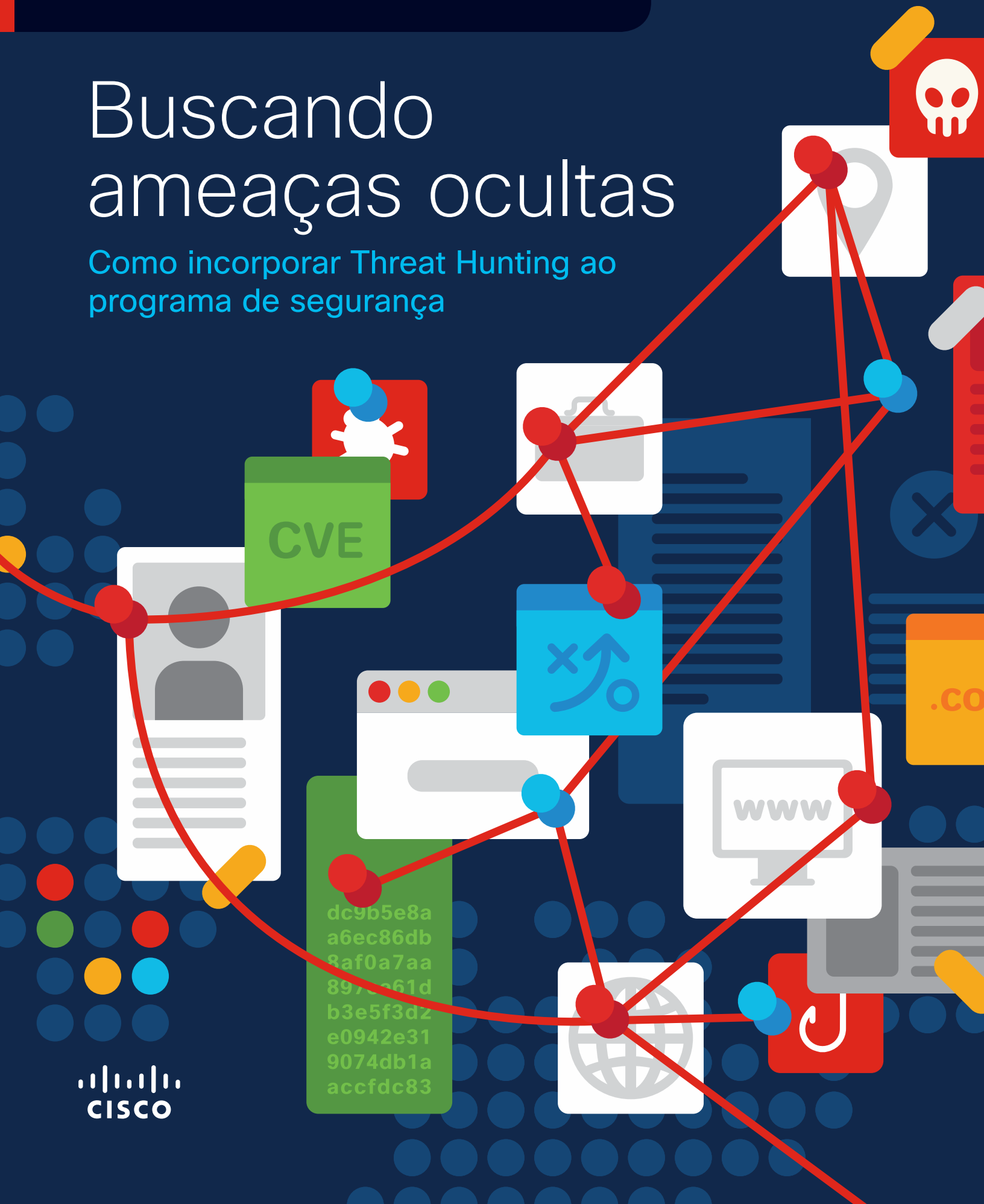
Buscando ameaças ocultas

Como incorporar Threat Hunting ao programa de segurança

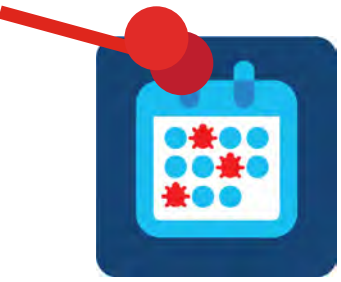


CISCO

Conteúdo

Introdução

São 13h e está tudo bem. Você voltou do almoço, e como responsável sênior pela busca de ameaças do SOC da empresa, acabou de checar os painéis SIEM para ver se há alertas de segurança. Nada fora do comum chamou sua atenção. Um projeto de automação recente reduziu muito o tempo necessário para fazer essa varredura de segurança, deixando livre um tempo valioso que anteriormente era gasto em tarefas manuais. Então, como você usa esse tempo que sobrou?



