

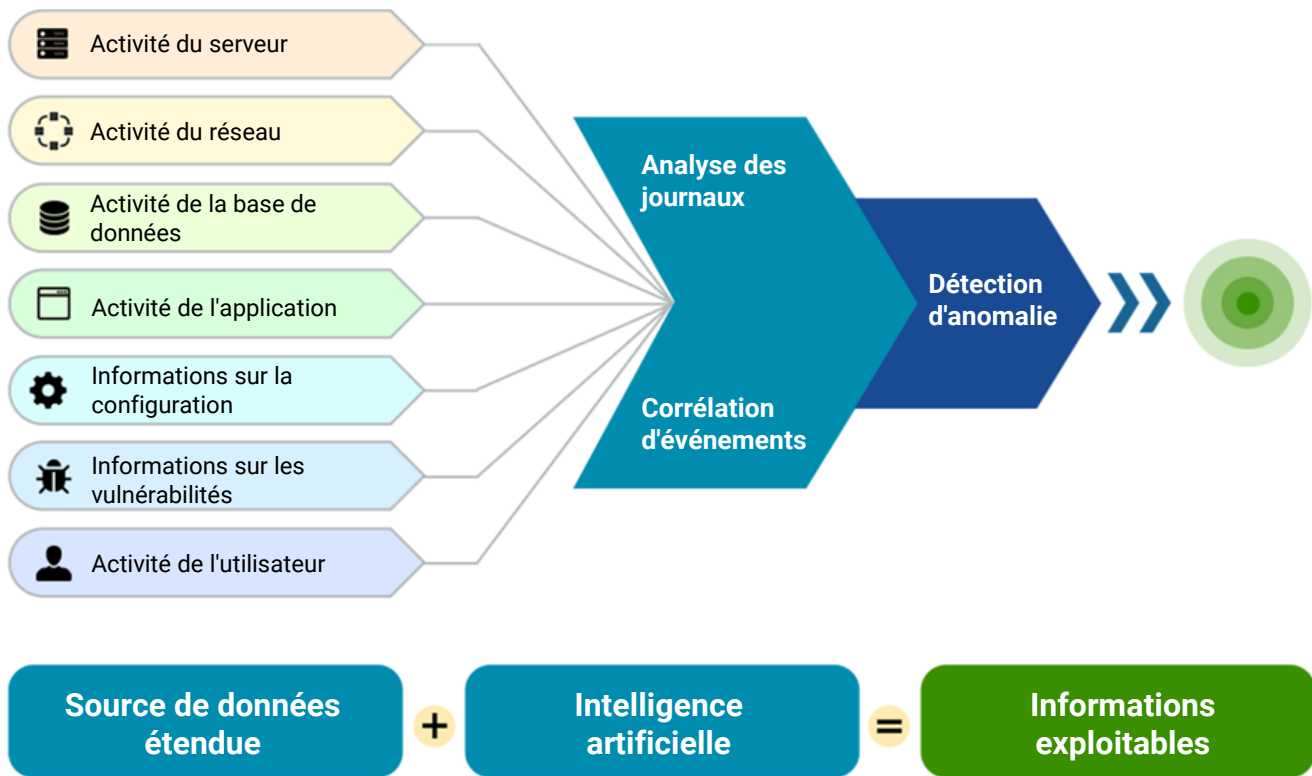


ManageEngine   
**EventLog Analyzer**

**Une solution complète de gestion des journaux**

<https://www.pgsoftware.fr/siem/eventlog-analyzer>

# Que peut faire EventLog Analyzer ?



# Programme

---

## 1. Gestion des journaux

- Collecte des journaux
- Analyse des journaux
- Corrélation des journaux
- Archivage des journaux

