Sri Lanka Institute of Information Technology

Information Security Project

Assignment 01 – Project Proposal Submission

IE3092 – Secure Software System

Open-Source SoC Platform

Submitted by:

Student Registration Number	Student Name
IT20077624	P.A Daham Thameera
IT20021870	Dilshan K. N

Date of submission
20th August 2022

Table of Contents

Introduction

Many security analysts are concerned about the quantity of occurrences they must manage and how they can do so in an effective and timely manner. To address that main issue, an Incident Management system was built. This system is a platform that allows security incidents to be created and tracked in an efficient and streamlined manner. This tool is built for companies of all sizes in Cybersecurity industries who are looking to improve productivity and process management.

Multiple SOC and CERT analysts can work on investigations at the same time. All team members have real-time access to information about new or existing cases, tasks, observables, and IOCs thanks to the built-in live stream. Special notifications enable them to manage or assign new tasks, as well as examine new MISP events and alerts from a variety of sources, including email reports, CTI providers, and SIEMs. They may then immediately import and study them.

A simple yet robust template engine may be used to construct cases and related tasks. You may use dynamic dashboards to automate laborious operations and add metrics and custom data to your templates to drive your team's activity, identify the types of investigations that take a long time, and drive your team's activity. Analysts may keep track of their work, attach evidence or important files, add tags, and import password-protected ZIP packages containing malware or questionable data without having to open them.

Add one, hundreds, or thousands of observables to each case you build, or directly import them from a MISP event or any alert provided to the platform. Triage and filter them as soon as possible. Use Cortex and its analyzers and responders to get valuable knowledge, accelerate your investigation, and limit risks. To feed your threat intelligence, use tags, mark IOCs, sightings, and identify previously seen observables. When investigations are finished, export IOCs to one or more MISP instances

Literature Review

The SOC is the information security department that constantly monitors, analyzes, and improves an enterprise's security condition. The SOC team's aim is to discover, assess, and respond to cybersecurity risks utilizing technical solutions and powerful process management. Security centers often contain information security professionals, engineers, and managers that monitor all procedures that take place. To handle security concerns as quickly as possible, SOC staff collaborate closely with incident response teams.

Because of rising cybersecurity threats, continual alert fatigue, and industrial problems, SOCs are insufficient. SOC analysts are continuously exhausted. Routine and complex procedures are mechanized to save the analyst's time and speed up the operation. With attackers becoming more agile by the day, cyber-security industry executives concur that "automation" is a necessary in today's cyber-threatened world.

Prior to the creation of a SOC, security duties are frequently congested and hand-to-hand. Who does what task, how problems are addressed, and how they are documented do not follow a set procedure. Workflows for incident management should be designed with the SOC from the start of the process to guarantee that each phase takes place in a larger context. Workflows lead to the clarification of each team member's position and duties, ensuring that no stone is left unturned.

Many businesses desire technological solutions that will support their visibility strategy and respond to network events while remaining within their budget. A complete set of tools is required to achieve optimal security coverage of your information systems. SIEM (Security information and event management) systems, incident tracking and management systems, intrusion detection and intrusion prevention (IDS/IPS/IDPS) systems, a threat intelligence (CTI) platform, packet capture and analysis tools, and automation tools are the main components of any effective SOC. The following steps must be performed by a SOC team using its technology.

- Network monitoring
- Endpoint management
- Asset discovery
- Threat intelligence
- Behavioral monitoring
- Data loss prevention
- Ticketing systems
- Policy compliance
- Incident response

To well function of all the above mentioned technologies, selecting of perfect combination of open-source tools are essential.

Project Functionality

This proposal mainly focuses on how the security incident management system solves the critical security events that must be investigated and responded to quickly. Any comprehensive site security system should include incident management software. It not only helps to safeguard your facilities, but it also frequently connects with other technologies to assist make your operations more efficient. Here are some of the reasons why you should use incident management software.

- Detect and respond to issues quickly
- Consolidate incident information in one place
- Classify, categorize, and prioritize incidents
- Meet compliance and mitigate liability
- Review and analyze incidents to improve security

To address all the above concerns, we thought to develop a scalable, open source, and free Security Incident Response Platform meant to make life simpler for SOCs, CSIRTs, CERTs, and any other information security practitioner dealing with security events that must be investigated and responded to quickly.

