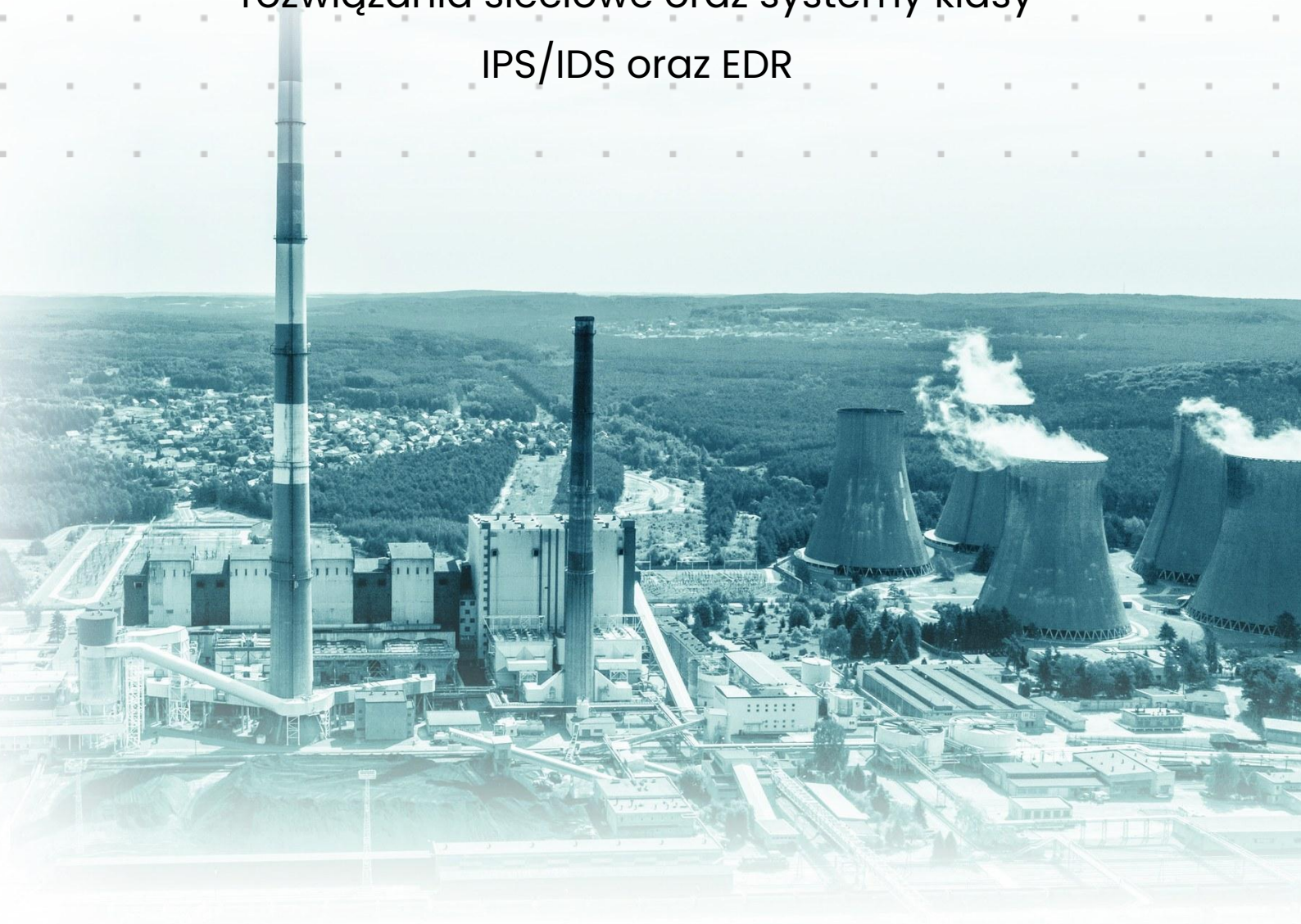
ELMARK Automatyka

CYBERBEZPIECZNA CIEPŁOWNIA

Propozycja zabezpieczenia systemów sterowania w oparciu o przemysłowe rozwiązania sieciowe oraz systemy klasy IPS/IDS oraz EDR



Izba Gospodarcza Ciepłownictwo Polskie

Jesteśmy partnerem Izby Gospodarczej Ciepłownictwo Polskie.

Spis treści

Wstęp **2**

Ogólna topologia proponowanego rozwiązania **3**

Zabezpieczenie połączenia ciepłowni z miejską siecią ciepłowniczą **5**

Zabezpieczenie dostępu serwisowego **6**

Szczegółowy opis proponowanych rozwiązań **8**

Intrusion Prevention System – TXOne Networks 8

EdgeIPS 216 PRO Rugged 8

EdgeIPS 103 9

EdgeOne 9

Endpoint Detection and Response – TXOne Networks 9

Stellar ICS 10

Switch zarządzalny – MOXA 10

EDS-4012-4GS 11

RKS-G4028 w wersji L2 lub L3 11

SDS-3008/3016 12

Firewall OT – MOXA 12

EDR-8010-VPN-2GSFP 13

OnCell G4302-LTE4 13

Oprogramowanie do zarządzania infrastrukturą informatyczną – MOXA 13

MXView One 14

Zakres oferowanego wsparcia Elmark Automatyka dla partnerów **15**

Konsultacje koncepcyjne 15

Szkolenia 15

Materiały dodatkowe **16**

Dane kontaktowe **17**

Elmark Automatyka S.A.

ul. Bukowińska 22 lokal 1B, 02-703 Warszawa
tel. (+48) 22 773 79 37; elmark@elmark.com.pl

NIP: 5252072585; REGON: 013144306
KRS: 0000803828, Sąd Rejonowy dla M.St. Warszawy XIV Wydz. Gosp. KRS
Kapitał Zakładowy: 650.000 zł w pełni opłacony

elmark.com.pl

Wstęp

Cyberbezpieczeństwo OT nie musi oznaczać całodobowego zespołu security ani przebudowy systemu, który dziś poprawnie prowadzi proces. Powinno chronić to, co już działa - nie komplikować tego.

Jeżeli odpowiadają Państwo za automatykę, utrzymanie ruchu, infrastrukturę techniczną lub rozwój ciepłowni, nowe rozwiązania muszą przede wszystkim pasować do realiów zakładu. Powinny zwiększać poziom bezpieczeństwa, ale nie tworzyć przy tym kolejnego systemu, który wymaga stałej obsługi, ciągłej analizy zdarzeń i dodatkowego obciążenia zespołu technicznego.

Dlatego założeniem jest ochrona tego, co już działa. **Nie zaczynamy od pytania, co trzeba wymienić. Zaczynamy od tego, jak zabezpieczyć istniejącą infrastrukturę.** W wielu przypadkach poziom bezpieczeństwa można podnieść bez przebudowy całej architektury czy readresacji sterowników, wprowadzając ochronę dokładnie tam, gdzie jest ona potrzebna. Pozwala to rozwijać cyberbezpieczeństwo etapami, bez niepotrzebnego ingerowania w systemy, które są sprawdzone, znane Państwa zespołowi i odpowiadają za ciągłość pracy zakładu.

W naszym podejściu nie poprzestajemy na samym podglądaniu ruchu w sieci OT. System nie tylko go monitoruje, ale też aktywnie chroni komunikację i kluczowe urządzenia, zgodnie z regułami, które sami Państwo ustalicie. Dzięki temu większość pracy związanej z nadzorem bierze na siebie system, a Państwa zespół zajmuje się tylko tym, co naprawdę wymaga decyzji człowieka. Odpowiedzialność za bezpieczeństwo zostaje po Państwa stronie, ale bez konieczności posiadania całodobowego zespołu, który pilnuje monitoringu systemu.

Jako Elmark Automatyka S.A. pomagamy dobrać rozwiązania do rzeczywistej architektury Państwa zakładu — tak, aby cyberbezpieczeństwo zwiększało odporność infrastruktury OT, a nie jej złożoność. W dalszej części materiału pokazujemy, jak realizować to podejście w praktyce: od segmentacji i aktywnej ochrony komunikacji, przez zabezpieczenie kluczowych urządzeń, po bezpieczną telemetrię i zdalny dostęp do obiektów rozproszonych.

Dodatkowo, w materiale przygotowaliśmy **OPISY FUNKCJONALNO-UŻYTKOWE** proponowanych rozwiązań.

Zapraszamy do lektury!

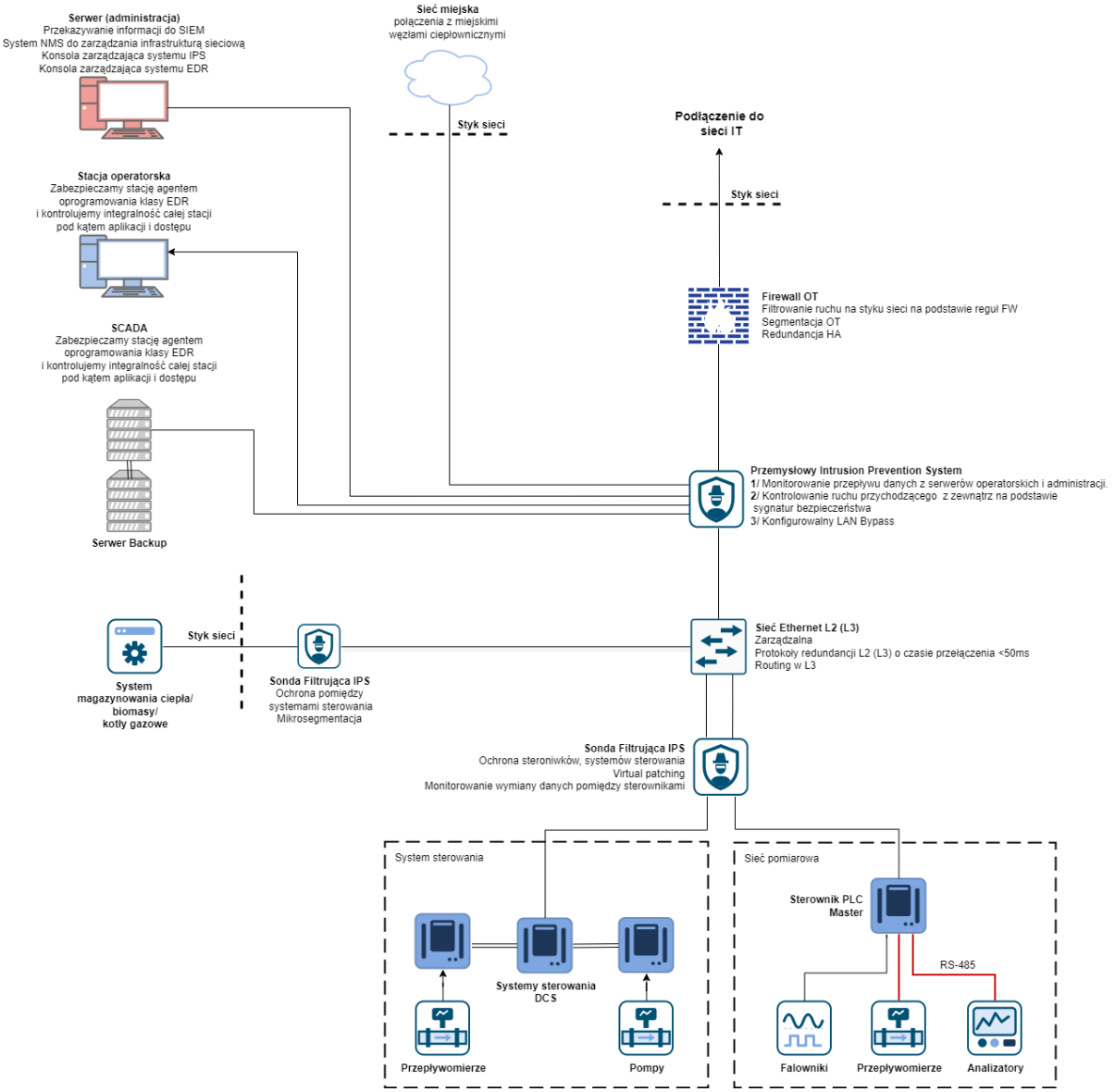
Elmark Automatyka S.A.

