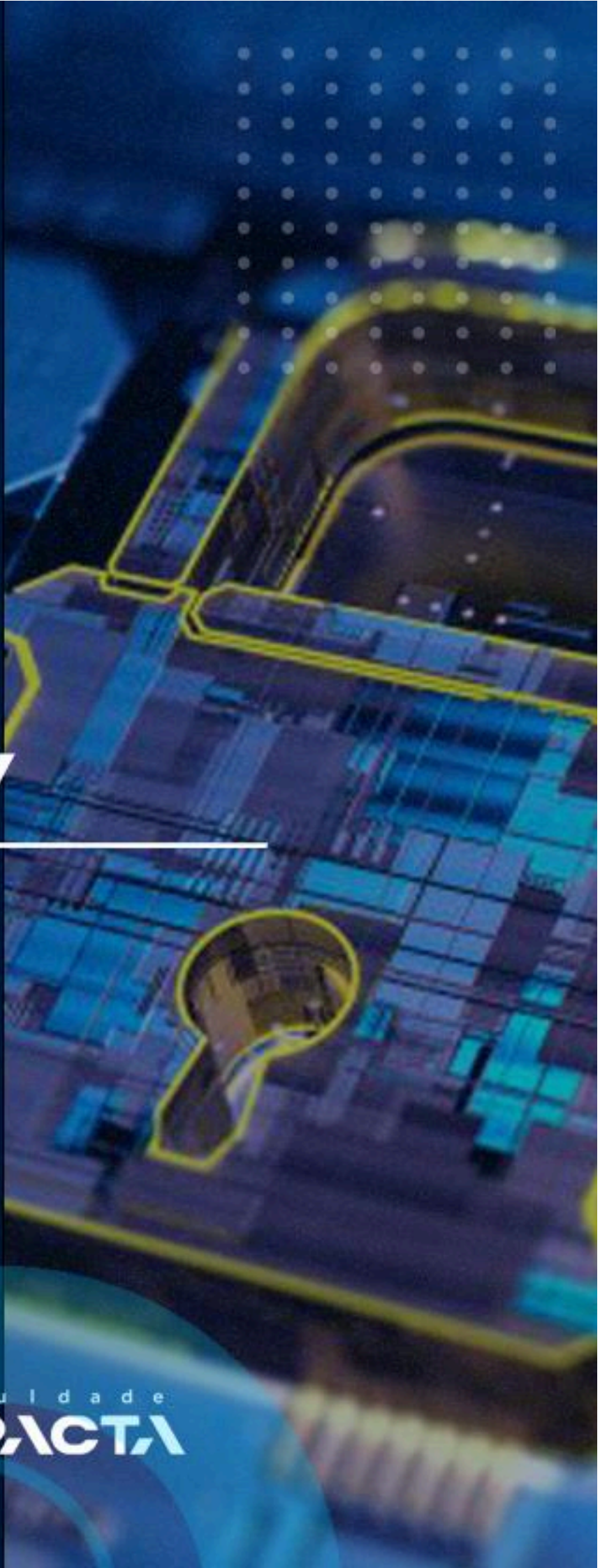
NEaD
Núcleo de Educação a Distância

CYBER SECURITY



Faculdade IMPACTA

8

Monitorando o tráfego de rede

Alex Sandro da Silva Feitosa

Resumo

Nessa aula, daremos início ao estudo sobre a importância do monitoramento de redes, destacando por que essa prática é fundamental para garantir o bom funcionamento e a segurança dos sistemas. Abordaremos os principais motivos que tornam o monitoramento uma atividade essencial no ambiente de TI, como a detecção de falhas, o controle de desempenho e a prevenção de ameaças. Além disso, será apresentado um panorama geral sobre como esse monitoramento é realizado na prática, utilizando ferramentas e métodos apropriados. Essa introdução servirá como base para aprofundarmos o tema ao longo do conteúdo.

1.1. Monitoramento de rede

1.1.1 Topologia de segurança de rede

Para atenuar ameaças, todas as redes devem estar protegidas.

A rede requer uma infra-estrutura de segurança que consiste em firewalls, sistemas de detecção de intrusões (IDS), sistemas de prevenção de intrusões (IPS) e software de segurança de terminais para proteger.

Esses métodos e tecnologias são usados para introduzir monitoramento automatizado, criar alertas de segurança ou bloquear automaticamente dispositivos ofensivos.

Para redes grandes, uma camada extra de proteção é adicionada.

Dispositivos como firewalls e IPS operam com base em regras pré-configuradas e monitoram o tráfego e comparam com as regras configuradas. Se houver uma correspondência, o tráfego é tratado de acordo com a regra.