The Incident Management system provides a variety of techniques for storing data, files, and indexes based on your requirements. However, we strongly advocate utilizing Apache Cassandra as a scalable and fault-tolerant database even on a solitary production server. The storage of files and indexes might vary based on your goal arrangement; for a single server, the local filesystem is appropriate, whereas several choices are available in the event of a cluster configuration

- **Alert Management**

Go through your dedicated and detailed Alert page, make comments, identify similar Alerts, and define custom statuses and fields. Then decide whether or not they should be escalated to investigations or to incident response.

- **Case management**

Create cases and associated tasks and observables. Identify similar cases and alerts, define the PAP (Permissible Actions Protocol) level on each Observable, or improve your Incident Response process using a simple yet powerful template engine.

- **Multi-Tenant Environments**

Define the different organizations and teams and get them to work in a dedicated or collaborative mode: tenants' cases can be isolated or investigated by users from different organizations based on customizable roles and permissions.

- **Advanced User management**

Define and customize user profiles, assign them to users within their organizations and synchronize them via LDAP or AD.

- **Notifications Framework**

Define notification rules to invoke Webhooks, send emails, Slack, and Mattermost messages or call custom HTTP requests.

- **Metrics and dashboards**

Compile and correlate statistics on cases, tasks, observables, metrics, and more to generate useful KPIs and MBOs with our dynamic dashboard engine.

- **Comprehensive APIs**

Get full access to documented APIs to implement workflows or develop any automated scripts using TheHive data

- **MISP Integration**

Get shared Indicators of compromise quickly imported and ready to use or share yours easily with your communities by connecting TheHive with MISP.

Methodology & Business Model

In this project, we use open source and free solutions to get our project done. So, collaborating with the TheHive project we are planning to build the solution for the customers. And also we use collaborative tools with the TheHive project. These are the tools,

- Cortex Engine
- VirusTotal
- Alienvault
- Cloudera Sandbox

If customers want to carry out the project with them, they need to pay for additional features.

- **Free Version**

Since, all the tools are open source but some of the tools restrict some features for the free license. But for the project testing, these free licenses are enough.