Threat hunting é uma atividade que você planeja e executa regularmente para ajudar a fortalecer a postura de segurança.

Talvez seja a hora de pensar em threat hunting Threat hunting envolve ir além do que já sabemos ou fomos alertados. O software de segurança só nos alerta para os riscos e comportamentos que sabemos que são mal-intencionados. Optar por threat hunting é se aventurar no desconhecido.

Threat hunting é um exercício de segurança ativo, com a intenção de encontrar e erradicar os invasores que penetraram no ambiente sem disparar o alarme. Isso contrasta com as investigações e as respostas tradicionais que se originam de alertas exibidos após a detecção de atividades potencialmente mal-intencionadas.

A realidade

É claro que esse cenário pode parecer um pouco idealista. Quero dizer, quem na verdade tem uma tarde livre para se dedicar a isso? Há sempre algo a mais que precisa ser feito, não é?

A realidade é que, na maioria das vezes, a busca de ameaças não é uma atividade que você faz por capricho. Também não é algo que você faz em uma investigação contínua como a próxima etapa de um procedimento. Em vez disso, é uma atividade que você planeja e executa regularmente para ajudar a fortalecer a postura de segurança. Basicamente, é mais uma ferramenta do seu arsenal de segurança.

Nada disso parece fácil de ser feito quando a agenda está lotada e a lista de tarefas é longa. No entanto, há alguns benefícios significativos que você observa quando reserva um tempo na agenda para realizar atividades de threat hunting.

Prevenir é melhor que remediar

Para começar, identificar e erradicar ameaças desconhecidas e não detectadas é sempre algo positivo. Mesmo quando uma ameaça específica não é descoberta, as atividades de threat hunting geralmente identificam pontos fracos no ambiente, que você pode melhorar para definir novas políticas. Em última análise, o resultado de threat huntings regulares reduz de forma significativa a superfície de ataque para futuros agentes mal-intencionados.

Também há oportunidades substanciais de desenvolver o que é aprendido durante uma campanha de threat hunting. Essas atividades podem identificar áreas onde o alerta do comportamento mal-intencionado pode ser colocado em prática e onde é possível usar automação para repetir um escopo específico da busca de ameaças. Dessas áreas, você pode realizar atividades adicionais de threat hunting, fortalecendo e expandindo a proteção e os recursos.

Por onde começar

O objetivo deste documento é fornecer uma visão geral do que é threat hunting. Vamos explorar os aspectos de threat hunting, destacar por que é um esforço interessante, quem deve estar envolvido, o quê e onde você deve procurar, e quando deve fazê-lo.

Há também uma série de disciplinas de segurança com tarefas que se sobrepõem à de threat hunting. Vamos compará-las e contrastá-las, mostrando que, embora threat hunting seja semelhante a outras tarefas, merece um lugar especial no seu arsenal de segurança.

Por fim, discutiremos como você pode desenvolver campanhas de threat hunting eficazes na empresa. O mais difícil é determinar por onde começar. Para ajudar, começamos com as etapas mais simples para que você possa desenvolver uma postura de threat hunting e fortalecer a segurança da empresa no processo.

Threat Hunting VS. _____

No que diz respeito às disciplinas de segurança, threat hunting é uma especialidade relativamente nova. Consequentemente, há sobreposições com outras práticas relacionadas à segurança. Na verdade, muitas pessoas atualmente envolvidas em threat hunting já têm experiência com essas outras funções na vida profissional. A seguir, veja algumas comparações rápidas com outras disciplinas.

Resposta a incidentes

Essa função é talvez a mais semelhante à de threat hunting. Ambos lidam diretamente com ameaças no ambiente. A principal diferença é que a resposta a incidentes é reativa. Você sabe que há algo errado, ou pelo menos que algo anormal tentou acessar a rede, devido a alertas de segurança, ao comportamento da rede ou do endpoint, ou por outras evidências. Em contrapartida, quando você aplica threat hunting, não há necessariamente qualquer evidência de uma ameaça. Em vez disso, você está procurando ativamente por algo em vez de tentar conter e corrigir o que você já sabe que está lá.

Teste de penetração

A atividade de threat hunting e os testes de penetração também compartilham algumas semelhanças. Na realidade, ambos tentam procurar pontos fracos na rede. No entanto, os testes de penetração geralmente buscam problemas de configuração ou vulnerabilidades conhecidas para obter acesso a uma rede ou a informações confidenciais. O objetivo de fazer threat hunting não é necessariamente obter acesso a nada, mas sim identificar ameaças ocultas em um ambiente, erradicá-las e configurar políticas para evitá-las no futuro.