ul. Bukowińska 22 lokal 1B, 02-703 Warszawa
tel. (+48) 22 773 79 37; elmark@elmark.com.pl

NIP: 5252072585; REGON: 013144306
KRS: 0000803828, Sąd Rejonowy dla M.St. Warszawy XIV Wydz. Gosp. KRS
Kapitał Zakładowy: 650.000 zł w pełni opłacony

elmark.com.pl

Ogólna topologia proponowanego rozwiązania



Rys. 1 Propozycja zabezpieczenia obiektu ciepłowniczego

Cel zastosowania: *segmentacja i mikrosegmentacja sieci OT oraz kontrola komunikacji na wszystkich jej stykach, czyli z siecią IT, siecią miejską i nowymi układami sterowania (np. magazyn ciepła, biomasa, kotły gazowe), ochrona sterowników, systemów sterowania i stacji SCADA oraz centralne zarządzanie całą infrastrukturą bez ingerencji w działającą architekturę*

Elmark Automatyka S.A.

ul. Bukowińska 22 lokal 1B, 02-703 Warszawa
tel. (+48) 22 773 79 37; elmark@elmark.com.pl

NIP: 5252072585; REGON: 013144306
KRS: 0000803828, Sąd Rejonowy dla M.St. Warszawy XIV Wydz. Gosp. KRS
Kapitał Zakładowy: 650.000 zł w pełni opłacony

elmark.com.pl

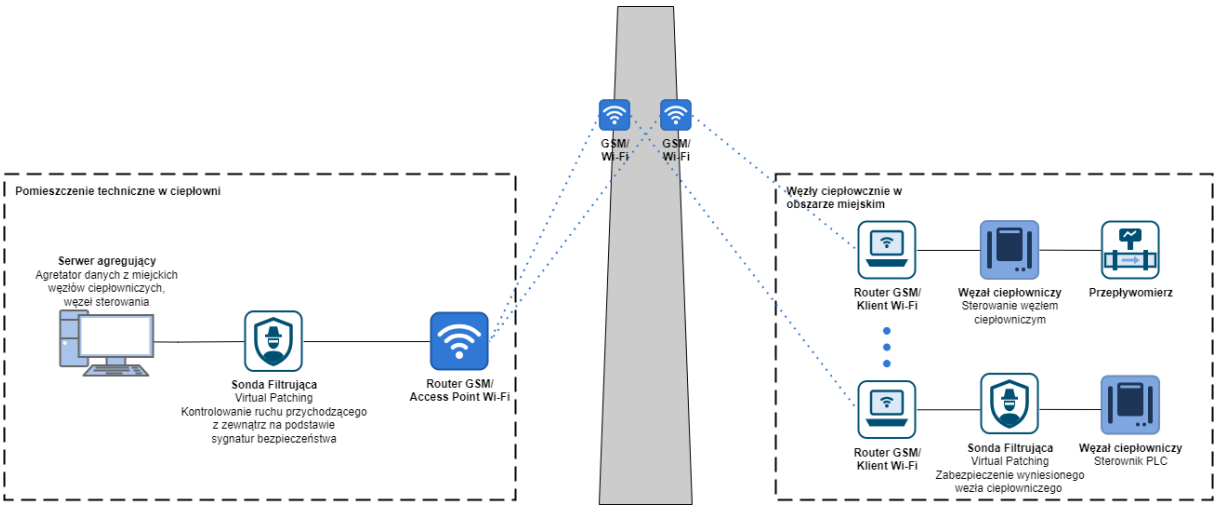
Koncepcja systemu bazuje na wdrożeniu kompletnego systemu bezpieczeństwa odpowiadającego wymaganiom Ustawy o Krajowym Systemie Cyberbezpieczeństwa. Zakłada ona wdrożenie segmentacji oraz mikrosegmentacji infrastruktury OT, zabezpieczenie kluczowych assetów uwzględniając sieci rozproszone, zabezpieczenie połączeń serwisowych oraz wdrożenie w pełni zarządzalnej i centralnie zarządzanej infrastruktury sieciowej.

Proponowana topologia systemu ICS przedstawia zintegrowane podejście do cyberbezpieczeństwa w przedsiębiorstwach ciepłowniczych. Kluczowym elementem są urządzenia firewall OT, segmentujące sieć OT od IT oraz kontrolujące ruch VPN. Przemysłowy system IPS zapewnia monitoring ruchu sieciowego, ochronę przed atakami oraz virtual patching (zarządzanie podatnościami w systemie sterowania). Zarządzalne switche realizują segmentację sieci VLAN, kontrolują ruch sieciowy i umożliwiają zdalne zarządzanie. Endpointy (stacje SCADA oraz operatorska) chronione są przez agentów EDR, zapewniając bezpieczeństwo aplikacji i integralność systemów. Całość infrastruktury nadzorowana jest centralnie z poziomu serwera administracyjnego z systemem NMS (Network Management System) oraz konsolami zarządzającymi IPS i EDR.

Korzyści:

- kontrola ruchu na styku sieci (IT, sieć miejska, nowe układy sterowania) oraz podział sieci OT na strefy
- ochrona sterowników i systemów sterowania sondami IPS również tych niewspieranych już przez producenta (virtual patching)
- ochrona stacji SCADA i operatorskich agentem EDR: integralność systemu i kontrola aplikacji
- zwiększona ciągłość działania dzięki redundancji sieci oraz firewall w układzie HA
- centralny nadzór nad infrastrukturą z jednego miejsca: system NMS, konsole IPS i EDR, przekazywanie zdarzeń do SIEM

Zabezpieczenie połączenia ciepłowni z miejską siecią ciepłowniczą



Rys. 2 Propozycja zabezpieczenia ciepłowni oraz węzłów ciepłowniczych.

