cynet

The Guide for

Solving Alert Overload and Handling

for Lean IT Security Teams

Learn

- The impact of excess alerts on cybersecurity and analyst effectiveness.
- Considerations for alert management outsourcing.
- How response automation helps reduce the burden of alert overload.
- Key tools to consider for automating the threat detection and response process.

Intro

Alarming research reveals the stress and strain the average cybersecurity team experiences on a daily basis. As many as 70% of teams report feeling emotionally overwhelmed by security alerts. Those alerts come at such high volume, high velocity, and high intensity that they become an extreme source of stress. So extreme, in fact, that people's home lives are negatively affected. Alert overload is bad for those who work in cybersecurity. But it's even worse for everyone who depends on cybersecurity.

This is a gigantic issue in the industry, yet few people even acknowledge it, let alone deal with it. We aim to correct that in this ebook, starting by shining a light on the cause of the problem and the full extent of its consequences.

The same research cited above showed that most security teams feel overwhelmed by the number of alerts that demand their attention every day. Not surprising considering that the average team receives 10,000 alerts a day. Most banks get hit with 100,000 or more in a 24 hour period, and as many as 40% of banks deal with double that number. No matter the exact figure, the sheer amount of security alerts far exceeds what any security team can address.

A fact these teams are more than willing to admit. Upwards of 55% of security professionals surveyed feel less than fully confident they can prioritize threats and respond to everything that requires attention.

Security teams are no strangers to feeling like they're up against an insurmountable number of alerts. The average daily alert total was in the five figures as far back as 2014. Research suggests the number has risen in recent years, which makes perfect sense given the rising number of cyber threats overall. IT security teams are up against an unrelenting onslaught of attacks that announce their arrival by triggering an alarm, one after another after another.

This is a problem. Alerts are more than just a source of workplace stress – they're an issue that makes effective cybersecurity impossible for multiple reasons. And things will only get worse. We will explore those reasons in the next section. Then we will confront them head on. If your lean security team struggles with alert overload, don't despair. This guide will outline a number of practical solutions in the coming pages.

Why Alerts Make Cybersecurity Worse

Anyone who doesn't work on the front lines of cybersecurity will struggle to understand what it's like. How many other professionals are given a responsibility - in this case responding to alerts - then given exponentially more work than they could ever hope to handle? Failure would feel like the only option, and a cybersecurity disaster would appear imminent. Who would thrive in those conditions?

No one, which explains why the vast majority of security professionals feel emotionally overwhelmed. We should be concerned about the high rates of discontent because talent shortages are already a huge issue for the industry. There are over **4 million unfilled positions** worldwide, with indications that the gap between supply and demand will only get wider. As it becomes harder and more expensive to recruit cybersecurity talent, companies will need to retain their existing talent at all costs. But if their work days are dominated by nonstop alarms and their home lives are suffering, people will burnout and leave, some from the industry entirely.

Worsening talent shortages and poor morale are one way that alert overload makes cybersecurity worse. Another way that more alerts leads to more successful attacks is by exhausting and outwitting the defenders. Consider that most security teams can only investigate around **56% of alerts** they receive (sometimes far less), and only 34% of those alerts are legitimate. That means almost half of all alerts get ignored, and almost half the time spent investigating gets wasted. With so much activity that goes unmonitored, attacks have a high probability of success...even when they trigger an alarm.

Perhaps the clearest indication of how attack overload affects cybersecurity is this: more than 40% of security professionals surveyed admit to turning off alerts, walking away from their computer, or waiting for someone else to step in. This means that alarms are having the exact opposite of their intended effect; instead of igniting the team into action, alarms inspire indifference and often get ignored.

We wouldn't accept this in any other emergency situation - imagine if fire fighters and ambulances got so many calls that they stopped responding. So why do we accept it in cybersecurity?

