Implantação e Gerenciamento de Agentes

Instalação, configuração, atualização e verificação do agente Cyber Crucible, incluindo integração, requisitos do sistema e configuração de rede.

- Como posso testar a conexão com esses domínios?
  - Verificação de Cadeias de Certificados
- Como monitorar a Integridade do Agente?
- Quais versões do Windows são compatíveis com a Cyber Crucible?
- Quais são as Taxas Normais de Consumo de Recursos para RAM e CPU?
- Como posso verificar se o Cyber Crucible está em execução no sistema?
- Como sei quando um agente termina a Autoconfiguração Após a Instalação?
- Processo de Integração
- Implantação em um Ambiente Já Infectado
- Como posso testar a conexão TLS com esses domínios?
- Por que posso precisar de um proxy?
- Qual é a quantidade de dados produzida pela Cyber Crucible?
- Como faço para desinstalar vários agentes de uma só vez?
- Como faço para desinstalar um único agente?
- Testando se o Software Cyber Crucible Está "Funcionando"
- Como Gerenciar Configurações de Proxy

Como posso testar a conexão com esses domínios?

Como posso testar a conexão com esses domínios?

Verificação de Cadeias de Certificados

O script PowerShell a seguir pode ser utilizado para exibir a cadeia de certificados obtida por uma determinada máquina. Isso pode ser útil para depurar problemas de SSL ou investigar o impacto de uma configuração de firewall SSL.

Uso

Na linha de comando do PowerShell, execute o script com o parâmetro -TargetHost. Por exemplo:

```
.\Get-SslCertificateChain.ps1 -TargetHost "agent.oauth.rpp.cybercrucible.com"
```

Em gera a seguinte saída:

```
SSL Connection established to agent.oauth.rpp.cybercrucible.com:443
Certificate Chain:
  Leaf Certificate (Subject): CN=agent.oauth.rpp.cybercrucible.com
True
    - Subject: CN=agent.oauth.rpp.cybercrucible.com
      Issuer: CN=E7, O=Let's Encrypt, C=US
      Thumbprint: 2E401711BBC229F34B8A13D0233264CFBB155C82
      Valid From: 10/05/2025 06:06:01
      Valid To: 01/03/2026 05:06:00
    - Subject: CN=E7, O=Let's Encrypt, C=US
      Issuer: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Thumbprint: 3B73C17E3DF87CF3AA77F1389219EB5EDD519E7F
      Valid From: 03/12/2024 20:00:00
      Valid To: 03/12/2027 18:59:59
    - Subject: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Issuer: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Thumbprint: CABD2A79A1076A31F21D253635CB039D4329A5E8
      Valid From: 06/04/2015 07:04:38
      Valid To: 06/04/2035 07:04:38
```

Como monitorar a Integridade do Agente?

Monitoramento de Agente Offline/Online

Página de Agentes

Na página de Agentes, a data e hora do último check-in **por atividade** é registrada. De modo geral, se um agente de software estiver funcionando e conectado à Internet, cada comportamento deverá ter uma data de menos de algumas horas. Algumas atividades são acionadas por atividades no endpoint, enquanto outras são definidas por temporizadores, mas com um deslocamento de "jitter" de até 30 segundos, para que os clientes não tenham picos na atividade de rede.

85753879.png?width=680

Gerenciamento de Notificações Offline

Para configurar a notificação de agentes offline, use a página de Notificações de Segurança.

Essas notificações destinam-se às seguintes situações:

1. Há um problema de rede entre um agente e os servidores da Cyber Crucible. Isso pode ser devido a um firewall (motivado por um hacker, ou apenas por operações de TI), ou o agente está em execução, mas offline. A proteção é mantida durante os períodos offline, mas as notificações à equipe de segurança não ocorrerão até que o agente volte a ficar online.
2. Há um problema com o software da Cyber Crucible. Isso é muito, muito raro. Por favor, abra um chamado de suporte com a Cyber Crucible imediatamente, caso isso ocorra.
3. A máquina está desligada. Este é o cenário mais comum. A seguir, discutiremos as melhores práticas.

85688410.png?width=680

Melhores práticas para Notificação Offline

Uma consideração importante sobre a notificação offline é que uma máquina que foi desligada aparecerá como offline para os servidores da Cyber Crucible. Estações de trabalho, propensas a serem ligadas e desligadas durante as operações normais de negócios, produziriam notificações offline durante pausas para almoço, deslocamentos entre locais ou durante feriados.

As melhores práticas para grupos já separam servidores de estações de trabalho. Servidores geralmente são melhor atendidos com períodos de notificação offline mais curtos, caso haja algum problema. Grupos focados em estações de trabalho são melhores para períodos mais longos de aparência offline.

Muitos clientes da Cyber Crucible consideram melhor criar notificações automatizadas apenas para grupos de servidores, e filtrar periodicamente um dos campos de data na página Gerenciar Agentes por uma data, como “Mostrar-me agentes cujo campo de Atualização de Dados da Máquina não foi atualizado na última semana”.

85688417.png?width=453

Agentes Que Não Estão Totalmente Atualizados

Os agentes da Cyber Crucible exigem uma reinicialização para atualizar. Um entendimento mais aprofundado dos algoritmos de atualização pode ser encontrado aqui. Quando um agente informa que uma reinicialização resultará em uma atualização, a página de Agentes lista quais máquinas requerem uma atualização e estão prontas para atualizar após a reinicialização. Às vezes, máquinas que não são reinicializadas com frequência (normalmente servidores) acumulam várias atualizações antes de realmente atualizar. Vemos um exemplo disso na captura de tela. O horário da última reinicialização também está disponível.

O relatório executivo semanal da Cyber Crucible identifica o número de agentes que requerem uma atualização, e quantos deles estão prontos para atualizar assim que forem reinicializados. Os dois motivos mais comuns pelos quais uma máquina requer uma atualização, mas não está pronta/preparada, são:

1. A máquina esteve offline, como um funcionário de férias.
2. A máquina teve uma falha/renovação de hardware ou de software importante, e a Cyber Crucible, na verdade, não está mais nessa máquina.

Fora esses dois casos, as atualizações normalmente ocorrem muito rapidamente, e sem envolvimento do administrador, além das atividades normais de aplicação de patches e reinicialização.

85688423.png

Quais versões do Windows são compatíveis com a Cyber Crucible?

Versão Desktop	Versão Servidor	Suporte
11 10 8.1 8	2025 2022 2019 2016 2012 R2 2012 R1	Totalmente compatível.
7	2008 R2	É necessário aplicar patch para suporte à assinatura de código SHA-2.
Vista e versões anteriores	2008 R1 e versões anteriores	Não compatível.

Quais são as Taxas Normais de Consumo de Recursos para RAM e CPU?

O uso típico de CPU é de 1% ou menos (que aparece como 0% na maioria das ferramentas de monitoramento, como o Gerenciador de Tarefas).

O uso típico de RAM é inferior a 10 MB. A maioria do uso em desktops e servidores é de cerca de 5MB.

Também monitoramos o uso de memória do driver no espaço do kernel, para verificar quaisquer problemas.

Como posso verificar se o Cyber Crucible está em execução no sistema?

Serviços

Abra o Gerenciador de Tarefas.

Clique na aba Serviços.

Ordene por nome, se necessário, e role até CyberCrucibleAgent/ Cyber Crucible Agent

image-20250811-181519.png

Driver de Kernel

Abra um prompt de comando como Administrador.

Execute o comando observado na captura de tela abaixo:

fltmc.exe | find “CCRRSecMon”

3047503.png?width=561
fltmc.exe lista os drivers carregados.

Provavelmente há vários, então o comando find mostra apenas o driver do Cyber Crucible, chamado CCRRSecMon.

Se o driver estiver listado, ele está carregado e em execução corretamente no sistema operacional.

Como sei quando um agente termina a Autoconfiguração Após a Instalação?

Na página Agents (Agentes) do painel, cada agente possui alguns registros de data e hora indicando a última vez que recebeu determinados tipos de informação. Um agente é considerado como tendo concluído a autoconfiguração quando, além de ter uma licença válida atribuída, apresenta registros de data e hora nas seguintes colunas:

- Last Validation Check
- Latest Schedules Download
- Latest Tailored Behaviors Download
- Latest Certificate Bundle Download

Além disso, se o Grupo tiver

Processo de Integração

- Gestão de Grupos
- Configuração de Alertas de Segurança do Agente
- Melhores Práticas de Planeamento da Instalação do Agente
- Instalar o Agente
- Estratégias de Atualização para Grupos e Agentes
- Como Investigar a Causa Raiz de uma Resposta de Extorsão
- Comportamentos Personalizados
- Integração REST

Gestão de Grupos

Antes de instalar os agentes, os utilizadores podem querer preparar-se configurando os seus grupos. Siga as instruções de Gestão de Grupos aqui.