Cel zastosowania: *kontrola komunikacji pomiędzy ciepłownią a rozproszonymi węzłami w obszarze miejskim, ochrona serwera agregującego przed ruchem z zewnątrz oraz zabezpieczenie odległych i trudno dostępnych węzłów, których niezawodność ma znaczenie dla infrastruktury miejskiej*

Połączenie z miejską siecią ciepłowniczą to jeden z najbardziej wystawionych punktów styku w całej infrastrukturze zakładu. Ruch z węzłów trafia do serwera agregującego w ciepłowni, więc incydent po stronie jednego węzła nie powinien mieć drogi do kluczowych systemów zakładu.

Dlatego na styku sieci po stronie ciepłowni, pomiędzy punktem dostępowym a serwerem agregującym, proponujemy zastosowanie sondy filtrującej IPS. Aktywnie chroni ona ruch przychodzący z zewnątrz na podstawie sygnatur bezpieczeństwa i kontroluję komunikację nieautoryzowaną lub złośliwą, zanim dotrze do serwera. Dzięki virtual patchingowi chroni też przed wykorzystaniem znanych podatności, bez ingerencji w sam serwer i bez zmiany adresacji.

Ochrona po stronie ciepłowni nie obejmuje jednak samych węzłów. Węzły miejskie są często zlokalizowane w miejscach odległych, trudno dostępnych lub krytycznych z perspektywy infrastruktury miejskiej, gdzie każda awaria oznacza dojazd ekipy. W takich lokalizacjach zalecamy zabezpieczenie sterownika węzła osobną sondą filtrującą, zainstalowaną pomiędzy

Elmark Automatyka S.A.

ul. Bukowińska 22 lokal 1B, 02-703 Warszawa
tel. (+48) 22 773 79 37; elmark@elmark.com.pl

NIP: 5252072585; REGON: 013144306
KRS: 0000803828, Sąd Rejonowy dla M.St. Warszawy XIV Wydz. Gosp. KRS
Kapitał Zakładowy: 650.000 zł w pełni opłacony

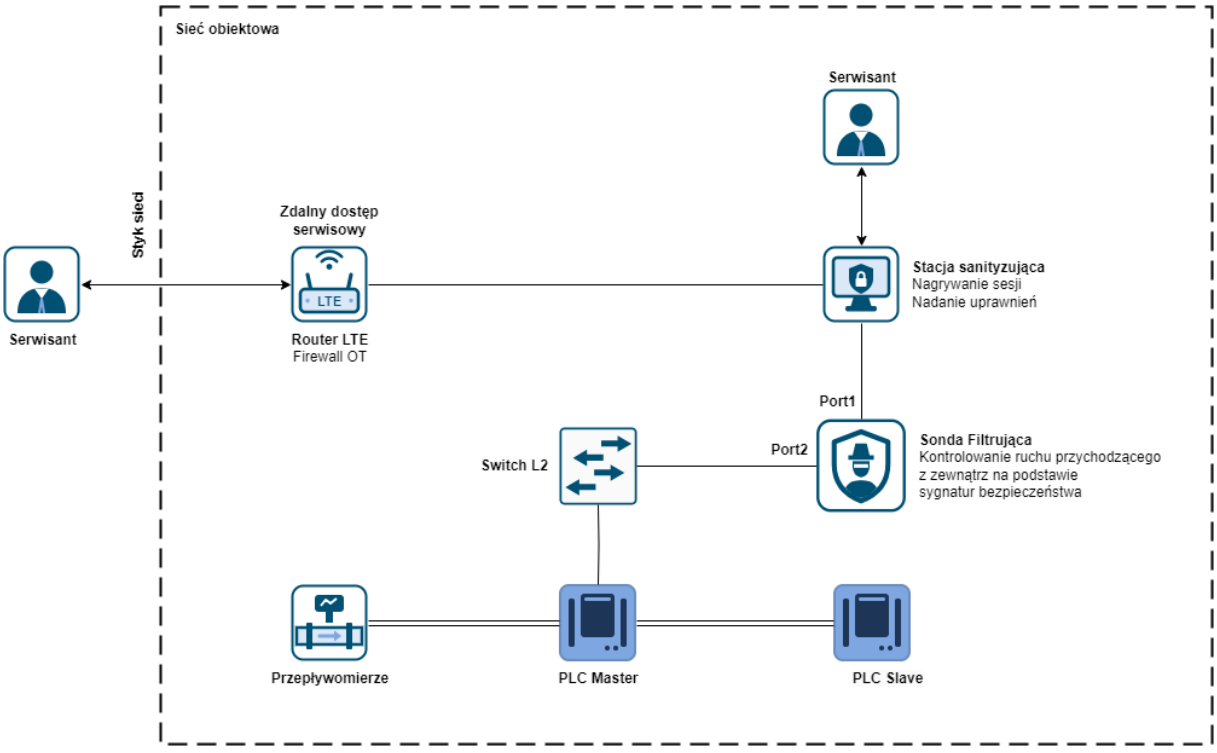
elmark.com.pl

łącznością a sterownikiem. Ochronę można wdrażać etapami, zaczynając od najbardziej wrażliwych węzłów.

Korzyści:

- ochrona serwera agregującego przed ruchem z zewnątrz, na styku ciepłowni z siecią miejską
- lokalna ochrona wyniesionych węzłów w miejscach odległych, trudno dostępnych i krytycznych
- możliwość etapowego wdrożenia, od najbardziej wrażliwych węzłów, bez zmian w istniejącej architekturze

Zabezpieczenie dostępu serwisowego



Rys. 3 Propozycja zabezpieczenia dostępu serwisowego zdalnego oraz na obiekcie.

Cel zastosowania: *kontrolowane udostępnianie sieci OT serwisantom, zarówno zdalnie, jak i z poziomu obiektu, z ochroną sterowników przed nieautoryzowanymi i błędnymi komendami oraz pełną odpowiedzialnością za każdą sesję*

Dostęp serwisowy jest nieodzowny dla utrzymania ruchu, a jednocześnie bywa jednym z najczęstszych wektorów ataku na sieć OT. Producenci kotłów, palników czy sterowników potrzebują dostępu do swoich urządzeń, a zespół utrzymania ruchu musi wiedzieć, kto, kiedy i do czego miał dostęp.

