IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The Integration Imperative for XDR

Marc Solomon

Marc Solomon
Chief Marketing Officer
ThreatQuotient

Biography

Marc Solomon is the Chief Marketing Officer at ThreatQuotient (https://www.threatq.com) where he leads all aspects of the company's global marketing strategies, initiatives and programs. He has a strong track record driving growth and building teams for fast growing security companies, resulting in several successful liquidity events.

Prior to ThreatQuotient he served as Vice President of Security Marketing for Cisco Systems' following its $2.7 billion acquisition of Sourcefire, Inc. While at Sourcefire, Marc served as Chief Marketing Officer and Senior Vice President of Products.

Marc has also held leadership positions at Fiberlink MaaS360 (acquired by IBM), McAfee (acquired by Intel), Everdream (acquired by Dell), Deloitte Consulting and HP. Marc also serves as an Advisor to a number of technology companies, including Valtix.

Marc blogs at https://www.threatq.com/category/blog-posts/

Keywords Extended Detection and Response (XDR), Cyber security, Threat detection, Threat response, Cyber threats, Data, cloud-based architecture
Paper type Opinion

Abstract

Large security vendors with Extended Detection and Response (XDR) offerings position their solution as integrating their own set of products which may include a couple of third-party products already part of their suite and providing a central screen or single pane of glass to be able to see all the data. However, as the author of this article explains the integration imperative for XDR raises important questions.

Introduction

The largest cybersecurity companies in the world, industry analysts and other security experts are talking about the emergence of Extended Detection and Response (XDR) solutions, which Gartner defines[1] as solutions that "automatically collect and correlate data from multiple security products to improve threat detection and provide an incident response capability."

Organizations often protect themselves using many different technologies, including firewalls, IPS/IDS, routers, web and email security, and endpoint detection and response solutions. They also have SIEMs and other tools that house internal threat and event data – ticketing systems, log management repositories, case management systems. They may rely on one or two "large vendors" to handle the bulk of their security tasks, but typically they use at least a few best-of-breed vendors for controls the larger vendors do not have or do not excel in. Many studies, going back years, find that some Global 2000 enterprises have as many as 80 different security vendors in their environment. This happens naturally over time with different teams, budgets and departments making independent decisions.

Vendors also must be able to accommodate the reality that not every organization will have all their tools from a single provider out of the gate, and the appetite to rip and replace is low. Not to mention the fact that new vendors and solutions will continue to emerge given the ongoing innovation required to keep up with new use cases, threats and threat vectors. However, whichever path to XDR is selected, integration with existing tools in the security infrastructure is essential for XDR solutions to merit and capitalize on all the attention.

What data are you looking at in that central console?

Data can come from any of the solutions that are part of the XDR offering at any time and, given alert overload, we're probably talking about massive amounts of data. Without context from external intelligence sources, it's impossible to determine relevance and prioritization. This is because the data isn't curated for the specific customer environment it could be noise, which lowers users' confidence in the data and their ability to make the right decisions.

What happens with organizations that aren't starting with a clean slate and have a variety of best-of-breed solutions across departments and teams?

To deal with this, many of these larger vendors are now creating marketplaces, hoping that smaller vendors will use their APIs to build integrations with them. This is starting to happen. But if you have been in the software industry for a while, you understand that this takes a lot of time and isn't easy to maintain. If a smaller vendor has products that actually compete with the main vendor, the integration may never happen.

How do you integrate on-premises legacy tools with XDR's cloud-based architecture?

Even if the XDR solution vendor has great APIs that are "easy" to write to, getting data from on-premises, legacy applications to a cloud platform is a considerable undertaking. An XDR implementation can quickly turn into a very large consulting project requiring significant time and budget. Alternatively, some organizations may choose to outsource the entire function to a managed detection and response (MDR) service provider that offers XDR as a service. MDR is a growing category in cybersecurity services and is an offshoot of the traditional Managed Security Service Providers (MSSPs). Unlike MSSPs, MDR companies don't manage traditional security tools and technologies like firewalls but are there to detect, respond and address attacks.

To help XDR solutions deliver on their promise, what is needed is a platform focused on integration, serving as a central repository for data and intelligence from internal and external sources, and as a conduit between existing security technologies and cloud-based XDR offerings. More than a central screen or single pane, the platform delivers a single source of truth for teams and tools, bringing in third-party intelligence to enrich data from internal tools with context and prioritize it for action. This single source of truth can prioritize and filter out noise, share knowledge, serve as organizational memory and become a custom enrichment source for all teams and tools to use to accelerate security operations.

In conclusion

With preprocessed, curated data, teams have high confidence that the data is relevant. Confidence in data leads to confidence in decision making which, in turn, leads to confidence in automating those decisions and actions. This gives a platform that also integrates with third-party security controls, allowing relevant, prioritized threat intelligence to flow through all systems, playbooks and processes. Actions – automated or manual – are based on the right data and can be executed quickly.

Clearly, integration is imperative for XDR – enabling effective detection and efficient response.

Reference

[1] https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/