Qual função de trabalho SOC gerencia todos os recursos do SOC e serve como um ponto de contato para a organização ou cliente maior?

Gerenciador SOC

Qual função de trabalho SOC processa alertas de segurança e encaminha tickets para o nível 2, se necessário?

Analista de segurança cibernética

Qual função de trabalho SOC é responsável pela investigação profunda de incidentes?

Responsável pela resposta a incidentes

Qual dispositivo integra informações de segurança e gerenciamento de eventos em uma única plataforma?

SIEM

Qual dispositivo integra ferramentas e recursos de orquestração para responder automaticamente a eventos de segurança?

SOAR

A qual pessoal de um SOC tem a tarefa de verificar se um alerta acionado pelo software de monitoramento representa um verdadeiro incidente de segurança?

Pessoal de nível 1

Tópico 2.1.0 - Em um SOC, o trabalho de um Analista de Alerta de Nível 1 inclui o monitoramento de alertas recebidos e a verificação de que um verdadeiro incidente de segurança ocorreu.

Depois que um incidente de segurança é verificado em um SOC, um respondedor de incidentes revisa o incidente, mas não consegue identificar a origem do incidente e formar um procedimento de mitigação eficaz. A quem o tíquete de incidente deve ser escalado?

Uma PME para investigação mais aprofundada

Tópico 2.1.0 - Um respondente a incidentes é um profissional de segurança de nível 2 em um SOC. Se o respondente não puder resolver o tíquete de incidente, o tíquete de incidente deve ser encaminhado para o próximo nível de suporte, um Camada 3.Uma PME de nível 3 investigaria mais aprofundadamente o incidente.

Quais dois serviços são fornecidos pelos centros de operações de segurança? (Escolha duas.)

Gerenciamento de soluções abrangentes de ameaças

Monitoramento de ameaças de segurança de rede

Tópico 2.1.0 - Os Centros de Operações de Segurança (SOCs) podem fornecer uma ampla gama de serviços para se defender contra ameaças aos sistemas de informação de uma organização. Esses serviços incluem monitoramento de ameaças à segurança de rede e gerenciamento de soluções abrangentes para combater ameaças. Garantir trocas de roteamento seguras e fornecer conexões seguras à Internet são tarefas normalmente executadas por um centro de operações de rede (NOC). Responder a invasões de instalações é normalmente a função e responsabilidade do departamento de polícia local.

Qual métrica é usada em SOCs para avaliar o tempo médio necessário para identificar que ocorreram incidentes de segurança válidos na rede?

MTTD

Tópico 2.1.0 - Os SOCs usam muitas métricas como indicadores de desempenho de quanto tempo o pessoal leva para localizar, interromper e corrigir incidentes de segurança.

Horas paradas

Tempo Médio para Detectar (MTTD)

Tempo médio de resposta (MTTR)

Tempo Médio para Conter (MTTC)

Tempo para o controle

Qual métrica de KPI o SOAR usa para medir o período de tempo que os atores da ameaça têm acesso a uma rede antes de serem detectados e o acesso dos atores da ameaça ser interrompido?

Horas paradas

Tópico 2.1.0 - As métricas comuns do indicador de desempenho (KPI) compiladas pelos gerentes de SOC são as seguintes:

• Tempo de permanência: o período de tempo que os atores da ameaça têm acesso a uma rede antes de serem detectados e o acesso dos atores da ameaça interrompido

• Mean Time to Detect (MTTD): o tempo médio que o pessoal do SOC leva para identificar incidentes de segurança válidos ocorreu na rede

• Mean Time to Responder (MTTR): o tempo médio necessário para parar e corrigir um incidente de segurança

• Mean Time to Conter (MTTC): o tempo necessário para impedir que o incidente cause mais danos aos sistemas ou dados

Qual é a função do SIEM?

Para analisar todos os dados que firewalls, appliances de rede, sistemas de detecção de intrusões e outros dispositivos geram e instituem medidas preventivas

Tópico 2.1.0 - Um sistema de gerenciamento de eventos e informações de segurança (SIEM) faz sentido a todos os dados gerados por firewalls, dispositivos de rede, sistemas de detecção de intrusões e outros dispositivos. Os SIEMs 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.

O que é uma característica da plataforma de segurança SOAR?

