Proyecto de Inteligencia de Amenazas con OpenCTI

Fecha: 21/07/2025

Introducción

La ciberseguridad moderna exige un enfoque proactivo frente a las amenazas digitales. En este contexto, las plataformas de Threat Intelligence (CTI) como **OpenCTI** permiten gestionar, analizar y compartir conocimiento sobre indicadores de compromiso (IoCs), actores de amenazas, malware y técnicas de ataque.

Este proyecto tiene como objetivo la implementación y uso práctico de **OpenCTI** como una solución de inteligencia de amenazas. Se busca documentar incidentes reales de phishing, smishing y malware mediante la creación de bundles STIX 2.1, automatizar su generación, y visualizar las relaciones entre actores, técnicas y objetos maliciosos.

A través de esta iniciativa, se desarrolla una experiencia práctica y aplicada en **CTI (Cyber Threat Intelligence)**, fortaleciendo competencias clave en análisis de amenazas, uso de estándares abiertos como STIX, y operación de plataformas de inteligencia como OpenCTI.

Objetivo general

Diseñar, implementar y documentar un sistema de gestión de inteligencia de amenazas mediante la plataforma **OpenCTI**, que permita cargar y visualizar incidentes reales usando indicadores de compromiso en formato STIX 2.1, automatizando su creación y mejorando la visibilidad de las amenazas.

Objetivos específicos

Este manual tiene como objetivos principales:

Instalar y configurar OpenCTI en un entorno local utilizando Docker Compose, garantizando su funcionamiento estable.

Documentar incidentes de ciberseguridad reales, recopilando IoCs como hashes, URLs, remitentes maliciosos y archivos ejecutables.

Generar bundles STIX 2.1 con los IoCs mediante scripts en Python, estandarizando la información y facilitando su importación a OpenCTI.

Visualizar y relacionar los datos cargados, utilizando las capacidades gráficas de OpenCTI para mostrar conexiones entre amenazas, actores y técnicas MITRE ATT&CK.

Desarrollar habilidades prácticas en Threat Intelligence, automatización de procesos y análisis de amenazas.

1. Requisitos previos

Sistema operativo recomendado:

- Ubuntu Server 20.04 o superior
- También funciona en Debian y derivados

Requisitos de sistema:

- CPU: 4 núcleos mínimo
- RAM: 8 GB mínimo (ideal: 16 GB)
- Almacenamiento: 50 GB o más
- Docker y Docker Compose instalados

Dependencias:

- Docker
- Docker Compose
- Git

1. Instalación de OpenCTI (con Docker Compose)

Paso 1: Clonar el repositorio oficial de OpenCTI

- git clone https://github.com/OpenCTI-Platform/docker.git opencti
- cd opencti

Paso 2: Crear archivo .env

- cp .env.sample .env

Paso 3: Iniciar todos los contenedores

- docker-compose -f docker-compose.yml up -d

La primera vez puede tardar varios minutos. Puedes monitorear con:

- docker-compose logs -f

Paso 4: Acceder a la interfaz web

- http://localhost:8080

3. Registro inicial de datos

Crear usuario administrador

1. Ingresa al panel web
2. Registra un nombre, correo, contraseña
3. Inicia sesión como **admin**

Carga inicial de datos

1. Desde el dashboard, puedes:
   - Crear **Organizaciones**
   - Cargar archivos STIX manualmente
   - Ingresar **Indicadores de compromiso (IoCs)**
   - Crear **Malware**, **Actors**, **Tools**, etc.
2. Alternativamente, puedes importar un bundle STIX desde tu equipo:
   - Menú lateral: Import files
   - Arrastra el .json o súbelo manualmente

4. Objetivos del Proyecto con OpenCTI

Objetivo	Descripción
Centralizar incidentes	Documentar y analizar incidentes de seguridad en una única plataforma.
Gestionar IoCs	Cargar, categorizar y relacionar indicadores como hashes, IPs, dominios, rutas y archivos.
Enriquecer conocimiento	Relacionar malware, amenazas y TTPs usando MITRE ATT&CK.
Automatización	Generar bundles STIX automáticamente con scripts en Python.
Visualizar relaciones	Usar los gráficos de OpenCTI para mostrar vínculos entre actores, malware e IoCs.
Fomentar CTI	Desarrollar capacidades de Threat Intelligence en un entorno controlado.

5. Recursos adicionales

- Documentación oficial
- Repositorio de GitHub
- MITRE ATT&CK Navigator
- STIX 2.1 Spec

5. Scripts

El script **automatiza la creación de un archivo STIX 2.1** en formato .json a partir de un archivo Excel que contiene una lista de direcciones IP maliciosas y nombres de agentes. Este JSON está estructurado para ser **importado directamente en OpenCTI**.

mas en
🌐 OpenCTI-Academico/Scripts at ab0e84be17af556d1fb1a760d41a47e7e5432742 · johannsoto/Ope...

Elaborado por: Johann Alexander Soto Hernandez