LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

ISO 27001:2013 & LOGmanager

Poradnik integracji

Abstrakt

Każda organizacja stosuje liczne środki bezpieczeństwa, aby utworzyć i utrzymać odpowiedni poziom ochrony swojego biznesu przed zagrożeniami takimi jak ataki hakerskie, katastrofy naturalne czy incydenty operacyjne. Niestety, ze względu na wysoki poziom skomplikowania tematu oraz ilość najróżniejszych procesów, procedur oraz narzędzi, bezpieczeństwo organizacji często staje się niezorganizowane lub nawet nieadekwatne w stosunku do ryzyka.

ISO 27001:2013 to międzynarodowy standard bezpieczeństwa dostarczający sprecyzowanych wymagań dotyczących tworzenia, implementowania, zarządzania i ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji (eng. ISMS – Information Security Management System). Istnieje wiele powodów, dla których warto przejść przez proces certyfikacji ISO – niektóre organizacje robią to, aby osiągnąć zgodność z zapisami prawnymi kraju w którym działają, standardami czy nawet SLA – inne po prostu aby udowodnić swoim klientom, że podchodzą do tematu bezpieczeństwa na poważnie. Posiadanie ISMS wdrożonego zgodnie z zapisami ISO 27001:2013 jest dowodem na dojrzałość organizacji w zakresie bezpieczeństwa.

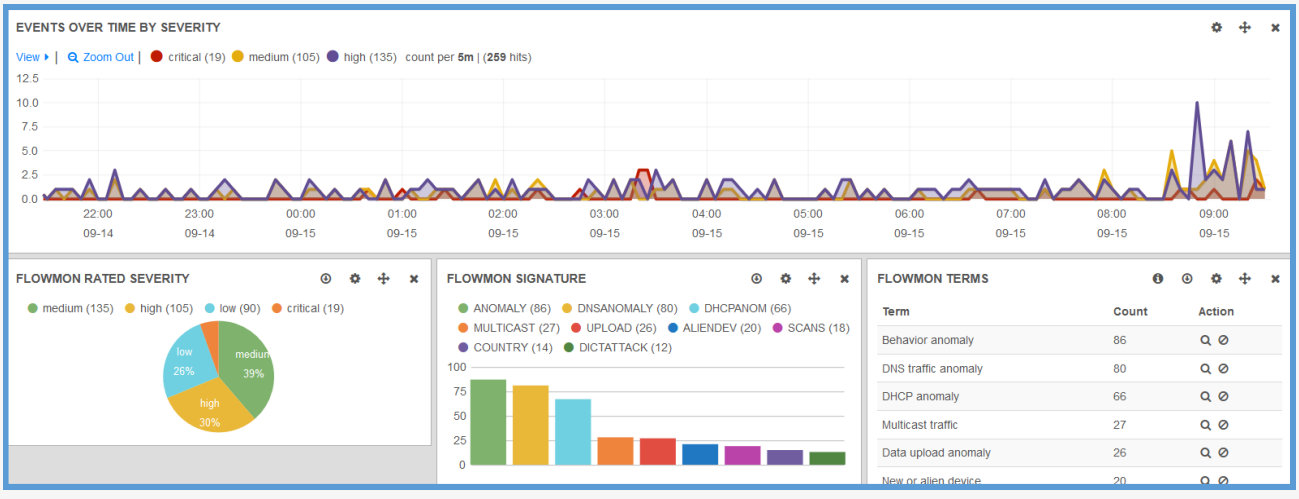
Niezależnie od powodu, spełnienie wszystkich wymagań ISO 27001:2013 nie jest łatwym zadaniem. Standard ten uwzględnia ponad 100 zapisów, poruszających niemal każdy aspekt działania organizacji, od polityk i procedur, zasobów ludzkich, fizycznej kontroli dostępu czy kontaktów z zewnętrznymi dostawcami, do zabezpieczeń skupionych bardziej na IT takich jak zbieranie i monitorowanie logów, kryptografia czy ochrona przed złośliwym oprogramowaniem.

Nie istnieje system, które rozwiązałby wszystkie problemy związane z wdrożeniem ISO. Jedyna słuszna metoda na uzyskanie certyfikacji to poruszanie się krok po kroku do celu. Oczywiście nie oznacza to, że nie można usprawnić tego procesu – rozwiązania SIEM takie jak LOGmanager, dzięki ich holistycznemu wglądowi w infrastrukturę, są ogólnie znanym i akceptowanym wsparciem w osiąganiu zgodności z najróżniejszymi standardami, nie tylko ISO.

Cel dokumentu

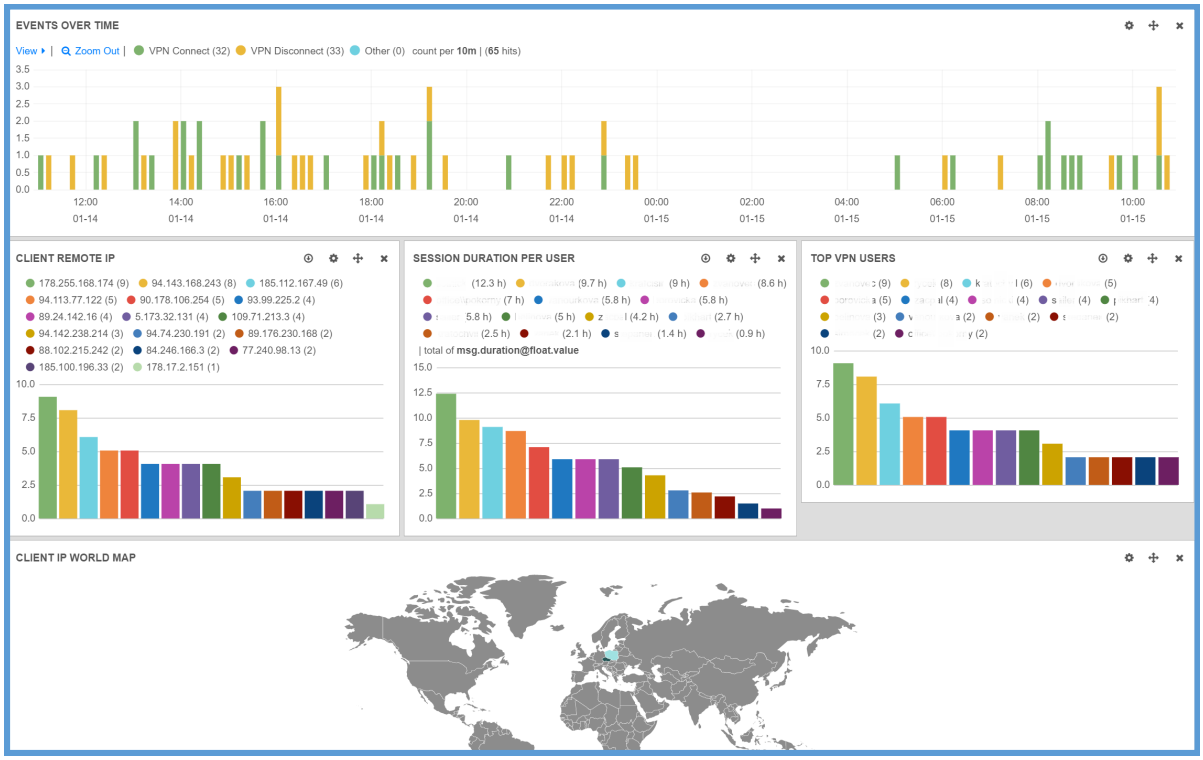
Celem tego dokumentu jest dostarczenie przejrzystych informacji, które z zapisów ISO 27001:2013 można spełnić lub przynajmniej ułatwić osiągnięcie zgodności wykorzystując system LOGmanager.

LOGmanager to rozwiązanie SEM/SIEM zbierające logi z dowolnego urządzenia w sieci, umożliwiające przechowywanie ich w niezmodyfikowanej formie oraz udostępniające je do przeszukiwania i analizy. LOGmanager pozwala także na tworzenie powiadomień (alertów) w przypadku wykrycia w logach zdefiniowanych uprzednio parametrów oraz korelację zdarzeń pomiędzy różnym źródłami. Główną siłą systemu jest jego prosty i intuicyjny interfejs, utworzony z myślą o małych-średnich organizacjach i wiecznie zabieganych administratorach.



Wizualizacja danych z systemu Flowmon w systemie LOGmanager.

