

Security Lifecycle Review

Czy wiesz, co znajduje się w Twojej sieci? Większość firm nie może obserwować wszystkich działań i urządzeń w swoich sieciach, co znacznie utrudnia wykrywanie zagrożeń. Narzędzie Security Lifecycle Review (SLR) umożliwia ocenę bezpieczeństwa aplikacji i urządzeń Internetu rzeczy (IoT), a także wykrywanie luk w zabezpieczeniach, zagrożeń i czynników ryzyka w środowisku informatycznym w sposób dostosowany do potrzeb każdej firmy. Gdy firma wie, gdzie znajdują się najbardziej ryzykowne elementy, może skupić się właśnie na nich, opracować plan działania i polepszyć skuteczność swoich zabezpieczeń.

Korzyści z rozwiązania SLR

- **Pełna widoczność sieci:** Firma widzi wszystkie aplikacje i urządzenia używane w sieci oraz wszelkie próby złamania zabezpieczeń swoich systemów.
- **Ryzyko określone ilościowo:** Firma może śmiało podejmować decyzje oparte na danych, ustalać priorytety oraz wdrażać odpowiednie działania związane z technologiami lub strategiami na podstawie wyciągniętych wniosków.
- **Oszczędność czasu:** W jednym raporcie znajdują się kluczowe czynniki ryzyka i zalecenia, co zapewnia oszczędność czasu, dzięki czemu zespół odpowiedzialny za bezpieczeństwo może lepiej skupić się na swoich najważniejszych zadaniach.

Czym jest SLR?

SLR to bezpłatne, wyspecjalizowane narzędzie do oceny ryzyka, które generuje sumaryczny raport zawierający takie dane, jak liczba i typy zagrożeń i luk w zabezpieczeniach wykrytych w sieci we wskazanym okresie. W raporcie tym znajdują się również zalecenia dotyczące zmniejszenia ryzyka i polepszenia stanu bezpieczeństwa.

Widoczność urządzeń IoT i związanego z nimi ryzyka	Ryzyko dotyczące aplikacji SaaS i innych aplikacji	Analiza zabezpieczeń DNS	Analiza aktywności związanej z adresami URL	Zagrożenia wg kraju docelowego
Luki w zabezpieczeniach aplikacji	Analiza zagrożeń	Analiza przesyłania plików	Analiza szkodliwego oprogramowania	Wykorzystana przepustowość

Rys. 1: Zawartość raportu SLR¹

Raport SLR można sporządzić podczas wstępnej oceny lub w ramach standardowej kontroli zabezpieczeń. Wyniki są oparte na danych zgromadzonych w okresie przeglądu (trwającym zwykle siedem dni), a proces ich generowania przebiega nieinwazyjnie.

Dlaczego warto stosować raport SLR?

Aby efektywnie zarządzać bezpieczeństwem sieci i wdrożyć niezawodny system zapobiegania włamaniom (IPS), przedsiębiorstwo musi mieć dogłębny wgląd w swoje środowisko informatyczne. Wszystkie zagrożenia muszą być regularnie oceniane w celu przypisania do nich odpowiedniego ryzyka. Efektywne zarządzanie priorytetami i zasobami umożliwia zmniejszenie tego ryzyka, opracowanie najskuteczniejszego systemu zabezpieczeń oraz zapobieganie atakom i przestojom w pracy.

Za pomocą narzędzia SLR można szybko i łatwo przeglądać aplikacje, zagrożenia i luki w zabezpieczeniach sieci. Raport zawiera szczegółowe informacje dotyczące aplikacji SaaS (ang. software-as-a-service - oprogramowanie jako usługa) i innych aplikacji, ruchu danych (w odniesieniu do adresów URL), typów treści, urządzeń IoT (zob. rys. 3) oraz znanych i nieznanymi zagrożeń penetrujących sieć (zob. rys. 4), wraz z zaleceniami dotyczącymi największych czynników ryzyka i obszarów priorytetowych, na których należy się skupić (zob. rys. 5).

