LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

LOGmanager - POC

Integralną częścią każdego procesu zakupowego LOGmanagera są testy funkcjonalności produktu – zwane inaczej PoC (Proof of Concept). Testy umożliwiają weryfikację działania systemu LOGmanager w środowisku produkcyjnym, najczęściej w kontekście specyficznych problemów danej infrastruktury i potwierdzenie przydatności produktu do realizacji zadania zarządzania logami. Warto mieć na uwadze, że PoC z założenia pokrywa jedynie wybrane use-case'y klienta (zazwyczaj do 5ciu) i w żaden sposób nie może zastąpić pełnego wdrożenia LOGmanagera.

PoC jest realizowane przez certyfikowanego partnera systemu LOGmanager, zazwyczaj przy wsparciu inżyniera producenta.

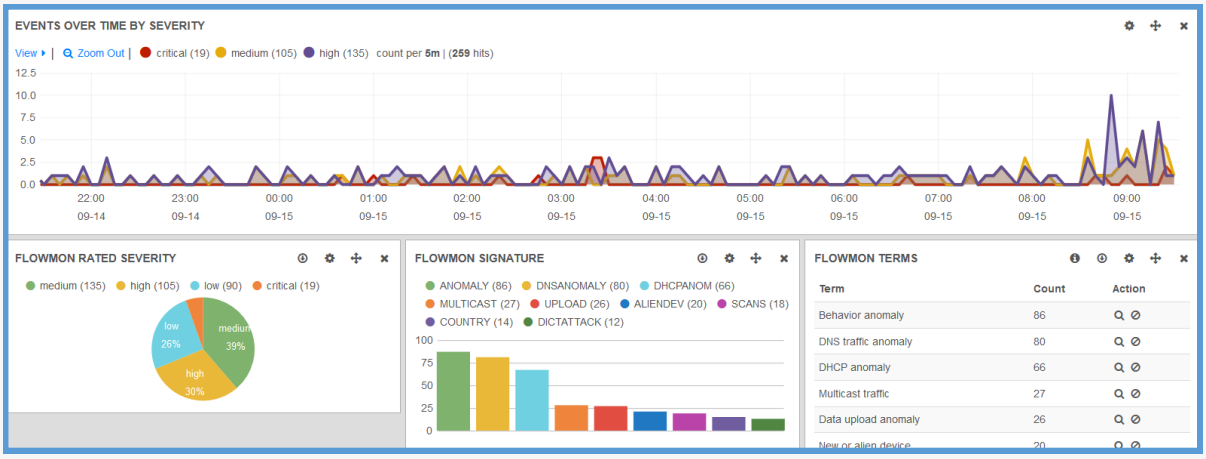
Broszura w szczegółach definiuje pojedyncze kroki które powinny być wykonane, aby przeprowadzić udane PoC – w tym odpowiedzialności każdej zainteresowanej strony, harmonogram oraz check-listę instalacyjną.

Wywiad Techniczny

Jak sugeruje nazwa, celem PoC jest udowodnienie konceptu, rozumianego jako użyteczność systemu do realizacji funkcjonalności zarządzania logami. Ponieważ jest to skomplikowany temat zahaczający o wiele różnych obszarów IT, **podstawowe wymagania które produkt powinien spełnić muszą być uzgodnione i zaakceptowane przez każdą ze stron przed rozpoczęciem PoC. Rozpoczynanie testów bez wcześniejszego ustalenia konkretnego celu, może doprowadzić do zakończenia projektu z negatywnym wynikiem.**

Poniżej znajduje się lista pytań mających na celu lepsze zrozumienie wymagań klienta w kontekście zarządzania logami:

1. Cele/Zadania – Co starasz się osiągnąć? Jaki jest główny powód rozważania zakupu rozwiązania SEM/SIEM?
2. Krytyczność – Czy problem który starasz się rozwiązać jest nagły, w takim sensie że każdy moment zwłoki jest dla Ciebie kosztowny?
3. Sukces – Jak zamierzasz mierzyć sukces testów? Czy było to do tej pory rozważane?
4. Wymagania – Czy masz jakieś specyficzne wymagania co do rozwiązania - ograniczenia wynikające z prawa, regulacji, polityk?
5. Funkcjonalności – Jakie funkcjonalności najbardziej Cię interesują – przykładowo: raportowanie, alertowanie, korelacje, szybkie wyszukiwanie danych, wizualizacje?
6. Konkurencja – Czy masz doświadczenie z innymi rozwiązaniami do zarządzania logami? Czy testowałeś inne produkty ale ostatecznie stwierdziłeś, że nie są dla Ciebie? Czy planujesz testować inne produkty?



Harmonogram

Testy PoC rozwiązania LOGmanager zazwyczaj trwają minimum 2 tygodnie. Każde PoC jest inne, toteż ciężko zdefiniować dokładne kroki, niemniej jednak z dotychczasowych doświadczeń wynika, że poniższy harmonogram sprawdza się najlepiej:

Faza przygotowania:

1. Wywiad techniczny – 30min max – rozpoznanie głównych problemów i potrzeb z zakresu zarządzania logami.
2. Prezentacja LOGmanager/demo – 1 do 2 godzin – przegląd najważniejszych funkcjonalności produktu w kontekście wcześniejszego wywiadu.
3. Wymiarowanie środowiska i oferta – utworzenie oferty w oparciu o wymiarowanie środowiska. Celem jest upewnienie się, że klient dysponuje wystarczającym budżetem na zakup rozwiązania.
4. Spotkanie przygotowawcze – 30min – celem spotkania jest ostateczne zdefiniowane kryteriów sukcesu dla PoC.

Faza PoC:

1. Instalacja – 2 do 3 godzin – instalacja rozwiązania demo w środowisku klienta i konfiguracja wybranych źródeł danych.
2. Tuning – 1 do 2 godzin – podłączenie kolejnych źródeł. Konfiguracja funkcjonalności wymaganych przez klienta (na przykład alertowanie, dashboardy, raporty).
3. Kolejne spotkania zgodnie z potrzebami. Ciągły nadzór nad postępami PoC.
4. Podsumowanie – 1 do 2 godzin – przegląd zebranych danych, prezentacja realizacji głównych celów uzgodnionych z klientem.

Odpowiedzialności

Aby testy PoC zakończyły się sukcesem każda zaangażowana strona podlega pewnym odpowiedzialnościom, które powinna spełnić.

Poniżej opisane zostały wymagania w stosunku do każdej ze stron:

Klient:

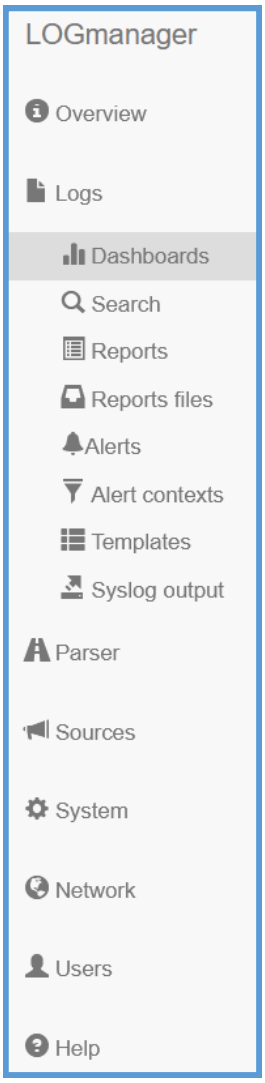
- Definicja głównych celów PoC (wspólnie z Inżynierem producenta/partnera).
- **Dostarczenie jasno zdefiniowanych kryteriów sukcesu dla PoC.**
- **Aktywne uczestnictwo w wywiadzie technicznym.**
- Wyznaczenie inżyniera odpowiedzialnego za nadzór nad postępami PoC w kontekście wcześniejszych ustaleń.
- Wypełnienie listy wymagań instalacyjnych.
- Wypełnienie dokumentu wymiarującego, zapewnienie dostępności budżetu na podstawie otrzymanej oferty.
- W przypadku PoC odbywającego się on-site, zapewnienie oddzielnego pomieszczenia do każdego spotkania PoC.

Partner:

- **Wsparcie klienta w definicji celów PoC oraz kryteriów sukcesu.**
- Wyznaczenie inżyniera odpowiedzialnego za prowadzenie PoC w kontekście wcześniejszych ustaleń.
- Przygotowanie oferty w oparciu o wymiarowanie środowiska.
- Koordynacja komunikacji pomiędzy stronami.

Inżynier partnera lub producenta:

- Instalacja rozwiązania.
- Konfiguracja rozwiązania w zgodzie z wymaganiami.
- Wsparcie inżyniera klienta w obsłudze produktu, przekazanie podstawowej wiedzy o produkcie.
- Rozwiązywanie bieżących problemów, odpowiadanie na techniczne pytania.
- Utworzenie pisemnego podsumowania PoC.
- Po zakończeniu PoC – wyczyszczenie produktu z danych klienta.



