STRATEGIA CYBERBEZPIECZEŃSTWA W KONTEKŚCIE NIS2

Piotr Czarnecki

Wiceprezes Zarządu NetFormers

Sebastian Strzelak

Prezes Zarządu NetFormers

Dyrektywa NIS 2

Strategia bezpieczeństwa oczami Zarządu NetFormers

Sebastian Strzelak
Piotr Czarnecki

NetFormers
Warszawa, 23.04.2024 r

Czym się zajmujemy od 13 lat?

- Monitoring ruchu
- Integracja systemów
- Bezpieczeństwo sieciowe
- Rozwiązania sieciowe
- Usługi doradcze

NETFORMERS

NetFormers w liczbach

13 lat
doświadczenia na rynku

40
wykwalifikowanych pracowników

> 700
zadowolonych klientów

> 1200
zrealizowanych projektów

NETFORMERS

Współpracujemy z wiodącymi dostawcami rozwiązań cybersecurity na rynku

GŁÓWNI PARTNERZY:

FORTINET

CISCO

LiveAction

radware

IBM

JUNIPER NETWORKS

Extreme networks

BlackBerry

KELA

Infoblox

BACKBOX

INGRAM MICRO

NETFORMERS

Rozwijamy się nieustannie

3x

DIAMENTY FORBESA

Jesteśmy trzykrotnymi laureatami nagrody przyznawanej firmom, które w ostatnich latach odnotowały ponadprzeciętną dynamikę wzrostu przychodów.

Diamenty Miesięcznika Forbes 2024

Diamenty Miesięcznika Forbes 2023

Diamenty Miesięcznika Forbes 2022

NETFORMERS

Cybersecurity nie ma dla nas tajemnic

W 2022 zostaliśmy wyróżnieni nagrodą **Cisco Partner of the Year** w kategorii Cybersecurity.

W 2023 zostaliśmy wyróżnieni nagrodą **Cisco Marketing** za TOPową ilość skutecznych działań marketingowych

Referencje

KLIENCI KOMERCYJNI I PUBLICZNI

Każdego dnia wytrwale pracujemy na zaufanie naszych Klientów.

Z dumą prezentujemy opinie wystawione przez Firmy zadowolone ze współpracy.

z NetFormers. Wierzymy, że Twoja firma również dołączy do tego grona.

Klienci Komercyjni:

GENERALI · wiener VIENNA INSURANCE GROUP · mBank · PKO Finat

atman non-stop-data 100% · T-Mobile · NETIA · Anwim

CD PROJEKT · synevo · Radial powering bpostgroup

Klienci Publiczni:

KOMENDA GŁÓWNA POLICJI · ZUS ZAKŁAD UBEZPIECZEŃ SPOŁECZNYCH · NFZ Narodowy Fundusz Zdrowia · COI centralny ośrodek informatyki

ARiMR Agencja Restrukturyzacji i Modernizacji Rolnictwa · Ministerstwo Rolnictwa i Rozwoju Wsi · Warmińsko-Mazurski Urząd Wojewódzki w Olsztynie

KATOLICKI UNIWERSYTET LUBELSKI JANA PAWŁA II KUL 1918 · PSK Politechnika Świętokrzyska · SGGW SZKOŁA GŁÓWNA GOSPODARSTWA WIEJSKIEGO

Certyfikaty

Zakres certyfikatów, jakie posiadają nasi inżynierowie:

CISCO | FORTINET

01 Certyfikaty Cisco

8x

6x

4x

1x

3x

2x

02 Certyfikaty Fortinet

4x

1x

2x

6x

NETFORMERS

Dyrektywa NIS2

NETFORMERS

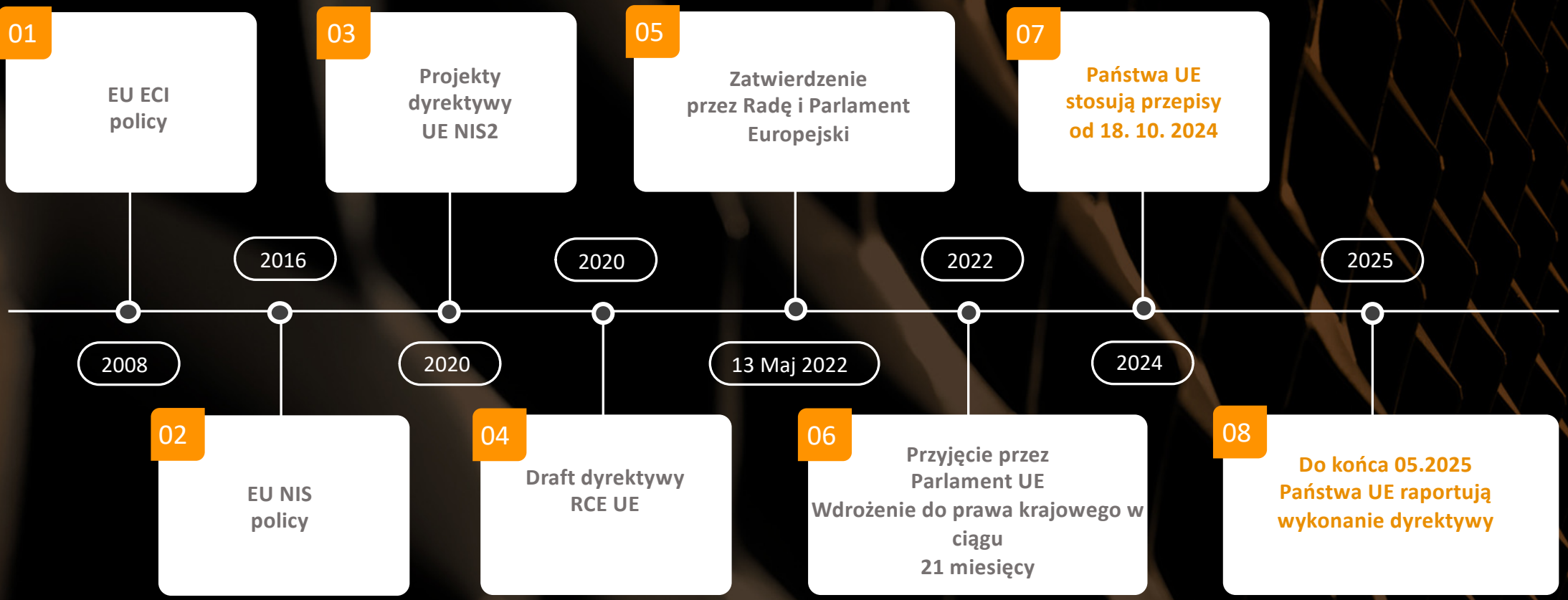
Dyrektywa (UE) 2022/2555 Parlamentu Europejskiego i Rady UE

z dnia 14 grudnia 2022 r.

- Zwiększenie poziomu świadomości sytuacyjnej EU
- Zmniejszenie niespójności w zakresie odporności cybernetycznej
- Zwiększenie poziomu cyberbezpieczeństwa

NETFORMERS

Kalendarz NIS2



NETFORMERS

Podmioty kluczowe – NIS2

- Bankowość (DORA)
- Infrastruktura rynku finansowego (DORA)
- Zdrowie
- Woda pitna
- Ścieki
- Infrastruktura cyfrowa
- Zarządzanie usługami ICT (między przedsiębiorstwami)
- Administracja publiczna
- Przestrzeń kosmiczna

Energia

- Elektryczność
- Wodór
- Sieci ciepłownicze i chłodnicze
- Olej
- Gaz

Transport

- Lotnictwo
- Transport wodny
- Kolejnictwo
- Transport drogowy

NETFORMERS

Podmioty ważne – NIS2

- Poczta i firmy kurierskie
- Gospodarka odpadami
- Produkcja i dystrybucja chemikaliów
- Produkcja i dystrybucja żywności
- Działalność wytwórcza
- Dostawcy usług cyfrowych
- Badania naukowe

Produkcja

- Urządzenia medyczne / diagnostyczne
- Komputery i elektronika
- Sprzęt elektryczny
- Maszyny i urządzenia (gdzie indziej niesklasyfikowane)
- Pojazdy mechaniczne, przyczepy
- Pozostałe urządzenia transportowe

NETFORMERS

Zadania NIS2

Uwierzytelnianie wieloskładnikowe

stosowanie rozwiązań w tym zakresie lub ciągłego uwierzytelniania,

Bezpieczeństwo łańcucha dostaw,

w tym związane z nim aspekty dotyczące relacji między każdym podmiotem a jego dostawcami

Bezpieczeństwo sieci i systemów informatycznych

w zakresie ich tworzenia, rozwoju i utrzymania, w tym obsługa podatności i ich wykrywania

Polityka i procedury

(testowanie i audyt) służące ocenie skuteczności środków zarządzania ryzykiem cybernetycznym

Podstawowe praktyki w zakresie higieny cyber

i szkolenia w zakresie cyberbezpieczeństwa;

Bezpieczeństwo zasobów ludzkich, polityka kontroli dostępu

i zarządzanie aktywami;

Ciągłość działania

i zarządzanie kryzysowe

Polityka bezpieczeństwa

analiza ryzyka i polityka bezpieczeństwa systemów informatycznych

Obsługa incydentów

zapobieganie, wykrywanie i reagowanie na incydenty)

Stosowanie kryptografii i szyfrowania

NETFORMERS dla zadania:

Analiza ryzyka i polityka bezpieczeństwa

systemów informatycznych

01 **Analiza stanu dokumentacji,** w tym polityki bezpieczeństwa (ewentualne przygotowanie polityki bezpieczeństwa)

02 **Weryfikacja procedur** i ich wykonywalności

03 **Opis i analiza ryzyk** oraz metod ich mitygacji

04 **Ocena obecnego stanu technicznego** doradztwo w zakresie rozwoju i doboru rozwiązań

NETFORMERS

Bezpieczeństwo sieci

i systemów informatycznych

NETFORMERS dla zadania:

SASE

Bezpieczny dostęp do usług brzegowych (w skrócie SASE) to chmurowa architektura zabezpieczeń, która łączy sieć rozległą zdefiniowaną programowo (SD-WAN) ze skonsolidowanym stosem zabezpieczeń dostarczanych w chmurze obejmującym składniki SWG, CASB, ZTNA i FWaaS.

Next Generation Firewall

Od lat serce rozwiązań bezpieczeństwa, które zapewnia firmom nie tylko ciągłość działania, ale także skuteczną ochronę przed zagrożeniami z zewnątrz. Dzięki wbudowanym zaawansowanym funkcjom bezpieczeństwa, takim jak application awareness and control, intrusion prevention, threat intelligence użytkownicy zyskują kolejny poziom ochrony na styku z siecią publiczną.

Secure Access

Bezpieczny dostęp ma na celu ochronę przed nieuprawnionym dostępem, wyciekiem danych i innymi zagrożeniami bezpieczeństwa poprzez wdrożenie kontroli i protokołów weryfikujących tożsamość i uprawnienia użytkowników lub systemów próbujących uzyskać dostęp do zasobów. Może to obejmować techniki takie jak uwierzytelnianie wieloskładnikowe, kontrola dostępu oparta na rolach, wirtualne sieci prywatne (VPN-y), warstwa bezpiecznego gniazda (SSL) oraz inne protokoły i technologie bezpieczeństwa.

NETFORMERS

Stosowanie kryptografii

i szyfrowania

NETFORMERS dla zadania:

Szyfrowanie sieci LAN (MACSEC)

to ustandaryzowane rozwiązanie bezpieczeństwa sieciowego, które zapewnia ochronę transmisji danych w korporacyjnych sieciach LAN poprzez szyfrowanie na poziomie warstwy łącza, co pomaga w zapobieganiu atakom na dane i zapewnia spójność z wymogami regulacyjnymi dotyczącymi prywatności danych.

- Przełączniki Cisco
- Przełączniki FortiSwitch
- Przełączniki Juniper
- Przełączniki Extreme Networks

SSL offload

to technika, która polega na przeniesieniu obciążenia związanego z szyfrowaniem SSL/TLS z serwerów aplikacyjnych na specjalnie przystosowane do tego urządzenia, takie jak sprzętowe urządzenia do balansowania obciążenia lub specjalne akceleratory kryptograficzne.