Configuração de Alertas de Segurança do Agente

Os utilizadores podem configurar notificações por email para eventos de segurança, incluindo atividades de ransomware, acessos de identidade anómalos e agentes offline. As instruções podem ser encontradas aqui.

Melhores Práticas de Planeamento da Instalação do Agente

Alguns ambientes têm um comportamento e configuração semelhantes de utilizadores, aplicações e sistemas em toda a sua atividade empresarial. Outros têm grupos especializados que se comportam de forma diferente, como uma equipa de vendas em comparação com uma divisão de engenheiros de software.

A implementação e configuração são tão rápidas que dedicar alguns minutos a planear uma instalação num subconjunto de computadores de secretária ou servidores que partilhem os mesmos comportamentos empresariais ou aplicações permitir-lhe-á avaliar se é necessário ter em conta alguma aplicação.

Além disso, é muito comum a Cyber Crucible descobrir software de gestão e VPNs previamente desconhecidos (e não autorizados), scripts de administração não autorizados, software mal configurado, ou até mesmo infeções durante a implementação inicial.

Instalar o Agente

Quando estiver pronto para instalar os seus agentes, as instruções podem ser encontradas aqui e aqui

Estratégias de Atualização para Grupos e Agentes

Para gerir as estratégias de atualização para grupos e agentes, siga as instruções aqui.

Como Investigar a Causa Raiz de uma Resposta de Extorsão

A página de Resposta de Extorsão pode ser encontrada no separador Operações na barra lateral. As instruções sobre como investigar a causa raiz de um alerta podem ser encontradas aqui.

Comportamentos Personalizados

As instruções para criar comportamentos personalizados podem ser encontradas aqui.

Integração REST

Alguns utilizadores podem querer integrar com o nosso servidor REST. A página de Integração REST com documentação pode ser encontrada no nosso website no separador Administração na barra lateral.

Implantação em um Ambiente Já Infectado

- Contexto
- O Que Acontece Imediatamente Após a Instalação
- O Que Acontece com Malware Dormente, Aguardando Tarefas Futuras?
- Detalhes Adicionais - Reinicializações Podem Ser Valiosas

Contexto

As implantações de clientes da Cyber Crucible resultam rotineiramente na descoberta de infecções anteriormente desconhecidas. As redes normalmente não estão livres de infecções, mesmo que as ferramentas de defesa de segurança cibernética existentes tenham dado sinal verde.

Um ataque de ransomware fornece um ponto de demarcação, ou ponto crucial, altamente visível, para que uma empresa meça com que frequência os hackers conseguem realizar um novo ataque com sucesso, e qual é o grau de sucesso desses ataques.

- Relatórios de código aberto e inteligência de ameaças revelam uma taxa de reataque de clientes que não são da Cyber Crucible de cerca de 80%.
- A Cyber Crucible observou que cerca de 10% dos endpoints têm pelo menos uma tentativa de roubo de identidade, como senhas, chaves ou tokens, por período de 90 dias.
- A Cyber Crucible observa que os atacantes tentam retomar uma posição em um ambiente aproximadamente uma vez por mês.

Do ponto de vista de resposta a incidentes ou forense, a Cyber Crucible é uma excelente ferramenta para retomar o controle da rede. Especialmente para vítimas de ataques, suspeitamos que os atacantes mantêm visibilidade sobre o estado de recuperação e a saúde financeira das vítimas, para melhor cronometrar quando atacar novamente.

O Que Acontece Imediatamente Após a Instalação

A Cyber Crucible começa automaticamente a suspender programas em execução que sejam observados se comportando de forma maliciosa.

A implantação do produto Cyber Crucible pode resultar na suspensão de múltiplos programas em múltiplas máquinas, à medida que o ambiente é limpo.

Às vezes, uma implantação parcial da Cyber Crucible pode resultar em uma tentativa do hacker de retomar o controle através das máquinas que não possuem a proteção da Cyber Crucible.

