Razem dbamy o Wasze bezpieczeństwo.
Sprinttech Sp. z o. o.

SECURITY
OPERATIONS
CENTER

Bezpieczeństwo w zasięgu ręki
Zabezpiecz swoje dane i infrastrukturę z najlepszymi ekspertami w branży.
Sprinttech oferuje usługi Security Operations Center (SOC), które zapewniają kompleksową ochronę przed zagrożeniami cyfrowymi 24/7.
Dzięki doświadczeniu oraz szerokiemu wachlarzowi certyfikatów i rozwiązań technologicznych,

- **SOC to** kompleksowe rozwiązanie odpowiadające na współczesne zagrożenia cyberbezpieczeństwa oraz potrzeby naszych klientów.

- Wdrożenie usługi nie wymaga dodatkowych narzędzi - dostarczamy je w ramach usługi. SprintTech oferuje Security Operations Center oparty na własnym zespole analityków bezpieczeństwa IT oraz Zespole Reagowania na Incydenty, wykorzystujący specjalistyczne narzędzia do wykrywania, analizy, reagowania i przeciwdziałania incydentom bezpieczeństwa. Współpracujemy z czołowymi producentami rozwiązań cyberbezpieczeństwa.

- Nasz doświadczony zespół obecnie obsługuje obszary monitorowania, analizy i reagowania na incydenty w kilkunastu organizacjach o różnych zakresach operacyjnych, takich jak sektor branży finansowej, medycznej, e-commerce, produkcji oraz administracji publicznej.

- W ramach współpracy zapewniamy dedykowanego opiekuna, który będzie odpowiedzialny za Państwa bezpieczeństwo.

sprintTECH

OFERTA SPRINTSOC

PARAMETRY	SMART SOC	SOC CUSTOM
TECHNOLOGIA	Lekki agent instalowany na stacje robocze, urządzenia sieciowe	Wykorzystanie infrastruktury klienta (uzupełnienie o technologie do uzyskania pełnej widoczności sieci i użytkowników)
LICZBA UŻYTKOWNIKÓW	**Do 200 użytkowników**	**Bez limitu**
USŁUGI	• Monitorowanie i analizowanie logów z urządzeń końcowych (stacje robocze, serwery, urządzenia sieciowe) • Reagowanie na incydenty krytyczne • Uproszczone raportowanie • Threat Intelligence • Platforma Klienta • Wdrożenie SIEM / EDR • Integracja z systemami klienta • Retencja danych	• Monitorowanie i analizowanie logów z urządzeń końcowych (stacje robocze, serwery, urządzenia sieciowe) • Threat Intelligence • Platforma Klienta • Wdrożenie SIEM / EDR • Integracja z systemami klienta • Testy penetracyjne kluczowych systemów • Proktywne wykrywanie zagrożeń (threat hunting) • Pełna reakcja na incydenty • Szczegółowe Raportowanie • Konsultacje w zakresie cyberbezpieczeństwa • Analiza powłamaniowa • Retencja danych
LIMIT	**Do 200 użytkowników i 100 serwerów**	**Bez limitu**
EXTRA (usługi opcjonalne)	• Audyt zgodności • Przygotowanie SZBI • Konsultacje w zakresie cyberbezpieczeństwa • Rozszerzone raportowanie • Wsparcie prawne • Threat Hunting • Administracja/utrzymanie IT (infrastrukturą cyberbezpieczeństwa) • Zarządzanie podatnościami • SOAR • Przegląd i nadzór konfiguracji urządzeń sieciowych • Analiza powłamaniowa • System obsługi zgłoszeń • PAM • WAF	• Brand Awareness • Wsparcie prawne • Monitorowanie OT • Administracja/utrzymanie IT (infrastrukturą cyberbezpieczeństwa) • Zarządzanie podatnościami • SOAR • Przegląd i nadzór konfiguracji urządzeń sieciowych • PAM • WAF • Pełnomocnik ds. bezpieczeństwa • Przygotowanie SZBI
INFRASTRUKTURA	SAAS	SAAS / ON-Premisie

Zaufaj profesjonalistom.

Sprinttech to Twój partner w zapewnieniu bezpieczeństwa w erze cyfrowych zagrożeń. Skontaktuj się z nami i zapewnij sobie pełną ochronę przed cyberzagrożeniami.

PODNIEŚ Z NAMI POZIOM BEZPIECZEŃSTWA TWOJEJ ORGANIZACJI

Najlepszym sposobem na sprawdzenie poziomu bezpieczeństwa organizacji są **audyty i testy penetracyjne**, czyli tzw. pentesty, które polegają na przeprowadzeniu symulowanego cyberataku.

Dowiedz się, czy Twoja organizacja jest odporna na ataki hakerskie, jak może się przed nimi zabezpieczyć oraz jak poprawnie tworzyć i konfigurować infrastrukturę bezpieczeństwa.