- Fortinet FortiADC
- F5 Big-IP
- Citrix NetScaler

Tunele VPN

to powszechnie znana i stosowana technologia używana przez wszystkich, którzy cenią sobie prywatność, bezpieczeństwo oraz wolność w korzystania z Internetu. Szyfrowanie transmisji zapewnia poufność oraz integralność przesyłanych informacji a zarazem zabezpiecza wewnętrzne zasoby firmy przed nieautoryzowanym dostępem z zewnątrz.

- Cisco FirePower NGF
- Fortinet FortiGate UTM

NETFORMERS

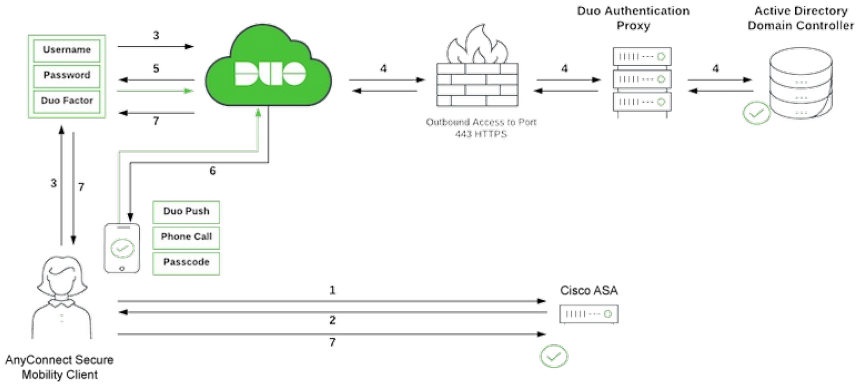
Stosowanie rozwiązań (MFA)

w zakresie uwierzytelniania wieloskładnikowego lub ciągłego uwierzytelniania

NETFORMERS dla zadania:

Cisco DUO

Cisco DUO to rozwiązanie zabezpieczeń skoncentrowane na wieloczynnikowym uwierzytelnieniu (MFA) oraz bezpieczeństwie dostępu



Forti Authenticator + Forti Token

Fortinet również oferuje rozwiązanie (MFA) oparte o serwer uwierzytelniający współpracujący z tokenami mobilnymi oraz sprzętowymi

FORTINET®

FortiToken Strong Authentication

NETFORMERS

Bezpieczeństwo zasobów ludzkich

polityka kontroli dostępu i zarządzanie aktywami

NETFORMERS dla zadania:

Network Admission Control (NAC)

NAC to rozwiązanie, które zapewnia bezpieczne zarządzanie dostępem do sieci firmowej. Oferuje pełną kontrolę nad tym, kto łączy się z Twoją siecią, skąd to robi i z jakiego urządzenia korzysta. Zarządzanie dostępem przeprowadzane jest z jednej centralnej lokalizacji. W związku z tym znacznie ułatwia i usprawnia cały proces i zapewnia spójność polityk bezpieczeństwa w sieciach LAN, WAN i VPN.

01 **Kto?** user

02 **Kiedy?** czas

03 **Skąd?** urządzenie

CISCO

FORTINET

Extreme networks

NETFORMERS

NETFORMERS dla zadania:

Podstawowe praktyki higieny cybernetycznej

i szkolenia z zakresu cyberbezpieczeństwa

01

Szkolenia dedykowane
budowanie świadomości zagrożeń, wzorce zachowań i reakcji na incydenty

02

Warsztaty techniczne
dla administratorów, mające na celu lepsze poznanie posiadanych narzędzi I nabycie umiejętności ich użycia

03

Raporty OSINT
pokazujące jak widać naszą organizację na zewnątrz i czego można się dowiedzieć bez łamania prawa

04

Threat Intelligence
monitoring aktywności różnego rodzaju grup w Internecie i Darknecie, daje sygnały ostrzegawcze przed potencjalnym atakiem lub wyciekiem danych

NETFORMERS

Bezpieczeństwo łańcucha dostaw

z uwzględnieniem kwestii bezpieczeństwa relacji pomiędzy podmiotami

NETFORMERS dla zadania:

Threat Intelligence Platform

- Dowiedz się o zagrożeniu, zanim zostaniesz ofiarą ataku

Zero Trust Network Access

- Nie ufaj nikomu, nie znasz, nie wpuszczaj, udostępniaj tylko to co konieczne (**Cisco/Fortinet/Extreme Networks**)

Full Stack Observability

- Kontroluj procesy od A do Z, awaria u dostawcy może zabić Twój biznes.