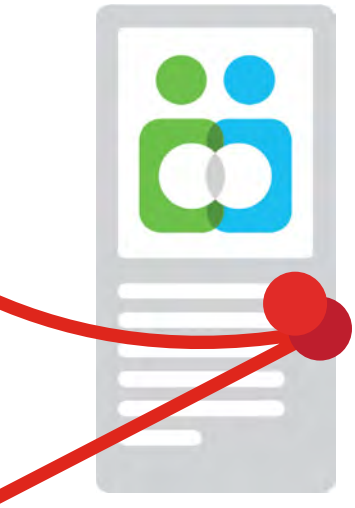
Gerenciamento de riscos

A ideia no gerenciamento de riscos é determinar os pontos fracos na rede ou, no caso de sistemas, determinar a gravidade, priorizar e, em seguida, tomar as medidas apropriadas para corrigi-los. Isso pode envolver a identificação de fontes de ameaças, e a atividade de threat hunting pode ajudar a fornecer uma avaliação de risco. No entanto, essas avaliações geralmente são muito mais abrangentes do que a simples busca de ameaças, observando todos os possíveis riscos, conhecidos e desconhecidos.

Avaliação de comprometimento

Também semelhante à threat hunting, a avaliação de comprometimento consiste em descobrir se a rede foi violada por agentes desconhecidos e mal-intencionados. No entanto, é um exercício muito mais amplo do que threat hunting. Durante as avaliações de comprometimento, várias ferramentas são instaladas na rede, para procurar qualquer coisa fora do comum. Em contrapartida, threat hunting começa com uma ideia ou um cenário muito específico e mantém o foco nesse escopo.

As 5 perguntas



A equipe de threat hunting provavelmente vai se sobrepor à equipe de resposta a incidentes, e vai aprimorar suas habilidades e melhorar os tempos de resposta quando confrontados com um incidente real.

Descobrir por onde começar pode ser um desafio ao estabelecer atividades de threat hunting na empresa. Utilizar as cinco perguntas, frequentemente usadas no jornalismo, pode ser uma boa maneira de começar a planejar o processo.

Por quê?

O investimento antecipado na detecção proativa de ameaças pode fortalecer consideravelmente a postura de segurança de uma empresa. O fato é que existem os invasores organizados, qualificados e bem financiados. Se você se tornar alvo de um desses grupos, eles poderão trabalhar diligentemente buscando uma fraqueza para entrar. Infelizmente, não é possível descobrir tudo, mesmo com as melhores ferramentas de segurança. É aqui que entra em ação a atividade de threat hunting, cuja principal função é encontrar apenas esses tipos de invasores.

Um bônus adicional de fazer threat hunting é que essa atividade gera familiaridade com ferramentas e técnicas que são muito importantes quando ocorre uma invasão ou uma violação. A equipe de threat hunting provavelmente vai se sobrepor à equipe de resposta a incidentes, e vai aprimorar suas habilidades e melhorar os tempos de resposta quando confrontados com um incidente real. Isso pode ser encarado como prática quando há problemas.

Identificar quem

Criar essa equipe de threat hunting pode parecer tão assustador quanto montar uma equipe de super-heróis para derrotar um inimigo comum. Parte da montagem dessa equipe é reunir pessoas com diferentes habilidades e conhecimentos.

Se você é uma grande empresa, então a primeira etapa pode ser tão simples quanto reservar um período do mês para que um grupo (ou equipe tiger) planeje, execute e relate uma campanha de threat hunting. No entanto, se você é uma empresa pequena com poucas pessoas (talvez apenas uma!) dedicadas a TI, isso talvez não seja tão fácil. Levando isso em conta, pode ser que você queira trazer a experiência de terceiros para ajudar. Isso tem vantagens e desvantagens. O lado positivo é que você provavelmente terá acesso a pessoas que tenham as habilidades de threat hunting de que você precisa. No entanto, uma equipe externa de threat hunting não estará tão familiarizada com os prós e contras específicos da sua rede como o pessoal interno.

Independentemente disso, há certas habilidades essenciais para uma equipe que vai realizar uma campanha de threat hunting:

- **Familiaridade com endpoint e segurança de rede**

  Isso é evidente. Você precisará de membros experientes da equipe de SOC ou TI com amplos conhecimentos sobre problemas de segurança e melhores práticas.

- **Compreensão da análise de dados**

  Muitas vezes, threat hunting demanda padrões de instigação de dados brutos. Um entendimento da análise estatística ajudará a identificar os padrões nos dados. A visualização de dados é igualmente importante para detectar e compartilhar as anomalias.