Uma parte importante do analista de segurança cibernética é analisar todos os alertas gerados pelos dispositivos de rede e determinar a validade dos alertas.

Métodos de monitoramento de rede

As operações diárias de uma rede consistem em fluxo de tráfego, uso de largura de banda e acesso a recursos. Esses padrões identificam o comportamento normal da rede.

Para determinar o comportamento normal da rede, o monitoramento da rede deve ser implementado.

As ferramentas como IDS, analisadores de pacotes, SNMP, NetFlow e outras são usadas para monitoramento de rede.

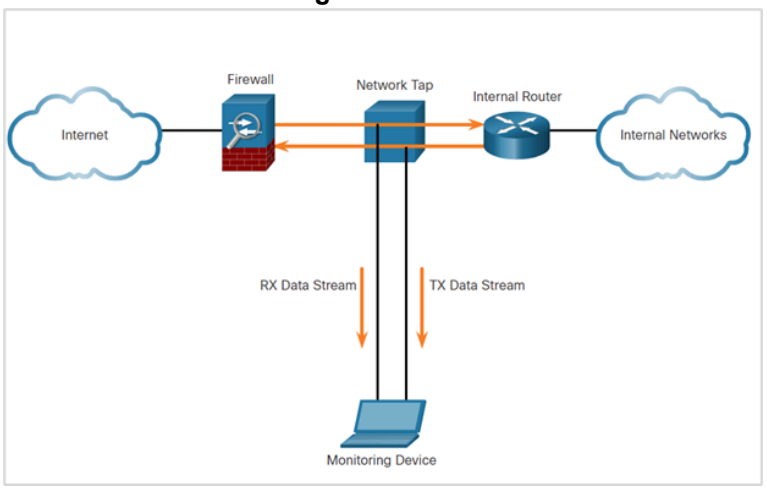
Existem dois métodos comuns usados para capturar o tráfego e enviá-lo para dispositivos de monitoramento de rede:

Taps de rede, também conhecidos como Test Access Points (TAPs)

Espelhamento de tráfego usando o SPAN (Switch Port Analyzer) ou outro espelhamento de porta.

Network Taps

Figura 1.1 TAP



Fonte: CCNA Cyber OPS Associate v1, 2020.

Um Tap de rede é um dispositivo de divisão passiva implementado em linha entre um dispositivo de interesse e a rede.

Um toque encaminha todo o tráfego, incluindo erros de camada física, para um dispositivo de análise, permitindo que o tráfego chegue ao destino pretendido.

Aqui, o Tap envia simultaneamente o fluxo de dados de transmissão (TX) do roteador interno e o fluxo de dados de recebimento (RX) para o roteador interno em canais separados e dedicados.

Isso garante que todos os dados cheguem ao dispositivo de monitoramento em tempo real.

Os Taps são à prova de falhas, o que significa que o tráfego entre o firewall e o roteador interno não é afetado.

A captura de dados para monitoramento de rede requer que todo o tráfego seja capturado.

Técnicas especiais, como espelhamento de portas, devem ser empregadas para contornar a segmentação de rede imposta pelos switches de rede.

O espelhamento de portas permite que o switch copie quadros recebidos em uma ou mais portas para uma porta SPAN (Switch Port Analyzer) conectada a um dispositivo de análise.

A tabela identifica e descreve os termos SPAN.

Tabela 1.1. Identificação e descrição dos termos SPAN

Termo do SPAN	Descrição
Tráfego de entrada	Tráfego que entra no switch
Tráfego de saída	Tráfego que sai do switch.
Porta de origem (SPAN)	As portas de origem são monitoradas à medida que o tráfego que as insere é replicado (espelhado) para as portas de destino.
Porta de destino (SPAN)	Uma porta que espelha portas de origem. As portas SPAN de destino geralmente se conectam a dispositivos de análise, como um analisador de pacotes ou um IDS.

Fonte: do autor, 2022.

A associação entre as portas de origem e uma porta de destino é chamada de sessão SPAN.

Em uma única sessão, uma ou várias portas podem ser monitoradas.

