Detecção de Intrusão

1. Detecção e resposta em endpoints (EDR)
2. Monitoramento de integridade de arquivos (MIA)
3. Sistema de engano
4. IDS baseado em host
5. IDS de rede

HORIZON TECH

1. Monitoramento de segurança para endpoints em redes locais e em nuvem

Hoje, os desktops corporativos representam uma das principais áreas de risco de segurança para as organizações. À medida que os agentes mal-intencionados projetam cada vez mais seus ataques para evitar as ferramentas tradicionais de prevenção e proteção de endpoints, as organizações buscam a EDR (detecção e resposta em endpoints) para obter visibilidade adicional, incluindo evidências de ataques que podem não acionar regras de prevenção. No entanto, embora muitas equipes de segurança reconheçam a necessidade de detecção avançada de ameaças para endpoints, a maioria não possui recursos para gerenciar uma solução EDR autônoma.

A Horizontech pode ajudar. Nossa solução elimina o custo e a complexidade de adicionar mais uma solução individual ao seu ferramental de segurança. Oferecemos EDR como parte de uma plataforma unificada para detecção avançada de ameaças, resposta a incidentes e conformidade. De forma automatizada, busca ameaças nos endpoints e nos ambientes em nuvem e na rede local, para detectar e responder a ameaças onde quer que elas ocorram. E com a inteligência contínua de ameaças da equipe de pesquisa de segurança de parceiros da Horizontech, suas defesas permanecem atualizadas à medida que as ameaças evoluem.

Diferentemente das soluções de segurança individual, nossa solução combina vários recursos de segurança em uma plataforma de nuvem unificada, incluindo EDR, SIEM, detecção de intrusão, avaliação de vulnerabilidades e muito mais, oferecendo os recursos essenciais de segurança necessários para um alto nível de segurança em seu ambiente sem complexidade.

Com os recursos de EDR integrados, é possível realizar o monitoramento de segurança de terminais e redes em ambientes na nuvem e na rede local.

Buscas automatizadas de ameaças e sistema de engano

- Busca automatizada de ameaças em todos os lugares onde as ameaças modernas aparecem
- Detecção de movimentações laterais maliciosas na rede
  nvestigação rápida de ameaças mais com informações contextuais sobre o ativo infectado
- Priorização automaticamente das ameaças oferecendo uma resposta mais rápida e eficaz a incidentes
- Relatório de Sandbox de arquivos utilizados em infecções e invasão
  nvestigação e resposta a incidentes com orquestração integrada
- Detecta ações maliciosas na rede com baixa taxa de falso positivo

Visibilidade de segurança em ambientes na nuvem e na rede local

- Visibilidade da segurança e o monitoramento de todos os seus ativos críticos
- Economize significativamente utilizando nossos serviços de segurança
- Relatórios customizados e pré-criados de conformidade

Acelere os esforços de conformidade com o gerenciamento de segurança unificado

- Atende os requisitos de conformidade para monitoramento de integridade de arquivos (MIA)
- Demonstração fácil de conformidade com painéis e modelos de relatórios pré-criados
- Gerenciamento de log de ativos, otimizando o atendimento de conformidade

Buscas automatizadas de ameaças e sistema de engano

Quando se trata de resposta a incidentes, a velocidade é importante. Por exemplo, se for detectado atividades maliciosas no tráfego da rede, como um host que se comunica com um servidor de comando e controle conhecido, nossa solução permite uma investigação completa pois incluirá a consulta ao host para obter mais informações, como uma lista de processos em execução e conexões de rede. No entanto, se for preciso trabalhar com várias ferramentas de segurança para coletar essas informações e relacioná-las manualmente, isso poderá atrasar muito a investigação e sua resposta. Em vez disso, nossa solução automatiza a busca e a priorização de ameaças, permitindo uma resposta a incidentes mais rápida e eficaz.

Busca automática de ameaças

Diferentemente das soluções individuais que detectam apenas ameaças em ativos, a solução de segurança da Horizontech detecta ameaças modernas onde quer que elas apareçam. Nossa plataforma unificada correlaciona de forma inteligente os eventos da rede, movimentação lateral na rede e dados de ativos, oferecendo a melhor posição para detectar ameaças com antecedência e segurança.