- **Uma curiosidade inata**

  Threat hunting não é uma atividade comum. Às vezes, pode ser até comparada a uma busca artística. Ela requer um pensamento criativo, que conecte itens aparentemente não relacionados ou questione: " Eu me pergunto o que aconteceria se..."

Para realizar qualquer procedimento relacionado à busca de ameaças, é necessário ter o log adequado e habilitado para realizar a busca.

Um bônus da atividade de threat hunting, sob a perspectiva de um profissional de segurança, é que é divertido. A atividade de threat hunting oferece às pessoas do departamento de SOC ou TI a chance de dar uma pausa na natureza reativa do dia a dia de suas funções e a chance de partir para o ataque. Essas tarefas ativas e gratificantes para os funcionários podem muitas vezes levar a taxas de retenção mais elevadas de funcionários do SOC, mantendo-os em uma área onde é difícil encontrar pessoas altamente qualificadas e onde se troca de emprego com frequência.

Quando buscar

Por fim, as buscas mais bem-sucedidas são as planejadas. Você precisa definir um escopo para a busca, identificar metas claras e reservar um tempo para realizá-la. Quando você terminar, avalie as etapas para melhorar a postura de segurança, estabelecendo manuais de segurança para abordar os resultados dali por diante.

Em outras ocasiões, talvez você queira realizar uma atividade de threat hunting quando suspeitar que algum comportamento de risco pode ter ocorrido.

- **Um usuário específico está baixando muito mais dados em um determinado dia do que o normal?**
- **Algum usuário tentou entrar em um sistema ao qual ele não tem acesso?**
- **Um administrador parece estar apagando os bash logs?**

Muitos desses comportamentos podem indicar ações mal-intencionadas que comprometeram um dispositivo, e é um lugar bastante indicado para começar a fazer uma busca de ameaças.

Por fim, há momentos em que uma busca de ameaças pode surgir inesperadamente. Alguma notícia sobre segurança digital que chamou a atenção do CIO já resultou em um e-mail ou telefonema perguntando se a empresa está vulnerável? Essa é uma pergunta perfeitamente válida, e ter um processo em andamento para consultas de campo como essa pode economizar uma quantidade significativa de tempo e recursos.

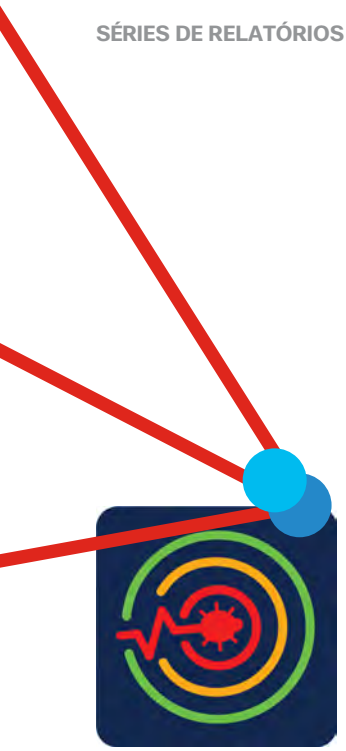
O quê e onde

Por fim, os dados são fundamentais para qualquer busca de ameaças. Para realizar qualquer procedimento relacionado à threat hunting, é necessário ter o log adequado e habilitado para realizar a busca. O fato é que, se você não consegue ver o que está acontecendo nos sistemas, então não pode responder da mesma forma.

A escolha dos sistemas a serem considerados dependerá frequentemente do escopo da busca. Uma busca pode ser nos endpoints do departamento de finanças e outra pode se concentrar nos servidores da Web. Em alguns casos, você pode até querer instalar ferramentas no ambiente para monitorar tipos específicos de tráfego. Os logs acompanhados por esses sistemas temporários serão utilizados na busca.

É claro que habilitar o log pode encher com rapidez os ativos de armazenamento e coletar logs pode facilmente consumir tempo da equipe. Isso pode demandar a anulação de recursos físicos para armazenar logs e a configuração de automação básica para enviá-los para esse local. No curto prazo, é necessário ser seletivo em relação à extensão com que você configura os sistemas para registro. A utilização de ferramentas, como o software de gerenciamento de eventos e informações de segurança (SIEM), pode levar um tempo até tornar a análise de logs mais rápida e fácil.

Nas primeiras atividades de threat hunting, o resultado pode incluir uma lista de perguntas que não puderam ser respondidas com base nos logs disponíveis. Com o tempo, ficará mais claro quais sistemas precisam ter o log habilitado e em que nível, para obter os resultados desejados.



