Painel & Relatórios

Utilizando a aplicação web da Cyber Crucible - visibilidade de agentes, atividade de processos, análises de memória e relatórios executivos.

A Cyber Crucible pode responder silenciosamente a um ataque, mas sem me alertar/notificar?

Você pode constatar que existem cenários legítimos em que não deseja que uma aplicação faça algo (provavelmente nas suas máquinas), mas não precisa ser notificado sempre que isso ocorrer.

Esta é uma situação diferente daquela em que você precisa de algo na lista de permissões (whitelist), na qual nenhuma ação é tomada pela prevenção de extorsão de dados da Cyber Crucible.

A funcionalidade que você está procurando é a de respostas automáticas silenciosas.

Tornando uma resposta automática existente silenciosa no futuro:

Primeiro, vá para a página Manage Incidents. Em breve, estaremos alterando o nome para Manage Responses.

Segundo, clique no botão de alto-falante/volume, conforme mostrado abaixo.

4784131.png?width=680
Clicar neste botão abre a janela modal “Silence Incident” ou “Silence Auto-Response”.

Temos análises que verificam se uma resposta deve ser silenciosa com base em programas e argumentos previamente selecionados.

Neste caso, vemos que o Adobe executa um servidor web como parte do seu conjunto de software, e não queremos nenhum alerta futuro de que o servidor web foi suspenso.

(Neste caso, inserimos um JavaScript malicioso no arquivo que o Adobe executou, e a Cyber Crucible suspendeu o servidor web do Adobe para impedir o roubo ou a criptografia de dados.)

4784138.png
Clique em “Take me to Silent Responses Page”

Haverá um menu para inserir essa regra de silêncio específica, mas vamos primeiro observar a página:

5013506.png?width=680
Vemos aqui que as regras são baseadas tanto no processo quanto nos argumentos do processo para uma resposta automática, que não deve ser incluída em e-mails de notificação ou outros alertas.

A suspensão ainda ocorre - apenas não há notificação sobre ela.

Vemos aqui que não queremos que o navegador Microsoft Edge, ou o navegador Chrome, possam ser executados ao usar esses argumentos, com wildcards antes e depois para contemplar outros argumentos presentes.

(Explicação técnica de segurança: Ambos os navegadores executam um trecho de código idêntico, que carrega os navegadores em segundo plano sem uma janela na tela, a fim de escanear e ler seus arquivos de forma oculta. Não queremos que nossos navegadores web façam isso pelas nossas costas!)

Independentemente de você estar criando uma regra de resposta silenciosa totalmente preventiva ou não, a mesma janela abaixo (na próxima seção) é o próximo passo.

Criando uma Resposta Silenciosa

Aqui vemos tanto o caminho do programa quanto os argumentos do programa. Wildcards são permitidos, para garantir que algo como um nome de usuário ou número de versão de aplicação não impeça que sua regra comportamental funcione.

Um exemplo de por que os wildcards são necessários é porque pode haver um programa em todas as áreas de trabalho dos seus funcionários que estão em um grupo.

C:\Users\mary\Desktop\runme.exe
C:\Users\joe\Desktop\runme.exe

A solução seria:

C:\Users*\Desktop\runme.exe

5046277.png

Aqui, vemos que estamos criando uma resposta silenciosa para todo o grupo TEMPORARY GIRAFFE 2, para um caminho do Adobe Created Cloud, e queremos silenciar apenas as respostas que possuem um argumento específico (neste caso, um caminho de arquivo para um determinado arquivo javascript).

Não há partes exclusivas no caminho, como nomes de usuário, então podemos criar a regra como está.

As respostas podem ser nomeadas, sendo os nomes exclusivos por grupo.

As regras começam a ser distribuídas para os agentes em poucos minutos.

Como posso investigar a causa raiz de um evento?

Existem três blocos de construção de análise disponíveis para você durante a investigação de um alerta.

Atualmente, é mais provável que um invasor conduza uma variedade de atividades em um sistema, usando uma combinação de técnicas na memória e sequestro de processos (injeção ou hollowing), do que executando um programa óbvio de “hacker.exe”.

Análise de Memória

O primeiro bloco de construção é encontrado na própria página de Resposta ou Incidente. A análise de memória acompanha os comportamentos do processo na memória durante a inspeção contínua de possíveis comportamentos de extorsão de dados (roubo ou criptografia).

Um estado de memória que indica provável adulteração é tipicamente indicativo de um problema.

Isso nem sempre é malicioso em si, pois práticas de programação inadequadas ou bugs de software também podem resultar na adulteração do estado de memória de um programa em execução.

63504385.png?width=680
Aqui vemos uma instância em que um processo do Adobe Acrobat exibe possíveis comportamentos de extorsão de dados após abrir um PDF baixado, e vemos que a memória do processo do Acrobat havia sido modificada. O processo Acrobat.exe no disco não foi afetado de forma alguma.

A análise forense da memória envolvida com o Acrobat.exe suspenso provavelmente indicará um problema de preocupação - possivelmente um exploit em uso, senão injeção de processo ou hollowing de processo.

Para respostas de extorsão com um valor de Memória Modificada igual a Verdadeiro, há um ícone de download na coluna Análise de Causa Raiz para baixar o arquivo de Diferença de Memória (Memory Diff) da resposta:

63602693.png?width=680
O Arquivo de Diferença de Memória (Memory Diff File) é o código-fonte compilado do que foi injetado no programa. Provavelmente contém malware e/ou código de exploit, para que um analista de malware ou de segurança examine. Observe que este arquivo não contém o programa inteiro, apenas a parte que foi alterada por meio de um exploit ou técnica de ataque como injeção de processo. Saiba mais sobre este arquivo aqui.

Análise de Injeção de Processos

O primeiro indicador de que pode haver um evento de injeção de processo relevante para uma resposta automatizada é a coluna Threads Remotas Não Confiáveis para um Incidente/Resposta. Isso indica que a análise comportamental em nível de kernel revelou uma thread remota não confiável sendo observada com o processo conduzindo roubo de dados ou comportamento semelhante a ransomware.

63471635.png?width=680
Uma investigação mais aprofundada pode ser realizada na página de Injeção de Processos. O valor Verdadeiro em Threads Remotas Não Confiáveis é um bom indicador de que deve-se acessar essa página.

A coluna Análise de Causa Raiz também possui um ícone para redirecioná-lo automaticamente para a página de Injeções, mostrando apenas as injeções de processo relacionadas à resposta

63602703.png?width=680
Após clicar no ícone de injeções, você será direcionado para a página de Injeções de Processos, onde verá apenas as injeções de processo relacionadas à resposta:

63569930.png?width=680
Aqui, na página de Eventos de Injeção de Processos, vemos o caminho e os argumentos do processo injetor, e o caminho e os argumentos do processo injetado. Geralmente, os argumentos desempenham um papel muito importante na análise de memória ou indicam, por exemplo, quais comandos do PowerShell devem ser executados. Os IDs de processo também estão presentes, para ajudar a rastrear injeções iterativas realizadas à medida que um invasor pula de processo em processo, ou para consultar a análise de causa raiz na página de Criação de Processos.

63438879.png?width=680
Como sabíamos que o rundll32.exe era, na verdade, um fornecedor de antivírus? Continue lendo!

Análise de Criação de Processos

É muito raro que um invasor use apenas um processo durante seu ataque. Ele pode nem saber que as ferramentas que está usando estão gerando novos processos e utilizando diversas ferramentas administrativas no sistema infectado.

A página de Criação de Processos rastreia todos os processos que abrem outros processos (ou a si mesmos), os argumentos usados e os IDs de processo, ou Pids, para cada origem e destino.

Isso é realizado no nível do kernel, o que significa que nada é perdido.

Observação: a telemetria da Microsoft possui parte desses dados, mas não todos. Optamos por não usar essa fonte de dados, pois observamos que ela deixa de registrar eventos importantes ou é desativada por invasores durante um ataque.

O quão boa é nossa visibilidade?

Juntando tudo - uma investigação completa

O quão boa é nossa visibilidade, e quão rápido você pode realizar uma Análise de Causa Raiz? Confira este exemplo - um antivírus, com algumas das permissões mais altas em um sistema, foi observado tentando injetar código em nosso software Cyber Crucible. Esperamos que fosse para investigar nosso software, mas ainda assim entramos em modo de autoproteção (ou seja, isso fez com que nosso software rejeitasse a adulteração do antivírus... não há portas dos fundos que permitam acesso para edição ou uso de nosso software por terceiros externos).

Então, vamos começar aqui, com uma resposta automatizada:

63569937.png?width=680
Obviamente, o Cyber Crucible não é ransomware. Vemos aqui uma tentativa de injeção de processo envolvendo comportamento suspeito de thread remota, em conjunto com comportamentos semelhantes à extorsão de dados.

OK - vamos ver o que está acontecendo em Eventos de Injeção de Processos clicando no ícone de injeções. 5 segundos depois - já temos nossa resposta!

63471644.png?width=56463438879.png?width=680

Mas espere - rundll? Isso não é um hacker, é? Certamente, não é um programa hacker.exe. Vamos fazer alguma filtragem, para obter nossa resposta na página de Criação de Processos. Não temos uma captura de tela aqui, mas os IDs de processo estão disponíveis para todas as respostas e injeções de processo. Vamos voltar à página de respostas e clicar no ícone de criações de processo para nos levar à página de Criações de Processos e filtrar automaticamente a grade para mostrar as criações de processo relacionadas a esta resposta.

63537184.png63438886.png?width=680

Rápido e fácil, agora vemos que a “raiz” (sem trocadilhos) foi o WebRoot, um fornecedor de antivírus, que gerou um processo rundll32.exe para carregar uma das DLLs do WebRoot, que então tentou fazer *algo* com o software do Cyber Crucible, para forçá-lo a percorrer arquivos como uma ferramenta de roubo de dados.

Por que escolhemos mostrar este exemplo?

Temos inúmeros exemplos de técnicas de invasores, com níveis variados de competência por parte deles. Os antivírus alcançam um nível de permissões em um sistema que exige um nível muito alto de habilidade, tecnologia e preparação por parte dos invasores. O Cyber Crucible detectar comportamentos “semelhantes a hackers” de uma ferramenta de segurança convencional e, em seguida, interrompê-los automaticamente, demonstra alguns dos mais altos níveis de excelência em engenharia e segurança de nossa parte, sem se perder em exploits individuais ou técnicas específicas de invasores.

O que a Página de Injeções de Processo mostra?

As injeções de processo são uma capacidade de engenharia de software que pode surgir em um contexto não malicioso, ou ser usada diretamente por um atacante. Na verdade, a injeção de processo e as técnicas associadas são uma das favoritas dos atacantes, por uma variedade de razões que estão fora do escopo deste artigo (mas, se você perguntar, podemos indicar treinamentos).

A Cyber Crucible expõe eventos de injeção de processo em nível de kernel. Isso significa que você tem visibilidade completa de todos os processos e suas informações, independentemente das permissões desse processo. Algo que descobrimos é que, uma vez que atacantes ou software atingem um certo nível de permissões, muitas das fontes tradicionais de telemetria para ferramentas de segurança ficam em silêncio. Nunca perder um dado importante e nunca ficar em silêncio é uma grande parte do nosso design de produto de confiança zero.

Na página de Injeções de Processo, você verá o seguinte por evento, com filtros disponíveis para refinar suas consultas:

CC_Showing_All_Process_Injection_Columns.mp4
Normalmente, no decorrer de uma investigação, você constatará que há atividade adicional na página de Criação de Processo.

O que a Página de Criações de Processos mostra?

É muito raro, possivelmente nunca, que um atacante execute um ataque inteiro a partir de dentro de um único processo.

O fato de uma ferramenta de ataque ou uma biblioteca do Windows estar utilizando múltiplos processos e programas do Windows é, por vezes, invisível para os usuários do malware (ou seja, os criminosos).

Os comportamentos de processos representam uma fonte importante de variáveis durante a tomada de decisão da Cyber Crucible, a qual envolve indicadores comportamentais provenientes de diversas fontes.

Por vezes, esses comportamentos de processos podem, em última instância, resultar na suspensão de um processo devido a roubo de dados ou criptografia por ransomware, podendo ser rastreados desde o ponto de entrada do atacante no sistema até a execução final do software de extorsão.

Em outras ocasiões, o rastreamento de processos pode identificar acesso remoto não autorizado, fraude, ameaça interna ou software inesperado, mas não extorsão de dados. Ou seja, algo que o software de prevenção de extorsão de dados da Cyber Crucible não suspenderá automaticamente, mas que ainda assim é importante conhecer.

Independentemente de os dados do processo fazerem parte de um ataque de extorsão de dados, de outro evento digno de nota, ou apenas de um comportamento normal do programa, as informações de origem e destino dos programas, incluindo os argumentos do programa, são disponibilizadas. Isso fornece um conjunto rico de dados para rastrear atacantes, inclusive aqueles que utilizam táticas de “living off the land”.

Abaixo está uma captura de tela do tipo de dados que podem ser coletados a partir das criações de processos.

CC_process_creation_demo.mp4

O que são Resumos de Relatórios Executivos?

Introdução

Os Resumos de Relatórios Executivos são relatórios enviados por e-mail aos usuários que detalham informações sobre licenças, agentes e comportamentos de máquinas dos usuários. Os relatórios contêm um resumo de todos os grupos aos quais o usuário pertence, seguido por um resumo para cada grupo individual.

Os usuários têm a opção de receber relatórios semanais e mensais, além de poderem escolher o formato do relatório enviado no e-mail (HTML, ZIP, etc.).

Como Ativar e Desativar o Recebimento de Relatórios

Após fazer login em nosso site e navegar até a página de Configurações da Conta, os usuários verão as opções para definir suas preferências de recebimento de relatórios semanais e mensais, além de configurar o formato do relatório enviado no e-mail.

24051723.png?width=442

Exemplo de Conteúdo do Relatório

23887914.png?width=44224084489.png?width=44223855156.png?width=442

Como faço para exibir agentes ocultos?

Acesse a página Agents e localize a coluna Dashboard Visibility.

86048770.png?width=680
O filtro padrão dessa coluna faz com que os agentes ocultos não sejam exibidos.

Para exibir os agentes ocultos, abra o filtro dessa coluna e marque a caixa Hidden, desmarcando a caixa Visible, e clique em Apply.

Isso exibirá apenas os agentes ocultos. A partir daí, você pode realizar as operações normais de gerenciamento de agentes, incluindo a alteração da visibilidade.

86016006.png?width=45386016013.png?width=680

Como ocultar ou remover um agente?

É importante entender que remover um agente também excluiria todos os dados coletados por meio desse agente. Essa informação pode ser útil algum dia para uma investigação futura.

Em vez disso, ocultar o agente da visualização, das notificações ou dos alertas é provavelmente a ação desejada.

Há duas maneiras de fazer isso.

Atualização em Massa de Agentes

O primeiro método é mais fácil se houver vários agentes que precisam ser ocultados do aplicativo web.

Primeiro, selecione os agentes que deseja ocultar, na página Agentes.

Normalmente, os usuários utilizam filtros com base no status de instalação, nome da máquina ou endereço IP primeiro.

Segundo, selecione o ícone “Bulk Set Agent Default Visibility” (Definir Visibilidade Padrão dos Agentes em Massa).

86048779.png?width=680
Aparecerá um modal onde você pode selecionar se a visibilidade padrão dos agentes selecionados será oculta ou visível. Em seguida, clique no botão “Update Selected Agents” (Atualizar Agentes Selecionados).

86081547.png?width=448
A configuração padrão para notificações de segurança é enviar alertas de agente offline para agentes ocultos. Saiba mais sobre notificações de segurança aqui.