Investigue ameaças mais rapidamente com informações contextuais

Nossa solução, permite investigar e responder a incidentes de segurança mais rapidamente com todas as informações relevantes sobre ameaças necessárias em um único painel. Consolidamos as informações relevantes sobre todos os alarmes, incluindo o ativo afetado, suas vulnerabilidades, eventos relacionados à rede e desktops, orientações passo a passo sobre respostas, proporcionando uma rápida resposta ao incidente.

Priorização automática de resposta a incidentes

Nossa solução detecta automaticamente ameaças avançadas de endpoint, incluindo aquelas projetadas para driblar as ferramentas antivírus tradicionais, usando inteligência contínua contra ameaças das equipes de pesquisa. A equipe de pesquisa de segurança de parceiros Horizontech, trabalha em seu nome para pesquisar ameaças emergentes e em evolução no mundo e atualiza continuamente sua plataforma com a mais recente inteligência de ameaças acionável, incluindo regras de correlação e consultas de endpoint. Isso permite automatizar as atividades de busca de ameaças, para concentrar recursos na investigação de incidentes e na resposta rápida.

Acelere a investigação e resposta a incidentes com orquestração

Nossa plataforma permite uma aceleração das atividades de investigação e resposta a incidentes por meio de consultas proativas em endpoints, orquestração avançada de segurança e recursos de automação de resposta a incidentes.
A Horizontech consegue fazer consultas pró ativamente nos ativos monitorados a qualquer momento, para obter dados que adicionam contexto às investigações de ameaças. Por exemplo, é possível gerar alertas para qualquer tipo de evento, como a instalação de um software ou mudança de configurações. Com a capacidade de automatizar ações de orquestração e resposta, a Horizontech consegue responder com muito mais rapidez e eficiência para conter ameaças.

Visibilidade e o monitoramento da segurança para ativos críticos

Embora as soluções independentes de EDR ofereçam visibilidade do endpoint, elas não fornecem visibilidade completa de todo o seu ambiente. Para isso, você também deve ter visibilidade das atividades que acontecem nas redes locais, nas contas de nuvem pública e nos aplicativos de nuvem críticos para os negócios, como o Office 365 e o G Suíte. As abordagens em silos do monitoramento de segurança podem deixar pontos cegos em seu programa de segurança e criar sobrecarga adicional, pois sua equipe deve manter e trabalhar em vários sistemas diferentes para investigar e responder a ameaças. Para obter visibilidade completa e centralizada da segurança de todos os seus ativos críticos, você deve ter as habilidades e os recursos para integrar várias ferramentas e fontes de dados.

Com a Horizontech, você obtém visibilidade e monitoramento de segurança centralizados e completos de todos os seus ativos críticos, investigando seus incidentes de segurança mais rapidamente com um contexto completo do que está acontecendo em suas redes, ambientes em nuvem e endpoints, mesmo quando estão desligados a rede corporativa. Em uma plataforma unificada, a Horizontech combina os recursos essenciais de segurança e a inteligência acionável de ameaças necessárias para detectar e responder às ameaças modernas em todos os lugares em que elas aparecem.

Com a plataforma centralizada da segurança de endpoints, plataformas na nuvem, aplicativos na nuvem e redes locais, a Horizontech detecta ameaças mais cedo, investiga e responde mais rapidamente e apoia sua empresa nos esforços de conformidade.

- Maior valor em seu investimento inicial e operações contínuas
- Automatização da busca de ameaças em todos os lugares onde as ameaças modernas aparecem, não apenas os endpoints
- Investigação e priorização de resposta mais rapidamente com uma visão consolidada de todas as ameaças, vulnerabilidades e ativos
- Informações do cenário de ameaças em evolução com inteligência contínua sobre ameaças
- Simplicidade e eficiência nas atividades de resposta a incidentes com orquestração e automação de segurança
- Consolidação de suas ferramentas de segurança com uma plataforma tudo-em-um que combina recursos essenciais de segurança como SIEM, gerenciamento de logs, previsão, IDS, engano, avaliação de vulnerabilidades e muito mais

Aceleração ao atendimento de conformidade

As soluções independentes tornam desafiador para as equipes de segurança demonstrar conformidade, exigindo esforço manual em vários sistemas para se preparar para cada auditoria. A Horizontech adota uma abordagem diferente.

