SANS

Um white paper da SANS

Por que a EDR tradicional não funciona — e o que fazer em relação a isso

Escrito por **Jake Williams**

Junho de 2019

Patrocinado por:

McAfee

Introdução

Se você trabalha com segurança da informação e não vive em uma caverna, certamente já ouviu falar de EDR. A EDR (Endpoint Detection and Response), ou detecção e resposta para endpoints, promete revolucionar a forma como os analistas de segurança neutralizam ataques. Infelizmente, tal como muitas outras soluções na área de segurança da informação, a EDR não correspondeu às expectativas.

Uma argumentação típica de venda de EDR seria algo assim: "Sim, sabemos que você pode verificar alertas no SIEM, abrir um tíquete de escalação no seu software de produtividade e avisar um administrador de sistemas para que ele tome uma providência. Mas no tempo que tudo isso leva, o atacante pode realizar uma invasão e se apoderar dos seus dados. O problema não é você não ter capacidade de detecção suficiente; o problema é isso estar espalhado por toda parte. Mesmo assim, como você responde a isso? Tempo é dinheiro, e o tempo está do lado do atacante. É por isso que você precisa da EDR. Ela consolida as funções de detecção e as funções de resposta em uma única plataforma."

Porém, como você provavelmente já adivinhou, a EDR não se mostrou à altura dessas expectativas otimistas.

Uma das maiores falhas nas distribuições de EDR é que a EDR não se integra simplesmente com as outras ferramentas (SIEM, IDS, DLP etc.) utilizadas pelos analistas de segurança. Outro problema comum em distribuições de EDR é a típica separação de papéis entre TI e segurança cibernética. A plataforma de EDR abrange ambas as linhas de negócios; a segurança cibernética desempenha tradicionalmente a função de detecção, enquanto a TI costuma assumir a função de resposta. Sempre que uma função de resposta é realizada, há algum risco de algum sistema ficar fora do ar.

Como a TI leva a culpa por qualquer indisponibilidade de sistema, faz sentido que ela seja tradicionalmente encarregada do gerenciamento de todas as funções de resposta. A EDR, ao abranger funções tradicionais de detecção e resposta, quebra esse paradigma, abrindo caminho para problemas com processos e fluxos de trabalho.

Mesmo havendo questões relacionadas a processos a serem resolvidas na organização, muitas plataformas de EDR são incapazes de funcionar como uma autêntica solução unificada conforme prometido pelo fornecedor. Em muitas plataformas de EDR falta integração com um SIEM. Outras são totalmente voltadas para o endpoint, negligenciando completamente o papel que o tráfego de rede desempenha tanto na eliminação de falsos positivos quanto na produção de um contexto valioso para alarmes positivos reais.

Nas seções seguintes, examinaremos outros desafios inerentes às plataformas de EDR tradicionais e o que se pode fazer para superá-los em uma implementação de EDR eficaz. Também apresentamos uma lista de itens a verificar que você deve levar em conta ao escolher e distribuir uma plataforma de EDR.

Causas-raízes das deficiências da EDR

Como muitos sistemas de segurança da informação, a EDR tem um histórico de não fazer jus às capacidades anunciadas. Da mesma forma que as distribuições de SIEM podem ser decepcionantes, esse resultado parece contraditório. Considerando-se produtos relativamente maduros, deve haver um traço comum às suas deficiências. Nesta seção e na figura 1, examinamos várias razões pelas quais os sistemas de EDR, quando distribuídos em campo, frequentemente descumprem o que é anunciado.

