Design Guide
ISH VISION

1. INTRODUÇÃO

No cenário cada vez mais complexo da segurança da informação, a detecção proativa de ameaças direcionadas é fundamental para garantir a proteção de ambientes críticos. É com esse propósito que o ISH Vision emerge como uma solução de vanguarda. Este produto inovador visa oferecer uma detecção de ameaça eficaz contra ataques que miram especificamente os sistemas e dados dos nossos clientes.

No mundo digital interconectado, as ameaças cibernéticas evoluíram para ataques altamente personalizados e direcionados. O ISH Vision é a resposta estratégica para esse desafio, projetado para identificar esses ataques de maneira ágil e precisa. Com algoritmos de detecção avançados e análises comportamentais inteligentes, a solução procura padrões e anomalias sutis que poderiam passar despercebidos pelas abordagens convencionais.

Neste contexto, este documento explora a essência do ISH Vision como um ativo crítico na defesa cibernética. Examina como o produto emprega tecnologias de ponta para identificar comportamentos maliciosos e atividades suspeitas, contribuindo para uma postura de segurança preventiva e estratégica. À medida que mergulhamos nas características fundamentais e nos benefícios do ISH Vision, revelaremos como ele se torna um aliado confiável na constante batalha contra ameaças cibernéticas direcionadas.

2. POSICIONAMENTO E CONCEITO

O NIST (Instituto Nacional de Padrões e Tecnologia) através do seu guia 800-61 defini um processo de resposta a incidente em 4 grandes grupos:

Preparação e Planejamento (Preparation and Planning): Este grupo envolve a criação de políticas, procedimentos e recursos necessários para responder efetivamente a incidentes. Isso inclui a identificação de equipes de resposta, a alocação de responsabilidades e o desenvolvimento de planos de ação.

Detecção e Análise (Detection and Analysis): Neste grupo, a detecção de incidentes é priorizada. Isso abrange a identificação de atividades suspeitas ou anômalas, a coleta de dados relevantes e a análise para determinar a natureza e a gravidade do incidente.

Contenção, Erradicação e Recuperação (Containment, Eradication, and Recovery): Aqui, o foco está em conter a propagação do incidente, eliminar ameaças e recuperar sistemas afetados. São implementadas ações para restaurar a normalidade e minimizar o impacto do incidente.

Lições Aprendidas e Atualizações (Lessons Learned and Updates): O último grupo concentra-se na revisão pós-incidente. As lições aprendidas são documentadas, avaliando o desempenho da resposta e identificando áreas de melhoria. Com base nas experiências, as políticas, procedimentos e planos são atualizados.

