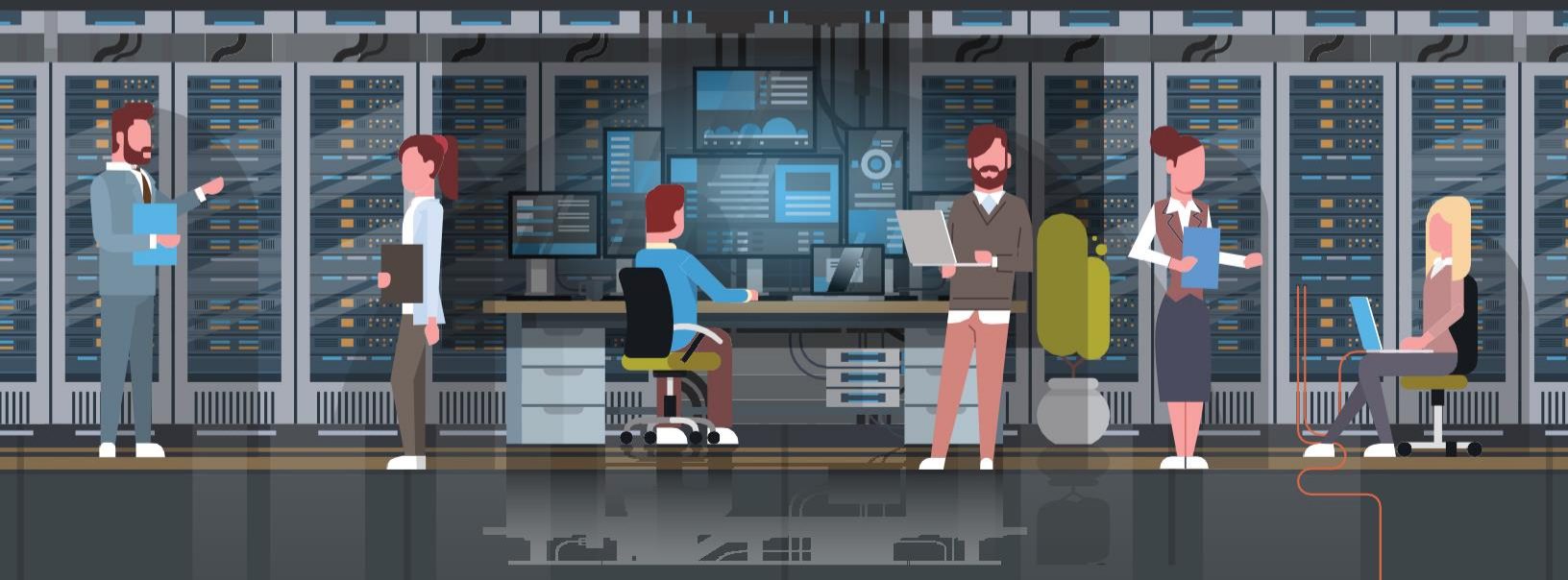
ManageEngine
EventLog Analyzer

Monitoramento e auditoria de atividades de usuários privilegiados



www.manageengine.com/br/eventlog/

Introdução

De todas as contas de usuário em sua organização, as de usuário privilegiados têm mais influência na segurança de rede devido ao poder administrativo. Os armazenamentos de dados confidenciais da sua organização, os servidores críticos e outros dispositivos da rede importantes são tão seguros quanto as contas confiadas a seus cuidados.

Essas contas, pertencentes aos administradores de banco de dados da sua organização, aos administradores de sistema e de rede são alvos principais para invasores externos que buscam obter controle total sobre recursos. Mas as ameaças externas não são o único problema com o qual as organizações precisam se preocupar. Os administradores podem expor intenções mal-intencionadas abusando de seus privilégios ou agir descuidadamente com suas credenciais ou sistemas.

