VARS

7 SIGNS YOU MIGHT NEED A NEW DETECTION AND RESPONSE SOLUTION

Powered by Cynet

Introduction

In many aspects of life, we tend to get complacent with the status quo. Even when there are better options, it's against human nature to change. The familiar is comfortable. The unknown is, well, unknown.

In the world of threat detection and response, innovation is constant and technology obsolescence happens overnight. It's difficult for practitioners to stay abreast of new developments. Between simply being too busy to stay on top of the continuously evolving market and the constant security vendor hype, many security practitioners keep their heads down and make do with what they have.

To help those of you that have been too busy to stay up to date with the latest security technology developments and are struggling to get by with older technology, we're offering up some signs that may indicate that it's time for a change.

> *"A ship in harbor is safe, but that is not what ships are built for."*
>
> John A. Shedd

1. If you ignore all but the highest risk alerts, you may need a new detection and response solution...

The combination of lean security teams with detection systems that generate massive quantities of alerts means little to no time for proper alert investigation and follow up. Hence, only the highest risk alerts gain attention.

Putting aside the inevitable segment of false positive alerts, many real alerts are being overlooked because they are below the risk threshold that triggers an investigation. The reality is that every alert should be investigated, even if the alert is quickly dismissed as trivial or false. In fact, some severe attacks start out as minor blips on the radar – an abnormal startup process, a file that looks slightly suspicious – before they wreak havoc.

So, what does this mean for your detection and response tools? If your team is ignoring almost every alert it receives, your detection tools are not doing a lot of the work they should be.

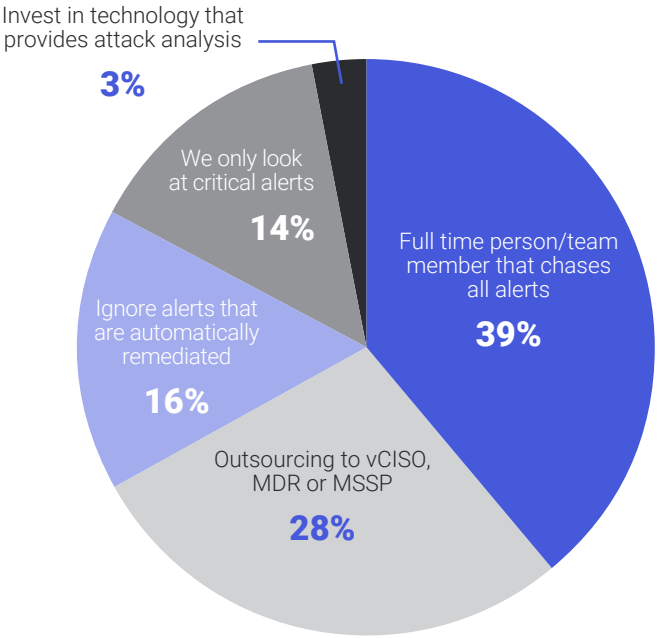
The solution? Find a platform, such as extended detection and response (XDR), that automatically collect and analyze alerts from multiple streams of telemetry so that seemingly benign signals are properly assessed in context and alerts become much more accurate.

2. If you need to use five separate tools to investigate a single threat, you may need a new detection and response solution...

If investigating alerts was quick and simple, we wouldn't need to focus so much on alert accuracy.

The unfortunate reality is that manually investigating alerts requires analysts to access multiple systems to piece together the story behind the alert. This leads to the "multiple panes of glass" dilemma that all but the largest companies with unified SIEM and SOAR tools face. Each alert investigation requires multiple minutes to multiple hours, which adds up with the volume of alerts most companies face today.

A recent survey of 200 CISOs with smaller (five or less) security teams shows that 39% of these companies dedicate a full time analyst to chase down alerts. More alarming is that 14% only look at critical alerts, meaning any alert that may have been miscategorized is ignored. And 16% ignore alerts that have been automatically remediated, although the single remediated threat may be only one component of a larger, ongoing attack.

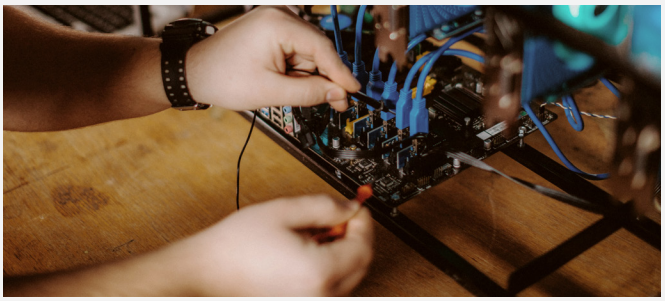


An alternative solution is to consolidate investigation into a single, unified, automated platform. Instead of relying on manually navigating a variety of tools, using an XDR that natively combines threat signals and can automatically launch an investigation to determine the root cause and scope of a detected threat. More importantly, it lets you respond faster and more efficiently to cut off a threat before it becomes a problem.

