ARICOMA

Logger a jeho výhody

Systém pro Log management přináší řadu řešení pro výzvy, které souvisí s legislativními požadavky, ochranou infrastruktury, a dalšími aspekty provozu IT ve firmách. Tyto systémy jsou klíčové pro efektivní správu, sledování a analýzu logů (záznamů) generovaných různými zařízeními a aplikacemi.

Hlavní výhody systému pro Log management

Centralizuje logy z mnoha zdrojů, včetně serverů, aplikací a síťových zařízení, do jedné platformy. Toto umožňuje IT týmům mít kompletní a integrovaný pohled na všechna logová data, což usnadňuje jejich analýzu a správu. Centralizace dat také výrazně zlepšuje dohledatelnost událostí a incidentů v síti.

Analýza logů může odhalit problémy v konfiguraci systémů, chyby v aplikacích nebo přetížení infrastruktury. Log management pomáhá identifikovat a řešit tyto problémy, což vede ke zvýšení efektivity a stabilitě IT prostředí.

Sběr logů poskytuje rozsáhlé možnosti vyhledávání a analýzy, včetně full-textového vyhledávání, grafické prezentace dat, a tvorby komplexních dotazů. To umožňuje rychle nalézt specifické informace a získat hlubší porozumění o událostech v síti.

Naše řešení Logger představuje pokročilé řešení Log managementu určené především pro malé a střední podniky a instituce. Je založeno na open-source platformách Wazuh a OpenSearch, které byly speciálně přizpůsobené pro potřeby efektivního a dlouhodobého ukládání logů z rozmanitých infrastrukturních zdrojů.

Řešení **Logger** poskytuje přehled o chování IT systémů jako celku a manažerům i správcům **umožňuje sledovat a vyhodnocovat** okamžitý stav i historický vývoj a odhadovat trendy. Je navrženo pro snadnou integraci se Security Operations Centers (SOC), což zvyšuje jeho využitelnost a přispívá ke zvýšení úrovně zabezpečení IT prostředí.

Řešení Logger nabízí **komplexní služby** v oblasti sběru, analýzy a archivace logů s rozšířenými bezpečnostními funkcemi **pro pokročilý monitoring a ochranu**. Logger překonává tradiční řešení Log managementu díky své škálovatelnosti a integraci mnoha SIEM funkcí, jako jsou skenování zranitelností, systémové kontroly (SCA) a detekce příčných hrozeb (XDR).

Naše řešení Logger **je navrženo tak, aby splňovalo různé požadavky na výkon**. Díky variantnímu řešení, dokážeme rozsah nasazení a funkcionalit přizpůsobit objemu sledovaných zdrojů, jako jsou agenti a síťové prvky. To umožňuje zajistit efektivní zpracování a analýzu rozsáhlých datových toků.

Na běžném serverovém hardware může Logger zpracovat **až 1000 událostí za sekundu (EPS) a 5000 toků (Flow) za minutu**. Jde o ideální nasazení pro organizace, které potřebují robustní řešení pro monitorování a analýzu své síťové infrastruktury a zajištění bezpečnosti dat.

Vhodný hardware a konfiguraci systému navrhujeme tak, aby poskytovala maximální efektivitu při sledování stanoveného počtu zdrojů. To zákazníkům umožňuje volbu konfigurace, která nejlépe odpovídá jejich specifickým potřebám a možnostem. Logger poskytuje **flexibilní a škálovatelné řešení,** které lze efektivně implementovat v různých provozních prostředích.

Technické specifikace

- Sběr logů probíhá pomocí protokolů Syslog, TCP/UDP, HTTP, HTTPS, JSON. Systém dokáže zpracovat i mnoho dalších.
- Podpora Netflow v1,5,6,7,9
- Systém podporuje velké množství zdrojů například: REST API, textové soubory, Radius, Active Directory, MS SQL databáze, Windows Event Log (včetně rozšířených možnosti), syslog, netflow, SNMP trap, Office365, Windows Sysmon (sledování řádkových příkazů (CMD, powershell, terminal apod.), vytváření procesů, změny registrů, souborů, detekce síťové komunikace, DNS překladů a další operačního částí systému)
- Sběr logů může v případě podporovaných zdrojů probíhat šifrovaně za pomocí SSL nebo TLS.
- Pro standardně nepodporované zdroje umožňuje řešení Logger vytvářet vlastní dekodéry, které se starají o normalizaci příchozích dat (zdrojová ip = srcip, jmeno = username, …). Díky interaktivnímu testovacímu nástroji je možné online testovat funkčnost dekodéru za pomocí vzorku příchozího logu.
- Příchozí logy je možné obohatit o statické nebo dynamické informace, například o geolokaci IP adresy.
- Naše řešení je vybudováno na systému Wazuh a OpenSearch, jejichž předností je možnost širokých uživatelských úprav a přizpůsobení pracovního prostředí (dashboardu) a jednoduché intuitivní ovládání s podporou moderních webových prohlížečů (Chrome, Edge, Safari, Firefox a dalších). Zákazníkům nabízíme mnoho předpřipravených dashboardů například Active Directory, firewall a další. Uživatelské dashboardy mohou obsahovat mapy, grafy, histogramy i strukturované tabulky.
- Díky databázi postavené na OpenSearch (která je součástí systému) je vyhledávání napříč všemi daty, které jsou za pomocí dekodéru efektivně normalizované (např. zdrojová IP adresa, cílová IP adresa), rychlé, intuitivní a díky využití dotazovacího jazyka, také velmi efektivní a jednoduché.
- Pro větší přehlednost je možné informace ze všech zdrojů sdružovat do datových sad, které za pomocí logických podmínek vytváří pravidla pro korelace, alarmy, dashboardy, a integrace do dalších systémů, které umožňují dále data zpracovávat například v tiketovacích systémech.
- Logger obsahuje rozšířenou předpřipravenou sadu korelačních pravidel a alarmů, které umožňují upozornit na překročení nastavených hodnot, pokud základní pravidla nestačí. Uživatelská pravidla na základě přání zákazníka jsou samozřejmostí.
- Za pomocí agenta pro Windows, Linux a MacOS je možné provádět sběr informací o instalovaných aplikacích, aktualizacích a nastaveních systému. Tak dokáže Logger zranitelnosti a konfigurační chyby nejen detekovat, ale také o nich zákazníka notifikovat a nabídnout postup pro řešení.
- Agent také dokáže plnit roli základního kontrolního prvku ochrany proti rootkitům, malware a neobvyklému chování. Nenahrazuje specializované anti-X řešení.
- Pro další možné využití a zpracování uložených i vyhledaných informací je možné využít export dat do CSV.
- Nasazení Loggru je podporováno pro Virtualizace na Hyper-V, nebo VMware.
- Uživatele je možné ověřovat lokálně nebo s využitím integrace s Active Directory, s granulárním nastavením pro různé role.