**Introdução**

2.0.1

**Por que devo fazer este módulo?**

Se você estiver fazendo este curso, você pode estar considerando uma carreira em segurança CyberOps. Quais tecnologias você precisa estar ciente? Que tipos de empregos estão disponíveis? Onde você pode encontrar esses empregos? Continue lendo para descobrir!

2.0.2

**O que vou aprender neste módulo?**

**Título do módulo:** Lutadores na guerra contra o crime cibernético

**Objetivo do módulo:** Explicar como se preparar para uma carreira em operações de segurança cibernética.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| O SOC moderno | Explique a missão do centro de operações de segurança (SOC). |
| Tornando-se um Defensor | Descrever os recursos disponíveis para se preparar para uma carreira nas operações da segurança cibernética. |

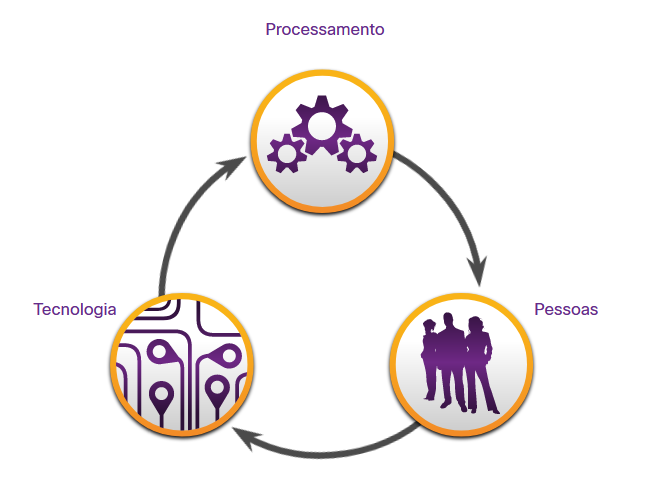
# O Centro de Operações de Segurança Moderno

2.1.1

## Elementos de um SOC

A defesa contra as ameaças atuais requer uma abordagem formalizada, estruturada e disciplinada. Normalmente, as organizações usam os serviços de profissionais em um Centro de Operações de Segurança (SOC). Os SOCs oferecem uma ampla gama de serviços, desde monitoramento e gerenciamento até soluções abrangentes de ameaças e segurança hospedada que podem ser personalizadas para atender às necessidades dos clientes. Os SOCs podem ser totalmente internos, de propriedade e operados por uma empresa, ou elementos de um SOC podem ser contratados a fornecedores de segurança, como os [Managed Security Services] (<http://www.cisco.com/c/en/us/products/security/managed-services.html>) da Cisco.

Como ilustrado na figura, os principais elementos de um SOC, são pessoas, processos e tecnologias.



A figura mostra os três elementos de um centro de Operações de Segurança ou SOC. Os três elementos são pessoas, processos e tecnologia.

TecnologiaPessoasProcessamentoElementos de um Centro de Operações de Segurança

2.1.2

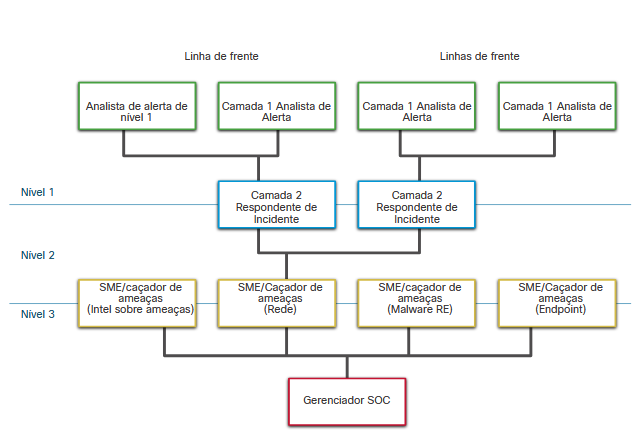
## Pessoas no SOC

As funções de trabalho em um SOC estão evoluindo rapidamente. Tradicionalmente, os SOCs atribuem funções de trabalho por níveis, de acordo com a experiência e as responsabilidades necessárias para cada um. Os trabalhos de primeiro nível são mais de nível inicial, enquanto os empregos de terceiro nível exigem ampla experiência.

