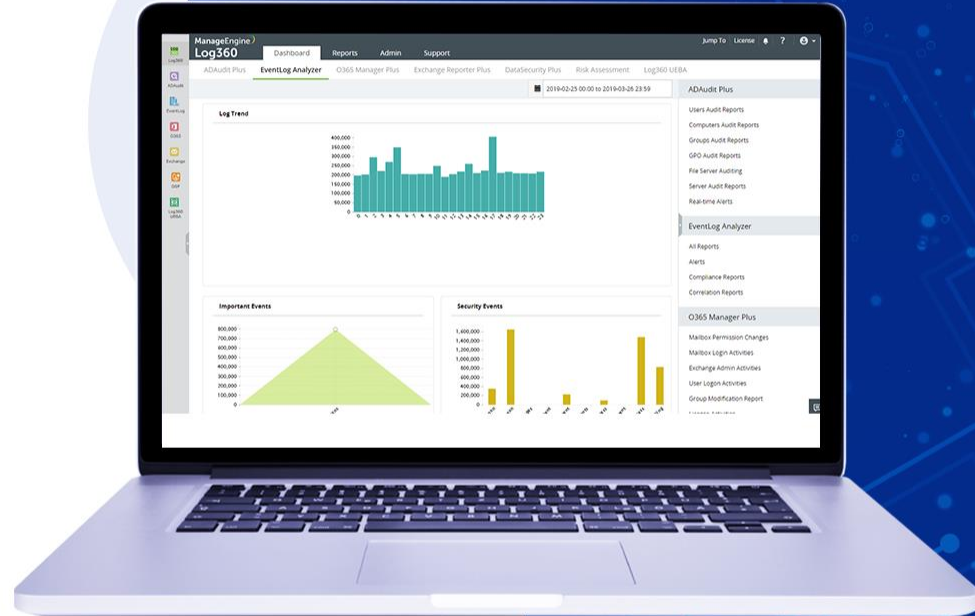


ManageEngine
Log360

**Une solution SIEM
complète pour
votre réseau.**



Gestion intégrée de la conformité

Restez en conformité avec les normes PCI DSS, GDPR, FISMA, HIPAA, SOX, GLBA grâce à des modèles de rapports prêts pour l'audit. Tableau de bord exclusif pour visualiser l'état de conformité de votre réseau.

Vous permet de modifier les modèles de rapport existants pour répondre aux politiques de sécurité internes et vous permet également de créer facilement vos propres rapports de conformité avec des composants réutilisables.



Analytiques de sécurité

Détecte les intrusions et les menaces sur le réseau en analysant les événements provenant des périphériques réseau, des serveurs, des bases de données, des serveurs Web, des plateformes Office 365, des serveurs Exchange et d'AD.

Des tableaux de bord intuitifs et des rapports prédéfinis vous aident à détecter les anomalies et à y répondre instantanément.



Renseignements sur les menaces

Détecte les attaques à leurs débuts grâce à sa base de données globale intégrée sur les menaces IP et à son processeur de flux de menaces STIX/TAXII qui identifie les entités malveillantes interagissant avec votre réseau.

Le système d'alerte en temps réel est lié au système de gestion des incidents, ce qui vous permet de détecter rapidement les incidents de sécurité et de les résoudre.



ManageEngine
Log360

Pourquoi Log360
est une **solution**
SIEM complète

Supervision du cloud

Détecte les événements anormaux en surveillant les activités se déroulant dans les environnements PaaS et IaaS tels qu'Azure, Amazon Web Services et les applications SaaS comme Salesforce.



Repère les activités telles que le téléchargement non autorisé d'informations sur les clients à partir de Salesforce grâce à des rapports et des alertes prédéfinis.

Gestion des incidents

Comprend un système intégré de suivi des incidents qui vous permet d'attribuer automatiquement des propriétaires aux alertes de sécurité, de suivre le processus de résolution des incidents, etc.

S'intègre à JIRA, ServiceNow, ServiceDesk Plus, Zendesk et d'autres outils de centre d'assistance pour rationaliser le suivi et la résolution des incidents.



Analyse du comportement de l'utilisateur (UBA)

Repère les anomalies sans intervention manuelle grâce à des techniques sophistiquées d'apprentissage automatique.

Détecte les volumes inhabituels de connexions, d'activités sur les fichiers, de verrouillages, etc. grâce à un tableau de bord intuitif et à des rapports exhaustifs.