3. If your EDR requires multiple optional add-ons to work properly, you may need a new detection and response solution...

Many EDR providers list several platform tiers with increasing levels of features and capabilities – for increasing levels of cost. Others provide a core EDR solution, but require add-ons for features such as forensics, threat hunting, automated remediation, and others. By the time you're done configuring what you need, the cost has skyrocketed, and the implementation and operation have become far more difficult.

Adding in services only exacerbates this problem – professional service fees for integration and configuration, MDR services, threat hunting services, health checks, training, the list goes on and on. Many EDR providers are more adept at finding new revenue sources than finding cyberthreats!

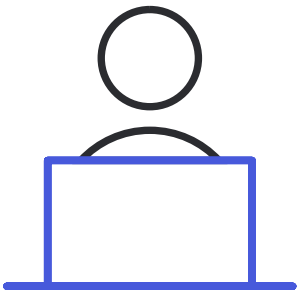


Alternatively, you can find a provider that includes all features and services for a single, transparent price. This way you don't have to decide whether you spend your limited budget on threat hunting services or automated remediation capabilities. Cynet, for example, includes all capabilities, features, and services for one price – full XDR prevention and detection, extended automated response capabilities and a full 24/7 MDR service all included.

4. If only one person on your team knows how to manage your EDR, you may need a new detection and response solution...

Another side effect of a large and complex security stack is a steep learning curve. Most EDRs and other detection software are typically quite complex. Setting them up, calibrating them, tailoring them to an organization, and then maintaining them, requires a significant time investment in training someone to do it.

A study by Cynet found that almost 80% of companies take over four months getting up to speed when deploying and becoming proficient in top security tools. Organizations with large budgets and security teams can dedicate a few team members to manage this, but leaner teams can't afford the luxury, and instead often just set one person to orchestrate the security strategy. Relying on one team member to manage security software makes the entire system less secure since any absence or unavailability would result in a massive security gap.



It also means that any major incident response will be slowed down, since a single person can't reasonably handle every single facet of a crisis. Even in the best and most peaceful of times, having only a single person who can fix a complex system is not ideal. The problem is compounded when you consider that a Cynet survey found that 47% of companies feel their biggest challenge is a lack of skills and experience.

The solution is to simplify and lower the accessibility barrier. Instead of complex systems that require an advanced degree and months of training, organizations should look for tools that reduce these barriers and allow for more team members to be experts in as little time as possible. Cynet, for instance, was purpose built with an intuitive user interface that can be quickly and easily mastered within days. This means that teams don't need to divert massive resources to learning a new system, individuals don't have to be overloaded with work, and security can be more efficient.

5. If your EDR suddenly claims to be an XDR but nothing has changed, you may need a new detection and response solution...

XDR is the latest hot trend in threat protection, so every security vendor wants in – whether they truly are an XDR or not. As with any new technology, confusion abounds so many vendors believe they can define XDR as anything they desire. A vendor with both an EDR and cloud security solution will claim to be an XDR although the two solutions are not truly integrated, and they have little response automation capabilities. Some "Open XDR" vendors are providing little more than a glorified SIEM/SOAR platform that requires extensive integration, configuration, and maintenance; completely the opposite of what XDR should provide, yet they're calling their solution XDR.

It's understandably difficult to determine what is and what is not an XDR solution. It's difficult to assess a vendor's level of integration between various controls and the overall ability to analyze signals to improve detection accuracy. Look for solutions with native capabilities built from the ground up vs. integrated after the fact and "hybrid XDR" solutions that provide most capabilities out of the box but can also integrate signals and data from other vendor solutions and system components.

Alternatively, you can find a provider that includes all features and services for a single, transparent price. This way you don't have to decide whether you spend your limited budget on threat hunting services or automated remediation capabilities. Cynet, for example, includes all capabilities, features, and services for one price – full XDR prevention and detection, extended automated response capabilities and a full 24/7 MDR service all included.

6. If you're paying more for your managed detection and response (MDR) than your EDR tools, you may need a new detection and response solution...

A 2019 survey by Tripwire found that 80% of security professionals found it difficult to find people with the right security skills. Out of those, 69% claimed the skill shortage directly impacted their security operations.

Compound the lack of adequate staffing with EDR tools that are difficult and time consuming to operate, and you've got a mix that puts many companies in a disaster situation. An MDR has become a necessity for many organizations, especially with the volume of alerts and endpoints most security teams must manage. The question is, if you have to spend additional budget on an MDR to help manage your EDR, then what is your EDR really doing for you? When you need to spend more on the people to help you manage your solution than on the solution itself, it's time to upgrade.

Instead, you should look for a detection and response tools that provide an MDR service as part of its offering – by default. Cynet, for example, offers 24/7 MDR already included in its cost, giving you full access to a team of experts that can complement your team and provide key resources that free up organizations' time to focus on other critical tasks.

7. If you've looked longingly at Deception technology, but have never been able to afford it, you may need a new detection and response solution...