## 2. Audit complet

- Audit des périphériques réseau
- Audit des applications

## 3. Renseignements sur les menaces

- Alertes de flux de menaces
- Gestion des incidents

## 4. Système intégré de gestion de la conformité

## 5. Différenciateurs de produits

# Gestion des journaux

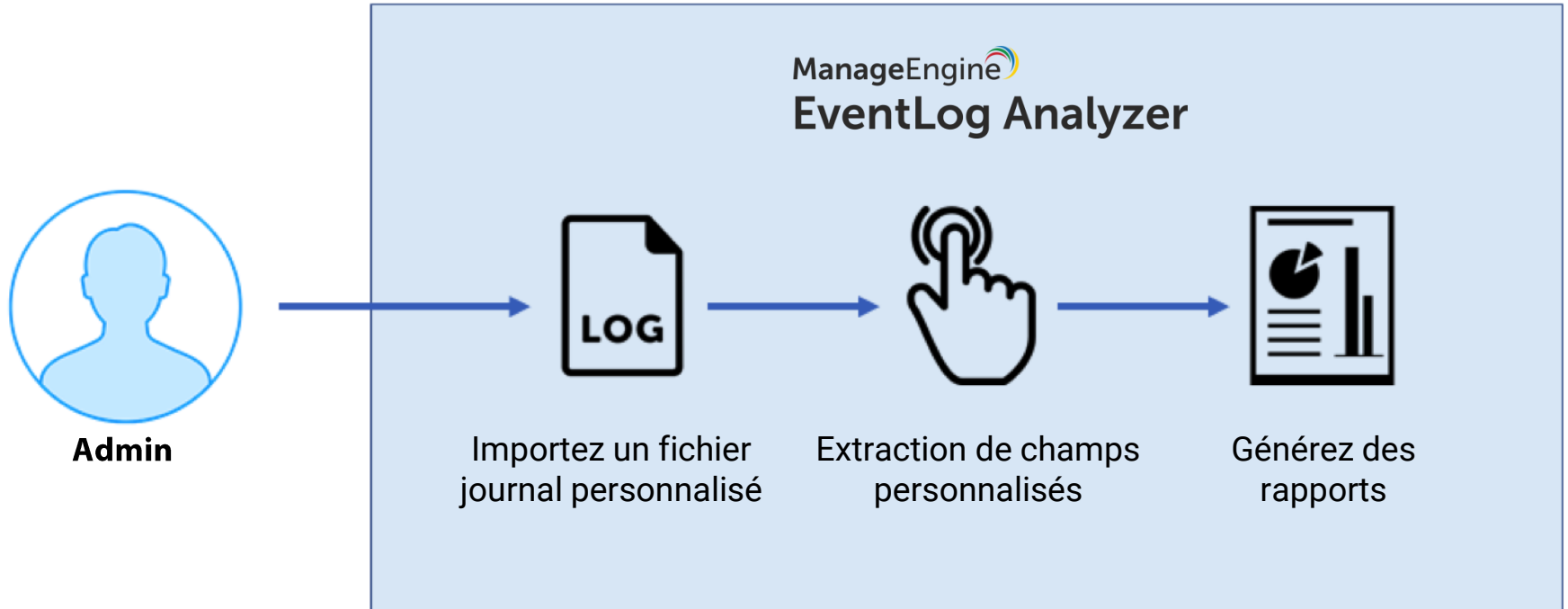


# Gestion des journaux

---

- **Prend en charge les méthodes de collecte de journaux avec et sans agent.**
- **Prend en charge +600 sources de journaux, notamment:**
  - Périphériques réseau : routeurs, commutateurs, IDS/IPS et pare-feu.
  - Serveurs Windows et Linux/Unix, machines IBM AS400
  - Serveurs Oracle et Microsoft SQL
  - Serveurs Apache et IIS
  - Scanners de vulnérabilité, solutions de renseignement sur les menaces, etc.
- **Permet d'analyser tout format de journal lisible par l'homme à partir de dispositifs personnalisés, d'applications internes, etc.**

# Collecte des journaux : Analyse personnalisée des journaux



# Collecte des journaux : Analyse personnalisée des journaux

The screenshot displays a log analysis tool interface. A dialog box titled "Extract Additional Fields" is open, showing the configuration for a custom field named "Port\_number".

**Extract Additional Fields**

Log Type : admp-app2-cogserver.log

Select & click the field value to be extracted

10.38.12.85-9300 7652 2010-03-03 17:37:47.838  
Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/reportService/1.absolute

Field Name(s) should only be alphanumeric. i.e [a-zA-Z0-9\_]{1,255}

Details for field value : 7652

Field Name \* Port\_number

Generated Pattern : [Validate](#) this pattern (or) [Choose](#) another pattern

(?sm)(?!\s\*(?<Port\_number>.+))s+

[Save Pattern](#) [Cancel](#) [Ask Support](#)

**Matched Log Messages (23)**

Message : 10.38.12.85-9300 7652 2010-03-03 17:37:45.010 -5 EDEA0CACEDB602F1C883EAF55BAA3E8AAA19E90 dv2ws92Mlx42qMssMq22wwhdG4vC9hsG2MhGyl 687 Thread-2707 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/reportService/1.absolute

Port\_number:7652

Message : 10.38.12.85-9300 7652 2010-03-03 17:37:46.010 -5 B64467B4285B805FDC916314C3964A71F2B14A04 jy2Mshj8 GMC4sqh9Ch2MG4y8C2vC99GqMjGMlvd 42178 Thread-10906 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/contentManagerService/1

Port\_number:7652

Message : 10.38.12.85-9300 7652 2010-03-03 17:37:47.838 -5 B64467B4285B805FDC916314C3964A71F2B14A04 sG2v8lM w8lG9sy9vG9j8sq122vsq2sG84wq9ll 42180 Thread-26316 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/contentManagerService/1

Port\_number:7652

Message : 10.38.12.85-9300 7652 2010-03-03 17:37:47.978 -5 B64467B4285B805FDC916314C3964A71F2B14A04 ylsyq9lw2 dv8w8q2jv8vlls4ww44d4q1vj2hlvj 42182 Thread-10906 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/contentManagerService/1

# Analyse des journaux

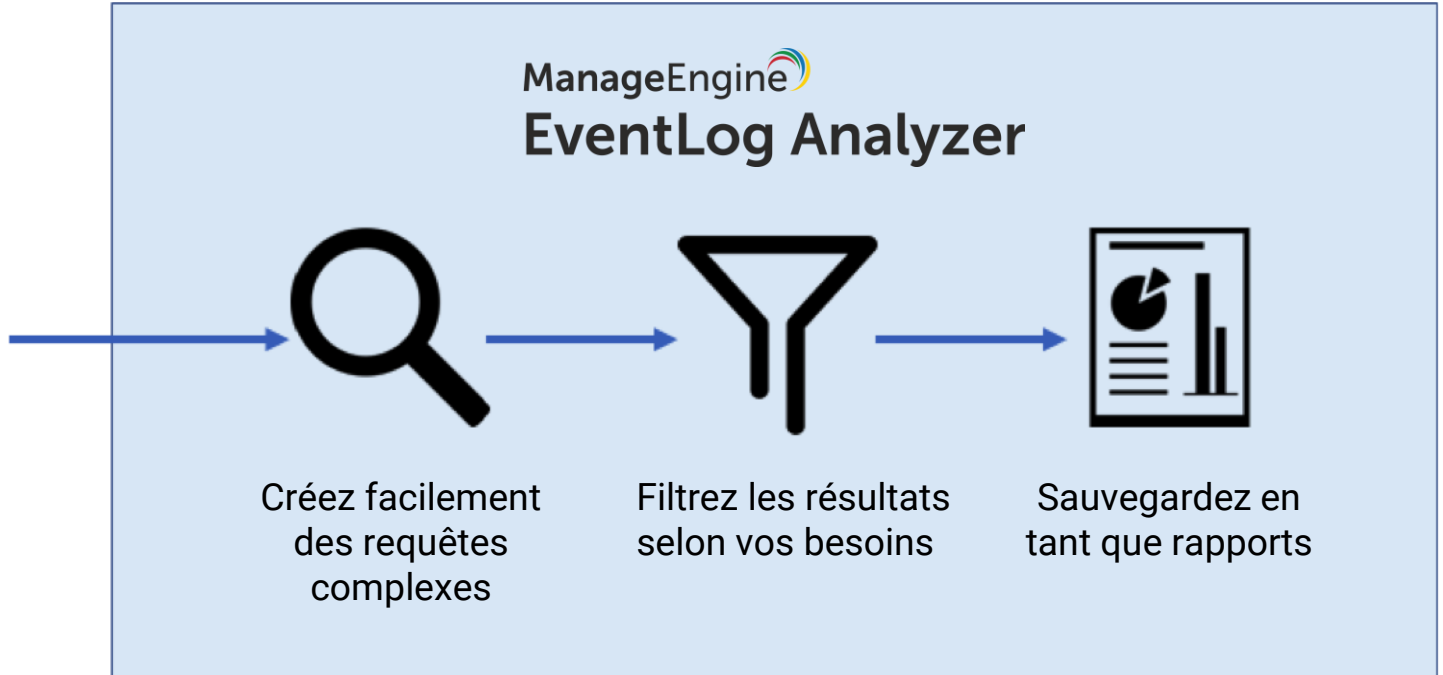
---

- **+1000 rapports et profils d'alerte prêts à l'emploi pour répondre à vos besoins en matière de sécurité, d'audit et de conformité.**
- **Création de rapports et de profils d'alerte personnalisés pour répondre à vos besoins spécifiques.**
- **Effectuez des analyses détaillées des journaux et recherchez parmi des millions de journaux à l'aide d'un moteur de recherche rapide et facile à utiliser, capable de traiter:**
  - **20 000 syslogs/seconde**
  - **2 000 journaux d'événements Windows/seconde**

