Wymagania dla systemu analizy i zarządzania zdarzeniami.

System zarządzania logami (SIEM) ma zapewnić mechanizmy nadzoru nad całością wdrożonych systemów w zakresie bezpieczeństwa i ciągłości działania sieci komputerowej. Musi również pozwalać na identyfikację ew. zagrożeń na podstawie informacji pochodzącej z całej infrastruktury teleinformatycznej.

Podstawowymi zadaniami dla systemu SIEM są:

- wykrywanie awarii i innych problemów na podstawie logów i metryk pozyskiwanych z urządzeń i systemów informatycznych.
- zapewnienie mechanizmów monitorujących użytkowników infrastruktury teleinformatycznej,
- monitorowanie funkcjonowania aplikacji i urządzeń w celu szybszego reagowania na możliwe problemy i awarie,
- zarządzanie wykrywaniem, priorytetyzowaniem i rozwiązywaniem incydentów,
- zbieranie, zapisywanie i przechowywanie logów na czas określony przez prawo i regulaminy wewnętrzne.
- korelacja informacji pochodzących z różnych źródeł w celu wykrycia zaawansowanych zagrożeń i eliminacji fałszywych alarmów.

Wdrożony system SIEM musi pozwalać na podłączenie dowolnego źródła logów, również logów pochodzących z niestandardowych aplikacji wykorzystywanych obecnie i w przyszłości przez Zamawiającego.

System SIEM służyć będzie do alarmowania w przypadku wykrycia potencjalnych nadużyć bądź ataków. Wykorzystywany będzie również jako podstawowe narzędzie do rozwiązywania incydentów bezpieczeństwa przez pracowników działu IT oraz do nadzoru operacyjnego nad infrastrukturą. W związku z tym musi pozwalać na kontrolę dostępu do danych i narzędzi, w taki sposób by nie możliwe było nieautoryzowane usunięcie całości lub części informacji.

Zamawiający wymaga wdrożenia systemu SIEM w następującym zakresie:

- instalacja i konfiguracja systemu,
- integracja z systemami źródłowymi określonymi w wymaganiach szczegółowych,
- przygotowanie raportów, dashboardów i alarmów dla ww. źródeł danych zgodnie z

wytycznymi zamawiającego. Zakładane jest przygotowanie przez wykonawcę 20 raportów, 5 dashboardów i 50 definicji alarmów.

- Przeprowadzenia warsztatów szkoleniowych w języku polskim dla 4 osób poza siedzibą zamawiającego obejmujące następujące zagadnienia:
  - architektura systemu
  - podstawy użytkowania, w tym zarządzanie incydentami i analiza zdarzeń,
  - tworzenie nowych raportów, alarmów i dashboardów
  - tuning systemu i optymalizacji wydajności raportów, alarmów i dashboardów,
  - podstawy administracji,
  - procedury obsługi systemu.

  Szkolenie musi obejmować wykład teoretyczny oraz odpowiednie ćwiczenia i laboratoria. Zamawiający nie dopuszcza wykorzystania do szkolenia wdrożonego środowiska. Każdy uczestnik szkolenia musi być wyposażony we własną kopię środowiska szkoleniowego w postaci maszyny wirtualnej lub dostępu do środowiska w chmurze. Uczestnicy będą wyposażeni we własne laptopy.

  W przypadku szkolenia poza Lublinem Wykonawca pokryje koszty dojazdu, noclegu i wyżywienia.

Wymagania szczegółowe:

1. System SIEM musi pobierać logi z wielu różnych elementów systemów informatycznych Zamawiającego, poddawać je korelacji i na tej podstawie przedstawiać administratorom wiarygodne informacje na temat stanu bezpieczeństwa i wykrytych incydentów.
2. System SIEM musi zostać skonfigurowany tak aby pozyskiwał logi z następujących źródeł danych Zamawiającego:
   - serwery Microsoft ActiveDirectory
   - serwer Microsoft DHCP,
   - serwer Microsoft DNS,
   - serwer plików Microsoft,
   - urządzenia sieciowe firmy Cisco w zakresie logów: syslog, snmp, netflow (Catalyst 6509,Catalyst 2950, Catalyst 2960, catalyst3560)
   - firewall Paloalto PA-3020 - syslog, netflow,
   - ubiquiti unifi – syslog,

- mikrotik – syslog,
- systemy operacyjne serwerów (Windows Server, Linux),
- system poczty Zimbra,
- serwerów aplikacji www,
- baz danych Oracle,
- infrastruktury VMware

3. Przez pozyskiwanie logów rozumie się: pobranie logów i zapisanie w bazie systemu SIEM, klasyfikacja zdarzeń wg typów (np. zalogowanie użytkownika, nawiązanie połączenia, itp.) parsowanie logów, czyli nadanie kontekstów znaczeniowych dla poszczególnych fragmentów logu np. username, source_ip itp.

