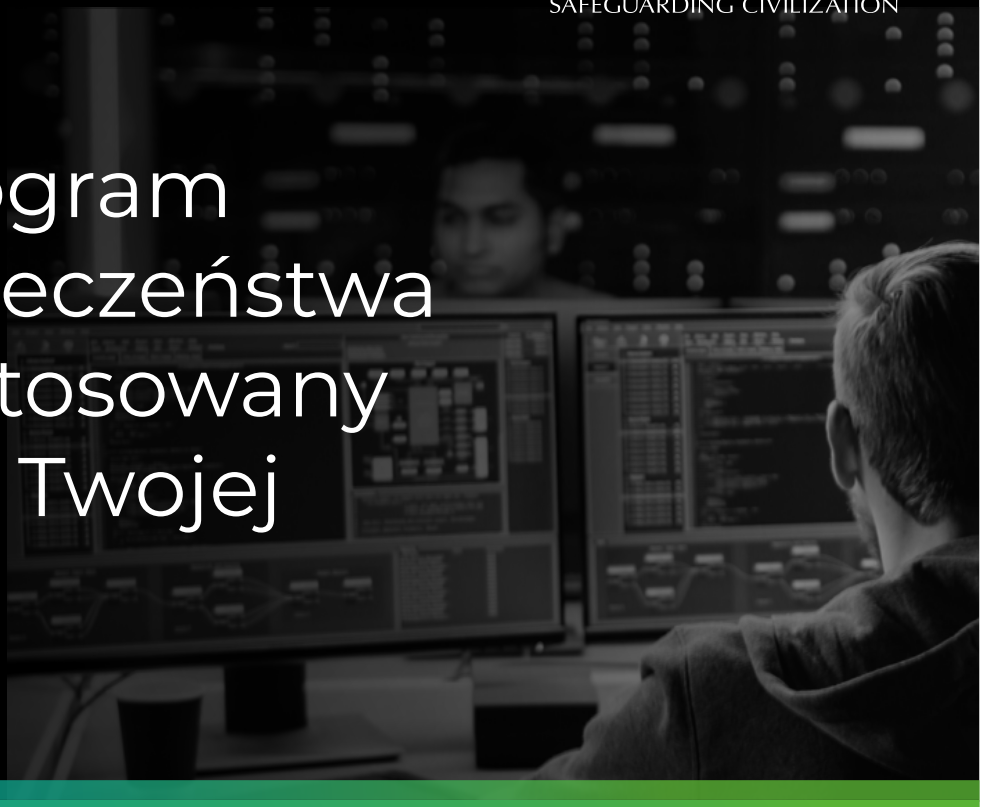
apius TECHNOLOGIES

DRAGOS SAFEGUARDING CIVILIZATION

# Zbuduj program cyberbezpieczeństwa ICS/OT dostosowany do potrzeb Twojej organizacji



## Nasz zespół ds. usług profesjonalnych pomoże Ci zacząć

Niezależnie od tego, czy dopiero zaczynasz tworzyć program cyberbezpieczeństwa technologii operacyjnej (OT), czy chcesz zoptymalizować już istniejący, mamy dla Ciebie strategiczne usługi, które pomogą Ci ocenić Twoje możliwości i wzmocnić Twoją pozycję w obszarze bezpieczeństwa. Wykorzystaj nasze doświadczenie, by poznać najlepsze praktyki w zakresie ochrony przed zagrożeniami ukierunkowanymi na unikalne systemy, ruch sieciowy i luki występujące w środowisku OT.

