Accurate, Fast and Transparent Incident Response Services

We combine IR experts with the Cynet 360 technology to deliver professional incident resolution

The race against time to contain the incident

Whether its ransomware encrypting your data, info-stealing malware in your network or data breaches containing sensitive data, you need to receive the precise details of the attack to take the right course of action. The clock is ticking and you need to contain the threat, scope the incident, assess the damage and remediate. It's a race to get back to business as quickly as possible. You need dedicated help that provides you with speedy answers and also ensures that your systems will be kept secure after the incident.

Incident Response that combines experience and dedicated technology

Cynet's Incident Response (IR) service combines deep security analysis experience together with Cynet 360, its world-class proprietary investigative and security technology. The combination first and foremost means that you achieve the fastest and most accurate results. Cynet's proactive 24/7 security team acts as your extended team, leading any required analysis, ensuring that nothing is overlooked and generating the results you need. Moreover, you can decide to keep Cyne360 post-resolution to protect your systems against future attacks.

Key Benefits

Best of breed IR tech
Cynet's proprietary IR tech means that we look at alerts and information coming from endpoints, users and networks. This gives us the necessary visibility for IR and since everything is automated – to get to it quickly.

IR setup that's fast and scalable
No need to involve open source or manual tools. Our tech is easy to deploy, allowing for speed and scale across endpoints.

IR that's transparent
You get a dedicated IR project manager and point of contact, keeping you in touch at least daily and typically every few hours.

Reports that you need
Ranging from executive summaries to detailed IoCs that can be exported to CSV for consumption by other systems, or to manually update systems across the environment.

Security post-resolution
At the end of the IR process, you have the option to keep Cynet 360 to secure your systems against future breaches.

The Cynet
Incident Response Methodology

Triage

Human interaction is key and our first step sets the groundwork for engagement. Each company has a different background and needs so we first clearly define expectations, process stakeholders, known incident details and IT systems. Cynet then builds and shares the IR setup and game plan details. While this is the initial step, it follows us throughout the whole process, collaborating with your team, as well as any required third party, in order to reach an effective, transparent, and speedy resolution.

Deployment:

To get to accurate results, the Cynet 360 Autonomous Breach Detection Platform is deployed on your endpoints. This is a lightweight XDR agent that seamlessly integrates Next-Generation AV (NGAV), Endpoint Detection and Response (EDR), User Behavioral Analytics Rules (UBA Rules), Network Detection and Response (NDR) and Deception. Cynet deploys up to 5000 endpoints in less than an hour.

Policy Creation

Cynet investigators create a customized policy within Cynet 360, beyond the provided alerts and remediations on hosts, files, users and network. These customized detections and remediations are based on the information gathered in triage and data gathered in the initial deployment and deployed across the IT environment. For instance, the Cynet team may find it relevant to alert on a suspicious port to a malicious IP or on a malicious file based on its file properties.

Recommendations and Mitigations

Based on the Indicators of Attack (IOAs), Cynet provides recommendations and mitigations on the endpoint, as well as across the IT and security environment. For instance, Cynet may block traffic to/from a revealed malicious IP. Revealed malicious IPs can also be fed to other systems such as to your third party firewall. Other mitigations may include isolating the machine from the network or disabling a user.

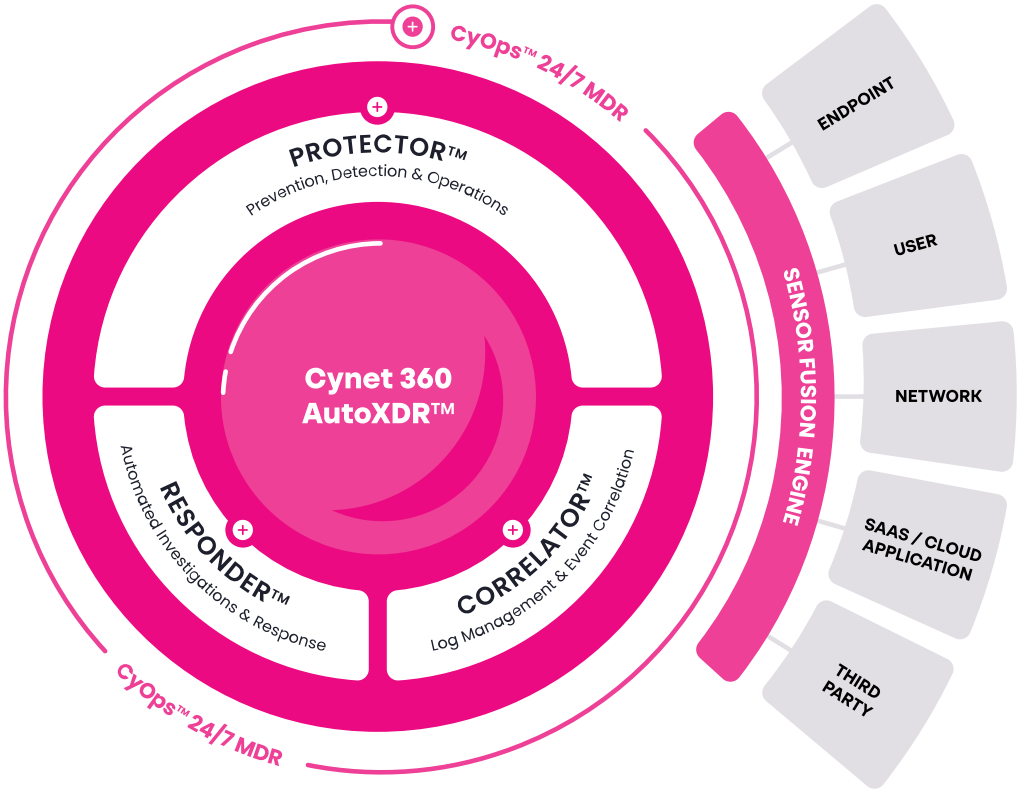
Summary and malware analysis reports

We provide you with all the reports you need, including an executive-level summary report with an overview of any malware analysis performed. Companies typically serve this report to their C-board and legal teams and some companies further share this report with their cyber-insurance company. Cynet provides additional, detailed technical reports that your security and IT teams can use to bolster your company's protections.

About Us

Cynet's end-to-end, natively automated XDR platform, backed by a 24/7 MDR service was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size or skills.

Cynet delivers the prevention and detection capabilities of EPP, EDR, NDR, Deception, UBA rules and CSPM, together with alert and activity correlation and extensive response automation capabilities.



Our vision is to enable security teams to put their cybersecurity on autopilot and focus their limited resources on managing security rather than operating it.

Bring sanity back to cybersecurity with a fresh approach that makes protecting your organization easy and stress-less.

Learn More