Zabezpieczenie ISO27001	Opis zabezpieczenia	Jak LOGmanager pomaga osiągnąć zgodność
A.6.2 Urządzenia mobilne i telepraca		
Cel: Zapewnić bezpieczeństwo telepracy i stosowania urządzeń mobilnych		
A.6.2.1 Polityka stosowania urządzeń mobilnych	Należy wprowadzić politykę oraz wspierające ją zabezpieczenia w celu zarządzania ryzykami wynikającymi z użytkowania urządzeń mobilnych.	Zbieraj logi z MDM/VPN/Bezpośrednio w celu monitorowania wykorzystania urządzeń i ich lokalizacji.
A.6.2.2 Telepraca	Należy wdrożyć politykę oraz wspierające ją zabezpieczenia w celu ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania telepracy.	Zbieraj logi z VPN i stacji końcowych w celu monitorowania logowania/wylogowania użytkowników i ich lokalizacji. Zbieraj logi z AV aby wykrywać zagrożenia malware. Utwórz alerty dotyczące krytycznych zdarzeń takich jak próby logowania brute force lub z podejrzanych lokalizacji (np. z państw nie związanych w żaden sposób z organizacją).
A.9.1 Wymagania biznesowe wobec kontroli dostępu		
Cel: Ograniczyć dostęp do informacji i środków przetwarzania informacji		
A.9.1.2 Dostęp do sieci i usług sieciowych	Użytkownicy powinni mieć dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia.	Zbieraj logi z Kontrolerów Domeny/VPN/Urządzeń WLAN w celu śledzenia udanych/nieudanych zdarzeń uwierzytelniania i potwierdzania skuteczności wdrożonej polityki dostępu. Utwórz alerty dotyczące nieuprawnionych logowań.



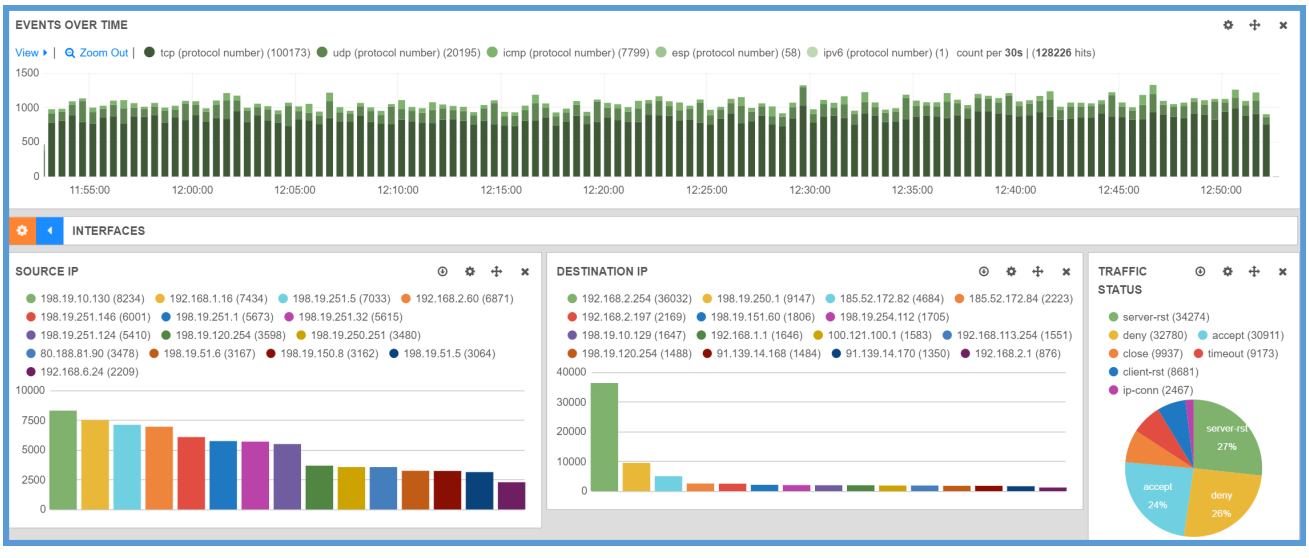
Statystyki VPN — czas trwania sesji, najczęściej obserwowani użytkownicy, lokalizacja GeoIP.

