NEaD
Núcleo de Educação a Distância

# CYBER SECURITY

Faculdade IMPACTA

# 1

# O Perigo do Mundo Digital

Alex Sandro da Silva Feitosa

***Resumo***

*Nessa aula iniciaremos com a memorização de quem são os atores de ameaças, amadores, hacktivistas, grupos do crime organizado, patrocinados pelo Estado e grupos terroristas, entre outros. Abordaremos sobre o Sistema Operacional Windows, Linux, e protocolos e conectividade das redes.*

## Introdução

Vamos identificar os principais atores de ameaças, como amadores, hacktivistas, grupos criminosos, patrocinados por Estados e terroristas. Também abordaremos os fundamentos dos sistemas operacionais Windows e Linux, além de protocolos e conectividade de redes.

## 1.1. O Perigo do hack

### 1.1.1 Evil Twin - Gêmeo Mau

Os atacantes (hackers) podem configurar hotspots Wi-Fi abertos que simulam ser redes legítimas. Esses hotspots falsos, conhecidos como “gêmeos malvados” (Evil Twins), são usados para enganar usuários e capturar suas informações.

### 1.1.2 Empresas Chantageadas

Funcionários de uma organização frequentemente são induzidos a abrir arquivos anexos que instalam ransomware em seus dispositivos.

Uma vez instalado, o ransomware começa a coletar e criptografar os dados presentes nesses dispositivos.

O objetivo dos atacantes é obter ganho financeiro, mantendo os dados da empresa inacessíveis até que o resgate seja pago.

### 1.1.3 Nações Alvo - Stuxnet

Alguns malwares atuais são tão sofisticados e caros para desenvolver que especialistas em segurança acreditam que apenas uma nação ou um grupo de nações teria a influência e os recursos necessários para criá-los.

Esse tipo de malware pode ser projetado para atacar infraestruturas críticas vulneráveis de uma nação, como sistemas de reservatórios de água ou redes elétricas.

Um exemplo bastante conhecido é o worm Stuxnet, que se propagava por unidades USB e infectava sistemas operacionais Windows. Ele foi especificamente direcionado ao software desenvolvido pela Siemens para seus Controladores Lógicos Programáveis (PLCs).

### 1.1.4 Evil Twin - Gêmeo Mau

Os atacantes podem configurar redes Wi-Fi abertas e “invasoras” que simulam ser redes legítimas.

Essas redes falsas também são conhecidas como “gêmeos malvados” (Evil Twins).

### 1.1.5 Quem são os atacantes?

**Figura 1.1 Atores de Ameaças**

**Fonte: CCNA Cyber OPS Associate v1, 2020.**

Os atacantes são indivíduos ou grupos que realizam ataques cibernéticos. Eles incluem, mas não se limitam a:

- Amadores

  Também conhecidos como script kiddies, possuem pouca ou quase nenhuma habilidade técnica. Geralmente utilizam ferramentas prontas ou instruções

encontradas na internet para lançar ataques. Mesmo usando ferramentas básicas, seus ataques podem causar danos significativos.

- Hacktivistas
  São hackers que protestam contra ideias políticas e sociais. Eles compartilham artigos e vídeos, vazam informações confidenciais e interrompem serviços web com tráfego ilegítimo, utilizando ataques do tipo DDoS (Distributed Denial of Service).
- Grupos de crime organizado
  A maior parte das ameaças de hacking é motivada por ganhos financeiros. Esses cibercriminosos buscam acesso privilegiado a contas bancárias, dados pessoais e outras informações confidenciais que possam ser usadas para obtenção de lucro.
- Grupos patrocinados por Estados-nação
  Às vezes, países invadem outros países ou interferem em suas políticas internas por meio do ciberespaço. Muitas vezes, esses grupos estão interessados em espionagem industrial, roubando projetos, propriedade intelectual e outras informações que possam dar vantagem competitiva no comércio internacional.
- Grupos terroristas
  Utilizam ferramentas da internet para espalhar o medo por meio de ações violentas, tanto físicas quanto psicológicas.

Os ataques cibernéticos são atos maliciosos e intencionais que têm como objetivo causar impacto negativo a indivíduos ou organizações.