Serwisant może łączyć się z obiektem na różne sposoby. Zdalnie, po łączu komórkowym, przez router LTE z funkcją firewalla OT, który stanowi styk sieci. Dopuszcza on wyłącznie zdefiniowany ruch i terminuje szyfrowane połączenie VPN, dzięki czemu obiekt nie wymaga publicznego adresu ani otwartych portów. Albo lokalnie, z poziomu obiektu, przez stację sanityzującą, która nadaje uprawnienia i nagrywa przebieg sesji. W żadnym z tych przypadków serwisant nie podłącza swojego komputera bezpośrednio do przełącznika ani sterownika.

Niezależnie od sposobu połączenia, wspólnym elementem jest sonda filtrująca, umieszczona na drodze do sieci sterowania, przed przełącznikiem. Kontroluje ona ruch przychodzący z zewnątrz na podstawie sygnatur bezpieczeństwa i jest ostatnią warstwą ochrony, zanim komunikacja dotrze do sterowników PLC i urządzeń pomiarowych. Sonda egzekwuje reguły i głęboką inspekcję protokołów, np. dopuszcza komendy zapisu tylko z autoryzowanych hostów. Dzięki virtual patchingowi chroni też sterowniki podatne lub niewspierane już przez producenta, bez ingerencji w ich konfigurację.

Korzyści:

- brak bezpośredniego dostępu serwisanta do sieci sterowania, każdy dostęp przechodzi przez kontrolowane punkty
- ochrona sterowników przez sondę filtrującą, niezależnie od źródła połączenia
- zgodność z podejściem „defense-in-depth” i wymaganiami IEC 62443 w obszarze zdalnego dostępu

Szczegółowy opis proponowanych rozwiązań

Poniżej opisujemy urządzenia i systemy, które proponujemy w trzech przedstawionych wcześniej topologiach. Dla każdego rozwiązania podajemy cel zastosowania, najważniejsze funkcje oraz miejsce, w którym sprawdza się w architekturze zakładu.

Intrusion Prevention System – TXOne Networks

Cel zastosowania: *ciągłe monitorowanie rzeczywistego ruchu w sieci OT i blokada (na podstawie reguł ustalonych przez administratora) nieautoryzowanych i złośliwych pakietów, aby zapobiec zakłóceniom procesów sterowania, minimalizować powierzchnię ataku (poprzez szybką izolację incydentów) i chronić krytyczne zasoby OT przed cyberatakami*

System IPS stale monitoruje ruch sieciowy w poszukiwaniu zagrożeń, zapewniając aktywną ochronę infrastruktury ICS przed atakami. Dzięki funkcji virtual patchingu chroni przed wykorzystaniem luk bezpieczeństwa, umożliwiając szybkie reagowanie na podatności systemu sterowania, zanim zostaną wdrożone pełne aktualizacje bądź modernizacje. Wdrożenie systemu bazującego na aktywnej ochronie pozwala na utworzenie stref bezpieczeństwa bez ingerencji w istniejącą infrastrukturę (brak konieczności readresacji sterowników) oraz minimalizowanie powierzchni ataku. System IPS upraszcza wdrożenie procedur związanych z reakcją na incydent bądź zdarzenie. Zarządzany centralnie z poziomu konsoli Edge One, która agreguje zdarzenia z końcówek i przesyła je do SOC w postaci logu.

Możliwość skonfigurowania do pracy jako Intrusion Detection System.
Możliwość pracy i aktualizacji w środowisku pozbawionym dostępu do internetu

EdgeIPS 216 PRO Rugged

https://www.elmark.com.pl/sklep/txone-networks/txone-networks-edgeips-pro-216

Wielokanałowa sonda do zastosowań w budynkach administracyjnych lub serwerowniach OT. Jej zadaniem jest kontrolowanie ruchu z serwerów oraz ruchu przychodzącego z innych segmentów oraz budynków administracyjnych. Kontroluje również ruch z warstwy zarządzającej do warstwy sterowania. Możliwe jest również przekierowanie ruchu poprzez RSPAN do poszczególnych interfejsów. Korzyści:

- zabezpieczenie podatności systemów SCADA oraz m.in. baz danych SQL
- zabezpieczanie krytycznych dla ciągłości działania urządzeń np. serwerów SCADA

- głęboka inspekcja pakietów przemysłowych: S7comm (na poziomie funkcji), Modbus TCP (na poziomie rejestrów)
    - ograniczanie wysyłania pakietów typu write tylko do zautoryzowanych hostów
- monitorowanie i filtrowanie ruchu np. budynkach socjalno-administracyjnych, gdzie w jednej lokalizacji jest dużo połączeń
- zarządzanie podatnościami poprzez virtual patching
    - ochrona niewspieranych już przez producenta urządzeń

EdgeIPS 103

https://www.elmark.com.pl/sklep/txone-networks/edgeips-103

Sonda jednokanałowa umożliwiająca ochronę pojedynczego assetu np. Master PLC kotłowni. Pozwala również filtrować / monitorować ruch przy przejściu na sterowanie ręczne po wyzwoleniu komendy z panelu HMI. Korzyści:

- bezpośrednia ochrona kluczowego assetu z indywidualnymi politykami bezpieczeństwa
- monitorowanie i filtrowanie ruchu do kluczowych dla procesu sterownia urządzeń
- głęboka inspekcja pakietów przemysłowych: S7comm (na poziomie funkcji), Modbus TCP (na poziomie rejestrów)
- zarządzanie podatnościami poprzez virtual patching
    - ochrona niewspieranych już przez producenta urządzeń

EdgeOne

Konsola zarządzająca systemem IPS umożliwiająca scentralizowaną konfigurację, monitoring i aktualizację urządzeń zabezpieczających, takich jak wymienione wcześniej sondy EdgeIPS. Konsola nie wymaga dostępu do internetu i może w pełni funkcjonalnie pracować w środowisku odizolowanym. Korzyści:

- Pełen wgląd w stan zabezpieczeń infrastruktury ICS
- Szybkie reagowanie na zagrożenia
- Grupowa konfiguracja urządzeń zgodnie z politykami dla danej strefy bezpieczeństwa
- Integracja ze SIEM