Zabezpieczenie ISO27001	Opis zabezpieczenia	Jak LOGmanager pomaga osiągnąć zgodność
A.9.2 Zarządzanie dostępem użytkowników		
Cel: Zapewnić dostęp uprawnionym użytkownikom i zapobiec nieuprawnionemu dostępowi do systemów i usług.		
A.9.2.1 Rejestrowanie i wyrejestrowywanie użytkowników	W celu umożliwienia przydzielania praw dostępu należy wdrożyć formalny proces rejestrowania i wyrejestrowywania użytkowników.	Zbieraj logi z Kontrolera Domeny w celu śledzenia tworzenia/usuwania/zawieszania kont użytkowników. Przesyłaj logi audytowe potwierdzające akcję utworzenia/usunięcia konta do systemu ticketowego. Utwórz alert dotyczący prób użycia kont zawieszonych lub usuniętch.
A.9.2.2 Przydzielanie dostępu użytkownikom	Należy wdrożyć formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników.	Zbieraj logi z Kontrolera Domeny w celu śledzenia akcji nadawania/obierania praw dostępu. Przesyłaj logi audytowe potwierdzające akcję nadawania/obierania praw dostępu do systemu ticketowego.
A.9.2.3 Zarządzanie prawami uprzywilejowanego dostępu	Przydzielanie i wykorzystywanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować.	Zbieraj logi z Kontrolera Domeny w celu śledzenia akcji nadawania/obierania praw dostępu dla kont uprzywilejowanych. Monitoruj logowania/wylogowania kont uprzywilejowanych. Utwórz cykliczne raporty dotyczące wykorzystania kont uprzywilejowanych aby zapewnić właściwe wykorzystanie (np. odebranie przywilejów nieużywanego konta). Przesyłaj logi audytowe potwierdzające akcję nadawania/obierania praw dostępu do systemu ticketowego.
A.9.3 Odpowiedzialność użytkowników		
Cel: Zapewnić rozliczalność w celu ochrony ich informacji uwierzytelniających.		
A.9.3.1 Stosowanie poufnych informacji uwierzytelniających	Użytkownicy powinni mieć obowiązek przestrzegania przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających.	Zbieraj logi z Kontrolera Domeny/Stacji Końcowych i śledź wykorzystanie kont w celu wykrywania wykorzystania pojedynczego konta przez więcej niż jednego użytkownika.

Zabezpieczenie ISO27001	Opis zabezpieczenia	Jak LOGmanager pomaga osiągnąć zgodność
A.9.4 Kontrola dostępu do systemów i aplikacji		
Cel: Zapobiec nieuprawnionemu dostępowi do systemów i aplikacji.		
A.9.4.1 Ograniczenie dostępu do informacji	Dostęp do informacji oraz funkcji systemu aplikacyjnego należy ograniczać zgodnie z polityką kontroli dostępu.	Zbieraj logi z systemów plików i monitoruj dostęp do danych przez autoryzowanych użytkowników. Utwórz alerty dotyczące nieautoryzowanego użycia bądź podejrzanych zdarzeń (np. duża ilość usuniętych plików w krótkim czasie).
A.9.4.2 Procedury bezpiecznego logowania	Tam, gdzie polityka kontroli dostępu tego wymaga, dostęp do systemów i aplikacji powinien być kontrolowany przez procedurę bezpiecznego logowania.	Zbieraj logi dotyczące logowania/wylogowania oraz sukcesu/porażki tych akcji. Utwórz alerty dotyczące prób uzyskania dostępu do kont metodą siłową (Brute Force).
A.9.4.4 Użycie uprzywilejowanych programów narzędziowych	Wykorzystywanie uprzywilejowanych programów narzędziowych umożliwiających obejście zabezpieczeń systemów i aplikacji, powinno podlegać ograniczeniom i ścisłemu nadzorowi.	Loguj wykorzystanie uprzywilejowanego oprogramowania.
A.9.4.5 Kontrola dostępu do kodów źródłowych programów	Dostęp do kodu źródłowego programów powinien być ograniczony.	Zbieraj logi dotyczące dostępu i zmian w repozytoriach.
A.10.1 Zabezpieczenia kryptograficzne		
Cel: Zapewnić właściwe i skuteczne wykorzystanie kryptografii do ochrony poufności, autentyczności i/lub integralności informacji.		
A.10.1.2 Zarządzanie kluczami	Należy opracować politykę dotyczącą korzystania, ochrony i okresów ważności kluczy kryptograficznych i wdrożyć ją na wszystkich etapach cyklu życia kluczy.	Zbieraj i loguj zdarzenia dotyczące zarządzania kluczami (np. utworzenie/usunięcie/modyfikacja).
A.11.1 Obszary bezpieczne		
Cel: Zapobiec nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacjach i środkach przetwarzania informacji należących do organizacji.		
A.11.1.2 Fizyczne zabezpieczenie wejść	Bezpieczne strefy należy chronić odpowiednimi zabezpieczeniami wejść zapewniającymi dostęp wyłącznie osobom uprawnionym.	Zbieraj logi z urządzeń kontroli dostępu w celu monitorowania czasów wejścia/wyjścia do/z obiektu i pomieszczeń.

