Tripwire Log Center

Gerenciamento centralizado de logs simplificado

Dado o ambiente atual de ameaças de segurança sofisticadas, as soluções de análise de segurança e as exigências de conformidade normativa, a necessidade de uma solução de log mais inteligente ficou evidente.

À medida que o volume e a sofisticação das ameaças cibernéticas aumentam, as organizações precisam vasculhar montanhas de dados para identificar ameaças reais. A abordagem tradicional de confiar em ferramentas inadequadas de coleta de logs para fornecer dados de logs e eventos cada vez maiores, a implementações de SIEM (security information event management) caros e de grande escala não é mais suficiente.

O Tripwire® Log Center™ fornece coleta, análise e entrega de logs centralizados seguros e confiáveis. O Tripwire Log Center se integra à sua infraestrutura existente e inclui uma grande biblioteca de regras de correlação, capacitando sua equipe a monitorar, detectar e responder rapidamente a ameaças em seu ambiente.

Não importa se você coleta logs estritamente por conformidade normativa ou para aumentar o conhecimento de ameaças cibernéticas , o Tripwire Log Center garante que o processo seja seguro e confiável.

O que distingue o Tripwire Log Center?

O Tripwire Log Center oferece uma alternativa às abordagens tradicionais para atender às necessidades organizacionais de detecção antecipada de violações, conformidade e coleta de logs segura e confiável.

Dados forenses centralizados

O Tripwire Log Center integra dados do Tripwire Enterprise e do Tripwire IP360™, proporcionando às organizações uma percepção das relações entre eventos suspeitos, alterações do sistema, configurações frágeis e vulnerabilidades atuais. Essa rica combinação de informações permite que você identifique riscos e priorize seus esforços de segurança com mais eficiência. Para aqueles que usam o CIS Controls (20 controles de segurança essenciais) como uma estrutura de segurança, a Tripwire protege sua infraestrutura crítica, correlacionando dados e fornecendo contexto a partir dos quatro primeiros controles.

Habilitando o conhecimento local

A implantação do Tripwire Log Center no nível de departamento ou de agência permite uma resposta mais rápida e a investigação de incidentes, colocando os dados nas mãos das pessoas que conhecem isso melhor, ou seja, os engenheiros e operadores locais. Uma ferramenta SIEM ou analítica centralizada pode fornecer grande valor em um amplo conjunto de dados, mas a investigação de um incidente exige dados detalhados em mãos. O Tripwire Log Center pode sustentar uma função de análise centralizada enquanto simultaneamente permite a visibilidade local.

Análises eficientes

A maioria dos SIEMs e ferramentas de análise de segurança é licenciada com base no consumo, sejam dados indexados ou eventos por segundo, que é um modelo que sofre com o alto custo, difícil planejamento de orçamento e pouca flexibilidade. O Tripwire Log Center pode ser usado para coletar e armazenar todos os eventos de log, enquanto apenas encaminha os que são relevantes para as ferramentas de análise centralizadas. Isso reduz o custo das ferramentas de análise e melhora a flexibilidade.

Conformidade Econômica

A maioria dos padrões de conformidade exige a coleta e o armazenamento de eventos de log, mas atender a esses requisitos com um SIEM centralizado pode ser caro. Também pode ser difícil garantir que os requisitos de conformidade geográfica sejam atendidos para o armazenamento de logs. O Tripwire Log Center pode ser usado como a ferramenta abrangente de armazenamento de logs para conformidade, a um custo menor do que os SIEMs tradicionais. O Tripwire Log Center também pode suportar manter os dados de logs locais em uma geografia, enquanto fornece acesso centralizado para análise. Os clientes usam o Tripwire Log Center para atender aos requisitos e demonstrar conformidade com os padrões PCI DSS, NERC CIP, NIST-800-53, HIPAA e outros.

