STORMSHIELD

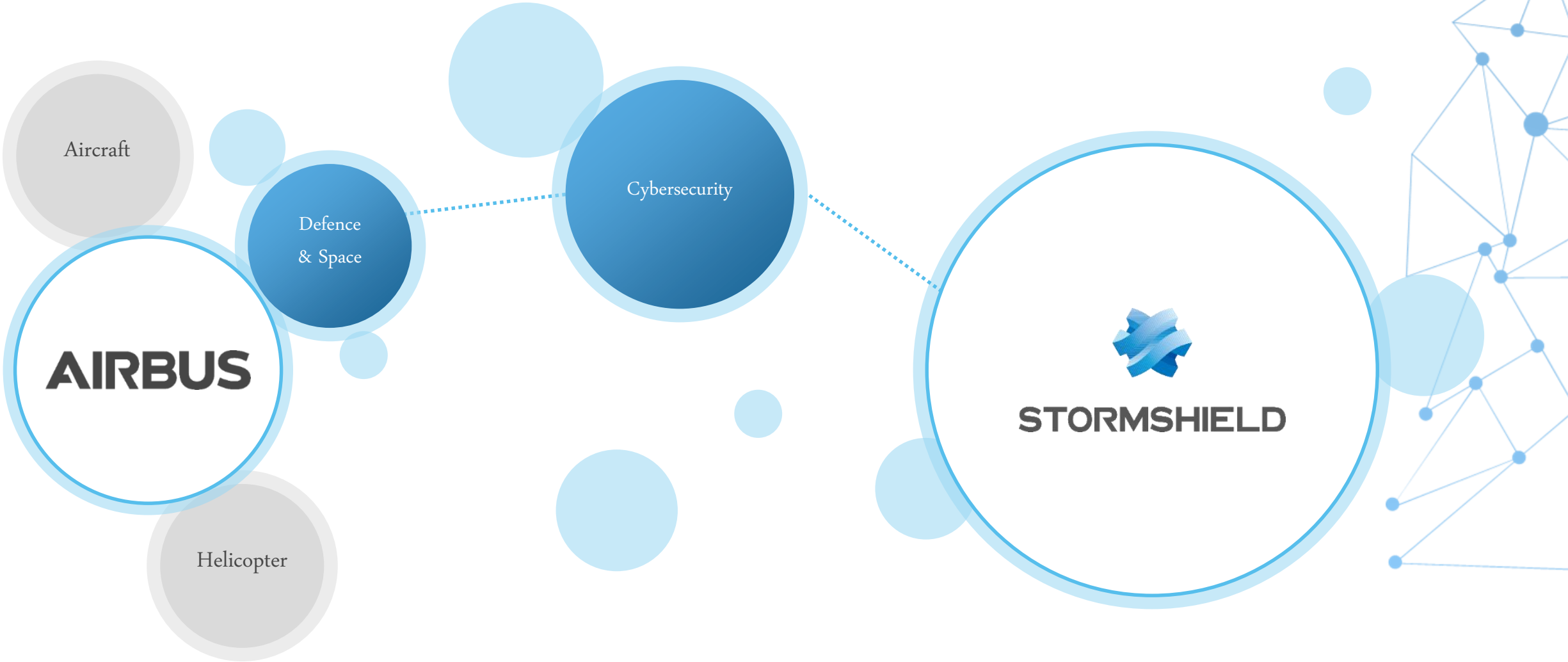
Network Endpoint Data

Zaawansowana ochrona sieci przemysłowych

GAZTERM 2021

Paweł Śmigielski
Błażej Buczyłko

Stormshield i Airbus



Bezpieczny europejski wybór

CYBERSECURITY™
MADE IN EUROPE

EU RESTRICTED

NATO

COMMON CRITERIA

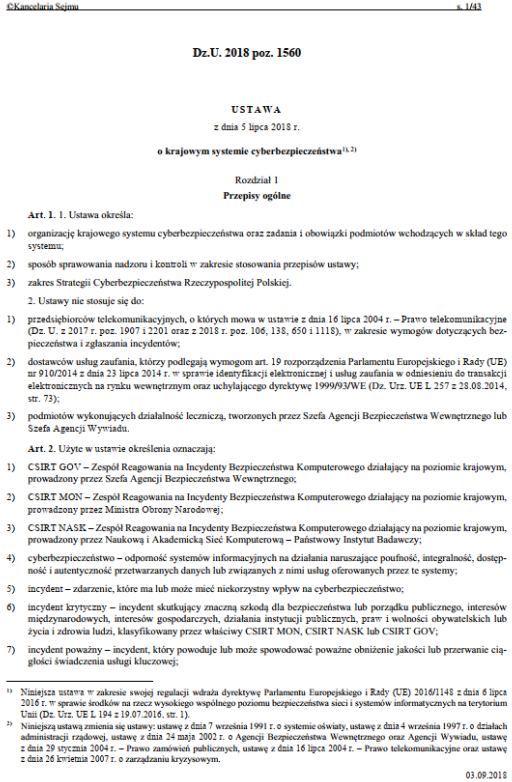
COMMON CRITERIA

Rozwiązania dostosowane do polskiego rynku

INTERFEJS WSPARCIE TECHNICZNE DOKUMENTACJA

Uwarunkowania prawne

Ustawa o KSC



©Kancelaria Sejmu s. 1/43

Dz.U. 2018 poz. 1560

USTAWA

z dnia 5 lipca 2018 r.

o krajowym systemie cyberbezpieczeństwa[1), 2)]

Rozdział 1

Przepisy ogólne

Art. 1. 1. Ustawa określa:

1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;
2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;
3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

2. Ustawy nie stosuje się do:

1) przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138, 650 i 1118), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;