# Analyse des journaux : Analyse forensique des journaux



**Admin**



# Analyse des journaux : Analyse forensique des journaux

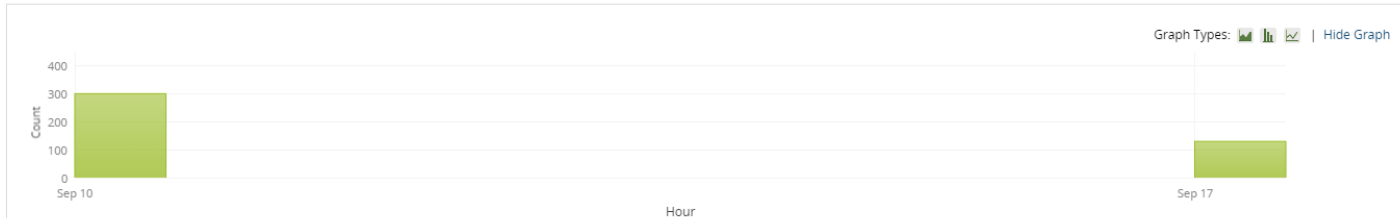
192.168.218.136. Pick Device All Log Types ▾

Basic | Advanced

USERNAME = "administrator"

Go Save Search Save as Alert

✕ Clear Search



How to extract fields? Showing : 1 - 10 of 431 View per page : 10 Add/Remove Fields

Message : Windows Installer installed the product. Product Name: Oracle VM VirtualBox 5.2.2. Product Version: 5.2.2. Product Language: 1033. Manufacturer: Oracle Corporation. Installation success or error status: 0. 126244

Profile Value : - Target User : - Accesses : - GUID : - Source Port : 514 Process Name : - Group Domain : - Chantype Details : - Rule Name : - Target Ip : - Source : Ms  
Installer Previous Value : - Session Type : - Member Group SID : - Share Path : - SID Filtering : - Severity : Information Service Type : - Packet Discarded : - Domain : -  
Fault Module : - Object Name : - Top And Least Values for field - SEVERITY

Top Values				Least Values			
Value	Count	Percentage		Value	Count	Percentage	
failure	215	49.88%	<div style="width: 49.88%;"></div>	information	87	20.19%	<div style="width: 20.19%;"></div>
success	129	29.93%	<div style="width: 29.93%;"></div>	success	129	29.93%	<div style="width: 29.93%;"></div>
information	87	20.19%	<div style="width: 20.19%;"></div>	failure	215	49.88%	<div style="width: 49.88%;"></div>

Service Name : Oracle VM Virtual  
:- Security Id : - Passwd  
Type : - Machine Name : -  
- Version : 5.2.2 Max Pa  
- Update Name : - Lock  
- New Filename : - Encr  
17:59:30 Username : admin

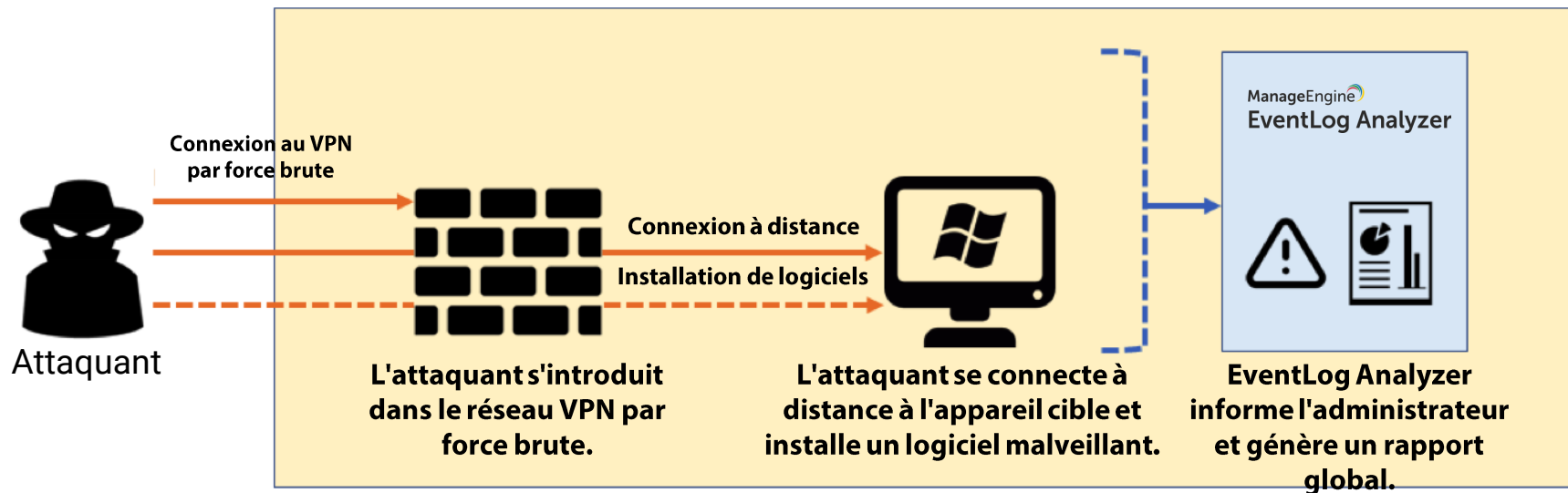
Malware Name  
pires : - File  
Object type :  
Privilege :  
Intelligence :  
Sep 2017,

# Corrélation des journaux

---

- **Plus de 30 règles de corrélation prédéfinies pour détecter les schémas d'attaque sur l'ensemble des appareils.**
- **Détectez les anomalies telles que les installations logicielles suspectes, les attaques telles que l'activité des vers, et plus encore.**
- **Visualisez des rapports agrégés qui présentent la trace des journaux sous forme de chronologie.**
- **Constructeur de règles de corrélation personnalisées pour créer et détecter des modèles d'attaque spécifiques à votre environnement professionnel.**

# Corrélation des journaux: Exemple



# Corrélation des journaux: Événements corrélés

The screenshot displays the EventLog Analyzer interface. A modal window titled "Event history" is open, showing a list of correlated events. The background interface includes a search bar, a sidebar with threat categories, and a main log view.

