CYBERGYM Security Operations Centre (SOC) as a Service

Our worldwide experts, monitoring and securing your organization

At CYBERGYM, your cybersecurity is very much our business. To complement our comprehensive range of live cyber training and true-to-life qualification and certification solutions, we also offer a selection of value-added services, including SOC as a Service. Now you can leave it to our experts to identify, mitigate and collect forensics for any cyber incident, while minimizing escalation and brand damage.

Every day cyberattacks are growing in frequency and severity; organizations, governments and providers of critical services recognize that it's no longer enough for them to rely on technology and internal teams alone. Many are implementing a dedicated, in-house Security Operations Centre (SOC), hiring skilled security personnel to carry out real-time analysis of security data from different systems, and provide a holistic view of the organization's security status detecting suspicious activities, unauthorized access, abnormal behaviour or patterns, and potential attacks.

But establishing a SOC presents its challenges, including the scarcity of professional personnel with proven experience, expertise and knowledge; the cost and time required for initial and ongoing staff training; designing effective data collection and correlation methodologies; and the lead time required until the SOC is up and running. CYBERGYM's SOC as a Service solution offers a cost-effective, reliable alternative to building your own SOC.

How we do it

Our comprehensive SOC as a Service solution gives you the benefits of quick implementation and operation of a SOC, operated and managed 24/7/365 by CYBERGYM's expert team

// Designing, with you, the data collection methodologies to be implemented, including the systems that will be monitored, the events that will prompt an alert and routine operations (such as updates etc.) that will be carried out, and implementing the necessary technology tools

// Designing, with you, the cyber-threat model according to which the SIEM system optimization will be determined, and implementing the required SIEM configuration

// Monitoring, detecting and analyzing your organization's security events, in real time

// Safely managing data collected from your organization, including encrypting and sending it to CYBERGYM's SIEM system, where there is a log correlation among various security systems

// Continuously adapting the data collection methodology and system configuration

// Providing access to in-depth reports and dashboards, enabling you to keep your board members and executives informed

SOC as a Service levels

CYBERGYM offers three levels of SOC-as-a-Service:

// **SOC as a Service Essentials**

- 24x7 monitoring.
- Collector software installed in your own environment.
- 5 admin accounts.
- Minimum of 8 collectors

// **SOC as a Service Gold**

- Ongoing optimization of the SIEM system to your evolving cyber-threat model
- 24x7 monitoring
- Business hours access to CYBERGYM security team for incident investigation
- Collector software installed in your environment
- 10 admin accounts
- Access to CYBERGYM's additional services at a discounted rate
- Minimum of 10 collectors

// **SOC as a Service Platinum**

- 2-way exchange of security and threat information between your environment and thousands of other sites around the world
- 24x7 monitoring
- Business hours access to a dedicated CYBERGYM security engineer
- Collector software installed in your environment
- 10 admin accounts
- Annual Vulnerability Assessment of your IT environment
- Access to CYBERGYM's additional services at a discounted rate
- Minimum of 12 collectors

What to expect from CYBERGYM's SOC as a 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.
- **Knowledge** - we have extensive knowhow in instructing and mentoring training sessions and cyber-event management in a variety of sectors.
- **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.
- **Proven methodologies** - we get your SOC up and running quickly using our expertise in the design and implementation of data collection and correlation methodologies to protect your organization.
- **Tailored solutions** - working together with you, we will identify your specific needs and apply the individualized tools required to meet them.
- **CYBERGYM's revolutionary Cyberwarfare Arena** - the only platform that facilitates real-life simulations of cyber warfare.

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.