

[Voltar](#) [Anterior](#) [Próximo](#)

Fundamentos de SOC - Security Operations Center (online)

40 aula(s) no total

25 aula(s) completa(s) **0 aula(s) iniciada(s)**

- > Bem-vindo(a)!
- > Aula 1 - Introdução ao SOC
- > Aula 2 - SIEM
- > Aula 3 - Threat Intelligence
- > Aula 4 - Framework
- > Aula 5 - KPI
- > Aula 6 - Criando um SOC
 - > Catálogo de serviço
 - > Necessidade e desejo
 - > Desafios e benefícios
 - > Melhores práticas
 - > E se for um prestador?
- > Aula 7 - Workflow
- > Aula 8 - Metodologia SIM
- > Pesquisa de satisfação

Teste seus conhecimentos

Parabéns, você acertou 100% das questões. Continue assim, você está no caminho certo!

Você ainda pode responder 1 vezes, deseja tentar novamente? [Clique aqui](#)

1. Qual dos serviços abaixo não fazem parte de um SOC?

- Cleanup
- Monitoração
- Tuning
- Assessment

Nenhuma das alternativas anteriores está correta.**Resposta correta:** Nenhuma das alternativas está correta.**Pontuação: 1 / 1**

2. Com qual das ferramentas abaixo não é possível realizar cleanup?

- Firewall
- IPS
- HUB
- SIEM
- Nenhuma das alternativas anteriores está correta.

Resposta correta: HUB**Comentário do professor:**

HUB é um equipamento de rede que transmite ou repete informações na rede.

Pontuação: 1 / 1

3. O que é um SNOC?

- Service Network Operations Center
- System Network Operations Center
- Security Networking Operations Center
- Security Network Operations Center
- Security Network Operations Command

Resposta correta: Security Network Operations Center**Pontuação: 1 / 1**

4. Qual a escala de trabalho ideal para a atuação do SOC?

- 24 X 7 horas
- 8 X 5 horas
- 8 X 7 horas

Todas as alternativas anteriores estão corretas.**Comentário do professor:**

A escala de horas ideal para o trabalho do SOC pode variar conforme a necessidade do cliente/negócio. Isso torna qualquer horário ideal.

Pontuação: 1 / 1

5. Qual das afirmações abaixo está correta?

- Quanto mais alerta melhor.
- Quanto menos alerta melhor.
- O número ideal de alertas é em torno de 100 por dia.
- O número ideal de alertas é menor de 50 por dia.

Nenhuma das alternativas anteriores está correta.**Resposta correta:** Nenhuma das alternativas anteriores está correta.**Pontuação: 1 / 1**

6. Quais os benefícios de um SOC?

- Resposta a incidente, agilidade na resposta, redução de custo e redução de complexidade.
- Resposta a incidente, quadro de funcionário maior, redução de custo e redução de complexidade.
- Resposta a incidente, agilidade na resposta, monitoramento de incidentes de TI e redução de complexidade.
- Nenhuma das alternativas anteriores está correta.

Resposta correta: Resposta a incidente, agilidade na resposta, redução de custo e redução de complexidade.**Pontuação: 1 / 1**

7. Quais incidentes o SOC deve analisar?

- Falso-positivo
- Incidentes críticos
- Incidentes de TI
- Correlacionados

Todos os incidentes de segurança da informação.**Resposta correta:** Todos os incidentes de segurança da informação.**Pontuação: 1 / 1**

8. Quais as formas de defender o investimento do SOC?

- Compliance, controles e framework.
- Controles, assessment e redução de complexidade.
- Compliance, controles e redução de complexidade.
- Novas ferramentas, controles e redução de complexidade.
- Todas as alternativas anteriores estão corretas.

Resposta correta: Compliance, controles e redução de complexidade.**Pontuação: 1 / 1**

Dúvidas

Bloco de Notas