Enterprise Security Fundamentals

Instructor : Cristian Calinescu

Microsoft MTA, MCSA and MCSE certified
Microsoft Cybersecurity Proffesional certified
Comptia Security + certified

Restrict Lateral Movement
Overview

Techniques you can use to restrict lateral movement

- ✓ **Code Integrity Policies**

Code Integrity Policies

- Old version: Applocker and Software Restriction Policies
- Windows Defender Device Guard
- Only allow specifically whitelisted code to run
- If the application/code isn't pre-approved, it isn't allowed to run
- Improve security posture of servers
- Simpler to configure on servers as fewer scripts and applications need to be whitelisted compared to workstations

Restrict Lateral Movement
Overview

Techniques you can use to restrict lateral movement

- ✓ **Code Integrity Policies**
- ✓ **Network Segmentation**
- ✓ **No common accounts or passwords**
- ✓ **Logon script sanitation**
- ✓ **Apply software updates and patches**