Wymagania instalacyjne

Poniższa lista definiuje dane potrzebne do przeprowadzenia szybkiej i bezproblemowej instalacji. Dołączony do tego dokumentu jest arkusz Excel, który powinien zostać wypełniony przez klienta i dostarczony do Inżyniera odpowiedzialnego za prowadzenie PoC przed rozpoczęciem testów.

1. **Lista źródeł danych które mają być zbierane przez LOGmanagera, w tym:** Typ źródła (nazwa producenta, funkcja systemu, wersja oprogramowania); IP źródła; Port docelowy na który wysyłane będą logi; Przewidywana ilość logów z systemu (mało, średnio, dużo);
2. **Dane sieciowe potrzebne do wdrożenia systemu:** Adres IP; Maska podsieci; Brama domyślna; Podstawowy DNS; Zapasowy DNA; Server/y NTP;
3. **Dane przekaźnika SMTP (potrzebne do wysyłania alertów bezpieczeństwa i systemu):** Adres IP/Nazwa hosta; Port; Źródłowy adres email (adres email widoczny jako nadawca wiadomości – pole FROM); Login/hasło, jeżeli przekaźnik SMTP wymaga podania poświadczeń; Adres email administratora (adres email na który LOGmanager będzie wysyłał powiadomienia o problemach operacyjnych, takich jak kończące się miejsce w buforze);
4. **W przypadku potrzeby integracji z LDAP:** Adres IP serwera LDAP; Adres IP zapasowego serwera LDAP; Port; Podstawowa struktura, np.: DC=test,DC=example,DC=com; Sufiks, e.g.: @test.example.com; Login/hasło dostępowe; Lista grup uprzywilejowanych które mają mieć dostęp do systemu;
5. **W przypadku wykorzystania agenta WES**: Skonfigurowany Rekord DNS SRV zgodnie z dokumentacją: (https://doc.logmanager.cz/manual/3.5.2/en/devices/microsoft-windows-event-sender.html)

Wymagania fizyczne

1. PoC realizowane jest na platformie demo, wykorzystującej PC Intel NUC (115mm x 111mm x 48.7mm). Wymagania co do miejsca to niewielka płaska przestrzeń oraz pojedyncze źródło zasilania, najlepiej podłączone do UPSa.
2. Połączenie ethernet – 100/1000Base-T w VLANie przeznaczonym do transferu logów. Dostęp do Internetu na czas trwania PoC nie jest wymagany, ale zdalny dostęp do rozwiązania dla inżyniera odpowiedzialnego za testy jest mile widziany.

