Organize and Store Cyber Threat Information in Knowledge Base

- Organizations generally collect threat information from a **wide variety of sources**, including open sources, external sources, and commercial threat feeds
- Based on the usage, it is necessary to **store** and **organize** threat indicators in a knowledge base

Information stored in the knowledge base include the following:

- The source of a threat indicator
- The established rules for using and sharing a threat indicator
- The date and time an indicator was collected
- The lifetime of validity for a threat indicator
- Whether the attacks that are related to a threat indicator have targeted specific organizations or industry sectors
- Whether an indicator is associated with Common Weakness Enumeration (CWE), Common Vulnerability Enumeration (CVE), Common Configuration Enumeration (CCE), or Common Platform Enumeration (CPE) records
- Threat actors or threat actor groups associated with an indicator
- Threat actor aliases, if any exist
- The TTPs used by a threat actor
- The associated threat actor's motives and intent
- The different types of individuals targeted by the associated attacks
- The systems targeted in the associated attacks

Threat Intelligence Reports

- Threat intelligence reports are **prose documents** that include details about various types of attacks, TTPs, threat actors, systems, and information being targeted

- These reports include information related to threats that have been collected, aggregated, transformed, analyzed, and enriched to provide **actionable contextual intelligence** for organizations' decision-making processes

Notes:

Generating Concise Reports

- Disseminate timely and **relevant threat intelligence** frequently within the organization to increase internal awareness of relevant threats.

Elements required to create concise, actionable, and customized threat intelligence reports:

1. Report Details
2. Client Details
3. Test Details
4. Executive Summary
5. Traffic Light Protocol (TLP)
6. Analysis Methodology
7. Threat Details
8. Indicators of Compromise
9. Recommended Actions

Threat Intelligence Dissemination

- The dissemination of threat intelligence **helps consumers** gain a more **detailed insight into the threats** that organizations might face
- The information is usually disseminated through either a **manual process** or **automated process**

Essential criteria for the consumer to acquire and benefit from the intelligence:

The right content	Intelligence must consist of good-quality content that provides the consumer with an understanding of threats and their harmful consequences, which can help in developing a mitigation plan
The right presentation	Intelligence must be concise, accurate, and easily understandable; it must consist of a right balance between tables, narrative, numbers, graphics, and multimedia
The right time	Intelligence must be disseminated within a required time frame so that consumers can make timely and effective decisions regarding security

Notes: