- Nesta prova, faça o que se pede, usando, caso deseje, o espaço para rascunho indicado no presente caderno. Em seguida, transcreva o texto para o **CADERNO DE TEXTO DEFINITIVO DA PROVA DISCURSIVA**, no local apropriado, pois **não será avaliado fragmento de texto escrito em local indevido**.
- Qualquer fragmento de texto além da extensão máxima de linhas disponibilizadas será desconsiderado.
- No **Caderno de Texto Definitivo**, identifique-se apenas no cabeçalho da primeira página, pois não será avaliado texto que tenha qualquer assinatura ou marca identificadora fora do local apropriado.
- Na avaliação do relatório técnico, ao domínio do conteúdo serão atribuídos até **40,00 pontos**, dos quais até **2,00 pontos** serão atribuídos ao quesito apresentação (legibilidade, respeito às margens e indicação de parágrafos) e estrutura textual (organização das ideias em texto estruturado).

-- PROVA DISCURSIVA --

Estudantes, professores e funcionários da Universidade ACME conectam-se à rede de computadores da instituição várias vezes ao dia por meio de vários terminais, como *laptops*, telefones e outros dispositivos pessoais, o que pode abrir portas a *cibercriminosos* e colocar dados confidenciais em risco, deixando a universidade vulnerável a um ataque devastador.

Com mais de 16.000 alunos de ensino superior, 1.500 professores e 2.000 funcionários, e o aumento de vulnerabilidades em potencial que podem colocar a rede em risco, o setor de segurança da informação da instituição considerou crucial ter um forte programa de gerenciamento de vulnerabilidades e adotou como solução uma plataforma de gerenciamento de vulnerabilidades diferente de outras – a Wagner Vulnerability Manager (VM de linha de frente).

Para ajudar a gerenciar as ameaças contínuas e atender aos requisitos de proteção de dados e exigências de conformidade, o setor de segurança da referida instituição de ensino recorreu à defesa digital para uma solução de gerenciamento de vulnerabilidades. Com a utilização da VM Wagner da VAD, a ACME está simplificando os processos e melhorando a segurança dos dados, por meio da identificação efetiva de vulnerabilidades internas e externas que podem ser exploradas por criminosos cibernéticos e *hackers*.

Anteriormente, a ACME usava outra ferramenta popular de varredura de rede para auxiliar o gerenciamento de vulnerabilidades, mas tinha de lidar com relatórios que forneciam grande quantidade de dados estáticos e estranhos, então, em vez de continuar buscando, junto ao fornecedor anterior, informações e assistência, decidiu procurar uma nova solução, o que a levou a optar pela VAD.

A equipe de segurança da informação da ACME descobriu que a VM Wagner da VAD é capaz de fornecer uma solução personalizável e fácil de usar. A Wagner VM é avançada, intuitiva e econômica. Apoiada por tecnologia de ponta, a Wagner VM identifica rapidamente os pontos fracos em uma rede e prioriza os ativos para garantir que os esforços de correção reduzam o risco de segurança o mais rápido possível. É também um console instintivo suportado por uma arquitetura baseada em nuvem, que elimina gastos de capital contínuos e libera o cliente de preocupações com a obsolescência da tecnologia e o fardo de realizar atualizações de *software* e *hardware*.

A ACME descobriu que os relatórios gerados e entregues via Wagner VM são acionáveis e permitem que a equipe avance rapidamente nos problemas e simplifique os esforços de correção. A ACME experimenta menos falsos positivos, o que economiza tempo, e a Wagner VM não requer semanas de treinamento de pessoal. Isso significa que mais membros da equipe de segurança da universidade podem usar a ferramenta e ter acesso aos dados baseados em função. "Os dados da Wagner VM são distintos e não requerem uma longa descrição, e as questões críticas são muito claras – as grandes coisas não se perdem na confusão", diz o analista de segurança sênior da Universidade ACME.

A equipe de tecnologia da informação da ACME também aprecia que, depois de corrigir um problema, seus membros podem redigitalizá-lo imediatamente e descobrir, quase em tempo real, se a correção efetivamente solucionou o problema. "Podemos usar a Wagner VM para identificar facilmente os problemas em nossa rede, o que é mais importante para nós do que em outras organizações porque não temos acesso direto ao *endpoint*", diz o diretor de tecnologia da universidade.

A tecnologia de ponta VAD é inovadora no gerenciamento de vulnerabilidades. A poderosa tecnologia de varredura patenteada, complementada por um algoritmo avançado de correlação de *host* de rede com patente pendente, produz resultados altamente precisos. Ao contrário das ferramentas baseadas em premissas, usadas anteriormente pela universidade, que armazenam dados em silos, a tecnologia da VAD ajuda a identificar tendências e discrepâncias por meio da análise de dados agregados. Isso permite que a VAD gere rapidamente resultados mais precisos e completos e alerte a ACME rapidamente sobre quaisquer vulnerabilidades potenciais que possam ameaçar sua segurança. Em qualquer rede, os ativos nem sempre permanecem no lugar. A correlação de *host* de rede da VAD rastreia e reconcilia ativos e seus dados, mesmo quando seus endereços IP mudam, fornecendo um incomparável gerenciamento de vulnerabilidades. Outras ferramentas fornecem apenas um instantâneo estático de risco, o que resulta em uma visão imprecisa de toda a postura de segurança. Com tantos *endpoints* diferentes e em constante mudança em sua rede, a ACME pode usar a solução de gerenciamento de vulnerabilidades da VAD para resolver quaisquer problemas.

A ACME também descobriu que, com a VAD, é possível ter acesso a especialistas que podem ser uma extensão de sua organização, com uma abordagem de luva branca para suporte. A equipe de analistas de segurança pessoal sob demanda da VAD está disponível para ajudar a definir os requisitos, criar estratégias e executar efetivamente um programa de gerenciamento de vulnerabilidades adaptado à organização.

Embora a configuração seja simples e a plataforma seja intuitiva, quando surgem dúvidas, o suporte ao cliente facilita o gerenciamento dos problemas cotidianos, incluindo-se a priorização de remediação e atribuições.

Considerando que a gestão da segurança da informação incentiva a adoção de políticas, procedimentos, guias e demais elementos relevantes, cujo escopo deve compreender o gerenciamento de riscos baseado em análises de custo/benefício para a organização, redija um relatório técnico, com base na análise da situação hipotética em que figura a Universidade ACME, de acordo com as normas NBR 27001:2013 e NBR2700, a respeito dos seguintes aspectos:

1 políticas e organização de segurança da informação; [**valor: 10,00 pontos**]
2 segurança em recursos humanos; [**valor: 18,00 pontos**]
3 controle de acesso. [**valor: 10,00 pontos**]

RASCUNHO – 1/3

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	

RASCUNHO – 2/3

31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	
51	
52	
53	
54	
55	
56	
57	
58	
59	
60	

RASCUNHO – 3/3

61	
62	
63	
64	
65	
66	
67	
68	
69	
70	
71	
72	
73	
74	
75	
76	
77	
78	
79	
80	
81	
82	
83	
84	
85	
86	
87	
88	
89	
90	