StationGuard

Bezpieczeństwo cybernetyczne i funkcjonalny monitoring dla sieci elektroenergetycznej

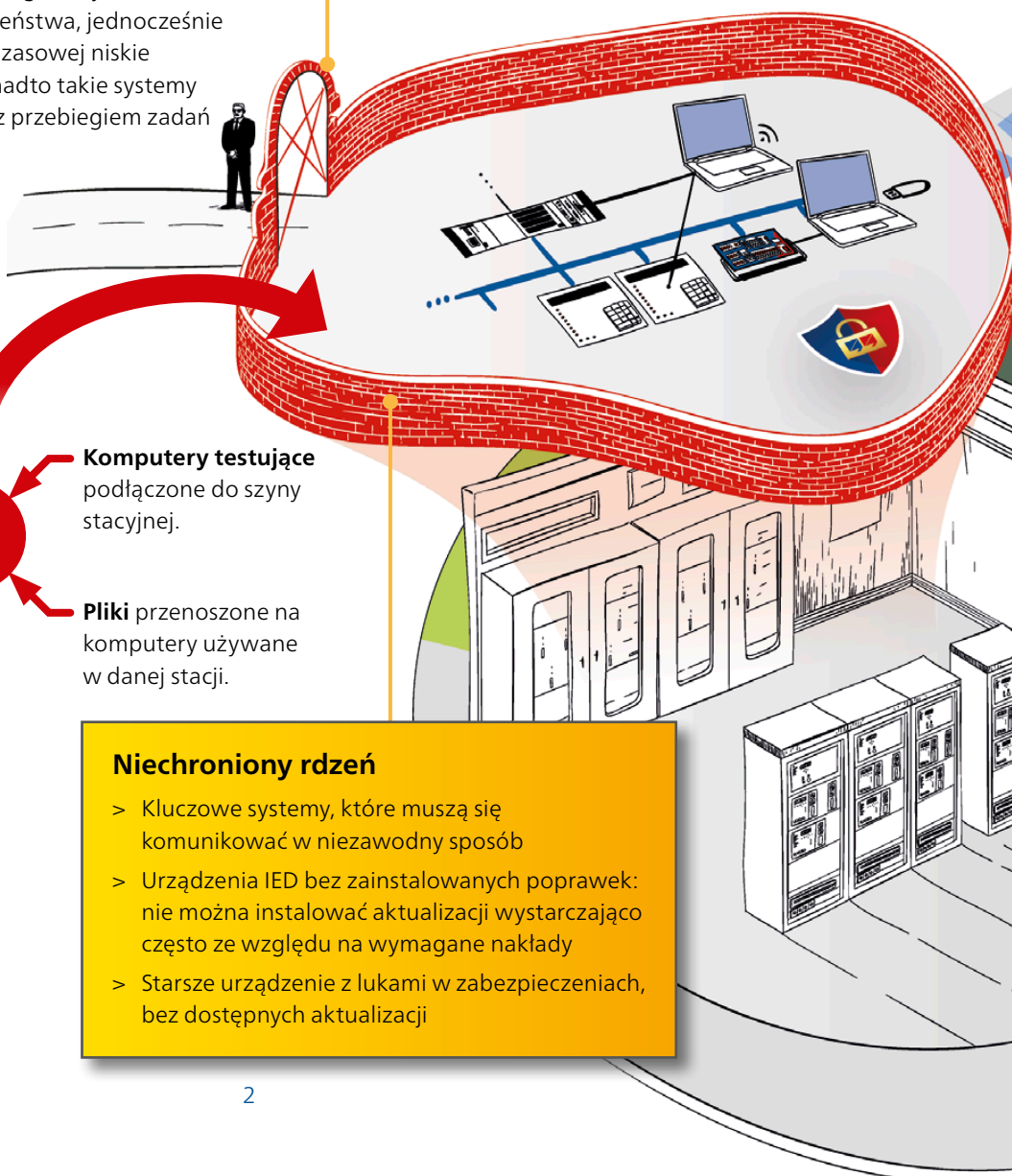
Bezpieczeństwo informatyczne w stacjach

W ostatnich latach odnotowano wzrost liczby ataków cybernetycznych skierowanych przeciwko kluczowym systemom sterowania w zakładach produkcyjnych i obiektach należących do dostawców energii. Dlatego też w wielu obiektach wdraża się procedury zmniejszające ryzyko związane z atakami cybernetycznymi. Do tej pory środki tego rodzaju były związane przede wszystkim z sieciami informatycznymi i stanowiskami dyspozytorskimi. Jednak stacje i ich sieci również stanowią krytyczne wektory ataku. W konsekwencji, procesy związane z obsługą i serwisem tych stacji również muszą być uwzględniane w ocenie ryzyka w zakresie bezpieczeństwa cybernetycznego.

Dla zapewnienia kompleksowej ochrony stacji przed atakami, strategia bezpieczeństwa musi obejmować wszystkie poziomy. Koncepcja bezpieczeństwa stacji rozciąga się od kontroli fizycznego dostępu, poprzez monitorowanie dostępu cyfrowego, aż do monitorowania podejrzanych lub zakazanych czynności w sieci. Wymaga to systemów, które oferują wysoki poziom bezpieczeństwa, jednocześnie zapewniając w długiej perspektywie czasowej niskie nakłady związane z utrzymaniem. Ponadto takie systemy powinny być łatwe do zintegrowania z przebiegiem zadań roboczych i serwisowych.

Zapora sieciowa

Zapory sieciowe gwarantują, że tylko konkretne punkty końcowe będą mogły się komunikować z urządzeniami stacji, wyłącznie przy użyciu dozwolonych protokołów. Istnieją jednak sposoby na obejście zapory.



Punkty ataku obchodzące zapory sieciowe:

Dostęp zdalny dla celów serwisowych i sterowania.

Komputery testujące podłączone do szyny stacyjnej.

Komputery serwisowe podłączone do sieci lub bezpośrednio do urządzeń IED.

Pliki przenoszone na komputery używane w danej stacji.

Niechroniony rdzeń

- Kluczowe systemy, które muszą się komunikować w niezawodny sposób
- Urządzenia IED bez zainstalowanych poprawek: nie można instalować aktualizacji wystarczająco często ze względu na wymagane nakłady
- Starsze urządzenie z lukami w zabezpieczeniach, bez dostępnych aktualizacji

Zapory sieciowe nie zapewniają wystarczającej ochrony

Istnieje wiele sposobów na obejście zapory. W wielu stacjach korzysta się ze zdalnego dostępu do rejestracji zakłóceń lub do celów serwisowych. Takie połączenia stanowią ścieżkę, przez którą złośliwe oprogramowanie może się przedostać do urządzeń stacji.

Komputery serwisowe i używane do testów stanowią wektor ataku. Są one podłączane do całej sieci, bezpośrednio do poszczególnych zabezpieczeń lub sterowników.

Obrona głęboka

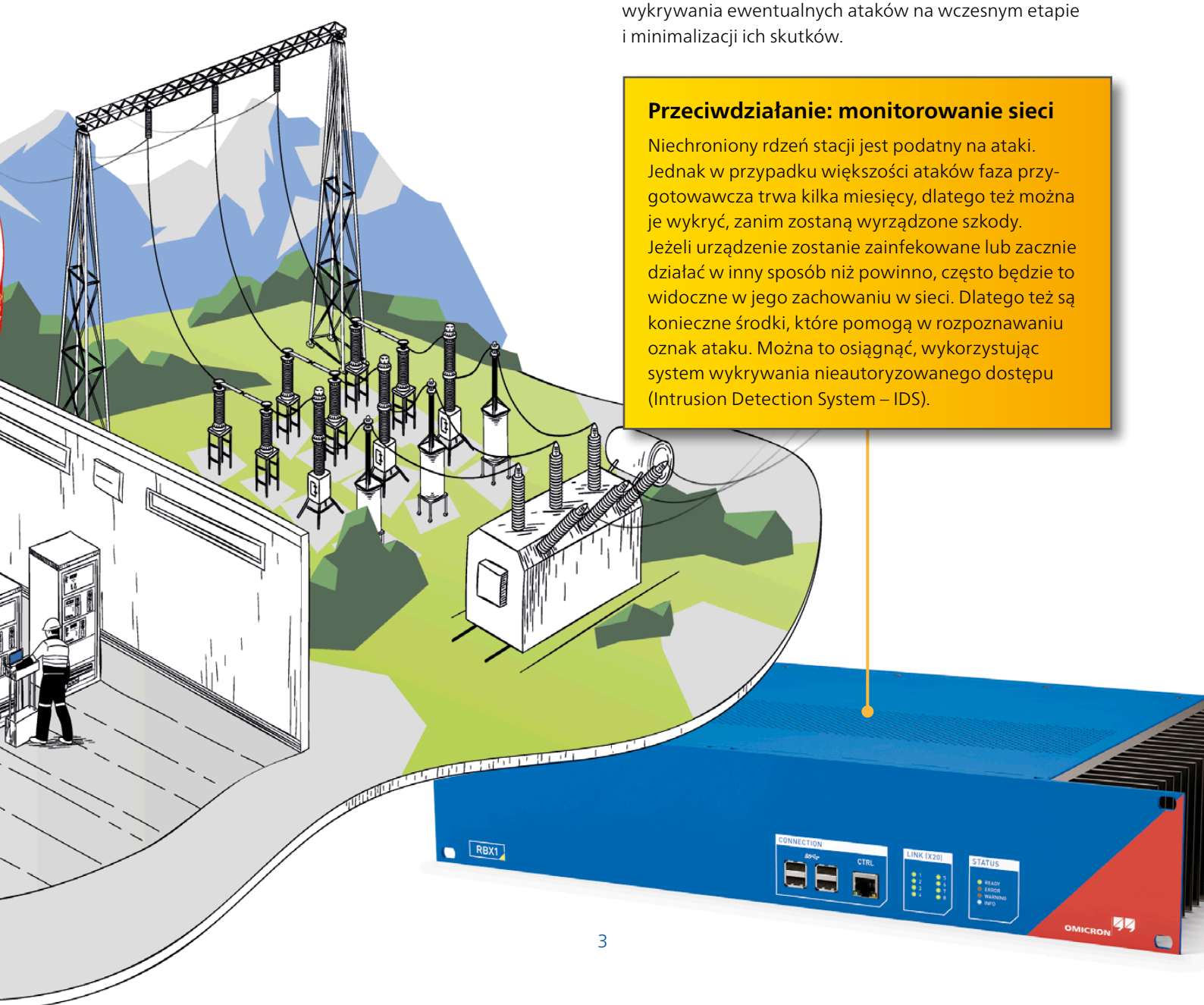
Zasada obrony głębokiej (Defense-in-Depth), jak podano w IEC 62443, zaleca, aby stosować nie tylko środki, które „utwardzają skorupę", ale również wprowadzają wiele warstw i poziomów rezerwy awaryjnej, które pomagają w zapewnieniu strefowego poziomu bezpieczeństwa.