O objetivo da atividade de threat hunting deve ser descobrir TTPs de um invasor, os mais valiosos, porque são difíceis de o invasor substituir.

A pirâmide de dificuldades

O pesquisador de segurança David Blanco surgiu com uma abordagem chamada Pirâmide de dificuldades, que descreve como dificultar os ataques de adversários na rede. Cada uma das seis camadas representa diferentes abordagens que você pode ter, começando com a mais simples até a mais difícil.

Por exemplo, na base da pirâmide estão os hashes. Os arquivos que carregam hashes mal-intencionados conhecidos são simples de detectar e também simples de o invasor substituir. O mesmo vale para endereços IP, embora isso dê um pouco mais de trabalho para encontrar e para um invasor substituir, sendo assim uma parte menor da pirâmide. Os domínios são um pouco mais difíceis, os artefatos de rede são ainda mais difíceis etc.

O objetivo da atividade de threat hunting deve ser descobrir táticas, técnicas e procedimentos (TTPs) de um invasor. Esses são os mais valiosos porque são difíceis de substituir pelo invasor. Muitas vezes, isso é o mais difícil e/ou demorado de identificar, principalmente porque exige comparar pontos de dados de diferentes conjuntos de dados e fazer conexões em que a relação entre eles não é tão aparente no início.

O truque é que, à medida que você sobe na pirâmide, força os criminosos a gastarem mais recursos para atacar a rede, tornando-a mais complicada e aumentando as chances de eles serem pegos. O objetivo final da pirâmide de dificuldades é que, seguindo seus princípios, a rede se torna tão desafiadora para hackear que os invasores buscam outros alvos mais simples.

Fonte: David J. Bianca, blog pessoal

Como buscar

Há uma série de maneiras de abordar uma atividade de threat hunting. Os recursos e as habilidades disponíveis serão essenciais para o detalhamento de uma campanha de threat hunting.

A seguir, começamos com formas simples e básicas de iniciar threat hunting e, em seguida, trabalharemos em termos de complexidade. A ideia aqui é que, após cada atividade de threat hunting, você possa desenvolver o que aprendeu. O planejamento de manuais, automação e mudanças de política, quando necessário, oferece uma base para técnicas mais avançadas.

Análise dos logs

Às vezes, as atividades de threat hunting mais simples decorrem de pesquisas ou relatórios sobre ameaças descobertas recentemente. Hoje em dia, é uma prática comum incluir indicadores de comprometimento (IoCs) junto com a pesquisa para que outras pessoas usem. Geralmente, esses pontos de dados são compostos por endereços IP, URLs, domínios, hashes de arquivo ou outros IoCs que compõem uma ameaça.

Uma das maneiras mais simples de iniciar uma atividade de threat hunting é comparar os logs dos sistemas com IoCs. As ferramentas de linhas de comando ou scripts simples podem ser suficientes para você começar. O uso de um SIEM é outro método para comparar rapidamente IoCs com logs. Também há produtos de segurança mais avançados que podem facilitar threat hunting, permitindo que você copie e cole IoCs em um painel para checar se eles foram vistos no ambiente.

Quando você se sentir confortável com essas atividades, poderá se aprofundar nos logs e começar a descobrir novos IoCs que podem existir. Agora que as habilidades de análises de dados entram em jogo. A aplicação de modelos estatísticos a logs, como clustering ou distribuição de frequência, pode ajudar a esclarecer as anomalias. Por fim, você espera chegar ao topo da pirâmide de dificuldades e identificar os TTPs de um invasor.

Testando uma teoria

Alguns podem argumentar que simplesmente comparar os logs aos IoCs conhecidos não é verdadeiramente threat hunting. O raciocínio é que você está simplesmente combinando

Threat Hunting em ação

Jeff Bollinger gerencia as investigações de segurança da CSIRT aqui na Cisco. A seguir, veja um relato em primeira mão de uma atividade de threat hunting que a equipe dele realizou.

"Ao analisar os dados históricos de endpoint do Cisco AMP para obter indicadores de comprometimento, vimos um dropper binário suspeito que tinha sido excluído pelo usuário.

Recuperamos o binário ao restaurar o arquivo único do backup (corporativo) do usuário e pudemos revertê-lo e extrair outros indicadores (nomes de hosts C2), e então aplicamos à nossa telemetria de rede.

Isso gerou hosts adicionais afetados que não acionaram o hash do dropper original".

Ao mesmo tempo, se você for o veterano experiente da equipe, evite pensar que já viu isso antes. Em vez disso, busque comprovar que não é uma ameaça. Se você não conseguir fazer isso de forma improvisada, pesquise mais.

1:1. Nesses casos, para qualificar como threat hunting, você precisa se aprofundar mais.

