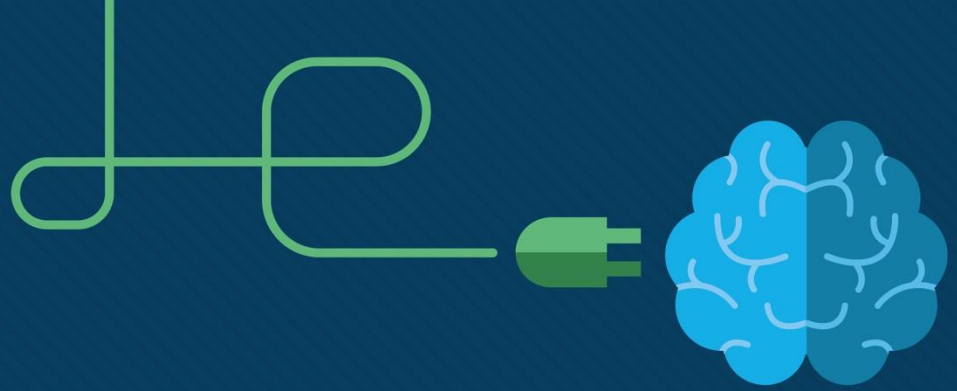


Módulo 2: Combatentes na guerra contra o crime cibernético

CyberOps Associate v1.0

Objetivos do módulo

Título do módulo: Combatentes na guerra contra o crime cibernético

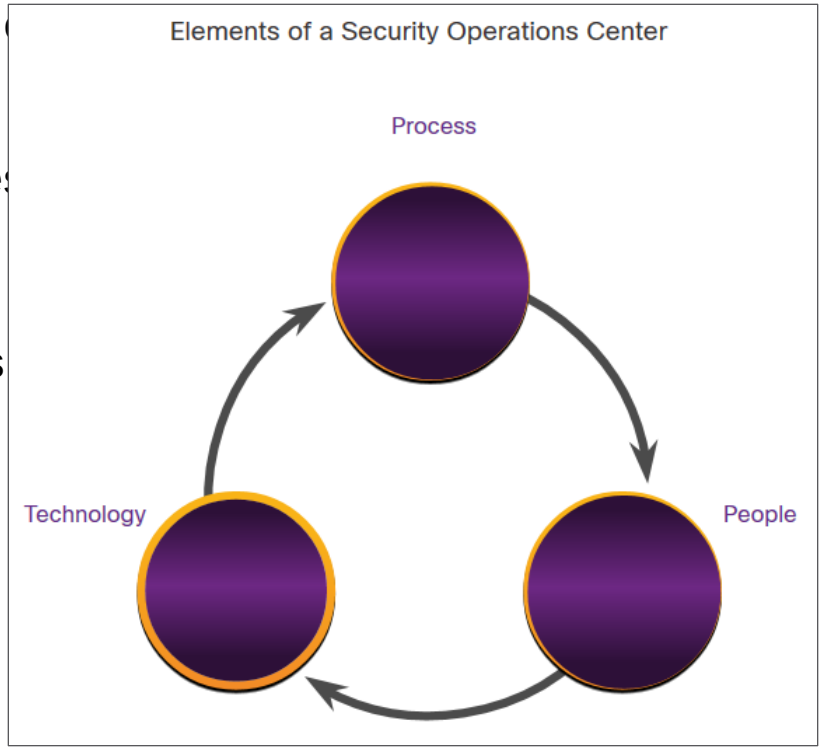
Objetivo do módulo: Explicar como se preparar para uma carreira em operações de segurança cibernética.

Título do Tópico	Objetivo do Tópico
O Centro de Operações de Segurança Moderno	Explique a missão do Security Operations Center (SOC).
Tornando-se um Defensor	Descrever os recursos disponíveis para se preparar para uma carreira nas operações da segurança cibernética.