Time	Event Description	Details
13:50:52 05 Jan 2018	A software is installed on Windows. Windows Installer installed the product. Product Name: Oracle VM VirtualBox 5.2.2. Pr...	<a href="#">Details</a>
13:44:58 05 Jan 2018	A windows account successfully logs on using remote logon. An account was successfully logged on. Subject: Security ID: 5-1-0-0 Account Name: - ...	<a href="#">Details</a>
13:42:40 05 Jan 2018	A user successfully logged on to the network using Fortinet VPN. date=2018-01-05 time=13:42:40 devname=FortiGate-VM devid=FGVMEV0000000000 I...	<a href="#">Details</a>
13:42:13 05 Jan 2018	A user failed to log on to the network using Fortinet VPN. date=2018-01-05 time=13:42:13 devname=FortiGate-VM devid=FGVMEV0000000000 I...	<a href="#">Details</a>
13:42:09 05 Jan 2018	A user failed to log on to the network using Fortinet VPN	<a href="#">Details</a>
13:42:09 05 Jan 2018	A user failed to log on to the network using Fortinet VPN. date=2018-01-05 time=13:42:09 devname=FortiGate-VM devid=FGVMEV0000000000 I...	<a href="#">Details</a>

Background interface details:

- EventLog Analyzer Home
- Search available reports
- System/server threats
- Web server threats
- Database threats
- Ransomware attacks
- File integrity threats
- Potential Windows threats
  - Repeated registry entry failures
  - Multiple system audit policy changes
  - Possible worm activity
  - Excessive application crashes
  - Windows backup repeated failures
  - Eventlogs cleared
  - Notable account lockouts
  - Unexpected shutdowns
  - Suspicious service installed
  - Suspicious software installation
- Potential Unix threats
- Scheduled Reports

Log view details:

- 2017-12-10 00:00 to 2018-01-08 23:59
- 1 - 3 of 3 | 10
- History
  - [View History](#)
  - [View History](#)
  - [View History](#)

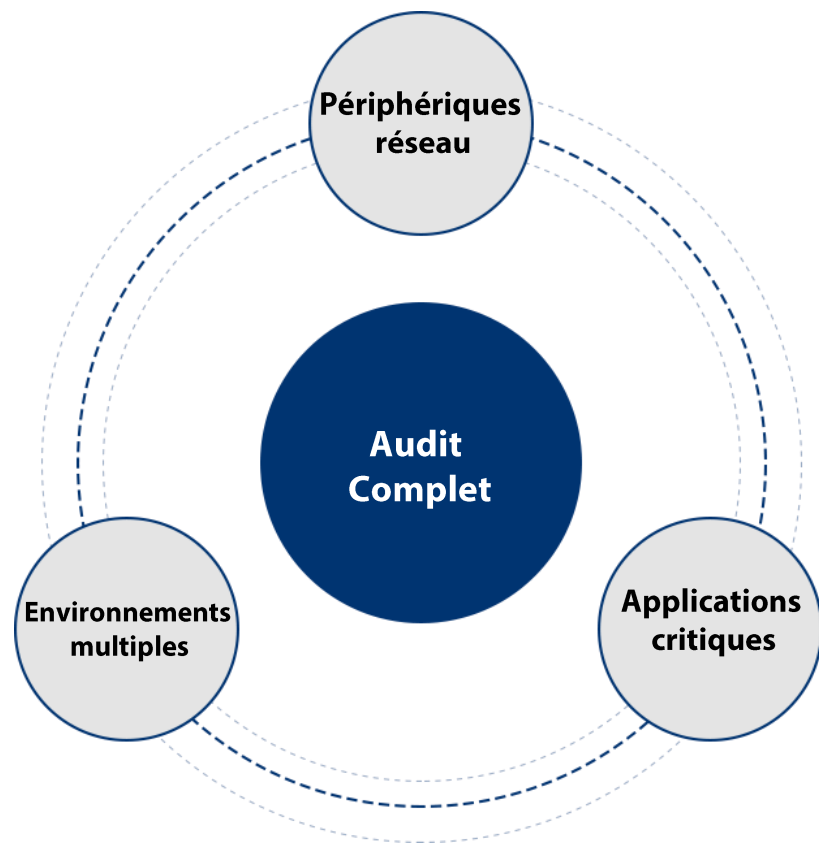
# Archivage des journaux

---

- **Les fichiers journaux sont cryptés afin de garantir que les données des journaux sont sécurisées pour les analyses forensiques, la conformité et les audits internes futures.**
- **Par défaut, un fichier d'archive des journaux contenant tous les journaux bruts reçus est créé toutes les 24 heures. Ces fichiers sont ensuite compressés tous les 7 jours pour économiser de l'espace sur le disque dur.**
- **À tout moment, le fichier peut être chargé dans la base de données de l'EventLog Analyzer et des rapports peuvent être générés pour les données d'événements archivées.**

