THREAT HUNTING:
A CAÇA ÀS AMEAÇAS OCULTAS

Postura proativa de busca às vulnerabilidades é tendência em segurança da informação

2S
Transforme sua empresa com tecnologia

cisco
Gold Partner

ÍNDICE

1. INTRODUÇÃO

Renato Carneiro
Presidente da 2S Inovações Tecnológicas

Mais que um lema para todo profissional que trabalha com segurança da informação, a frase “não existe sistema 100% seguro” deve ser encarada como um ponto de partida para a busca permanente e insistente por ameaças. A necessidade de investimento em especialistas e sistemas de detecção, prevenção e monitoramento existe porque não há profissional infalível, ou ferramenta capaz de garantir percepção total de ameaças - o que não significa uma derrota, mas sim a oportunidade de estar em alerta constante.

Se um equipamento é capaz de enxergar 99% das possíveis falhas, o 1% restante pode significar um risco ainda maior – afinal, as ameaças que normalmente “furam” as defesas convencionais são justamente as mais avançadas, direcionadas a ambientes específicos e capazes de causar os maiores estragos.

O assunto chama atenção das empresas na medida em que, apesar de todo esforço - e investimentos - em segurança da informação, o cibercrime causou prejuízos estimados entre US$ 445 bilhões e US$ 600 bilhões em todo o mundo em 2016, segundo estudo divulgado recentemente pela McAfee. O montante representou até 0,8% do Produto Interno Bruto (PIB) mundial naquele ano.

Esse cenário contextualiza as táticas de combate às ameaças virtuais, particularmente no se que refere ao threat hunting (caça às ameaças, na tradução literal). Trata-se de um termo relativamente novo e de uma abordagem de segurança da informação que pressupõe a postura proativa, garimpando ameaças que já tenham ultrapassado as defesas iniciais e estejam instaladas no ambiente de rede da organização.

O threat hunting é um trabalho bastante sofisticado, que não depende apenas de software e hardware reativos, mas também de pessoal qualificado, profundo conhecimento do cenário global de ameaças e, principalmente, paciência para identificar sinais de anormalidade de ameaças que talvez sequer tenham se manifestado.

Mas, afinal, o que é exatamente o threat hunting e como ele funciona?

2. POR DENTRO DO THREAT HUNTING

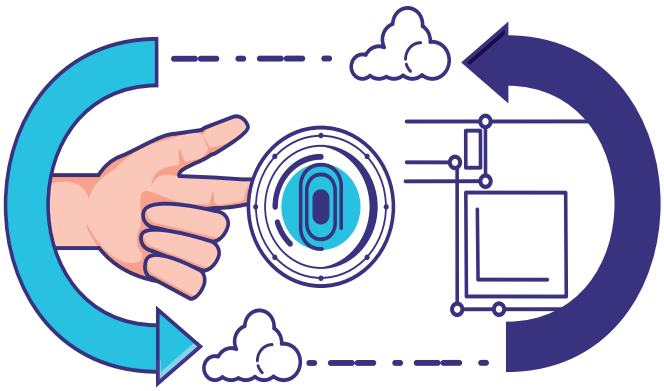
Imagine um vírus feito sob medida para uma empresa ou organização - uma ameaça que considera as peculiaridades do ambiente de computação de, por exemplo, uma instituição financeira, e que seja baseada no que há de mais moderno em termos de linguagem e método de infiltração.

