

{{Name}}

30 de junho de 2021

**ÍNDICE**

[1. OBJETIVO RESPOSTA INCIDENTE DE SEGURANÇA 4](#_Toc72411861)

[2. FRAMEWORK DA GESTÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO 4](#_Toc72411862)

[2.1 Preparação 5](#_Toc72411863)

[2.2 Detecção e Triagem & Priorização 5](#_Toc72411864)

[2.3 Análise 6](#_Toc72411865)

[2.4 OBJETIVO 6](#_Toc72411866)

[2.5 DETECÇÃO 7](#_Toc72411867)

[2.6 CONTENÇÃO 7](#_Toc72411868)

[2.7 ERRADICAÇÃO 7](#_Toc72411869)

[2.8 RECUPERAÇÃO 7](#_Toc72411870)

[2.9 PRÉ-REQUISITO 7](#_Toc72411871)

[2.10 REFERENCIAS 7](#_Toc72411872)

[2.11 Pós incidente 8](#_Toc72411873)

[2.12 Ciclo completo. 9](#_Toc72411874)

[3. Matrizes de gestão de incidente 10](#_Toc72411875)

[4. Matriz RACI 11](#_Toc72411876)

[5. ACIONAMENTO 12](#_Toc72411877)

[6. Notificação da resposta a incidente. 13](#_Toc72411878)

[6.1 Notificação por Telegram 14](#_Toc72411879)

[6.2 Notificação por E-mail 14](#_Toc72411880)

[7. Definição de Playbook 15](#_Toc72411881)

[8. Topologia do SOAR 16](#_Toc72411882)

**índice de figuras**

[Figura 1 – Framework Incidente Response 5](#_Toc61257461)

[Figura 2 – Fluxo de Preparação 6](#_Toc61257462)  
[Figura 3 – Fluxo de detecção e Triagem & Priorização de Preparação 7](#_Toc61257462)

[Figura 4 – Fluxo de Análise 7](#_Toc61257463)

[Figura 5 – Fluxo de Contenção, Erradicação e Recuperação 9](#_Toc61257464)

[Figura 6 – Fluxo Pós Incidente 9](#_Toc61257465)

[Figura 7 – Ciclo completo da gestão de incidente](#_Toc61257466) 10

[Figura 8 – Modelo de Abertura de Ticket na Central de Relacionamento 14](#_Toc61257467)

[Figura 9 – Notificação de Incidente por Telegram 15](#_Toc61257468)

[Figura 10 – Notificação de Incidente por E-MAIL 16](#_Toc61257469)

[Figura 11 – Exemplo de um Playbook. 16](#_Toc61257470)

[Figura 12 – Topologia da Automação. 17](#_Toc61257471)

**ÍNDICE DE TABELAS**

[Tabela 1 – Modelo de preparação de equipamento 6](file:///C:\Users\IMG1\Downloads\model.docx#_Toc61257472)

[Tabela 2 – Matriz de Gestão de Incidente 11](file:///C:\Users\IMG1\Downloads\model.docx#_Toc61257473)

[Tabela 3 – Matriz RACI 13](file:///C:\Users\IMG1\Downloads\model.docx#_Toc61257474)

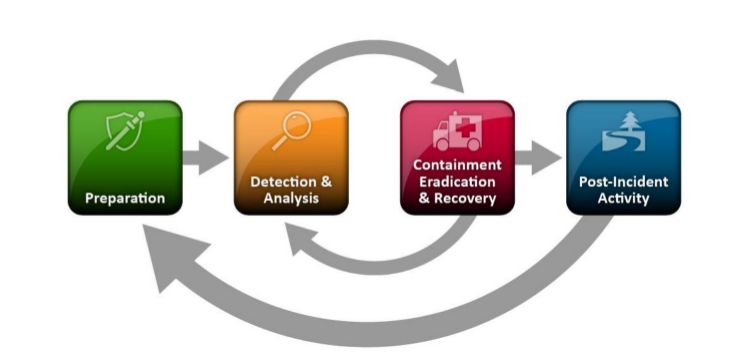
[Tabela 4 – Contato da Central de Atendimento 13](file:///C:\Users\IMG1\Downloads\model.docx#_Toc61257475)

1. OBJETIVO RESPOSTA INCIDENTE DE SEGURANÇA

Detalhar o processo de preparação, detecção, contenção, erradicação e recuperação dos incidentes de segurança da informação para responder com êxito a tipos de ameaças de incidentes específicos. Baseado nas boas práticas e utilizando como referência o framework do NIST.SP.800-61r2 e SANS Institute.