* **Analista de Alerta de Nível 1** - Esses profissionais monitoram alertas recebidos, verificam se um incidente verdadeiro ocorreu e encaminham tickets para o Nível 2, se necessário.
* **Respondente a Incidentes de Nível 2** - Esses profissionais são responsáveis pela investigação aprofundada de incidentes e aconselham a correção ou a ação a serem tomadas.
* **Caçador de Ameaças de Nível 3** - Esses profissionais possuem habilidades de nível especializado em rede, endpoint, inteligência contra ameaças e engenharia reversa de malware. Eles são especialistas em rastrear os processos do malware para determinar seu impacto e como ele pode ser removido. Eles também estão profundamente envolvidos na busca de ameaças potenciais e na implementação de ferramentas de detecção de ameaças. Os caçadores de ameaças buscam ameaças cibernéticas presentes na rede, mas ainda não foram detectadas.
* **Gerente SOC** - Este profissional gerencia todos os recursos do SOC e serve como ponto de contato para a organização ou cliente maior.

Este curso oferece preparação para uma certificação adequada para o cargo de Analista de Alerta de Nível 1, também conhecido como Analista de Segurança Cibernética ou CyberOps Associate.

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



A figura mostra um tipo de fluxograma. No topo estão os Analistas de Alerta de Nível 1 da linha de frente. Seu trabalho flui para os Respondentes a Incidentes de Nível 2, que estão logo abaixo deles na figura, no Nível 1. O trabalho dos Respondentes a Incidentes de Nível 2 é considerado Nível 2. Ele flui para o Expertes/Caçadores de Assunto Nível 3 no Nível 3. Eles são divididos em 4 tipos de SME/caçadores: inteligência contra ameaças, rede, malware e ponto de extremidade. O trabalho das PME/caçadores de nível 3 flui para o gerente de SOC.

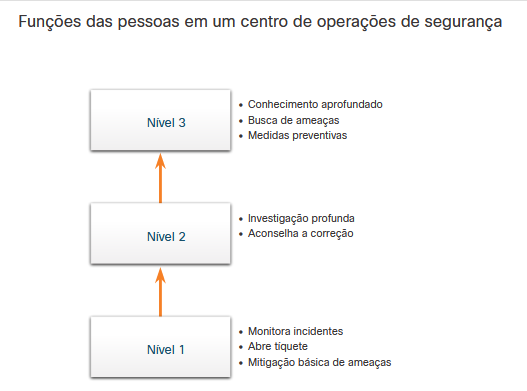
Nível 2Linhas de frenteNível 1Linha de frente Nível 3Analista de alerta de nível 1Camada 1 Analista de AlertaCamada 1 Analista de AlertaCamada 1 Analista de AlertaCamada 2 Respondente de IncidenteCamada 2 Respondente de IncidenteSME/caçador de ameaças  
(Intel sobre ameaças)SME/Caçador de ameaças  
(Rede)SME/caçador de ameaças  
(Malware RE)SME/Caçador de ameaças  
(Endpoint)Gerenciador SOC

2.1.3

## Processo no SOC

O dia de um analista de segurança cibernética geralmente começa com o monitoramento de filas de alertas de segurança. Um sistema de emissão de tíquetes é freqüentemente usado para atribuir alertas a uma fila para que um analista investigue. Como o software que gera alertas pode acionar alarmes falsos, um trabalho do analista de segurança cibernética pode ser verificar se um alerta representa um verdadeiro incidente de segurança. Quando a verificação for estabelecida, o incidente pode ser encaminhado aos investigadores ou a outro pessoal de segurança para ser tratado. Caso contrário, o alerta pode ser descartado como um alarme falso.

Se um tíquete não puder ser resolvido, o Analista de segurança cibernética encaminhará o tíquete para um Respondente de Incidente de Nível 2 para uma investigação e correção mais aprofundadas. Se o Respondente a Incidentes não puder resolver o tíquete, ele será encaminhado para o pessoal do Nível 3 com conhecimento profundo e habilidades de caça a ameaças.



A figura explica os papéis das pessoas no SOC. No Nível 1, os analistas monitoram tickets, abrem tickets e realizam mitigação básica de ameaças. No Nível 2, os respondentes a incidentes conduzem uma investigação profunda e aconselham a remediação. No Nível 3, as PME/caçadores usam seu conhecimento profundo, caçam ameaças e realizam medidas preventivas/

Funções das pessoas em um centro de operações de segurança

 Conhecimento aprofundado

 Busca de ameaças

 Medidas preventivasNível 3

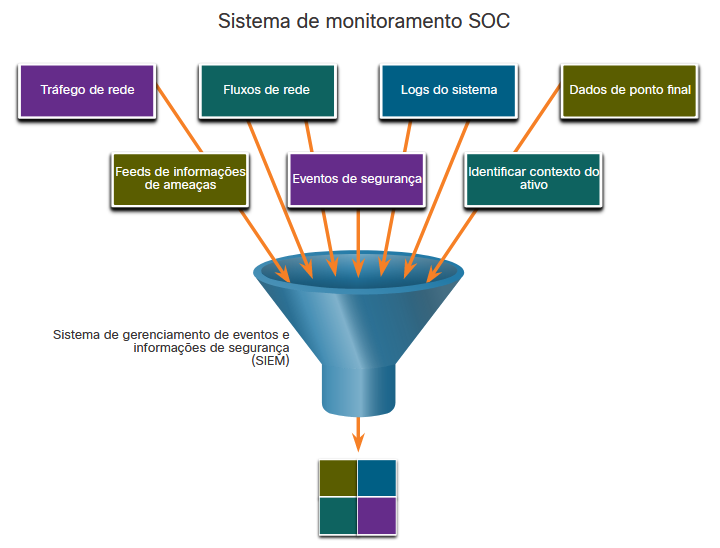
 Investigação profunda

 Aconselha a correçãoNível 2

 Monitora incidentes

 Abre tíquete

 Mitigação básica de ameaças Nível 1



2.1.4

## Tecnologias no SOC: SIEM

Como mostrado na figura, um SOC precisa de um SIEM (Security Information and Event Management System, sistema de gerenciamento de eventos e informações de segurança) ou seu equivalente. O SIEM faz sentido de todos os dados gerados por firewalls, dispositivos de rede, sistemas de detecção de intrusões e outros dispositivos.

Os sistemas SIEM são usados para coletar e filtrar dados, detectar e classificar ameaças e analisar e investigar ameaças. Os sistemas SIEM também podem gerenciar recursos para implementar medidas preventivas e lidar com ameaças futuras. As tecnologias SOC incluem um ou mais dos seguintes:

* Coleta, correlação e análise de eventos
* Monitoramento da segurança
* Controle de segurança
* Gerenciamento de logs
* Avaliação de vulnerabilidade
* Controle de vulnerabilidades
* Inteligência de ameaças

A figura é uma representação simplificada de um sistema de monitoramento SOC. Informações sobre tráfego de rede, fluxos de rede, registros do sistema, dados de ponto de extremidade, feeds de ameaças de inteligência, eventos de segurança e contexto de ativos de identificação são fornecidas no sistema de monitoramento de segurança.

Sistema de monitoramento SOC

Sistema de gerenciamento de eventos e informações de segurança

(SIEM) Tráfego de rede

Fluxos de rede

Logs do sistema

Dados de ponto final

Feeds de informações de ameaças

Eventos de segurança

Identificar contexto do ativo

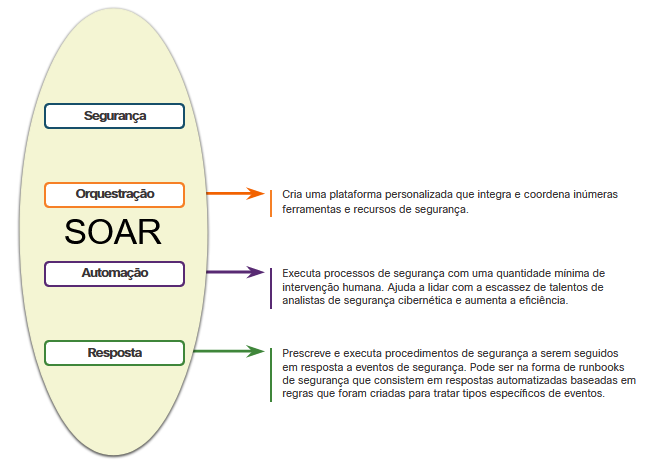
2.1.5

## Tecnologias no SOC: SOAR

SIEM e orquestração de segurança, automação e resposta (SOAR) são frequentemente emparelhados, pois possuem recursos que se complementam.

