The Guide for

Threat Visibility

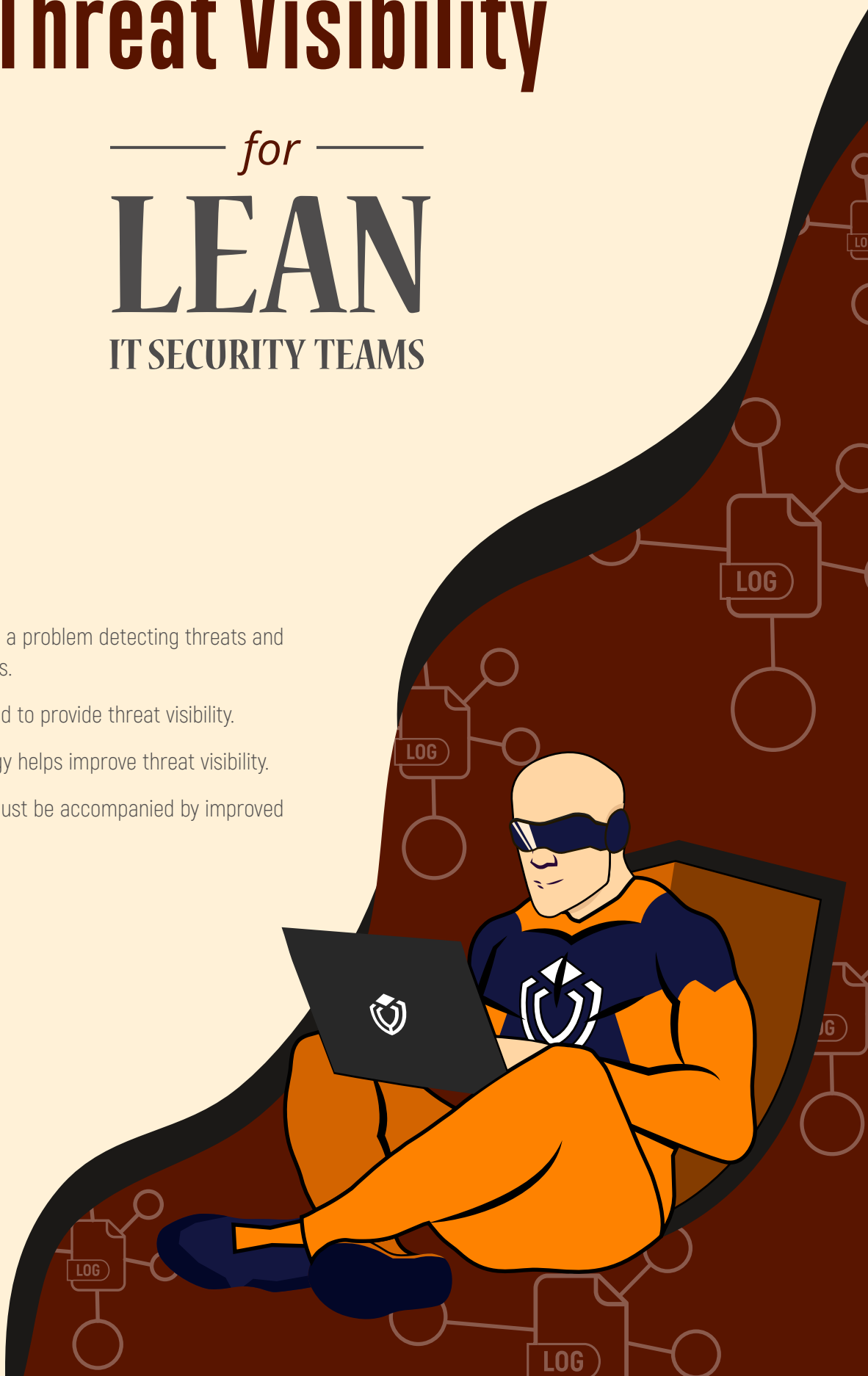
for

LEAN

IT SECURITY TEAMS

Learn:

- Why we continue to have a problem detecting threats and the hidden consequences.
- The key technologies used to provide threat visibility.
- How deception technology helps improve threat visibility.
- Why improved visibility must be accompanied by improved response capabilities.



