Security Operations Center

Zespół operatorów identyfikujących i zabezpieczających najbardziej krytyczne miejsca w organizacji.

Czym jest SOC?

SOC, dzięki synergii wielu rozwiązań oraz wymianie informacji pomiędzy nimi, pozwala odnaleźć szereg problemów związanych z bezpieczeństwem, które do tej pory były niezauważalne.

Security Operations Center jest miejscem, w którym bezpieczeństwo IT, informatyka śledcza, a także procedury i ludzie współpracują ze sobą tworząc wyższy poziom bezpieczeństwa.

Wyższy poziom bezpieczeństwa

Security Operations Center (SOC) czyli zaawansowany monitoring sieci jest miejscem, w którym bezpieczeństwo IT, procedury i zespoły tworzą efektywny system, który pozwala na śledzenie, wykrywanie, jak i zabezpieczenie najbardziej krytycznych miejsc w organizacji.

DATA CENTER

COIG

Tylko bieżąca wymiana informacji może ustrzec nas przed zagrożeniami i zapewnić pełną ochronę przed potencjalnymi atakami.

SOC to najbardziej zaawansowana usługa, która składa się z kilku elementów składowych:

- procesów i technologii służących do zarządzania i ulepszania stanu bezpieczeństwa organizacji
- ludzi - analityków bezpieczeństwa i inżynierów

Informacja o usłudze

Najważniejsze elementy usługi SOC to:

Oprogramowanie
Obejmuje oprogramowanie, którego moduły analizują dane z systemów teleinformatycznych, monitoruje i analizuje aktywność w sieciach, serwerach, bazach danych, aplikacjach, witrynach internetowych i innych systemach, wyszukując luki, które mogłyby wskazywać na incydenty lub próby naruszenia bezpieczeństwa.

Analitycy bezpieczeństwa i inżynierowie
Drugim ważnym elementem usługi są analitycy bezpieczeństwa i inżynierowie nadzorujący kluczowe procesy związane z bezpieczeństwem. Pracownicy SOC monitorują i reagują na zdarzenia oraz pomagają zapewnić organizacjom szybkie wykrycie incydentu oraz podejmują działania zaradcze korzystając z dedykowanych narzędzi.

Zespół SOC

Zespół SOC prowadzi monitorowanie, analizę i rozwiązywanie incydentów pojawiających się w nadzorowanych systemach. Zapewnia kontrolę aktualnego stanu bezpieczeństwa poprzez wykrywanie incydentów za pośrednictwem oprogramowania SIEM oraz reagowanie na pojawiające się zdarzenia przy użyciu modułu SOAR.

Wdrożenie i świadczenie usługi SOC poprzedzone jest audytem teleinformatycznym infrastruktury klienta, dzięki czemu możliwe jest dokonanie inwentaryzacji, wskazanie kluczowych serwerów oraz przyspieszenie prac wdrożeniowych.

W skład zespołu SOC wchodzą doświadczeni eksperci posiadający poniższe certyfikaty

- CISM
- CDPSE
- audytor wiodący ISO 27001
- audytor wiodący ISO 22301

Zadania zespołu SOC

Efektywne zarządzanie cyberbezpieczeństwem firmy umożliwia zminimalizowanie zagrożeń.

Opis funkcjonalności:

01 identyfikacja, klasyfikacja i obsługa incydentów oraz eliminacja tzw. false-positive

02 automatyczna i dynamiczna analiza ryzyka cyberzagrożeń dla procesów i zasobów na podstawie danych zgromadzonych i stale aktualizowanych w procesie inwentaryzacji

03 badanie ruchu sieciowego

06 badanie zawartości maili

07 zarządzanie podatnościami poprzez kompleksowe podejście do obsługi - systemy jakimi dysponujemy posiadają interfejsy integracji z wiodącymi rozwiązaniami do skanowania podatności

08 operacyjne zarządzanie i wykorzystywanie technologii bezpieczeństwa IT

09 przyjmowanie zgłoszeń

10 gromadzenie i przechowywanie informacji o zdarzeniach z całej infrastruktury IT

11 monitorowanie stanu bezpieczeństwa systemów

12 automatyzacja zadań analizy i reakcji na incydenty - przebieg prac odbywa się zgodnie ze scenariuszami dostosowanymi do każdego etapu procesu obsługi incydentu (playbook)

13 analiza szczegółowa w ramach threat hunting - przeszukiwanie sieci w celu wykrywania i eliminacji zaawansowanych zagrożeń

14 monitorowanie działań użytkowników i administratorów

15 gromadzenie i zabezpieczanie dowodów, śladów i logów

16 w ramach analizy powłamaniowej i informatyki śledczej m.in. namierzenie i śledzenie atakującego, analiza złośliwego oprogramowania

Wdrożenie i świadczenie usługi SOC poprzedzone jest audytem teleinformatycznym infrastruktury klienta, dzięki czemu możliwe jest dokonanie inwentaryzacji, wskazanie kluczowych serwerów oraz przyspieszenie prac wdrożeniowych.