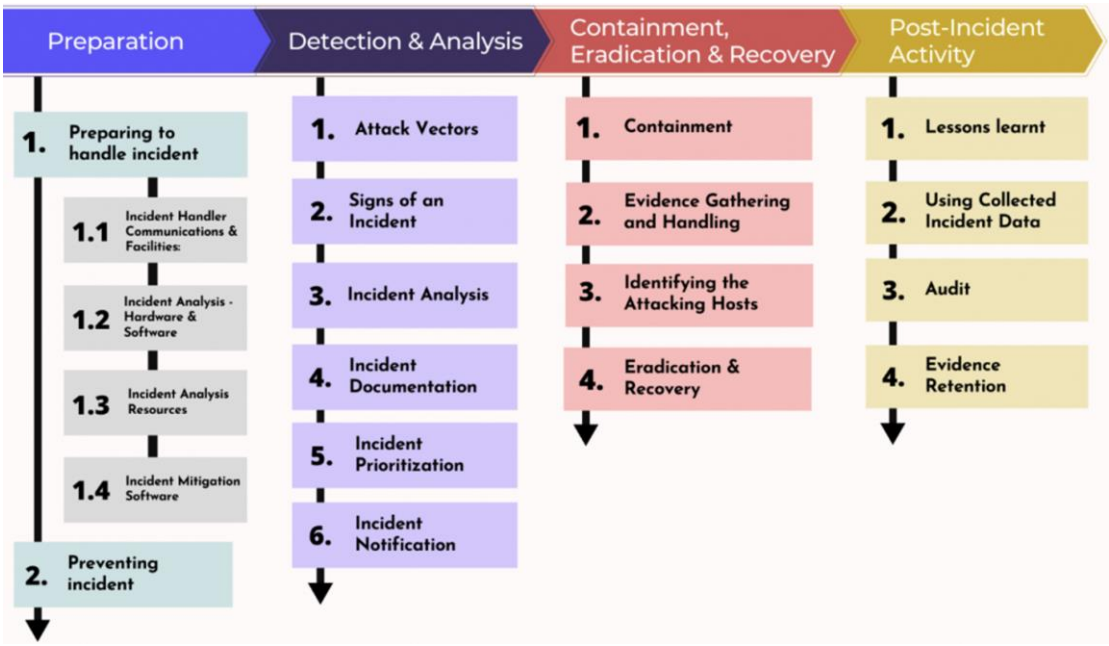


Figura 1 - NIST 800-61 Revision 2 - Computer Security Incident Handling Guide

A ISACA é uma organização profissional global que se dedica a melhorar a governança, gestão e uso de tecnologia da informação e sistemas de informação, e várias das suas publicações temos o seguinte texto:

"Não é possível proteger aquilo que não é conhecido"

Diante disso o ISH Vision assim que habilitado para o cliente, disponibiliza o benefício da automação da fase de Detecção e Análise segundo o NIST, esta que talvez seja a fase mais complexa e desafiadora da resposta a incidente, pois é nesta fase que se torna conhecido o incidente possibilitando assim a aplicação das corretas respostas de maneira rápida.

Após a detecção de maneira automática feita pelo ISH Vision, eventualmente o cliente pode demandar a execução dos demais fases da resposta, a qual a ISH atende através do seu amplo portfólio de serviços.

3. ARQUITETURA DO PRODUTO

A base de qualquer solução tecnológica é a sua arquitetura. No caso do ISH Vision, essa arquitetura não apenas sustenta o produto, mas também impulsiona a sua eficácia na detecção de ataques direcionados. Nesta seção, serão explorados os alicerces técnicos sobre os quais o ISH Vision se ergue. Desde a interconexão dos componentes até a sinergia entre algoritmos avançados, será examinado como a arquitetura foi meticulosamente projetada para fornecer uma visão abrangente e integrada da segurança cibernética.