Sécurité des données

Détecte automatiquement les données personnelles et sensibles dans l'infrastructure Windows grâce à des stratégies prédéfinies de détection des données confidentielles. Protège ces données grâce à la fonction étendue de surveillance de l'intégrité des fichiers.

Surveille la création, la suppression, la modification et les changements de permission des fichiers et des dossiers dans les serveurs de fichiers Windows, NetApp, EMC, etc.





Analytiques de sécurité

Console centrale pour information

Périphériques réseau et application

- Modifications de la configuration des dispositifs de sécurité
- Activité de la base de données et du serveur Web



Solutions pour terminaux

- Principales vulnérabilités du réseau
- Menaces identifiées par les solutions de gestion des menaces

Office 365 et Exchange Server

- Analyse du trafic des boîtes mails
- Statistiques sur le trafic, le contenu et les autorisations pour Exchange Server



Active Directory

- Activité des utilisateurs privilégiés
- Modifications critiques de l'AD

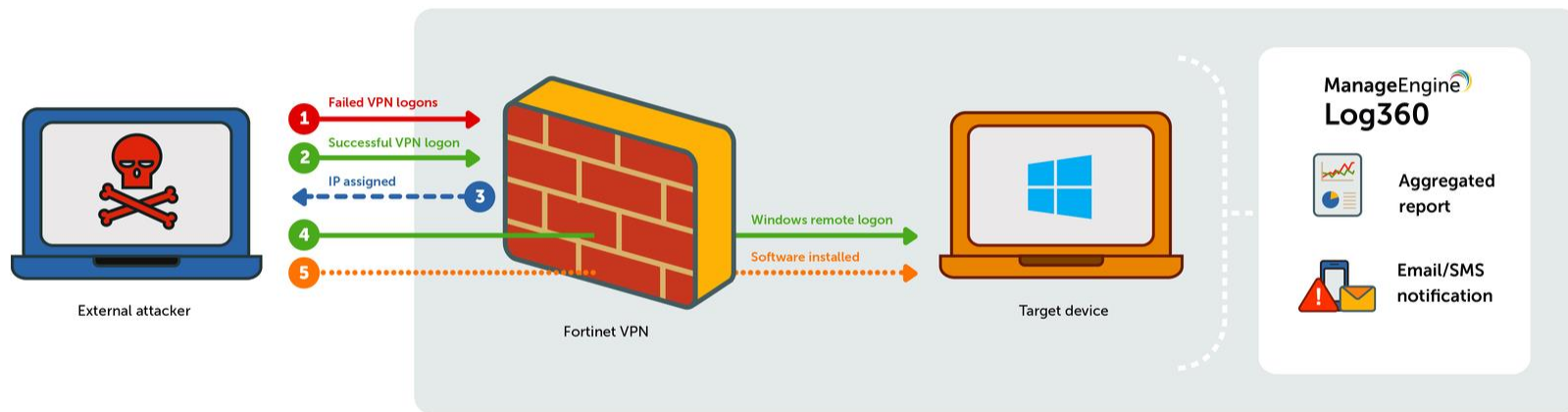


Corrélation avancée des événements

- Détection d'incidents basée sur des modèles
- **Plus de 30 règles prédéfinies** : Détection des logiciels suspects, du cryptojacking, de l'activité des vers, etc.
- Tableau de bord d'aperçu des incidents
- Chronologie détaillée des incidents
- Créateur de règles de corrélation personnalisées avec des filtres avancés basés sur les champs.

Détection des installations logicielles suspectes

Suspicious software installations



- 1** At least 5 failed VPN logons in 10 minutes
- 2** Successful VPN logon in next 2 minutes
- 3** IP address assigned in next 2 minutes
- 4** Successful remote logon to target device in next 15 minutes
- 5** Malicious software installation in next 30 minutes

Analyse forensique des journaux

- Le puissant moteur de recherche basé sur Elasticsearch vous aide à analyser des incidents complexes et à découvrir la cause première en quelques minutes.
- **Recherche de base et avancée** : Utilisez des options flexibles pour créer des requêtes de recherche à partir de zéro ou utilisez l'interface de création de requêtes avancées.
- Recherchez dans les journaux bruts et formatés, y compris dans les archives de journaux.
- Enregistrez les recherches sous forme de rapports ou d'alertes

