KRESTON
EZRA YEHUDA-ROZENBLUM
CONSULTING, CONTROL & RISK MANAGEMENT

Anti-virus and firewall are not enough...

The Most Effective Cybersecurity Solution is 24/7 Monitoring & Incident Response

Our partner at the Tel Aviv Security Operations Center ("SOC") has a team of security experts with real-world experience stemming from tactical and technological units of law enforcement and the military, specializing in cyber-defense experts in security architecture, cyber-hacking and cracking, advanced forensics, malware analysis, and investigation, designed for enterprises and governments, in fields as varied as finance through telecommunications and energy to critical infrastructure spheres.

The SOC is operated by elite Israeli cybersecurity experts, providing monitoring, detection and incident response by an experienced incidence-response team in real-time that is proactive and knows exactly how to proceed the moment a breach is identified.

The SOC is technology-agnostic, working with all of the leading systems, and enhancing an organization's security by adding capabilities without the need for additional technology.

Optional Internal or Local SOC Buildout and Cybersecurity Training

For clients that wish to build and operate their own internal SOC, KRESTON IL can provide guidance starting from the design phase and throughout the operations and training phases. The Tel Aviv SOC can also provide back-up to an internal SOC or, alternatively, a local SOC, to handle escalations and incident response, and can also take over monitoring functions on nights, weekends, and holidays when staff are otherwise unavailable.

On-Demand Emergency Incident Response

Even if an organization is not monitored by our SOC contractually, and an attack occurs or a breach is suspected, KRESTON IL can provide (subject to availability) incident response globally.

KRESTON
EZRA YEHUDA-ROZENBLUM
CONSULTING, CONTROL & RISK MANAGEMENT

Hacking Simulations and Assessments that Strengthen Company IT / OT

At the request of CEOs, Boards of Directors, CTO/CIOs, and CISOs, the Tel Aviv SOC's Red Team legally hacked over 100 multinational corporations, including many Fortune 100/500 companies, that wanted to know how well-protected they were in actuality, not only theoretically, even though most of the companies participating have implemented security systems and measures and are compliant with various security standards.

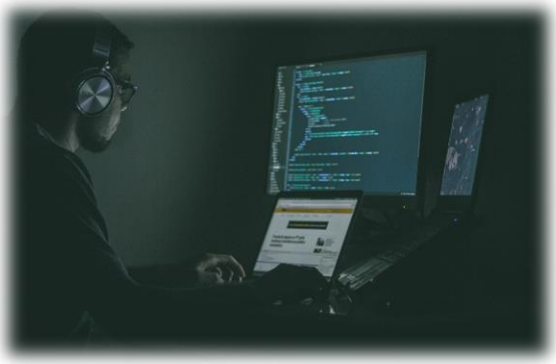
After conducting over 100 hacking simulations, offensive assessments, and dozens of monitoring gap-analyses, in almost all cases, the SOC's Red Team was neither timely detected, nor effectively blocked, nor identified by the client's Security Operations Center.

Advanced Hacking Simulations

Only by challenging security at the hands of qualified and experienced personnel can companies truly identify the gaps and vulnerabilities in organizational security.

The SOC brings together professional hackers to create the most efficient and realistic hacking simulations. The hacking simulations are specifically designed to mimic a realistic attack scenario and identify security gaps, provide practical recommendations, and actionable steps for remediation.

This exercise simulates the actions of a real hacking team intent on executing malicious actions from infiltration and theft through sabotage. It is executed on an organizational level and can simulate anything from a low-level random attack to a well-funded, highly targeted attack.



Cyber Readiness Assessment

The Cybersecurity Readiness Assessment is based on a real attacker's approach, whereby an elite team of experts, guided by practical defense methodology, investigates the organization's IT/OT security posture, consisting of security systems and software, security teams, working procedures, monitoring and response capabilities, as well as many other elements.

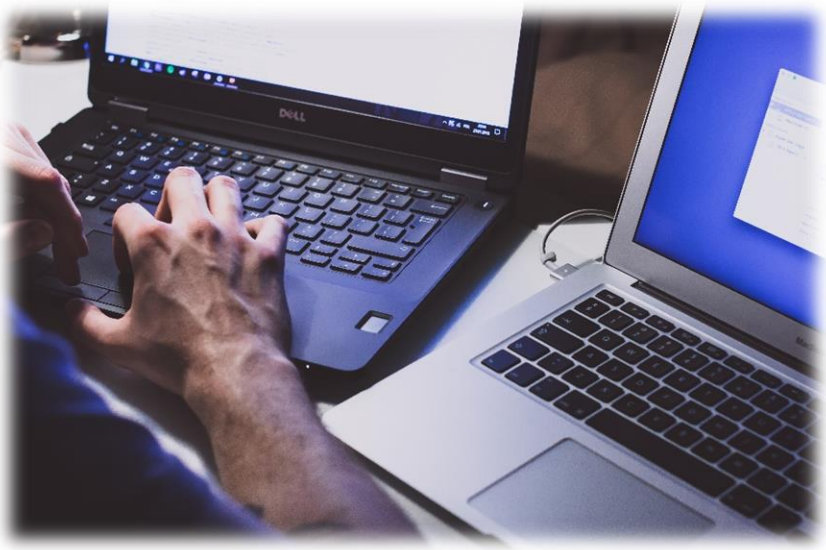
The assessment will generate a detailed report, outlining a clear breakdown of the actual cyber defense capabilities of the organization, specifying the gaps between theoretical measures in place and actual capabilities, and providing insights of overall organizational preparedness for attacks, all while helping prioritize security tasks and validating a security roadmap.

KRESTON
EZRA YEHUDA-ROZENBLUM
CONSULTING, CONTROL & RISK MANAGEMENT

Anti-Phishing – the ultimate email defense

Nearly every cyber-attack, breach, or 'CEO Fraud' situation, employs email exploitation. The leading Anti-Phishing platform promoted by KRESTON IL can detect and stop such breaches. The world's first phishing prevention, detection and response platform has been especially designed to address the advanced phishing threats of today.

The difference between being protected by a team of experts or not, and taking measures before a breach, is the difference between a thriving business or devastating consequences…



OUR PARTNERS:

CYBERHAT
proactive cyber defense

CYREBRO

IRONSCALES
World's 1st *Automated Phishing* Prevention, Detection & Response

CYREBRO Core