### 1.1.6 Quão segura é a Internet das Coisas?

A Internet das Coisas (IoT) permite que indivíduos conectem dispositivos eletrônicos, eletrodomésticos e outros equipamentos à internet, com o objetivo de melhorar sua qualidade de vida.

No entanto, muitos desses dispositivos conectados não possuem seus firmwares atualizados para a versão mais recente. Alguns modelos mais antigos sequer recebem suporte para atualizações de segurança.

Essa situação cria vulnerabilidades que podem ser exploradas por atacantes, representando um grande risco para a segurança dos proprietários desses dispositivos.

## 1.2. Impacto das Ameaças

### 1.2.1 PII, PHI e PSI?

Informações Pessoais Identificáveis (PII) são todos os dados que podem ser usados para identificar um indivíduo, como nome, número de seguro social, data de nascimento, números de cartão de crédito, entre outros.

Cibercriminosos têm como objetivo obter essas informações ou arquivos de PII para comercializá-los na dark web. As informações roubadas geralmente são usadas para criar contas falsas, como cartões de crédito, contas bancárias e empréstimos fraudulentos.

A comunidade médica cria e mantém Registros Médicos Eletrônicos (EMRs), que contêm Informações de Saúde Protegidas (PHI), um subconjunto das PII.

Outro tipo de PII são as Informações de Segurança Pessoal (PSI), que incluem nomes de usuário, senhas e outros dados relacionados à segurança, utilizados pelos indivíduos para acessar informações ou serviços na rede.

### 1.2.2 Vantagem Competitiva Perdida

- O vazamento de propriedade intelectual para concorrentes representa uma ameaça séria à sustentabilidade e à inovação de uma empresa.
- Além disso, a incapacidade de proteger os dados pessoais dos clientes compromete a confiança do público, um ativo intangível essencial.
- Essa perda de confiança pode, por sua vez, resultar diretamente na perda da vantagem competitiva — um diferencial difícil de recuperar em mercados altamente disputados.

### 1.2.3 Política de impacto de ameaças e segurança nacional

- As ameaças cibernéticas não afetam apenas empresas privadas — governos e infraestruturas críticas também estão na linha de frente.
- Grupos de hackers apoiados por Estados-nação podem causar interrupções significativas ou até destruição de serviços essenciais em países adversários, representando um novo tipo de guerra silenciosa.
- A crescente dependência da internet para operações comerciais, financeiras e administrativas tornou as redes digitais alvos estratégicos. A interrupção dessas atividades pode gerar impactos devastadores, incluindo o colapso de setores econômicos inteiros, comprometendo a estabilidade e a soberania nacional.

## 1.3. Protegendo as empresa contra o crime cibernético

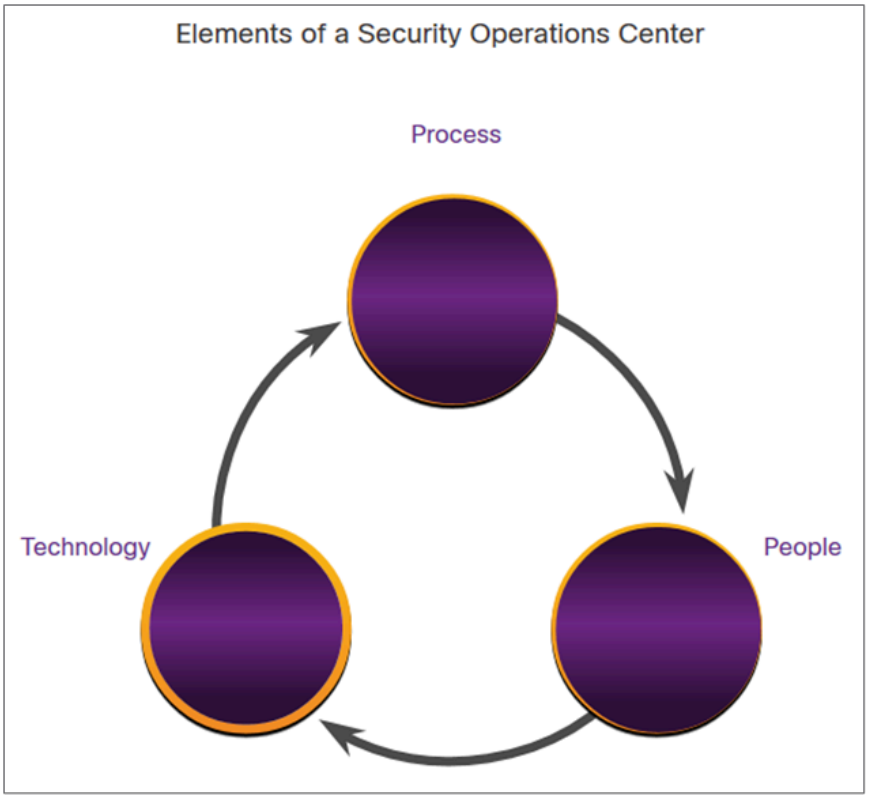
### 1.3.1 SOC - O moderno centro de operações de segurança