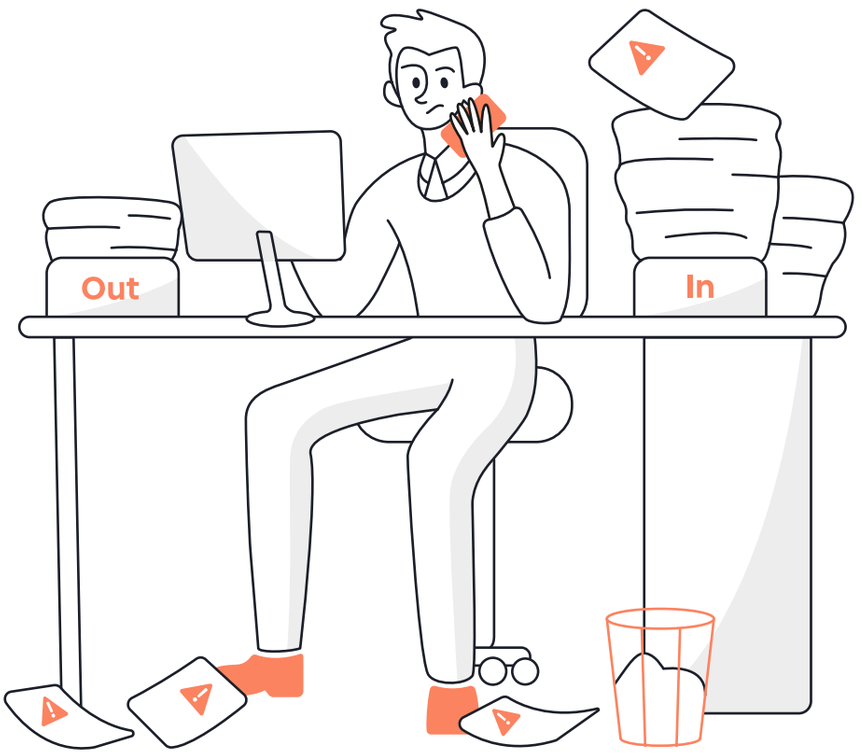
How Alerts Become Overwhelming

Before we can solve this problem, we need to explore where it originates from. That's especially true in the case of alerts, which are a standard tool in not just cybersecurity but all security. How did something that normally works quite well transform from asset to obstacle to existential threat? The reason is two-fold:

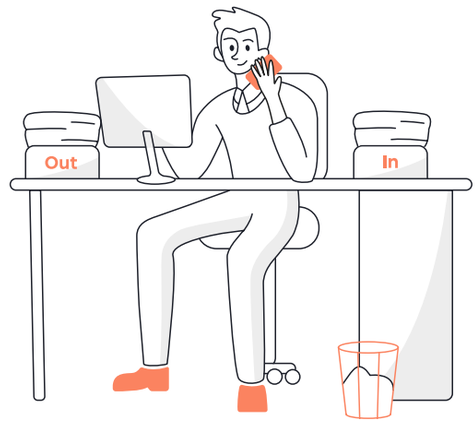
- There are thousands of alerts each day for an obvious reason: there are thousands of attacks each day. Estimates vary, but all suggest that even small and midsize organizations come under attack thousands of times daily. High already, attacks skyrocketed during the Covid-19 pandemic, when the FBI observed a **300% increase**. There are no signs to suggest that cyber attacks will slow down. That means alerts will keep increasing, except faster than before.
- Wanting to error on the side of caution, security monitoring tools are notoriously sensitive when set to the default controls. They regularly mistake legitimate traffic for something malicious, leading to huge numbers of illegitimate alerts. One study suggests that most security teams (75%) spend an **equal or greater** amount of time chasing false positives as they spend chasing legitimate security threats.

To put into perspective how alerts can overwhelm even an army of security professionals, do some basic arithmetic. The average alert takes at least **10 minutes** to investigate. If 5,000 alerts occurred in one day (around half the average), it would take 833 hours to respond to them all, meaning it would take 100+ professionals an entire 8-hour shift to cover everything. Even worse, half that effort would go to waste on false alarms.

This can't continue. Security teams of any size need to reduce the number of alerts they encounter, but the effort doesn't end there. Teams also need to refine how they respond to alerts so they take action before the damage starts



Is Outsourcing the Answer?