Para incluir playbooks predefinidos que permitem a resposta automática a ameaças específicas

Tópico 2.1.0 - As plataformas de segurança SOAR oferecem os seguintes recursos:

• Recolher 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

Um profissional de segurança de rede solicitou uma posição de Nível 2 em um SOC. O que é uma função de trabalho típica que seria atribuída a um novo funcionário?

Investigar mais incidentes de segurança

Tópico 2.1.0 - Em um SOC típico, o trabalho de um respondedor de incidentes de Nível 2 envolve investigação aprofundada de incidentes de segurança.

Se um SOC tiver uma meta de 99,99% de tempo de atividade, quantos minutos de tempo de inatividade por ano seriam considerados dentro de sua meta?

52.56

Tópico 2.1.0 - Dentro de um ano, há 365 dias x 24 horas por dia x 60 minutos por hora = 525.600 minutos. Com a meta de tempo de atividade 99,99% do tempo, o tempo de inatividade precisa ser controlado sob 525.600 x (1-0,9999) = 52,56 minutos por ano.

Qual organização oferece a certificação CySA+ neutra do fornecedor?

CompTIA

Tópico 2.2.0 - A certificação CompTIA Cybersecurity Analyst (CySA+) é uma certificação profissional de segurança neutra no fornecedor.

Na operação de um SOC, qual sistema é freqüentemente usado para permitir que um analista selecione alertas de um pool para investigar?

Sistema de emissão de bilhetes

Tópico 2.1.0 - Em um SOC, um sistema de tickets é normalmente usado para um sistema de gerenciamento de fluxo de trabalho.

Como um sistema de gerenciamento de eventos e informações de segurança em um SOC pode ser usado para ajudar o pessoal a lutar contra ameaças à segurança?

Coletando e filtrando dados

Tópico 2.1.0 - Um sistema de gerenciamento de eventos e informações de segurança (SIEM) combina dados de várias fontes para ajudar o pessoal da SOC a coletar e filtrar dados, detectar e classificar ameaças, analisar e investigar ameaças e gerenciar recursos para implementar medidas preventivas.

Quais três tecnologias devem ser incluídas em um sistema de gerenciamento de eventos e informações de segurança em um SOC? (Escolha três.)

Inteligência de ameaças

Rastreamento de vulnerabilidades

Monitoramento da segurança

Tópico 2.1.0 - As tecnologias em um SOC devem incluir o seguinte:

Coleta, correlação e análise de eventos

Monitoramento de segurança

Controle de segurança

Gerenciamento de log

Avaliação de vulnerabilidade

Controle de vulnerabilidades

Inteligência de ameaças

Os appliances de firewall, VPNs e IPS são dispositivos de segurança implantados na infra-estrutura de rede.

Um invasor envia um pedaço de malware como anexo de email para funcionários de uma empresa. Qual é o propósito provável do ataque?

Busca e obtenção de segredos comerciais

O que é guerra cibernética?

É um ataque destinado a pertubar, corromper ou explorar interesses nacionais

Que tipo de malware tem o objetivo principal de se espalhar pela rede?

worm

Qual é o risco potencial ao usar um hotspot sem fio gratuito e aberto em um local público?

O tráfego da rede pode ser sequestrado e as informações roubadas

A pedido dos investidores, uma empresa está procedendo com a atribuição cibernética com um ataque particular que foi conduzido a partir de uma fonte externa. Qual termo de segurança é usado para descrever a pessoa ou dispositivo responsável pelo ataque?

Ator de ameaça

Que nome é dado a um hacker amador?

Hacker inexperiente

O que normalmente motiva os cibercriminosos a atacar redes em comparação com hacktivistas ou hackers patrocinados pelo estado?

Ganho financeiro

O que é um botnet?

Uma rede de computadores infectados que são controlados como um grupo

O que é um hotspot sem fio desonesto?

É um ponto de acesso que parece ser de um negócio legítimo, mas foi realmente criado por alguém sem a permissão do negócio

Qual é a melhor definição de informações de identificação pessoal (PII)?

Dados coletados pelas empresas para distinguir identidades de indivíduos

O que foi usado como arma de guerra cibernética para atacar uma instalação de enriquecimento de urânio no Irã?

Stuxnet

Uma empresa paga uma quantia significativa de dinheiro aos hackers, a fim de recuperar o controle de um servidor de e-mail e dados. Que tipo de ataque de segurança foi usado pelos hackers?

