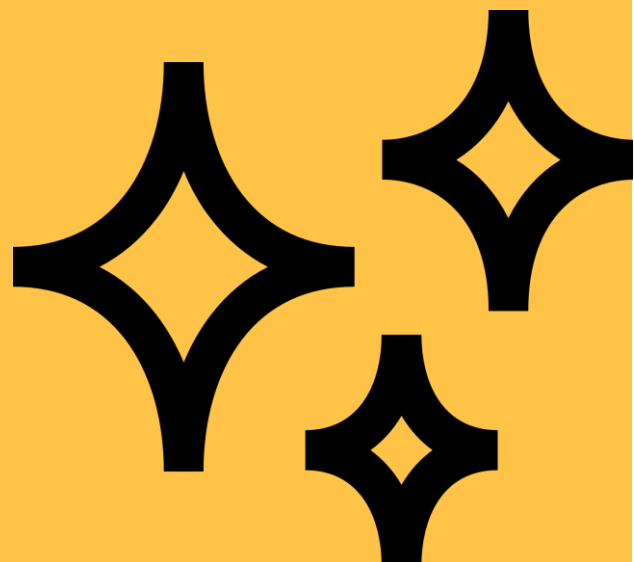




Service Definition Document

Cyber Security Threat Intelligence Service



Contents

| | |
|--|---|
| Solution Overview | 2 |
| Aim and Objectives | 2 |
| What is Cyber Threat Intelligence Service? | 2 |
| Key Features | 3 |
| Key Benefits | 3 |
| Scope and Duration | 4 |
| Deliverables | 4 |
| Data Protection & GDPR | 5 |
| Why iomart? | 6 |

Solution Overview

Aim and Objectives

The primary aim and objective of this cyber threat intelligence service is to provide organisations with comprehensive and actionable intelligence about potential cyber threats, enabling them to proactively identify, prevent, and respond to cyber-attacks and security breaches.

Objectives:

- Identify emerging cyber threats, malicious actors, and attack vectors that could pose risks to the organisation.
- Analyse the organisation's current security posture and vulnerabilities to assess potential risk exposure.
- Monitor various sources of threat intelligence, including open-source, dark web, and proprietary databases, to gather relevant data.
- Contextualise and analyse collected data to provide insights into the motives, capabilities, and tactics of threat actors.
- Provide actionable recommendations and mitigation strategies to enhance the organisation's security measures and reduce the risk of successful attacks.
- Continuously monitor and update threat intelligence to ensure the organisation stays ahead of the evolving threat landscape.
- Support incident response and forensic investigations by providing relevant threat intelligence and analysis.
- Facilitate informed decision-making by providing a comprehensive understanding of the cyber threat environment.
- Enable compliance with industry regulations and security standards related to risk management and threat monitoring.
- Protect the organisation's assets, reputation, and business continuity by proactively addressing potential cyber threats.

This cyber threat intelligence service aims to empower organisations with the knowledge and tools necessary to anticipate, detect, and respond effectively to cyber threats, minimising the impact of security incidents and breaches.

What is Cyber Threat Intelligence Service?

In the current digital age, where incidents and data breaches are becoming increasingly common, it is vital to understand the specific threats your organisation is facing. We are excited to offer a custom and tailored Threat Intelligence Report. This premium service provides:

- Threat Analysis: A thorough examination of potential threats uniquely relevant to your organisation.
- Exposure Assessment: Evaluating your organisation's current vulnerability to these threats.
- Brand and Domain Threat View: Insights into threats specifically targeting your brand and domains.
- IP Address Exposure Check: Examine key personnel's exposure based on associated IP addresses, assessing potential risks.

- Industry-Specific Threat Activity: Analysis of threat activities prevalent in your company's sector.
- Common Vulnerability Identification: Identification of vulnerabilities commonly exploited in your industry vertical.
- Custom Security Recommendations: Tailored strategies to bolster your organisation's cybersecurity posture.

A specialised report based on campaign interaction of users that may need additional training.

Key Features

- Threat analysis including thorough examination of potential threats.
- An exposure assessment will evaluate your organisation's current vulnerability.
- Brand and domain threat view.
- IP address exposure check.
- Industry-specific threat activity.
- Common vulnerability identification and vulnerabilities commonly exploited in your industry.
- Custom Security Recommendations with Tailored strategies.
- A report based on campaign interaction of users requiring training.