Podsumowanie dla ACME

NAJWAŻNIEJSZE WNIOSKI

664 UŻYWANE APLIKACJE W sieci używane są 664 aplikacje, które mogą stwarzać ryzyko dotyczące bezpieczeństwa i problemy dla działalności firmy. Gdy przedsiębiorstwo nie ma kontroli nad funkcjami o znaczeniu nieważnym, pracownicy mogą używać aplikacji niezwiązanych z pracą, a hakerzy — wykorzystywać tę sytuację w celu włamania się do systemu i kradzieży danych.	130 APLIKACJE WYSOKIEGO RYZYKA Zaobserwowano 130 aplikacji wysokiego ryzyka, w tym aplikacji mogących wprowadzać lub ukrywać szkodliwe działania, wysłać pliki poza sieć lub nawiązywać nieautoryzowane połączenia.	211 APLIKACJE SaaS W sieci zaobserwowano 211 aplikacji SaaS. Aby utrzymać nad nimi kontrolę administracyjną, należy wdrażać takie aplikacje SaaS, które będą zarządzane przez zespół działu informatycznego.
121 744 EKSPLOITY WYKORZYSTUJĄCE LUKI W ZABEZPIECZENIACH W środowisku przedsiębiorstwa zaobserwowano łącznie 121 744 eksploity wykorzystujące luki w zabezpieczeniach, mające na celu doprowadzenie do wycieku informacji, wykonanie kodu lub stosowanie algorytmów sitowych.	123 285 ZAGROŻENIA ŁĄCZNIE W sieci wykryto łącznie 123 285 zagrożeń, w tym eksploity wykorzystujące luki w zabezpieczeniach, znane i nieznane szkodliwe oprogramowanie oraz aktywność mającą na celu wysyłanie informacji do serwerów sterowania i kontroli (C&C).	74 SZKODLIWE PROGRAMY W środowisku przedsiębiorstwa wykryto 60 znanych i 14 nieznanymi szkodliwych programów.

Rys. 2: Strona podsumowania raportu SLR

Strona podsumowania zawiera ogólny przegląd aplikacji i zagrożeń wykrytych w sieci przedsiębiorstwa.

1. Zwróć uwagę na wymagane subskrypcje.

Bezpieczeństwo IoT

środa, 1 stycznia 2020 r. – poniedziałek, 23 marca 2020 r.

Dzisiaj przedsiębiorstwa używają nie tylko tradycyjnych aplikacji i urządzeń informatycznych, lecz również urządzeń służących konkretnym celom, podłączonych do Internetu i usprawniających codzienne czynności, w tym urządzeń z zakresu technologii operacyjnych (OT) oraz urządzeń znanych powszechnie jako urządzenia Internetu rzeczy (IIoT). Urządzenia IIoT często stwarzają duże ryzyko dla przedsiębiorstw, ponieważ w odróżnieniu od rozwiązań informatycznych nie są objęte typowym procesem zarządzania cyklem życia (od wdrożenia poprzez bieżące utrzymanie po ostateczne wycofanie). Rozwiązanie Palo Alto Networks IoT Security wykorzystuje zaawansowane algorytmy uczenia maszynowego w celu wykrywania takich urządzeń i związanych z nimi czynników ryzyka oraz dostarczania zaleceń, które pomagają w ich lepszym zabezpieczeniu oraz koordynowaniu zarządzania ich cyklem życia.

NAJWAŻNIEJSZE WNIOSKI

574	4	12
WYKRYTE URZĄDZENIA IoT	ALERTY DOTYCZĄCE URZĄDZEŃ IoT	WYKRYTYCH LUK W ZABEZPIECZENIACH IoT
W sieci przedsiębiorstwa wykryto 574 urządzenia IoT. 110 z nich scharakteryzowano jako krytyczne, 130 – o dużym poziomie istotności, a 140 – o średnim poziomie istotności. Największe ryzyko dotyczy następujących profili urządzeń: Polycam IP Phone (153), Aruba Instant AccessPoint (107), Polycam Device (104), Polycam Video Conferencing Device (111) i Avaya IP Phone (131).	W sieci wykryto 4 alerty: 1 o znaczeniu krytycznym, 1 o wysokim poziomie istotności i 1 o średnim poziomie istotności. Najczęstsze typy alertów: nieprawidłowe zachowanie (4).	W sieci wykryto 12 luk w zabezpieczeniach, z czego 3 zostały potwierdzone (w tym 2 o znaczeniu krytycznym i 1 o średnim poziomie istotności), podczas gdy 9 to potencjalne luki w zabezpieczeniach (w tym 4 o znaczeniu krytycznym, 1 o wysokim poziomie istotności i 2 o średnim poziomie istotności).

