CYBERMOAT
Redefining Cyber Security Defense

Cyber Moat is a leading Cyber Security Risk Management Consultancy firm that provides professional creative solutions and cyber security training to information security problems for global clients.

Our services include:
Cyber Program Assessment and implementation, Business Continuity Plan (BCP), Incident Response Plan (IRP), Incident Response Team (IRT), Digital Forensics and Incident Response (DFIR), Cyber Warfare and Table Top Training (TTT) Cyber Security Compliance Assessments and preparation for audits like GDPR, ISO 27001 and Ongoing Penetration Testing.

We have based our services on two cyber security pillars:

Readiness services –focused on cross organizational hyper realistic training and crisis simulation, these are structured to strengthen your cyber reflex.

Resilience services– focused on the wider aspect of reacting and recovering from a cyber security incident, these services are structured to strengthen and preserve your business advantage during and after a crisis.

We specialize in building and operating hyper-realistic Cyber Security Training Arenas for academics and enterprise clients. Among our clients you may find major financial institutes and leading companies around the world. We offer unique knowledge in the technology and methodology, as well as out-of-the-box ingenuity and a thorough grasp of the operational patterns of hackers.

Our company is led by a team of elite Cyber Security professionals, who are among the world's pioneers in information security. Each of them has vast experience in the field and the highest level of expertise in developing and implementing Cyber Security.

Our professional team have extensive experience working with different types of enterprises in varied industries and with a variety of infrastructures and systems. Over the past 20 years our experts have experienced real life cyber crisis and helped organizations from different sectors to resist and respond to single and multiple events. We have witnessed the change in cyber-attack landscape and technology, and through CyberMoat we react.

You can experience the right training for you, by THE experts who train HSBC, Millennium bank, Israeli cyber units, IL prime minister office, critical infrastructure and many more like: Coca Cola, Carlsberg, Philips, Roche, Israel Electric Company, HSBC, Millennium Bank, 8200 Intelligent Units, Tel Aviv City, Teva, Roche, Mazor Robotics, countries in Europe, critical infrastructure and utilities companies.

For more information please call 305-240-7148 or email us at: erez@cybermoat.net

CYBERMOAT
Redefining Cyber Security Defense

Cyber Resilience – Its not about "IF", Its about "When & How"

CyberMoat Resilience services are designed to understand, examine and improve your cyber security in a structured and comprehensive method, with the right modularity and customization that allows you to focus on the business processes of your organization, and to allocate your resources to where they are needed most.

Our services include a range of established, existing and mature cyber security services, which are structured to take your cyber security strategy into fully supported hands on implementation

We have established Business Continuity Management (BCM) and Risk Services at the core of our cyber resilience approach, and have embedded our unique "Red Button" service to link the resilience pillar with the readiness pillar of CyberMoat main services.

These mature, well defined, and established Services include: Emergency Management (EM); Crisis (or Incident) Management (CM); Business Continuity Planning (BCP); IT Disaster Recovery Planning (IT DRP) or IT Service Continuity Management (IT SCM).

The cybermoat resilience implementation is structures to align with the leading standards and cyber relater regulatory requirements. The implementation deliverables allow your organization to establish the required assurance and cyber compliance.

We combine structured assesment based on the ISO 27001 and NIST definitions of over 20 domains of cybersecurity, with a bottom up assessment – from your SCADA and OT to your IT and Data Assets

Incident response	Architecture	Privacy	Access control	Policy & standards	3rd party
Governance	SDLC	Application security	Network security	Data protection	Preventive monitoring
Recovery	BCP	Security operations	Security strategy	Humint	Measure and report
Back up protocols	Awareness	DRP	Data classification	Change mgmt	Access mgmt

CYBERMOAT
Redefining Cyber Security Defense

Cyber Readiness -We believe that cyber training is crucial.

Our cyber readiness program is structured to create the best possible alignment between the current training that already exists in your organization, with the CyberMoat readiness training program.

The vast "hands on" experience of our team has led us to perfect our methods and to align them on 2 basic truths:

- **Response mechanisms will work only if they are part of your day to day** – we customize our training delivery to the existing scale, structure and objectives of your NAC, SOC, SIEM, IRT and IT DR teams or mechanisms. We understand the various challenges posed on these teams in different organizations, and we aim to minimize the disruption of your existing structures. Our goal is to ensure that the unique CyberMoat Training will be embedded into your day to day. Since we have witnessed its importance from first hand when responding to our clients' cyber incidents.

