WHITE PAPER

WATCHGUARD WYKRYWANIE I ODPOWIEDŹ NA ZAGROŻENIA

PCI-DSS ANTI-MALWARE WHITE PAPER

BHAVNA SONDHI | CISA, QSA (P2PE), PA-QSA (P2PE)

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

SPIS TREŚCI

STRESZCZENIE

WatchGuard Technologies, Inc. (WatchGuard) zaangażował Coalfire Systems, Inc (Coalfire), uznanego specjalistę ds. Bezpieczeństwa kart płatniczych (PCI) i firmę Payment Application - QSA (PAQSA), do przeprowadzenia niezależnej oceny technicznej zagrożenia WatchGuard Threat Detection and Response (TDR). Firma Coalfire przeprowadziła czynności oceniające, w tym testy techniczne, ocenę architektoniczną i walidację zgodności.

W tym artykule Coalfire opisuje, w jaki sposób rozwiązanie WatchGuard TDR może wspierać spełnienie standardów PCI Data Security Standard (PCI DSS) v3.2.1, w szczególności wymagań dotyczących ochrony przed złośliwym oprogramowaniem (5.X) oraz ryzyka podatności (6.1, częściowy) dla obsługiwanych systemów operacyjnych, opartych na testach i dowodach zebranych podczas tej oceny. Aby w pełni przestrzegać standardów, organizacja musi wdrożyć zasady i procedury związane z tymi wymaganiami. W przypadku warunków dotyczących ochrony przed złośliwym oprogramowaniem organizacja powinna określić, w jaki sposób chroni, wykrywa i zgłasza nieprawidłowości, a także przeszkolić swoich pracowników w zakresie procedur ochrony przed zagrożeniami, wykrywania ich i zgłaszania. Wyjaśnienie czynności testowych przeprowadzonych podczas przeglądu Coalfire jest zawarte w tym dokumencie.

O ROZWIĄZANIU WATCHGUARD THREAT DETECTION AND RESPONSE (TDR)

WatchGuard oferuje usługi technologii cyberbezpieczeństwa w zakresie ochrony sieci, Wi-Fi, uwierzytelniania wieloskładnikowego i inteligentnej sieci. WatchGuard TDR, to zaawansowany zbiór narzędzi, służących ochronie przed złośliwym oprogramowaniem. Rozwiązanie koreluje wskaźniki zagrożenia z urządzeniem Firebox[1] i czujniki hosta, aby powstrzymać znane i nieznane złośliwe oprogramowanie. Podstawę narzędzia tworzy oparty na chmurze, silnik korelacyjny - ThreatSync, który analizuje dane o zdarzeniach w celu identyfikacji podejrzanego zachowania. Zagrożenia oceniane są na podstawie specjalnej skali. TDR to moduł, wchodzący w część pakietu Total Security Suite firmy WatchGuard.

Rozwiązanie WatchGuard TDR wykorzystuje zróżnicowane formy wykrywania (omówione poniżej), za pośrednictwem czujnika WatchGuard Host Sensor, aby znaleźć zaawansowane zagrożenia złośliwym oprogramowaniem.

- Sygnatury - rozwiązanie WatchGuard TDR wykorzystuje wykrywanie oparte na sygnaturach. Jest to pierwszy poziom ochrony, który informuje o zagrożeniach klasy korporacyjnej oraz podejrzanych zdarzeniach występujących na punktach końcowych. Metoda oparta na sygnaturach, sprawdza czy dane oprogramowanie lub plik jest zagrożeniem.
- Heurystyka - rozwiązanie WatchGuard TDR wykorzystuje reguły i algorytmy do wyszukiwania poleceń, które mogą wskazywać na naruszenie bezpieczeństwa sieci.
- Analiza behawioralna - rozwiązanie WatchGuard TDR przeprowadza również analizę behawioralną w celu śledzenia zachowania incydentów jako pomocniczy mechanizm wykrywania. WatchGuard zapewnia moduł Host Ransomware Prevention, który śledzi działania związane z atakami ransomware, aby zapobiec atakom szyfrowania plików.
- Analiza plików w Sandboxsie - rozwiązanie WatchGuard TDR wykorzystuje własną usługę Advanced Persistent Threat Blocker (APT Blocker) firmy WatchGuard do analizy nowych plików zidentyfikowanych przez czujnik hosta jako zagrożenie. Wynik analizy zostaje oznaczony jako poziom zagrożenia APT, a następnie system przypisuje go do pliku.

ODBIORCY

Ten dokument skierowany został do trzech docelowych odbiorców:

[1] WatchGuard Firebox to urządzenie zabezpieczające, które zapewnia bezpieczeństwo w zarządzaniu sieciami, VPN, uwierzytelnianiem itp. WatchGuard Firebox nie jest objęty zakresem tego raportu.

1. **Społeczność QSA i audytorów wewnętrznych:** Grupa odbiorców, która ocenia rozwiązania typu WatchGuard TDR z punktu widzenia handlowca oraz dostawcy usług PCI DSS.
2. **Administratorzy i inni specjaliści ds. Bezpieczeństwa:** Odbiorcy oceniający rozwiązanie pod kątem wykorzystania WatchGuard TDR w swoich organizacjach.
3. **Organizacje handlowców i dostawców usług:** Ta grupa odbiorców może oceniać rozwiązanie WatchGuard TDR pod względem wdrożenia w ich środowisku wykorzystywanym do obsługi płatności kartami.

ZGODNOŚĆ PCI DSS

Zestaw wymagań branżowych, które mają pomóc chronić informacje o kartach płatniczych. Rada Standardów Bezpieczeństwa PCI (SSC) została ustanowiona przez głównych operatorów kart płatniczych (American Express, Discover, JCB, MasterCard i Visa). Standard opiera się na programach bezpieczeństwa marek kart oraz najlepszych praktykach branżowych w zakresie bezpieczeństwa.

CELE	WYMAGANIA
Buduj i utrzymuj bezpieczną sieć	1. Trzymaj dane posiadaczy kart w bezpiecznym środowisku chronionym przez firewalla. 2. Nie korzystaj z ustawień fabrycznych dostarczonych przez dostawce. Regularnie zmieniaj hasła.
Chroń dane posiadaczy kart	3. Chroń dane posiadaczy kart. 4. Szyfruj dane posiadaczy kart podczas przesyłania ich w sieci publicznej.
Zastosuj system do zarządzania lukami w zabezpieczaniach	5. Chroń wszystkie systemy przed złośliwym oprogramowaniem i regularnie aktualizuj oprogramowanie lub programy antywirusowe. 6. Rozwijaj bezpieczne systemy i aplikacje.
Wdrażaj środki kontroli dostępu	7. Ogranicz dostęp do danych posiadaczy kart zgodnie z wymaganiami biznesowymi. 8. Wprowadź uwierzytelnianie dostęp do komponentów systemu. 9. Ogranicz fizyczny dostęp do danych posiadacza karty.
Stale monitoruj swoją sieć	10. Śledź i monitoruj cały dostęp do zasobów sieciowych oraz danych posiadaczy kart. 11. Regularnie testuj systemy i procesy bezpieczeństwa.
Wzmacniaj bezpieczeństwo informacji	12. Utrzymuj zasady dotyczące bezpieczeństwa informacji dla całego personelu.

Tabla 1: Cele i wymagania PCI DSS

PCI DSS ma zastosowanie do wszystkich organizacji, które przechowują, przetwarzają lub przekazują dane posiadaczy kart. Wszystkie organizacje, których dotyczy zagadnienie, muszą być zgodne z ww. standardem.

METODOLOGIA

Coalfire przeprowadził wieloaspektową ocenę techniczną, korzystając z najlepszych praktyk branżowych i audytowych. Testy zostały przeprowadzone zdalnie od 9 października 2018 do 12 października 2018.