Jednym z takich środków jest zapewnienie aktualizacji zabezpieczeń urządzeń IED. Jednak związane z tym nakłady i koszty są wysokie, przez co aktualizacje nie zawsze mogą być instalowane na czas. Starsze urządzenie często w ogóle nie mogą być aktualizowane, ponieważ dostawca przestaje wydawać aktualizacje do nich.

Dlatego też jest ważne, aby urządzenia, które nie mogą być odpowiednio chronione, były monitorowane w celu wykrywania ewentualnych ataków na wczesnym etapie i minimalizacji ich skutków.

Przeciwdziałanie: monitorowanie sieci

Niechroniony rdzeń stacji jest podatny na ataki. Jednak w przypadku większości ataków faza przygotowawcza trwa kilka miesięcy, dlatego też można je wykryć, zanim zostaną wyrządzone szkody. Jeżeli urządzenie zostanie zainfekowane lub zacznie działać w inny sposób niż powinno, często będzie to widoczne w jego zachowaniu w sieci. Dlatego też są konieczne środki, które pomogą w rozpoznawaniu oznak ataku. Można to osiągnąć, wykorzystując system wykrywania nieautoryzowanego dostępu (Intrusion Detection System – IDS).



Jak działają systemy detekcji włamań (IDS)

Systemy wykrywania nieautoryzowanego dostępu są najczęściej oparte na jednym z dwóch poniższych podejść:

1. Podejście bazujące na sygnaturach (czarna lista)

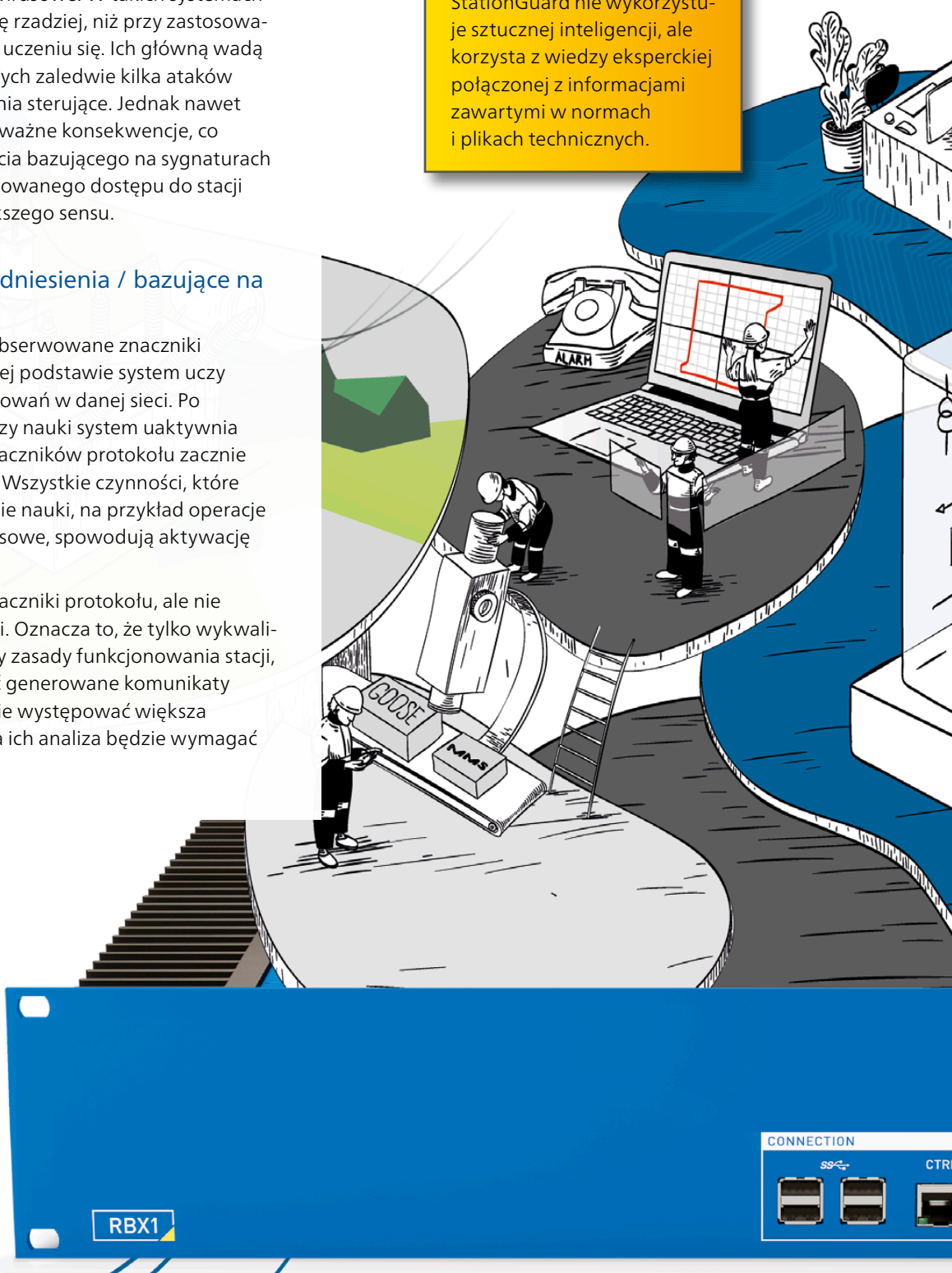
System IDS skanuje sieć w poszukiwaniu wzorców znanych ataków – jest to podejście wykorzystywane również przez skanery antywirusowe. W takich systemach fałszywe alarmy pojawiają się rzadziej, niż przy zastosowaniu podejścia bazującego na uczeniu się. Ich główną wadą jest to, że do dzisiaj jest znanych zaledwie kilka ataków na zabezpieczenia i urządzenia sterujące. Jednak nawet pierwszy atak może mieć poważne konsekwencje, co oznacza, że przyjęcie podejścia bazującego na sygnaturach przy wykrywaniu nieautoryzowanego dostępu do stacji wydaje się pozbawione większego sensu.

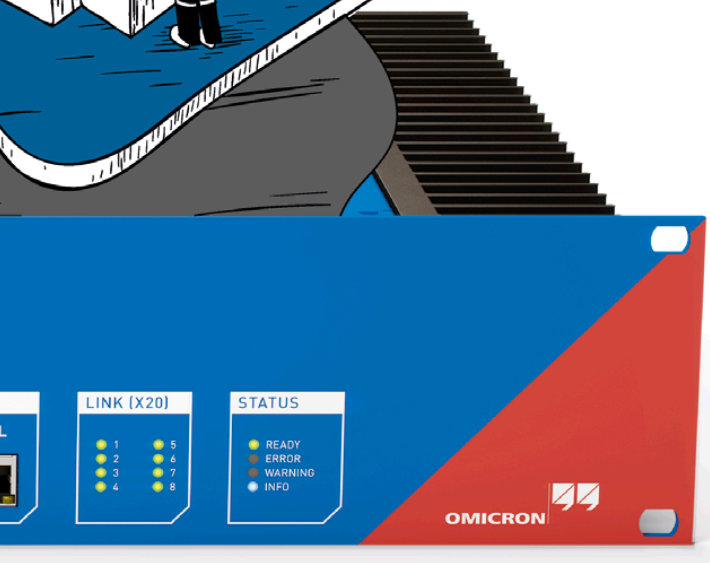
2. Podejście punktu odniesienia / bazujące na uczeniu się

Podczas fazy nauki są obserwowane znaczniki określonego protokołu i na tej podstawie system uczy się normalnego wzorca zachowań w danej sieci. Po zakończeniu początkowej fazy nauki system uaktywnia alarm, gdy tylko któryś ze znaczników protokołu zacznie zachowywać się nietypowo. Wszystkie czynności, które nie były uwzględnione w fazie nauki, na przykład operacje przełączania lub prace serwisowe, spowodują aktywację alarmu.

