

Introdução

- "Red Team": segurança ofensiva - ataque ("ethical hacking", "penetration testing")
- "Blue Team": segurança defensiva - proteção (resposta a incidentes, análise forense)
- "Purple Team": integração de táticas defensivas com resultados ofensivos
 - recolha de dados e implementação

Centro de Operações de Segurança (SOC): equipa composta essencialmente por analistas de segurança organizados para detectar, analisar, responder a, reportar sobre e prevenir incidentes de cibersegurança

→ Um SOC fornece defesa contra atividade não autorizada em redes de computadores, incluindo atividades de monitorização, deteção, análise (de tendências e padrões), resposta e restauração

Quais as funções principais?

1. Identificar
2. Proteger
3. Detectar
4. Responder
5. Recuperar

Qual a coisa mais importante?

1. Conhecer o eleitorado
2. Imaginar como pode ser atacado
3. Encontrar os meios para o defender

Serviços Reativos:

1. Monitorizar Postura de Segurança
2. Fimção de Comando
3. Iniciar e Gerir Resposta a Incidente
4. Gestão de Vulnerabilidades
5. Forense / Descoberta
6. Relatórios
7. Análise de Malware
8. Detecção de Intrusões
9. Auditoria / Avaliação

Serviços Proativos:

1. Monitorização de Segurança da Rede
2. Casa de Ameaças
3. Monitorização da Saúde da Plataforma e Apoio
4. Inteligência de Ciberameaças
5. Integração de Inteligência de Ameaças

Analista do SOC: classifica o alerta, procura a causa e recomenda medidas de remediação

- Nível 1: monitorização diária 24/7; investigação e mitigação básicas
- Nível 2: investigação detalhada dos sistemas que levantam alertas escalados por 1
- Nível 3: investigação avançada (CSIRT); prevenção; forense; casa de ameaças

Respondente a Incidente: realiza a avaliação inicial de violações de segurança

Casa das Ameaças: investiga proativamente potenciais ameaças/vulnerabilidades

Engenheiro de Segurança: mantém a infraestrutura de soluções SIEM e SOAR

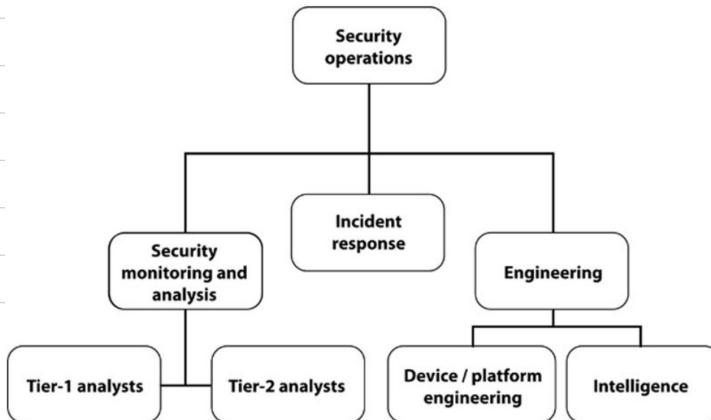
Gestor do SOC: assume responsabilidades de gestão tais como orçamentos, estratégias, gestão de pessoal e coordenação de operações

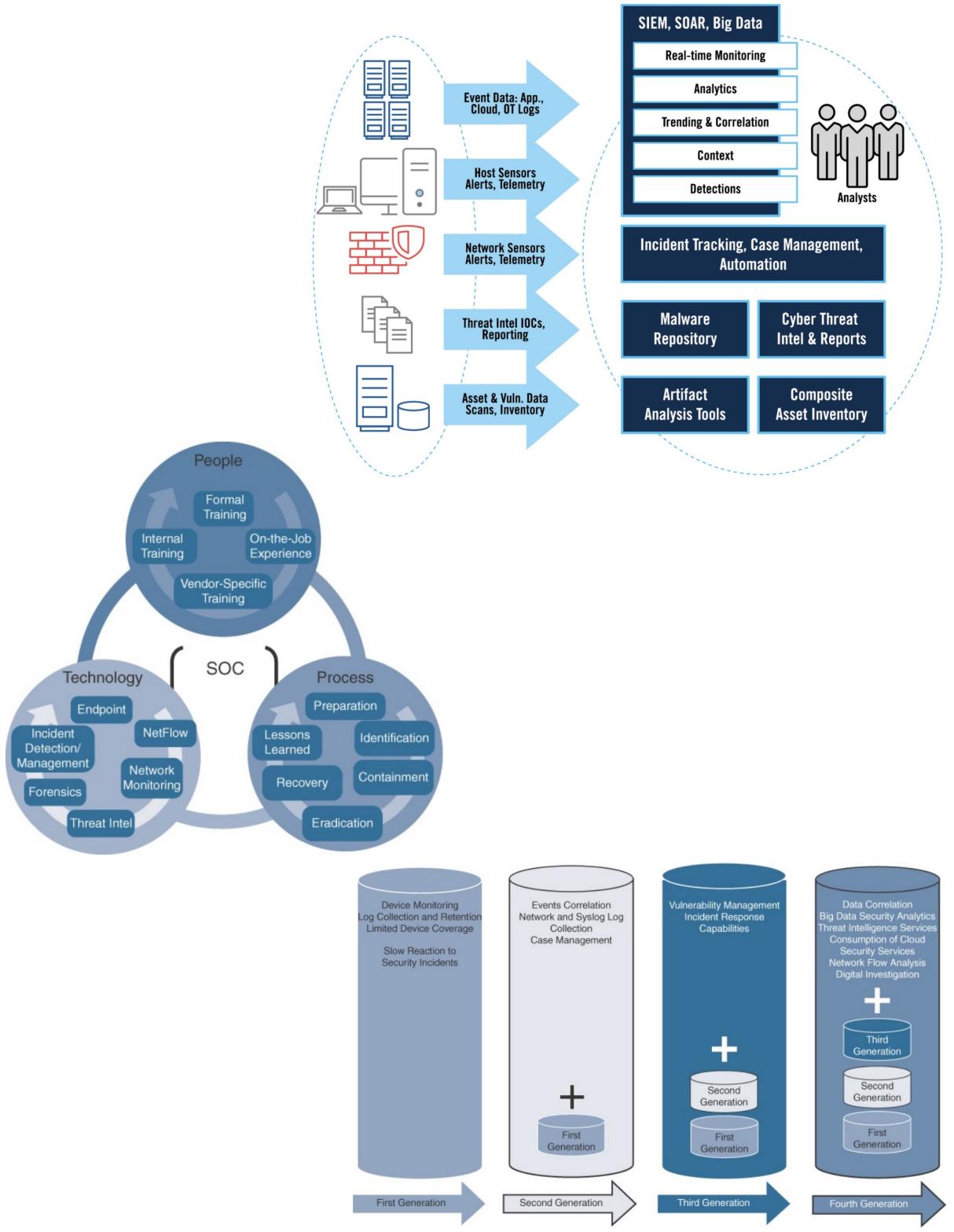
Quais os desafios?