Para adicionar a isso, várias políticas de conformidade, como leis PCI-DSS e SOX, requerem a auditoria completa da atividade de usuários privilegiados. Isso torna o monitoramento de atividades do usuário privilegiado não apenas uma preferência, mas uma necessidade. Este guia explica as melhores práticas para o seu monitoramento e como o EventLog Analyzer pode ser usado para reportar todas as atividades de usuários privilegiados e alertá-los sobre qualquer atividade suspeita.

Melhores práticas de monitoramento para usuários privilegiados

1. Realize um inventário regular de ativos críticos e contas privilegiadas.

Em redes de médio a grande porte, é importante acompanhar os sistemas e aplicações críticas recém-adicionados, juntamente com as contas privilegiadas associadas a eles. Rastreie usuários recém-criados e alterações de permissão para saber quais direitos de contas foram elevados. Essa conscientização ajuda a manter total visibilidade e controle sobre a rede para que nenhuma atividade privilegiada seja perdida.

2. Aplique práticas robustas para a segurança das contas privilegiadas.

Como as contas privilegiadas são alvos de invasores, ele ajuda a aplicar protocolos de segurança rígidos em torno delas, como requisitos de complexidade de senha, contas exclusivas para cada usuário, políticas de acesso claramente definidas e muito mais. Você também pode rastrear alterações de senha e atividades de logon para identificar tentativas de hacking, anomalias no uso da conta, compartilhamento de contas e mais.

3. Forneça apenas as permissões necessárias.

Até mesmo usuários privilegiados podem ter muitos privilégios. Um usuário pode receber acesso de gravação a uma pasta confidencial quando precisar apenas lê-la, ou pode ter acesso a um banco de dados inteiro quando precisar trabalhar apenas com registros selecionados. Quando os recursos críticos podem ser acessados por vários usuários desnecessários, isso aumenta as chances de uma violação. É por isso que os usuários privilegiados só devem receber os direitos de que necessitam.

4. Mantenha uma separação de tarefas entre usuários privilegiados e aqueles que realizam a auditoria.

As ferramentas e os processos usados para monitorar seus usuários privilegiados não devem ser gerenciados por eles mesmos. Os administradores da sua solução de monitoramento devem ser independentes daqueles da rede restantes. Essa separação de tarefas ajuda a garantir que os usuários privilegiados não possam interferir em seus testes ou relatórios de auditoria. Confie suas atividades de monitoramento e auditoria de segurança ao seu centro de operações de segurança (SOC).

5. Relatório sobre todas as atividades privilegiadas.

Não é necessário monitorar todas as ações de funcionários regulares, mas é importante rastrear as atividades de usuários privilegiados. Qualquer ação realizada por um deles, como uma falha de logon ou alteração de configuração, pode ser um indicador de um ataque contínuo, apesar de parecer inocente. Manter relatórios detalhados será útil durante auditorias de conformidade ou investigações forenses.

Auditoria da atividade de usuário privilegiado com o EventLog Analyzer: Relatórios importantes

O EventLog Analyzer é uma solução de auditoria abrangente que permite monitorar centralmente todos os dispositivos, servidores e aplicações da rede. A solução ajuda a monitorar constantemente seus usuários privilegiados e fornece testes e relatórios detalhados de auditoria. Também alerta caso qualquer atividade suspeita seja detectada.

Alguns tipos de relatórios principais incluem:

Monitoramento de atividades de logon: a auditoria de logons ajuda a entender quando e como os administradores fazem logon na rede, para ser possível detectar anomalias como compartilhamento de contas, tentativas de hacking ou tempos de logon irregulares.

Relatórios: Logons do UNIX | Logoffs do Unix | Logons com falha do Unix | Logons do roteador | Logons com falha do roteador | Logons de firewall | Logons com falha do firewall | Relatórios de monitoramento de atividades da sessão

Alterações de conta do usuário: o monitoramento das alterações de conta do usuário ajuda a manter o controle das várias contas privilegiadas em sua rede, bem como das feitas nas configurações da conta.

