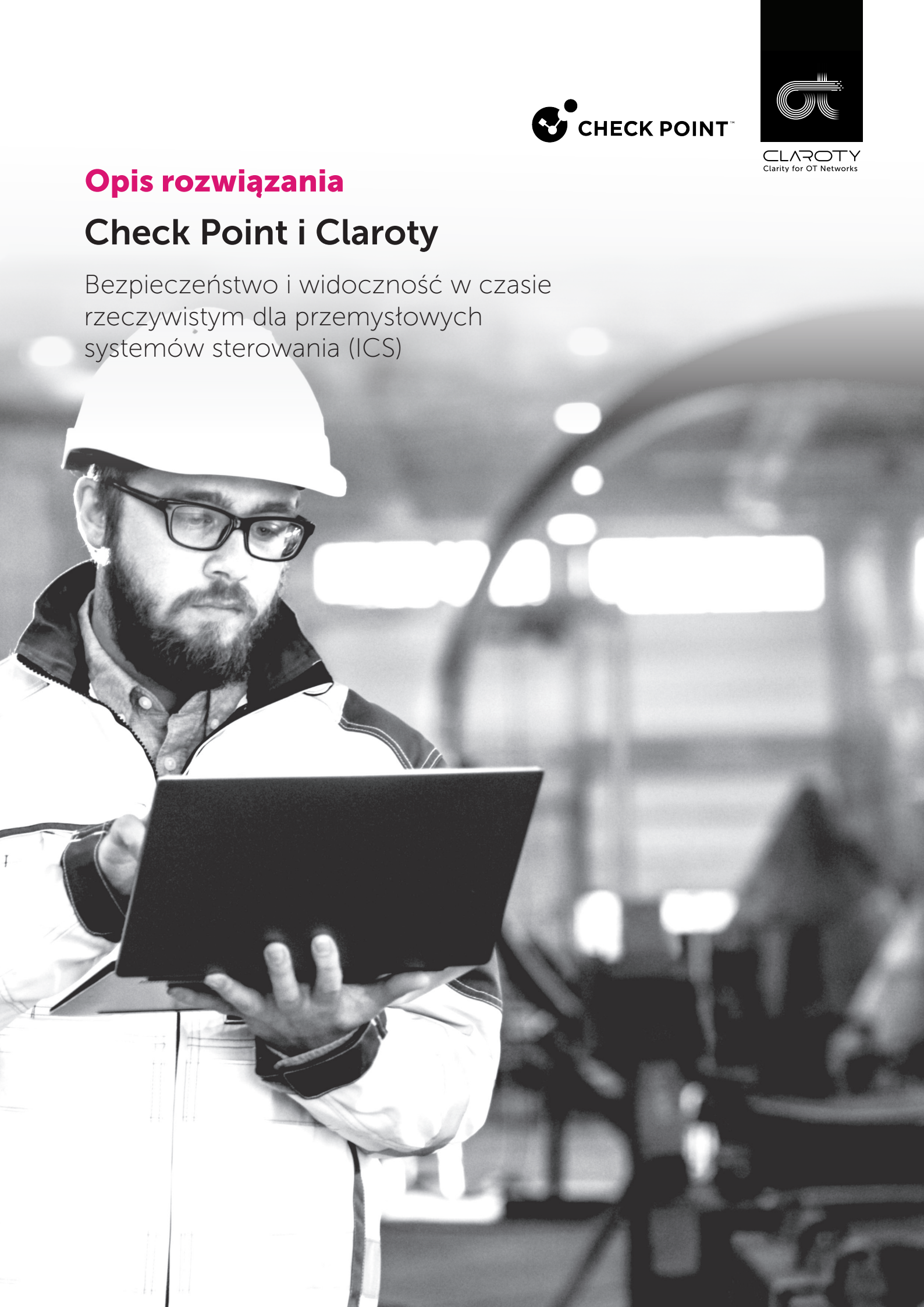
CHECK POINT™

CLAROTY
Clarity for OT Networks

Opis rozwiązania

Check Point i Claroty

Bezpieczeństwo i widoczność w czasie rzeczywistym dla przemysłowych systemów sterowania (ICS)



