QUESTÃO 29 – Prova Tipo 01 – SIEM × IDS/IPS E ANÁLISE FORENSE DIGITAL

Concurso: PC-ES - IBADE
Pedido: ANULAÇÃO DA QUESTÃO

I – DO OBJETO DO RECURSO

A presente questão exige do candidato **conhecimento técnico especializado em segurança da informação corporativa**, ao tratar de forma direta e aprofundada de:

- **SIEM (Security Information and Event Management)**;
- **IDS/IPS (Intrusion Detection/Prevention Systems)**;
- **correlação de eventos de segurança**;
- **inteligência de ameaças**;
- **apoio à análise forense digital**.

Trata-se de cobrança típica de **ambientes corporativos complexos de segurança**, própria de **analistas de segurança, especialistas em SOC e profissionais de resposta a incidentes**, absolutamente incompatível com o conteúdo programático previsto no edital.

II – DO CONTEÚDO PREVISTO NO EDITAL

O edital do certame prevê, no item **Segurança da Informação**, apenas:

6.1 Conceitos de integridade, confidencialidade, autenticidade e disponibilidade da informação.
6.2 Tipos de ameaças: malware, ransomware, spyware, trojans e ataques cibernéticos.
6.3 Ferramentas de proteção: antivírus, firewall, autenticação de dois fatores, criptografia e backups.

Em nenhum momento o edital:

- menciona **SIEM**;
- menciona **IDS ou IPS**;
- autoriza estudo de **correlação de eventos**;
- prevê **inteligência de ameaças (threat intelligence)**;
- trata de **análise forense digital associada a ferramentas corporativas**.

O conteúdo editalício restringe-se a **noções gerais de segurança**, voltadas à compreensão básica de ameaças e ferramentas comuns, **não à arquitetura de segurança corporativa avançada**.

III – DA EXTRAPOLAÇÃO MANIFESTA DO NÍVEL DO CONTEÚDO

A questão exige que o candidato:

- diferencie conceitualmente **SIEM de IDS/IPS**;
- compreenda o papel do **SIEM como agregador e correlacionador de eventos**;
- conheça o uso de **logs de múltiplas fontes**;
- entenda a aplicação do SIEM em **análise forense digital**.

Esse nível de exigência **não é introdutório**.

Trata-se de conteúdo típico de:

- cursos de **Segurança da Informação em nível avançado**;
- formações em **SOC, Blue Team e Resposta a Incidentes**;
- concursos para **Analista de Segurança da Informação ou Especialista em TI**.

Não se confunde, em hipótese alguma, com o estudo básico de antivírus, firewall e conceitos gerais de segurança.

IV – DA INADEQUAÇÃO DA ALTERNATIVA CONSIDERADA CORRETA (LETRA C)

A alternativa **C**, apontada como correta pela banca, afirma:

"O SIEM agrega e correlaciona eventos de segurança de múltiplas fontes, fornecendo inteligência de ameaças e suporte à análise forense, enquanto o IDS/IPS atua em pontos específicos da rede."

Ainda que a assertiva esteja **tecnicamente correta em ambiente especializado**, isso **não legitima a questão**, pois:

- **SIEM não consta no edital**;
- **IDS/IPS não constam no edital**;
- **correlação de eventos não consta no edital**;
- **inteligência de ameaças não consta no edital**;
- **análise forense digital associada a SIEM não consta no edital**.

Em concursos públicos, **a correção técnica não supre a ausência de previsão editalícia**, sob pena de violação direta às regras do certame.

V – DA IMPOSSIBILIDADE OBJETIVA DE PREPARO DO CANDIDATO

O candidato que seguiu fielmente o edital:

- estudou conceitos básicos de segurança da informação;
- revisou malware, firewall, antivírus e backups;
- compreendeu ameaças comuns e práticas gerais de proteção.

Não havia qualquer indicação de que deveria estudar:

- ferramentas corporativas de correlação de eventos;
- arquiteturas de monitoramento de segurança;
- integração de múltiplas fontes de logs;
- suporte forense por meio de SIEM.

Isso caracteriza **impossibilidade objetiva de preparo**, pois o candidato **não pode ser penalizado por não estudar conteúdo que o edital não autorizou**.

VI – DA VIOLAÇÃO AO PRINCÍPIO DA VINCULAÇÃO AO EDITAL

O edital constitui a **lei interna do concurso**, vinculando integralmente a banca examinadora.

Ao cobrar **SIEM e IDS/IPS em nível conceitual avançado**, a banca:

- extrapolou o conteúdo programático;
- violou o princípio da vinculação ao edital;
- comprometeu a isonomia entre os candidatos;
- transformou a questão em avaliação de **especialização técnica**, e não de noções básicas.

A questão deixa de avaliar **conhecimentos gerais de informática** e passa a exigir **formação técnica avançada em segurança da informação**, o que é juridicamente inadmissível.

VII – DO PEDIDO

Diante da:

- ausência total de previsão editalícia sobre SIEM e IDS/IPS;
- cobrança indevida de correlação de eventos e inteligência de ameaças;

- extrapolação manifesta do conteúdo programático;
- exigência de conhecimento típico de cargos especialistas;
- impossibilidade objetiva de preparo do candidato;
- violação direta ao princípio da vinculação ao edital;

REQUER-SE A ANULAÇÃO DA QUESTÃO 29, por afronta direta ao edital do certame.