Activity 10.3: Security Architecture Terminology

1. Heuristics: A technique used to find previously unknown malware by observing behaviors common to malicious software
2. DMARC: An email authentication, policy, and reporting protocol
3. Reverse engineering: The process of disassembling or decompiling a malware package to understand what it does
4. Digital signature: A means of providing assurance that an email has not been modified and that it was sent by the correct sender that relies on a certificate and public key cryptography
5. UEBA: A technology designed to monitor end user behavior to prevent targeted attacks and insider threats
6. DKIM: An email authentication method designed to detect forged sender addresses
7. SOAR: A technique used to find previously unknown malware by observing behaviors common to malicious software.
8. SPF: An email authentication technique that detects forged sender addresses.