Renseignements sur les menaces

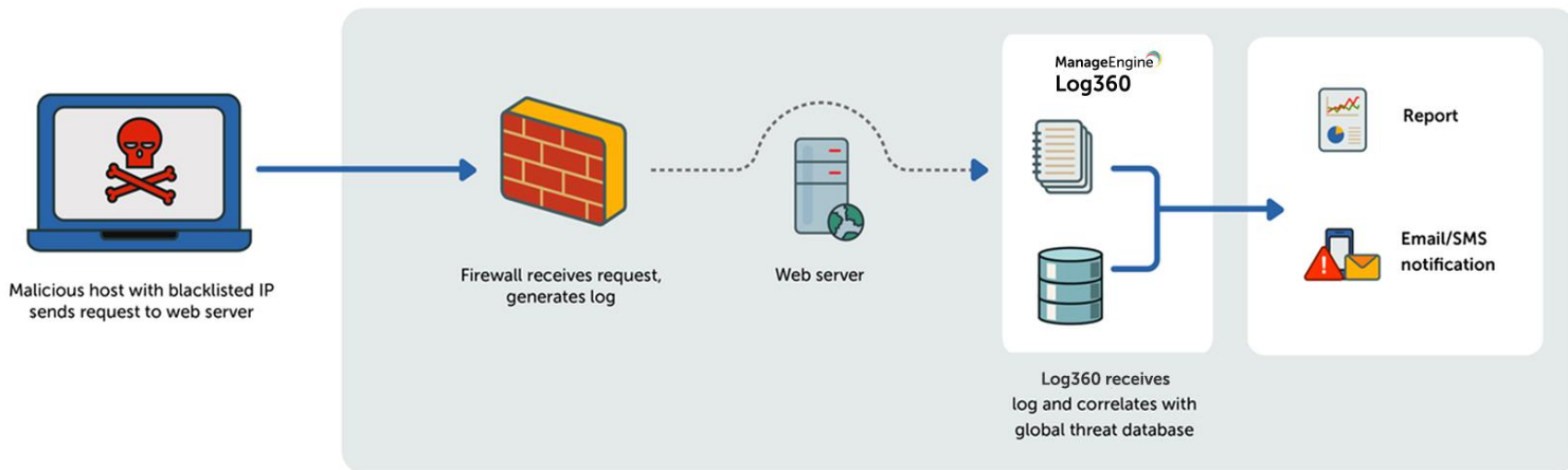


Renseignements sur les menaces

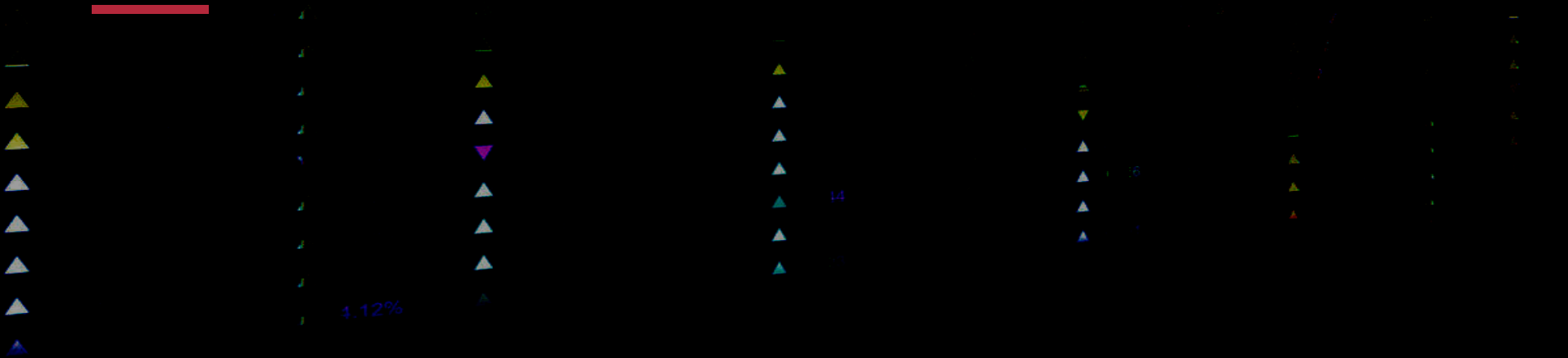
- Détectez les intrus dans le réseau grâce aux données des flux de menaces.
- Alertes en temps réel pour les URL, IP et noms de domaine malveillants.
- Ajout de flux de menaces STIX/TAXII personnalisés
- Aucune configuration nécessaire
- Mises à jour dynamiques et quotidiennes