Check Point i Claroty – bezpieczeństwo i widoczność w czasie rzeczywistym dla przemysłowych systemów sterowania (ICS)

Najważniejsze cechy rozwiązania

- **Znakomita widoczność** sieci przemysłowych systemów sterowania umożliwia ocenę, monitorowanie i neutralizowanie potencjalnych zagrożeń dla infrastruktury krytycznej.
- **Usprawnione wykrywanie zagrożeń** dzięki kontekstowemu powiadamianiu w czasie rzeczywistym, co zwiększa integralność procesów i odporność na ataki.
- **Zerowy wpływ na przemysłowe sieci sterowania** – nieinwazyjny sposób działania, bez instalacji agentów na punktach końcowych oraz bez przestojów i zakłóceń w pracy sieci przemysłowych.

Czynniki biznesowe

Choć przedsiębiorstwa poczyniły znaczne postępy w zakresie ochrony swoich biznesowych sieci IT, sieci przemysłowych systemów sterowania (ICS) wciąż są zagrożone. Wiele z tych sieci i związanych z nimi zasobów zostało uruchomionych dziesiątki lat temu bez uwzględnienia cyberbezpieczeństwa i niekiedy opierało się na przestarzałym oprogramowaniu. Coraz częściej stają się one celem wyrafinowanych ataków cybernetycznych. Wiele udokumentowanych ataków, takich jak Industroyer CrashOverride, WannaCry, BlackEnergy i STUXNET, spowodowało znaczące szkody operacyjne, zakłócając zarówno bezpieczeństwo środowiska, jak i ludzi.

Jak dotąd uzyskiwanie w czasie rzeczywistym pełnego wglądu w sieci ICS, wykorzystywane protokoły i urządzenia specyficzne dla niektórych procesów było niezwykle trudne, przez co przedsiębiorstwa przemysłowe w dużej mierze nie otrzymywały żadnych informacji o potencjalnych zagrożeniach. Bez kontekstowego wglądu operacje przemysłowe nie były w stanie chronić sieci sterowania przed cyberatakami i zapobiegać zakłóceniom w produkcji.

Zintegrowany, kompleksowy system bezpieczeństwa

Zintegrowane rozwiązania Check Point i Claroty dodają funkcję wykrywania włamań do systemów ICS oraz pasywnego monitorowania sieci OT w ramach kompleksowego pakietu zabezpieczeń firmy Check Point. Rozwiązania sieciowe Check Point Security, takie jak urządzenia serii 15xxx w szczególności przemysłowy wzmacniany 1570R, zabezpieczają brzeg sieci, połączenia IT z OT oraz strefy w ramach sieci przemysłowych.

Rozwiązanie Claroty z funkcją nieprzerwanego wykrywania zagrożeń (ang. Continuous Threat Detection, CTD) podłączamy do portu SPAN lub Mirror w standardowych rozwiązaniach Check Point Security Gateway lub Check Point Rugged Security Appliance, które automatycznie wykrywają zasoby w sieci przemysłowej i monitorują połączenia sieciowe, aby zapewnić wykrywanie anomalii i zagrożeń w czasie rzeczywistym oraz generowanie alertów dotyczących integralności procesów. Zagregowane alerty są przekazywane bezpośrednio do konsoli Check Point Smart Management Console.

Dzięki ujednoliconemu raportowaniu oraz szczegółowemu wglądowi w ruch SCADA przedsiębiorstwa mogą wykryć każde zagrożenie dla aplikacji, procesu lub sieci. Ponadto ułatwia ono ewentualną późniejszą analizę przeprowadzonego ataku. Zintegrowana analiza sieci i punktów końcowych pokazuje całą sekwencję zdarzeń poprzedzającą atak, co zapewnia pełny wgląd w sieci korporacyjne i sieci sterowania.

