Cynet

The Guide for

Achieving 24X7 Threat Monitoring and Response

for

LEAN

IT SECURITY TEAMS

Learn:

- Why 24x7 threat monitoring should no longer be considered optional.
- How cybersecurity talent shortages can be overcome.
- How the two-pillar approach helps lean security teams achieve 24x7 threat monitoring.

primenet

Intro

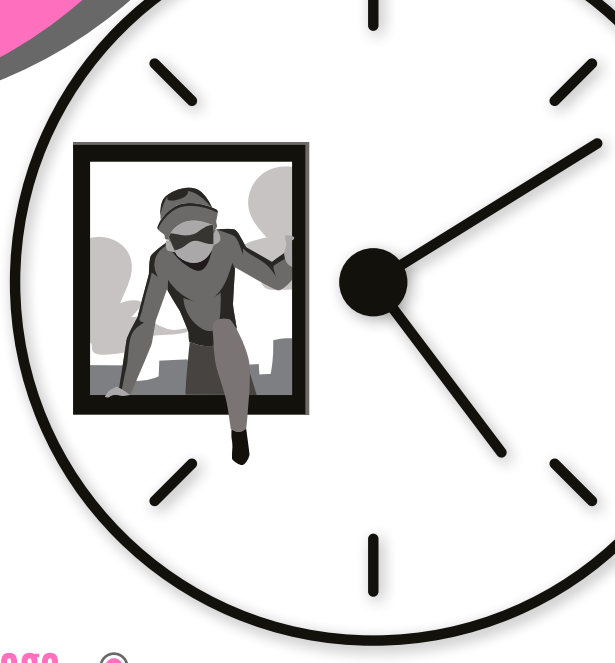
Cyber crime doesn't sleep. Digital attacks can arrive at every hour of the day or night. They can occur repeatedly, often relentlessly, any time of the year, including holidays. And whenever they appear, attacks can be carefully disguised to avoid detection while armed with malicious code intended to cripple an organization. This creates a situation where security teams must be on guard 24x7x365 – and any lapse in vigilance can lead to catastrophe.

Making matters worse, the attack landscape has never been larger. Now that the standard IT infrastructure encompasses multiple servers, networks, and clouds along with countless remote endpoints, cyber criminals have an abundance of weaknesses to exploit and multiple ways to reach their intended targets. Not only do security teams need to monitor for threats without ever blinking; they need to look in a dozen directions at once.

Under the circumstances, cybersecurity feels like an impossible undertaking. Unfortunately, there's plenty of recent evidence backing up that conclusion. Cyber attacks have gotten exponentially worse in recent years according to every metric that matters: frequency, intensity, complexity, and severity. Worse, it appears that no organization is safe following successful attacks on major corporations and government agencies alike. Round-the-clock threat monitoring may be the universal goal. In one high-profile incident after another, however, attackers prove there are still blind spots they can sneak through unnoticed.

Dire as the situation may seem, 24x7 threat monitoring can be achieved, along with immediate, effective response the minute something alarming appears on the horizon. It doesn't take an army of security professionals, an overstuffed security stack, or endless funds to spend on defenses either. Even lean security teams can stay on guard at all times, without fail, provided they take certain steps.

We will outline those steps in the following guide. But first, we will explore why 24x7 threat monitoring and response will only get more important for cybersecurity...and only get more difficult too.



How Cyber Criminals Use Timing to Their Advantage

Criminals have always preferred to operate during "off hours," and cyber criminals are no different. Research into the recent outbreak of ransomware attacks confirms at much: 76% of all infections take place outside normal business hours, with almost half striking at night, and over a quarter waiting until the weekend. Attackers do this strategically to take advantage of security teams that are either understaffed during second and third shifts or not staffed at all.

Holidays give attackers the same advantage. For example, the SolarWinds attack that hit everyone from the US Department of Defense to Cisco chose Memorial Day weekend to make its presence known, banking on the fact that security pros would be absent on vacation or distracted by holiday plans.

Knowing that attacks will come when they are least expected, it might be tempting to bump up security on night, weekends, or holidays. But hackers are savvy about deploying the element of surprise. They have found ways to weaponize the 9-5 workday as well, often by turning employees into attack enablers. For instance, the majority of malicious emails arrive on Tuesdays when, for various reasons, email open rates are 20% higher. They also pick up during the afternoons when people are likely to be at their desks and cleaning up their inbox. The hard truth for security teams is that attacks could start at 2 pm or 2 am. Cybersecurity, therefore, must remain at full strength for every minute of the day.