Ponadto system zna tylko znaczniki protokołu, ale nie rozumie, co dzieje się w stacji. Oznacza to, że tylko wykwalifikowany informatyk, znający zasady funkcjonowania stacji, będzie umiał zinterpretować generowane komunikaty alarmowe. Dlatego też będzie występować większa liczba fałszywych alarmów, a ich analiza będzie wymagać znacznego nakładu sił.

StationGuard nie wykorzystuje sztucznej inteligencji, ale korzysta z wiedzy eksperckiej połączonej z informacjami zawartymi w normach i plikach technicznych.





3. Podejście StationGuard

Stacje elektroenergetyczne i systemy SCADA są deterministyczne, co oznacza, że zachowanie urządzeń na stacji i systemów SCADA jest jasno określone, nawet w sytuacjach wyjątkowych, np. podczas działań zabezpieczeń.

W oparciu o tę charakterystykę, można zastosować całkowicie nowe podejście do wykrywania ataków cybernetycznych: znając funkcje każdego urządzenia, StationGuard tworzy model całego systemu automatyki, a następnie porównuje każdy pakiet sieciowy z tym modelem aktualizowanym w czasie rzeczywistym. Jest to odpowiednik podejścia opartego na białej liście, w którym są opisane wszystkie dopuszczalne zachowania, a każda odbiegająca od nich aktywność domyślnie uaktywnia alarm. Korzystając z tego podejścia, można również wykrywać zupełnie nowe rodzaje ataków.

Biała lista systemu StationGuard jest niezwykle szczegółowa. Nawet wartości sygnału zawarte w komunikatach są oceniane przy użyciu modelu systemowego. Umożliwia to wykrywanie nie tylko zagrożeń cybernetycznych i zabronionych działań, ale również problemów z funkcjami automatyki i systemu SCADA. Dlatego właśnie to połączenie wykrywania nieautoryzowanego dostępu i monitoringu funkcjonalnego nazwaliśmy „funkcjonalnym monitoringiem bezpieczeństwa" (Functional Security Monitoring) – jest to podejście, które rozwijamy od 2010 roku. To połączenie wiedzy z zakresu systemów elektroenergetycznych i bezpieczeństwa sprawia, że system StationGuard jest tak skuteczny.

Konfigurowanie systemu StationGuard nie wymaga fazy nauki, a jedynie kilku informacji wejściowych od użytkownika opisujących cel każdego urządzenia. W przypadku stacji działających zgodnie z IEC 61850 można znacząco przyspieszyć ten proces, importując pliki SCL.

Korzyści

- Mała liczba fałszywych alarmów, ponieważ system StationGuard zna procesy zachodzące w systemach elektroenergetycznych
- Komunikaty alarmowe są zrozumiałe dla osób nieznających protokołu
- Niezawodne wykrywanie nieupoważnionych działań

Podejście białej listy w systemie StationGuard

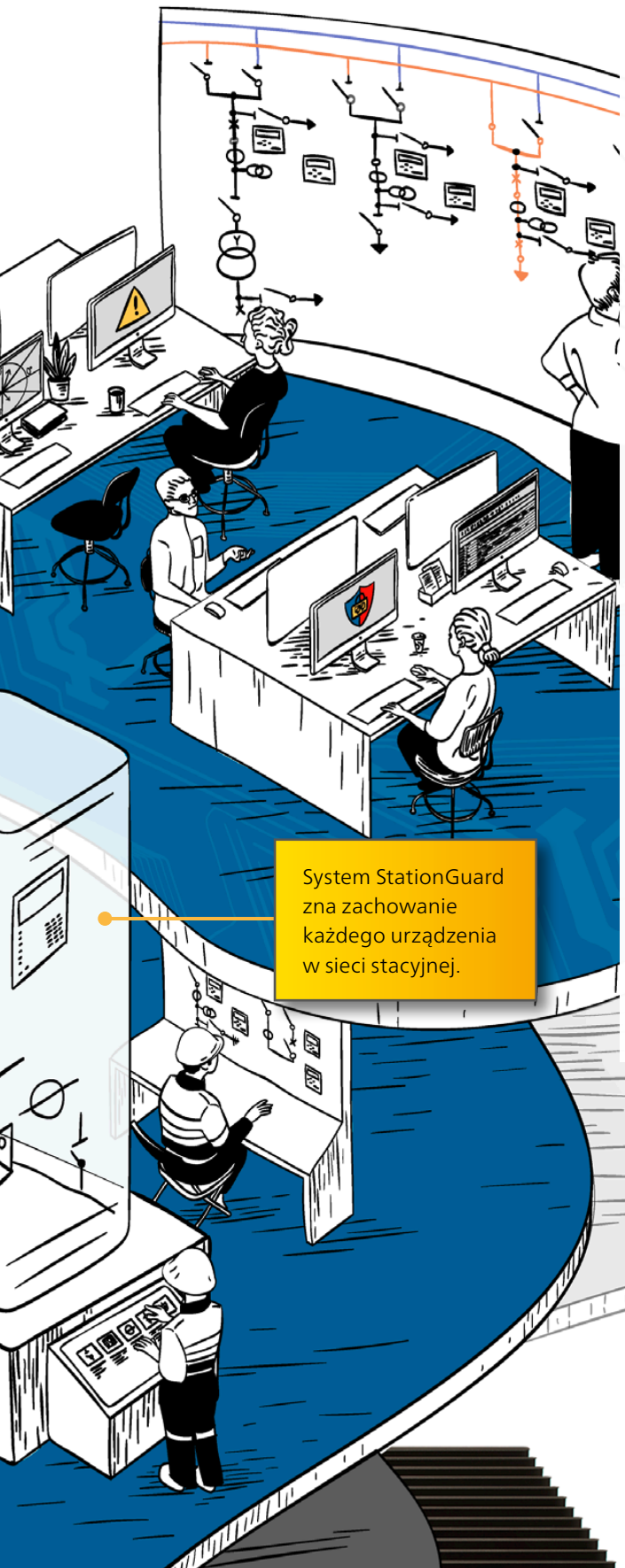
Bezpieczeństwo w najdrobniejszych szczegółach

Fakt, że cały ruch w sieci jest monitorowany i weryfikowany w tak szczegółowy sposób oznacza, że system wykrywa nie tylko zagrożenia bezpieczeństwa informatycznego, takie jak nielegalne kodowanie lub nieupoważnione operacje sterowania. StationGuard rozpoznaje również błędy komunikacji i problemy z synchronizacją czasową, a zatem różne nieprawidłowości w działaniu stacji. Gdy system IDS stosuje również schemat jednokreskowy, nie ma żadnych granic, do których nie może sięgać monitoring.

Przykłady: StationGuard aktualnie rozpoznaje 35 różnych kodów alarmów dla komunikatów GOOSE, od prostych sekwencji błędów numerycznych do złożonych pomiarów, takich jak nadmierne opóźnienie transmisji komunikatów. W tym ostatnim przypadku czasy otrzymywania pakietów są mierzone i porównywane z sygnaturami czasowymi zdarzeń zawartymi w komunikacie. Jeżeli zmierzony czas transmisji jest dłuższy niż dopuszczalny przez IEC 61850-5, StationGuard generuje komunikat alarmowy, który wskazuje, że może być problem z wysyłającym urządzeniem IED, siecią lub synchronizacją czasową.

StationGuard sygnalizuje również stany krytyczne i potencjalnie szkodliwe błędy kodowania dla kilkudziesięciu innych protokołów.

Tego rodzaju szczegółowe analizy są przeprowadzane również na innych protokołach IT/OT.



Komunikacja MMS, IEC 60870-5-104 i DNP3

System StationGuard wie, jakie funkcje są kontrolowane przez poszczególne punkty danych. Przykładowo, to samo polecenie może być wykorzystywane do sterowania wyłącznikiem, przełącznikiem zaczepów, a także do zmieniania ustawień trybu testu urządzenia. Wpływ na stację jest wyraźnie inny w każdym przypadku. StationGuard umie dokonać tego rozróżnienia i wie, które urządzenie i w jakiej sytuacji powinno sterować określonymi zasobami. Te drobiazgowe zezwolenia są dokumentowane i mogą być analizowane przez system StationGuard.

Inne protokoły

StationGuard przeprowadza głęboką inspekcję pakietów dla dziesiątków systemów elektroenergetycznych i klasycznych protokołów IT. Dzięki temu StationGuard nie tylko wykrywa naruszenia kodowania w tych protokołach, ale również potrafi stwierdzić, czy kontrola nad numerami portów, np. połączeń zdalnych, nie została przejęta przez nieoczekiwane aplikacje (spoofing portów).