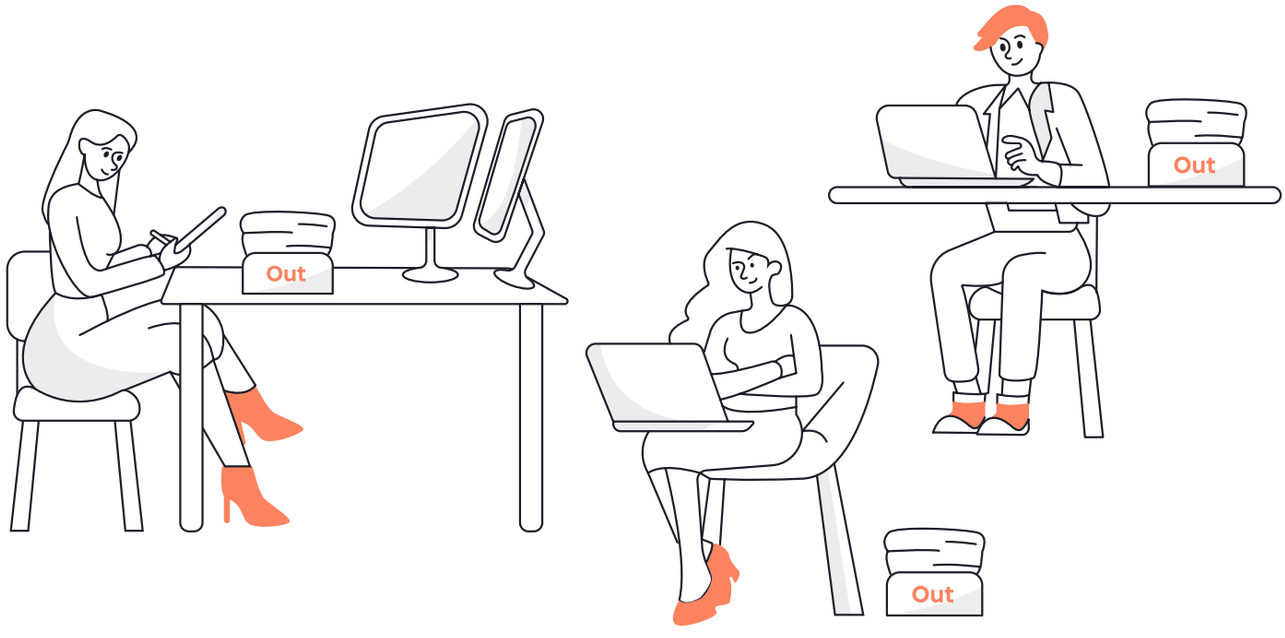
If it takes an army to keep up with alerts, outsourcing is one way to enlist the requisite ranks. Various managed detection and response (MDR) providers can take on some or all of the duty to investigate alerts and respond as necessary.

The advantage of this approach is that you can tap into as much security talent as you need and quickly scale that resource as necessary. Recruiting an equivalent amount of talent is unthinkable. MDR providers also remove some of the most time-, labor-, and stress-intensive workloads from the security team and shift them to a unit built for triage. Outsourcing certainly deserves consideration. But that consideration must include the downsides as well.

Let's start with the costs. While outsourcing may cost less than hiring full-time staff, it can still be expensive. Paying someone to handle dozens or hundreds of hours of work doesn't come cheaply, and it adds up fast over an ongoing basis. Even if outsourcing can (and probably should) play some role in a detection and response strategy, it can't handle the entire workload at its present volume. Few companies would green-light the considerable cost.

Another way that outsourcing fails to fix alert overload is by misunderstanding when to contact the security team. In some cases, MDR providers get overzealous about reaching out, including times when the security teams doesn't need to be alerted or involved. The overload just comes from a different source. In other cases, MDR providers may not be eager enough to get the security team involved, resulting in preventable security issues that find different ways to waste time and resources.

As we said, outsourcing can absolutely be an asset. But it's never a complete solution.