1. demasiados alertas de segurança
2. rastrear os cibercrimes
3. modificações e reconfigurações depois de cada violação
4. escassez de conhecimento
5. falta de ferramentas apropriadas, integração e automação

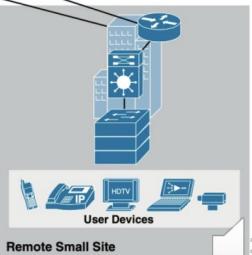
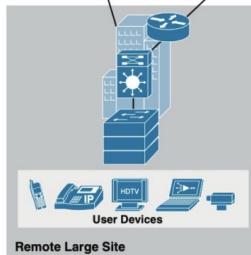
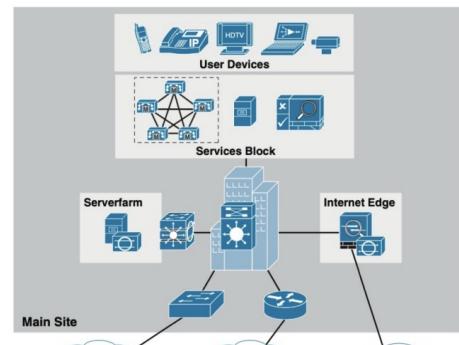
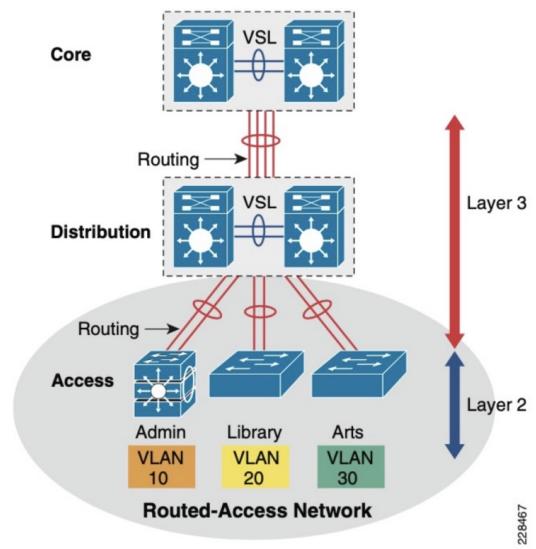
Madureza dos Programas SOC:

1. Primeira Geração: só monitoriza logs dos dispositivos, pelo que tem conhecimento limitado baseado nos dados que não monitorizados
2. Segunda Geração: correlaciona e consolida logs para transformar dados em eventos de segurança, simplificando a monitorização e melhorando a resposta a incidentes
3. Terceira Geração: tem mais experiência com capacidades do SOC e é capaz de gerenciar mais serviços, como gestão de vulnerabilidades e conformidade
4. Quarta Geração: tem as tecnologias e os serviços mais recentes, alinha as ferramentas e expande a visibilidade para outras redes através de inteligência de ameaças, reputação de segurança e serviços na nuvem



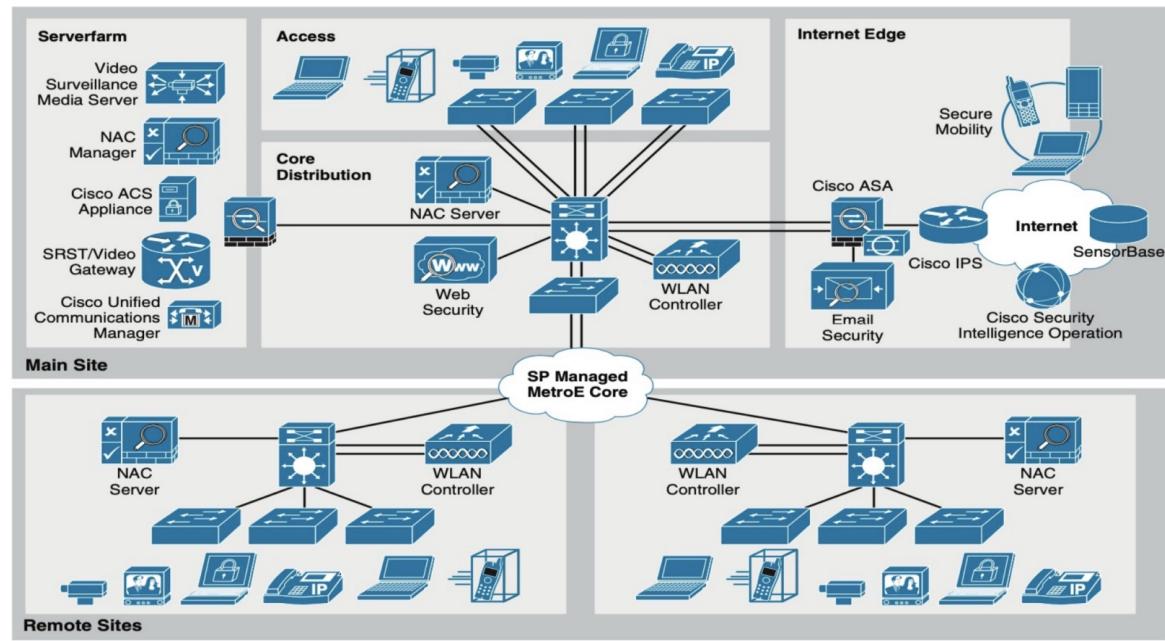


Typical SME architecture



3

Typical SME architecture – more detail



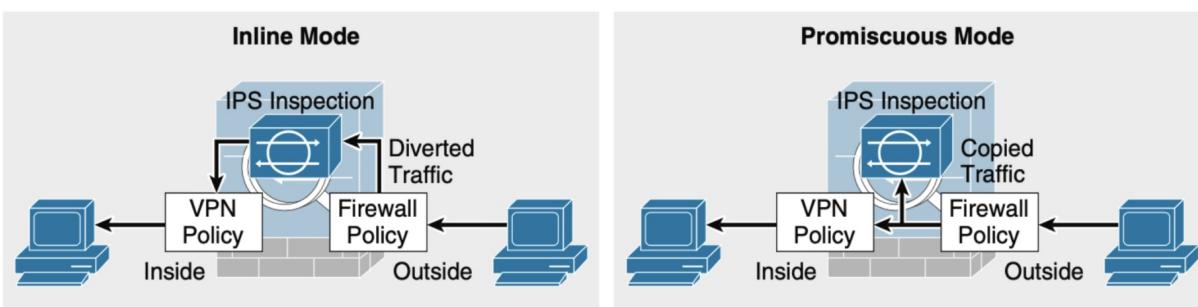
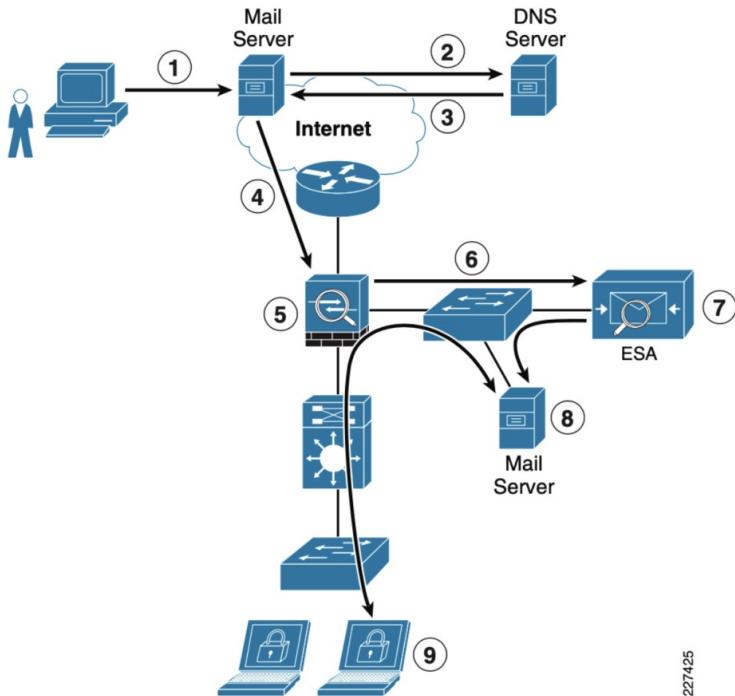
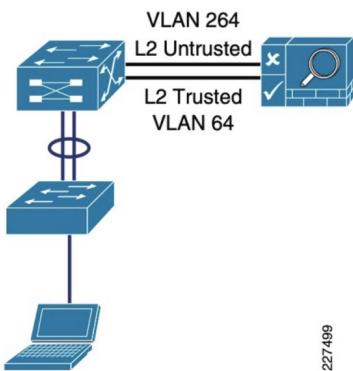


