THREATQUOTIENT™

Enabling
eXtended Detection & Response (XDR)

XDR is a Movement

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 as solutions that "automatically collect and correlate data from multiple security products to improve threat detection and provide an incident response capability." If this were possible today, imagine the gains in Mean Time to Detection (MTTD) and Mean Time to Respond (MTTR) to an attack or active threat in your environment.

I refer to XDR as a movement because it is gaining traction by expanding its approach to achieve its goal. In March, which seems like a lifetime ago, Gartner talked about XDR as a vendor-locked, cloud-based offering. But at the virtual Gartner Security and Risk Management Summit 2020 in September, VP analyst Peter Firstbrook discussed an alternative approach which broadens the category to include a best-of-breed XDR strategy. Further fueling momentum, Gartner called XDR the number one trend CISOs should understand to strengthen security initiatives.

We have the definition of XDR by Gartner above, but what does it really mean from a practical standpoint? Let me start with a simple and important statement:

$$XDR \neq EDR + NDR^{1}$$

Unfortunately, this is how some have viewed the development of XDR – bridging the gap between endpoint and network detection and response. However, XDR has a broader, more complicated reality:

$$XDR = EDR + NDR + CDR^{2} + \text{the dozens of existing security tools}$$

This reality forces the need for a best-of-breed strategy, at a minimum from a transition standpoint, but more likely for an ongoing basis.

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

[1] NDR = Network Detection and Response, as defined by Gartner
[2] CDR = Cloud Detection and Response, as defined by Gartner

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.

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. The reasons are obvious for a best-of-breed approach, but even single-source XDR requires integrations to deliver on the promise. I want to talk about two key types of integrations that are needed:

1. Integration with third-party data and intelligence feeds – companies use an average of five external feeds within their environment[3]. These can include commercial sources, open source, government, industry, existing security vendors – as well as frameworks like MITRE ATT&CK. Having the ability to utilize this data as part of your detection and response strategy is critical. It improves the breadth, speed and relevance of detections, rather than just relying on a vendor's intelligence.
2. Integration with third party systems – this is important for multiple reasons. First, additional telemetry, context and events from internal systems is key to putting the pieces together for detection. This data from internal systems is often overlooked but is one of the best sources of intelligence, and when combined with external data will improve detection. Second, integrating with the internal systems will allow for faster response and the right mix of automation and manual actions. Systems become more effective and people more efficient.

[3] https://searchsecurity.techtarget.com/feature/Threat-intelligence-offers-promise-but-limitations-remain

OK, so now that we have a baseline for XDR, the question becomes "Where do we start?" to realize the benefits. There are several paths, but the most common is starting with a company's EDR implementation and then adding capabilities. Think of it this way:

- EDR: endpoint detection and response from a single vendor, using that vendor's detection content
- EDR +: a vendor's EDR solution plus integration with third-party data and intelligence for faster, more effective detection.
- EDR ++: a vendor's EDR solution plus integration with third-party data and intelligence for faster, more effective detection, plus integration with the other tools in your infrastructure for more efficient response.

To truly become a movement that more organizations can get behind, what's needed is a conduit between an XDR solution and the data sources and security tools it needs to interoperate with. A centralized platform that bridges these gaps can provide the integrations and intelligence for all teams and tools to use which helps with detection, understanding and response and unleashes the full potential for XDR.

The Integration Imperative for XDR

Large security vendors with 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. But that's raises some important questions:

1. *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. 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.

2. 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. And if a smaller vendor has products that actually compete with the main vendor, the integration may never happen.

3. *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 cyber security 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's 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.

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. Because that platform also integrates with third-party security controls, relevant, prioritized threat intelligence can 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.

The ThreatQ Platform: Powering the XDR Movement

To meet the integration imperative for Extended Detection and Response (XDR) companies need a platform that serves as single source of truth for more effective detection, and as a conduit for efficient response. ThreatQ is that platform.

The ThreatQ platform takes a threat-centric approach to security operations because we believe you cannot defend against what you do not understand. We have deep roots in threat intelligence management which positions us perfectly to address the XDR use case of extended detection. What's more, because threat intelligence is the lifeblood of security operations, our customers efficiently and effectively address multiple use cases from within the platform – spear phishing, threat hunting, alert triage, vulnerability management, and the other XDR use case of incident response.

ThreatQ aggregates and normalizes external and internal threat intelligence, augmenting it with internal event data and context. An automated scoring framework filters out noise, prioritizes intelligence based on parameters users set and actions that intelligence either automatically or for human consumption. The platform also serves as organizational memory for learning and improvement. Teams and tools feed data, events and what has been captured, back to the platform. It stores and prioritizes the data collected from all investigations. Correlating detections over time, the platform can help identify a broader campaign versus viewing each incident independently, so that teams can respond more quickly and accurately to an incident.

Because it supports bi-directional integration, the ThreatQ platform sends associated data back to the right tools across the security ecosystem for efficient response. An open, extensible architecture allows for strong integration and interoperability with existing tools – including that one product the XDR vendor may not be familiar with. Standard interfaces are used for ingestion and exporting, and custom connectors can be written and deployed within hours to connect to new data sources and security controls to address emerging threats.

Over the last several months, I've spoken with many vendors of all sizes in the security space as well as customers. One customer told me this week, we want to go with "Company X's" XDR solution moving into 2021, but we need you to integrate with these five third-party products. I think this will be an ongoing problem for every company with an XDR project in 2021 or even 2022. Their main use cases will need additional integrations and I believe doing this through the ThreatQ platform is the way to solve this problem because the integrations are already done. Plus, it can also solve the problem of being an on-site collector for the XDR vendors with cloud-based solutions.

Any XDR solution needs data curation, the ability to work on-premises and the ability to integrate with the actual products that enterprises or MDRs are using. With a platform like ThreatQ, the XDR movement is poised for success. Enterprises will get more out of their existing resources – teams and tools – and XDR will deliver on its promise to enable high-quality detections faster and more efficient response.