## Współpracuj z najbardziej doświadczonym zespołem ekspertów ICS/OT

To żaden sekret, że nasz zespół jest największym atutem firmy Dragos. Nasi specjaliści od systemów sterowania przemysłowego (ICS) stoją na pierwszej linii obrony podczas największych, globalnych ataków na cyberbezpieczeństwo przemysłowe i cieszą się wysokim uznaniem w branży. Wesprzemy Cię, abyś mógł zoptymalizować obecne zasoby i zbudować program cyberbezpieczeństwa OT najlepiej dopasowany do Twoich potrzeb. Dzięki dogłębnej znajomości sektora i ekspertyzie w obszarze OT nasz zespół usługowy jest godnym zaufania doradcą w obliczu ciągle ewoluującego krajobrazu zagrożeń i pomoże Ci skutecznie wygrać walkę z nimi.

# Potrzebujesz programu cyberbezpieczeństwa OT. Od czego zacząć?

## Zadbaj o proaktywne zabezpieczenie środowiska OT, korzystając z naszego Rapid Response Retainer.

Stawka w środowiskach OT jest znacznie wyższa niż w IT – chodzi tu o zagrożenia dla ludzkiego życia, infrastruktury, operacji i bezpieczeństwa środowiskowego. Umowa na usługi natychmiastowego reagowania (ICS Incident Response – IR) stanowi fundament do budowy i optymalizacji mechanizmów bezpieczeństwa w Twoim środowisku OT. Biorąc pod uwagę zróżnicowanie urządzeń, protokołów komunikacyjnych oraz przeciwników, wpływ incydentu OT różni się w zależności od branży i wymaga strategii uwzględniającej unikalne ryzyka. Grupy cyberprzestępcze stale poszukują podatnych elementów, dlatego kluczowe jest nieustanne ocenianie i rozwijanie możliwości obronnych oraz ulepszanie planu reagowania na incydenty. Dostosowanie koncepcji bezpieczeństwa ICS/OT do realiów Twojego środowiska jest kluczowe, by zbudować odporność cybernetyczną wymaganą przez infrastrukturę przemysłową.

### KORZYŚCI Z RAPID RESPONSE RETAINER

- SPECJALIŚCI Z DOŚWIADCZENIEM W ZAKRESIE ZARZĄDZANIA KRYZYSOWEGO W OT
- GWARANTOWANY CZAS REAKCJI (SLA) DLA KLIENTÓW KORZYSTAJĄCYCH Z DRAGOS PLATFORM W PRZYPADKU WYSTĄPIENIA INCYDENTU
- EKSPERCI Z DOŚWIADCZENIEM W INWESTYGACJI W TWOICH SYSTEMACH PRZEMYSŁOWYCH
- ELASTYCZNE GODZINY, KTÓRE MOŻESZ WYKORZYSTAĆ NA INNE USŁUGI

## Szybka reakcja dzięki Dragos Platform

Subskrypcja Dragos Platform nie jest wymagana do zakupu Rapid Response Retainer, ale wysoce ją rekomendujemy. Dragos Platform zapewnia wgląd w środowisko – inwentaryzację zasobów OT, analizę ruchu sieciowego i informacje o lukach, co zwiększa dokładność i pozwala lepiej zrozumieć urządzenia w Twojej infrastrukturze.

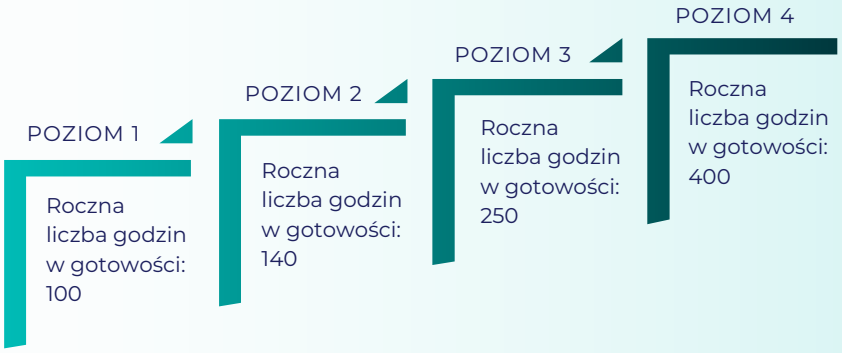
## Dlaczego Dragos Platform?

