



Gerenciamento de incidentes de
segurança sem problemas com

SIEM

Gerenciamento de incidentes de segurança sem problemas com SIEM

A detecção de incidentes e sua resposta são dois lados igualmente críticos da mesma moeda. As organizações se esforçam para reduzir o tempo necessário para detectar e responder a incidentes de segurança para limitar o tempo que um invasor deve violar ou interromper sua rede. Usando um sistema eficaz que pode controlar tanto a detecção quanto a resposta a incidentes, as organizações podem fazer exatamente isso. O gerenciamento de incidentes é a ponte que conecta os dois, permitindo que você supervisione um incidente desde a detecção até o encerramento.

O módulo de gerenciamento de incidentes do **EventLog Analyzer** permite que os administradores gerenciem facilmente os incidentes de segurança em tempo real. Os principais recursos incluem:

- Um painel de incidentes intuitivo que exibe incidentes de segurança classificados por prioridade e fonte.
- Um sistema interno totalmente integrado para atribuir incidentes a usuários responsáveis e acompanhar seu status.
- Atribuição automatizada de ticket com base no dispositivo ou grupo de dispositivos que causou o alerta, ou atribuição manual diretamente do painel.
- Integração com ferramentas populares de gerenciamento de incidentes externos, ManageEngine ServiceDesk Plus e ServiceNow.

O painel de incidentes

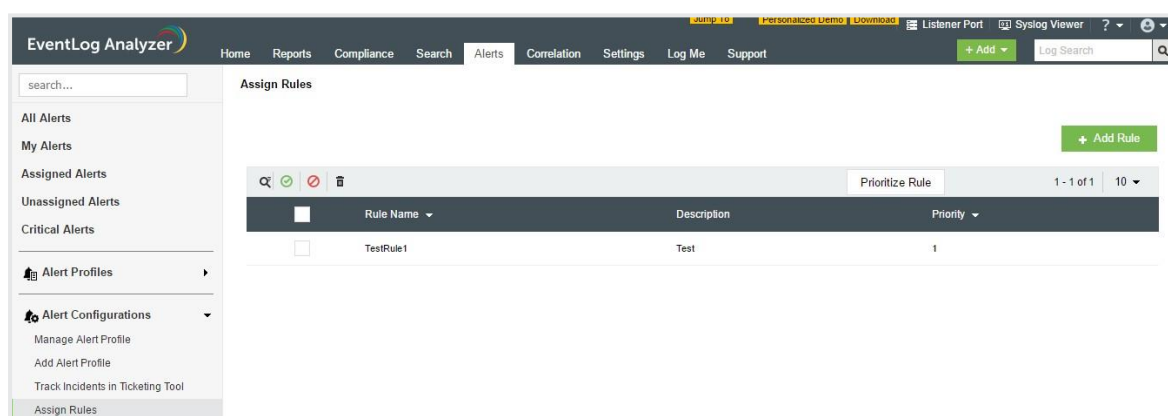
The screenshot displays the 'Alerts' section of the EventLog Analyzer. At the top, there's a navigation bar with 'Alerts' selected. Below it, a search bar and a date range filter (2017-06-26 00:00 - 2017-06-26 19:10) are visible. The main content area shows a 'Severity' gauge chart and a table of alerts. The table has the following data:

Time Generated	Device	Severity	Owner Name	Status	Message
Jun 26 2017 19:09:34	CHERRY-LINUX	High	-	Open	sshd:Failed password for invalid user djf from 19
Jun 26 2017 19:09:14	ITS-CHERRY	High	-	Open	sshd:Failed password for invalid user djf from 19
Jun 26 2017 19:01:18	sw-test1	High	-	Open	sshd:Failed password for invalid user vishnu from ssh2
Jun 26 2017 18:58:01	sw-test1	High	-	Open	sshd:Failed password for invalid user djf from 19
Jun 26 2017 18:57:16	ITS-CHERRY	High	-	Open	sshd:Failed password for invalid user djf from 19

O painel principal de gerenciamento de incidentes pode ser acessado na guia **Alertas** no EventLog Analyzer. Os administradores podem o usar para:

- Visualizar um relatório de todos os incidentes de segurança (ou alertas) apresentados como um gráfico ou tabela.
- Realizar várias ações relacionadas ao ticket, incluindo sua atribuição a usuários específicos, atualizar o status (aberto, em andamento ou fechado) ou adicionar notas relevantes usando o ícone de atualização (✎).
- Selecionar uma das várias exibições diferentes das informações – todos os alertas, atribuídos ao usuário conectado, atribuídos ou não atribuídos, alta prioridade e pertencentes a um perfil de alerta específico – no lado esquerdo do menu.

