

eccouncil.org — Certification

* Career Paths

- CEH → Pen Tester / Red Team
- Risk → Risk Analyst
- IS Governance → Policies / Compliance
- SOC → Monitoring / Incident Response
- Forensics → Investigation / Evidence

* Antivirus

Detect, Prevent, Remove Malware

- Signature based → Known threats
- Heuristic/Behavior → Unknown

* Zero-Day Attack

- New vulnerability
 - No patch available
 - Vendor unaware
- 0 days to fix

* Free vs Paid Antivirus

- Free → Basic protection, limited updates and features
- Paid → Frequent updates, real time protection, ransomware protection, firewall, enterprise management.

* 3rd Party Vendors

Cisco, Kaspersky, McAfee, Symantec, Bit defender, ESEC

* CIA Triad

- Confidentiality (Encryption)
- Integrity (Hashing)
- Availability (No down time)

Authenticity (genuine identity)

Non-repudiation (cant deny action)

Access control (authorized access only)

