MATRYCA PRODUKTOWA

DAGMA
BEZPIECZEŃSTWO IT

Lokalne Centra Cyberbezpieczeństwa

Jak rozwiązania z portfolio DAGMA wspierają minimalny zakres zadań LCC

Materiał porządkuje siedem obszarów wskazanych w przekazanym załączniku „Minimalny zakres zadań LCC" i zestawia je z rozwiązaniami z portfolio DAGMA.
To mapa technologiczna do pierwszej analizy projektu - nie katalog zakupowy i nie potwierdzenie automatycznej zgodności projektu z wymaganiami naboru.

OBSZAR LCC	ESET	SEKOIA	ACRONIS	HOLM SECURITY	SEGURA	STORMSHIELD	SAFETICA	GATEWATCHER	BARRACUDA
1 Obsługa cyberzagrożeń i incydentów	●	●	●					●	
2 Zarządzanie aktywami i wsparcie SZBI	●		●						
3 Bezpieczne wersje oprogramowania, aktualizacje i podatności	●		●	●					
4 Zarządzanie uprawnieniami dostępu	●				●				
5 Ochrona danych i kopie zapasowe	●		●			●	●		●
6 Bezpieczeństwo komunikacji i poczty elektronicznej	●		●				●		●
7 Cyberhigiena i rozwój kompetencji pracowników	●		●	●					●

Jak czytać matrycę? Niebieska kropka oznacza, że dane rozwiązanie zostało przypisane do danego obszaru w przygotowanym zestawieniu.
Szczegółowe role technologii znajdują się na kolejnych stronach.

CYBERSECURITY FROM EUROPE

Szczegółowe mapowanie technologii

Poniższe opisy zostały zredagowane dla czytelności na podstawie przekazanych materiałów produktowych i minimalnego zakresu zadań LCC.

1

Obsługa cyberzagrożeń i incydentów

Powiązanie regulacyjne: Zał. 4 do ustawy o KSC: pkt I.12 i I.18; ustawa o KSC: art. 8 ust. 1 pkt 2 lit. f), pkt 4 oraz pkt 5 lit. d).

ESET	ESET Inspect i AI Advisor - wsparcie detekcji, analizy i obsługi zdarzeń bezpieczeństwa.
Sekoia	Zarządzanie incydentami, detekcja zagrożeń oraz natywna integracja z listami IOC (Indicator of Compromise).
Acronis	Centralne zarządzanie cyberbezpieczeństwem i incydentami oraz wsparcie ciągłości działania przez odtworzenie kluczowej infrastruktury lokalnie lub w zasobach chmurowych producenta (Cyber Protect / Disaster Recovery).
Gatewatcher	NDR (Network Detection and Response): widoczność ruchu w środowiskach IT i OT, detekcja znanych i nieznanych zagrożeń, analiza behawioralna, Threat Hunting, analiza incydentów, alertowanie w czasie rzeczywistym i automatyzacja reakcji.

2

Zarządzanie aktywami i wsparcie SZBI

Powiązanie regulacyjne: Zał. 4 do ustawy o KSC: pkt I.1; ustawa o KSC: art. 8 ust. 1 pkt 2 lit. m).

ESET	Raporty i dashboardy wspierające widoczność zarządzanego środowiska.
Acronis	Inwentaryzacja sprzętu i oprogramowania (Hardware and Software Inventory) w Acronis Cyber Protect.

3

Bezpieczne wersje oprogramowania, aktualizacje i zarządzanie podatnościami

Powiązanie regulacyjne: Zał. 4 do ustawy o KSC: pkt I.2 oraz I.15-I.16; ustawa o KSC: art. 8 ust. 1 pkt 3 oraz pkt 5 lit. b).

ESET	Vulnerability & Patch Management - identyfikacja podatności i wsparcie zarządzania aktualizacjami.
Acronis	Skanowanie i zarządzanie podatnościami oraz audyt w oparciu o bazy CVE.
Holm Security	Wyszukiwanie podatności w systemach, również OT, oraz w aplikacjach webowych.

4 Zarządzanie uprawnieniami dostępu

Powiązanie regulacyjne: Zał. 4 do ustawy o KSC: pkt I.4-I.7; ustawa o KSC: art. 8 ust. 1 pkt 2 lit. n).