Komponenty architektury

Platforma Claroty jest w pełni zintegrowanym rozwiązaniem, które podłącza się do sieci bez użycia agentów. Została ona zaprojektowana w celu zwiększenia świadomości dot. zdarzeń w sieci w czasie rzeczywistym oraz szczegółowej widoczności sieci ICS. Wielowarstwowy model wdrożenia umożliwia monitorowanie środowisk z wieloma przełącznikami i wieloma topologiami sieci. Rozwiązanie jest szybkie i łatwe we wdrożeniu oraz nie ma żadnego wpływu na sieć czy integralność procesów przemysłowych. Claroty wykorzystuje następujące elementy w ramach instalacji:

Serwer CTD (Continuous Threat Detection) jest fizycznym lub wirtualnym serwerem, który w czasie rzeczywistym zapewnia cyberbezpieczeństwo i widoczność operacyjną przemysłowych sieci sterowania w rozproszonych środowiskach i architekturach sieciowych.

Check Point i Claroty – bezpieczeństwo i widoczność w czasie rzeczywistym dla przemysłowych systemów sterowania (ICS)

Sensor serwera CTD
Wysunięty sensor analizy CTD, zdalne rozszerzenie serwera CTD. Używany w lokalizacjach o ograniczonym dostępie fizycznym lub w wielu odległych, odizolowanych ośrodkach o ograniczonych możliwościach agregacji z siecią Out-of-band.

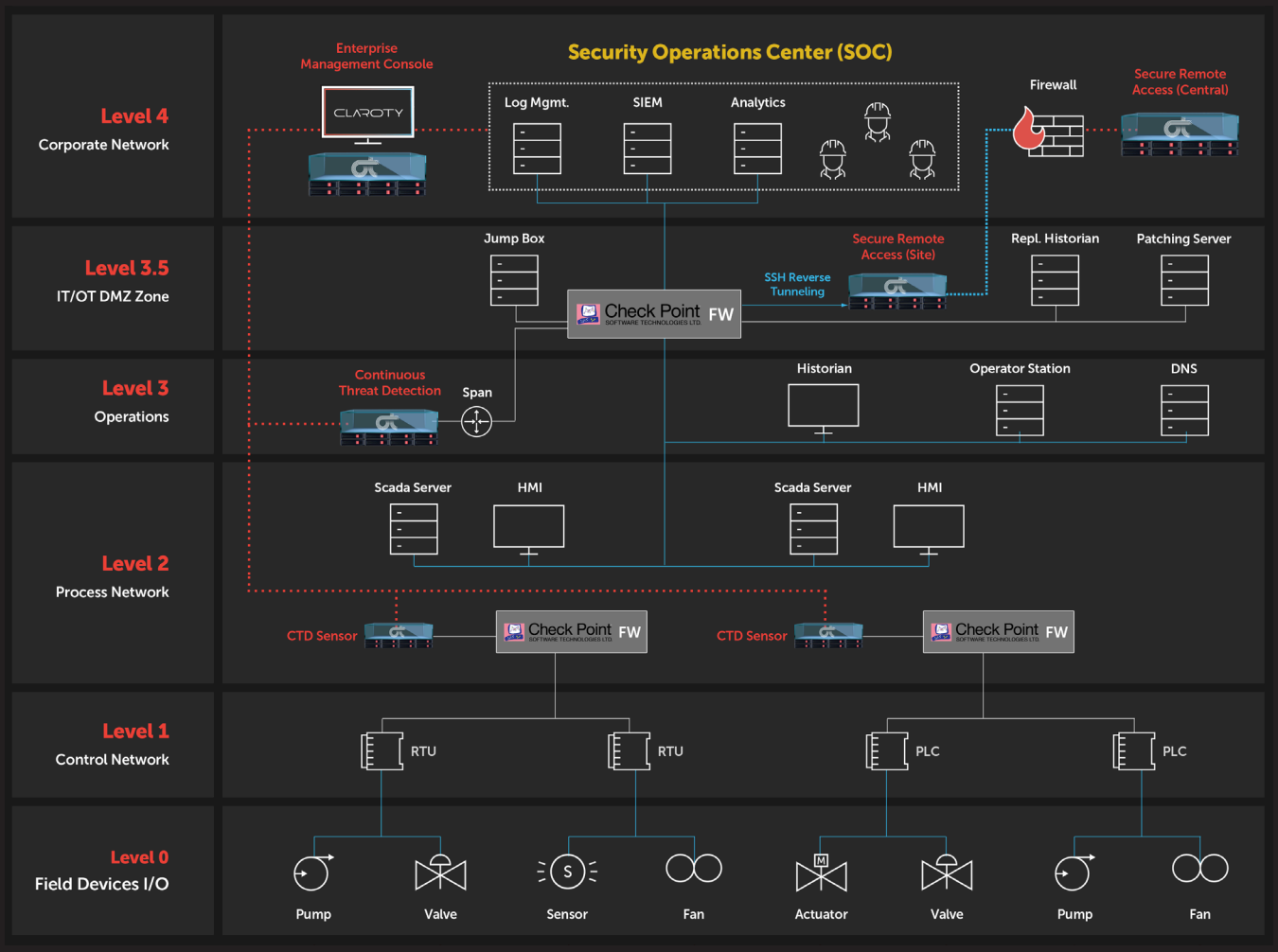
Bezpieczny dostęp zdalny – minimalizacja ryzyka, jakie stanowią dla sieci OT zdalni użytkownicy, w tym pracownicy i osoby trzecie, za pomocą w pełni zarządzalnego interfejsu, przez który łączą się wszyscy użytkownicy zewnętrzni.