2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73);
3) podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

Art. 2. Użyte w ustawie określenia oznaczają:

1) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
2) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;
3) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
4) cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
6) incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;
7) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;

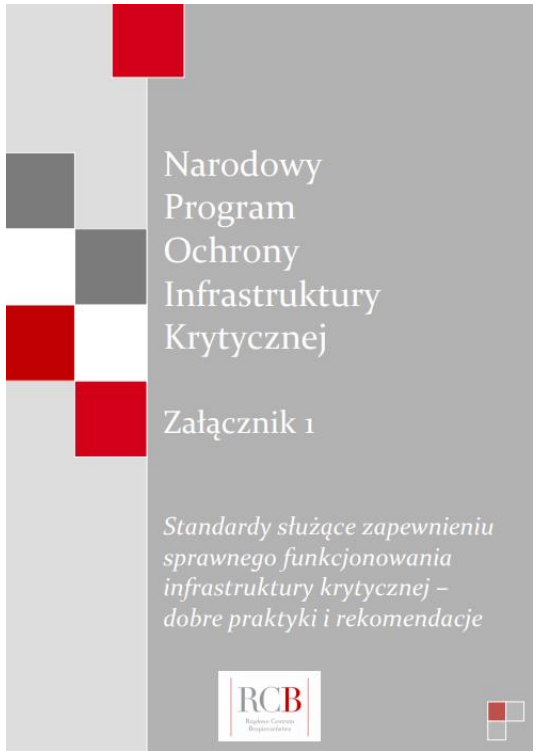
[1)] Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1).

[2)] Niniejszą ustawą zmienia się ustawy: ustawę z dnia 7 września 1991 r. o systemie oświaty, ustawę z dnia 4 września 1997 r. o działach administracji rządowej, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne oraz ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

