Soluções de gerenciamento de eventos e informações de segurança
Para o suporte de seus objetivos de TI

Tivoli® software

Perceba todos os benefícios das informações de segurança e do gerenciamento de eventos para operações e conformidade.

Highlights

- Facilite os esforços de conformidade com recursos centralizados de painéis e relatórios
- Ajude a proteger a propriedade intelectual e privacidade fazendo uma auditoria do comportamento de todos os usuários – com ou sem privilégios
- Gerencie as operações de segurança de forma efetiva e eficiente com respostas, investigação, priorização e correlação de eventos de segurança centralizadas.

Integre a grande variedade de recursos de SIEM

O conceito de informações de segurança e gerenciamento de eventos (SIEM) é familiar: centralize eventos relevantes para a segurança e analise dados consolidados para obter insights de segurança valiosos sobre os quais sua organização pode agir. Infelizmente, não tem sido fácil ter uma visão completa de SIEM.

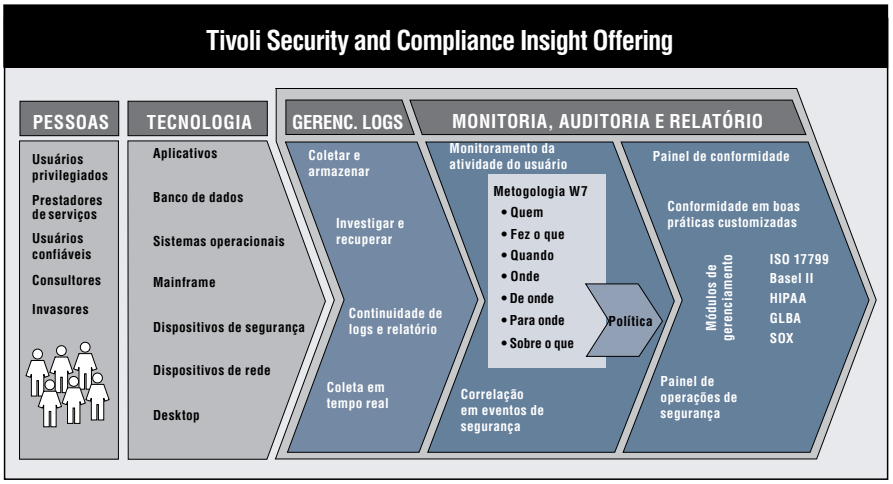
Fornecedores se especializaram em fornecer aspectos diferentes de SIEM. Alguns oferecem um painel de gerenciamento orientado a eventos de rede em tempo real que facilita o reconhecimento de ataques e o gerenciamento de incidentes – e como resultado, isso melhora a resiliência da rede e do recurso. Outros fornecedores oferecem um painel de análise de informações para avaliar com que eficácia uma organização adere às suas políticas de controle.

Mas a maioria das organizações quer constatar os benefícios que ambos os painéis podem fornecer. Consequentemente, elas adquirem vários produtos de diferentes fornecedores e sofrem com a fraca integração dos produtos. Ou fazem diversas customizações para alcançarem seus objetivos de SIEM: otimizar os esforços de conformidade e proteger a propriedade intelectual, a confidencialidade dos dados e as operações de segurança centralizadas.

Hoje, a IBM oferece uma alternativa. O IBM Tivoli Security and Compliance Insight Offering é composto por dois produtos que trabalham juntos para ajudar você a perceber toda a promessa do SIEM corporativo. Com a oferta do Tivoli, você pode centralizar a coleta de logs e a correlação de eventos em sua empresa. E é possível alavancar um painel de conformidade avançado para vincular eventos de segurança e comportamento do usuário às suas políticas corporativas.

A IBM oferece uma solução de SIEM completa, incluindo o seguinte:

- *Painel de conformidade de segurança*
- *Painel de operações de segurança para gerenciamento de incidentes*
- *Correlação de eventos em tempo real*
- *Auditoria de mainframe e sistema operacional*
- *Integração com operações de TI*
- *Relatórios e gerenciamento de log*
- *Auditoria de aplicativos e banco de dados*
- *Privileged-user monitoring and auditing (PUMA)*
- *Relatório regulamentar*
- *Ligação do gerenciamento de identidade.*



O Tivoli Security and Compliance Insight Offering permite obter de ponta a ponta, informação de segurança holística e gerenciamento de eventos.

