Schedule Document

Dark Web Monitoring

Public
Aztech IT Solutions
01/08/2019

Schedule Document

Dark Web Monitoring – Threat Detection

This schedule contains additional terms and conditions, service description & Service Levels applicable to the associated Order Form and Aztech's General Terms and Conditions.

1. Overview

Aztech's Dark-Web Monitoring service is a Threat Intelligence managed service. By monitoring the Dark Web, the service provides alerting for the client to potential threats, system attacks and compromised users passwords.

Information discovered by the service will be critical to the security integrity of the client. It is important that the information from the service is escalated to the appropriate areas within the client's organisation that mitigating actions can be taken by the client's IT department.

If we assume that eventually, a breach will take place it is critical to detect and respond as soon as possible. How can this detect and response?

How can this detect, and response window be reduced to stop the outflow of client information, stop the attacks and limit the damage done?

Implementing Dark Web Monitoring will assist in:

- Identify compromised credentials, passwords and personally identifiable information actively being sold on the Dark Web
- Detect and alert newly found compromised credentials, passwords and personally identifiable information on the dark web.

Aztech will be your Security Operations Centre (SOC), utilising the technology and processes to highlight the threats facing your organisation found from monitoring the Dark Web. Any anomalies found which should be investigated will be alerted to your internal team.

The Aztech SOC team will see the types of threats directed against your organisation and will escalate to your internal IT team for investigation and action if required.

2. Overview

This schedule outlines the scope of works ("SOW") delivered to the "Customer" by Aztech's SOC and professional services teams.

The "SOC" (Security Operations Centre) services are designed to alert, detect and respond to security threats in line with SOC services purchased in the service order form.

Services are delivered during business hours from our HQ in Milton Keynes. "out of business hours" services are delivered by our 24/7 technical and security teams.

Our **Technical Support Centres** are currently located in;

- Milton Keynes, United Kingdom

2.1 Dark Web Service Features

Various services may include and will be determined by the service order form;

- 24/7/365 Dark Web Monitoring
- Ticket Creation Upon Detection of Alert
- Access to Aztech Client Portal
- Daily, Monthly Reporting
- Client- Self Management Portal
- Client Training & On-Boarding

3. General Definitions

"SOC" (Security Operation Centre)" Aztech service name for a set of monitoring and managed security services delivered to it's clients from it's UK Technical Support Centre.

"Incident" means an unplanned interruption to a service or a reduction in service quality.

"Change Request" means a request from a user for an operational change.

"Alert" means a system generated monitoring alert that is potentially service affecting and in need of review or attention.

"Event" means a system generated informational monitoring alert that is not service affecting.

"Ticket" – means the tickets which are raised in relation to Incident or Request

"Ticket Number" means the unique number issued when logging a fault with Aztech.

"RMM" means Remote Monitoring & Management. A toolset in which Aztech utilise to deliver parts of the service.

"SLA " means Service Level Agreement. The terms that set out and govern the guaranteed response and target resolutions times.

"Response Time" means the time for an Aztech resource to respond to the logged incident or service request.

"Resolution Time" means the length of time from the issue of the fault ticket number to repair and resolution or the service and/or associated equipment.

"Patch Management" means the updating of software updates in accordance with the approved "patch policy" document

"Maintenance Window" the agreed time and schedule in which patches, software updates and equipment re-starts can occur.

"Planned Outage" means in maintaining the service provided, Aztech may with reasonable notice require a temporary outage in service. Wherever possible Aztech will agree the outage with you in advance of the required work.

"Third Party Attributable Faults" means in the event that a Service Affecting or Non-Service Affecting Fault is identified as being attributable to a third party this measurement period shall not be included in service availability measurements. Such faults do not qualify for rebates or compensation. Aztech will endeavour to resolve and rectify such Third-Party Attributable Faults as soon as possible.

"Time to Resolve Fault (TTRF)" means the length of time from the issue of the fault ticket number to repair and resolution or the service circuit and/or associated equipment.

"Service Desk" Means Aztech's fault management centre, which operates the Aztech Service Desk Ticket system, Monitoring Tools and Fault resolution Services.

"User" means an authorised employee, contractor or agent of the Customer who has access to the Service Desk for the support of their Customer owned Desktop Device or Devices.

"Vendor" means a third-party original equipment manufacturer that builds, supplies and provides warranty support.