Para adotar uma abordagem formalizada, estruturada e disciplinada na defesa contra ameaças cibernéticas, as organizações recorrem frequentemente aos serviços especializados de um Centro de Operações de Segurança (SOC).

Esses centros oferecem uma gama abrangente de serviços, que vão desde o monitoramento contínuo e a gestão de incidentes até soluções integradas de resposta a ameaças e segurança personalizada baseada em hospedagem.

Os SOCs podem ser totalmente internos — de propriedade e operação exclusiva da organização — ou operados de forma híbrida, com a terceirização parcial ou total de suas funções a fornecedores especializados, como os Serviços de Segurança Gerenciados da Cisco.

**Figura 1.2 Elementos de um SOC**




**Fonte: CCNA Cyber OPS Associate v1, 2020.**

Os Centros de Operações de Segurança (SOCs) organizam suas funções por níveis, conforme a experiência exigida e a complexidade das responsabilidades atribuídas a cada cargo. Essa estrutura hierárquica garante uma resposta eficiente e especializada a incidentes de segurança cibernética.

- Nível 1 – Analista de Alerta:
  Responsável pelo monitoramento inicial dos alertas recebidos pelo sistema. Avalia se o alerta corresponde a um incidente real e, em caso afirmativo, encaminha o ticket para o próximo nível para investigação aprofundada. Trata-se de uma função de entrada, com foco em triagem e análise preliminar.
- Nível 2 – Respondente de Incidente:
  Realiza a investigação detalhada dos incidentes reportados. Este profissional avalia o escopo e a gravidade do problema, fornece orientações para remediação e recomenda ações corretivas para mitigar riscos e prevenir recorrências.
- Nível 3 – Caçador de Ameaças (Threat Hunter):

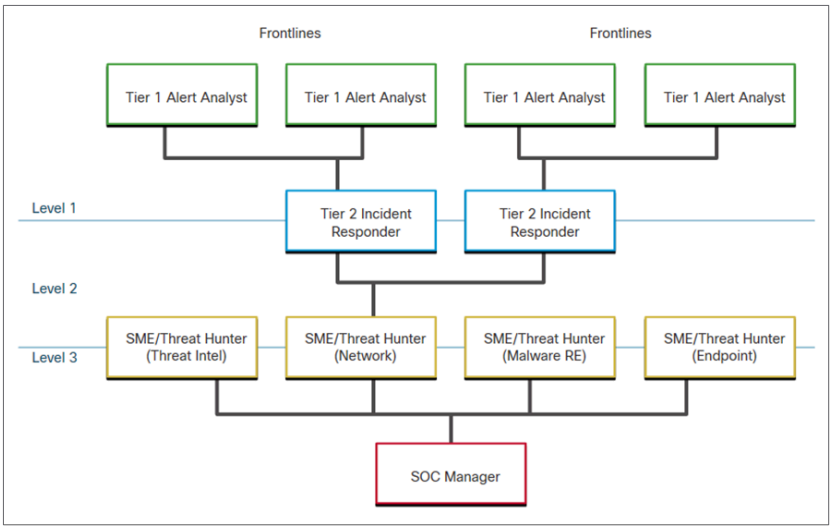
Profissionais altamente especializados em áreas como redes, endpoints, inteligência de ameaças, engenharia reversa de malware e análise comportamental. São responsáveis por identificar e mitigar ameaças avançadas que ainda não foram detectadas pelos sistemas automatizados. Também atuam no desenvolvimento e ajuste de ferramentas de detecção proativa.