Relatórios: Contas de usuário adicionadas ao UNIX | Contas de usuário excluídas do Unix | Grupos Unix adicionados | Grupos Unix excluídos | Mudanças de senha | Mudanças de senha com falha | Grupos especiais atribuídos ao novo logon | Administradores de endpoint da Symantec adicionados | Relatório de descoberta de administrador do Nessus | Falhas de privilégio administrativo elevadas do Nessus

Mudanças no sistema e na configuração: o rastreamento de importantes mudanças de configuração feitas por contas privilegiadas é essencial, pois uma única que seja feita pode criar uma brecha de segurança que permite que um hacker obtenha acesso à sua rede.

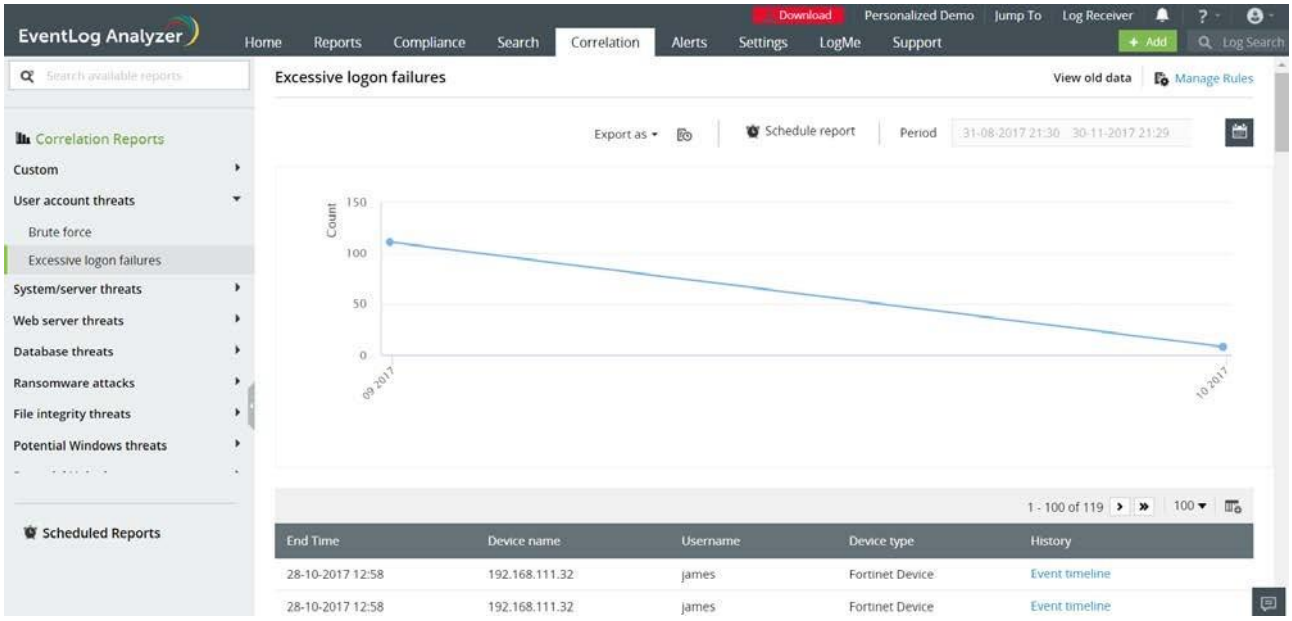
Relatórios: Software instalado | Instalações de software com falha devido a falhas de privilégio | Atualizações do Windows instaladas | Mudanças de registro | Backup e restauração do Windows | Regra de firewall adicionada | Regra de firewall excluída | Mudanças de configurações de firewall | Mudanças de configuração do roteador | Comandos do roteador executados

Acesso a dados confidenciais: a auditoria da atividade privilegiada em servidores de arquivos e bancos de dados críticos ajuda a proteger dados corporativos confidenciais contra acesso não autorizado.

