

Log Management med LogInspect

Beskyt din virksomhed ved at få kontrol over dine krav til:

Compliance

Trusler

Optimering

ImmuneSecurity leverer software-løsninger med fokus på IT-sikkerhed og i særdeleshed SIEM og Log Management. ImmuneSecurity har tradition for at være en partner for vores kunder. De lytter til deres krav og tilpasser løbende løsningerne. Kendetegnet ved ImmuneSecurity's løsninger er nem installation, brugervenlighed, nem administration og god support.

Reports

Templates

Add Template View All Jobs

List Actions: Select All Deselect All Delete Selected Delete All View Jobs For Selected

Title	Description	Created	Actions
test for september	This report is generated by a small amount of the PCI compliance	2009-10-14 11:09:09	
Firewall Activity	Firewall statistics	2009-08-31 13:35:58	
SOX Compliance Report	User activity and application related data	2009-08-31 13:35:58	
Information Security Report	User activity, security, events, netflow analysis and incidents	2009-08-31 13:35:58	
DS484 Compliance Report	Similar to SOX report, but with security information added.	2009-08-31 13:35:58	
GLBA Compliance Report	All user activity info and audit log changes.	2009-08-31 13:35:58	
HIPAA Compliance Report	All user activity info, audit log changes and total number of syslog events	2009-08-31 13:35:58	
Test PCI Jan. 2010	All user login info and audit log changes.	2009-08-31 13:28:58	

Page 1 of 1

List Actions: Select All Deselect All Delete Selected Delete All View Jobs For Selected

Displaying 1 - 8 of 8

LogInspect's indbyggede rapportgenerator gør det nemt at lave compliance dokumentation

Om ImmuneSecurity

ImmuneSecurity er en skandinavisk virksomhed, som fokuserer på at sikre aktiver i virksomheder og organisationer. ImmuneSecurity's engagerede medarbejdere står klar til at supportere vores kunder med at nå deres mål inden for compliance, IT-sikkerhed og andre IT-operationelle udfordringer.

LogInspect - omdan en SIEM løsning til en reel forretningsmæssig værdi.

Der er flere og flere virksomheder og organisationer, der indser og accepterer, at en Log Management-løsning har en forretningsmæssig værdi. Automatisering af regulerende processer, forbedret effektivitet af retstekniske undersøgelser gør det nemmere at foretage fejlfinding, og man opnår en langt bedre sikkerhed.

LogInspect er en intelligent platform, som anvender begivenheder og hændelser fra de millioner af logs, der i dag findes i enhver IT-infrastruktur. De filtrerede og korrelerede resultater vises i LogInspect's betjeningspanel, der kan konfigureres alt afhængig af brugerens roller, rettigheder og ansvar.

Investeringsafkast:

- LogInspect leverer en værdifuld need-to-have dokumentation for compliance i en let forståelig rapport, som kan brugerdefineres...
- LogInspect er et must-have værktøj til sikkerhed og beskyttelse af din virksomheds aktiver, som fx trusler fra brud på IT-sikkerheden i dit netværk ...
- LogInspect leverer et dybdegående indblik i effektiviteten af IT-infrastrukturen ved at fremhæve områder, der kan optimeres og hvor omkostningerne kan reduceres ...
- LogInspect er nemt at implementere, intuitivt, sikkert og kan brugertilpasses meget hurtigt via det veldesignede betjeningspanel ...

LogInspect har en ROI på mindre end 6 måneder.

LogInspect indsamler og opbevarer data fra enhver kilde ...

- LogInspect giver dig mulighed for at få et sikkert og centraliseret log arkiv, der automatisk analyserer logmeddelelserne i real-tid. Log konsolidering og sikker opbevaring af dokumentation via én enkelt konsol gør det let for dig at få adgang til og administrere alle dine oplysninger. Det sikre arkiv vil sikre, at du ikke mister nogen logmeddelelser på grund af et systemnedbrud eller et hacker angreb.

LogInspect analyserer og alarmerer automatisk

- Den indbyggede og intelligente loganalyse motor vil automatisk detektere og alarmere dig, når en kritisk hændelse opstår. Et event (hændelse) kunne være et løbende angreb, et kompromitteret system, et system nedbrud eller brugergodkendelse.