- Gerente de SOC:
  Supervisiona todas as operações do SOC, coordena os recursos humanos e tecnológicos e atua como principal ponto de contato entre o SOC e a organização ou o cliente. Também é responsável pela definição de estratégias e pela melhoria contínua dos processos de segurança.

As funções de nível 1 geralmente são posições de entrada, adequadas para profissionais iniciando suas carreiras em segurança cibernética. Já as de nível 3 exigem ampla experiência técnica, visão analítica refinada e conhecimento aprofundado sobre o ambiente de ameaças.

A figura abaixo, que é originária do Instituto SANS, representa graficamente como essas funções interagem entre si.

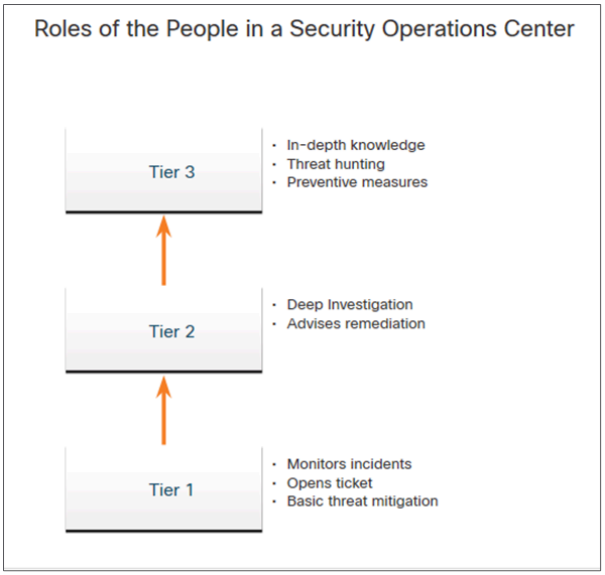
**Figura 1.3 SOC**




**Fonte: CCNA Cyber OPS Associate v1, 2020.**

### 1.3.2 Detalhando os Níveis operacionais do SOC

**Figura 1.4 Níveis de um SOC**




**Fonte: CCNA Cyber OPS Associate v1, 2020.**

Um analista de segurança cibernética desempenha um papel fundamental no monitoramento de alertas de segurança e na investigação inicial dos incidentes potenciais. Para organizar e gerenciar esse processo, é utilizado um sistema de emissão de tickets, que distribui automaticamente os alertas gerados por ferramentas de segurança para as filas dos analistas responsáveis.

O software de monitoramento, embora eficaz, pode gerar alarmes falsos (falsos positivos). Assim, cabe ao analista verificar se o alerta recebido representa, de fato, um incidente de segurança real. Essa verificação inicial é crucial para evitar desperdício de recursos e garantir que apenas ameaças legítimas avancem no fluxo de resposta.

- Se confirmado como incidente verdadeiro, o ticket é escalado para os investigadores ou para outros membros da equipe de segurança para tratamento adequado.
- Se identificado como alarme falso, o alerta é encerrado e descartado.

Caso o analista de segurança não consiga resolver o ticket ou se o incidente exigir análise mais detalhada, o caso é encaminhado para um Respondente de Incidentes (Nível 2). Esse profissional realizará uma investigação mais aprofundada e aplicará ou recomendará as medidas de remediação necessárias.

Se, mesmo após essa etapa, o incidente continuar sem solução, o ticket é então escalado para o Nível 3 (Caçadores de Ameaças ou especialistas avançados), que possuem maior expertise técnica para lidar com ameaças complexas ou persistentes.