Détection des installations logicielles suspectes

Inbound malicious IP



Analyse avancée des menaces



Analyse avancée des menaces

- Intégration avec un fournisseur fiable de renseignements sur les menaces
- Une meilleure compréhension de la menace signalée
- Classification IP/URL
- Score de réputation

Threat Analytics

External Threats

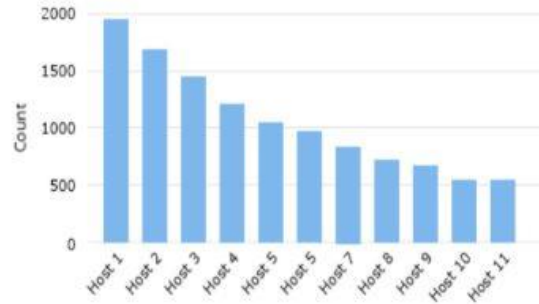
External Threats

Export As Schedule

Select Device

Period

Top Attacked Hosts **Threats by Category**



« < 1-10 of 100 > » 25 ▾

Time of Occurrence	Malicious Source	Attacked Host	Threat Category	Reputation Score	Advanced Threat Analytic
08 Sep 2018 02:23:43	192.165.234.12	192.165.234.12	Malicious	20	View
08 Sep 2018 02:23:43	192.165.234.12	192.165.234.12	Malicious	70	View
08 Sep 2018 02:23:43	cfremaux60.free.fr	192.165.234.12	Real Estate	30	View
08 Sep 2018 02:23:43	192.165.234.12	192.165.234.12	Malicious	20	View

Advanced Threat Analytics



Info

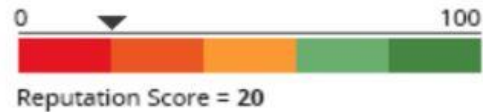
Geo Info

Phishing Info



cfremaux60.free.fr

High Risk



Category	: Real Estate
Domain name	: fraud.com
Domain age	: 6 months
Flagged as malicious on	: 07 Sep 2018 09:30:54
Last occurrence on threat list	: 07 Sep 2018 09:30:54
No. of times it occurred on threat list	: 32



Recommendation: Block the URL.