4. System SIEM musi umożliwiać pobieranie danych następującymi protokołami:
   - syslog UDP/TCP,
   - trap SNMP,
   - informacje przechowywane w bazach danych: Oracle, MS SQL, MySQL, PostgreSQL. Musi istnieć możliwość instalacji sterowników do innych typów baz danych w standardzie JDBC lub ODBC,
   - pliki tekstowe,
   - Windows EventLog,
   - NetFlow v5 i v9, sFlow.

   Pobieranie danych z ww. protokołów musi być możliwe bez wykorzystania agenta dla monitorowanych urządzeń i serwerów.

5. System SIEM musi umożliwiać pozyskiwanie danych z nasłuchu sieci. Zbierane informacje muszą obejmować wartości wszystkich nagłówków połączeń (odpowiednik NetFlow i sFlow) do warstwy 4 ISO/OSI, oraz do warstwy 7, dla następujących protokołów:
   - DHCP,
   - DNS,
   - HTTP,
   - IMAP,
   - SIP,
   - SMB,
   - SMTP.

6. Rozwiązanie musi umożliwiać analizowanie logów wielolinijkowych. Maksymalny wspierany rozmiar pojedynczego logu nie może być mniejszy niż 256kB.

7. System SIEM musi pozwalać na akceleracje zapytań i raportów, które wykonywane są często, tak by automatycznie budował agregaty pozwalające na szybkie wykonania raportu obejmującego długie okresy czasu (np. 6 miesięcy). Akceleracja musi być dostępna zarówno dla raportów wbudowanych jak i własnych definiowanych przez użytkownika. Raporty takie powinny być dostępne w maksymalnie 10 sekund od ich uruchomienia dla dowolnego okresu czasu.
8. System SIEM musi umożliwiać zrównoleglenie wyszukiwania na wiele procesów i serwerów w celu przyśpieszenia wyszukiwania.

9. System SIEM musi utrzymywać centralne repozytorium logów z możliwością ich przeglądania w formie rzeczywistej (raw) oraz udostępniać użytkownikowi dane w formie znormalizowanej (z uwzględnieniem znaczenia poszczególnych zmiennych/pól logu). Dostęp do danych w formie rzeczywistej jak i znormalizowanej musi być możliwy w oparciu o te same narzędzia.

10. Wyszukiwanie danych musi być możliwe z wykorzystaniem filtrów opartych o dane znormalizowane np. zapytanie o konkretny adres IP występujący jako adres źródłowy połączeń. System musi również pozwalać na wyszukiwanie danych w oparciu o wyrażenia regularne zastosowane wobec całego logu jak również pojedynczych pól.

11. System SIEM musi umożliwiać pobieranie danych niezbędnych do korelacji danych i priorytetyzacji zdarzeń w oparciu o tożsamość użytkownika oraz priorytet i przeznaczenie hostów. System musi umożliwiać pobieranie tych informacji z:
    - ActiveDirectory/LDAP,
    - Bazy CMDB metodami JDBC lub ODBC,
    - Pliki CSV,

12. System SIEM musi posiadać raporty/dashboardy związane z obsługą serwerów Microsoft DHCP wykorzystywanych przez Zamawiającego, co najmniej uwzględniające następujące zagadnienia:
    - wyszukiwanie wg przyznanych adresów i adresów MAC,
    - monitorowanie transakcji DHCP w czasie rzeczywistym.

13. System SIEM musi posiadać raporty/dashboardy związane z obsługą serwerów Microsoft ActiveDirectory wykorzystywanych przez Zamawiającego, co najmniej uwzględniające następujące zagadnienia:
    - dostępność poszczególnych usług AD i DNS,
    - raporty zmian w strukturze katalogu,
    - zalogowania i wylogowania użytkowników,
    - raportowanie zablokowanych kont,
    - raportowanie zmian w obiektach AD.

14. System musi umożliwiać prezentację skorelowanych zdarzeń związanych z użytkownikiem pochodzących ze źródeł nie posiadających informacji o użytkowniku – na podstawie jego adresu IP.

15. Musi istnieć możliwość prezentacji opisu zasobu w postaci serwera lub stacji roboczej obejmującego: nazwę, właściciela, funkcję, kontakt, nawet jeżeli w samym logu występuje wyłączenie adres IP lub MAC tego zasobu.

16. System SIEM musi umożliwiać korelację zdarzeń pochodzących z różnych systemów źródłowych na podstawie dowolnych pól i zmiennych logu lub dowolnych innych danych wzbogacających log (dane o tożsamości, geolokalizacja, dane o zasobach)

17. Musi istnieć możliwość zastosowania reguł korelacyjnych dla danych historycznych, w celu wykrycia podobnych zdarzeń w przeszłości.