03.09.2018

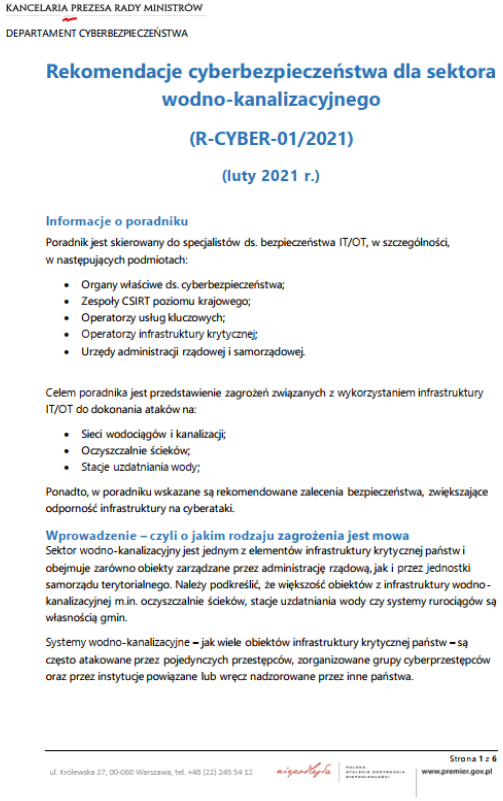
Zapewnienie bezpieczeństwa teleinformatycznego

- Bezpieczeństwo automatyki przemysłowej



Rekomendowane środki techniczne

- Rekomendacje 1-10



KANCELARIA PREZESA RADY MINISTRÓW

DEPARTAMENT CYBERBEZPIECZEŃSTWA

Rekomendacje cyberbezpieczeństwa dla sektora wodno-kanalizacyjnego

(R-CYBER-01/2021)

(luty 2021 r.)

Informacje o poradniku

Poradnik jest skierowany do specjalistów ds. bezpieczeństwa IT/OT, w szczególności, w następujących podmiotach:

- Organy właściwe ds. cyberbezpieczeństwa;
- Zespoły CSIRT poziomu krajowego;
- Operatorzy usług kluczowych;
- Operatorzy infrastruktury krytycznej;
- Urzędy administracji rządowej i samorządowej.

Celem poradnika jest przedstawienie zagrożeń związanych z wykorzystaniem infrastruktury IT/OT do dokonania ataków na:

- Sieci wodociągów i kanalizacji;
- Oczyszczalnie ścieków;
- Stacje uzdatniania wody;

Ponadto, w poradniku wskazane są rekomendowane zalecenia bezpieczeństwa, zwiększające odporność infrastruktury na cyberataki.

Wprowadzenie – czyli o jakim rodzaju zagrożenia jest mowa

Sektor wodno-kanalizacyjny jest jednym z elementów infrastruktury krytycznej państw i obejmuje zarówno obiekty zarządzane przez administrację rządową, jak i przez jednostki samorządu terytorialnego. Należy podkreślić, że większość obiektów z infrastruktury wodno-kanalizacyjnej m.in. oczyszczalnie ścieków, stacje uzdatniania wody czy systemy rurociągów są własnością gmin.

Systemy wodno-kanalizacyjne – jak wiele obiektów infrastruktury krytycznej państw – są często atakowane przez pojedynczych przestępców, zorganizowane grupy cyberprzestępców oraz przez instytucje powiązane lub wręcz nadzorowane przez inne państwa.

ul. Królewska 27, 00-060 Warszawa, tel. +48 (22) 245 54 12 www.premier.gov.pl Strona 1 z 6

Portfolio

Małe sieci i zdalne oddziały


SN160


SN160W


SN210


SN210W


SN310

Średnie i duże sieci


SN510


SN710


SN910

Sieci korporacyjne i data center


SN2100


SN3100


SN6100

Sieci przemysłowe



SNi20 SNi40

Maszyny wirtualne i rozwiązania chmurowe

Microsoft Azure
amazon web services
openstack
vmware
Microsoft Hyper-v
CITRIX
KVM

