Detecção e resposta a Ameaças

1. Ameaças internas
2. Ransomware
3. Detecção avançada de ameaças

HORIZON TECH

1. Ameaças internas

Detectar e minimizar ameaças internas

Na sequência de violações de alto nível em que funcionários confiáveis estavam envolvidos, as empresas estão cada vez mais preocupadas com as ameaças que esses funcionários representam, como:

- Funcionários descontentes que procuram danificar sistemas ou roubar dados
- Usuários envolvidos em espionagem corporativa ou patrocinada pelo estado
- Usuários desavisados, clicando em e-mails de phishing
- Usuários ilegalmente baixando torrents
- Prestadores de serviços/terceirizados atuando dentro da empresa

A detecção de ameaças internas pode ser desafiadora porque geralmente se estende por uma infinidade de sistemas e serviços. O aumento dos serviços em nuvem complica os esforços de detecção de ameaças internas porque muitas ferramentas de segurança tradicionais são incompatíveis com a arquitetura em nuvem, criando pontos cegos no seu plano de segurança. A nossa plataforma fornece visibilidade em seus ambientes locais, nuvem privada e nuvem pública, permitindo detectar ameaças internas em toda a infraestrutura crítica. Nossa proteção consegue abranger desde endpoints, IoT e ativos de rede à dispositivos específicos por setor, como por exemplo: indústria, saúde, financeiro e todos os outros.

Oferecemos recursos essenciais de detecção e gerenciamento de ameaças internas, incluindo:

- Detecção de intrusão de rede (NIDS)
- Detecção de intrusão na nuvem
- Logs de acesso à nuvem (Azure: Insights, AWS: CloudTrail, S3, ELB)
- Sistema de engano com armadilhas bem elaboradas

Detecção de escalonamento de privilégios

- Sistema de detecção de intrusão de host (HIDS)
- Monitoramento de Integridade de Arquivos (MIA)
- Detectar tentativas de acesso não autorizado a usuários
- Monitore serviços essenciais de SaaS, como Office 365 e G Suite

Correlação de Eventos

- Informações de segurança e gerenciamento de eventos (SIEM)
- Detectar comunicações com hosts maliciosos
- Painel centralizado que prioriza ameaças

Visibilidade de ameaças internas em sua infraestrutura crítica

As técnicas de detecção de ameaças internas dependem da visibilidade do que está acontecendo em sua infraestrutura crítica. No entanto, o aumento da nuvem pública representa um ponto cego de segurança para muitas organizações, porque os métodos tradicionais de segurança não foram criados com a nuvem em mente. A detecção eficaz de ameaças internas requer uma solução criada para acomodar todos os ambientes que você precisa proteger.

É por isso que a Horizontech utiliza uma plataforma unificada que ajuda a detectar e entender a atividade em qualquer combinação de ambientes locais, nuvem privada e nuvem pública, incluindo ameaças provenientes de usuários mal-intencionados ou descuidados em sua organização.

Nossa plataforma também o alerta sempre que um usuário insere um dispositivo em uma porta USB em um sistema que você está monitorando, mantendo-o informado sobre atividades potencialmente não autorizadas que podem levar ao roubo de dados.

Os ambientes em nuvem representam um desafio único para os esforços de detecção de ameaças internas, porque os métodos tradicionais de segurança de rede não são compatíveis com a infraestrutura em nuvem e devido à quantidade de danos que um único usuário pode causar. (Imagine suas chaves de acesso root entrando nas mãos erradas.)

Fornecemos visibilidade total dos ambientes em nuvem, usando sensores criados especificamente para uso com ganchos diretos nas APIs da nuvem para alavancar os extensos controles que os provedores de serviços incorporaram à arquitetura da nuvem.

Além de habilitar os recursos de detecção de intrusão na nuvem para a AWS e o Azure, nossos sensores oferecem suporte à detecção de ameaças internas com informações detalhadas sobre quem efetua login no plano de gerenciamento e quais ações são executadas. Por exemplo,- conseguimos saber se alguém criou ou destruiu máquinas virtuais, criou novos serviços ou alterou as configurações de suas máquinas virtuais (por exemplo, de oito para dezesseis gigabytes ou de um processo para vários).

Usamos esses dados para detectar ameaças internas, como o uso descuidado ou mal-intencionado de suas chaves de acesso raiz - antes que sua conta suba rapidamente.

Escalada de privilégios

A maioria das empresas rastreia as atividades de usuários privilegiados como uma prática essencial de segurança. Para contornar isso, os especialistas procurarão escalar privilégios para obter acesso a informações, subverter controles, danificar sistemas ou facilitar a exfiltração de dados confidenciais - enquanto estiverem voando sob o radar.

Nossa plataforma fornece os recursos necessários para identificar a escalada de privilégios e responder a ela rapidamente, limitando o escopo do impacto de um invasor malicioso em sua organização.

