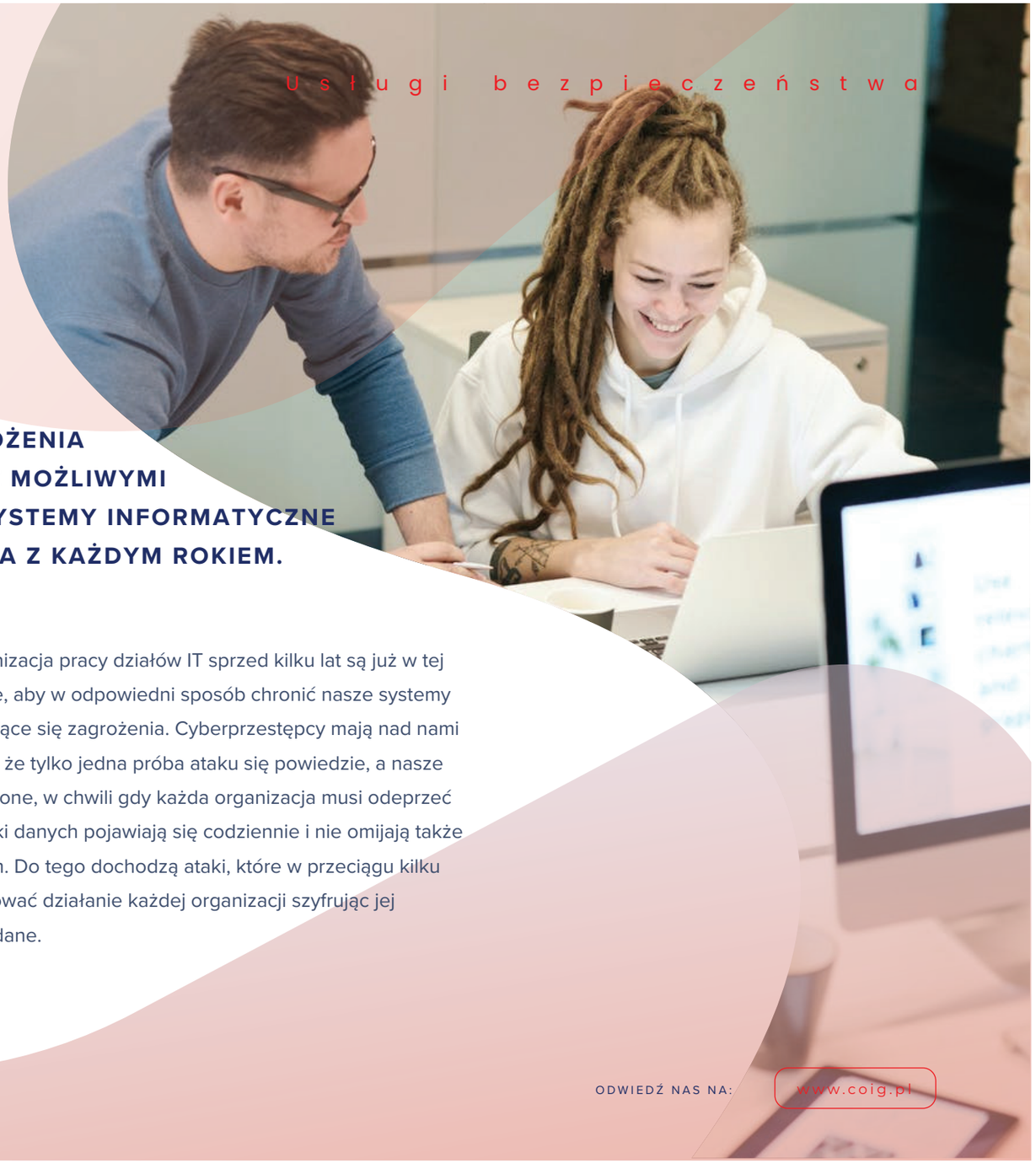


Security Operations Center

DATA CENTER

POZIOM ZAGROŻENIA ZWIĄZANEGO Z MOŻLIWYMI ATAKAMI NA SYSTEMY INFORMATYCZNE FIRMY WZRASTA Z KAŻDYM ROKIEM.

Zabezpieczenia i organizacja pracy działów IT sprzed kilku lat są już w tej chwili niewystarczające, aby w odpowiedni sposób chronić nasze systemy i reagować na pojawiające się zagrożenia. Cyberprzestępcy mają nad nami przewagę – wystarczy, że tylko jedna próba ataku się powiedzie, a nasze dane mogą być zagrożone, w chwili gdy każda organizacja musi odeprzeć wszystkie ataki. Wycieki danych pojawiają się codziennie i nie omijają także naszych rodzimych firm. Do tego dochodzą ataki, które w przeciągu kilku godzin, mogą sparaliżować działanie każdej organizacji szyfrując jej najcenniejszą rzecz – dane.