Ma to na celu przeprowadzanie aktualizacji oprogramowania, okresowych konserwacji i innych czynności supportowych na zasobach w sieciach przemysłowych.

EMC (Enterprise Management Console) – ujednolicona konsola, agregująca i konsolidująca dane z różnych produktów Claroty. Scentralizowany interfejs zarządzania wyświetla ujednolicony widok zasobów, zdarzeń i alertów, co czyni go idealnym rozwiązaniem dla zespołów SOC w obrębie całego przedsiębiorstwa.

Przykładowa architektura wdrożenia

Poniższy rysunek przedstawia integrację zapory sieciowej Check Point i rozwiązań Claroty w konwergentnych środowiskach IT i OT, w oparciu o architekturę modelu Purdue. W tym scenariuszu system ciągłego wykrywania zagrożeń Claroty analizuje ruch przychodzący i wychodzący, podczas gdy zapory sieciowe Check Point są umieszczane w strategicznych punktach wykrywania i zapobiegania. Umożliwia to blokowanie lub ograniczanie komunikacji dla pojedynczego węzła lub pomiędzy węzłami, aby skutecznie zapobiegać zakłóceniom operacji o znaczeniu krytycznym.



Rys. 1 – CTD dostarcza szczegółowe informacje dotyczące zasobów OT do zapory sieciowej Check Point