Construído como uma plataforma unificada para gerenciamento de segurança e conformidade, a solução da Horizontech acelera e simplifica o atendimento de conformidade, permitindo que as equipes de segurança monitorem todos os seus ambientes críticos em um único painel. Com recursos como monitoramento de integridade de arquivos embutido, modelos de relatório pré-criados e gerenciamento centralizado de logs, nossa solução reduz drasticamente o tempo, os recursos e os custos associados à conformidade

Atender requisitos de conformidade para monitor a integridade de arquivos (MIA)

Muitos padrões de conformidade exigem que você execute o FIM (em inglês: File Integrity Monitor) ou português MIA (Monitoramento da Integridade do Arquivo), incluindo o PCI DSS 3.2. Com os recursos integrados de EDR da nossa solução, é possível pode acelerar os esforços de conformidade sem precisar introduzir um software adicional de monitoramento de integridade de arquivos (MIA). Nossa solução detecta automaticamente alterações suspeitas ou anômalas em arquivos e registros críticos no Windows e Linux, bem como nos locais na nuvem, como o Office 365 Sharepoint e o G Suíte. E, fornece uma visão consolidada das informações atualizadas dos ativos,

incluindo software e serviços, vulnerabilidades, alterações feitas nos arquivos principais e eventos de segurança, além de modelos de relatórios de conformidade pré-criados, é possível disponibilizar rápido e facilmente essas informações durante uma auditoria de conformidade.

Logs organizados para otimizar o atendimento de conformidade

O gerenciamento de logs é um princípio básico de qualquer programa de segurança e conformidade, mas a maioria das soluções de segurança não fornece os recursos completos e seguros de gerenciamento de logs necessários para investigações forenses e fins de conformidade. Gerenciar logs de terminal separadamente em uma solução SIEM e EDR é complicado e ineficiente.

A Horizontech pode centralizar e simplificar todos os seus logs de segurança e conformidade em um local seguro na nuvem. Nossa solução coleta e armazena automaticamente os dados de log da rede e de endpoints, incluindo logs brutos com registro de data e hora, em um ambiente seguro e certificado. Isso alivia o ônus de ter que gerenciar e proteger logs no local, enquanto fornece um ambiente de gerenciamento de logs pronto para conformidade.

Demonstre facilmente a adaptação com painéis pré-criados e modelos de relatório

A solução Horizontech inclui uma biblioteca de modelos pré-criados que podem ser usados para produzir relatórios avançados para demonstrar a execução durante uma auditoria. Na implantação, fornecemos modelos de relatório para monitoramento de integridade de arquivos do Windows e Linux, que podem dar suporte aos seus requisitos de conformidade com o PCI DSS. Além disso, os modelos de relatório pré-criados para eventos, inclui histórico de comandos, eventos do Docker, atividade de login e muito mais, simplificam a exibição da visibilidade disponível para monitorar atividades na rede e dispositivos.

2. Monitoramento de integridade de arquivos

Alterações em servidores críticos geralmente sinalizam uma violação. É por isso que é essencial usar o MIA (monitoramento da integridade dos arquivos) para sistemas críticos, gerando um alerta assim que ocorrerem alterações nos arquivos críticos do sistema, nos arquivos de configuração e nos dados confidenciais, bem como nos arquivos de log e auditoria modificado para ocultar os rastros de um atacante. De fato, se esses servidores estiverem no escopo do CDE(Cardholder Data Environment), os requisitos do PCI DSS 10.5.5 e 11.5 determinam que deve-se instalar o software MIA para passar na auditoria.

Nossa plataforma ajuda a atender a esses requisitos do PCI DSS com o monitoramento da integridade de arquivos integrado à sua plataforma unificada para detecção de ameaças, resposta e gerenciamento de conformidade. Simplificando a segurança e a conformidade com a visibilidade centralizada de seus ambientes locais e na nuvem, incluindo AWS e Azure, além de aplicativos em nuvem como o Office 365 e G Suíte, ajudando a eliminar pontos cegos potencialmente perigosos. Nossa plataforma unificada combina vários recursos de segurança em um único painel, incluindo SIEM, gerenciamento de logs, detecção de intrusões, avaliação de vulnerabilidades, automação de resposta a incidentes e muito mais, garantindo que você tenha as ferramentas essenciais ao seu alcance para demonstrar e manter a conformidade, e são recursos cruciais de detecção e resposta a ameaças em todo o ambiente.

