

## **1. SIEM (Security Information and Event Management) - System analizy i korelacji zdarzeń występujących w sieci PIP WAN**

W ramach Umowy wymagane jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń PIP WAN oraz dodatkowo musi wspierać obsługę aplikacji typu agent na systemy Windows i Linux.

Rozwiązanie musi być dostarczone w postaci rozwiązań wirtualnych z możliwością migracji/installacji na platformach sprzętowych również pochodzących od tego samego producenta urządzeń bezpieczeństwa.

### **Wymagania sprzętowe**

Dostarczona platforma sprzętowa musi spełniać następujące wymagania:

- 1) Serwer wraz z akcesoriami do montażu w standardowej szafie technicznej o szerokości szyn 19 cali.
- 2) Maksymalna wysokość serwera to 2U.
- 3) Dwa procesory o minimalnych parametrach 2.4 GHz, 16 rdzeni/32 wątki, 24 MB cache.
- 4) Minimum 128GB pamięci operacyjnej minimum DDR4, ECC
- 5) Minimum dwa dyski SSD klasy Read Intensive tworzące RAID0. Dyski muszą mieć możliwość wymiany w czasie pracy.
- 6) Minimum 8 dysków SATA 6 Gb/s o pojemności co najmniej 8TB, które będą tworzyć grupę RAID6. Dyski muszą mieć możliwość wymiany w czasie pracy.
- 7) Kontroler zdalnego zarządzania wraz z licencją na połączenia zdalnej konsoli. Dedykowany port sieciowy dla komunikacji zarządzającej serwerem.
- 8) Karty sieciowe o interfejsach minimum: 2x1Gb RJ45 oraz 2x10Gb SFP+ wraz z wkładkami.
- 9) Redundantne zasilacze typu hot-swap.
- 10) Gwarancja producenta na cały okres etapu drugiego. Czas reakcji na uszkodzenia to następny dzień roboczy, w miejscu instalacji rozwiązania.
- 11) Uszkodzone dyski w czasie gwarancji, które zostaną wymienione na sprawne, muszą pozostać u Zamawiającego.
- 12) Serwer musi posiadać wolne sloty umożliwiające rozbudowę o dodatkową pamięć operacyjną o minimum 256GB.
- 13) Serwer musi istnieć możliwość rozbudowy ilości dysków o co najmniej 2 sztuki.

- 14) Do serwera musi być załączony komplet kabli zasilających oraz prowadnice, uchwyty dla poprawnego montażu w szafie 19 cali.
- 15) Serwer musi być certyfikowany do pracy z wybranym wirtualizatorem.
- 16) Dla zapewnienia wysokiej dostępności wymaga się dostawy co najmniej dwóch serwerów tego samego typu i konfiguracji.

#### **Wymagania Licencyjne**

- 1) System SIEM musi współpracować domyślnie (funkcje przygotowane przez producenta rozwiązania przez przedstawieniem oferty) z wszystkimi elementami nowej struktury sieciowej
- 2) Oferowany SIEM musi zapewnić obsługę w zakresie odbierania logów i monitorowania systemów co najmniej w ilości 80 GB surowych danych na dobę
- 3) W systemie musi być zapewniona obsługa agentowa co najmniej 92 serwerów.
- 4) Oferowany SIEM musi być wyposażony w subskrypcje reputacji wskaźników (IOC – indicator of compromise) od tego samego producenta co najmniej w zakresie: adresy IP, domeny, adresy URL. Informacje o reputacji muszą pochodzić z komercyjnego źródła, najlepiej tego samego producenta.
- 5) Dostarczone licencje muszą być w formie subskrypcji na okres trwania umowy.
- 6) Dostarczone licencje muszą pozwalać na zbudowanie środowiska bez pojedynczego punktu potencjalnej awarii czyli w pełni redundantnego.
- 7) Oferowany system będzie zainstalowany na dedykowanej platformie sprzętowej. Wymaga się, aby na platformie sprzętowej został zainstalowany system wirtualizacyjny, który będzie tworzył klaster maszyn wirtualnych systemu SIEM. System wirtualizacyjny musi być objęty wsparciem technicznym producenta o czasie równym subskrypcji SIEM.

#### **Logowanie**

- 1) Podgląd logowanych zdarzeń w czasie rzeczywistym.
- 2) Komunikacja systemów bezpieczeństwa, z których przesyłane są logi, z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem protokołów/portów: UDP/514.
- 3) Wydajność SIEM nie może być mniejsza niż 5 000 EPS (zdarzeń na sekundę odbieranych w trybie ciągłym).
- 4) SIEM musi być w stanie przetwarzać informacje otrzymywane z wykorzystaniem protokołu NetFlow.
- 5) Rozwiązanie SIEM musi mieć możliwość zbierania danych z monitorowanych urządzeń, również innych niż logi, co ma być osiągalne poprzez nie mniej niż:

- a) aktywne wykrywanie urządzeń wewnątrz sieci bez wykorzystania dodatkowego oprogramowania typu agent oraz wsparcie dla takich metod pobierania zdarzeń jak:  
SNMP, Syslog, Windows Management Instrumentation (WMI) i Open Management, Microsoft RPC, Cisco SDEE, Checkpoint LEA, JDBC, VM SDK, Telnet, SSH, HTTPS, IMAP, POP3, import z pliku CSV, REST API
  - b) zdolność do monitorowania statusu oraz dostępności usług takich jak: DNS, FTP, TCP, UDP, ICMP, JDBC, LDAP, SMTP, IMAP, POP3, POP3S, SSH, HTTP, HTTPS
- 6) Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:
- a) Ad możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows,
  - b) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application,
  - c) zdolność do monitorowania integralności plików,
  - d) zdolność do monitorowania rejestru systemowego,
  - e) zdolność do monitorowania urządzeń zewnętrznych (removable devices),
  - f) zdolność do wykonywania poleceń PowerShell wraz z odsyłaniem wyniku ich działania w postaci logów,
  - g) zdolność do wykonywania poleceń WMI wraz z odsyłaniem wyniku ich działania w postaci logów,
  - h) agent instalowany na systemach z rodziny Windows musi komunikować się z SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS,
  - i) zdolność do monitorowania takich parametrów jak obciążenie CPU, zajętość RAM, zajętość dysku, obciążenia sieci, działających aplikacji,
  - j) agent Windows musi mieć możliwość buforowania zbieranych zdarzeń w wypadku utraty komunikacji z pozostałymi elementami klastra SIEM.
- 7) Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Linux (Linux Agent), które posiadają nie mniej niż następujące możliwości:
- a) możliwość zbierania logów z wykorzystaniem protokołu syslog,
  - b) możliwość zbierania logów z plików tekstowych,
  - c) zdolność do monitorowania integralności plików,
  - d) zdolność do monitorowania pliku w oparciu o jego sumę kontrolną,
  - e) musi istnieć możliwość monitorowania stanu agentów w konsoli

- zarządzającej systemu,
- f) zdolność do monitorowania takich parametrów jak obciążenie CPU, zajętość RAM, zajętość dysku, obciążenia sieci, działających aplikacji.

### **Zbieranie danych:**

- 1) Zebrane dane muszą być przechowywane w sposób skompresowany.
- 2) SIEM musi mieć możliwość anonimizacji zebranych danych w zakresie nie mniejszym niż: adresy IP, nazwy hostów, adresy email, nazwy użytkowników. Proces ten ma być możliwy w oparciu o role/profile użytkowników administracyjnych. Ujawnienie danych (deanonimizacja) ma się odbywać z wykorzystaniem użytkownika udzielającego lub zabraniającego jej wykonania. W przypadku zatwierdzenia wspomnianego żądania, dane są ujawniane na określony czas, po którym powtórnie ulegają anonimizacji.
- 3) SIEM nie może wykorzystywać klasycznej relacyjnej bazy danych (np: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP.
- 4) Musi istnieć możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania.
- 5) Musi istnieć możliwość zbudowania struktury rozproszonej, aby zapewnić większą wydajność zapisu i wyszukiwania.
- 6) Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, zdarzeń i innych ustrukturyzowanych informacji.