Por exemplo, a Cyber Crucible foi certa vez instalada em apenas uma parte dos desktops de uma vítima recente de violação de dados. Os hackers tentaram desinstalar a Cyber Crucible conectando-se a partir das máquinas desprotegidas e, por fim, começaram a desligar as máquinas protegidas.

O Que Acontece com Malware Dormente, Aguardando Tarefas Futuras?

Um malware que não está agindo em nome dos atacantes é acionado quando o malware começa a acessar dados.

Vamos percorrer um cenário:

Duas máquinas têm malware nelas. Vamos chamá-las de Máquina A e Máquina B.

Ambas as amostras de malware são atualmente indetectáveis pelas suas ferramentas de segurança favoritas.

O malware da Máquina A não faz nada, apenas aguarda instruções. A Cyber Crucible não detecta o malware. O malware também ainda não é detectável por outras ferramentas de segurança.

O malware da Máquina B está tentando acessar dados ou dados de identidade. Imediatamente após um ataque bem-sucedido, os comportamentos mais comuns que observamos, quando os atacantes atribuem tarefas ao seu malware, são garantir que possuem dados de identidade atualizados, como senhas ou tokens, e enumerar novos dados. Ou seja, em parte, "obter as novas senhas após os administradores redefinirem as senhas", e, em parte, "ficar de olho em busca de novos dados".

Na Máquina B, a Cyber Crucible suspende imediatamente a aplicação.

Depois de um período que varia de um mês a um ano, o malware da Máquina A é finalmente identificado após um número suficiente de vítimas ter reportado o malware aos bancos de dados

dos fornecedores de segurança. Quanto mais disciplinados forem os atacantes na distribuição dessa amostra, mais tempo esse malware específico permanecerá indetectado.

O malware da Máquina B foi neutralizado, congelado no lugar.

O malware da Máquina A está preso. No segundo (bem, 100 milissegundos) em que tenta acessar quaisquer dados ou informações de identidade, o malware da Máquina A é suspenso. O cliente está protegido, mesmo que o malware exista por dias, ou até anos, sem ser detectado por outras ferramentas.

Detalhes Adicionais - Reinicializações Podem Ser Valiosas

Algumas de nossas análises são mais precisas quando o ciclo de vida do processo pode ser rastreado desde o início da aplicação até o estado presente.

Reinicializar uma máquina após a instalação pode ser vantajoso.

Programas já em execução antes da instalação não terão inspeção analítica completa por parte da Cyber Crucible. A reinicialização força esses programas a reiniciarem, proporcionando, assim, inspeção completa a todos os programas.

Como posso testar a conexão TLS com esses domínios?

Além de simplesmente executar um ping nos domínios utilizados pela Cyber Crucible para garantir que seu endpoint consiga alcançar todos os endereços de rede corretos, o instalador do Cyber Crucible Agent inclui um argumento de teste que garante que uma conexão TLS/SSL válida possa ser estabelecida em ambas as direções com todos os servidores necessários.

Untitled-20240410-185719.png
Basta adicionar `--test-connection` à execução do instalador, certificando-se de ainda incluir o(s) id(s) de grupo e os tokens OAuth necessários para realizar a autenticação. Acima está uma captura de tela mostrando a única modificação necessária no script .bat fornecido, e uma saída bem-sucedida.

Anexos:

▨ Untitled-20240410-185719.png (image/png)

Por que posso precisar de um proxy?

Embora toda a detecção e proteção comportamental do agente Cyber Crucible ocorra no endpoint, sem necessidade de enviar amostras para a nuvem para análise, o agente do endpoint ainda requer uma conexão com um servidor para receber informações de licenciamento, configuração, atualizações de software, etc.

Se a sua rede estiver bloqueada a ponto de não permitir conexões com os intervalos de IP onde os servidores da Cyber Crucible estão hospedados, então pode ser necessário configurar um proxy para permitir que o agente (somente) alcance seu servidor para instalação. Consulte How to Manage Proxy Configurations para obter informações sobre como configurar o agente.

Que tipo de proxy posso usar?

A partir da versão 4.4.6.3 do agente Cyber Crucible, as configurações de proxy suportam Socks5. Não há restrição quanto ao local onde o servidor está hospedado (localmente ou externamente), desde que as restrições de rede permitam que os agentes o alcancem. Um exemplo de diagrama é apresentado abaixo, mostrando uma configuração simples de proxy em que o servidor Socks5 está hospedado dentro da rede bloqueada e tem permissão apenas para se conectar a uma máquina externa que faz o tunelamento do tráfego.