Rendimento mais rápido: Atenue os riscos após a instalação

O Tripwire Log Center tem uma interface de 'arrastar e soltar' que permite definir e personalizar rapidamente as regras de correlação. Quando uma regra de correlação é acionada, você escolhe a ação: armazenar para gerar relatórios, alertar proativamente ou iniciar uma ação programada. O construtor de regras do Tripwire Log Center reduz a necessidade de conhecimento especializado e recursos para criar regras complexas. O Tripwire Log Center vem com os pacotes de soluções listados abaixo. Consistindo em regras de correlação, painéis e outras ferramentas para segurança e conformidade, sua equipe pode empregá-las para uma rápida configuração.

Pacotes de solução de ameaças e segurança

- Ameaças internas
- Auditoria e autenticação de usuários
- Detecção de negação de serviço
- Detecção de violação e intrusão
- Auditoria de rede e sistema
- Integração de controle de vulnerabilidade e cibercriminalidade
- Auditoria de banco de dados

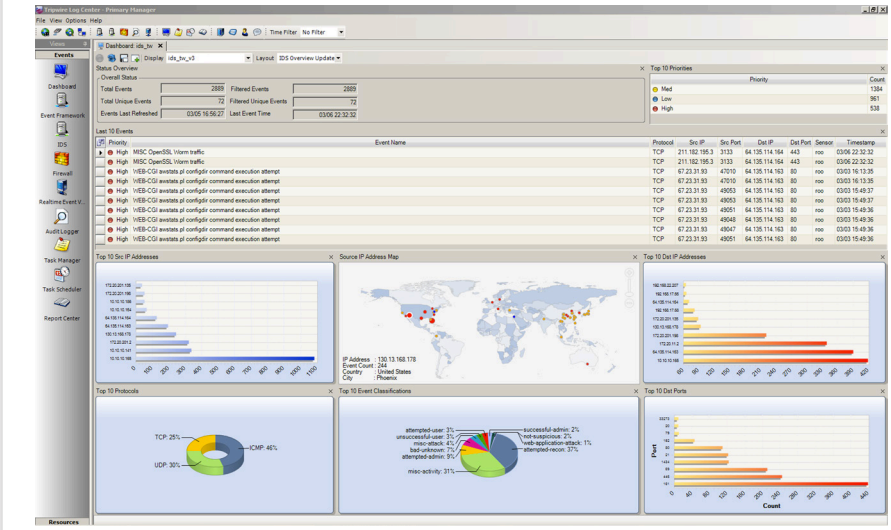

Figura 1 Os painéis de controle de segurança e as exibições de análise de tendências ajudam você a gerenciar seus riscos de segurança e detalhar dinamicamente as áreas que exigem maior controle.

