COIG

Usługi bezpieczeństwa IT

DATA CENTER

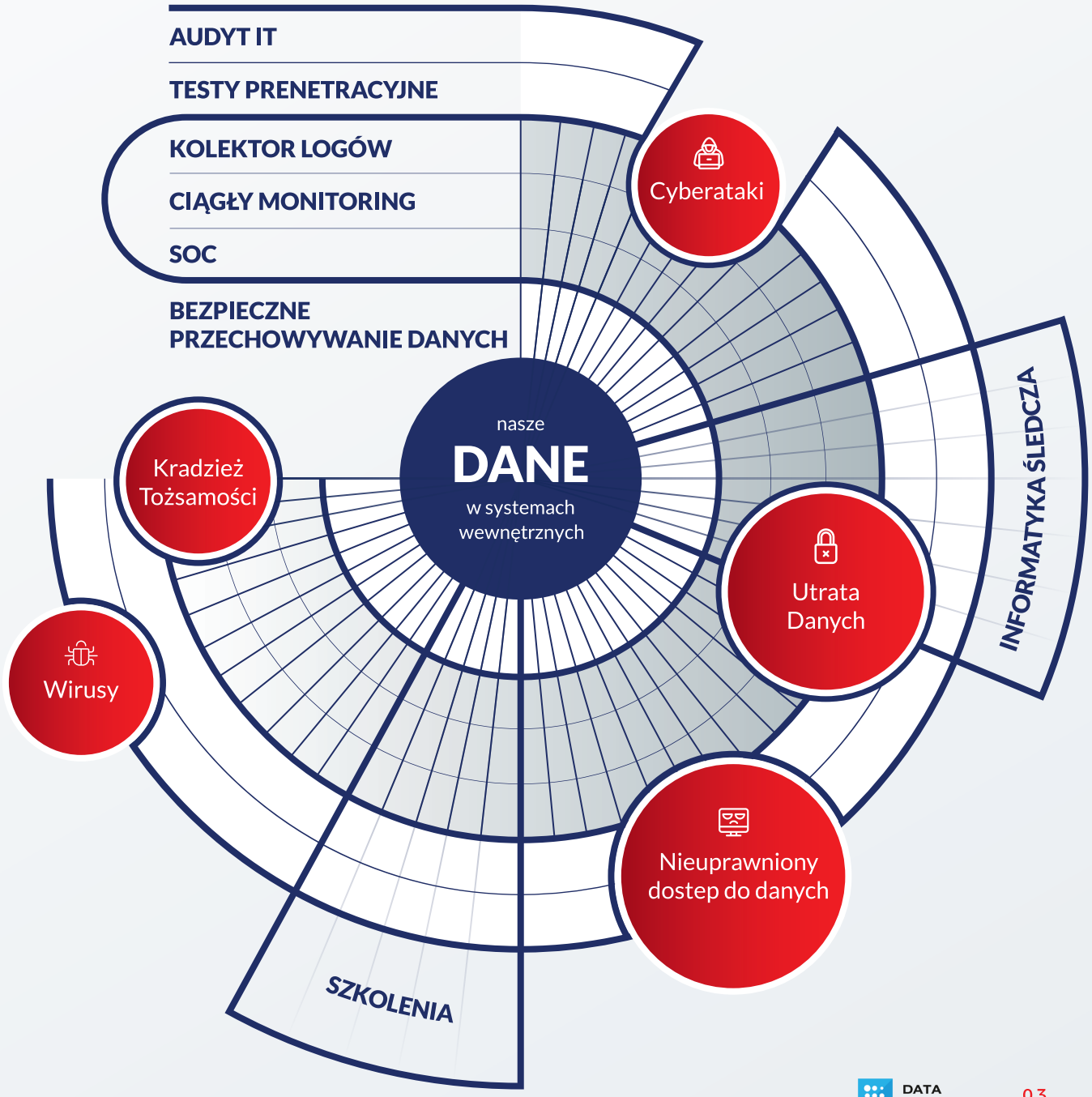
www.coig.pl

Grupa Kapitałowa WASKO

Sieć i jej zagrożenia

WE WSPÓŁCZESNEJ GOSPODARCE INFORMACJA JEST NIE TYLKO ZASOBEM EKONOMICZNYM NIEZBĘDNYM DO FUNKCJONOWANIA ALE WSPÓŁDECYDUJE O POTENCJALE EKONOMICZNYM I MOŻLIWOŚCIACH ROZWOJOWYCH.

Gromadzenie i przetwarzanie danych w formie elektronicznej powoduje, że są one podatne na nowy rodzaj zagrożeń ze strony cyberprzestępców. Nie ma dziś rozwiązań, które zagwarantują pełne bezpieczeństwo informacji, ale my wiemy jak zapewnić ich najwyższą ochronę.


