Sprawdź dojrzałość swojej organizacji z SANS ICS 5 Critical Controls

The SANS 5 Critical Controls for ICS Cybersecurity jest niezbędny do zabezpieczenia Systemów Sterowania Przemysłowego (ICS) przed rosnącym krajobrazem zagrożeń. Wskaźniki te zapewniają usystematyzowane podejście do zwiększenia poziomu bezpieczeństwa środowisk OT, gwarantując ochronę infrastruktury krytycznej. Zostały zaprojektowane, aby rozwiązywać powszechne podatności i wektory ataku, pomagając organizacjom skutecznie zapobiegać, wykrywać i reagować na cyberzagrożenia.

W 94% przypadków Dragos w 2023 roku ujawniło znaczące braki w jednym lub więcej wskaźników.

Misją Dragos jest ochrona cywilizacji. Chcemy współpracować z Tobą i z Apius, aby chronić Twoje środowisko przemysłowe i infrastrukturę krytyczną, na której wszyscy polegamy.

- Platforma Dragos dostarcza najskuteczniejszą technologię ochrony cyberbezpieczeństwa przemysłowego, dając klientom wgląd w ich zasoby OT, IT i IoT, podatności urządzeń, zagrożenia oraz działania naprawcze.
- Platforma opiera się na wiedzy wywiadowczej o cyberzagrożeniach OT firmy Dragos, dogłębnych badaniach nad grupami threat activity, ransomware i narzędziami wymierzonymi w technologię operacyjną oraz infrastrukturę krytyczną.
- Nasi Threat Hunterzy, reagujący na incydenty OT i konsultanci ds. oceny proaktywnej pomagają tworzyć największy na świecie zespół ekspertów ds. cyberbezpieczeństwa OT, dostarczając kluczowe zasoby, które pomogą Ci wdrożyć technologie cybernetyczne i zmniejszyć ryzyko w OT.

The SANS ICS 5 Critical Controls

PLAN REAGOWANIA NA INCYDENTY ICS

Opracuj i utrzymuj plan reagowania na incydenty dostosowany do środowisk ICS. Plan ten powinien zawierać procedury wykrywania, reagowania na oraz odzyskiwania po incydentach cybernetycznych.

OBRONNA ARCHITEKTURA

Zaprojektuj i wdróż architekturę sieci, która segmentuje i izoluje krytyczne systemy. Ta architektura powinna minimalizować powierzchnię ataku i ograniczać potencjalny wpływ incydentu cybernetycznego.

BEZPIECZNY DOSTĘP ZDALNY

Wdróż bezpieczne rozwiązania dostępu zdalnego w celu kontrolowania i monitorowania dostępu do środowisk ICS. Obejmuje to użycie uwierzytelniania wieloskładnikowego, szyfrowanej komunikacji oraz ścisłych kontroli dostępu.

ZARZĄDZANIE PODATNOŚCIAMI W OPARCIU O RYZYKO

Przeprowadzaj regularne oceny podatności i priorytetyzuj działania naprawcze w oparciu o ryzyko dla krytycznych systemów. Obejmuje to identyfikację, ocenę i łagodzenie podatności w komponentach ICS.

WIDOCZNOŚĆ I MONITORING SIECI ICS

Ustanów ciągły monitoring sieci ICS w celu wykrywania i reagowania na anomalie oraz potencjalne zagrożenia. Obejmuje to wdrożenie narzędzi i technologii zapewniających widoczność ruchu sieciowego i aktywności systemu.

Podróż Cyberbezpieczeństwa OT (Wdrożenie, Operacjonalizacja, Optymalizacja)

Podróż Cyberbezpieczeństwa OT to etapowe podejście do wdrażania 5 Critical Controls SANS ICS (5 krytycznych punktów kontrolnych). **Składa się z trzech głównych faz:**

IMPLEMENTACJA

Ustanów podstawowe elementy dla 5-ciu krytycznych punktów kontrolnych. Ta faza koncentruje się na wprowadzeniu początkowych środków bezpieczeństwa i zapewnieniu, że podstawowe zabezpieczenia są na miejscu.

OPERACJONALIZACJA

Zintegruj wskaźniki z codziennymi operacjami. Ta faza obejmuje doskonalenie procesów, zwiększanie możliwości oraz zapewnienie skutecznego zarządzania i utrzymania kontroli.