O Tivoli Security and Compliance Insight Offering fornece uma base abrangente a partir da qual é possível endereçar seus requisitos de SIEM – agora e no futuro. Como resultado, você ajuda a diminuir sua exposição a violações de segurança; controla os custos da coleta, da análise e do relatório de eventos de conformidade; e gerencia a complexidade de uma infraestrutura heterogênea.

Facilite os esforços de conformidade

O Tivoli Security and Compliance Insight Offering fornece um painel de auditoria corporativo robusto que, em contraste com soluções competitivas, pode coletar logs de uma grande variedade de tipos de dispositivos e pode vincular dados operacionais do dia a dia à análise baseada em política da qual os auditores precisam. A solução permite que responsáveis pela segurança de informações executivas e auditores tenham uma visão única de todas as atividades relevantes na empresa a partir deste painel.

Com uma visão rápida, eles podem ver quantas atividades foram registradas e comparam perfis de usuários com as informações que estão acessando. Este painel de auditoria da empresa representa uma metodologia W7 com patente pendente, permitindo que seus usuários interpretem dados de log nativos utilizando uma linguagem facilmente compreensível: Quem, Fez o que, Quando, Onde, De onde, Para onde e Sobre o que.

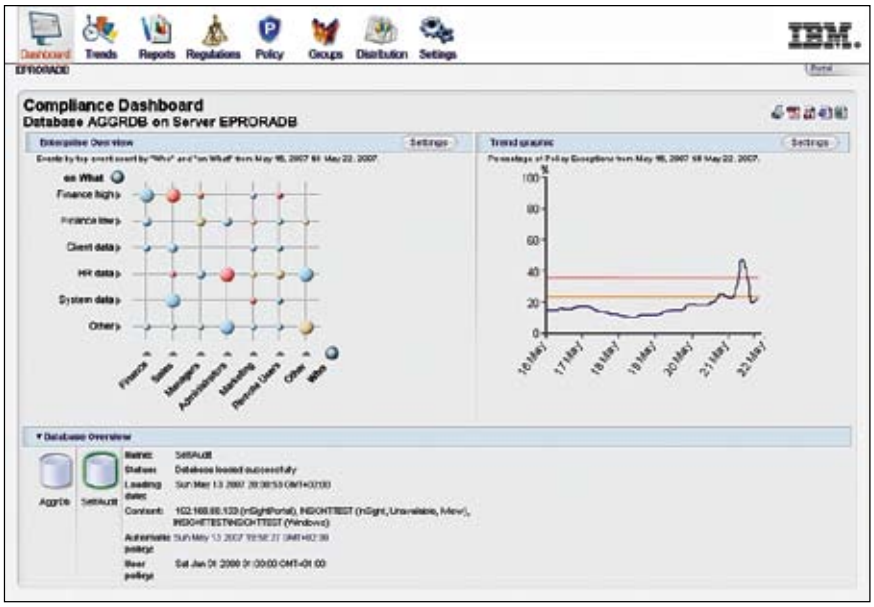
O painel de auditoria corporativo ajuda você a visualizar violações de política com o passar do tempo. Além disso, é possível alavancar bancos de dados de logs que ajudam você a atender a requisitos de conformidade e relatório variáveis de seus negócios. Por exemplo, talvez você queira registrar bancos de dados para serem estruturados por departamento, regulamento ou tipo de tecnologia.

Além do mais, o Tivoli Security and Compliance Insight Offering oferece um relatório de continuidade de log de "visão rápida" que ajuda a demonstrar aos auditores que você coleta cada log, conforme prometido.

Para facilitar esforços de conformidade com requisitos específicos, como o Sarbanes-Oxley (SOX) e Healthcare Information Portability and Accountability Act (HIPAA), a oferta inclui uma ampla variedade de módulos de gerenciamento. Cada módulo fornece ajuda extremamente detalhada:

- *Um modelo de classificação de ativo mostra as classes de informações, pessoas e ativos em sua empresa que são afetados – utilizando o vocabulário empregado pelo regulamento ou pela melhor prática.*

Estudo de Caso: Uma cadeia de mercearias da Fortune 1000 nos Estados Unidos utiliza o Tivoli Security and Compliance Insight Offering para fazer a auditoria de atividades automatizadas, bem como para relatórios específicos padronizados para SOX, HIPAA e o padrão Payment Card Industry (PCI). A solução economiza tempo, recursos e dinheiro da empresa.