Cynet

Intro

Cybersecurity depends on seeing every threat attempting to infiltrate an IT environment. Unfortunately, threat visibility has always been an unruly challenge. Security teams find themselves inundated with alerts (often leading to alert overload, a problem we addressed in another guide). Yet many of these are false alarms, and often the worst attacks creep in unnoticed. Despite seeing more than ever, security teams still don't have the threat visibility they need to stay ahead of attacks.

Recent research helps put this problem into perspective. Up to 64% of security teams feel only somewhat confident in their organization's security posture, and lack of visibility deserves much of the blame. Differentiating real vs false threats, dealing with visibility gaps, and facing an unmanageable alert volume were all specific pain points that respondents cited. The vast majority (89%) listed phishing, web, and ransomware attacks as their biggest worries. However, fewer than half have continuous visibility into these attack vectors. These number make clear that how we currently look for threats is doing more to hurt security than help.

The solution, unfortunately, involves what seems like contradictory aims. On one hand, security teams need visibility into an ever expanding attack surface populated by new and evolving threats. That means more alarms. Which leads into the second requirement for threat visibility: the ability to rank and filter alarms by importance. In that way, security teams need to know more but respond less–an inversion of the current situation.

In this guide, we will explore how threat visibility became such a widespread problem and why it has bigger implications for cybersecurity than seems obvious. Then we will explain the solution. Any security team, even the leanest and greenest, can drown out the false alarms and see the worst attacks earlier.

Why Detection Feels Like a Losing Battle

Security teams need to ask themselves a fundamental question: Why do so many attacks go undetected? Estimates vary, but one study suggests only 26% of attacks get detected by one of the many security solutions in place for exactly that purpose. The reason why involves the attackers, the defenders, and the increasingly digital world that both operate in.

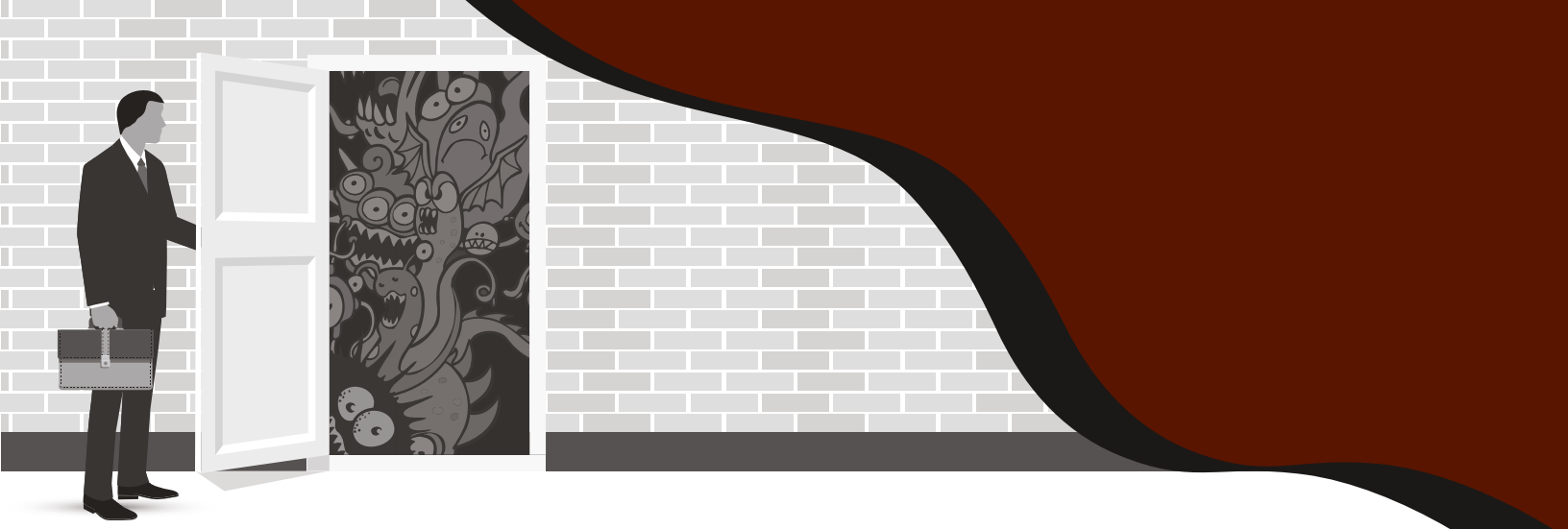
One reason attacks have skyrocketed in recent years is the complexity of today's IT environments. The traditional defensive perimeter has collapsed as companies have rushed into the cloud, embraced exponentially more endpoints, and permitted third-party access. Modern IT has evolved at the breakneck pace of business rather than the careful stride of cybersecurity, resulting in an IT environment that's so big and complex it resists any attempt to monitor what's happening.

