# Threat intelligence

ISO 27002 Control 5.7

## Control

Information relating to information security threats should be collected and analyzed to produce threat intelligence

## Purpose

To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken

## Why is it important ?

- To facilitate informed actions to prevent the threats from causing harm to the organization
- To reduce the impact of such threats

## How can it be organized ?

- At strategic level : by exchanging high-level information about the changing threat landscape
- At tactical level : information about attacker methodologies, tools and technologies involved
- At operational level : details about specific attacks

## Which kind of sources ?

- Identify sources of information that can provide relevant, insightful, contextual, and actionable threat information
- Internal sources can include event logs, crash reports, penetration testing, audits, or investigations
- External sources may include public authorities, standardisation bodies, Computer Attack Alert and Response Centres (CERTs), service providers, partners, media or online communities
- Examples include : ENISA, CCB, TISP, TIAF, TIEI

## Link with other frameworks

- NIST 800-53 rev5 : PM-16, RA-10
- NIST CSF 2.0 : ID.RA-02

Renaud Dardenne
Asphalia Consulting