LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

ČSN/ISO 27001:2013 a LOGmanager

Integrační návod

Abstrakt

Každá organizace používá vícero bezpečnostních opatření k vytvoření a udržování ochrany před nejrůznějšími hrozbami, jako jsou falešní hráči, přírodní katastrofy nebo provozní incidenty IT. Bohužel kvůli složitosti problematiky a velkému počtu nástrojů, které je třeba implementovat, má zabezpečení tendenci být v kritických oblastech neuspořádané nebo může dokonce zcela chybět.

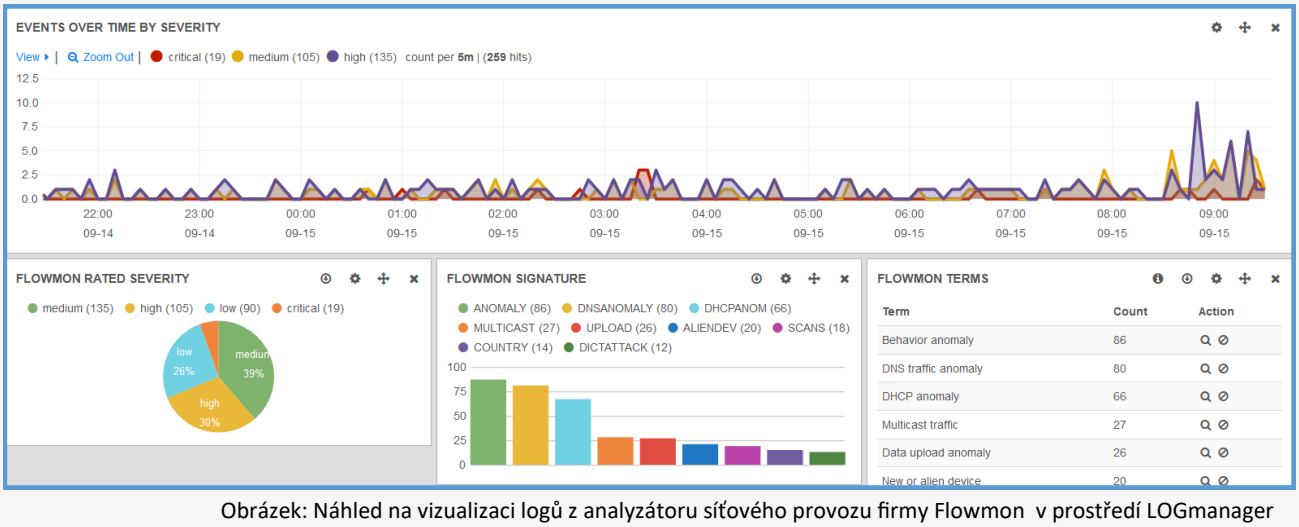
ČSN/ISO 27001: 2013 je mezinárodní standard, jehož cílem je poskytnout jasné požadavky na zavedení, implementaci, údržbu a neustálé zlepšování Systému řízení bezpečnosti informací - *Information Security Management System (ISMS).* Implementace ISMS v souladu s normou ČSN/ISO 27001: 2013 je důkazem vyspělosti zabezpečení organizace. Existuje více důvodů, proč využít certifikaci ISO - některé společnosti ji používají k dodržování různých zákonů a předpisů, standardů, SLA - jiné jen proto, aby svým klientům dokázaly, že bezpečnost berou vážně.

Ať už je důvod jakýkoli, splnění všech požadavků ČSN/ISO 27001:2013 není snadným úkolem. Standard popisuje přes 100 opatření, která pokrývají více oblastí činnosti organizace, od zásad a postupů, lidských zdrojů, fyzické kontroly, zabezpečení majetku až po cílené kontroly zaměřené na IT, jako je logování a monitorování, řízení přístupu, kryptografie nebo malware. Neexistuje jedno zařízení, které by vyřešilo všechny problémy, s nimiž se můžete během implementace setkat. Obecně neexistuje jednoduchý způsob, jak to udělat - pouze správný způsob, jak postupovat krok za krokem.

To samozřejmě neznamená, že bychom neměli hledat pomoc v externím řešení. O systémech SIEM je díky jejich celostnímu pohledu na mnoho částí IT infrastruktury známo, že jsou velkou pomocí při dosahování souladu s různými normami a předpisy, protože nám pomáhají splnit některé z cílů ISO, nebo je dokonce plní zcela.