# Audit Complet

---

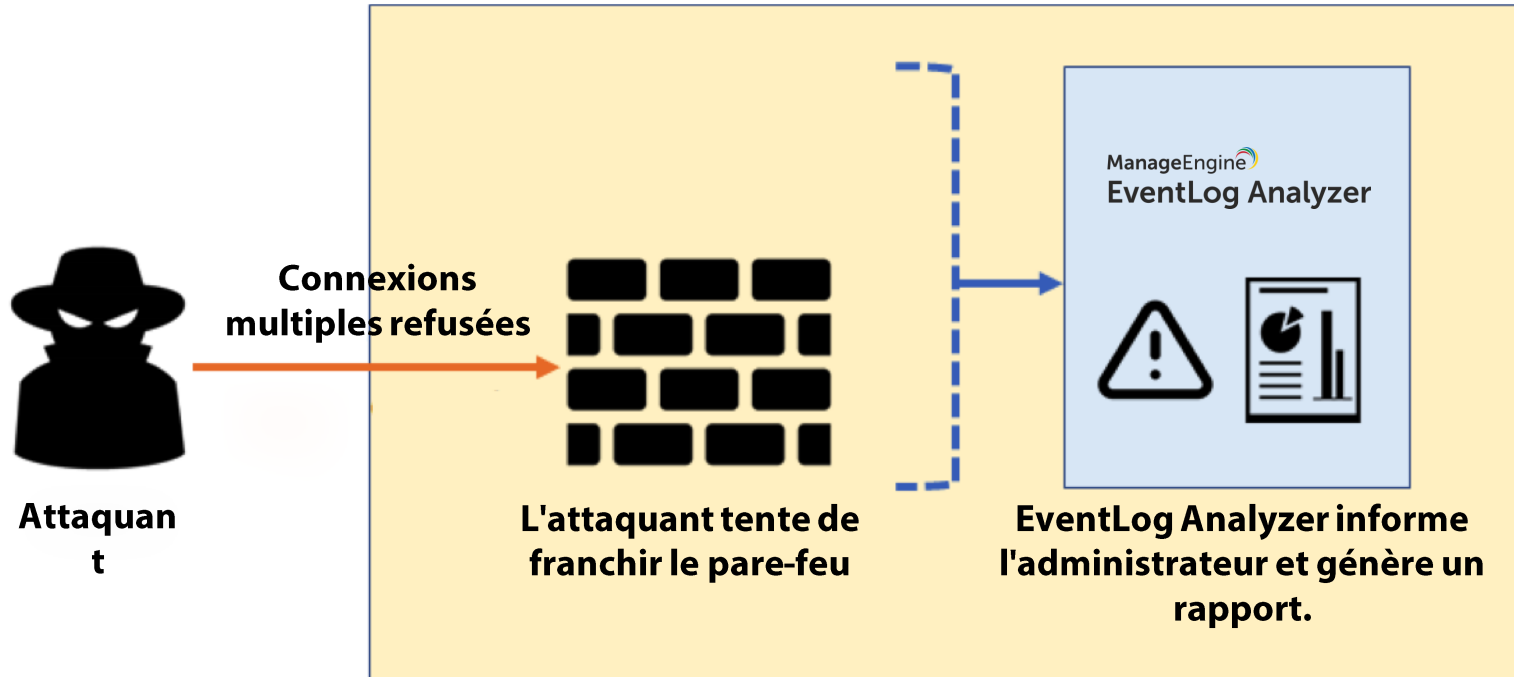


# Audit des périphériques réseau

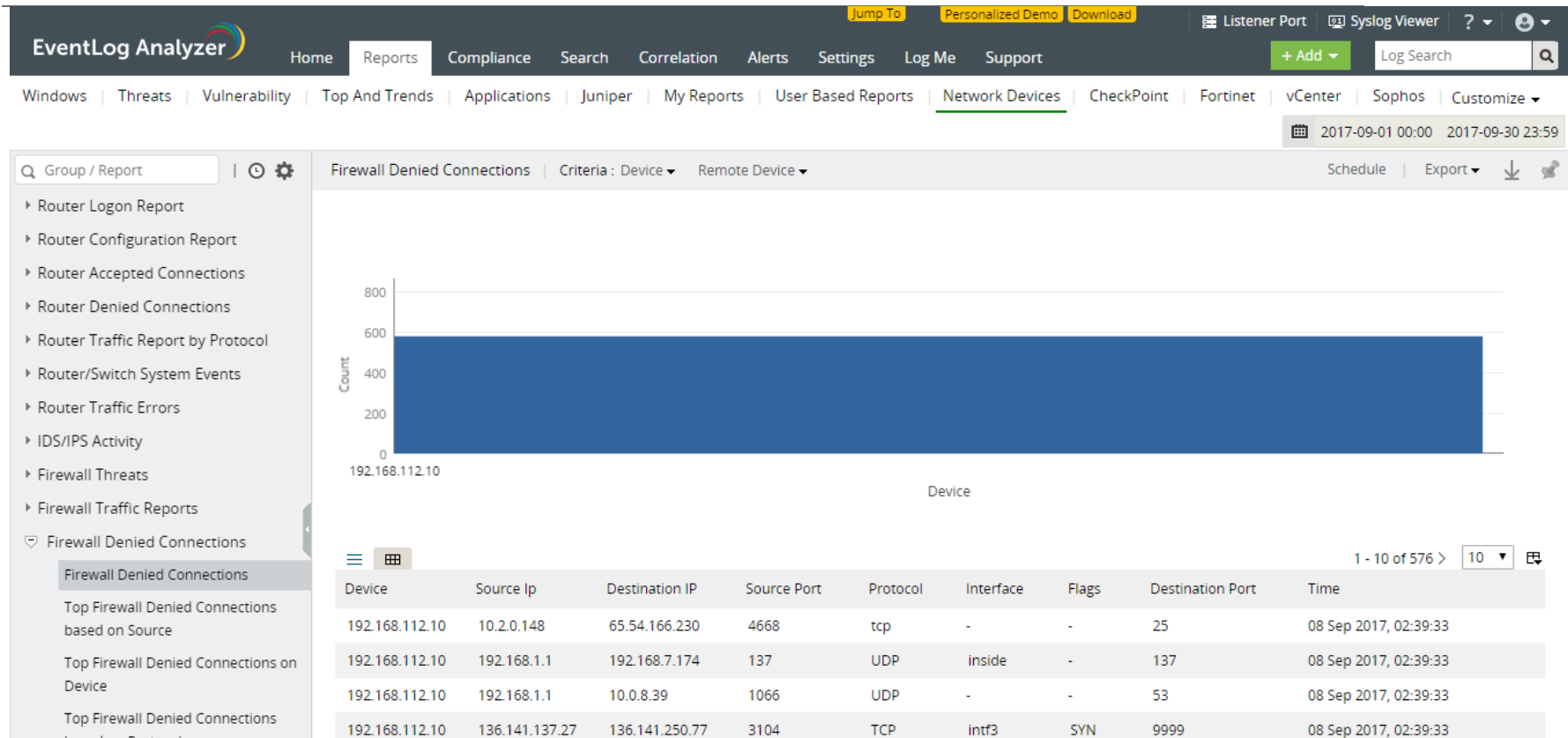
---

- **Surveillez les configurations des pare-feu et les modifications des règles.**
- **Identifiez les tentatives d'accès non autorisées et les escalades de privilèges sur les dispositifs du périmètre.**
- **Détectez les connexions refusées, les menaces et autres incidents anormaux sur vos routeurs, commutateurs, pare-feu et dispositifs IDS/IPS.**