2.1 O moderno centro de operações de segurança

Elementos de um SOC

- Para usar uma abordagem formalizada, estruturada disciplinada para se defender contra ameaças cibernéticas, as organizações geralmente usam os serviços de profissionais de um Centro de Operaçõe de Segurança (SOC).
- Os SOCs oferecem uma ampla gama de serviços, desde monitoramento e gerenciamento até soluções abrangentes de ameaças e segurança hospedada personalizada.
- 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 Serviços de Segurança Gerenciados da Cisco.



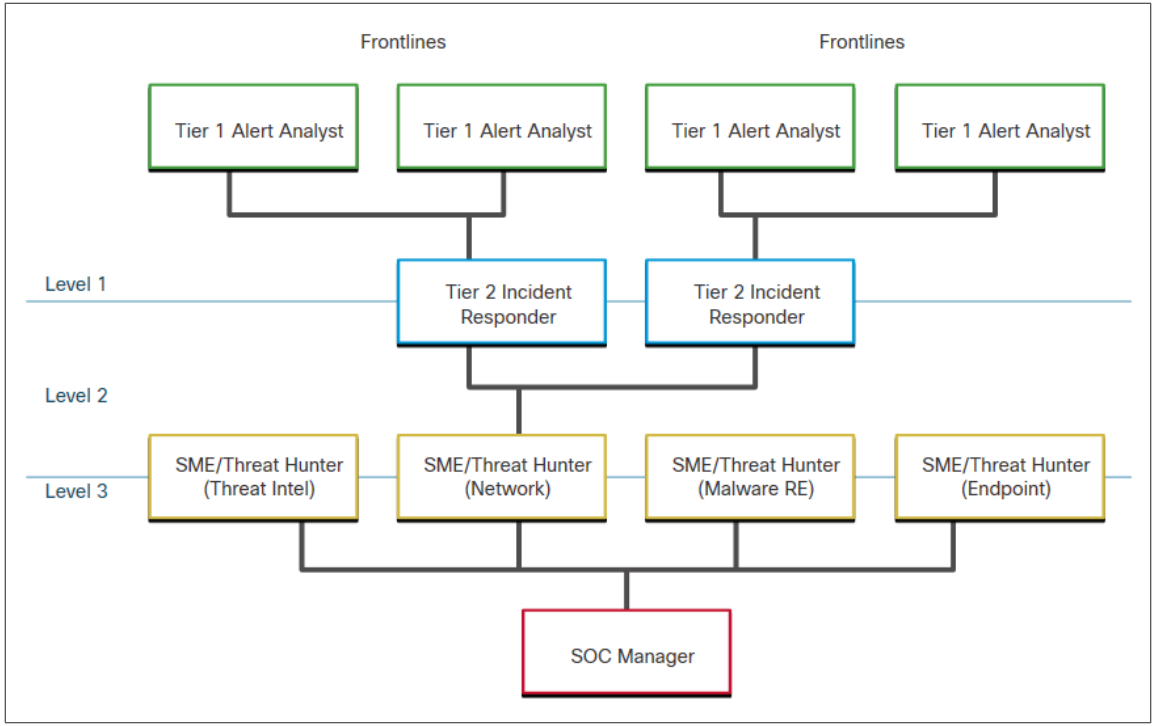
Pessoas no SOC

Os SOCs atribuem funções de trabalho por níveis, de acordo com a experiência e as responsabilidades necessárias para cada um.

Níveis	Responsabilidades
Camada 1 Analista de alerta	Monitore alertas recebidos, verifique se ocorreu um incidente verdadeiro e encaminhe tickets para o Nível 2, se necessário.
Camada 2 Respondente de Incidente	Responsável pela investigação aprofundada dos incidentes e aconselhar a remediação ou a ação a ser tomada.
Camada 3 Caçador de ameaças	Especialistas em rede, endpoint, inteligência contra ameaças, engenharia reversa de malware e rastreamento dos 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.
Gerenciador de SOC	Gerencia todos os recursos do SOC e serve como ponto de contato para a maior organização ou cliente.

