Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 8ª REGIÃO

CARGO 15: ANALISTA JUDICIÁRIO/ÁREA: APOIO ESPECIALIZADO/ESPECIALIDADE: TECNOLOGIA DA INFORMAÇÃO

Prova Discursiva

Aplicação: 06/11/2022

PADRÃO DE RESPOSTA DEFINITIVO

1) Solução *Zero Trust Network Access* (ZTNA) e seu objetivo

O acesso de confiança zero à rede (ZTNA) é uma solução de segurança de TI que fornece acesso remoto seguro a aplicativos, dados e serviços de uma organização com base em políticas de controle de acesso claramente definidas.

O ZTNA difere das redes privadas virtuais (VPNs) porque concede acesso apenas a serviços ou aplicativos específicos, enquanto as VPNs concedem acesso a uma rede inteira.

Quando o ZTNA está em uso, o acesso a aplicativos ou a recursos específicos é concedido somente depois que o usuário é autenticado no serviço ZTNA.

Após a autenticação, o ZTNA concede ao usuário acesso ao aplicativo específico por um túnel criptografado seguro, que oferece uma camada extra de segurança ao proteger aplicativos e serviços em endereços IP que, de outra forma, ficariam visíveis.

A ZTNA fornece acesso controlado a recursos com reconhecimento de identidade e contexto, reduzindo a área de superfície para ataque. ZTNA começa com uma postura de negação padrão de confiança zero. Ele concede acesso com base na identidade dos humanos e seus dispositivos — além de outros atributos e contexto, como hora/data, geolocalização, postura do dispositivo etc. — e oferece, de forma adaptativa, a confiança apropriada exigida no momento.

2) Solução *Privileged Access Management* (PAM) e seu objetivo

As ferramentas Gerenciamento de Acesso Privilegiado (PAM) ajudam as organizações a fornecer acesso privilegiado seguro a ativos críticos e atender aos requisitos de conformidade, gerenciando e monitorando contas e acessos privilegiados.

As ferramentas PAM oferecem recursos que permitem aos líderes de segurança e risco descobrir contas privilegiadas em sistemas, dispositivos e aplicativos para gerenciamento posterior.

Em um ambiente corporativo, "acesso privilegiado" é um termo usado para designar acesso ou habilidades especiais acima e além de um usuário padrão. O acesso privilegiado permite que as organizações protejam sua infraestrutura e seus aplicativos, executem negócios com eficiência e mantenham a confidencialidade de dados confidenciais e infraestrutura crítica.

3) Solução *Security Information and Event Management* (SIEM) e seu objetivo

Simplificando, o SIEM é uma solução de segurança que ajuda as organizações a reconhecer possíveis ameaças e vulnerabilidades de segurança antes que elas tenham a chance de interromper as operações de negócios. Ele apresenta anomalias de comportamento do usuário e usa inteligência artificial para automatizar muitos dos processos manuais associados à detecção de ameaças e resposta a incidentes e tornou-se um item básico nos centros de operações de segurança (SOCs) modernos para casos de uso de gerenciamento de segurança e conformidade.

A tecnologia de gerenciamento de informações e eventos de segurança (SIEM) oferece suporte à detecção de ameaças, conformidade e gerenciamento de incidentes de segurança por meio da coleta e análise (em tempo quase real e histórico) de eventos de segurança, bem como uma ampla variedade de outras fontes de dados contextuais e de eventos.

Os recursos principais são um amplo escopo de coleta e gerenciamento de eventos de *log*, a capacidade de analisar eventos de *log* e outros dados em fontes diferentes e recursos operacionais (como gerenciamento de incidentes, painéis e relatórios).

QUESITOS / CONCEITOS

Quesito 2.1 Solução *Zero Trust Network Access* (ZTNA) e seu objetivo
0 – Não discorreu sobre a solução.
1 – Discorreu somente sobre a solução ou somente sobre seu objetivo.
2 – Discorreu sobre a solução, mas não explicou seu objetivo.
3 – Discorreu sobre a solução e explicou seu objetivo.

Quesito 2.2 Solução *Privileged Access Management* (PAM) e seu objetivo
0 – Não discorreu sobre a solução.
1 – Discorreu somente sobre a solução ou somente sobre seu objetivo.

2 – Discorreu sobre a solução, mas não explicou seu objetivo.
3 – Discorreu sobre a solução e explicou seu objetivo.

Quesito 2.3 Solução *Security Information and Event Management* (SIEM) e seu objetivo
0 – Não discorreu sobre a solução.
1 – Discorreu somente sobre a solução ou somente sobre seu objetivo.
2 – Discorreu sobre a solução, mas não explicou seu objetivo.
3 – Discorreu sobre a solução e explicou seu objetivo.