Implemente o MIA em seus ativos críticos

- Monitore o acesso desde o arquivo a dados confidenciais no seu CDE(Cardholder Data Environment) e saiba quando são feitas alterações nos arquivos críticos
- Armazena detalhes de alarmes acionados pelo MIA para identificar quem acessou, baixou e modificou arquivos críticos
- Relate facilmente as atividades do MIA usando os relatórios PCI DSS integrados e crie suas próprias visualizações e relatórios personalizados para revisão
- Simplifique a auditoria de servidores com detecção combinada de intrusão de host e MIA
- Oferecemos o monitoramento de integridade de arquivos, o monitoramento de registros, o IDS baseado em host e o sistema de engano juntos em uma solução
- Monitora privilégios de usuários de acordo com os requisitos do PCI DSS

Prepare-se rapidamente para conformidade com nossa solução
Atinja seus objetivos de conformidade com mais rapidez e orçamento com a nossa solução

Implemente o monitoramento da integridade de arquivos em seus ativos críticos

De um modo geral, devemos ser seletivos sobre onde e como habilitar sua solução MIA, pois muitos arquivos de sistema e aplicativos mudam frequentemente em um ambiente dinâmico. Você devemos nos concentrar no monitoramento da integridade de arquivos críticos em ativos dentro do escopo para detectar modificações não autorizadas que possam indicar dispositivos ou aplicativos comprometidos. Em outras palavras, instale o MIA sempre que precisar monitorar as alterações feitas nos servidores no escopo.

Os recursos internos de MIA da nossa solução permite monitorar facilmente os sistemas que contêm dados confidenciais no CDE, na nuvem ou no local, alertando-o sobre as alterações feitas nos arquivos críticos. Mas não pára por aí, podemos correlacionar os dados de monitoramento de integridade de arquivos com outros dados em todo o ambiente, para visibilidade e contexto completos. Qualquer acesso ou modificação a um arquivo monitorado é rastreado, e os recursos de correlação de nossa plataforma geram um alarme para notificá-lo sobre qualquer atividade anômala contra o arquivo. E, embora nem todos os acessos e alterações exigem uma resposta, é importante monitorar todas as atividades para determinar primeiro uma linha de base e depois detectar qualquer anormalidade, como violações de políticas ou possível comprometimento do sistema. O resultado final é uma inteligência acionável que permite priorizar de acordo com a necessidade.

Por último, mas não menos importante, são os modelos personalizáveis e predefinidos para o PCI DSS e outros regulamentos de conformidade que tornam rápido e simples a revisão da atividade do MIA em seu ambiente e a geração rápida de relatórios de auditoria no local.

O padrão PCI DSS é explícito nisso. Se você precisar demonstrar conformidade com o PCI DSS, instale o MIA em seus ativos críticos para rastrear alterações em:

- Arquivos críticos do sistema, incluindo executáveis do sistema e de aplicativos
- Arquivos de configuração e arquivos de conteúdo, incluindo dados do titular do cartão e outras informações confidenciais
- Arquivos de log e auditoria centralmente armazenados, históricos ou arquivados
- Chaves e credenciais digitais usadas para autenticação e autorização seguras de entidades e usuários

Nossa solução entrega visibilidade abrangente e uma trilha de auditoria necessária, permitindo rastrear facilmente alterações em arquivos críticos, independentemente da localização do ativo, permitindo validar qualquer alteração que tenha sido autorizada, esperada e que não comprometa a integridade ou segurança dos dados contidos nesses arquivos ou impactar negativamente as operações de segurança dos sistemas críticos para os negócios.

Auditoria de servidores com detecção de intrusão de host, engano e MIA

MIA, Monitoramento de Registro do Windows, HIDS e engano juntos

Turbinamos a implementação do MIA correlacionando dados com um sistema de detecção de intrusão baseado em host (HIDS) e com o sistema de engano.

Permitindo o monitoramento da integridade dos arquivos, o monitoramento do registro do Windows, a detecção de intrusão baseada em host (HIDS) e detecção de movimentação lateral maliciosa, oferecendo os mais robustos controles de detecção de intrusão e gerenciamento de alterações na nossa solução.

Monitoramos atividades privilegiadas de usuários e administradores

Monitorar a atividade privilegiada do usuário em seus sistemas e contas críticos é uma prática recomendada de segurança essencial. De fato, muitos padrões regulatórios, incluindo o PCI DSS, exigem explicitamente.

A implementação do IDS baseado em host permite monitorar a atividade do usuário em seus sistemas críticos. Esses eventos são capturados, processados e correlacionados com outros dados para fornecer o contexto necessário para uma resposta eficaz a incidentes.