One of the more valuable tools to emerge in recent years is deception technology. For organizations, the ability to lay traps and catch attackers that have successfully bypassed other layers of defense before they can do any harm is critical. However, not everyone can afford deception tools on top of the costs of their existing security stacks.

There are two major issues with deploying deception technology. The first is cost – deception tools are expensive and are often not included in many EDR offerings. This means that for teams that are looking to keep lean security stacks, adding deception tools is a tough sell. For many security teams, then, deception technology becomes a luxury rather than a necessity.

The second roadblock to adopting deception technology is the technical barrier to access. Deception tools are complex software and require finesse and a good deal of know-how to properly deploy. When they work, these tools are an excellent deterrent. When they don't, though, they become rather expensive bells and whistles.

Instead, you can find platforms that include deception tools by default. Much like with an MDR, having a built-in deception suite lets you quickly set up, calibrate, and properly deploy deception tools. Cynet's built-in deception suite takes a few minutes to master, deploy, and monitor. Instead of having to add a hefty price tag to your monthly security bill, you can take advantage of the added layer of protection that is native to the Cynet platform.

Final Thoughts

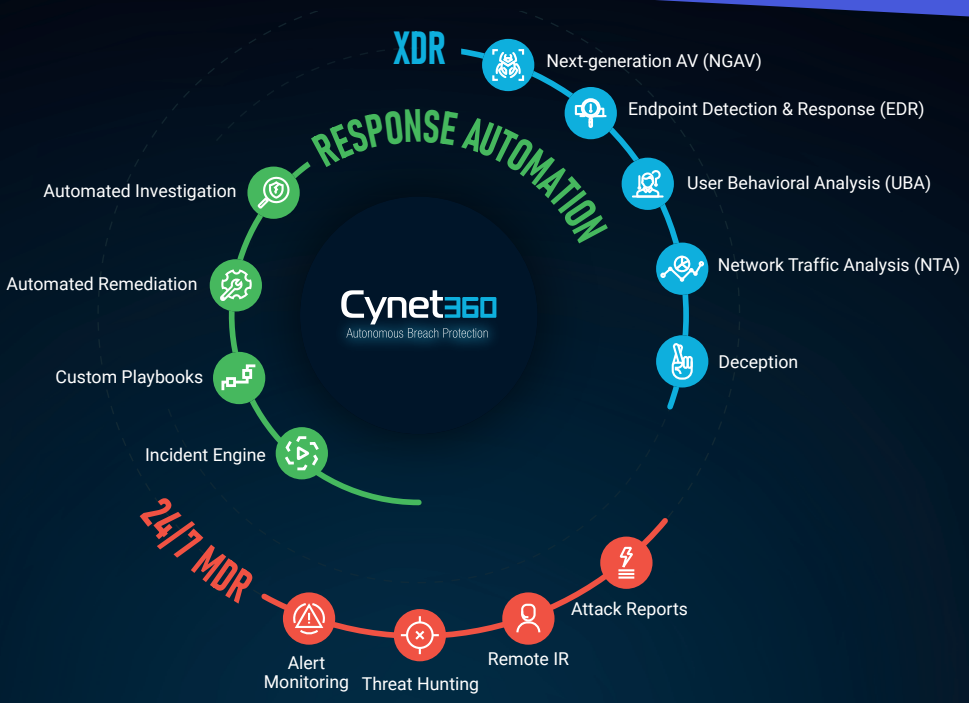
It's time to get more from your detection and response.

If any of the above considerations resonate, then it's certainly time to start looking for a better detection and response tool. EDR offers some great advantages, and in some cases can be a great frontline, but in today's heavily networked organizations, it's rarely the only thing you need. Instead of simply adding more tools, you should be looking for fewer tools that can give you everything you need.

XDR offer a great upgrade from EDR, extending your protection from endpoints to the entire environment and reducing the number of different tools necessary for protection. Instead of a disparate set of tools, dashboards, and remediation methods, you can simply look through a single pane of glass and get all the answers, visibility, and protection you need.

More importantly, the right XDR can also add vital tools that take your defenses beyond your current defenses – providing tools such as included MDR and deception technology. Instead of having to scrap together a security stack, you can get one ready-made for you out of the box. Stop simply adding to a solution that's not doing what you need and find a security platform that gives you what you want.

About Cynet and VARS



Cynet

Cynet enables any organization to put its cybersecurity on autopilot, streamlining and automating their entire security operations while providing enhanced visibility and protection, regardless of the security team's size, skill or resources and without the need for a multi-product security stack. It does so by natively consolidating the essential security technologies needed to provide organizations with comprehensive threat protection into a single, easy-to-use XDR platform; automating the manual process of investigation and remediation across the environment; and providing a 24-7 proactive MDR service - monitoring, investigation, on-demand analysis, incident response and threat hunting - at no additional cost.

VARS

At the cutting-edge of the information security industry, VARS selects and offers innovative, award-winning solutions to small, medium and large corporations, across North America.

VARS addresses the pressing needs of our modern cybersecurity world, providing you with constant guidance and support.