As companies take on a bigger digital footprint, cyber criminals see profitable new opportunities to exploit, leading to an avalanche of new attacks that have never been seen before. Since most security technologies work at stopping known threats, the escalating number of novel attacks means more get through undetected. More activity in the cybercriminal under-sphere will mean more threats that we can't recognize, let alone stop.

Now to bring the defenders into the equation, the proliferation of attack types and IT assets has led to a patchwork of security technologies. Most will monitor some but not all the attack surface. And while they may have rudimentary integrations, disconnected defenses struggle to offer a complete, current, and accurate perspective on the threat landscape. Instead of bringing things into focus, they obscure what's most important.

Research confirms as much: IBM reports that despite improving efforts to plan for, detect, and respond to cyberattacks, the actual ability to contain them has declined by 13%. One explanation for that phenomenon is the proliferation of segmented security tools that make the security stack bigger but not necessarily stronger. IBM showed that the average company uses 45 different tools, yet those with 50+ feel less confident about detection and response.

Most security teams are at a moment where the noise drowns out the signal. It can make cybersecurity feel like an endless uphill battle and an inevitable losing effort. Unfortunately, it may be even worse than it seems.



The Hidden Consequences of Poor Visibility

More than just an obstacle to cybersecurity, poor threat visibility makes it essentially impossible to protect an organization from devastating cyber attacks. After all, you can't stop what you can't see. Just as problematically, you can't secure what you can't monitor. Given how many threats remain invisible and how many dark corners still exist in the IT environment, it's unrealistic to think a company is secure...or anywhere close. Remember what the IBM stats revealed: cybersecurity is slipping.

That's especially alarming for a few reasons. First, as companies become more digital-dependent and attacks become more merciless, any attack may cause deep, lasting damage to the bottom line. Cyber attacks have become an existential threat. Cyber security should be getting better, not worse.

The second reason to be alarmed relates to the cost of cybersecurity. Even lean teams spend a large part of the IT budget on security, and larger organizations may invest seven figures or more. However, rising spending hasn't even maintained the status quo because attackers have gained much more ground in recent years, as seen by the sudden outbreak of high-profile, high-stakes attacks.

Cybersecurity professionals are a third factor to consider. Problems related to threat visibility leave these professionals overworked responding to false alarms and discouraged by missing grave threats. No wonder the majority of pros in a recent survey said the stress of the job kept them up at night. Morale and burnout are serious problems in cybersecurity, and they contribute to a talent shortage that leaves many teams understaffed.

One can draw a link between poor threat visibility and the greatest problems in cybersecurity today: ballooning costs, exhausted security teams, and inadequate defenses. That means improving threat visibility, which we will explore shortly, has a positive impact that extends to all aspects of cybersecurity.

Key Technologies for Threat Visibility

It's better to think of the modern IT environment as a vast maze rather than a huge open landscape. Seeing everything and looking everywhere isn't possible with just one security tool. True threat visibility starts by having all the pieces to detect elusive threats sneaking through complex environments. Those pieces include:

EDR – Endpoints can be a target, entry point, or lateral leaping pad for many threats. Endpoint detection and response (EDR) solutions can prevent attacks from executing files and terminate suspicious runtime processes...provided they can recognize threats as such.

NDR – When active threats infiltrate a network, the network detection and response (NDR) tool should pick up on it immediately. With visibility into standard communication between endpoints, network analytics tools are efficient in detecting post-compromise activities that surface in anomalous network traffic.

NGAV – Though EDR will be able to catch more threats than next-generation antivirus (NGAV), it's important to have NGAV in the mix. It will use signatures to instantaneously identify malware that carries a known signature so the security team can eliminate the "low-hanging fruit" of threats and focus elsewhere instead.

UBA Rules – Since new and evasive threats can't be identified by a signature, it's important to monitor for unusual activity with a user behavior analysis (UBA) tool. They excel at spotting emerging threats that evade detection elsewhere, but the analysis takes time, especially soon after implementation. Therefore, UBA works better in conjunction with other tools.