AUDYT IT
TESTY PRENETRACYJNE
KOLEKTOR LOGÓW
CIĄGŁY MONITORING
SOC
BEZPIECZNE PRZECHOWYWANIE DANYCH
nasze
DANE
w systemach wewnętrznych
Cyberataki
Kradzież Tożsamości
Utrata Danych
Wirusy
Nieuprawniony dostep do danych
INFORMATYKA ŚLEDCZA
SZKOLENIA

Audyt IT

Usługi bezpieczeństwa

Celem usługi audytu bezpieczeństwa jest analiza, identyfikacja procesów związanych z przetwarzaniem danych, weryfikacja zabezpieczeń logicznych i fizycznych, weryfikacja dokumentacji związanej z ochroną danych oraz ocena zgodności z aktualnym stanem prawnymi wewnętrznymi regulacjami. Audyt służy potwierdzeniu że procedury wewnętrzne organizacji, systemy informatyczne oraz urządzenia nie posiadają luk zarówno proceduralnych jak i teleinformatycznych które mogą doprowadzić do utraty bądź wycieku danych.

- Zgodność stosowanych procedur i rozwiązań z prawem
- Zgodność stosowanych procedur i rozwiązań ze standardami i dobrymi praktykami
- Bezpieczeństwo techniczne
- Bezpieczeństwo organizacyjne, przestrzeganie procedur
- Czynnik ludzki – weryfikacja
- Raport końcowy

WYNIKIEM AUDYTU JEST RAPORT ZAWIERAJĄCY PEŁNĄ INFORMACJĘ O STANIE BEZPIECZEŃSTWA IT ORGANIZACJI WRAZ Z ZALECENIAMI POAUDYTOWYMI.

Testy Penetracyjne

Usługi bezpieczeństwa

REALIZUJEMY KOMPLEKSOWE USŁUGI PRZEPROWADZANIA TESTÓW PENETRACYJNYCH. CELEM TAKICH TESTÓW JEST UZYSKANIE PEWNOŚCI, ŻE ŚRODOWISKO INFORMATYCZNE JEST ODPORNE NA CYBERATAKI.

Testy takie polegają na przeprowadzeniu w sposób całkowicie kontrolowany próby ataku. Celem testów penetracyjnych jest identyfikacja i wykrywanie niezabezpieczonych przed nieuprawnionymi osobami i procesami dróg dostępu do systemów, aplikacji webowych, infrastruktury sieciowej oraz przeprowadzanie testów socjotechnicznych (badanie świadomości użytkowników).

WYNIKIEM PRZEPROWADZONYCH TESTÓW JEST RAPORT Z OPISEM WYKRYTYCH PODATNOŚCI ORAZ SUGEROWANYMI ZALECENIAMI BEZPIECZEŃSTWA.

Kolektor logów

Log Colector

Scentralizowany system monitorowania logów z urządzeń i systemów znajdujących się w infrastrukturze organizacji.

Główną zaletą rozwiązania jest niskie obciążenie zasobów informatycznych, wysyłających logi do systemu. System umożliwia tworzenia powiadomień zarówno przy pomocy wiadomości e-mail jak i sms. Jest on niezwykle pomocny podczas analizy cyberataków z uwagi na możliwą archiwizację logów z urządzeń i systemów przedsiębiorstwa. Realizujemy usługę udostępnienia i wdrożenia oprogramowania oraz ciągłej analizy zebranych danych.

Ciągły monitoring

Continous Monitoring

Zaawansowany monitoring sieci - pozwala na wykrywanie, śledzenie i blokowanie niebezpiecznej transmisji w sieci informatycznej organizacji. Może wykorzystywać m.in. sztuczną inteligencję do analizy zagrożeń, dzięki czemu jest w stanie wykryć także nieznane dotąd ataki. Zespół naszych wykwalifikowanych inżynierów realizuje usługę wdrożenia oprogramowania, monitorowania w trybie 24/7 oraz proaktywnego reagowania na incydenty.

SOC

Security Operation

Zaawansowany monitoring sieci - pozwala na wykrywanie, śledzenie i blokowanie niebezpiecznej Jest to najbardziej zaawansowana usługa obejmująca oprogramowanie, którego moduły analizują między innymi dane z systemów teleinformatycznych organizacji, stosują analizę behawioralną, wspierają dokumentowanie technicznych aktywów informatycznych i proaktywnie wskazują ewentualne luki. Drugim elementem usługi jest wsparcie w trybie ciągłym wykwalifikowanych inżynierów, którzy monitorują i reagują na zdarzenia w środowisku informatycznym oraz podejmują działania zaradcze korzystając z dedykowanych narzędzi.

