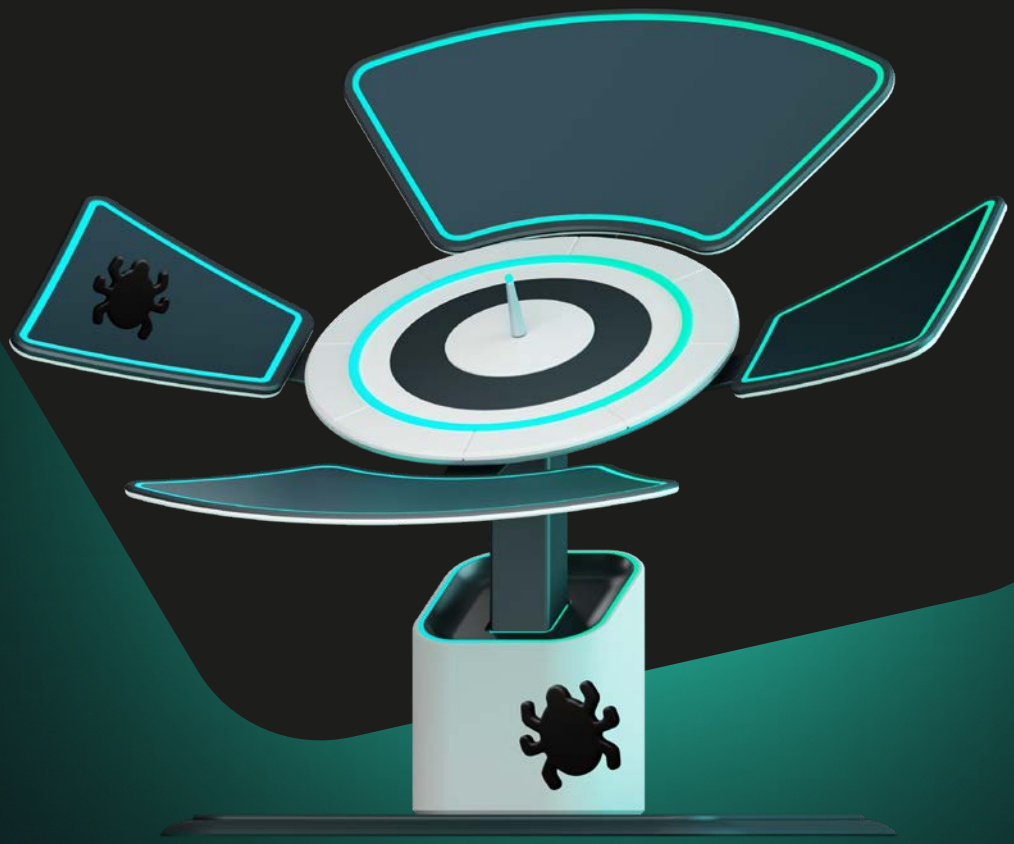
kaspersky



Análise de dados históricos em operações de segurança: o papel da busca retrospectiva

Este artigo foi escrito por Sergey Soldatov, chefe do Centro de Operações de Segurança da Kaspersky. Ele aborda a função essencial da identificação proativa de ameaças na detecção de ameaças persistentes avançadas (APTs) que conseguem burlar soluções de segurança automatizadas, destacando-a como um componente essencial da estratégia de detecção e resposta de um SOC moderno. Com base em práticas de detecção do mundo real, o artigo destaca como a identificação proativa de ameaças complementa as operações do SOC baseadas em alertas por meio de uma análise retrospectiva e de uma investigação baseada em hipóteses, utilizando dados de telemetria como logs de EDR/NDR.

A identificação proativa de ameaças é a única forma de reconhecer ameaças persistentes avançadas (APTs), pois ela consegue identificar ameaças que não foram detectadas e remediadas por soluções de detecção automatizadas. As APTs são projetadas com cuidado, e os atacantes conhecem os controles de segurança que precisam contornar para não ser detectados. Portanto, a identificação proativa de ameaças preenche a lacuna entre os ataques realizados e a capacidade de detecção das soluções de segurança automatizadas. Ela assume que a segurança da infraestrutura que está sendo monitorada foi comprometida e, então, tenta comprovar a violação. Essa suposição de que a segurança foi comprometida significa que as soluções de segurança existentes falharam. Portanto, a única forma de encontrar a origem da violação é por meio da análise manual de logs. Um analista precisa de logs detalhados de atividades em sistemas operacionais (SO) e redes, e esses logs semelhantes ao EDR/NDR são conhecidos como "telemetria", que são dados brutos utilizados para a lógica de detecção e a base para a identificação proativa de ameaças manual.

A identificação proativa de ameaças é semelhante à pesquisa de ameaças, em que especialistas tentam detectar atividades suspeitas usando telemetria de sensores da Internet. Em seguida, eles fazem uma investigação para garantir que se trata de uma ameaça genuína e, então, fornecem a lógica de detecção. É basicamente assim que a pesquisa de malware funciona. No entanto, as APTs são diferentes para cada vítima. É impossível encontrá-las na Internet, pois elas existem apenas na infraestrutura da vítima. A identificação proativa de ameaças é uma pesquisa de ameaças operacionalizada que é adaptada a uma infraestrutura específica. Ela permite a descoberta de ameaças avançadas que burlaram as soluções de segurança.

Mas quando se fala em segurança, sempre há uma compensação, e a engenharia de detecção não é exceção: uma maior sensibilidade da lógica de detecção significa uma maior ocorrência de falsos positivos (FPs) para a equipe do SOC analisar. É por isso que, na prática, a lógica de detecção é dividida em função da precisão, ou seja, em função da taxa de verdadeiros positivos (TPR) das regras de detecção. Cada organização tem diferentes tipos de lógica de detecção. Isso pode ser baseado em padrões de comportamento atômico na telemetria, como o início de um processo ou as conexões de rede. Também pode envolver uma sequência complexa de eventos de telemetria atômica, como o início de um processo com reputação desconhecida após um login de rede bem-sucedido que foi precedido por várias tentativas fracassadas.