Figure 5-7 Typical Data Flow for Inbound E-mail Traffic



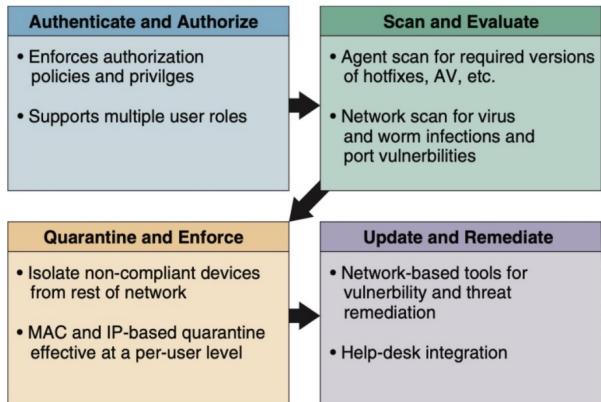
227425

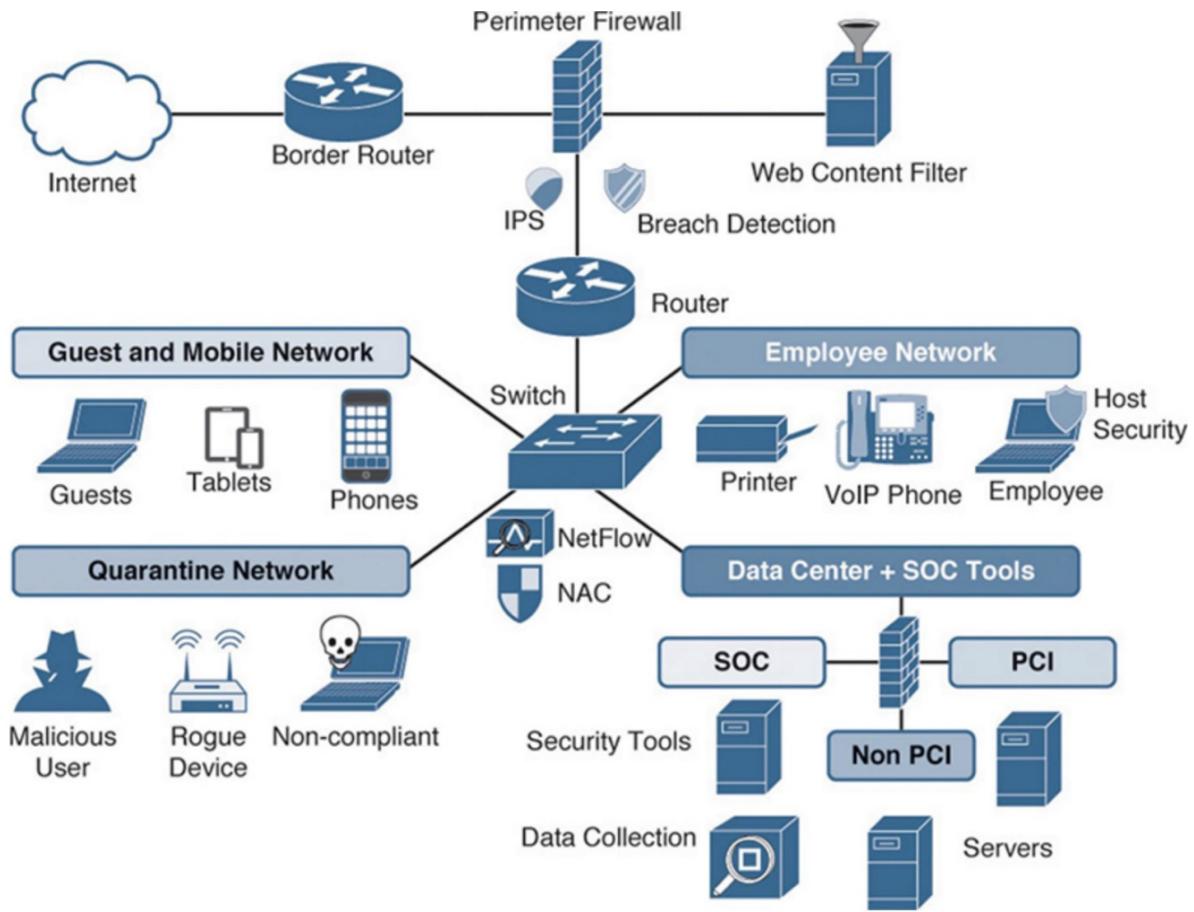
Figure 5-18 Layer 2 OOB Topology

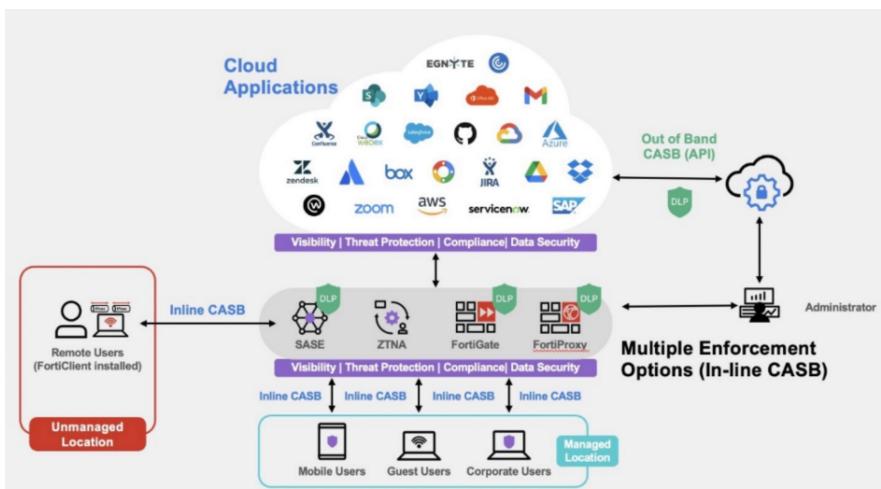
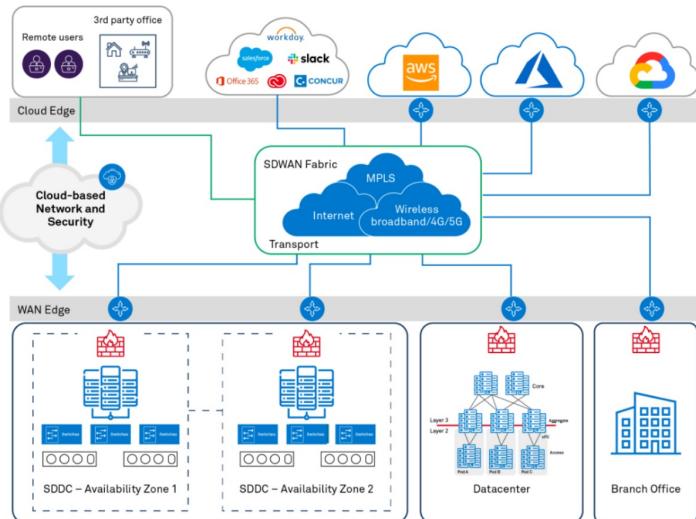
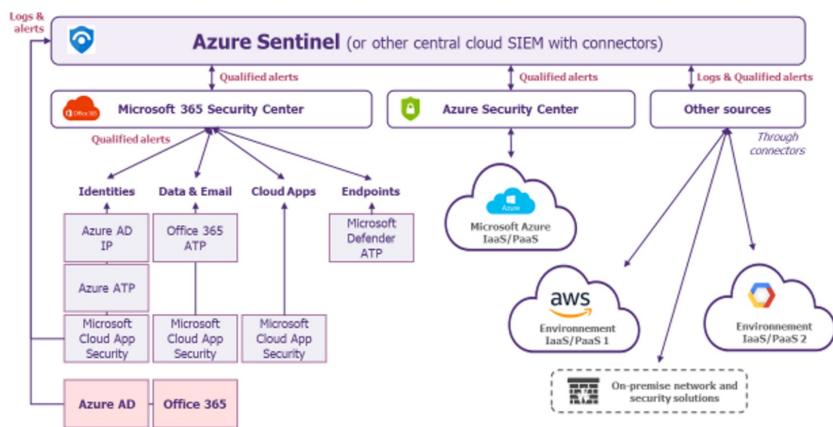


227499

Figure 5-19 The Four Functions of the NAC Framework

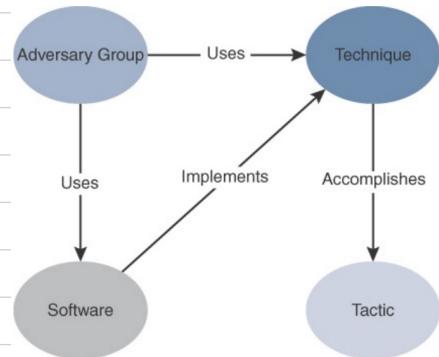






MITRE ATT&CK

Framework MITRE ATT&CK: modelo de deteção de intrusos compreensivo e baseado no conhecimento que mapeia as táticas, técnicas e procedimentos (TTPs) dos usados/usados pelos cibercorrentes - contexto e linguagem comum



Tática: objetivo técnico do adversário

Técnica: como o adversário alcança o objetivo

Procedimento: o que o adversário faz

Advanced Persistent Threat (APT): cibercoriente sofisticado e sustentado no qual um intruso estabelece uma presença não detectada numa rede de maneira a roubar dados sensíveis durante um período prolongado de tempo - ataque cuidadosamente planeado e desenhado para infiltrar numa organização específica, escapar a medidas de segurança existentes e passar despercebido

Objetivos: cibercoriente; hacking; destruição; ganho financeiro

Fases:

1. Infiltração
2. Escalação e Movimento Lateral
3. Exfiltração

Logs, Eventos e Alertas

Log: forma mais básica de informação que um sistema pode gerar — regista informação básica sobre algo que aconteceu

1. Quem?
2. O que?
3. Quando?
4. Onde?
5. Porque?

Tipos de Fontes: 1. Aplicação 2. Ambiente 3. Rede 4. Nuvem

Fontes:

1. IAM e Controles de Segurança
2. Infraestrutura de Rede
3. Informação da Infraestrutura e de Negócios Não-Log

Evento: input para um SOC que tem de ser filtrado e revisado para determinar se requer mais investigação ou análise — pode ser um log, mas com contexto específico

Alerta: evento graduado e/ou de interesse que tipicamente dispara uma notificação pré-configurada ou alarme porque algo alcançou um nível específico e requer atenção por uma pessoa responsável com as ferramentas apropriadas e autoridade para investigar — eventos suficientemente críticos para requererem algum nível de atenção