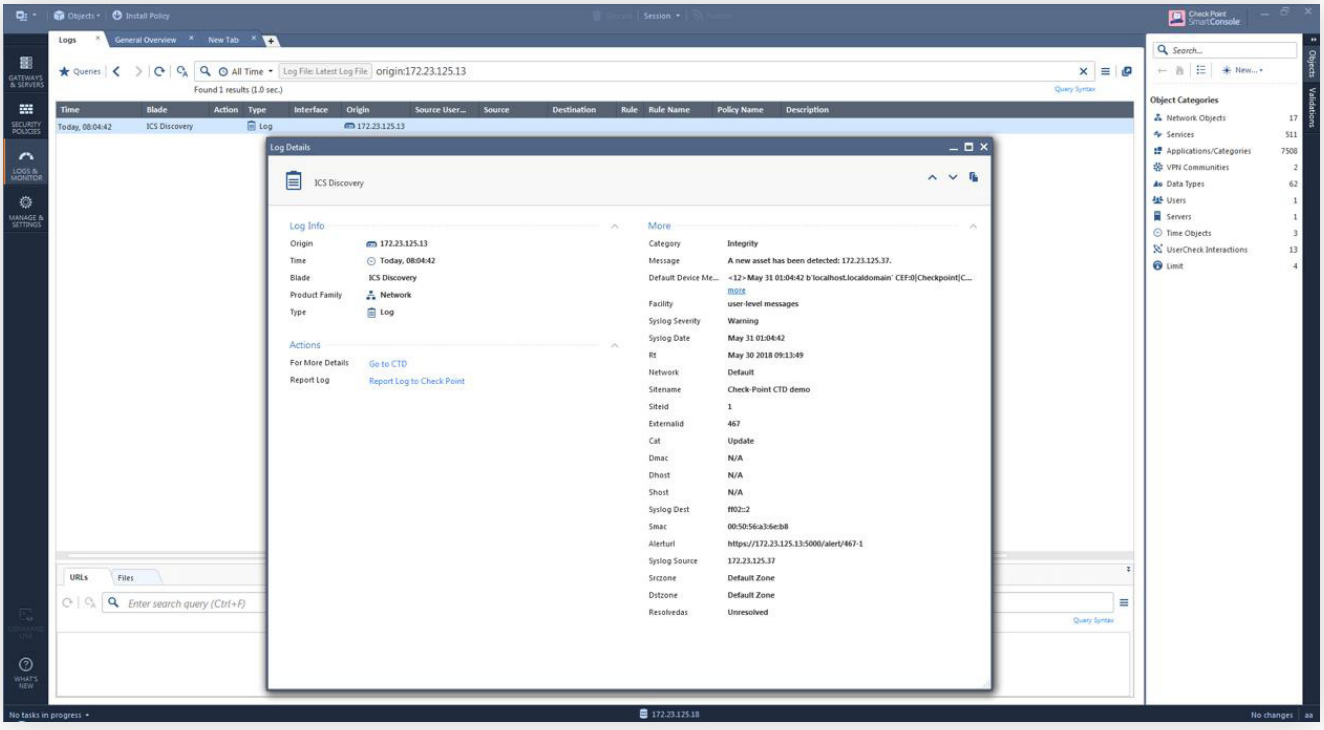
Check Point i Claroty – bezpieczeństwo i widoczność w czasie rzeczywistym dla przemysłowych systemów sterowania (ICS)

Bezpieczeństwo i widoczność w czasie rzeczywistym

Rozwiązanie Claroty jest dostępne w różnych formach, obsługujących szeroki zakres przemysłowych systemów sterowania i protokołów[1] oraz łatwo integruje się z istniejącymi aplikacjami IT/OT. Rozwiązuje ono w znacznym stopniu problem bezpieczeństwa przemysłowych sieci sterowania dzięki kompleksowemu zabezpieczeniu i widoczności w czasie rzeczywistym. Wszystko to jest osiągalne przy zerowym wpływie na procesy produkcyjne i zasoby firmowe.

Poniżej przedstawiono kilka unikalnych funkcjonalności zintegrowanych w konsoli Check Point Management Console:

- Doskonała widoczność przemysłowych systemów sterowania (ICS)
- Identyfikowanie luk w zabezpieczeniach – w tym znanych podatności i problemów związanych z działaniem sieci
- Wykrywanie zmian w profilu zabezpieczeń
- Stałe monitorowanie w poszukiwaniu znanych i nieznanych zagrożeń
- Proaktywne wykrywanie zagrożeń



Rys. 2 – Alerty CTD widoczne w konsoli Check Point Smart Management Console

[1] Lista zawiera najczęściej używane protokoły. Pełna lista obsługiwanych protokołów znajduje się tutaj: https://www.claroty.com/protocol.pdf. Claroty będzie oferować wsparcie dla dodatkowych protokołów zgodnie z zapotrzebowaniem klientów. Skontaktuj się z nami, aby dowiedzieć się więcej.