Prepare-se rapidamente para conformidade

Embora o monitoramento da integridade dos arquivos seja um componente crítico da conformidade com o PCI DSS, além de outros padrões regulamentares, as ferramentas MIA por si só não são suficientes para passar na sua próxima auditoria. Você precisa de uma ampla variedade de tecnologias e recursos de segurança para demonstrar a conformidade com os outros requisitos do PCI DSS. E, embora possa parecer tentador usar uma ferramenta de monitoramento de integridade de arquivo autônoma - seja de código aberto ou comercial - para passar na sua próxima auditoria, não é um atalho viável para conformidade.

Para a maioria das equipes de segurança de TI, é um desafio significativo obter, adquirir e integrar todas as soluções de segurança de múltiplos pontos necessárias para estar pronto para conformidade. Isso não apenas consome tempo, recursos e orçamento significativos, mas a maioria das organizações precisa estar pronta para auditoria ontem.

Nossa solução aborda a urgência, os altos custos e os desafios técnicos complexos que envolvem a conformidade com o PCI. Ao reunir vários recursos de segurança essenciais necessários para atender à conformidade em uma plataforma unificada - incluindo descoberta de ativos, avaliação de vulnerabilidades, detecção de ameaças (incluindo malware e ransomware), resposta a incidentes e gerenciamento e relatórios de log de conformidade - a Horizontech oferece um serviço rápido, acessível e solução de gerenciamento de conformidade fácil de usar.

Se seus ambientes de portadores de cartão tocam sua infraestrutura local, a nuvem da AWS ou do Azure ou existem em um ambiente híbrido, nossa plataforma oferece um conjunto abrangente de tecnologias de segurança e inteligência integrada contra ameaças que podem ser totalmente implantadas em dias, não semanas ou meses. Com isso, você pode se preparar para sua auditoria de abordagem rápida e manter o gerenciamento contínuo de segurança e conformidade durante todo o ano.

Veja como a Horizontech suporta os Requisitos do PCI DSS
<criar tabela (requisito PCI x Funcionalidades de serviço>

3. Monitoração e proteção de rede com sistema de engano

Nossa plataforma utiliza uma nova geração de tecnologia de anti-fraude que fornece detecção e prevenção de violações em tempo real. Nossa solução comprovada em campo engana os possíveis invasores com armadilhas prontas para uso (armadilhas) que "imitam" seus verdadeiros ativos. Centenas ou milhares de armadilhas podem ser implantadas com pouco esforço, criando um campo de minas virtual para ataques cibernéticos, gerando alertas sobre qualquer atividade maliciosa com inteligência acionável imediatamente.

Devido a alta precisão de alertas e detecção o sistema de engano oferece uma grande vantagem para equipes de segurança. A detecção imediata de movimentações laterais maliciosas na rede, dá uma visão ampla e instantânea de ações que possam trazer prejuízo para sua empresa.

Utilizando ativos falsos recheados de informações falsas porém customizadas para a sua empresa, esta tecnologia faz com que atacantes sejam ludibriados com informações aparentemente importantes da empresa enquanto a equipe de segurança recebe um alerta na primeira movimentação malicioso.

Além de identificar com alta precisão movimentações maliciosas na rede, nossa solução também implementa chamarizes para desviar atacantes de ativos críticos da rede, levando o atacante para os dispositivos falsos com informações falsas sem que ele perceba, e continue entregando métodos e formas de ataque, que são repassados para a equipe de resposta a incidentes.

Detecção de movimentações laterais e mais

- Detectar ações de reconhecimento na rede
- Dispara gatilhos de mitigação automática de acordo com as ferramentas de rede
- Implementa de forma automatizada iscas em ativos críticos da rede
- Detecta conexões a rede TOR
- Monitora uplinks por assinaturas de C&C (command&control)
- Gera relatório sandbox de arquivos suspeitos
- Detecta tráfego de assinaturas conhecidas como maliciosas

Simula diversos tipos de dispositivos, atendendo a todos os setores

- Linux, MAC, windows, android, iphone
- Indústria (scada), Saúde, Finanças (swift)
- Dispositivos IoT
- Criação de simulações customizadas para sua empresa

Tecnologia que oferece proteção com falso-positivo próximo a zero

A forma como a tecnologia de engano funciona, baseado em fatos, garante uma taxa muito baixa de falso-positivo. As armadilhas ficam passivas na rede, não são anunciadas como serviço então, na rotina diária da rede, um funcionário nunca vai acionar uma armadilha, isso mostra que caso uma armadilha seja acionada, é porque alguém ou um malware efetuou alguma movimentação além do escopo permitido pela empresa, acionando as armadilhas.