Grandes equipes de operações de segurança (SecOps) usam ambas as tecnologias para otimizar seu SOC. Estima-se que 15% das organizações com uma equipe de segurança de mais de cinco pessoas utilizarão o SOAR até o final de 2020.

As plataformas SOAR são semelhantes às SIEMs na medida em que agregam, correlacionam e analisam alertas. No entanto, a tecnologia SOAR vai um passo além integrando inteligência contra ameaças e automatizando os fluxos de trabalho de investigação e resposta de incidentes com base em manuais desenvolvidos pela equipe de segurança.



A figura mostra os quatro elementos do SOAR: segurança, orquestração, automação e resposta. Orquestração - integra e coordena inúmeras ferramentas e recursos de segurança. Automação - ajuda a lidar com a escassez de talentos de analistas de segurança cibernética e aumenta a eficiência. Resposta - pode ser na forma de runbooks de segurança que consistem em respostas automatizadas baseadas em regras que foram criadas para tratar tipos específicos de eventos.

S O A R

Cria uma plataforma personalizada que integra e coordena inúmeras ferramentas e recursos de segurança. SegurançaOrquestraçãoExecuta processos de segurança com uma quantidade mínima de intervenção humana. Ajuda a lidar com a escassez de talentos de analistas de segurança cibernética e aumenta a eficiência.RespostaAutomação Prescreve e executa procedimentos de segurança a serem seguidos em resposta a eventos de segurança. Pode ser na forma de runbooks de segurança que consistem em respostas automatizadas baseadas em regras que foram criadas para tratar tipos específicos de eventos.

Plataformas de segurança SOAR:

* Reunir dados de alarme de cada componente do sistema.
* Fornecer ferramentas que permitam que os casos sejam pesquisados, avaliados e investigados.
* Enfatizar a integração como um meio de automatizar fluxos de trabalho complexos de resposta a incidentes que permitem respostas mais rápidas e estratégias de defesa adaptativas.
* Incluir playbooks predefinidos que permitem a resposta automática a ameaças específicas. Os playbooks podem ser iniciados automaticamente com base em regras predefinidas ou podem ser acionados pelo pessoal de segurança.

SOAR enfatiza ferramentas de integração e automação de fluxos de trabalho SOC. Ele orquestra muitos processos manuais, como a investigação de alertas de segurança, que exigem apenas intervenção humana quando necessário. Isso libera o pessoal de segurança para lidar com questões mais urgentes e investigação de ponta e remediação de ameaças. A futura adoção de plataformas SOAR sofisticadas retornará as operações SOC e as funções de trabalho.

Os sistemas SIEM produzem necessariamente mais alertas do que a maioria das equipes de SECops pode investigar de forma realista, a fim de capturar de forma conservadora o maior número possível de explorações potenciais. A SOAR processará muitos desses alertas automaticamente e permitirá que o pessoal de segurança se concentre em explorações mais complexas e potencialmente prejudiciais.

2.1.6

## Métricas SOC

Um SOC é extremamente importante para a segurança de uma organização. Independentemente de o SOC ser interno a uma organização ou fornecer serviços a várias organizações, é importante entender o quão bem o SOC está funcionando para que possam ser feitas melhorias nas pessoas, processos e tecnologias que compõem o SOC.