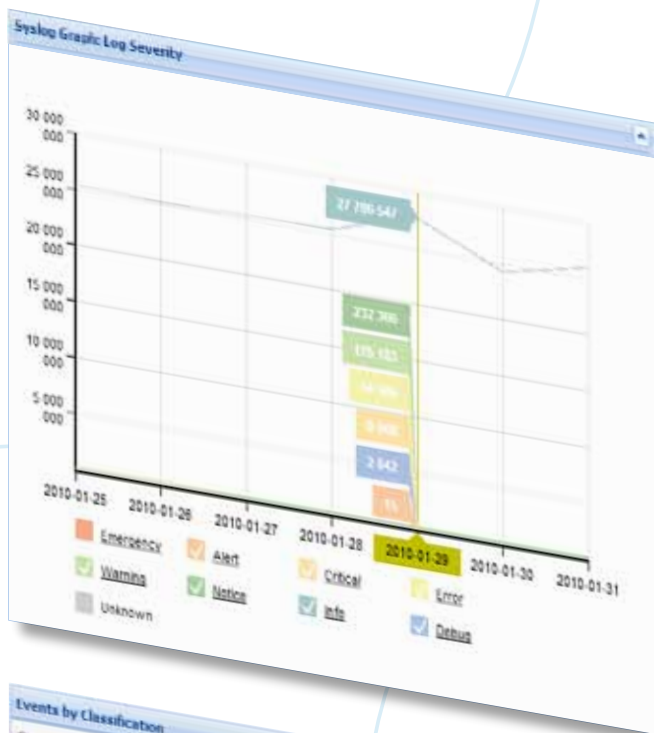
LogInspect - betjeningspanelet

- Log Management kan være meget værdifuldt, hvis de indsamlede oplysninger bruges proaktivt. LogInspect giver dig et struktureret overblik, så du kan reagere hurtigt og spotte nye tendenser og gå i dybden med de relevante oplysninger.

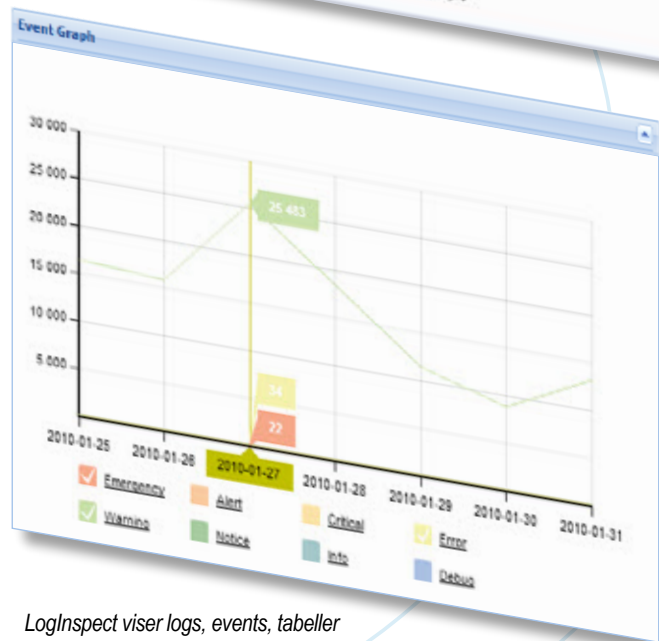
LogInspect - Revision og compliance på den nemme måde

- LogInspect kan hjælpe dig med at opnå et fuldstændigt overblik over dit netværk, og hjælper dig med at overholde virksomhedens gældende regler på området. LogInspect indeholder prædefinerede skabeloner til de mest almindelige compliance- og sikkerhedsrapporter.