DATA CENTER

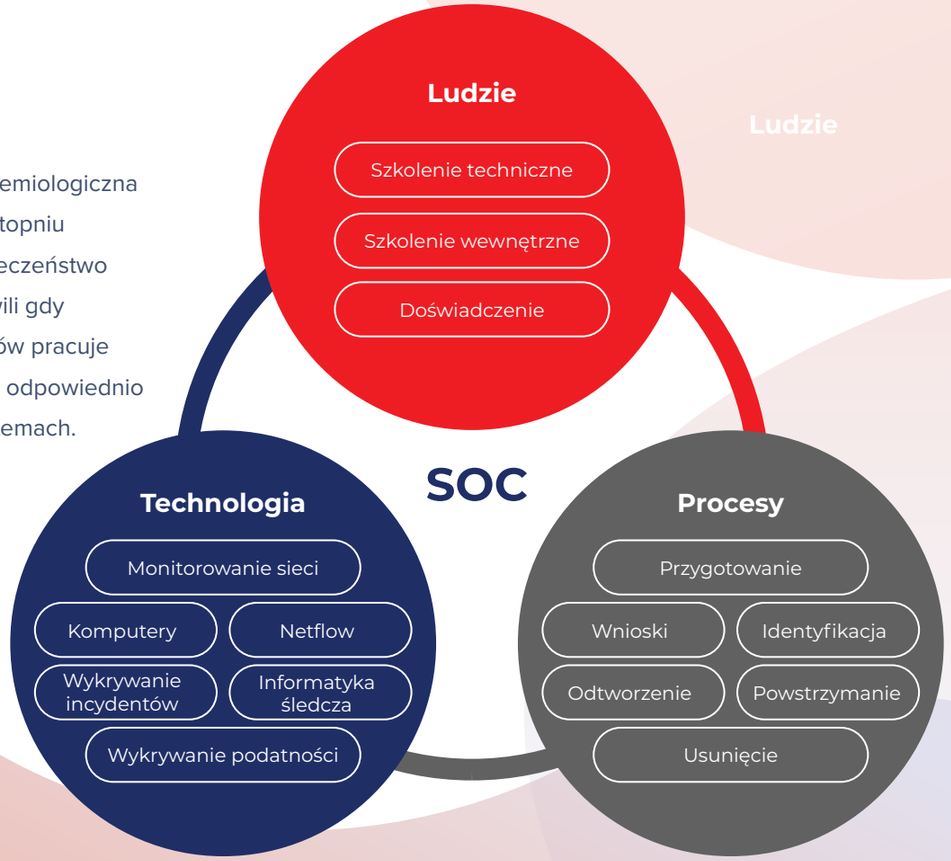
S O C

Fundamenty Security Operation Center

Usługi bezpieczeństwa

Zgodnie z niedawno opublikowanym raportem ENISA , ataki stają się coraz bardziej wyrafinowane, dokładnie zaplanowane, pojawiające się na dużą skalę i co najważniejsze – większość ataków nie jest wykrywana.
Według raportu, głównymi zagrożeniami dla firm w chwili obecnej jest – złośliwe oprogramowanie (malware), ataki wykorzystujące WWW, Phishing, ataki na aplikacje WWW oraz SPAM.

Obecna sytuacja epidemiologiczna jeszcze w większym stopniu wystawia na niebezpieczeństwo nasze systemy, w chwili gdy większość pracowników pracuje zdalnie na nie zawsze odpowiednio zabezpieczonych systemach.



Ludzie

Usługa Security Operation Center to rozwiązanie, które:

- Umożliwia korelację zdarzeń oraz wczesne wykrywanie pojawiających zagrożeń
- Posiada odpowiednie procedury związane z wykrywaniem podatności i ich usuwaniem
- Umożliwia wdrażanie odpowiednich procesów związanych z obsługą incydentów
- Zawiera odpowiednie narzędzia, które umożliwią nam zbieranie informacji, korelowanie, analizę, odpowiednią reakcję na pojawiające się zdarzenia
- Bazuje na sprawdzonym oprogramowaniu polskiego producenta firmy eSecure

ODWIEDŹ NAS NA: www.coig.pl

Stosujemy:

SecureVisio SOAR

UŻYWAMY SPECJALISTYCZNEGO ROZWIĄZANIA SECUREVISIO SOAR SŁUŻĄCEGO DO AUTOMATYZACJI ZARZĄDZANIA I REAGOWANIA NA INCYDENTY ORAZ USPRAWNIENIA INNYCH PROCESÓW ZARZĄDZANIA BEZPIECZEŃSTWEM.

Funkcje i korzyści rozwiązania:

- **Unifikacja narzędzi**
  jedna graficzna konsola zawiera wszystkie narzędzia i informacje potrzebne do wyjaśniania i obsługi incydentów
- **Uporządkowana praca ludzi**
  proces zarządzania incydentami (Workflow) odbywa się etapowo, zgodne z obowiązującymi standardami (m.in. ISO/IEC 27035)
- **Integracja narzędzi i źródeł danych**
  Playbooki automatycznie uruchamiają narzędzia i pozyskują dane ze źródeł zewnętrznych (m.in. Threat Intelligence, Vulnerability Assessment)
- **Automatyzacja odpowiedzi na incydenty**
  gotowe do użycia reakcje na różne rodzaje incydentów, w tym usuwanie cyberprzestępców z systemów wewnętrznych

Unikalne własności :

- **Zunifikowane zarządzanie podatnościami**
  współpraca z narzędziami Vulnerability Assessment i CVE oraz zintegrowane narzędzia Workflow i Playbook do zarządzania podatnościami
- **Symulacja i wizualizacja zagrożeń**
  analiza incydentów i podatności jest wspomagana za pomocą graficznych narzędzi symulacji ataków i innych zagrożeń
- **Priorytetyzacja biznesowa**
  incydenty są automatycznie priorytetyzowane w odniesieniu do ważności zasobów dla organizacji (tzn. wspomaganych procesów, wrażliwych informacji)
- **Metryki efektywności z kontekstem biznesowym**
  kluczowe wskaźniki efektywności KPI (key performance indicator) oraz kluczowe wskaźniki ryzyka KRI (key risk indicator) w odniesieniu do procesów biznesowych

ODWIEDŹ NAS NA: www.coig.pl

esecure | SECUREVISIO

DATA CENTER

Stosujemy:

SecureVisioNextGen SIEM:

Właściwości rozwiązania:

- **Wiele metod detekcji**
  reguły korelacji (SIEM), analiza behawioralna użytkowników i systemów (UEBA), Threat Intelligence
- **Szeroki zakres analizy**
  analiza zdarzeń bezpieczeństwa (logi), aktualnych podatności, informacji Threat Intelligence oraz oszacowanej wielkości ryzyka
- **Wiele metod odczytu logów**
  Syslog, e-mail, Windows Event Forwarding, a także możliwość odczytu logów z baz danych oraz plików płaskich
- **Graficzny edytor parserów**
  predefiniowany zestaw parserów może zostać rozszerzony o nowe parsery tworzone za pomocą graficznego edytora
- **Repozytorium zdarzeń**
  specjalistyczna baza danych do długoterminowego składowania i szybkiego wyszukiwania zdarzeń bezpieczeństwa

Unikalne własności :

- **Elektroniczna dokumentacja sieci systemów IT**
  wykrywanie incydentów odbywa się w kontekście informacji na temat aktualnej sieci i systemów IT wykrywanych za pomocą funkcji Auto-Discovery
- **Elektroniczna dokumentacja danych osobowych**
  wykrywanie incydentów odbywa się w kontekście informacji na temat danych osobowych przetwarzanych w systemach IT i wymagań bezpieczeństwa RODO
- **Świadomość biznesowych skutków incydentu**
  wykrywanie incydentów odbywa się ze świadomością ryzyka (norma ISO/IEC 27005) i biznesowych skutków naruszenia bezpieczeństwa
- **Dynamiczne reguły SIEM**
  reguły korelacji SIEM automatycznie dostosowują się do zmian sieci i systemów IT oraz aktualnej wielkości ryzyka

ODWIEDŹ NAS NA: www.coig.pl

DATA CENTER

COIG SA

Od wielu lat budujemy i ciągle rozwijamy własny Zespół Cyberbezpieczeństwa. Wpieramy usługę SOC posiadając doświadczenie, odpowiednio wykwalifikowaną kadrę (posiadającą certyfikaty CISM, CEH, CISSP, CCSP, audytora wiodącego ISO 27001 i wiele innych), która w ciągły sposób (24/7/365) reaguje na pojawiające się zagrożenia.

Nasze rozwiązanie SOC bazujące na ludziach, procesach i technologii umożliwi Państwu wczesne wykrywanie podatności i incydentów, odpowiednie reagowanie i obsługę pojawiających się zagrożeń.

Proponujemy Państwu wdrożenie w dwóch wariantach:

01 **Bezpośrednie wdrożenie kompletnego SOC w modelu własnym w sieci informatycznej Państwa organizacji**

02 **Usługa świadczona przez COIG w modelu chmurowym**

COIG

Ul. Mikołowska 100 | 40-065 Katowice,
dc@coig.pl

ODWIEDŹ NAS NA: www.coig.pl