Muitas métricas ou indicadores chave de desempenho (KPI) podem ser projetadas para medir diferentes aspectos específicos do desempenho do SOC. No entanto, cinco métricas são comumente usadas como métricas SOC. Observe, no entanto, que as métricas que descrevem o desempenho geral freqüentemente não apresentam uma imagem precisa da operação SOC devido à diversidade de ameaças à segurança cibernética. Várias métricas comuns compiladas pelos gerentes de SOC são:

* **Tempo de permanência** — o período de tempo que os atores da ameaça têm acesso a uma rede antes de serem detectados e seu acesso é interrompido.
* **Tempo médio para detectar (MTTD)** — o tempo médio que o pessoal do SOC leva para identificar incidentes de segurança válidos ocorreu na rede.
* **Tempo médio para responder (MTTR)** — o tempo médio necessário para parar e corrigir um incidente de segurança.
* **Tempo médio para conter (MTTC)** — o tempo necessário para impedir que o incidente cause mais danos aos sistemas ou dados.
* **Tempo de controle** — o tempo necessário para impedir a propagação de malware na rede.

2.1.7

## Segurança corporativa e gerenciada

Para redes de médio e grande porte, a organização se beneficiará com a implementação de um SOC de nível empresarial. O SOC pode ser uma solução interna completa. No entanto, muitas organizações maiores terceirizarão pelo menos parte das operações SOC para um provedor de soluções de segurança.

A Cisco tem uma equipe de especialistas que ajudam a garantir a resolução de incidentes oportuna e precisa. A Cisco oferece uma ampla variedade de recursos de resposta, preparação e gerenciamento a incidentes, incluindo:

* Serviço Cisco Smart Net Total Care para Resolução Rápida de Problemas;
* Equipe de resposta a incidentes de segurança do produto (PSIRT) da Cisco;
* Equipe de resposta a incidentes de segurança de computadores da Cisco (CSIRT);
* Serviços Gerenciados Cisco;
* Operações Táticas Cisco (TacOps);
* Programa de Segurança Física e Segurança da Cisco.

2.1.8

## Segurança versus disponibilidade

A maioria das redes empresariais deve estar em funcionamento o tempo todo. A equipe de segurança entende que, para que a organização cumpra suas prioridades, a disponibilidade da rede deve ser preservada.

Cada empresa ou setor tem uma tolerância limitada para o tempo de inatividade da rede. Essa tolerância é geralmente baseada em uma comparação do custo do tempo de inatividade em relação ao custo de garantia contra o tempo de inatividade. Por exemplo, em uma pequena empresa de varejo com apenas um local, pode ser tolerável ter um roteador como um único ponto de falha. No entanto, se uma grande parte das vendas dessa empresa for de compradores on-line, o proprietário pode decidir fornecer um nível de redundância para garantir que uma conexão esteja sempre disponível.

O tempo de atividade preferencial geralmente é medido no número de minutos de inatividade em um ano, conforme mostrado na tabela. Por exemplo, um tempo de atividade de “cinco noves” significa que a rede está acima de 99,999% do tempo ou inativa por não mais de 5 minutos por ano. “Quatro noves” seria um tempo de inatividade de 53 minutos por ano.

| **Disponibilidade %** | **Tempo de inatividade** |
| --- | --- |
| 99.8% | 17,52 horas |
| 99,9% (“três noves”) | 8,76 horas |
| 99,99% (“quatro noves”) | 52,56 minutos |
| 99,999% (“cinco noves”) | 5.256 minutos |
| 99,9999% (“seis noves “) | 31,56 segundos |
| 99,99999% (“sete noves “) | 3,16 segundos |

No entanto, a segurança não pode ser tão forte que interfira com as necessidades dos funcionários ou funções empresariais. É sempre um tradeoff entre forte segurança e permitir um funcionamento eficiente dos negócios.

2.1.9

## Verifique sua compreensão - Identifique a Terminologia SOC

# Tornando-se um Defensor

2.2.1

## Certificações

Uma variedade de certificações de segurança cibernética que são relevantes para carreiras em SOCs estão disponíveis em várias organizações diferentes.

**Cisco Certified CyberOps Associate**

A certificação Cisco Certified CyberOps Associate fornece um primeiro passo valioso na aquisição do conhecimento e das habilidades necessárias para trabalhar com uma equipe de SOC. Pode ser uma parte valiosa de uma carreira no campo empolgante e crescente das operações de segurança cibernética.