Platforma Dragos jest wyposażona w celu wsparcia procesów reagowania na incydenty, dostarczając wywiad o zagrożeniach OT od jednego z czołowych zespołów badawczych w branży.

**Platforma to kulminacja naszej wiedzy o OT, wdrożona w formie kodu i skalowalna w tempie maszynowym.**

# Gwarantowany czas reakcji

Klienci Rapid Response Retainer korzystają ze skróconego czasu reakcji. Każdy poziom gotowości (retainer) ma wbudowaną Umowę o Poziomie Usługi (SLA), która gwarantuje rejestrację incydentu w ciągu 1 godziny i gotowość specjalisty w ciągu 48 godzin.




Wszyscy klienci z Rapid Response Retainer korzystają z obniżonego współczynnika zużycia godzin (0,75x) przy użyciu Dragos Platform

Dragos Platform zapewnia narzędzia do trybu triage i prowadzenia śledztw związanych z potencjalnymi incydentami, oferując scentralizowane rejestry danych kryminalistycznych, warsztat śledczy (investigation workbench) oraz szczegółowe widoki chronologiczne. Przekłada się to na szybszą reakcję, mniejsze zużycie godzin gotowości i wykracza poza jednorazową ocenę; dostarcza kluczowe informacje o zasięgu ataku i zaatakowanych urządzeniach.

## Wykorzystaj maksymalnie wartość gotowości dzięki dodatkowym usługom

Każdy Rapid Response Retainer rozpoczyna się od Retainer Readiness Onboarding Workshop – warsztat ten zawiera omówienie zakresu umowy, sposobu jej aktywacji, możliwych scenariuszy po jej uruchomieniu (w tym próbne połączenie z gorącą linią reakcji na incydenty czyli hotline IR) i wielu innych. Klienci otrzymują kwartalne raporty o wykorzystanych godzinach, a wszystkie pozostałe godziny można spożytkować na inną usługę Dragos. Skontaktuj się z opiekunem handlowym Apius, aby dowiedzieć się, które usługi najlepiej pasują do pozostałych godzin.

# Ćwiczenia typu Tabletop

## Przetestuj swój plan reagowania na rzeczywisty cyberatak

Lepiej zrozum mocne i słabe strony reagowania na incydenty w Twojej organizacji, trenując scenariusze obrazujące, jak w praktyce mógłby wyglądać atak na Twoje środowisko przemysłowe. Oferujemy gotowe scenariusze idealne do ćwiczeń zespołu reagowania na incydenty lub przygotowujemy scenariusze dostosowane do pracy wielu działów w organizacji.

# Pakiet usług oceny cyberbezpieczeństwa OT

## Poznaj swoje najważniejsze systemy

Zrozumienie, które systemy ICS są najbardziej kluczowe i jaka może być skala skutków cyberataku na nie, jest niezbędne do ustalania priorytetów w obszarze zabezpieczeń, detekcji i reagowania.

### OCENA ZAGROŻEŃ

Wykorzystując Dragos Platform do zdalnej inspekcji próbek ruchu w sieci OT, szukamy poszlak wskazujących na istniejące lub wcześniejsze naruszenie bezpieczeństwa.

### PRZEGLĄD ARCHITEKTURY CYBERBEZPIECZEŃSTWA OT

Otrzymaj strategiczne rekomendacje dotyczące łagodzenia luk w zabezpieczeniach OT związanych z projektem sieci, konfiguracją oraz połączeniami z systemami wewnętrznymi i zewnętrznymi.

