

# The Importance of 24/7 Coverage

## Don't Let Cyber Attacks Catch You Off Guard

[REQUEST A FREE TRIAL](#)

Cybercrime 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.

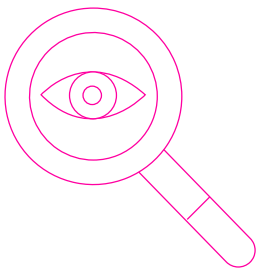
It's a dire situation. The outlook is worse for lean security teams at small to medium sized enterprises (SMEs) because they have fewer resources to expend on 24x7 monitoring and lightning-fast incident response.

### The Solution

Achieving 24x7 cyber protection is actually easier than you would think. Cynet combines Automated Threat Response with a 24x7 Monitoring and Response service to ensure your organization is fully protected around the clock.

## Automated Threat Response

Advances in machine learning and artificial intelligence have enabled automated systems to outperform humans, especially on common, repetitive tasks. They are especially helpful for enforcing best practice approaches for users that don't have the domain expertise. Here's how automation can significantly improve threat response.

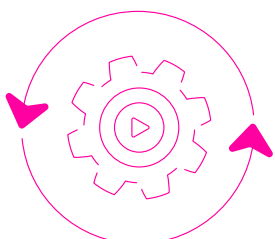
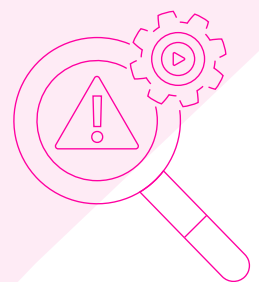


### Visibility

Automated systems can ingest signals from multiple domains to detect threats more accurately with lower false positives. Seemingly benign signals may indicate a dangerous threat when combined – something perhaps not obvious to a non-expert human analyst, but something an automated systems can achieve instantaneously. Detecting threats using automated AI that is constantly trained with new attack approaches is ideal.

### Automated Investigation

Cybercriminals know most SMEs lack 24x7 coverage, which is why most ransomware attacks target these organizations on off-hours. Therefore, every alert, no matter the risk or time of day, must be investigated to determine whether the threat is dangerous or perhaps part of a larger, stealthy attack. Automated threat response systems can instantly investigate alerts to determine the root cause and scope of an attack.

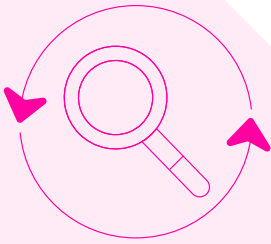


### Automated Response

Preventing data breaches requires that identified threats are quickly and thoroughly eradicated. Automated Response systems are available 24x7 to perform simple remediation actions or execute highly sophisticated response playbooks that involve logic and multiple potential response actions. Response playbooks are especially useful to address dangerous threats like ransomware by not only containing the threat itself, but also the root cause and any traces of the threat across the environment.

# 24x7 Monitoring and Response

While automation can be a godsend to security teams, nothing beats a 24x7 Monitoring and Response service staffed by a team of cybersecurity experts. This puts a seasoned team in place to monitor and protect your organization at all times, even when your team is unavailable.

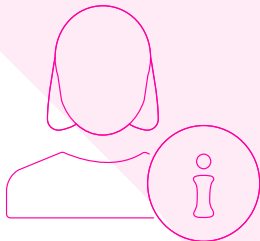
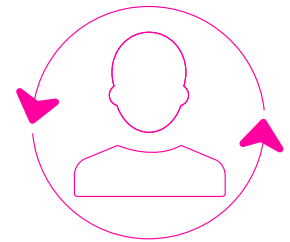


## 24x7 Monitoring

World-class cybersecurity experts monitor client environments every moment of every day to ensure that no dangerous signals are overlooked.

## 24x7 Response

To ensure all potential threats are thoroughly investigated and eradicated across the environment, incident response experts are available to contain and eliminate threats before any damage can be done.



## Expert Advice and Oversight

Have a complex cybersecurity question? Not sure your protections are configured optimally? Unsure if a process is legitimate? Cybersecurity experts are available to you at all times to help.

## Key Takeaway

24x7 cybersecurity protection is not only available for large enterprises with dozens of cybersecurity analysts. Even the smallest companies can achieve full 24x7 cybersecurity protection with the right tools and partners.

[REQUEST A FREE TRIAL](#)