Ramsomware

Quais são as três categorias principais de elementos em um centro de operações de segurança? (Escolha três.)

Pessoas

Processos

Tecnologias

A qual pessoal de um SOC é atribuída a tarefa de procurar ameaças em potencial e implementar ferramentas de detecção de ameaças?

Camada 3 SME

Corresponda a métrica SOC à descrição. (Nem todas as opções são usadas).

tempo necessário para impedir que o incidente cause mais danos aos sistemas ou dados - MTTC

período de tempo em que os atores da ameaça têm acesso a uma rede antes de seu acesso ser interrompido – Dwell Time

​tempo médio para identificar que ocorreram incidentes de segurança válidos na rede - MTTD

​​tempo médio necessário para parar e corrigir um incidente de segurança – MTTR

Um SOC está procurando um profissional para preencher uma vaga de emprego. O funcionário deve ter habilidades de nível especializado em rede, endpoint, inteligência contra ameaças e engenharia reversa de malware para procurar ameaças cibernéticas ocultas na rede. Qual trabalho dentro de um SOC requer um profissional com essas habilidades?

Caçador de ameaças

Qual organização é uma organização internacional sem fins lucrativos que oferece a certificação CISSP?

(ISC2)

O termo analista de operações cibernéticas se refere a qual grupo de funcionários em um SOC?

Pessoal de nível 1

Qual trabalho exigiria a verificação de que um alerta representa um verdadeiro incidente de segurança ou um falso positivo?

Analista de alerta

Qual é o benefício de uma organização usar o SOAR como parte do sistema SIEM?

O SOAR automatiza a investigação de incidentes e responde a fluxos de trabalho com base em playbooks.

Quais são as três tecnologias que devem ser incluídas em um sistema de gerenciamento de eventos e informações de segurança SOC? (Escolha três.)

Inteligência de log

Gerenciamento de log

Monitoramento de segurança

Como um sistema de gerenciamento de eventos e informações de segurança (SIEM) em um SOC ajuda o pessoal a lutar contra as ameaças à segurança?

combinando dados de várias tecnologias

Que tipo de arma de guerra cibernética era Stuxnet?

Worm

Um funcionário se conecta sem fio à rede corporativa com um telefone celular. O funcionário configura o telefone celular para atuar como um ponto de acesso sem fio que permite que novos funcionários se conectem à rede corporativa. Que tipo de ameaça à segurança melhor descreve essa situação?

ponto de acesso invasor

Qual ataque cibernético envolve um ataque coordenado de uma botnet de computadores zumbis?

DDos

Quando um usuário liga o PC na quarta-feira, o PC exibe uma mensagem indicando que todos os arquivos do usuário foram bloqueados. Para obter os arquivos não criptografados, o usuário deve enviar um e-mail e incluir uma ID específica no título do e-mail. A mensagem também inclui maneiras de comprar e enviar bitcoins como pagamento para a descriptografia do arquivo. Depois de inspecionar a mensagem, o técnico suspeita que ocorreu uma violação de segurança. Que tipo de malware poderia ser responsável?

Ransomware

Qual exemplo ilustra como o malware pode ser escondido?



Um e-mail é enviado para os funcionários de uma empresa com um anexo que se parece com uma atualização de antivírus, mas na verdade consiste em um spyware.

O que é a Dark Web?

É parte da internet que só pode ser acessado com software especial.

Uma empresa acaba de ter um incidente de segurança cibernética. O ator da ameaça parecia ter um objetivo de interrupção da rede e parecia usar uma ferramenta comum de hack de segurança que sobrecarregava um determinado servidor com uma grande quantidade de tráfego. Esse tráfego tornou o servidor inoperável. Como um analista certificado de segurança cibernética classificaria esse tipo de ator de ameaças?

Amador

Um grupo de usuários na mesma rede está reclamando de seus computadores rodando lentamente. Depois de investigar, o técnico determina que esses computadores fazem parte de uma rede zumbi. Que tipo de malware é usado para controlar esses computadores?

Botnet

Qual declaração descreve a guerra cibernética?

É um conflito baseado na Internet que envolve a penetração das redes e sistemas de computador de outras nações.

Quais sites um usuário deve evitar ao se conectar a um hotspot sem fio gratuito e aberto?

sites para fazer compras