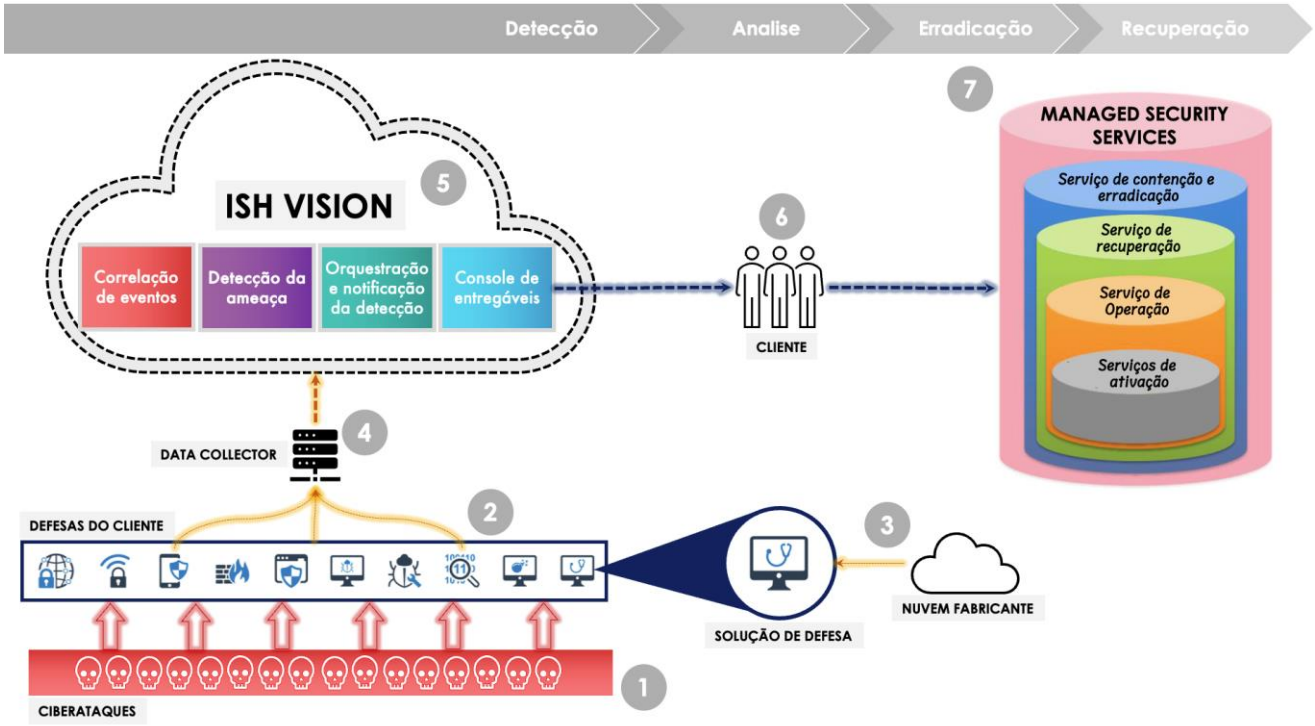


Figura 2 - Arquitetura do produto ISH Vision

a. ***Item 1 – Ciberataques:*** Todos os dias ataques cibernéticos são direcionados aos ambientes das empresas onde os atacantes (hackers) possuem diversas motivações: financeiro, espionagem, ativismos, extorsão, sabotagem, curiosidade, dano a reputação, dentro outras. Os atacantes utilizam técnicas, táticas e procedimentos (TTPs) na expectativa de encontrar sucesso no processo de invasão.

b. ***Item 2 – Defesas do cliente:*** Os ataques são direcionados a superfícies de ataques. A superfície de ataque cibernético inclui todas as áreas expostas e suscetíveis a serem exploradas, seja através de vulnerabilidades de software, configurações inadequadas, fraquezas de autenticação ou quaisquer outras falhas de segurança. Quanto maior a superfície de ataque, maior é o potencial de riscos e ameaças à

segurança. Uma das práticas essenciais na segurança cibernética é reduzir a superfície de ataque, minimizando o número de pontos vulneráveis e implementando medidas de segurança para proteger cada ponto de acesso. Uma das diversas medidas mais comuns é posicionar tecnologias e/ou soluções adequadas para cada parte da superfície, como por exemplo um antivírus para a camada de endpoint da superfície de ameaça.

c. ***Item 3 – Soluções de defesa*:** Tais soluções de terceiros em geral detectam ameaças diariamente baseado em assinaturas e inteligência de ataque, que recebem das diversas nuvens dos seus fabricantes, algumas inclusive já usam metodologia de aprendizado de máquina e/ou inteligência artificial para identificar novos ataques.

   Importante ressaltar que tais tecnologias não são um componente do ISH Vision, e sim uma tecnologia que é um ativo do próprio cliente, a qual está instalado sobre uma superfície de ameaça do seu parque.

d. ***Item 4 – Data Collector:*** Uma vez que tais soluções e tecnologias detectam uma ameaça, além das diversas ações que cada solução se propõe, todas sem exceção geram um evento sobre tal detecção de ameaça, e então apresenta-se o primeiro componente do ISH Vision, o Data Colllector, que tem um único objetivo de centralizar todos estes eventos de invasões em curso no ambiente e encaminhar para o core da plataforma do ISH Vision.

e. ***Item 5 – ISH Vision:*** Os eventos então chegam ao produto ISH Vision que são processados seguindo a ordem das funcionalidades e/ou módulos descritos abaixo:

   i. ***Correlação de eventos***
   Módulo que tem por objetivo receber todos os eventos, e correlacioná-los a fim de entender quais são parte do mesmo ou diferentes ataques.

