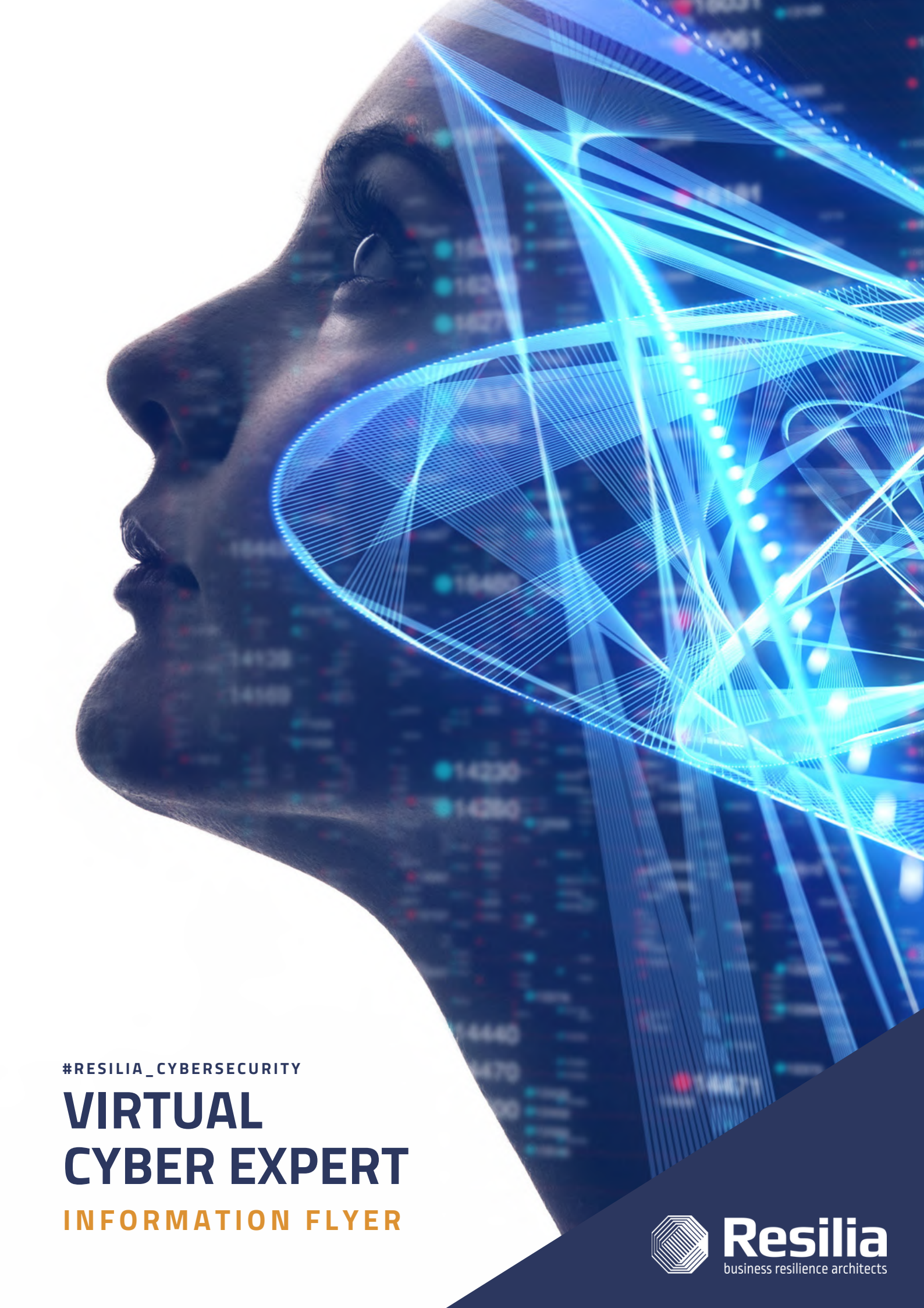


#RESILIA_CYBERSECURITY

VIRTUAL CYBER EXPERT

INFORMATION FLYER

Resilia
business resilience architects

Resilia

Virtual Cyber Expert (VCISO)

is a service for companies that want to comprehensively and conveniently manage cybersecurity and protect their organizations against cyber threats.

The service combines the competences and experience of a team of cybersecurity experts with advanced technologies.

Thanks to VCISO, you gain comprehensive support in a complex processes that you don’t need to know about!

Why the Virtual Cyber Expert service is worth using:

You gain a guarantee of the effectiveness of cybersecurity solutions implemented in three areas: formal and procedural, technological and organizational.

You can be sure that **your organization is secured and protected in accordance with the latest level of knowledge** and using the best tools.

You receive **full support from a team of cybersecurity experts**.

You minimize the costs associated with employing, maintaining and training a team of employees responsible in your organization for cybersecurity.

You reduce the costs associated with the purchase of advanced technologies supporting cybersecurity management:

- monitoring of IT systems / applications / infrastructure,
- scanning systems / applications / IT infrastructure to detect vulnerabilities,
- conducting automatic security test,
- conducting social engineering tests (phishing, smishing and vishing campaigns).

You save time that you can use for the development of core services in your company.

You don't have to constantly check whether **you operate in accordance with the current cybersecurity law**, guideliness and best practices.

You can count on our availability, **flexibility and speed of action**.

Resilia

What do you get as part of our service?

- **A dedicated team of specialists** supporting your organization's cybersecurity management process in all dimensions: Blue, Red and Purple Teaming.
- **Cybersecurity monitoring** of IT systems / apllications / infrastructure using advanced tools.
- **Analysis of events** in IT systems / applications / infrastructure.
- **Vulnerability detection service**.
- Ongoing **support in the management of identified vulnerabilities**.
- Periodic **automatic security tests** of IT systems / applications / infrastructure.

every 3rd company

has struggled with security incidents last year

According to the #CyberMadeInPoland report (published in 2021)

- Ongoing **response to cybersecurity incidents** and support in their handling.
- **Support in developing a cybersecurity awareness program** among employees.
- Cybersecurity **trainings**.
- Periodic **social engineering tests**.
- Handling **correspondence with external stakeholders** concerning cybersecurity issues.

Resilia

Resilia

What does a dedicated VCISO?

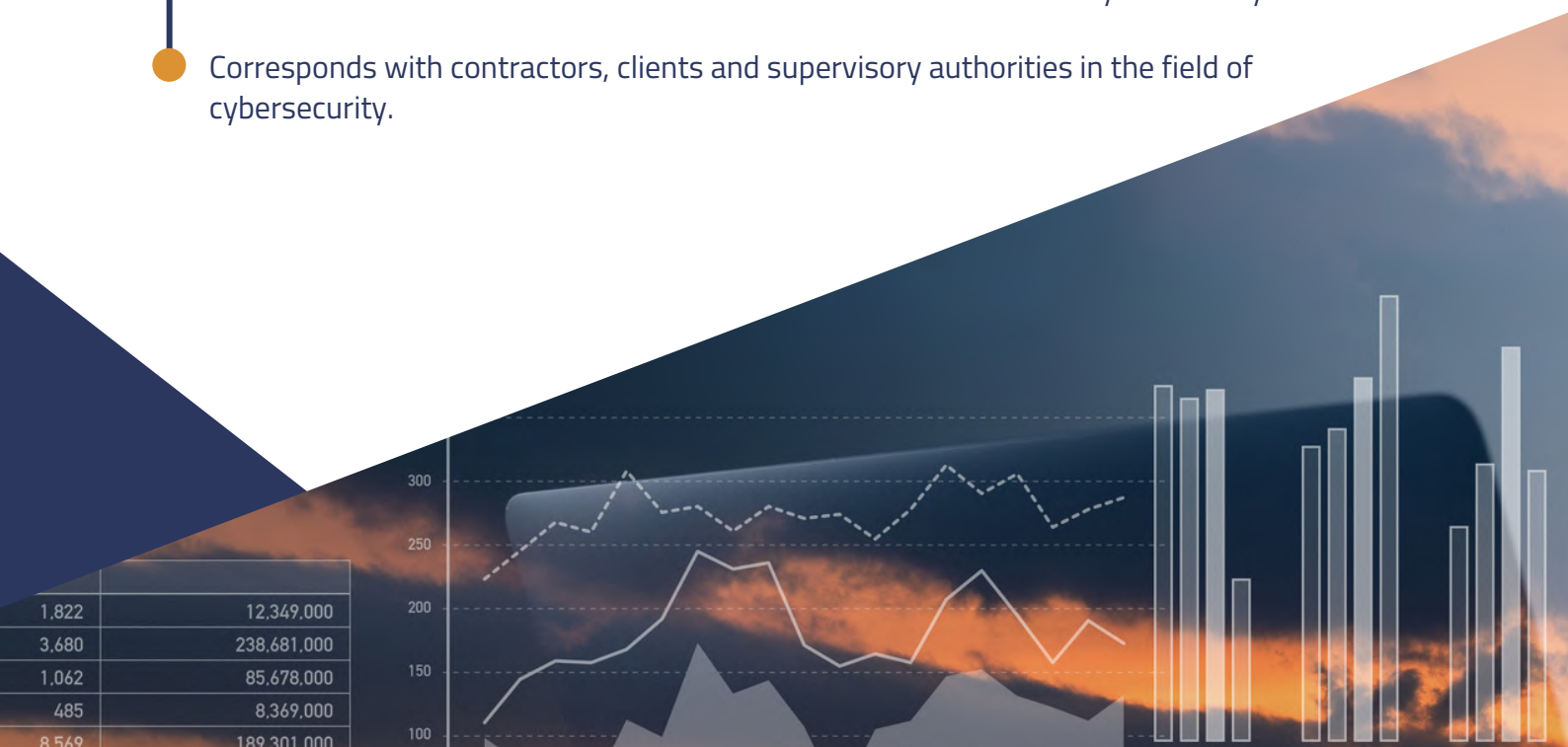
Depending on the chosen package of services, Virtual Cyber Expert:

- Conducts an assessment of the organization cybersecurity maturity at the formal-procedural, technological and organizational level based on international standards and frameworks in the field of cybersecurity and information security*.
- Conducts an assessment of the level of cybersecurity awareness among employees.
- Verifies identified cybersecurity threats.
- Prepares an action plan aimed at the optimal increase of the organization cybersecurity level based on international standards and frameworks, national regulations and best practices**.
- Updates and develops cybersecurity management procedures in connection with the existing documentation in the field of information security / IT / personal data protection.
- Monitors changes in cybersecurity legal requirements.
- Conducts a Business Impact Analysis (BIA) for key IT services.
- Supports the organization in the regular assessment of cybersecurity threats and keeps a register.
- Supports the organization in preparing and conducting of cybersecurity audits of critical suppliers.
- Provides support during external cybersecurity audits.
- Participates in a cybersecurity awareness program building.
- Conducts systematic cybersecurity training for employees.

** Among others: NIST Cybersecurity Framework, NIST SP 800-53, CIS Critical Security Controls for Effective Cyber Defense, ISO 27001.*

*** Among others: NIST Cybersecurity Framework, NIST SP 800-53, CIS Critical Security Controls for Effective Cyber Defense, ISO 27001, the Act of 5 July 2018 on the National Cybersecurity System.*

- Supports the organization in the selection, implementation and management of security systems based on tools such as: SIEM, SOAR, WAF, IPS, IDS, EDR, XDR, PIM, PAM, DAM, MFA, DLP (to the necessary extent, on the basis of decision after cybersecurity threats analysis).
- Performs social engineering tests (phishing, smishing, vishing campaigns) aimed at examining the level of cybersecurity awareness among employees / organization's resistance to cyber threats.
- Performs automatic security tests of IT systems / applications / infrastructure.
- Monitors IT systems / applications / infrastructure using SIEM / SOAR tools, etc.
- Performs an initial analysis of events.
- Performs periodic scans of IT systems / applications / infrastructure in order to detect vulnerabilities (data from EDR, NDR, XDR class tools).
- Supports the organization in handling incidents, keeps a register of incidents.
- Carries out activities such as REKON (monitoring cyber threats information with the use of open sources) and REKON Continuous (continuous monitoring of cyber threats in the network including closed forums, Deep and Dark Web).
- Performs Threat Hunting activities.
- Supports the organization in managing the identified technical and organizational vulnerabilities.
- Coordinates or carries out activities in the field of IT Forensic after cybersecurity incidents.
- Corresponds with contractors, clients and supervisory authorities in the field of cybersecurity.



Proposed subscription models

Governance Services

TASKS	PACKAGE TYPE		
	BASIC	MEDIUM	PRO
Support of a cybersecurity expert	✓	✓	✓
Assessment of the organization cybersecurity level – as-is	✓	✓	✓
Assessment of the cybersecurity awareness level among employees – as-is	✓	✓	✓
Review of identified cybersecurity threats	✓	✓	✓
Preparing an action plan to increase the level of cybersecurity of the organization	✓	✓	✓
Preparing a cybersecurity awareness program among employees	✓	✓	✓
Updating / developing cybersecurity procedures	✓	✓	✓
Monitoring compliance with internal procedures and legal provisions in the field of cybersecurity	✓	✓	✓
Support in the cyber threats assessment process		✓	✓
Keeping a cyberthreats register		✓	✓
Cybersecurity trainings		✓	✓
Support in preparing and conducting cybersecurity audits of critical suppliers		✓	✓
Support during external cybersecurity audits			✓
Support in a Business Impact Analysis (BIA) for key IT services			✓
Support in the selection, implementation and management of security systems and tools (to the necessary extent, on the basis of decisions after the cybersecurity threats analysis)			✓

There is a possibility of individual selection of the service package. Services can be provided in various time dimensions: from 0.25 FTE to 1 FTE with a contract concluded for a minimum of 6 months.

Resilia

Analytical and Technological Services

TASKS	PACKAGE TYPE		
	BASIC	MEDIUM	PRO
Support of a cybersecurity analyst	✓	✓	✓
Automatic monitoring of compliance with selected requirements, including KSC, KNF, NIST CSF, NIST 800-53	✓	✓	✓
REKON – monitoring cybersecurity threats in the network based on information from open sources	✓	✓	✓
Support in the process of identifying, prioritizing and managing vulnerabilities	✓	✓	✓
Support in handling cybersecurity incidents (including: preparation, identification,assessment, analysis of causes, repair / removal of effects)	✓	✓	✓
Conducting automatic security test		✓	✓
REKON Continuous - continuous monitoring of cyber threats in the network including closed forums, Deep and Dark Web		✓	✓
Social engineering tests, including phishing, smishing, vishing		✓	✓
Reporting of detected technical cybersecurity incidents		✓	✓
Monitoring logs from agreed systems / applications / elements of IT infrastructure using SIEM tools in a selected scope, including: availability of IT services, events, file integrity, configuration, user actions, leaks of e-mail addresses / passwords (compromising e-mail accounts) / other relevant data			✓
Preliminary event analysis			✓
Scanning systems / applications / IT infrastructure to vulnerabilities detect (data from EDR, NDR, XDR class tools)			✓
Support in hardening systems, including the selection of appropriate tools and configuration			✓
Implementation of Threat Hunting activities			✓
Support in the initial forensic analysis and selection of professional IT Forensic solutions			✓

There is a possibility of individual selection of the service package. Services can be provided in various time dimensions: from 0.25 FTE to 1 FTE with a contract concluded for a minimum of 6 months.

Resilia

Additional IT tools that might be added to VCISO subscription

SERVICE	DESCRIPTION
SOC Lite	Standard Package, handling 100 EPS (Event per Second), 10 data sources
VCISO Platform	SaaS platform for providing a remote VCISO service
Phishing & awareness	SaaS platform for social engineering tests and awareness training
Automatic security tests	Platform providing automatic tests of web applications and IT infrastructure
Digital Risk Protection	Platform providing Internet, Deep Web and Dark Web monitoring, for the purpose of preventive detection of cyber threats

Resilia

Interested in subscribing our VCISO?

If you have any questions – contact us!

kontakt@resilia.pl
+48 22 243 39 37

Paweł Dworucha
pdworucha@resilia.pl
+48 730 023 462

Marcin Marczewski
mmarczewski@resilia.pl
+ 48 602 727 215

www.resilia.pl/en/
facebook.com/resiliapl
linkedin.com/company/resilia/

#RESILIA_CYBERSECURITY