Atribuição automatizada de tickets



Usando regras, o EventLog Analyzer pode gerar tickets automaticamente assim que um alerta é acionado. As regras atribuem incidentes a usuários com base no dispositivo ou grupo de dispositivos que acionou o alerta. Sua lista pode ser acessada selecionando **Atribuir Regras** em **Configurações de Alerta** no lado esquerdo do painel de incidentes. A partir daqui os administradores podem:

- Adicionar novas regras, selecionando o botão **Adicionar Regra**.
- Priorizar regras, selecionando o botão **Priorizar Regra**. Se mais de uma regra se aplicar a qualquer dispositivo, aquela com prioridade mais alta será usada para atribuir o ticket.
- Habilitar, desabilitar ou excluir regras, conforme necessário.

Para adicionar uma nova regra, insira um nome de regra, descrição (opcional), o conjunto de dispositivos ou grupos de dispositivos aos quais ela se aplica e o usuário aos tickets de incidente será atribuído.

Integração do help desk externo

The screenshot shows the EventLog Analyzer web interface. The main menu includes Home, Reports, Compliance, Search, Alerts, Correlation, Settings, Log Me, and Support. The left sidebar contains navigation options like All Alerts, My Alerts, Assigned Alerts, Unassigned Alerts, Critical Alerts, Alert Profiles, and Alert Configurations. The main content area is titled 'Track Incidents in Ticketing Tool' and features two tabs: 'Service Desk Configuration' and 'Service Now Configuration'. The 'Service Now Configuration' tab is selected, displaying the following configuration fields:

- *Service Desk Server Name/IP: Server Name/IP
- *Service Desk Port: 8080
- Protocol: HTTP
- Authentication: Local (selected), Active Directory
- *Login Name: admin
- *Password: Password

A green 'Test and Save' button is located at the bottom of the configuration form.

O EventLog Analyzer também se integra a duas soluções populares de help desk, ManageEngine ServiceDesk Plus e ServiceNow. Para configurar uma integração, selecione **Rastrear Incidentes na Ferramenta de Emissão de Tickets** no painel principal de incidentes.

Para integrar o EventLog Analyzer com o ServiceDesk Plus, insira o nome do servidor (ou endereço IP), o número da porta para onde enviar as informações do incidente, o protocolo de comunicação e um par de credenciais válidas de administrador.

This screenshot shows a close-up of the 'Service Now Configuration' tab in the EventLog Analyzer interface. The configuration fields are:

- *Sub Domain Name: Sub Domain Name
- *Login Name: admin
- *Password: Password

A green 'Test and Save' button is positioned at the bottom center of the configuration area.

Para integrar com o ServiceNow, insira o nome do subdomínio e um par de credenciais de administrador válidas.

Depois que o EventLog Analyzer é integrado a qualquer um desses help desks, todas as informações de incidentes são encaminhadas para o software de emissão de tickets, onde podem ser gerenciadas conforme necessário.

O EventLog Analyzer permite o gerenciamento eficiente de incidentes e garante que as organizações fiquem por dentro de todo o ciclo de vida de um incidente, desde a detecção até a resolução.

Sobre o EventLog Analyzer

O **EventLog Analyzer** é um software abrangente de gerenciamento de logs e conformidade de TI para SIEM. Ele fornece informações detalhadas sobre os logs de sua máquina na forma de relatórios, que ajudam a minimizar ameaças a fim de alcançar a segurança completa da rede.

Blog - <https://blogs.manageengine.com/eventlogalyzer>

Sobre a ManageEngine

A **ManageEngine** fornece as ferramentas de gerenciamento de TI em tempo real que capacitam a equipe para atender às necessidades da organização relacionadas a serviços e suporte.

Em todo o mundo, mais de 60.000 empresas estabelecidas e emergentes – incluindo mais de 60 por cento das empresas da Fortune 500 – confiam nos produtos da ManageEngine para garantir o desempenho ideal de sua infraestrutura de TI crítica, incluindo redes, servidores, aplicações, desktops e mais. A ManageEngine é uma divisão da Zoho Corp., com escritórios em países do mundo inteiro, entre eles Estados Unidos, Reino Unido, Índia, Japão e China.



Email:

support@eventlogalyzer.com

Ou



Ligação gratuita:

+1 925 924 9500 (Ligação gratuita)

+1-408-352-9254

Ou



Visite <https://www.manageengine.com/br/eventlog/> para obter informações detalhadas sobre a solução e todos os seus recursos.

www.eventlogalyzer.com