Testowanie składało się z następujących zadań:

1. Przegląd techniczny architektury rozwiązania WatchGuard TDR i jego komponentów.
2. Wdrożenie oprogramowania Host Sensor w środowisku laboratoryjnym WatchGuard TDR z zaostrzonymi politykami skonfigurowanymi dla systemu operacyjnego Windows.
3. Wprowadzenie plików binarnych złośliwego oprogramowania w systemach lokalnych z zainstalowanym oprogramowaniem Host Sensor.
4. Potwierdzenie zdolności Host Sensor do blokowania i usuwania znanych próbek złośliwego oprogramowania dla punktów końcowych Windows.
5. Przegląd funkcji skanowania w czasie rzeczywistym (plik/proces/rejestru, analiza bazowa i analiza behawioralna) oferowany przez rozwiązanie WatchGuard TDR dla punktów końcowych systemu Windows.
6. Czy baza danych sygnatur Host Sensor jest aktualna i posiada funkcję automatycznej aktualizacji.
7. Weryfikacja, czy funkcje automatycznej aktualizacji czujnika hosta i ręcznej aktualizacji istnieją i działają zgodnie z przeznaczeniem, zapewniając status za pośrednictwem portalu WatchGuard TDR.
8. Przegląd interfejsu użytkownika (UI) portalu WatchGuard TDR w celu potwierdzenia, że administrator może zarządzać różnymi wymaganymi funkcjami i czujnikami punktów końcowych za pośrednictwem interfejsu użytkownika.
9. Przegląd powiadomień o szczegółach incydentów bezpieczeństwa dostarczonych skonfigurowanym użytkownikom z portalu WatchGuard TDR.
10. Przegląd dzienników wygenerowanych przez czujnik hosta w celu przejrzenia działań, które wystąpiły w systemie.

PODSUMOWANIE

Poniższe ustalenia zostały oparte na testach i dowodach zebranych podczas tej oceny:

- Po prawidłowym wdrożeniu zgodnie z wytycznymi dostawcy, rozwiązanie WatchGuard TDR może zapewnić pokrycie PCI DSS dla PCI DSS Wymaganie 5 - „Ochrona wszystkich systemów przed złośliwym oprogramowaniem i regularne aktualizowanie oprogramowania lub programów antywirusowych”, Wymaganie 2.4 Utrzymanie zapasów i część Wymagania 6.1 dla Ranking ryzyka podatności.
- Narzędzie WatchGuard TDR wykryło i skutecznie uniemożliwiło wykonanie znanych próbek złośliwego oprogramowania dla punktów końcowych systemu Windows.
- Rozwiązanie WatchGuard TDR skutecznie osłabiło szkodliwe oprogramowanie na punktach końcowych systemu Windows po skonfigurowaniu z Cybercon[2] . Ustawienia poziomu 3 i dodatkowe domyślne zasady zalecane przez WatchGuard mogą zapewnić ustawienia niezbędne do spełnienia wymagań PCI DSS.
- Domyślna polityka APT Blocker rozwiązania WatchGuard TDR umożliwia czujnikom hosta wysyłanie podejrzanych plików do piaskownicy w celu analizy przez APT Blocker.
- WatchGuard TDR uniemożliwia dostanie się do sieci nieautoryzowanym użytkownikom
- WatchGuard TDR odpowiednio generuje dzienniki zdarzeń, dzięki którym można łatwo śledzić złośliwe działania, zgodnie z wymaganiami PCI DSS dla punktów końcowych systemu Windows.
- Rozwiązanie WatchGuard TDR może zapewnić szczegółowe informacje o stanie systemu w zakresie PCI DSS, aby pomóc spełnić wymaganie 2.4 dla urządzeń z systemem Windows.

[2] Poziom Cybercon (Cyber Condition) to termin opracowany dla rozwiązania WatchGuard TDR. Poziom Cybercon reprezentuje gotowość przedsiębiorstwa do obrony przed atakami na obsługiwane systemy operacyjne.

- Mechanizm analityczny ThreatSync w rozwiązaniu WatchGuard TDR przypisuje punkty zdarzeniom, które wystąpiły na punktach końcowych i klasyfikuje je w skali od 0 (znane dobre) do 10 (krytyczne), gdzie 10 oznacza zagrożenie o najwyższym natężeniu.
- Silnik analityczny ThreatSync w narzędziu WatchGuard TDR zestawia wyniki wskaźników na punkcie końcowym (hoście) i przypisuje ogólną ocenę incydentów, która odzwierciedla ogólne bezpieczeństwo zagrożeń dla tego punktu końcowego.

Załącznik A: Omówienie wymagań PCI DSS. Zawiera szczegółowe ustalenia zawarte w tym raporcie.

UWAGI OCENY

Zakres oceny koncentrował się na walidacji zastosowania rozwiązania WatchGuard TDR w środowisku PCI DSS, w szczególności w celu uwzględnienia jego wpływu na wymagania PCI DSS 5.X, 2.4 i 6.1 (częściowe). Rozwiązanie WatchGuard TDR, jeśli zostanie prawidłowo wdrożone zgodnie z wytycznymi firmy WatchGuard zapisanymi w ich podręczniku, może zostać wykorzystane do spełnienia technicznych części powyższych wymagań. Rozwiązanie WatchGuard TDR zapewnia różne funkcje zapewniające zgodność z powyższymi wymaganiami. Ponieważ jednak większość środowisk i konfiguracji komputerowych znacznie się różni, należy zauważyć, że korzystanie z tego produktu nie gwarantuje bezpieczeństwa, a nawet najbardziej solidne rozwiązania antywirusowe mogą zawieść, jeśli zostaną nieprawidłowo wdrożone i utrzymywane. Strategia kompleksowej obrony zapewniająca wiele warstw ochrony powinna być stosowana jako najlepsza praktyka podczas korzystania z rozwiązania do ochrony punktów końcowych WatchGuard TDR. Aby uzyskać odpowiedzi na pytania dotyczące zasad i konfiguracji oraz sprawdzonych metod, skontaktuj się z WatchGuard. Uwaga! Producent oferuje pakiet Total Security Suite, który łączy moduł TDR z innymi przydatnymi funkcjami oferowanymi przez WatchGuard. Aby uzyskać dodatkowe informacje, skonsultuj się z WatchGuard, niniejszy raport koncentruje się wyłącznie na rozwiązaniu WatchGuard TDR.

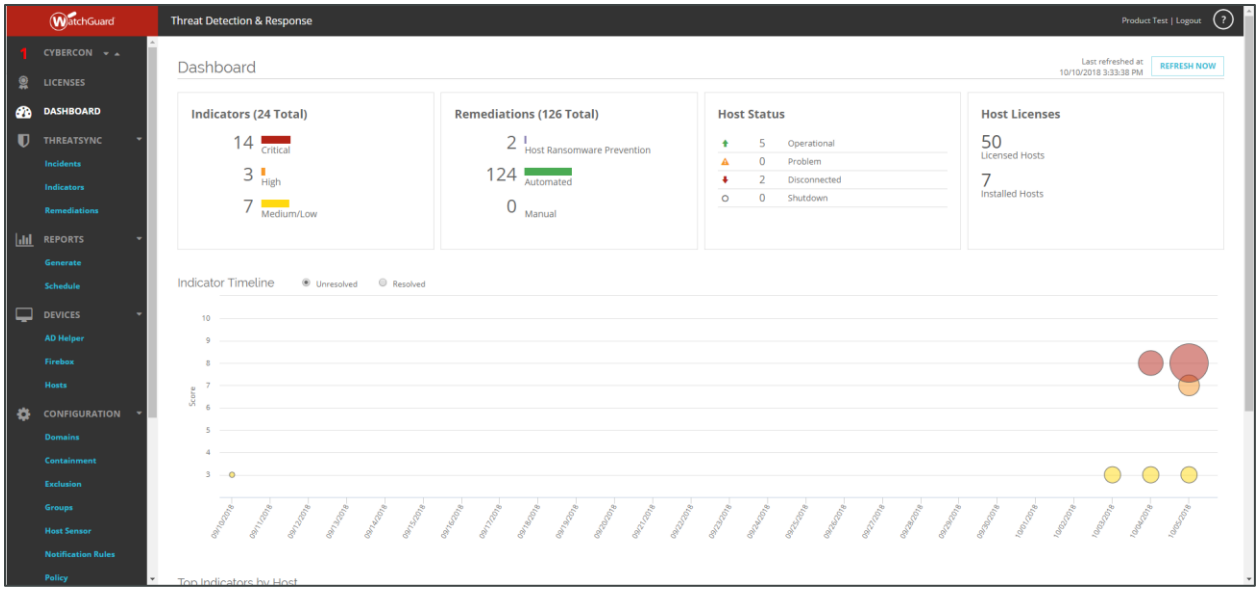
Nie należy twierdzić, że zastosowanie rozwiązania WatchGuard TDR gwarantuje pełną zgodność z PCI DSS. Lekceważenie wymagań PCI i sprawdzonych metod kontroli bezpieczeństwa dla systemów i sieci znajdujących się w zakresie PCI DSS lub poza nim może wprowadzić wiele innych zagrożeń dla bezpieczeństwa lub ciągłości biznesowej w organizacji. Celem każdego biznesu przy wyborze rozwiązań do zabezpieczenia sieci, powinno być ograniczanie ryzyka biznesowego i bezpieczeństwa.