Endpoint Detection and Response – TXOne Networks

Cel zastosowania: *ciągłe monitorowanie stacji operatorskich i serwerów ICS oraz błyskawiczne wykrywanie i izolacja złośliwych działań, blokowanie nieautoryzowanego instalowania aplikacji czy*

użycia nośników USB, aby zapobiec rozprzestrzenianiu się zagrożeń i zachować integralność krytycznych procesów OT

TXOne Stellar ICS to rozwiązanie bezpieczeństwa punktów końcowych zaprojektowane specjalnie z myślą o środowiskach przemysłowych ICS/OT. Składa się z agenta Stellar oraz centralnej konsoli StellarOne do zarządzania. Zapewnia skuteczną ochronę endpointów w środowisku izolowanym, wspiera nawet bardzo stare systemy i kładzie nacisk na niezakłócanie procesów technologicznych. Jego architektura z lokalną konsolą zarządzającą idealnie pasuje do odizolowanych sieci – pozwala utrzymywać aktualność zabezpieczeń i mieć centralny nadzór bez dostępu do Internetu. Dodatkowe funkcje jak whitelisting aplikacji, nauczanie behawioralne, tryb maintenance czy kontrola USB sprawiają, że narzędzie spełnia rygorystyczne wymagania norm ICS i praktyk bezpieczeństwa (IEC 62443, NERC CIP itp.) obowiązujących w przemyśle.

Istnieje możliwość zakupu oprogramowania z licencją wieczystą (Perpetual Lockdown) co jest unikatowe w przypadku rozwiązań tej klasy.

Stellar ICS

https://www.elmark.com.pl/sklep/txone-networks/txone-networks-stellar

Główne korzyści systemu Stellar ICS:

- **Szeroka obsługa systemów**: wspiera praktycznie wszystkie wersje Windows używane w przemyśle – od najnowszych Windows 10/11 poprzez Windows 7, a nawet Windows XP czy 2000
- **Whitelisting** – blokowanie uruchomienia nieznanego pliku/programu zapobiegając niepożądanym zmianom
- Antywirus i EDR offline
- Tryb Serwisowy dla pracowników Utrzymania Ruchu
- Kontrola USB
- Centralne Zarządzanie bez konieczności komunikacji z chmurą lub internetem – praca w środowisku izolowanym
- Zgodność z wymaganiami przemysłowymi

Switch zarządzalny – MOXA

Cel zastosowania: *segmentacja sieci OT (np. poprzez VLAN i ACL), kontrola oraz monitorowanie ruchu na poziomie portów, redundancja komunikacji a w konsekwencji ograniczenie rozprzestrzeniania się zagrożeń i ochrona infrastruktury OT na poziomie sieciowym*

MOXA to wiodący producent rozwiązań komunikacyjnych dla przemysłu, który uzyskał certyfikat IEC 62443-4-1. Zastosowanie w sieci OT przełączników zarządzalnych niesie za sobą szereg korzyści. Przede wszystkim wdrożenie segmentacji sieci (VLAN, ACL) umożliwiając separację systemów na poziomie logicznym. Mając na uwadze zachowanie ciągłości działania możliwe jest wdrożenie protokołów redundancji jak Turbo Ring v2 o bardzo szybkim czasie zbieżności (50ms).

Wszystkie switche MOXA mają licencję wieczystą i nie wymagają dodatkowych subskrypcji na aktualizacje oprogramowania

EDS-4012-4GS

https://www.elmark.com.pl/sklep/moxa/eds-4012

Zarządzalny przełącznik firmy MOXA. Idealny do zastosowań w sieci dystrybucyjnej systemów ciepłowniczych, gdzie istotne są bardziej zaawansowane funkcje bezpieczeństwa. Sprawdzi się do połączenia np. w topologii pierścienia różnych obiektów za pomocą łącza światłowodowego. Dzięki technologii SPAN/RSPAN umożliwia wdrożenie systemów detekcji zagrożeń jak choćby lokalna instalacja sondy EdgeIPS 103 na wydzielonym porcie. Certyfikowany zgodnie z wymagającą normą cyberbezpieczeństwa dla przemysłu IEC 62443-4-2. Dodatkowe:

- Wymienialny moduł zasilania – szybki serwis na wypadek awarii bez konieczności odsyłania całego urządzenia
    - Moduł zasilania posiada możliwość obracania – w przypadku modernizacji jest duża szansa, że nie będziemy musieli wymieniać szafek, ponieważ przewody zasilania możemy wprowadzić od frontu
- System operacyjny – wspólny dla całej rodziny EDS-4000

RKS-G4028 w wersji L2 lub L3

https://www.elmark.com.pl/sklep/moxa/rks-g4028-l2
https://www.elmark.com.pl/sklep/moxa/rks-g4028-l3

Zarządzalny, modułowy przełącznik firmy MOXA w obudowie rack 19" (1U). Idealny do zastosowań w centralnym punkcie sieci zakładu – w serwerowni lub dyspozytorni elektrociepłowni, gdzie zbiegają się łącza światłowodowe z poszczególnych systemów. Dzięki modułowej budowie pozwala rozbudować konfigurację nawet do 28 portów Gigabit o różnych typach złączy (RJ45, SFP), co umożliwia dopasowanie urządzenia do istniejącej infrastruktury oraz jej etapową rozbudowę bez wymiany przełącznika. Certyfikowany zgodnie z wymagającą normą cyberbezpieczeństwa dla przemysłu IEC 62443-4-2. Dodatkowe:

- Redundantne, izolowane zasilanie – wersja wysokonapięciowa 110/220 VAC/VDC lub niskonapięciowa 24/48 VDC, z dwoma wejściami zasilania zabezpieczającymi ciągłość pracy na wypadek zaniku jednego źródła
- Dostępny w wariancie L2 (przełączanie i segmentacja w warstwie 2 – VLAN, ACL) oraz L3, który dodatkowo zapewnia routing międzysieciowy (OSPF, routing statyczny) i redundancję routingu VRRP – do trasowania ruchu pomiędzy strefami/VLAN zakładu bez osobnego routera
- Technologia SPAN/RSPAN umożliwiająca wpięcie sondy detekcji zagrożeń (np. EdgeIPS) na wydzielonym porcie

SDS-3008/3016

https://www.elmark.com.pl/sklep/moxa/sds-3008
https://www.elmark.com.pl/sklep/moxa/sds-3016

Zarządzalny przełącznik firmy MOXA. Idealny do zastosowań w sieci dostępowej np. w kotłowni lub węźle cieplnym. Dzięki wsparciu dla protokołu MRP switch może pracować w pierścieniu ze sterownikami Siemensa. Jest to upgrade do infrastruktury zarządzalnej w miejscach, gdzie dotychczas powszechnie wykorzystywano switche niezarządzalne. Charakteryzuje się małymi wymiarami dzięki czemu możliwa będzie jego instalacja w już istniejących szafkach bez konieczności ich wymiany.

