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?

SRL 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 bezpieczeniach aplikacji	Analiza zagrożeń	Analiza przesyłania plików	Analiza szkodliwego oprgramowania	Wykorzystana przepustowość

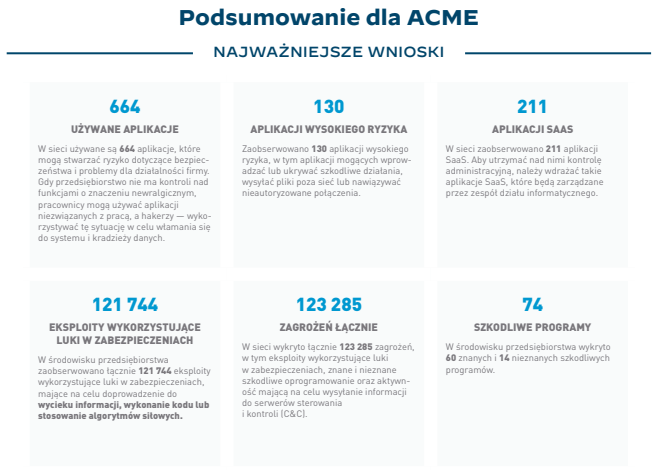
Rys. 1: Zawartość raportu SLR[1]

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 nieznanych zagrożeń penetrujących sieć (zob. rys. 4), wraz z zaleceniami dotyczącymi największych czynników ryzyka i obszarów priorytetowych, na których należy się skupić (zob. rys. 5).



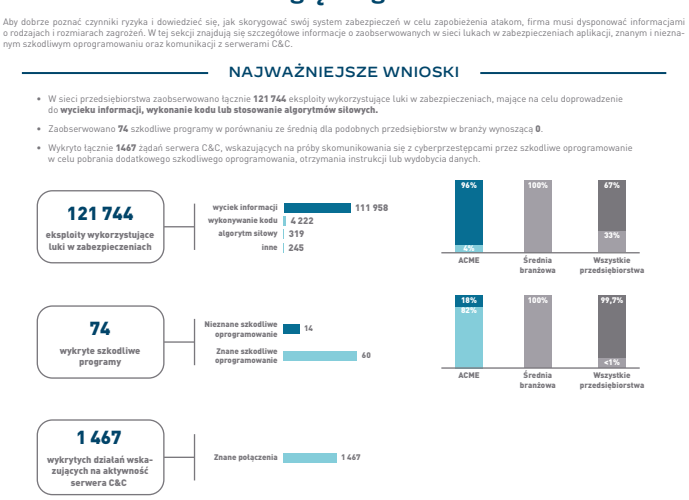
Rys. 2: Strona podsumowania raportu SLR

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

1. Zwróć uwagę na wymagane subskrypcje.

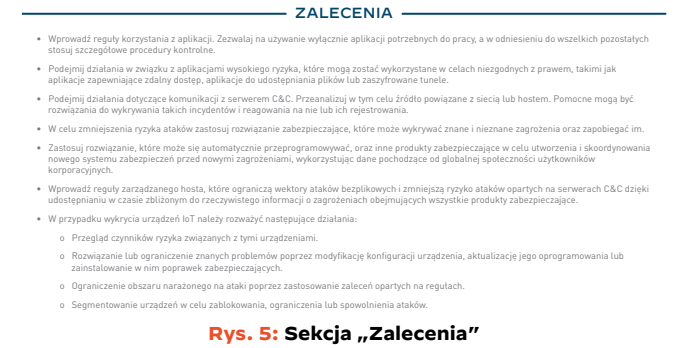
Rys. 3: Sekcja „Bezpieczeństwo IoT"

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



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.



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 z 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 SRL 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 zaczynać? 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 cyberzabezpieczeń, 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.

paloalto NETWORKS
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