OK

Analyse du comportement des utilisateurs et des entités

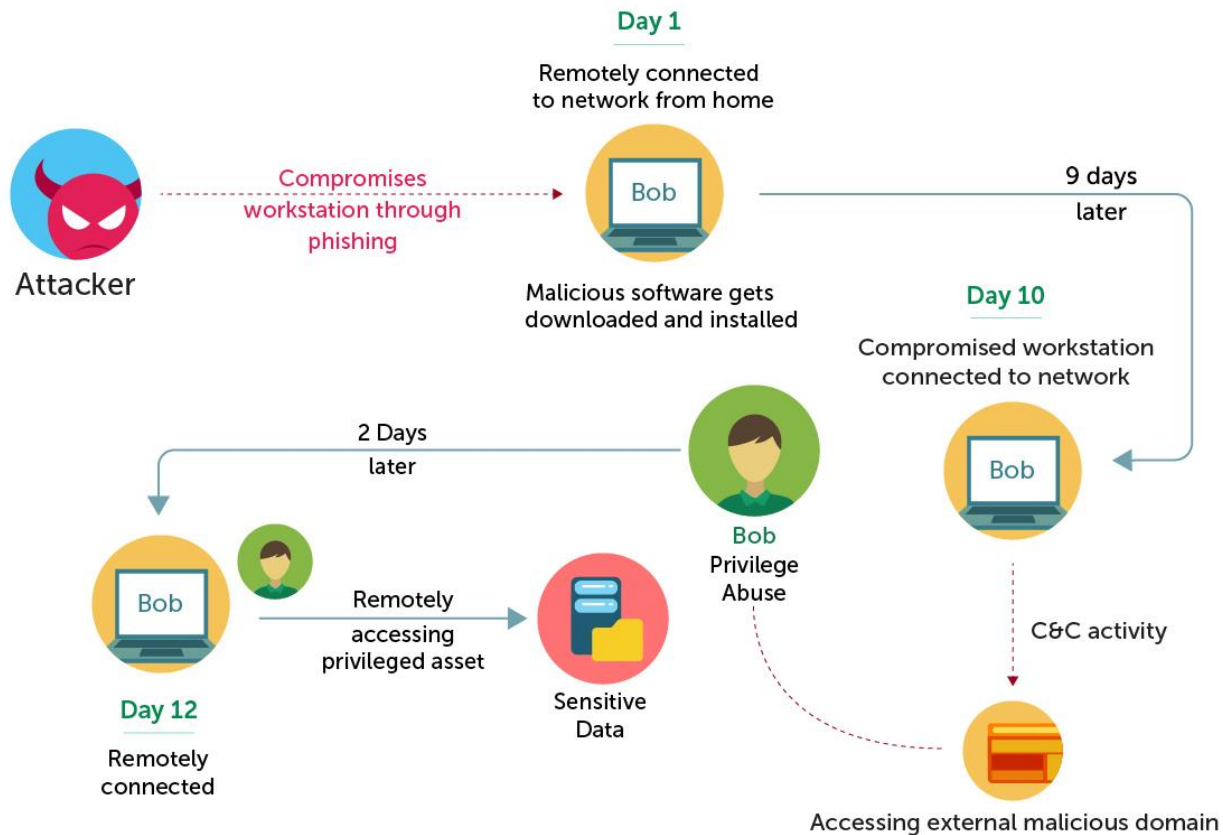


Analyse du comportement des utilisateurs et des entités

- Détection d'anomalies basée sur l'apprentissage automatique
- **Détection de comportements anormaux:** Basée sur le temps, le rythme ou le nombre
- **Hiérarchisation des menaces basée sur le score de risque:** Déterminez le degré de risque posé par une menace identifiée.
- Ajoutez les utilisateurs et les entités à haut risque à une liste de surveillance.
- **Corroboration des menaces:** Identifiez les indicateurs de menaces communes (compromission de comptes, exfiltration de données, etc.).

Cas d'utilisation:

Poste de travail compromis et tentative d'exfiltration de données





Sécurité des données

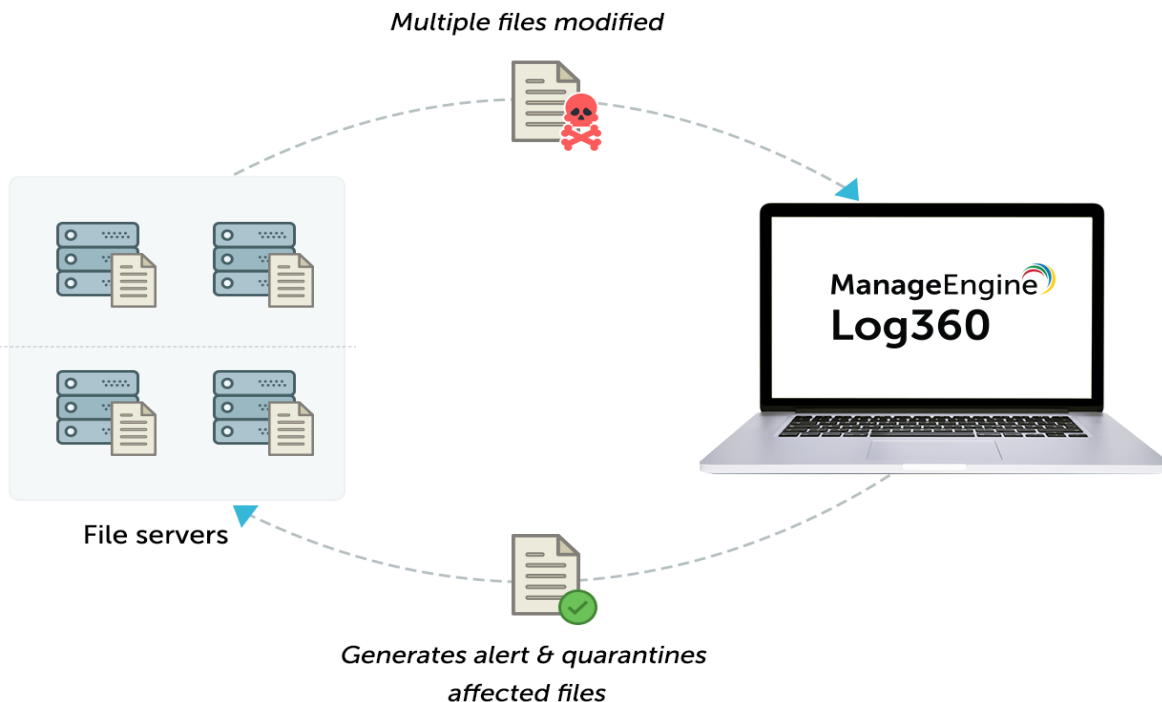
Sécurité des données

- Découvrez les données sensibles (PII, PHI, etc.) sur votre réseau à l'aide de stratégies prédéfinies et personnalisées.
- Garantisiez l'intégrité des fichiers et dossiers confidentiels grâce à la surveillance de l'intégrité des fichiers.
- Recevez des alertes en temps réel pour les accès non autorisés aux fichiers, les changements de permission et les modifications.

Détection des installations logicielles suspectes

Ransomware
detection

Ransomware
response



Gestion des incidents



Gestion des incidents

Systeme de ticket intégré :

- Attribution automatique des tickets d'incident
- Suivi du statut des incidents
- Maintien d'une base de connaissances interne des incidents résolus

Transfert des informations sur les incidents à une solution externe d'assistance:

- Solution de centre d'assistance pris en charge : ServiceDesk Plus, ServiceNow, Jira Service Desk, ZenDesk, BMC Remedy, Kayako



All Alerts

My Alerts

Assigned Alerts

Unassigned Alerts

Critical Alerts

Profile Based Alerts



Correlation Alert Profiles



Alert Configurations



Manage Alert Profiles

Incident Management

Assign Rules

Manage Incident Tool Configuration

Incident Tool	ManageEngine ServiceDesk Plus	
* Server Name/IP	ServiceNow	
* Protocol	ManageEngine ServiceDesk Plus	
* Authentication	Jira Service Desk	
* Login Name	Zendesk	
* Password	Kayako	
* Subject	BMC Remedy Service Desk	
* Message	Password	
	E.g.:\$SOURCE from \$HOSTNAME	Macros
		Macros

Test and Save

Cancel

Supervision du cloud



Environnements Cloud

Obtenez des informations sur :



AWS: Amazon S3, Amazon EC2, les pare-feu d'applications Web (WAF), le service de bases de données relationnelles (RDS), et plus.



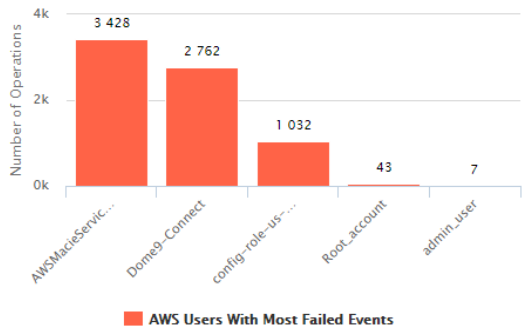
Microsoft Azure: Activité des utilisateurs, modifications apportées aux groupes de sécurité du réseau, réseaux virtuels, zones DNS, bases de données, etc.



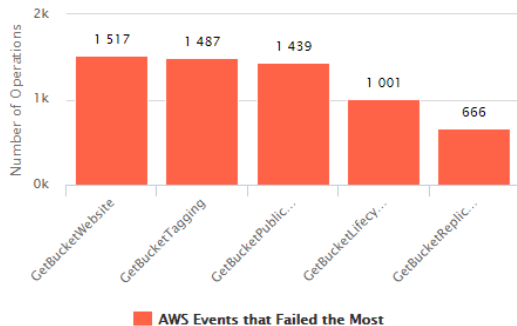
Salesforce: Activités de connexion, de rapport, de contenu et de recherche.

Account **aws_test (aws)** Period **02-25-2019 - 03-26-2019**

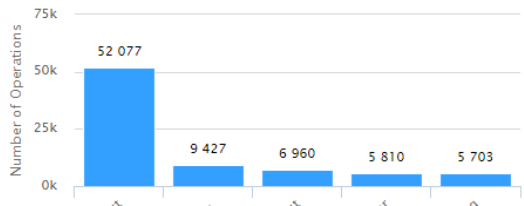
Failed activity by Users



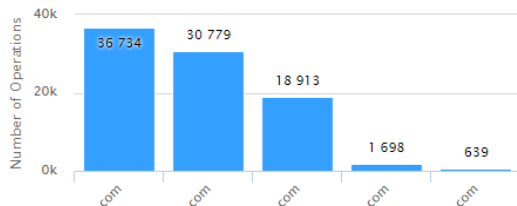
Failed activity by Actions



Activity by Users



Top Modified Services



Alerts

Alert "TestAlert" triggered for event (eventDataId = fc7e9c83-349d-461b-8b09-c7753b368fda).

