Incident Response Glossary

This document is designed to cover all acronyms used in the Incident Response domain of the Blue Team Level 1 certification training course.

This document is TLP:White, and can be shared without breaching the Terms and Conditions of the BTL1 course.

Learn more about Blue Team Level 1 and purchase the certification here – https://securityblue.team/why-btl1/

CERT // Computer Emergency Response Team – A team that are responsible for responding to computer security incidents. Most governments have their own CERTs responsible for security research and defense.

CSIRT // Computer Security Incident Response Team – Another name used to describe teams that respond to security related incidents, consisting of security, IT, and other personnel from important business departments such as; legal, communications, human resources.

IRP // Incident Response Plan – An incident response plan is a set of instructions to help IT staff detect, respond to, and recover from network security incidents. These types of plans address issues like cybercrime, data loss, and service outages that threaten daily work.

IOC // Indicator of Compromise – Intelligence gathered from malicious activity, intrusions, or incidents. An example would be a piece of malware that was observed in an attack against an organization. The file hashes and file name can be shared with other organizations so they can add it to blocklists or perform threat exposure checks.

TTP // Tools, Techniques, and Procedures – MITRE have defined over 240 unique tactics used by adversaries, known as TTPs. You can find them here, each with detailed descriptions, and the threat actors that have been known to use them.

DMZ // Demilitarized Zone – is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet.

EDR // Endpoint Detection and Response – An EDR solution is typically an analysis platform with software agents that run on endpoints, continuously sending information to the EDR server for correlation, detecting anomalies and security events. EDRs can be configured to take automatic actions, such as stopping network connections and generate alerts for security analysts to investigate.

AV // Antivirus Solution – A security solutions installed on endpoints such as laptops and desktops that detects and removes the presence of malicious software using signature matching, or anomaly-based detection.

ISAC // Information Sharing and Analysis Center – A collective of organizations, typically operating in the same industries, that share actionable and strategic intelligence surrounding cyber-attacks with the goal of improving each other's defenses and ability to respond to security events and incidents.

IDS/IPS/IDPS // Intrusion Detection and Prevention System – Typically systems will have either Intrusion Detection functionality, reporting on unusual or suspicious activity by generating alerts and logs, or Intrusion Prevention functionality, working to autonomously stop attempts without needing to wait for human intervention.

HIDS // Host Intrusion Detection System – an IDS working specifically on an endpoint such as a laptop or desktop, that generates alerts when suspicious or malicious activity is detected.

HIPS // Host Intrusion Prevention System – an IPS working specifically on an endpoint such as a laptop or desktop, that can take automated actions when suspicious or malicious activity is detected.

NIDS // Network Intrusion Detection System – an IDS that monitors network traffic, that generates alerts when suspicious or malicious activity is detected.

NIPS // Network Intrusion Prevention System – an IPS working specifically to detect and respond to suspicious or malicious network traffic, completing actions such as blocking or resetting connections.

FW // Firewall – A software or hardware device that uses rules to allow or restrict traffic passing through the firewall. Software versions on endpoints can be known as local firewalls, and software firewalls on internet-facing servers can be known as Web Application Firewalls (WAFs).

NGFW // Next-Generation Firewall – Combines a traditional firewall with other network device filtering functions, such as an application firewall using in-line deep packet inspection, and an intrusion prevention system.

SIEM // Security Information and Event Management – Logs are sent to a centralized location to provide analysts the ability to perform real-time analysis of security alerts generated by applications and network hardware.

GPO // Group Policy Object – are collections of Group Policy settings that defines what actions a system or user group can perform, limiting the potential for malicious harm by reducing permissions and rights available to users.

PCAP // Packet Capture – A file that contains stored information of network traffic that has

Sysmon // System Monitor – can be used as an extensive ruleset for providing relevant data to security operation centers, defenders and threat hunters. Think of it as a more detailed version of Windows Event logs.