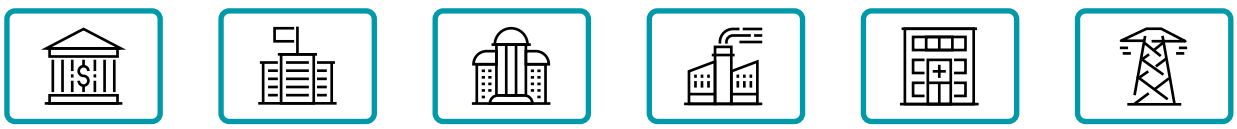
comCERT

Grupa Asseco

KATALOG USŁUG BEZPIECZEPIECZEŃSTWA IT DLA PODMIOTÓW MEDYCZNYCH

ComCERT SA jest polską firmą, wchodzącą w skład Grupy Kapitałowej Asseco Poland S.A. oraz liderem na rynku usług cyberbezpieczeństwa. Usługi świadczymy od 2011 roku i stanowią one bezpośrednie wsparcie dla zespołów bezpieczeństwa IT, ośrodków SOC oraz zespołów CSIRT/CERT. Dzięki wieloletniemu doświadczeniu w zakresie świadczenia usług cyberbezpieczeństwa, praktycznej znajomości specyfiki zagrożeń występujących w kraju i za granicą oraz wieloletniej współpracy z szeregiem przedsiębiorstw nasz zespół jest w stanie zapewnić najwyższą jakość świadczonych usług. Oferujemy kompleksowe szkolenia, produkty i usługi w zakresie cyberbezpieczeństwa, stanowiące pełną ofertę odpowiadającą potrzebom zespołów cyberbezpieczeństwa dużych i średnich podmiotów.

ComCERT wspiera w powyższym zakresie m.in. szpitale wojewódzkie oraz inne jednostki budżetowe powołane przez Ministra Zdrowia, największe banki działające w Polsce, większość operatorów elektroenergetycznych systemów dystrybucyjnych poziomu krajowego, operatorów infrastruktury krytycznej w sektorze paliwowym, największych operatorów telekomunikacyjnych, podmioty centralnej administracji Państwa.



DEDYKOWANE ROZWIĄZANIA BEZPIECZEŃSTWA IT DLA PLACÓWEK MEDYCZNYCH

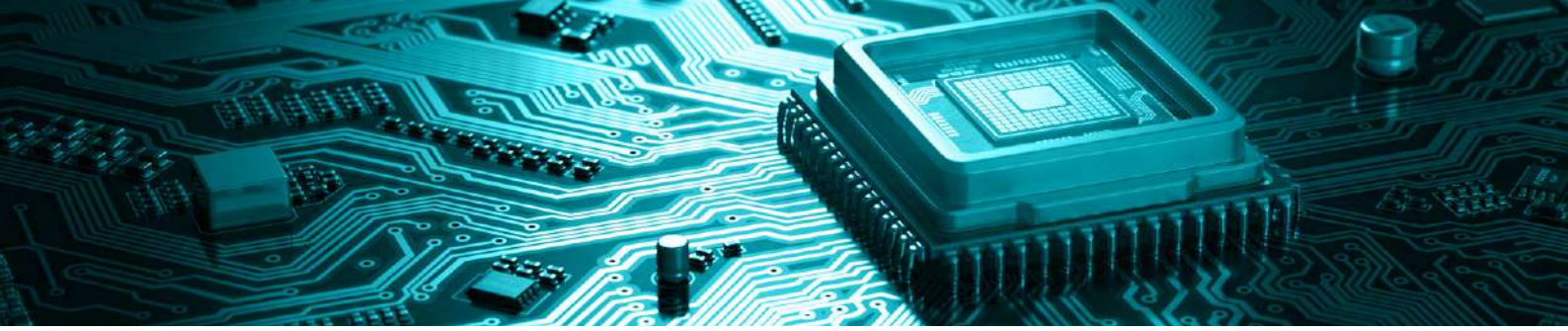
Zakres usługi monitorowania bezpieczeństwa SOC dla podmiotów medycznych