Obsługiwane protokoły (głęboka inspekcja pakietów)

- IEC 61850
- IEC 60870-5-104
- DNP3
- PRP/HSR
- Modbus TCP
- Synchrofazor
- DLMS/COSEM
- AMI
- TASE.2/ICCP
- FTP
- HTTP
- RDP
- NTP
- ARP, DHCP, ICMP
- MySQL, MS SQL, PostgreSQL
- HTTPS, SSH (wykrywanie aplikacji, bez odszyfrowywania)
- telnet
- RIPv2
- SSDP
- ...

Korzyści

> Każdy pakiet jest porównywany z modelem systemu (białą listą)

> Są wykrywane nie tylko zagrożenia cybernetyczne, ale również problemy z funkcjami i komunikacją

> StationGuard nadzoruje funkcje zabezpieczeń całej komunikacji w stacji i systemu SCADA

Dostosowany do potrzeb systemów elektroenergetycznych

Do konfiguracji, obsługi i serwisowania konwencjonalnych systemów wykrywania nieautoryzowanego dostępu (IDS) są niezbędni wykwalifikowani informatycy oraz inżynierowie obsługujący systemy sterowania i automatyki. Specjaliści w obu tych dziedzinach muszą być w pogotowiu przez całą dobę, aby można było zareagować, gdy pojawi się alarm. Związane z tym koszty są nieakceptowalne dla wielu przedsiębiorstw. StationGuard oferuje przedsiębiorstwom energetycznym nową, prostszą w utrzymaniu alternatywę.

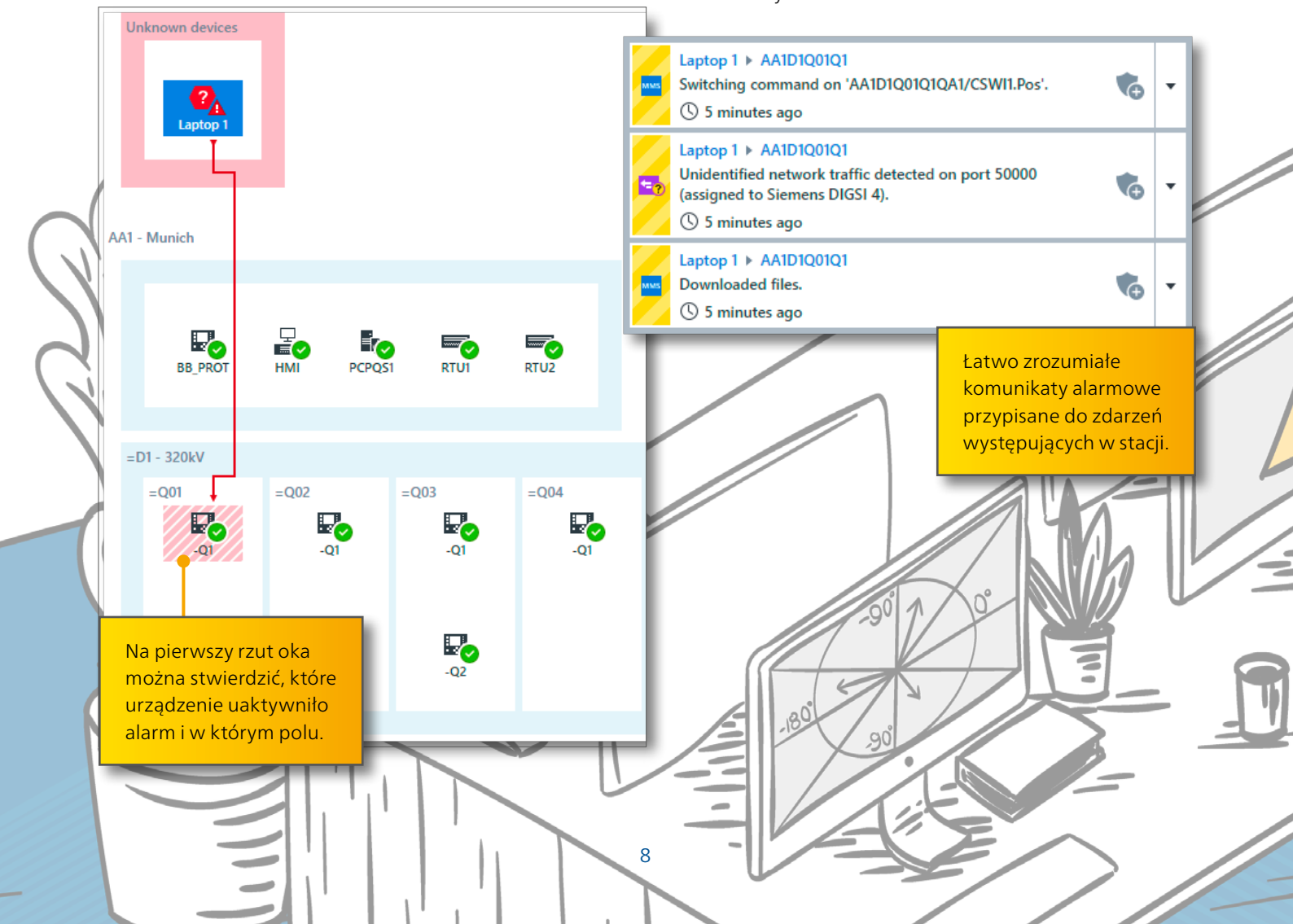
StationGuard zna typowe funkcje realizowane w stacji i wie, w jaki sposób są najczęściej używane urządzenia informatyczne, takie jak komputery przemysłowe i testujące. Wszystkie te informacje są dostępne automatycznie, więc konfiguracja systemu StationGuard do normalnego działania jest szybka.

Konfiguracja

Po podłączeniu systemu StationGuard do portów lustrzanych (mirror ports) przełączników sieciowych są rozpoznawane wszystkie urządzenia komunikujące się w sieci.

W przypadku stacji działających w standardzie IEC 61850, można importować techniczne pliki SCL w celu automatycznej identyfikacji wszystkich urządzeń IED i umieszczenia ich na schemacie stacji. Gdy komunikacja nie pasuje do informacji zawartych w plikach SCL, StationGuard zgłasza błędy konfiguracji IEC 61850. Jest to szczególnie przydatne w fazie fabrycznych testów akceptacyjnych i testów odbioru końcowego.

W przypadku stacji lub systemów SCADA wykorzystujących protokoły IEC 60870-5-104, DNP3 lub Modbus, urządzenia IED i terminale RTU można klasyfikować ręcznie, używając wstępnie zdefiniowanych reguł, za pomocą kilku kliknięć. Następnie wszystkie pozostałe urządzenia informatyczne można przypisać do ich konkretnych ról, takich jak przełączniki lub komputery przemysłowe. Te role również można modyfikować.



Normalna praca

StationGuard analizuje całą komunikację i wie dokładnie, które informacje mogą być transmitowane w danym momencie, a które nie. Które urządzenia mogą być aktywne w danej chwili? Które polecenia sterujące są dozwolone i czy odpowiedź na te polecenia ma sens? Które pomiary są transmitowane? Czy synchronizacja komunikatów jest prawidłowa? Umożliwia to wykrywanie na wczesnym etapie wszystkich prawdopodobnych problemów z urządzeniami IED lub z siecią, zanim ulegną awarii.

Ten kompleksowy monitoring funkcji i bezpieczeństwa jest unikatowy i zapewnia korzyści znacznie wykraczające poza to, czego normalnie można oczekiwać od systemu wykrywania nieautoryzowanego dostępu (IDS).

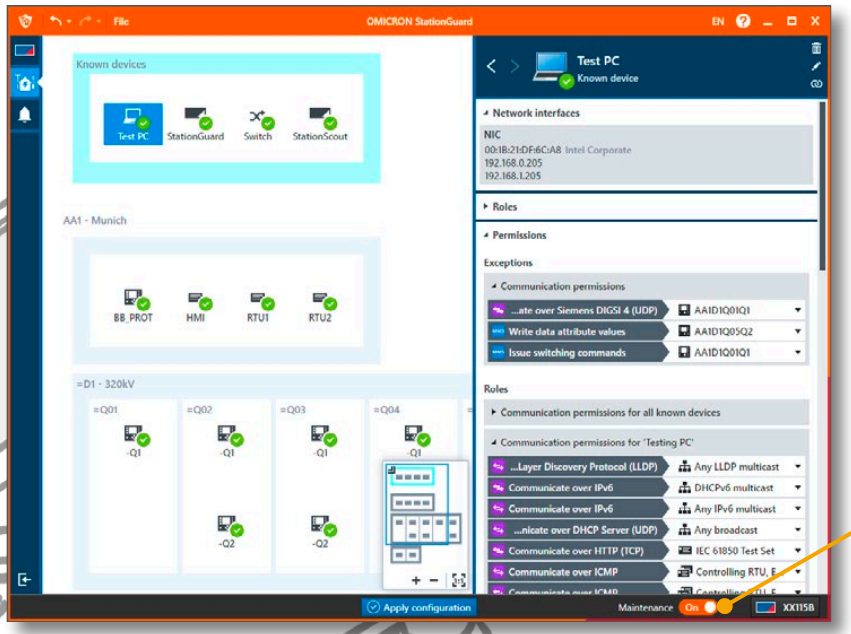
Graficzny interfejs użytkownika umożliwia inżynierom zajmującym się zabezpieczeniami i sterowaniem szybkie opanowanie systemu StationGuard, ponieważ jest on spójny ze schematami znajdującymi się w dokumentacji i widokiem zdarzeń elementów sterowania stacji.

