ATECH IOMART

Service Definition Document

Cyber Security Threat Intelligence Service

Contents

Solution Overview

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 service providing regular reporting and continuous monitoring of specific artifacts.

Threat Assessment Report delivered on a quarterly cadence containing the following:

- **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.

Continuous Threat Monitoring across deep, dark and open Internet.

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
- Dark, deep and open web monitoring of keywords/proprietary information

Key Benefits

- Proactive threat identification
- Risk mitigation
- Improved security posture
- Targeted resource allocation
- Compliance and regulatory adherence
- Competitive advantage
- Informed decision making

Aims and Objectives

Aims

The primary aim 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

Key objectives include:

- 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.

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.

What to Expect

- 24/7 monitoring and alerting
- Priority 1 alerts investigated within 30 minutes
- Monthly summary reports and quarterly reviews
- Clear escalation paths and communication protocols

Data Protection & GDPR

Atech, part of the Iomart Group, 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 to take steps at the request of the Data Subject prior to entering a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary 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 Partner with Atech?

Credentials and Capability

Atech is the one of the UK's most accredited providers of secure hybrid cloud managed services, delivering deep expertise across Microsoft technologies, data protection, and cybersecurity. We hold Microsoft designations for **Modern Work, Security, Infrastructure (Azure)** and are recognised as an **Azure Expert MSP** - a status achieved by only 60 partners globally and 15 in the UK.

As part of the Microsoft AI Cloud Partner Program, we have validated technical capabilities across the full cloud lifecycle. Our inclusion in the **Azure Expert MSP Program** reflects proven excellence in people, processes, and tools, ensuring sustainable, repeatable, and scalable managed services. This means you can rely on a partner that consistently delivers best practice and operational efficiency.

Partnering with us gives you access to over **200 Microsoft cloud specialists**, including **two Microsoft MVPs**, ensuring unparalleled technical depth and experience.

Microsoft Endorsements and Specialisations

We hold multiple Microsoft Solutions Partner designations, including:

- Digital & App Innovation (Azure)
- Data & AI (Azure)
- Business Applications

Figure 1: Microsoft Accreditations

In addition, we have achieved advanced specialisations in areas such as:

- Cloud Security
- Identity and Access Management
- Threat Protection
- Infra & Database Migration
- Azure Virtual Desktop
- Enterprise Application Migration to Azure

Figure 2: Microsoft Designations

These credentials validate our ability to deliver complex, secure, and innovative solutions aligned to Microsoft best practices.

Security and Compliance

Security is at the heart of our services. Atech is **ISO 27001 certified, Cyber Essentials Plus accredited**, and a member of the **Microsoft Intelligent Security Association (MISA)** – an invitation-only program granting access to Microsoft's top security experts. We also hold **CREST accreditation** and participate in the **Microsoft MSSP Program**, one of only 12 partners in the UK, giving our customers direct benefits such as access to product teams and funded workshops.

Further reinforcing our security leadership:

- **Microsoft Gold Partner Status** alongside **Azure Expert MSP**
- **Microsoft MSSP Program** (1 of only 12 UK partners)
- **Microsoft Fastrack Ready Partner** (1 of only 300 globally)
- **Microsoft XDR status**

These credentials provide you with assurance that security is embedded throughout design, migration, and ongoing management. Combined with our advanced specialisations and industry recognition, they demonstrate our ability to deliver secure, compliant, and future-ready solutions.


ATECH IOMART
6 Atlantic Quay, 55 Robertson Street, Glasgow, G2 8JD