Wariant I – uruchomienie monitoringu bezpieczeństwa opartego o narzędzie Elastic SIEM w wersji darmowej

1	Wdrożenie Elastic SIEM w wybranym przez Zamawiającego modelu: a. on-premise b. w chmurze prywatnej Zamawiającego
2	Podłączenie wybranych na podstawie analizy źródeł logów oraz uruchomienie zaimplementowanych w Elastic SIEM reguł korelacyjnych
3	Strojenie zaimplementowanych w Elastic SIEM reguł korelacyjnych (dobranie warunków i progów wyzwolenia reguł, identyfikacja oczywistych fałszywych alarmów)
4	Uruchomienie automatycznej notyfikacji o alertach lub informowanie za pośrednictwem analityka 1L-SOC ComCERT dla zdarzeń krytycznych.

Wariant II – uruchomienie monitoringu bezpieczeństwa opartego o narzędzie klasy EDR ESET PROTECT Enterprise

1	Wdrożenie ESET PROTECT Enterprise w wybranym przez Zamawiającego modelu: a. on-premise b. jako rozwiązanie chmurowe
2	Podłączenie wybranych przez Zamawiającego do monitoringu hostów oraz uruchomienie zaimplementowanych w EDR reguł korelacyjnych
3	Strojenie EDR (dobranie warunków i progów wyzwolenia alertów, identyfikacja oczywistych fałszywych alarmów)
4	Uruchomienie automatycznych scenariuszy reakcji.



Zakres usługi audytu bezpieczeństwa IT dla podmiotów medycznych

Audyt bezpieczeństwa informacji jest procesem przeprowadzanym w celu zidentyfikowania zagrożeń mogących skutkować utratą poufności, integralności lub dostępności informacji. Jego celem jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego.

Podczas wykonywania audytu i diagnozy stanu cyberbezpieczeństwa w badanym podmiocie wykorzystujemy specjalny algorytm skorelowany z ankietą oraz silnikiem gry „Cyber Twierdza''. Pozwala on w automatyczny sposób zidentyfikować ewentualne luki systemu cyberbezpieczeństwa i wskazać właściwe rekomendacje w celu podniesienia jego poziomu. Wszystko działa dzięki zastosowaniu wspomnianego powyżej algorytmu, który badania audytowego dokonuje w zautomatyzowany sposób. Algorytm został opracowany przez grono ekspertów z zakresu ISO 27001, ISO 22301, ochrony danych osobowych, Ustawy o krajowym systemie cyberbezpieczeństwa i innych dziedzin cyberbezpieczeństwa.

Zadaniem podmiotu biorącego udział w audycie jest wypełnienie ankiety oraz dołączenie do niej dokumentacji będącej materiałem dowodowym. Na podstawie wypełnionego dokumentu zostanie przygotowany plan i harmonogram audytu.

Ankietą jest specjalistyczna elektroniczna platforma, która powstała po to, by usprawnić proces audytu cyberbezpieczeństwa oraz zminimalizować jego koszty poprzez skorelowanie uzyskanych odpowiedzi z algorytmem generującym właściwy raport. Metoda jest testowana i doskonalona od 2020 roku przez audytorów w organizacjach prywatnych, rządowych i samorządowych oraz w wielu sektorach gospodarki. W efekcie zapewnia to rzetelną diagnozę cyberbezpieczeństwa.

Główną zaletą tej metody jest szybkość wykonania audytu – od 2 do 3 dni.

PODSTAWOWE ROZWIĄZANIA BEZPIECZEŃSTWA IT DLA PLACÓWEK MEDYCZNYCH

Wdrożenie i integracja systemów bezpieczeństwa teleinformatycznego

Zakres usług wdrożeniowych wskazuje kluczowe usługi związane z projektowaniem, wdrażaniem, utrzymaniem i rozwojem infrastruktury techniczno-systemowej. Obszar specjalizacji naszych pracowników obejmuje m.in. systemy klasy Firewall, VPN, WAF, DAM, EDR, DLP, SIEM i SOAR.
Dzięki współpracy i autoryzacji wiodących producentów oferujemy usługi w modelu multi-vendor, czyli wykluczające uzależnienie się od jednego producenta.

- DOSTAWA SYSTEMÓW
- PROJEKTOWANIE SYSTEMÓW
- WDRAŻANIE SYSTEMÓW
- INTEGRACJA SYSTEMÓW
- UTRZYMANIE I SERWIS
- MODERNIZACJA I ROZWÓJ
- DORADZTWO TECHNOLOGICZNE
- WSPARCIE W ADMINISTRACJI
- ZARZĄDZANIE UPRAWNIENIAMI

Usługi typu SOC/CERT

Budowa zespołów SOC/CERT w podmiotach medycznych

ComCERT posiada własny zespół SOC i jako pierwszy komercyjny CERT w Polsce dysponuje wiedzą ekspercką i doświadczeniem w zakresie budowy i zarządzania komórkami SOC i CSIRT/CERT. W ramach naszych usług świadczymy wsparcie funkcjonujących u Klienta procesów monitorowania cyberbezpieczeństwa, obsługi incydentów i opracowania koncepcji SOC. Posiadamy kompetencje do całościowego zaprojektowania i wdrożenia komórki SOC/CERT.

SIM3 | FIRST | MITRE | Opracowanie koncepcji SOC/CSIRT | Implementacja komórki SOC/CERT

Outsourcing SOC

W ramach usługi Outsourcing SOC świadczymy wsparcie 1, 2, 3 linii dla naszych klientów.

1. Linia SOC

- Wsparcie ekspertów ComCERT 24/7
- Monitorowanie i detekcja zdarzeń
- Triage

2. Linia SOC

- Tryb 8/5 wraz z gotowością podjęcia działań w pozostałych godzinach
- Analiza logów
- Działania zmierzające do powstrzymania lub izolacji incydentu oraz zmniejszenie jego skutków

3. Linia SOC

- Tryb 8/5 wraz z gotowością podjęcia działań w pozostałych godzinach
- Analiza malware'u
- Konsultacje ekspertów ComCERT
- Zarządzanie scenariuszami
- Ocena bezpieczeństwa
- Zarządzanie źródłami Threat Intelligence
- Forensics
- Usługi skanów podatności

Doradztwo i audyty bezpieczeństwa

ComCERT ma w swoim portfolio szereg usług audytowych związanych z obowiązującymi normami i regulacjami. Projekty te są dedykowane zarówno podmiotom medycznym, które chcą przeanalizować swoją strategię cyberbezpieczeństwa i dokonać identyfikacji działań wymaganych do osiągnięcia określonego poziomu cyberbezpieczeństwa, jak i tym, które potrzebują określonego rodzaju audytu w związku z wymaganiami prawnymi. Specjaliści ComCERT to certyfikowani audytorzy z wieloletnim doświadczeniem.

System Zarządzania Bezpieczeństwem Informacji

Audyt zgodności z Ustawą o krajowym systemie cyberbezpieczeństwa

Audyt stopnia dojrzałości zespołów cyberbezpieczeństwa (metodyki SIM3/ENISA)

Audyt zgodności z normami ISO 22301, ISO 27001

Tworzenie i podnoszenie kwalifikacji zespołów SOC, CSIRT/CERT oraz szkolenia dostosowane do potrzeb Klienta

KONTAKT

ul. Adama Branickiego 13
02-972 Warszawa

+48 22 112 06 83

biuro@comcert.pl
www.comcert.pl

ComCERT SA
Siedziba w Warszawie, 02-972, przy ul. Adama Branickiego 13.
Wpis do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000406425, NIP 5252524691