OPTYMALIZACJA

Ciągłe doskonalenie i rozwijanie programu bezpieczeństwa. Ta faza skupia się na zaawansowanych środkach bezpieczeństwa, bieżących ocenach i dostosowywaniu się do ewoluujących zagrożeń.

Porównaj swoją dojrzałość i wyznacz kolejne kroki

Jak korzystać z tego podręcznika

Wiele firm przemysłowych docenia, że OT/ICS różni się od IT w organizacji pod względem misji, ryzyka i wpływu. Dlatego proste kopiowanie i wklejanie strategii bezpieczeństwa IT do OT będzie mało skuteczne i może być destrukcyjne. Jednak może być trudno zrozumieć, na jakie dokładnie ryzyka organizacja powinna się przygotować w kontekście cyberbezpieczeństwa przemysłowego. Ten podręcznik pomoże Ci stworzyć plan wypełnienia luk, ale najpierw musisz uzgodnić podstawy – co próbujesz chronić (Twoje zasoby, uszeregowane według krytyczności) i przed czym chronisz te systemy (scenariusze zagrożeń istotne dla Twojej branży). Gdy już uzgodnisz te podstawy, Twój Opiekun Klienta i Architekt Rozwiązań z Apius i Dragos pomogą Ci wykorzystać ten podręcznik do zidentyfikowania luk i możliwości.

Zgodność wokół priorytetów – Co próbujesz osiągnąć?

Społeczność cyberbezpieczeństwa ma wiele do nauczenia się od społeczności inżynierii bezpieczeństwa przemysłowego i może zastosować ten sam sposób myślenia o ryzykach, które staramy się niwelować. Od członka zarządu po praktyka powinna istnieć zgodność co do tego, co próbujemy razem osiągnąć. Postrzeganie ryzyka jedynie przez pryzmat jego oceny, ram i regulacji lub innych kreatywnych miar ostatecznie może stanowić utrudnienie. Celem powinny być łatwo komunikowane scenariusze na prostym do zrozumienia poziomie, gdzie każdy może zrozumieć, czy jest przygotowany na dane scenariusze, czy nie. To nie jest rozmowa o tym, jaki poziom precyzyjnych inwestycji jest wymagany – zamiast tego, jest to problem binarny. Albo jesteśmy przygotowani na scenariusz, albo nie.

Organizacje, które chcą być dobrze przygotowane na potrzeby cyberbezpieczeństwa przemysłowego, jednocześnie komunikując je w prosty sposób na wszystkich poziomach organizacji, powinny osiągnąć następujące cele:

- Zidentyfikować scenariusze oparte na danych wywiadowczych i konsekwencjach, które są istotne dla Twojej organizacji.
- Określić priorytetowe obiekty przemysłowe A, B i C.
- Sporządzić wykres obecnego postępu w ramach 5 krytycznych wskaźników i określić kolejne kroki dla każdego z priorytetowych obiektów A, B i C, korzystając z tego podręcznika.
- Uzyskać zgodność na poziomie zarządu w kwestii scenariuszy z określonymi inwestycjami w bezpieczeństwo wymaganymi do wypełnienia luk zidentyfikowanych w ćwiczeniu z podręcznika.
- Z czasem dodawać scenariusze i zwiększać ich wdrożenie w obiektach A, B i C w miarę zmieniającego się środowiska ryzyka.

Wytyczne dotyczące klasyfikacji obiektów przemysłowych

Nie wszystko w firmie jest krytyczne i warte ochrony na tym samym poziomie zasobów jak pozostałe elementy. Organizacje powinny zidentyfikować swoje priorytetowe obiekty A, B i C, wykorzystując informacje od zarządu i zespołu wykonawczego.

Rozważ następujące kwestie podczas klasyfikowania swoich priorytetowych obiektów A, B i C:

- Istniejące wewnętrzne priorytetyzacje dla obiektów lub procesów o wysokim, średnim i niskim wpływie.
- Zależności związane z przychodami lub produktywnością.
- Wpływ na zdrowie, bezpieczeństwo i środowisko
- Obiekty z planowanymi przyszłymi inwestycjami, możliwości typu "greenfield".