**Certificação de analista de segurança cibernética CompTIA**

A certificação CompTIA Cybersecurity Analyst (CySA+) é uma certificação profissional de TI neutra no fornecedor. Ele valida o conhecimento e as habilidades necessárias para configurar e usar ferramentas de detecção de ameaças, realizar análises de dados, interpretar os resultados para identificar vulnerabilidades, ameaças e riscos para uma organização. O objetivo final é a capacidade de proteger e proteger aplicativos e sistemas dentro de uma organização.

**( ISC) ² Certificações de segurança da informação**

(ISC) ² é uma organização internacional sem fins lucrativos que oferece a altamente aclamada certificação CISSP. Eles oferecem uma gama de outras certificações para várias especialidades em segurança cibernética.

**Certificação Global de Garantia de Informações (GIAC)**

A GIAC, fundada em 1999, é uma das mais antigas organizações de certificação de segurança. Oferece uma ampla gama de certificações em sete categorias.

**Outras Certificações Relacionadas à Segurança**

Pesquise por “certificações de segurança cibernética” na Internet para encontrar informações sobre outros fornecedores e certificações independentes de fornecedores.



2.2.2

## Aprofundar meus conhecimentos

**Graus**

Qualquer pessoa que considere uma carreira no campo da segurança cibernética deve considerar seriamente a obtenção de um diploma técnico ou bacharel em ciência da computação, engenharia elétrica, tecnologia da informação ou segurança da informação. Muitas instituições de ensino oferecem trilhas e certificações especializadas relacionadas à segurança.

**Programação em Python**

A programação de computadores é uma habilidade essencial para quem deseja seguir uma carreira em segurança cibernética. Se você nunca aprendeu a programar, então Python pode ser a primeira língua a aprender. Python é uma linguagem de código aberto orientada a objetos que é rotineiramente usada por analistas de segurança cibernética. É também uma linguagem de programação popular para sistemas baseados em Linux e redes definidas por software (SDN).

**Habilidades Linux**

Linux é amplamente utilizado em SOCs e outros ambientes de rede e segurança. As habilidades do Linux são uma adição valiosa ao seu conjunto de habilidades enquanto você trabalha para desenvolver uma carreira em segurança cibernética.



2.2.3

## Informações sobre carreira

Uma variedade de sites e aplicativos móveis anunciam empregos de tecnologia da informação. Cada site tem como alvo uma variedade de candidatos a empregos e fornece ferramentas diferentes para os candidatos pesquisarem sua posição de trabalho ideal. Muitos sites são agregadores de locais de trabalho. Os agregadores de sites de empregos reúnem listas de outros quadros de empregos e sites de carreiras de empresas e as exibem em um único local.

**Indeed.com**

Anunciado como o site de empregos número 1 do mundo, o Indeed.com atrai mais de 180 milhões de visitantes únicos por mês de mais de 50 países diferentes. Indeed.com é verdadeiramente um site de empregos mundial. Ajuda empresas de todos os tamanhos a contratar os melhores talentos e oferece a melhor oportunidade para quem procura emprego.

**CareerBuilder.com**

O CareerBuilder atende a muitas empresas grandes e de prestígio. Como resultado, esse site atrai candidatos específicos que normalmente têm mais educação e credenciais mais altas. Os empregadores que postam no CareerBuilder geralmente obtêm mais candidatos com diplomas universitários, credenciais avançadas e certificações do setor.

**USAJobs.gov**

O governo federal dos Estados Unidos publica todas as vagas no site USAJobs.

**Glassdoor**

O site glassdoor.com fornece informações salariais para diferentes tipos de trabalho, empresas e locais. Procure por “analista de segurança cibernética” para ver os salários e os requisitos para as vagas atuais.

**LinkedIn**

O LinkedIn é uma rede profissional de mais de 630 milhões de usuários em mais de 150 países com a missão de ajudar as pessoas a serem mais produtivas e bem-sucedidas. O LinkedIn também é uma ótima fonte de informações sobre carreira e oportunidades de emprego.



2.2.4

## Obtendo Experiência

**Estágios**

Os estágios são um excelente método para entrar no campo de segurança cibernética. Às vezes, os estágios se transformam em uma oferta de emprego em tempo integral. No entanto, mesmo um estágio temporário permite que você ganhe experiência no funcionamento interno de uma organização de segurança cibernética. Os contatos que você faz durante um estágio também podem ser um recurso valioso à medida que você continua sua carreira. Pesquise na internet os melhores sites para localizar estágios de segurança de rede.