Główne cechy:

- Selektywne zbieranie logów i ich archiwizacja w bezpiecznym miejscu
- Możliwa podstawowa analiza zdarzeń
- Niezależny od systemów informatycznych

Główne cechy:

- Ciągłe badanie podatności systemów teleinformatycznych
- Ciągła analiza zdarzeń – alerty dla zdarzeń krytycznych
- Reakcja pierwszej linii
- Wsparcie drugiej linii
- Wdrażane w modelu chmurowym bądź wersji stacjonarnej

Główne cechy:

- Najbardziej rozwinięta forma proaktywnego monitoringu
- Wsparcie wykwalifikowanych inżynierów COIG
- Usługa świadczona przez Dostawcę Usług Cyberbezpieczeństwa – COIG
- Wdrożenie oprogramowania wspierającego personel/inżynierów COIG
- Możliwość instalacji wybranych modułów oprogramowania dostosowanych do potrzeb danej organizacji

Informatyka śledcza

W przypadku cyberprzestępstw niezwykle ważne staje się zabezpieczenie w sposób wiarygodny cyfrowych danych dowodowych.

Zabezpieczenie śladów przestępstwa jest jednym z warunków dla rozpoczęcia procedury przywrócenia systemów informatycznych do stanu pierwotnego umożliwiającego prawidłową pracę organizacji. Należy również pamiętać o zabezpieczeniu danych przed ewentualnym powtórnym atakiem. Wykwalifikowany zespół COIG realizuje kompleksową usługę związaną z przypadkami cyberprzestępstw, począwszy od zbierania i odzyskiwania danych po analizę i tworzenie raportów z incydentów.

Główne cechy:

01 Profesjonalna analiza zdarzeń w systemach informatycznych.

02 Zebranie i zabezpieczenie materiału dowodowego mającego wartość sądową.

03 Posiadamy certyfikowany sprzęt i personel o wymaganych kwalifikacjach.

04 Spełniamy warunki określone ustawą o krajowym systemie cyberbezpieczeństwa.

Bezpieczne przechowywanie danych

Oferujemy możliwość gromadzenia, przetwarzania i przechowywania danych w DataCenter COIG. Spełniamy najwyższe standardy.

PN-ISO/IEC 27001:2013, ISO 9001:2015

- Backup i archiwizacja danych
- Migracja i relokacja danych
- Udostępnianie zasobów w chmurze (publiczna lub prywatna)
- Budowa systemów wysokiej dostępności
- Administracja systemami
- Kolokacja
- Bezpieczeństwo sieciowe
- Rozwiązania IT dedykowane dla Klienta

Dedykowane usługi:

Ochrona ruchu pocztowego

w tym:

Ochrona przed spamem, Analiza linków i załączników, Kwarantanna wiadomości

Monitoring bezpieczeństwa stacji roboczych

Ciągłe badanie podatności na incydenty bezpieczeństwa.

Systemy DLP

(Data Loss Prevention)

Rozwiązanie informatyczne służące do ochrony danych przed wyciekiem. Obejmuje zarówno wycieki przypadkowe (nieostrożności pracowników), jak i celowe (kradzieży).

Monitoring

Wydajności systemów teleinformatycznych.

Kompetencje naszego Zespołu:

CISM	Certified information security manager
CEH	Certified ethical hacker
ISO 27001	Audytorzy wiodący iso 27001

Szkolenia

Usługi szkoleniowe

COIG REALIZUJE USŁUGI SZKOLENIOWE Z ZAKRESU WYMAGAŃ PRAWNYCH, ORGANIZACYJNYCH I TECHNICZNYCH DOTYCZĄCYCH BEZPIECZEŃSTWA DANYCH INFORMATYCZNYCH I SYSTEMÓW.

Ochrona danych osobowych

Dotyczy szczegółowych interpretacji aktualnego stanu prawnego obejmującego przepisy prawa UE i prawa krajowego (ustawy i rozporządzenia).

Cyberbezpieczeństwo

Szkolenie z programem obejmującym aktualny stan prawny, w tym dyrektywę UE NIS i ustawę o krajowym systemie cyberbezpieczeństwa wraz z rozporządzeniami wykonawczymi.

Obsługa i współpraca z SOC

Szkolenie specjalistyczne organizowane w związku z wdrażaniem u klienta kompletnego SOC-a w modelu własnym lub usługi świadczonej przez COIG.

Analiza i zarządzanie ryzykiem IT

Specjalistyczne szkolenie dotyczące światowych standardów i frameworków , głównie udostępnionych przez ISACA z uwzględnieniem normy ISO/IEC 27005 oraz ISO 31000 w obszarze metodyki analizy i zarządzania ryzykiem informatycznym.

COIG SA
ul. Mikołowska 100
40-065 Katowice
coig@coig.pl

WWW.COIG.PL

rozwiązania, które tworzą przyszłość