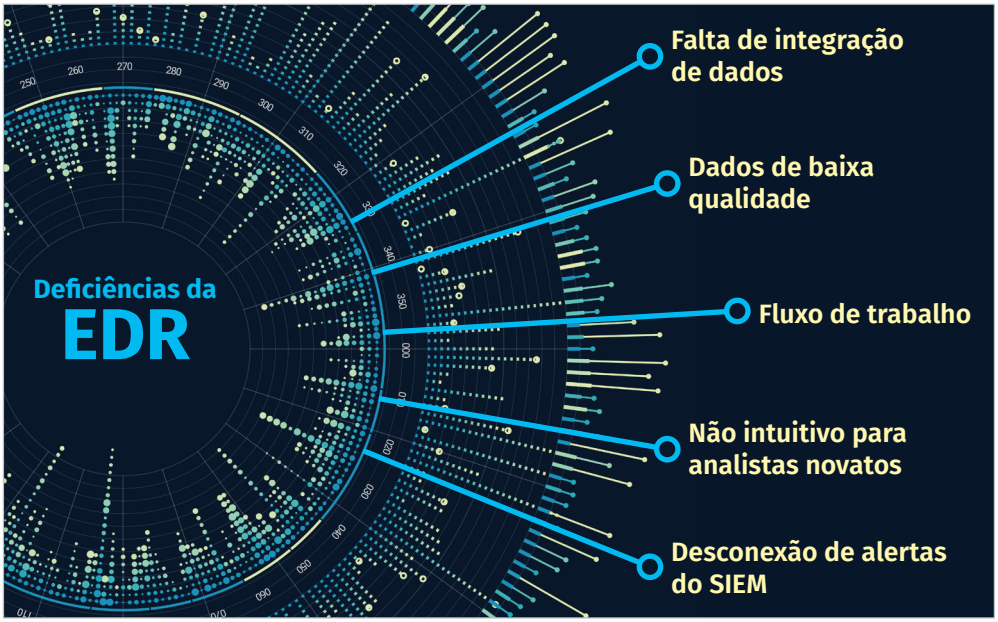

Figura 1. Deficiências da EDR

Falta de integração com dados de outras fontes

A primeira e talvez mais comum causa-raiz de falhas em distribuições de sistemas de EDR é a falta de integração com dados de outras fontes. Embora a integração mais frequentemente exigida com a plataforma EDR seja o SIEM, várias outras fontes de dados podem ajudar a enriquecer os alertas da EDR, bem como eliminar alarmes falsos positivos. Idealmente, as ferramentas de EDR deveriam integrar-se com:

- Logs de DNS
- Logs de fluxo de tráfego de rede ou NetFlow
- Logs de proxy de Web
- Dados de inventário de TI
- Resultados de varreduras de vulnerabilidades
- Logs de DHCP
- Informações de logon do Active Directory
- Logs de fornecedores de autenticação por múltiplos fatores

Embora a lista acima certamente não seja completa, a maioria das plataformas de EDR atuais não se integra com essas fontes de dados. Alguns fornecedores de EDR dirão que a maioria dos tipos de dados listados acima podem ser assimilados no sistema SIEM e que suas plataformas de EDR, por sua vez, integram-se com o SIEM.

Apesar disso, por que preferiríamos usar o SIEM através da EDR se essa é a única integração oferecida? Por que não simplesmente encaminhar os dados de EDR para o SIEM e analisar os dados lá? É uma possibilidade, mas trata a EDR como uma ED (uma ferramenta de detecção sem opção de resposta). Após decidirmos qual será a providência a ser tomada, precisamos mudar de contexto, do SIEM para a EDR, para realizar a ação de resposta. Esse fluxo de trabalho complicado não é compatível com a promessa de eficiência que inspirou a adoção de uma solução de EDR. Ele também posiciona a EDR como subordinada ao SIEM.

Dados de investigação de baixa qualidade

Dados investigativos de baixa qualidade são uma outra deficiência comum da EDR. Praticamente toda solução de EDR atualmente no mercado pode examinar dados de endpoint, como listas de processos, chaves e valores do Registro e conexões de rede ativas. Esses dados são valiosos na identificação de uma intrusão, mas os próprios dados são incompletos. Eles carecem do contexto que outras ferramentas (como um SIEM) utilizam para eliminar falsos positivos e destacar verdadeiros alertas positivos.

Um exemplo de dados de EDR de baixa qualidade que causam um alarme perdido é o do spray de senhas. Em um ataque de spray de senhas, o atacante tenta utilizar a mesma senha em várias contas do domínio (frequentemente todas elas). Sem a integração dos logs armazenados no SIEM, a EDR pode deixar passar esse ataque.

Dados de baixa qualidade não são uma característica de um sistema de EDR específico (ou mesmo dos sistemas de EDR em geral). Trata-se mais de uma questão de visibilidade. Os sistemas de EDR costumam analisar dados de um único endpoint de cada vez, enquanto um SIEM correlaciona dados de nível mais alto entre múltiplos endpoints (incluindo dados de rede). Muitas organizações esperam que uma EDR substitua um SIEM para detecções no endpoint, mas ficam decepcionadas ao descobrir que não estão tendo uma visão completa com a EDR.

Muitas alternâncias necessárias para concluir a análise de qualidade

Em muitos casos nos quais são realizadas investigações incompletas, todos os dados disponíveis para concluir uma investigação são disponibilizados para o analista. O problema fundamental é que o analista não percebe que os dados estão disponíveis por estar olhando para o lugar errado. Isso acontece frequentemente quando o sistema de EDR não possui integração com o SIEM. O analista recebe um alerta no sistema de EDR e, então, precisa alternar para o SIEM para obter dados adicionais. Infelizmente, os dados podem não estar armazenados no SIEM de uma maneira que propicie uma investigação fácil.

Uma causa comum para esse problema é o DHCP. Muitos logs no SIEM contêm apenas informações de endereços IP. Porém, outros logs contêm apenas informações de nome de host. Naturalmente, alguns logs contêm ambos. A maioria dos sistemas de EDR utiliza algum tipo de agente instalado no endpoint, portanto, a identificação de instalação é a que faz mais sentido como identificador exclusivo para o endpoint. No entanto, é improvável que essa informação seja capturada no SIEM, o que significa que são necessárias várias alternâncias para correlacionamento e alerta entre o sistema de EDR e o SIEM.

As coisas se complicam ainda mais quando os dados necessários não estão todos disponíveis no SIEM. Por exemplo, logs de DHCP (essenciais para correlação de outros dados valiosos) frequentemente não são sequer preenchidos no SIEM. Em outros casos, os logs de DHCP são encaminhados para o SIEM, mas têm uma retenção mais curta que outros dados que precisam dos logs de DHCP para fins de contexto. Cada alternância necessária para que o analista tenha uma visão completa do evento reduz a probabilidade de uma investigação abrangente.

Analistas novatos frequentemente não começam com o pé direito

Muitos sistemas de EDR decepcionam em aplicações do mundo real por oferecerem opções demais aos analistas. Essa abundância excessiva de opções de configuração pode sobrecarregar (e frequentemente sobrecarrega) analistas menos experientes.

Desde que a EDR encontrou seu lugar no ecossistema de segurança da informação como um todo, ela foi geralmente considerada como tendo um papel decisivo na consulta de endpoints. Enquanto isso, um SIEM tinha um papel passivo (assimilando e correlacionando dados de logs). Contudo, o papel ativo da EDR tem seu preço. O uso pleno da EDR exige que se saiba o que perguntar, uma questão que afeta desproporcionalmente os analistas novatos.

Você pode fazer perguntas ao SIEM, mas as suas opções limitam-se aos dados já armazenados. Essa limitação leva a algumas questões difíceis que os engenheiros precisam responder antes de um incidente, conforme mostrado na figura 2.

Embora possamos nos basear nas melhores práticas para responder a essas perguntas, é impossível responder a todas elas com precisão quanto a um incidente específico dentro de uma organização específica.

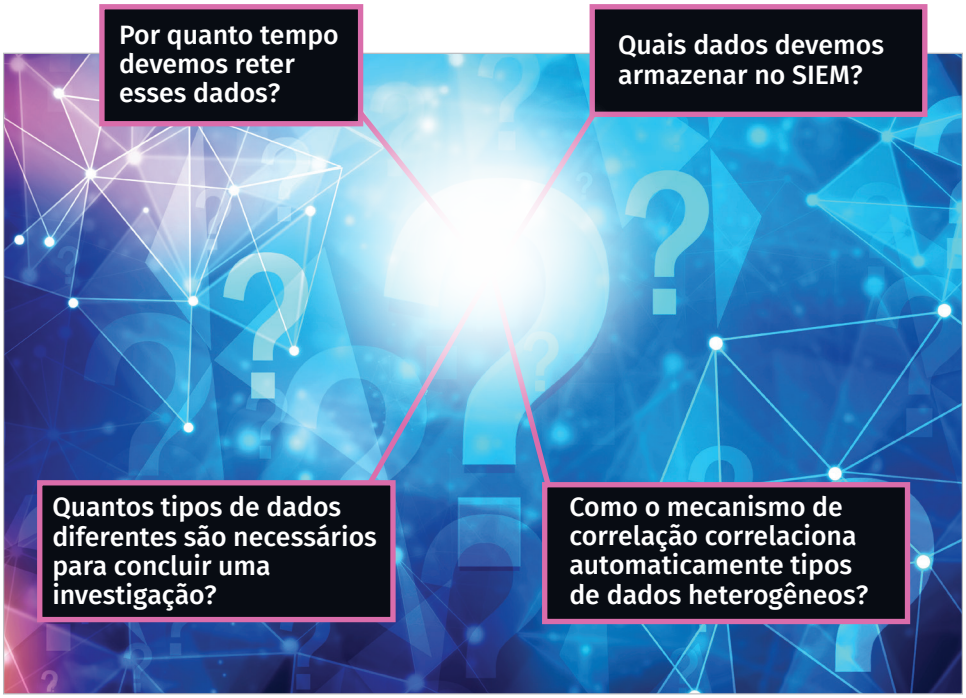

Figura 2. Considerações sobre a arquitetura de registro de dados

O sistema de EDR preenche essa lacuna. O SIEM armazena e correlaciona os logs com mais chances de serem úteis durante uma investigação, mas o sistema de EDR dá ao analista o máximo de flexibilidade para fazer perguntas que eles não sabiam que precisariam responder. Uma situação que exemplifica como a EDR preenche lacunas é quando surgem novas classes de ataque. Como os perpetradores de ameaças estão constantemente atualizando suas técnicas, as organizações precisam ser capazes de adaptar suas técnicas investigativas com a mesma rapidez. É nisso que a EDR supera as outras tecnologias atualmente no mercado: com a flexibilidade de consultar ativamente endpoints protegidos.

A EDR pode ajudar a resolver o problema de acúmulo de dados que algumas organizações também sofrem com outras soluções. Como a EDR permite ao analista consultar dados de endpoint em tempo real, não há tanta necessidade de "registrar tudo, para o caso de precisarmos de algo mais tarde". Quando há necessidade de dados de endpoint específicos, os analistas podem satisfazer o requisito de coleta de dados.