Podemos usar nossa plataforma para detectar e alertar sobre a escalada de privilégios que não possui uma solicitação de alteração correspondente, implantando um agente em seus sistemas, permitindo coletar informações críticas de seus servidores e estações de trabalho.

Os eventos do agente são encaminhados para nossa plataforma, permitindo monitorar grupos de administradores para novos usuários e tomar medidas caso os usuários estejam sendo adicionados aos grupos de maneira inadequada. Você também pode usar o MIA (Monitoramento da integridade de Arquivos) para rastrear alterações em seus ativos.

Além disso, nossa ferramenta correlaciona eventos suspeitos para detectar quando o acesso de um usuário a sistemas e aplicativos críticos pode ser malicioso. Isso permite que possamos detectar, responder e neutralizar a ameaça interna imposta por funcionários que tentam ignorar os controles de segurança escalando seus direitos ou que sequestrem credenciais de usuário para fins maliciosos.

Se sua organização usa o Office 365, você pode usar a nossa plataforma para monitorar a escalada de privilégios, auditando alterações em funções ou grupos no Exchange Online. Você também pode acompanhar atividades como acesso de usuário e gerenciamento de caixa de correio.

Como os usuários do Office 365 às vezes aumentam os privilégios delegando o acesso da caixa de entrada a outro usuário (por exemplo, a um assistente administrativo), é importante ter registros forenses caso um e-mail caia em mãos erradas.Podemos investigar facilmente quem acessou a caixa de entrada ou enviou mensagens de email.

Correlação de Eventos

Os seres humanos, diferentemente dos computadores, geralmente são de natureza imprevisível. Como tal, a detecção de ameaças internas geralmente requer a capacidade de correlacionar eventos aparentemente benignos para detectar ameaças internas que ocorrem em vários sistemas. Os insiders geralmente respondem pelos controles de segurança existentes e tentam manter suas atividades "baixas e lentas" para evitar acionar alarmes.

Podemos vincular eventos díspares nos ambientes local, nuvem privada e nuvem pública e correlacionar eventos relacionados a usuários mal-intencionados. Nosso forte mecanismo de correlação usa regras de correlação integradas para detectar relacionamentos entre diferentes tipos de eventos que ocorrem em um ou mais ativos monitorados para identificar atividades suspeitas. Desta forma, conseguimos rapidamente entregar um correlacionamento de eventos poderoso, que começa a funcionar logo após a implementação de nossa plataforma de segurança.

É aí que a inteligência de ameaças produzida pela equipe de pesquisa de segurança de nossos parceiros intervém para ajudar. Pense nisso como uma extensão para sua equipe de TI - eles estão constantemente realizando pesquisas avançadas sobre ameaças atuais e desenvolvendo atualizações para a inteligência de ameaças da nossa plataforma. Além das assinaturas de vulnerabilidade, você recebe atualizações contínuas das regras de correlação SIEM, assinaturas IDS, artigos da base de conhecimento e muito mais.

2. Ransomware

Pare ransomwares utilizando detecção avançada de ameaças

Atualmente, o ransomware é uma das principais preocupações de segurança das organizações. Atores maliciosos continuam a desenvolver novas técnicas e estratégias para induzir as vítimas a baixar e instalar ransomware em seus sistemas, e muitas equipes de TI estão mal equipadas para responder.

O ransomware é um tipo de malware que criptografa arquivos em um sistema, tornando-os inacessíveis até que você pague um resgate (geralmente na forma de uma criptomoeda como bitcoin ou cartões pré-pagos) em troca da chave de descriptografia. Dada a complexidade e a variedade de novas ameaças de ransomware que surgem diariamente, pode ser difícil para equipes de TI de qualquer tamanho descobrir como detectar e responder a ransomware enquanto gerencia o restante de suas necessidades de segurança cibernética.

Diferentemente das soluções alternativas, a plataforma da Horizontech simplifica e acelera a detecção de ameaças, para que as equipes de TI possam responder rapidamente a ameaças de ransomware e conter surtos com defesa direcionada, automatizada e orquestrada. Capacitamos as equipes de TI com visibilidade completa de toda a superfície de risco, unificando o monitoramento de segurança em ambientes em nuvem, na rede local e híbridos.

À medida que os padrões de atividade de ransomware evoluem, a Equipe de pesquisa de segurança de parceiros Horizontech e o Open Threat Exchange (OTX) mantêm a nossa plataforma atualizada com atualizações contínuas e automáticas de inteligência de ameaças. Essa inteligência de ameaças inclui os mais recentes indicadores de ameaças, vulnerabilidades e orientações para respostas. Está totalmente operacional e pronto para uso, para que organizações de todos os tamanhos possam detectar e conter rapidamente a atividade de ransomware sem precisar gastar tempo pesquisando ameaças emergentes ou escrevendo regras de correlação.

Além disso, o oferecemos recursos avançados de orquestração e automação de segurança, além de integração imediata com as principais ferramentas de segurança de terceiros, como Palo Alto Networks, Carbon Black e Cisco Umbrella. Assim, planejamos e executamos as atividades de resposta de ransomware diretamente de nossa plataforma, economizando tempo e esforço preciosos.

Oferecemos os recursos essenciais de segurança necessários para a detecção de ransomware:

- Detecção e resposta rápida a ameaças de ransomware
- Detecção de ameaças em tempo real com recursos essenciais de segurança integrados
- Resposta coordenada a incidentes com análise e relatórios integrados

Monitore todos os ambientes com detecção abrangente de intrusões

- Monitoramento de segurança unificado do Office 365 e outros aplicativos em nuvem para detectar ameaças de ransomware desde o início
- Detecção de intrusão na nuvem (AWS e Azure) - alerta sobre eventos críticos nos ambientes da AWS e do Azure, consistentes com os indicadores de ransomware.
- Detecção de intrusão de rede - alerta sobre a atividade conhecida de comunicação de ransomware com base em atualizações contínuas da equipe de pesquisa de segurança de perceiros.
- Detecção de intrusão de host - alerta sobre atividade de ataque de ransomware conhecida detectada nos servidores críticos em todos os seus ambientes
- Detecção de movimentação lateral - detecta movimentações laterais maliciosas utilizando poderoso sistema de engano

Reduza o tempo entre a detecção e a resposta com a orquestração e automação de segurança

- A inteligência integrada contra ameaças fornecida pela equipe de pesquisa de segurança de parceiros da Horizontech fornece aviso antecipado de indicadores de ataque de ransomware e atividade no mundo
- Resposta automatizada a incidentes acionada por meio de forte integração com ferramentas de segurança de terceiros como Cisco Umbrella, Palo Alto Networks e Carbon Black

3. Detecção avançada de ameaças

A segurança da sua organização depende da capacidade de detectar e responder rapidamente a ameaças emergentes nos ambientes na nuvem e na rede local. No entanto, os métodos e estratégias de ataque evoluem constantemente, tornando a detecção de ameaças um alvo sempre em movimento.

A maioria das organizações simplesmente não tem recursos ou tempo para pesquisar extensivamente o cenário global de ameaças para os últimos vetores de ataque, nem pode gastar tempo analisando todos os indicadores de que um ataque está acontecendo.

A plataforma Horizontech foi criada com essas organizações em mente. Realizamos detecção avançada de ameaças nos ambientes na nuvem e na rede local. Combinando vários recursos essenciais de segurança - descoberta de ativos, avaliação de vulnerabilidades, detecção de intrusões, monitoramento comportamental, detecção e resposta de terminais, correlação de eventos SIEM e gerenciamento de logs - em um console unificado. Isso nos fornece tudo o que precisamos para identificar, analisar e responder rapidamente a ameaças emergentes - em uma solução econômica e fácil de usar.

Além disso, a equipe de pesquisa de segurança de parceiros Horizontech trabalha em seu nome para pesquisar as mais recentes ameaças e vulnerabilidades globais e fornece atualizações de inteligência de ameaças continuamente. Dessa forma, você obtém a garantia de monitoramento de segurança sempre atualizada e com ótimo desempenho, mesmo sem uma equipe de segurança interna dedicada.

A Horizontech aproveita a inteligência de ameaças do Open Threat Exchange (OTX) - a maior comunidade mundial de inteligência de ameaças abertas, formada por especialistas em segurança, pesquisadores e profissionais de TI em todo o mundo, que fornecem informações globais sobre as últimas tendências de ataques, maus atores, indicadores de comprometimento, e indústrias afetadas.

Concentramos nas ameaças que importam

- Avaliamos rapidamente ameaças com priorização automática de alertas
- Tomamos decisões informadas com detalhes completos sobre cada alarme, incluindo uma descrição da ameaça, seu método e estratégia e recomendações sobre resposta

Obtenha visibilidade avançada de ameaças:

- Realizamos a detecção de ameaças em várias camadas para seus ambientes locais e na nuvem, usando os sistemas internos de detecção de intrusão baseados em host, engano, rede e nuvem da nossa plataforma aliado à recursos de detecção em end-points

- Pesquisamos e analisamos facilmente ameaças com uma visão consolidada de seus ativos, vulnerabilidades e atividades maliciosas em seu ambiente

- Eliminamos seus pontos cegos de segurança agregando e correlacionando eventos de todos os seus dispositivos, servidores, endpoints e aplicativos, além de monitorar as atividades de usuários e administradores

Mantemos a segurança com inteligência contínua sobre ameaças fornecida

- Recebemos dados de inteligência contínua sobre ameaças da equipe de pesquisa de segurança de parceiros Horizontech, entregue automaticamente na nossa plataforma.

- Aproveitamos os dados de ameaças da maior comunidade aberta de inteligência de ameaças do mundo - OTX

- Ficamos a frente das ameaças emergentes com regras de correlação que são atualizadas continuamente e automaticamente com a mais recente inteligência de ameaças