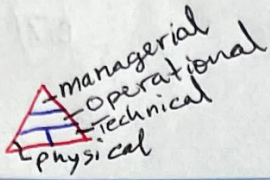
Willian Prado
07/01/2025
Sec+



Security

Cathegory	Type
Managerial	preventive
Operational	detective
Technical	Corrective
Physical	Directive
Administrative	Deterrent
	Compensating
	Physical (sec+ verb)

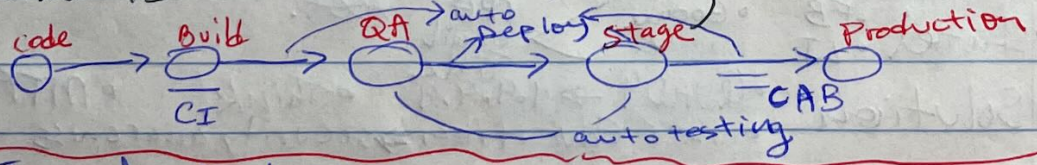
CISO
Security Policy
SOC
Dev Ops
Dev Sec Ops
CICS

Continuous Integration (CI) - Catch bugs early & ensure that new code integrates smoothly w/ the existing codebase.

Continuous Delivery (CD) - ensure that software is always in a deployable state.

IBM
YTB- What is continuous integration?
- always watching the code, build, test it.

YTB- What is continuous delivery?



Topic 2A Threat Actors

vulnerability weakness in a system.
threat - potential harmful event, intention or unintentio
likelihood probability/chance
impact money $$ value placed on threat
risk likelihood & impact of threat exploiting vulnerability
vulnerability + threat = risk (Impact * Likelihood)

YTB- Types of actors & their motives

William Prado
07/01/2025

HWK. Guy Fawkes

YTB - Attack Surface vs. Attack Vector.

Client-based agent - sftw install + run on each host + reports back to mgt server

agentless - host does not contain sftw

Message-based vectors.
- email, • short message Service (SMS)
- Instant messaging (IM) • Web + social media
- voice calls.

Social Engineer.
- Greed • Fear

Compromise
- Creps, • Cntrl, • IP

- Intel • FB • LI • Google > ~~ORG~~ email Title ~~Asst.~~
- Solution • QUAD9 → 9.9.9.9 • Think! • ~~MFA~~
  • User Education ⇒ security awareness training

RAT - remote access trojan
MFA - multifactor Authentication

Water hole attacker

Advanced persistent threat - is a stealthy, prolonged cyberattack in which an intruder gains unauthorized access to a network + remains undetected for an extended period.