Oferta

# COIG SOC
# SOC Standard | SOC Pro | SOC Elite

www.coig.pl

COIG

CYBER SECURITY

# SOC Standard – Bezpieczeństwo IT dla małych i średnich przedsiębiorstw

**SOC Standard** to przystępna cenowo usługa monitorowania bezpieczeństwa IT, stworzona specjalnie z myślą o małych i średnich firmach, które chcą chronić swoją infrastrukturę bez konieczności budowania własnego zespołu bezpieczeństwa.

## Korzyści dla Twojej firmy:

### Spokój dzięki codziennemu monitoringowi

Twoja infrastruktura IT jest monitorowana całodobowo ze wsparciem ekspertów w dni robocze w godzinach 8:00–16:00, co pozwala szybko wykrywać potencjalne zagrożenia i reagować zanim wyrządzą szkody.

### Podstawowa detekcja zagrożeń

Zyskujesz ochronę przed najczęstszymi atakami i incydentami – bez konieczności inwestowania w drogie systemy bezpieczeństwa.

### Powiadomienia o incydentach

W przypadku wykrycia zagrożenia otrzymujesz powiadomienie w trybie best effort, co pozwala Ci szybko podjąć działania.

### Wsparcie ekspertów

W cenie usługi otrzymujesz do 4 roboczogodzin miesięcznie na reagowanie na incydenty – to realna pomoc w kryzysowych sytuacjach.

### Elastyczność i rozwój

W każdej chwili możesz rozszerzyć usługę o:

- wsparcie 24/7;
- integrację z dodatkowymi systemami;
- biuletyn z aktualnymi zagrożeniami;
- konsultacje z ekspertami.

### Monitoring OT

Dzięki dedykowanym sondom logującym, możliwe jest skuteczne i bezinwazyjne zbieranie danych z urządzeń przemysłowych (PLC, HMI, RTU itp.).
3 linia (L3) wsparcia oparta o zespół automatyków.

### Stała, przewidywalna cena

Za jedyne 2 600,00* PLN netto miesięcznie otrzymujesz profesjonalne wsparcie SOC bez ukrytych kosztów.

# SOC PRO – Zaawansowane Centrum Operacji Cyberbezpieczeństwa dla wymagających firm

**SOC PRO** to usługa dedykowana średnim i dużym organizacjom, które potrzebują ciągłego nadzoru nad bezpieczeństwem IT oraz natychmiastowej reakcji na incydenty. Bazując na doświadczeniu zespołu COIG oraz nowoczesnych technologiach, SOC PRO zapewnia kompleksową ochronę infrastruktury IT – 24 godziny na dobę, 7 dni w tygodniu.

## Dlaczego warto wybrać SOC PRO?

### Monitoring 24/7/365

Nieprzerwane nadzorowanie środowiska IT z wykorzystaniem zaawansowanych narzędzi takich jak SIEM, UEBA, EDR i DLP, pozwala na szybkie wykrywanie i neutralizowanie zagrożeń.

### Zaawansowana analiza i detekcja

Dzięki integracji z systemami klasy enterprise, SOC PRO umożliwia wykrywanie anomalii, analizę zachowań użytkowników oraz ochronę danych wrażliwych – wszystko w czasie rzeczywistym.

### Dedykowany zespół analityków L2

Zespół specjalistów nie tylko powiadamia o incydentach, ale również dostarcza ich analizę, rekomendacje i wspiera w eskalacji.

### Tygodniowe raporty i rekomendacje

Regularne zestawienia z podsumowaniem działań, wykrytych incydentów i rekomendacjami pozwalają na bieżąco optymalizować politykę bezpieczeństwa.

### Proaktywne działania – Threat Hunting

Zespół COIG aktywnie poszukuje ukrytych zagrożeń, zanim staną się one realnym problemem dla Twojej organizacji.

### Rozszerzone możliwości

- Integracja z dodatkowymi elementami infrastruktury;
- Biuletyn cyberbezpieczeństwa z aktualnymi zagrożeniami;
- Konsultacje z ekspertami COIG;
- Kwartalne testy penetracyjne – praktyczna ocena.

### Dla kogo?

Dla firm, które oczekują najwyższego poziomu ochrony, zgodnego z najlepszymi praktykami branżowymi i standardami ISO 27001.

### Monitoring OT

Dzięki dedykowanym sondom logującym, możliwe jest skuteczne i bezinwazyjne zbieranie danych z urządzeń przemysłowych (PLC, HMI, RTU itp.).

3 linia (L3) wsparcia oparta o zespół automatyków.

### Cena od: 8 900,00* PLN netto miesięcznie

# SOC ELITE – Cyberbezpieczeństwo klasy enterprise bez kompromisów

**SOC ELITE** to najwyższy poziom ochrony oferowany przez COIG – stworzony z myślą o organizacjach o złożonej strukturze, wysokich wymaganiach regulacyjnych i potrzebie pełnej kontroli nad bezpieczeństwem IT. To kompleksowe, całodobowe wsparcie operacyjne, analityczne i strategiczne, realizowane przez doświadczony zespół COIG CSIRT.

## Korzyści dla Twojej organizacji:

**Monitoring 24/7 przez zespół SOC**

Stały nadzór nad środowiskiem IT – niezależnie od lokalizacji, architektury (on-prem, cloud, hybrid) czy skali działania.

**Threat Intelligence z globalnych źródeł**

Dostęp do aktualnych danych o zagrożeniach z renomowanych źródeł międzynarodowych pozwala na szybsze reagowanie i lepsze przewidywanie ataków.

**Zespół reagowania COIG CSIRT**

Zespół reagowania na incydenty, gotowy do działania – z pełnym wsparciem w analizie, eskalacji i neutralizacji zagrożeń.

**Proaktywny Threat Hunting**

Zaawansowane techniki wykrywania ukrytych zagrożeń, zanim staną się one realnym problemem.

**Raporty dzienne + dashboard w czasie rzeczywistym**

Pełna transparentność – codzienne raporty oraz dostęp do interaktywnego panelu z aktualnymi danymi o stanie bezpieczeństwa.

**Integracja z polityką bezpieczeństwa klienta**

Usługa dostosowana do Twoich procedur, standardów i wymagań – SOC ELITE działa w zgodzie z strategią bezpieczeństwa.

**Obsługa wielu lokalizacji i środowisk**

Niezależnie od tego, czy działasz lokalnie, globalnie, w chmurze czy w środowisku hybrydowym – zapewnia spójne i skuteczne wsparcie.

**Dodatkowe elementy strategiczne:**

- Symulacje ataków (Red Teaming) – testowanie odporności organizacji na rzeczywiste scenariusze ataków;
- Szkolenia dla zespołów IT i użytkowników – budowanie świadomości i kompetencji w zakresie cyberbezpieczeństwa;
- Wykorzystanie narzędzi AI w predykcji i analizie.

**Dla kogo?**

Dla organizacji, które wymagają najwyższego poziomu ochrony, zgodnego z najlepszymi praktykami branżowymi, normami ISO oraz regulacjami sektorowymi.

**Monitoring OT**

Dzięki dedykowanym sondom logującym, możliwe jest skuteczne i bezinwazyjne zbieranie danych z urządzeń przemysłowych (PLC, HMI, RTU itp.). 3 linia (L3) wsparcia oparta o zespół automatyków.

**Cena od: 24 900,00* PLN netto miesięcznie.**

| Wariant | SOC Standard | SOC Pro | SOC Elite |
|---|---|---|---|
| **Opis** | **Dla małych i średnich przedsiębiorstw** | **Dla średnich firm wymagających ciągłego nadzoru i szybkiej reakcji** | **Cyber-bezpieczeństwo klasy enterprise** |
| **Monitorowanie** | | | |
| 24/7 | ✓ | ✓ | ✓ |
| Automatyczne powiadamianie o zdarzeniach/incydentach | ✓ | ✓ | ✓ |
| Analiza w oparciu o automat SOAR | | ✓ | ✓ |
| Analiza przez TEAM SOC | | | ✓ |
| **Detekcja zagrożeń** | | | |
| Podstawowa | ✓ | ✓ | ✓ |
| Zaawansowany SIEM , UEBA, EDR, DLP | | ✓ | ✓ |
| Threat Intelligence z globalnych źródeł | | | ✓ |
| **Reakcja** | | | |
| Powiadamianie w trybie best effort | ✓ | ✓ | ✓ |
| Zespół SOC powiadamia o incydentach wraz z analizą | | ✓ | ✓ |
| Zespół reagowania COIG CSIRT | | | ✓ |
| Konsultacje w sprawie incydentów | do 4h/msc | bez ograniczeń | bez ograniczeń |
| Dedykowany zespół analityków L2 | w ramach konsultacji | ✓ | ✓ |
| Proaktywny Threat Hunting | | | ✓ |
| Tygodniowe raporty i rekomendacje | | ✓ | ✓ |
| Wsparcie w analizie i eskalacji incydentów | | | ✓ |
| Raporty dzienne + dashboard w czasie rzeczywistym | | ✓ | ✓ |
| Integracja z polityką bezpieczeństwa klienta | | | ✓ |
| Obsługa wielu lokalizacji i środowisk (on-prem, cloud, hybrid) | | | ✓ |
| **Cena miesięcznie (PLN netto)** | 2 600* | od 8 900* | od 24 900* |

| | | | |
|---|---|---|---|
| **Opcje dodatkowo płatne** | | | |
| Integracje z infrastrukturą dodatkową | ✓ | ✓ | ✓ |
| Symulacje ataków (Red Teaming) | | | ✓ |
| Szkolenia dla zespołów IT i użytkowników | | | ✓ |
| Biuletyn cyberbezpieczeństwa | ✓ | ✓ | ✓ |
| Analiza zgodności infrastruktury klienta z przepisami | ✓ | ✓ | ✓ |
| Threat Hunting | | | ✓ |
| Kwartalne testy penetracyjne/socjotechniczne | | | ✓ |
| Integracja z systemami OT | | ✓ | ✓ |
| Monitoring o365 | | ✓ | ✓ |
| Wdrożenie polityk bezpieczeństwa (SZBI/SZCD) | | | ✓ |

*Cena zależy od ilości monitorowanych końcówek i wybranych opcji dodatkowych. Zostanie doprecyzowana po przeprowadzonej analizie wymagań.

## Backup w Data Center COIG

Usługa realizuje wykonywanie kopii bezpieczeństwa kluczowych danych w Data Center COIG. Kopie krytycznych danych znajdują się poza lokalizacją w której pracuje infrastruktura produkcyjna. Takie rozwiązanie podnosi poziom bezpieczeństwo danych organizacji, zgodnie z zasadą 3-2-1. Usługa może także zostać wzbogacona o odtworzenie systemów i danych w Data Center COIG.

**Cena usługi 2 600,00 PLN netto/miesiąc z założeniami:**

- Dane backupowe w łącznej ilości 2 TB
- Backup wykonywany z retencją 1 kopia dziennie
- Okres przechowywania danych backupu 30 dni.

## Usługi w zakresie cyberbezpieczeństwa

| Produkt | Opis usługi | Cena od (PLN netto): |
|---|---|---|
| Audyt IT | Analiza zabezpieczeń zastosowanych w organizacji w celu ochrony informacji | 10 000,00 |
| Audyt OT | Audyt bezpieczeństwa automatyki przemysłowej | 17 000,00 |
| System Zarządzania Bezpieczeństwem Informacji (SZBI) | Stworzenie nowej dokumentacji SZBI zgodnie z wymaganiami normy ISO 27001, ISO 27005, ISO 3100 | 15 000,00 |
| Szkolenia z zakresu cyberbezpieczeństwa | Podstawowe zasady cyberhigieny, zagrożenia w cyberprzestrzeni, zasady bezpieczeństwa, warsztat praktyczny | 8 000,00 |
| Kampania phishingowa | Kontrolowany atak phishingowy na przedsiębiorstwo (testy socjotechniczne) | 5 000,00 |
| Testy penetracyjne | Testy bezpieczeństwa aplikacji webowych (np. iBOK) | 12 000,00 |

## Infrastruktura IT i oprogramowanie

| Produkt | Przeznaczenie |
|---|---|
| Serwery | Instalacja systemów SIEM/SOAR/EDR, AD |
| Macierze dyskowe (NAS/SAN) | Lokalne przechowywanie kopii zapasowych (backup) |
| Zapora sieciowa (Next Gen Firewall/UTM) | Ochrona przed atakami, kontrola ruchu w sieci, filtrowania aplikacji, bezpieczeństwa styku sieci Internet z usługami wewnętrznymi |
| Switche zarządzalne | Segmentacja sieci |
| Oprogramowanie backupu | Ochrona przed utratą danych |
| Oprogramowanie AV/EDR/XDR | Ochrona stacji roboczych |
| Oprogramowanie DLP | Ochrona przed wyciekiem danych |
| Oprogramowanie IDM/PAM | Zarządzanie uprawnieniami użytkowników |
| NAC | Weryfikacja urządzeń i użytkowników łączących się z siecią |
| MDM | Zabezpieczenie urządzeń mobilnych |
| MFA | Uwierzytelnianie wieloskładnikowe, zabezpieczanie tożsamości cyfrowej |
| NEDAPS-SEC | Platforma do automatyzacji zarządzania bezpieczeństwem IT, integrująca monitorowanie, analizę i reagowanie na zagrożenia oraz badająca podatności |