Esta É Uma Ferramenta de Monitoramento Como Meus Outros Painéis de Segurança?

A resposta é: depende de como você e sua organização desejam utilizar a ferramenta, mas provavelmente "não".

É importante observar as estratégias de design de produto da Cyber Crucible:

1. A proteção deve ser hiperautomatizada, e não deve exigir cuidado e atenção constantes (atenção a alertas), nem ajustes manuais (configuração) por parte dos usuários.
2. Para equipes de segurança com mais recursos, a telemetria valiosa deve estar disponível para elas, para atividades avançadas de caça a ameaças, ou para apoiar atividades de perícia forense e resposta a incidentes.
3. A ação nº 2 acima não deve, de forma alguma, degradar a proteção implementada para a ação nº 1.

O feedback mais comum que recebemos da liderança de TI é que seus funcionários não sabiam que a Cyber Crucible já os estava protegendo há semanas.

Temos muitos usuários que utilizam a ferramenta de três formas:

Configurar e Esquecer (Como Seus Detectores de Fumaça)

Muitas organizações não têm recursos para ter caçadores de ameaças analisando a telemetria da Cyber Crucible (ou de outra ferramenta), mas desejam que o risco de extorsão de dados esteja "fora de sua lista de preocupações". Isso é perfeitamente aceitável, e a Prevenção de Extorsão de Dados da Cyber Crucible foi projetada exatamente para isso.

Esses usuários não têm recursos para dedicar tempo a analisar os feeds de dados de Injeção de Processo, Proteção de Credenciais e Criação de Processo.

Portanto, constatamos que, a menos que estejam respondendo a uma rara resposta automatizada da Cyber Crucible, ou realizando gerenciamento de inventário, como quando uma nova máquina precisa ter a Cyber Crucible implantada nela...

...eles simplesmente não fazem login no portal web da Cyber Crucible, e deixam a automação simplesmente fazer seu trabalho.

Isso é perfeitamente aceitável!

Caça a Ameaças Avançada + Proteção Automatizada

As capacidades de injeção de processo, monitoramento de uso de credenciais e criação de processo fornecem um conjunto rico de dados, capturados por meio de análises comportamentais em nível de kernel, para realizar a caça a ameaças.

A proteção automatizada entra em ação assim que se inicia o roubo de dados, o roubo de credenciais (token, senha) ou a criptografia por ransomware. Para tudo o mais - este é um excelente recurso.

A constatação mais comum até o momento é a presença de ferramentas de gerenciamento remoto não gerenciadas (pelo menos pelos administradores de TI atuais) instaladas pelos usuários. Sim, elas às vezes resultam em uma proteção automatizada contra extorsão (ou seja, a RMM não gerenciada é usada por um agente malicioso), mas é sempre melhor conhecer mais sobre seu ambiente previamente, de qualquer forma!

Aqui está um vídeo rápido de um tipo de ataque que vimos sendo utilizado por atacantes, em múltiplos ambientes de clientes, que foi usado com sucesso para evadir as soluções de EDR dos clientes (preferimos não citar nomes... foram 3 produtos em quatro empresas).

rr-com-dll.mp4

Análise Forense e Remediação Pós-Incidente

Existem alguns tipos de casos de uso para os dados da Cyber Crucible.

O primeiro é para que um profissional de segurança de uma empresa, ou um profissional de TI, possa investigar a causa raiz da suspensão de um programa. Para alguns clientes, que normalmente instalam nosso software e depois só fazem login novamente quando há novos funcionários para integrar, eles nunca usaram nenhuma funcionalidade da Cyber Crucible, exceto a página de Gerenciamento de Agentes. Ficamos felizes em ajudá-los a aprender sobre a análise de

causa raiz - que é indolor e simples para usuários técnicos e semitécnicos.

O segundo tipo de cliente para análise forense pós-incidente são empresas de DFIR que são chamadas para investigar um problema em um cliente, às vezes a pedido da seguradora cibernética, e a Cyber Crucible é instalada após um incidente. (Ei, nem sempre podemos estar lá antes do atacante, por mais que queiramos... caso contrário, todas as empresas do mundo nos teriam, e a extorsão seria coisa do passado!)

A melhor forma de descrever uma implementação após um ataque de extorsão é "confusa". Não porque somos difíceis de instalar ou de começar a proteger. Muito pelo contrário! Nesse caso, os atacantes normalmente já se movimentaram pelo sistema, e estão incorporados em sistemas operacionais, equipamentos de rede, Active Directory, e operam em memória. Várias máquinas acabam tendo processos suspensos, e às vezes os atacantes até tentam recuperar o controle. É um pouco como tomar um remédio que faz você se sentir mal no início, mas que é necessário para melhorar de vez.

Clientes que já estão estressados, às vezes reagem emocionalmente a "mais" ruído, à medida que os atacantes são finalmente descobertos e derrotados. Há muita educação sobre por que ou como suas pilhas de segurança já implementadas não encontraram os atacantes. No final, porém, a empresa recupera o controle sobre sua infraestrutura de TI. Eles não se tornarão uma das 80-90% das empresas que são re-extorquidas um ou dois anos depois, no que chamamos de "economia de assinatura de extorsão".

O terceiro tipo de cliente que temos é um MSSP que, frequentemente, é parceiro da Cyber Crucible, e que está respondendo a uma proteção automatizada da Cyber Crucible. Eles precisam descobrir a forma como o atacante conseguiu obter uma posição temporária, e fechar quaisquer brechas de segurança. A boa notícia é que os relatórios de conformidade com a HIPAA ou outros normalmente reportam pouca ou nenhuma violação de confidencialidade, devido à velocidade da resposta automatizada. Muitas vezes, o MSSP relata "nada a relatar", o que deixa todos os envolvidos satisfeitos. Bem, exceto o criminoso.

Revision #1
Created 2026-07-24 05:43:51 UTC by Dennis Underwood
Updated 2026-07-24 05:43:51 UTC by Dennis Underwood