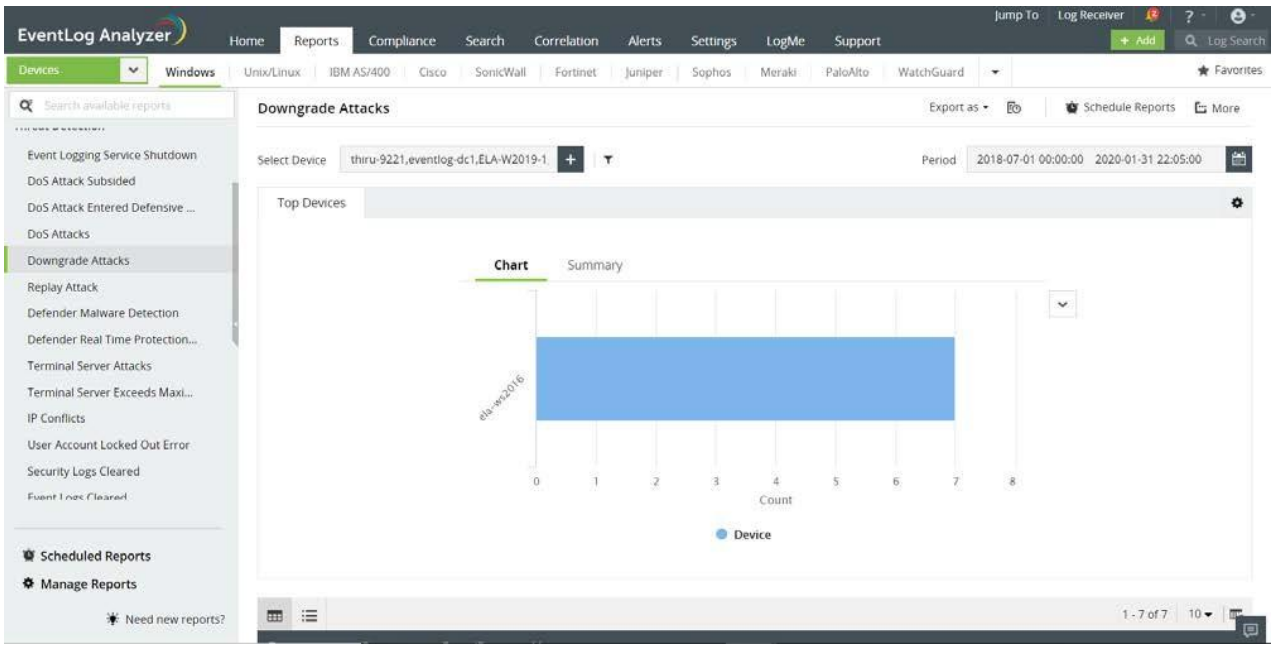
Auditoria da atividade de usuário privilegiado com o EventLog Analyzer:

Relatórios: Relatórios de auditoria DDL | Abusos de privilégio | Mudanças de autoridade administrativa | Mudanças de permissão | Mudanças de proprietário | Relatório de backup de banco de dados | Permissão de banco de dados negada | Violação de acesso | Mudanças de permissão de arquivo