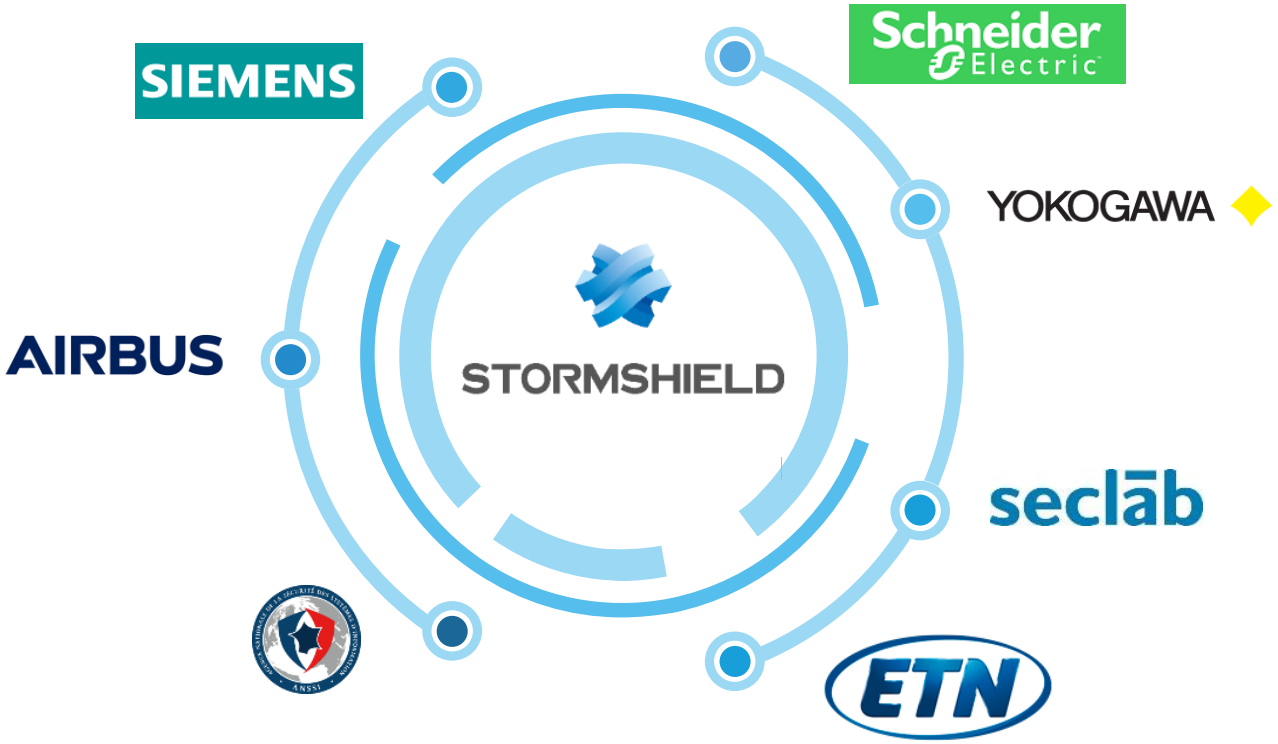
Rozwiązania dla sektora przemysłowego

IT/OT end to end protection

STORMSHIELD

Doświadczenie w przemyśle

Od ponad 10 lat, Stormshield zapewnia ochronę systemów OT oraz styku sieci IT/OT.