WATCHGUARD ROZWIĄZANIE TDR. ARCHITEKTURA I BEZPIECZEŃSTWO

Poniżej opisano kluczowe komponenty narzędzia WatchGuard TDR:

Usługa subskrypcji wykrywania zagrożeń i reagowania na nie: Usługa TDR jest hostowana w chmurze, wymaga ona subskrypcji z danymi do logowania umożliwiającymi dostęp do portalu WatchGuard TDR. Portal WatchGuard TDR może służyć do konfigurowania ustawień konta, ustawień czujnika hosta oraz monitorowania i zarządzania incydentami bezpieczeństwa. Administratorzy mogą
z poziomu portalu TDR - zarządzać, monitorować i konfigurować polityki.

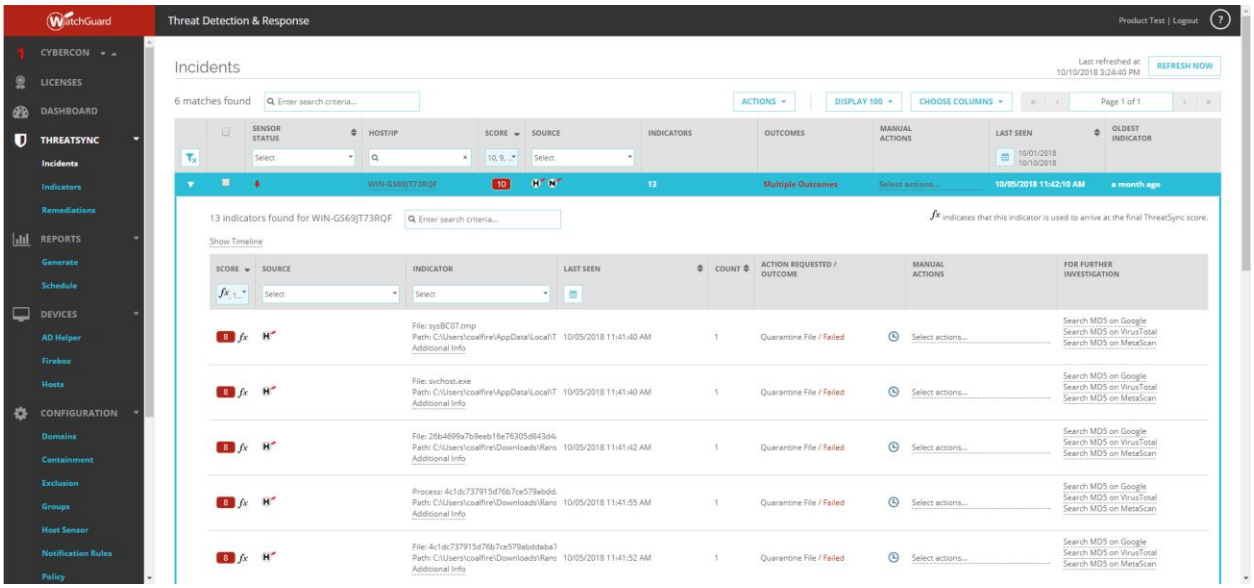
Rysunek 1: Przedstawia pulpit nawigacyjny WatchGuard TDR, na którym widoczne są wskaźniki wraz z poziomem krytyczności, środkami zaradczymi, statusem hosta, harmonogramem oraz listą najważniejszych wskaźników, które wystąpiły na hostach.



Rysunek 1: Pulpit nawigacyjny WatchGuard TDR

Wskaźniki (na rysunku poniżej) przedstawiają zdarzenia odebrane z czujnika hosta i ocenione przez narzędzie analityczne ThreatSync. Użytkownicy lub administratorzy mogą zobaczyć wszystkie wskaźniki w systemie, tworzyć szybkie wykresy słupkowe i kołowe oraz wykonywać wszelkie ręczne działania w systemach hosta.

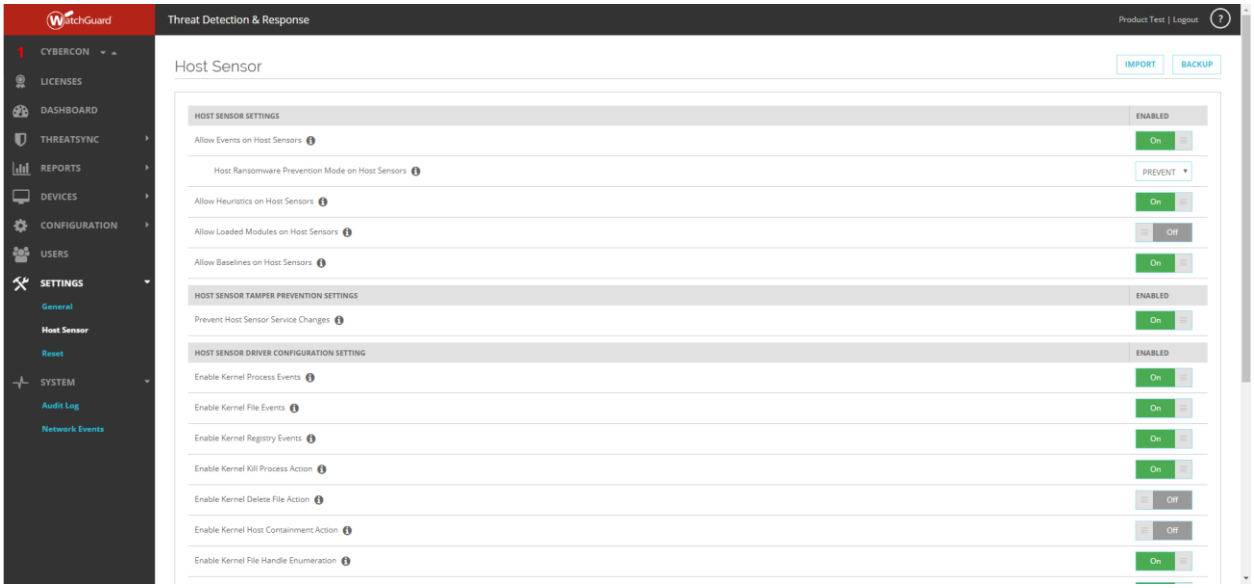
Gdy WatchGuard TDR otrzyma informacje o zdarzeniu od czujnika hosta, silnik analityczny ThreatSync sprawdza zdarzenie i przypisuje ocenę zagrożenia na podstawie analizy. Zgłoszenie, któremu przypisano ocenę "zagrożenie", staje się wskaźnikiem. Wyższe wyniki wskazują na większe prawdopodobieństwo, że obserwowane zdarzenie lub obiekt stanowi zagrożenie.