O painel do Tivoli Compliance Insight Manager permite que você obtenha uma visão geral de sua postura de conformidade com a segurança, entenda atividades do usuário e monitore usuários privilegiados comparados com estruturas de uso aceitável e política de segurança.

- *Um modelo de política avalia dados de eventos com relação a uma política customizada que recomenda quem deve ter permissão para acessar informações e até que ponto o indivíduo pode lidar com os dados.*
- *Um centro de relatórios representa os modelos de política e classificação de ativos para fornecer dezenas de relatórios de conformidade relevantes adequados aos regulamentos e melhores práticas.*

Proteja a propriedade intelectual e sua privacidade

com acesso a dados financeiros e sensíveis e a capacidade de fazer mudanças que podem causar interrupções operacionais, usuários privilegiados com acesso extensivo através de aplicativos e plataformas podem executar ações acidentais ou dolosas que violam políticas da empresa e levam a incidentes de furto de identidade e furto de propriedade intelectual. Cada vez mais, auditores requerem que você comprove que pode monitorar e fazer auditoria do acesso a dados corporativos críticos ou sensíveis.

Ao mesmo tempo, o trabalho de usuários privilegiados é crítico para o sucesso dos seus negócios. Sua estratégia para monitorar, relatar e investigar suas atividades não deve impedir sua produtividade.

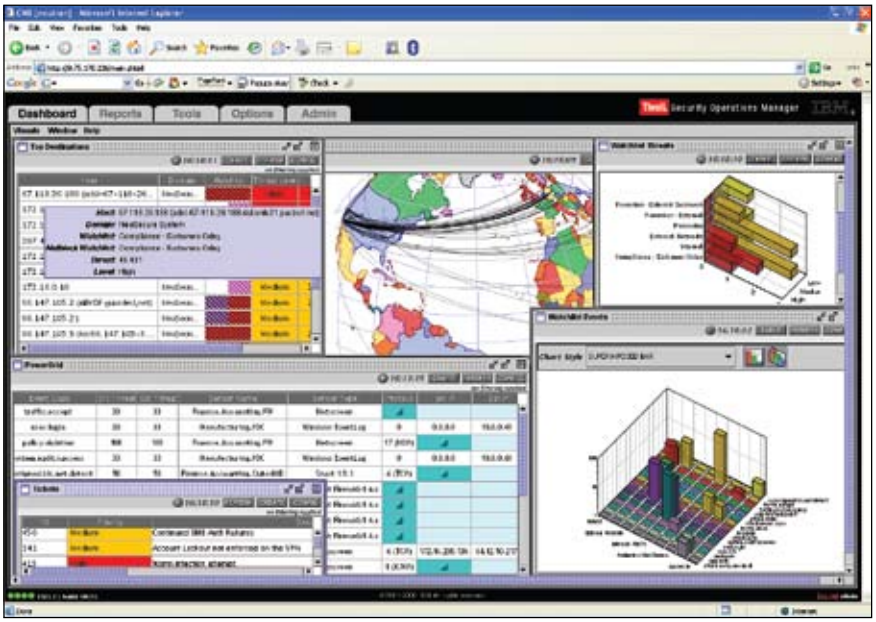
O Tivoli Security and Compliance Insight Offering ajuda você a fazer uma auditoria do comportamento dos usuários na empresa. Recursos PUMA incluem um painel que o permite fazer pesquisas detalhadas em relatórios detalhados de fácil compreensão, onde é possível ver quem em sua organização acessa recursos de informações vitais. Em vez de ler logs secretos, você pode visualizar dados normalizados que tenham sido sincronizados e classificados em grupos lógicos nos sistemas. Eventos excepcionais são sinalizados de acordo com a gravidade dos riscos, de modo que você possa se concentrar naqueles mais importantes. E toda coleta e análise de dados são feitas sem interferir nas atividades autorizadas de usuários privilegiados.

Para proteger ainda mais os dados sensíveis, o Tivoli Security and Compliance Insight Offering inclui a capacidade de fazer auditoria em bancos de dados e mainframes, onde administradores de bancos de dados e de sistemas têm acesso extensivo que deve ser monitorado. A oferta apresenta muito mais do que provisões de dados de syslog básicos; ela coleta e interpreta logs de auditoria nativos para facilitar esforços de conformidade. Além disso, o Tivoli Security and Compliance Insight Offering vincula informações sobre o usuário a nomes de usuário, grupos e muito mais.