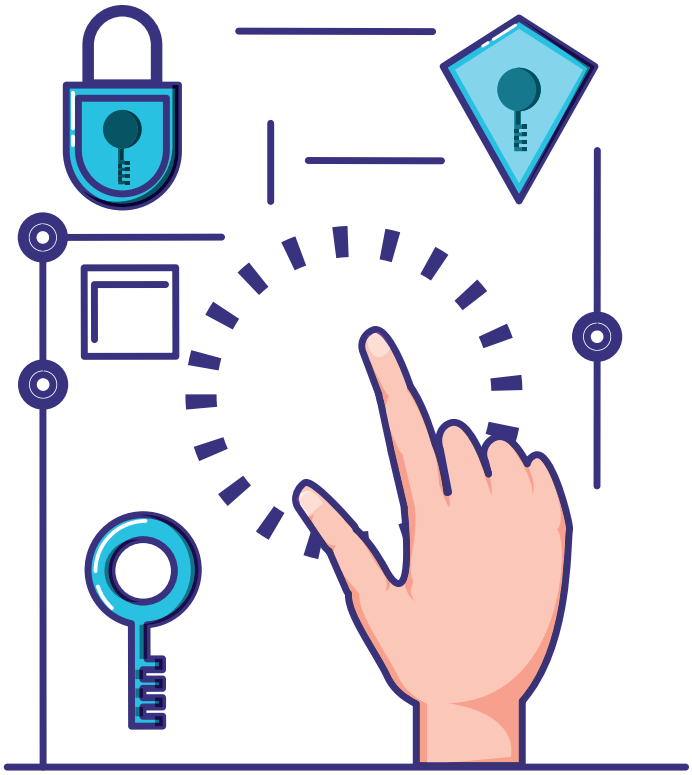
Esse vírus é enviado por e-mail para uma pessoa do RH, disfarçado de currículo. Um comando é executado assim que o funcionário abre a mensagem e rapidamente se espalha para outras máquinas conectadas. Aparentemente, nada muda para os usuários, mas os cibercriminosos agora têm acesso aos dados dessa organização sem que os antivírus ou firewalls sejam um obstáculo.

Mesmo companhias em tese superprotegidas podem ser vítimas de ataques direcionados. O caso da RSA, empresa especialista em tokens de segurança, é emblemático. Em 2011, grupos hackers provavelmente financiados por governos acessaram os geradores de senha usados por fabricantes de armas do exército norte-americano. Ou seja, o *core business* da companhia foi diretamente afetado, e os danos financeiros (e de reputação) foram incalculáveis.

2. POR DENTRO DO THREAT HUNTING

Como os hackers conseguiram? Um simples e-mail com duas frases (“Estou encaminhando o arquivo para sua revisão. Por favor, abra e visualize-o”) e um arquivo de Excel chamado “2011 Recruitment Plan” (Plano de Recrutamento 2011)”. O receptor do e-mail não só foi engenhosamente enganado como a ameaça foi desenhada especialmente para o ambiente daquela companhia.





Somente uma busca ativa, utilizando ferramentas modernas e executada por um profissional especializado, seria capaz de encontrar malwares deste tipo depois da infecção. Em poucas palavras, o threat hunting é a busca capaz de encontrar ameaças ignoradas por defesas tradicionais. E esses gargalos existem porque as ferramentas convencionais são reativas, ou seja, agem apenas quando uma ameaça é detectada. O threat hunting, por sua vez, não ocorre necessariamente quando se encontra um incidente na rede, ou quando se enxerga algo diferente acontecendo no ambiente de uma organização. O processo utiliza esses indícios, mas não há ponto de partida preciso, muitas vezes.

O objetivo, afinal, é localizar ameaças avançadas e sofisticadas, que impõem formas de ação inusitadas e personalizadas para cada alvo. Ameaças comuns são conhecidas e catalogadas, podendo ser identificadas por antivírus comuns; as avançadas, por sua vez, são capazes até mesmo de criar mutações para não serem percebidas.