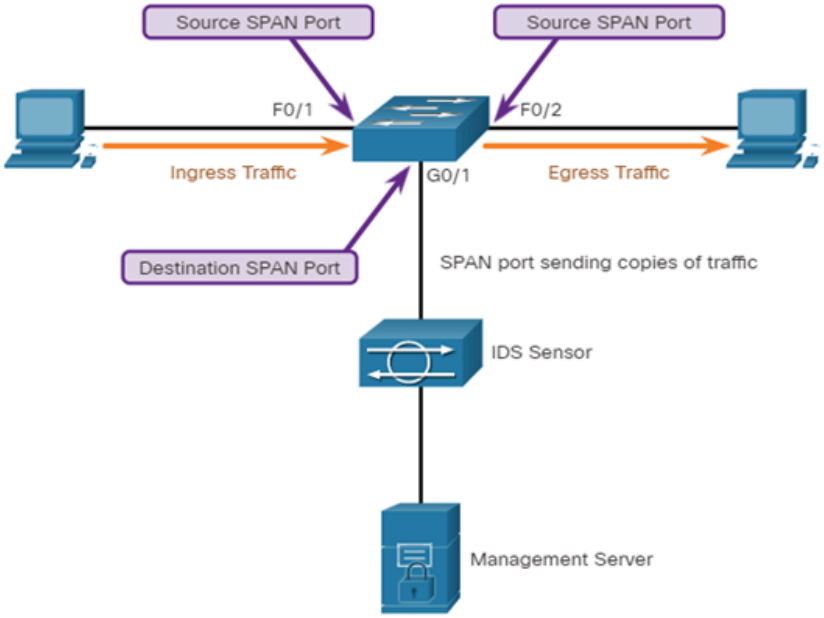
Em alguns switches Cisco, o tráfego de sessão pode ser copiado para mais de uma porta de destino.

Uma VLAN de origem pode ser especificada na qual todas as portas na VLAN de origem se tornam fontes de tráfego SPAN.

Observação: uma variação de SPAN chamada SPAN Remote SPAN (RSPAN) permite que um administrador de rede use a flexibilidade de VLANs para monitorar o tráfego em switches remotos.

Comutador interconectando dois hosts e espelhando tráfego para um IDS e Servidor de Gerenciamento de Rede.

Figura 1.2 IDS



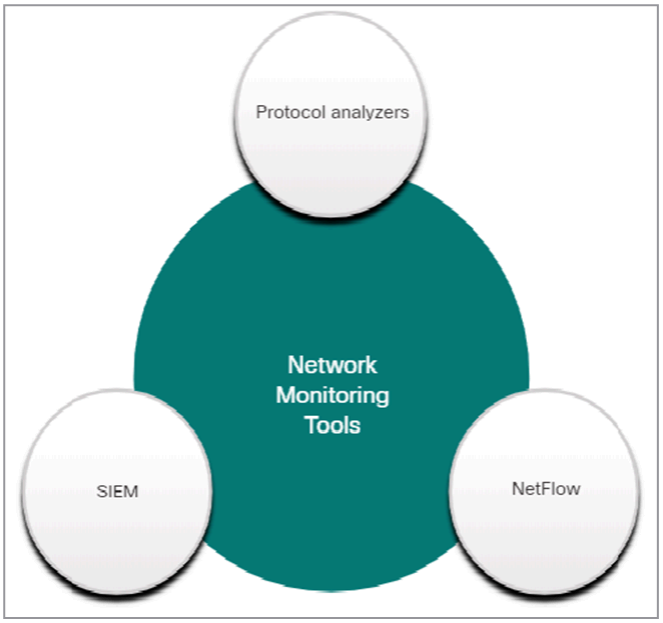
Fonte: CCNA Cyber OPS Associate v1, 2020.

1.1.1 Introdução a Ferramentas de Monitoramento

As ferramentas comuns que são usadas para monitoramento de segurança de rede incluem:

- Analisadores de protocolo de rede como Wireshark e Tcpdump
- NetFlow
- Sistemas de gerenciamento de eventos e informações de segurança (SIEM)
- É comum que os analistas de segurança confiem em arquivos de log e SNMP (Simple Network Management Protocol) para detecção de comportamento de rede.

Figura 1.3 Ferramentas de Monitoramento TAP



Fonte: CCNA Cyber OPS Associate v1, 2020.

