Israel Electric

SOPHIC PRO

TOP LEVEL AWARENESS WORKSHOP- CYBER-ATTACK AND RECOVERY SCENARIO SIMULATION FOR C-LEVEL

"A DAY IN THE LIFE OF A CISO"

One of the key elements impacting the organization's cyber sturdiness is the lack of understanding by the most important individuals - the decision makers.
In Israel Electric Corporation's (IEC) experience, based on analysis of hundreds of events involving cyber risks, this is one of the most common factors of cyber defense and resilience failures. This workshop is designed as an active simulation game, exposing participants to real dilemmas and solutions based on IEC's vast experience, while providing them with a rough estimation of the organization's cyber defense quality as presented by the participants.

Main Goals

- Leveraging decision-makers' understanding of the cyber phenomena.
- To be in the cockpit during the reality-like cyber crisis: to experience the differences compared to other types of crisis.
- To reconsider the management intense support for the cyber organizational activities.
- To better understand the meaning of a balanced cyber organization

Values to participant

- Increasing cyber awareness across the organization
- Understanding and avoiding cyber management pitfalls
- Developing practical understanding of cyber decision's main dilemmas
- Creation of efficient 'cyber' communication

Outcomes

- Gaps report mitigation plans
- Key performance indicators for measurement of the organization's cyber quality
- Presentation of session & materials
- Follow-up activities report

Target Audience	Number of Participants	Duration
▪ C-level Management ▪ High-level executives ▪ Ministries management ▪ Regulatory bodies ▪ Members of the board	Up to 15	5 Hours working

Israel Electric

"ANATOMY OF ICS CYBER-ATTACK"

This workshop focuses on providing information on practical steps taken by a hacker in the process of a cyber-attack against ICS systems and Networks. The participants will experience all of the hacking stages via real-life demonstrations of the ICS reconnaissance stage on SCADA systems and personnel through the Shodan and Google Hacking search engines .The participants will also learn about Active Cyber Defense Cycle and what are the basic cybersecurity steps needed to reduce exploitable Weaknesses and Attacks against ICS Systems.

Main Goals
- Gain deeper insight into professional cyber terms;
- Identifying some of the current techniques and tools used by a hacker;
- Describing and identifying basic principles for active cyber defense;
- Applying steps and procedures for a variety of situations;

Values to participant
- Increase of professional and cyber term understanding
- Understand real life threats on ICS systems and actions to reduce exposure.
- Understanding and analyzing the OT/IT dilemma.
- Detailed knowledge of attackers' techniques and behaviors.

Outcomes
- Summary report of the workshop discussions, finding and materials.
- Tools to track threats, vulnerabilities and attacks vectors on ICS.

Target Audience	Number of Participants	Duration
▪ Operation managers ▪ Cyber managers ▪ IT managers	Up to 15	3 Days working

While tools, technology and tactics change, all cyber- attacks have one thing in common, they're all human- driven.

Knowing the motivations and tendencies behind your cyber adversaries can help you make the right strategic decisions and investments to better protect your organization

About Sophic
The Sophic suite of cyber security solutions has been created and proven by the Israel Electric Corporation - one of Israel's leading critical infrastructure organizations solely responsible for supplying electricity to the whole country. Operating in a very challenging geopolitical environment, we are also one of the most targeted organizations in the world, having experienced our first cyberattack 25 years ago. This dubious distinction has driven our engineers, together with cyber security specialists from elite units in the Israel Defense Forces, to leverage the most cutting-edge technology to ensure we stay one step ahead of the threats we face.

Contact us to learn more how our solutions can benefit your organization:
iecmarketing@iec.co.il | +972-072-3433813