20 days ago

Alert "TestAlert" triggered for event (eventDataId = ad077ad3-5401-4086-a353-764e4ffc0bd3).

20 days ago

Alert "TestAlert" triggered for event (eventDataId = d87ac50d-6227-4b53-912e-002c99c2df2e).

21 days ago

Alert "TestAlert" triggered for event (eventDataId = 4d7bfa82-44a4-4560-b7d9-ef167f8d4614).

21 days ago

Alert "TestAlert" triggered for event (eventDataId = 802390e5-f297-4f9b-b820-5a5b5e1896c4).

21 days ago

[View All](#)

Settings

[Alert Profiles](#)

[Schedule Reports](#)

Reports

[Recent Error Events](#)

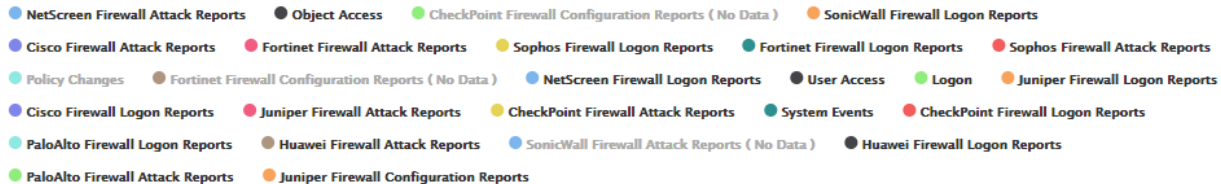
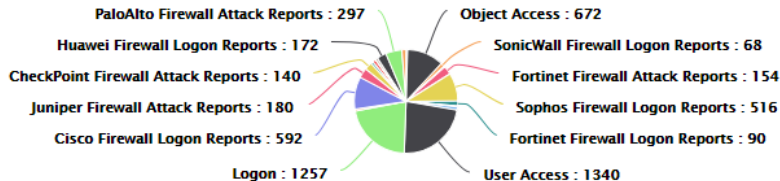
Conformité réglementaire



Conformité

- **Rapports de conformité prêts à l'emploi pour :** PCI DSS | SOX | GLBA | HIPAA | GPG | GDPR | ISO 27001 | ISLP
- Création de rapports de conformité personnalisés pour les politiques de conformité nouvelles ou internes.
- Alertes de conformité prédéfinies disponibles
- **Archivage automatique des journaux :** Conservez les journaux aussi longtemps que l'exigent les exigences réglementaires.
- Les archives sont sécurisées et inviolables.

Compliance Overview



About PCI Compliance

EventLog Analyzer can make your enterprise to comply with the Payment Card Industry Data Security Standard (PCI-DSS) Requirement 10. This section mandates payment service providers and merchants to track and report on all access to their network resources and cardholder data through system activity logs. The presence of logs in networked environment allows thorough forensic analysis when something does go wrong. Without system activity logs it would be difficult to determine the cause of a compromise.



**Autres points
forts**

Fonctionnalités supplémentaires : Sécurité du produit

- ✓ **Transmission sécurisée des données:** Cryptez toutes les communications entre Log360 et votre navigateur grâce au protocole sécurisé HTTPS.
- ✓ **Contrôle d'accès basé sur les rôles:** Limitez l'accès des utilisateurs aux dispositifs ajoutés et aux fonctionnalités du produit grâce à des rôles d'utilisateur.
- ✓ **Audit des utilisateurs:** Auditez toutes les actions des utilisateurs d'EventLog Analyzer.
- ✓ **Haute disponibilité:** Désignez un serveur secondaire qui prendra le relais en cas de défaillance du serveur primaire.

Prix et reconnaissances

- ✓ Reconnu par le Gartner Magic Quadrant pour SIEM, pour la quatrième fois consécutive.
- ✓ Choix des clients de Gartner Peer Insights pour SIEM, 2019.
- ✓ Placé en tête du classement Software Reviews Customer Experience Diamond pour SIEM, 2019.



ManageEngine[®]
Log360

Merci!

Contact

helpdesk@pgsoftware.support