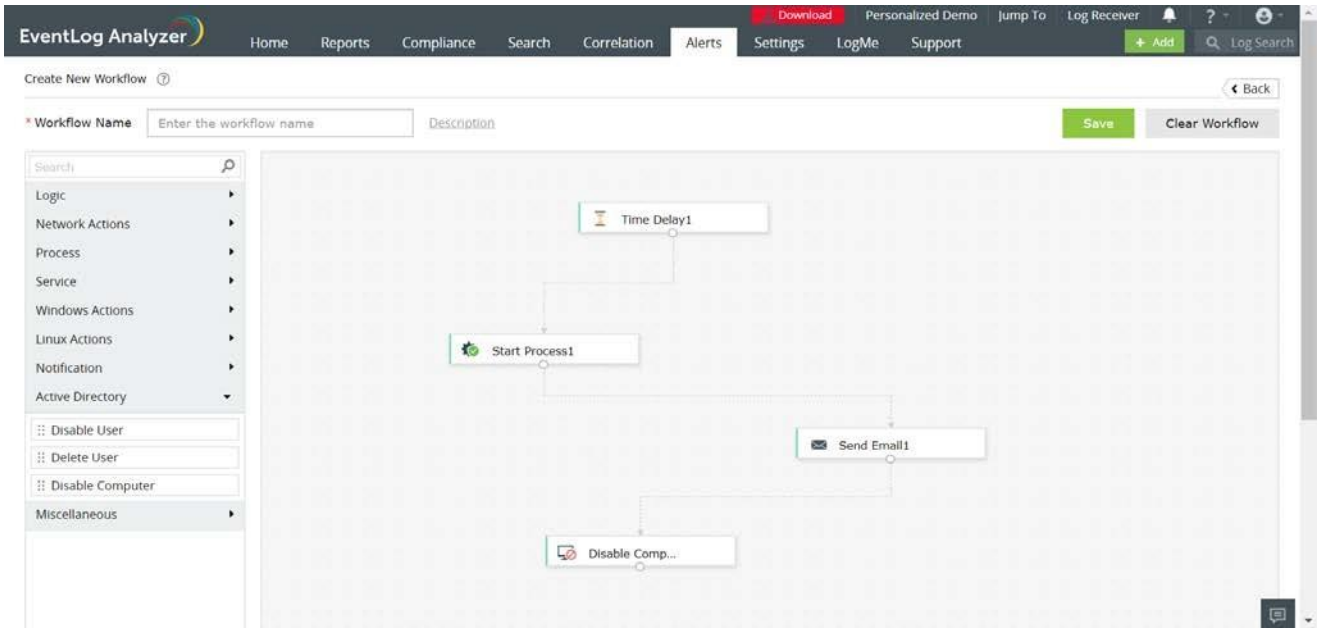
Destaques do EventLog Analyzer



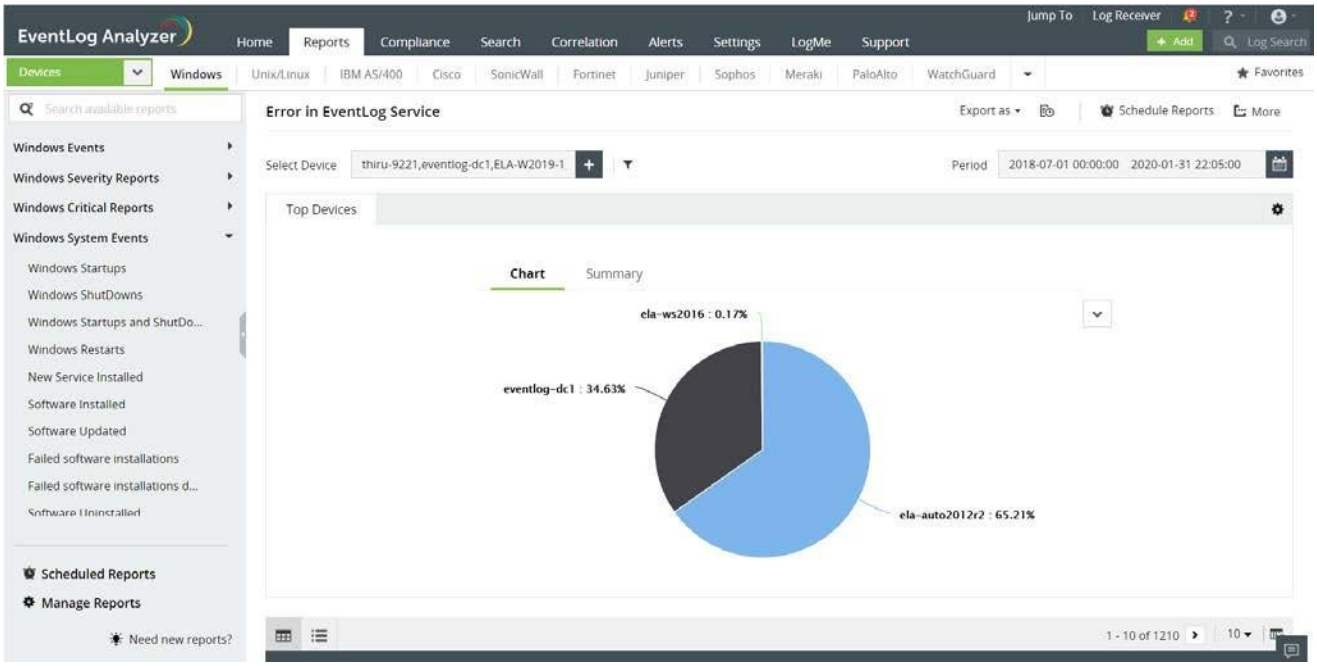
Correlação de eventos avançada: o mecanismo de correlação avançada contém mais de trinta regras de ataque predefinidas, incluindo aquelas para ransomware, força bruta e muito mais. Você pode correlacionar logs de várias fontes e criar regras para se adequar ao seu ambiente de negócios.



