LogicHub

Understanding XDR

Kumar Saurabh

XDR is a natural evolution of EDR

EDR vendors are leaning into the fact that most attacks touch more than just the endpoints. Understanding the true scope of an attack requires broad visibility from multiple vectors

When you look at a typical kill chain you might see an attacker start with something like a phishing attack. Once they get an initial foothold on the user's endpoint (something that EDR products can easily detect), they typically try one of many lateral movement techniques to propagate quickly.

The real danger is when they jump onto another box that houses a crown jewel target like a database with all your user credentials before the EDR can stop the attack. Once they've infiltrated that data, they have easy access to valid credentials and are able to initiate new attacks that can evade detection by an EDR.

In order to truly understand this type of attack, you need to quickly pull all the disparate pieces together for analysis to see a complete picture of how they're related.

EDR is a piece of the puzzle, but it does not provide full visibility into the kill chain.

LogicHub

But this is not a new concept

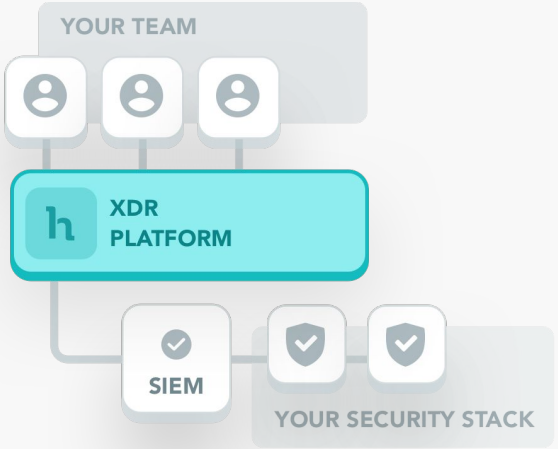
The same realization that you need to pull disparate sources of data together for analysis is what led to the birth of SIEM almost 20 years ago.

But the real question that raises for a buyer is whether or not they need both XDR and SIEM when the visibility problems that they're both designed to solve are 95% similar.

LogicHub

The answer is that from a buyer's perspective the label should not matter. What should matter is that the solution(s) they choose have the detection and response capabilities that solve the problems their security teams face.

If SIEM alone cannot solve them, they need to augment the SIEM. But by just buying a new product isn't a good enough strategy. You have to figure out whether XDR will actually solve the problems that your SIEM does not.



LogicHub

Open vs. Closed

the 2 flavors of XDR

LogicHub

When determining whether or not XDR can help your organization, you need to start by understanding that there are two vendor philosophies of how to deploy XDR.

The closed version focuses primarily on integrating multiple portfolio products from the same vendor, even though many of those products were result of acquisitions. In fact, sometimes the primary XDR platform itself is the result of an acquisition.

Much like SIEMs, open XDR is vendor agnostic. In some ways SIEM vendors are the pure play XDR vendors. They have the advantage of being able to integrate technologies from multiple vendors with ease.*

Open XDRs are also primarily pure play vendors whose **sole** focus is on delivering XDR and not other things like EDR, NDR, Firewalls, Prevention, Identity, Threat Intel, etc.

**This advantage can be neutralized if the portfolio vendors invest heavily in integrating with products from other vendors.*

The challenges in detection and response driving the need for XDR

- Most security teams don’t have access to the skills or personnel necessary to effectively manage the 20+ tools they have in their security stack
- The proverbial “single pane of glass” still very hard and expensive to build, particularly on your own
- There are too many alerts to investigate, and in many cases 95% or more are false positive

LogicHub

- Security teams are bogged down by repetitive and overly manual investigation and triage processes that take too much time to perform in depth, leaving them vulnerable to attacks that get overlooked
- Most security teams struggle with detecting the many threats that hide in the gray area between obviously bad and obviously good activity
- A majority of security analysts spend a significant amount of time on mundane tasks that don’t adequately utilize their training or skills
- Automation platforms are either not powerful enough to execute critical playbooks, or they’re too expensive to purchase and deploy, and fail to deliver a positive ROI

The difference between ~~theory~~ marketing and practice

LogicHub

Vendors claim they have already solved the problem.

Practitioners think otherwise.

Can you tell the difference?

XDR that actually works.

XDR that claims it does

Evaluating XDR vendors

LogicHub

Determine how easily can you build your dream “single pane of glass”

Visibility - How powerful are their Dashboards and Case Management capabilities?

Analytics - How well can they stitch all the data together and get the answers you need?

Automation - Can you easily take relevant actions with the click of a button?

Assess how effectively can they find threats

Accuracy - Absence of evidence is not evidence of absence (Carl Sagan)

Intelligence - Throw a bunch of known attacks mixed in with normal activity - can they detect it?

Autonomy - Don’t tell them what those attacks are. Attackers won’t.

Evaluating XDR vendors

LogicHub

Evaluate and score their alert precision

If they generate 20 alerts, how many of them are actual incidents?

How quickly and effectively can they eliminate false positives?

How easily can security analysts provide that feedback to improve accuracy?

How well does the system learn from the feedback provided by analysts?

Determine if you are getting all the relevant context of an attack in the alerts

Is there any critical data missing from the alert?

How much do you still have to figure out on your own?

How easily can you automate the steps you would take to piece it all together?

Evaluating XDR vendors

LogicHub

Test the decision automation process for the 95% of alerts that are not real incidents

Is the platform's decision automation accuracy better than that of a human analyst?

Does the platform test and validate decision automation accuracy?

Does the system have the ability to learn from security analysts and environmental attack history?

(Don’t Even)

Trust but verify

(All the claims)