Suponhamos que um novo adversário seja descoberto utilizando um novo ataque de carregamento lateral (sideloading) de DLLs no ambiente da organização. Para investigar o ataque, o analista precisa descobrir as DLLs carregadas em cada endpoint da empresa. Embora esses dados possam, tecnicamente, ser registrados toda vez que um novo processo é iniciado e relatado ao SIEM, o volume dos dados torna essa abordagem impraticável. Uma abordagem muito melhor consiste em consultar esses dados sob solicitação utilizando a EDR para localizar todos os processos nos quais a DLL maliciosa foi carregada lateralmente nos processos das vítimas. Isso não apenas exige menos armazenamento, mas a consulta também tem chances de ser concluída mais rapidamente com dados em tempo real da EDR do que com dados históricos do SIEM (os quais podem não ser mais aplicáveis, de qualquer forma).

O processamento de um alerta do SIEM exige um nível de qualificação radicalmente diferente do que fazer perguntas não estruturadas à EDR. Analistas novatos têm dificuldades por não saber sequer quais perguntas fazer. Como resultado, eles costumam não valorizar a EDR. Essa situação se agrava em organizações com carência de analistas de segurança da informação seniores. Soluções de EDR que proporcionam interfaces intuitivas e ferramentas para criação de roteiros investigativos ajudam a fechar a lacuna para analistas novatos, possibilitando que estes comecem com o pé direito.

Os alertas do SIEM estão desconectados dos alertas da EDR

Na maioria das distribuições de EDR que temos observado em campo, há uma desconexão entre alertas gerados pelo SIEM e pela EDR. Em alguns casos, isso se deve a uma falta de integração; em outros casos, a processos implementados antes da EDR ser distribuída. O ditado “cachorro velho não aprende truque novo” certamente se aplica à segunda hipótese.

Mesmo analistas experientes no uso de um SIEM podem achar menos intuitiva a natureza ativa de uma EDR. As plataformas de EDR com suporte para fluxos de trabalho definidos pelo usuário proporcionam mais valor para organizações com analistas novatos.

Contudo, se a EDR pode facilmente assimilar dados de SIEM e utilizar esses dados para gerar alertas ou agregar contexto aos alertas de EDR existentes, talvez o velho ditado não se aplique afinal. A conclusão é que: sistemas de EDR que não conseguem assimilar dados de outras fontes constituem mais uma solução isolada. Considerando-se que os ataques de hoje em dia mudam rapidamente suas características, as organizações não podem se dar ao luxo de distribuir soluções que não se integrem prontamente com outras.

Muitos produtos de SIEM integram um sistema de emissão de tíquetes dentro do próprio software. Muitas organizações utilizam a solução de tíquetes integrada do SIEM como ferramenta de gerenciamento de casos e rastreamento de alertas. Infelizmente, a maioria dos sistemas de EDR não consegue se integrar de maneira simples com essas ferramentas proprietárias de gerenciamento de casos.

Uma maneira de evitar esse problema é utilizar uma arquitetura de operações de segurança preparada para o futuro. Quando possível, evite soluções proprietárias, que não dispõem de interfaces externas. Embora existam requisitos adicionais de licenciamento e homens-horas de configuração necessárias para utilizar um sistema de emissão de tíquetes externo, provavelmente o investimento inicial é compensado pela facilitação de mudanças futuras na arquitetura.

Quando se utiliza um sistema de emissão de tíquetes centralizado, tanto o SIEM quanto a EDR alimentam o mesmo sistema. Isso cria um local único onde o analista pode identificar todos os alertas relevantes, independentemente de onde o sistema gerou o alerta. Infelizmente, em muitíssimos casos, o analista recebe os alertas do SIEM imediatamente, como parte do fluxo de trabalho estabelecido, mas precisa verificar o sistema de EDR regularmente para ver se há algum alerta novo. Uma solução paliativa

para esse problema seria enviar os alertas de EDR para o SIEM e, em seguida, configurar regras de correlação no SIEM para gerar tíquetes automaticamente para os alertas de EDR. Essa solução está longe de ser ideal, pois a EDR torna-se efetivamente um produto de segunda categoria subordinado ao SIEM.

EDR — detecção não é tudo

Até aqui este documento concentrou-se nos fluxos de trabalho e capacidades de detecção de um sistema de EDR. Porém, uma EDR é mais do que apenas detecção. Evidentemente, as capacidades de resposta também são importantes. No entanto, ao avaliar sistemas de EDR, os usuários frequentemente descobrem que as capacidades de correção e resposta são meramente um acréscimo às capacidades de detecção. Conforme examinamos ciclos de vida de produtos, frequentemente observamos que os recursos de detecção recebem bem mais aperfeiçoamentos que os recursos de resposta.