Rysunek 2: Wskaźniki i incydenty WatchGuard TDR

Czujnik hosta: Czujnik hosta jest instalowany na komputerach w sieci organizacji. Czujnik hosta może zbierać dane kryminalistyczne z systemu hosta i wysyłać je do chmury WatchGuard TDR w celu analizy. Czujnik monitoruje również zachowania oprogramowania ransomware. Składa się z danych kryminalistycznych plików, procesów, połączeń sieciowych i kluczy rejestru na hoście.

Administratorzy mogą skonfigurować czujnik hosta, aby zgłaszał zagrożenia bezpieczeństwa lub podejmował działania w przypadku określonych typów zagrożeń w celu rozwiązania problemu. Czujnik hosta może automatycznie poddawać kwarantannie pliki, zatrzymywać procesy, blokować lub izolować hosta od sieci oraz usuwać wpisy rejestru, jeśli zidentyfikuje plik lub proces jako zagrożenie.



Rysunek 3: Konfiguracje czujnika hosta WatchGuard

ThreatSync: Opiera się na chmurze analizującej korelacje i oceny zagrożeń, która zapewnia praktyczny wgląd w zagrożenia atakujące systemy końcowe. ThreatSync zbiera, koreluje i analizuje dane o zagrożeniach z kanałów WatchGuard Host Sensor, Firebox i informacje o zagrożeniach.

ThreatSync przypisuje wskaźnik zagrożenia i rangę zdarzeniom, które wystąpiły w Fireboxie i punktach końcowych; ważne jest, aby zespoły ds. bezpieczeństwa znały najbardziej krytyczne zagrożenia, aby mogły sklasyfikować środki zaradcze związane z wydarzeniem. ThreatSync można skonfigurować tak, aby wysyłał automatyczne powiadomienia e-mail po wykryciu i naprawieniu incydentów i wskaźników.

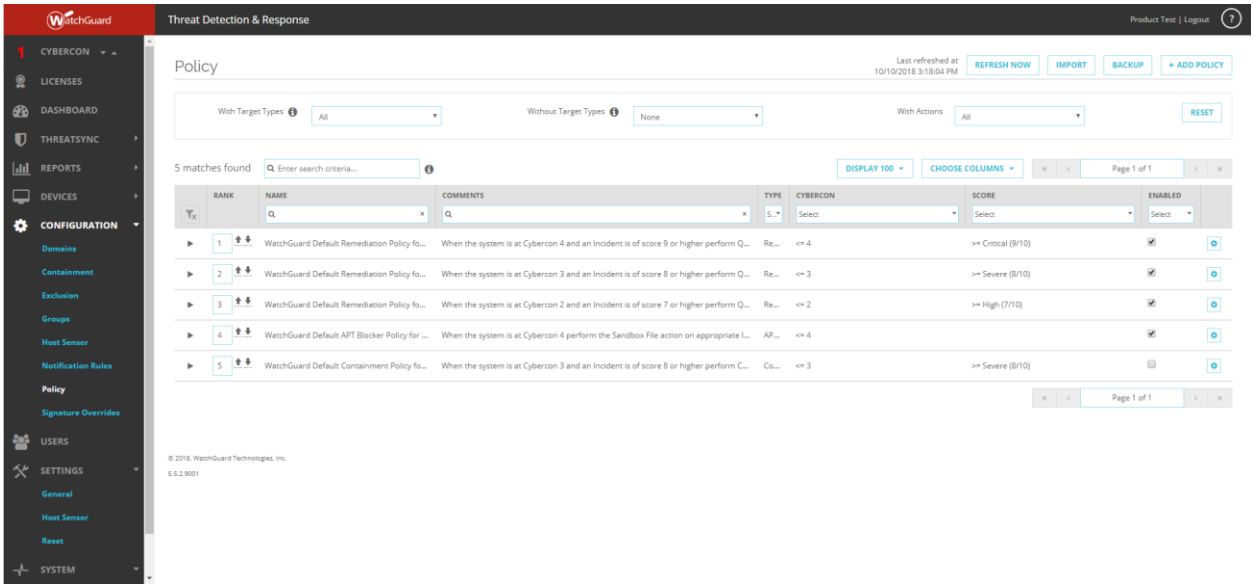
WatchGuard TDR umożliwia użytkownikom konfigurowanie zasad w oparciu o potrzeby organizacyjne. Dzięki punktowaniu zagrożeń i ustalaniu priorytetów zapewnianym przez ThreatSync, użytkownicy mogą konfigurować zasady inicjowania działań naprawczych na podstawie oceny lub zakresu zagrożenia, w tym procesu zabijania, pliku kwarantanny i usuwania wartości klucza rejestru. Administratorzy mogą ustawić zasady dotyczące podejrzanych plików / procesów / kluczy rejestru w piaskownicy i eskalować wyniki ThreatSync na podstawie wyników piaskownicy. Administratorzy mogą również ustawić zasady izolowania / zatrzymywania hosta od reszty sieci na podstawie wyniku. Na przykład organizacje o niskim ryzyku ataku mogą zdecydować się na zautomatyzowanie odpowiedzi tylko na zagrożenia o wysokiej pozycji, które uzyskały ocenę 8 lub wyższą. Jednakże, gdyby znaleźli się w grupie większego ryzyka ataku, mogliby zdecydować się na automatyczną naprawę zagrożeń z wynikiem 6 lub wyższym.[3]

Rozwiązanie WatchGuard TDR zostało skonfigurowane do testowania, aby spełnić wymagania dotyczące ochrony przed złośliwym oprogramowaniem dla PCI DSS. Odpowiednia polityka[4], rekomendacje odnotowane przez WatchGuard powinny być wdrażane przez organizację korzystającą z rozwiązania WatchGuard TDR. Należy pamiętać, że domyślne ustawienia Cybercon Level[3]

[3] Informacje techniczne, Wykrywanie i reagowanie na zagrożenia WatchGuard https://www.watchguard.com/wgrd-products/security-services/threat-detection-and-response

Default TDR policies are defined here: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/tdr/tdr_policy_tips_c.html

Oprócz domyślnych skonfigurowanych polityk APT Blocker może obecnie spełniać niezbędne wymagania dotyczące kontroli. Poziom Cybercon reprezentuje gotowość przedsiębiorstwa do obrony przed atakami. Cybercon Level 3 może wykryć zagrożenie (wynik 8 lub wyższy) i zapewnić najwyższy poziom odpowiedzi i środków zaradczych.



Rysunek 4: Polityki WatchGuard

OCENA BEZPIECZEŃSTWA TECHNICZNEGO

METODY OCENY

Do oceny potencjalnej zgodności PCI DSS z rozwiązaniem WatchGuard TDR wykorzystano następujące metody:

1. Analiza architektury i konfiguracji zgodnie z wytycznymi dostawcy.
2. Wdrożenie czujnika hosta na komputerach testowych z systemem Windows w środowisku zwirtualizowanym z zaostrzonymi zasadami wymuszanymi w celu wykrywania i zapobiegania znanemu złośliwemu oprogramowaniu.
3. Przypisanie zdefiniowanego profilu zasad (Cybercon Level i domyślny APT Blocker) dla systemu Windows w celu zapewnienia wymagań standardów zgodności.
4. Sprawdzenie konfiguracji agenta w celu potwierdzenia ochrony nie może zostać wyłączone przez osoby niebędące administratorami.
5. Wykonywanie ataków bezplikowych, które obejmowały złośliwe próbki binarne (w tym oprogramowanie ransomware, backdoor, oprogramowanie szpiegowskie, wirusy i robaki).
6. Przegląd WatchGuard TDR pod kątem weryfikacji wykrywania, wykonywania, zapobiegania i usuwania wszystkich próbek złośliwego oprogramowania. Ponadto ocena składników portalu opartego na chmurze w celu sprawdzenia, czy czujnik hosta jest aktualny i chroni przed zagrożeniami w czasie rzeczywistym.
7. Przegląd alertów o incydentach wykrytych i zabezpieczonych.
8. Przegląd narzędzi systemu dostępnych z poziomu Portalu WatchGuard TDR.
9. Przegląd zagrożeń i ocen przypisanych do tych zdarzeń z poziomu portalu WatchGuard TDR.

