



&lt; Voltar

&lt; Anterior Próximo &gt;

## Fundamentos de SOC - Security

Operations Center (online)

40 aula(s) no total

16 aula(s) completa(s) 0 aula(s) iniciada(s)

&gt; Bem-vindo(a)!

&gt; Aula 1 - Introdução ao SOC

&gt; Aula 2 - SIEM

&gt; Aula 3 - Threat Intelligence

□ Threat Intelligence     ♡ Teste seus conhecimentos 

&gt; Aula 4 - Framework

□ Tipos de framework     □ NIST x SANS     □ Playbook     ♡

&gt; Aula 5 - KPI

&gt; Aula 6 - Criando um SOC

&gt; Aula 7 - Workflow

&gt; Aula 8 - Metodologia SIM

&gt; Pesquisa de satisfação

## Teste seus conhecimentos

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

Você ainda pode responder 2 vezes, deseja tentar novamente?

Clique aqui

## 1. O que é um framework?

- Uma comunidade em prol de melhorias para SOC.
- Uma empresa.
- Algo similar ao ISO27002.
- Uma norma regulamentadora de SOC.

Uma estrutura que auxilia na criação de um SOC.

Resposta correta: Uma estrutura que auxilia na criação de um SOC.

## Comentário do professor:

Os frameworks são estruturas de controle usadas como ferramenta na construção de uma equipe de resposta a incidente.

Pontuação: 1 / 1

## 2. Quais dos itens abaixo não são um framework de resposta a incidente?

- NIST, ISO27002 e ISACA.
- SANS, ISO27002 e LGPD.
- ISO27002, GDPR e ISO27035.
- NIST, LGPD e GDPR.

ISO27002, LGPD e GDPR.

Resposta correta: ISO27002, LGPD e GDPR.

## Comentário do professor:

ISO27002 fala sobre segurança da informação, mas não tem resposta a incidente como foco.

LGPD e GDPR são leis de proteção de dados e não têm associação com resposta a incidente.

Pontuação: 1 / 1

## 3. Quantas etapas existem no framework do NIST e do SANS?

- NIST=5 / SANS=4
  - NIST=6 / SANS=3
- NIST=4 / SANS=6
- NIST=5 / SANS=6
  - NIST=6 / SANS=4

Resposta correta: NIST=4 / SANS=6

## Comentário do professor:

SANS=6 (Preparação, Identificação, Contenção, Erradicação, Recuperação, Lições aprendidas)

NIST= 4 (Preparação, Detecção e Análise, Contenção-Erradicação-Recuperação, Atividade pós-incidente)

Pontuação: 1 / 1

## 4. O que é um playbook?

- Processo de segurança da informação
- Manual de boas práticas
- Procedimento de melhoria

Procedimento de resposta a incidente

Resposta correta: Procedimento de resposta a incidente

Pontuação: 1 / 1

## 5. Quais dos itens abaixo fazem parte de um playbook?

- Escalonamento

- Áreas envolvidas

- Manual para responder um incidente

- Papéis e responsabilidade

Todas as alternativas anteriores estão corretas.

Resposta correta: Todas as alternativas anteriores estão corretas.

## Comentário do professor:

Em um playbook, deve haver o máximo de informação possível para a resposta dos incidentes, dentre elas: Todos os envolvidos, escalonamento, papéis e responsabilidade e como responder ao incidente tecnicamente.

Pontuação: 1 / 1

Dúvidas

Bloco de Notas