

Bezpieczeństwo to proces – wybierz etap, od którego chcesz zacząć

Cyber zagrożenia nieustannie ewoluują, dlatego skuteczna ochrona nie może być jednorazowym działaniem. To ciągły proces wymagający wiedzy, technologii i szybkiej reakcji. Usługa SOC (Security Operations Center) to kompleksowe wsparcie ekspertów, które pozwala nie tylko wykrywać incydenty bezpieczeństwa, ale też im skutecznie przeciwdziałać – 24/7/365.

Modele subskrypcji usługi SOC

W zależności od potrzeb i dojrzałości Twojej organizacji, oferujemy trzy modele subskrypcyjne. Niezależnie, czy dopiero zaczynasz swoją drogę z cyberbezpieczeństwem, czy szukasz zaawansowanego centrum operacyjnego z pełnym pakietem proaktywnych usług – mamy dla Ciebie odpowiednie rozwiązanie.



MDR (Managed Detection and Response)

Podstawowe monitorowanie końcówek i firewalli

Idealne na start – ochrona 24/7 urządzeń końcowych z wykorzystaniem EDR/XDR i firewalli



SOC na start

Rozszerzona ochrona oparta na analizie zdarzeń

Całodobowy monitoring SIEM/EDR/NDR, zbieranie logów i jedna kampania phishingowa rocznie



SOC Advanced

Pełne wsparcie dla wymagających organizacji

Cztery kampanie phishingowe, dark web monitoring i regularne testy Red Team – kompleksowa ochrona

Sprawdź, czym różnią się poniższe modele subskrypcji

Monitorowanie i alertowanie	MDR	SOC na start	SOC Advanced
Analizowanie incydentów 24/7/365 Zespół SOC w zależności od ustalonego SLA bada alarmy i potencjalne zagrożenia, eliminuje fałszywe alarmy, ustala priorytety dla alarmów. Działanie w trybie całodobowym	✓	✓	✓
Tworzenie scenariuszy bezpieczeństwa Zespół we współpracy i koordynacji z Klientem tworzy scenariusze bezpieczeństwa, np. na wypadek ataku phishingowego lub ransomware	✓	✓	✓
Utrzymywanie aktualności reguł Zespół analityków stale aktualizuje reguły i dostosowuje je do infrastruktury Klienta	✓	✓	✓
Threat Intelligence Dostarczanie informacji o potencjalnie nowych zagrożeniach, atakach i sposobach postępowania z nimi	✓	✓	✓
Skanowanie podatności sieci WAN Skanowanie sieci WAN Klienta w poszukiwaniu możliwych podatności. Częstotliwość: raz w miesiącu		✓	✓

Reagowanie na zdarzenia, raportowanie i doradztwo	MDR	SOC na start	SOC Advanced
Koordinowanie reakcji na incydent 24/7/365 Analitycy SOC razem z Klientem reagują na incydent. Działanie w trybie całodobowym	✓	✓	✓
Reagowanie na incydent 24/7/365 Zespół SOC automatycznie reaguje na incydent na podstawie wcześniej ustalonych scenariuszy, na przykład poprzez izolację hosta, zabicie procesu czy dodanie reguły na firewall. Działanie w trybie całodobowym			✓
Raporty Częstotliwość automatycznych raportów podsumowujących działania SOC	1/miesiąc	1/miesiąc	1/tydzień
Kontakt z CSIRT Zespół SOC jest przydzielony jako kontakt z sektorowym CSIRT			✓

Usługi proaktywne	MDR	SOC na start	SOC Advanced
Wsparcie architekta bezpieczeństwa Ilość godzin wsparcia w miesiącu, które Klient otrzymuje w celu analizy i poprawy infrastruktury bezpieczeństwa	2h	4h	10h
Kampania phishingowa Częstotliwość wykonywania kampanii phishingowych w roku. Brak ograniczeń odnośnie skali kampanii		1	4

Monitorowanie dark web Monitorowanie wycieków danych i hasel oraz tzw. black marketu		Add-on	✓
Red Team Regularne testy wykonywane przez zespół red team w celu proaktywnego wykrywania potencjalnych wektorów ataku			✓

Technologie	MDR	SOC na start	SOC Advanced
EDR / XDR Wykorzystanie dedykowanych systemów w celu monitorowania, analizy i reakcji na zagrożenia w punktach końcowych takich jak komputery, laptopy czy serwery <i>Wykorzystywane rozwiązania: CrowdStrike Falcon, Elastic XDR, Microsoft Defender XDR</i>	✓	✓	✓
Vulnerability Management Wykorzystywanie systemów do zarządzania podatnościami w celu identyfikacji, eliminacji słabych punktów w sieciach LAN <i>Wykorzystywane rozwiązania: CrowdStrike Falcon, Elastic XDR, Microsoft Defender Vulnerability Management</i>	✓	✓	✓
SIEM Narzędzie do zbierania logów z infrastruktury Klienta, przechowywania, korelacji oraz alarmowania <i>Wykorzystywane rozwiązania: Elastic SIEM, Splunk Enterprise Security, CrowdStrike Falcon Next-Gen SIEM</i>		✓	✓
Machine Learning Wykorzystanie uczenia maszynowego do analizy dużych zbiorów danych w celu identyfikowania anomalii w ruchu sieciowym czy działaniach użytkowników			✓
SOAR Wykorzystanie narzędzia w celu skrócenia czasu reakcji poprzez reagowanie na incydenty w sposób zautomatyzowany <i>Wykorzystywane rozwiązania: Splunk SOAR, TheHive, CrowdStrike Falcon Fusion SOAR</i>			✓
Threat Intelligence PRO Wykorzystanie dedykowanego systemu w celu dostarczania informacji o potencjalnie nowych zagrożeniach, atakach i sposobach postępowania z nimi <i>Wykorzystywane rozwiązania: CrowdStrike Falcon, Recorded Future</i>		Add-on	Add-on

**Nie jesteś pewien, jaki model wybrać?
Zapraszamy do kontaktu z Działem Sprzedaży.**

[Skontaktuj się z nami](#)