Security Lifecycle Review

Skutečně víte, co se děje ve vaší síti? Většina společností postrádá ucelený přehled o aktivitách a zařízeních ve svých sítích, takže jsou v naprosté nevědomosti o bezpečnostních rizicích. Služba Security Lifecycle Review (SLR) poskytuje individuální bezpečnostní posouzení aplikací, IoT zařízení (internetu věcí), bezpečnostních slabin, hrozeb a rizik ve vašem prostředí. Jakmile máte představu o tom, kde jsou největší rizika, můžete určit, na co se soustředit, vypracovat akční plán a upevnit svou bezpečnostní pozici.

Přínosy služby SLR

- **Ucelený přehled:** Uvidíte, jak se protivníci snaží narušit vaši obranu, jaké různé aplikace se ve vaší síti používají a jaká všechna zařízení jsou k síti připojená.
- **Kvantifikované riziko:** Můžete s jistotou dělat rozhodnutí podložená daty, priorizovat a na základě získaných poznatků implementovat patřičné zásady nebo provést technologické kroky.
- **Úspora času:** Jediná sestava shrnuje klíčová rizika a doporučení, aby se vaše bezpečnostní týmy mohly soustředit na hlavní priority.

Co je SLR?

Cílené, bezplatné posouzení bezpečnostních rizik. Výsledkem SLR je zpráva, která shrnuje objem a typy hrozeb, jimž je síť vystavena, a slabin identifikovaných v síti za určené časové období. Zahrnuje taky doporučení, jak omezit celkovou rizikovou expozici a zlepšit bezpečnostní pozici.

Přehled o IoT zařízeních a souvisejících rizicích	Rizika související s SaaS a dalšími aplikacemi	DNS Analýza zabezpečení	URL Analýza aktivity	Hrozby podle cílové země
Slabiny aplikací	Analýza hrozeb	Analýza přenosů souborů	Analýza malwaru	Spotřebovaná šířka pásma

Obrázek 1: Zjištění ve vaší zprávě SLR[1]

SLR se dá provést při prvotním posouzení nebo v rámci pravidelné bezpečnostní kontroly. Zjištění vycházejí z dat shromážděných za sledované období (obvykle sedm dnů), přičemž data se shromažďují neintruzivně.

Proč provést SLR?

Pro účinnou správu zabezpečení sítě a robustní systém prevence narušení (IPS) potřebujete hluboký vhled do prostředí své organizace. Všechny hrozby by se měly pravidelně vyhodnocovat a měla by se jim přiřazovat relativní rizika. Pak budete moct s ohledem na tato rizika efektivně spravovat priority a zdroje, vytvořit pevnou bezpečnostní pozici a účinně bránit narušením provozu a útokům.

SLR je rychlý a jednoduchý způsob, jak si udělat představu o aplikacích, hrozbách a slabinách v síti. Zpráva uvádí podrobnosti o softwaru používaném jako služba (SaaS) a dalších aplikacích, o provozu vzhledem k URL, o typech obsahu, IoT zařízeních (viz obrázek 3) a o známých i neznámých hrozbách vstupujících do vaší sítě (viz obrázek 4). Nechybí ani doporučení ohledně největších rizik a oblastí, na které je potřeba se prioritně zaměřit (viz obrázek 5).

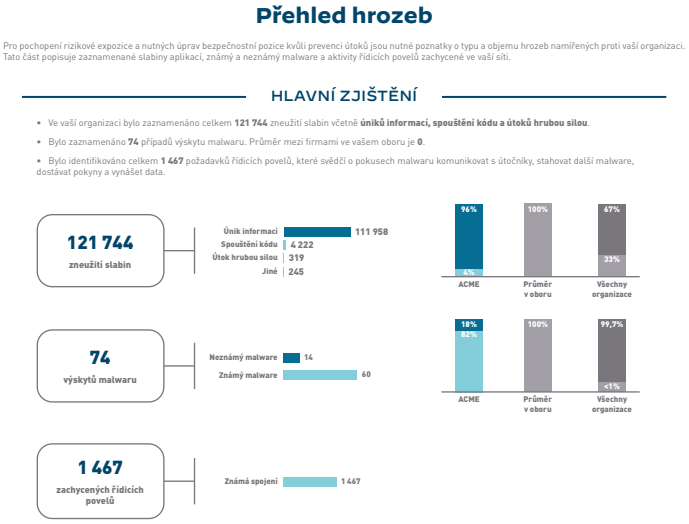
Obrázek 2: Stručné shrnutí SLR

Stručné shrnutí poskytuje vysokoúrovňový přehled o aplikacích a hrozbách zaznamenaných v síti.

1. Vyžaduje určitá předplatná.

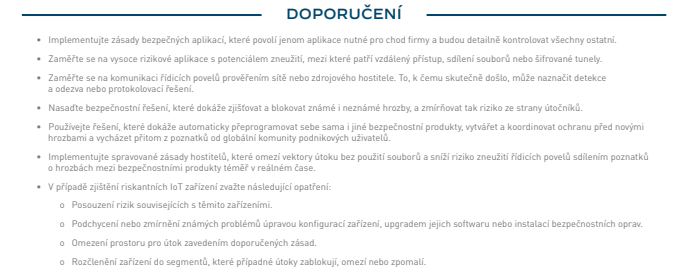
Obrázek 3: Část „Zabezpečení IoT"

Část „Zabezpečení IoT" poskytuje špičkový přehled a priorizaci rizik souvisejících s IoT zařízeními, abyste mohli lépe spravovat zabezpečení IoT v průběhu celého životního cyklu zařízení.



Obrázek 4: Část „Přehled hrozeb"

Část Přehled hrozeb uvádí typy a objem hrozeb namířených proti vaší organizaci včetně známého a neznámého malwaru, neoprávněných řídicích povelů a slabin aplikací.



Obrázek 5: Část „Doporučení"

Poslední část zprávy SLR shrnuje klíčová zjištění a poskytuje doporučení, jak může vaše organizace zareagovat na největší zjištěná rizika.

Nejčastější otázky (FAQ)

Jak můžu SLR spustit?
K samoobslužnému spuštění SLR se dostanete na Portálu zákaznické podpory. Pokud potřebujete pomoc, obraťte se na svého obchodního zástupce. SLR je rovněž k dispozici jako aplikace poskytovaná v cloudu.

Nejsem zákazník Palo Alto Networks. Můžu spustit SLR?
Ano! Obraťte se na místního obchodního zástupce nebo si vyžádejte SLR online.
Zprávu SLR pro vaši organizaci vypracujeme spuštěním SLR ve vašem prostředí. Jedná se o neintruzivní proces. SLR se dá spustit na virtuálním i fyzickém firewallu.

Jak často mám SLR spouštět?
Zákazníci Palo Alto Networks můžou spouštět SLR na vyžádání tak často, jak potřebují. Doporučujeme pravidelně vyhodnocovat bezpečnostní rizika spouštěním SLR přinejmenším každých 90 dní nebo vždycky, kdy ve vaší síti došlo k podstatné změně.

Můžu získat jednu zprávu SLR pro několik zařízení?
Ano, funkce multi-statsdump merge umožňuje nahrát soubory statsdump z několika zařízení a vygenerovat souhrnnou zprávu SLR.

Další zdroje

- Další otázky? Navštivte náš Portál zákaznické podpory.
- Chcete začít? Navštivte nás online a vyžádejte si SLR https://start.paloaltonetworks.com/security-lifecycle- review-risk-assessment.html
- Spouštíte SLR sami? Přečtěte si náš stručný návod SLR QuickStart Guide.
- Potřebujete s aplikací SLR poradit? Přečtěte si technickou dokumentaci.

Předplatná, která jsou nutná pro SLR

Pro nejucelenější přehled o svém prostředí budete potřebovat:

- **Obecné:** Předplatná WildFire, URL Filtering, Threat Prevention
- **Část IoT:** Předplatné Cortex™ Data Lake a aktivní instance IoT Security
- **Část DNS:** Předplatné DNS Security

O společnosti Palo Alto Networks

Palo Alto Networks, globální lídr na poli kybernetického zabezpečení, utváří budoucnost postavenou na cloudech technologiemi, které proměňují způsob fungování lidí a organizací. Naším posláním je coby preferovaný partner pro kybernetické zabezpečení chránit náš způsob života v digitálním věku. Pomáháme řešit největší bezpečnostní výzvy světa inovacemi, které staví na nejnovějších objevech v oblasti umělé inteligence, analytiky, automatizace a koordinace. Poskytováním integrované platformy a podporou rostoucího ekosystému partnerů jsme v popředí ochrany cloudů, sítí a mobilních zařízení tisíců organizací. Jde nám o to, aby den ode dne bylo na světě bezpečněji. Další informace najdete na webu 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