Já destacamos uma razão para isso: a EDR oferece capacidades que costumavam ser parte das atribuições da segurança cibernética, bem como da equipe de TI. No entanto, apesar das capacidades empregadas por duas equipes diferentes, os requisitos de financiamento para os sistemas de EDR costumam ser responsabilidade dos departamentos de segurança cibernética somente.

Aparentemente, os fornecedores de EDR estão apenas respondendo à demanda do mercado. Os fornecedores presumem que os tomadores de decisões das equipes de segurança cibernética são mais propensos a valorizar recursos de detecção do que de resposta. Acreditamos, porém, que essa presunção é incorreta. Muitas das funções de consulta que podem ser realizadas por uma EDR também podem ser desempenhadas por software tradicional de gerenciamento de ativos de TI, como um SCCM. A principal vantagem da distribuição de EDR só se torna aparente quando as funções de resposta da EDR são equacionadas. Nesta seção destacamos alguns dos recursos de resposta ideais para sistemas de EDR.

Recursos de resposta ideais para sistemas de EDR

- Terminar processos em execução
- Evitar a execução de processos dependendo do nome, caminho, argumentos, processo principal, editor ou hash
- Impedir que processos específicos comuniquem-se pela rede
- Impedir que processos se comuniquem com endereços IP ou nomes de host específicos
- Desinstalar serviços
- Editar chaves do Registro e seus valores
- Desligar ou reinicializar um endpoint
- Desconectar usuários de um endpoint
- Excluir arquivos e diretórios do sistema operacional, mesmo que estejam ativamente em uso (o que pode exigir uma reinicialização)

A maioria dos sistemas de EDR oferece algumas dessas capacidades. Um dos recursos mais frequentemente negligenciados é o de reinicialização da máquina. Os autores de malware costumam instalar malware que emprega interceptação de rootkit em modo de usuário. Interceptações que impedem a exclusão de chaves do Registro e seus valores são instaladas no sistema operacional para que o malware persista entre reinicializações. Os arquivos e diretórios utilizados pelo malware ficam ocultados para os processos enquanto o malware está sendo executado. O malware frequentemente persiste por meio de um serviço regulado pelo gerenciador de controle de serviços.

Não havendo a capacidade de realizar uma reinicialização remota em um sistema, o malware que emprega as técnicas listadas acima pode ser impossível de ser neutralizado por meio da EDR. Os analistas precisam ter a capacidade de reagir rapidamente e de conter um incidente. A abordagem tradicional de simplesmente restaurar uma imagem do sistema toda vez que há um alerta antivírus simplesmente não pode ser expandida para as ameaças de hoje em dia.

A maioria dos sistemas de EDR atualmente permite aos analistas terminar processos individuais. Porém, muitos desses mesmos sistemas carecem da capacidade de impedir que um processo idêntico seja reiniciado imediatamente. Eles deixam literalmente que o analista perca tempo em uma perseguição inútil na qual o atacante sempre leva vantagem e o defensor está sempre correndo atrás do prejuízo. Ao avaliar um sistema de EDR, verifique cuidadosamente se o sistema de EDR permite aos analistas prevenir proativamente uma técnica conhecida de um atacante em vez de simplesmente responder a ela.

Um outro problema comum com sistemas de EDR é o uso de interpretadores de scripts, como PowerShell ou cscript. Ambos interpretadores de scripts são utilizados regularmente em operações de sistema normais, mas ambos são frequentemente utilizados por malware também. O sistema de EDR precisa dar ao analista alguma capacidade de diferenciar entre uso legítimo e ilegítimo dos interpretadores de scripts.

Lista de itens a conferir na avaliação de soluções de EDR

Ao longo dos últimos anos, o espaço de soluções de EDR tornou-se relativamente congestionado. As organizações devem avaliar devidamente as soluções de EDR se desejam maximizar a probabilidade de que a EDR satisfaça as necessidades de sua missão. Esta seção oferece uma lista de recursos a conferir que, idealmente, contribuirá para o sucesso da distribuição de EDR em uma organização. Nem todos os recursos mencionados na lista são necessários para assegurar sucesso em qualquer distribuição, mas são incluídos por terem se mostrado capacidades importantes para as organizações.

Recurso	Prioridade	Justificativa
Capaz de consultar todos os endpoints, grupos predefinidos de endpoints ou grupos criados conforme a necessidade por outros dados de consulta	ALTA	Durante uma investigação, os analistas precisam configurar, conforme a necessidade, grupos que não podem ser previstos no momento da instalação da EDR. Frequentemente são criados grupos com base em uma outra consulta realizada à EDR (por exemplo, para listar todos os hosts nos quais o usuário X tenha efetuado login nos últimos sete dias).
A funcionalidade de resposta satisfaz as necessidades previstas da organização	ALTA	A organização deve rever os incidentes que foram trabalhados no passado e examinar as ações de resposta realizadas manualmente para determinar se a EDR pode substituí-las. Uma EDR que não ofereça opções de resposta apropriadas para o fluxo de trabalho da organização deve ser preterida.
Integração com SIEM	ALTA	A integração com o SIEM é um recurso altamente desejável em uma EDR. Idealmente, a integração deve ser bidirecional, mas a EDR precisa ser capaz de fornecer dados para o SIEM.
Suporte para fluxo de trabalho para analistas novatos	ALTA	Além de proporcionar o máximo de flexibilidade para os analistas seniores, a EDR deve acomodar fluxos de trabalho predefinidos (e configuráveis) para o pessoal menos experiente que requer mais orientação durante uma investigação.
Integração com sistema de emissão de tíquetes	MÉDIA	A EDR deve ser capaz de fornecer dados para um sistema de emissão de tíquetes de terceiros (por exemplo, JIRA).
Grupos de privilégios separados para ações de consulta e de resposta	MÉDIA	A separação de privilégios para criação de consultas e realização de ações de resposta é fundamental para uma maior adoção da plataforma de EDR. Muitos usuários que precisam consultar dados (por exemplo, ao caçar ameaças) não devem ter a capacidade de terminar processos como os de exclusão de arquivos.
Processamento de IOCs	MÉDIA	Idealmente, a EDR deve poder processar IOCs em múltiplos formatos, como Yara e OpenIOC, mas pelo menos um formato deve ser suportado.
Integração com o hipervisor para grupos de varredura	MÉDIA	Nos ambientes de TI modernos, os servidores migram facilmente entre hipervisores físicos. A EDR examina os recursos do usuário nos servidores hóspedes, o que pode fazer com que um hipervisor seja sobrecarregado. Quando a EDR tem suporte para integração com hipervisor, os grupos de varredura podem ser dinâmicos.
Integração com Syslog	BAIXA	A EDR deve ser capaz de enviar alarmes via syslog para proporcionar o máximo de flexibilidade na integração com outros sistemas.
Limitação do impacto das varreduras	BAIXA	A EDR deve oferecer opções de configuração para limitar o impacto das varreduras que são executadas. Segundo os usuários, a interrupção dos negócios é um dos problemas que limitam a adoção por parte das organizações.
Múltiplos locais de exportação de dados	BAIXA	Alguns produtos só permitem integração com um único sistema de acompanhamento (por exemplo, o syslog só pode ser um destino). Isso limita a flexibilidade na construção de uma arquitetura de sistema completa.
Integração com API	BAIXA	A integração com a API permite que a organização personalize o enriquecimento de dados e as atividades de resposta. As organizações que atualmente automatizam interações entre sistemas podem priorizar esse item.

Casos de uso de EDR

O caso de uso óbvio para um sistema de EDR consiste em detecção de intrusões e automatização da resposta. Nesta seção, examinamos alguns exemplos de casos de uso de como uma EDR pode ser operacionalizada em campo. Certamente há mais casos de uso do que podemos cobrir nesta seção, mas esses exemplos destacam os tipos de fluxos de trabalho viabilizados pela implementação de uma solução de EDR.

A EDR detecta um processo chamado lsass.exe sendo executado como usuário comum

A situação

O processo denominado **`lsass.exe`** só deve ser executado sob um contexto de sistema, nunca sob um contexto de usuário comum. Como um analista novato pode não saber que somente uma única instância do processo **`lsass.exe`** pode estar em execução em um host Windows, a EDR destaca esse fato e aciona um alerta, dando início a uma investigação. No processamento do alerta, o analista consulta a EDR para saber quais processos estão em execução no endpoint e descobre que um processo **`lsass.exe`** espúrio está sendo executado como um processo secundário de **`cmd.exe`**. O processo **`cmd.exe`** está sendo executado como secundário de **`winword.exe`**. Agora o analista suspeita que o processo espúrio é, provavelmente, resultado de um ataque de phishing com um documento do Word malicioso. Os horários de início dos processos levam o analista a concluir que o e-mail de phishing acabou de ser aberto, o que constitui uma oportunidade ideal para a EDR levar o incidente da intrusão para a detecção e daí para a correção em questão de poucos minutos.

O papel da EDR

Reconhecendo que o processo **`lsass.exe`** espúrio é certamente malicioso, o analista procura conexões de rede envolvendo quaisquer dos processos espúrios e descobre que o processo **`lsass.exe`** está se comunicando com um endereço IP da Europa Oriental. O analista utiliza a EDR para terminar imediatamente os processos espúrios (**`lsass.exe`**, **`cmd.exe`** e **`winword.exe`**). O analista também utiliza o sistema de EDR para procurar quaisquer endpoints que estejam se comunicando com o endereço IP suspeito. O analista descobre dois endpoints adicionais e pede informações de sistema (processos em execução e informações sobre configuração de serviços, por exemplo) a esses sistemas. Esses sistemas não estão utilizando um processo **`lsass.exe`** espúrio como o original, mas mesmo assim a EDR facilita a identificação dos processos maliciosos.

