UNIVERSITÄTS BIBLIOTHEK FRANKFURT AM MAIN

CI/CD/CDon't?

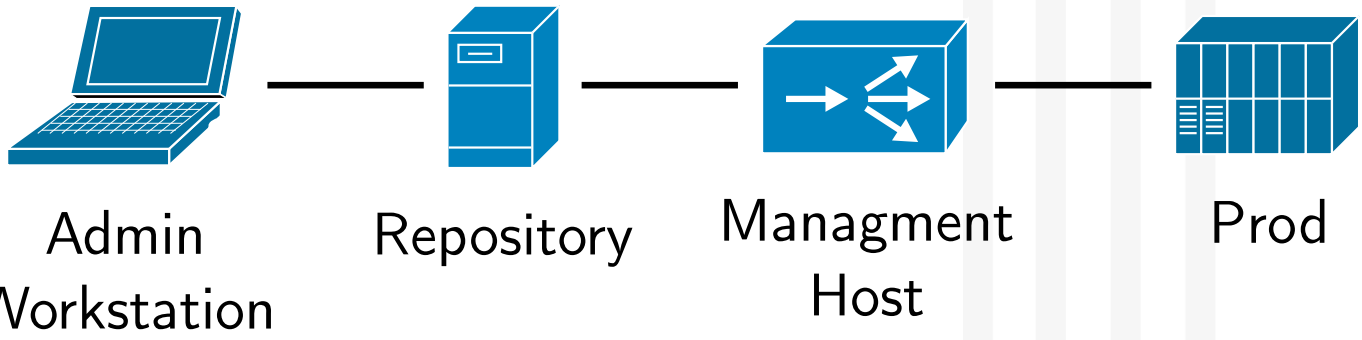
Deliberations on the threat model of continuous delivery systems

Jens Heinrich

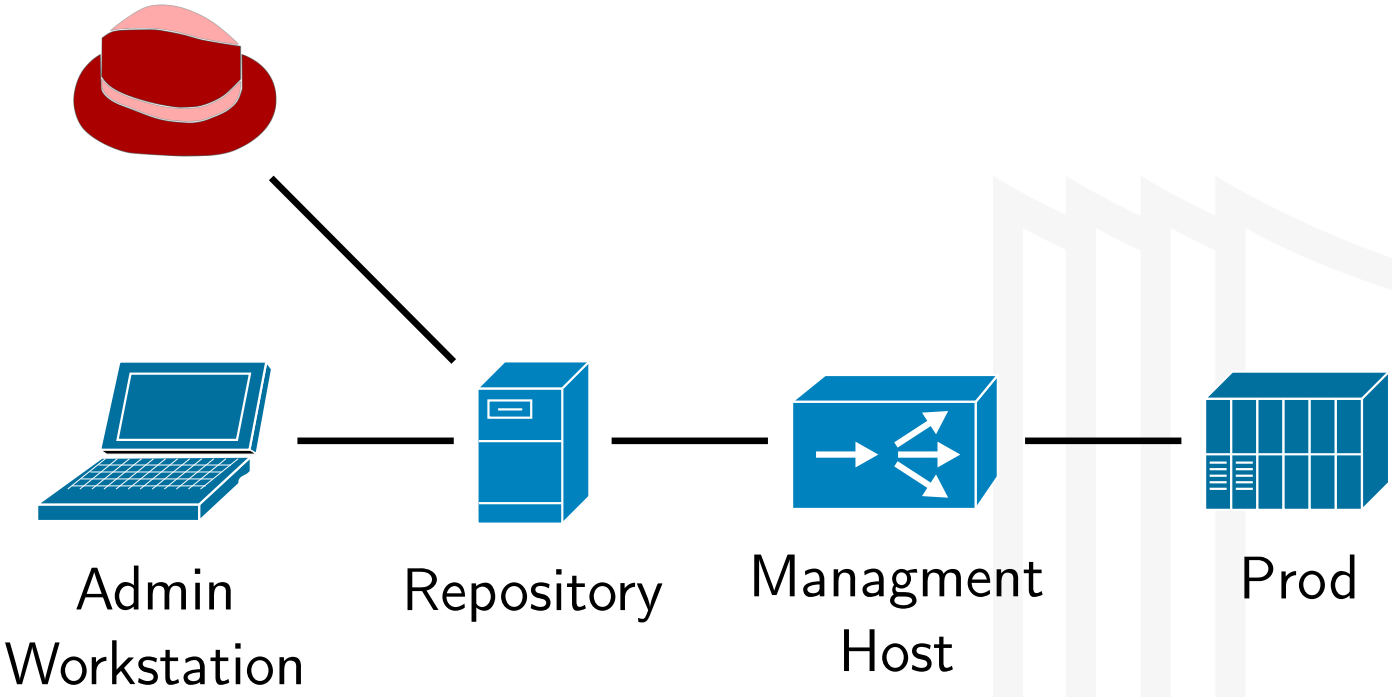
Universitätsbibliothek Johann Christian Senckenberg