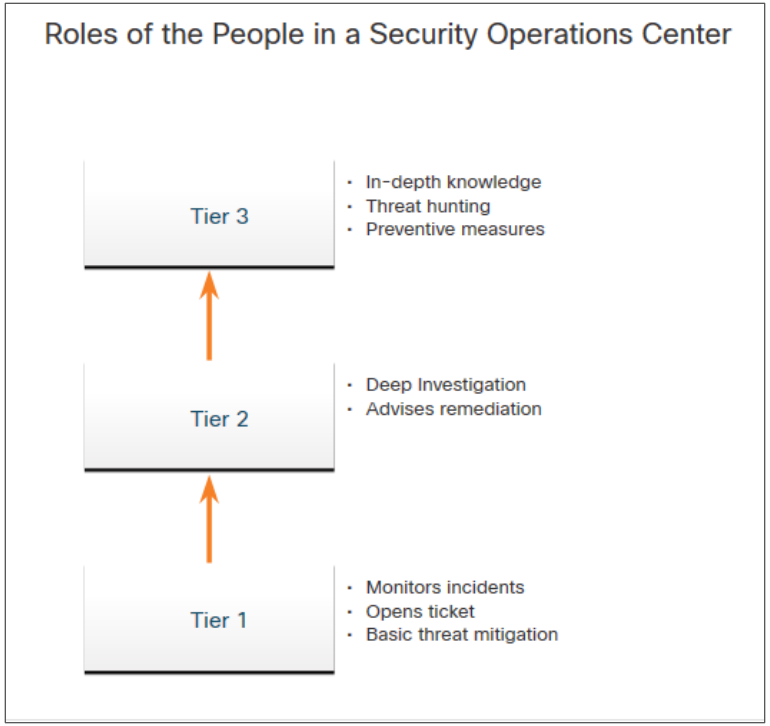
Pessoas no SOC (cont.)

- Os trabalhos de primeiro nível são mais de nível inicial, enquanto os empregos de terceiro nível exigem ampla experiência.
- A figura, que é originária do Instituto SANS, representa graficamente como essas funções interagem entre si.