### **Korelacja Logów**

W zakresie korelacji zdarzeń SIEM musi zapewniać:

- 1) Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
- 2) Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
- 3) SIEM ma posiadać możliwość aktualizacji online dla parserów, reguł, raportów oraz typów wspieranych urządzeń. Aktualizacja ta musi być niezależna od oprogramowania systemowego (OS, funkcje wykonawcze, etc.) które ma posiadać swoje wersjonowanie.
- 4) Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System ma korelować zdarzenia co najmniej dla następujących kategorii eventów:
  - Malware,

- Kontroli aplikacji,
- Email,
- IPS,
- Traffic,
- Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.

## **Raportowanie**

W zakresie raportowania SIEM musi zapewniać:

- 1) SIEM musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
  - a) listę najczęściej wykrywanych ataków,
  - b) listę najbardziej aktywnych użytkowników,
  - c) listę najczęściej wykorzystywanych aplikacji,
  - d) listę najczęściej odwiedzanych stron WWW,
  - e) listę krajów, do których realizowana jest komunikacja,
  - f) listę najczęściej wykorzystywanych polityk firewalla,
  - g) informacje o realizowanych połączeniach IPSec.
- 2) Generowanie raportów co najmniej w formatach: CSV, PDF i RTF.
- 3) Tworzenia raportów z wykorzystaniem graficznego edytora pozwalającego na podgląd pliku PDF przed jego wygenerowaniem.
- 4) Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
- 5) Funkcję definiowania własnych raportów.
- 6) Możliwość spolszczenia raportów.
- 7) Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

## **Analityka**

System SIEM musi mieć możliwość:

- wyszukiwania zdarzeń (events) w czasie rzeczywistym bez konieczności indeksowania oraz używania wyrażeń logicznych takich jak AND, OR, NOT czy też cudzysłowów,
- System musi posiadać co najmniej 2000 gotowych reguł korelacyjnych wprowadzonych przez producenta.
- zagnieżdżania wyników wyszukiwań w oparciu o operatory IN oraz NOT IN
- wyszukiwania w oparciu o słowa kluczowe oraz w oparciu o sparsowane atrybuty zdarzeń względem analizowanych danych,
- wyszukiwania historycznego z zastosowaniem kwerend zagnieżdżonych, ze wsparciem dla filtrowania typu Boolean,

grupowaniem w oparciu o agregację danych, filtry czasowe, wyrażenia regularne, wyrażenia matematyczne.

- wyszukiwania w oparciu o zapytania wstępne uruchamiane zgodnie harmonogramem
- wyszukiwania w oparciu o niemniej niż następujące operatory: include =, !=, <, >, IS NULL, IS NOT NULL, contains, not contains, contains regex, not contains regex,
- wykorzystania mechanizmów Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym, gdzie system sam decyduje o wyborze optymalnego. W wyniku działania opisanych mechanizmów Machine Learning system ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyłeń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie.
- wykorzystywania obiektów wykrytych i znajdujących się bazie urządzeń (CMDB), użytkowników i ich tożsamości oraz lokalizacji podczas wyszukiwania i tworzenia reguł
- tworzenia harmonogramu raportów i dostarczania ich pocztą elektroniczną
- wykorzystania dynamicznych list pozwalających na obserwację źródeł generujących zdarzenia krytyczne, wraz z możliwością wykorzystania tychże list w dowolnej regule raportującej

### **Zarządzanie**

- 1) System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczyć dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
- 2) Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
- 3) System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów bezpieczeństwa, z których przesyłane są logi.