1. FRAMEWORK DA GESTÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Este documento abrange a inserção do framework da gestão de incidente de segurança da informação.



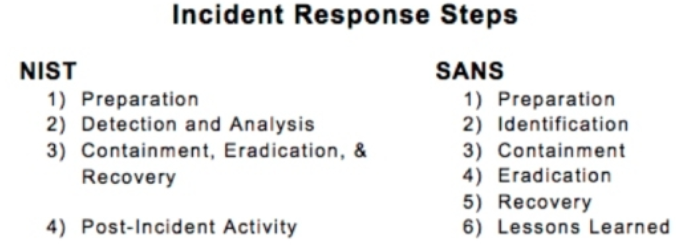


Figura 1 – Framework Incidente Response

# Preparação

O primeiro passo a ser dado no plano de respostas a incidentes é a preparação. Inicialmente deve-se definir parâmetros concretos de utilização de informações, estabelecendo quais níveis hierárquicos podem ter acesso a quais tipos de informação.

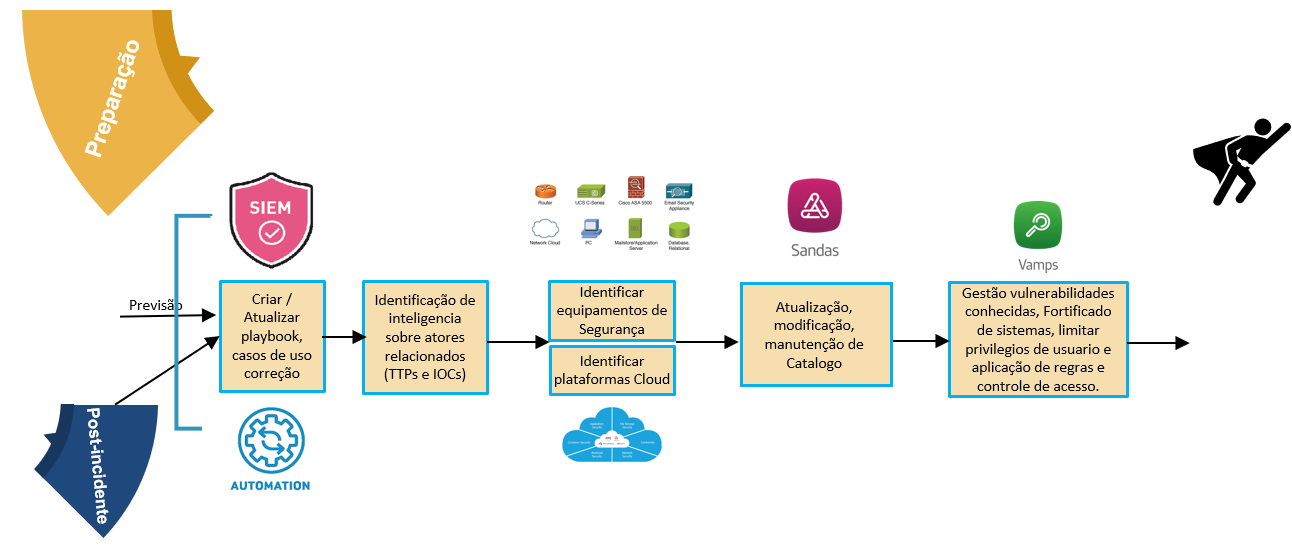


Figura 2 – Fluxo de Preparação

Para iniciarmos a preparação da resposta de incidente, precisamos de um levantamento dos devices do ambiente e topologia. Com isso, conseguimos realizar um trabalho consultivo de resposta a incidente. Ex.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | IP Equipamento | Sistema Operacional | Serviço do device | Localização do Equipamento | Criticidade |
| SV | IP Interno | Windows | Act Directory | DMZ/Rede interna | Alto |

Tabela 1 – Modelo de preparação de equipamento

# Detecção e Triagem & Priorização

Em primeiro lugar, a própria fase de detecção conterá um conjunto de subprocessos com etapas estruturadas para monitorar a rede, o SIEM, os indicadores de captura etc. Cada subprocesso seria um manual, executado manualmente ou automatizado. Nesta fase é demonstrada como realizar tratativa do alerta/incidente gerado e definição passo a passo para finalização ou encaminhamento do mesmo para equipe, que possa tratar o caso de forma precisa.

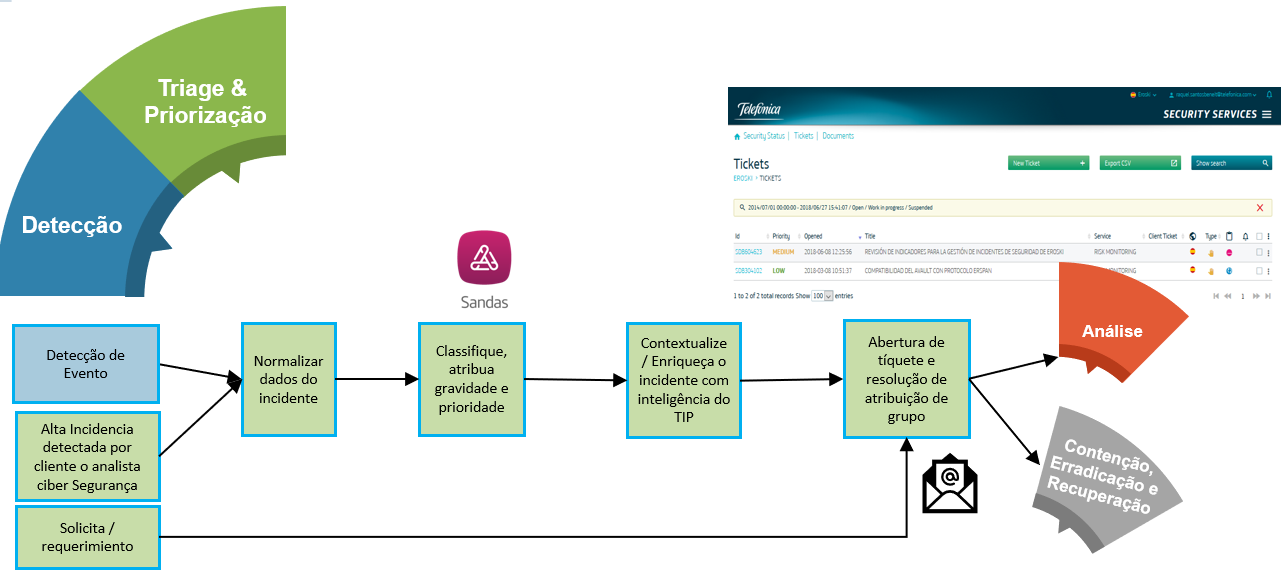


Figura 3 – Fluxo de detecção e Triagem & Priorização

# Análise

Análise é identificar o incidente é o primeiro passo a se tomar como resposta a uma possível emergência. Após a identificação, segue-se os protocolos de execução de acordo com o treinamento e os protocolos pré-definidos.