### OCENA CYBERBEZPIECZEŃSTWA OT

Kompleksowa ocena obejmująca techniczną analizę sieci OT, a także przegląd kluczowych osób i procesów wpływających na bezpieczeństwo OT w Twojej organizacji.

| CELE | OCENA ZAGROŻEŃ | PRZEGLĄD ARCHITEKTURY CYBER-BEZPIECZEŃSTWA OT | OCENA CYBER -BEZPIECZEŃSTWA OT |
|---|---|---|---|
| Przegląd programu | | | ✓ |
| Ramowy model zarządzania zbieraniem danych | | | ✓ |
| Analiza kluczowych zasobów | | | ✓ |
| Przegląd topologii | | ✓ | ✓ |
| Przegląd standardów i regulacji* | | ✓ | ✓ |
| Przeszukiwanie wskaźników naruszenia bezpieczeństwa | ✓ | ✓ | ✓ |
| Wykrywanie zagrożeń | ✓ | ✓ | ✓ |
| Inwentaryzacja zasobów | ✓ | ✓ | ✓ |
| Ocena podatności zasobów | ✓ | ✓ | ✓ |

* Standards and Regulations Review obejmuje TSA SD-2, NIST-CSF, NERC-CIP, IEC 62443, KSA NCA ITCC oraz australijskie regulacje SLACIP/SOCIP. Każda OT Architecture Review jest unikalna, skontaktuj się z nami pod adresem sales@apius.pl, aby omówić dostosowanie przeglądu do Twoich potrzeb.

## Popraw swoje bezpieczeństwo

- Zidentyfikuj zasoby OT, luki w zabezpieczeniach i ewentualne naruszenia.
- Uzyskaj informacje ułatwiające raportowanie zgodności z regulacjami.
- Zrozum swoje kluczowe zasoby i oceń dojrzałość programu cyberbezpieczeństwa OT.
- Otrzymaj zarówno taktyczne, jak i strategiczne rekomendacje wzmacniające obronę ICS.

# Oceny podatności (Vulnerability Assessments)

## Uzyskaj wgląd w możliwe ścieżki ataków w Twoim środowisku OT

- Wyszukaj słabe punkty i nieprawidłowe konfiguracje w sieci OT, hostach, urządzeniach polowych i aplikacjach.
- Zidentyfikuj scenariusze ukazujące możliwe wektory ataku i sposoby na ulepszenie struktury bezpieczeństwa.
- Połącz wyniki z taktykami, technikami i procedurami realnych przeciwników.
- Skorzystaj z wywiadu o zagrożeniach (intel-driven) w celu prześledzenia aktywności grup atakujących

## Przykładowe wyniki z oceny podatności (Vulnerability Assessment Sample Findings)

Poniższa tabela prezentuje przykładowe znaleziska z raportu (After Action Report) po wykonaniu Oceny Podatności. Pozwala ona klientom priorytetyzować zarządzanie podatnościami według poziomu istotności.

| ID | TYTUŁ PODATNOŚCI | OPIS | WAGA |
|---|---|---|---|
| 1 | Zasoby ICS/OT skonfigurowane z dostępem do Internetu | Dragos wykrył kilka stacji/serwerów ICS/OT bezpośrednio łączących się z Internetem. Urządzenia ICS/OT nie powinny komunikować się z siecią internetową bezpośrednio – komunikacja powinna następować poprzez proxy lub serwer pośredniczący w wzmocnionej strefie DMZ. | C |
| 2 | Zidentyfikowano ponowne użycie haseł | Dragos zidentyfikował sytuację, w której konta administratora w środowisku systemu sterowania procesami używają identycznych haseł na wielu maszynach, co znacznie poszerza powierzchnię ataku. | H |
| 3 | Uprzywilejowane konta ICS/OT zalogowane w interfejsach HMI | Dragos zarejestrował przypadki korzystania z uprzywilejowanych kont użytkowników w stacjach operatorskich HMI. Te konta zapewniają dostęp do obszarów zakładu wykraczających poza podstawowy zakres pracy operatora. | M |
| 4 | Luki w zabezpieczeniach sterowników PLC od dostawcy | Dragos Platform wykryła luki w zabezpieczeniach sterowników PLC należących do pewnego dostawcy. Mogą one bezpośrednio wpłynąć na działanie oraz kontrolę maszyn produkcyjnych. | L |

Legenda w kolumnie „Waga” może oznaczać: C (Critical), H (High), M (Medium), L (Low) – lub dowolne inne stopniowanie zdefiniowane w raporcie.