   Os produtos posicionados sobre a superfície do cliente têm a capacidade de detectar de forma individual as tentativas de ataque, porém a capacidade de correlacionar todos os eventos e entender que as táticas, técnicas e processos presentes nos eventos fazem parte de um mesmo ataque é função do modulo de correlação de eventos do ISH Vision. Tal função é essencial durante um ataque, pois os atacantes desenvolvem técnicas de "cortina de fumaça" para aparentar está invadindo uma empresa por uma área da superfície onde na verdade está invadindo por outra.

Um engenheiro de defesa sem o módulo de correlação do ISH Vision além de gastar muito tempo em entender o que está acontecendo, pois teria que abrir as diversas consoles dos equipamentos de maneira individual, ainda assim seria facilmente manipulado pelo atacante durante o processo de invasão.

Importante ressaltar que a inteligência de detecção de ameaças baseado em assinaturas estão presentes nas tecnologias do ambiente do cliente, a qual não faz parte do produto ISH Vision.

Ainda cabe afirma que o módulo de correlação de eventos não depende de assinaturas próprias para funcionar, ou seja, desde o momento da sua ativação é entregue para o cliente todo o benefício da correlação permanecendo imutável durante todo o período da vigência da licença contratada, sendo esta correlação feita de maneira automática através dos diversos algoritmos do produto.

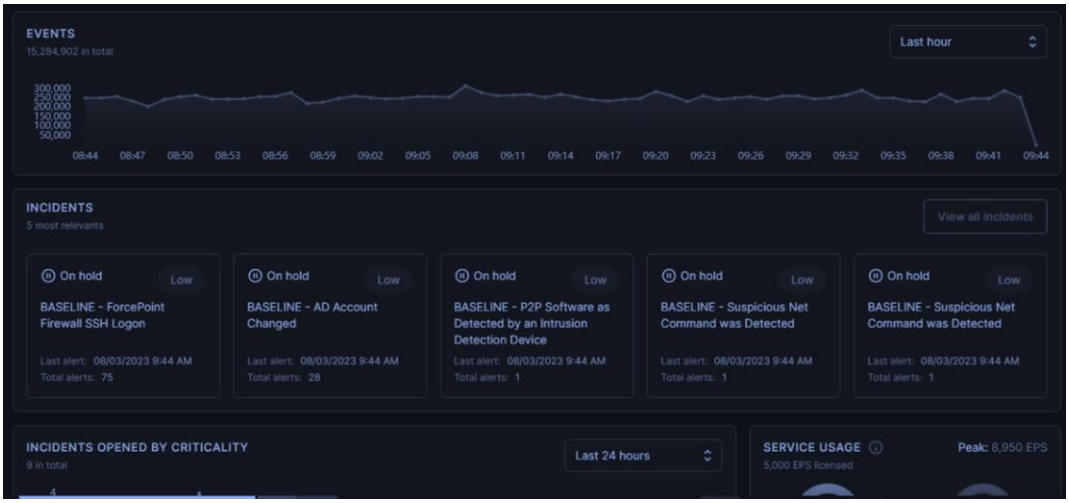


Figura 3 - Módulo de correlação de eventos do ISH Vision

ii. Detecção de ameaças

Após a correlação de eventos realizado pela função e/ou módulo anterior, chega-se em uma possível ameaça detectada, que é declarada como de fato um incidente após ser analisado pelo módulo de ameaça.

Tal módulo possui um algoritmo avançado de detecção de comportamento de atividade anômala, diferenciando as atividades de rede conhecidas das anômalas através de fórmulas de indicadores de comprometimento.

Indicadores de Comprometimento (IOCs, do inglês "Indicators of Compromise") são informações específicas que indicam que um sistema, rede ou ambiente pode ter sido comprometido por atividades maliciosas ou

cibernéticas. Essas informações são coletadas a partir de observações de padrões, comportamentos ou elementos que geralmente não ocorreriam em circunstâncias normais.

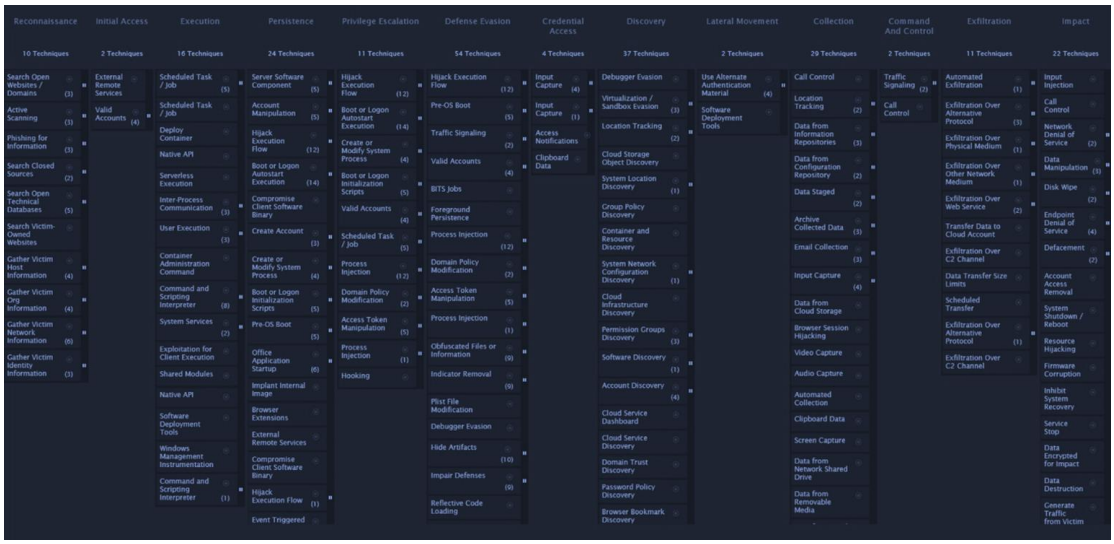
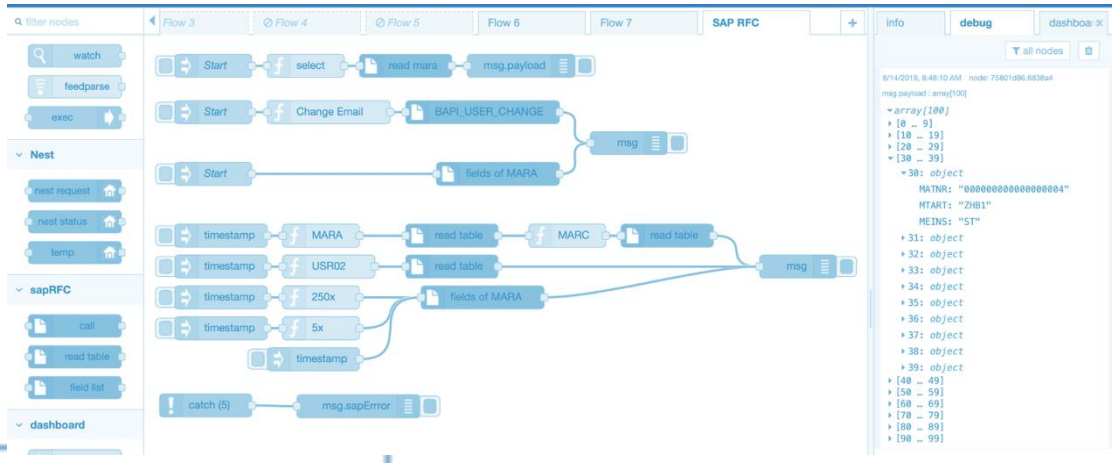


Figura 4 - Módulo de detecção de ameaça do ISH Vision

iii. Orquestração e notificação de ameaças

Após a declaração do incidente, o módulo de orquestração e notificação entra em ação, por sua vez este tem a função de orquestrar e automatizar o envio de notificação de ameaça ao cliente, e as recomendações do que precisa ser feito para mitigar tal incidente em curso.

No geral, tal módulo permite que as equipes de segurança aumentem sua eficiência, reduzam o tempo de resposta a ameaças e coordenem melhor as ações. Ele integra ferramentas de segurança, proporcionando uma abordagem mais eficaz para lidar com incidentes cibernéticos.



iv. Console de entregáveis

Todo os módulos da ferramenta estão posicionados no back-end da ferramenta, ou seja, o cliente não visualiza tais interfaces, porém para acompanhamento dos entregáveis prometidos pela solução o cliente possui uma interface conhecida como modulo de entregáveis denominada ISH Vision Portal, onde são apresentados todos os indicadores chaves das entregas realizadas pela plataforma.