Agora é que a criatividade desempenha o seu papel. Você precisa de uma teoria sobre onde uma ameaça pode residir, os vetores que ela pode ter usado para alcançar seu objetivo ou as técnicas exploradas. A seguir, veja algumas ideias sobre o tipo de investigação que você pode realizar.

- **Ler notícias sobre segurança**

  As últimas notícias sobre o cenário de ameaças podem estar cheias de material para uma busca de ameaças. Por exemplo, se ocorreu uma vulnerabilidade importante, recentemente divulgada em um processo do Windows, investigue se alguma atividade estranha ocorreu em torno desse processo. Claro, preste atenção especial ao material que se aplica ao seu setor. Por exemplo, se você trabalha com aviação, um ladrão de cartão de crédito não seria uma alta prioridade. Por outro lado, se você trabalha em bancos, uma ameaça encontrada atacando um ICS não se aplicaria.

- **Analisar relatórios de comportamento estranho**

  Investigue relatórios incomuns de atividade da equipe. Os sistemas hibernando foram ativados repentinamente durante a noite? Investigue o que está ativando os sistemas. Um escritório informou que encontrou dados internos em uma fonte externa? Procure por indícios de vazamento de dados.

- **Filtrar o normal para encontrar o anormal**

  A atividade incomum é um bom ponto de partida, mas nem sempre é fácil de detectar. Às vezes, você precisa ir mais fundo para encontrá-la. Observe uma atividade específica com um objetivo mal-intencionado em mente. Por exemplo:

  - Procure por longas conexões de rede, o que pode ser um sinal de vazamento de dados. Filtre as que são esperadas e veja se alguma das que permanecem são suspeitas.
  - Analise os picos de atividade da CPU e os processos que os criam, o que pode indicar cryptomining ou uma atividade de registro de infostealer. Filtre aqueles que são bem conhecidos e examine aqueles que não são.
  - Que tipo de arquivos a ferramenta BITSAdmin está baixando? Ela pode ser usada para extrair ferramentas mal-intencionadas, pois muitas ameaças usam ferramentas locais para mascarar suas ações. Cancele os downloads regulares que você está esperando e concentre-se no resto.
  - Observe as tarefas agendadas. Os invasores podem adicionar suas próprias tarefas para lançar determinadas atividades mal-intencionadas. Há alguma que não seja executada por administradores de sistema? Investigue qualquer uma que pareça suspeita.

Todos os casos em que o comportamento parece fora do comum são áreas privilegiadas para aprofundar e encontrar a causa principal. No entanto, é importante abordar qualquer coisa encontrada com um pouco de cautela. Só porque algo parece estranho, não significa necessariamente que seja um agente mal-intencionado. Certifique-se de comparar as descobertas com outras fontes de dados antes de chegar a qualquer conclusão. Ao mesmo tempo, se você for o veterano experiente da equipe, evite pensar que já viu isso antes. Em vez disso, busque comprovar que não é uma ameaça. Se você não conseguir fazer isso de forma improvisada, pesquise mais.

Vá atrás da fonte

Você conseguiu identificar uma ameaça na rede, determinar o que a permitiu entrar e tomar medidas para evitar que isso aconteça novamente. No entanto, na próxima vez que você executar uma atividade de threat hunting, descobrirá que os invasores voltaram de outra maneira.

Se a empresa está sendo uma constante vítima de ataques, talvez seja recomendável investigar quem está invadindo, a infraestrutura usada para a invasão e tentar desativar o grupo.

No entanto, não estou sugerindo que você assuma uma prática ostensiva de hacking contra invasores. Por mais tentador que isso possa ser, há uma série de problemas ao seguir esse caminho.

Para começar, se você invade uma infraestrutura mal-intencionada, os invasores podem perceber e rebater duas vezes mais forte. No entanto, sua motivação desta vez pode não ser roubar informações, mas sim vingança, desativando ou destruindo os sistemas à medida que aparecem.

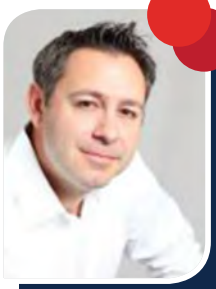
Outra razão para não hackear de volta é que, na maior parte do mundo, isso é ilegal. Apesar do fato de que os sistemas em questão estão realizando atividades ilegais, hacking ostensivo ainda é hacking.

A boa notícia é que ainda há muito o que pode ser feito. Os IoCs de um ataque podem revelar muito sobre os invasores sem precisar tocar nas redes.