OPIS ŚRODOWISK TESTOWYCH

Rozwiązanie WatchGuard TDR było hostowane w środowisku WatchGuard Lab w celach testowych, a agent Host Sensor został zainstalowany w systemach o następujących konfiguracjach:

System hostowane w środowisku FireboxV w chmurze:

- Windows 2008 R2 z domyślnie wyłączonymi aplikacjami antywirusowymi
- Windows 10 64-bit z domyślnie wyłączonymi aplikacjami antywirusowymi
- Windows 2012 R2 z domyślnie wyłączonymi aplikacjami antywirusowymi
- Windows 7 64-bit z domyślnie wyłączonymi aplikacjami antywirusowymi

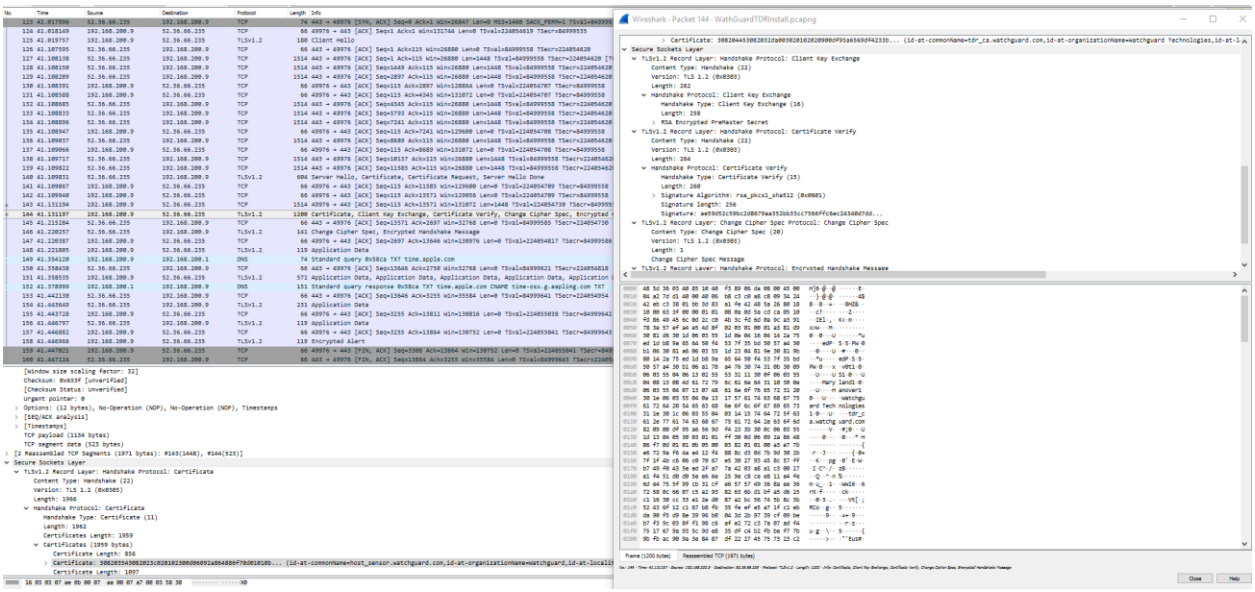
System nie hostowane w środowisku FireboxV w chmurze:

- Windows 10 Pro z bezpośrednim dostępem RDP

OCENA RUCHU SIECIOWEGO

Snifer portów Ethernet Wireshark został użyty do monitorowania ruchu dla komponentów w ramach rozwiązania WatchGuard TDR:

- Ruch z komputera z systemem Windows z oprogramowaniem Host Sensor do rozwiązania WatchGuard TDR hostowanego w chmurze WatchGuard TDR (Rysunek 5): Żadne wrażliwe dane nie są przesyłane przez sieć z komputera z systemem Windows do środowiska chmury WatchGuard TDR, a żadne dane dziennika lub informacje o alertach są szyfrowane za pomocą protokołu TLS 1.2.



Rysunek 5: Komunikacja między komputerem z systemem Windows a rozwiązaniem WatchGuard TDR. Zaszyfrowane dane (dzienniki i informacje o aktualizacjach) są zawsze przesyłane za pośrednictwem protokołu TLS 1.2.

NARZĘDZIA

Standardowe narzędzia Coalfire wykorzystane do tej oceny technicznej obejmowały:

NAZWA NARZĘDZIA	OPIS
Live Malware Samples	Przykładowe pliki binarne znanego złośliwego oprogramowania dla systemów operacyjnych Windows: • Przykładowe złośliwe oprogramowanie dla systemu znane jako Malware DB ze strony http://thezoo.morirt.com/. • Próbki szkodliwego oprogramowania uzyskane przez dostawców *Uwaga - odwiedzanie i pobieranie z powyższych witryn może prowadzić do infekcji złośliwym oprogramowaniem; z tego powodu Coalfire zdecydowanie odradza odwiedzanie tych witryn.
Wireshark	Sniffer portów Ethernet do obserwowania ruchu przychodzącego i wychodzącego z systemu

REFERENCJE

PCI SSC - standard bezpieczeństwa danych: https://www.pcisecuritystandards.org/documents/pci_dss_v3.pdf

PCI SSC - Standard bezpieczeństwa danych aplikacji płatniczych S- przewodnik wersja 3.2: https://www.pcisecuritystandards.org/documents/PA-DSS_v3-2.pdf

Dokumentacja produktu WatchGuard - https://www.watchguard.com/wgrd-resource-center/

ZAŁĄCZNIK A: ZGODNOŚĆ WYMAGAŃ PCI DSS

* Uwaga: Niektóre funkcje opisane w poniższych tabelach wykraczają poza wymagania PCI DSS. Są one odnotowywane do wszystkich celów związanych z przeglądem odbiorców

Chociaż rozwiązanie WatchGuard TDR pomaga w spełnieniu wymagań PCI DSS, organizacje handlowców lub dostawców usług są nadal zobowiązane do stworzenia odpowiednich zasad lub procedur, aby spełnić niezbędne wymagania.

OPIS POZIOMU ZGODNOŚCI	OPIS
✓	Zgodność bezpośrednio obsługiwana przez rozwiązanie WatchGuard TDR.
✓	Działania organizacji w celu uzyskania pełnej zgodności.

PCI DSS WYMAGANIE	DEFINICJA TESTU WALIDACJI PCI	SPEŁNIENIE WYMOGÓW	ROZWIĄZANIE WATCHGUARD TDR BADANIA I WYNIKI
2.4 Prowadzenie inwentaryzacji komponentów systemu, które są objęte zakresem PCI DSS.	2.4.a Zbadaj inwentaryzację systemu, aby upewnić się, że prowadzona jest lista komponentów sprzętowych, programowych i zawierających opis funkcji / zastosowania każdego z nich.	✓	W przypadku wszystkich składników systemu, w których wdrożono WatchGuard Host Sensor, administratorzy mogą korzystać z rozszerzenia. WatchGuard TDR Portal do pomocy w tworzeniu i zarządzaniu inwentaryzacją systemu. Organizacje są jednak nadal odpowiedzialne za utrzymanie dokładności i rejestrację nowych systemów, aby zapewnić dokładność inwentaryzacji, a także za wyeksportowanie tej listy w celu uwzględnienia opisu funkcji wspomnianych urządzeń. Rozwiązanie WatchGuard TDR może pomóc użytkownikom w częściowym wdrożeniu lub spełnieniu wymagań dotyczących utrzymania zapasów. Organizacja nadal wymaga prowadzenia dokumentacji wszystkich innych systemów operacyjnych lub urządzeń niewymienionych poniżej. **Procedura testowa:** Coalfire zainstalował Host Sensor na punktach końcowych Windows i potwierdził, że działa i łączy się z portalem WatchGuard TDR. Hosty punktów końcowych były przeglądane w oknie Urządzenia -> Hosty, które zawierało nazwę hosta, adres IP, typ systemu operacyjnego, stan instalacji, wersję czujnika itp. Dla wszystkich punktów końcowych, w których wdrożono czujnik hosta.