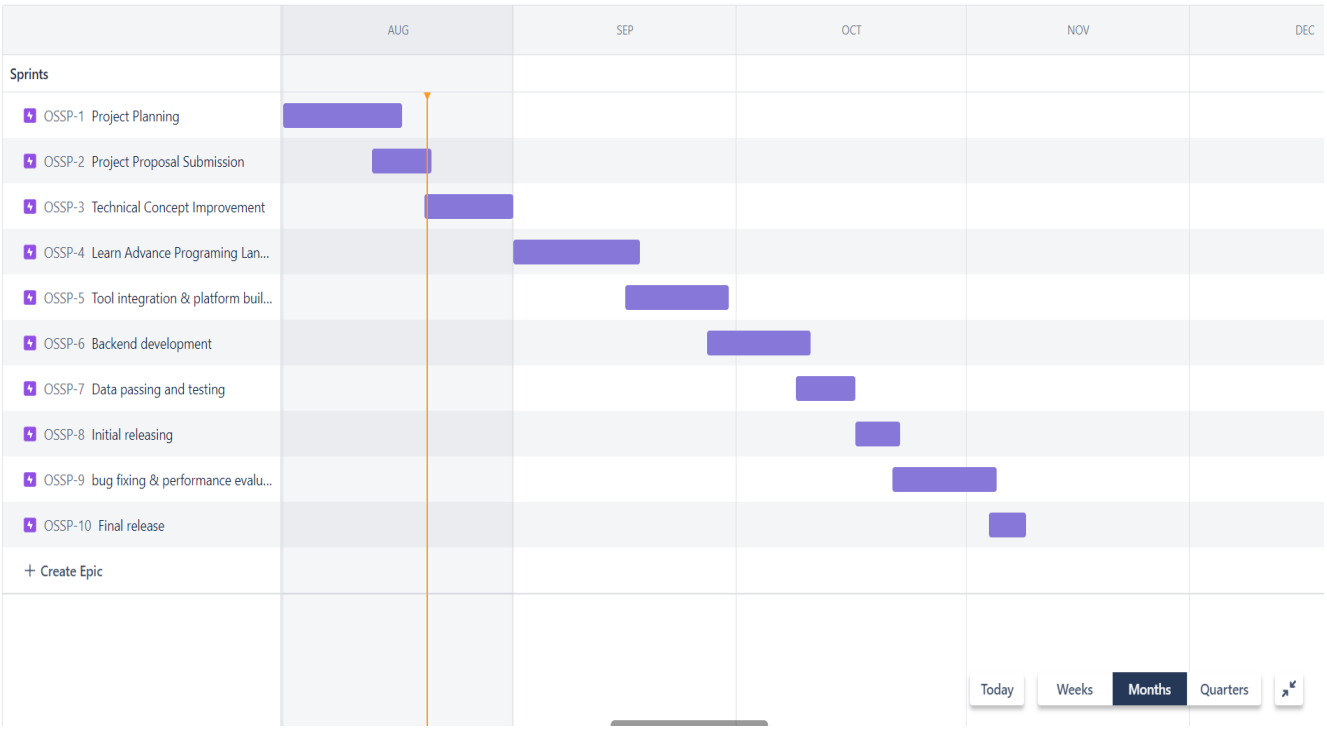
- **Paid Version**

Paid version include all inclusive functionality. Subscribers can select their preferred choice of subscription plan.

- **Trail Version**

Trail version expires within 30 days. In this version, we provide all core functions with limited resources.

Timeline with Agile Sprints



Technology and Architecture

- **The Hive project**

A scalable, open source, free Security Incident Response Platform that is tightly integrated with MISP (Malware Information Sharing Platform) is created to make life easier for SOCs, CSIRTs, CERTs, and any other information security professional dealing with security incidents that must be quickly investigated and addressed.

The Hive is a fully open-source platform but if we use TheHive Cloud platform it will be managed by the Hive group and it occurs the cost of the product. So, in this project, we use an open-source platform, and because of that, we need to customize and manage the product also this is an On-Prem solution.