Serwisowanie i rozruch

Testy i serwisowanie są ważne i nie mogą generować żadnych fałszywych alarmów. Jednocześnie należy zapewnić wysoki poziom bezpieczeństwa informatycznego. W celu spełnienia tych wymagań system StationGuard oferuje „tryb serwisowy". Czynności związane z konserwacją i testami są dopuszczalne wyłącznie po uaktywnieniu tego trybu.

W wielu scenariuszach ataku są wykorzystywane słabości w protokołach dostawców lub interfejsach internetowych. Dlatego też StationGuard może wygenerować alarm, gdy podczas normalnej pracy pojawi się komunikacja z narzędziami producenta i dopuścić ją tylko w trybie serwisowym. W systemie StationGuard można rejestrować komputery przemysłowe i testery, zanim zostaną użyte, aby umożliwić wykonywanie autoryzowanych zadań bez generowania fałszywych alarmów.

Nie ma to ujemnego wpływu na bezpieczeństwo podczas wykonywania testów: gdy zainfekowany komputer testujący będzie się komunikować w podejrzany sposób, zostanie uaktywniony alarm.



Niektóre działania są dozwolone jedynie w trybie konserwacji.

Zalety

- Wyjątkowo łatwa konfiguracja
- Brak fałszywych alarmów podczas rutynowych testów przy zachowanym wysokim poziomie bezpieczeństwa
- Brak fazy nauki, natychmiastowa ochrona

Szybka reakcja dzięki zrozumiałym komunikatom alarmowym

Wiarygodna identyfikacja przyczyn alarmów

Alarmy uaktywniane przez system zabezpieczeń powinny pomagać operatorowi, a nie wprowadzać jeszcze większe zamieszanie. Dlatego też alerty systemu StationGuard nie tylko pojawiają się na liście zdarzeń, ale są również prezentowane graficznie na schemacie ogólnym. Zdarzenia zachodzące w systemie elektroenergetycznym kryjące się za pakietami sieciowymi są identyfikowane i prezentowane przy użyciu jasnej terminologii.

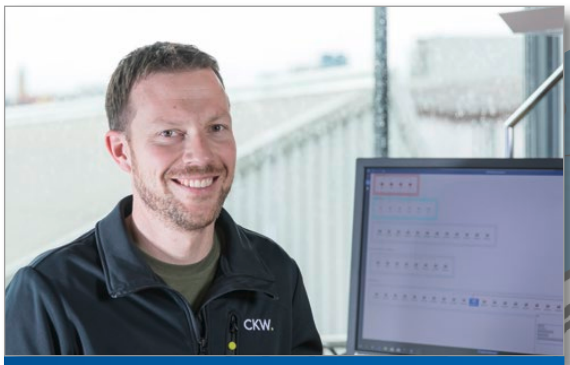
Rozważmy następujący przykład: komputer testujący próbuje sterować wyłącznikiem, używając protokołu MSS. Powiązany z tym zdarzeniem komunikat alarmowy nie jest prezentowany za pomocą terminów protokołu, ale jest interpretowany zgodnie z tym, co aktualnie dzieje się w stacji. Zawiera informacje takie jak: Co się stało? Które urządzenie jest za to odpowiedzialne?

Umożliwia to ekspertom ds. bezpieczeństwa informatycznego oraz inżynierom zajmującym się systemami SCADA i zabezpieczeniami podjęcie skutecznej współpracy w celu określenia przyczyny alarmu. Inżynierowie pracujący w stacji będą zatem mogli korzystać z komunikatów alarmowych IDS, tak jakby analizowali dziennik operacyjny, listę zdarzeń lub listę ostrzeżeń na sterowniku stacyjnym.

Analizowanie i przekazywanie alertów

Łatwym sposobem integracji systemu StationGuard w starszych stacjach jest użycie wyjść binarnych platformy RBX1. Obecność niepotwierdzonego alarmu jest sygnalizowana na wyjściach binarnych, które mogą być połączone z terminalem RTU i zintegrowane z listą sygnałów SCADA.

Alternatywnie nasze łatwe do zrozumienia komunikaty alarmowe mogą być również przekazywane przy użyciu protokołu syslog. Są dostępne różne wtyczki programowe, które umożliwiają integrację systemu StationGuard z systemem zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM) oraz z systemami ticketowymi używanymi przez różnych dostawców.



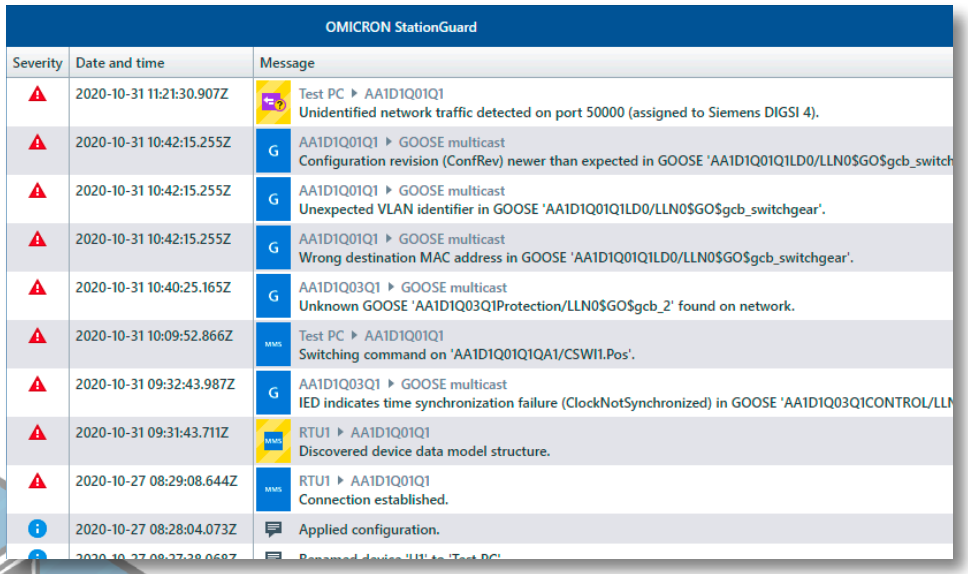
„Praca z systemem StationGuard jest naprawdę łatwa. Wszystkie potrzebne informacje są wyświetlane w przejrzysty sposób, bez stosowania żargonu informatycznego. Wszystko to w najwyższej jakości oferowanej przez firmę OMICRON, do której jesteśmy już przyzwyczajeni."

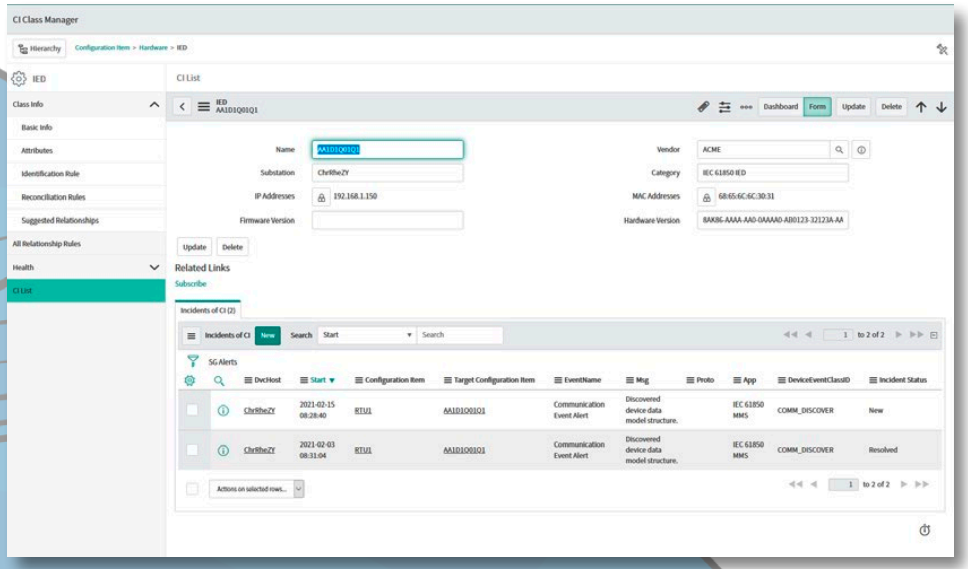
Yann Gosteli
kierownik ds. systemów automatyki stacyjnej
CKW AG, Szwajcaria

Dziennik zdarzeń

Oprócz widoku graficznego, alarmy są również zapisywane w dzienniku zdarzeń. W dzienniku są rejestrowane zmiany konfiguracji i potwierdzenia alarmów dokonane przez użytkowników. Dziennik stanowi również zapis zdarzeń krytycznych, takich jak operacje sterowania, zmiany trybu testu urządzeń IED i pobieranie plików (włącznie z nazwami plików).

W dzienniku zdarzeń można, na przykład, filtrować wszystkie przeszłe zdarzenia związane z konkretnym urządzeniem. Można więc wykrywać tendencje, nawet w przypadku zdarzeń występujących tylko sporadycznie..