# Audit des périphériques réseau : Tentative de violation du pare-feu



# Audit des périphériques réseau : Tentative de violation du pare-feu

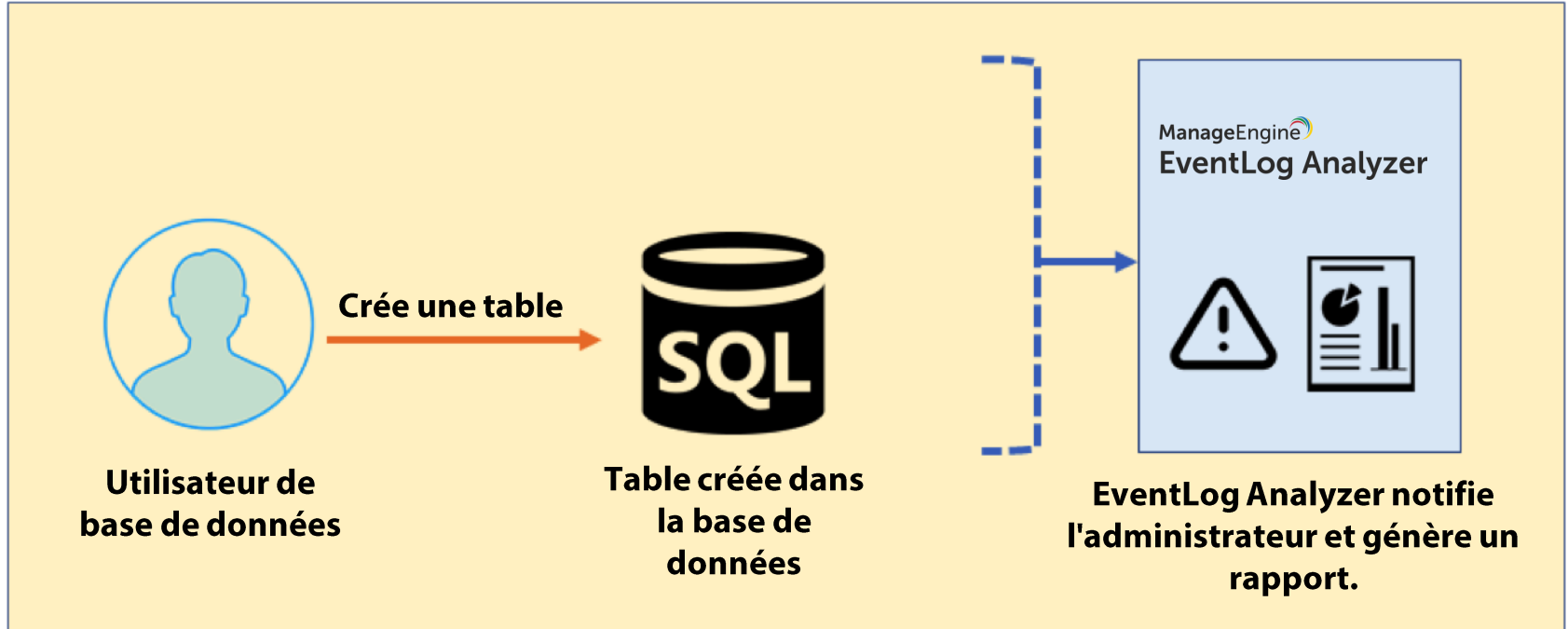


# Audit des applications

---

- **Automatisez l'importation des données des journaux d'applications: Extrayez des rapports de sécurité à partir des journaux importés et analysez les journaux d'applications internes à l'aide de l'analyseur de journaux personnalisé.**
- **Sécurisez les serveurs web IIS et Apache: Identifiez les activités anormales telles que les événements d'erreur, les tentatives de connexion échouées et les attaques de serveur en temps réel.**
- **Auditez les bases de données Microsoft SQL Server et Oracle: Suivez les actions des utilisateurs, les requêtes DML et DDL, les modifications des bases de données et les changements de compte serveur.**
- **Audit des scanners de vulnérabilité et des solutions de renseignement sur les menaces: Obtenez des informations détaillées sur les principaux ports et hôtes vulnérables, les infections, les vols de données, les risques de sécurité potentiels, etc.**

# Audit des applications : Tables créées par un utilisateur spécifique



# Audit des applications : Tables créées par un utilisateur spécifique

Windows | Threats | Vulnerability | Top And Trends | Applications | Juniper | My Reports | User Based Reports | Network Devices | CheckPoint | Fortinet | vCenter | Sophos | Customize ▾