Costuma-se dizer que a lógica de detecção "caça" comportamentos maliciosos. Embora o termo oficial seja "indicadores de ataque" (IoAs), vamos chamá-los de "detectores" para facilitar a compreensão. TPR é a característica da precisão de um detector, ou seja, a proporção entre os verdadeiros positivos do detector e o total de detecções (verdadeiros positivos mais falsos positivos). Detectores com uma taxa alta de TPR (e, portanto, com um número baixo de falsos positivos) podem ser convertidos em alertas que serão analisados pela equipe do SOC. Detectores que geralmente geram FPs, mas que ainda são um indicador importante de ataques realizados, são usados para enriquecer a análise de eventos suspeitos.

Anteriormente mencionamos que a identificação proativa de ameaças é conduzida sob a suposição de que já ocorreu uma violação, o que significa que ela é conduzida como uma busca retrospectiva em dados históricos. Na prática, ela é executada como um processo interno dedicado dentro do SOC, geralmente por analistas de nível dois. Os analistas de nível um são responsáveis pelo processamento de alertas operacionais dentro de um tempo de processamento de alerta predefinido, que geralmente é especificado em um contrato de nível de serviço. Para realizar uma identificação proativa de ameaças retrospectiva, é preciso aprender a identificar um ataque ou uma atividade suspeita, e entender quais rastros podem ter sido deixados na telemetria coletada. Ao identificar possíveis rastros, a equipe do SOC formula hipóteses sobre o que pode ser considerado um IoC ou IoA. Na prática, há inúmeras hipóteses possíveis. Há todo um banco de dados de hipóteses onde elas são classificadas com base na TPR, cenários de uso e outros parâmetros. Os detectores mencionados acima com uma TPR baixa (que não são implementados como lógica de alerta e usados para análises futuras) são utilizados nas hipóteses. Isso representa a compensação: não implementaremos detectores com baixa TPR em alertas, para não sermos sobrecarregados pela quantidade de falsos positivos que consomem a capacidade de investigação da equipe do SOC.

Detectores com baixa TPR são propensos a gerar muitos falsos positivos e, portanto, são negligenciados de propósito como parte da lógica de alerta em tempo real. Incluí-los sobrecarregaria a equipe do SOC com alertas falsos, reduzindo sua eficiência. No entanto, o valor gerado por esses detectores não é completamente descartado. Em vez disso, eles são usados para dar suporte à identificação proativa de ameaças baseada em hipóteses, na qual os analistas fazem uma revisão periódica dos dados para procurar ameaças furtivas (ou menos óbvias) que podem não acionar alertas de alta confiança. Portanto, esses detectores contribuem para a detecção de ameaças, mas de uma forma que não prejudica a capacidade operacional. A combinação da detecção baseada em alertas com a identificação proativa de ameaças baseada em hipóteses oferece uma estratégia equilibrada e abrangente. Confiar apenas em alertas aumenta o risco de ameaças perdidas (falsos negativos), enquanto confiar apenas na busca manual atrasa a detecção.

É claro que cada ameaça detectada manualmente é analisada e a lógica automática de detecção e correção é introduzida (se possível do ponto de vista técnico). Já explicamos que a identificação proativa de ameaças é a base para a pesquisa de ameaças utilizada para criar nossos detectores, e há pelo menos dois exemplos da sua utilização que tornam essa identificação indispensável. O primeiro exemplo são as ameaças completamente novas: apesar de serem raras, seu impacto pode ser enorme. Isso ocorre porque a implementação de ataques novos é extremamente cara, e o criminoso espera que ela seja lucrativa. Quanto mais complexo o ataque, mais caro é prepará-lo. Portanto, o investimento na preparação do ataque deve ser compensado pelo lucro para o criminoso, o que impacta diretamente no dano causado à vítima. Daí a dependência simples: quanto mais complexo o ataque, maior o dano potencial, pois o atacante deve compensar os investimentos no ataque.

O segundo exemplo é menos óbvio, mas muito comum na prática: cenários de "living off the land", em que os atacantes exploram ferramentas e recursos legítimos do sistema. Há muitos padrões de comportamento que são indistinguíveis de atividades legítimas e esses gatilhos não podem ser filtrados. Eles devem ser monitorados de forma contínua para garantir que se enquadram no escopo da atividade legítima do usuário, incluindo, quando necessário, entrar em contato com os usuários para esclarecer as circunstâncias.

Para concluir, é impossível superestimar os benefícios da busca retrospectiva para um SOC moderno. Abordamos apenas o essencial do importante processo do SOC, mas é o suficiente para gerar uma compreensão preliminar, e os detalhes se tornarão mais claros na prática.

Sobre a Kaspersky

A Kaspersky é uma empresa de privacidade digital e segurança cibernética global fundada em 1997. Com mais de um bilhão de dispositivos protegidos contra ameaças cibernéticas emergentes e ataques direcionados, a inteligência de ameaças profunda e a expertise em segurança da Kaspersky estão constantemente se transformando em soluções e serviços inovadores para proteger empresas, infraestrutura crítica, governos e consumidores em todo o mundo. O portfólio abrangente de segurança da empresa inclui proteção de endpoint líder, produtos e serviços de segurança especializados, bem como soluções de imunidade cibernética para combater ameaças digitais sofisticadas e em constante evolução. Ajudamos mais de 200.000 clientes corporativos a proteger o que mais importa para eles. Saiba mais em www.kaspersky.com.

www.kaspersky.com.br