Organizacje powinny określić, jakie kryteria i wagi decydują o tym, jak ważny jest dany obiekt z perspektywy cyberbezpieczeństwa, a następnie zastosować tę analizę do wszystkich obiektów w całej organizacji. Na przykład firma energetyczna może ustalić, że większość ich obiektów wytwarzających jest priorytetu A wraz z niektórymi obiektami przesyłu; że niektóre obiekty przesyłu i dystrybucji są priorytetu B; oraz że niektóre obiekty wytwarzające, przesyłu i dystrybucji są obiektami priorytetu C. Naturalnym punktem wyjścia jest założenie, że 25% obiektów OT organizacji będzie zaliczać się do klasyfikacji "krytyczne" lub priorytetu A, 45% do klasyfikacji "średnie" lub priorytetu B, a 30% do obiektów klasy C. Po sklasyfikowaniu tych obiektów jesteś gotów wykorzystać ten podręcznik do zidentyfikowania swoich obecnych luk i możliwości.

Plan Reagowania na incydenty specyficzne dla OT

Miej plan reagowania na incydenty uwzględniający operacje, z naciskiem na integralność systemu i zdolności odzyskiwania podczas ataku.

ETAPY	KLUCZOWE KAMIENIE MILOWE	POSTĘP
Implementacja	☐ Opracowałeś plan reagowania na incydenty OT, korzystając ze specyficznych scenariuszy zagrożeń dla swojej branży; zorganizowałeś zasoby do reagowania (ludzi, procesy, technologie) ☐ Współpracowałeś z interesariuszami i podzieliłeś się planem w całej organizacji	☐ Wdrożono w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Wdrożono w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**
Operacjonalizacja	☐ Rozwijaj plan reagowania na incydenty na podstawie najnowszych informacji o zagrożeniach (Dragos WorldView Threat Intelligence) ☐ Przeprowadzaj ćwiczenia symulacyjne (TTX) dla wszystkich grup interesariuszy, śledząc i poprawiając wyniki, aż nie będą zgłaszane żadne większe wyzwania w kluczowych zdolnościach	☐ Operacjonalizowano w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Operacjonalizowano w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**
Optymalizacja	☐ Dodaj scenariusze oparte na konsekwencjach do swojego planu reagowania na incydenty ☐ Przeprowadzaj TTX bez większych wyzwań dla scenariuszy opartych zarówno na konsekwencjach, jak i zagrożeniach	☐ Zoptymalizowano w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Zoptymalizowano w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**

Obronna Architektura

Zaprojektuj architekturę, która wspiera widoczność, zbieranie logów, identyfikację zasobów, segmentację, przemysłowe strefy DMZ oraz kładzie nacisk na komunikację procesów.

ETAPY	KLUCZOWE KAMIENIE MILOWE	POSTĘP
Implementacja	☐ Masz dokładną, aktualną inwentaryzacje zasobów OT i diagramy sieciplementacja ☐ Ustanów polityki i procedury segmentacji dla sieci IT i OT ☐ Wdróż oprogramowanie do widoczności i monitorowania sieci ICS (Platforma Dragos)	☐ Wdrożono w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Wdrożono w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**
Operacjonalizacja	☐ Widoczność i monitorowanie sieci ICS potwierdza, że połączenia zewnętrzne są znane, kontrolowane i monitorowane ☐ Collection Management Framework (CMF) są ukończone dla najcenniejszych zasobów ☐ CMF jest skorelowany ze scenariuszami zagrożeń	☐ Operacjonalizowano w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Operacjonalizowano w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**
Optymalizacja	☐ Widoczność i monitorowanie sieci ICS stale potwierdza, że środki bezpieczeństwa pozostają skuteczne ☐ CMF jest ukończony dla wszystkich zasobów OT ☐ CMF jest zintegrowany z Twoim planem reagowania na incydenty OT	☐ Zoptymalizowano w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Zoptymalizowano w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**

Widoczność i monitorowanie sieci ICS

Umożliwiaj ciągłe monitorowanie bezpieczeństwa sieci w środowisku ICS przy użyciu narzędzi świadomych protokołów oraz możliwości analizy interakcji systemów.