📅 2017-09-01 00:00 2017-09-30 23:59

🔍 Group / Report



Created Tables | Criteria : Device ▾ | User ▾ | Remote Device ▾

Schedule | Export ▾ | 📄 | 👤

Dropped clusters

Altered Clusters

Created Tables

Dropped Tables

Altered Tables

Selected Tables

Inserted Tables

Updated Tables

Deleted Tables

Created functions

Dropped functions

Altered functions

Created Schemas

Created procedures

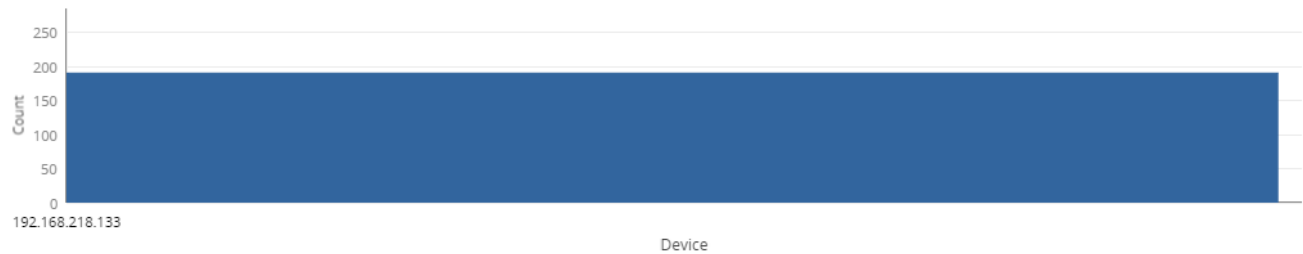
Dropped procedures

Altered procedures

Executed procedures

Created triggers

Dropped triggers

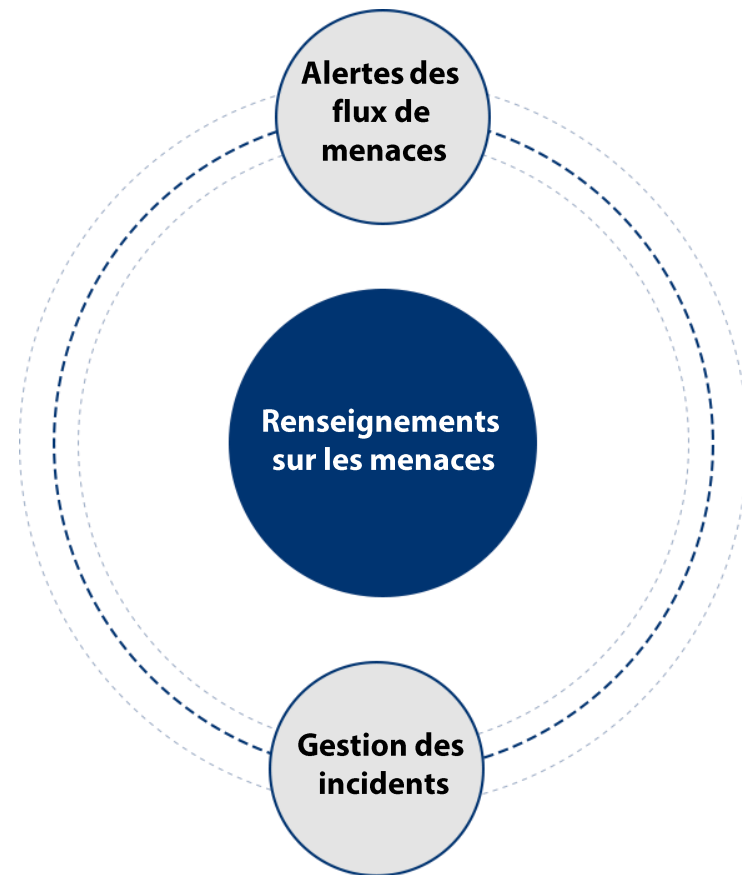


1 - 10 of 190 > 10 ▾ 🗕

Device	Username	User Device	Terminal	Object Creator	Object Name	Comment Text	Time
Username = SCOTT X							
192.168.218.133	SCOTT	ELA-RHEL6-64	pts/2	SCOTT	VIVEK	-	09 Sep 2017, 02:56:25
192.168.218.133	SCOTT	ELA-RHEL6-64	pts/2	SCOTT	VIVEK	-	09 Sep 2017, 02:56:25
192.168.218.133	SCOTT	ELA-RHEL6-64	pts/2	SCOTT	DEPT_10	-	09 Sep 2017, 02:56:25
192.168.218.133	SCOTT	vishnu-2268	unknown	SCOTT	NEW_PRODUCT	-	09 Sep 2017, 02:56:25
192.168.218.133	SCOTT	vishnu-2268	unknown	SCOTT	NEW_PRODUCT	-	09 Sep 2017, 02:56:25

# Renseignements sur les menaces

---



# Alertes sur les flux de menaces

---

- **EventLog Analyzer traite plusieurs flux de menaces basés sur des sources ouvertes et STIX/TAXII.**
- **Base de données de plus de 600 millions d'IP, d'URL et de domaines malveillants, mise à jour dynamiquement.**
- **Recevez des alertes en temps réel lorsque du trafic est détecté en provenance ou à destination d'IP, d'URL et de domaines suspects.**
- **Aucune configuration préalable n'est nécessaire pour mettre en place cette fonctionnalité.**

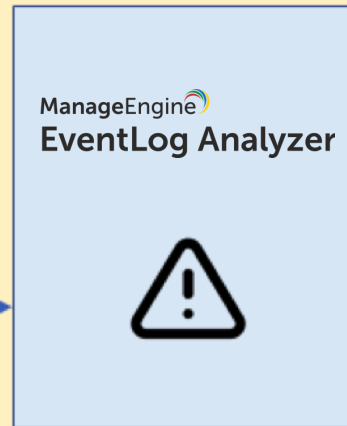
# Alertes sur les flux de menaces: Exemple



**Attaquant**



**Une IP malveillante connue  
tente de contacter le  
réseau**



**EventLog Analyzer informe  
l'administrateur en temps  
réel.**

# Alertes sur les flux de menaces: Exemple

2016-10-16 00:00 2016-10-16 16:35

Alert Profiles [List] + Add Alert Profile Export to: Showing 1 - 50 of 1965 > > 50

Time Generated	Host	Severity	Message
Oct 16, 2016 14:13:59	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:57	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:45	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:45	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:42	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:38	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:34	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:32	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:30	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:30	10.0.0.10	High	Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:23	10.0.0.10	High	Malicious IP found - 222.186.56.42

Alert Profiles [List]

- login (419)
- Special\_Logon (0)
- test1234567 (0)
- Default Threat (1965)
- Head test (0)
- File\_Deletion (0)

# Gestion des incidents

---

- **Gérez les incidents de sécurité à l'aide de la console de gestion des incidents intégrée.**
- **Assignez automatiquement les tickets d'incident aux opérateurs.**
- **Suivez les tickets d'incident, utilisez plusieurs vues pour filtrer les tickets, et plus encore.**
- **Vous pouvez également transmettre les tickets d'incident à ServiceDesk Plus ou à ServiceNow.**

# Gestion des incidents

The screenshot displays the 'EventLog Analyzer' web interface. A modal dialog titled 'Update Alert' is open, allowing for the configuration of an alert. The dialog includes the following fields:

- \*Assign To:** A dropdown menu with 'operator' selected.
- Notes:** A text area containing 'admin' and 'operator' (the latter is highlighted in green).
- \*Status:** A dropdown menu with 'Open' selected.

At the bottom of the dialog are 'Save' and 'Cancel' buttons. The background interface shows a table of alerts with the following columns: Time Generated, Device, Severity, Owner Name, Status, and Message.