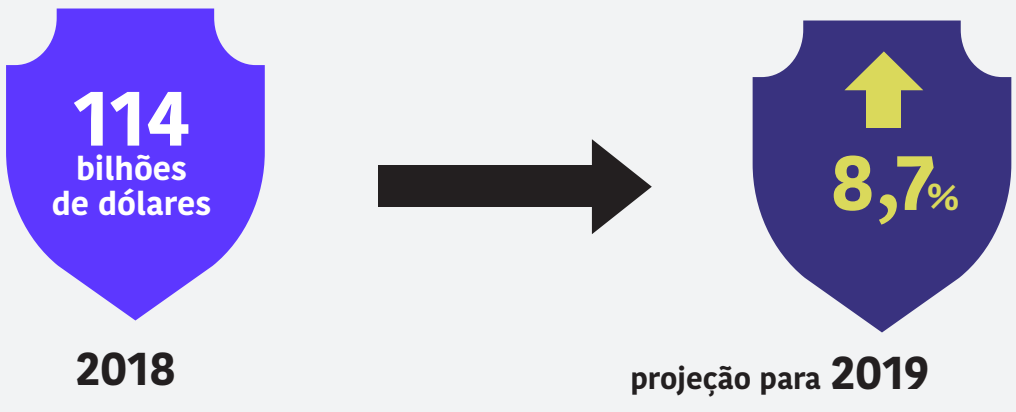
2. POR DENTRO DO THREAT HUNTING

Assim, o threat hunting é uma soma de ferramentas e ações executadas por humanos. Esses profissionais são especialistas com conhecimento metodológico profundo e qualificações específicas, e podem enxergar o que está acontecendo em uma rede ou ambiente de TI, ao mesmo tempo em que identificam comportamentos ou indícios de ameaças de acordo com informações colhidas em bases de inteligência.

Essas bases externas normalmente são propriedade de empresas especialistas em segurança, e as origens dessas informações são diversas. A Cisco, por exemplo, possui o Talos Intelligence Group, um dos mais importantes times comerciais de inteligência sobre ameaças do mundo, formado por analistas, pesquisadores e engenheiros. Esse time trabalha não só na identificação de ameaças, mas também faz a engenharia reversa para entender como elas funcionam e operam no ambiente, quais técnicas, procedimentos e ferramentas são utilizados para isso, entre outras informações, desde as mais simples até as mais complexas. Os dados são, então, catalogados e passam a integrar a base utilizada por especialistas de threat hunting no mundo todo.

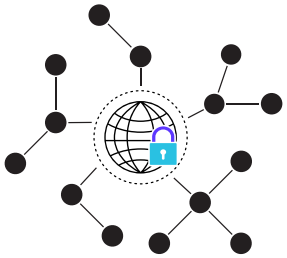
Ainda não há estudos ou relatórios que estimem o tamanho do mercado de threat hunting no mundo ou no Brasil, mas analistas e consultorias acompanham a tendência de perto. Afinal, o mercado de segurança da informação é imenso – cerca de US$ 114 bilhões em 2018, segundo o Gartner, com crescimento de 8,7% projetado para este ano.

Mercado de segurança da informação:



3. FERRAMENTAS E METODOLOGIA

Emanuel Almeida, engenheiro consultor de sistemas da Cisco Advanced Threat Solutions, explica que o threat hunting pode começar de três formas, a partir de:



1. INTELIGÊNCIA

Especialistas incluem uma ameaça nas bases de informação que é de interesse dos operadores de segurança. Eles verificam se há indicadores de comprometimento no ambiente que monitoram.

2. MUDANÇAS DE COMPORTAMENTO NO AMBIENTE

Ocorre com a orientação analítica e situacional, ou seja, a partir de mudança no comportamento de conexões entre máquinas ou links de internet, por exemplo. Um consumo muito alto de internet pode ser uma situação atípica e indicar um problema, servindo como ponto de partida para uma investigação.

3. INDICAÇÃO DE EQUIPAMENTOS REATIVOS

Baseada em alertas gerados por mecanismos de segurança reativos, como um firewall ou ferramenta analítica de comportamento. Quando é encontrado um dado anormal, surge-se uma hipótese para investigação.

Fonte: Emanuel Almeida, Cisco

3. FERRAMENTAS E METODOLOGIA

É importante notar que a orientação é só o início de uma investigação - e seus rumos podem ser imprevisíveis. Um evento apontado por um firewall, por exemplo, pode levar a outros malwares hospedados em um site, que estão igualmente infectando o ambiente monitorado. Uma informação adicional pode mudar os rumos de uma “caçada”.