A melhor abordagem para que os agentes mal-intencionados sejam desligados é reunir qualquer IoC que você possa descobrir, de hashes até TTPs, criar um perfil do invasor e, em seguida, entregar esses detalhes para as devidas autoridades. Essas autoridades são o melhor método para buscar e encerrar as atividades de um invasor por meios legais.

A melhor abordagem para que os agentes mal-intencionados sejam desligados é reunir qualquer IoC que você possa descobrir, de hashes até TTPs, criar um perfil do invasor e, em seguida, entregar esses detalhes para as devidas autoridades.

Claro que, para todas as empresas, exceto as maiores e mais direcionadas, isso nem sempre é algo que pode ser feito com tanta facilidade internamente. Como resultado, a maior parte das empresas pode e deve contar com equipes de pesquisa de segurança externas que fizeram da investigação de tais ataques sua principal função. O grupo de inteligência de ameaças, como o Talos Intelligence ou os serviços de resposta a incidentes da Cisco, estão aqui para ajudar nesses casos.



Utilizando Threat Hunting

Sean Mason, diretor de gerenciamento de ameaças para os serviços de consultoria de segurança da Cisco, reflete sobre como suas equipes aproveitaram o recurso de threat hunting na Cisco.

"Eu realmente comecei a entender e valorizar a atividade de threat hunting em 2011, logo após o hack RSA. Participei de muitas reuniões para debater sobre como poderíamos detectar esse tipo de ameaça. Isso realmente nos fez pensar de forma diferente. Também percebemos o tipo de lacunas de visibilidade que tínhamos. Ao longo dos anos, várias equipes em que participei têm usado threat hunting de formas diferentes: seguindo proativamente um palpite, respondendo a um incidente ou sendo diligente após ler notícias recentes sobre segurança. Posso dizer honestamente que, depois de mais de oito anos utilizando threat hunting em vários cenários, considero-a um componente essencial para todo programa de segurança bem-sucedido".

As consequências

Por mais importante que seja identificar e erradicar ameaças ocultas na rede, descobrir como entraram e tomar medidas para evitar ataques futuros talvez sejam os aspectos mais importantes da atividade de threat hunting. Planeje uma reunião após as operações para falar sobre a busca. Nela, mostre o problema encontrado e discuta o que precisa ser feito para corrigi-lo. Em seguida, implemente as alterações de política de rede para bloqueá-lo.

Às vezes, as melhores campanhas de threat hunting não descobrem nada. O beneficio aqui é que você agora sabe concretamente que a via investigada não é um risco para a sua empresa.

Às vezes, não se trata de encontrar uma ameaça, mas sim descobrir pontos fracos na empresa. Uma campanha de threat hunting bem-sucedida pode descobrir um servidor configurado incorretamente ou uma violação de política que precisa ser corrigida. E, por mais intuitivas que possam parecer, às vezes, as melhores campanhas de threat hunting não descobrem nada. O benefício aqui é que você agora sabe concretamente que a via investigada não é um risco para a empresa.

A adição de automação é outra etapa de busca essencial após a ameaça. Após a conclusão de uma busca de ameaças, é importante verificar periodicamente para ver se a atividade que você descobriu não foi retomada. Converta o que foi encontrado em um processo que possa ser executado novamente. Configure uma armadilha com alertas quando acionada. Com o tempo, isso se tornará seu manual de segurança.

Conclusão

Não há como saber se a rede está completamente livre de ameaças. Isso não significa que a busca seja inútil. O benefício de fazer threat hunting, além de desenraizar ameaças que conseguiram passar pelas suas defesas, é que você pode melhorar ainda mais a postura de segurança.

Pense em threat hunting como se fosse um pedreiro. Ao construir uma casa, comece com o primeiro círculo de tijolos, adicione argamassa para mantê-los no lugar e, em seguida, adicione outra camada de tijolos. Repita o processo camada por camada, construindo as paredes.

Com threat hunting, a primeira camada de tijolos pode estar ativando o registro e o armazenando. A argamassa é a automação que mantém os logs chegando regularmente. A próxima camada de tijolos compara logs com IoCs. Automatize esses processos para manter os tijolos no lugar. Continue aprendendo com as camadas de análise de dados, testando teorias etc.

Em breve, você criará um processo de busca de forte e estável que lhe dará a tranquilidade de saber que a empresa sempre vai estar tão livre de ameaças quanto o ambiente estiver.

Ferramentas de Threat Hunting

A seguir, estão algumas ferramentas recomendadas que podem ser usadas para threat hunting. Embora a lista esteja longe de ser finita, elas ajudarão quando forem usadas.