Zabezpieczenie ISO27001	Opis zabezpieczenia	Jak LOGmanager pomaga osiągnąć zgodność
A.12.2 Ochrona przed szkodliwym oprogramowaniem		
Cel: Zapewnić informacjom i środkom przetwarzania informacji ochronę przed szkodliwym oprogramowaniem.		
A.12.2.1 Zabezpieczenia przed szkodliwym oprogramowaniem	Należy wdrożyć zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników.	Zbieraj logi ze wszystkich narzędzi bezpieczeństwa w sieci w celu konsolidacji widoków do jednej konsoli. Zbieraj logi z oprogramowania antywirusowego i generuj cykliczne raporty w celu potwierdzenia aktualności sygnatur. Utwórz alerty dotyczące incydentów wykrytych przez narzędzia bezpieczeństwa. Wykonuj okresowe aktywności threat hunting (np. przeglądanie logów dotyczących ruchu sieciowego w celu wykrycia podejrzanych kanałów komunikacji). Wykorzystuj system LOGmanager do prowadzenia procesu odpowiedzi na incydenty i ustalania głównej przyczyny (eng. Root Cause Analysis).
A.12.4 Rejestrowanie zdarzeń i monitorowanie		
Cel: Rejestrować zdarzenia i zbierać materiał dowodowy.		
A.12.4.1 Rejestrowanie zdarzeń	Należy tworzyć, przechowywać i systematycznie przeglądać dzienniki zdarzeń rejestrujące działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji.	Wykorzystaj system LOGmanager do zbierania logów z dowolnego źródła w Twojej infrastrukturze i przechowuj tak długo, jak będzie to konieczne (w zależności od dostępnej przestrzeni dyskowej - lub na zewnętrznym storage). Wykorzystaj istniejące bądź stwórz własne wizualizacje logów aby usprawnić proces ich analizy. Wykorzystaj istniejące lub stwórz własne alert dotyczące zdarzeń bezpieczeństwa.
A.12.4.2 Ochrona informacji w dziennikach zdarzeń	Środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń należy chronić przed manipulacją i nieuprawnionym dostępem.	Logi przechowywane w systemie LOGmanager nie mogą być usunięte ani zmodyfikowane. Logi podlegające archiwizacji na zewnętrznych nośnikach są podpisywane cyfrowo, dzięki czemu można bezsprzecznie potwierdzić ich integralność i wykorzystać jako dowód w sprawie sądowej.
A.12.4.3 Rejestrowanie działań administratorów i operatorów	Działania administratorów i operatorów systemów należy rejestrować, a dzienniki chronić i systematycznie przeglądać.	Wykorzystaj LOGmanagera do zbierania logów z dowolnego źródła dotyczących akcji uprzywilejowanych użytkowników. Przeglądaj lokalne logi systemu LOGmanager aby monitorować wprowadzane zmiany w konfiguracji.
A.12.4.4 Synchronizacja zegarów	Zegary wszystkich istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa należy zsynchronizować z jednym wzorcowym źródłem czasu.	LOGmanager dodaje własny znacznik czasu (eng. Timestamp) do każdego odebranego logu, tym samym zapewniając odpowiednią synchronizację czasu wszystkich logów.

