JARGON BUSTER

The following provides a list of terms used within the delivery of Services. This list is not exhaustive but is designed to assist non-technical people in understanding terms used within the delivery of the Services.

Term	Description
ACH	Analysis of Competing Hypothesis
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
Attack	Attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset
Attack Surface	An attack surface is the total sum of vulnerabilities that can be exploited to carry out a security attack. Attack surfaces can be physical or digital. Both physical and digital attack surfaces should be limited in size to protect surfaces from anonymous, public access.
Attack Vector	A path or route used by the adversary to gain access to the target
Availability	The property of being accessible and usable upon demand by an authorised entity
Bayes' Theorem	Bayes' Theorem (alternatively Bayes' law or Bayes' rule) describes the probability of an event, based on prior knowledge of conditions that might be related to the event.
Cyber Threat Intelligence	According to CERT-UK, Cyber Threat Intelligence (CTI) is an "elusive" concept. CTI is based on the collection of intelligence using open-source intelligence (OSINT), social media intelligence (SOCMINT), human intelligence (HUMINT), technical intelligence or intelligence from the deep and dark web. CTI's key mission is to research and analyse trends and technical developments in three areas: • Cybercrime • Hacktivism • Cyberespionage (advanced persistent threat, APT or Cyber spying)
Decision Criteria	The thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result.
Decision Matrix Analysis	A method of analysing options as rows on a table, and the factors you needed as columns. Each option/factor combination is then scored, the score is then weighted by the relative importance of the factor, these scores are then added up to give an overall score for each option.
Decision Tree Analysis	A decision tree is a decision support tool that uses a tree-like model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility. It is one way to display an algorithm that only contains conditional control statements.
Event	The occurrence or change of a particular set of circumstances
Evidence	Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action. Evidence

The information contained within this document, or subsequently provided, whether verbally or in documentary form, is confidential to Maintel Europe Limited ("Maintel") and is provided to the organisation named within this document only. It shall not be published, disclosed or reproduced wholly or in part to any other party without our prior written consent. Maintel has made reasonable efforts to ensure the accuracy and validity of the information provided herein. Maintel should be notified of all requests for disclosure of Maintel supplied information under the Freedom of Information Act.

	does not necessarily prove the truth or existence of something but contributes to establishing proof.
Exploit	An Exploit is taking advantage of a weakness or a flaw in the system to intrude, attack it.
Impact	The result of an unwanted incident
Indicator	The measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs.
Information Security Event	The identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.
Information Security Incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Information Security Incident Management	The processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.
Integrity	The property of accuracy and completeness.
Investigation	The collection and analysis of evidence with the goal of identifying the perpetrator of an attack or unauthorised use or access.
Kipling	A form used to assist in the basic investigation of an incident so named after a quote from a Rudyard Kipling poem; I keep six honest serving-men (They taught me all I knew); Their names are What and Why and When and How and Where and Who.
Level of Risk	The magnitude of a risk expressed in terms of the combination of consequences and their likelihood
Likelihood	The chance of something happening
Mitigation	The limitation of any negative consequence of a particular event
Monitoring	Determining the status of a system, a process or an activity
Monitoring Policy	Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted.
OSINT	Open Source Intelligence (OSINT) is the collection and analysis of information that is gathered from public, or open, sources.
Penetration Test	A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might. In a penetration test, if a vulnerability is identified and an exploit exists for that vulnerability then the exploit will be used to gain access to the target device.
Phishing	A type of electronic mail attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering.

Probability	The extent to which an event is likely to occur.
Remediation	After vulnerabilities are identified and assessed, appropriate remediation can take place to mitigate or eliminate the vulnerability.
Risk	The effect of uncertainty on objectives.
Security Information and Event Management (SIEM)	Process in which network information is aggregated, sorted and correlated to detect suspicious activities.
Security Perimeter	A well-defined boundary within which security controls are enforced.
Target	Person or asset selected as the aim of an attack.
Threats	Threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organisation.
Threat Actor	A person who performs a cyber attack or causes an accident.
Threat Analysis	An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against enterprise assets
Timeline	The order in which events occur
TTP	Tactics, Techniques and Procedures
Vulnerability	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.
Vulnerability Assessment	Vulnerability assessment refers to the process of identifying risks and vulnerabilities in computer networks, systems, hardware, applications, and other parts of the IT ecosystem. Vulnerability assessments provide security teams and other stakeholders with the information they need to analyse and prioritise risks for potential remediation in the proper context. Vulnerability assessments are a critical component of the vulnerability management and IT risk management lifecycles, helping protect systems and data from unauthorised access and data breaches. The main difference between a Vulnerability Assessment and a Penetration Test is that the Vulnerability Assessment stops after the vulnerability has been identified. It does not run exploits to gain access to targets. As such the potential impact of a Vulnerability Assessment is less than that of a Penetration Test.

FURTHER DEFINITIONS ARE AVAILABLE FROM

https://www.bsigroup.com/en-GB/Cyber-Security/Glossary-of-cyber-security-terms/

https://www.isms.online/cyber-security/glossary-of-cyber-terms/

https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

https://m.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf