As an industry we use plenty of acronyms and jargon that mean it can be difficult for even seasoned professionals to keep up. This document aims to serve as a handy jargon-busting guide. Heard a phrase you didn't understand that's not in this document? Message us using the details at the bottom of this page so we can add it to later versions!

APT – *Advanced Persistent Threat (Group)*. Attacker groups who use sophisticated techniques, often aimed at high value targets to steal information mainly for commercial gain, competitive advantage or financial gain. This is also used by state actors to gain sensitive information about other governments. Typically, they do this stealthily and with extreme patience, sitting on a network for months or even longer before they plan to exfiltrate any information.

Attack surface – the range of different ways in which an attacker would get into your environment. Keeping this as small as possible is a basic starting point for any cyber strategy. Actors will look for the weak points into an environment which expose something that they are looking for. This could be a weak web server, unsecure end user devices or a vulnerability in a commonly used bit of technology. Typically, the weakest entry point into a network that can be overtly used.

Attack vector – (also called threat vector), the specific route or method for an attacker to gain access into a network. This is what is used once the attack surface is understood by an attacker.

Blue team – the defensive side of cyber security – a team responsible for building and maintaining cyber security defences against attackers. This includes but isn't limited to detection and response tools and processes.

BEC – *Business Email Compromise*. A type of social engineering designed to trick a victim into performing a specific action by pretending to be a senior member of an organisation, often a CEO or CFO. The most common objectives are to get the finance team to transfer money to the attackers or for admins to provide credentials or personal information.

Credential stuffing – an unsophisticated, but effective technique whereby attackers attempt to login to accounts en masse using a large database of usernames and passwords, often bought off the back of a data breach from the Dark Web. The effectiveness comes from the fact that many people will use the same email and password for multiple accounts; if the original account breached didn't have useful information in it, it's likely another account will (e.g. payment card details).

Cyber Essentials – an NCSC certification primarily aimed at smaller businesses and schools that helps organisations master the basics of cyber security to protect against the most common cyber-attacks. Cyber Essentials is self-certified, with technical verification to be certified to 'Cyber Essentials Plus'.

Cyber maturity – how well cyber security is ingrained into an organisation, covering technical security, processes, people (and culture), supply chains and more. Improving your cyber maturity puts you on a programme of continuous improvement, focusing on incremental gains rather than big purchases that claim to fix everything.

(D)DoS – *(Distributed) Denial of Service*. An attack with the objective of overloading a server or web application to interrupt services. They can be used in a number of ways, most commonly by hacktivists looking to cause disruption to a target organisation or as part of a ransomware attack aimed at causing the most possible interruption to service to force an early payment to restore

systems. DDOS types of attacks can also expose the vulnerabilities in a network that aim to show service outages to organisations, but the real intent is to expose other attack vectors into an environment to enable the theft of data or to implant a piece of malware to start a long-term attack.

DPI – *Deep Packet Inspection*. Each packet that passes across a network has a wealth of information within it, from source and destination to user information and even payload information that can be recreated to understand what messages are being sent. Examining the full detail of data packets as they pass through a monitored tool provides additional visibility over standard log collection. In some circumstances, unless specific tools are used, then encrypted data generally cannot be inspected. Using DPI is probably the quickest way to analyse real-time threats in a network using threat intelligence and can monitor data on the fly.

EDR – *Endpoint Detection and Response*. Focuses on protecting endpoints (devices, servers, printers etc.) Analysis threats and signals from these endpoints and may automatically block or send to analysts for further review. Think a more comprehensive and adaptable Anti-Virus solution that can in most cases provide a remedial action to a vulnerable endpoint.

Encryption – effectively converts a string of data (e.g. a message) into an unreadable format, often during transit or storage, with the intended recipient (device or account) having the digital 'key' to read it. In theory this means that anyone accessing the data without the 'key' cannot read it.

False positive – specifically relating to a SOC function, a false positive refers to an alert that could, in theory, be an indicator of an attack, but turns out to be legitimate (e.g. a home worker logging in from a new device or having moved house and changed IP address). Too many false positives can be a big issue for analysts as they cannot close them without investigation, but while dealing with them could be missing real threats.

Hacktivist – using computer-based methods to make a political point. Can be through a number of methods, such as hacking an organisation opposed to their beliefs, through a DDoS attack or through website defacements (hacking the web server to put a new message on the target organisation's webpage). Whilst often not after financial gain, can cause brand damage to organisations.

IDS – *Intrusion Detection System*. Analyses network traffic for signatures that match known threats.

IOC – *Indicator of Compromise*. Anything that could suggest a potentially malicious activity, often gathered through logs or network traffic. Often used together by analysts to build a picture of an overall attack and identify the appropriate next steps.

IPS – *Intrusion Prevention System*. Analyses traffic like an IDS, but can also prevent that packet from being delivered based on the kind of attack it detects.

ITSM – *Information Technology (IT) Service Management*. Specifically talking about an ITSM system, this is the tool that allows IT teams to follow the pre-agreed practices, processes and workflows to make changes to IT environments. Integrating your security team with an ITSM system will allow a central place for tickets and changes, reducing time to respond and duplication of tickets.

MDR[i] – *Managed Detection and Response*. A service that combines EDR and NDR, often with some elements of an analyst team to provide a broader level of security.

MFA – *Multi-Factor Authentication* (also used synonymously with 2FA). Is a way of making accounts more secure, by setting up a trusted second (or more) mode of verification, beyond a standard password or set of biometrics that is needed to log in, change passwords and more. The most common MFA tools are via a mobile phone app or phone number, which shares a code with the user to input into the tool they're trying to access.