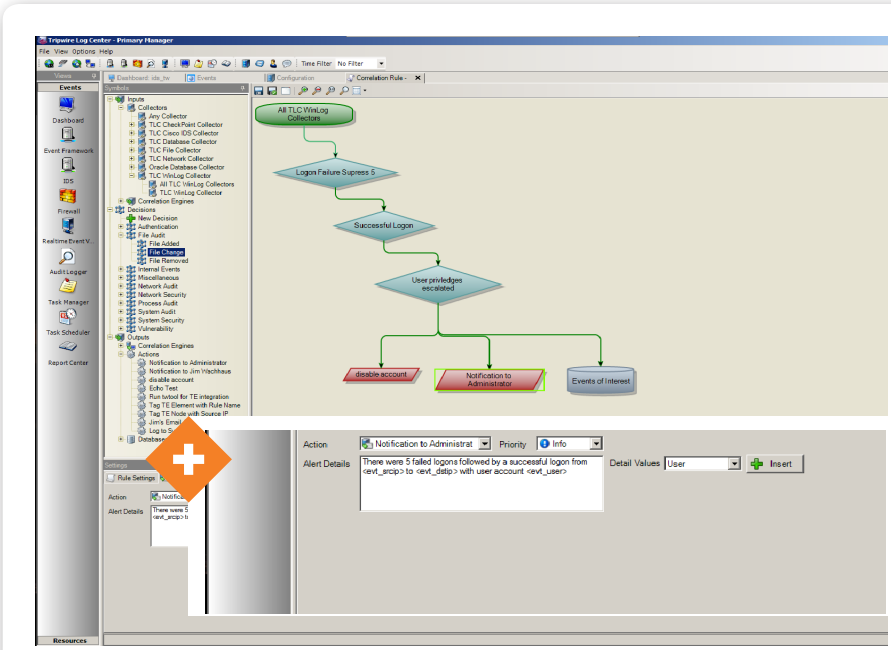

Figura 2 O Tripwire Log Center permite que você defina combinações complexas de eventos criando facilmente regras de correlação com um criador gráfico de regras de "arrastar e soltar".

Pacotes de solução de conformidade

- NERC
- PCI
- NIST 800-53

Tripwire Integrations

- Tripwire Enterprise
- Tripwire IP360™

Você também terá uma visão de alto nível do seu estado de segurança com a correlação avançada de eventos, os painéis e os recursos de análise de tendências da solução, além de poder acessar facilmente dados históricos de investigações forenses.

O Tripwire Log Center facilita a coleta e o compartilhamento de dados de segurança. A classificação com base em padrões da atividade de log e evento suporta buscas entre plataformas e dispositivos, o que produz resultados abrangentes e precisos para investigações de segurança ou em relatórios de conformidade.

Contexto empresarial e de usuário

O Asset View no Tripwire Enterprise pode ser usado para identificar e categorizar seusativos por contexto empresarial. O Tripwire Log Center pode usar automaticamente o contexto do Tripwire Enterprise através de listas dinâmicas de correlação. Além disso, o Tripwire Log Center integra-se ao Active Directory, que permite monitorar usuários e grupos de usuários específicos com base em seus atributos, como títulos, grupos e funções.

A combinação do contexto empresarial e de usuário permite que você monitore facilmente ativos e usuários que, juntos, podem garantir uma observação mais detalhada, por exemplo, de seus ativos de maior valor aos quais os contratantes têm acesso. Você pode priorizar ainda mais o risco correlacionando eventos suspeitos do Tripwire Log Center com alterações suspeitas detectadas pelo Tripwire Enterprise e vulnerabilidades identificadas pelo Tripwire IP360.

Recursos do Tripwire Log Center

Coleta segura e confiável de log

A coleta completa, segura e confiável de logs do Tripwire Log Center garante que as organizações possam atender aos requisitos normativos para o log e tenham os dados de que precisam para análise de segurança e resposta a incidentes. O agente do Tripwire Axon®, usado para coletar dados de log, garante que, se um sistema, dispositivo ou outro ativo falhar, você tenha certeza de que seus dados de log estão seguros. O Tripwire Log Center oferece suporte à coleta de logs sem agente para plataformas nas quais os agentes não podem ser instalados. Além disso, a Tripwire oferece altos níveis de compactação para reduzir as demandas de armazenamento e, ao mesmo tempo, proteger os logs contra alterações.