2020–03–14/15
CiderSecurityCon

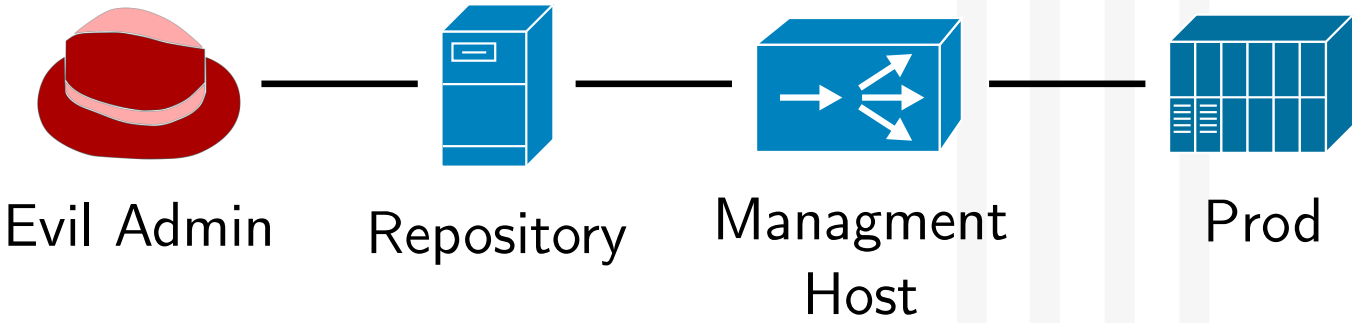
Concept



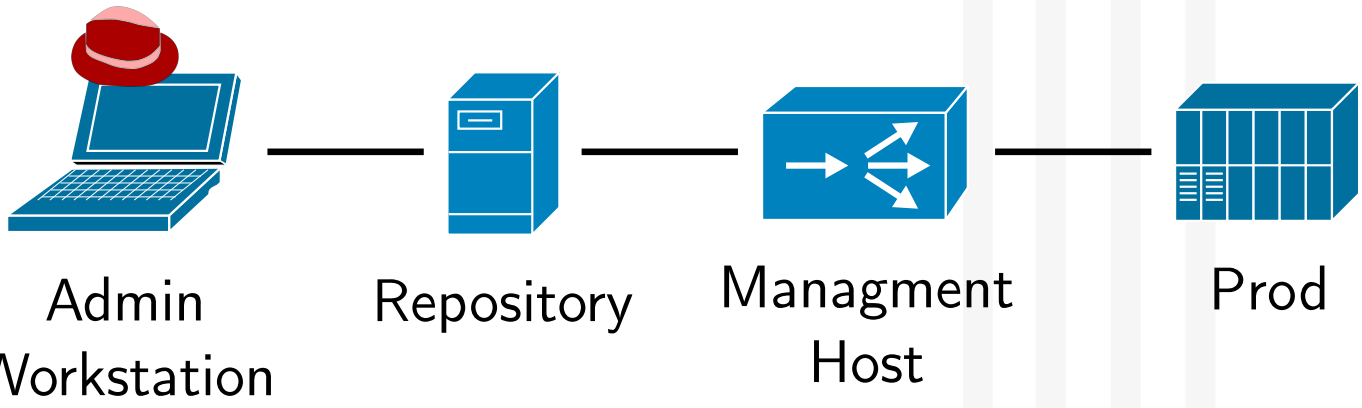
Attackvectors-Impersonation



