TANIUM

ARTIGO TÉCNICO

Como as soluções Tanium Threat Response aumenta a detecção e resposta de endpoint (EDR) e SIEM

O uso da Tanium Threat Response com sua solução existente de detecção e resposta de endpoint (EDR) oferece resposta rápida a incidentes e busca em tempo real.

CONTEÚDO

Conclua investigações mais rapidamente e busque dados arbitrários em tempo real.

Quer você esteja respondendo a alertas ou realizando uma busca, uma vez que um ataque tenha sido detectado, é literalmente uma corrida contra o relógio para investigar e responder.

À medida em que os analistas investigam incidentes e conduzem suas buscas, eles aproveitam de um rico conjunto de informações e experiências de investigação encontradas em suas soluções de Gerenciamento de Informações e Eventos de Segurança (SIEM) e Detecção e Resposta de Endpoints (EDR). Combinadas, essas ferramentas darão aos analistas um bom, mas muitas vezes incompleto, sentido da extensão do ataque. Os analistas quase sempre precisam de mais visibilidade e controle do que essas soluções podem oferecer. Eles precisam ter uma visão em tempo real de alta fidelidade do que exatamente aconteceu e ainda podem estar se escondendo nas sombras.

Embora as soluções SIEM e EDR fornecerem uma grande participação dessas informações, há um limite que muitos investigadores encontram – um ponto onde a visibilidade termina e força os analistas a trazer ferramentas adicionais para completar a imagem. Essa é frequentemente a longa cauda da carga de trabalho do analista e requer experiência adicional e é onde os analistas gastam grande parte do seu tempo.

As organizações medem seu desempenho em relação a esses desafios com KPIs como Tempo médio para detectar (MTTD), Investigar (MTTI) e Responder (MTTR) e, se você for como seus colegas, está sempre procurando novas maneiras de melhorar os números. As organizações esperaram há muito tempo que seus provedores de SIEM e EDR existentes entregassem os recursos necessários para abordar essa longa cauda do trabalho, mas a realidade é que as soluções de SIEM e EDR não são bem adequadas para atender a essas necessidades restantes. Consequentemente, eles deixaram esses recursos para outras pessoas cumprirem.

Precisa de soluções SIEM e EDR não abordadas.

Há várias categorias de recursos críticos que os fornecedores de SIEM e EDR não fornecem que exigem ferramentas e processos adicionais, incluindo:

- As investigações exigem acesso a dados adicionais, que chamamos de dados arbitrários, que vão além do que as soluções SIEM e EDR foram projetadas para coletar. Outras ferramentas são usadas para adquirir esses dados sob demanda e em escala, o que é uma tarefa demorada. Os
- Analistas precisam da capacidade de obter dados de estado de endpoint em tempo real dos endpoints em escala (por exemplo: configuração ou estados-chave de registro, arquivo). Eles precisam ser capazes de obter esses dados juntamente com a data do estado histórico para detectar alterações anômalas. Os
- SIEM e EDRs coletam dados em uma cadência periódica que varia de acordo com a fonte e o tipo de dados para que os tipos de dados possam

ser minutos, horas ou até mais antigos. O acesso a dados em tempo real de endpoints é um requisito para concluir com sucesso investigações e busca

- SIEM e EDRs têm regras de coleta e retenção de dados que inevitavelmente eliminam dados, levando a lacunas e contexto ausente que é necessário para concluir investigações e buscas
- Além das ferramentas básicas de contenção SIEM e EDRs não fornecem um conjunto completo de recursos de contenção nem a capacidade de remediar e trazer os endpoints de volta para um estado seguro e compatível
- Muitas soluções carecem de visibilidade abrangente para todos os endpoints, levando a pontos cegos e complexidade ao tentar avaliar a totalidade do ataque