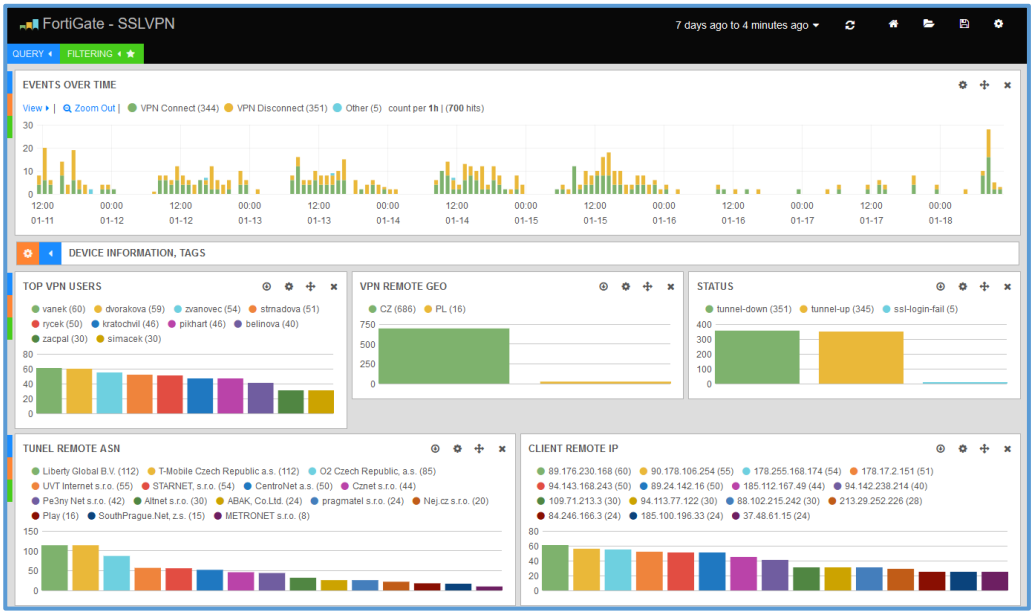
Cíle tohoto dokumentu

Cílem tohoto dokumentu je poskytnout jasné pokyny, která opatření normy ISO 27001: 2013 lze splnit nebo alespoň podpořit LOGmanagerem. LOGmanager je nástroj SEM / SIEM, který shromažďuje logy ze všech zařízení v infrastruktuře, ukládá je bezpečným a nemodifikovatelným způsobem po dlouhou dobu a umožňuje rychlé vyhledávání a vizualizaci. Může také zasílat upozornění při splnění definovaných podmínek a korelovat mezi událostmi pocházejícími z různých zdrojů. Díky popsaným schopnostem je to dokonalý systém pro ukládání auditních záznamů aktivit (které je vyžadováno v několika bodech ISO), pro zasílání upozornění na hrozby a pro poskytování rychlého a bezpečného přístupu k logům.



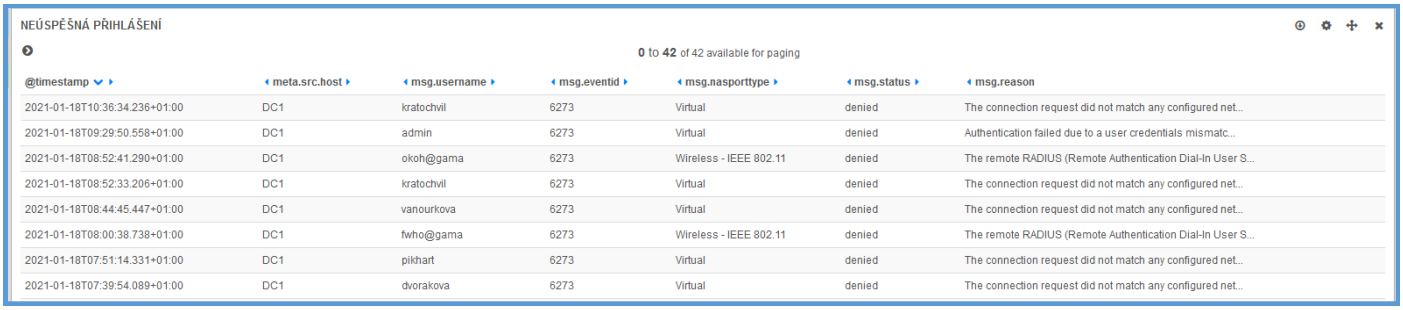
Obrázek: Náhled na vizualizaci logů z analyzátoru síťového provozu firmy Flowmon v prostředí LOGmanager