Wtyczka programowa StationGuard ServiceNow (TM)

StationGuard pasuje do Twojej strategii bezpieczeństwa informatyczn

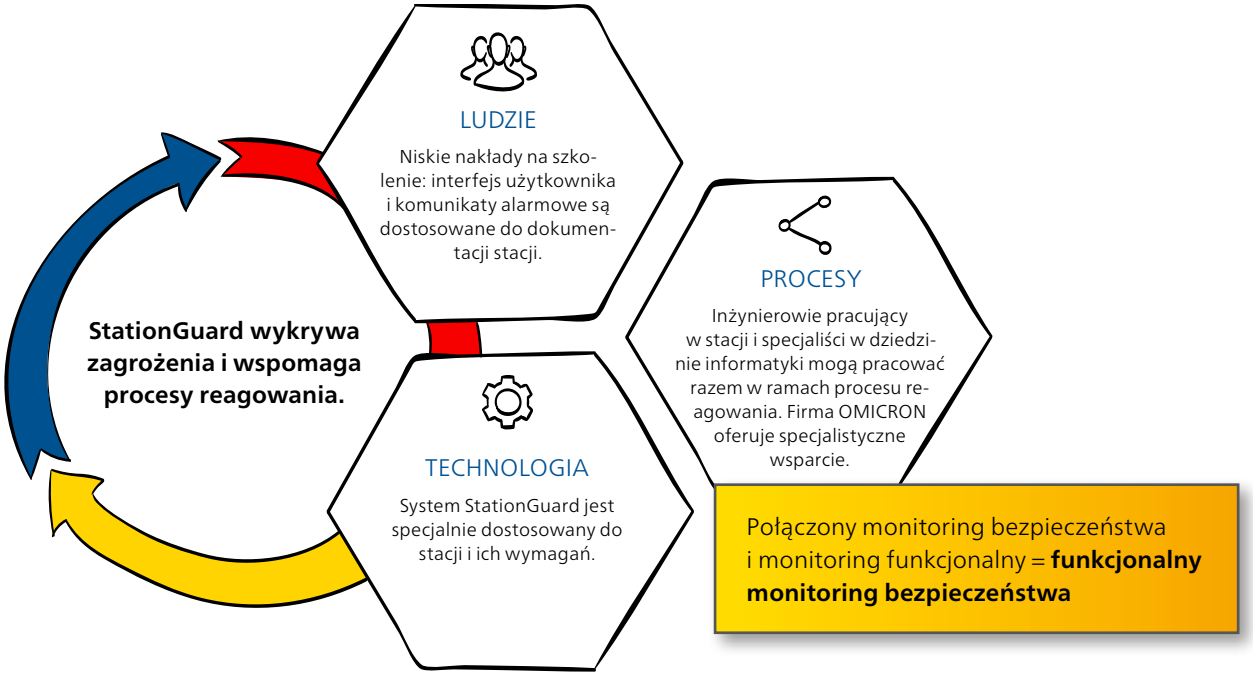
Zabezpieczenia cybernetyczne działają prawidłowo tylko wtedy, gdy ludzie, procesy i technologia współpracują ze sobą. Jedno z kluczowych pytań brzmi zatem następująco: Jakie procesy są realizowane, gdy pojawi się alarm bezpieczeństwa? Celem systemu StationGuard jest technologiczne wspomaganie tych procesów reagowania w najlepszy możliwy sposób.

Gdy inżynierowie wykonują prace w stacji, restartują urządzenia lub gdy mają miejsce zdarzenia związane z ochroną, często wstępują fałszywe alarmy. StationGuard zna typowe zdarzenia, a interfejs użytkownika jest dostosowywany do schematów i terminologii używanych w stacji. Umożliwia to inżynierom szybkie określenie, czy alarm jest efektem znanej operacji, czy może wymaga dalszego zbadania przez ekspertów ds. bezpieczeństwa.

Dzięki połączeniu specyficznej dla danej stacji wizualizacji przeznaczonej dla inżynierów zajmujących się zabezpieczeniami, ze szczegółowymi informacjami przeznaczonymi dla ekspertów ds. bezpieczeństwa, wszystkie osoby mogą pracować wspólnie nad poszukiwaniem przyczyny alarmu.

Pełna integracja z procesami zabezpieczającymi technologie operacyjne

- √ **Dziennik zdarzeń**
  StationGuard rejestruje krytyczne działania, takie jak operacje przełączania, zmiany konfiguracji urządzeń IED lub potwierdzenia alarmów.
- √ **Wykrywanie i eksportowanie urządzeń**
  Są wykrywane wszystkie urządzenia w sieci, a spis urządzeń można eksportować. Szczegółowe informacje dotyczące urządzeń są gromadzone na podstawie ruchu w sieci i importowanych plików technicznych (SCL), dzięki czemu wśród nich znajdują się szczegółowe informacje dotyczące sprzętu i wersji firmware'u.
- √ **Integracja z systemami SIEM i systemami ticketowymi**
  System StationGuard można łatwo zintegrować z wieloma systemami SIEM i systemami ticketowymi używanymi przez wielu dostawców, przy pomocy protokołu syslog i naszych wtyczek programowych.
- √ **Ślady sieciowe**
  Dla każdego zdarzenia zostaje utworzony ślad sieciowy zgodny z Wireshark (PCAP), dostępny do dalszej analizy.
- √ **Uwierzytelnianie użytkowników[1]**
  Jest możliwe skonfigurowanie integracji z usługami LDAP / Active Directory za pośrednictwem centralnego systemu zarządzania StationGuard. Wyłącznie autoryzowani użytkownicy mogą zmieniać konfigurację lub aktywować tryb serwisowy.



nego

Rygorystycznie wzmocniona platforma

√ **Bezpieczny kryptoprocesor**
Klucze i certyfikaty są przechowywane wyłącznie w zabezpieczonym przed penetracją i fałszerstwami układzie scalonym zgodnym z ISO/IEC 11889.

√ **Bezpieczny łańcuch bootowania**
Do weryfikacji sygnatur każdego ładowanego modułu oprogramowania jest używany kryptoprocesor. Dzięki temu będzie dozwolone uruchamianie wyłącznie oprogramowania firmy OMICRON.

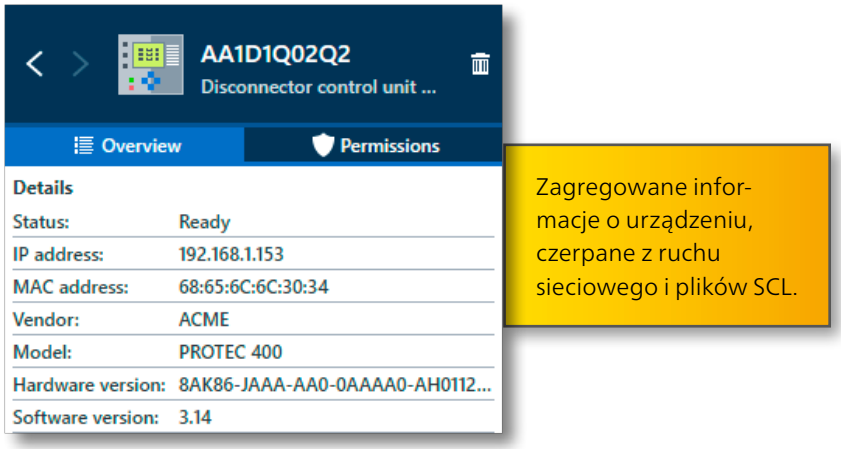
√ **Podpisane i zaszyfrowane aktualizacje**
Urządzenie StationGuard akceptuje wyłącznie te aktualizacje firmware'u, które są podpisane przez firmę OMICRON. Aktualizacje oprogramowania komputerowego również są podpisane.

√ **Pełne szyfrowanie dysków**
Kryptoprocesor jest używany do szyfrowania wszystkich danych za pomocą klucza unikatowego dla każdego urządzenia.

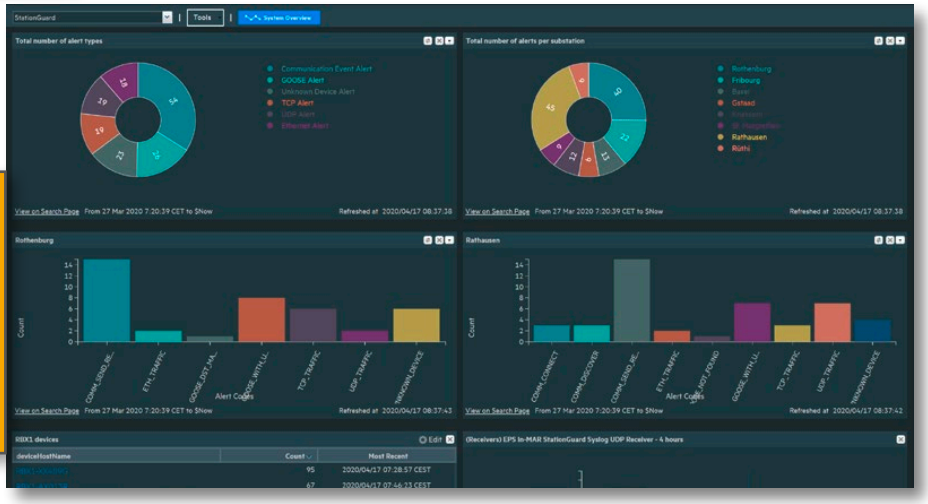
√ **Specjalny, wzmocniony system operacyjny**
Używany jest dedykowany, wzmocniony system Linux. Każdy proces otrzymuje wyłącznie te uprawnienia, które są absolutnie niezbędne do realizacji zleconego zadania.

