Cyber Security Threat Intelligence

Purpose

Cyber threat intelligence (CTI) is the proactive process of collecting, analyzing, and disseminating information about potential and current cyber threats to help in incident detection and/or prevention. In addition, we support Syensqo stakeholders to make informed decisions and mitigate cyber threats to our people, systems, networks, and data assets.

Main Responsibilities

- Data Collection: Gathering data from various sources such as open-source intelligence (OSINT) and internal security logs.
- Analysis: Analyzing collected data to identify emerging threats, trends, attack techniques, and indicators of compromise (IoCs) relevant to Syensqo.
- Contextualization: Providing context to threat data by understanding the threat actor motivations, tactics, techniques, and procedures (TTPs), and their potential impact on Syensqo's operations.
- Dissemination: Sharing actionable intelligence with relevant stakeholders within Syensqo to facilitate timely response and decision-making. Integrating cyber threat intelligence into Syensqo's processes can enhance threat detection and response capabilities.

Goals

- Early Threat Detection: Assist with the identification and detection of threats at the earliest possible stage, enabling proactive mitigation measures to be implemented before significant harm occurs.
- Risk Mitigation: CTI works directly with the Syensqo GRC team in order to help reduce the organization's exposure to cyber threats by providing actionable intelligence that supports informed risk management decisions.
- Incident Response Enhancement: Enhance incident response capabilities by providing relevant context and guidance to responders, enabling them to effectively contain, eradicate, and recover from security incidents.
- Security Awareness: Increase overall security awareness among employees and stakeholders by sharing insights into emerging threats and best practices for protecting against them.

CTI Reports Library

In this section, you will find both current and archived Cyber Threat Intelligence (CTI) reports. These reports provide valuable insights into Syensqo's cyber threat landscape, offering intelligence at tactical, operational, and strategic levels. By reviewing these reports, you can stay informed about current and emerging threats, and long-term trends relevant to our organization's cybersecurity.

Please note that these reports are confidential. Sharing or reproducing them is strictly prohibited without prior authorization from the Cyber Threat Intelligence (CTI) team.

- **Annual Reports** : A strategic report based on a forecasting exercise that assesses the cyber threat landscape and the main threat trends that will be the most relevant for Syensqo in the upcoming year.
- **Quarterly Reports** : An operational-level report that tracks the evolution of key threat trends identified in the Annual Report. It monitors shifts in threat trajectories, assesses geopolitical developments, changes in attacker capabilities, and notable attacks.
- **Biweekly Reports** : A tactical/operational report that leverages internal and external data to inform about significant attacks and the attackers' tactics, techniques, and procedures (TTPs), along with recommended proactive defense measures.
- **Monthly Summaries** : Summarised versions of the above reports presented at the monthly IT Newsletter.