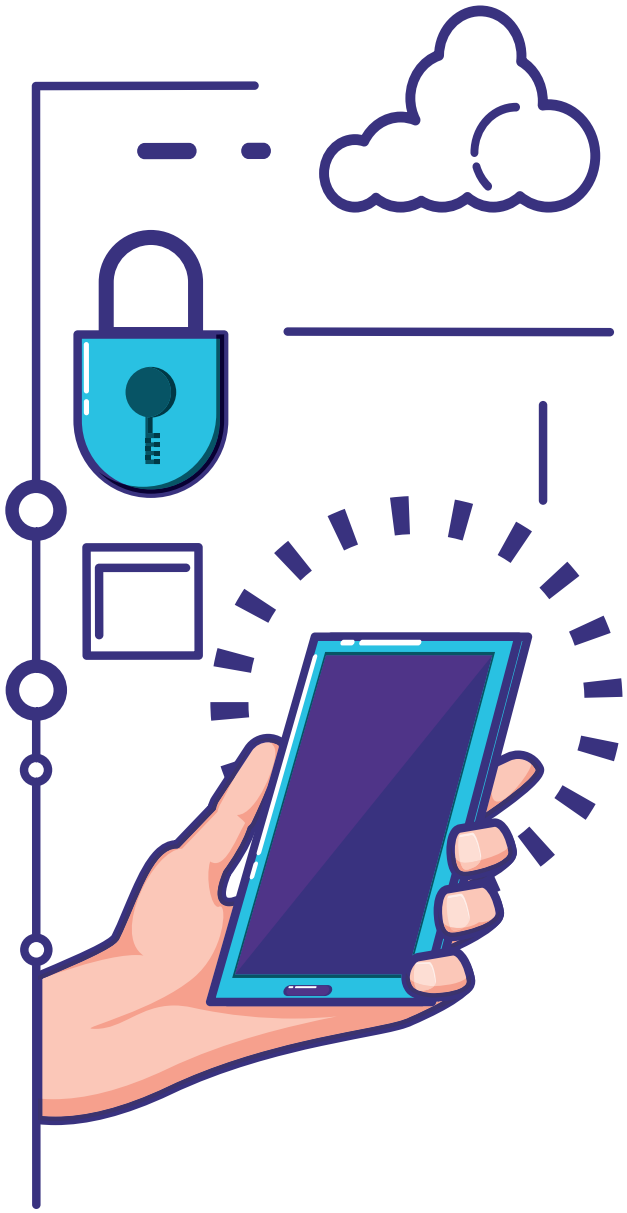
Nesse contexto, a visibilidade do ambiente como um todo, explica Almeida, facilita o trabalho de threat hunting. Essa visão integral ajuda a fazer a correlação de eventos com as bases de inteligência externas. Quanto mais fontes de informação de inteligência e sobre os ambientes monitorados, e quanto maior a qualidade dessas fontes, melhor.

Não existe uma única ferramenta que automatize o threat hunting, muito menos uma receita que sirva para detecção de todo tipo de ameaça. O ideal é cobrir todo o ambiente com monitoramento reativo e detecção proativa, mantendo proteção para pontos de acesso (endpoints), com antivírus tradicionais e outros recursos mais avançados, como motores comportamentais, que identifiquem condutas estranhas de usuários.

Integrar ferramentas de segurança tradicionais e ter capacidade de extrair dados analíticos delas é fundamental. Não adianta fazer o monitoramento reativo e não compartilhar os resultados com outros sistemas. E um dos caminhos para obter essa integração é por meio de APIs (Application Programming Interface), ou Interface de Programação de Aplicativos. Fabricantes como a Cisco têm apostado nos últimos anos em criar um portfólio de segurança abrangente, por meio de aquisições de empresas. O objetivo é proteger não só gateways web ou de e-mail, mas também detectar ameaças conhecidas e desconhecidas por meio de visibilidade da rede, não só dos dispositivos nela conectados.

4. BENEFÍCIOS E LIMITES

O threat hunting não veio para substituir outras tecnologias de segurança da informação. Ao contrário, ele reforça a importância de software e hardware especializados, na medida em que eles automatizam atividades mais simples e facilitam a vida dos gestores criando eventos e bloqueios, por exemplo.



Mas, por outro lado, toda operação de segurança não pode depender só desses pilares. Automação e orquestração permitem aos profissionais se livrarem de tarefas corriqueiras e repetitivas, concentrando-se em atividades mais estratégicas – como o threat hunting. Alguém precisa buscar o que é desconhecido.

Essa tarefa exige pessoas com conhecimento específico e apurado das ferramentas da organização. Se elas trabalham para um banco, por exemplo, precisam saber como extrair informações do ambiente e como operar as ferramentas de segurança, além de correlacionar eventos com as bases de inteligência disponíveis. E há certificações disponíveis no mercado para qualificar os profissionais interessados.