Oblast ISO27001	Popis opatření	Jak může LOGmanager pomoci s dosažením
A.6.2 Mobilní zařízení a práce na dálku		
Cíl: Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku		
A.6.2.1 Politika mobilních zařízení	Musí být přijata politika a relevantní bezpečnostní opatření pro zvládání rizik spojených s používáním mobilních zařízení.	Shromažďuje logy z MDM/VPN/Directly pro sledování používání a polohy zařízení.
A.6.2.2 Práce na dálku	Musí být aplikována politika a relevantní opatření na ochranu informací, které jsou přístupné, zpracovávané nebo ukládané v místech pro práci na dálku.	Shromažďuje logy z VPN a ze zařízení, aby bylo možné sledovat přihlašování a odhlašování uživatelů a jejich lokaci. Shromažďuje logy z AV pro monitoring hrozeb. Upozorňuje na kritické události, jako jsou například pokusy o přihlášení hrubou silou nebo podezřelá zdrojová IP adresa přihlašovaného (např. neočekávaná země).
A.9.1 Požadavky organizace na řízení přístupu		
Cíl: Omezit přístup k informacím a vybavení pro zpracování informací.		
A.9.1.2 Přístup k sítím a síťovým službám	Uživatelé musí mít přístup pouze k těm sítím a síťovým službám, pro jejichž použití byli zvlášť oprávněni.	Shromažďuje logy z Domain Controlleru/VPN/ bezdrátových zařízení pro sledování úspěšných/ neúspěšných autentizačních událostí a pro potvrzení správně fungující kontroly přístupu podle očekávání. Upozorní na pokusy o neoprávněný přístup.



Obrázek: SSL VPN statistiky— možná vizualizace informací o VPN v LOGmanageru.

Oblast ISO27001	Popis opatření	Jak může LOGmanager pomoci s dosažením
A.9.2 Řízení přístupu uživatelů		
Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k systémům a službám.		
A.9.2.1 Registrace a zrušení registrace uživatele	Pro přidělování přístupových práv musí být implementován proces formalizované registrace uživatele včetně jejího zrušení.	Shromažďuje logy z Domain Controlleru pro sledování registrace/zrušení registrace/suspenze. Upozorní na použití suspendovaných nebo smazaných účtů. Přepošle kopii auditního logu s potvrzením akce registrace/zrušení/suspenze k uložení v tiketovacím systému jakožto důkaz.
A.9.2.2 Správa uživatelských přístupů	Pro přidělování a odebírání přístupových práv všem typům uživatelů ke všem systémům a službám musí být implemento-ván formalizovaný proces správy uživatelských přístupů.	Shromažďuje logy z Domain Controlleru pro sledování přidělování/odebírání práv. Přepošle kopii auditního logu s potvrzením akce přidělení/odebrání práv k uložení v tiketovacím systému jakožto důkaz.
A.9.2.3 Správa privilegovaných přístupových práv	Musí být omezeno a řízeno přidělování a používání privilego-vaných přístupových práv.	Shromažďuje logy z Domain Controlleru pro sledování přidělování/odebírání privilegovaných práv. Monitoruje přihlašování/odhlašování k privilegovaným účtům. Posílá pravidelné reporty o používání privilegovaných účtů, aby bylo vyhověno procesu kontroly (ukončení přístupu s vyšším oprávněním, není-li používán). Přepošle kopii auditního logu s potvrzením akce přidělení/odebrání práv k uložení v tiketovacím systému jakožto důkaz.
A.9.3 Odpovědnosti uživatelů		
Cíl: Učinit uživatele odpovědné za ochranu jejich autentizačních informací.		
A.9.3.1 Používání tajných autentizačních informací	Při používání tajných autent. informací musí být po uživatelích vyžadováno, aby dodržovali postupy stanovené organizací.	Monitoruje, které účty jsou používány více než jedním uživatelem (sdílené účty).