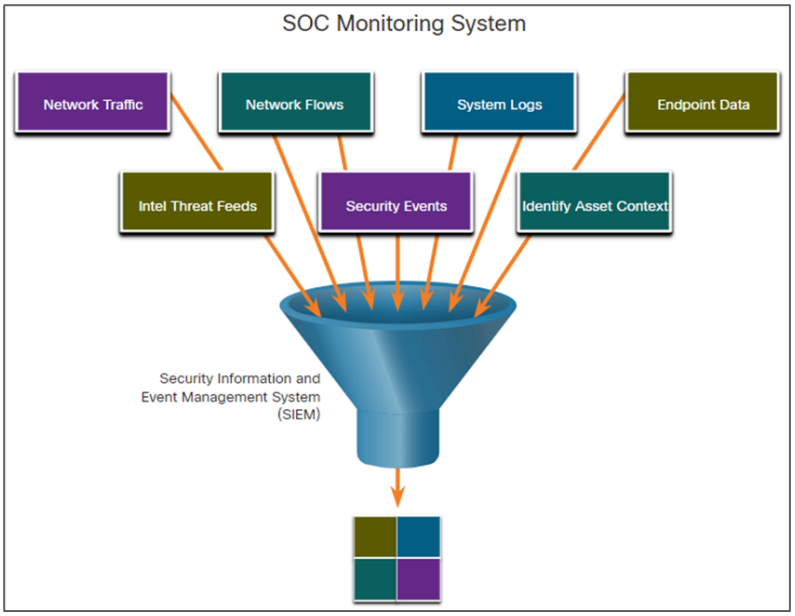
Esse processo escalonado garante agilidade, precisão e profundidade na resposta a incidentes de segurança cibernética.

### 1.3.3 Tecnologias do Cibercrime no SOC: SIEM

Um Centro de Operações de Segurança (SOC) depende fortemente de sistemas SIEM (Security Information and Event Management – Gerenciamento de Informações e Eventos de Segurança) para interpretar e correlacionar os dados gerados por firewalls, dispositivos de rede, sistemas de detecção de intrusões (IDS/IPS) e outros dispositivos de infraestrutura crítica.

Esses sistemas coletam, filtram e analisam grandes volumes de dados, detectando e classificando possíveis ameaças. Além disso, possibilitam a investigação de incidentes e, em alguns casos, ajudam na aplicação de medidas preventivas para lidar com ameaças futuras.

**Figura 1.5 SIEM**




**Fonte: CCNA Cyber OPS Associate v1, 2020.**

Para aumentar ainda mais a eficiência operacional e acelerar a resposta a incidentes, muitas organizações integram os sistemas SIEM com plataformas SOAR (Security Orchestration, Automation and Response – Orquestração, Automação e Resposta de Segurança).

As tecnologias SOAR complementam os SIEMs ao oferecer:

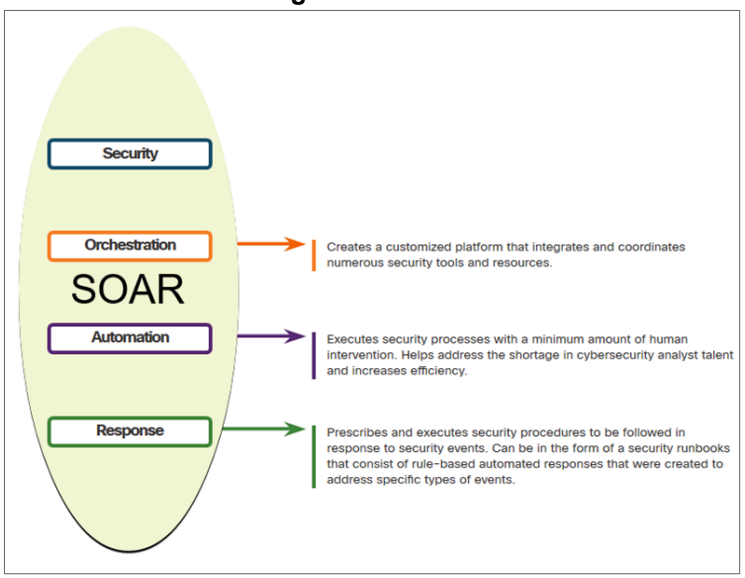
- Integração de inteligência contra ameaças: Coleta e análise de dados de fontes externas e feeds de ameaças para enriquecer a detecção e resposta.
- Automatização de fluxos de trabalho: Execução automática de ações com base em manuais (playbooks) definidos previamente, reduzindo o tempo de resposta e a carga operacional sobre a equipe.
- Orquestração de ferramentas de segurança: Conecta e coordena diferentes soluções de segurança em um único ambiente integrado.

- Análise e resposta padronizadas: Garante consistência nas ações tomadas diante de incidentes similares.