Zarządzanie lukami w zabezpieczeniach **Wymaganie 5: Ochrona systemów przed złośliwym oprogramowaniem, regularna aktualizacja oprogramowania**			
5.1 Wdrażanie antywirusa we wszystkich systemach powszechnie atakowanych przez złośliwe oprogramowanie (szczególnie osobiste komputery i serwery).	5.1 Próbki składników, w tym wszystkich typów systemów operacyjnych, na które zwykle wpływa złośliwe oprogramowanie, sprawdź, czy wdrożono oprogramowanie antywirusowe, jeśli istnieje odpowiednia technologia antywirusowa.	✓	Rozwiązanie WatchGuard TDR zapewnia następujące funkcje: • WatchGuard Host Sensor można pobrać z WatchGuard TDR Portal -> Konfiguracja -> Host Sensor z instalatorami dostępnymi dla systemów operacyjnych Windows. • Zapewnia bezpośredni monitoring możliwość obsługi systemów wykorzystujących czujniki za pośrednictwem portalu WatchGuard TDR. **Procedura testowa:** WatchGuard TDR wygenerował rekord dziennika, który wskazywał, że czujnik hosta wykrył zagrożenie i zebrał dane z punktów końcowych systemu Windows. Uzyskane zdarzenie związane z wykrywaniem i zapobieganiem zagrożeniom dla punktów końcowych systemu Windows
5.1.1 Upewnienie się, że wszystkie programy antywirusowe są zdolne do wykrywania, usuwanie i zabezpieczanie przed wszystkimi znanymi typom złośliwego oprogramowanie.	5.1.1 Sprawdzenie dostarczonej dokumentacji i konfiguracji antywirusa: • Wykrycie wszystkich znanych typów złośliwego oprogramowania, • Usuniecie wszystkich znanych rodzajów złośliwego oprogramowania • Ochrona przed wszystkimi znanymi typpami złośliwego oprogramowanie *Przykładowe typów złośliwego oprogramowania obejmuje wirusy, trojany, robaki, spyware, adware i rootkity.*	✓	Rozwiązanie WatchGuard TDR zapewnia następujące funkcje: • WatchGuard ThreatSync, to oparty na chmurze mechanizm analizy korelacji i punktacji, który zapewnia wgląd w zagrożenia na punktach końcowych. Zapewnia wykrywanie i pomaga w zapobieganiu pojawienia się złośliwego oprogramowania. Po odpowiedniej konfiguracji, WatchGuard TDR zapewnia ochronę w czasie rzeczywistym . • Host Sensor wdrożony na punktach końcowych komunikuje się z silnikiem ThreatSync w czasie rzeczywistym, gdzie sprawdza i wykrywa znane cyberzagrożenia. • Rodzaje złośliwego oprogramowania, które można wykryć, obejmują oprogramowanie ransomware, (PUA), backdoor, dropper, spyware, wirus, robak i trojan.

			Procedura testowa **1. Wykrywanie wszystkich „ZNANYCH" typyów złośliwego oprogramowania:** Wykryte typy złośliwego oprogramowania obejmowały oprogramowanie ransomware, PUA, backdoor, dropper, oprogramowanie szpiegowskie, wirusy, robaki i trojany. Ataki bezplikowe i plikowe zostały przeprowadzone przy użyciu różnych zestawów próbek, aby sprawdzić, że rozwiązanie WatchGuard TDR chroni przed znanymi typami ataków złośliwego oprogramowania na system operacyjny Windows. **2. Usuwanie wszystkich „ZNANYCH" typów złośliwego oprogramowania:** Rodzaje złośliwego oprogramowania, które zostały usunięte i poddane kwarantannie, obejmowały oprogramowanie ransomware, PUA, backdoor, dropper, oprogramowanie szpiegowskie, wirusy, robaki i trojany dla systemu operacyjnego Windows. Coalfire wykazał, że Host Sensor usunął i poddał kwarantannie pliki, które zostały wykryte jako złośliwe oprogramowanie. **3. Ochrona przed wszystkimi „ZNANYMI" typami złośliwego oprogramowania:** Rodzaje złośliwego oprogramowania, którym udało się zapobiec, obejmowały oprogramowanie ransomware, PUA, backdoor, dropper, oprogramowanie szpiegowskie, wirusy, robaki i trojany dla systemu operacyjnego Windows. Coalfire wykazało, że rozwiązanie wykryło i zablokowało znane złośliwe oprogramowanie, które znajdowało się na liście znanych złośliwych programów z VirusTotal.
5.1.2 W przypadku systemów uznawanych za często zagrożone złośliwym oprogramowaniem należy przeprowadzać okresowe audyty w celu zidentyfikowania i oceny rozwijających się zagrożeń.	5.1.2 Przeprowadź wywiady z personelem, aby sprawdzić, czy ewoluujące zagrożenia złośliwym oprogramowaniem są monitorowane i oceniane pod kątem systemów, które obecnie nie są uważane za powszechnie narażone na szkodliwe oprogramowanie, aby potwierdzić, czy takie systemy nadal nie wymagają oprogramowania antywirusowego.	✓	Jest to wymóg dotyczący procedury. Klienci (handlowcy lub usługodawcy) muszą okresowo oceniać systemy, z których korzystają, aby upewnić się, że nie są one uważane za często dotknięte problemem. WatchGuard Host Sensor można wdrożyć na punktach końcowych organizacji, a wdrożenia byłyby wymagane do oceny i identyfikacji zagrożeń złośliwym oprogramowaniem na tych punktach końcowych. **Procedura testowa:** Coalfire pokazało, jak łatwo można pobrać Host Sensor z portalu WatchGuard TDR i zainstalować na dowolnym obsługiwanym systemie operacyjnym Windows. Coalfire potwierdził, że każdy system z czujnikiem hosta może zostać oceniony pod kątem zagrożeń.

5.2 Upewnij się, że wszystkie mechanizmy antywirusowe są aktywne oraz: • **Na bieżąco aktualizwane** • **Wykonuj okresowe skanowanie** • **Generują dokumentacje audytu, przechowywane zgodnie z wymaganiami PCI DSS 10.7**	5.2.a Sprawdź zasady i procedury, aby upewnić się, że oprogramowanie antywirusowe i definicje muszą być aktualne.	✓	5.2.a: Rozwiązanie WatchGuard TDR zapewnia następujące funkcje: • Host Sensor zapewnia ochronę w czasie rzeczywistym przed złośliwą aktywnością. WatchGuard TDR wykonuje ręcznie skanowanie linii bazowej co godzinę lub częściej. Można to zrobić na urządzeniu lub globalnie na wszystkich urządzeniach. Skany bazowe obejmują spis plików, który jest przesyłany do analizy do ThreatSync w chmurze WatchGuard. • Administratorzy mogą skonfigurować plan bazowy częściej niż co godzinę. Podstawowe skanowania są wykonywane w czasie rzeczywistym i zużywają mniej zasobów procesora / pamięci RAM niż tradycyjne skanowanie antywirusowe. • Host Sensor można skonfigurować tak, aby był automatycznie aktualizowany z chmury, gdy dostępna jest nowa wersja. Baza sygnatur jest aktualizowana; Jednak rozwiązanie WatchGuard TDR opiera się na analizie behawioralnej w celu wykrycia złośliwej aktywności. **Procedura Testowa:** Coalfire zaobserwowało i potwierdziło, że czujnik WatchGuard Host Sensor był na bieżąco aktualizowany, a podstawowe skany były wykonywane częściej niż co godzinę.
	5.2.b Sprawdzić konfiguracje antywirusowe, w tym główną instalację oprogramowania, aby zweryfikować mechanizmy antywirusowe: • Skonfigurowany do wykonywania automatycznych aktualizacji • Skonfigurowany do wykonywania okresowych skanów.	✓	5.2.b: Rozwiązanie WatchGuard TDR zapewnia następujące funkcje: • WatchGuard TDR jest aktualizowany przez WatchGuard bezpośrednio w chmurze. Definicje bazy danych Host Sensor są aktualizowane automatycznie przez rozwiązanie WatchGuard TDR. • Można skonfigurować tak, aby był automatycznie aktualizowany z portalu WatchGuard TDR oraz Szczegóły dotyczące wersji Host Sensor można przejrzeć w portalu WatchGuard TDR.

