TLP : CLEAR

DFIR-IRIS

Plataforma de Resposta a Incidentes

Jorge Loureiro [1]

[1] jorge.loureiro@ipb.pt

Agenda

TLP : CLEAR

TheHive
- Componentes
- Templates & Taxonomia
- Frameworks de resposta a incidentes
- Processo de Resposta a Incidentes

DFIR-IRIS
- Componentes
- Processo de Migração
- Trabalho Futuro

TheHive

TheHive4

TLP : CLEAR

TheHive4 é uma solução intuitiva e customizável que automatiza um conjunto de procedimentos na resposta a incidentes.

TheHive

Componentes

Componentes

TLP : CLEAR

Cortex:

- **Analyzers** e **Responders**.

MISP Threat Sharing (MISP):

- Malware Information Sharing Platform.

ThePhish:

- Uma ferramenta automatizada de análise de e-mails de phishing, baseada no **TheHive**, **Cortex** e **MISP**.

Imap2TheHive

- Um conector leve e de código aberto que permite a ingestão automática de alertas de e-mail na plataforma **TheHive**.

- **TheHive2LaTeX**
  - Script para criação de relatórios em *LaTeX*.
- **Backups**

TLP : CLEAR

TheHive

Templates & Taxonomia

Templates & Taxonomia

TLP : CLEAR

- A plataforma recorre ao uso de *Templates* para definir as várias fases de resposta a um incidente.
- Definição da *Taxonomia* para a classificação dos diversos tipos de incidentes.

TLP : CLEAR

TheHive

Frameworks de resposta a incidentes

NIST & SANS

TLP : CLEAR

Figure: National Institute of Standards and Technology

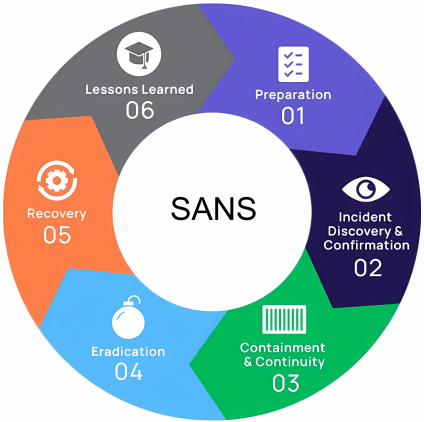


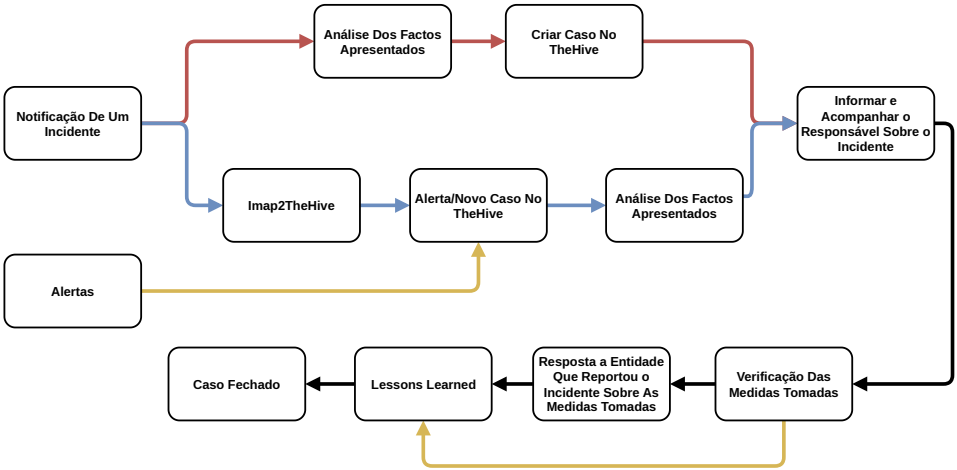
Figure: SysAdmin, Audit, Network, and Security

TheHive

Processo de Resposta a Incidentes

Processo de Resposta a Incidentes

TLP : CLEAR



TheHive

TheHive5

TheHive5

TLP : CLEAR

Com o lançamento da nova versão, a solução migrou para um modelo pago e encerrou o suporte ao **TheHive4**.

DFIR-IRIS

DFIR-IRIS

TLP : CLEAR

- **DFIR-IRIS** é uma solução de código aberto, similar ao **TheHive**, flexível e com uma comunidade ativa que busca melhorar a plataforma e automatizar os procedimentos de resposta a incidentes.

DFIR-IRIS

Componentes

Componentes

TLP : CLEAR

- **Módulos**
  - **MISP**
  - **IntelOwl**: é uma solução de *OSINT* de código aberto para obter dados de ameaças sobre um artefato.
  - **VirusTotal**: é um serviço online que analisa arquivos e URLs suspeitos para detectar conteúdo malicioso, utilizando antivírus e scanners de websites.
- **Customers**
- **Timeline**
- **Graph**: ajuda os investigadores a compreender a correlação entre vários elementos de um caso, como IOCs, ativos, eventos e/ou utilizadores.
- **Relatórios**: criação de relatórios com informação dos casos, recorrendo a um template customizavel.
- **Backups**: suporte nativo para a criação de backups.
- **Templates** e **Taxonomia**

TLP : CLEAR

DFIR-IRIS

Processo de Migração

Processo de Migração

TLP : CLEAR

- Adaptação dos Templates para o **DFIR-IRIS**;
- Definição da Taxonomia;
- Criação dos vários Customers;
- Uso das APIs;
- Criação de scrips em *Python*;
- Uso de boas práticas:
  - Armazenamento de artefactos relacionados com os casos fora da plataforma, estando esses encriptados;
  - Referência no caso de onde se localiza esse artefacto;
  - Uso de *Tags* para identificar as entidades relacionadas com o caso e classificação do tipo de incidente;
  - Backup atualizado, no caso de ser necessário reverter ou aceder a plataforma antiga.

DFIR-IRIS

Trabalho Futuro

Trabalho Futuro

TLP : CLEAR

- Módulo para interligar a plataforma com a solução **Cortex**, para execução dos Analyzers e Responders;
- Criação de uma solução com funcionalidades similares ao **ThePhish**;
- Automatização da criação de alertas, como **Imap2TheHive**;
- Módulo para geração de relatórios em *LaTeX*.

Demo

TLP : CLEAR

DFIR-IRIS disponibiliza um demo acessível através do seguinte link.

- `https://v200.beta.dfir-iris.org/welcome`


ipb
INSTITUTO POLITÉCNICO
DE BRAGANÇA
CSIRT