# Testy penetracyjne (Penetration Tests)

## Oceń podatności, które mogą zostać wykorzystane w Twoim środowisku

Wykorzystując moc Dragos Platform, testy penetracyjne dostarczają szczegółowych informacji o sieciach i strefach OT podatnych na skanowanie, aby móc ocenić rzeczywiste zagrożenia w Twoim środowisku OT.

### SIEĆ

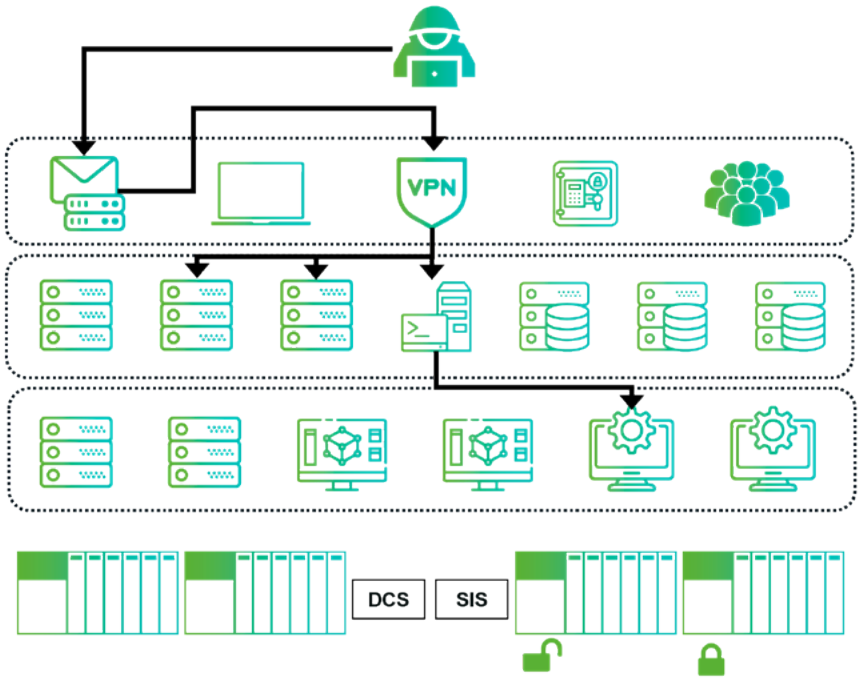
- Próby przełamania systemu i eskalacji uprawnień.
- Wykorzystanie dostępu w celu przemieszczenia się (pivot) w obrębie sieci.

### URZĄDZENIA

- Identyfikacja powierzchni ataku urządzeń.
- Weryfikacja skuteczności zastosowanych środków bezpieczeństwa.

### APLIKACJE

- Wyszukiwanie luk w sprzęcie i oprogramowaniu.
- Rekomendacje ekspertów wzmacniające bezpieczeństwo całościowe.




Poniżej przykład symulacji tzw. „assumed breach", obrazującej taktyki, techniki i procedury przeciwnika służące do uzyskania dostępu do sieci.

# Threat Hunts

## Wykrywaj, ujawniaj i powstrzymuj luki oraz zagrożenia w środowisku OT

Odkryj nieznane wcześniej zagrożenia w swojej sieci ICS i zidentyfikuj słabości w architekturze, mechanizmach bezpieczeństwa oraz procedurach, aby uniknąć naruszeń. Nasze polowania na zagrożenia (threat hunts) są realizowane nieinwazyjnie, bez zakłócania procesów operacyjnych i przestojów, z wykorzystaniem Dragos Platform do analiz kryminalistycznych.