PCI-DSS
SOX
HIPAA
Basel-II
ISO17799
ISO27001



Classification	Count	Last Update
Successful user authentication		
Failed user authentication	19110	2010-01-26 17:36:00
Application Error	8	2010-01-27 15:19:06
Application Notice	22	2010-01-31 19:19:06
Access control violation	22000	2010-01-27 21:45:59
User login	4	2010-01-28 11:38:01
Network issues	21878	2010-01-28 10:44:58
Failed administrative authentication	4	2010-01-28 00:30:52
Account Modified	8	2010-01-29 14:33:50
Network service banner changed	5	2010-01-26 16:25:29
	42	2010-01-25 01:19:00



LogInspect viser logs, events, tabeller og grafer i en let konfigurerebar widget.

Funktioner i LogInspect:

Risk Assessment

Fortrolighed, integritet, tilgængelighed (CIA). Med denne model er det muligt at gennemføre en beregning af en trussels indvirkning og tildele den en scoring/ranking og fokusere på de vigtigste events først.

Betjeningspanelet – der giver overblik

Det avancerede betjeningspanel er baseret på WEB 2,0 og giver mulighed for at lave en individuel brugerkonfiguration. Visningen af informationer i betjeningspanelet er afhængigt af brugernes roller og rettigheder. Betjeningspanelet viser kritiske events og sikkerhedsbrister i real-tid.

Event Korrelation

LogInspect's Event Correlation Engine (ECE) kan detektere adfærd som fx flere mislykkede login, efterfulgt af et vellykket login fra samme bruger, der vil udløse et "Attempted Brute-force Login" event.

LogInspect's Network Abnormally Detection Engine (NADE) kan udløse et event på baggrund af uregelmæssigheder i netflowet. Fx kan en "Muligt smittet Spam Host" påvises bare ved at kigge på adfærden i netværkstrafikken.

Active Respons Engine

Tillader at brugerne modtager en e-mail på baggrund af opståede sikkerhedshændelser og giver mulighed for automatisk at blokere en IP i Firewall eller lukke brugerne, hvis mistænkelige sikkerhedshændelser opstår.

Open Rule Framework

Open Rule Framework giver mulighed for, at alle brugere kan oprette regler og tillader at dele regler om krav, herunder underskifter for korrelation, log signatur eller NADE. LogInspect's ImmuneSecurity Certified Signatures opdateres automatisk med nye regler når de foreligger, så er du altid up-to-date.

Rapportering out-of-the-box

LogInspect indeholder standard skabeloner til fx rapportering om compliance som PCI, SOX, DS-484, HiPAA m. fl. og er en del af LogInspect's standardversion. Skabelonerne kan tilpasses efter behov eller oprette en brugerdefineret rapport ved hjælp af den intuitive LogInspect Report Wizard.

Systemkrav

LogInspect leveres som en prækonfigureret enhed men kan også afvikles problemfrit i et VMware miljø. LogInspect er skalerbar og kan således tilpasses ethvert behov og størrelse.

Licensering

LogInspect's licensering er baseret på en årlig afgift, der omfatter alle nye opgraderinger, patches og signature abonnementer samt e-support via ImmuneSecurity Ticket System, og der er således ingen yderligere maintenance.



ImmuneSecurity's Managed Services ... sætter nye standarder for SIEM og Log Management

LogInspect's SIEM løsning er kompleks på den nemme måde - nem implementering og ingen maintenance er bare nogen af fordelene ved LogInspect. Mange virksomheder har allerede opdaget yderligere fordele ved at lade ImmuneSecurity håndtere rapporteringen og administrationen af LogInspect.

Skræddersyet Log Management løsning og administreret tjeneste, der typisk leveres på uge-, måneds- eller kvartalsbasis

Om Draware™ A/S:

Vi er uafhængige eksperter i netværk og server management inklusive discipliner som helpdesk, loganalyse, remote control, NMS, dokumentation mm. Vi hjælper dig i alle faser fra POC over indkøb til implementering, undervisning, support og maintenance,

Danmark:

Draware™ A/S
Teglgården 46
DK- 3460 Birkerød
Tlf.: (+45) 45 76 20 21
Fax: (+45) 45 76 41 21
E-mail: info@draware.dk

Sverige:

Draware™ A/S
Teglgården 46
DK- 3460 Birkerød
Tlf.: 020 1 20 20 26
Fax: (+45) 45 76 41 21
E-mail: info@draware.se