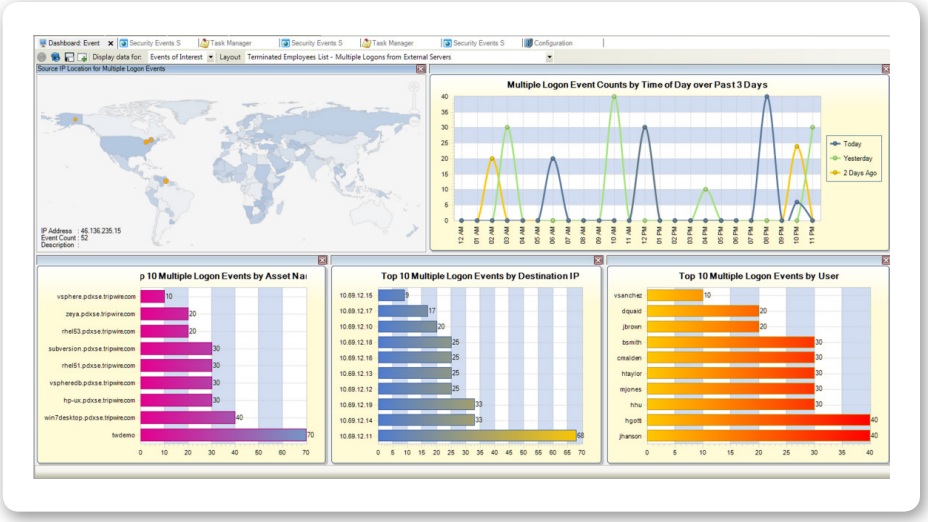

Figura 3 Obtenha os principais indicadores de atividade de violação, adicionando contexto empresariais e de usuários aos seus esforços de detecção de incidentes.

Armazenamento, indexação e procura de logs

Os logs coletados são armazenados e indexados para uma busca eficiente, permitindo a verificação de todos os detalhes coletados durante uma investigação do incidente. O Tripwire Log Center pode armazenar logs de forma centralizada ou distribuí-los por meio de gerentes secundários para manter o armazenamento local e, ao mesmo tempo, facilitar o acesso centralizado.

Correlação de eventos

Enquanto o Tripwire Log Center coleta amplamente eventos de log, ele também pode filtrar informações através do uso de seu mecanismo de correlação. Regras de correlação pré-construídas são incluídas em várias plataformas e finalidades, incluindo padrões de conformidade e casos de uso de segurança. Os clientes podem criar regras de correlação personalizadas usando a interface simples de 'arrastar e soltar' no Tripwire Log Center.

Filtragem e Encaminhamento

As ferramentas de análise de segurança exigem dados de diversas fontes para obter resultados precisos, e os dados de log são uma fonte importante. O Tripwire Log Center pode fornecer a infraestrutura de coleta para oferecer de forma segura e confiável dados de log a ferramentas de análise centralizadas, como um SIEM. O Tripwire Log Center pode filtrar os eventos que envia, reduzindo o ruído gerado pelo envio de cada evento para um SIEM e reduzindo o custo das ferramentas de análise que são licenciadas por dados indexados ou eventos por segundo.

Descoberta de ativos

O Tripwire Log Center pode extrair os dados de log coletados para descobrir ativos anteriormente desconhecidos por meio de sua atividade e interação com os ativos monitorados. Esse método passivo de descoberta de recursos não depende de varreduras de rede nem de monitoramento de tráfego capturado. Os usuários podem adicionar ativos descobertos ao Tripwire Log Center para coleta de logs.

Integração com produtos da Tripwire

Os produtos da Tripwire são projetados para oferecer recursos exclusivos, mas também para agregar valor ao trabalharem juntos. O Tripwire Log Center pode usar os dados de vulnerabilidade do Tripwire IP360 e os dados de contexto empresarial do Tripwire Enterprise para fornecer resultados de correlação mais precisos e completos. O Tripwire Enterprise pode exibir eventos de log diretamente do Tripwire Log Center em sua interface de usuário, resultando em menos tempo gasto na troca de contexto e ferramentas.

A Tripwire é a líder mais confiável para estabelecer uma forte base de cibersegurança. Em parceria com empresas da Fortune 500, organizações industriais e agências governamentais, a Tripwire protege a integridade de sistemas críticos em ambientes físicos, virtuais, em nuvem e de DevOps. O premiado portfólio da Tripwire proporciona os mais importantes controles de segurança, inclusive descoberta de ativos, gerenciamento seguro de configurações, gestão de vulnerabilidades e de registros. Como pioneira no monitoramento da integridade de arquivos (file integrity monitoring, FIM), a experiência da Tripwire se fundamenta em uma trajetória de mais de 20 anos de inovação, ajudando organizações a descobrirem, minimizarem e monitorarem suas superfícies de ataque. **Mais informações em tripwire.com**

Saiba mais em tripwire.com e receba notícias, tendências e valiosas informações sobre segurança em tripwire.com/blog, ou conecte-se conosco no LinkedIn, no Twitter e no Facebook.

TLC7DS3jPTBR 1803