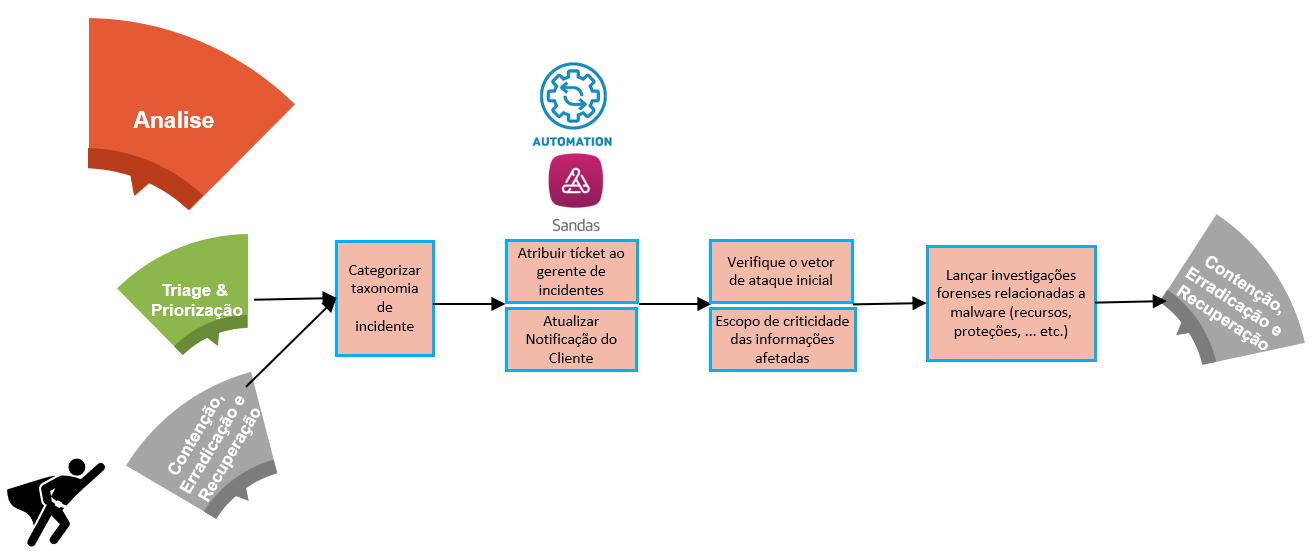


Figura 4 – Fluxo de Análise

# 2.4 OBJETIVO

{{Objetivo}}

# DETECÇÃO

{{Detecção}}

# CONTENÇÃO

{{Contenção}}

# ERRADICAÇÃO

{{Erradicação}}

# RECUPERAÇÃO

{{Recuperação}}

# PRÉ-REQUISITO

{{Pré-Requisito}}

# REFERÊNCIAS

{{Referências}}

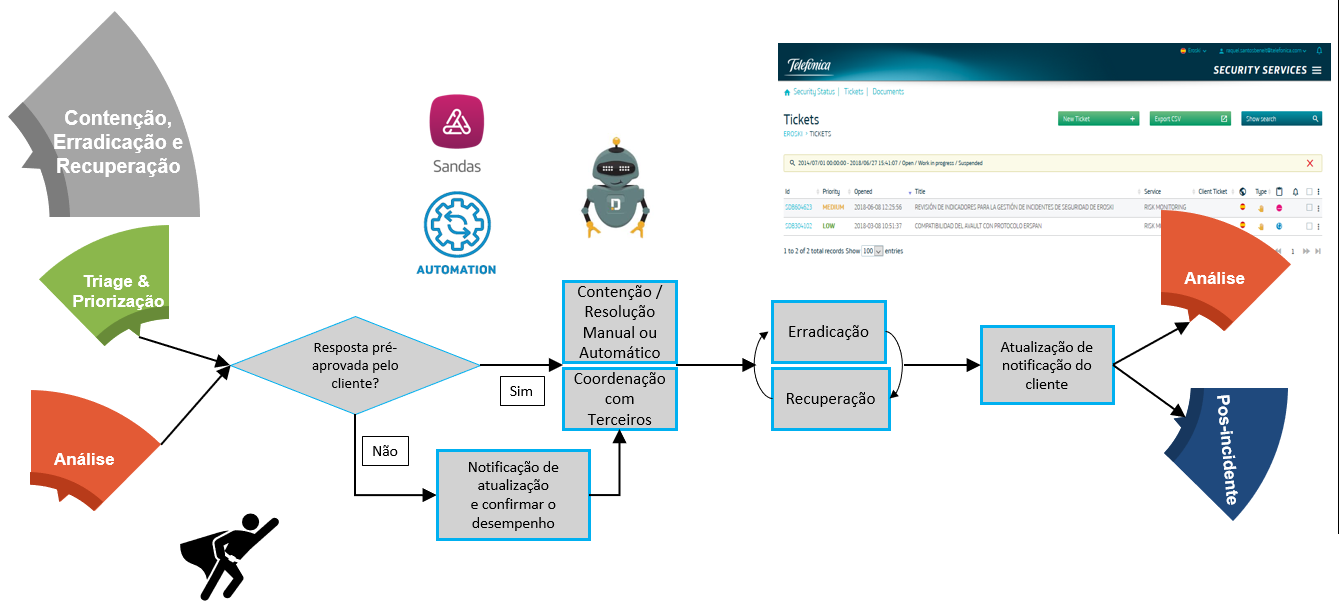


Figura 5 – Fluxo de Contenção, Erradicação e Recuperação

# Pós incidente

No Pós Incidente é o momento de lições aprendidas, onde é possível revisar o incidente, analisar os GAPs na infraestrutura de segurança e propor as ações corretivas necessárias para evitar que o incidente ocorra novamente.