√ **Szyfrowana komunikacja pomiędzy jednostką a komputerem**
Komunikacja pomiędzy systemem StationGuard a komputerem jest szyfrowana za pomocą protokołu TLS (Transport Layer Security).

√ **Nasi specjaliści nieustannie rozwijają nasze systemy...**
Specjaliści z firmy OMICRON stale wdrażają nowe środki, jeszcze bardziej wzmacniając bezpieczeństwo naszej platformy.



Zagregowane informacje o urządzeniu, czerpane z ruchu sieciowego i plików SCL.



Analiza przyczyn źródłowych zamieszczana przez system StationGuard w alertach umożliwia wykorzystanie inteligentnych statystyk w systemach SIEM oferowanych przez wszystkich dostawców.

Trzy różne opcje platformy

Czujniki StationGuard są dostępne na trzech różnych platformach. Zależnie od Twoich potrzeb, możesz używać systemu StationGuard na platformie sprzętowej RBX1, MBX1 lub na maszynie wirtualnej. Cała inteligencja systemu StationGuard jest zawarta w czujniku, więc czujniki pracują autonomicznie – nie jest wymagane stałe połączenie z serwerem centralnym.

StationGuard na platformie RBX1

System StationGuard pracujący na platformie RBX1 jest dostosowanym do indywidualnych potrzeb rozwiązaniem IDS chroniącym automatykę stacyjną i systemy SCADA przez zagrożeniami cybernetycznymi i atakami dnia zerowego. Montowana na stelażu 19-calowa platforma RBX1 jest przeznaczona do użytku w trudnym środowisku sieci energetycznej. Posiada wydajność i pamięć wystarczające do rejestracji wszystkich zdarzeń związanych z ruchem, nawet jeżeli od wystąpienia zdarzenia minęło dużo czasu.

Platforma RBX1 ma niezrównane zabezpieczenia, takie jak pełne szyfrowanie dysku, kryptoprocesor zgodny z ISO/IEC 11889, a także zindywidualizowany bezpieczny interfejs UEFI (Unified Extensible Firmware Interface). Wyjścia binarne umożliwiają łatwą integrację alertów systemu IDS z listą sygnałów SCADA.

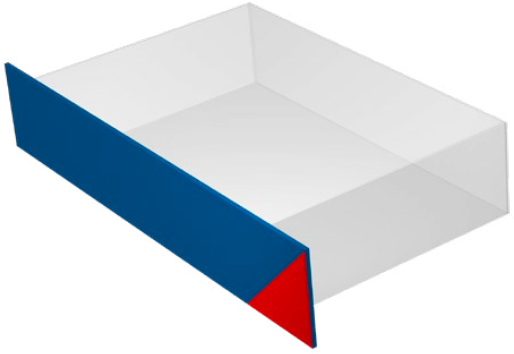
StationGuard na platformie MBX1

System StationGuard pracujący na jednostce sprzętowej MBX1 oferuje taki sam wysoki poziom bezpieczeństwa, jak wersja montowana na stelażu. Używając mobilnej wersji systemu StationGuard, możesz przeprowadzać szybkie oceny bezpieczeństwa stacji lub sieci SCADA, a także szybko generować listy urządzeń obejmujące wszystkie urządzenia w sieci.

Na etapach rozruchu i konserwacji wielu inżynierów, a także usługodawców zewnętrznych, podłącza swoje urządzenia do wrażliwej sieci stacji. StationGuard na platformie MBX1 idealnie się nadaje do tymczasowego monitorowania sieci podczas tego rodzaju działań. System będzie generować alarm w przypadku niedozwolonych zachowań i zarejestruje wszystkie czynności krytyczne, które miały miejsce podczas rozruchu i serwisowania.

StationGuard na platformie maszyn wirtualnych

Czujniki systemu StationGuard są również dostępne jako urządzenie wirtualne, które można instalować na istniejących już w stacjach platformach obliczeniowych.



Tak samo, jak w przypadku platformy sprzętowej, wersja wirtualna również może pracować całkowicie niezależnie, rejestrując i zapisując zdarzenia, nawet jeżeli nie ma stałego połączenia z serwerem centralnym. Proszę zauważyć, że podczas pracy na maszynach wirtualnych, w porównaniu z systemami StationGuard działającymi na platformach RBX1 i MBX1, mogą pojawić się pewne ograniczenia techniczne w zakresie monitoringu funkcjonalnego aplikacji magistrali procesowej.

Specyfikacja techniczna platformy RBX1

Warunki środowiskowe

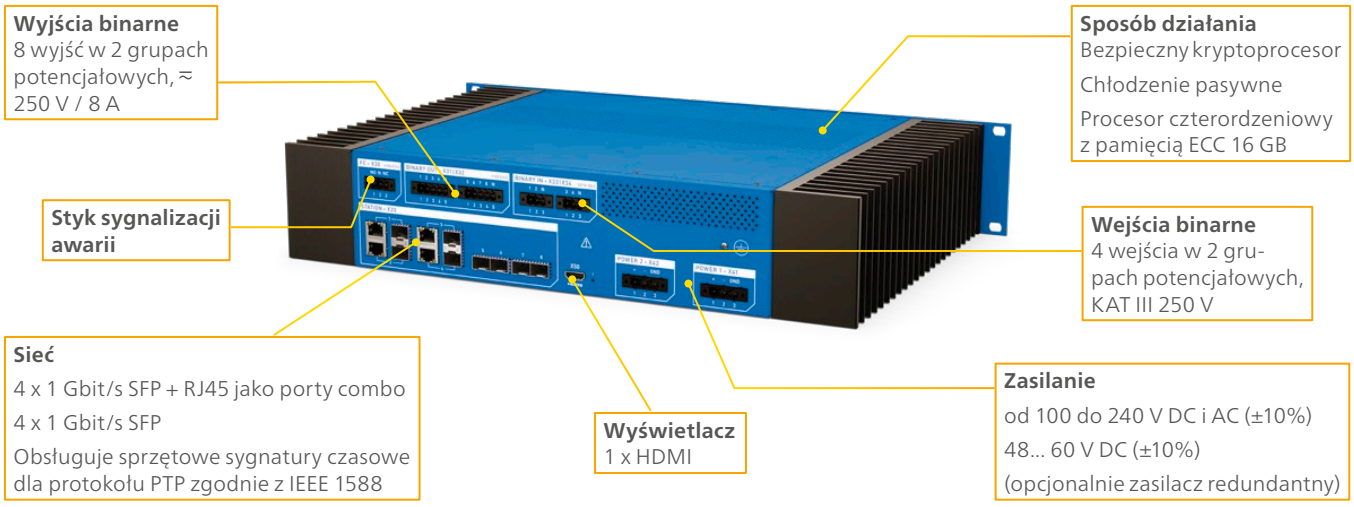
Temperatura pracy	-20°C ... +55°C
Temperatura przechowywania	-25°C ... +70°C
Wilgotność względna	5%... 95% (bez kondensacji)
Stopień ochrony IP zgodnie z IEC 60529	IP30

Normy

Normy dotyczące produktu	IEC 61850-3 IEEE 1613 Poziom ważności: Klasa 1
Normy EMC	IEC 61326-1 IEC 60255-26, IEC 61000-6-5
Bezpieczeństwo	EN 60255-27, EN 61010-1, EN 61010-2-030

Więcej szczegółów można znaleźć w arkuszach danych technicznych.

Widok z tyłu platformy RBX1



Widok z przodu platformy RBX1

Z systemem StationGuard oferujemy znakomity poziom bezpieczeństwa cybernetycznego

Dogłębna wiedza z zakresu technologii operacyjnej (OT)

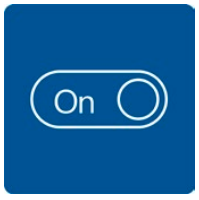
Firma OMICRON ma ponad 30 lat doświadczenia z technologią OT. Ta wiedza jest wbudowana w czujniki systemu StationGuard i pozwala na precyzyjne zgłaszanie wszystkich odbiegających od normy zachowań operacyjnych, takich jak włamania (ataki), problemy funkcjonalne, czy proste czynności serwisowe.

specjalistyczna wiedza z zakresu technologii OT

Natychmiastowy rozruch

W obiektach zgodnych z IEC 61850 StationGuard jest uruchamiany natychmiastowo przy użyciu opcji importu pliku SCL. Z kolei w zakładach zgodnych z IEC 60870-5-104 faza konfiguracji systemu StationGuard może zostać znacznie skrócona dzięki zastosowaniu naszych predefiniowanych ról. W obu przypadkach czas pomiędzy pierwszym podłączeniem systemu StationGuard do sieci, a rozpoczęciem rzeczywistego wykorzystywania jego możliwości jest niezwykle krótki. Nie są potrzebne długie fazy konfigurowania, szkolenia i nauki.

natychmiastowa ochrona



Tryb serwisowy o dużych możliwościach

Tryb serwisowy w jeszcze większym stopniu zwiększa poziom bezpieczeństwa. Podczas normalnej pracy konserwacja jest zabroniona i natychmiast wykrywana. W przypadku zaplanowanych czynności serwisowych, StationGuard może odpowiednio zareagować (korzystając z trybu serwisowego) i zabezpieczyć wszystkie prace, nawet te, które są wykonywane w tym stadium.

bezpieczeństwo na każdym etapie pracy

Wyposażony odpowiednio do środowiska

System StationGuard można łatwo zintegrować z istniejącym środowiskiem przy użyciu jego złącz, wykorzystując go razem z systemami zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM) lub silnymi systemami ticketowymi, takimi jak ServiceNow. Ponadto wyjścia binarne starszych systemów StationGuard można połączyć na stałe z operacyjnym centrum bezpieczeństwa (SOC), co pozwala na uzyskanie optymalnej integracji.

współpraca z systemami innych dostawców

Głęboka inspekcja pakietów aż do ostatniego bitu

System dzienników StationGuard jest idealnie przygotowany do analizy określonych (długoterminowych) zachowań, a możliwości sniffera Wireshark PCAP umożliwiają analitykom głęboki wgląd w podejrzane pakiety, nawet na poziomie pojedynczych bitów.