Zabezpieczenie ISO27001	Opis zabezpieczenia	Jak LOGmanager pomaga osiągnąć zgodność
A.13.1 Zarządzanie bezpieczeństwem sieci		
Cel: Zapewnić ochronę informacji w sieciach oraz wspomagających je środkach przetwarzania informacji.		
A.13.1.1 Zabezpieczenia sieci	Sieci powinny być zarządzane i nadzorowane w celu ochrony informacji w systemach i aplikacjach.	Zbieraj logi z urządzeń sieciowych. Utwórz alerty dotyczące krytycznych zdarzeń. Monitoruj dane z wielu źródeł w celu detekcji anomalii w ruchu sieciowym.
A.13.1.2 Bezpieczeństwo usług sieciowych	Umowy dotyczące wszystkich usług sieciowych, świadczonych wewnętrznie lub zlecanych na zewnątrz, powinny zawierać zidentyfikowane mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania.	Zbieraj logi z urządzeń sieciowych. Korzystając z wizualizacji przeglądaj parametry techniczne urządzeń oraz skuteczność reguł zapór sieciowych. Utwórz alerty dotyczące krytycznych zdarzeń.
A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych		
Cel: Zapewnić, żeby bezpieczeństwo informacji było nieodłączną częścią systemów informacyjnych w całym cyklu życia. Dotyczy to również wymagań wobec systemów informacyjnych dostarczających usług w sieciach publicznych.		
A.14.1.2 Zabezpieczanie usług aplikacyjnych w sieciach publicznych	Informacje przesyłane w sieciach publicznych, związane z usługami świadczonymi przez aplikacje, należy chronić przed nieuczciwymi działaniami, sporami dotyczącymi umów oraz nieuprawnionym ujawnieniem i zmianami.	Zbieraj logi z Kontrolera Domeny oraz urządzeń sieciowych. Utwórz alerty dotyczące zmian wprowadzanych w politykach GPO mogących zaszkodzić publicznym usługom. Monitoruj ruch sieciowy w celu detekcji niezaszyfrowanych kanałów komunikacji (np. przesyłanie danych via FTP).



Wizualizacja ruchu sieciowego

Zabezpieczenie ISO27001	Opis zabezpieczenia	Jak LOGmanager pomaga osiągnąć zgodność
A.14.3 Dane testowe		
Cel: Zapewnić ochronę danych stosowanych do testów.		
A.14.3.1 Ochrona danych testowych	Dane testowe należy starannie wybierać, chronić i nadzorować.	Zbieraj logi dotyczące dostępu do danych testowych w celu monitorowania kto uzyskuje do nich dostęp i kiedy.
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami		
Cel: Zapewnić ochronę aktywów organizacji udostępnianych dostawcom.		
A.15.1.2 Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	Należy ustanowić wszystkie istotne wymagania dotyczące bezpieczeństwa informacji i uzgodnić je z każdym dostawcą, który może uzyskać dostęp, przetwarzać, przechowywać, przesyłać lub dostarczać elementy infrastruktury teleinformatycznej dla przetwarzania informacji należących do organizacji.	Zbieraj logi z urządzeń sieciowych/kontrolera domeny/ systemów plików (oraz innych) w celu monitorowania działań zewnętrznych dostawców.
A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami		
Cel: Zapewnić spójne i skuteczne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji, z uwzględnieniem informowania o zdarzeniach i słabościach.		
A.16.1.2 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Zdarzenia związane z bezpieczeństwem informacji należy zgłaszać odpowiednimi kanałami zarządczymi tak szybko, jak tylko to jest możliwe.	Zbieraj logi ze wszystkich narzędzi bezpieczeństwa w sieci w celu ujednolicenia widoku zdarzeń. Utwórz alerty i odbieraj powiadomienia o potencjalnych incydentach bezpieczeństwa via email. Utwórz dzienne raporty bezpieczeństwa.
A.16.1.7 Gromadzenie materiału dowodowego	Organizacja powinna określić i stosować procedury identyfikacji, gromadzenia, pozyskiwania i utrwalania informacji, które mogą stanowić materiał dowodowy.	Logi zapisane w bazie danych systemu LOGmanager nie mogą być usunięte, a logi przechowywane na zewnętrznych nośnikach w ramach procesu archiwizacji są podpisywane cyfrowo, dzięki czemu mogą stanowić materiał dowodowy. Dostęp do logów zawierających poufne informacje może być ograniczony do wybranej grupy użytkowników.

Uwagi oraz sugestie co do treści prosimy kierować na adres: security-team@logmanager.com.

O PRODUCENCIE

LOGmanager powstał w 2014 roku jako flagowy produkt Czeskiej firmy Sirwisa A.S. z siedzibą w Pradze. Wybrane referencje od naszych klientów można znaleźć na stronie www.logmanager.pl. Do ich grona zaliczają się organizacje każdego rozmiaru i z każdej branży, m.in. finansowe, ubezpieczenia, IT, jednostki Rządowe i inne. Na życzenie skontaktujemy państwa z wybranym klientem, który zgodził się na udzielenie referencji LOGmanager.