Compliance

1. LGPD
2. ISO 27001
3. HIPAA
4. PCI/DSS
5. SOC 2

HORIZON TECH

1. Acelere a conformidade com LGPD utilizando nossa plataforma

O LGPD (Lei Geral de Proteção de Dados) exige que as organizações que lidam com os dados pessoais, mantenham esses dados seguros e aplica grandes penalidades às organizações que não cumprem. Infelizmente, as soluções tradicionais de monitoramento de segurança podem não ajudar as organizações a atender aos requisitos de LGPD.

Nossa solução fornece uma plataforma unificada de monitoramento de segurança e gerenciamento de conformidade para acelerar o atendimento à conformidade com LGPD. Ao integrar vários recursos em uma única plataforma, oferecemos visibilidade de toda a sua estrutura de segurança o que simplifica o processo de conformidade.

O LGPD exige que as organizações mantenham um plano para detectar uma violação de dados, avaliem regularmente a eficácia das práticas de segurança e documentem evidências de conformidade. Em vez de direção técnica específica, o regulamento coloca o ônus nas organizações para manter as melhores práticas de segurança de dados.

A partir do primeiro dia, nossa solução já está pronta para conformidade com LGPD, ajudando a detectar violações de dados, monitorar a segurança dos dados e documentar que você atende aos requisitos. Nossa plataforma unificada centraliza recursos essenciais, como descoberta de ativos, varredura de vulnerabilidades, detecção de intrusões, monitoramento comportamental, SIEM, gerenciamento de logs e atualizações de inteligência de ameaças.

Possuímos modelos de relatórios pré-criados para ajudá-lo a provar a conformidade com os requisitos regulamentares e a aderir às estruturas de segurança de TI como ISO 27001 e NIST CSF. Embora o LGPD não define nem prescreve requisitos de relatórios específicos, seguir a ISO 27001 pode ser uma maneira eficaz de demonstrar que seus controles técnicos de segurança estão alinhados com as melhores práticas reconhecidas globalmente. O uso dos modelos de relatório de conformidade com a ISO 27001 servem como base para ajudar a adicionar estrutura aos seus esforços de atendimento ao LGPD.

Oferecemos os recursos essenciais de segurança necessários ao software de conformidade com LGPD:

- Diminuímos a superfície de ataque com descoberta de ativos e verificação de vulnerabilidades.
- Detectamos intrusões e possíveis violações de dados com a detecção de intrusão incorporada.
- Preparamos para a investigação forense com retenção e gerenciamento de logs.

Detectar, Investigar e Relatar Violações de Dados

- Detectamos violações rapidamente com o sistema de engano, detecção de intrusão de rede (NIDS), detecção de intrusão de host (HIDS) e detecção de intrusão de nuvem (CIDS)
- Identificamos atividade anômala com monitoramento comportamental
- Documente a estrutura de conformidade com modelos de relatório pré-criados, juntamente com relatórios totalmente personalizáveis

Reduza o tempo de resposta a incidentes para minimizar a exposição de dados

- Responda a incidentes rapidamente com ações de resposta automatizadas
- Limite a exposição potencial aos dados, reduzindo o tempo total de resposta

Mantenha seu plano de segurança atualizado com atualizações contínuas de inteligência contra ameaças

- Obtemos as informações mais recentes sobre ameaças, com o trabalho de pesquisa da equipe de segurança de nossos parceiros.
- Atualizamos constantemente nossas bases com as atualizações de inteligência contra ameaças continuamente entregues em nossa plataforma.

Simplifique o gerenciamento de segurança e conformidade à LGPD

Diferentemente das soluções pontuais que abordam um aspecto da conformidade com LGPD por vez, nossa plataforma oferece suporte a várias funções de conformidade, integrando cinco recursos essenciais de segurança em uma solução unificada:

- Descoberta de ativos
- Verificação de vulnerabilidades
- Monitoramento Comportamental
- Detecção de intruso
- SIEM e Gerenciamento de Log

A abordagem unificada que possuímos oferece visibilidade completa de sua estrutura de segurança em um único painel, simplificando a demonstração de conformidade com a segurança do LGPD.

Com os recursos de descoberta de ativos que utilizamos, podemos criar e manter um inventário completo dos ativos críticos que precisam ser monitorados para cumprir os requisitos de LGPD, fornecendo visibilidade de segurança de seus esforços de proteção de dados.

O Artigo XXX da LGPD exige que as organizações tomem medidas técnicas para garantir a proteção de dados, incluindo o monitoramento constante da eficácia do seu plano de segurança.

Nossa plataforma pode verificações regulares de vulnerabilidades de seus ativos críticos para ficar atualizado sobre patches essenciais e minimizar sua superfície de ataque. No caso da vulnerabilidade explorada pelo ransomware WannaCry, por exemplo, as verificações de vulnerabilidades da nossa solução identificariam sistemas sem patch, para aplicar patches ou isolá-los dos dados essenciais.