MITRE ATT&CK – an open-source and globally used framework that stores the known tactics, techniques and procedures (TTPs) used by adversaries. https://attack.mitre.org/

MSP – *Managed Service Provider*. An organisation that manages the IT estate of others as part of an outsourced service. Includes the set up and management of networks (on-premise and cloud) and everything that is entailed, including end-user devices, printers, broadband etc. Often MSPs will provide some services of MSSPs (or even be both), such as managing firewalls and AV as a minimum.

MSSP – *Managed Security Service Provider*. Manages and monitors security devices, tools and systems as part of an outsourced service. Whilst services focused on vary, commonly an MSSP may be expected to provide managed firewalls, IDS, AV, VPNs and vulnerability scanning. Some MSSP's will also be MSP's and SOC providers, but they may choose to partner with other organisations who specialise in these capabilities.

Nation state – (as a phrase) can be preceded by threats, hackers or attacks and refer to an attack on critical national infrastructure (CNI), governments, military or other important businesses. Often difficult to identify the true perpetrators as governments will naturally pass on the blame to other organisations (who may have acted on their behalf or of their own behalf). Is increasingly becoming a modern form of warfare and a hot topic for world leaders to discuss in diplomatic meetings.

NDR[i] – *Network Detection and Response*. Monitors the network of an organisation for anomalous behaviour based on a known benchmark. Alerts security teams of suspicious behaviour for action.

Phishing – a method with the primary objective of getting credentials for a user in an organisation, installing malware onto a device or network or directly collecting money from individuals. Usually uses email, texts of phone calls and can be highly targeted and sophisticated (spear-phishing) or very generic. Phishing is the most common route into an organisation for attackers and can be a one-off attack or part of a larger ransomware campaign.

Playbook – the processes a SOC team will go through based on the use case they are presented with. Also called runbooks

POLP – *Principle of Least Privilege*. Quite simply, giving people in the organisation access to as little as is possible and for the shortest time possible for them to still run their jobs effectively. The aim is to reduce the admin accounts and other access that may be used by or a target for attackers, reducing the attack surface available.

Purple team – a relatively new (and arguably pointless)[ii] term the refers to red and blue teams working closely together to provide ongoing feedback and transferring knowledge.

Red team – the offensive side of cyber security, red teams look to break into networks in pre-agreed tests (although, for example a SOC team will likely not be informed to test certain elements). The findings form work for 'blue teams' to do to improve the network security. Common terms for red teams are 'ethical hackers' or penetration (pen) testers.

Script kiddie – a derogatory term for a relatively unskilled person who attempts to hack networks and websites using basic scripting and programmes. Whilst they may not present much of a threat to organisations from a data theft perspective, simply defacing the company's website can cause brand damage and so shouldn't be ignored as a threat.

SIEM – *Security Information Event Management*. Most commonly known as a multi-use tool used by security teams to correlate data, alerts and events across multiple systems using logs and other sources. Often used as the dashboard for security teams to work from when monitoring a network. It can be forgotten that SIEM is actually a process which defines the management of security event

information and the terminology has been widely adopted as a technology by the security industry, but it is important not to forget that there is a process that has to manage and tune the technology.

SOAR – *Security Orchestration, Automation and Response*. Allows organisations to collect information and data about security threats and automatically respond, without the need for human intervention. Often used alongside (or integrated into) a SIEM technology and other tools to reduce the basic 'alert bashing' for a security team, to free up human resource for more complex analysis and decision making. The definitions on when a remedial action can happen versus when human intervention should review can be the hardest blocker to adopting SOAR technologies as nobody wants to be responsible for quarantining the "CEOs laptop" at 10pm.

SOC[i] – *Security Operations Centre*. Will take on a range of tasks covering all the detection & response acronyms. A true SOC should add people and processes to XDR to provide full coverage and build out playbooks for response.

Threat Intel – any information available about threats and threat actors that can be used to reduce the success of attacks by strengthening defences or building use cases and playbooks around them. Threat Intel can be gained from a number of sources through commercial organisations, open sources, governments, industry specific intelligence and even through organisations that trawl the dark web looking for specific indicators associated with organisations. This information is all compiled into Indicators of Compromises that can be used to automatically search the large amounts of log information and network traffic looking for potential compromises.

TTPs – *Tactics, Techniques & Procedures*. The activities, tools or methods used by a specific threat actor (or group of) to reach their goals. Understanding these can build out use cases and playbooks should key triggers and trends be spotted in a network as well as help to prioritise investment in defences based on an organisation's potential threat.

Use case – a scenario and an associated set of rules that trigger to a specific event that happens in an IT environment that may require SOC action and will have an associated playbook (or more) attached to it based on a set of known truths.

XDR[i] – *eXtended Detection and Response*. Adds to other detection and response (EDR, MDR, etc) with a SIEM and SOAR functionality – This is what a lot of organisations refer to when they talk about their SOC.

Zero-day – a vulnerability that has only just been discovered by the vendor (or by threat hunting groups), meaning they've had zero days to patch it. If a threat actor becomes aware of them, they normally will not exploit them for a longer period of time in order to go undetected on a network and plan their attack – even if the exploit is patched, they will still be in the network by that point.

Zero trust – the concept of IT management that states that devices on a network should not be trusted by default, even if they have previously been verified, effectively requiring devices and credentials to re-certify themselves each time they are used. Zero trust is most commonly used in privilege management for admin types of roles or within the supply chain of an organisation.

---

[i] N.B. NDR, MDR, XDR and SOC can often be used interchangeably and can be accused of being marketing spin for what are essentially part of the same continuum of services.

[ii] Pointless because 'purple teaming' is what should be happening with red & blue teams anyway – if a red team exercise is not informing blue team defence improvements then there's little point in running it.