#RESILIA_CYBERSECURITY

WIRTUALNY CYBER EKSPERT

INFORMACJE O USŁUDZE

Resilia
architekci odporności biznesu

Resilia

Wirtualny Cyber Ekspert (VCISO)

to usługa dla firm, które chcą kompleksowo i wygodnie zarządzać cyberbezpieczeństwem oraz chronić swoje organizacje przed cyberzagrożeniami.

Usługa łączy kompetencje i doświadczenie zespołu ekspertów z zakresu cyberbezpieczeństwa z zaawansowanymi technologiami.

Dzięki VCISO zyskujesz wsparcie w skomplikowanych procesach, na których nie musisz się znać!

Dlaczego warto skorzystać z usługi Wirtualnego Cyber Eksperta?

Zyskujesz gwarancję skuteczności rozwiązań cyberbezpieczeństwa wdrażanych w trzech obszarach: formalno-proceduralnym, technologicznym i organizacyjnym.

Masz pewność, że Twoja **organizacja jest zabezpieczona i chroniona zgodnie z najnowszym poziomem wiedzy** oraz z wykorzystaniem zaawansowanych narzędzi.

Otrzymujesz pełne **wsparcie zespołu ekspertów** z zakresu cyberbezpieczeństwa.

Minimalizujesz koszty związane z zatrudnieniem, utrzymaniem i szkoleniem zespołu pracowników odpowiedzialnych w Twojej organizacji za cyberbezpieczeństwo.

Ograniczasz koszty związane z zakupem zaawansowanych technologii wspierających zarządzanie cyberbezpieczeństwem:

- monitorowanie systemów / aplikacji / infrastruktury IT,
- skanowanie systemów / aplikacji / infrastruktury IT w celu wykrywania podatności,
- przeprowadzanie automatycznych testów bezpieczeństwa,
- przeprowadzanie testów socjotechnicznych (kampanii phishingowych, smishingowych, vishingowych).

Oszczędzasz czas, który możesz przeznaczyć na rozwój podstawowej działalności Twojej firmy.

Nie musisz sam nieustannie kontrolować, czy **działasz zgodnie z aktualnymi przepisami prawa** z zakresu cyberbezpieczeństwa.

Możesz liczyć na naszą dostępność, **elastyczność i szybkość działania**.

Resilia

Co otrzymujesz w ramach współpracy?

- **Dedykowany zespół specjalistów** wspierający proces zarządzania cyberbezpieczeństwem Twojej organizacji we wszystkich wymiarach: Blue, Red i Purple Teaming.
- **Usługę monitorowania cyberbezpieczeństwa systemów / aplikacji / infrastruktury IT** z wykorzystaniem zaawansowanych narzędzi i analizy zdarzeń.
- **Usługę wykrywania podatności**.
- Bieżące **wsparcie w zarządzaniu zidentyfikowanymi podatnościami**.
- Cykliczne **automatyczne testy bezpieczeństwa** systemów / aplikacji / infrastruktury IT.

co 3. firma
zmagała się z naruszeniami bezpieczeństwa w ostatnim roku

wg raportu #CyberMadeInPoland „Cyberbezpieczeństwo polskich firm 2021"

- Bieżące **reagowanie na incydenty** w obszarze cyberbezpieczeństwa i wsparcie w ich obsłudze.
- **Wsparcie w opracowaniu programu podnoszenia świadomości cyberbezpieczeństwa** wśród pracowników.
- **Szkolenia** z zakresu cyberbezpieczeństwa.
- Cykliczne **testy socjotechniczne**.
- **Obsługę korespondencji** w zakresie cyberbezpieczeństwa z zewnętrznymi interesariuszami.

Resilia

Resilia

Czym zajmuje się dedykowany VCISO?