O responsável por executar as atividades de threat hunting deve, ainda, conhecer a metodologia a fundo, criando hipóteses com diferentes orien-

4. BENEFÍCIOS E LIMITES

tações. Construir e executar hipóteses é grande parte do trabalho de cientista. Não é fácil buscar algo que ainda não se conhece ao certo.

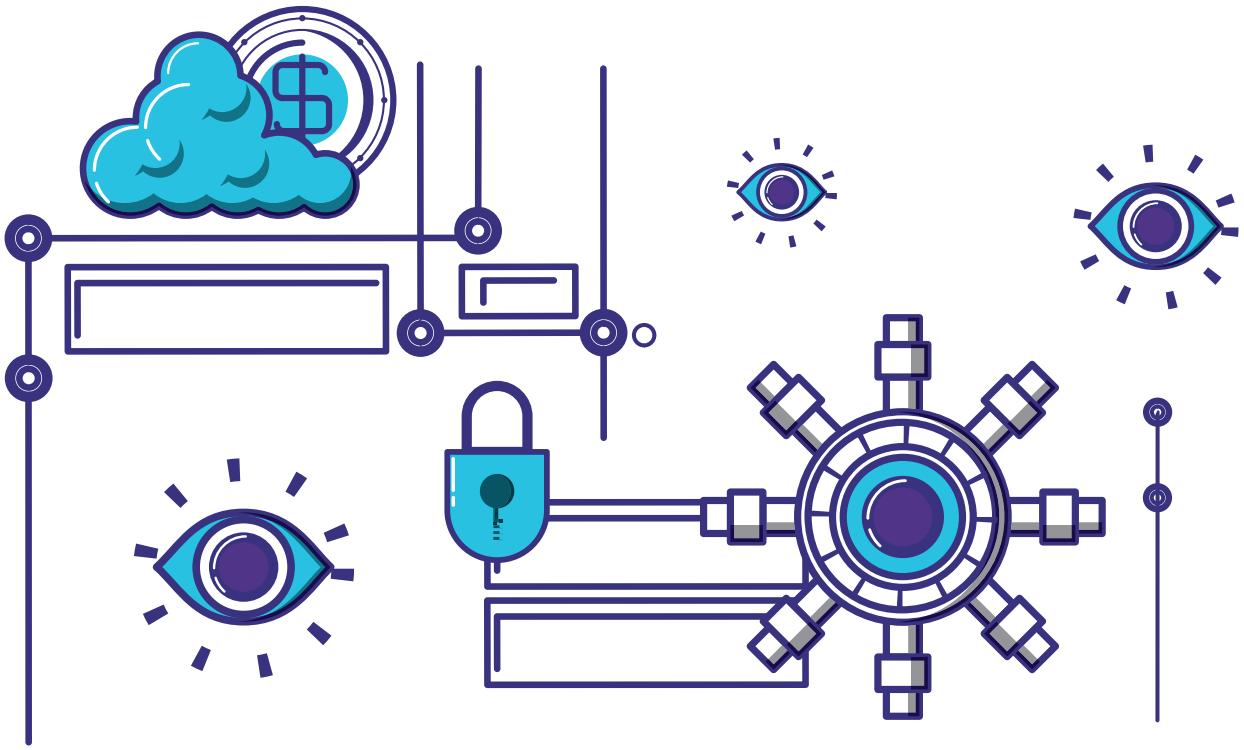
Por essa complexidade, há duas opções de implementação: a empresa pode ter uma estrutura interna de threat hunting, executada, por exemplo, por um funcionário do time de monitoramento, que tem facilidade para enxergar o ambiente como um todo. Ou pode, ainda, contratar serviço externo. Mas há um alerta: é necessária estreita colaboração entre times interno e externo para que ambos aprendam juntos sobre o ambiente de rede da empresa monitorada, executando “caçadas” de forma recorrente.

Apesar da sofisticação, os benefícios do threat hunting são extensíveis para qualquer organização. Afinal, as ameaças (e os criminosos) não têm preconceitos e afetam empresas de todos os segmentos e portes. Aliás, para especialistas, a ameaça é até maior para as pequenas e médias que costumam não ter uma parcela dos orçamentos destinados à segurança da informação, e não calculam o prejuízo decorrente de vazamento de dados.