How to Reduce Alerts

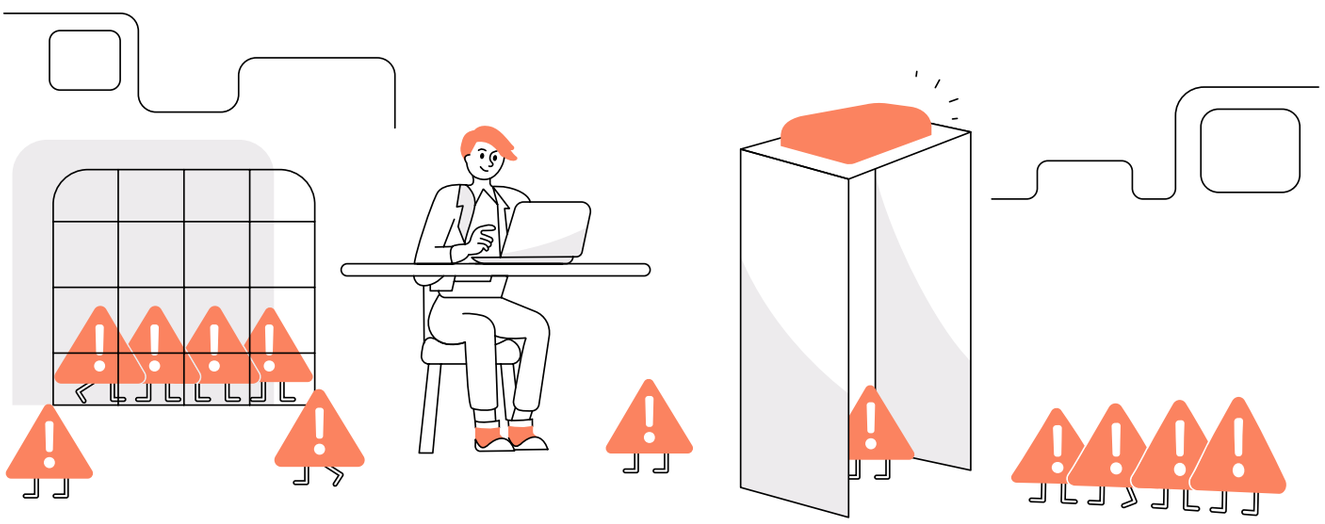
Any effort to fix alert overload starts by rethinking when and why the security team needs to be involved. We have already established that many alerts are actually legitimate traffic rather than threats. Eliminating these bogus emergencies could reduce alert volumes significantly (and save a tremendous amount of effort in the process). But the effort only starts there.

Many legitimate alerts can be eliminated as well. For example, the security team may receive an alert about port scanning. But since they can't do anything in response, the alert only serves as a distraction and source of anxiety. Many other default alerts could also be disabled once the security team knows which ones matter and which ones don't.

When alerts can't be disabled, consider aggregation instead. Many security tools allow for similar events to go out as a single alert. The security team receives fewer alerts while still keeping a full event history for analysis or auditing. We suggest investigating the alert settings on any security tool (present or future), and changing the default controls as necessary. Whenever possible, adapt the tool to the team, not the other way around.

Finally, find ways to expedite how you investigate alerts that you can't eliminate or aggregate. One way is to correlate alarms with known activities, like when a planned patch installation disables security tools in bulk as the system recycles. Any other time, the security team would want to know that security tools are going offline, but there's a simple explanation during patching. Calibrating tools to "quiet" alerts during known events or scheduled times will give the security team more time to focus on the actual emergencies.

Unfortunately, even when real attacks are the only alerts arriving, the security team may still be over-matched. In today's security landscape, attacks are fast, furious, and frequent, arriving by the thousands day in and day out. Few if any security teams have the people power to respond to every attack, let alone put adequate defensive measures in place to fight off the foes. The truth is that reducing alerts to a minimum doesn't solve the overload problem. Because the problem isn't about alerts – it's about response.



Introducing Automated Response

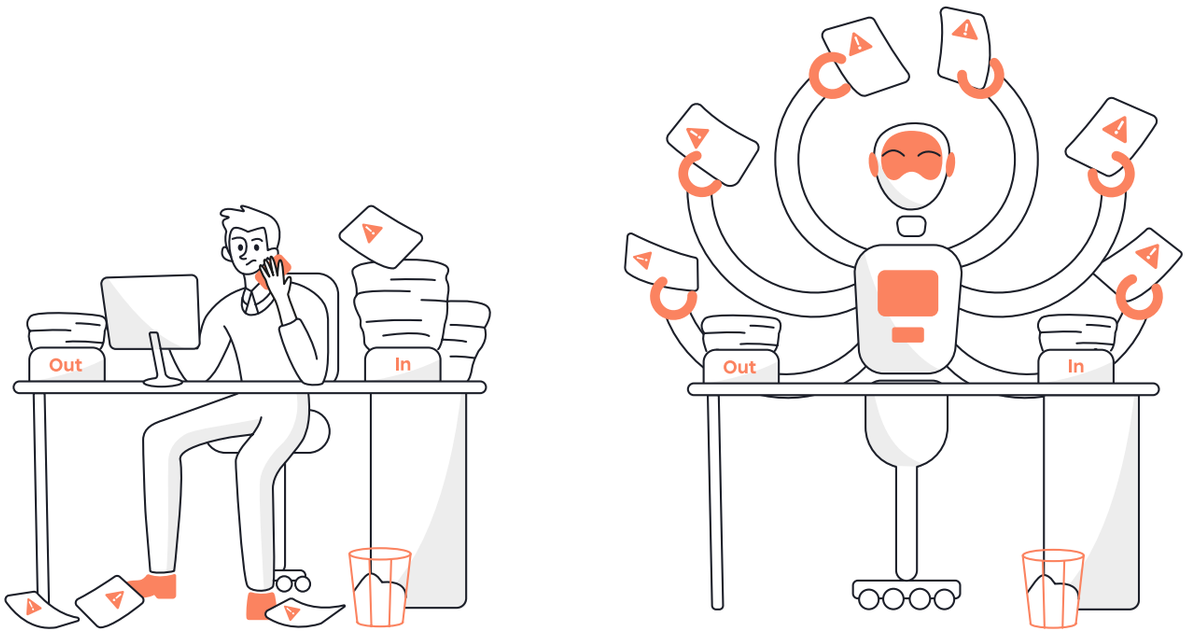
How can security teams, especially the leanest among them, respond to thousands of daily threats? With automation.