Unikalna oferta dla systemów przemysłowych

NETWORK SECURITY

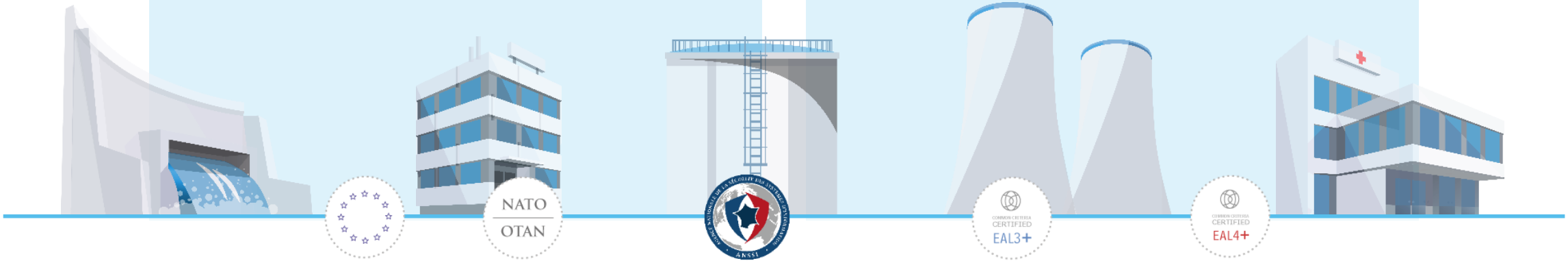
SNS - NETWORK SECURITY

Next-generation firewall

ENDPOINT SECURITY

SES - ENDPOINT SECURITY

Ochrona stacji roboczych



EU RESTRICTED

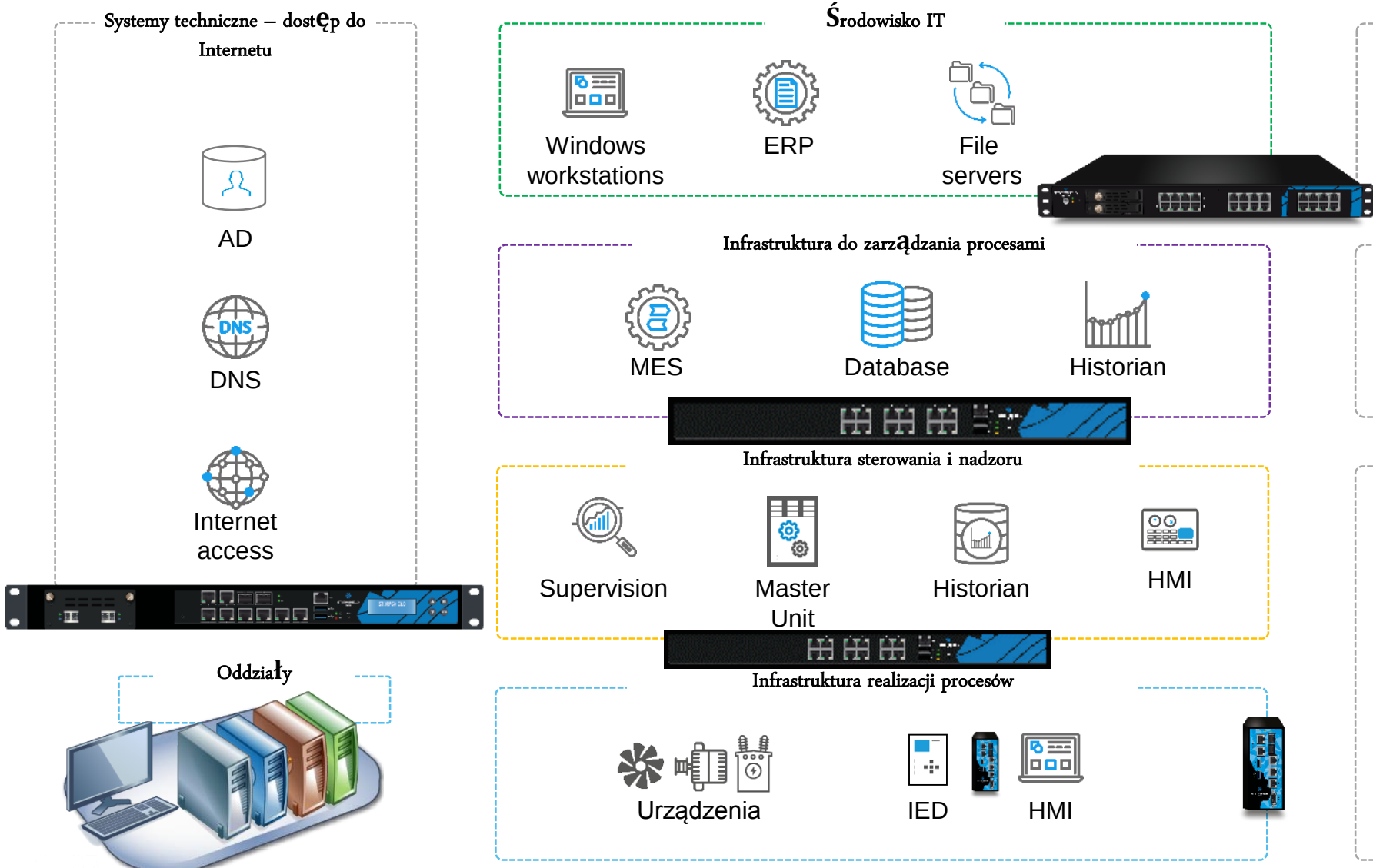
NATO

QUALIFIED INDUSTRIAL FW

COMMON CRITERIA

COMMON CRITERIA

Przykładowa segmentacja sieci



SNi20 i SNi40 – przemysłowe UTMy

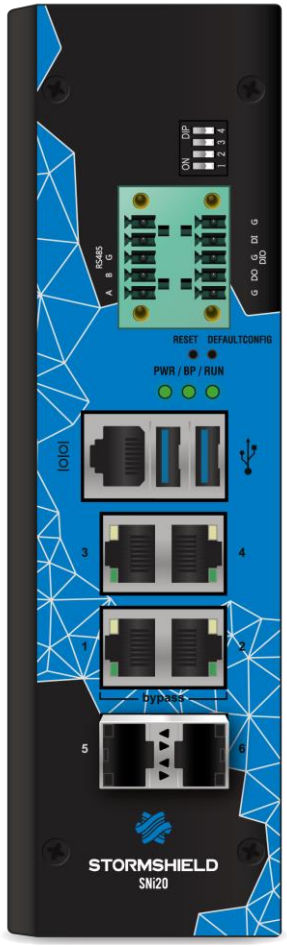
Funkcjonalności podstawowe

- Przemysłowy UTM (FW + IPS)
- VPN
- Bypass
- Obsługa protokołów przemysłowych na poziomie komend (DPI):

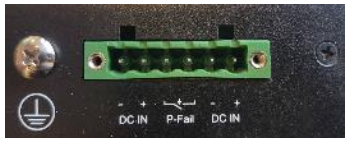
Modbus, UMAS, OPC, PROFINET, SIMATIC S7 SIEMENS, EtherNet/IP, ASHRAE BACnet

oraz
CIP (Rockwell)
IEC 60870-5-104
IEC 61850-3
(+ własne sygnatury)

SNi20 - parametry



• Wymiary	210 x 60 x 155 mm
• Waga	1,75 kg
• Montaż	szyna DIN 35 mm (Norma EN 50022)
• Zasilanie	2x12-48VDC 3-0.75A
• Zużycie (Idle) DC @+25°C	15 W
• Pobór mocy (max) DC @+25°C	19 W
• Temperatura pracy	-40° do +70°C
• Wilgotność względna (bez kondensacji)	0% do 95%
• Liczba wentylatorów	brak
• Pamięć	karta SD
• MTBF w 25°C	35,1 lat