Mas há um porém: a falta de tecnologias e pessoal adequados pode inviabilizar o threat hunting. Ferramentas de detecção, profissionais qualificados e dedicados à atividade, além de acesso à base de inteligência são fundamentais para que o modelo funcione - e requerem investimento. Apesar disso, parte das empresas brasileiras, principalmente as grandes, têm adquirido grau de maturidade suficiente para considerar o investimento em threat hunting. Diante dos riscos crescentes, elas buscam esse tipo de proteção.

Bancos e instituições financeiras são os principais interessados, além de empresas de telecomunicações, graças principalmente à natureza sensível dos dados que guardam. Possuem, assim, um nível de maturidade maior em segurança, com times de resposta a incidentes, monitoramento e análise forense já estabelecidos. Essa não é, no entanto, a realidade da maioria das empresas.

5. VALE INVESTIR EM THREAT HUNTING?



Muitas vezes relegado na composição do orçamento de tecnologia, a falta de investimento em segurança da informação pode custar caro em casos de crise. Os prejuízos podem não ser só financeiros, mas de confiança e imagem – custos, muitas vezes, intangíveis, mas unanimemente altos.

O threat hunting, portanto, vale a pena para empresas cuja guarda de dados é o principal ativo. Ele permite uma postura de segurança mais forte, que cobre até mesmo ameaças feitas sob medida, por meio de uma abordagem proativa. Aumenta ainda a confiança sobre o que realmente acontece no ambiente de rede, dando maior visibilidade e compreensão da infraestrutura.

Quando se fala de ferramentas reativas, o mercado é profícuo em fornecer as melhores soluções. Mas, por mais eficientes que sejam, existem ameaças que se aproveitam da falsa sensação de segurança para atuarem discretamente. Elas só podem ser encontradas com ações proativas, identificando o que os gestores de rede acreditam que não pode estar acontecendo.

Em suma: adquirir novas ferramentas e contratar especialistas em threat hunting não será mais caro do que um dano público à sua reputação.

CSO, para que te quero?

Por Carlos Monaco*

Com ele à frente da segurança, é mais fácil planejar, definir e implementar estratégias efetivas; só na América Latina, o gap de talentos na área deve chegar a 185 mil profissionais até 2022

Diante dos ataques recentes que paralisaram companhias de todo o mundo, os CEOs têm colocado a segurança da informação como prioridade na agenda, cobrando atuação efetiva e imediata dos CIOs. Percebe-se, por exemplo, muitas empresas que não tinham uma área dedicada à proteção, muito menos um CSO (Chief Security Officer), começarem a olhar com mais atenção para o assunto.

Segundo um levantamento do Centro de Cibersegurança e Educação, ligado ao (ISC)², principal instituto voltado à educação e certificações profissionais em cibersegurança, feito com mais de nove mil companhias, 70% das organizações não têm o número suficiente de profissionais de segurança para enfrentar os desafios com os quais se deparam atualmente. Além disso, o gap de talentos na área deve atingir 1,8 milhão em 2022, um aumento de 20% em relação a 2015. Na América Latina, a escassez deve chegar a 185 mil profissionais até 2022.

Contar com uma equipe dedicada apenas à proteção de dados é vital nos dias de hoje quando as ameaças têm sido frequentes e estão a cada dia mais sofisticadas, com hackers bem preparados e com conhecimento profundo sobre o nível de proteção de seus alvos. Com o CSO à frente da segurança da empresa, fica mais fácil planejar, definir e implementar estratégias realmente efetivas já que ele é o mais capacitado para entender as informações que circulam na empresa e identificar o nível de importância de cada uma, com o apontamento de possíveis riscos e brechas.

No caso de uma invasão, o CSO consegue colocar de maneira mais rápida o plano em prática utilizando as soluções certas para combater os hackers. Além de conscientizar os profissionais sobre o que é seguro ou não e quais as responsabilidades de cada um na proteção da companhia, ele pensa no antes – para prevenir o problema – e no depois – para minimizar os danos e prejuízos caso o ataque aconteça.

** Carlos Monaco é diretor de vendas da 2S.*

7. CONTATOS

Renato Carneiro
Presidente

João Paulo Wolf
Diretor de Soluções e Serviços

Gisele Braga
Gerente de Transformação Digital

www.2s.com.br

essense
sharing knowledge