Figura 6 – Fluxo Pós Incidente

# Ciclo completo.

Estabelecer de forma clara e precisa as metodologias e processos de trabalho entre as diferentes áreas da organização, bem como os meios de comunicação com outras instituições em relação a incidentes.

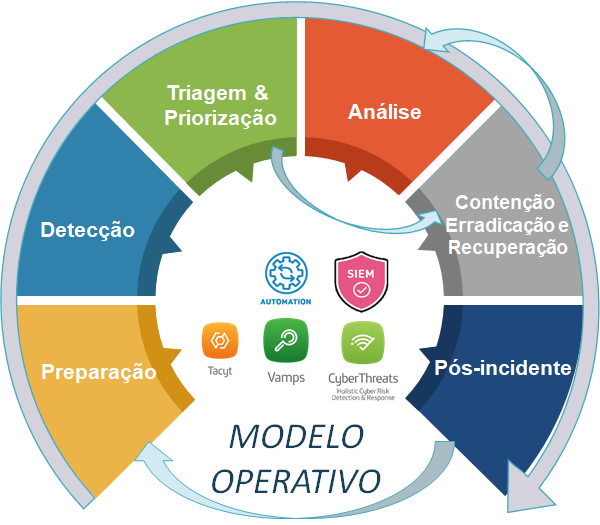


Figura 7 – Ciclo completo da gestão de incidente

1. Matrizes de gestão de incidente

A Gestão de Incidentes é um processo ITIL que tem como principal objetivo restaurar a operação normal do serviço o mais rápido possível, minimizando os prejuízos à operação do negócio e garantindo assim o melhor nível de serviço e disponibilidade.

|  |  |  |  |
| --- | --- | --- | --- |
| Descrição | Notificação de incidente | Resposta incidente 8/5 | Resposta incidente 24/7 |
| Preparação |  |  |  |
| Detecção |  |  |  |
| Triagem & Priorização |  |  |  |
| Contenção |  |  |  |
| Erradicação |  |  |  |
| Recuperação |  |  |  |
| Pós incidente |  |  |  |
| Notificação 24/7 |  |  |  |
| Gestão dos Equipamentos |  |  |  |
| Relatório do incidente |  |  |  |
| Playbook |  |  |  |

Tabela 2 – Matriz de Gestão de Incidente

1. Matriz RACI

|  |  |  |
| --- | --- | --- |
| **ATIVIDADES** | **RESPONSABILIDADES** | |
| **Preparação** | **VIVO** | **CLIENTE** |
| Disponibilizar Política de Segurança | **I** | **R** |
| Disponibilizar lista de equipamentos que terão logs encaminhados para o SIEM | **I** | **R** |
| Preparar SIEM para recebimento dos logs | **R** | **I** |
| Disponibilizar Matriz de Acionamento | **R** | **I** |
| Disponibilizar recursos para detecção e resposta | **R** | **I** |
|  |  |  |
| **Detecção** |  |  |
| Criar lista de Casos de Uso | **R** | **C |A** |
| Definir Prioridade/Criticidade | **I** | **R** |
| Criar Runbooks para o operalização “SOC” | **R** | **C | I** |
| Validar o correto funcionamento dos casos de uso | **R** | **I** |
| Criar Dashboards | **\*** | **A |** **C |** **I** |
| Criar Relatórios | **\*** | **A** **| C** **| I** |
|  |  |  |
| **Contenção** |  |  |
| Identificar os Incidentes de Segurança | **R | I** | **R | I** |
| Mitigar o Incidente de Segurança | **R** | **I** |
| Tomar medidas de segurança necessárias (Exemplo: bloqueio de IP no Firewall) | **\*** | **R |C | I** |
| Coletar evidências | **\*** | **I** |
|  |  |  |
| **Erradicação** |  |  |
| Identificar causa raiz do Incidente de Segurança | **R | I** | **R | I** |
| Identificar e remediar todos os ativos comprometidos | **R | I** | **R | I** |
| Identificar e eliminar a causa raiz do Incidente de Segurança | **R | I** | **R | I** |
| Ferramentas para erradicação “Exemplo: Antivírus, IPS, e etc.” | **I** | **R** |
|  |  |  |
| **Recuperação** |  |  |
| Restaurar os sistemas, ativos afetados Exemplo: Backup) | **I** | **R** |
| Corrigir vulnerabilidades para evitar novos incidentes | **I** | **R** |
| Validar se os sistemas, ativos estão limpos e livres da causa raiz | **C | I** | **R** |
|  |  |  |
| **Lições Aprendidas** |  |  |
| Criar Plano de Resposta a Incidentes | **R** | **C | I** |
| Atualizar plano de Resposta a Incidentes | **R** | **C | I** |

|  |  |
| --- | --- |
| **R** | **Responsável** |
| **A** | **Aprovador** |
| **C** | **Consultado** |
| **I** | **Informado** |

\* verificar itens do contrato. Neste caso podemos ser responsáveis ou apenas consultado.

Tabela 3 – Matriz RACI

1. ACIONAMENTO

As solicitações de atendimento deverão ser registradas exclusivamente na Central de Relacionamento Digital (Service Desk), com cópia para o Security Operations Center (SOC) onde o atendimento é realizado 24x7.



Tabela 4 – Contato da Central de Atendimento

Assunto do e-mail: <CLIENTE> - Vivo Managed Security Services

[breve descrição]

No corpo do e-mail, descrever o Incidente/Solicitação/Consulta conforme o modelo abaixo:

Nome da pessoa para contato\*:

Telefone(s)\*:

Produto: VIVO MANAGED SECURITY SERVICES

Tipo da Solicitação: ( ) Incidente | ( ) Solicitação | ( ) Consulta

Descrição detalhada para o chamado\*:

Evidências (Print):



Figura 8 – Modelo de Abertura de Ticket na Central de Relacionamento

1. Notificação da resposta a incidente.

Notificação do Incidente é respeitável quando se realiza com clareza e rapidez. Para que as áreas responsáveis consigam atuar com assertividade na remediação do incidente.

Atualmente as formas de notificação e realizada pelo envio de mensagem via Telegram, envio de e-mail e por ligação telefônica.

* 1. Notificação por Telegram

Para a notificação via Telegram é criado um grupo no Telegram com os exceptivos usuários, após isso é criado o BOT na ferramenta de SOAR da Eleven Paths e assim que tiver o incidente a mensagem com o incidente e enviado no grupo correspondente na plataforma do Telegram

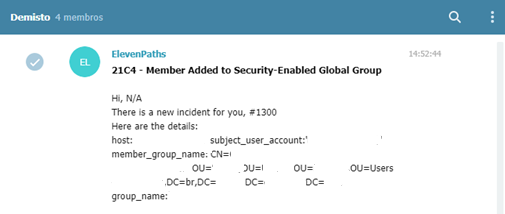


Figura 9 – Notificação de Incidente por Telegran

* 1. Notificação por E-mail

O envio do e-mail é a forma mais antiga para envio de notificação. Nesta notificação utilizamos o protocolo SMTP de forma criptografa “TLS” com as credenciais para envio dos e-mails as equipes responsáveis.

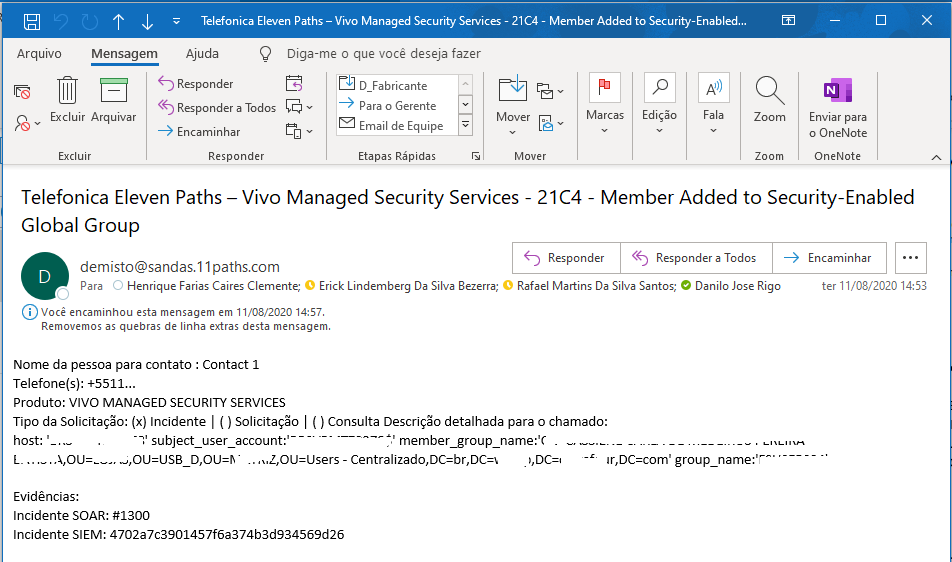


Figura 10 – Notificação de Incidente por E-MAIL

1. Definição de Playbook

Um Playbook é definido como um conjunto de regras, descrevendo pelo menos uma ação a ser executada com dados de entrada e disparada por um ou mais eventos. É um componente crítico da cibersegurança, especialmente em relação à orquestração, automação e resposta de segurança.