SOCKS5H.png

Essa configuração permite que os agentes se conectem aos seus servidores, mantendo ao mesmo tempo a política de rede. Exige apenas 1 regra que permite que o host Socks5 alcance seu servidor proxy externo em uma única porta (ssh). Isso garante que todo o tráfego não apenas ocorra na porta 443, mas também seja duplamente encapsulado em SSH antes de sair da rede, sem exigir nenhum redirecionamento de porta de entrada (port-forwarding).

Qual é a quantidade de dados produzida pela Cyber Crucible?

Os dados coletados pelo agente da Cyber Crucible passam por múltiplas camadas de filtragem, a fim de eliminar o ruído decorrente do excesso de telemetria bruta. Os dados brutos produzidos pelos sensores do kernel são reduzidos [**Filtro nº 1**] para diminuir tanto o uso de memória do endpoint quanto a largura de banda de rede por agente. Em seguida, a API REST associará a telemetria bruta de processo/endpoint recebida a respostas automatizadas, de modo que o analista possa optar por visualizar apenas os dados relevantes [**Filtro nº 2**].

Blank diagram-20240523-165941.png

Como visto na figura acima, os endpoints de estações de trabalho de um cliente médio podem produzir vários gigabytes de dados brutos de sensores ao longo de um período de 24 horas, enquanto apenas alguns megabytes desses dados serão relevantes para um alerta do SOC caso um ataque seja tentado.

Como faço para desinstalar vários agentes de uma só vez?

Desinstalar vários agentes de uma só vez é simples.

Vá até a página Agents.

Recomendamos usar filtros, como filtros de nome da máquina, grupo, endereço IP ou versão, para exibir na tela o maior número possível de agentes. Isso é especialmente útil para usuários com centenas ou milhares de agentes em um grupo.

85983282.png?width=680
Aqui, usamos a tecla shift, enquanto clicávamos em 3 linhas, para selecionar três agentes.

O botão Uninstall All Selected Agents fica no canto superior esquerdo, acima da grade.

Depois que as permissões forem verificadas no servidor, confirmando que você tem permissão nos grupos dos agentes, os comandos de desinstalação serão emitidos.

Os agentes recebem um comando de desinstalação assinado digitalmente. A assinatura é usada pelos agentes para validar que o comando realmente veio da Cyber Crucible, e não de um criminoso tentando remover o seu software de proteção.

Depois que os agentes validam o comando, eles preparam o sistema para a desinstalação na próxima reinicialização.

A coluna Attention exibirá a entrada “Uninstall in Progress” e mostrará um botão Cancel Uninstall na célula.

Assim que a máquina for reiniciada, o agente valida se a desinstalação está sendo realizada e remove todos os arquivos.

É importante observar que o agente confirmará “um último olá” antes de se desinstalar completamente, portanto, às vezes os agentes permanecerão presentes por um curto período após a reinicialização. Isso ocorre porque, em alguns ambientes de rede, a conexão pode não funcionar corretamente por até 30 segundos após a área de trabalho ficar visível. Observe que, assim que as desinstalações forem concluídas, as licenças são automaticamente removidas dos agentes.

Como faço para desinstalar um único agente?

Acesse a página Agents.

Localize o agente desejado e clique no ícone de lixeira na coluna Agent Name:

86081562.png?width=680

Testando se o Software Cyber Crucible Está "Funcionando"

Introdução

O Cyber Crucible foi projetado para funcionar sem interromper os usuários finais ou funcionários, ao mesmo tempo em que notifica discretamente os usuários do Dashboard escolhidos (normalmente membros selecionados das equipes de TI e Segurança) sobre as respostas automatizadas.

Muitos dos simuladores de ransomware ou malware não capturam com precisão o comportamento de um hacker. Embora isso cause problemas para ferramentas como o Cyber Crucible que (corretamente) identificam a simulação como um falso positivo, isso não é necessariamente algo ruim.

Alguns fornecedores chegam a construir seus mecanismos de detecção em torno desses simuladores para parte de sua funcionalidade de detecção, para garantir que quaisquer testes de clientes sejam aprovados com louvor.