Anything short of that enables attacks to infiltrate a tech stack, often without raising any alarm in the process. The average amount of time attacks dwell without being noticed was recently measured at 239 days for companies without security automation. That number is roughly the same as previous years, meaning that hackers have about eight months to steal, corrupt, or destroy whatever they want. This underscores the importance of not just monitoring but seeing every threat advancing towards an organization. It also indicates the importance of monitoring for threats that have already made their way into the organization. It also emphasizes the link between monitoring and response: if security teams don't see attacks early enough, they often can't respond until it's too late.

According to IBM, the cost of a data breach is both higher than ever and increasing faster than expected. The average cost rose to a record $4.24 million in 2021, a jump of almost 10% from the year before. Attacks generally become more expensive the longer they go unnoticed or unresolved. However, in the age of ransomware, when one bad click can quickly lock up a company's data, attacks don't need much time to take full effect.

It's a dire situation. The outlook seems even worse for lean security teams because they have fewer resources to expend on late-night monitoring and lightning-fast incident response. Worst of all, things won't improve any time soon. Everyone should expect monitoring and response to get harder, significantly so, in the immediate future.

The People Problem in Cybersecurity

It's no mystery why most companies struggle with 24x7 monitoring and response: they don't have enough staff. Keeping eyes on the infrastructure at all times means running three shifts a day, often with multiple people in the security center at any given time. Recruiting all those people, especially to work nights and weekends, isn't easy for any security team regardless of size.

Talent shortages in cybersecurity are nothing new. Studies from 2017 predicted there would be 1.5 million unfilled cybersecurity positions by 2020. That proved to be a vast underestimation considering the talent shortage has grown to 4 million people as of 2021.

Without an adequate talent pipeline, security teams have a brutal time filling all the roles they need. More than half the teams surveyed report that skills shortages are creating a "bad" or "very bad" situation at their companies. Since the demand for talent far exceeds the supply, companies compete fiercely to attract security experts and often pay handsomely (some might even say excessively) for new hires. The result: few security teams are fully staffed, and fewer still have the means to get there. Lean security teams suffer the worst considering that lean is often a nicer way of saying bare bones.

There's no reason to think the talent shortage will end anytime soon. Rather, it's likely to get worse. As cybersecurity threats become a bigger business risk, companies will need to rely on ever more security pros. Lacking that staff, however, they will ask more of the existing staff, contributing to higher rates of turnover and burnout. This is a self-perpetuating problem. One that will only make 24x7 monitoring and response less realistic as time goes on.

People problems in cybersecurity come as excellent news to attackers. They have good reason to think their schemes will succeed more often in a future with understaffed security centers populated by overworked or under-trained security teams. But that's also good news for the defenders, because it highlights the solution to the problem: remove people from the equation as much as possible. This approach is actually easier than expected using a two-pillar strategy we will outline in the remainder of this guide.

Automation: The First Pillar of 24x7 Monitoring

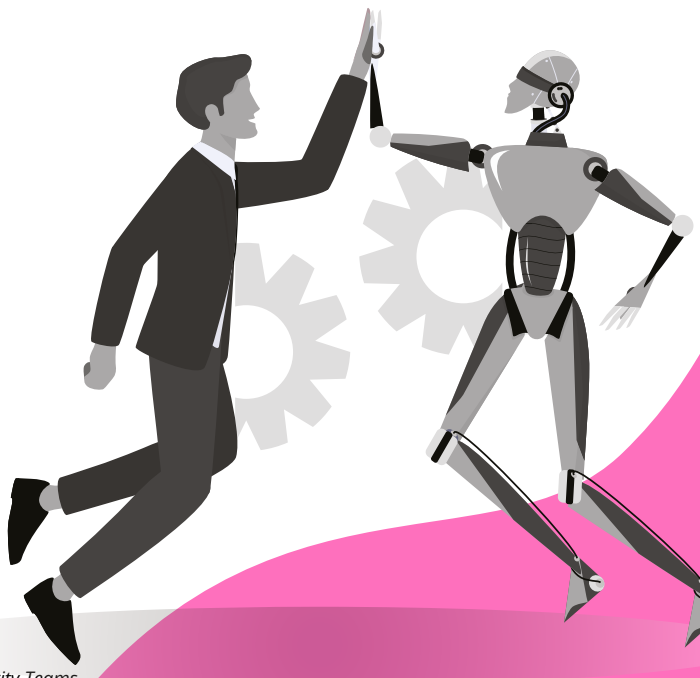
Multiple metrics show that cybersecurity automation makes companies better equipped to deal with cyber threats, but perhaps none more compelling than a study showing that organizations spend $1.5 million less on data breaches when they have fully-deployed security automation.

