



CYBERGYM IT Incident Response Services

Identifying and containing threats; preventing damage to your organization

As well as improving the cyber-defense skills of your workforce through training and arena activities, CYBERGYM also provides value-added security services, including in the field of IT Incident Response. We invite you to leverage the unique skillset of our experts, to enhance your organization's overall cybersecurity posture and maturity.

Keeping your critical data, assets and systems safe from cyberattack requires continuous monitoring and analysis. If your organization is threatened by a cybersecurity breach, or is hit by an actual cyber incident, a concrete, coordinated response is demanded. Once the threat has been averted, and the resulting damage has been minimized and controlled, lessons must be learned and measures must be put into place, to prevent the occurrence of a future incident. All this is the responsibility of your IT Incident Response Team.

In today's climate of increasingly-complex cyberwarfare, the growing skills gap and shortage of trained cybersecurity professionals is reaching crisis point. You need an immediate, professional, structured approach to dealing effectively with any critical cyber threat or incident, and that's just what the CYBERGYM IT Incident Response Team of hackers and forensics experts delivers.

How we do it

Our IT Incident Response Team gives you the benefit of three distinct services operated and managed 24/7/365 by CYBERGYM's expert team

// **Pre-Incident Response:** Putting in place an incident response plan and ensuring that the initial steps are taken to facilitate an effective response. This involves:

- Identifying key roles and responsibilities within your IT & networking department, including who will liaise with media, law enforcement, insurance and C-suite personnel, as and when required
- Carrying out an initial vulnerability assessment/ penetration test (priced separately)
- Identifying critical network architecture/ critical assets/ single points of failure, and putting in place suitable protective measures, such as offsite backups
- Putting in place workplace continuity contingencies
- Ensuring C-suite/ executive buy-in
- Running table-top exercises and training (recommended)

// **Incident Response:** Delivering an actual response following suspicion or detection of a network breach, through relevant courses of action which may include:

- Forensic analysis, including identifying the threat, any loss of data/ data exfiltration, impact on your business processes, whether the threat is live/ ongoing
- Quarantine of infected systems/ endpoints/ assets
- Preservation of evidence
- Recovery & restoration of your network

// **Post-incident Response:** After the immediate threat or attack has been addressed and resolved, additional steps are taken to prevent future incidents. This involves:

- In-depth analysis of the attack, by studying preserved data, logs, etc
- Writing and delivering reports, covering details such as the method/ vector of the attack, its impact (including data and assets that have been lost), and our recommendations for securing your organization against future breaches
- Conducting follow-up briefings, monitoring and training

What to expect from CYBERGYM's IT Incident Response Service

// **Professional personnel** - our personnel are trained to analyze and correlate events in different organizational environments – from IT to critical infrastructure - and undergo ongoing professional development.

// **Experience** - our expert team has proven battlefield experience in detecting, mitigating and recovering from different attacks, in both IT and operational environments.

// **Out-of-the-box thinking** - our experts have knowledge of both attacking and protecting critical infrastructure, so they can thoroughly prepare your organization according to your cyber threat model.

// **Tailored solutions** - working together with you, we will identify your specific needs and apply the individualized tools required to meet them.

About CYBERGYM

CYBERGYM provides tailored cyber-training solutions to organizations around the world. With the most relevant threat model and a technological environment configured to your technological setup, we make sure your people gain the experience they need, as individuals and as a team. CYBERGYM further qualifies your general workforce and executives, delivering an all-inclusive, organization-wide solution.

Founded in 2013 by experienced veterans of Israel's prestigious intelligence organizations, CYBERGYM gives you peace of mind knowing that your teams are always ready, and cyber investments are maximized.