Check Point i Claroty – bezpieczeństwo i widoczność w czasie rzeczywistym dla przemysłowych systemów sterowania (ICS)

Typowe zastosowania

Ujednolicone spojrzenie na IT-OT

Zapory sieciowe Check Point są umieszczane w strategicznych punktach wykrywania i zapobiegania, natomiast rozwiązanie Claroty automatycznie identyfikuje i klasyfikuje zasoby w całej sieci ICS. Łącznie rozwiązania te zapewniają skonsolidowany widok zasobów w środowiskach IT i OT. Stale aktualizują zasoby oraz zapewniają dokładne i aktualne właściwości urządzeń, ich klasyfikację, konfigurację i kontekst sieciowy z jednego repozytorium. Dodatkowo Claroty umożliwia proaktywne blokowanie lub ograniczanie komunikacji dla pojedynczego węzła lub pomiędzy węzłami, aby skutecznie zapobiegać zakłóceniom operacji o znaczeniu krytycznym.

Wykrywanie zagrożeń OT w czasie rzeczywistym

Claroty pomaga administratorom identyfikować i naprawiać problemy, które mogą mieć wpływ na bezpieczeństwo, takie jak podatności, błędna konfiguracja sieci, hasła przesyłane czystym tekstem, niezabezpieczone połączenia i wiele innych. Dzięki generowaniu i udostępnianiu kontekstowych alertów przez zaporę sieciową Check Point zespoły SOC i bezpieczeństwa natychmiast dowiadują się o zdarzeniu i uzyskują szczegółowe informacje niezbędne do szybkiego zbadania problemu oraz podjęcia współpracy z zespołami produkcyjnymi w celu jego rozwiązania.

Potrzeba segmentacji sieci

Potrzeba proaktywnej segmentacji pomiędzy sieciami IT i OT, jak również w obrębie środowiska sieci OT (mikrosegmentacja, strefy itp.), aby zapobiec przypadkowemu przenikaniu z korporacyjnej sieci IT do sieci OT.

Ścisła integracja między rozwiązaniem CTD Claroty a rozwiązaniami Check Point wykorzystuje istniejącą infrastrukturę sieciową, aby osiągnąć następujące cele:

- **Zautomatyzowane tworzenie reguł segmentacji sieci** – wykorzystując istniejącą infrastrukturę sieciową, przedsiębiorstwa mogą proaktywnie generować reguły mikrosegmentacji dla zasobów sieciowych specyficznych dla OT.
- **Automatyzacja wirtualnej segmentacji** – przedsiębiorstwa, które chcą segmentować niższe poziomy modelu Purdue, gdzie proaktywne blokowanie jest zabronione, mogą wykorzystać zautomatyzowany mechanizm tworzenia wirtualnych stref Claroty. W tym scenariuszu każde naruszenie komunikacji pomiędzy strefami natychmiast wywołuje alarm.
- **Powstrzymywanie ataków w czasie rzeczywistym** – wykorzystując istniejącą infrastrukturę sieciową, przedsiębiorstwa mogą proaktywnie ograniczać skutki aktywnych ataków. W tym scenariuszu alert pochodzący z systemu ciągłego wykrywania zagrożeń (CTD) Claroty skutkuje automatyczną kwarantanną/izolacją szkodliwego urządzenia.

Kontakt

CLICO Sp. z o.o. | ul. Oleandry 2, 30-063 Kraków, tel.: 12-3783700
www.clico.pl

www.checkpoint.com