Ações reais de malware, como a criptografia de ransomware, correm o risco de criptografar ou corromper dados de forma irrecuperável. Na Cyber Crucible, já vimos até ransomware ativar secretamente outros malwares na rede, ou realizar outras ações que poderiam prejudicar a empresa que está tentando testar o Cyber Crucible.

Portanto, você não quer usar malware, e também não quer usar um simulador tão preciso a ponto de correr o risco de corromper acidentalmente seus dados.

Testando o Cyber Crucible

Existe uma maneira fácil de testar o Cyber Crucible sem usar malware ou uma simulação tão realista que coloque em risco os dados sua empresa ou os seus.

O Cyber Crucible avalia os acessos à identidade digital a cada milissegundo do dia. Muitas dessas identidades digitais são armazenadas nos navegadores - é por isso que os atacantes colocam os navegadores web no topo da lista para seus ataques automatizados.

A análise comportamental de acesso à identidade do Cyber Crucible resultará em uma das três respostas:

1. Não fazer nada
2. Ocultar os dados
    1. aplicativo legítimo conhecido que passa em todas as verificações de memória e kernel, mas não precisa de acesso àquele dado de identidade específico - exemplo: Windows Explorer não explorado
3. Suspender o processo
    1. aplicativo legítimo conhecido que deveria ter acesso ao dado de identidade, mas foi hackeado, ou
    2. um aplicativo estranho

Aqui estão dois locais comuns para usuários do Windows:

Neste caso, o nome de usuário do Windows é "denni", e estes são os locais onde os dados de sessão são armazenados. Você pode descobrir que a variável %LOCALAPPDATA% funciona para você, caso não queira descobrir o nome de usuário.

- C:\Users\denni\AppData\Local\Google\Chrome\User Data\Default\Sessions
    - %LOCALAPPDATA%\Google\Chrome\User Data\Default\Sessions
- C:\Users\denni\AppData\Local\Microsoft\Edge\User Data\Default\Sessions
    - %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Sessions

A Visualização Sem o Cyber Crucible Instalado

Vamos primeiro ver como uma dessas pastas se apresenta com o Explorer.exe, sem o Cyber Crucible instalado.

Screenshot 2025-05-14 103339.png
Aqui, vemos múltiplas Sessões do Chrome sob o perfil "default" do Google Chrome.

Essas informações normalmente contêm dados sensíveis que um atacante desejaria usar para sequestrar sessões com programas importantes, como portais de administração de TI, bancos, e-mail, ou ferramentas de armazenamento como Google Drive ou Dropbox.

A Visualização Com o Cyber Crucible Instalado

Após instalar o Cyber Crucible, um teste rápido pode ser realizado, sem usar malware ou qualquer tipo de técnica criminosa ou uso indevido de equipamentos de TI.

Neste caso, o mesmo local de armazenamento de sessão do navegador é usado:

- C:\Users\denni\AppData\Local\Google\Chrome\User Data\Default\Sessions
  - %LOCALAPPDATA%\Google\Chrome\User Data\Default\Sessions
- C:\Users\denni\AppData\Local\Microsoft\Edge\User Data\Default\Sessions
  - %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Sessions

Screenshot 2025-05-14 103620.png
O Cyber Crucible, imediatamente após a instalação, já está bloqueando o acesso aos dados naquela pasta.

Observe que este é exatamente o mesmo processo do Explorer que já estava em execução no momento da instalação, portanto o programa em execução teve seu acesso subitamente revogado na camada do "disco rígido" ou kernel. Mesmo programas benignos, explorados ou malwares que já estejam em execução são avaliados corretamente pelo Cyber Crucible.

Visualizando seu Teste no Dashboard do Cyber Crucible

Existe um grande número de acessos a dados de identidade em um sistema em execução, o tempo todo.

O Software as a Service e os programas baseados em nuvem resultaram em muitos sites e aplicativos que têm conteúdo limitado no próprio site, enquanto o navegador (ou navegador incorporado para aplicativos) se comunica constantemente com servidores de dados para preencher planilhas, tabelas, gráficos e conteúdo de mídia social.

Página de Acesso à Identidade

Os acessos à identidade considerados apropriados para o Cyber Crucible suspender o aplicativo infrator são listados na página de Acesso à Identidade.

Estas são situações em que o programa que acessa os dados de identidade deve ser interrompido, e não apenas ter os dados ocultados.