Key Benefits

- Proactive threat identification: Helping identify potential cyber threats, vulnerabilities, and attack vectors before they can be exploited, enabling proactive defence measures.
- Risk mitigation: By understanding the threat landscape, organisations can implement appropriate security controls and countermeasures to mitigate the identified risks effectively.
- Improved security posture: Regular threat intelligence exercises help organisations stay informed about the latest threats and attack techniques, allowing them to strengthen their overall security posture continuously.
- Targeted resource allocation: Threat intelligence provides insights into the most critical areas of risk, enabling organisations to prioritise and allocate security resources more effectively.
- Compliance and regulatory adherence: Many industries and regulatory bodies mandate regular risk assessments and threat monitoring, which threat intelligence exercises can fulfil.
- Competitive advantage: By staying ahead of potential threats, organisations can maintain business continuity and protect their assets, reputation, and competitive edge.
- Informed decision-making: Comprehensive threat intelligence empowers organisations to make well-informed decisions about their security strategies, investments, and incident response plans.

Overall, a threat intelligence exercise is a proactive approach to cybersecurity that helps organisations anticipate, detect, and respond to potential threats more effectively, minimising the risk of costly breaches or disruptions.

Scope and Duration

It is anticipated that on commencement of the Cyber Threat Intelligence Service, it will take approximately 3 to 4 weeks of elapsed time to complete each of the component pillars, develop report and present to all stakeholders.

Deliverables

The deliverable for the Cyber Threat Intelligence Service is the performance of the necessary consulting services along with a final written report.

Key Outcomes

- Business-led, rather than technology focused.
- Engagement from top level management in exercises.
- Minimal overhead due to experienced project planning and experienced consultants delivering each workshop.
- Helps solve client problems rather than impose solutions.
- Prioritised roadmap informs next steps leading to follow on work to mitigate residual risk.

Data Protection & GDPR

iomart is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. Our Data Protection policy sets forth the expected behaviours of iomart Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to an iomart Contact (i.e. the Data Subject). iomart, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in our Data Protection policy (available on request).

iomart's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all iomart Employees and Third Parties to share in this commitment.

iomart uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of iomart Entities.
- To provide services to iomart customers.
- The ongoing administration and management of customer services.
- The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.
















Each iomart Entity will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, iomart will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party

Why iomart?

Here's why you should use iomart for your solution:

- Expertise and Experience – our experienced team of consultants are experts in their field, offering advice and guidance to bridge any knowledge gaps within your organisation.
- Resource Scalability – our consultants act as an extension of your own team, temporarily scaling up resources to carry out particular projects and activities on your behalf.
- Future Ready – our consultants use best practice to design services fit for tomorrow's world, keeping you ahead of the competition and at the edge of innovation.
- Customised – our consultants tailor their services to meet your individual requirements ensuring meaningful results that really matter to your organisation.
- Security – with the increase in cybersecurity attacks, particularly ransomware, our services always place the security of your data at the forefront of everything they do.
- Continuous Improvement – we are ITIL aligned and follow a rigorous process to identify where you are today, where you want to be tomorrow, and how you get there.
- Highly accredited – we are highly accredited, as shown below, so you can be assured that your projects, team, and data are in safe hands.

| ★ Welcome to straightforward ★ | | ★ Managing Risk ★ | | ★ Environment + Societal + Governance ★ | | | |
|---|---|---|---|--|---|---|---|
| Quality | Service | Security | Stability | Environment | Energy | Safety | |
|  |  |  |  |  |  |  | |
| → Fully Integrated Management System Standards ← | | | | | | | |
| Customer Assurance Sales, Service & Support | | Business Confidence Group resilience & integrity | | Waste Control & Recycling | Managing Utilisation | Employee Wellbeing | |
| Quality as a Service Managed Service Agreement Service Level Agreements | | Data Protection | Business Continuity | Environmental Responsibilities | Climate Change Responsibilities | Health Protection Responsibilities | |
| Customer Assurance | | Business Resilience | | Sustainable Goals | | | |
|  |  |  |  |  |  |  |  |