Glossary terms

Terms and definitions

Advanced persistent threat (APT): An instance when a threat actor maintains unauthorized access to a system for an extended period of time

Attack surface: All the potential vulnerabilities that a threat actor could exploit

Attack tree: A diagram that maps threats to assets

Attack vector: The pathways attackers use to penetrate security defenses

Bug bounty: Programs that encourage freelance hackers to find and report vulnerabilities

Common Vulnerabilities and Exposures (CVE®) list: An openly accessible dictionary of known vulnerabilities and exposures

Common Vulnerability Scoring System (CVSS): A measurement system that scores the severity of a vulnerability

CVE Numbering Authority (CNA): An organization that volunteers to analyze and distribute information on eligible CVEs

Defense in depth: A layered approach to vulnerability management that reduces risk

Exploit: A way of taking advantage of a vulnerability

Exposure: A mistake that can be exploited by a threat

Hacker: Any person who uses computers to gain access to computer systems, networks, or data

MITRE: A collection of non-profit research and development centers

Security hardening: The process of strengthening a system to reduce its vulnerability and attack surface

Threat actor: Any person or group who presents a security risk

Vulnerability: A weakness that can be exploited by a threat

Vulnerability assessment: The internal review process of a company’s security systems

Vulnerability management: The process of finding and patching vulnerabilities

Vulnerability scanner: Software that automatically compares existing common vulnerabilities and exposures against the technologies on the network

Zero-day: An exploit that was previously unknown