Rys. 3: Sekcja „Bezpieczeństwo IoT”

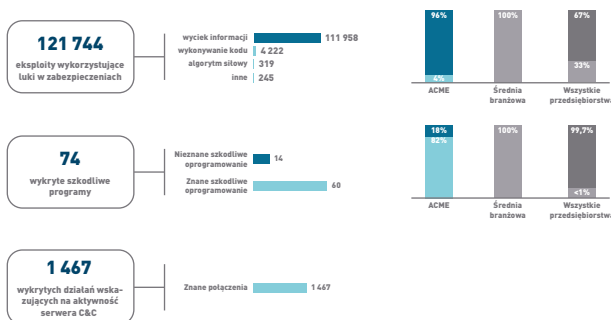
Sekcja ta zapewniła znakomitą widoczność urządzeń IoT uszeregowanych według ryzyka. Dzięki temu firma może efektywniej zarządzać bezpieczeństwem urządzeń IoT przez cały cykl ich eksploatacji.

Przegląd zagrożeń

Aby dobrze poznać czynniki ryzyka i dowiedzieć się, jak skorygować swój system zabezpieczeń w celu zapobieżenia atakom, firma musi dysponować informacjami o rodzajach i rozmiarach zagrożeń. W tej sekcji znajdują się szczegółowe informacje o zaobserwowanych w sieci lukach w zabezpieczeniach aplikacji, znanym i nieznanym szkodliwym oprogramowaniu oraz komunikacji z serwerami C&C.

NAJWAŻNIEJSZE WNIOSKI

- W sieci przedsiębiorstwa zaobserwowano łącznie 121 744 eksploity wykorzystujące luki w zabezpieczeniach, mające na celu doprowadzenie do wycieku informacji, wykonanie kodu lub stosowanie algorytmów silowych.
- Zaobserwowano 74 szkodliwe programy w porównaniu ze średnią dla podobnych przedsiębiorstw w branży wynoszącą 0.
- Wykryto łącznie 1467 żądań serwera C&C, wskazujących na próby skomunikowania się z cyberprzestępcami przez szkodliwe oprogramowanie w celu pobrania dodatkowego szkodliwego oprogramowania, otrzymania instrukcji lub wydobycia danych.



Rys. 4: Sekcja „Przegląd zagrożeń”

W sekcji „Przegląd zagrożeń” można znaleźć informacje o rodzajach i skali ataków wymierzonych przeciwko firmie, takich jak znane i nieznane szkodliwe oprogramowanie, aktywność serwerów C&C oraz luki w zabezpieczeniach aplikacji.

ZALECENIA

- Wprowadź reguły korzystania z aplikacji. Zezwalaj na używanie wyłącznie aplikacji potrzebnych do pracy, a w odniesieniu do wszelkich pozostałych stosuj szczegółowe procedury kontrolne.
- Podjęj działania w związku z aplikacjami wysokiego ryzyka, które mogą zostać wykorzystane w celach niezgodnych z prawem, takimi jak aplikacje zapewniające zdalny dostęp, aplikacje do udostępniania plików lub zaszyfrowane tunele.
- Podjęj działania dotyczące komunikacji z serwerem C&C. Przeanalizuj w tym celu źródło powiązane z siecią lub hostem. Pomocne mogą być rozwiązania do wykrywania takich incydentów i reagowania na nie lub ich rejestrowania.
- W celu zmniejszenia ryzyka ataków zastosuj rozwiązanie zabezpieczające, które może wykrywać znane i nieznane zagrożenia oraz zapobiegać im.
- Zastosuj rozwiązanie, które może się automatycznie przeprogramowywać, oraz inne produkty zabezpieczające w celu utworzenia i skoordynowania nowego systemu zabezpieczeń przed nowymi zagrożeniami, wykorzystując dane pochodzące od globalnej społeczności użytkowników korporacyjnych.
- Wprowadź reguły zarządzania hostami, które ograniczają wektory ataków bezpołkowych i zmniejszają ryzyko ataków opartych na serwerach C&C dzięki udostępnianiu w czasie zbliżonym do rzeczywistego informacji o zagrożeniach obejmujących wszystkie produkty zabezpieczające.
- W przypadku wycieku urządzeń IoT należy rozważyć następujące działania:
 - Przegląd czynników ryzyka związanych z tymi urządzeniami.
 - Rozwiązanie lub ograniczenie znanych problemów poprzez modyfikację konfiguracji urządzeń, aktualizację jego oprogramowania lub zainstalowanie w nim poprawek zabezpieczających.
 - Ograniczenie obszaru narażonego na ataki poprzez zastosowanie zaleceń opartych na regulacjach.
 - Segmentowanie urządzeń w celu zablokowania, ograniczenia lub spowolnienia ataków.