Automation has long been positioned as the solution for cybersecurity. However, it was only quite recently that automation became the game-changer it was always hyped to be. The integration of various security tools that used to operate independently – anitvirus, endpoint detection and response, user behavior analytics, and others – enables security teams to now automate vast amounts of work they used to do manually. For example, rather than monitoring multiple points across the attack landscape and correlating signals for threat detection, technology can do this work automatically. Enough good intelligence allows automation to see anything unusual and distinguish real threats from legitimate actions. Security teams receive an alert only when something requires their attention or intervention.

Lean security teams can make big strides towards security automation with a web application firewall (WAF). With the right configurations and scale, a WAF can serve as a strong defensive perimeter around an organization, one that sees and stops most attacks before they do damage. WAF as a service options are now available. Lean teams can utilize this service to make a powerful WAF, beholden to an SLA, the automatic defender of the organization that neutralizes more attacks without involvement from the security team.

That said, relying on WAF alone is like erecting guard towers without putting anyone on watch. For reasons we covered, putting human monitors in place isn't realistic, but automation fills the same roles. Integrated tools monitoring multiple points of telemetry 24 hours a day ensures that anything the WAF can't catch, including sophisticated and evasive threats, shows up on the radar and sounds the alarm. The right tools working in concert puts threat monitoring on autopilot so that 24x7 monitoring and response isn't compromised in any way by human resources. Automation means that security centers are always fully staffed and never less than completely alert.

Here is where newer Extended Detection and Response (XDR) tools can help. These platforms monitor multiple telemetry in a single platform, allowing lean security teams to see into the nooks and crannies of their environment, not just the one point of entry monitored by siloed detection tools. This approach provides layered security protection out of the box, so if something is missed by one detection technique it can be seen by one of the other detection mechanisms. There are no silver bullets, so XDR combines multiple types of firepower in a single platorm.



Outsourcing: The Second Pillar of 24x7 Monitoring

Automation can handle most if not all of threat monitoring. And it can enable the response, too, by automatically putting prescribed playbooks into action so that nothing delays defensive maneuvers. However, security pros still need to decide when they should be involved with conducting forensic analysis on the attack and orchestrating a complete mitigation strategy. People are still key to the process.

Recruiting is one way to assemble a battle-ready blue team, but outsourcing is often the better option. Outsourcing providers offer access to diverse, robust security teams on demand. Clients can get whatever support they need with monitoring and response at a fraction of the cost of hiring. With this resource to fall back on, no security team lacks the size, strength, or smarts it needs to respond to attacks, whenever they arrive and in whatever form they assume.

Cybersecurity outsourcing comes in two varieties. Managed Security Service Providers (MSSP)s will essentially run everything. Think of this as outsourcing the whole security center. MSSPs are a good option for companies with no security team or one person handling security plus the rest of IT. These providers aim to be all-encompassing, which can be an asset for companies that truly need everything. However, MSSPs sometimes push clients to use siloed security tools that work poorly or not at all with the security tools a company already has in place. For teams that want to keep some of their security operations in-house, the limitations of MSSPs could become liabilities.

The other variety to consider is Managed Detection and Response (MDR). These providers don't offer the same breadth of services as MSSPs. Instead, they offer world-class detection and response capabilities from a team serving on the front lines of cybersecurity. These providers distinguish themselves through their foresight and tenacity. Lean teams can add these security hawks to their ranks to start excelling at detection and response. Yet these same teams can still manage most of their security posture in-house – especially the parts they can manage during the traditional workday.