Enquanto o SIEM fornece a visibilidade e correlação dos eventos de segurança, o SOAR transforma essa inteligência em ações automatizadas e coordenadas, tornando os processos de SecOps (operações de segurança) mais rápidos, eficazes e escaláveis.

Grandes equipes de operações de segurança utilizam essas duas tecnologias em conjunto para otimizar seus SOCs, garantindo uma postura de defesa mais ágil, automatizada e resiliente diante de ameaças complexas.

**Figura 1.6 SOAR**




**Fonte: CCNA Cyber OPS Associate v1, 2020.**

As plataformas SOAR desempenham um papel essencial na modernização e automação das operações de segurança cibernética. Elas foram projetadas para reunir, coordenar e automatizar as ações necessárias para detectar, investigar e responder a incidentes de forma eficiente e padronizada.

As principais funcionalidades das plataformas SOAR incluem:

- Coleta centralizada de dados de alarme:
  Reúnem e consolidam dados de alertas provenientes de todos os componentes do ecossistema de segurança — como firewalls, SIEMs, sistemas de detecção de intrusões, antivírus, e outras ferramentas de monitoramento.
- Ferramentas para investigação e análise:
  Oferecem recursos integrados para pesquisa, avaliação e investigação de casos de segurança, permitindo que os analistas compreendam o escopo e a natureza dos incidentes com mais profundidade e agilidade.
- Integração e automação de fluxos de trabalho:
  Enfatizam a integração com diversas soluções de segurança, visando a orquestração de processos e a automação de fluxos de resposta complexos. Isso

permite respostas mais rápidas, coordenadas e adaptativas frente a ameaças emergentes.

- Uso de playbooks predefinidos:
  Incorporam playbooks — conjuntos de instruções automatizadas para lidar com ameaças específicas. Esses playbooks podem ser disparados automaticamente com base em regras definidas ou iniciados manualmente pela equipe de segurança, proporcionando flexibilidade operacional e resposta consistente.

Com essas capacidades, as plataformas SOAR reduzem o tempo de resposta a incidentes, aliviam a carga operacional dos analistas e aumentam a eficiência geral do SOC, transformando operações reativas em estratégias proativas e automatizadas de defesa cibernética.

## 1.4 Você conhece?

A plataforma Cisco Networking Academy (NetAcad) disponibiliza um conjunto de máquinas virtuais destinadas à realização de testes laboratoriais e simulações práticas. Esses recursos permitem que os alunos e profissionais desenvolvam habilidades técnicas em um ambiente controlado e realista, essencial para o aprendizado aplicado em redes e segurança cibernética.

Para acessar e utilizar essas máquinas virtuais, siga o passo a passo descrito no Anexo I – Recursos Necessários, localizado ao final deste texto.

### 1.5 Reflexão

Vantagens:

- Ambiente isolado para testes:
  Permite testar novos aplicativos, sistemas operacionais ou configurações sem afetar o computador principal (host), reduzindo riscos.

- Snapshots e pontos de restauração:
  É possível salvar o estado atual da máquina virtual (snapshot) antes de realizar mudanças. Caso algo dê errado, a máquina pode ser revertida para um estado anterior, facilitando a recuperação rápida.

- Flexibilidade e portabilidade:
  Máquinas virtuais podem ser facilmente copiadas, movidas e executadas em diferentes computadores, facilitando a distribuição de ambientes padronizados.

- Economia de recursos físicos:
  Permite rodar múltiplos sistemas operacionais simultaneamente em um único hardware, otimizando o uso dos recursos disponíveis.

Desvantagens:

- Consumo de recursos do host:

Máquinas virtuais utilizam espaço em disco, memória RAM e poder de processamento do computador principal, o que pode impactar o desempenho geral, especialmente em hardware limitado.

- Performance reduzida:
  Em alguns casos, a virtualização pode gerar uma queda no desempenho das aplicações, principalmente em tarefas que exigem alta capacidade gráfica ou processamento intensivo.hi

- Complexidade de configuração:
  A criação, configuração e manutenção de máquinas virtuais podem demandar conhecimento técnico específico, o que pode ser uma barreira para usuários iniciantes.