# Dragos OT Watch

## – ZARZĄDZANE POLOWANIA NA ZAGROŻENIA

### Zaufany partner dla Twoich operacji bezpieczeństwa

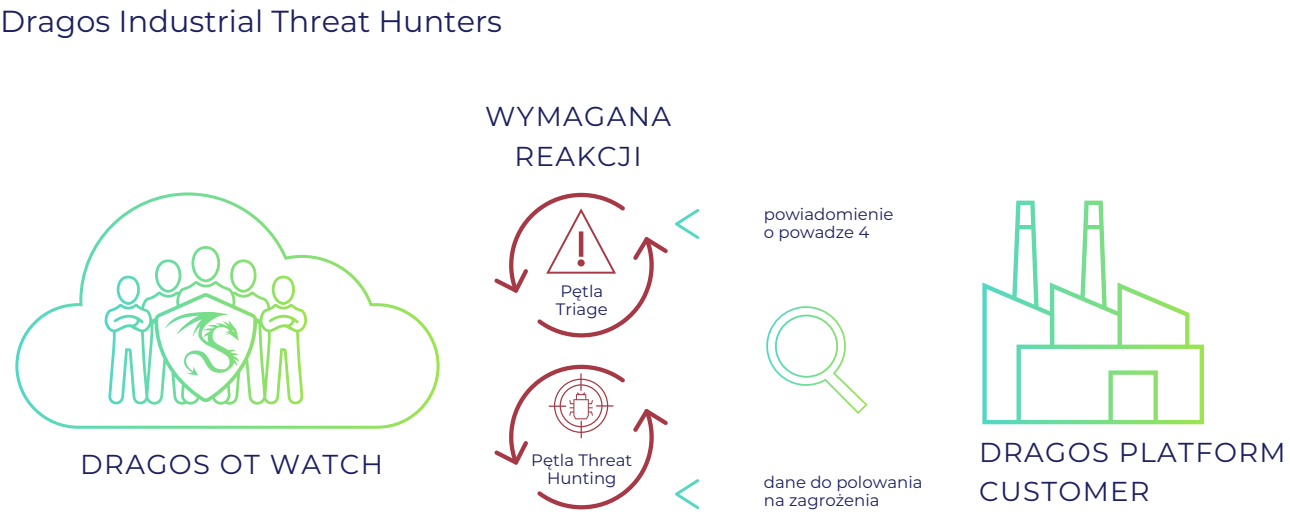
Dostępna wyłącznie dla klientów Dragos Platform, subskrypcja OT Watch zapewnia Ci elitarny zespół specjalistów od Threat Huntingu w środowiskach przemysłowych. Mogą oni przejąć obsługę Dragos Platform w Twoim imieniu i zająć się codziennymi operacjami bezpieczeństwa lub skupić się w całości na Threat Huntingu, integrując się z już istniejącymi procesami cyberbezpieczeństwa OT. W ramach OT Watch nasz zespół staje się częścią Twojego zespołu.

## Co zyskujesz dzięki OT Watch

- Proaktywne polowania na zagrożenia wsparte wywiadem Dragos Threat Intelligence.
- Priorytetyzację i wstępną analizę powiadomień wraz z informacją o potencjalnych skutkach i rekomendacjami dalszych kroków.
- Mniejsze ryzyko długotrwałego pozostawania atakujących w ukryciu, co mogłoby zagrażać ciągłości biznesu i bezpieczeństwu operacji.

**Dostępne wyłącznie dla klientów Dragos Platform.**

## Jak działa OT Watch




# Zapraszamy do współpracy.

Jesteśmy w TOP 3 rankingu dostawców rozwiązań cyberbezpieczeństwa w 2023!

COMPUTERWORLD TOP200

Skontaktuj się z nami w celu przeprowadzenia demonstracji systemów cyberbezpieczeństwa w naszej lub Twojej infrastrukturze!

www.apius.pl

sales@apius.pl