Sistemas de monitoramento de rede tradicionais (como NetFlow e captura de pacotes completos) não têm a granularidade proporcionada pela EDR. Embora os sistemas de monitoramento de rede tradicionais possam indicar para o investigador um endpoint que esteja se comunicando com um endereço IP suspeito, eles não chegam a identificar os processos realmente envolvidos. Infelizmente, esse aspecto da EDR significa que o investigador precisa incluir mais um sistema na investigação. Por outro lado, a EDR permite ao investigador identificar os processos específicos envolvidos na comunicação (e terminá-los).

Embora o primeiro sistema tenha acabado de ser comprometido e possa ser facilmente resolvido, ainda não se sabe quando as máquinas recém-identificadas foram comprometidas. O analista examina mais detidamente as informações retornadas pela EDR e descobre que o mecanismo de persistência é um arquivo LNK no diretório de inicialização do usuário, o qual é removido por meio da EDR.

O analista utiliza a EDR para coletar outras anomalias forenses do sistema, incluindo manipuladores de arquivo abertos dos processos maliciosos identificados. Essa ação ajuda a identificar um arquivo anteriormente desconhecido utilizado pelo malware, o qual é posteriormente repassado aos especialistas em engenharia reversa da organização. Com engenharia reversa, é possível decodificar o arquivo, o qual contém uma lista de domínios de callback utilizada pelo malware. É importante observar que

esse arquivo (e os recém-descobertos indicadores de comprometimento) não teria sido encontrado sem a ajuda da EDR.

Apesar do malware ter nomes de processos e hashes de arquivo diferentes, o EDR identificou que todos os três sistemas compartilham o número de versão de arquivo "**`1.0.29.5`**". O analista utiliza a EDR para procurar quaisquer sistemas que estejam executando processos com esses metadados de arquivo executável. Esse tipo de detecção simplesmente não é possível sem a EDR porque tal nível de detalhamento é algo que jamais seria registrado com um SIEM tradicional.

Para concluir a resposta, a EDR é utilizada para terminar quaisquer processos em execução restantes, confirmar a remoção do arquivo **`.LNK`** utilizado para proporcionar persistência e bloquear a comunicação de rede com os endereços IP e nomes de domínio descobertos.

Este estudo de caso destaca o valor da EDR por vários motivos. Primeiro, na máquina detectada inicialmente, o incidente é detectado e corrigido dentro de um único painel em questão de minutos. Segundo, o analista consegue identificar imediatamente os processos que se comunicam com os endereços IP maliciosos em tempo real (em vez de alternar entre sistemas). Por último, o analista pode realizar consultas para obter informações que nunca seriam registradas em um SIEM (o número de versão do arquivo, por exemplo), assegurando que nenhuma variante do malware deixe de ser detectada no ambiente.

A EDR detecta comportamentos suspeitos

A situação

A organização recebe novas informações de inteligência sobre ameaças segundo as quais uma ameaça APT notória por visar a organização está utilizando o diretório **`%USERPROFILE%\AppData\Roaming\SharePoints`** para preparar dados para vazamento. A organização não observou atividade do grupo de APT em sua rede recentemente e está apreensiva com a possibilidade de que indicadores recém-divulgados possam ser observados em sua rede. Caso sejam descobertos tais indicadores, a organização deseja ter a capacidade de reagir rapidamente e remover o atacante da rede.

O papel da EDR

A EDR é encarregada de consultar cada máquina da rede quanto à presença do diretório **`%USERPROFILE%\AppData\Roaming\SharePoints`**, identificado por meio de inteligência contra ameaças como um indicador de comprometimento (IOC). O diretório é descoberto em quatro máquinas, duas na matriz e duas em sucursais remotas diferentes, onde a organização não dispõe de uma equipe de segurança da informação ou TI no local. Detectar uma intrusão é sempre aquém do ideal, mas detectar uma intrusão onde não há suporte local acarreta complicações extras.

O analista consulta imediatamente informações sobre o processo, incluindo DLLs carregadas e dados de conexão de rede das quatro máquinas afetadas, através da EDR. O analista não vê imediatamente processo algum que pareça malicioso, mas observa uma DLL não familiar, **`kernel64.dll`**, carregada no espaço de endereçamento de **`explorer.exe`** (o desktop do usuário). Encontrar a DLL carregada em **`explorer.exe`** é consistente com o IOC compartilhado, também vinculado ao usuário (em vez de à máquina).

Ao examinar os dados de conexão de rede, o analista observa que, em três das máquinas afetadas, o processo **`explorer.exe`** tem uma conexão com um endereço IP externo na porta TCP 33389. O analista pensa em utilizar a EDR para bloquear imediatamente a comunicação com o endereço IP, mas decide não fazê-lo até que consultas adicionais possam ser feitas à EDR.