SIEM & SOAR – Teams need a security information and event management (SIEM) tool to serve as a repository for log data from every detective and preventative control in the environment, plus from all systems, devices, and applications. A SIEM tool will mine this data for evidence of threats, and if it has a tool for security orchestration, automation, and response (SOAR), it can address the mitigation effort as well.

Integrate Everything to See in 360 Degrees

Security teams need each of the tools outlined in the previous section. None can provide adequate threat visibility individually–and complete visibility isn't possible when one of these tools is missing. Even so, implementing each one will still leave huge gaps in visibility.

Why? For the reason we touched on earlier: Poor integration between a patchwork of security tools. To the extent that the tools mentioned above can share threat intelligence and alerts with one another, the effort is slow, uninformed, and incomplete. That leaves large sections of the attack landscape in a blind spot. Integration issues are also a direct cause of alert overload since security pros must deal with separate alerts from multiple tools.

Integration proves key to the entire effort. Threat visibility won't work without it because seeing everything in one place means having all signals in one place from endpoints, networks, user controls, and beyond. More than just integration, though, security tools should ideally run on the same platform as each other so that nothing inhibits visibility in any direction.

The need for more integrated and intelligent forms of detection has been apparent for a while, leading to the development of extended detection and response (XDR). By integrating NGAV, EDR, UBA Rules, and NTA Rules under one umbrella, XDR extends the range and resolution of threat visibility. Security teams can spot attacks sooner, in greater quantity, from more directions, and with improved accuracy. If cybersecurity relied on a series of spotters before, XDR works like long-range radar, exposing attacks in every direction no matter what evasive measures they take.

The right XDR tool can replace some key pieces of the security stack, often at a lower cost. More importantly, it can seamlessly integrate those pieces to dramatically improve their performance.

Deceptive Technologies: The Secret Weapon in Your Arsenal

XDR can have another component we haven't touched on yet: deceptive technologies. The component outlined in the previous segment works to make all threats visible by integrating signals from all relevant sources. The deceptive component has the same goal-to expose threats-but relies on a different technique.

Deceptive technologies trick attacks by luring them towards fake assets. The security team will set up dummy accounts or files that look like prime targets but have no actual value. Therefore, anything that tries to access those files or accounts must be malicious. Attacks that managed to evade detection elsewhere may be undone by deceptive technologies that lure the attack into a trap. Alternatively, when deception doesn't work, other tools can still register the attack. That's why deceptive technologies are an important component of XDR, something that enhances threat visibility and provides an additional layer of protection.

The great advantage of deceptive technologies is the almost total absence of false positives since attacks are the only things attracted to dummy assets. The security team isn't distracted by irrelevant alerts. Instead, they learn the location and characteristics of attacks that are inside and in-progress–eg. the ones worth focusing on. In the quest to reduce the quantity and improve the quality of alerts reaching the security team, deceptive technologies play a big role.

However, they invite some challenges as well - challenges that also apply to XDR more broadly and threat visibility in general. Specifically: How can security teams stop all the threats they're suddenly seeing? Improvements in detection must be accompanied by improvements in response. Otherwise, cybersecurity doesn't improve at all.

With Great Visibility Comes Great Responsibility

Important as it may be to improve threat visibility, it's only the beginning of the effort. Security teams–lean ones in particular–may find their stress levels soaring once they can see the many threats looming on the horizon. The situation may look even worse than before without a way to add speed and scale to the response effort.

Automation improves both speed and scale more than an army of security pros could–so long as it is integrated within the XDR. When both work together, all the signals and data collected by the constituent parts of the XDR feed into the automation engine to give it an enhanced understanding. That enables the automation to investigate the attack faster to determine its root cause and full impact. Then, based on what's known about the attack, automation can orchestrate a playbook recommended for that attack, taking specific steps to neutralize the threat and mitigate the damage. Ideally, automation can handle the entire remediation effort for user, network, and endpoint attacks. And when the security team must be involved, vital information feeds into graphical layout of the attack to keep decision-makers fully informed.