Processo no SOC

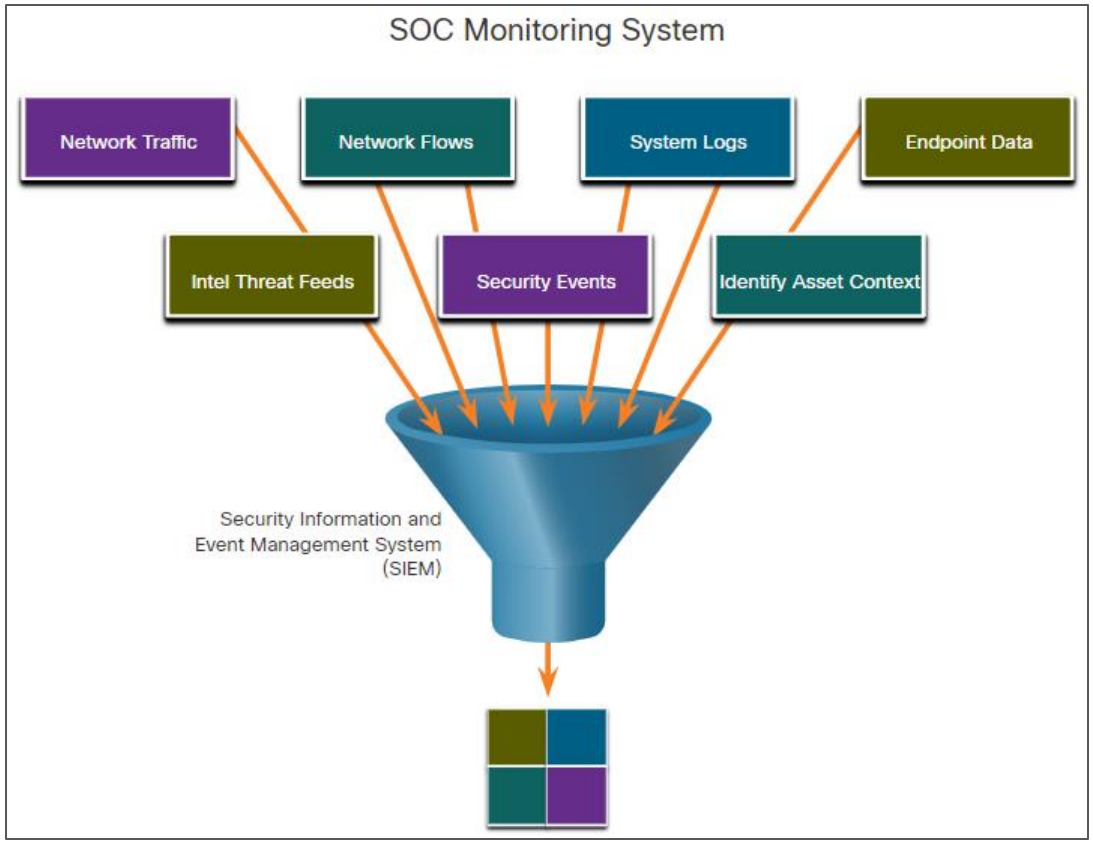
- Um analista de segurança cibernética é necessário para monitorar filas de alertas de segurança e investigar os alertas atribuídos. Um sistema de emissão de tickets é usado para atribuir esses alertas à fila do analista.
- O software que gera os alertas pode acionar alarmes falsos. O analista, portanto, precisa verificar se um alerta atribuído representa um verdadeiro incidente de segurança.
- Quando essa verificação for estabelecida, o incidente pode ser encaminhado aos investigadores ou a outro pessoal de segurança para ser tratado. Caso contrário, o alerta será descartado como um alarme falso.
- Se um tíquete não puder ser resolvido, o Analista de segurança cibernética encaminha o ticket 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 um pessoal de Nível 3.



Combatentes na Guerra contra as

Tecnologias do Cibercrime no SOC: SIEM

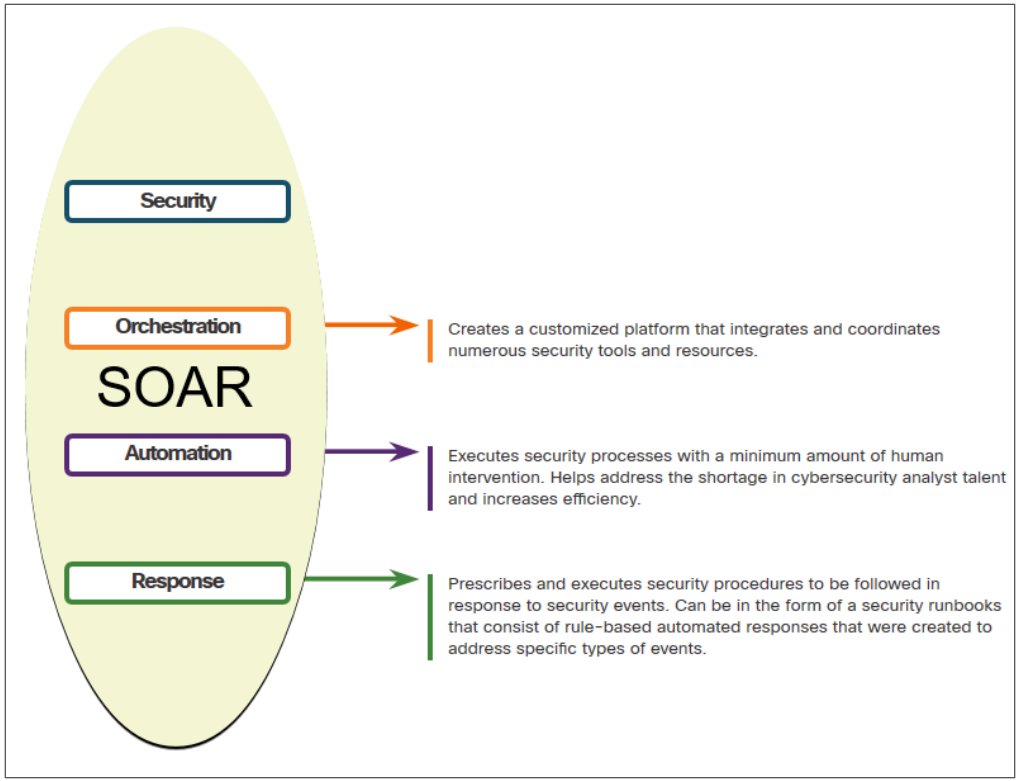
- Um SOC precisa de um sistema SIEM (*Security Information and Event Management*, gerenciamento de eventos e informações de segurança) para entender os dados gerados por *firewalls*, dispositivos de rede, sistemas de detecção de intrusões e outros dispositivos.
- Os sistemas SIEM coletam e filtram dados e detectam, classificam, analisam e investigam ameaças. Eles também podem gerenciar recursos para implementar medidas preventivas e lidar com ameaças futuras.



