# Building a web application

## Background Information

The Mandiant® Intelligence Center™ released a [report](https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf) exposing APT1's multi-year, enterprise-scale computer espionage campaign. APT1 is one of dozens of threat groups Mandiant tracks around the world and considered to be one of the most prolific in terms of the sheer quantity of information it has stolen.

[Structured Threat Information Expression (STIX™)](https://oasis-open.github.io/cti-documentation/stix/intro.html) is a language and serialization format used to exchange cyber threat intelligence (CTI). STIX website has an example use case where the Mandiant APT1 report is converted into [JSON representation](https://oasis-open.github.io/cti-documentation/examples/example_json/apt1.json) of the STIX format.

## Requirements

Build a web application that reads the STIX JSON representation of Mandiant’s APT1 report and displays the threat report information to users. You should build web components that allows users to perform the following activities:

1. Enable user to view detailed information on the malwares and tools used in the campaign.
   1. Users should be able to search/filter the data by type, name, and kill chain phrases.
2. (Optional) Enable user to view on a map the location of the threat actors identified.
   1. Use markers to mark on the map the location of the threat actors.
   2. The markers should be placed dynamically based on the JSON data, and not static images.
3. Enable user to view the attack patterns of APT1, and describe it according to the Mandiant [kill change phrases](https://www.mandiant.com/resources/targeted-attack-lifecycle?gclsrc=aw.ds&&utm_source=Google&utm_medium=cpc&utm_campaign=PROD|M-Trends|SP|EN|Performance&utm_content=all&utm_term=en&cid=us&gclid=EAIaIQobChMIp4GS5tCY-AIVEBsrCh1GNQDLEAAYASAAEgJj1vD_BwE).
4. Enable user to view in graph format the relationship between the different STIX objects as represented in the JSON file. See example of graph below.
   1. The graph should be drawn programmatically using the JSON data and not use static image.

Diagram

Description automatically generated

## Link and References

* Mandiant’s APT1 report: <https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf>
* Mandiant Targeted Attack Lifecycle: <https://www.mandiant.com/resources/targeted-attack-lifecycle>
* STIX Version 2.1 Specification: <https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html>
* STIX example JSON representation of Mandiant APT1 report: <https://oasis-open.github.io/cti-documentation/examples/example_json/apt1.json>

## Assessment

Based on the application requirements, you should design and build the dashboards to display the report to the user. You will be assessed based on the following:

* UI/UX design of the dashboard and web components
* Functionality
* Code design and readability

You are free to use any programming language, any open-source framework and libraries to build your application.

## Submission

Please provide a shareable link to a single zipped file that includes the application source code, as well as a README file that provides instructions on how to install and run the application.