Neste caso, o Explorer não foi interrompido após a infinidade de verificações que o Cyber Crucible realizou. Em vez disso, os dados foram apenas ocultados.

Screenshot 2025-05-14 103741.png
Portanto, não há violações de acesso à identidade listadas aqui.

Página de Ocultação de Acesso à Identidade

O Cyber Crucible tem, opcionalmente, a capacidade de mostrar aos clientes do Dashboard situações em que dados de identidade foram ocultados, mas nas quais o programa que acessava os dados não foi interrompido.

O Explorer não foi explorado nem malicioso neste teste; ele estava apenas acessando dados de identidade altamente privilegiados dos navegadores Chrome e Edge.

A maioria dos usuários não tem acesso a essas informações, dada a carga adicional nas máquinas e redes dos clientes ao transmitir esses dados para os servidores do Cyber Crucible.

Por favor, solicite se desejar acesso, mas saiba que a atividade que você está vendo não é uma atividade maliciosa, mas sim comportamentos de privacidade de dados de identidade que o Cyber Crucible realiza sob uma perspectiva de GRC, ou aplicação de políticas.

Identity Hide Explorer.mp4
Aqui, vemos neste pequeno vídeo que o Explorer foi impedido de visualizar os dados de sessão do navegador, mesmo que o próprio Explorer não tenha sido interrompido.

Como Gerenciar Configurações de Proxy

- Onde Encontrar a Configuração de Proxy Atual de um Grupo
- Como Atualizar um Grupo para Habilitar um Servidor Proxy
- Como Atualizar um Grupo para Não Usar um Proxy
- Como Remover uma Configuração de Proxy Salva em um Grupo
- Como Instalar um Agente Usando um Proxy
- Onde Posso Ver se um Agente Consegue Contornar o Proxy?

Observe que apenas agentes na versão 4.4.6.3 ou superior possuem essa capacidade

Onde Encontrar a Configuração de Proxy Atual de um Grupo

Os usuários podem visualizar a configuração de servidor proxy atual de um grupo para os agentes seguirem, primeiro navegando até a página Groups encontrada na aba Administration na barra lateral.

A configuração de servidor proxy atual de um grupo pode ser encontrada na coluna “Proxy Server Config“ na grade.

Se o grupo não tiver uma configuração de servidor proxy habilitada, será exibido o texto “Do Not Use Proxy“.

Proxy Server Config Column.png
Se o grupo tiver uma configuração de servidor proxy habilitada, a URL da configuração de proxy atual será exibida

Proxy Server Config Enabled.png

Como Atualizar um Grupo para Habilitar um Servidor Proxy

Os usuários podem habilitar os agentes de um grupo para usar um servidor proxy clicando primeiro no ícone de gerenciar configurações de proxy na coluna “Proxy Server Config” na página Groups. Ao clicar nesse ícone, será exibida uma janela modal onde os usuários podem gerenciar as configurações de servidor proxy do grupo.

Manage Proxy Server Config Icon.png
A janela modal Manage Proxy Server Configuration que aparece é usada para visualizar e gerenciar as configurações de servidor proxy do grupo. Os usuários podem salvar múltiplas configurações dentro de um grupo, e todas as configurações salvas são exibidas na grade dessa janela modal. Observe que todas as configurações de servidor proxy salvas para um grupo também aparecerão na janela modal Download Agent.

Para selecionar uma configuração de servidor proxy para o grupo, a configuração deve primeiro ser enviada no New Proxy Configuration Form. Esse formulário fica oculto por padrão; clique no toggle para exibi-lo.

Manage Proxy Server Configs Modal.pngNew Proxy Configuration Form.png
Após enviar o novo formulário de configuração, ele será exibido abaixo na grade da janela modal.

Para selecionar uma configuração de proxy para os agentes deste grupo usarem, primeiro selecione a configuração desejada e depois clique no ícone de edição acima da grade.

Select Config for Group.png
Após clicar no ícone de edição da configuração de proxy desejada, a configuração de servidor proxy atual do grupo agora é atualizada e pode ser vista nesta janela modal e na coluna “Proxy Server Config”. Os agentes deste grupo agora usarão a configuração de proxy atualizada do grupo. Observe que, se um agente receber instruções para mudar para um servidor proxy inacessível, ele não fará a mudança até que esse servidor se torne acessível.