Cisco Thousand Eyes, AppDynamics, Intersight, **Live Action**

Threat Intelligence Platform to rozwiązanie, które wykrywa i informuje o konkretnych zagrożeniach cybernetycznych, ukierunkowanych bezpośrednio na daną organizację

Platforma działa jak tajny agent, który niepostrzeżenie uzyskuje informacje o potencjalnych zagrożeniach i dostarcza je klientom, zanim ci staną się ofiarami ataku. Może on informować o skradzionych hasłach, nieautoryzowanym sprzedaży danych firmowych lub nawet o planowanych atakach na infrastrukturę IT firmy.

KELA

NETFORMERS

Obsługa incydentów

zapobieganie, wykrywanie i reagowanie na incydent

NETFORMERS dla zadania:

Forti SIEM

Cisco Secure Network Analytics (StealthWatch)

- Monitorowanie ruchu sieciowego (NetFlow)
- Wykrywanie zagrożeń (algorytmy AI)
- Analiza zachowań użytkowników (wzorce)
- Reagowanie na zagrożenia (automatyzacja)

Cisco/Fortinet/BlackBerry XDR Extended Detection and Response

- Zbieranie i korelacja danych
- Wykrywanie zaawansowanych zagrożeń
- Automatyzacja odpowiedzi na incydenty
- Integracja i współpraca

NETFORMERS

Ciągłość działania

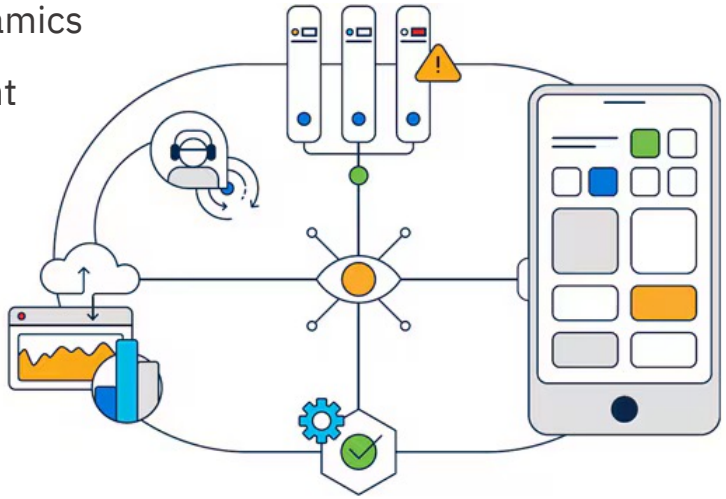
I zarządzania kryzysowe

NETFORMERS dla zadania:

Full Stack Observability

Cisco (FSO) to zaawansowane rozwiązanie do monitorowania i zarządzania wydajnością całej infrastruktury IT, od aplikacji po infrastrukturę sieciową i chmurową.

- Cisco ThousandEyes
- Cisco AppDynamics
- Cisco Intersight



BackBox

BackBox to elastyczne narzędzie do automatyzacji i zarządzania infrastrukturą sieciową, które zapewnia scentralizowaną kontrolę nad sprzętem sieciowym i bezpieczeństwem.

- Automatyczne tworzenie kopii zapasowych konfiguracji
- Zarządzanie zmianami
- Automatyzacja zadań
- Zarządzanie urządzeniami wielu producentów
- Raportowanie i analiza

BACKBOX

NETFORMERS

NETFORMERS dla zadania:

Polityki i procedury (testy i audyty)

oceniające skuteczność środków zarządzania ryzykiem cybernetycznym

01 **Analiza stanu dokumentacji,** w tym polityki bezpieczeństwa (ewentualne przygotowanie polityki bezpieczeństwa)

02 **Weryfikacja procedur** i ich wykonywalności

03 **Opis i analiza ryzyk** oraz metod ich mitygacji

04 **Przygotowanie rekomendacji** zmian i rozwoju

NETFORMERS

Podsumowując...

Thank You

Zapraszamy na kolejne sesje.