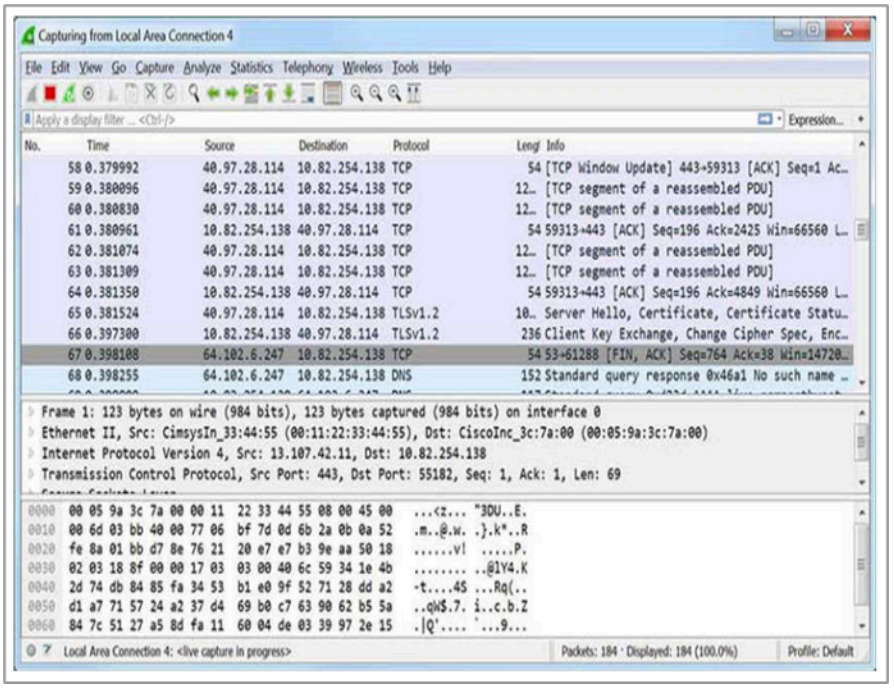
Analisadores de protocolo de rede (ou aplicativos de “sniffer de pacotes”) são programas usados para capturar tráfego.

Os analisadores de protocolo exibem o que está acontecendo na rede através de uma interface gráfica do usuário.

Os analisadores de protocolo de rede não são usados apenas para análise de segurança, mas também para solução de problemas de rede, desenvolvimento de software e protocolo e educação.

Como mostrado na figura, o Wireshark é usado em ambientes Windows, Linux e Mac OS. É uma ferramenta muito útil para aprender comunicações de protocolo de rede.

Figura 1.4 Wireshark



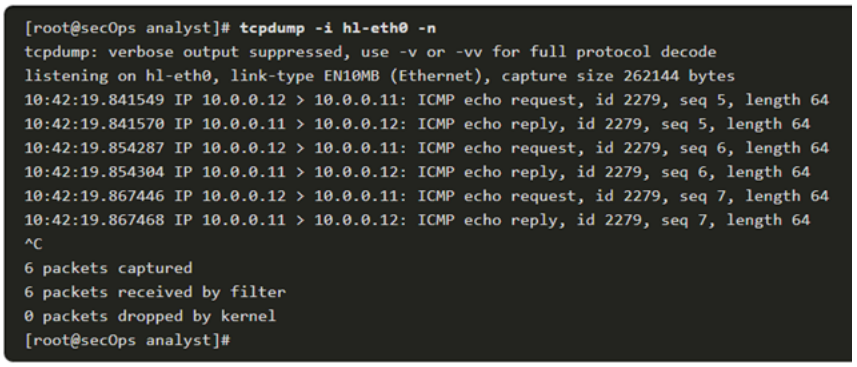
Fonte: CCNA Cyber OPS Associate v1, 2020.

Os quadros capturados pelo Wireshark são salvos em um arquivo PCAP que contém informações sobre o quadro, interface, comprimento do pacote, carimbos de data/hora e todos os arquivos binários enviados pela rede.

O Wireshark pode abrir arquivos que contenham tráfego capturado de outros softwares, como o utilitário tcpdump.

O exemplo na saída do comando exibe um exemplo de captura tcpdump de pacotes ping.

Figura 1.4 Tcpdump



Fonte: CCNA Cyber OPS Associate v1, 2020.

Observação windump é uma variante do Microsoft Windows do tcpdump.tshark, uma ferramenta de linha de comando Wireshark semelhante ao tcpdump.

Netflow

NetFlow é uma tecnologia Cisco IOS que fornece estatísticas 24 horas por dia, 7 dias por semana em pacotes que fluem através de um roteador Cisco ou switch multicamada.

NetFlow é o padrão para coletar dados operacionais IP em redes IP.

O NetFlow pode ser usado para monitoramento de rede e segurança, planejamento de rede e análise de tráfego. Ele fornece uma trilha de auditoria completa de informações básicas sobre cada fluxo de IP encaminhado em um dispositivo.

Embora o NetFlow armazene informações de fluxo em um cache local no dispositivo, ele deve sempre ser configurado para encaminhar dados para um coletor NetFlow que armazena os dados NetFlow.