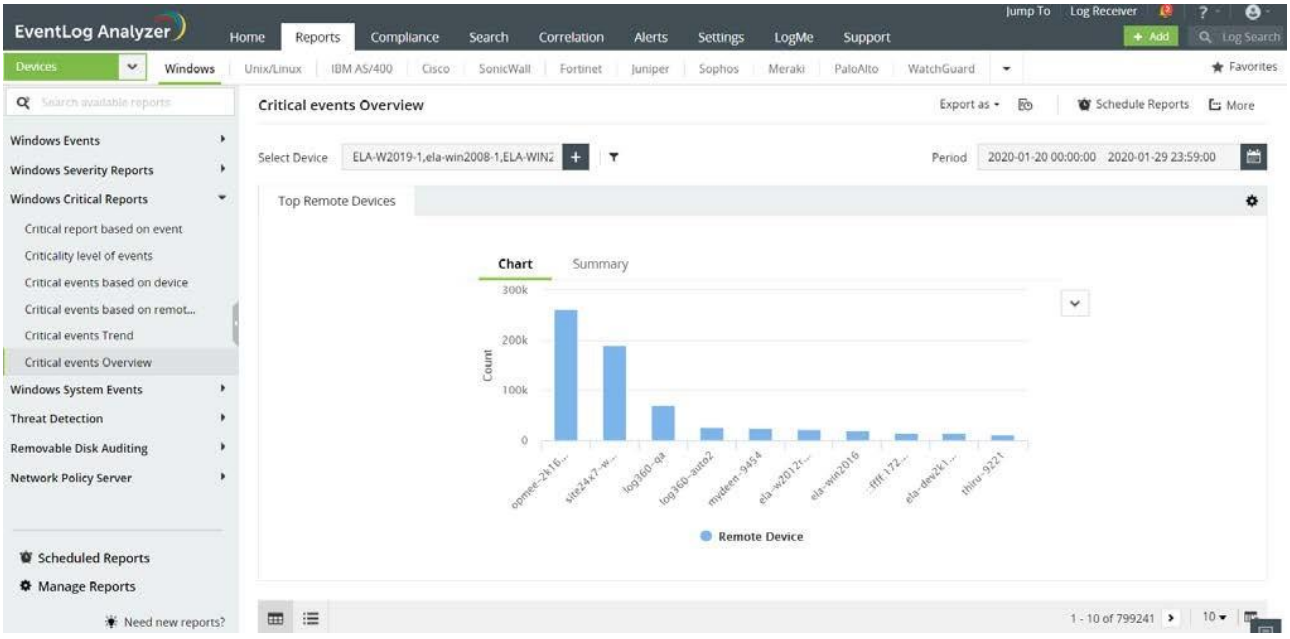
Inteligência contra ameaças dinâmica: a plataforma avançada de inteligência contra ameaças vem com um processador de feed STIX/TAXII integrado. Você pode obter alertas em tempo real para tráfego de entrada e saída suspeito de domínios maliciosos e servidores de retorno de chamada. Além disso, o add-on de análise avançada de ameaças fornece percepções mais profundas sobre a fonte, incluindo detalhes sobre a pontuação de reputação do IP, o histórico de quando foi sinalizado, a geolocalização da origem da ameaça e muito mais.