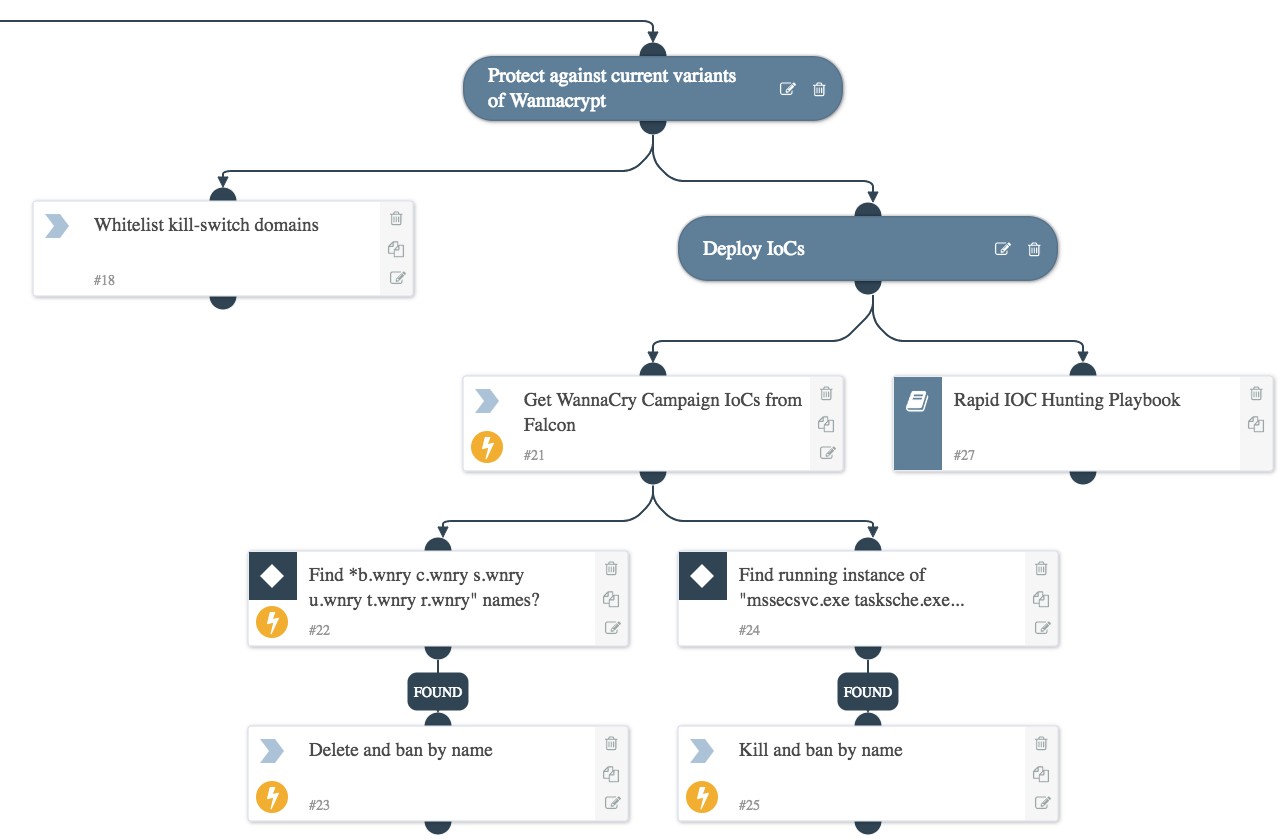


Figura 11 – Exemplo de um Playbook.

1. Topologia do SOAR

A topologia de rede é o canal no qual o meio de rede está conectado aos computadores e outros componentes de uma rede de computadores ou cloud. Há várias formas nas quais se podem organizar a interligação entre redes e cloud.

Uma imagem contendo texto

Descrição gerada automaticamente

Figura 12 – Topologia da Automação.

|  |
| --- |
|  |
|  |

