# Threat intelligence THIN

Developing and sharing actionable insights on current and potential security threats to the success or integrity of an organisation.

|  |
| --- |
| **Guidance Notes:**Activities may include, but are not limited to:* gathering data from a variety of open or proprietary intelligence sources
* processing and classifying threat data to make it useful and actionable by others
* packaging the data for use by consumers of the information
* enabling the use of the data automatically by security tools
* providing threat intelligence to help others mitigate vulnerabilities or to respond to security incidents.
 |

## Level 2

Contributes to routine threat intelligence gathering tasks.
Monitors and detects potential security threats and escalates in accordance with relevant procedures and standards.

## Level 3

Performs routine threat intelligence gathering tasks.
Transforms collected information into a data format that can be used for operational security activities.
Cleans and converts quantitative information into consistent formats.

## Level 4

Collates and analyses information for threat intelligence requirements from a variety of sources.
Contributes to reviewing, ranking and categorising qualitative threat intelligence information.
Creates threat intelligence reports.
Evaluates the value, usefulness and impact of sources of threat intelligence sources.

## Level 5

Plans and manages threat intelligence activities.
Identifies which are the most impactful threat categories and what types of information can help defend against them. Reviews, ranks and categorises qualitative threat intelligence information.
Provides expert advice on threat intelligence activities.
Leads the production and editing of threat intelligence reports that enhance the intelligence production workflow. Distributes information and obtains feedback about the value, usefulness and impact of the data.

## Level 6

Sets direction, plans and leads the organisation’s approach to threat intelligence, including the use of suppliers.
Identifies requirements for threat intelligence based on the assets to be protected and the types of intelligence that can help protect those assets.
Engages with, and influences, relevant stakeholders to communicate results of research and the required response.
Ensures quality and accuracy of threat intelligence information. Reviews threat intelligence capabilities.