Segura — Kontrola dostępu do systemów, urządzeń i poświadczeń uprzywilejowanych przez Access Groups / Access Policies; zasada najmniejszych uprawnień; ograniczenia czasowe; wielopoziomowa akceptacja; uzasadnienie dostępu; recertyfikacja i audit log; możliwość szybkiej dezaktywacji lub zmiany zakresu uprawnień.

ESET — ESET Secure Authentication - uwierzytelnianie wieloskładnikowe jako dodatkowa warstwa kontroli dostępu.

5 Ochrona danych w systemach informacyjnych, w tym kopie zapasowe

Powiązanie regulacyjne: Zał. 4 do ustawy o KSC: pkt I.3 lit. b), I.10-I.11 oraz I.13; ustawa o KSC: art. 8 ust. 1 pkt 2 lit. f) oraz pkt 5 lit. a) i c).

ESET — ESET Secure Authentication oraz Full Disk Encryption - dodatkowe mechanizmy ochrony dostępu i danych.

Acronis — Backup endpointów, serwerów i maszyn wirtualnych, z możliwością przechowywania kopii poza lokalizacją, w tym w chmurze w Polsce.

Stormshield — Warstwa sieciowa wspierająca poufność, integralność i dostępność: firewall, IPS, VPN, HA; monitoring ruchu; VPN IPSec/SSL; MFA dla VPN; segmentacja i kontrola dostępu; logi i raporty wspierające obsługę incydentów; mechanizmy ograniczające skutki incydentu.

Barracuda — Backup Service oraz Cloud-to-Cloud Backup: ochrona serwerów, aplikacji i danych lokalnych oraz Microsoft 365; lokalne i chmurowe kopie, granularne odzyskiwanie, Rapid Recovery, ochrona po ransomware i Disaster Recovery.

Safetica — Safetica zabezpiecza dane na komputerach pracowników przed wyciekiem poprzez kontrolę przepływu informacji, klasyfikację danych oraz egzekwowanie polityk ochrony danych na endpointach.

6 Kontrola bezpieczeństwa komunikacji i poczty elektronicznej

Powiązanie regulacyjne: Zał. 4 do ustawy o KSC: pkt I.9; ustawa o KSC: art. 8 ust. 1 pkt 2 lit. l).

ESET — Mail Security / Cloud Office Security - ochrona poczty i środowisk komunikacyjnych.

Acronis — Wielowarstwowa ochrona poczty e-mail, a dodatkowo backup i archiwizacja skrzynek pocztowych.

Safetica — Monitorowanie informacji przesyłanych przez klienta pocztowego, blokowanie prób wysłania danych wrażliwych oraz klasyfikacja treści na endpointach.

Barracuda — Email Gateway Defense i M365 Protection: ochrona przed spamem, phishingiem, malware i złośliwymi linkami; ciągłość poczty, backup M365 oraz Incident Response dla złośliwych wiadomości.

7 Cyberhigiena i doskonalenie kompetencji pracowników

Powiązanie regulacyjne: Zał. 4 do ustawy o KSC: pkt I.14 oraz I.17 lit. a-d; ustawa o KSC: art. 8 ust. 1 pkt 2 lit. d), i) oraz j).

ESET	Cybersecurity Awareness Training - rozwój świadomości i cyberhigieny pracowników.
Acronis	Security Awareness Training w języku polskim, możliwość wykorzystania własnych materiałów, testy kompetencji i świadomości oraz kampanie phishingowe
Holm Security	Phishing & Awareness Training - szkolenia i symulacje phishingowe wspierające rozwój świadomości użytkowników.
Barracuda	Security Awareness - szkolenia użytkowników i symulacje phishingowe wspierające rozwój świadomości bezpieczeństwa.

Ważne! Matryca pokazuje, w jaki sposób wskazane technologie mogą wspierać poszczególne obszary LCC. Dobór rozwiązania, jego konfiguracja, zakres usług oraz sposób organizacji procesów powinny zostać każdorazowo zweryfikowane dla konkretnego partnerstwa JST. Samo wdrożenie produktu nie oznacza automatycznego spełnienia wymagań programu lub przepisów.

Masz pytania? Skontaktuj się z nami!

kontakt@dagma.pl / +48 32 259 11 01

www.dagma.eu

DAGMA
BEZPIECZEŃSTWO IT

CYBERSECURITY FROM EUROPE