- **Training and testing cannot be performed "In Situ"**– we address the organization as a whole, knowing that a strong, precise and swift cyber response must be through alignment between the response strategy decision makers (senior mgmt.) And the hands on cyber fighters (IT teams & InfoSec teams). Our multi sector experience allows us to create a customized table top training for senior management, hands on training in our cyber range, and a combined boot camp structured to take your readiness to reality. One step ahead of your attacker.

Cybermoat's cyber readiness services include Table Top Training, hands on training, IRT Training, Board Of Directors Training, PR Training, IT DR Training, BCM Training, structuring of annual cyber training plan, GDPR training, ISO preparedness training and more.

CYBERMOAT READINESS PROGRAM

TABLE TOP C-LEVEL EXERCISE

- Table top training exercises (TTT) allows clients to evaluate their preparedness to respond to a cybersecurity incident by simulating a realistic tailormade and probable cyber security scenario specific to the client and their industry. The objectives of the exercise(s) are to pose a risk to the organization and evaluate key executives decision making capabilities during a crisis.

INCIDENT RESPONSE PLAN (IRP)

- Customer has already recognized the importance of having an incident response methodology as a vital part of its overall organizational security governance. Whilst an incident response policy was already formalized, detailed procedures are also required in order to provide detailed action items necessary to execute and support the overall policy. The procedures assist customer related teams to fully function throughout any security incident and improving the overall response level.
- The suggested project shall enable customer to convert the high-level policy into the daily tasks derived from it.

INCIDENT RESPONSE TEAM (IRT)

- An incident response team or emergency response team (ERT) is a group of people who prepare for and respond to any emergency incident, such as a natural disaster or an interruption of business operations. Incident response teams are common in public service organizations as well as in organizations. This team is generally composed of specific members designated before an incident occurs, although under certain circumstances the team may be an ad hoc group of willing volunteers.
- Incident response team members ideally are trained and prepared to fulfill the roles required by the specific situation (for example, to serve as incident commander in the event of a large-scale public emergency). As the size of an incident grows, and as more resources are drawn into the event, the command of the situation may shift through several phases. In a small-scale event, usually only a volunteer or ad hoc team may respond. In events, both large and small, both specific member and ad hoc teams may work jointly in a unified command system. Individual team members can be trained in various aspects of the response, either be it medical assistance/first aid, hazardous material spills, hostage situations, information systems attacks or disaster relief. Ideally the team has already defined a protocol or set of actions to perform to mitigate the negative effects of the incident.

CYBER MOAT PENETRATION TESTING (PT)

Verify that your security controls are in place and functioning.

Whether you need to prove regulatory compliance, satisfy a request from senior management, or demonstrate security maturity to your clients, a penetration test is a great mechanism to accomplish your goals.

WHAT IS A PENETRATION TEST?

Penetration testing, aka "ethical hacking," is a procedure to evaluate the security of your entire network infrastructure, i.e. computer systems, networks, users, and applications. It simulates an attack from malicious outsiders (unauthorized) and/or malicious insiders (authorized) to identify attack vectors, vulnerabilities and control weaknesses. It implements a variety of manual techniques supported by automated tools and looks to exploit known and unknown vulnerabilities.

Our security offensive experts identify specific weaknesses in an organization's security operation. By safely attempting to discover and exploit the vulnerabilities of your network, applications, people, and more, we find the "leaks" in your system before damage occurs.

WHAT DOES PENETRATION TESTING, TEST?

- **NETWORKS**
- **PHYSICAL SECURITY**
- **WIRELESS LOCAL AREA NETWORK (WLAN)**
- **PEOPLE (SOCIAL ENGINEERING)**
- **DATABASES**
- **WEB APPLICATIONS**
- **APPLICATIONS**
- **RED TEAMS**
- **CLOUD SECURITY**
- **AND MORE!**

DO YOU REALLY NEED A PENETRATION TEST?

Penetration testing is often confused with another type of technical security testing, namely: "vulnerability assessments." They couldn't be more different from each other.

The information obtained, the effort required, and the financial costs incurred are very different between these two assessments.

So, make sure you know which one you need, and if you're unsure about your particular assessment needs, please contact us.

WE'LL BE HAPPY TO ASSIST YOU!