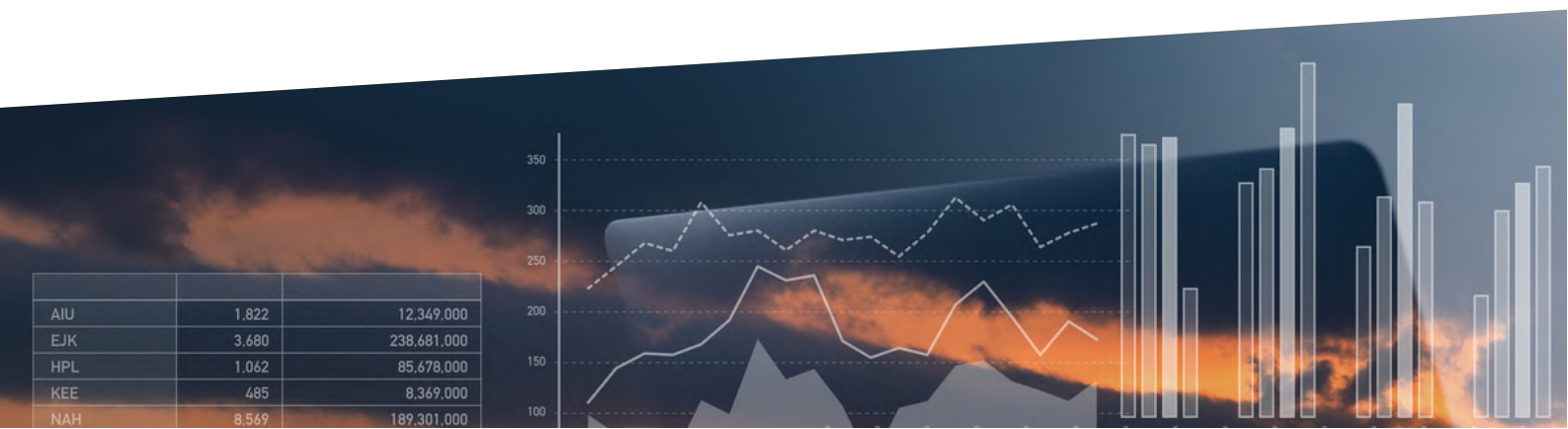
W zależności od wybranego pakietu usług Wirtualny Cyber Ekspert:

- Przeprowadza ocenę stanu cyberbezpieczeństwa organizacji as-is na poziomie formalno-proceduralnym, technologicznym i organizacyjnym w oparciu o międzynarodowe standardy i frameworki z zakresu cyberbezpieczeństwa i bezpieczeństwa informacji*.
- Przeprowadza ocenę poziomu świadomości cyberbezpieczeństwa as-is wśród pracowników.
- Weryfikuje zidentyfikowane zagrożenia cyberbezpieczeństwa.
- Opracowuje plan działań zmierzających do optymalnego podniesienia poziomu cyberbezpieczeństwa organizacji w oparciu o międzynarodowe standardy i frameworki, regulacje krajowe** oraz najlepsze praktyki.
- Aktualizuje i opracowuje procedury zarządzania cyberbezpieczeństwem w powiązaniu z istniejącą dokumentacją z zakresu bezpieczeństwa informacji / IT / ochrony danych osobowych.
- Monitoruje zmiany w wymaganiach prawnych z zakresu cyberbezpieczeństwa.
- Przeprowadza analizę BIA dla kluczowych usług IT (analizę wpływu przerwania ciągłości działania poszczególnych usług IT na działalność biznesową).
- Wspiera organizację w cyklicznej ocenie zagrożeń cyberbezpieczeństwa i prowadzi ich rejestr.
- Wspiera organizację w przygotowaniu i przeprowadzaniu audytów cyberbezpieczeństwa u krytycznych dostawców.
- Stanowi wsparcie podczas audytów zewnętrznych dotyczących cyberbezpieczeństwa.

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

*** Między innymi: NIST Cybersecurity Framework, NIST SP 800-53, CIS Critical Security Controls for Effective Cyber Defense, ISO 27001, ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.*

- Uczestniczy w budowie programu podnoszenia świadomości cyberbezpieczeństwa.
- Prowadzi systematyczne szkolenia dla pracowników z zakresu cyberbezpieczeństwa.
- Wspiera organizację przy wyborze, implementacji i zarządzaniu systemami bezpieczeństwa w oparciu o narzędzia klasy m.in.: SIEM, SOAR, WAF, IPS, IDS, EDR, XDR, PIM, PAM, DAM, MFA, DLP (w niezbędnym zakresie na podstawie decyzji po analizie zagrożeń cyberbezpieczeństwa).
- Realizuje testy socjotechniczne (kampanie phishingowe, smishingowe, vishingowe) mające na celu badanie poziomu odporności organizacji na cyberzagrożenia / świadomości cyberbezpieczeństwa wśród pracowników.
- Realizuje automatyczne testy bezpieczeństwa systemów / aplikacji / infrastruktury IT.
- Monitoruje systemy / aplikacje / infrastrukturę IT z zastosowaniem narzędzi klasy SIEM / SOAR itp.
- Dokonuje wstępnej analizy zdarzeń.
- Wykonuje cykliczne skany systemów / aplikacji / infrastruktury IT w celu wykrywania podatności (dane z narzędzi klasy EDR, NDR, XDR).
- Wspiera organizację w obsłudze incydentów i prowadzi ich rejestr.
- Realizuje działania typu REKON (monitorowanie informacji na temat cyberzagrożeń z wykorzystaniem otwartych źródeł) oraz REKON Continuous (ciągłe monitorowanie cyberzagrożeń w sieci rozszerzone o zamknięte fora, w tym Deep oraz Dark Web).
- Wykonuje działania z zakresu Threat Hunting.
- Wspiera organizację w zarządzaniu zidentyfikowanymi podatnościami technicznymi i organizacyjnymi.
- Koordynuje lub realizuje działania z zakresu IT Forensic po incydentach cyberbezpieczeństwa.
- Prowadzi korespondencję z kontrahentami, klientami i organami nadzoru w zakresie cyberbezpieczeństwa.



Proponowane modele współpracy

Usługi Governance

ZADANIA	RODZAJ PAKIETU		
	BASIC	MEDIUM	PRO
Wsparcie eksperta cyberbezpieczeństwa	✓	✓	✓
Ocena stanu cyberbezpieczeństwa organizacji as-is	✓	✓	✓
Ocena poziomu świadomości cyberbezpieczeństwa pracowników as-is	✓	✓	✓
Przegląd zidentyfikowanych zagrożeń cyberbezpieczeństwa	✓	✓	✓
Opracowanie planu działań w zakresie podniesienia poziomu cyberbezpieczeństwa organizacji	✓	✓	✓
Opracowanie programu podniesienia świadomości cyberbezpieczeństwa wśród pracowników	✓	✓	✓
Aktualizacja / opracowanie procedur z zakresu cyberbezpieczeństwa	✓	✓	✓
Monitorowanie zgodności z wewnętrznymi procedurami i przepisami prawa z zakresu cyberbezpieczeństwa	✓	✓	✓
Wsparcie w procesie oceny zagrożeń cyberbezpieczeństwa		✓	✓
Prowadzenie rejestru zagrożeń cyberbezpieczeństwa		✓	✓
Realizacja szkoleń z zakresu cyberbezpieczeństwa		✓	✓
Wsparcie w przygotowaniu i przeprowadzaniu audytów cyberbezpieczeństwa u krytycznych dostawców		✓	✓
Wsparcie w przeprowadzanych zewnętrznych audytach cyberbezpieczeństwa			✓
Realizacja analizy BIA dla kluczowych usług IT			✓
Wsparcie przy wyborze, implementacji i zarządzaniu systemami bezpieczeństwa (w niezbędnym zakresie na podstawie decyzji po analizie zagrożeń cyberbezpieczeństwa)			✓

Istnieje możliwość indywidualnego doboru pakietu usług.
Usługi mogą być świadczone w różnych wymiarach czasowych: od 0,25 FTE do1 FTE przy umowie zawartej na minimum 6 miesięcy.

Resilia

Usługi analityczno-technologiczne

ZADANIA	RODZAJ PAKIETU		
	BASIC	MEDIUM	PRO
Wsparcie analityka cyberbezpieczeństwa	✓	✓	✓
Automatyczne monitorowanie zgodności z wybranymi wymaganiami, w tym m.in. KSC, KNF, NIST CSF, NIST 800-53	✓	✓	✓
REKON - monitorowanie zagrożeń cyberbezpieczeństwa w sieci na podstawie informacji z otwartych źródeł	✓	✓	✓
Wsparcie w procesie identyfikacji, priorytetyzacji i zarządzania podatnościami	✓	✓	✓
Wsparcie przy obsłudze incydentów i naruszeń cyberbezpieczeństwa (w tym etapy: przygotowanie, identyfikacja, ocena, analiza przyczyn, naprawa / usunięcie skutków)	✓	✓	✓
Realizacja automatycznych testów bezpieczeństwa		✓	✓
REKON Continuous - ciągłe monitorowanie cyberzagrożeń w sieci rozszerzone o zamknięte fora, w tym Deep oraz Dark Web		✓	✓
Realizacja testów socjotechnicznych, w tym typu phishing, smishing, vishing		✓	✓
Raportowanie wykrytych technicznych incydentów i naruszeń cyberbezpieczeństwa		✓	✓
Monitorowanie logów z uzgodnionych systemów / aplikacji / elementów infrastruktury IT z wykorzystaniem narzędzi klasy SIEM w wybranym zakresie, w tym m.in.: dostępności usług IT, zdarzeń, integralności plików, konfiguracji, działań użytkowników, wycieków adresów e-mail / haseł (kompromitacji kont e-mail) / innych istotnych danych			✓
Wstępna analiza zdarzeń			✓
Skanowanie systemów / aplikacji / infrastruktury IT w celu wykrywania podatności (dane z narzędzi klasy EDR, NDR, XDR)			✓
Wsparcie przy utwardzaniu systemów, w tym w doborze odpowiednich narzędzi oraz konfiguracji			✓
Realizacja działań typu Threat Hunting			✓
Wsparcie we wstępnej analizie powłamaniowej i wyborze profesjonalnych rozwiązań IT Forensic			✓

Istnieje możliwość indywidualnego doboru pakietu usług.
Usługi mogą być świadczone w różnych wymiarach czasowych: od 0,25 FTE do1 FTE przy umowie zawartej na minimum 6 miesięcy.

Resilia

Jakie usługi IT oferujemy w ramach współpracy?

USŁUGA	OPIS USŁUGI
SOC Lite	Pakiet Standard, obsługa 100 EPS (ang. Event per Second), 10 źródeł danych
Platforma VCISO	Platforma SaaS do zdalnej realizacji usługi VCISO
Phishing & awareness	Platforma SaaS do testów socjotechnicznych i szkoleń awareness
Automatyczne testy bezpieczeństwa	Platforma do realizacji automatycznych testów web aplikacji i infrastruktury sieciowej
Digital Risk Protection	Platforma oferująca funkcjonalności monitorowania sieci Internet, Deep Web i Dark Web w celu prewencyjnego wykrywania cyberzagrożeń

Resilia

Chcesz „wynająć” naszego VCISO?

Masz pytania?

Skontaktuj się z nami!

kontakt@resilia.pl
+48 22 243 39 37

Ewa Jońska
ejonska@resilia.pl
+ 48 502 335 354

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

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

#RESILIA_CYBERSECURITY