

Class activity

Dean offers threats

Students propose controls (adv. students categorize)

Dean summarizes / critiques

REPEAT per domain



WHY THREATS & CONTROLS?

Exam requires 30–40% application

This is how we build application skill

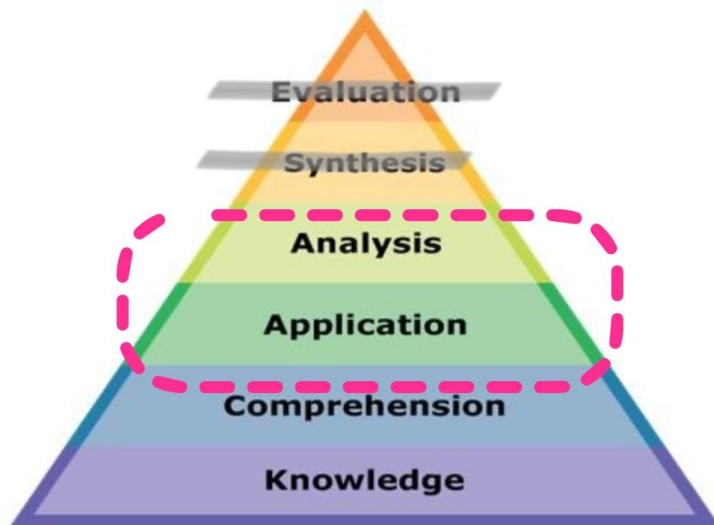
You must recognize

- Synonyms

- Core controls & threats

Required inputs

- CISSP definitions 90–95%



THREATS IN CONTEXT = EXAM QUESTION



What asset is attacker attacking?

What tool are they using?

What weakness is present?

What attribute is attacker attacking?

What domain is attacker attacking?

If you cannot tell the above

Look at options– try to categorize them



00 PRACTICE MY THREATS – STUDENT CONTROL



#	Threat	Control
1	Flooded cellar full of piranha fish	Thick boots /drain/ cage/ run away
2	Faulty parachute	Backup parachute
3	Lion	Cage/
4	Dragon	pokemon ball
5	Helicopter	
6	Bad Training	Quiz & Test / get another trainer TTT
7	Loaded gun in Keanu Reeves hands	Popcorn /trench coat



01 PRACTICE TECHNICAL THREATS – STUDENT CONTROL



#	Threat	Control
1	Brute Force	
2	O.S. Fingerprinting	
3	Audit Finding	
4	War driving	
5	Fire	
6	Fraud	
7	Vandalism	



Only if you are consistently correct at control

Categorize YOUR control

Prevent

Detect

Recover

Deter

Correct

Direct

THREATS AND CONTROLS – WHERE IS THIS FROM?



Hal Tipton (RIP) is the father of the CISSP.

Hal & I had a discussion about the exam and how it was built.

Dean made this game.

Major document is hidden

<http://www.blacksheepnetworks.com/security/info/misc/handbook/003-006.html#H>