Nossa solução consegue identificar as mais singelas movimentações laterais, conhecidas como stealth scans, que são softwares que conseguem fazer reconhecimento de uma rede sem que as proteções tradicionais consigam detectar. Até conexões incompletas, ou seja, que não finalizaram a negociação de protocolo (handshake) são detectadas pelo nosso sistema.

Tecnologia que oferece proteção com falso-positivo próximo a zero

Ao ser gerado um alerta seja de armadilhas ou do sistema IDS, vários recursos de segurança essenciais são correlacionados, incluindo descoberta de ativos, avaliação de vulnerabilidades, detecção de ameaças (incluindo malware e ransomware), resposta a incidentes e gerenciamento e relatórios de log de conformidade, o que permite uma visão ampla do ataque, onde informações cada ferramenta complementa com suas informações inerentes e todos os dados são correlacionados, por exemplo:

1. Foi detectada uma movimentação lateral de reconhecimento

2. Alguns minutos depois, um servidor crítico registrou logon do administrador vindo de uma estação de trabalho identificada com origem da ação no passo 1.

3. Outros servidores também reportaram a tentativa de logon de administrador vindo do servidor comprometido no passo 2

4. Arquivos de sistema e registros do windows do servidor comprometido foram alterados

5. Alto tráfego de rede registrado tendo como origem o servidor comprometido

De posse de todas essas informações, é possível tomar ações de resposta a incidentes e também configurar respostas automatizadas de mitigação.

4. Monitoração e proteção de sistemas críticos com IDS baseado em host

Um IDS baseado em host é um sistema de detecção de intrusão que monitora a infraestrutura do computador em que está instalado, analisando o tráfego e registrando o comportamento malicioso. Um HIDS oferece uma visibilidade profunda do que está acontecendo em seus sistemas críticos de segurança. Com ele, pode-se detectar e responder a atividades maliciosas ou anômalas descobertas em seu ambiente.

Por si só, a detecção de intrusão no host não fornece uma imagem completa da sua segurança. É necessário correlacionar os dados de log do HIDS com outros dados críticos de segurança e com a mais recente inteligência de ameaças do mundo real.

Nossa solução facilita a análise e a correlação de segurança, combinando IDS baseado em host com IDS baseado em rede e nuvem e também com o sistema de engano, trazendo informações ricas que permitem a resposta rápida a incidentes.

Detecção de alterações e ameaças aos seus sistemas críticos

- Detecta tentativas de acesso não autorizado
- Identificar atividades anômalas
- Identifica quando e quem acessou e alterou arquivos críticos com o Monitor de Integridade de Arquivos (MIA)
- Protege a integridade de seus ativos e dados

Utilizamos o Host IDS como parte de uma plataforma de segurança que inclui:

- Descoberta e inventário de ativos
- Avaliação de vulnerabilidade
- IDS de rede e nuvem
- Detector de movimentação lateral
- Monitoramento Comportamental
- Resposta a Incidentes
- Correlação de eventos SIEM e gerenciamento de logs

Detecta ameaças em sistemas críticos

O sistema de detecção de intrusão (HIDS) embutido em nossa plataforma monitora seus sistemas críticos e gera alertas sobre qualquer atividade não autorizada ou anômala que ocorra.

Um agente leve é executado em cada host monitorado, rastreando as alterações feitas nos arquivos críticos do sistema, nos arquivos de configuração, nos arquivos de log, nas configurações do Registro e até nos arquivos de conteúdo importantes. O agente do HIDS coleta essas informações e as envia à nossa plataforma para avaliação e correlação com outros dados ambientais e inteligência de ameaças.