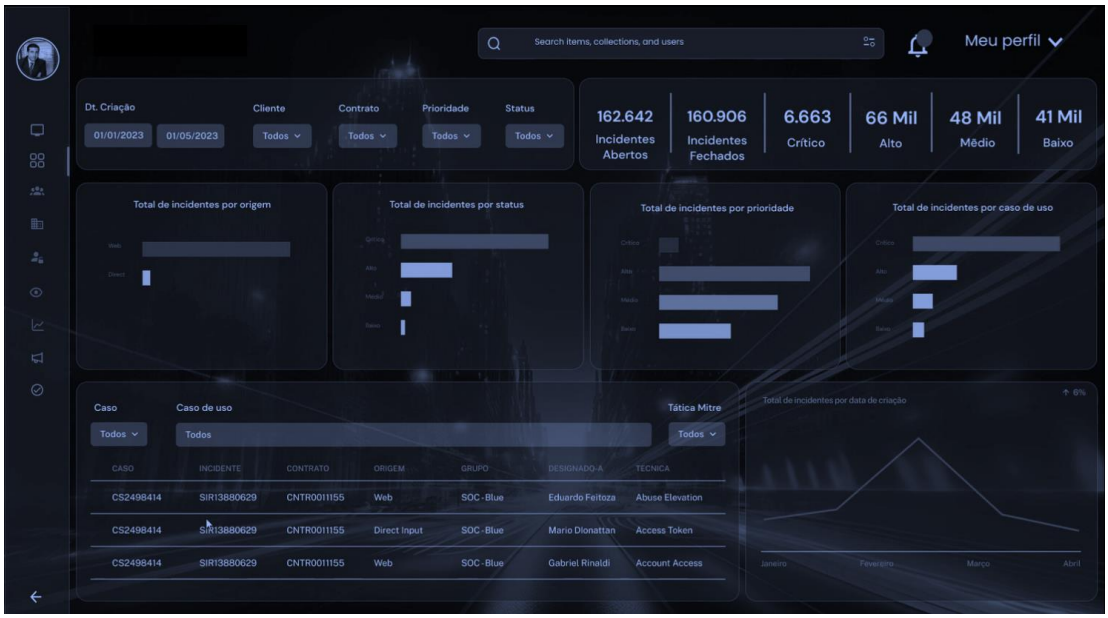


Figura 5 - ISH Vision Portal

f. **Item 6 – Cliente:** Além de possuir uma console para acompanhamento de maneira estratégica os entregáveis e indicadores da solução, o cliente ainda a cada detecção de ameaça recebe por e-mail uma notificação, trazendo informamos detalhadas sobre a ameaça e o que fazer para mitigar tal tentativa de invasão em curso.

Prezados,

Detectamos a seguinte violação de segurança no ambiente. Segue maiores informações abaixo:

PRIORIDADE	STATUS	GRAVIDADE	DESCRIÇÃO	ID
Medium	New	30	[redacted] - BASELINE - Command Execution Through PowerShell Process	INC-268931

INICIAR	DURAÇÃO	ORIGENS	CRIADO POR	CONTAGEM DE EVENTOS
2023-08-08T12:44:39.098Z	2023-08-08T12:44:39.098Z	Event Stream Analysis	[redacted] All Alerts	3

