cynet

# How to protect your organization with a small IT Security team

REQUEST A FREE TRIAL

The single biggest cybersecurity threat doesn't come from outside an organization and it doesn't involve anything digital either. People are the biggest problem. Or, more specifically, a lack of people.

The average security center takes on the herculean task of monitoring complex environments for evasive threats on constant attack. And when one of those attacks inevitably succeeds, the security team must immediately initiate a full-scale response where every minute matters. Cybersecurity is a huge, ceaseless, and stressful undertaking for any team. So, it doesn't help that most teams are understaffed, under-skilled, and struggling to recruit.

The right roster for a security team depends on multiple factors: the size of the company, the contents of the tech stack, the level of security required, the amount of funding available etc. Most smaller organizations simply cannot afford the number and array of security experts typically employed by larger enterprises, which typically includes the following roles:

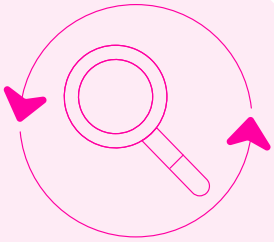
- **Security Analyst** – Professionals who analyze security events and perform incident response as necessary – the frontlines of cybersecurity. An effective security team should have enough analysts available for each of three shifts so the team can be on guard 24x7.
- **Security Engineer** – Someone who performs threat modeling and trains engineers on security. Security engineers also run red team exercises and perform penetration testing.
- **Security Architect** – The person who designs security controls for an organization and performs risk analysis. This role is typically hard to outsource.
- **Security Project Manager** – Every team needs someone to oversee various initiatives, keep progress on track, and coordinate/collaborate with project managers on other teams.
- **Security Vendor Manager** – As third-party risk analysis becomes increasingly important, security teams will need someone to handle this responsibility.
- **Security Operations Support** – This role manages security technology and supports the analysis team. Lean teams often expect analysts to also handle security operations.
- **Internal Auditor** – Increasing cyber compliance requirements create the need for an internal security auditor to regularly verify that security measures comply.
- **Chief Information Security Officer** – This executive leads the security team and reports to the board of directors. A CISO serves as the public face of the security team.

## The Solution

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

# 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. Instead of hiring and training people to handle key security responsibilities, consider outsourcing those responsibility to a trusted security services provider. This puts a seasoned team in place to monitor and protect your organization at all times, usually at a lower cost than full-time employees working in-house.

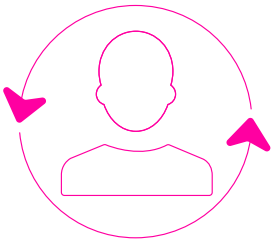


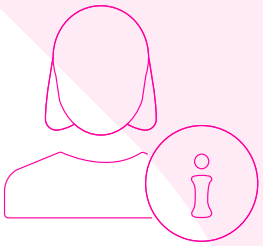
## 24x7 Monitoring

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.



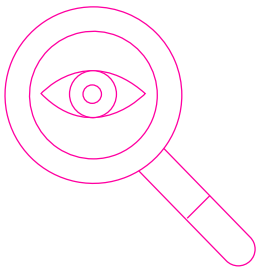


## Expert Advice and Oversight

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

# 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.

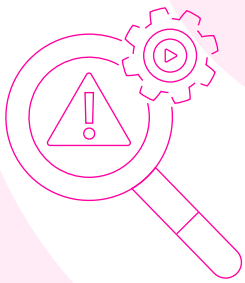


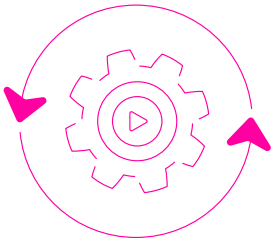
## Visibility

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.

## 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.

# Key Takeaway

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

**REQUEST A FREE TRIAL**