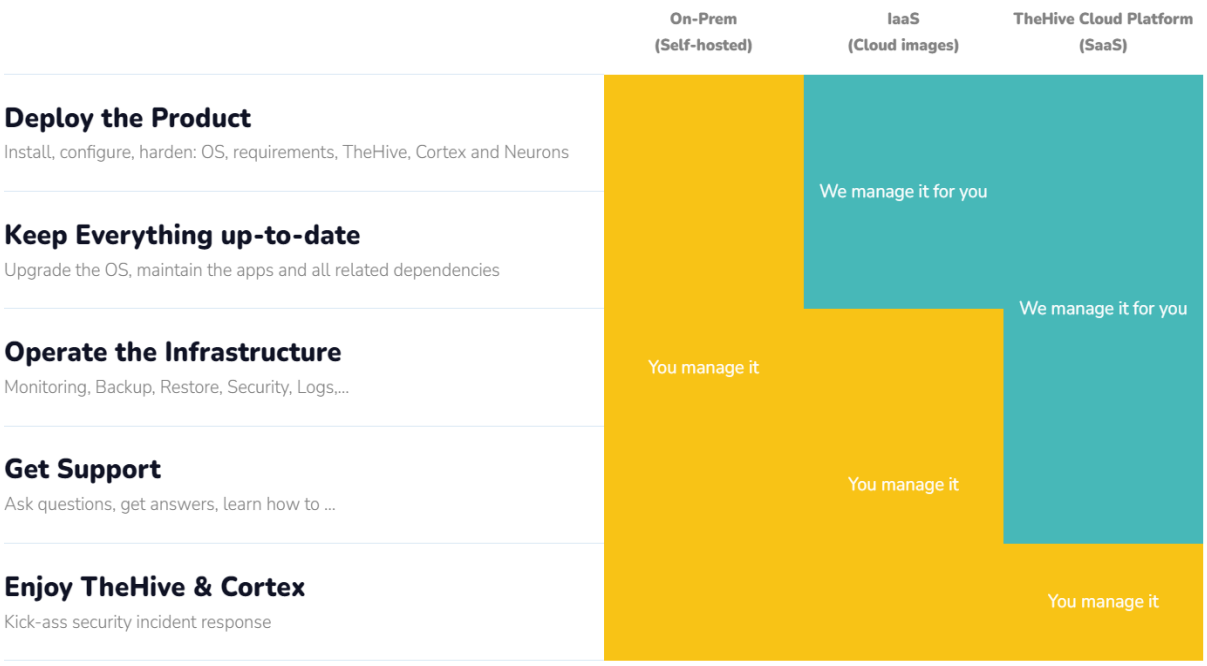


Figure 1

- **Cortex Engine**

The cortex makes it possible to use a Web interface to study observables like IP and email addresses, URLs, domain names, files, or hashes. Additionally, analysts may automate these processes and send significant amounts of observable data using TheHive, the Cortex REST API, bespoke scripts, or MISP from different SIRP systems. Thanks to its Active Response capabilities, Cortex greatly simplifies the confinement phase when utilized in combination with TheHive.

Cortex is helping to interact with APIs of various threat feeds. Cortex is also a fully open-source platform. So, if they are a cost with any APIs we are willing to connect we need to pay for this Engine. But for this project, we chose open-source threat feeds and that will cost-free.

- **VirusTotal**

VirusTotal is also free to use with the minimal features set. So, in this project, we use the free platform under these features, Many of the endpoints and services made available via the VirusTotal API are open to all registered users, however many others are exclusively available to our premium clients. The VirusTotal Premium API is made up of those endpoints and features, and this reference will identify them correctly

> **! Public API constraints and restrictions**
>
> The Public API is limited to **500 requests per day and a rate of 4 requests per minute**.
> The Public API **must not** be used in commercial products or services.
> The Public API **must not** be used in business workflows that do not contribute new files.
> You are not allowed to register multiple accounts to overcome the aforementioned limitations.

- **Alienvault**

Alienvault is also free to use with the minimal features set. You can quickly synchronize the Threat Intelligence provided in OTX with the tools you use to monitor your environment thanks to the OTX DirectConnect API. You may combine the DirectConnect agents with your

infrastructure to find threats aimed at your environment. Utilize the DirectConnect SDK (available in Java and Python) to create your integration for the community if there isn't a pre-built agent for the goods you use

- **Cloudera Sandbox**

Cloudera Sandbox needs a subscription, but they provide a free trial for testing. And this is out of scope request and an additional feature.