Cisco Threat Response

O Cisco Threat Response automatiza as integrações com todos os produtos de segurança da Cisco e aplica a inteligência de ameaças do Cisco Talos e de fontes de terceiros aos eventos de segurança, para pesquisar automaticamente os indicadores de comprometimento (IoCs) e confirmar ameaças rapidamente. Também oferece a capacidade de coletar e armazenar informações de investigação importantes, gerenciar e documentar o progresso e as descobertas e corrigir ameaças diretamente no painel.

Cisco Threat Grid

O Threat Grid combina sandbox avançado com inteligência de ameaças em uma solução unificada para proteger as empresas contra malware. Com uma base de conhecimento robusta e contextual sobre malware, você vai entender o que o malware está fazendo, ou tentando fazer, qual o tamanho da ameaça e como se defender dela.

Cisco Stealthwatch

O Cisco Stealthwatch é uma solução abrangente de visibilidade e tráfego de rede e análise de segurança de nuvem. E pode até detectar malware no tráfego criptografado sem descriptografá-lo. Oferece detecção avançada de ameaças, resposta acelerada a ameaças e segmentação de rede simplificada, usando aprendizado de máquina multicamada e modelagem de entidades. Com análises comportamentais avançadas, você pode descobrir quem está na rede ou na infraestrutura de nuvem pública e o que eles estão fazendo.

Cisco Advanced Malware Protection (AMP) for Endpoints

O AMP não apenas protege os endpoints, mas pode ajudar na análise de malware e na busca proativa de ameaças. Os recursos de pesquisa robustos do AMP permitem encontrar várias informações, como arquivo, hash, URL, endereço IP, chaves de registro, usuários, processos, aplicações e muito mais. Também pode mostrar o ciclo de vida de um arquivo no ambiente, desde a primeira vez que foi visto, o que fez no endpoint e outras informações.

Umbrella Investigate

O Investigate oferece a visão mais completa das relações e da evolução dos domínios, IPs, sistemas autônomos (ASNs) e hashes de arquivo. Acessível por meio do console da Web e da API, a inteligência de ameaças avançada do Investigate adiciona o contexto de segurança necessário para descobrir e prever ameaças.

Ferramentas de segurança das informações e gerenciamento de eventos (SIEM)

Ter um SIEM é um passo fundamental na realização de atividades de threat hunting, especialmente ao começar. Um SIEM bem configurado pode reduzir consideravelmente a quantidade de tempo gasto coletando arquivos de log e realizando análises básicas. Alguns exemplos de SIEMs bem conhecidos são Splunk, IBM QRadar e Exabeam.

Ferramentas de monitoramento de endpoint

Há uma série de ferramentas disponíveis para coletar registros detalhados de endpoints. O log de eventos integrado do Windows é um bom lugar para começar, e ferramentas mais complexas, como Sysmon e Monitor de processo, podem estender os recursos de log. (Há até configurações previamente criadas para ajudá-lo a começar.) Em Macs da Apple, cheque o console para ver os logs.

Analisadores de pacotes

São ferramentas que podem ser usadas para monitorar o tráfego de rede. Aplicativos (como Wireshark e tcpdump) e APIs (como pcap) são ferramentas bastante usadas para coletar informações sobre os dados que estão sendo transferidos em toda a rede.

O Cisco Cybersecurity Series

Ao longo da última década, a Cisco publicou uma série de informações sobre inteligência de ameaças para profissionais de segurança interessados no status global da segurança digital. Estes relatórios abrangentes têm fornecido detalhes dos cenários de ameaças e as implicações para as empresas, bem como as melhores práticas para se defenderem contra os impactos das violações de dados.

Na nova abordagem da nossa liderança de pensamento, a Cisco Security está publicando vários artigos baseados em pesquisas e orientados por dados sob o banner Cisco Cybersecurity Series. Ampliamos o número de títulos para incluir relatórios diferentes para profissionais de segurança com interesses diferentes. Apelando para a profundidade e amplitude da experiência de pesquisadores de ameaças e inovadores no setor de segurança, a coleção anterior de relatórios da série 2019 inclui o Relatório de Privacidade de Dados, o Relatório de Ameaças, o Relatório de Referência do CISO, o Relatório de Segurança de e-mail, e outros ainda virão ao longo do ano.

Para obter mais informações e todos os relatórios e cópias arquivadas, acesse www.cisco.com/br/securityreports.

Sede nas Américas
Cisco Systems, Inc.
San Jose, CA

Sede na Ásia-Pacífico
Cisco Systems (USA) Pte. Ltd.
Cingapura

Sede na Europa
Cisco Systems International BV Amsterdam,
Holanda

A Cisco possui mais de 200 escritórios em todo o mundo. Os endereços, números de telefone e de fax estão disponíveis no site da Cisco www.cisco.com/go/offices.

Publicado em agosto de 2019 THRT_05_0819_r1