ETAPY	KLUCZOWE KAMIENIE MILOWE	POSTĘP
Implementacja	☐ Wdrożyłeś oprogramowanie do widoczności i monitorowania sieci ICS w obiektach wysokiego ryzyka ☐ Widoczność i monitorowanie sieci ICS obejmuje: • Czujniki po stronie OT na granicy IT/OT (L3/3.5) • Czujniki do monitorowania ruchu E-W przy najcenniejszych zasobach i powiązanych procesach (L1-L2)	☐ Wdrożono w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Wdrożono w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**
Operacjonalizacja	☐ Widoczność i monitorowanie sieci ICS spełniają wymagania widoczności zidentyfikowane w Twoim planie reagowania na incydenty ☐ Personel OT posiada umiejętności i wiedzę, aby wykonywać następujące zadania: • weryfikacja inwentaryzacji zasobów • zarządzanie detekcją • klasyfikacja i badanie incydentów • łagodzenie krytycznych i wysokiej pewności podatności (podatności typu "NOW" na Platformie Dragos) • monitorowanie zdalnych sesji dostępu stron trzecich ☐ Zintegruj krytyczne alerty z istniejącym systemem SIEM, aby były widoczne dla zespołu operacyjnego cyberbezpieczeństwa	☐ Operacjonalizowano w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Operacjonalizowano w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**
Optymalizacja	☐ Widoczność została rozszerzona na całą sieć OT w obiektach wysokiego ryzyka ☐ Logowanie jest scentralizowane i zautomatyzowane ☐ Personel ds. bezpieczeństwa posiada umiejętności i wiedzę do realizacji zaawansowanych przypadków użycia, w tym: • poszukiwanie zagrożeń • weryfikacja środków bezpieczeństwa • obsługa "następnych" podatności	☐ Zoptymalizowano w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Zoptymalizowano w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**

Bezpieczny Zdalny Dostęp

Zidentyfikuj wszystkie punkty zdalnego dostępu i dozwolone środowiska docelowe oraz wdróż dostęp na żądanie i uwierzytelnianie wieloskładnikowe (MFA) tam, gdzie to możliwe.

ETAPY	KLUCZOWE KAMIENIE MILOWE	POSTĘP
Implementacja	☐ Wszystkie połączenia zewnętrzne są udokumentowane i monitorowane ☐ Uwierzytelnianie wieloskładnikowe zostało wdrożone pomiędzy sieciami IT i OT	☐ Wdrożono w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Wdrożono w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**
Operacjonalizacja	☐ Połączenia zewnętrzne są ograniczone czasowo, regionalnie, itp. ☐ Połączenia zewnętrzne mogą być szybko rozłączone bez wpływu na OT ☐ Wszystkie połączenia zewnętrzne są kierowane przez punkty kontrolne, takie jak jump-hosty, z wzmożonym monitoringiem	☐ Operacjonalizowano w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Operacjonalizowano w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**
Optymalizacja	☐ Połączenia zdalne są domyślnie wyłączone, włączane tylko na żądanie ☐ Bezpieczne połączenia zdalne i dostawcy są ograniczeni i zredukowani do minimum, zgodnie z potrzebami biznesowymi	☐ Zoptymalizowano w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Zoptymalizowano w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**

Zarządzanie podatnościami oparte na ryzyku

Zrozum cyfrowe wskaźniki cybernetyczne oraz warunki pracy urządzeń, aby podejmować decyzje dotyczące zarządzania podatnościami w środowisku OT w oparciu o ryzyko.

ETAPY	KLUCZOWE KAMIENIE MILOWE	POSTĘP
Implementacja	☐ Opracuj powtarzalny, skalowalny proces mapowania podatności na zasoby ☐ Priorytetyzuj podatności z uwzględnieniem ryzyka istotnego dla OT ☐ Wszelkie CVE w ścieżce ataku (np. ransomware lub PIPEDREAM) oraz CVE związane z aktywnymi exploitami są odpowiednio łagodzone	☐ Wdrożono w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Wdrożono w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**
Operacjonalizacja	☐ Najcenniejsze zasoby i ich podatności są śledzone, monitorowane i aktualizowane ☐ Działania związane z podatnościami OT są zintegrowane z istniejącym systemem zarządzania usługami	☐ Operacjonalizowano w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Operacjonalizowano w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**
Optymalizacja	☐ Śledź, monitoruj i aktualizuj wszystkie zasoby OT i ich podatności	☐ Zoptymalizowano w _____ z _____ krytycznych (lub Klasy A) obiektów ☐ Zoptymalizowano w _____ z _____ średnich (lub Klasy B) obiektów **Pozostałe obiekty i uwagi:**