NEÚSPĚŠNÁ PŘIHLÁŠENÍ

0 to 42 of 42 available for paging

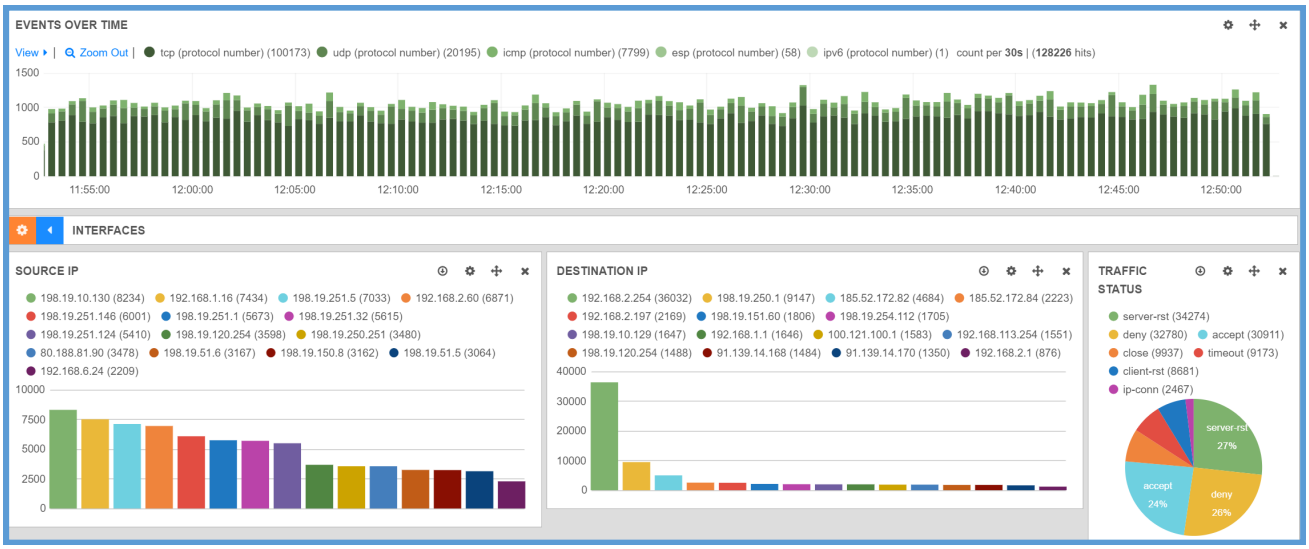
@timestamp	meta.src.host	msg.username	msg.eventid	msg.nasporttype	msg.status	msg.reason
2021-01-18T10:36:34.236+01:00	DC1	kratochvil	6273	Virtual	denied	The connection request did not match any configured net...
2021-01-18T09:29:50.558+01:00	DC1	admin	6273	Virtual	denied	Authentication failed due to a user credentials mismatc...
2021-01-18T08:52:41.290+01:00	DC1	okoh@gama	6273	Wireless - IEEE 802.11	denied	The remote RADIUS (Remote Authentication Dial-In User S...
2021-01-18T08:52:33.206+01:00	DC1	kratochvil	6273	Virtual	denied	The connection request did not match any configured net...
2021-01-18T08:44:45.447+01:00	DC1	vanourkova	6273	Virtual	denied	The connection request did not match any configured net...
2021-01-18T08:00:38.738+01:00	DC1	fwho@gama	6273	Wireless - IEEE 802.11	denied	The remote RADIUS (Remote Authentication Dial-In User S...
2021-01-18T07:51:14.331+01:00	DC1	pikhart	6273	Virtual	denied	The connection request did not match any configured net...
2021-01-18T07:39:54.089+01:00	DC1	dvorakova	6273	Virtual	denied	The connection request did not match any configured net...

Obrázek: Tabulka neúspěšných přihlášení k MS AD v LOGmanageru.