			• Host Sensor prowadzi monit na poziomie procesora w czasie rzeczywistym, umożliwiając badanie procesów w celu zablokowania złośliwych zachowań, zanim punkt końcowy zostanie uszkodzony. **Wnioski z testu:** • Coalfire zauważył, że oprogramowanie Host Sensor działające na punktach końcowych systemu Windows zostało automatycznie uaktualnione, gdy dostępna była nowa wersja. • Coalfire potwierdził, testując rozwiązanie, że Host Sensor wykonywał ciągłe monitorowanie na poziomie procesora w czasie wykonywania, umożliwiając badanie procesu w celu zablokowania złośliwych zachowań, zanim punkt końcowy zostanie uszkodzony. Szkodliwe próbki zostały przetestowane w celu potwierdzenia, że były monitorowane i blokowane w czasie rzeczywistym, negując potrzebę okresowych skanów.
	5.2.c Przeanalizuj próbkę składników systemu, w tym wszystkie typy systemów operacyjnych, na które zwykle wpływa złośliwe oprogramowanie, aby sprawdzić, czy: • Oprogramowanie antywirusowe i definicje są aktualne. • Okresowe skany są wykonane.	✓	5.2.c: Rozwiązanie WatchGuard TDR zapewnia następujące funkcje: • W przypadku rozwiązania WatchGuard TDR sygnatury zagrożeń są przechowywane w centralnej bazie danych ThreatSync i aktualizowane co 24 godziny. Host Sensor wysyła zapytania do tej bazy danych w czasie rzeczywistym dla systemów Windows. • Hashe są utrzymywane w zewnętrznej usłudze weryfikacji złośliwego oprogramowania, która zawiera wszystkie sygnatury. Host Sensor uzyskuje dostęp do wszystkich odpowiednich baz danych za pomocą skrótów w czasie rzeczywistym za pośrednictwem ThreatSync. **Wnioski z testu:** • Coalfire potwierdził, że sygnatury są aktualizowane automatycznie przez rozwiązanie WatchGuard TDR i że są aktualne dla testowanych systemów operacyjnych. • Coalfire potwierdziło, testując, że Host Sensor wykonywał ciągłe

			monitorowanie na poziomie procesora w czasie wykonywania, umożliwiając badanie procesów w celu zablokowania złośliwych zachowań, zanim punkt końcowy zostanie uszkodzony. Szkodliwe próbki zostały przetestowane w celu potwierdzenia, że były monitorowane i blokowane w czasie rzeczywistym, eliminując potrzebę okresowego skanowania.
	5.2.d Sprawdź konfiguracje antywirusowe, w tym główną instalację oprogramowania i przykładowe składniki systemu, aby dowiedzieć się cz • Generowanie dziennika oprogramowania antywirusowego jest włączone • Dzienniki są przechowywane zgodnie z wymaganiami PCI DSS 10.7.	✓	5.2.d Rozwiązanie WatchGuard TDR zapewnia następujące funkcje: • Dzienniki antywirusowe są generowane przez Host Sensor na punktach końcowych. Wymaga to ręcznego procesu wysyłania dziennika do scentralizowanej lokalizacji przez administratorów. • Zdarzebua, które wystąpiły na punktach końcowych systemu Windows, dostarczają szczegółowych informacji na temat złośliwych działań, które miały miejsce za pośrednictwem portalu WatchGuard TDR. Informacje te są łatwo dostępne przez jeden miesiąc; jednak administratorzy mogą eksportować te dane, aby spełnić wymagania PCI DSS. • Dzienniki incydentów można wyeksportować z portalu WatchGuard TDR lub bezpośrednio z punktów końcowych systemu Windows, a administratorzy mogą następnie skonfigurować system tak, aby dzienniki były przekazywane na ich zewnętrzne serwery syslog. • Dzienniki audytów dla WatchGuard TDR Portal są dostępne za pośrednictwem konsoli. Są łatwo dostępne przez trzy miesiące i zapewniają funkcję eksportu. **Wnioski:** • Coalfire wykazał, że informacje o incydentach (dzienniki antywirusowe) były zawsze włączone i można je było pobrać bezpośrednio z portalu WatchGuard TDR. Jednak można było wyeksportować je tylko przez jeden miesiąc z portalu WatchGuard TDR. Administratorzy mogliby je wyeksportować w celu zachowania w celu spełnienia wymagań PCI DSS.

			• Coalfire wyodrębnił dzienniki bezpośrednio z punktów końcowych systemu Windows i potwierdził, że zawierały one wszystkie informacje rejestrowania antywirusów. Można zaplanować raportowanie do scentralizowanej lokalizacji w celu przechowywania zgodnie z wymaganiami PCI DSS. • Coalfire confirmed that the audit logs for the cloud-based management portal was available through the audit log feature provided by the WatchGuard TDR Portal. The organization is required to retain the audit logs information to meet the PCI DSS requirements.
5.3 Upewnienie się, że mechanizmy antywirusowe są aktywne i nie mogą być wyłączane ani zmieniane przez użytkowników, chyba że zostały specjalnie autoryzowane przez kierownictwo na podstawie indywidualnych przypadków przez ograniczony czas. **Uwaga: rozwiązania antywirusowe można tymczasowo wyłączyć tylko wtedy, gdy istnieje uzasadniona potrzeba techniczna, autoryzowana przez kierownictwo indywidualnie dla każdego przypadku. Jeśli ochrona antywirusowa musi zostać wyłączona w określonym celu, musi zostać formalnie zatwierdzona.** **Konieczne może być również wdrożenie dodatkowych środków bezpieczeństwa w czasie gdy ochrona antywirusowa nie jest aktywna.**	5.3.a Sprawdź konfiguracje oprogramowania antywirusowego, w tym główną instalację oprogramowania i przetestuj system, aby sprawdzić, czy oprogramowanie antywirusowe jest aktywnie uruchomione.	✓	5.3.a: Rozwiązanie WatchGuard TDR zapewnia następujące funkcje: Konsolę interfejsu użytkownika, która pokazuje stan monitorowania (Online / offline) wszystkich urządzeń wyposażonych w czujniki za pośrednictwem portalu WatchGuard TDR. Stan instalacji (Zainstalowana, Instalowana lub Oczekująca) jest również widoczny w portalu. **Wnioski:** W podglądzie konsoli na żywo na pulpicie nawigacyjnym i widoku hostów, można sprawdzić Host Sensor czy były aktywne (online / offline) i że polityka wymuszała odpowiednią konfigurację (ochrona AV włączona) zgodnie ze specyfikacjami PCI w zakresie zasobów PCI.
	5.3.b Sprawdź konfiguracje antywirusowe, w tym główną instalację oprogramowania, aby upewnić się, że oprogramowanie antywirusowe nie może być wyłączone ani zmienione przez użytkowników.	✓	5.2.a: Rozwiązanie WatchGuard TDR zapewnia następujące funkcje: Portal WatchGuard TDR zapewnia administratorom funkcje włączania i wyłączania ochrony urządzenia. Żaden nieautoryzowany użytkownik nie może wyłączyć oprogramowania Host Sensor działającego lokalnie na komputerze z systemem Windows. Żaden nieautoryzowany użytkownik nie może wyłączyć ochrony w portalu WatchGuard TDR.

			Wnioski Wykazano, że usługa Host Sensor ma włączoną ochronę przed manipulacją i że żaden użytkownik nie może manipulować usługami.
	5.3.c Przeprowadzaj audyty z personelem i obserwuj procesy, aby sprawdzić, czy oprogramowanie antywirusowe nie może zostać wyłączone lub zmienione przez użytkowników, chyba że zostały specjalnie upoważnione przez kierownictwo na podstawie indywidualnych przypadków przez ograniczony czas.	✓	5.3.c: Zgodnie z funkcją opisaną w 5.3.b. Jest to kontrola administracyjna i wymaga zezwolenia od kierownictwa, aby spełnić wymóg kontroli. **Wnioski:** Coalfire wykazał, że rozwiązanie WatchGuard TDR może być konfigurowane przez użytkownika z odpowiednim dostępem i istnieją konfiguracje, które wskazują, kiedy dokonano autoryzowanych zmian.
5.4: Upewnij się, że zasady bezpieczeństwa i procedury operacyjne do ochrony systemów przed złośliwym oprogramowaniem są udokumentowane i wykorzystywane przez wszystkich	5.4 Wykonaj audyt dokumentacji oraz personelu aby zweryfikować, czy zasady bezpieczeństwa i procedury operacyjne do ochrony systemów przed złośliwym oprogramowaniem są: • Udokumentowane, • Wykorzystywane • Znane wszystkim zainteresowanym stronom.	✓	Jest to wymóg oparty na zasadach i procedurach. Chociaż rozwiązanie WatchGuard TDR może pomóc w spełnieniu wymagań w zakresie ochrony przed złośliwym oprogramowaniem, to do administratorów należy tworzenie i dokumentowanie określonych zasad zgodnie z wymaganiami odpowiednich środowisk **Wnioski:** Firma Coalfire wykazała, że przeszukiwano dzienniki rozwiązania WatchGuard TDR i że zebrano statystyki dotyczące stanu oprogramowania klienckiego w celu potwierdzenia czasu pracy czujnika hosta oraz zgodności z zasadami.
6.1 Ustalenie procesu identyfikacji luk w zabezpieczeniach, korzystając z wiarygodnych zewnętrznych źródeł informacji o lukach w zabezpieczeniach. Utworzyć ranking ryzyka (na przykład „wysoki”, „średni” lub „niski”) dla nowo odkrytych luk.	6.1.a Sprawdź zasady i procedury, aby zweryfikować, czy zdefiniowano procesy dla: • Aby zidentyfikować nowe luki w zabezpieczeniach • Aby przypisać podatnościom ranking, który obejmuje identyfikację „wysokiego ryzyka” i „krytycznych” podatnościach. • Korzystać z renomowanych zewnętrznych źródeł informacji o lukach w zabezpieczeniach.	✓	Jest to wymóg dotyczący procesu / procedury i wymaga od klientów opracowania procesu identyfikacji luk w zabezpieczeniach i przypisania rankingu ryzyka. WatchGuard TDR obejmuje analizę sygnatur, heurystykę i analizę behawioralną w celu wykrycia i sklasyfikowania złośliwego oprogramowania. Funkcje te mogą być pomocne w ustalaniu typu złośliwego oprogramowania i mogą stanowić wskazówki dla klientów w celu sklasyfikowania zagrożeń związanych z typem złośliwego oprogramowania. **Wnioski:** Coalfire wykazało, że rozwiązanie WatchGuard TDR wykryło

			cyberzagrożenia i znane ataki złośliwego oprogramowania. Rozwiązanie WatchGuard TDR dostarczyło również szczegółowych informacji o zidentyfikowanych cyberzagrożeniach. Informacje te mogą następnie zostać wykorzystane przez klientów do celów klasyfikacji ryzyka.

WNIOSKI

Podczas testowania narzędzia WatchGuard TDR pod kątem różnych wymagań PCI-DSS, rozwiązanie wykazało wysoki poziom elastyczności w zakresie zarządzania punktami końcowymi, dostosowywania zasad, analizy plików, powiadomień, zarządzania użytkownikami, zarządzania urządzeniami i zarządzania czujnikiem hosta dla punktów końcowych za pośrednictwem portalu WatchGuard TDR.

Po przeanalizowaniu wymagań PCI DSS, Coalfire ustalił, poprzez ocenę techniczną, ocenę architektoniczną i walidację zgodności, że rozwiązanie WatchGuard TDR, jak opisano w tym dokumencie, wspomaga organizację w technicznych częściach ochrony przed złośliwym oprogramowaniem (5.X) wymagania, utrzymuje zapasy (2.4) i zmniejsza ranking ryzyka podatności (6.1, częściowe) dla obsługiwanych systemów operacyjnych. Możliwość osiągnięcia ogólnej zgodności z jakąkolwiek regulacją lub normą będzie zależała od konkretnego projektu. Organizacja musi również utworzyć u siebie zasady i procedury dotyczące sposobu, w jakim chroni przed złośliwym oprogramowaniem, wykrywa je i zgłasza, a także należy przeszkolić pracowników w zakresie procedur ochrony, wykrywania i zgłaszania złośliwego oprogramowaniem.

O AUTORACH

Bhavna Sondhi | Senior Security Consultant

Jest starszym konsultantem ds. Bezpieczeństwa w zespole walidacji rozwiązań w Coalfire. Jest odpowiedzialna za przeprowadzanie audytów PCI DSS, PA-DSS i P2PE, a także za tworzenie raportów technicznych. Dołączył do Coalfire w 2013 roku i wniósł do zespołu ponad 12-letnie doświadczenie w inżynierii oprogramowania i bezpieczeństwie informacji, prowadzi rozległe konsultacje i oceny w USA, Europie i Azji. Jako lider PA-QSA i P2PE-QSA, Bhavna wspiera oceny dla niektórych z największych dostawców oprogramowania płatniczego na świecie, a jej doświadczenie w inżynierii oprogramowania odgrywa kluczową rolę w zapewnieniu zespołom, że uznają znaczenie tworzenia bezpiecznego kodu i bezpieczeństwa informacji w swoich praktyki operacyjne.

Nick Trenc | Director

Dyrektor zespołu walidacji rozwiązań w Coalfire. Nick ma kilkuletnie doświadczenie w pracy w dziedzinie bezpieczeństwa informacji i ma dogłębną wiedzę na temat architektur bezpieczeństwa aplikacji, sieci i systemów. Posiada certyfikaty CISA, CISSP, QSA i PA-QSA.

Opublikowano w marcu 2019.

O COALFIRE

Coalfire to firma doradcza ds.cyberbezpieczeństwa, który pomaga organizacjom z sektora prywatnego i publicznego zapobiegać zagrożeniom, eliminować luki i skutecznie zarządzać ryzykiem. Zapewniając niezależne i dostosowane do potrzeb porady, oceny, testy techniczne i usługi w zakresie inżynierii cybernetycznej, pomagamy klientom w opracowywaniu skalowalnych programów, które poprawiają ich bezpieczeństwo, osiągają cele biznesowe i napędzają ich dalszy sukces. Coalfire jest liderem w dziedzinie cyberbezpieczeństwa od ponad 16 lat. Posiada biura w Stanach Zjednoczonych i Europie. Coalfire.com

Tłumaczenie: Łukasz Kuc (Net Complex) Kwiecień 2021