Glossary

[Dive into the world of cybersecurity incident detection and response.]

- **AD:** Abbreviation for Active Directory, a directory solution from Microsoft.
- **Directory:** A network component containing identities of different people, including passwords. It is responsible for authentication, verifying the identity of various users.
- **ANSSI:** Abbreviation for the National Agency for Information System Security. It is the administration in charge of supervising and promoting civil cybersecurity in France.
- **CERT:** Abbreviation for "Cyber Emergency Response Team," a security team specialized in incident response during emergencies and in monitoring vulnerabilities.
- **CNIL:** National Commission for Information Technology and Civil Liberties. This is the French administration responsible for ensuring digital privacy.
- **CSIRT:** Abbreviation for "Computer Security Incident Response Team," a security team dedicated to handling incidents.
- **CTI:** Abbreviation for "Cyber Threat Intelligence," which refers to the domain of cybersecurity focused on understanding threats and threat actors.
- **DSI:** Abbreviation for "Information Systems Directorate," the department within an organization responsible for managing all IT systems.
- **EDR:** Abbreviation for "Endpoint Detection and Response," a security tool installed on SI computers that detects suspicious activities through behavioral analysis and enables response measures on the machines.

- **EPP*:** Abbreviation for "Endpoint Protection Platform," a security tool located on SI computers that detects suspicious events through malware detection or behavioral analysis (often colloquially referred to as an antivirus).
- **Event ID:** A field in Windows event logs consisting of a number that references the type of event (login, scheduled task execution, etc.).
- **FP:** Abbreviation for "false positive," a detected security incident that is actually a false alarm.
- **FSN:** Abbreviation for Digital Service Provider.
- Hash (or imprint or condensate): A mathematical imprint of a piece of information, such as a file.
- **IDS (IPS):** Abbreviation for "Intrusion Detection System," a tool positioned in the network used to detect signs of attacks at the network protocol level.
- **IDS (IPS):** Abbreviation for "Intrusion Protection System," a security tool installed in front of servers to protect them by blocking attack traces at the network protocol level.
- **IOC:** Abbreviation for "indicators of compromise," traces left by a specific attacker. These may include an IP address, domain name, file imprint, or file name.
- **IP:** Abbreviation for Internet Protocol, a network protocol that allows two machines to communicate and is used as a fundamental building block of all modern networks.
- **Logs:** Files containing traces of events that occurred on a given system.
- **MDR:** Abbreviation for "Managed Detection and Response," a service that detects incidents and implements incident response measures.
- **MFA:** Multi-factor authentication (or 2FA for two-factor), an authentication method based on multiple factors. These can include knowledge of information like a password, possession of an object like a phone or USB key, or proof of physical state like fingerprints or facial recognition. Strong authentication refers to when multiple types of factors are combined.

- **MTTD:** Abbreviation for "Mean Time to Detect," the average time between the start of a confirmed security incident and the creation of the associated alert in the SOAR system.
- **MTTR:** Abbreviation for "Mean Time to Recovery," the average response time, meaning the time between the start of a confirmed security incident and the closure of the incident.
- **NDR:** Abbreviation for "Network Detection and Response," a security tool placed on the network that detects suspicious events based on behavior and allows incident response measures at the network level.
- **OIV:** Abbreviation for Operator of Vital Importance, an organization that manages an information system (SI) identified as highly critical on a national level by ANSSI.
- **OSE:** Abbreviation for Operator of Essential Service, an organization that manages a system identified as critical under European law.
- **Firewall:** A network device that blocks traffic from one port or IP address to another. A firewall de facto defines the networks at layer 4 of the OSI model.
- **Patchsplaining:** (neologism) A condescending attitude adopted by a security operator who does not listen to the needs and difficulties encountered by a user in the field.
- Patient Zero: The first system compromised in an incident, which is the origin of the chain of compromise.
- **PIR:** Abbreviation for "Post-Incident Review," a retrospective moment to reflect on a past incident to learn lessons from it.
- **Proxy (or proxy server):** A relay between a device and a web server, allowing traffic to be measured, filtered, or modified.
- **Purple Team:** A type of security audit aimed at challenging security teams by simulating a realistic attack while collaborating to help them improve.
- **Red Team:** A type of security audit designed to test the ability of a simulated attacker to achieve a specific objective.
- **RSSI:** Abbreviation for "Information Systems Security Manager," the person responsible for the security of an organization and the security teams.
- **Sandbox:** A program execution environment dedicated to testing and analyzing.
- **SI:** Abbreviation for Information System, referring to the entire set of digital tools necessary for an organization to function, such as computers, users, accounts, and software.

- **SIEM:** Abbreviation for "Security Information and Event Management," a tool for visualizing and analyzing security data.
- **SIGMA:** A rule syntax for detecting events in a specific type of log.
- **SIRP:** Abbreviation for "Security Incident Response Platform," a communication tool that acts as an interface with other teams within the organization to report on incidents.
- **SOAR:** Abbreviation for "Security Orchestration, Automation, and Response," a tool that manages alerts, investigations, incidents, and automates detection and response processes. It generally serves as an information-sharing interface within incident detection and response teams.
- **SOC:** Abbreviation for "Security Operations Center," a team responsible for supervising, detecting, and responding to security incidents within a given perimeter.
- **Tier 0:** To protect the organization, different zones of the information system are differentiated based on their criticality. Tier 2 is the zone containing workstations and users, Tier 1 is more critical, containing servers, applications, business administration accounts, and service accounts. Tier 0 is the most critical zone, containing the directory, directory administrators, and services that could compromise the entire SI, such as DNS or antivirus.
- **TTP**: Abbreviation for Tactics, Techniques, and Procedures, referring to the elements of the MITRE ATT&CK matrix, used to characterize a cyberattack.
- **VPN:** Abbreviation for "Virtual Private Network," which acts as a relay for all connections to a VPN server located in a distant network.
- **WAF:** Abbreviation for "Web Application Firewall," which detects and blocks known attack traces within the content of web requests.
- **Write-blocker:** A system that blocks writing to a storage medium to preserve the integrity of evidence in a digital investigation.
- **XDR:** Abbreviation for "Extended Detection and Response," a security tool that detects suspicious events based on behavior at the application and network levels and allows incident response measures at both the network and application levels.
- **YARA:** A rule syntax used to identify malicious files based on static characteristics.