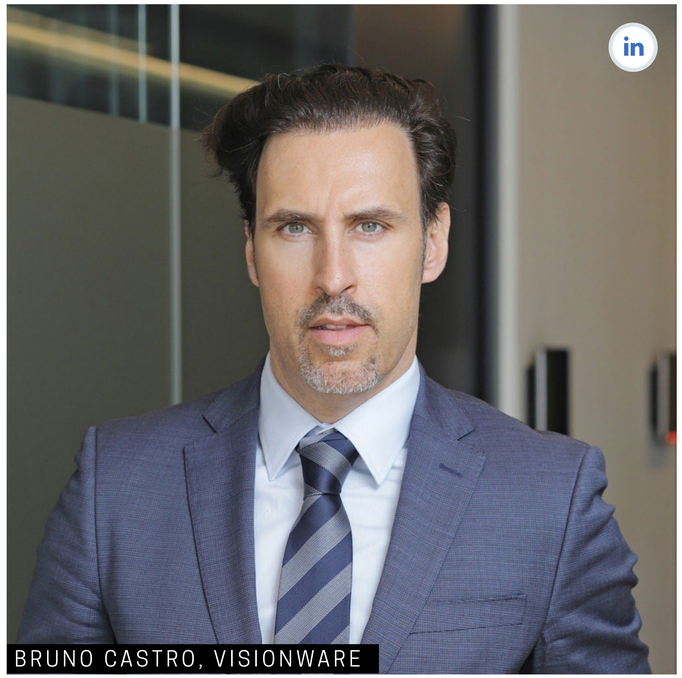
visionware

por Bruno Castro,
Fundador & CEO da VisionWare.
Especialista em Cibersegurança e Análise Forense

SIEM: UMA NECESSIDADE URGENTE PARA AS ORGANIZAÇÕES

O **SIEM - SECURITY INFORMATION AND EVENT MANAGEMENT** OU GESTÃO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA, CONSISTE NUMA DAS MAIS VALIOSAS FERRAMENTAS QUE AUXILIAM AS ORGANIZAÇÕES NA DETEÇÃO DAS MAIS RECENTES AMEAÇAS DE SEGURANÇA NAS SUAS REDES.


BRUNO CASTRO, VISIONWARE

O SIEM tem como objetivo principal, a análise das entradas do *log* para identificação de sinais de atividade maliciosa, **contribuindo para a cibersegurança como um todo**, já que possibilita que a empresa determine a natureza do ataque e o seu impacto nos negócios.

A gestão da Segurança de Informação nas organizações envolve a instalação de antivírus, firewall e outras formas de proteção, como o SIEM, que ajuda a filtrar grandes volumes de dados, priorizando os alertas de segurança. Através desta funcionalidade, as organizações podem detetar incidentes que não seriam percebidos de outra forma e assim minimizar os riscos negativos do seu impacto incluindo danos reputacionais.

À medida que as empresas avançam no caminho da sua transformação digital e tornam os seus ambientes de TI cada vez mais complexos, o SIEM (Security Information and Event Management), passou a ganhar um espaço de relevo quando passou a ser disponibilizado como serviço. Se antes a solução era mais restrita às grandes empresas e multinacionais pelo seu alto custo de aquisição e manutenção, atualmente ele pode ser adquirido por qualquer tipo de empresa, independentemente da sua dimensão, *as a service*, sendo gerido por

uma equipa especializada e terceirizada, com um investimento acessível mesmo para as pequenas e médias empresas.

Nesta evolução positiva do SIEM destaco aqui os 7 grandes motivos/razões para considerar a adoção do SIEM como um serviço, nomeadamente:

1) Custo vs. Benefício: é de reforçar que este serviço é extremamente vantajoso quando comparado ao investimento de se adquirir a solução completa para gestão interna;

2) Não carece de uma infraestrutura local: Isto é, a solução, além do custo de aquisição, não exige qualquer investimento adicional em infraestrutura para alocar a tecnologia e contratação de mão de obra especializada e específica.

3) Consultoria e customização da solução: O serviço vem acompanhado de uma consultoria e equipa especializada, a qual irá compreender e absorver os desafios de negócio de cada cliente e customizar a solução para atender aos seus requisitos específicos.

4) Fácil implementação: Ao contratar o serviço, a solução estará a funcionar em poucos dias, precisamente pela sua gestão altamente qualificada e especializada por equipas muito bem "oleadas";

5) Permite uma maior dedicação ao foco do negócio: A modalidade permite ao gestor/cliente ficar completamente concentrado e focado no seu negócio, deixando a gestão nas mãos dos verdadeiros experts na matéria;

6) É aplicável, de forma transversal, a todos os setores de atividade: O SIEM como serviço pode ser adquirido por qualquer tipo de organização que trabalhe com dados pessoais de terceiros.

7) É compliance com as principais regulamentações e diretivas setoriais: O serviço realiza ações exigidas por órgãos reguladores, como por exemplo, a correlação de logs e o armazenamento de dados, de acordo com determinadas diretrizes e orientações estratégicas.

Ao ser capaz de monitorizar todas as ações de cariz digital dentro de uma organização, e assente em processamento rápido – "near-real-time" através da sua estrutura de inteligência – podemos identificar comportamentos suspeitos ou até maliciosos numa fase inicial do ciberataque, permitindo responder atempadamente antes do próprio ciberataque ganhar dimensão ou maior impacto (negativo) na organização. Essencialmente, podemos associar o SIEM a um conjunto de sentinelas que está 24 horas/7 dias por semana/365 dias por ano, a guardar interruptamente o castelo e à procura de movimentos suspeitos que possam ser ou vir a tornar-se uma ameaça. Jamais seria possível realizar estas ações, por exemplo, por humanos.

A curto prazo, acredito que será obrigatório ter um SIEM em produção numa qualquer organização, independentemente da sua eficácia ou capacidade, tal como já é inquestionável possuir um antivírus ou uma firewall. Os SIEM terão um papel crítico na implementação de medidas de segurança preventiva e reativa no futuro do mercado. O grande desafio será saber escolher qual o SIEM que melhor responde às necessidades de cada organização. ◀