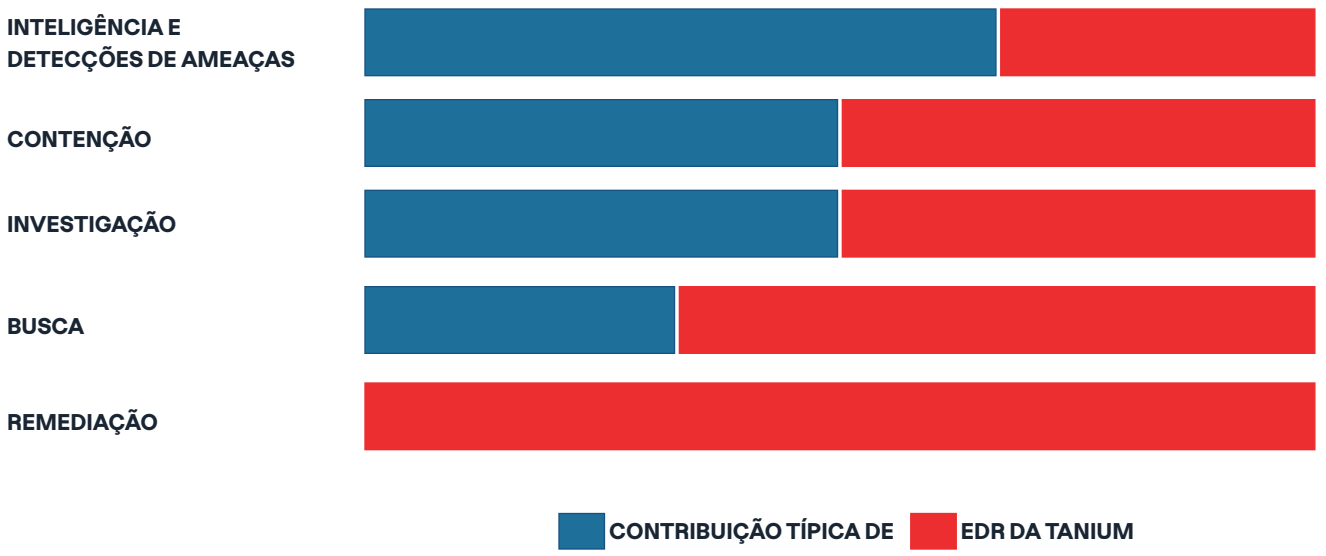
Solução

O uso da Tanium Threat Response em conjunto com suas soluções SIEM e EDR existentes oferece ao seu Centro de Operações de Segurança (SOC) uma oportunidade de acelerar drasticamente seu trabalho, reduzindo a complexidade e a experiência dos analistas de atrito durante investigações e tarefas de busca.

Seus investimentos em SIEM e EDR continuarão a ser a principal experiência para detecções e para iniciar investigações e buscas, no entanto, com a Tanium sendo usada em conjunto, você poderá consolidar as muitas ferramentas adicionais que suas equipes estão usando para concluir a longa cauda de suas investigações e processos de busca.

Com a Tanium, agora você pode:

- Adicionar e gerenciar com mais facilidade detecções personalizadas ao seu ambiente
- Executar mitigações avançadas de contenção e proteção do ambiente para restringir os invasores e impedir ataques além de apenas isolar dispositivos comprometidos
- Reunir e consultar todos os dados em tempo real, históricos e forenses necessários para entender um incidente ou realizar uma busca, em vez de apenas o que você pode dar ao luxo de trazer para o seu SIEM
- Conduza ações completas de remediação em escala para trazer os endpoints e serviços impactados de volta a um estado seguro e em conformidade.



Combinar seu conjunto de ferramentas SIEM e EDR com a Tanium permitirá que sua equipe atinja níveis mais altos de eficácia e aumente o desempenho para os principais KPIs do SOC. Com a Tanium, todos os analistas e investigadores podem realizar investigações e tarefas de busca mais avançadas. Eles poderão conduzi-los com menos ferramentas, menos experiência e em velocidades muito maiores.

Recursos adicionais Tanium para EDR e SIEM

Investigação

A Tanium oferece aos analistas a ampla gama de recursos de que precisam para concluir a longa e demorada cauda de suas investigações e permite que eles os concluam com maior confiança, velocidade e precisão.

Especificamente, a Tanium oferece a capacidade de:

- Realizar investigações usando dados em tempo real que são necessários para preencher as lacunas de visibilidade e cronograma que as soluções SIEM e EDR têm que coletam dados em uma cadência e os tornam uma visão do passado
- Para analistas que investigam um incidente para acessar dados arbitrários (ou seja, dados adicionais não coletados pelo EDR ou SIEM) de qualquer tipo (por exemplo, arquivos e conteúdo, chaves reg, variáveis env, descritores de arquivos, objetos mutex, execução do PowerShell, atividade do navegador, etc.)
- Para que os analistas acessem dados históricos configuráveis, incluindo dados arbitrários que normalmente não são coletados pelo EDR ou SIEM devido a implicações de desempenho e custo. A descentralização do armazenamento de dados nos próprios endpoints fornece aos analistas acesso ao conjunto de dados históricos mais rico possível
- Para obter acesso a todos os dados de eventos de seus endpoints. Nenhum dos dados do evento precisa ser filtrado, transformado ou descartado para abordar as implicações de desempenho e armazenamento do armazenamento centralizado
- Para personalizar o conjunto de dados forenses para adquiri-lo e coletá-lo em escala, o que normalmente é um desafio para o desempenho eficiente
- Para definir o escopo de um ataque em todos os endpoints usando consultas que podem aproveitar dados históricos e em tempo real (por exemplo: obter uma lista de endpoints que têm instâncias vulneráveis de log4j neles, procurar endpoints que tenham um arquivo específico)
- Comparar dados/estados nos endpoints ao longo do tempo, incluindo dados históricos de longo prazo, para ver se há anormalidades ou problemas atípicos
- . Para investigar incidentes usando sinais personalizados (por exemplo: processo filho da palavra != X) em tempo real e em escala para o trabalho de sniper que pode ser criado para corresponder contextualmente à organização ou ao exercício de investigação que está sendo feito
- Para importar TI e criar e executar IoCs personalizados (por exemplo, YARA, STIX-TAXII, OpenIOC) e executá-los em escala, de uma maneira segura e eficaz
- Para analisar qualquer endpoint e entender as oportunidades de movimento lateral relacionadas à identidade que um invasor pode ter sido capaz de explorar com um endpoint ou identidade comprometida
- Para criar, executar e salvar consultas de verificação simples, mas detalhadas, usando linguagem natural
- Para criar painéis personalizados para monitorar e garantir que as ações de remediação tomadas tenham sido executadas corretamente, completamente e confirmar que a reemergência não ocorreu

Busca

A Tanium oferece aos investigadores uma ampla gama de recursos adicionais que são complementares e aumentam suas experiências de busca EDR e SIEM. Ele fornece os recursos necessários para concluir suas buscas usando dados ao vivo e mais detalhados.

Especificamente, a Tanium oferece a capacidade de:

- Para buscas usando dados em tempo real que são necessários para preencher as lacunas de visibilidade e cronograma que as soluções SIEM e EDR têm, que coletam dados em uma cadência e os tornam uma visão do passado
- Para investigadores que rastreiam uma hipótese para acessar dados arbitrários em tempo real (ou seja, dados adicionais não coletados pelo EDR ou SIEM) de qualquer tipo (por exemplo, arquivos e conteúdo, chaves reg, variáveis env, alças de arquivos, objetos mutex, execução do PowerShell, etc.)
- Buscar com dados históricos configuráveis, incluindo dados arbitrários que normalmente não são coletados pelo EDR ou SIEM devido a implicações de desempenho e custo. A descentralização do armazenamento de dados para os próprios pontos terminais fornece aos investigadores acesso ao conjunto de dados mais rico possível sem aumentar os custos de armazenamento
- Para que os investigadores tenham acesso a todos os dados de eventos de seus pontos terminais. Nenhum dos dados do evento precisa ser filtrado, transformado ou descartado para abordar as implicações de desempenho e armazenamento do armazenamento centralizado
- Para buscar sinais personalizados (por exemplo: processo infantil da palavra != X) em tempo real e em escala para a caça ao sniper, que pode ser criado para corresponder contextualmente à organização ou ao exercício de caça que está sendo feito
- Para mudar de uma descoberta de busca para uma inteligência codificada e validações que os analistas podem usar para executar mais rapidamente a resposta a incidentes
- Para os investigadores importarem TI e criarem e executarem IoCs personalizados (por exemplo, YARA, STIX-TAXII, OpenIOC) e executá-los em escala, de uma maneira segura e eficiente
- Para buscar ameaças com base em comportamento atípicos específico para sua empresa e criar novas detecções com base na ameaça específica descoberta.