Console de gerenciamento de incidentes integrado: monitorar o processo de resposta e resolução de incidentes criando automaticamente tickets a partir de alertas e atribuindo-os ao administrador certo com base no dispositivo ou grupo de dispositivos que gerou o alerta. Rastrear os tickets de incidentes com a opção de emissão integrada ou de gerá-los em ferramentas de help desk externas - ServiceDesk Plus e ServiceNow. Você também pode escolher entre os vários fluxos de trabalho integrados que respondem automaticamente a incidentes, como desativar computadores comprometidos e bloquear contas de usuário hackeadas ou maliciosos.



Gerenciamento de logs abrangente: colete, analise, correlacione, pesquise e arquive dados de log de mais de 700 fontes de logs. Inclui um interpretador de logs personalizado para analisar qualquer formato de log legível por humanos.

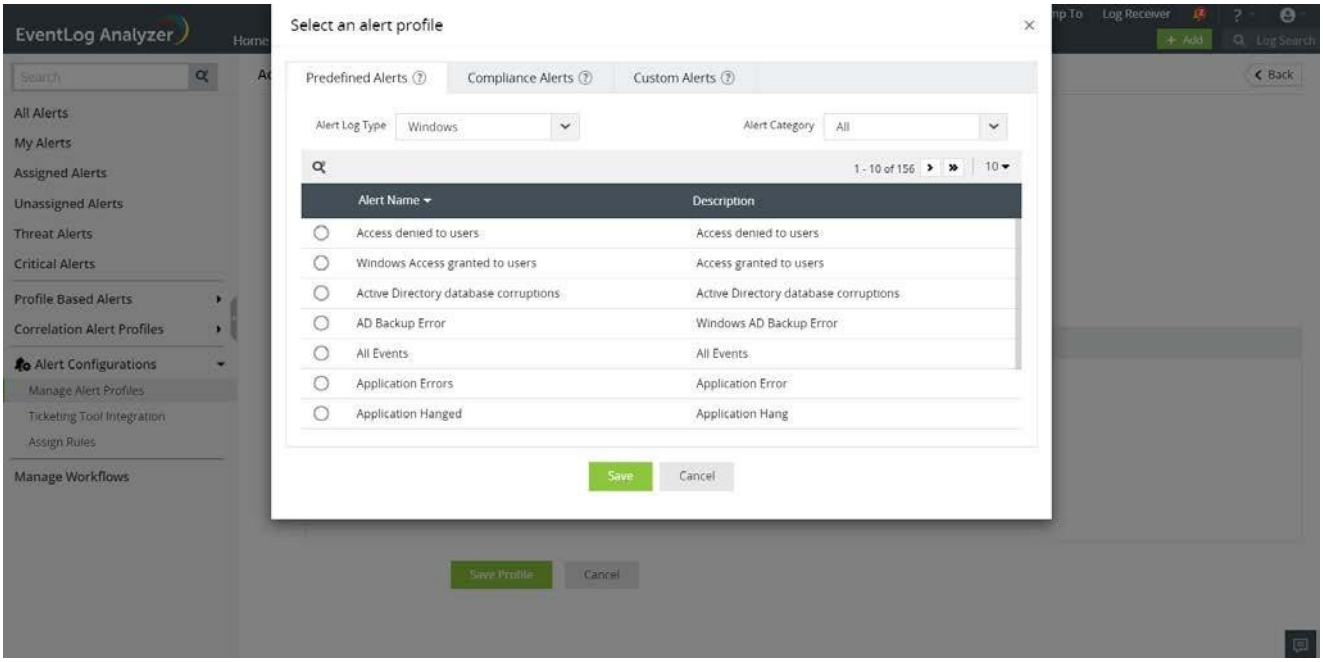


Relatórios de auditoria detalhados: acesse relatórios intuitivos que podem ser facilmente exportados ou programados. Esses relatórios incluem