Estudo de Caso: Um provedor de serviços financeiros e de turismo presente em mais de 130 países recorre ao Tivoli Security and Compliance Insight Offering para monitorar as atividades de usuários privilegiados e prestadores de serviços. A oferta ajuda a empresa a proteger sua propriedade intelectual em todas as operações globais e a atender aos requisitos de auditorias SOX e assessores PCI.

A IBM também permite que você integre o SIEM com as soluções de gerenciamento de acesso e identidade do Tivoli. Ao visualizar informações de identificação e eventos de segurança em conjunto, você pode entender melhor, por exemplo, quem está dando acesso para os usuários e alterando suas permissões e o que eles fazem com esse acesso e essas permissões.

Gerencie operações de segurança e ameaças de forma efetiva e eficiente monitorando milhares de dispositivos em toda a sua empresa, correlacionar eventos e hospedar riscos de rede representam uma tarefa pesada para a sua equipe de TI – que pode exigir uma quantidade substancial de esforço manual. Mas o Tivoli Security and Compliance Insight Offering inclui um painel de operações de segurança abrangente que dá aos gerenciadores de segurança uma visão em tempo real de painel único dos eventos de segurança correlacionados de diversos dispositivos na infraestrutura da empresa. A equipe de TI pode fazer uma pesquisa detalhada para identificar, investigar e gerenciar eventos excepcionais, ameaçadas e mau uso.



O Tivoli Security Operations Manager apresenta um painel de operações de segurança que facilita o reconhecimento de ataques, a priorização e o gerenciamento de incidentes.

O Tivoli Security and Compliance Insight Offering ajuda você a detectar de forma precisa e abrangente as ameaças à empresa, combinando técnicas de correlação complementares. Ao contrário das plataformas de gerenciamento de segurança que contam principalmente com a correlação baseada em regras, o Tivoli Security and Compliance

Insight Offering também oferece métodos de correlação de estatísticas, de vulnerabilidade e de suscetibilidade, já que métodos diferentes se adequam melhor aos diferentes tipos de ataques e de mau uso.

Após um incidente ser detectado, o painel facilita todo o processo de gerenciamento de incidente inteiro – desde a detecção inicial e priorização até a investigação em um clique, a escalação e, finalmente, as atividades de correção de incidentes. Desenhando boas práticas comprovadas para gerenciamento de incidentes, o Tivoli Security and Compliance Insight Offering controla todas essas atividades de modo que a equipe de conformidade possa utilizar as informações para determinar métricas para o sucesso.

Profundidade do mainframe:
O mainframe está cada dia mais se tornando um recurso integrado crítico dentro de uma empresa de redes. Muitas vezes, seus dados mais críticos residem nele, e os mesmos mandatos de conformidade, auditoria e política que afetam o restante de seu ambiente de TI se aplicam ao mainframe também. O Tivoli Security and Compliance Insight Offering alavanca eventos gerados pelo IBM Tivoli zSecure Alert, que reside no mainframe e monitora os subsistemas IBM z/OS, IBM Resource Access Control Facility (RACF), CA ACF2 e UNIX® para detectar intrusos e configurações incorretas. O Tivoli Security and Compliance Insight Offering também alavanca o IBM Tivoli zSecure Audit para monitorar e relatar a atividade do usuário privilegiado no sistema operacional e nos aplicativos críticos. Ao incorporar estas informações, o Tivoli Security and Compliance Insight Offering expande e aprofunda sua perspectiva de segurança corporativa.

A IBM também pode ajudar você a integrar estes recursos de operações de segurança com o restante de suas operações de TI, incluindo operações de rede, gerenciamento de riscos e gerenciamento de serviços. Como resultado, você pode alavancar outras informações de TI e processos em seus esforços de segurança e, opostamente, utilizar informações de segurança correlacionadas em soluções e painéis de operações de TI mais amplos.

Para mais informações
O Tivoli Security and Compliance Insight Offering fornece uma variedade completa de recursos de SIEM. Esta oferta inclui o seguinte:

- ***O IBM Tivoli Compliance Insight Manager*** *controla atividades do usuário privilegiado e de outros usuários em recursos de TI sensíveis ou confidenciais. Ele coleta, analisa e interpreta dados de log de auditoria nativos a partir de uma grande variedade de recursos de TI em sua empresa, incluindo sistemas operacionais, bancos de dados e aplicativos. Relatórios facilmente customizáveis e compreensíveis e um painel de conformidade são projetados para atender aos requisitos de conformidade e para facilitar respostas rápidas para um comportamento excepcional.*
- ***O IBM Tivoli Security Operations Manager*** *oferece gerenciamento de ameaça à segurança em tempo real. Seus recursos de gerenciamento de incidentes e correlação de eventos automatizados facilitam a resolução de resposta rápida e de preempção de problemas relacionados à segurança para maximizar a disponibilidade da rede. A integração com o IBM Tivoli Enterprise Console e o IBM Tivoli Netcool/OMNIbus – bem como com soluções da central de ajuda, como Remedy – ajuda o Tivoli Security Operations Manager a fornecer insight crítico para a resolução de problemas de TI e de operações para ajudar você a melhorar a resiliência e a disponibilidade do recurso.*

Além disso, o Tivoli zSecure Audit integra-se com o Tivoli Compliance Insight Manager para alimentar registros System Management Facility (SMF) de mainframe para um painel de conformidade e auditoria corporativo. Da mesma forma, para o gerenciamento de operações e ameaças em tempo real, o Tivoli zSecure Alert envia alertas em tempo real para o painel de gerenciamento de rede ou segurança central. Por exemplo, você pode enviar vários alertas de Protocolo Simples de Gerenciamento de Rede (SNMP) para o Tivoli Security Operations Manager para monitoramento de ameaças e correlação em tempo real.

Estudo de Caso: Um provedor de serviços de telecomunicações e wireless nos Estados Unidos com mais de 50 milhões de assinantes conta com o Tivoli Security and Compliance Insight Offering para correlacionar e monitorar automaticamente mais de 750 dispositivos de segurança de rede e 60.000 desktops e servidores globalmente. Como resultado, a empresa reduziu incidentes de segurança em 75% e aumentou a visibilidade da origem do problema de 25% para 90%. Além disso, o departamento de segurança pôde diminuir o tempo médio que levava para resolver os incidentes de 24 horas para 30 minutos.

Para saber mais sobre como o Tivoli Security and Compliance Insight Offering pode ajudar sua organização a facilitar a conformidade, proteger sua propriedade intelectual e sua privacidade e otimizar operações de segurança, entre em contato com seu representante IBM ou Parceiro de Negócios IBM ou visite: **ibm.com**/tivoli

Sobre o software Tivoli da IBM

O software Tivoli fornece um conjunto de ofertas e recursos para suportar o IBM Service Management, uma abordagem escalável e modular utilizada para entregar serviços mais eficientes e efetivos para seus negócios. Ajudando a atender às necessidades dos negócios de todos os portes, o software Tivoli permite que você entregue excelência de serviço no suporte aos seus objetivos de negócio através dos processos de integração e de automação, de fluxos de trabalho e de tarefas. A plataforma de gerenciamento de serviços Tivoli baseada em padrões abertos e altamente segura é complementada por soluções de gerenciamento operacionais proativas que fornecem visibilidade de ponta a ponta e controle. Ela também é amparada pelos serviços de classe mundial da IBM, pelo suporte IBM e por um ecossistema ativo de Parceiros de Negócios IBM. Os clientes e parceiros de negócios Tivoli também podem alavancar as boas práticas uns dos outros pela participação de Grupos de Usuários do IBM Tivoli executados independentemente em todo o mundo – visite: www.tivoli-ug.org

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – Brasil

O site da IBM pode ser encontrado em:
ibm.com

IBM, o logotipo IBM, ibm.com, Netcool, Netcool/OMNIbus, RACF, Tivoli, Tivoli Enterprise Console e z/OS são marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países.

ACF2 é uma marca registrada da CA, Inc. ou de uma de suas subsidiárias

UNIX é uma marca registrada de The Open Group nos Estados Unidos, em outros países, ou em ambos.

Outros nomes de empresas, produtos e serviços podem ser marcas registradas ou marcas de serviços de terceiros.

Renúncia de responsabilidade: O cliente é responsável por garantir a conformidade com os requisitos jurídicos. É responsabilidade exclusiva do cliente obter orientação de um advogado competente quanto à identificação e à interpretação de quaisquer leis e requisitos regulamentares relevantes que possam afetar os negócios do cliente e de quaisquer ações que o leitor possa ter que tomar para cumprir com tais leis. A IBM não fornece conselho jurídico, nem representa ou garante que seus serviços ou produtos irão garantir que o cliente esteja em conformidade com qualquer lei ou regulamento.

Produzido nos Estados Unidos da América
06-07

© Copyright IBM Corporation 2009
Todos os Direitos Reservados.

TIS10415-BRPT-00