%NICWIN-4-Security_4688_Microsoft-Windows-Security-Auditing: Security,rn=3796824778 cid=7652 eid=4,Tue Aug 08 01:26:04 2023,4688,Microsoft-Windows-Security-Auditing,,Audit Success,BRDC01-001.careplus.intranet,Process Creation,,A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: BRDC01-001$ Account Domain: CAREPLUS Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Process Information: New Process ID: 0x1a24 New Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Token Elevation Type: %%1936 Mandatory Label: S-1-16-16384 Creator Process ID: 0x864 Creator Process Name: C:\Windows\System32\cmd.exe Process Command Line: C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe echo nessus_cmd_Z2V0LWhlbHAgSW52b2t1LV3Ic3RNZXRob2Q=_start ; get-help Invoke-RestMethod ; echo nessus_cmd_Z2V0LWhlbHAgSW52b2t1LV3Ic3RNZXRob2Q=_stop ; echo nessus_cmd_SW52b2t1LV3Ic3RNZXRob2QgLUI1dGhvZCBHRVQgLUh1YWRlcnMgQHt9IGh0dHA6Ly8xNjkuMjU0LjE2OS4yNTQvb3BjL3Yxl2luc3RhbmNlIDI+JjE=_start ; Invoke-RestMethod -Method GET -Headers @{} http://169.254.169.254/opc/v1/instance ; echo nessus_cmd_SW52b2t1LV3Ic3RNZXRob2QgLUI1dGhvZCBHRVQgLUh1YWRlcnMgQHt9IGh0dHA6Ly8xNjkuMjU0LjE2OS4yNTQvb3BjL3Yxl2luc3RhbmNlIDI+JjE=_stop ; Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

 %NICWIN-4-Security_4688_Microsoft-Windows-Security-Auditing: Security,rn=3796830581 cid=8612 eid=4,Tue Aug 08 01:26:16 2023,4688,Microsoft-Windows-Security-Auditing,,Audit Success,BRDC01-001.careplus.intranet,Process Creation,,A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: BRDC01-001$ Account Domain: CAREPLUS Logon ID: 0x3E7 Target Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Process Information: New Process ID: 0x1f20 New Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Token Elevation Type: %%1936 Mandatory Label: S-1-16-16384 Creator Process ID: 0x2320 Creator Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Process Command Line: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Figura 6 - Notificação de ameaça para o cliente

g. **Item 7 - Managed Security Services:** Após analisar o incidente detectado em seu ambiente o cliente eventualmente pode não ter capacidade, disponibilidade e conhecimento de aplicar as ações que mitigariam tal ameaça, desta forma ele pode contratar os diversos serviços conhecidos como MSS (Managed Security Services) para mitigar, erradicar e/ou responder a um ataque.

   Também no grupo de MSS a ISH possui os serviços de ativação, também conhecidos no mercado como Professional Services, que tem por objetivo realizar a ativação de tal produto (ISH Vision) no ambiente do cliente.

   Vale ressaltar que os serviços de MSS não fazem parte do modelo de licenciamento do ISH Vision, eles de fato são serviços que são contratados a parte, de acordo com expectativas e necessidades do cliente.

4. Modelo de licenciamento

O ISH Vision possui modelo de licenciamento de subscrição, ou seja, para continuarem a ter acesso a plataforma os clientes precisam cumprir com os acordos de pagamento, e o correto uso do produto, bem como demais regras estabelecidas nos termos de uso e condições da plataforma, e/ou nas propostas técnicas e contratos estabelecidos com os determinados clientes.

Uma nova versão do produto é lançada sempre que houver mudanças significativa em suas funções core, e para ter acesso a este novo produto o cliente deve fazer um aditivo contratual adquirindo uma nova licença por um período determinado.

A vigência do licenciamento se dá a partir do momento que é disponibilizado o acesso do cliente a plataforma, que acontece imediatamente após os aceites dos termos de uso e condições da plataforma, e/ou nas propostas técnicas e contratos estabelecidos com os determinados clientes.

5. Considerações finais

A resposta a incidente se dá em quatro grandes fases, e o ISH Vision está posicionado como ferramenta de automação do grupo de detecção.

Após o ISH Vision ser habilitado para o cliente o mesmo receber de forma imediata todos os benefícios das soluções, e tais benefícios e funcionalidades permanecem disponíveis para o cliente durante todo o período de licença contratada, não havem a necessidade de atividade humana alguma ou qualquer tipo de atualização para o correto funcionamento da solução.

Os serviços que eventualmente o cliente tenha a necessidade de contratar, não fazem parte da solução ISH Vision, sendo estes contratados a parte denominado no catálogo de serviço da ISH e comumente conhecidos no mercado como Managed Security Services.