Utilizando os conhecimentos obtidos com as consultas anteriores, o analista utiliza a EDR para identificar todas as máquinas que estão se comunicando pela porta TCP 33389 ou com o endereço IP suspeito. Ele também consulta todos os processos que carregam uma DLL denominada **`kernel64.dll`**. O analista encontra cinco novas máquinas que carregam **`kernel64.dll`**. Como essas máquinas não contêm o diretório de preparação, elas não seriam localizadas com a inteligência sobre ameaças fornecida originalmente. O analista também descobre um outro endereço IP suspeito.

O analista utiliza a EDR para consultar as configurações do Registro de todos os usuários conectados nos computadores identificados para descobrir o mecanismo de persistência utilizado pelo malware. Todas as máquinas infectadas possuem uma entrada de execução automática para iniciar um aplicativo de terceiros, legítimo, de perfil do sistema. Como o aplicativo é assinado digitalmente, ele foi incluído na lista branca de aplicativos, mas está sendo utilizado para carregar lateralmente (sideload) uma DLL do disco, injetá-la em **`explorer.exe`** e sair. Consultas adicionais à EDR são realizadas para procurar outras máquinas com o aplicativo de perfil do sistema de terceiros instalado, mas nenhuma é descoberta.

Com a detecção concluída, os analistas passam à resposta. Eles utilizam a EDR para remover remotamente as chaves de execução automática do Registro utilizadas para fins de persistência e o aplicativo de perfil do sistema de terceiros (e as DLLs suspeitas carregadas lateralmente). Eles também utilizam a EDR para bloquear todas as comunicações com os endereços IP identificados. Embora as comunicações também devam ser bloqueadas no firewall, essa tarefa costuma ficar sob responsabilidade de uma outra equipe. A coordenação entre múltiplas equipes durante a resposta resulta em atrasos. Embora o bloqueio da comunicação com os endereços IP possa parecer inadequado durante as fases de identificação e determinação do escopo, o bloqueio deve ser imediato e descomplicado quando os encarregados da resposta decidem agir. Na nossa experiência, essa coordenação com a equipe de rede nunca é imediata e nem descomplicada, o que justifica ainda mais a proposta da EDR.

Os analistas também utilizam a EDR para coletar os arquivos nos diretórios de preparação para avaliar o impacto do incidente. Após coletar os arquivos, os analistas utilizam a EDR para remover os diretórios de preparação (e todos os arquivos coletados pelo atacante) das máquinas infectadas. Como etapa final, as máquinas são reinicializadas remotamente utilizando-se a EDR (a reinicialização é a melhor prática devido à técnica de injeção de código empregada) e são submetidas a uma nova varredura após o login, para confirmar que estão limpas.

O valor da EDR nesse incidente é particularmente alto em locais sem uma equipe específica de segurança da informação ou de TI. Sem a EDR, a organização não poderia ter respondido a todas as máquinas identificadas simultaneamente em diversos lugares. Em uma era na qual os atacantes se tornam cada vez mais sofisticados, as organizações precisam ter agilidade e negar ao atacante a oportunidade de reagir à sua resposta distribuindo malware novo e desconhecido.

Conclusão

O mercado de EDR, que já foi apenas um nicho, expandiu-se consideravelmente nos últimos anos. Porém, não é por serem rotulados como EDR que tais produtos possuem alguma paridade de recursos que seja ou que tenham se mostrado particularmente eficazes. Neste documento discutimos recursos a procurar ao considerar uma EDR, casos de uso para distribuição de uma EDR, armadilhas nas distribuições atuais de EDR e uma lista de itens a conferir ao avaliar produtos de EDR. As organizações que estão considerando um produto de EDR devem levar em conta as recomendações deste documento ao avaliar suas próprias distribuições, incluindo:

- Utilizar a lista de recursos de EDR a conferir
- Considerar as lições aprendidas para evitar problemas de distribuição de EDR
- Assegurar que a solução de EDR escolhida implemente os recursos de resposta apropriados
- Determinar de antemão como a integração com o SIEM e outras ferramentas afetará as distribuições de EDR
- Assegurar que a EDR acomode fluxos de trabalho que sejam usáveis por analistas novatos

Sobre o autor

Jake Williams é analista da SANS, instrutor sênior da SANS, autor de cursos e criador de vários desafios NetWars para uso no popular pacote de treinamento de segurança da informação da SANS em formato de jogo. Jake passou mais de uma década em funções de segurança da informação em diversas agências governamentais desenvolvendo especialidades em análises forenses ofensivas, desenvolvimento de malware e contraespionagem digital. Jake é fundador da Rendition InfoSec, que oferece testes de penetração, resposta a incidentes e análises forenses digitais e especialidade em vazamento de dados de nuvem, bem como as ferramentas e a orientação necessárias para proteger os dados do cliente contra ataques persistentes e sofisticados, tanto no local quanto na nuvem.

Patrocinador

A SANS agradece ao patrocinador deste documento:

McAfee™