Nasze projekty

Use cases

ZARZĄDZANIE SIECIĄ WODOCIĄGOWĄ

Ochrona End-to-end

Zabezpieczenie sieci dystrybucyjnej (Francja)

STORMSHIELD

ZARZĄDZANIE SIECIĄ WODOCIĄGOWĄ – Ochrona End to end

Topologia klienta

- 1 jednostka centralna
- 100 lokalizacji zdalnych

Wymagania klienta

- Bezpieczne połączenie do lokalizacji zdalnych

Wprowadzone zmiany

- Segmentacja z 5 barierami
- Kontrola i filtrowanie komunikacji z użyciem DPI
- VPN IPsec do ochrony połączeń
- Ochrona na styku IT/OT

SN710 - 3 klastry

IT/OT-VPN Koncentrator (x2)

SN3000 - 1 klaster

Bezpieczeństwo

200 x SNi40

2 na każdą lokalizację zdalną

STORMSHIELD

Dlaczego warto rozważyć nasze rozwiązania

OT

Rozpoznawanie protokołów przemysłowych i własne sygnatury

Ciągłość działania

Transparentne wdrożenie

Funkcja bypass

Logi i raporty

Zgodność ze standardami i certyfikacje

Niskie TCO

Redukcja kosztów inwestycyjnych i niskie koszty utrzymania

Dziękujemy

Paweł Śmigielski

Country Manager Poland

+48 570 107 205

pawel.smigielski@stormshield.eu

Błażej Buczyłko

Sales Manager Poland

+48 537 140 530

blazej.buczylko@stormshield.eu

STORMSHIELD