Phantom Cyber in 2018. And while it started life in the world of on-premises software, Splunk has offered cloud-based versions of its technology, delivered in software-as-a-service (SaaS) mode, for the best part of a decade.

The acquisition of TruSTAR advances Splunk's effort to build out its data management capabilities, in this case adding the ability to normalize and transform threat data from a wide range of sources, both internal and external.

TruSTAR is like a threat intelligence platform, but from different beginnings

If that sounds a bit like a threat intelligence platform (TIP), that's because there are definite overlaps between what TruSTAR offers and what the TIPs do. However, TruSTAR itself shuns the TIP moniker, not least because the original definition of a TIP was not what it came into existence to do.

TIPs arose around the middle of the last decade, specifically to address organizations' need to manage the threat data feeds, which were by then mushrooming. This proliferation can be explained as a response to the decreasing efficiency of signature-based approaches to threat protection, which had been on the wane since the mid-2000s. Alternatively, enterprises had begun amassing threat data to curate their own set of applicable indicators of compromise (IoCs) for threat detection, and multiple suppliers of threat data feeds sprang up to meet that need. Larger organizations then began to take up a multitude of feeds in the hope of widening their view on the threat landscape, but that raised a need for deduplication (to avoid working on the same threat, expressed differently by different feed providers) and normalization among feeds, so that

all threats would adhere to a common format and thus be capable of being analyzed by a single platform or at least in a uniform fashion.

By contrast, TruSTAR was founded in 2014 specifically to enable organizations and consortiums, such as the multiple Information Sharing and Analysis Centers (ISACs) that had sprung up in verticals such as financial services, retail, and healthcare, to share information among their members. It then pivoted to focus on customers' internal threat data, enabling them to bring in external sources once that was organized.

Threat intel plus response is the direction of the market

TruSTAR is also a cloud-native platform, which should bolster Splunk's credentials in the SaaS world, particularly against next-generation SIEMs (NG-SIEM), born-in-the-cloud competitors that have emerged in recent years from both industry heavy hitters such as Microsoft (the Azure Sentinel offering) and Google (Chronicle) and startups such as Devo and Securonix.

Omdia has closely observed the TIP sector over the years, looking in particular at the four leading players (Anomali, EclecticIQ, ThreatConnect, and ThreatQuotient). It is notable that, despite their best efforts, the TIP market as a whole has struggled to reach $200m in revenue, which can partly be attributed to the fact that TIPs are very much a high-end enterprise activity, requiring a security operations center (SOC) team with the knowledge to interpret threat data and make use of it by translating the resulting conclusions into actions.

In addition, when they first came to market, none of the TIPs actually facilitated that move from analysis into action. However, all the leading TIP players have sought to remedy that shortcoming in recent years:

- ThreatConnect now offers a SOAR module to work alongside its TIP.
- EclecticIQ partnered with a small endpoint detection and response (EDR) vendor called PolyLogyx to move toward an XDR offering.
- ThreatQuotient now enables both SOAR and XDR platforms from its platform.
- Even Anomali, the most diehard proponent of a pure analytics play, is now white-labeled by SOAR vendor Siemplify.

In this context, TruSTAR's absorption into Splunk not only makes it part of a much larger player but also enables integration of its platform with the Phantom SOAR technology Splunk has owned for the last three years.

Appendix

Further reading

Splunk .conf20 recap: SIEM vendor advances unified SecOps platform, offers friendlier pricing (November 2020)

Beyond SIEM: Where Security Management Needs to Go Next (September 2019)

Ovum Market Radar: Threat Intelligence Platforms (December 2018)

Author

Rik Turner, Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@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