kaspersky BRING ON THE FUTURE

Não, o EDR não está morto. Mesmo assim, vida longa ao XDR!

O XDR (Extended Detection and Response) geralmente é descrito como uma evolução natural do EDR (Endpoint Detection and Response), com funcionalidades de defesa de alto nível que vão além do endpoint a fim de incluir a rede, a nuvem, o servidor e outras camadas. Alguns entusiastas do XDR foram ainda mais longe, declarando a morte do EDR com a ascensão do XDR como o rei da cibersegurança. No entanto, a realidade é muito mais complexa.

Com o XDR entrando no Gartner Hype Cycle pela primeira vez, nós decidimos analisar mais profundamente o relacionamento entre o EDR e o XDR. Nós revelaremos por que as fontes do mundo real (como a MITRE ATT&CK) provam que a função do EDR como um sensor de endpoints (entre outras coisas) dentro de uma solução de XDR continuará a ser essencial em qualquer solução de segurança corporativa integrada, unificada e eficaz.

Primeiro, vamos esclarecer algumas definições:

Endpoint Detection and Response (EDR)) refere-se a soluções que gravam e armazenam comportamentos de nível de sistema de endpoint, usam diversas técnicas de análise de dados para detectar comportamentos suspeitos do sistema, fornecem informações baseadas em contexto, bloqueiam atividades maliciosas e fornecem sugestões de neutralização para restaurar os sistemas afetados. Fonte: Gartner

Extended Detection and Response (XDR) descreve uma plataforma unificada de detecção e resposta a incidentes de segurança que coleta e correlaciona automaticamente dados de vários componentes de segurança proprietários. Fonte: Gartner

A palavra "unificado" é essencial para entender o relacionamento entre o EDR e o XDR . Em vez de substituir o EDR, o XRD unifica diversas formas de telemetria em uma única plataforma. E, obviamente, a detecção (e resposta) no nível do endpoint deve continuar no centro de qualquer solução de XDR. Honestamente, é impossível ter um bom XDR sem um ótimo EDR.

Táticas, técnicas e atenuações do MITRE ATT&CK – o endpoint ainda reina

A maioria das táticas (de 14) na matriz corporativa Mitre ATT&CK tem origem no endpoint, com exemplos óbvios que incluem o Acesso Inicial (TA0001) e a Execução (TA0002). Em termos de técnica, o abuso de scriptsPowerShell para execução depende do comprometimento do endpoint, assim como a exploração de aplicativos voltados ao público, e execução acionada por eventos, para mencionar apenas três. Por razões óbvias, a relevância do EDR para táticas e técnicas móveis e ainda mais duradoura.

Quando se trata especificamente de acesso inicial, mesmo as ameaças modernas mais avançadas ainda dependem, com frequência, de vetores básicos de ataque, como o comprometimento de e-mails corporativos (BEC, Business Email Compromise), que aumentou em quase 100% em 2019. O grupo Sofacy (APT28) usou links e anexos de spearfishing, inclusive para membros da Campanha de Clinton em 2016.

A centralidade do endpoint para agentes de APTs é sucintamente descrita nas palavras da acusação contra supostos membros do APT28 declaradas pelo Tribunal Distrital dos EUA:

- Porque eles estavam: "dedicados a direcionar e-mails de spearphising e outras atividades de invasão de **computador** para organizações militares, políticas, governamentais e não governamentais,".

- Porque eles "monitoraram disfarçadamente os **computadores** de dezenas de funcionários do DCCC e do DNC".

- Porque o objetivo da conspiração do grupo era "invadir os computadores de pessoas e entidades nos EUA envolvidas na campanha presidencial americana de 2016, roubar documentos desses **computadores** e fazer a divulgação dos documentos roubados para interferir na eleição presidencial americana em 2016".

Embora o XDR possa de fato ser uma evolução natural do EDR, ele não eclipsa o EDR, nem remove a necessidade dele. Em alguns sentidos, pode ser mais preciso dizer que o XDR é realmente o resultado da própria evolução do EDR para trabalhar com formas de telemetria que vão além do nível do terminal, como parte de uma plataforma unificada. Visto dessa forma, o EDR permanece no centro de qualquer plataforma XDR eficaz.

Mesmo a integração de soluções heterogêneas em uma ferramenta de gerenciamento de eventos e informações de segurança (SIEM) não resolve completamente o problema. Idealmente, os fluxos de trabalho de segurança devem ser conectados nativamente a ferramentas de detecção (como no XDR), em vez de gerenciados por uma ferramenta separada.

Embora o XDR possa realmente ser uma evolução natural do EDR, ele não ofusca o EDR, nem acaba com a necessidade dele. De certa forma, pode ser mais preciso dizer que o XDR é o resultado da própria evolução do EDR em relação ao trabalho com formas de telemetria que superam o nível do endpoint como parte de uma plataforma unificada. Dessa maneira, o EDR permanece no núcleo de qualquer plataforma de XDR eficaz.

Um pouco sobre o UES (Unified Enterprise Security)

One of the key benefits of XDR is that it removes the problem caused by traditional best-of-breed product buying – a lack of integration between solutions. This lack of integration causes a number of problems, including unmanageably excessive alerts, delayed (or missed) updates, and sub-optimal configurations.

O UES se uniu ao XDR ao entrar para o Gartner's Hype Cycle de segurança de endpoints pela primeira vez em 2020. De acordo com a Gartner, o UES "envolve a segurança de estações de trabalho, bem como smartphones e tablets, com um único produto" e "combina elementos do EDR, EPP e MTD". O UES não é uma classe de ferramentas ou soluções, mas uma abordagem que busca proteger todos os tipos de endpoints (computador, tablet, celular) com um único produto.