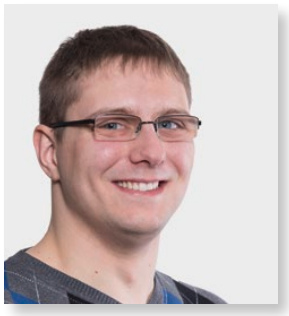
odpowiedzialny za Twoją komunikację

Wyjątkowe wsparcie

Specjalistyczne wsparcie StationGuard

W przypadkach, gdy alarm sygnalizuje nieautoryzowane zachowanie komputerów lub urządzeń polowych albo zachowanie, które jest niezgodne z normą, eksperci StationGuard mogą zaoferować wsparcie w zakresie analizy alertu. Nasi specjaliści mogą przeanalizować zapisy z sieci i określić, w oparciu o zachowania komunikacyjne i znane słabe punkty konkretnych urządzeń, czy dane zdarzenie może stanowić zagrożenie, czy też zostało spowodowane przez problemy techniczne.

W każdej chwili możesz się skontaktować z naszym działem wsparcia technicznego. Nasi konsultanci, po wykonaniu bezpiecznej transmisji danych związanych ze zdarzeniem, skontaktują się z jednym z ekspertów z biura firmy OMICRON. Nasi specjaliści znają zachowania komunikacyjne, a także słabe punkty zabezpieczeń, automatyki i urządzeń sterujących od niemal wszystkich dostawców z całego świata.



„Jako specjalista ds. luk w zabezpieczeniach urządzeń IED, dokładnie wiem, jak rozpoznać ataki na sieć. Chętnie wesprę Cię moją wiedzą!".

Stefan Lässer
ekspert w dziedzinie luk w zabezpieczeniach urządzeń IED wykonanych zgodnie z IEC 61850

„Jako członek grup roboczych ds. standaryzacji i autor wielu artykułów poświęconych komunikacji w stacjach, często jestem proszony o konsultacje, gdy pojawiają się złożone problemy z GOOSE, wartościami Sampled Values i komunikacją MMS".

Fred Steinhauser,
ekspert w dziedzinie stacji cyfrowych

Całodobowa pomoc techniczna

Gdy potrzebujesz szybkiej pomocy, otrzymasz najwyższej klasy wsparcie od naszych gruntownie przeszkolonych i wyspecjalizowanych techników, 24 godziny na dobę, siedem dni w tygodniu.

Jesteśmy dumni z naszego nadzwyczajnego wsparcia klientów i najwyższej jakości usług.

„Dołączyłem do działu pomocy technicznej firmy OMICRON w 2010 roku i od tej pory koncentruję się na normie IEC 61850".

Lukas Gassner
dział pomocy technicznej firmy OMICRON

24/7 support

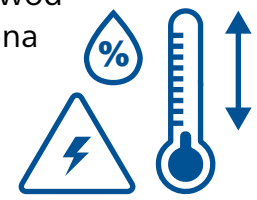
Tworzymy wartość dla Klienta poprzez ...

Jakość

Możesz polegać na najwyższych standardach bezpieczeństwa i ochrony

Najwyższa niezawodność potwierdzona w trakcie

72



godzin testów wygrzewania przed dostawą

Ponad

30.000

automatycznych testów programowych wykonywanych 24 godziny na dobę

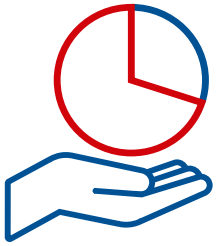
ISO 9001
TÜV & EMAS
ISO 14001
OHSAS 18001

Zgodność z normami międzynarodowymi

Innowacyjność

Oszczędź do

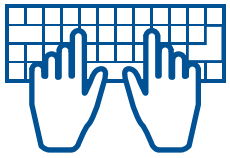
70%



czasu
podczas konfiguracji i obsługi

Ponad

200

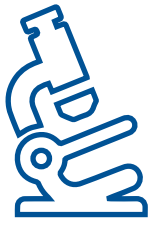


konstruktorów
dba o aktualność naszych rozwiązań

... gama produktów dostosowana do moich potrzeb

Ponad

15%

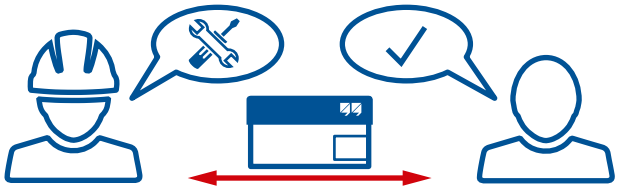


naszej rocznej wartości sprzedaży ponownie inwestujemy w badania i rozwój

Wsparcie

Zawsze dostępna profesjonalna pomoc techniczna

biura na całym świecie, z którymi można się kontaktować i uzyskać pomoc techniczną



Oszczędne i nieskomplikowane naprawy

Eksperci ds. bezpieczeństwa cybernetycznego zapewniają łatwe i szybkie rozwiązania

Wiedza

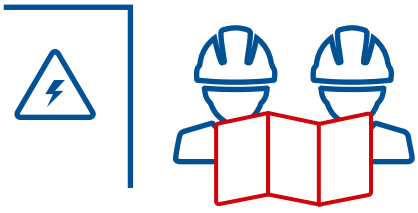
Ponad

300

kursów i liczne szkolenia praktyczne każdego roku

Częste spotkania użytkowników seminaria i konferencje organizowane przez OMICRON

tysiące dokumentów technicznych i not aplikacyjnych



Rozległa wiedza ekspercka wykorzystywana podczas rozruchu i konsultacji

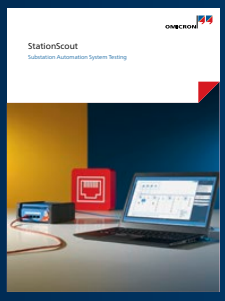
OMICRON to firma międzynarodowa, w której pracujemy z pasją nad ideami, które czynią systemy elektroenergetyczne bezpiecznymi i niezawodnymi. Nasze pionierskie rozwiązania są zaprojektowane w taki sposób, aby stawić czoła obecnym i przyszłym wyzwaniom stojącym przed branżą. Zawsze dokładamy wszelkich starań, aby wspomagać naszych klientów: reagujemy na ich potrzeby, zapewniamy znakomite wsparcie lokalne i dzielimy się naszą wiedzą.

W obrębie grupy OMICRON badamy i opracowujemy innowacyjne technologie stosowane na wszystkich polach w systemach elektroenergetycznych. Gdy przychodzi do testów elektrycznych urządzeń średniego i wysokiego napięcia, testowania zabezpieczeń, testowania stacji cyfrowych, a także rozwiązań w zakresie bezpieczeństwa cybernetycznego, klienci z całego świata ufają precyzji, szybkości i jakość naszych przyjaznych dla użytkownika rozwiązań.

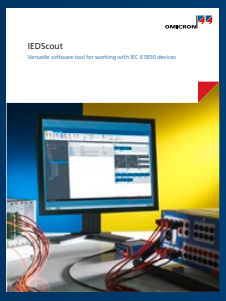
Założona w 1984 r. firma OMICRON czerpie ze swojej gruntownej wiedzy eksperckiej w zakresie energetyki. Oddany zespół złożony z przeszło 900 pracowników dostarcza rozwiązania, zapewniając przy tym całodobowe wsparcie przez cały tydzień w 25 centrach pomocy na całym świecie i służy klientom z ponad 160 krajów.

Szczegółowe informacje na temat rozwiązań opisanych w niniejszej broszurze można znaleźć w następujących publikacjach:

IEC 61850 – Broszura



StationScout – broszura



IEDScout – Broszura

DANEO 400 – Broszura

Szczegółowe informacje, dodatkowe publikacje oraz dane kontaktowe naszych oddziałów na całym świecie można znaleźć w naszej witrynie internetowej.

www.omicronenergy.com

L4299