Mange Proxy Server Config Modal Setting Enabled.pngGroup Proxy Config Enabled.png

Como Atualizar um Grupo para Não Usar um Proxy

Se um grupo tiver um servidor proxy habilitado para os agentes deste grupo usarem e os usuários quiserem atualizar o grupo para que os agentes deste grupo não usem um proxy, primeiro navegue até a página Groups e localize o grupo desejado na grade.

Em seguida, clique no ícone de gerenciar configurações de proxy na coluna “Proxy Server Config“. Ao clicar nesse ícone, será exibida a janela modal Manage Proxy Server Configuration.

Proxy Server Config Column 2.png
Nesta janela modal, clique no ícone x para atualizar os agentes deste grupo para não usar um servidor proxy e se conectar aos nossos servidores normalmente. Observe que a configuração de proxy atual não será removida das configurações de proxy salvas do grupo; esta é uma etapa

separada, explicada na seção abaixo.

Do Not Use Proxy Icon.png
Após clicar no ícone x, a janela modal será atualizada para refletir essa alteração e a coluna “Proxy Server Config“ deste grupo agora exibirá “Do Not Use Proxy“.

No Current Proxy Config Selected .pngDo Not Use Proxy Cell.png

Como Remover uma Configuração de Proxy Salva em um Grupo

Para remover uma configuração de proxy salva de um grupo, primeiro navegue até a página Groups e localize o grupo desejado na grade.

Em seguida, clique no ícone de gerenciar configurações de proxy na coluna “Proxy Server Config“. Ao clicar nesse ícone, será exibida a janela modal Manage Proxy Server Configuration.

Manage Proxy Server Config Icon.png
Nesta janela modal, clique na configuração de proxy salva que deseja remover para este grupo e, em seguida, clique no ícone de lixeira. Após clicar nesse ícone, a configuração de proxy selecionada não aparecerá mais na grade como uma configuração de proxy salva do grupo.

Remove Saved Config.png
Observe que, se você remover uma configuração de proxy salva de um grupo e essa configuração estiver definida como a configuração de servidor proxy atual do grupo, isso também atualizará a configuração de servidor proxy atual do grupo para não usar um proxy.

Como Instalar um Agente Usando um Proxy

Primeiro, navegue até a página Agents encontrada na aba Operations na barra lateral. Em seguida, clique no botão Download Agent. Ao clicar nesse botão, será exibida a janela modal Download Agent.

Download Agent Button.png
Nesta janela modal, se você selecionar um grupo que possui configurações de proxy salvas, a opção Select Proxy Configuration for Installer aparecerá com a configuração atual do grupo selecionada como valor padrão. Todas as configurações de proxy salvas do grupo também

aparecerão como opções, incluindo uma opção Do Not Use Proxy.

Download Agent Modal.pngDownload Agent Modal Proxy Config Options.png
Ao optar por usar um proxy para o instalador, o único tipo de instalador possível é o Command Line Installer.

Se você selecionar a opção Do Not Use Proxy, as opções normais de tipo de instalador serão exibidas.

Download Agent Modal Do Not Use Proxy.png
Observe que, se você selecionar uma configuração de proxy para o instalador que não seja a configuração atual do grupo, o instalador será executado com a configuração selecionada e, em seguida, mudará para a configuração de proxy atual do grupo após a instalação.

Onde Posso Ver se um Agente Consegue Contornar o Proxy?

Os usuários podem ver se os agentes conseguem se conectar aos nossos servidores sem usar um proxy, primeiro navegando até a página Agents encontrada na aba Operations na barra lateral. Em seguida, localize a coluna Agent is Able to Bypass Proxy na grade.

Observe que a coluna Agent is Able to Bypass Proxy não será visível a menos que o usuário seja membro de um grupo que tenha habilitado os agentes do grupo para usar um proxy.

Se o agente estiver em um grupo que habilitou o uso de um proxy e o agente não conseguir contornar o proxy para se conectar aos nossos servidores, o x vermelho será exibido na coluna. Veja um exemplo abaixo:

Agent Cannot Bypass Proxy.png
Se o agente estiver em um grupo que habilitou o uso de um proxy e o agente conseguir contornar o proxy e se conectar aos nossos servidores normalmente, a marca de verificação verde será exibida na coluna. Veja um exemplo abaixo:

Agent Can Bypass Proxy.png