O NetFlow pode monitorar a conexão de aplicativos rastreando contagens de bytes e pacotes para esse fluxo de aplicativo individual.

Ele envia as estatísticas para um servidor externo chamado coletor NetFlow.

O Cisco Stealthwatch coleta estatísticas do NetFlow para executar funções avançadas, incluindo:

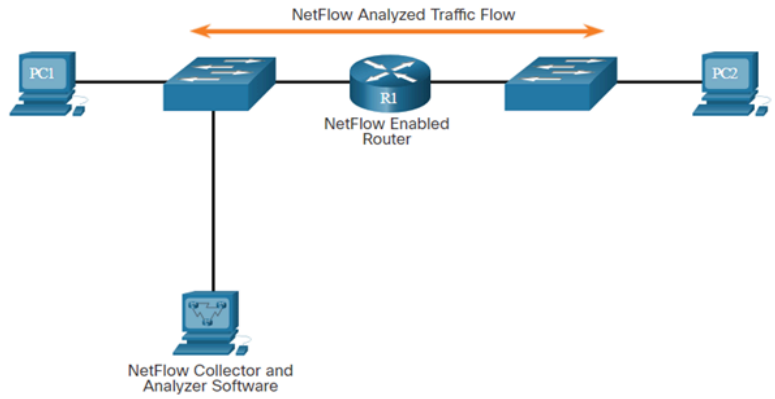
Flow stitching - Agrupa entradas individuais em fluxos.

Flow deduplication - Filtra entradas de entrada duplicadas de vários clientes NetFlow.

NAT stitching - Simplifica os fluxos com entradas NAT.

PC1 conectado ao PC2 usando HTTPS

Figura 1.4 Netflow



Fonte: CCNA Cyber OPS Associate v1, 2020.

SIEM

O SIEM (Security Information Event Management) é uma tecnologia usada em organizações empresariais para fornecer relatórios em tempo real e análise de longo prazo de eventos de segurança.

Os sistemas SIEM incluem as seguintes funções essenciais:

- Análise forense— A capacidade de pesquisar logs e registros de eventos a partir de fontes e fornecer informações completas para análise forense.
- Correlação— examina logs e eventos de diferentes sistemas ou aplicativos, acelerando a detecção e reação a ameaças de segurança.
- Agregação- Reduz o volume de dados de eventos consolidando registros de eventos duplicados.
- Relatórios- Apresenta os dados de eventos correlacionados e agregados em monitoramento em tempo real e resumos de longo prazo.

O SIEM fornece detalhes sobre a origem da atividade suspeita:

- Informações do usuário, como nome de usuário, status de autenticação, localização.
- Informações do dispositivo, como fabricante, modelo, versão do sistema operacional, endereço MAC, método de conexão de rede e localização.
- Informações de postura, como conformidade do dispositivo com a política de segurança e arquivos antivírus atualizados e patches do sistema operacional.

SOAR

Security Orchestration, Automation, and Response (SOAR) melhora o SIEM.

O SOAR ajuda as equipes de segurança a investigar incidentes de segurança e a adicionar coleta de dados aprimorada e várias funcionalidades que ajudam na resposta a incidentes de segurança.

Soluções SOAR:

- Fornece ferramentas de gerenciamento de casos que permitem que o pessoal de segurança cibernética pesquise e investigue incidentes, frequentemente integrando inteligência contra ameaças à plataforma de segurança de rede.
- Use inteligência artificial para detectar incidentes que auxiliem na análise e resposta a incidentes.
- Automatize procedimentos complexos de resposta a incidentes e investigações, que são tarefas potencialmente intensas de mão-de-obra executadas pela equipe do Centro de Operações de Segurança (SOC) executando livros de execução.
- Oferece painéis e relatórios para documentar a resposta a incidentes para melhorar os principais indicadores de desempenho do SOC e pode melhorar a segurança da rede para as organizações.
- O SOAR ajuda os analistas a responder à ameaça.

Um produto de código aberto chamado Security Onion inclui o pacote ELK para a funcionalidade SIEM.

ELK é um acrônimo para três produtos da Elastic:

- Elasticsearch - Documento orientado motor de busca de texto completo.
- Logstash - Sistema de processamento de Pipeline que conecta 'entradas' a 'saídas' com 'filtros' opcionais no meio.
- Kibana - Análise baseada em navegador e painel de pesquisa para Elasticsearch.
    - Observação: o SolarWinds Security Event Manager e o Splunk Enterprise Security são dois sistemas SIEM proprietários populares usados pelos SoCs.

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.