trecom

Mapa priorytetów technologicznych, procesowych i organizacyjnych w cyberbezpieczeństwie i bezpieczeństwie informacji.

Infografika

Sprawdź swoją dojrzałość w 9 filarach bezpieczeństwa.

Priorytety technologiczne i procesowe w bezpieczeństwie organizacji

Poziom potrzeb i dojrzałości	**Ochrona endpointów i urządzeń**	**Technologie sieciowe i infrastruktura**	**Zarządzanie dostępem i tożsamością**	**Zarządzanie podatnościami i poprawkami**	**Bezpieczeństwo danych**	**Kompetencje i świadomość pracowników**	**Procesy i zarządzanie bezpieczeństwem**	**Monitoring i reagowanie na zagrożenia**	**Usługi zewnętrzne**
Podstawowy	NextGen Antywirus, podstawowy EDR, aktualizacje OS, podstawowy hardening.	Firewall podstawowy, VPN, podstawowa segmentacja, podstawowe SD-WAN (proste zarządzanie ruchem, podstawowe QoS).	Podstawowe zarządzanie tożsamością (silne hasła), proste SSO, podstawowa kontrola ról i uprawnień w AD.	Podstawowe skanowanie podatności, ręczne zarządzanie poprawkami, podstawowe testowanie i wdrażanie łatek.	Ochrona poczty (antyspam, antyphishing), podstawowe zarządzanie danymi, podstawowe backupy (regularne kopie, lokalne przechowywanie).	Obowiązkowe szkolenia wprowadzające, cykliczne szkolenia podstawowe, kampanie awareness	Podstawowe polityki bezpieczeństwa, zarządzanie hasłami, reakcja ad hoc na incydenty, podstawowa segmentacja ról i separacja obowiązków (Tiering).	Platforma do zbierania logów oraz podstawowej korelacji i analizy zdarzeń bezpieczeństwa, podstawowa detekcja oraz analiza incydentów.	Podstawowy audyt bezpieczeństwa, reakcja ad hoc na incydenty, wsparcie IT w zakresie bezpieczeństwa (CISO as a Service oraz szacowanie i analiza ryzyk).
Średniozaawansowany	Zaawansowany EDR, XDR, kontrola aplikacji, MDM, cykliczny hardening.	MFA, IDS/IPS, zaawansowana segmentacja, VPN z MFA, ochrona DDoS, NDR, SD-WAN z funkcjami bezpieczeństwa (NGFW, UTM, SSL Inspection, zaawansowane QoS i routing aplikacyjny), XDR.	Systemy IAM z automatyzacją cyklu życia użytkownika, PAM, SSO z integracją, Least Privilege Access, wprowadzenie modelu Zero Trust dla AD.	Regularne skanowanie podatności, automatyzacja wykrywania i dystrybucji poprawek, harmonogramowanie wdrożeń, testowanie łatek.	Systemy DLP, zarządzanie podatnościami, ochrona poczty i komunikacji, szyfrowanie danych, szyfrowanie backupów z zabezpieczeniami (szyfrowanie, offline/immutable kopie, zgodność z RTO/RPO), WAF.	Cykliczne szkolenia łączące teorię z praktyką, regularne testy i kampanie phishingowe, symulacje ataków socjotechnicznych, programy certyfikacji wewnętrznej, budowa kultury bezpieczeństwa	Formalne procedury zarządzania incydentami, audyty, zarządzanie ryzykiem, testy penetracyjne, podstawowa automatyzacja SOAR, segmentacja sieciowa i separacja ról administracyjnych (Tiering).	SIEM, tworzenie i modyfikacja reguł, monitoring, automatyczna korelacja zdarzeń, SOC, podstawowe analizy forensic, raportowanie i eskalacja incydentów, monitorowanie Dark Web, monitorowanie aktywności i anomalii w AD.	Monitoring bezpieczeństwa co najmniej elementów krytycznych środowiska ICT lub SOC, współpraca z CSIRT, automatyzacja procesów, wsparcie w zarządzaniu incydentami, audyty bezpieczeństwa, usługi forensic na poziomie podstawowym.
Zaawansowany	Automatyzacja reakcji EDR/XDR, sandboxing, ochrona przed ransomware, ciągły hardening.	Zero Trust Network Access, mikrosegmentacja, SASE, NDR, XDR, zaawansowany SD-WAN (pełna integracja bezpieczeństwa, AI-driven routing, segmentacja mikro, zaawansowane zabezpieczenia WAN).	Zaawansowane IAM z adaptacyjnym uwierzytelnianiem (MFA, uwierzytelnianie kontekstowe), zaawansowane PAM, pełna implementacja Least Privilege Access, Zero Trust, rozbudowane SSO, zaawansowane polityki ochrony kont i sesji, ciągłe monitorowanie i analiza zachowań w AD	Zaawansowane zarządzanie podatnościami z integracją w SIEM, pełna automatyzacja patch management, testy regresji poprawek, raportowanie i audyt.	Zaawansowana integracja DLP z procesami biznesowymi, ochrona API i serwerów aplikacyjnych, WAF, ochrona systemów chmurowych i SaaS, szyfrowanie end-to-end, backupy z wielowarstwową ochroną (immutable storage, CDR, multiscanning, adaptive threat analysis).	Zaawansowane szkolenia, programy certyfikacji wewnętrznej z wielopoziomową strukturą, symulacje ataków, ćwiczenia red team i blue team, programy Bug Bounty, stały monitoring poziomu wiedzy i świadomości, analiza efektywności programów szkoleniowych. Promowanie kultury bezpieczeństwa jako wartości organizacyjnej, angażowanie wszystkich szczebli zarządzania,	Strategiczne zarządzanie ryzykiem, ciągłe doskonalenie, integracja z IT, zaawansowane testy penetracyjne, zaawansowany SOAR, pełna segmentacja ról administracyjnych (Tiering), zabezpieczenie replikacji AD, polityki ograniczające lateral movement.	SOC wspierany przez usługi zaawanasowane, w tym inżynierę detekcji, informatykę śledczą, zaawansowane SOAR, Threat Intelligence, automatyczne wykrywanie i reagowanie na zagrożenia dzięki XDR i NDR, pełne analizy forensic, monitorowanie Dark Web, zaawansowane monitorowanie i analiza aktywności w AD.	SOC wspierany przez usługi zaawanasowane, w tym inżynierę detekcji, informatykę śledczą, wsparcie w reagowaniu na incydenty i zarządzaniu kryzysowym, zaawansowane usługi forensic.

trecom | Cisco Partner

Potrzebujesz pomocy w obszarze NIS 2 lub UoKSC?

Umów się na bezpłatną konsultację i otrzymaj konkretne rekomendacje.

marketing@trecom.pl

O Trecom

Jako Trecom od ponad 25 lat rozwijamy, optymalizujemy i utrzymujemy złożone systemy IT. Jesteśmy jednym z liderów rynku polskiego w segmencie sieci, cyberbezpieczeństwa, systemów AV, UC oraz data center. Nasz zespół składa się z ponad 115 inżynierów i architektów.

Posiadamy ponad 70 partnerstw technologicznych z wiodącymi dostawcami technologii oraz obszerną ofertę szkoleń. Rozbudowane portfolio rozwiązań przekłada się na niemal nieograniczone możliwości projektowe.

Nasza oferta obejmuje audyt, doradztwo, projektowanie, wdrażanie oraz utrzymywanie infrastruktury IT oraz cyberbezpieczeństwa. Wspieramy naszych klientów również poprzez usługi zarządzane – SOC, NOC i Centrum Wsparcia.