**Bolsas e Prêmios**

Para ajudar a eliminar a lacuna nas habilidades de segurança, organizações como a Cisco e a INFOSEC introduziram programas de bolsas e prêmios que fornecem dinheiro aos alunos que atendem aos requisitos de qualificação. Pesquise na internet para descobrir oportunidades que são oferecidas atualmente.

**Agências Temporárias**

Se você está tendo dificuldades para encontrar seu primeiro emprego, uma agência temporária pode ser um ótimo lugar para começar. A maioria das agências temporárias irá ajudá-lo a polir o seu currículo e fazer recomendações sobre habilidades adicionais que você pode precisar obter para se tornar mais atraente para potenciais empregadores.

Muitas organizações usam agências temporárias para preencher vagas nos primeiros 90 dias. Então, se o funcionário for compatível, a organização pode se oferecer para comprar o contrato da agência temporária, convertendo o funcionário para um cargo permanente de tempo integral.

**Seu Primeiro Trabalho**

Se você não tem experiência no campo de segurança cibernética, provavelmente procurará uma empresa que esteja disposta a treiná-lo para uma posição semelhante a um analista de nível 1. Trabalhar para um call center ou suporte técnico pode ser o primeiro passo para obter a experiência de que você precisa para seguir em frente em sua carreira.

Quanto tempo você deve ficar no seu primeiro emprego? Geralmente, você quer passar por um ciclo de revisão completo antes de sair de uma empresa. Ou seja, você normalmente quer fazer isso durar 18 meses. Os potenciais empregadores normalmente vão querer saber se você atendeu ou excedeu as expectativas em seus empregos atuais ou passados.



2.2.5

## Laboratório - Como se tornar um defensor

Neste laboratório, você pesquisará e analisará o que é preciso para se tornar um defensor de rede.

# Resumo dos Lutadores na Guerra Contra o Cibercrime

2.3.1

## O que aprendi neste módulo?

**O Centro de Operações de Segurança Moderno**

Os principais elementos do SOC incluem pessoas, processos e tecnologias. As funções de trabalho estão evoluindo rapidamente e incluem níveis baseados em conhecimento e experiência. Essas funções incluem um Analista de Alerta de Nível 1, um Respondente de Incidentes de Nível 2, um Caçador de Ameaças de Nível 3 e um Gerente SOC. Um analista de nível 1 monitorará incidentes, abrirá tickets e realizará a mitigação de ameaças básicas.

Os sistemas SEIM são usados para coletar e filtrar dados, detectar e classificar ameaças e analisar e investigar ameaças. SEIM e SOAR costumam ser emparelhados. SOAR é semelhante ao SIEM. O SOAR vai um passo além ao integrar inteligência de ameaças e automatizar a investigação de incidentes e fluxos de trabalho de resposta com base em manuais desenvolvidos pela equipe de segurança. Os principais indicadores de desempenho (KPI) são elaborados para medir diferentes aspectos do desempenho do SOC. As métricas comuns incluem Tempo de espera, Tempo médio para detectar (MTTD), Tempo médio para responder (MTTR), Tempo médio para conter (MTTC) e Tempo para controlar.

Deve haver um equilíbrio entre segurança e disponibilidade das redes. A segurança não pode ser tão forte a ponto de interferir nos funcionários ou nas funções de negócios.

**Tornando-se um Defensor**

Uma variedade de certificações de cibersegurança que são relevantes para carreiras em SOCs estão disponíveis em diferentes organizações. Eles incluem Cisco Certified CyberOps Associate, CompTIA Cybersecurity Analyst Certification, (ISC) 2 Information Security Certifications, Global Information Assurance Certification (GIAC) e outros. Os sites de empregos incluem Even.com, CareerBuilder.com, USAJobs.gov, Glassdoor e LinkedIn. Você também pode considerar estágios e agências de trabalho temporário para ganhar experiência e começar sua carreira. Além disso, as habilidades de programação em Linux e Python aumentarão sua atratividade no mercado de trabalho.