SOPHIC PRO

RAPID CYBER MATURITY ASSESSMENT

CybergymIEC

Your challenge

In a world in which cyber threats grow and become more insidious every day, organizations of all sizes, across all industries, must understand their risk and take urgent action to protect themselves - especially in the critical infrastructure sector. But how do you achieve true insight into the cyber maturity of your organization so that you can identify and close any gaps on the one hand, while avoiding activities that do not contribute to your cyber sturdiness on the other?

To do this, you need to 'know yourself', meaning you have to understand all the cyber and operations aspects of your company.

Typically, cyber assessments are carried out every few years in a long and expensive process that can take several months. The report delivered at the end is usually just a snapshot of an organization's cyber picture, which is only relevant when the actual assessment occurs. What's more, results are likely to be presented as a detailed list of gaps, requiring the organization to translate recommendations into a roadmap of practical actions they can take to improve their cyber posture, including the resources and finance required. After that, limited tools and methods are available to enable continuous measuring and monitoring of progress towards achieving the desired level of cyber maturity.

Our solution

Sophic's Rapid Cyber Maturity Assessment (RCMA) is a unique model and methodology based on the Israel Electric Corporation's 25 years of experience as one of the most targeted organizations in the world.

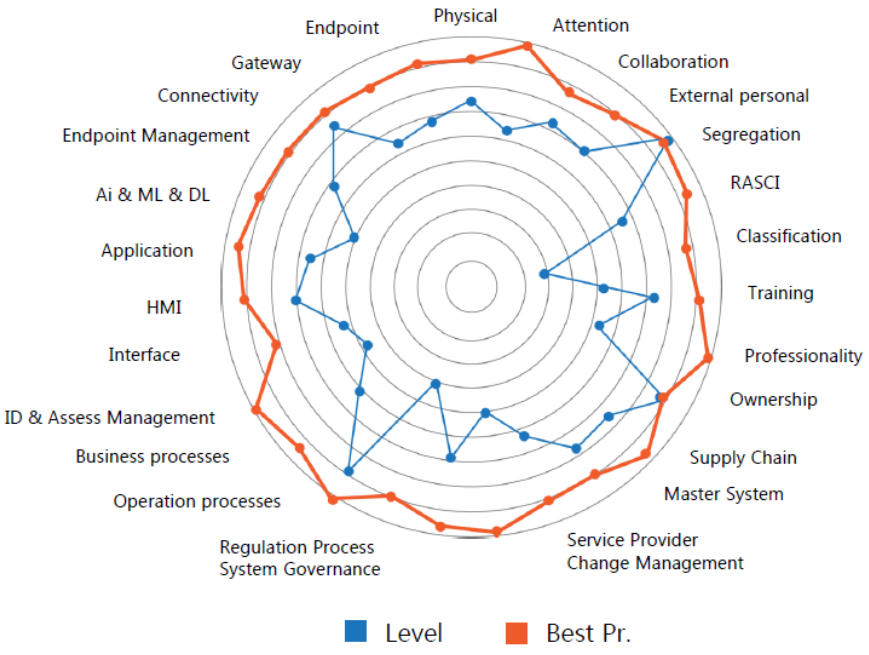
It provides a comprehensive, accurate, focused, and practical understanding of your organization's cyber posture and maturity level - and what you need to do to improve it. Customized to your specific environment, it enables you to optimize and balance your business risk appetite, operational needs, and cyber investments.

Systematic

Our assessment process begins with extensive preparation. As well as carrying out our research, we ask you to complete a questionnaire so that we can start to understand your organization and the technology, policies, processes, and procedures you already have in place.

Efficient

Carried out in just 7-12 weeks, our fast and efficient assessment uses a unique methodology to analyze selected data according to hundreds of control indicators, and internal and external information results are expressed as quantitative indices, enabling us to identify gaps and pitfalls that leave your organization vulnerable to cyberattack. In the meantime, you carry on your business as usual.



RCMA output showing the customer's current level of maturity (blue) v.s best practice (red), identifying gaps to be addressed in the roadmap

Actionable

Having given you a clear picture of your organization's cyber situation, we work with you to set goals for improving it. Creating a prioritized remediation plan, we recommend clear action points to implement, with measurable KPIs based on industry best practices – including NIST, NERC, ISO, ANSI, C2M2, INCD, GDPR, SABSA, HIPAA - and IEC's own battle-proven methodology.

In the plan, we include an estimate of the resources that will be required, address critical gaps and the most significant weaknesses, and make sure every dollar counts. We will advise you on how to eliminate activities, tools, and systems not contributing to the cyber maturity of your organization.

Ongoing

No organization works in a static environment - business objectives change, and your risk environment evolves. To ensure the action you take to improve your cyber posture remains relevant and gets you to the cyber maturity level you're aiming for, we offer a unique Continuous Cyber Maturity Support (C-RCMA) program in addition to the RCMA. On an annual basis, we support you in implementing your cyber roadmap, monitoring and measuring quarterly progress and KPIs, and identifying any roadblocks. We provide ongoing updates of maturity frameworks and methodologies and present any relevant new findings. Then, once a year, we re-assess your maturity level with an updated RCMA, producing a new report that reflects the most up-to-date situation, both in terms of the latest external and internal changes that influence your organization and the program.

Added value

We offer a selection of optional add-ons to the RCMA and C-RCMA described above.

- **Deep cyber organization quality -** a full cyber organization assessment based on unique methodology and tools, and 16 deterministic KPIs that check the ecosystems of the organization: internal, external, formal, communication, and more.
- **Vulnerability scanning** – test your IT & OT systems for access points that attackers could exploit.
- **Deep threat analysis** (DTA) – our expert DTA system uncovers internal and external threats to your organization that other solutions cannot detect.

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 about how Sophic can redefine your organization's cyber strategy and solutions.

www.cybergymIEC.com
sophic@iecyber.co.il

972-52-399-7965
972-76-863-4588