1. Falso Positivo: as ferramentas identificam incorretamente um evento preocupante
2. Verdadeiro Positivo: as ferramentas identificam corretamente um evento preocupante
3. Falso Negativo: as ferramentas incorretamente não identificam um evento preocupante
4. Verdadeiro Negativo: as ferramentas corretamente não identificam um evento não

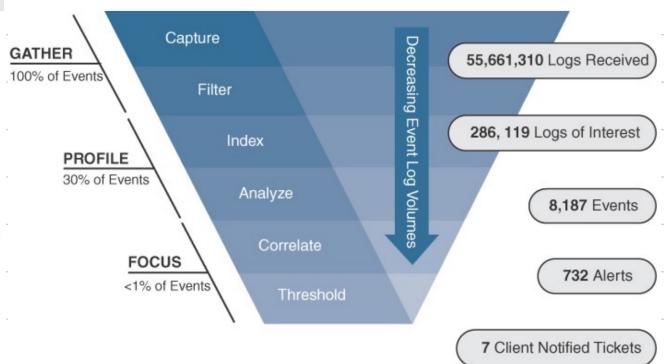
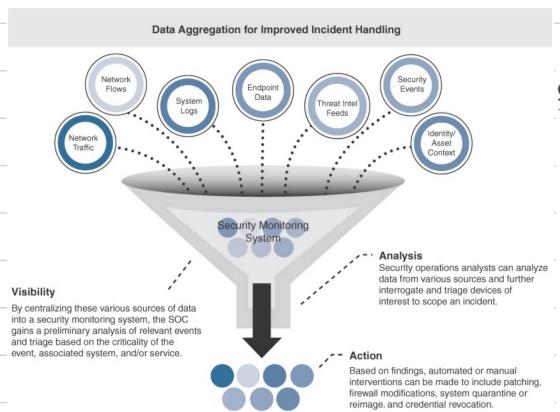
Use Cases

Use Case: conjunto de ações ou passos que definem as interações entre um ator, que pode ser uma pessoa, sistema ou serviço, e um sistema de modo a alcançar um objetivo particular

1. Compreender como mapear numa ou apoiar uma capacidade do negócio ou requisito
2. Projetar a questão que deve responder
3. Determinar e testar as fontes e os elementos de dados que dão a visibilidade necessária
4. Avaliar os dados ao estabelecer linhas de base normais e outras análises
5. Estabelecer os guias e processos que o SOC vai utilizar para filtrar casos
6. Visualizar os dados através de várias técnicas
7. Construir regras de correlação a partir de várias fontes de dados

Tipo {
1. Técnico
2. Lógica de Negócios
3. Comportamental

⚠ EXEMPLO DE USE CASE ⚠



Cyber Threat Intelligence

O contexto é a chave — um indicador sem o contexto necessário não diz muito, mas, com contexto, dá uma ideia da sua urgência, relevância e prioridade relativa

→ Ciber-Ameaça

Dark Web: mercados para ameaças emergentes — para compreender melhor o ambiente de ameaças e as tendências cibercriminosas

Type Squatting/Domain Abuse/URL Hijacking: a prática de registrar domínios de marcas conhecidas com o intuito de levar utilizadores a ver que não sites legítimos

→ Indicadores de Compromisso:

1. pegadas digitais que revelam como o modo de operação de um atacante
2. valores de hash associados com ficheiros maliciosos conhecidos
3. endereços IP perigosos conhecidos ou associados com atividades não normais
4. código/softwarcne malicioso que se pode encontrar nos dispositivos, na rede, ..