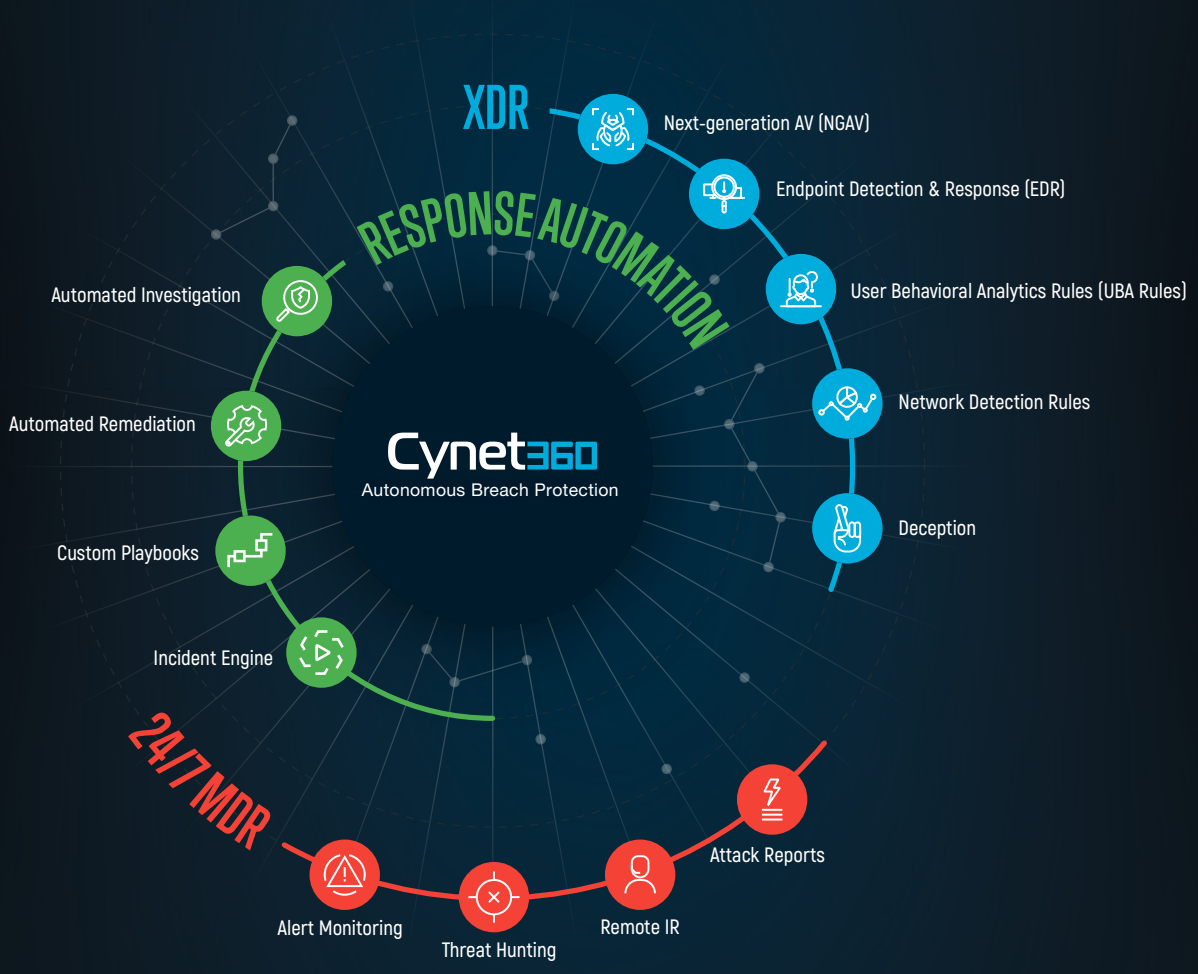
Another way to enhance response capabilities is with the help of a managed detection and response (MDR) provider. Even with automation, lean security teams may struggle to stay on guard 24/7, especially against a new generation of attacks. MDR providers can monitor an environment, bringing experience and expertise to threat hunting. They can also help plan and execute an incident response strategy that includes a comprehensive attack investigation. By design, these partners are equipped to handle whatever threats a security team encounters, thereby negating the disadvantage of being lean and equipping any security team to fight off the most formidable threats.

The formula for improving not just threat visibility but threat prevention as well looks something like this: XDR+automated response+MDR.

Cynet - Your "One Stop Shop" for Threat Protection

As the world's first autonomous breach protection solution, Cynet provides an all-encompassing platform equipped to see every threat and automatically leap into action. And when human intervention becomes necessary, included MDR services can handle the heavy lifting and apply an expert eye to the situation. With Cynet, security teams of any size have every resource they need to make cybersecurity work, now and into the future.

Don't let the security stack continue to get bigger. Consolidate around tools, techniques, and teams that have been battle tested and proven effective. Enhance threat visibility, along with everything else, with Cynet.



Learn more