



Real Cybersecurity



# CYE OFFERING FOR CRISIS MANAGEMENT & INCIDENT RESPONSE

**CYE Incident Response** offers 24/7 support for ensuring successful containment, remediation and recovery of a breach, reducing response time and minimizing business operational impact.

As more national-level cyber capabilities and hacking tools become accessible to the public, cyber-attacks against commercial organizations have become more sophisticated. The dearth of experts with the national-grade experience, the methodologies and the technologies to combat cyber incidents has left organizations and critical infrastructure vulnerable to a host of attacks. These attacks include denial of service, intellectual property theft, financial and health data breaches, insider threats and identity theft

CYE's focus is to minimize the incidents impact, while ensuring rapid recovery and business continuity.

The team's success is built on real-time knowledge regarding new attack vectors and fingerprints, sophisticated technologies to eradicate breaches and comprehensive expertise to recover systems and mitigate future risks.

CYE's 24/7 response teams include national-level security experts with vast expertise in rapidly investigating and mitigating attacks of any scale on any sophistication level in a multitude of different industries.

## CYE's Comprehensive incident management includes:

End-to-end breach response and containment to avoid additional damage

Assessment of damage and risk scoping as well as the business impact

Use of sophisticated threat hunting tools and methodologies

Prevention activities to harden the organization against future incidents

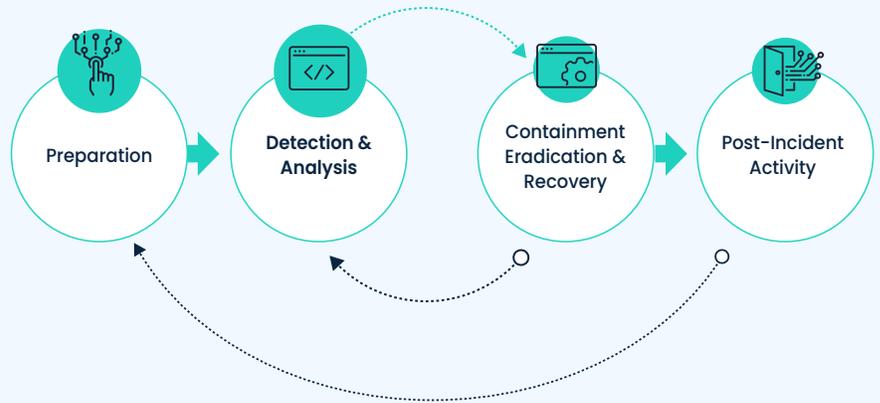
Training and guiding the stakeholders, employees, board members, suppliers and so on.

Providing strategic communication to protect organizational reputation and minimize legal liabilities and risks

Post event mitigation planning and a long-term architectural improvement



CYE's team has vast experience in handling security incidents all over the world. Due to the nature of those activities and stringent confidentiality agreements, CYE cannot refer you to specific customers that have used the incident management services.



### Incident Response services

This service provides customers with the ability to reduce the risk of cyberattacks, stop cyberattacks in their preliminary stages (before any actual damage has occurred), and mitigate cyberattacks quickly and professionally in real time. The actual Incident Response consists of several activities including IR Readiness (preparation), Threat identification, Threat Containment, Eradication, and Immediate Recovery.

### IR readiness

The IR Readiness service is utilized during peacetime. It includes scoping and providing a detailed analysis of customers' security architectures. Following the study, CYE then provides customers with detailed reports and recommendations for security architecture hardening in order to prevent future cybersecurity incidents. CYE then aids in the company's process of building an incident response plan, readiness process, and procedures for the security team and the organization to follow should another attack occur.

### Threat Hunting

The 'Find Evil' service includes the continuous proactive analysis conducted by CYE's experts to find malicious and clandestine activity in customer environments. The service is based on Data Forensics but includes threat hunting, threat Intelligence and deep web analysis. The service has a dependency – CYE agents must be installed in the customer network.

### Incident Response Management

The Incident Response consists of several activities. Since incidents frequently lead to a crisis, the response to an incident should start as soon as possible. Therefore, although some incidents require the CYE team to be onsite, the first mitigation steps start remotely to reduce the gap between incident start time and mitigation start time.

### Post IR improvement

This activity is based on analyzing the attackers attack route and is provided as the last step of the Incident Response. The activity includes conducting a detailed analysis of the customer's environment. The goal is to provide a plan for long-term architectural improvement.

### VIP Incident Response

The VIP incident is any action that leads to a situation where a VIP person or asset is jeopardized. These incidents may include extortion – threatening a VIP or a member of their family, discovering bugs or other evidence of threatening actions, finding leaked information about an intention of threatening a VIP or a VIP asset. The CYE team commits to being ready on-site to mitigate the actual incident within hours (4 hours remotely and 72 hours (about 3 days) on-site) with services consisting of on-site, physical, and cyber protection.

### Awareness training

The organization needs to be trained and able to fully understand the incident response plan as well as the roles and responsibilities in case of an incident. CYE teams provide personal guidance and best practices guidelines in order to prevent incidents and prepare an effective response if an incident occurs.

## About CYE

CYE brings a fact-based approach to organizational cyber defense, managing real business risks and optimizing the cybersecurity investment. CYE serves as a trusted advisor to medium-sized and Fortune 500 companies in multiple industries around the world.

CYE combines technology, domain experts, and community knowledge to support security decision makers with clear visibility to their real business risks and security posture.



Founded  
2012



Offices  
Israel (HQ), US, Europe



Investors  
EQT, 83North

## Fortune 5000 global customers in the following sectors

- Financial
- Technology
- Energy & Utilities
- Retail
- Healthcare
- Pharmaceuticals
- Manufacturing



CYE provides the means to proactively measure and ameliorate our overall security posture. Its AI-based prescriptive engine model enables us to truly optimize our cyber-security investment and Roi.

CISO at a F500 Company



## Trusted by



PHILIPS

DAIMLER

Microsoft

ZURICH

IEQT

Alcon



NOVARTIS



UBS

Honeywell