MISP: solução de software open-source para recolher, armazenar, distribuir e partilhar indicadores de cibersegurança, ameaças sobre incidentes de cibersegurança e análise de malware — o objetivo é fomentar a partilha de informação estruturada com a comunidade de cibersegurança



A Análise F orense D igital

Análise Forense Digital: o uso de métodos provados e derivados científicamente direcionados para a preservação, recolha, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais derivadas de fontes digitais com o propósito de facilitar a reconstrução de eventos determinados criminosos ou ajudar a antecipar ações não autorizadas demonstradas como sendo disruptivas às operações planeadas.

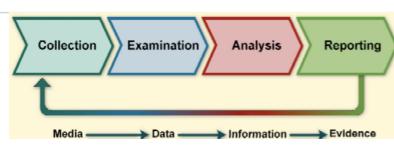
1. Recolha: depois de uma fuga, investigadores recolhem dados de SDs, contas de utilizador, dispositivos móveis e outros ativos de hardware e software acessados pelos atacantes — não feitas cópias de dados antes de os processar para preservar a integridade das evidências e impedir a alteração dos originais, realizando a investigação nas cópias

- a. Sistema de Ficheiros
- b. Memória
- c. Rede
- d. Aplicações

2. Examinacão: investigadores percorrem os dados por rastros de atividade ciber-criminosa, tal como e-mails de phishing, ficheiros alterados e conexões suspeitas

3. Análise: investigadores usam técnicas forenses para processar, correlacionar e extrair informações a partir de evidências digitais — podem referenciar feeds de "threat intelligence" open-source e proprietários para ligar as suas descobertas a atacantes específicos

4. Relatórios: investigadores compilam um relatório que explica o que aconteceu durante o evento de segurança e, se possível, identifica suspeitos ou culpados — o relatório pode conter recomendações para impedir ataques futuros e pode ser partilhado com reguladores e outras autoridades



SOAR

Objetivo:

1. garantir que todos os sistemas estão a funcionar de forma correta, rápida e eficaz
2. obter e correlacionar os dados necessários para reparar ameaças de falsos positivos
3. coordenar medidas de resposta apropriadas para remediar ameaças

Automação: reduz o tempo que leva a detectar e responder a incidentes repetitivos e falsos positivos para que os alertas não fiquem muito tempo por encerrados

Orquestração: permite partilhar informação facilmente, activando várias ferramentas para responder a incidentes como um grupo, mesmo quando os dados estão dispersos por uma rede complexa e por múltiplos sistemas ou dispositivos

O que está incluído no SOAR?

1. resposta a incidentes de segurança
2. Enriquecimento de dados com inteligência de ameaças
3. automação e orquestração de controles de segurança

Benefícios:

1. entregar um padrão mais alto de inteligência
2. melhorar a eficiência operacional
3. acelerar a resposta a incidentes
4. parallelizar a geração de relatórios e a captura de conhecimento

Desafios:

1. expectativas irrealistas
2. problemas de integração
3. excesso de confiança na automação
4. métricas pouco claras
5. experiência limitada

SOAR
CAPABILITIES IN
CYBER SECURITY

Threat
Intelligence

Endpoint Detection
& Response

Case Management
based
Incident Response

Security Operations
Automation

Vulnerability
Management

Playbook
Management

Resposta a Incidentes

Computer Security Incident Response Team (CSIRT): equipa que realiza, coordena e apoia a resposta a incidentes de segurança que envolvem riscos com uma constituição definida

1. Missão

2. Constituição

3. Autoridade

4. Serviços

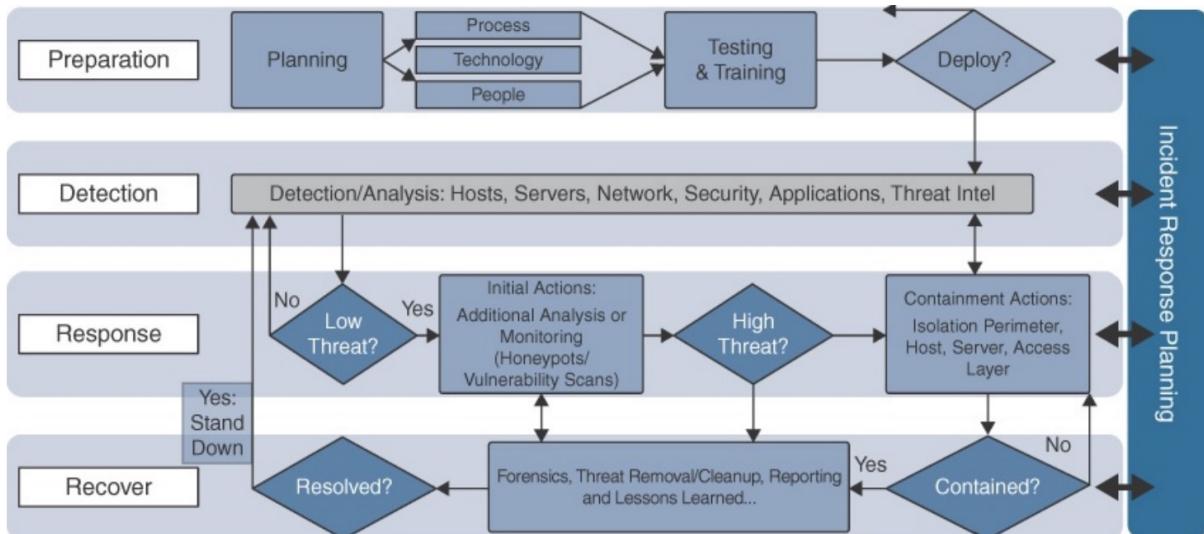
Traffic Light Protocol (TLP):

1. CLEAR: divulgação não limitada
2. GREEN: divulgação limitada, restrita à comunidade
3. AMBER: divulgação limitada, restrita aos participantes da organização e clientes
4. AMBER+STRICT: divulgação limitada, restrita aos participantes da organização
5. RED: não para divulgação, restrito só a participantes

Ciclo de Resposta a Incidentes:

1. Preparação: todas as atividades que se podem realizar antes do próprio incidente de maneira a permitir lidar melhor com ele - visões de ameaças, riscos e perigos
2. Detectão & Análise: detectar a ocorrência de um problema e decidir se é ou não um incidente para responder apropriadamente
 - a. vetores de ataque
 - b. percursos e indicadores
 - c. análise
 - d. documentação
 - e. priorização
 - f. notificação
3. Contenção:
 - a. escolher estratégia
 - b. recolher informação
 - c. identificar atacantes
4. Eradicação & Recuperação:
 - a. detectar malwares
 - b. desativar contas afetadas
 - c. identificar e mitigar vulnerabilidades
 - d. restaurar sistemas à normalidade
5. Atividade Pós-Incidente: lições aprendidas

Detection/Analysis



Threat Hunting

Atacante: só tem de ter sucesso numa vez — vantagem

Defesa: tem inúmeros sistemas e vulnerabilidades para proteger — desvantagem

Negócio:

1. prever e prevenir fugas de dados, incidentes de segurança e disruptões
2. reduzir custos e aumentar a eficiência
3. estender as capacidades de deteção e resposta
4. maximizar o investimento existente

"Dwell Time": número de dias que um atacante está presente na rede da vítima antes de ser detectado

Sem conhecimento do estado atual de compromisso, não há uma imagem incompleta da Postura de Cybersegurança

Threat Hunting: abordagem de cibersegurança proativa — processo de proativa e iterativamente procurar através de redes para detectar e isolar ameaças avançadas que escapam às soluções de segurança existentes \neq IDS, SIEM, ...

Presunção de Compromisso: a tecnologia de prevenção vai eventualmente falhar

Benefícios:

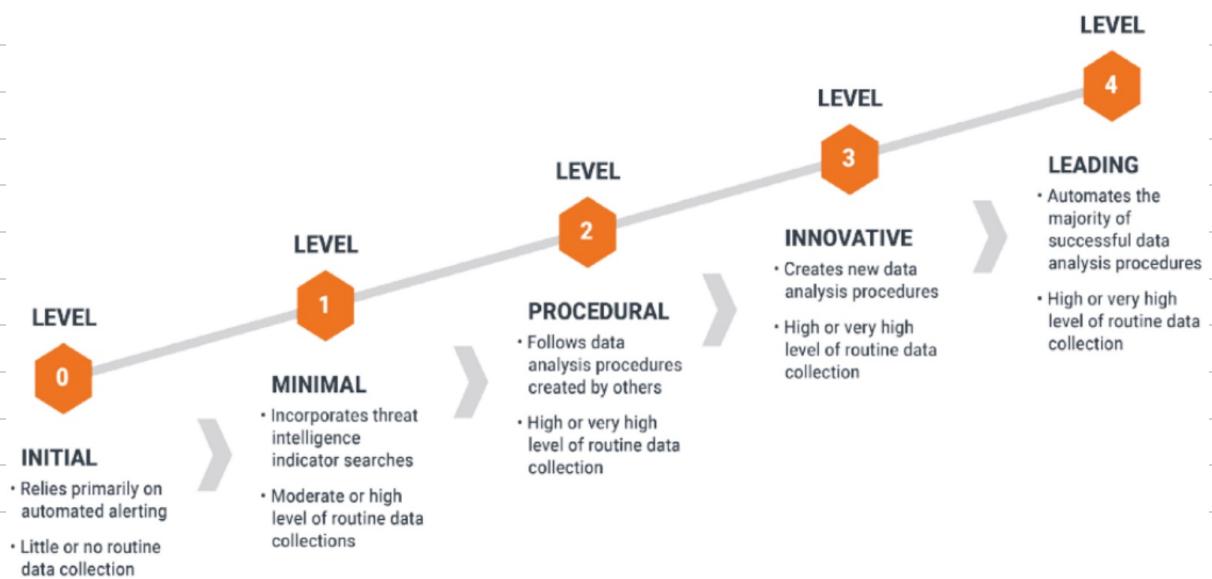
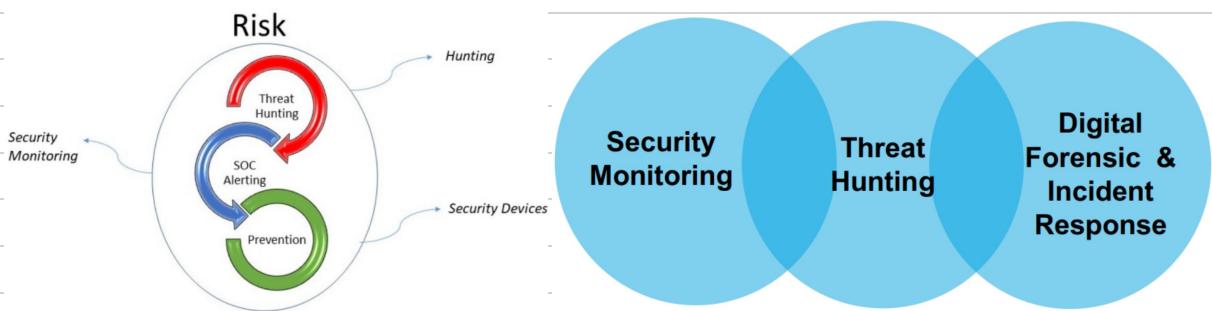
1. encontram adversários que ultrapassaram as proteções de segurança atuais
2. melhoria contínua das capacidades de deteção
3. deteção mais rápida e mais cedo de potencial compromisso
4. aumentar visibilidade do ambiente e superfície de ataque
5. melhorar a recolha de dados

Negócio: minimizar riscos residuais e "dwell time"
Técnico: detecção de ataques avançados, "non-malware attacks" e TTP

Alerting: reativo — detectar — o incidente começa quando a notificação chega
Hunting: proativo — pesquisar — pesquisa ativa por incidentes

Processo de Threat Hunting:

1. criar uma hipótese
2. investigar via ferramentas e técnicas
3. descobrir novos padrões e TTPs
4. informar e enriquecer análises



TESTE

- Resposta a Incidentes
- SIEM: o que é, o que faz e para que serve - playbooks e use cases
- SOAR: o que é, o que faz e para que serve - playbooks e use cases
- Logs: use cases e contexto
- Use Case: definição do início ao fim - compreender, projetar, determinar
- SOC: L1 ≈ L2
- IOC:
- Cyber-Ameaças
- SOC & Threat Intelligence
- Forense: ligação com CTI
- MITRE: TTP & APT

11/01/2023

Duration: 2 hours (no tolerance)

No study elements may be used.

Always justify your answers

Part I.

1. Define the primary objectives of a Security Operations Center (SOC) and explain how it contributes to an organization's overall cybersecurity posture. (2.0)
2. Explain how the MITRE ATT&CK framework can be used to map adversary techniques to mitigations. Provide two examples and explain each one. (2.5)
3. Define threat hunting and explain why it is considered a proactive approach to cybersecurity. Provide an example of a threat hunting scenario. (1.0)
4. Explain the concept of threat intelligence and how it contributes to threat detection in a SOC. Give two examples of threat intelligence outputs that can be useful for SOC. (2.5)
5. Explain the use of automation and orchestration in SOC operations. Provide examples of use cases where automation enhances incident response efficiency. (2.0)

Part II.

A medium-sized e-commerce company operates an online platform where customers can browse products, make purchases, and manage their accounts. The organization has a Security Operations Center (SOC) responsible for monitoring and responding to cybersecurity incidents.