Combatentes na Guerra contra as

Tecnologias do Cibercrime no SOC: SOAR

- SIEM e Security Orchestration, Automation and Response (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.
- As plataformas SOAR são semelhantes às SIEMs, pois agregam, correlacionam e analisam alertas. Além disso, a tecnologia SOAR integra inteligência contra ameaças e automatiza os fluxos de trabalho de investigação e resposta de incidentes com base em manuais desenvolvidos pela equipe de segurança.



Combatentes na Guerra contra as

Tecnologias do Cibercrime no SOC: SOAR (Condd.)

- Plataformas de segurança SOAR:
  - Reúna dados de alarme de cada componente do sistema.
  - Fornecer ferramentas que permitam que os casos sejam pesquisados, avaliados e investigados.
  - Enfatize 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.
  - Inclua 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.

Métricas SOC

- Seja interno a uma organização ou fornecendo 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 KPI (Principais Indicadores de Desempenho) podem ser projetadas para medir diferentes aspectos do desempenho do SOC. No entanto, cinco métricas são comumente usadas como métricas de SOC pelos gerentes de SOC.

Métricas	Definição
Horas paradas	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
Mean Time to Detect (MTTR)	O tempo médio necessário para parar e corrigir um incidente de segurança
Tempo Médio a Conter (MTTC)	O tempo necessário para impedir que o incidente cause mais danos aos sistemas ou dados
Time to Control	O tempo necessário para parar a propagação de malware na rede

Corporativo e Segurança Gerenciada

- Para redes de médio e grande porte, a organização se beneficiará com a implementação de um SOC de nível empresarial, que é uma solução interna completa.
- Organizações maiores podem terceirizar pelo menos uma parte das operações SOC para um provedor de soluções de segurança.
- 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
    - Cisco Computer Security Incident Response Team (CSIRT)
    - Cisco Managed Services
    - Operações Táticas Cisco (TacOps)
    - Programa de Segurança Física e Segurança da Cisco

Segurança vs. Disponibilidade

- 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 garantir contra o tempo de inatividade.
- 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.

2.2 Como tornar-se um defensor

Certificações

- Uma variedade de certificações de segurança cibernética relevantes para carreiras em SOCs estão disponíveis:
  - Cisco Certified CyberOps Associate
  - Certificação de analista de segurança cibernética d
  - (ISC) ² Certificações de segurança da informação
  - Certificação Global de Garantia de Informações (GIAC)

- Procure por “certificações de segurança cibernética” na Internet para saber mais sobre certificações de outros fornecedores
e fornecedores.