Architecture Diagrams

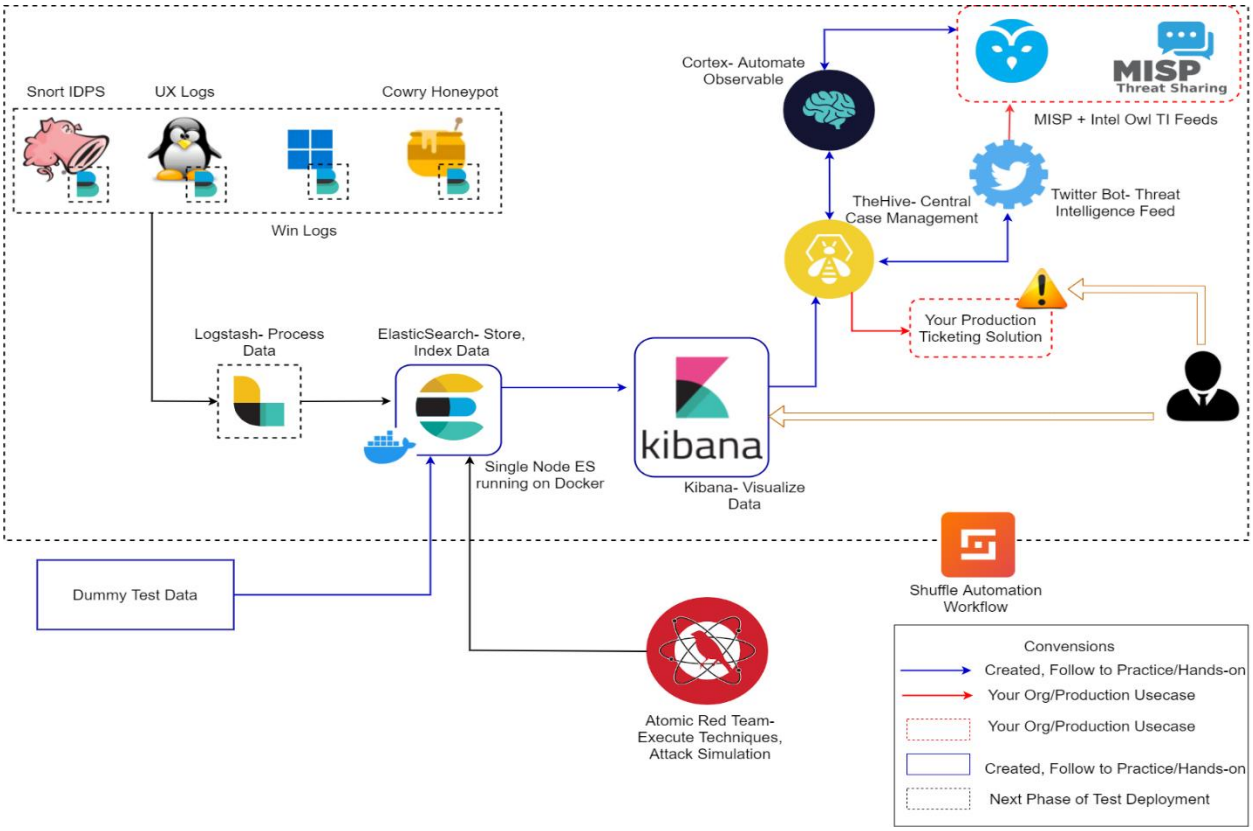


Diagram 01

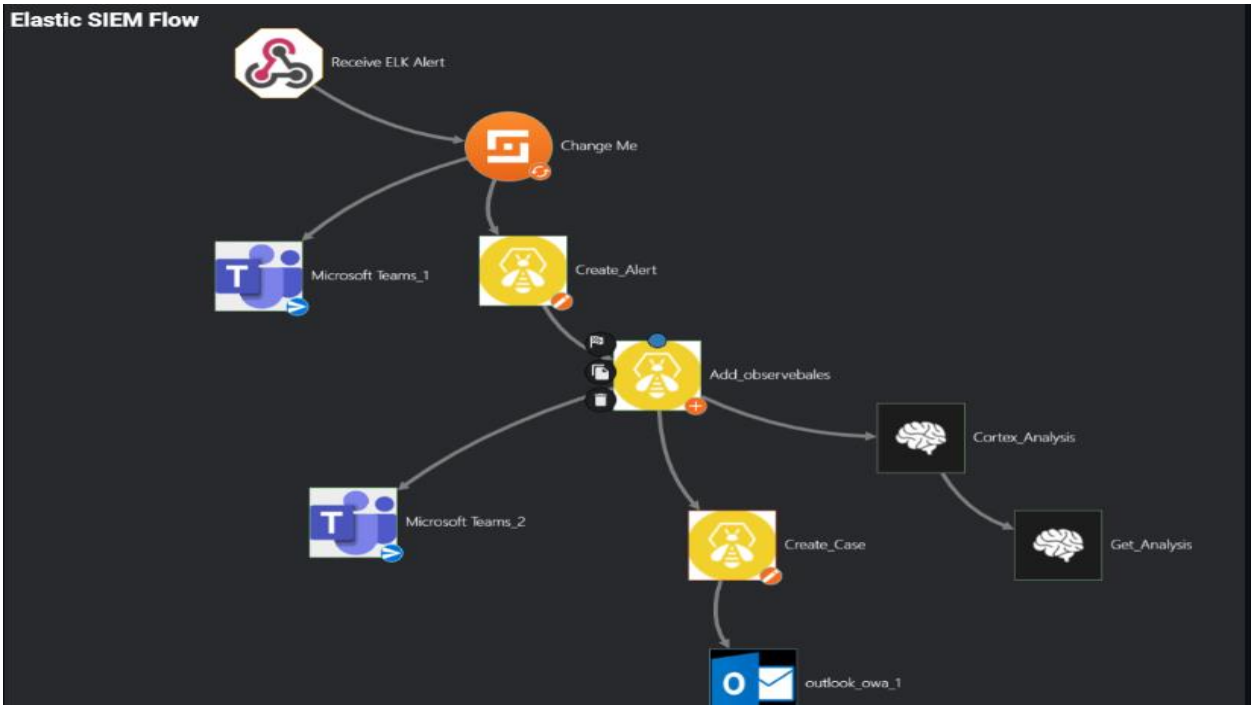


Diagram 02

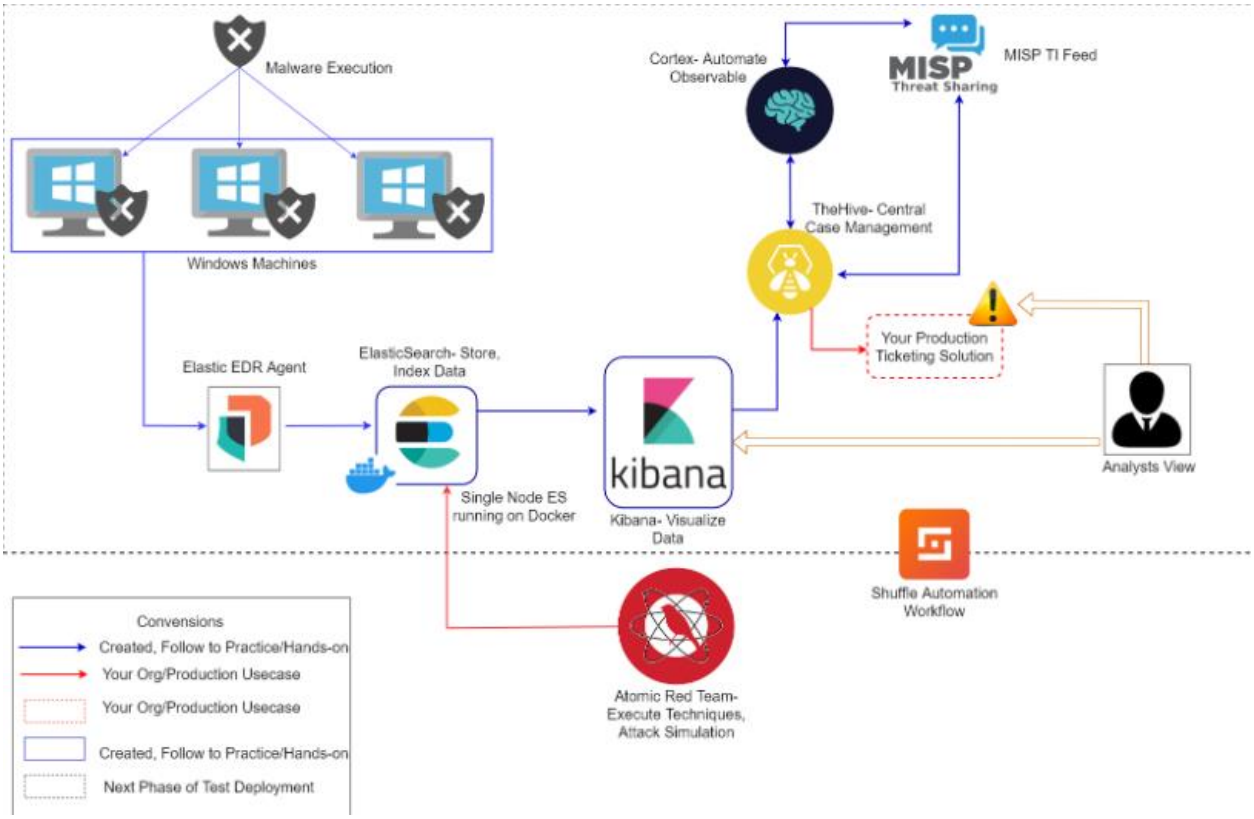


Diagram 03

Video Link

OneDrive Link :- https://mysliit-my.sharepoint.com/:f:/g/personal/it20021870_my_sliit_lk/EiEd060qwBNNrqiTdFyAlGcB2-aFDUBm3mr8yFA9L2Wk7Q?e=kgptQ6

References

http://docs.thehive-project.org/thehive/

https://github.com/TheHive-Project/CortexDocs

https://developers.virustotal.com/reference/public-vs-premium-api

https://otx.alienvault.com/api

https://dahamsocsolution.atlassian.net/jira/software/projects/OSSP/boards/1

https://socradar.io/how-to-build-a-soc-with-open-source-solutions/

https://www.investopedia.com/terms/b/businessmodel.asp