18. System SIEM musi analizować zdarzenia w oparciu o znaczniki czasu zawarte w oryginalnych logach jeśli tylko są dostępne.

19. System musi umożliwiać analizę logów w różnych językach, w tym co najmniej w języku angielskim i polskim. Znaki w logach źródłowych mogą być kodowane przy użyciu różnych stron kodowych.

20. System SIEM musi posiadać możliwość automatycznego reagowania na zdarzenie oraz powiadamiania administratorów. Musi istnieć możliwość wysłania email oraz możliwość

konfigurowania innych akcji w postaci skryptów, do których może być przekazywana dowolna liczba argumentów na podstawie treści alarmu.

21. System zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem musi posiadać możliwość tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być tworzone są w wielu formatach – minimum PDF, CSV, JPG.

22. System SIEM musi umożliwiać alarmowanie i raportowanie o anomaliach statystycznych dla dowolnych parametrów liczbowych zawartych w logach polegając na odchyleniach w stosunku do wartości przewidywanych (zarówno w górę, jak i w dół) z uwzględnieniem sezonowości (np. różnic wynikających z pory dnia, czy dnia tygodnia).
23. System SIEM musi umożliwiać raportowanie parametrów ilość pobranych danych, czas korzystania z internetu, ilość odwiedzanych stron, kategorie stron w oparciu o logi filtra URL Paloalto,

24. System SIEM musi umożliwiać raportowanie zablokowanych stron (liczba, kategoria, poziom ryzyka) w oparciu o logi filtra URL Paloalto,

25. System SIEM musi pozwalać na definiowanie własnych lub modyfikację raportów, zapytań i widoków w oparciu o zebrane dane.

26. Zestaw funkcjonalności analitycznych musi uwzględniać co najmniej następujące funkcje:
    - statystyki typu suma, średnia, mediana, odchylenie standardowe, najstarszy, najnowszy dla zadanego klucza (np. średni godzinny wolumen danych dla adresu źródłowego),
    - funkcje wykrywania anomalii danych liczbowych. Rozwiązanie musi pozwalać na wykrywanie anomalii dla dowolnych parametrów zawartych w logach, a nie tylko parametrów ruchu sieciowego.
    - rozwiązanie musi wykrywać rzadkie wystąpienia wartości i zdarzeń w określonym podzbiorze,
    - budowanie korelacji w oparciu o zdarzenia zawierające jednakowe wartości danych pól,
    - badanie zmian wartości danego pola i alarmowanie lub raportowanie w oparciu o zmianę tej wartości (np. wzrost liczby niepoprawnych zalogowań o 50%),

Wymagania techniczne

1. System SIEM musi zostać dostarczony w formie oprogramowania do zainstalowania na infrastrukturze wirtualnej VMware. Zamawiający na potrzeby wdrożenia udostępni infrastrukturę wirtualizacyjną ESXi 5.5 (8 cpu 2Ghz, 24GB ram, dysk: 5TB)
2. Komunikacja użytkownika z systemem SIEM musi odbywać się przy użyciu przeglądarki internetowej (wsparcie dla co najmniej: Internet Explorer, Firefox, Chrome). Nie jest dopuszczalne wymaganie instalacji jakiegokolwiek dedykowanego oprogramowania klienckiego na stacjach roboczych użytkowników w tym wtyczek i środowisk uruchomieniowych np.: Adobe Flash, Java lub Microsoft Silverlight.
3. System SIEM musi pozwalać na zebranie i analizę co najmniej **20GB** danych dziennie z wydajnością pozwalającą na obsługę do 10000 zdarzeń na sekundę w okresach największego obciążenia
4. Licencja nie może ograniczać liczby podłączonych urządzeń.
5. Licencja nie może być ograniczona czasowo. Zamawiający wymaga licencji bezterminowej.
6. System SIEM musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej CIFS lub NFS lub iSCSI w celu przechowywania danych archiwalnych. Dane archiwalne powinny być dostępne w systemie w ten sam sposób jak dane dostępne on-line. Dopuszczalne jest by dane dostępne były z mniejszą wydajnością.
7. System SIEM musi umożliwiać definiowanie precyzyjnych uprawnień administratorów w zakresie monitorowanego obszaru systemu informatycznego oraz dostępnych operacji w systemie zarządzania. Tożsamość administratorów musi być weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania – co najmniej RADIUS, LDAP i Active Directory.
8. System SIEM musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów – zalogowanie, wylogowanie, uruchamiane zapytania i zmiany konfiguracji systemu.