Remediação

A Tanium capacita as equipes de resposta a incidentes a desempenhar um papel maior no processo de remediação e a colaborar com as operações de TI usando as mesmas ferramentas. Ela os equipa com os recursos necessários para tomar qualquer ação necessária para trazer os dispositivos de volta a um estado de pré-violação que pode ser executado em tempo real e em escala.

Especificamente, a Tanium fornece:

- Recursos granulares de controle de acesso baseados em função para permitir que as equipes de Operações de TI e IR (Resposta a Incidentes) façam parceria e deleguem recursos de remediação conforme faz sentido para sua organização
- A capacidade de mudar de um alerta para dados sobre alterações de configuração (por exemplo: serviços instalados, arquivos adicionados, chaves de registro modificadas, processos em execução) feitos para o endpoint, às ações de remediação necessárias para trazer o endpoint de volta a um estado pré-violação em opções de segmentação
- Opções avançadas que permitem a execução em tempo real de ações de remediação para um único endpoint, um conjunto selecionado de endpoints ou até mesmo em toda a empresa, conforme necessário
- Recursos de remediação dinâmicos e extensíveis para orquestrar ações avançadas de remediação em várias etapas (por exemplo: correção baseada em script ou código baixo)
- Para criar, executar e salvar procedimentos de detecção e correção que podem ser executados automaticamente quando os pontos terminais anteriormente offline se reconectarem à rede
- Para criar, executar e salvar consultas de verificação simples, mas detalhadas, usando linguagem natural
- Para criar painéis personalizados para monitorar e garantir que as ações de remediação tomadas tenham sido executadas corretamente, completamente e confirmar que a reemergência não ocorreu.

Contenção

A Tanium oferece opções adicionais de contenção e restrição multiplataforma de alto valor para complementar as opções do seu fornecedor de EDR.

Especificamente, a Tanium fornece:

- Opções de contenção, como isolamento/quarentena, que podem ser executadas em escala nos endpoints afetados, ou ainda mais amplamente, em tempo real
- A capacidade de personalizar o comportamento de isolamento/quarentena. Os analistas podem escolher entre opções para isolar totalmente um dispositivo ou podem decidir quais endpoints e serviços podem continuar a ser contatados
- Mitigações implantáveis em tempo real que os analistas podem usar para restringir a atividade de um invasor em endpoints afetados ou mesmo naqueles que ainda não foram comprometidos. Por exemplo, o uso de organizações Tanium Enforce pode aplicar mitigações temporárias ou de longo prazo em tempo real, como: AppLocker, alterações de firewall, etc.

Inteligência e detecções de ameaças

A Tanium fornece a plataforma mais rica para complementar a inteligência de ameaças e as detecções provenientes do seu fornecedor de SIEM e EDR com detecções personalizadas adicionais de terceiros ou da sua própria organização. Detecções personalizadas podem ser criadas para refletir sobre atividades históricas, evidências em disco e fontes de dados de processo em tempo real, permitindo que você responda: “essa atividade é no meu ambiente” e alerte sobre exatamente o que é importante para a sua empresa.

Especificamente, a Tanium permite:

- Consumo e transformação de inteligência de ameaças externa (por exemplo: YARA, TAXII, STIX, CybOX) em detecções que são executadas na Tanium e opcionalmente enviadas ao seu SIEM.
- Uso de inteligência de ameaças externa relacionada a malware (por exemplo: Virus Total, Palo Alto WildFire) que pode ser usado como detecções executadas na Tanium e, opcionalmente, enviadas ao seu SIEM.
- Criação de detecções de multicondição personalizadas que podem ser provisionadas em escala
- Criação de detecções personalizadas que podem raciocinar sobre dados que vão além de indicadores simples baseados em hash (por exemplo: pesquisar sequências específicas como linhas de comando conhecidas como ruins, conectividade de rede anômala, etc.)
- Gerenciamento de todas as detecções personalizadas e inteligência de ameaças que foram inseridas na Tanium (por exemplo: segmentação, visualizações para gerenciar etc.)