IBM
Service Description

IBM X-Force® Threat Analysis Service

1. Scope of Services

IBM X-Force Threat Analysis Service (called "XFTAS") is a security intelligence service that is designed to deliver customized information about a variety of threats that could affect Customer network security.

The service provides threat information collected from the SOCs, trusted security intelligence from the IBM X-Force® research and development team, and the IBM Global Threat Operations Centre, and secondary research from other public and private resources. This combination of information helps to identify the nature and severity of external Internet threats. In addition to alerts and X-Force intelligence, each Customer registered security contact will receive detailed information regarding real-time Internet port metrics, Web defacements, worms and virus activity, as well as daily analysis of identified Internet threat conditions.

The details of your order (e.g., the services you require, contract period, and charges) will be specified in an Order.

Definitions of service-specific terminology can be found at www.ibm.com/services/iss/wwcontracts

2. IBM Responsibilities

2.1 Deployment and Initiation

During deployment and initiation, IBM will enable the Customer to access the Virtual-SOC, and will work with the Customer to activate XFTAS.

An assigned IBM deployment specialist will contact the Customer to request one name and e-mail address for each XFTAS subscription purchased. The individuals identified by the Customer will be the Customer's registered security contacts.

IBM will send each Customer registered security contact a welcome e-mail with a user ID and temporary password. The user will be required to change the password on the first login.

2.2 Ongoing Management and Support

After XFTAS has been established, and during any renewal contract period, IBM will provide XFTAS on a 24 hours/day by 7 days/week basis.

2.2.1 Licensing

XFTAS can be purchased with one of the following types of licenses:

Individual

The individual license entitles a single person in an organization to login to the Virtual-SOC and customize the delivery of XFTAS content. This person is entitled to view information in the portal and to receive e-mail notifications configured in the portal. The individual is not authorized to share or distribute XFTAS information. Although an organization can transfer an individual license from one person to another if needed, an individual license cannot be shared.

Distribution

The distribution license entitles a person with an individual license to distribute his/her customized content from the XFTAS to others in the organization. For example, an organization might designate a single person to be the administrator of security information for the company. This person would be responsible for customizing the information received from XFTAS, and then distributing that content to all affected parties at the company. The individual license would act as the number of "customised" versions of XFTAS information. The distribution license would act as the total number of recipients of the information, minus the individual licenses.

2.2.2 Key Features

The key features of XFTAS include:

a. Daily assessment and critical issues e-mail notifications

The daily assessment is delivered by e-mail to each Customer registered security contact. The e-mails provide information about the day's identified issues, in addition to a customized list of identified vulnerabilities, threats, and news articles that pertain to the Customer's business. As breaking news about critical vulnerabilities or threats emerges, IBM may send separate e-mail notifications to inform Customers about an alert, an advisory, or other security issues.

b. Daily assessment and vulnerability watch alert customization

Through the Virtual-SOC, Customers can enable e-mail notifications and customize the content delivered in the daily assessment. Customisation options include logical categories of information, such as business sector, region, and affected product (e.g. operating system, hardware, application, browser, and Web server).

c. Comprehensive information about vulnerabilities, active threats, and other security news

The Virtual-SOC provides comprehensive and easily searchable information about known vulnerabilities documented in the X-Force database, malware, Web defacements, security news, port activity, and alerts/advisories published by X-Force and by the United States Computer Emergency Readiness Team ("US-CERT").

d. IBM X-Force Threat Insight Monthly

The IBM X-Force Threat Insight Monthly is designed to highlight some of the most significant known threats and challenges facing security professionals today. This report is a product of IBM Managed Security Services and is compiled by the X-Force security intelligence team. Each issue focuses on one or more issues and provides a recap of recent significant, identified, online threats.

2.2.3   Virtual-SOC

The Virtual-SOC is a Web-based interface designed to enable delivery of key service details and on-demand protection solutions. The Virtual-SOC is designed to help deliver a consolidated view of the Customer's overall security posture. The portal is capable of merging data from multiple geographies or technologies into a common interface, allowing for comprehensive analysis, alerting, remediation, and reporting of identified threats and issues.

The Virtual-SOC is designed to provide real-time access for communications including ticket creation, security event handling, incident response, data presentation, report generation, and trend analysis.

3.   Customer Responsibilities

The Customer is responsible for keeping their user ID and password information confidential and not sharing it with anyone else.

The Customer agrees to adhere to their licensing agreement and not forward XFTAS information to individuals who do not have a proper license.

The Customer is responsible for maintaining current contact information in the Account Management section of the Virtual-SOC, configuring their e-mail alerting preferences, and tailoring their alerting preferences for vulnerabilities and news that pertain to their organization (optional).