**Learning Objective**

1. Understand Cyber Threat Intelligence
2. Understand Open sources Threat Intelligence
3. Consolidate on previous learning

**Activities A**

Using the internet, carry out research to **describe** in **your own word**, in saved Microsoft Word document, the followings:

1. Cyber Threat Intelligence (minimum 1 paragraph)
2. Key Concepts of Cyber Threat Intelligence
3. Threat Intelligence Cycle (minimum 1 page)
4. How to find out about emerging attack techniques and how to recognise them (minimum 1 page)

Please note down the hyperlink of external sources of information used. You will need to feedback to a group & the whole class your findings.

**Activities B**

1. Explain **Open-Source Intelligence** is
2. Identify what could be included in **Open-Source Intelligence data sets**
3. Explain why it is important to only use reliable and valid sources of Open-Source Intelligence information

**Cyber Threat Intelligence**

Gathering threat information, processing this information and analysing it to be able to identify the intentions, behaviour and capability of the bad actors is cyber threat intelligence. This intelligence is paramount to be able to be proactive in defending and protecting the systems against emerging threats, key threat actors hence cybercrime rather than being reactive.

**Key Concepts of CTI (Cyber Threat Intelligence)**

It is important that the cyber threat intelligence is relevant, timely and ready to be put in action. Security Orchestration, Automation, and Response (SOAR) approach makes sure that the security teams notice and respond faster to any possible threats.

Cyber:These are the threats that aim to cause harm in the cyber space.

Threats: These threats the potential harm that may be cause by cyber criminals to effect the integrity, confidentiality and availability of the systems.

Intelligence: It is an act of researching, gathering data about cyber threats, technical developments about Hactivisim, cybercrime and cyberespionage. Also analysing this data and making it meaningful and representable to the stakeholders to be able to draw up an action plan to stop the potential attacks.

CTI Sharing: Following all the efforts of gathering, transforming, analysing and interpreting data, it is important that organisations share this knowledge with other organisations to find a collaborative way to combat cybercrime. Sharing information strengthens the overall cyber security as different organisations may find different ways to prevent cybercrime and everyone can improve the security of their systems with this collaborative effort.

There are technical threat intelligence (TTI) tools that organizations develop and share with each other in order to fight with crime together. Various publishers, security experts and even hackers share this data on different platforms such as twitter, dark web, forums, social media etc

Threat Intelligence Cycle

The raw data gathered should be transformed into completed intelligence and this happens in various stages to help the decision making process and take action

in the darkweb. Obviously, this information varies strongly with regards to credibility, timeliness and level of detail, and it is difficult to acquire and assess it in an automated manner since the sources do not only vary content-wise but also regarding their structure and syntax. To understand these evolving threats, it is essential for security experts to