Oblast ISO27001	Popis opatření	Jak může LOGmanager pomoci s dosažením
A.9.4 Řízení přístupu k systémům a aplikacím		
Cíl: Předcházet neautorizovanému přístupu k systémům a aplikacím.		
A.9.4.1 Omezení přístupu k informacím	V souladu s politikou řízení přístupu musí být omezen přístup k informacím a funkcím aplikací.	Monitoruje, zda k datům přistupují pouze autorizovaní uživatelé. Upozorní na neautorizované použití.
A.9.4.2 Bezpečné postupy přihlášení	Pokud to politika řízení přístupu vyžaduje, musí být přístup k systémům a aplikacím řízen postupy bezpečného přihlášení.	Shromažďuje informace o úspěšném/neúspěšném přihlášení/odhlášení. Upozorní na zablokování účtu nebo na pokusy o přístup hrubou silou.
A.9.4.4 Použití privilegovaných programových nástrojů	Musí být omezeno a přísně kontrolováno použití programových nástrojů, které mohou být schopné překonat systémové nebo aplikační kontroly.	Loguje použití privilegovaných programových nástrojů.
A.9.4.5 Řízení přístupu ke zdrojovým kódům programů	Musí být omezen přístup ke zdrojovým kódům programů.	Sbírá logy o přístupu ke zdrojovým kódům programů a o změnách v nich.
A.10 Kryptografie		
Cíl: Zajistit řádné a efektivní používání kryptografie k ochraně důvěrnosti, autentičnosti a/nebo integrity informací.		
A.10.1.2 Správa klíčů	Politika pro používání, ochranu a dobu existence kryptografických klíčů musí být vytvořena a implementována po celou dobu jejich životního cyklu.	Loguje aktivity správy klíčů.
A.11.1 Bezpečné oblasti		
Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace.		
A.11.1.2 Fyzické kontroly vstupu	Aby bylo zajištěno, že je přístup do bezpečných oblastí povolen pouze oprávněným osobám, musí být tyto oblasti chráněny vhodným systémem vstupních kontrol.	Loguje data z fyzických kontrol vstupů/odchodů z bezpečné oblasti pro poskytnutí auditního záznamu.

Oblast ISO27001	Popis opatření	Jak může LOGmanager pomoci s dosažením
A.12.2 Ochrana proti malwaru		
Cíl: Zajistit, aby informace a vybavení pro zpracování informací byly chráněny proti malwaru.		
A.12.2.1 Opatření proti malwaru	Na ochranu proti malwaru musí být implementována opatření na jeho detekci, prevenci a obnovu, a to ve spojení s odpovídajícím bezpečnostním povědomím uživatelů.	Shromažďuje logy z více bezpečnostních zařízení a sledujte hrozby v jednotné konzoli. Shromažďuje logy z AV a generujte naplánované zprávy, abyste prokázali pravidelný proces skenování AV. Upozorní na detekci hrozeb bezpečnostními zařízeními. Provádí pravidelné činnosti lovu hrozeb (např. kontrola logů síťového provozu pro kanál Command & Control). V případě incidentu použijte LM k provedení analýzy hlavních příčin (kdo, kde, kdy, jak).
A.12.4 Zaznamenávání formou logů a monitorování		
Cíl: Zaznamenávat události a vytvářet záznamy.		
A.12.4.1 Zaznamenávání událostí formou logů	Musí být pořizovány, uchovány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.	Použijte LOGmanager ke sběru logů z jakýchkoliv zdrojů ve vaší infrastruktuře. Uchovávejte je tak dlouho, jak potřebujete (online v interní databázi, offline v digitálně podepsané záloze). Pro vizualizaci logů použijte připravené nebo vlastní dashboardy, které vám pomohou s procesem kontroly. Vytvořte si vlastní nebo použijte připravené vzory upozornění k proaktivnímu monitoringu hrozeb.
A.12.4.2 Ochrana logů	Prostředky pro zaznamenávání formou logů a logy musí být chráněny proti zfalšování a neoprávněnému přístupu.	Logy uložené v databázi LOGmanageru nemohou být smazány ani nijak modifikovány.
A.12.4.3 Logy o činnosti administrátorů a operátorů	Aktivity systémového administrátora a systémového operátora musí být logovány a logy chráněny a pravidelně přezkoumávány.	Použijte LOGmanager ke shromažďování auditních logů privilegovaných uživatelů z jakýchkoliv zdrojů ve vaší infrastruktuře. Monitorujte používání LOGmanageru a změny v něm provedené. Použijte připravené nebo vytvořte vlastní dashboardy pro vizualizaci logů, které vám pomohou s procesem kontroly.
A.12.4.4 Synchronizace hodin	Hodiny všech důležitých systémů pro zpracování informací musí být v rámci organizace nebo bezpečnostních domén synchronizovány s jediným referenčním zdrojem času.	LOGmanager přidává vlastní, důvěryhodné časové razítko ke každé přijaté zprávě, čímž zajistí synchronizaci času napříč všemi shromážděnými logy.