Tornando-se um

Defensor Educação

- **Graus**: Ao considerar uma carreira no campo da segurança cibernética, deve-se considerar seriamente seguir um grau técnico ou bacharelado em ciência da computação, engenharia elétrica, tecnologia da informação ou segurança da informação.
- **Programação Python**: Programação por computador é uma habilidade essencial para quem deseja prosseguir uma carreira em segurança cibernética. Se você nunca aprendeu a programar, então Python pode ser a primeira língua a aprender.
- **Habilidades com 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.

Fontes de Informações

- 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 sites de empregos que reúnem listas de outros quadros de empregos e sites de carreiras de empresas e os exibem em um único local.
    - Indeed.com
    - CareerBuilder.com
    - USAJobs.gov
    - Porta de vidro
    - Linkedin

Torne-se um defensor

obtendo

- **Estágios: Os**estágios são um excelente método para entrar no campo da 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
- **Bolsas de estudo e prêmios**: Para ajudar a fechar a lacuna de habilidades de segurança, organizações como Cisco e INFOSEC introduziram programas de bolsas de estudo e prêmios.
- **Agências Temporárias**: Muitas organizações usam agências temporárias para preencher vagas nos primeiros 90 dias. Se o funcionário for uma boa correspondência, a organização pode converter o funcionário em uma posição permanente em tempo integral.
- **Seu primeiro trabalho:** se você não tem experiência no campo da segurança cibernética, trabalhar em um call center ou suporte técnico pode ser o primeiro passo para ganhar a experiência de que precisa para seguir em frente em sua carreira.

2.3 Resumo de soldados na guerra contra o crime digital

O que aprendi neste módulo?

- Os principais elementos do SOC incluem pessoas, processos e tecnologias.
- As funções de trabalho incluem um Analista de Alerta de Nível 1, um Respondente a Incidentes de Nível 2, um caçador de ameaças de Nível 3 e um Gerente de SOC.
- Um analista de nível 1 monitora incidentes, abre tickets e executa mitigação básica de ameaças.
- Os sistemas SEIM são usados para coletar e filtrar dados, detectar e classificar ameaças e analisar e investigar ameaças.
- O SOAR integra informações sobre ameaças e automatiza os fluxos de trabalho de investigação e resposta de incidentes com base em manuais desenvolvidos pela equipe de segurança.
- Os KPIs são criados para medir diferentes aspectos do desempenho do SOC.Métricas comuns incluem tempo de espera, tempo médio para detectar (MTTD), tempo médio para responder (MTTR), tempo médio para conter (MTTC) e tempo para controle.

O que aprendi neste módulo? (Continuação)

- Deve haver um equilíbrio entre a segurança e a disponibilidade das redes. A segurança não pode ser tão forte que interfira com funcionários ou funções de negócios.
- Uma variedade de certificações de segurança cibernética que são relevantes para carreiras em SOCs estão disponíveis de diferentes organizações.

New Terms and Commands

• Security Operations Center (SOC) • Cybersecurity Analyst • CyberOps Associate • Tier 1 Alert Analyst • Tier 2 Incident Responder • Tier 3 Threat Hunter • SOC Manager	• Security Information and Event Management (SIEM) system • Security Orchestration, Automation and Response (SOAR) • Key Performance Indicators (KPI)	• Dwell Time • Mean Time to Detect (MTTD) • Mean Time to Detect (MTTD) • Mean Time to Contain (MTTC) • Time to Control • Job site aggregators • Temporary agencies

Referências

- https://www.youtube.com/watch?v=YVQriOVHl18&t=296s
- https://www.youtube.com/watch?v=Jynck9Yw_dg
- https://logz.io/blog/open-source-siem-tools/


CISCO