Os recursos internos de detecção de intrusões para sistemas baseados em rede, host, nuvem e engano permitem monitorar toda a sua infraestrutura crítica quanto a violações de dados. O monitoramento comportamental ajuda a identificar atividades anômalas que podem afetar seus dados armazenados.

Caso ocorra uma violação, nossos recursos de gerenciamento de logs do garantem que você possua os logs de eventos necessários para atender ao nível de investigação forense exigida pela regulamentação do LGPD

Detecte, investigue e relate com eficiência as violações de dados.

Para alcançar a conformidade com LGPD, é preciso demonstrar que possui um plano para monitorar a infraestrutura crítica que abriga dados pessoais. Fornecemos recursos essenciais de monitoramento de segurança para detectar, investigar e relatar violações de dados em seus ambientes.

Nossa solução oferece recursos nativos de detecção de intrusão na nuvem para o Azure e a AWS, permitindo detectar invasões em seus ambientes de nuvem pública. Fornecemos visibilidade da sua estrutura de segurança nos ambientes local, nuvem pública e nuvem privada, além de aplicativos em nuvem como o Microsoft Office 365 e o Google G Suíte.

A detecção de intrusões de rede (NIDS) identifica ameaças usando a detecção de anomalias com base em assinaturas, coletando dados de seus ambientes locais para detectar ataques maliciosos, intrusões de malware e outras ameaças potenciais aos seus dados.

A detecção de intrusão de host (HIDS) e o monitoramento de integridade de arquivos (MIA) fornecem visibilidade de segurança na camada do aplicativo, permitindo detectar atividades como comprometimento potencial do sistema, processos não autorizados e alterações em arquivos de configuração críticos.

A detecção de intrusões por engano identifica ameaças usando armadilhas espalhadas pela rede, que geram alarmes baseados em fatos que ocorrem, seja uma ação de reconhecimento, tentativa de exploração de vulnerabilidades, ação de malwares e outras ameaças em potencial às informações de dados pessoais.

Quando o detectamos uma ameaça em seus ambientes, é gerado alarme para chamar nossa atenção, permitindo uma resposta rápida e limitada o escopo de uma possível invasão. Nossa plataforma prioriza de forma inteligente os alarmes com base na gravidade da ameaça, para possamos saber quais incidentes responder primeiro.

É possível pesquisar e filtrar facilmente os dados de registro na nossa plataforma para investigar possíveis invasões e acessar todas as informações necessárias para uma investigação detalhada após uma violação de dados. As funções de pesquisa e filtragem granulares permitem girar em torno dos dados selecionados para uma análise mais profunda.

Reduza o tempo de resposta a incidentes para minimizar a exposição de dados

Para cumprir os regulamentos do LGPD, as organizações devem ter um plano para detectar e responder a uma potencial violação de dados para minimizar seu impacto nos cidadãos cujo os dados são de sua posse. No caso de um ataque ou invasão, um processo simplificado de resposta a incidentes pode ajudá-lo a responder rápida e efetivamente para limitar o escopo da exposição.

Utilizando nossa solução, podemos responder rapidamente a um evento, oferecendo uma visão unificada da estrutura de segurança de cada organização. Em vez de perder tempo reunindo informações de vários sistemas, executamos ações rápidas e confiantes com uma visão centralizada de todos os seus ativos, suas vulnerabilidades, quaisquer invasões ou tentativas de explorar essas vulnerabilidades, bem como informações sobre ameaças contextuais e orientações de correção.

Quando ocorre um incidente, os alarmes priorizados nos ajudam a concentrar primeiro nas ameaças mais importantes. Com dados detalhados de eventos e modelos de resposta a incidentes na ponta dos dedos, é fácil passar rapidamente da detecção para a resposta, em vez de perder tempo na pesquisa básica.

Com a nossa solução, podemos gerar alertas por email ou Amazon SNS para ajudá-lo a responder imediatamente às ameaças que afetam seus dados confidenciais.

Quando ocorre uma possível invasão, nossa solução permite automatizar ações de resposta a incidentes, bem como com as principais ferramentas de segurança de terceiros, como Cisco Umbrella, Palo Alto Networks e Carbon Black. Por exemplo, se detectarmos evidências de ransomware como o WannaCry, podemos desligar ou isolar o sistema e extrair dados adicionais para ajudar na investigação.

Com os recursos automatizados de resposta a incidentes que oferecemos, eliminamos tarefas manuais demoradas e passamos rapidamente da detecção para a resposta. Reduzir o tempo total de resposta limita o impacto potencial de invasões, ajudando a minimizar a exposição de dados e a atender aos requisitos de proteção.

2. ISO 27001
3. HIPAA
4. PCI/DSS
5. SOC 2