Firewall OT – MOXA

Cel zastosowania: *selektywne filtrowanie i inspekcja ruchu (w tym protokołów przemysłowych), aby uniemożliwić nieautoryzowany dostęp i zablokować złośliwe pakiety zanim dotrą do krytycznych systemów sterowania, realizacja bezpiecznego zdalnego dostępu do infrastruktury OT.*

Firewall na styku IT/OT oraz styku sieci obiektowej pełni kluczową rolę w **separacji ruchu sieciowego** między środowiskami biurowym (IT) a przemysłowym (OT), chroniąc krytyczne systemy sterowania przed zagrożeniami pochodzącymi z sieci korporacyjnej lub Internetu. Jego głównym zadaniem jest **filtrowanie pakietów** zgodnie z ustalonymi regułami bezpieczeństwa – dopuszczając tylko niezbędny i bezpieczny ruch. Firewall może również pełnić funkcję **bramy VPN**, umożliwiając bezpieczny zdalny dostęp dla integratorów lub serwisantów. W nowoczesnych rozwiązaniach (np. Moxa EDR-8010, OnCell G4302) możliwa jest też **inspekcja protokołów przemysłowych (DPI)**, co pozwala wykrywać i blokować nietypowe lub nieautoryzowane komendy SCADA/PLC. Dobrze skonfigurowany firewall na styku sieci jest fundamentem architektury typu **„defense-in-depth”**, wymaganej przez normy takie jak IEC 62443.

EDR-8010-VPN-2GSFP

https://www.elmark.com.pl/sklep/moxa/edr-8010

EDR-8010 to wielofunkcyjne urządzenie integrujące funkcje firewalla, NAT oraz routingu co umożliwia ścisłą kontrolę ruchu pomiędzy strefami IT/OT zabezpieczając krytyczną infrastrukturę przed nieautoryzowanym dostępem. Urządzenie można z powodzeniem wykorzystać na styku sieci OT z siecią biurową np. w budynku socjalno-administracyjnym. W przypadku dużej i rozproszonej architektury EDR-8010 może być również zastosowany do filtrowania ruchu przychodzącego / wychodzącego z danej lokalizacji lub szyfrowanego dostępu za pośrednictwem VPN.

Firewalle MOXA mają licencję wieczystą i nie wymagają dodatkowych subskrypcji na aktualizacje oprogramowania.

OnCell G4302-LTE4

https://www.elmark.com.pl/sklep/moxa/oncell-g4302-lte4

OnCell G4302-LTE4 to wielofunkcyjne urządzenie łączące w jednej obudowie router komórkowy oraz firewall przemysłowy, co pozwala objąć ochroną i podłączyć do centralnej sterowni obiekty rozproszone, do których nie doprowadzono łącza światłowodowego – węzły cieplne czy stacje pomiarowe. Urządzenie realizuje filtrowanie ruchu zgodnie z regułami bezpieczeństwa oraz wspiera głęboką inspekcję pakietów przemysłowych (DPI). Ciągłość transmisji telemetrii zapewnia podwójny slot SIM z automatycznym przełączaniem (failover), natomiast bezpieczny szyfrowany transport danych realizowany jest przez tunele VPN.

Firewalle MOXA mają licencję wieczystą i nie wymagają dodatkowych subskrypcji na aktualizacje oprogramowania.

Oprogramowanie do zarządzania infrastrukturą informatyczną – MOXA

Cel zastosowania: *scentralizowane monitorowanie i zarządzanie switchami przemysłowymi, zapewniające graficzną wizualizację topologii, zdalne zarządzanie konfiguracjami oraz firmware'ami oraz natychmiastowe alarmowanie o zdarzeniach, co wzmacnia bezpieczeństwo systemów sterowania i nieprzerwaną pracę.*

Oprogramowanie klasy NMS służy do zdalnego monitoringu i diagnostyki przemysłowej sieci Ethernet. Oferuje zintegrowaną platformę, która pozwala na zarządzanie urządzeniami sieciowymi poprzez SNMP.

MXView One

https://www.elmark.com.pl/sklep/moxa/mxview-one

To platforma do zarządzania infrastrukturą sieciową firmy MOXA wraz z możliwością uwzględnienia w wizualizacji serwerów portów szeregowych – powszechnie wykorzystywanych np. w aplikacjach licznikowych do konwersji starszych typów urządzeń do protokołu TCP. Korzyści wynikające z wdrożenia MXView jako NMS w środowisku OT w kontekście procedur cyberbezpieczeństwa oraz utrzymania ciągłości działania:

- **Automatyczne wykrywanie i wizualizacja urządzeń sieciowych oraz fizycznych połączeń**
  Ułatwia szybki przegląd i inwentaryzację urządzeń OT, co wspiera bieżący nadzór nad infrastrukturą ciepłowniczą.
- **Centralne zarządzanie konfiguracją i firmware dla urządzeń Moxa**
  Pozwala na spójne i bezpieczne aktualizacje oprogramowania urządzeń sieciowych bez konieczności lokalnej ingerencji. Przy dostępie do sieci możliwość weryfikowania czy urządzenia mają najbardziej aktualny firmware
- Różne opcje powiadomień i zdarzeń z własnymi progami i czasem trwania
- **Szczegółowe informacje o urządzeniach i wykresy wydajności poszczególnych punktów dostępowych i klientów**
  Pozwala analizować obciążenie i kondycję urządzeń OT, co może pomóc w wykrywaniu wczesnych symptomów awarii lub ataku.

Oprogramowanie ma licencję wieczystą i nie wymaga odnowień subskrypcji

Zakres oferowanego wsparcia Elmark Automatyka dla partnerów

Elmark Automatyka to dystrybutor specjalizujący się w dostarczaniu rozwiązań dla przemysłowych sieci OT, posiadający szeroki zespół inżynierów z wieloletnim doświadczeniem w dziedzinie cyberbezpieczeństwa ICS. Klienci kupujący u nas sprzęt otrzymują pełne wsparcie techniczne i inżynierskie bez konieczności zakupu dodatkowych usług. Dotyczy to wsparcia zarówno przedsprzedażowego (opracowanie koncepcji, PoC) oraz posprzedażowego (obsługa sprzętu, ewentualne problemy z konfiguracją i działaniem).

Konsultacje koncepcyjne

Z przyjemnością dzielimy się naszym doświadczeniem, oferując **nieodpłatne konsultacje koncepcyjne**. Wspólnie z Państwem przeanalizujemy topologię, dobierzemy odpowiednie urządzenia oraz lokalizacje sond filtrujących, tworząc efektywny i ergonomiczny system cyberbezpieczeństwa, który w pełni odpowie na potrzeby operatorów. Na podstawie koncepcji możemy przygotować gotowy wsad do wniosku wraz z opisem urządzeń do programu funkcjonalno-użytkowego.

Opis funkcjonalno-użytkowy poszczególnych rozwiązań znajduje się w sekcji „Materiały dodatkowe", na końcu tego materiału.

Szkolenia

Posiadamy szeroką ofertę szkoleniową, obejmującą zarówno zagadnienia ogólne z zakresu cyberbezpieczeństwa (np. norma IEC 62443), jak i szczegółową obsługę systemów zaprezentowanych w niniejszym dokumencie. Zachęcamy do zapoznania się z pełnym katalogiem naszych szkoleń, dostępnym tutaj: *Elmark Automatyka – Oferta Szkoleniowa*.

Elmark Automatyka S.A.

ul. Bukowińska 22 lokal 1B, 02-703 Warszawa
tel. (+48) 22 773 79 37; elmark@elmark.com.pl

NIP: 5252072585; REGON: 013144306
KRS: 0000803828, Sąd Rejonowy dla M.St. Warszawy XIV Wydz. Gosp. KRS
Kapitał Zakładowy: 650.000 zł w pełni opłacony

elmark.com.pl

Materiały dodatkowe

Poniżej zamieszczamy materiały uzupełniające zawierające szczegółowe opisy funkcjonalno-użytkowe proponowanych rozwiązań. Ponadto zamieszczamy artykuły techniczne precyzyjnie opisujące możliwości technologiczne wymienionych produktów. Ze względu na rozmiar dokumentów zamieściliśmy linki do pobrania plików w formie pliku edytowalnego:

Opis Przedmiotu Zamówienia:

1. Intrusion Prevention System (IPS): *OPIS FUNKCJONALNO-UŻYTKOWY - EdgeIPS.docx*
2. Endpoint Detection and Response (EDR): *OPIS FUNKCJONALNO-UŻYTKOWY - Stellar.docx*
3. Switch Zarządzalny:
    a. EDS-4012-4GS-LV: *OPIS FUNKCJONALNO-UŻYTKOWY - EDS-4012.docx*
    b. RKS-G4028 L2: *OPIS FUNKCJONALNO-UŻYTKOWY – RKS-G4028-L2.docx*
    c. RKS-G4028 L3: *OPIS FUNKCJONALNO-UŻYTKOWY – RKS-G4028-L3.docx*
    d. SDS-3008/SDS-3016: *OPIS FUNKCJONALNO-UŻYTKOWY - SDS-3000.docx*
4. Oprogramowanie do zarządzania infrastrukturą informatyczną:
    a. MXView One: *OPIS FUNKCJONALNO-UŻYTKOWY - MXView One.docx*
5. Firewall OT:
    a. EDR-8010-VPN: *OPIS FUNKCJONALNO-UŻYTKOWY - EDR-8010.docx*
    b. OnCell G4302-LTE: *OPIS FUNKCJONALNO-UŻYTKOWY – OnCell G4302-LTE.docx*

Artykuły techniczne rozszerzające wiedzę:

1. NIS2 – przewodnik dla sektora przemysłowego: *https://www.elmark.com.pl/blog/NIS2_przewodnik_dla_sektora_przemyslowego*
2. SDS-3000 a EDS-4000 – który przełącznik wybrać: *https://www.elmark.com.pl/blog/podstawowa-funkcje-zarzadzania-czy-pena-kontrola-nad-sieci-porwnanie-przecznikw-serii-sds-3000-oraz-eds-4000-*
3. Cyberbezpieczna ciepłownia bez rewolucji w OT: *https://www.elmark.com.pl/blog/cyberbezpieczenstwo-cieplowni-nis2-ksc-poradnik*
4. MXview One - zarządzanie siecią przemysłową *https://www.elmark.com.pl/blog/zarzadzanie-siecia-przemys%C5%82owa-z-mxview*

Dane kontaktowe

Daniel Michrowski
Menadżer ds. Sieci OT
tel. 605 054 073
e-mail: *daniel.michrowski@elmark.com.pl*

Michał Łęcki
Menadżer ds. Cyberbezpieczeństwa OT
tel. 601 868 636
e-mail: *michal.lecki@elmark.com.pl*

Tomasz Sokół
Menadżer ds. produktu
tel. 887 024 474
email: *tomasz.sokol@elmark.com.pl*



Elmark Automatyka S.A.

ul. Bukowińska 22 lokal 1B, 02-703 Warszawa
tel. (+48) 22 773 79 37; elmark@elmark.com.pl

NIP: 5252072585; REGON: 013144306
KRS: 0000803828, Sąd Rejonowy dla M.St. Warszawy XIV Wydz. Gosp. KRS
Kapitał Zakładowy: 650.000 zł w pełni opłacony

elmark.com.pl