"On-Boarding" means services provided by the Aztech's On-boarding and Service Readiness Team to bring the environment and Users into support.

"Managed Services" is the given name to Aztech's fully managed pro-active IT support services.

"Support Blocks" means pre-paid time-based support blocks for reactive ServiceDesk incidents and service requests.

1 Block = 1 Hour of support time. Support time is recorded by Aztech technicians in 15-minute increments as and when used. The number of allotted support blocks will be identified in the service order form.

Where support blocks are rolling month to month any unused time will be pooled and made available to be called upon or used at a later date. Pooled and unused support blocks can not renew past 12 months.

Should support blocks exceed the agreed or allotted amount you will be charged additionally. We will endeavour to warn you in advance that support time is running low and provide a quote or service order form for additional blocks. You accept that during P1 or P2 cases our technicians may attend to support incidents without seeking approval for additional blocks and that you will be charged at the standard block hour rate.

"Per user Per Month Support" means Aztech's proactive IT managed service support. As defined in the "managed services schedule" Pricing is billed at a fixed rate per user per month for every active user.

"Business Hours Support" means services being provided Monday to Friday 08:30am to 5:30pm excluding bank and public holidays

"Out of Business Hours Support" means services being provided Monday to Friday 5:30pm to 8:30am including bank and public holidays and all-day Saturday and Sunday.

"24/7/365 Support" means services being provided every day all day.

"SEIM" Security Event and Incident Management – Software used by Aztech to process log data and events from Assets. Its functions include:

• Normalisation – converting entries in logs and individual alerts into generalized Events independent of the device and its brand or version.

• Classification – giving Events a first classification, using Aztech proprietary Event Classification Policy Language, filtering out false positives or Events related to vulnerabilities absent in the targeted environment.

• Pattern matching – recognising patterns pointing to reconnaissance scans, infections or attacks

. • Statistics – calculating averages to discover trends and anomalies, and to allow comparisons.

• Workflow management – recording the activities for an Incident.

• Information management – managing the information needed to examine, evaluate, and classify Incidents.

• User management – defining the views and authorisation levels of users

3.1 Customer cooperation

Aztech expects any customer to co-operate to provide full notice and visibility of any cyber-attack incident when required, and to treat advanced notification of such as urgent. This may include sharing of information such as ransom emails or telephone calls.

3.2 Third parties

The Customer commits to fully manage all their customers and suppliers directly. Aztech will not interface directly with any third parties working with the Customer unless by prior arrangement. If the Customer requires Aztech to provide their customers with a customer care or NOC/SOC service this is available on request and subject to Professional Service Fees.

4. Fees

Fees will commence on the service go live date. Invoices are sent on the 1st of every month for a month in advance of service.

Fees may comprise any or all of the following.

4.1 Installation and set-up fees

Any applicable Design, Configuration, and Installation Fees for the implementation, on-boarding of NOC/ SOC or ITMS services shall be detailed on the Order Form.

Subscription fees are applied as and when the service is made available.

4.2 Warranty

Aztech does not warrant that Dark Web Monitoring will detect and prevent all possible threats and vulnerabilities or that such services will render the Customer's network and systems invulnerable to all security breaches and vulnerabilities.

4.3 Professional service fees

Additional tasks undertaken by Aztech at the request of the Customer will pre agreed by a separate order form and completed by the professional services teams.

5. Customer responsibilities

In order to deliver the service we expect the customer to provide:

- Named points of contacts for Aztech to Liaise with
- Domain Name in need of Monitoring
- Liaison with Aztech Engineering, Provisioning and project management teams.
- Liaison with Aztech Customer Support teams.

5.1 Approved Monitoring & Alerting

The Customer commits to working with Aztech during the on-boarding process to complete and sign-off an approved monitoring and alerting configuration worksheet. (worksheet document to be provided by Aztech) The completed configuration document should be added to the appendix of this schedule.

6. Event reporting and management

6.1 Event handling

Alerts and events will be recorded in the Aztech ticketing systems. The client will be notified of any alerts. If support or assistance is required by the client Aztech will record details of the request in its IT management system

6.2 Hours of Support

The Dark Web Monitoring service will provide automated 24/7/365 alerting via email and the ticketing system. The Aztech SOC team will respond to alerts during normal standard business hours Monday to Friday 8:30am to 5:30pm. If extended hours or full 24/7 response services are required the client will be required to purchase either a fully managed SOC service or additional out of business hours services.