Oblast ISO27001	Popis opatření	Jak může LOGmanager pomoci s dosažením
A.13.1 Správa bezpečnosti sítě		
Cíl: Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací.		
A.13.1.1 Opatření v sítích	K ochraně informací v systémech a aplikacích musí být sítě řízeny, spravovány a kontrolovány.	Shromažďuje logy ze zařízení v síti. Upozorní na kritické události. Koreluje data z více zdrojů pro detekci provozních anomálií v síti.
A.13.1.2 Bezpečnost síťových služeb	Musí být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní mechanismy, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb, ať už jsou zajišťovány interně nebo cestou outsourcingu.	Shromažďuje logy ze zařízení v síti. Pomocí vizualizace zkontrolujte technické parametry a pravidla brány firewall. Upozorní na kritické události a zneužití (příklad: opakované neúspěšné pokusy o přihlášení).
A.14.1 Bezpečnostní požadavky informačních systémů		
Cíl: Zajistit, aby se bezpečnost informací stala nedílnou součástí informačních systémů v jejich celém životním cyklu. To zahrnuje i požadavky na informační systémy, které poskytují služby ve veřejných sítích.		
A.14.1.2 Zabezpečení aplikačních služeb ve veřejných sítích	Informace přenášené ve veřejných sítích v rámci aplikačních služeb musí být chráněny před podvodnými aktivitami, zpochybňováním smluv, neoprávněným vyzrazením a modifikací.	Shromažďuje logy z Domain Controlleru a ze zařízení v síti. Upozorní na změny GPO a chyby, které mohou mít vliv na veřejné služby. Monitorujte nešifrovanou datovou komunikaci napříč veřejnou sítí (příklad: FTP, Telnet, SNMPv2).



Obrázek: Vizualizace síťového provozu dle Firewallu.

Oblast ISO27001	Popis opatření	Jak může LOGmanager pomoci s dosažením
A.14.3 Data pro testování		
Cíl: Zajistit ochranu dat používaných pro testování.		
A.14.3.1 Ochrana dat pro testování	Data pro testování musí být pečlivě vybrána, chráněna a kontrolována.	Shromažďuje příslušné logy operačních dat, aby bylo možné prokázat, kdy byla zkopírována pro testovací účely. Sledujte stav těchto dat (kdo k nim přistupoval a kdy).
A.15.1 Bezpečnost informací i v dodavatelských vztazích		
Cíl: Zajistit ochranu aktiv organizace, ke kterým mají dodavatelé přístup.		
A.15.1.2 Bezpečnostní požadavky v dohodách s dodavateli	Všechny požadavky relevantní bezpečnosti informací musí být ustaveny a odsouhlaseny s každým dodavatelem, který může přistupovat k informacím organizace, zpracovávat je, ukládat, komunikovat nebo je zajišťovat prvky IT infrastruktury.	Shromažďuje logy ze síťových zařízení/Domain Controlleru/přístupu k souborům (a další, pokud jsou relevantní) pro monitoring aktivity dodavatelů.
A.16.1 Řízení incidentů bezpečnosti informací a zlepšování		
Cíl: Zajistit odpovídající a efektivní přístup ke zvládání incidentů bezpečnosti informací zahrnujícímu komunikaci ohledně bezpečnostních událostí a slabých míst.		
A.16.1.2 Hlášení událostí bezpečnosti informací	Události bezpečnosti informací musí být co nejrychleji hlášeny příslušnými řídícími kanály.	Upozorní na vybrané bezpečnostní události. Provádí korelace mezi zdroji za účelem detekce potenciálních bezpečnostních incidentů. Shromažďuje logy ze všech bezpečnostních zařízení a agreguje je. Přijímejte nakonfigurovaná bezpečnostní upozornění prostřednictvím e-mailu. Generujte denní hlášení bezpečnostních incidentů.
A.16.1.7 Shromažďování důkazů	Organizace musí definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování informací, které můžou sloužit jako důkazy.	S logy shromážděnými LOGmanagerem není možné manipulovat, takže mohou být použity při vyšetřování incidentů (analýza hlavních příčin). Přístup k citlivým informacím může být omezen pouze na autorizovaný personál.

Návrhy a doporučení k tomuto návodu prosím zasílejte na email adresu: security-team@logmanager.cz

INFORMACE O VÝROBCI A DALŠÍ REFERENCE

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Na stránkách www.logmanager.cz naleznete vybrané reference. Mezi naše zákazníky patří nejen státní správa, ale i průmyslové podniky všech velikostí a oborů, obchodní společnosti, společnosti z oblasti bankovnictví a další. Pro podrobnější list referencí přímo z oblasti Vaší činnosti nás neváhejte poptat. Příslušné kontakty na stávající zákazníky, kteří souhlasí s uváděním na referenčním listu, rádi předáme.