FOLHETO

Proteção do One Identity para análises privilegiadas

Detecte e evite violações de segurança relacionadas ao acesso privilegiado

Benefícios

- Fornece insight sobre o que acontece em seu sistema de TI ao controlar e visualizar a atividade do usuário
- Autenticação contínua por meio da análise constante da dinâmica de pressionamento das teclas e movimentos do mouse
- Identifica desvios incomuns da atividade de linha de base com o aprendizado da máquina
- Reduz o tempo para detectar um incidente de segurança com informações contextuais e priorização baseada em risco de sessões gravadas
- Reduz o ruído dos alertas de segurança para que você possa se concentrar no que importa
- Melhora a segurança ao finalizar as conexões quando é emitido um alerta sobre atividades potencialmente prejudiciais

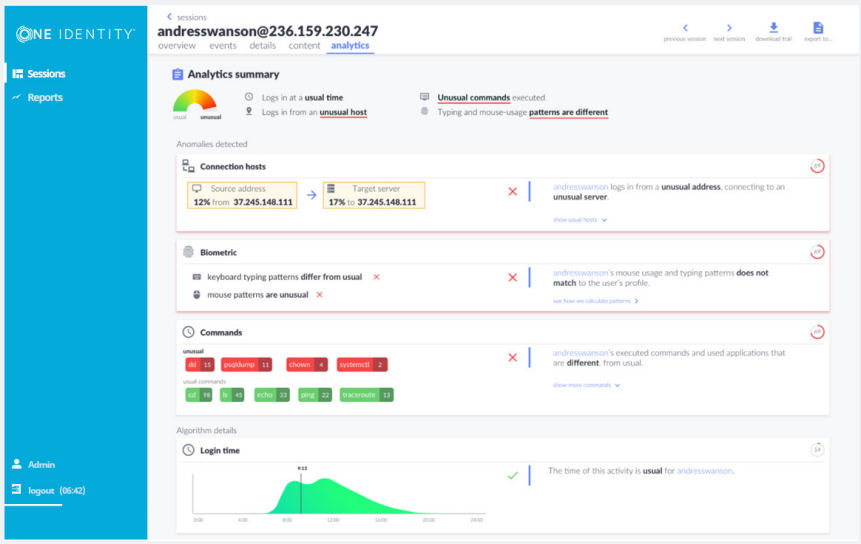
Visão geral

Como gerente de segurança de TI, você sabe melhor do que ninguém que a sua empresa nunca passará por uma violação de conta privilegiada. Hoje, as organizações demoram uma média de 206 dias[1] para identificar uma violação. E tempo significa dinheiro e risco. Dessa forma, independentemente de a violação acontecer de uma conta privilegiada sequestrada ou de um invasor da administração, quanto mais tempo demorar para que ela seja descoberta, mais tempo os intrusos terão para encontrar e roubar dados, além de somar um valor cada vez maior de multas e despesas forenses.

Você provavelmente teve de fornecer acesso privilegiado além de seus administradores confiáveis. Você pode ter realizado uma expansão para incluir administradores terceirizados de consultores externos que poderiam estar em qualquer lugar do mundo. Então, como garantir que os administradores com acesso privilegiado o utilizam para o bem e não para o mal?

Com o One Identity Safeguard for Privileged Analytics, você sabe quem são seus usuários mais arriscados, mantém um olhar constante para novas ameaças internas e externas e pode detectar um comportamento privilegiado incomum. Essa solução eficiente oferece visibilidade total dos usuários privilegiados e de suas atividades e, se houver algum problema, você poderá tomar medidas imediatas e estar bem posicionado para evitar violações de dados.

[1] *Ponemon's 2017 Cost of Data Breach Study (Estudo sobre o custo da violação de dados da Ponemon 2017)*



Determine usuários e comportamentos arriscados de forma fácil

Veja rapidamente se a atividade de um usuário é incomum e potencialmente arriscada com a visualização do resumo da análise. Ele contém um resumo de comandos incomuns, atividade biométrica e hosts de conexão.

Recursos

Detecte ameaças desconhecidas em tempo real

A segurança baseada em regras não detectará novos métodos de ataque externos ou funcionários mal-intencionados. O Safeguard for Privileged Analytics controla e visualiza a atividade do usuário em tempo real para uma melhor compreensão do que realmente acontece em seu ambiente de TI. Não são necessárias regras de correlação predefinidas; bastam os dados da sua sessão para que ele funcione.

Operação livre de padrões

Em vez de usar a correspondência baseada em padrões para detectar o comportamento "mal conhecido", que geralmente é incorreto, o Safeguard for Privileged Analytics usa dados coletados do seu ambiente de TI. Ele cria uma linha de base de comportamento "normal" e detecta desvios ao usar vários algoritmos de aprendizado de máquina.

Análise de conteúdo da tela

Ao analisar o conteúdo da tela de sessões privilegiadas e entender os comandos emitidos e títulos de janela, o Safeguard for Privileged Analytics pode enriquecer o perfil de comportamento da linha de base dos comandos e aplicações usados regularmente por seus usuários privilegiados. Essa análise granular facilita a identificação de comportamentos típicos e a detecção de roubos de identidade privilegiados.

Biometria comportamental

Cada usuário tem seu próprio padrão de comportamento idiossincrático, mesmo ao executar ações idênticas, como digitar ou mover um mouse. Os algoritmos incorporados no Safeguard for Privileged Analytics inspecionam essas características comportamentais capturadas pelo Safeguard for Privileged Sessions. A dinâmica do pressionamento de teclas e a análise do movimento do mouse não apenas ajudam a identificar violações, como também funcionam como uma autenticação biométrica contínua.

Reduza o ruído de alertas

O Privileged Analytics reduz o ruído de alertas gerado pelos SIEMs ao categorizar os eventos do usuário com base nos níveis de risco e desvio e ao realçar os eventos mais suspeitos. Os alertas podem ser enviados para SIEMs ou seus analistas de segurança podem visualizar uma lista priorizada de eventos na interface do usuário intuitiva, o que permite que eles se concentrem nos mais importantes.

Resposta automática

Na maioria dos cenários de ataque, os eventos de alto impacto são geralmente precedidos por uma fase de reconhecimento. Assim, a detecção e resposta durante essa fase são fundamentais para evitar atividades prejudiciais. A integração perfeita com o Safeguard for Privileged Sessions permite o encerramento automático da sessão sempre que ocorrer um evento altamente suspeito ou um comportamento mal-intencionado for detectado.

A abordagem do One Identity ao gerenciamento de acesso privilegiado

O portfólio One Identity inclui o conjunto mais abrangente do setor de soluções de gerenciamento de acesso privilegiado. Você pode aproveitar os recursos do One Identity Safeguard for Privileged Analytics com soluções para gerenciamento de senha e sessão, delegação granular da conta raiz do UNIX e da conta de administrador do Active Directory, os suplementos para preparar o sudo de código aberto para a empresa e registros de pressionamento de tecla para atividades raiz do Unix. Tudo isso é firmemente integrado à solução de ponte do Active Directory líder do setor.

Sobre o One Identity

O One Identity ajuda as organizações a obter o melhor Gerenciamento de Identidades e Acessos (IAM). Com a nossa combinação exclusiva de ofertas, inclusive um portfólio de soluções de governança de identidades, gerenciamento de acessos, gerenciamento privilegiado e identidade como serviço, as organizações podem alcançar total potencial, sem obstáculos de segurança e protegidas contra ameaças. Saiba mais em OneIdentity.com

Datasheet_2019_PAM-Privileged-Analytics_US_RS_41021