Com o IDS baseado em host da nossa plataforma, você obtém visibilidade granular dos sistemas e serviços em execução, para poder detectar facilmente:

- Sistemas comprometidos
- Escala de privilégios
- Instalação de aplicativos indesejados
- Modificação de binários críticos de aplicativos, dados e arquivos de configuração (por exemplo, configurações do registro, /etc/passwd)
- Processos escondidos
- Serviços críticos que foram parados ou que falharam ao iniciar
- Acesso de usuários aos sistemas

Detectar atividades não autorizadas e anômalas

Quando atividades maliciosas ou anômalas ocorrem em um sistema - como ataques baseados em autenticação de força bruta, alterações rápidas de arquivos ou um usuário efetuando login em um ativo não autorizado - o HIDS detecta as atividades e as envia à plataforma Horizontech para análise. Quando um alarme é gerado na plataforma, ele captura tudo o que você precisa saber sobre o incidente, incluindo informações de ativos (SO, software e identidade), dados de vulnerabilidade, comunicação de rede, dados brutos de log e muito mais.

Identifica alterações e acesso a arquivos críticos com a Monitoração de Integridade de Arquivos

O monitoramento da integridade de arquivos permite rastrear o acesso e as alterações feitas em arquivos confidenciais em seus sistemas críticos e é especificado para conformidade com regulamentos e normas como o PCI DSS. Isso fornece uma trilha de auditoria necessária e permite validar que as alterações foram autorizadas, esperadas e não prejudicam a integridade e a segurança dos binários do sistema e do aplicativo, além dos arquivos de configuração e dados.

Exibir tentativas com falha de obter acesso ao sistema

Saiba quais dos seus atacantes estão tentando se infiltrar antes de entrar. O recurso HIDS da nossa plataforma gera eventos em tentativas de autenticação com falha no Windows, MySQL, acesso remoto, serviço SSH e muito mais.

5. Monitoração e proteção de sistemas críticos com IDS baseado em rede

A Horizontech oferece um software de detecção de intrusão integrado como parte de um console de gerenciamento de segurança unificado completo. Ele inclui detecção de movimentação lateral maliciosa, detecção de intrusão de host (HIDS) embutida, detecção de intrusão de rede (NIDS) e detecção de intrusão de nuvem para ambientes de nuvem pública, incluindo AWS e Microsoft Azure, permitindo detectar ameaças à medida que surgem na sua nuvem crítica e infraestrutura em redes locais

- Provê a detecção de intrusões em qualquer ambiente com IDS na nuvem, IDS de rede e IDS baseados em host (incluindo File Integrity Monitoring (FIM))
- Use a taxonomia da cadeia de eliminação para avaliar rapidamente a intenção e a estratégia da ameaça
- Tomar decisões informadas com dados contextuais sobre ataques, incluindo uma descrição da ameaça, seu método e estratégia e recomendações sobre resposta
- Notificações automáticas para ser informado sobre as principais ameaças à medida que elas ocorrem
- Eficiência com análises poderosas que descobrem detalhes de ameaças e vulnerabilidades - tudo em um console

Vários tipos de sistemas de detecção de intrusão para qualquer ambiente

Nossa solução permite a detecção e resposta antecipadas a intrusões, com sistemas de detecção de intrusão em nuvem, detecção de movimentação lateral, detecção de intrusão de rede (NIDS) e detecção de intrusão de host (HIDS). Essas ferramentas monitoram o tráfego e os hosts, juntamente com as atividades do usuário e do administrador, procurando comportamentos anômalos e padrões de ataque conhecidos. O recurso SIEM integrado na plataforma correlaciona automaticamente os dados do IDS com outras informações de segurança para fornecer visibilidade completa de sua segurança.

Detecção de intrusão na nuvem

Embora o software tradicional de IDS e prevenção de intrusões (IPS) não seja otimizado para ambientes em nuvem pública, a detecção de intrusões continua sendo uma parte essencial do seu monitoramento de segurança na nuvem. É por isso que nossa plataforma fornece recursos nativos do sistema de detecção de intrusão na nuvem nos ambientes de nuvem da AWS e do Azure. Os sensores de nuvem criados especificamente para os ambientes de nuvem da AWS e do Azure aproveitam as APIs de gerenciamento da AWS e do Azure, oferecendo visibilidade total de todas as operações que acontecem nas suas contas de nuvem

Sistema de detecção de intrusão de rede (NIDS)

O recurso de sistema de detecção de intrusão de rede (NIDS) da nossa plataforma detecta ameaças conhecidas e padrões de ataque direcionados a seus ativos vulneráveis. Complementar com as ferramentas de detecção de anomalias e o sistema de engano, ele analisa o tráfego da rede local, procurando as assinaturas dos ataques mais recentes, infecções por malware, técnicas de comprometimento do sistema, violações de políticas e outras exposições, além de gerar alarmes que alertam quando ameaças são identificadas.