1. Draw what you understand about this architecture. (2.0)
2. Identify an incident that could happen in this system. (1.0)
3. Perform a situational awareness analysis of this system – ponder about possible vulnerabilities, defenses, and attacks. (3.0)
4. Describe the incident handling procedures that could implement in the SOC for this incident. (2.0)
5. Identify which sources of data you could deploy in the system to support the incident handling procedure. (2.0)

PARTE I

1. Os principais objetivos de um SOC são detectar, analisar, responder, reportar e prevenir incidentes de cibersegurança, fornecendo defesa contra atividade não autorizada em redes de computadores e incluindo monitorização, deteção, análise, resposta e recuperação. O SOC contribui para a postura de cibersegurança de uma organização ao protegê-la contra ciberameaças.

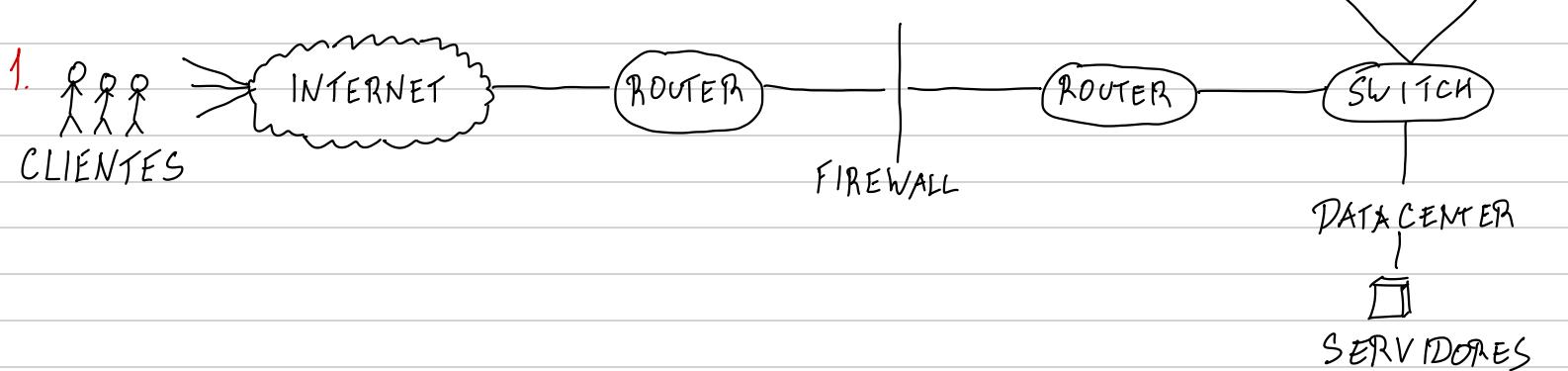
2. A framework MITRE ATT&CK pode ser usada para mapear técnicas de adversários mitigações ao identificá-las de forma clara e classificá-las/catalogá-las em determinadas táticas, que ajudam a delinear as capacidades de deteção de intrusões contra determinados atacantes e determinados procedimentos. Por exemplo, a técnica "Phishing" - mapeada na tática "Initial Access" - consiste em enviar e-mails fraudulentos que pareçam legítimos para enganar utilizadores e roubar as suas credenciais. Se detectada, o SOC pode forçar todos os utilizadores afetados a alterar as suas credenciais para proteger a empresa. Por exemplo, a técnica "Brute Force" - mapeada na tática "Credential Access" - consiste em tentar authenticar-se como um utilizador legítimo através da introdução de múltiplas possibilidades de credenciais. Se detectada, o SOC pode bloquear tentativas de início de sessão a partir do IP malicioso, por segurança.

3. Threat Hunting é o processo de procurar em dispositivos e redes de forma iterativa e proativa para detectar ameaças avançadas que escapam às soluções de segurança existentes. É uma abordagem proativa porque, ao contrário de um SOC tradicional regido por alertas, threat hunting efetua-se nem se ter recebido qualquer notificação de alerta ou incidente. Por exemplo, um cenário possível consiste em teorizar (lançar a hipótese) que a rede está infetada com ransomware e, para investigar, consultar/verificar os ficheiros e as suas informações, para confirmar se os nomes, tipos/extensões ou hashes foram alterados recentemente.

4. Threat Intelligence é o processo de conhecer os adversários/atacantes, principalmente aqueles que tendem a atacar organizações semelhantes à que se pretende proteger, para os identificar através de indicadores de compromisso e - conhecendo as suas táticas, técnicas e procedimentos - aumentar a segurança/proteção contra as suas próximas ações previstas. Isto contribui para a deteção de ameaças num SOC porque reconhecer um ataque através de um IOC ajuda a prever as suas próximas atividades maliciosas e assim, preveni-las ou mitigá-las. Por exemplo, um output de Threat Intelligence que pode ser útil para um SOC pode ser identificar que o atacante X, depois de a realizar a ação Y, tende a realizar a ação Z - assim, se a atividade Y for detectada, podem ser reforçados os controles de segurança para prevenir Z. Outro exemplo pode ser identificar um grupo API a partir de determinados IOC e, assim, conseguir prever qual o seu modo de operação para reforçar a monitorização de determinadas infraestruturas e/ou mitigar/resolver vulnerabilidades activamente exploradas pelo API.

5. Automação consiste em reduzir o tempo que leva a detectar e responder a incidentes repetitivos e falsos positivos para que os alertas não fiquem por endereçar durante longos períodos de tempo. Orquestração permite partilhar informações facilmente, permitindo que múltiplas ferramentas respondam a incidentes como um grupo, mesmo quando os dados estão dispersos por uma rede complexa e por múltiplos sistemas ou dispositivos. Por exemplo, automatizar o bloqueio na firewall de endereços IP que tentam constantemente fazer scans à rede ou tentativas de autenticação por ataques de força-bruta. Outro exemplo pode ser forçar - automaticamente - que um utilizador tenha de utilizar autenticação multi-fator (MFA) se iniciar sessão com credenciais corretas a partir de um endereço IP desconhecido (nunca anteriormente utilizado).