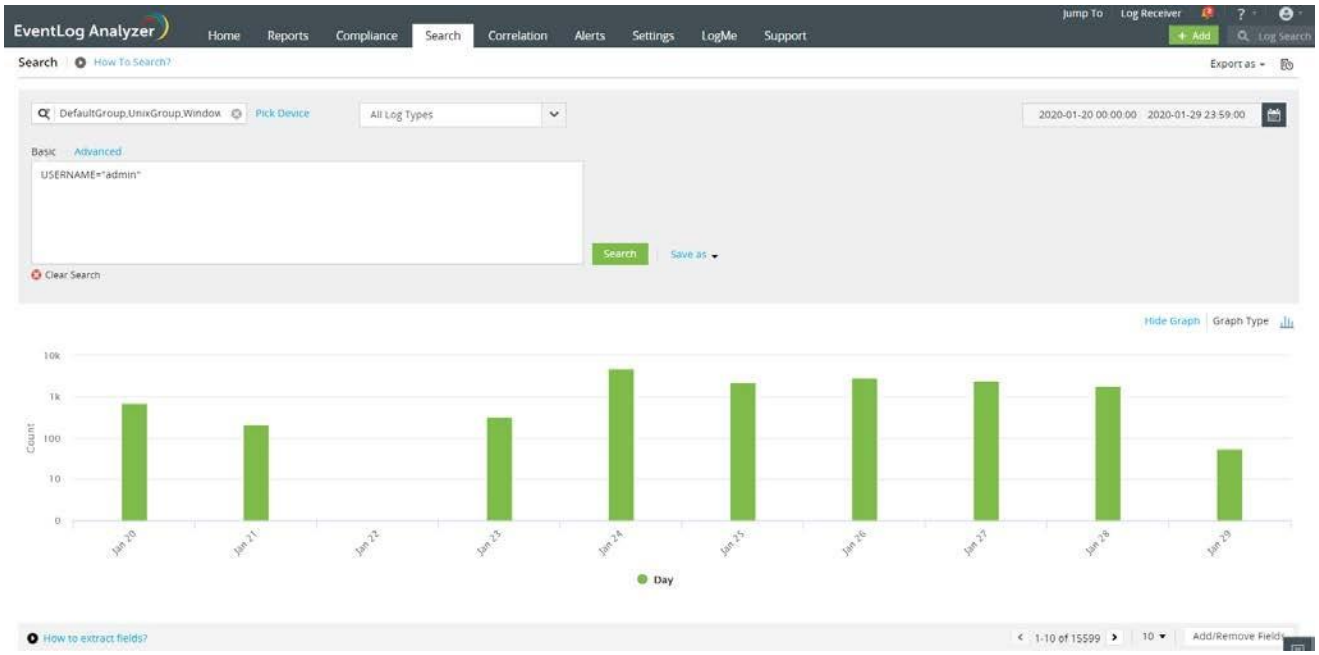
> **Relatórios de atividades de usuários privilegiados independentes:** obtenha relatórios individuais para várias atividades privilegiadas, como mudanças de configuração, instalações de software, acessos e mudanças de dados confidenciais e muito mais.

> **Relatórios consolidados:** obtenha uma visualização consolidada de todas as ações de usuários privilegiados em sua rede Windows no relatório de visão geral da atividade do usuário. O gráfico também pode ser dividido pelo usuário no relatório baseado no usuário.

> **Relatórios de conformidade:** gere relatórios predefinidos para várias políticas de conformidade, incluindo as leis SOX e PCI-DSS, que requerem a auditoria completa da atividade de usuários privilegiados



Alertas de segurança: receba notificações sobre qualquer atividade atípica ou suspeita de usuários privilegiados em sua rede. Obtenha alertas para eventos independentes ou vários eventos correlacionados em sua rede. Você também pode obter alertas baseados em feeds de ameaças e identificar a comunicação entre usuários privilegiados e entidades maliciosas conhecidas.



Investigações forenses: use o mecanismo de pesquisa avançada para investigar incidentes de segurança e descobrir sua causa-raiz. Você pode salvar os resultados da pesquisa como relatórios e usá-los para apresentar qualquer resultado.

As contas de usuários privilegiados têm muito poder em sua rede. Com o EventLog Analyzer, é possível garantir o seu uso de forma responsável e protegidos contra ataques