O fato de o UES ter entrado para o Hype Cycle ao mesmo tempo que o XDR não é uma coincidência. Ambos resolvem o problema da complexidade e refletem a urgente necessidade de integração e consolidação. Não é nenhuma surpresa que a pesquisa **Gartner's Security and IAM Solution Adoption Trend Survey, 2020**, descobriu que 25% das organizações de usuários finais estavam procurando por uma estratégia de consolidação de fornecedores.

A heterogeneidade e os limites da integração com SIEMs

Um dos principais benefícios do XDR é que ele remove o problema causado pela tradicional compra dos melhores produtos: a falta de integração entre as soluções. Essa falta de integração causa diversos problemas, incluindo a falta de capacidade de gerenciar alertas em excesso, atualizações atrasadas (ou esquecidas) e configurações inferiores.

Mesmo a integração de soluções heterogêneas com uma ferramenta de SIEM (Security Information and Event Management) não resolve completamente o problema. O ideal é que os fluxos de trabalho de segurança sejam conectados de modo nativo às ferramentas de detecção (como no XDR), em vez de serem gerenciados por uma ferramenta separada.

O EDR está exatamente no centro do XDR

É tentador interpretar o X em XDR não como "extended", mas como "cross", como em "Cross-layer Detection and Response". Afinal, o XDR representa uma extensão das funcionalidades de detecção e resposta entre as camadas de rede, dados, nuvem e, também, endpoint. As ferramentas de Endpoint Detection and Response continuarão no centro de qualquer solução de XDR.

Em uma olhada rápida na mais recente atividade do grupo que usa APTs detectada por nossa GReAT (Global Research and Analysis Team), os seguintes ataques e técnicas exigem a atenuação do EDR:

- O uso de um pacote ZIP malicioso contendo um pacote executável RAR malicioso com várias camadas de um **agente de ameaças desconhecido**. Em um dos incidentes, o pacote apresentava um tema de contenção da COVID-19.
- **DeathStalker** – usando intérpretes nativos do Windows para linguagens de script, como o powershell.exe e o cscript.exe.

Esses são apenas alguns exemplos de invasores que usam programas utilitários comuns para iniciar ataques contra determinados alvos. A visibilidade fornecida pelo EDR, particularmente (neste caso) de software, aplicativos e controles, pode proteger contra esse elemento do ciclo de ataques.

Os três pilares de todas as estratégias de proteção contra APTs bem-sucedidas

Nós incentivamos todos os nossos clientes corporativos com maturidade de TI a assegurar uma abordagem com empenho do que consideramos ser os três pilares de qualquer estratégia de segurança contra APTs. Ou seja, as equipes de segurança devem estar:

- **Equipadas:**
A cibersegurança é uma área de especialização em que até um profissional qualificado pode culpar legitimamente suas ferramentas. A proteção contra ataques multivetoriais e APTs exige uma plataforma consolidada unificada que forneça visibilidade total, eliminando silos obstrutivos e evitando o excesso de alertas e outras tarefas de rotina dentro do processo de resposta a incidentes.
- **Informadas:**
A especialização avançada existente das organizações com maturidade de TI nunca deve ser considerada como certa. Afinal de contas, o horizonte de crimes cibernéticos está em constante mudança e expansão. A educação contínua e a inteligência de ameaças robusta de um parceiro de cibersegurança confiável são essenciais.
- **Reforçadas:**
Quando uma APT é descoberta, até os analistas de segurança de TI mais avançados deveriam ter acesso a suporte externo para obter a opinião de terceiros, avaliação de segurança, busca de ameaças gerenciada e resposta a incidentes. Embora as APTs sejam altamente direcionadas, elas raramente visam apenas uma vítima. Especialistas externos podem lançar uma luz global de vários setores sobre os prováveis caminhos de uma APT e fornecer conselhos práticos sobre a melhor maneira de eliminá-la do sistema.

A Kaspersky entende os desafios envolvidos na defesa contra APTs e ameaças semelhantes. É por isso que nós criamos um conceito unificado que atende aos três pilares de uma estratégia de segurança contra APTs bem-sucedida. O Kaspersky Expert Security permite que sua equipe tenha menos trabalho com as ameaças sofisticadas e os ataques do tipo APT, atendendo aos desafios de discrição, persistência, silos e talento. Ele foi projetado e criado em torno de uma plataforma de XDR, tendo em mente organizações com segurança de TI madura. Ele apresenta recursos que aumentam os superpoderes da equipe interna de segurança de TI, incluindo inteligência de ameaças compreensiva, treinamento e orientação de especialistas.

Saiba mais sobre o Kaspersky Expert Security

Saiba mais sobre: kas.pr/expert-br

Kaspersky Expert Security

Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias de segurança de TI: business.kaspersky.com
Segurança de TI para pequenas e médias empresas: kaspersky.com/business
Segurança de TI para empresas: kaspersky.com/enterprise
Portal de inteligência de ameaças:: opentip.kaspersky.com
Ferramenta de portfólio interativo: kaspersky.com/int_portfolio

www.kaspersky.com.br

© 2021 AO Kaspersky Lab.
Marcas registradas e marcas de serviço são propriedade de seus respectivos proprietários.

Estamos comprovados. Somos independentes.
Nós somostransparente. Estamos empenhados em construir um ambiente mais seguro mundo, onde a tecnologia melhora nossas vidas. Qualé por isso que o protegemos, para que todos em todos os lugares tenham oportunidades infinitas que ele traz. Traga a segurança cibernética para um amanhã mais seguro.

Saiba mais em kaspersky.com/transparency

Proven. Transparent. Independent.