PARTE II



1. Um incidente que pode ocorrer neste sistema é um empregado caí num esquema de phishing por e-mail e, ao clicar num link malicioso, introduzir as suas credenciais numa página controlada pelo atacante que, assim, as rouba e, se não houver autenticação multi-fator, autenticar-se como um utilizador legítimo para, por exemplo, exfiltrar dados.
2. Um incidente que pode ocorrer neste sistema é um empregado caí num esquema de phishing por e-mail e, ao clicar num link malicioso, introduzir as suas credenciais numa página controlada pelo atacante que, assim, as rouba e, se não houver autenticação multi-fator, autenticar-se como um utilizador legítimo para, por exemplo, exfiltrar dados.
3. Neste sistema, podem existir vulnerabilidades aplicacionais (no código da loja online), ou ao nível dos controlos de segurança internos (gestão de permissões e de acessos, por exemplo), ou ao nível da falta de formação sobre cibersegurança. Estas vulnerabilidades podem ser exploradas por ataques de injecção, explots conhecidos, phishing, ... As defesas possíveis consistem em manter o software actualizado para proteger/resolver eventuais vulnerabilidades, rever e testar o código contra falhas de segurança, realizar ações de formação regular sobre boas práticas de cibersegurança.
4. Os procedimentos de resposta a este incidente pelo SDC podem ser: (1) Tentar preveni-lo, através de campanhas de phishing com contacto formativo e/ou ao identificarem automaticamente e-mails suspeitos de origem víctima; (2) detectá-lo, através da consulta dos logs do Active Directory para os inícios de sessão, procurando por actividade suspeita (localizações, endereços IP, horas, ...); (3) contê-lo, isolando imediatamente o utilizador visado e as suas máquinas da rede interna, para prevenir movimentos laterais e/ou exfiltrações de dados; (4) erradicá-lo, ao terminar todas as sessões e bloquear o inicio de sessão; (5) recuperá-lo, ao mudar as credenciais de acesso afectadas e (6) em pós-incidente, ponderar sobre a implementação de MFA e sobre políticas de acesso condicional para tentar evitar casos futuros semelhantes.
5. Para suportar o processo de resposta a este incidente, poderiam ser lançados no sistema colectores de logs do Active Directory para detetar inícios de sessão não autorizados e dos routers ou endpoints para investigar as páginas acedidas pela vítima e as credenciais introduzidas.

22/01/2023

Duration: 2 hours (no tolerance)

No study elements may be used.

Always justify your answers

Part I.

1. Identify and explain one capability that a Security Operations Center (SOC) should have and provide reasoning for whether this capability should be considered a mandatory or optional. (2.0)
2. A threat intelligence team identifies a new malware variant targeting financial institutions. How can MITRE ATT&CK assist the team in understanding the tactics and techniques employed by the malware, and how might this information be used to enhance the organization's defenses ? (2.5)
3. Explain the purpose and benefits of using the TLP(Traffic Light protocol) framework in incident response. (1.0)
4. Explain how IoCs(Indicator of Compromise) are used in threat intelligence to detect and respond to cyber threats. Provide two examples and explain each one. (2.5)
5. Enumerate three key benefits of incorporating automation into SOC workflows. (2.0)

Part II.

Consider a Linux box with the FTP(File Transfer Protocol) service running. The box has a network interface on a local switch. A router does port forwarding of the FTP service to the internet.

1. Draw what you understand about this architecture. (2.0)
2. Identify an incident that could happen in this system. (1.0)
3. Perform a situational awareness analysis of this system – ponder about possible vulnerabilities, defenses, and attacks. (3.0)
4. Describe the incident handling procedures that could implement in the SOC for this incident. (2.0)
5. Identify which sources of data you could deploy in the system to support the incident handling procedure. (2.0)

PARTE I

1. Uma capacidade que um SOC deve ter é monitorização, isto é, receber eventos/alertas gerados a partir de logs (de forma independente ou correlacionada) para conseguir responder adequadamente, seja através da execução de playbooks, seja ao escalá-lo para níveis superiores. Esta capacidade deve ser obrigatória porque é essencial/imprevisível para garantir a segurança de uma organização, dado que só é possível responder a alertas de segurança com lidar com incidentes se estes forem monitorizados continuamente.
2. A framework MITRE ATT&CK pode ajudar a equipa a compreender as táticas e técnicas utilizadas pelo malware ao mapear os procedimentos de forma clara, organizada e estruturada, para que seja possível perceber corretamente o que foi feito de malicioso, em que contexto/etapa de comprometimento se inseriu e o que deve ser feito para o mitigar. Esta informação pode ser usada para melhorar as defesas da organização ao auxiliar/facilitar a compreensão de qual o estado de comprometimento atual da organização (desde ataque inicial até comando e controlo) para decidir quais as ações a tomar, bem como contribuir para identificar o atacante com o apoio de Cyber Threat Intelligence e, assim, conseguir prever as suas próximas ações e defesas relevantes.
3. O Traffic Light Protocol tem como propósito classificar/catalogar informação de acordo com o seu nível de secretismo/confidencialidade, definindo, dessa forma, com quem pode ser partilhada. Os benefícios desta framework são plenamente comunicados de forma visualmente clara e evidente para todas as audiências qual o tratamento que deve ser dado à informação, bem como ser extremamente intuitiva, simples e fácil de utilizar dada a analogia com as cores do semáforo.
4. Os Indicadores de Compromisso não utilizados em Cyber Threat Intelligence (CTI) para detectar e responder a ciberameaças porque permitem identificar os atacantes através de valores de hash (assinaturas) ou endereços IP e, assim, prever as suas tendências e próximas ações para reforçar a segurança contra elas. Por exemplo, se for detetado malware ou um ficheiro malicioso com uma dada assinatura (valor de hash) presente numa base de dados pública ou conhecida de atores maliciosos, pode ser identificado o atacante. Por exemplo, se forem detetadas múltiplas tentativas de acesso não autorizado a partir de um endereço IP conhecido por estar associado a atividade criminosa, pode ser identificado o atacante.
5. Três benefícios de incorporar automação no SOC, nomeadamente através do uso de um SOAR, são: (1) integrar um standard mais alto de inteligência, (2) aumentar a eficiência operacional, (3) acelerar a resposta a incidentes e (4) parallelizar a geração de relatórios e a captura de conhecimento.

PARTE II

1.


SERVIDOR FTP
2. Um incidente que pode ocorrer neste sistema é um (Distributed) Denial-of-Service (DDoS) - um número elevado de pedidos ao servidor FTP que compromete a sua disponibilidade, inabilitando o funcionamento.
3. Neste sistema, possíveis vulnerabilidades podem ser a exposição à internet, a existência de portas/portos abertas expostas, utilizadas, a configuração do roteador com credenciais fracas ou predefinidas e erros no código do servidor que podem ser explorados. Estas vulnerabilidades podem ser exploradas através de scans maliciosos, ataques de força-bruta às credenciais de acesso, tentativas de DDoS, utilização de exploits conhecidos, ... As defesas possíveis consistem em atualizar os sistemas para as versões de software e firmwar mais recentes, fechar portas/portos abertos desnecessários, configurar adequadamente os dispositivos com credenciais fortes e autenticação multi-fator (se possível) e fechar a exposição à internet, forçando o acesso através de VPN ou, no mínimo, de uma whitelist de endereços IP permitidos, entre outros.
4. Os procedimentos que podem ser implementados no SOC para este incidente (DDoS) são: (1) tentar prevenir, através da instalação de um "load balancer" ou da aquisição de serviços de um Content Delivery Network (CDN); (2) detectá-lo, através da monitorização do número de pedidos FTP ou de tentativas de acesso para identificar comportamento anómalo; (3) contê-lo, diminuindo o rácio de admissão de pedidos ou de envio de respostas (rate throttling); (4) erradicá-lo, ao bloquear todos os endereços IPs maliciosos ao nível de uma eventual firewall; (5) recuperá-lo, restabelecendo a normal operação dos serviços e sistemas após um determinado período de tempo e (6) em pós-incidente, investigar sobre as origens do ataque e as motivações do atacante, bem como da importância de firewalls, load balancers, CDNs seguros de CS.
5. Para suportar o processo de lidar com este incidente podem ser lançados no sistema os logs do roteador para identificar os endereços IP maliciosos, conseguindo bloqueá-los numa eventual firewall.