## 1.6 Vamos praticar ?

### 1.6.1 TEDxMidwest

Veja o vídeo TEDx "Top Hacker Mostra-nos como é feito; Pablos Holman em TEDxMidwests " ( https://www.youtube.com/watch?v=hqKafI7Amd8 )

a. Localize o vídeo na internet e assista.
b. Escolha um dos hacks discutidos pelo Sr. Holman no vídeo e use seu mecanismo de busca favorito para conduzir algumas pesquisas adicionais sobre o hack.
c. Sobre o hack escolhido, responda as perguntas abaixo e esteja preparado para compartilhar seu trabalho em uma discussão em classe:

As respostas variam de acordo com o hack escolhido.

1. Qual é a vulnerabilidade que está sendo explorada?
2. Quais informações, dados ou controle podem ser obtidos por um hacker que explora esta vulnerabilidade?
3. Como o hack é executado?
4. O que, especificamente, nesse hack, interessou você?
5. Como você acha que esse hack poderia ser atenuado?

### 1.6.2 Laboratório - Estudos de caso de cibersegurança

Governos, empresas e usuários individuais são cada vez mais alvos de ataques cibernéticos, e especialistas prevêem que esses ataques provavelmente aumentarão no futuro. A educação em segurança cibernética tornou-se uma prioridade internacional de alto nível, especialmente porque incidentes de grande repercussão levantam o temor de que esses ataques possam ameaçar a economia global. O Centro de Estudos Estratégicos e Internacionais (CSIS) estima que o custo do crime cibernético para a economia global ultrapassa US$ 600 bilhões anualmente.

Neste laboratório, você irá estudar quatro ataques cibernéticos de alto impacto, preparando-se para discutir o "quem", "o quê", "por quê" e "como" de cada ataque.

**Passo 1:** Usando seu mecanismo de busca favorito, realize pesquisas para cada um dos ataques cibernéticos listados abaixo. Você também pode escolher outros ataques

amplamente divulgados na mídia. Sua pesquisa deverá incluir diversos tipos de fontes, como artigos de notícias e artigos técnicos.

- O vírus Stuxnet
- Violação de dados Marriott
- Violação de dados das Nações Unidas
- Violação do banco de dados de suporte ao cliente da Microsoft
- Violação de dados do Lifelabs

**Observação**: Você pode utilizar o navegador da web da máquina virtual instalada em um laboratório anterior para pesquisar os ataques. O uso da máquina virtual ajuda a evitar que malware seja instalado no seu computador.

**Passo 2:** Leia atentamente os artigos encontrados em sua pesquisa e esteja preparado para discutir e compartilhar suas descobertas sobre:

As respostas variam de acordo com o ataque cibernético escolhido.

1. Quem foram as vítimas dos ataques?
2. Quais tecnologias e ferramentas foram usadas no ataque?
3. Quando o ataque aconteceu dentro da rede?
4. Quais sistemas foram direcionados?
5. Qual foi a motivação dos atacantes neste caso? O que eles esperavam alcançar?
6. Qual foi o resultado do ataque? (dados roubados, resgate, danos no sistema, etc.)

## Considerações finais

Encerramos esta aula com uma compreensão inicial dos diferentes tipos de atores de ameaças e suas motivações. Também reforçamos os conceitos fundamentais dos sistemas operacionais Windows e Linux, além da importância dos protocolos e da conectividade para o funcionamento e a segurança das redes. Esses conhecimentos são essenciais para entender o cenário de ameaças e como proteger os sistemas de forma eficaz.

## Referências

Cisco Systems. **Cisco Networking Academy Program CCNA CyberOps Associate** v1, 2020. Disponível em: <https://www.netacad.com>.

SÊMOLA, Marcos**. Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

THOMAS, Tom. **Segurança de redes: primeiros passos**. Tradução de Flávio MORGADO. Rio de Janeiro: Ciência Moderna, 2007.

BEAL, A. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

STALLINGS, W. **Network security: applications and standards**. 3.nd. New Jersey: Prentice Hall, 2006.

**ASSOCIAÇÃO Brasileira de Normas Técnicas. NBR ISO/IEC 27001 E 27002** Tecnologia da informação.

WADLOW, Thomas A. **Segurança de redes: projeto e gerenciamento de redes seguras**. Rio de Janeiro: Campus, 2000.