Audyt bezpieczeństwa polega na określeniu stopnia zgodności audytowanego obiektu z ogólnie przyjętymi standardami lub normami. Przeprowadzamy szereg audytów dla instytucji i biznesu w zakresie normy ISO 27001, 22301, 9001, UKSC, KRI, RODO. Przeprowadzamy również międzynarodowy Program Oceny Cyberbezpieczeństwa w oparciu o ISO27001 i Nist Cybersecurity Framework.

Celem testów penetracyjnych jest praktyczna ocena bieżącego stanu bezpieczeństwa systemu w szczególności wykrycie możliwych podatności i przeprowadzenie próby przełamania zabezpieczeń. Wykonujemy testy infrastruktury, Active Directory, chmury, WIFI, OT. Przeprowadzamy testy automatyczne, pół-automatyczne oraz w pełni manualne z wykorzystaniem narzędzi komercyjnych wiodących producentów.

Testy Penetracyjne wykonane są zgodnie z metodologiami m.in.: PTES, Cyber Kill Chain, OWASP ASVS, OSSTMM. Scenariusze budowane są z uwzględnieniem macierzy Mitre Att&ck, a także autorskich metod dostosowanych do zakresu testów. Testy wykonujemy w metodyce: black box, grey box, white box.

AUDYTY

RODZAJ	OPIS
Audyt KSC	Weryfikacja gotowości do spełnienia wymagań i obowiązków wynikających z przepisów z ustawy o Krajowym Systemie Cyberbezpieczeństwa
Audyt zgodnosci z ISO 27001, 22301	Weryfikacja zgodności organizacji w obszarze technicznym i formalnym w zakresie norm dotyczących Bezpieczeństwa Informacji oraz ciągłości działania
Audyt KRI	Weryfikacja wymogów wynikających z rozporządzenia Rady Ministrów z 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności
Audyt DORA	Weryfikacja dostosowana do wymogów unijnego rozporządzenia DORA (UE nr.2022/2554) w sprawie operacyjnej odporności cyfrowej sektora finansowego- Digital Operational Resilience Act. (DORA)
Audyt NIS 2	Kompleksowa ocena gotowości Twojej organizacji do spełnienia wymogów NIS2
Audyt RODO	Identyfikacja i badanie procesów przetwarzania i ochrony danych osobowych występujących w organizacji (sprzedaż, marketing, HR) i analiza pod kątem przepisów wynikających z RODO
inne Audyt	Audyty bezpieczeństwa zgodne z zarządzeniem NFZ nr 8/2023/BBIICD. Audyt w zakresie projektu Cyfrowa Gmina, Audyty sieci OT, zgodne z ISA /IEC 62443

TESTY PENETRACYJNE

RODZAJ	OPIS
Testy aplikacji webowych	Weryfikacja bezpieczeństwa aplikacji i witryn internetowych z użyciem metodologii OWASP ASVS
Testy aplikacji mobilnych	Ocena bezpieczeństwa aplikacji mobilnych na Android i iOS, zarówno od strony użytkownika, jak i systemu.
Stress testy	Sprawdzenie odporności sieci i aplikacji na przeciążenia (np. DDoS).
Testy bazy danych	Testowanie podatności baz danych, m.in. na SQL Injection.
Testy infrastruktury	- Zewnętrzne: Testowanie systemów dostępnych z internetu. - Wewnętrzne: Symulacja ataków z wewnątrz organizacji.
Testy sieci OT	Testowanie systemów przemysłowych (SCADA, PLC, RTU) zgodnie z normą IEC 62443.
Testy rozwiązań chmurowych	Analiza bezpieczeństwa środowisk chmurowych pod kątem architektury, dostępu i konfiguracji.
Testy środowisk kontenerowych	Sprawdzanie bezpieczeństwa platform (Docker, Kubernetes, OpenShift) zgodnie z najlepszymi praktykami.

KORZYŚCI Z NASZYCH USŁUG

Identyfikacja i zarządzanie ryzykiem
Pomoc w zidentyfikowaniu, ocenie i przygotowaniu polityki zarządzania ryzykiem

Szczegółowy raport
Zawierający wykryte podatności i słabości oraz część techniczną i biznesową.

Zarządzanie podatnościami
Zapewnienie stałego cyklicznego nadzoru oraz obsługi podatności różnych środowisk

Obniżenie kosztów
Proaktywne zapobieganie zagrożeniom (threat hunting) oraz obniżenie kosztów związanych z obsługą incydentów

Zgodność z prawem i standardami
Zapewnienie kompleksowej opieki związanej z wdrożeniem standardów i norm

sprintTECH

SKONTAKTUJ SIĘ Z NAMI

+48 58 340 77 07 | kontakt@sprinttech.pl
sprinttech.pl
ul. Budowlanych 64E, 80-298 Gdańsk