CONTINENT8 technologies

SIEM & SOC

secure8

SECURE | SIEM & SOC

Descubra as Ameaças Ocultas em Seus Dados

Maximize a segurança ao mesmo tempo que minimiza o seu esforço: uma plataforma de Gestão de Incidentes e Eventos de Segurança (SIEM) é o alicerce da sua estratégia de defesa cibernética. No entanto, devido à constante manutenção e ajuste requeridos durante a implantação de uma equipe altamente treinada 24 horas por dia, 7 dias por semana, para investigar alertas de segurança em tempo hábil, é extremamente difícil fazê-lo bem.

A Continent 8 entrega uma solução abrangente para os desafios de gerenciar e monitorar um SIEM de classe mundial. Com um SIEM avançado construído na ELK Stack, a Continent 8 fornece inteligência em tempo real em seus logs e dados de eventos, aproveitando a inteligência de ameaças, regras personalizadas, aprendizado de máquina e análise comportamental avançada para identificar ameaças de segurança enquanto escala para lidar com qualquer volume. A equipe de especialistas em segurança da Continent 8 personalizará o SIEM para atender aos seus requisitos de negócios e políticas de segurança exclusivos. Desde seguir suas cartilhas até personalizar painéis e integrá-los ao seu sistema de emissão de tickets, nossa equipe tem tudo o que você precisa.

Visibilidade Centralizada

Elimine pontos cegos visualizando ou correlacionando dados entre endpoints, redes, nuvem e muito mais. Crie rapidamente painéis e relatórios personalizados para atender às necessidades de usuários individuais, grandes grupos ou clientes. Incorpore gráficos em seus aplicativos de negócios para obter visibilidade em tempo real. Incorpore intuitivamente o mapeamento geográfico aos seus dados para entender melhor as tendências baseadas em localização.

Elimina a Fadiga de Alerta

Se você já gerenciou um SIEM antes, provavelmente já lidou com a fadiga de alerta. Um fluxo aparentemente ininterrupto de falsos positivos que não podem ser facilmente separados das ameaças reais. É exatamente isso que nossa equipe de especialistas em segurança 24 horas por dia, 7 dias por semana, faz em seu nome. O Continent 8 otimizará consistentemente a plataforma correlacionando logs de eventos, fluxos de dados e informações de ameaças para minimizar falsos positivos enquanto investiga todo o comportamento anômalo e alertas que permanecem. O resultado: uma redução drástica no tempo médio para detectar ameaças e apenas um punhado de alertas que exigem ação real.

Solução Adaptada

Seguimos sua direção, não o contrário. Personalizamos os nossos manuais, gestão de casos, regras de escalonamento, painéis, relatórios e muito mais para alinhar com os seus requisitos de conformidade e políticas de segurança.

Solução SIEM Totalmente Gerenciada: Monitoramento de SOC 24x7, ajuste de plataforma e investigação de alertas e comportamentos anômalos

Detecção de Ameaça Avançada: Machine Learning e Análise Comportamental Avançada aprende os comportamentos típicos dos seus dados para sinalizar anomalias

Feeds Integrados de Ameaças: Insights de ameaças automatizados e integrados para ficar à frente das ameaças em evolução e de alto impacto

GET IN TOUCH
sales@continent8.com

Asia: +65 3165 4649
Europe: +44 1624 694625

Latin America: +54 11 5168 5637
North America: +1 514 461 5120

CONTINENT8.COM/SECURE

FACEBOOK TWITTER LINKEDIN YOUTUBE

CONTINENT8 technologies

SIEM & SOC

secure8

SECURE | SIEM & SOC

Monitoramento, Detecção e Resposta à Ameaças Críticas

Painéis Definidos Pelo Cliente

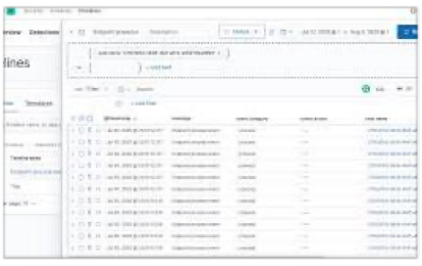
Dashboards nem sempre são um único formato que serve para todas as necessidades. É por isso que os personalizamos ou criamos novos para atender às suas necessidades. Afinal, os dashboards são parte integrante de qualquer solução SIEM para ajudá-lo a visualizar os dados de registro de incidentes e eventos de segurança em toda a sua infraestrutura ou para apenas acompanhar os requisitos regulamentares, como PCI ou SOX.

Linha do Tempo de Investigação

Uma linha do tempo descreve os eventos operacionais subjacentes a um incidente de segurança em ordens sequenciais. Dados de vários índices podem ser adicionados a uma linha do tempo para ajudar visualizar ameaças complexas. É uma ferramenta vital para os nossos especialistas em segurança seguirem o movimento de ameaças em sua infraestrutura e uma maneira fácil de validar o ameaça antes da remediação.

Mapas com Várias Camadas e Índices

Incorpore mapas em dashboards ou visualize-os de forma independente. Descreva como seus dados se encaixam em relação a recursos físicos, como fronteiras internacionais ou recursos específicos de negócios, como regiões de vendas. Você pode plotar documentos individuais ou usar agregações para plotar qualquer conjunto de dados, independentemente do tamanho.



Validação de Terceiros

Em conformidade com PCI-DSS e HIPPA. Validação pré e pós-execução da AV Comparatives, NSS Labs, VirusTotal, Forrester, SE Labs e MITRE. Participação no programa da MITRE para testes públicos, submetendo-se a pesquisadores da MITRE para testes independentes contra ataques direcionados.

TECHNICAL SUPPORT
support@continent8.com

Asia: +65 3165 4796
Europe: +44 1624 694611

Latin America: +54 11 5168 5643
North America: +1 514 461 5111

CONTINENT8.COM/SECURE

FACEBOOK TWITTER LINKEDIN YOUTUBE