Time Generated	Device	Severity	Owner Name	Status	Message
22 Sep 2017 17:59:00	Based on correlati...	High	-	Open	Correlation:Logon Success by Source Host rule
22 Sep 2017 17:59:00	Based on correlati...	High	-	Open	Correlation:Logon Success by Source Host rule
22 Sep 2017 17:59:00	Based on correlati...	High	-	Open	Correlation:Logon Success by Source Host rule
22 Sep 2017 17:59:00	Based on correlati...	High	-	Open	Correlation:Logon Success by Source Host rule

# Flux de travaux automatisés

---

- **Contenez les attaques ou réduisez leur impact en automatisant la gestion des réponses aux incidents.**
- **Associez des flux de travaux prédéfinis à un profil d'alerte pour remédier automatiquement à l'incident de sécurité détecté.**
- **Créez et gérez des flux d'incidents qui sont automatiquement exécutés lorsque des alertes de sécurité sont déclenchées.**
- **Utilisez les flux de travaux intégrés d'EventLog Analyzer ou personnalisez les règles de flux de travail en fonction de vos besoins à l'aide d'un constructeur de workflow flexible.**

# Flux de travaux automatisés

EventLog Analyzer Purchase now Jump To Log Receiver ? + Log Search

Home Reports Compliance Search Correlation Alerts Settings LogMe Support + Add





























Search


All Alerts  
My Alerts  
Assigned Alerts  
Unassigned Alerts  
Critical Alerts  
Profile Based Alerts  
Correlation Alert Profiles  
Alert Configurations  
Manage Workflows

## Manage Workflow

Workflow Credentials + Create Workflow

1-7 of 7 10

Actions	Workflow Name	Description	Associated Alert Profiles	Workflow History
   	Block USB	This workflow blocks the USB port on a potentia...	0	<a href="#">View History</a>
   	Delete User	This workflow deletes a potentially compromise...	0	<a href="#">View History</a>
   	Disable Computer	This workflow disables a potentially compromis...	0	<a href="#">View History</a>
   	Kill Process	This workflow kills a process on a potentially c...	0	<a href="#">View History</a>
   	Log Off and Disable User	This workflow logs off and disables a potential...	0	<a href="#">View History</a>
   	Popup Alert	This workflow displays a popup alert on the affe...	0	<a href="#">View History</a>
   	Stop Service	This workflow stops a service on a potentially c...	0	<a href="#">View History</a>



# Systeme intégré de gestion de la conformité

---

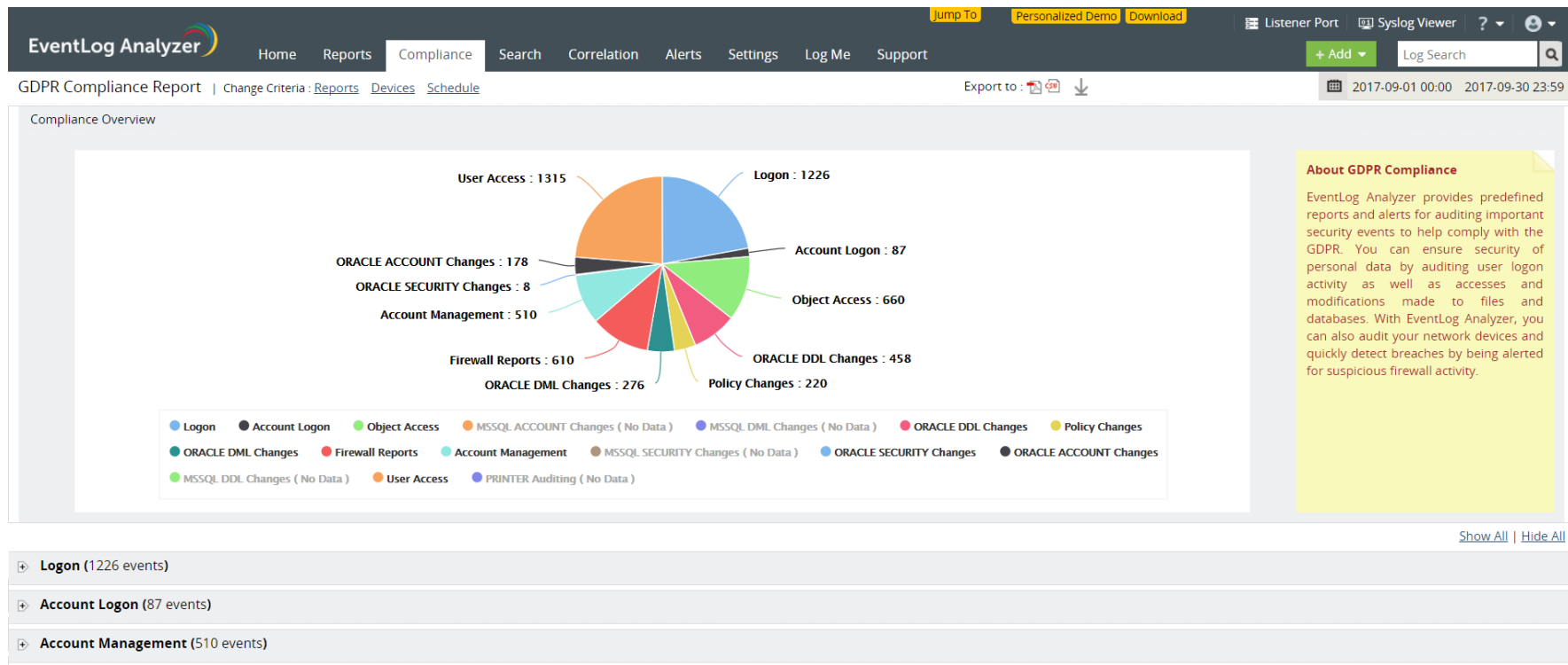


# Systeme intégré de gestion de la conformité

---

- **Obtenez des rapports de conformité prêts à l'emploi pour :**
  - PCI DSS
  - GDPR
  - FISMA
  - HIPAA
  - GLBA
  - SOX
  - ISO 27001
- **Modifiez les rapports existants ou créez de nouveaux rapports de conformité pour répondre aux politiques de sécurité internes.**
- **Répondez aux exigences de la plupart des stratégies de conformité en matière d'analyse forensique et d'archivage des journaux grâce à la puissante fonction de recherche et aux capacités d'archivage sécurisé des journaux.**

# Systeme integré de gestion de la conformité



# EventLog Analyzer : Différenciateurs du produit

---

- **Facile à déployer et à utiliser.**
- **Prend en charge un large éventail de sources de journaux.**
- **Pas d'add-ons !**
- **Peut être facilement intégré à une solution SIEM.**
- **Un modèle de licence simple.**

ManageEngine 

**Merci!**

---

[helpdesk@pgsoftware.support](mailto:helpdesk@pgsoftware.support)