Atualizar um Único Agente

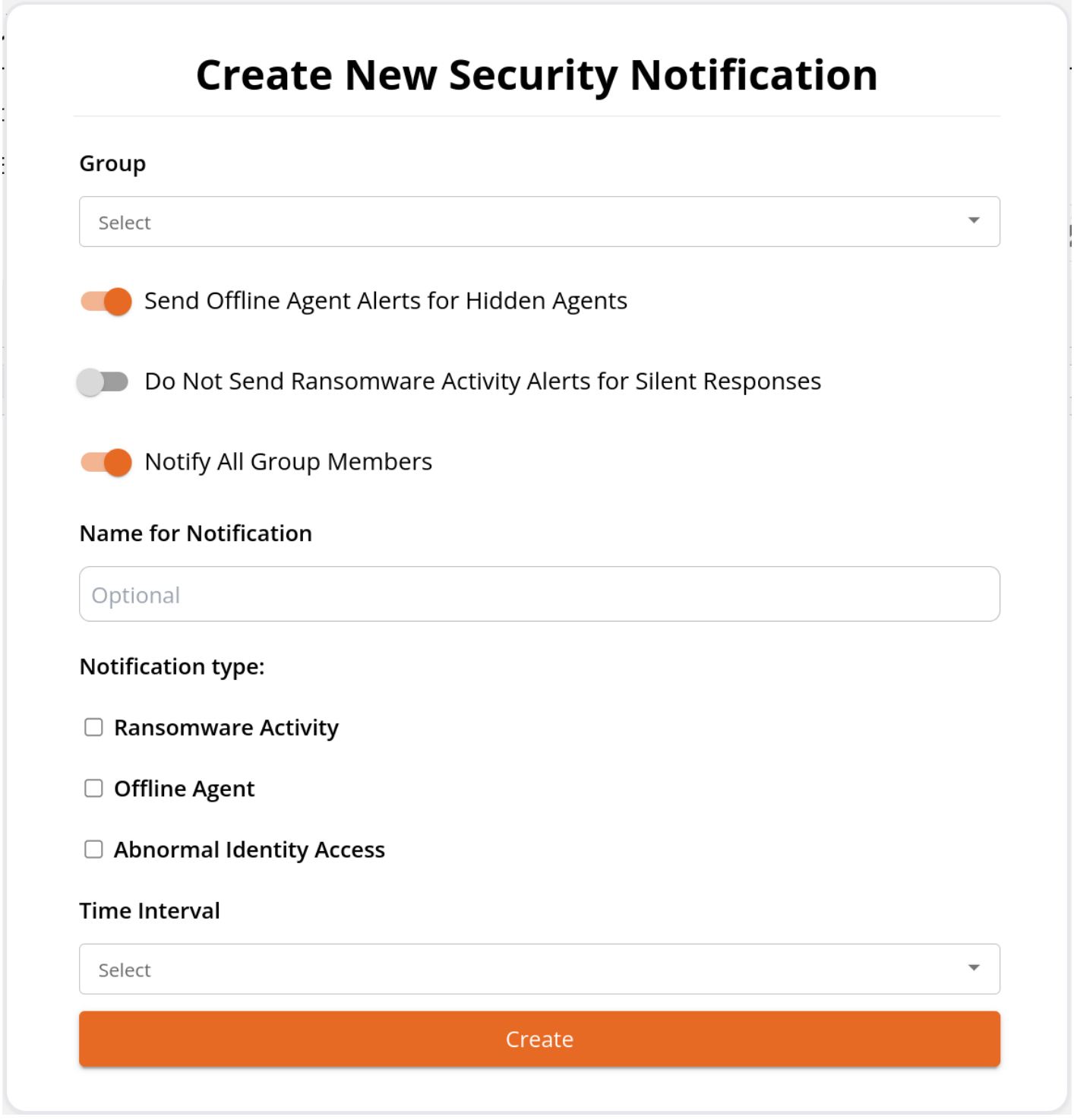
Na página Agentes, localize a Coluna de Visibilidade do Painel e alterne o controle deslizante Visível para o agente desejado a fim de alterar a visibilidade.

86016024.png?width=680

Se eu ocultar um agente, ainda receberei alertas e notificações?

A configuração padrão para notificações é enviar alertas de agente offline para agentes ocultos.

Vemos abaixo a configuração padrão durante a criação de notificações:



Normalmente, os usuários criam uma categoria de notificação separada para notificações de agentes ocultos, para os casos raros em que isso é desejado. Recomendamos que essas notificações tenham aliases de e-mail de destino diferentes e, possivelmente, um intervalo de notificação diferente.

Se uma notificação existente exigir uma atualização neste campo, acesse a página de Notificações de Segurança.

Role para a direita na grade até visualizar a coluna Enviar Alertas Offline para Agentes Ocultos e, em seguida, alterne o controle deslizante conforme desejado.

A alteração terá efeito imediatamente.