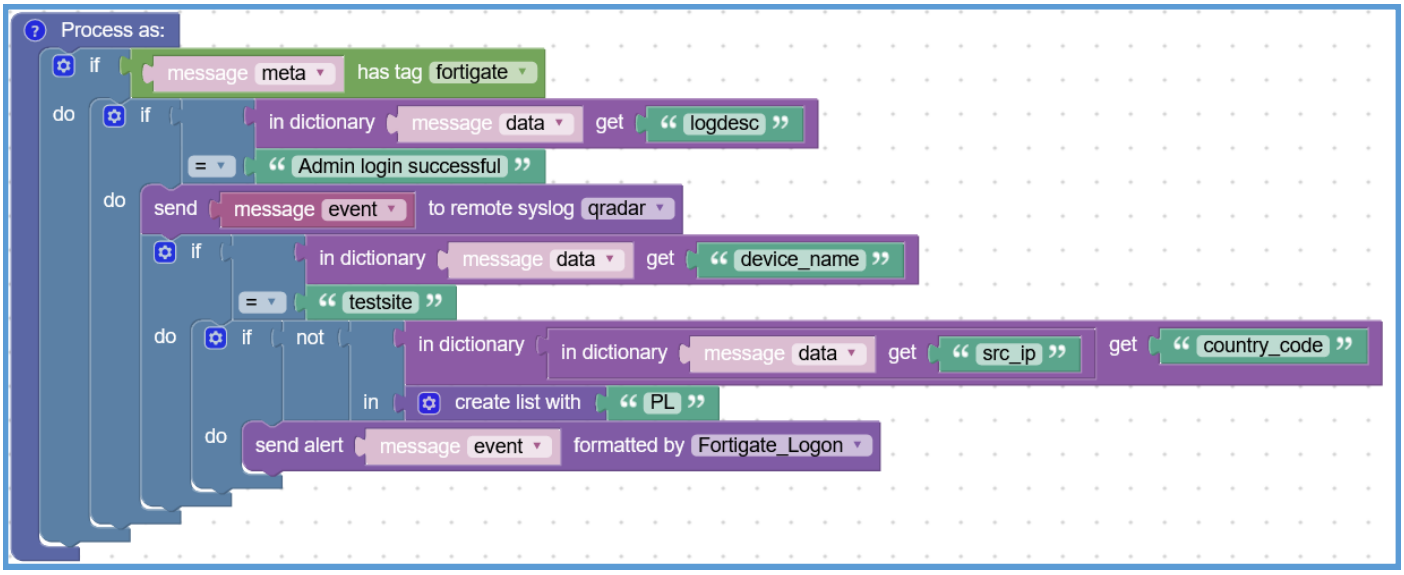
Check-lista instalacyjna

Instalacja rozwiązania LOGmanager na testy obejmuje uruchomienie rozwiązania w środowisku IT klienta i konfigurację zgodnie z wymaganiami. Czas potrzebny na instalację rozwiązania zależy od środowiska i wymagań klienta, ale zazwyczaj nie przekracza 3 godzin.

1. **Podstawowa konfiguracja:**
    - Podłączenie rozwiązania demo do sieci poprzez skonfigurowanie podstawowego interfejsu (Adres IP, Maska, Brama, DNS, NTP)
    - Sprawdzenie dostępności GUI.
    - Sprawdzenie dostępności serwera aktualizacji, sprawdzenie wersji LOGmanagera i aktualizacja do najnowszej (jeżeli wymagane).
    - Wyłączenie wysyłania telemetrii do producenta.
    - Konfiguracja SMTP i test wysyłania wiadomości.
    - Opcjonalnie:
        - Utworzenie grup użytkowników i praw dostępu do rozwiązania (lokalnie bądź za pomocą AD/LDAP).
        - W przypadku planowanego wykorzystania agenta WES, konfiguracja rekordu DNS SRV zgodnie z dokumentacją.

2. **Podłączenie źródeł logów i zdarzeń:**
    - Sprawdzenie dostępności klasyfikatora i parsera dla danego źródła. Dopisanie adresu IP do IP Prefix Listy (jeżeli konieczne).
    - Wsparcie inżyniera klienta w konfiguracji urządzeń źródłowych do wysyłania logów.
    - Weryfikacja poprawności zbierania i parsowania logów (sugerowane wykorzystanie natywnych dashboardów dla danego rodzaju źródła – grafy powinny być poprawnie wypełniane, wszelkie rozbieżności mogą świadczyć o niepoprawnym parsowaniu).
    - Dla systemów Windows:
        - Weryfikacja dostępności systemu LOGmanager ze stacji/serwera na porcie 443/20514/20515.
        - Upewnienie się co do poprawności rozwiązywania rekordu SRV na adres IP LOGmanagera.
        - Instalacja agenta WES na stacji/serwerze.
        - Weryfikacja poprawności dodania stacji do LOGmanagera w menu Windows Agents List.
        - Konfiguracja filtrów i ustawień zbierania logów globalnie lub per-stacja.
        - Weryfikacja poprawności pobierania i parsowania logów ze stacji/serwera

2. **W przypadku źródeł do których nie istnieją parsery:**
    - Utworzenie klasyfikacji na podstawie wybranego atrybutu META logu (np. źródłowe IP, port docelowy, nazwa programu w nagłówku syslog). Akcja klasyfikacji ustawiona na TAG.
    - Wsparcie inżyniera klienta w konfiguracji urządzenia źródłowego do wysyłania logów.
    - Weryfikacja poprawności zbierania i targowania logów.
    - Eksport logów do pliku CSV w formacie RAW.
    - Przekazanie wyeksportowanego pliku CSV do inżyniera producenta w celu tworzenia parsera.



Uwagi i komentarze dotyczące treści prosimy wysyłać na: security-team@logmanager.com.

O PRODUCENCIE ORAZ REFERENCJE

LOGmanager istnieje od 2014 roku jako flagowy produkt Sirwisa a.s., firmy z siedzibą w Pradze. Wybrane referencje dostępne są na stronie **www.logmanager.pl**. Nasi klienci pochodzą z każdego sektora rynku, od organizacji rządowych, finansowych, przez banki, telekomunikację, e-commerce i inne. Zachęcamy do kontaktu w celu poznania szczegółowych referencji z Twojego obszaru zainteresowania — na życzenie zorganizujemy spotkanie z wybraną Organizacją z naszej listy referencyjnej.