

# GLOSSARY

## Cybersecurity Foundations

With Malcolm Shore

Use these terms and definitions below to understand concepts taught in the course.

**Transcript Search:** note that you can search for terms directly within the course. To search video text, switch to the *Transcripts* tab, then press Cmd/Ctrl + F on your keyboard to run a search within the active transcript.

Term	Definition
APTs	Advanced Persistent Threats; Malware directed at political and military targets that can persist over a long period of time
COBIT	Control Objectives for Information Technologies; A framework ensuring enterprises have an effective and auditable set of governance and management processes for IT that deliver value for their stakeholders
cyber kill chain	Views an attack in seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action
NIST Cybersecurity Framework	An action-oriented approach to security that consists of three elements: the Framework Core, the Framework Profile, and the Framework Implementation Tiers
ransomware	A form of malware that encrypts files or storage systems on its target to lock out the legitimate owner, and then demands payment for the decryption key
rootkit	A form of malware often located in the operating system's kernel, and designed to hide, operate, and carry out its mission using normal system functions