Prova III – Banco de Dados não Relacional – DSM – Prof.ª Lucineide – 01/12/2025

Nome: _____ Valor: 2,0 pts. cada questão

Instruções

- Responda às questões de forma **discursiva**, clara e objetiva.
- Analise os trechos de código apresentados e **complemente, explique ou corrija** conforme solicitado.
- Justifique suas respostas quando solicitado.

TEMA – *Sistema de Segurança Digital Inteligente*

Uma empresa de tecnologia desenvolveu uma plataforma de **monitoramento de ameaças digitais**, que recebe dados de:

- logs de tentativas de invasão,
- alertas de varredura de portas,
- detecção de malware,
- sensores de tráfego suspeito,
- relatórios de vulnerabilidades,
- API de inteligência de ameaças,
- e automações de resposta.

O backend usa **MongoDB, Node.js, agregações e segurança no banco**.

Você deve analisar, interpretar e complementar trechos de código relacionados ao sistema.

Responda **discursivamente**.

---

1 – Cada servidor monitorado armazena uma lista de "alertas críticos", contendo:

- data/hora,
- tipo de ameaça,
- gravidade,
- IP de origem,
- ação recomendada.

Esses alertas são consultados constantemente junto ao próprio servidor durante incidentes.

Documento parcial:

```
{
  "servidor": "web01",
```

Prova III – Banco de Dados não Relacional – DSM – Prof.ª Lucineide – 01/12/2025

```
  "ip": "192.168.10.15",
  "alertas": [ ... ]
}
```

a) Complete o campo alertas com um exemplo realista.

b) Explique por que *embedding* é adequado neste cenário.

c) Cite uma situação em que *referencing* seria mais apropriado em segurança digital.

---

2 – A equipe quer encontrar alertas que indiquem tentativa de invasão por força bruta:

- tipo = “tentativa_login”,
- gravidade ≥ 4,
- IP contendo o prefixo “201.” (busca por regex).

Complete:

```
db.alertas.find({
  $and: [
    { tipo: "tentativa_login" },
    { gravidade: { _______: 4 } },
    { ip_origem: { _______: /^201\./ } }
  ]
});
```

a) Preencha as lacunas.

b) Explique como essa consulta auxilia na detecção de ataques reais.

---

3 – Abaixo, um pipeline incompleto:

```
db.alertas.aggregate([
  { $match: { tipo: "scan_portas" } },
```

```
  { $group: { _id: "$ip_origem", totalTentativas: { _______: 1 } } },
  { $sort: { totalTentativas: -1 } }
]);
```

a) Preencha a função agregadora.

b) Explique o que este relatório revela para o time de segurança.

c) Cite uma ação automática que o sistema poderia tomar com base nele.

---

4 – Analise a rota:

```
router.post("/alertas", async (req, res) => {
  try {
    const { tipo, gravidade, ip_origem } = req.body;

    if (!tipo || gravidade === undefined || !ip_origem) {
      return res.status(400).json({ erro: "Dados obrigatórios ausentes" });
    }

    const alerta = await Alerta.create(req.body);
    res.status(201).json(alerta);

  } catch (erro) {
    res.status(500).json({ erro: "Falha ao registrar alerta" });
  }
});
```

a) Explique a funcionalidade dessa rota.

b) Cite dois riscos de segurança caso a API esteja exposta sem autenticação.

c) Escreva o formato geral de uma string de conexão segura do MongoDB com autenticação.

Prova III – Banco de Dados não Relacional – DSM – Prof.ª Lucineide – 01/12/2025

5 – Analise os códigos a seguir:

Comandos:

```
mongodump --db cyberDefense --out ./backup
mongorestore --db cyberDefense ./backup/cyberDefense
```

Código de monitoramento:

```
mongoose.connection.on("_____", () => console.log("Banco conectado"));
mongoose.connection.on("_____", () => console.log("Banco desconectado"));
mongoose.connection.on("_____", err => console.error("Erro:", err));
```

a) Explique a finalidade de cada comando.

b) Por que backups são críticos em sistemas de segurança digital?

c) Complete os eventos de monitoramento.

PROVA PRÁTICA P3 – VERSÃO (Gabarito Completo)

Gabarito – Questão 1

a) Exemplo de alerta:

```
"alertas": [
 {
  "data": "2025-11-20T14:32:00Z",
  "tipo": "tentativa_login",
  "gravidade": 5,
  "ip_origem": "201.55.23.9",
  "acao": "bloquear_ip"
 }
]
```

Prova III – Banco de Dados não Relacional – DSM – Prof.ª Lucineide – 01/12/2025

b) Embedding é adequado porque:

- *alertas são consultados junto ao servidor,*
- *acesso rápido durante incidentes,*
- *reduz necessidade de $lookup,*
- *melhor performance (Aulas 2 e 5).*

c) Referencing seria indicado quando:

- *há milhões de eventos,*
- *eventos são compartilhados entre sistemas,*
- *relatórios analíticos são independentes da coleção principal.*

Gabarito – Questão 2

a)

- *$gte*
- *$regex*

b) *A consulta localiza acessos suspeitos com gravidade elevada e origem específica, útil para detectar ataques coordenados.*

Gabarito – Questão 3

a) *$sum*

b) *O relatório mostra quais IPs mais realizaram varreduras de portas — típico comportamento de invasores.*

c) *Ações possíveis:*

- *bloquear IP automaticamente,*
- *enviar alerta para analistas,*
- *ativar modo de resposta.*

Gabarito – Questão 4

a) *A rota registra um novo alerta após validação.*

b) *Riscos:*

- *envio massivo de alertas falsos,*
- *coleta indevida de dados sensíveis,*
- *ataques de negação de serviço.*

c) *Formato:*

mongodb://usuario:senha@localhost:27017/cyberDefense?authSource=admin

Gabarito – Questão 5

a)

- *mongodump: cria backup.*
- *mongorestore: restaura backup.*

b) *Em segurança digital, perda de logs impede identificar ataques.*

Dados são essenciais para auditorias e investigações.

c) *Eventos corretos:*

- *"connected"*
- *"disconnected"*
- *"error"*