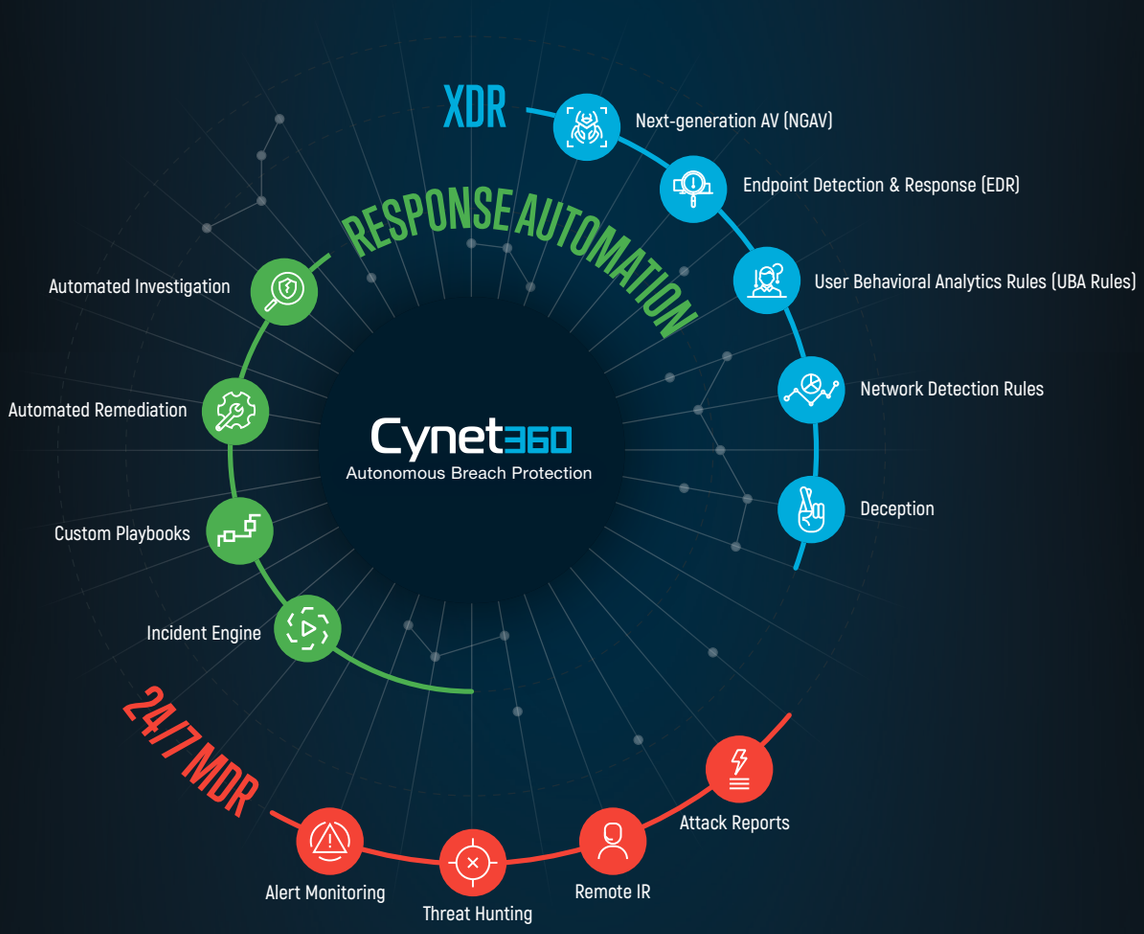
Outsourcing makes 24x7 threat monitoring and response attainable for anyone. Providers do the hard work to keep detection and response teams fully staffed and consistently vigilant. That means clients don't just have a staff member on watch in the security center at 3 am – they have a full team of diverse experts hunting for threats on their behalf. In that way, outsourcing doesn't just make threat monitoring and response an end-to-end activity – something that doesn't stop. It makes those activities exceptional at all times so that attackers can never use timing to their advantage again. The defenders don't sleep either.

Cynet – A Singular Solution for Breach Protection

Cynet brings the two pillars of 24x7 threat monitoring and response onto one platform. XDR built from multi-layered protection excels at seeing threats coming from any direction, even if they use novel or complex means of evading detection. Response automation turns alarms into immediate preventative actions that analyze the root cause of the attack and then remediate that specific attack, all without needing action from the security team. Included with the XDR platform are 24/7 MDR services that proactively look for threats and lead (or support) the incident response effort.

More than just a complete solution for autonomous breach protection, Cynet raises the bar for detection and response. By integrating more critical security tools on one seamless platform and then backing that platform with a dedicated MDR team, Cynet runs cybersecurity with unparalleled visibility, speed, and coordination. Crossed wires, missed signals, and delayed responses are not obstacles anymore once the core features of cybersecurity work in perfect sync in a single, integrated, natively-built platform.

Cybersecurity can't depend on the clock or the calendar. With XDR and MDR working together, it never waivers.



Learn more