

Glossary

The following terms are used throughout the Service Descriptions and have been provided for the purpose of clarity.

1. **Alert Condition (“AlertCon”)** – a global risk metric, developed by IBM, using proprietary methods. The AlertCon is based on a variety of factors, including quantity and severity of known vulnerabilities in the wild, exploits for these vulnerabilities, availability of these exploits to the public, mass-propagating worm activity, and global threat activity.
2. **Appliance** – a single hardware device containing pre-installed software.
3. **Customer Premise Equipment (“CPE”)** – service provider equipment that is located on the Customer's premises (physical location) rather than on the provider's premises, or in between. CPE can be owned by the Customer or by the provider.
4. **Extended Log Archival** – provides extended log archival capabilities for mission critical data or regulatory compliance.
5. **Host** – a machine that has a presence on the network. A Host has an IP address, and communicates with other Hosts on the network.
6. **IBM Virtual Security Operations Center (“Virtual-SOC”)** – the Web portal that provides information about the Customer's managed services.
7. **IBM X-Force® Threat Analysis Service (“XFTAS”)** – enables proactive security management through comprehensive evaluation of global online threat conditions and detailed analyses. The service provides a combination of threat information collected from IBM Security Operations Centers (“SOCs”) and trusted security intelligence from the X-Force research and development team.
8. **Intrusion Detection** – passive techniques which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Intrusion detection will alert when known bad activity is detected, but will make no attempt to block the actions.
9. **Intrusion Prevention** – techniques which monitor network traffic and system activity for the presence of malicious actions. Intrusion prevention will alert when known bad activity is detected, and will block this activity as defined by the protection agent policy.
10. **Security Content** – updated information, delivered in the form of X-Press Updates that provides the Agent with additional detection and blocking capabilities. A Security Content Update is designed to enhance the detection capabilities of the security product. These updates are published from time to time as new security vulnerabilities and threats are identified.
11. **Security Incident** – an event having the potential to cause damage to Customer environments by breaching the confidentiality, integrity, or availability of Customer systems.
 - Priority 1 Security Incident - require Customers to take immediate defensive actions. System compromise, worm infections, and massive denial-of-service (“DOS”) attacks are grouped into this classification.
 - Priority 2 Security Incident - require Customers to take action within 12-24 hours of notification from the SOC. Incidents such as unauthorized local scanning activity, unverifiable security events (e.g., security events with unknown impact), and attacks targeted at specific servers or workstations are grouped into this classification.
 - Priority 3 Security Incident – encompasses activity on a network or server that is not directly actionable. Discovery and vulnerability scanning, information gathering scripts, and other reconnaissance probes are grouped into this classification.
12. **Security Operations Center (“SOC”)** – a physical location where security data is centralized and network monitoring and analysis is performed. IBM manages a global network of SOCs which are securely connected and use redundant systems designed to ensure high availability.
13. **Service Level Agreements (“SLAs”)** – a contract between a network service provider and a customer that specifies, usually in measurable terms, what services the network service provider will furnish.
14. **Service Level Objectives (“SLOs”)** – performance characteristics relevant to the delivery of an overall service.

15. **Transmission Control Protocol (“TCP”)** – a set of rules (protocol) used along with the Internet Protocol (“IP”) to send data, in the form of message units, between computers over the Internet.
16. **Virtual Private Network (“VPN”)** – a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.
17. **X-Force® Protection System (“XPS”)** – serves as a data warehouse for event data from a variety of security devices, applications, and platforms.