Document number: OC.36
Document Name: Threat Intelligence Policy
Document Owner: Operations Director
Issue Date: 01/05/2024
Current Revision Date: 01/05/2024

prevision research
THE DATA COLLECTION EXPERTS

Threat Intelligence Policy

Objective and Scope

Threat intelligence is the process of gathering, analysing and contextualising information about current and future cyberattacks, providing knowledge and understanding of threats.

The objective of the Prevision Research Threat Intelligence Policy is to organise and assign responsibility for the collection of intelligence that could provide evidence of a potential or real threat and the subsequent analysis, communication, escalation and action for protecting the confidentiality, integrity and availability of personal identifiable information of individuals, business intelligence and the information management system.

Roles, Responsibilities and Authorities

Roles and responsibilities for this policy are shared between the Operations Director, ISMS Representative and the Privacy Officer. These roles share specific responsibility for ensuring threat intelligence is monitored, analysed and actioned in a timely manner.

Where an incident occurs, the senior assigned role taking overall leadership is delegated to the Operations Director.

Legal and Regulatory

Title	Reference
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
Market Research Society Code of Conduct	https://www.mrs.org.uk/pdf/MRS-Code-of-Conduct-2019.pdf
Market Research Society Fair Data Principles	https://www.fairdata.org.uk/10-principles/

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
Threat Intelligence Policy				5.7

Related Information

- Information Security Policy

Threat Intelligence Policy

Policy

Information security threats are risks related to the confidentiality, integrity and availability of information used in the company.

Prevision Research collects and analyses information about an existing or suspected threat to make informed decisions and take preventive measures to mitigate risk and /or reduce the impact of an event.

Threat intelligence needs to be relevant to the organisation and its information systems, be accurate, timely and in sufficient detail to be informative, be provided in the context of business risks and credible.

There are typically three levels of threat intelligence:

1. Strategic level

   Executive level investment in assessing the organisation's threat potential and vulnerabilities, then acting on them to resource and develop measures to monitor and counter the threat risk.

   These are longer term strategic planning activities involving an Information Security Strategic Plan in place.

2. Tactical level

   Tactical information gathering and analysis is short term, more practical and actionable involving the ongoing collection of information about what’s happening in the cyber domain and what can be learnt from it.

   Threat Intelligence Plans developed by Threat Intelligence Groups in the workplace are an effective, informative and timely tool.

3. Operational level

   Information gathering and analysis level typically managed by IT professionals and others using information intelligence gathering software and other activities such as penetration testing.

   This information provides the ‘how’ and ‘where’ factors in terms of pre-empting and defending against attacks, supporting investigations into attacks and improving overall security levels.

Threat Intelligence Principles

Intelligence is considered a potential threat if it is about:

1. High level secure information systems that reflect, or appear to reflect a change in the landscape of a current situation that is neither known, expected nor planned.
2. Suspect activities or tactics about information security threats including hearsay about new or changed tools, methodologies or other introduced technologies not open to scrutiny or ICT discussion.
3. Known specific attacks on operational systems.

Tactical threat intelligence plans and threat intelligence groups

Prevision Research threat intelligence plans form the basis of keeping informed and acting expeditiously in the instance of a suspected threat.

Threat Intelligence Policy

Nominated representatives (refer roles and responsibilities) shall be assigned to create a Threat Intelligence Group:

1. Establish communications with IS risk groups known to monitor threat intelligence in their respective roles (IT l Privacy l ISMS Compliance) e.g. like businesses, independent advisors, government agencies and cyber security groups
2. Monitor communications and activities of the related group for any suspect intelligence.
3. Undertake an initial analysis of information to determine accuracy of information, reliability of source and determine whether to escalate based on initial information.
4. Decide whether to silo the information to see what develops or escalate for further investigation.
5. Escalation shall involve IT analysis and /or factual investigation and reporting to the relevant internal group
6. Depending on the risk nature of the investigation/analysis report, the Infosec Incident Management Team or other senior management representative shall be consulted for direction and action.

Post threat intelligence processing:

- preventive measures shall be assigned,
- further detection methods/technologies shall be introduced as appropriate,
- the need for additions or change to the audit and test program shall be reviewed,
- outcomes communicated throughout the organisation, and also
- externally to interested parties including those involved in threat intelligence activities.

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change or a policy breach is known to have occurred.

Periodic reviews shall take into account feedback from infosec groups, regulatory groups and audits. Changes to the policy must be approved by a senior executive then communicated to all previous persons or organisations with access to the policy.

Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N