Rys. 5: Sekcja „Zalecenia”

Ostatnia sekcja raportu SLR podsumowuje najważniejsze wnioski i zawiera zalecenia dotyczące działań, jakie należy podjąć w odniesieniu do najważniejszych wykrytych czynników ryzyka.

Często zadawane pytania (FAQ)

Jak uruchomić narzędzie SLR?

Samoobsługowe narzędzie SLR jest dostępne w [Portalu Wsparcia Klienta](#). Jeśli potrzebujesz pomocy, skontaktuj się z przedstawicielem handlowym. Narzędzie SLR jest również dostępne jako [aplikacja w chmurze](#).

Nie jestem klientem Palo Alto Networks. Czy mogę korzystać z narzędzia SLR?

Tak! Skontaktuj się z lokalnym przedstawicielem handlowym lub [zamów SLR przez Internet](#).

Aby przeprowadzić analizę bezpieczeństwa sieci SLR w Twojej firmie, możemy uruchomić narzędzie SLR w jej środowisku. Proces ten przebiega nieinwazyjnie. Narzędzie SLR można uruchomić dla wirtualnej lub fizycznej zapory sieciowej.

Jak często należy przeprowadzać analizę bezpieczeństwa sieci SLR?

Klienci Palo Alto Networks mogą przeprowadzać analizę SLR na żądanie, tak często, jak jest to potrzebne. Zalecamy regularne przeprowadzanie analizy bezpieczeństwa za pomocą narzędzia SLR co najmniej raz na 90 dni lub po wprowadzeniu każdej istotnej zmiany w sieci.

Czy mogę wygenerować jeden raport SLR obejmujący wiele urządzeń?

Tak, funkcja łączenia zrzutów statystyk umożliwia wysyłanie plików z takimi zrzutami z wielu urządzeń w celu wygenerowania zbiorczego raportu SLR.

Dodatkowe zasoby

- Czy masz inne pytania? Odwiedź nasz [Portal Wsparcia Klienta](#).
- Możemy zacząć? Odwiedź naszą stronę i zamów raport SLR <https://start.paloaltonetworks.com/security-lifecycle-review-risk-assessment.html>
- Używasz narzędzia SLR sterowanego przez klienta? Przeczytaj naszą instrukcję „[Szybki start](#)” dla narzędzia SLR.
- Potrzebujesz pomocy w obsłudze aplikacji SLR? Przeczytaj naszą [dokumentację techniczną](#).

Subskrypcje wymagane w powiązaniu z narzędziem SLR

Aby uzyskać najbardziej kompleksowy widok swojego środowiska, firma potrzebuje subskrypcji następujących usług:

- Ogólne:** WildFire, filtrowanie adresów URL, przeciwdziałanie zagrożeniom
- Sekcja IoT:** Cortex™ Data Lake i aktywna instancja IoT Security
- Sekcja DNS:** DNS Security

Informacje o firmie Palo Alto Networks

Palo Alto Networks, lider światowego rynku cyberbezpieczeństwa, kształtuje przyszłość ukierunkowaną na rozwiązania chmurowe dzięki technologiom zmieniającym sposób działania użytkowników i przedsiębiorstw. Pragniemy stać się preferowanym przez klientów partnerem w dziedzinie cyberbezpieczeństwa, dbającym o ochronę cyfrowego środowiska. Pomagamy zmierzyć się z najtrudniejszymi wyzwaniami, nieustannie tworząc innowacyjne rozwiązania oparte na najnowszych osiągnięciach w obszarze sztucznej inteligencji, analizy danych, automatyzacji i koordynacji procesów. Oferujemy zintegrowaną platformę zabezpieczeń i wspieramy działania coraz większej sieci partnerów. Zajmujemy wyjątkową pozycję na rynku: zapewniamy bezpieczeństwo dziesiątkom tysięcy przedsiębiorstw i instytucji korzystających z różnych chmur, sieci i urządzeń mobilnych. „Nasza wizja to świat, w którym każdy dzień jest bezpieczniejszy i pewniejszy niż poprzedni”. Więcej informacji można znaleźć na stronie www.paloaltonetworks.com.



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2020 Palo Alto Networks, Inc. Palo Alto Networks jest zastrzeżonym znakiem towarowym firmy Palo Alto Networks. Listę znaków towarowych Palo Alto Networks opublikowano na stronie <https://www.paloaltonetworks.com/company/trademarks.html>. Wszelkie inne znaki użyte w niniejszym dokumencie mogą być znakami towarowymi odpowiednich firm. security-lifecycle-ds-072420