Enterprise Security Fundamentals

Instructor : Cristian Calinescu

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

Blue Team Kill Chain
Overview

Most common objectives

- ✓**Gather baseline data**
- ✓**Detect**
- ✓**Alert**
- ✓**Investigate**
- ✓**Plan a response**
- ✓**Execute**

Blue Team Kill Chain

Overview

- ✓Gather baseline data
- ✓Detect
- ✓Alert
- ✓Investigate
- ✓Plan a response

Measured Response

- Plan and execute a response
- Don’t play “Whack a mole” with the intruder
- Real intruders are likely to have been present for some time before detection
- They have likely built in fail safe strategies to retain access if discovered
- The first time the intruder is aware that they have been detected, should be after they have been ejected
- If they are aware their activity is detected, they may institute countermeasures

Blue Team Kill Chain
Overview

✓Gather baseline data

✓Detect

✓Alert

✓Investigate

✓Plan a response

✓Execute

Blue Team Post Mortem

After Red team attack, Blue Team should:

- Determine why vulnerabilities the Red Team exploited were present
- Determine what the Blue Team could have done better
- Where are the detection mechanisms lacking