Automated response works like this: Security teams create response playbooks for the most common or critical alerts they receive. Those playbooks dictate exactly what mitigation and remediation measures to follow and in what order to keep the threat under control, whether by quarantine or eradication. When an alert arrives, the corresponding playbook automatically goes into effect, either working with complete autonomy or else working alongside a security pro.

The most obvious advantage of automation is being able to respond to alerts at scale. Automated tools can respond to exponentially more attacks than a human (or many humans) can. Furthermore, automation can respond at lighting fast speed to get in front of attacks and stop damage preemptively. Technology doesn't make careless mistakes, either, as it works meticulously through a defensive playbook. For all these reasons, automation offers a powerful antidote to alert overload combined with a serious fortification of cybersecurity.

We must, however, apply the same objective evaluation to automation that we did to outsourcing. The disadvantages of automation apply mostly to the unpredictability of letting a self-driven system take the reins of cybersecurity. One common problem happens when an automated response, particularly the kind driven by machine learning, blocks both malicious and legitimate traffic. These unpredictable instances can be annoying for the security team and for users throughout the organization. Problems can also be hard to undo if the actions taken by automation haven't been carefully documented along the way.

A bigger hurdle confronting any team wanting to implement automation is putting the constituent technology in place. We will outline those pieces in the next section, but suffice it to say that automating response involves many tools working in concert with one another. One missing piece may compromise the whole effort. Therefore, the hardest part about automated response is getting started in the first place.



Tools that Facilitate Automation

Response encompasses a number of different activities: spotting the threat, diagnosing the attack, planning the response, stopping the spread, eliminating the danger etc. It makes sense that automating most or all of this effort takes numerous tools. That list includes:

- **Endpoint Detection and Response (EDR)** – AI examines applications and user behavior to spot activities that deviate from normal patterns, suggesting the presence of something malicious. Then it automates the response.
- **Network Detection and Response (NDR)** – AI scans networks for anything unusual or suspicious and then automates the response based on any threats detected.
- **Security Orchestration, Automation, and Response (SOAR)** – A component of security information event management (SIEM) that leverages collected threat intelligence to automate and expedite the response.
- **Extended Detection and Response (XDR)** – Combining detection and response across multiple points of telemetry, XDR takes a farther and more comprehensive view than either EDR or NDR. That said, it's better seen as a supplement to those tools than as a replacement.
- **Managed Detection and Response (MDR)** – In conjunction with security technology, an outsourced MDR provider can serve as a backstop for the security team, stepping in to provide assistance at scale or expertise on demand. Choosing the right vendor is key though.
- **Intrusion Prevention System (IPS)** – Though somewhat dated, IPS remains a valuable network protection tools. By now there are open-source tools like Suricata and SNORT that are both robust and free, making them ideal for lean security teams.
- **Firewalls** – Both a means to control what ports and protocols are allowed between a sourceand destination and also a means to prevent anomalous network traffic, firewalls remain as important as ever, even more with the rise of zero trust cybersecurity.
- **Antispam** – Spam and other malicious messages continue to be a major vector for attacks. Most companies will need both gateway and API-based antispam solutions, including tools like URL filtering, impersonation prevention, and attachment sandboxing. Unfortunately, overly-aggressive antispam efforts can block legitimate, often important communications.
- **DNS Filtering** – AI uses threat intelligence to assess if a URL destination has malicious intent or hosts content blocked by the company. By only scanning DNS requests, this filtering tool eliminates the privacy concerns of web proxies that scan much more.

Knowing what tools it takes to automate response doesn't address the bigger challenge for lean security teams: putting all of them in place. Installing each one (even if a few were already in the security stack) would require huge amounts of time, adaptation, and investment, followed by a major effort to integrate tools and share threat intelligence between them. Only after all that was complete would automated response live up to its full potential. Therefore, automation may seem appealing but unattainable. We will prove otherwise.

Autonomous Breach Protection Made Easy

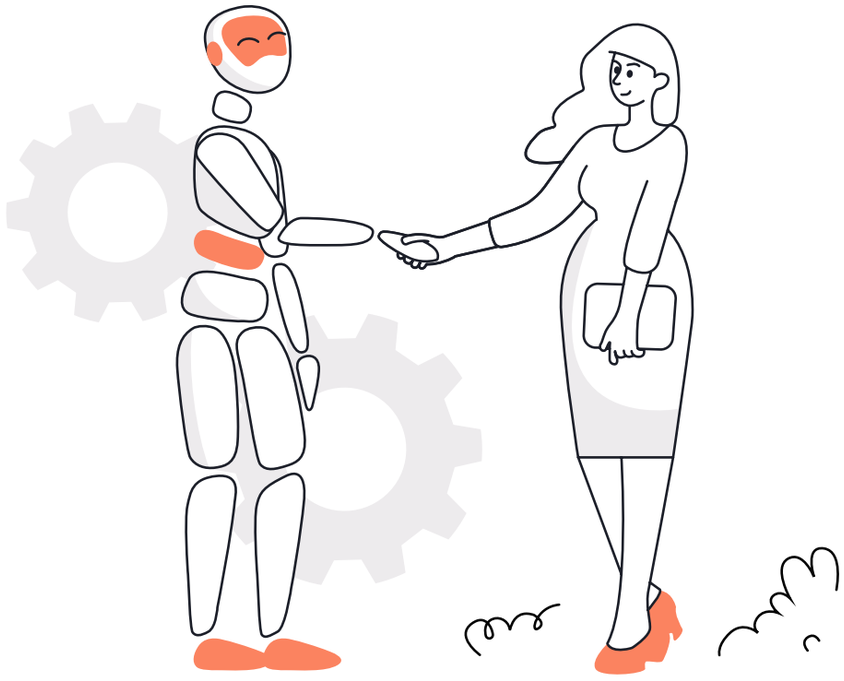
Trying to automate response in a piecemeal way would be extremely laborious and technical when possible at all. Many issues make it difficult to link together applications from different vendors and integrate data sets that live in separate silos. Therefore, the whole effort rests on integration.

Having many of the tools on the previous page unified on the same platform unleashes the power of automation. When EDR, NDR, MDR, and other mission-critical security solutions all operate under one umbrella, it has two major benefits.

First, it makes automated response relatively easy to implement in terms of the time and technical expertise involved. Many implementations get condensed into one. Plus, relying on a single, all-in-one solution costs less than paying for each of the constituent parts separately. There's also management and maintenance to consider – one solution versus multiple.

The second benefit involves the automation itself. When automation receives signals coming from all points in the environment – not just those monitored by a specific tool – it can see threats sooner, identify them faster, and institute the most informed response plan possible. And with integrated tools, the response doesn't stop or stumble when it reaches the boundary between one product and another. Instead, the response carries out whatever the playbook calls for and moves with agility at the same pace as attacks. Automated response truly excels when every cybersecurity tool works as one.

Alert overload is the next thing to improve. Once more of the response effort runs on autopilot, the number of alerts blaring at the security team drops dramatically. Most of them get handled automatically without needing any input from the team. And when input is necessary, the security team has more time to work, more insights to work with, and powerful automation to work alongside. More than just the solution to alert overload, integrated tools and automated response are the future of cybersecurity – a future where the defenders reclaim the advantage.



Cynet: A Single Solution for Cybersecurity

If your IT security team suffers from alert overload (or anything approaching it), the solution is in sight. Cynet has pioneered the first end-to-end breach protection solution that work autonomously. By natively integrating EDR, NGAV, Network Analytics, User Analytics and Deception technologies into a single XDR platform, Cynet has created an incident engine that fully automates response and remediation. The backing of a 24/7 MDR service with a world- class team included at no additional cost ensures that automated response has input from security experts whenever necessary.

With automation worrying about alerts, your security team can focus on other matters: studying threats, hardening resources, training users, revising policies, making plans etc. Overload and burnout become far less likely. So do successful attacks.

Learn More