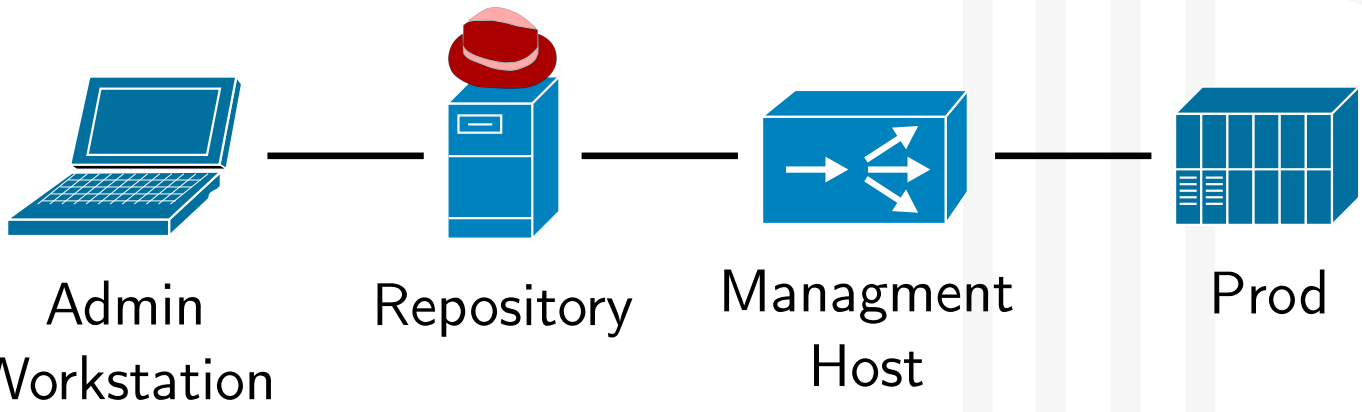
Attackvectors-Evil Admin



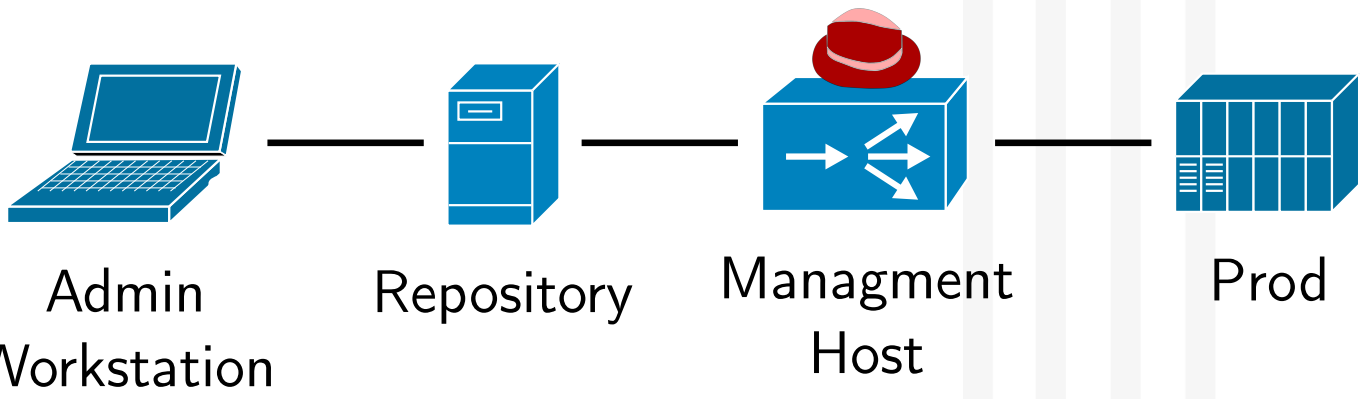
Attackvectors-Compromised Workstation



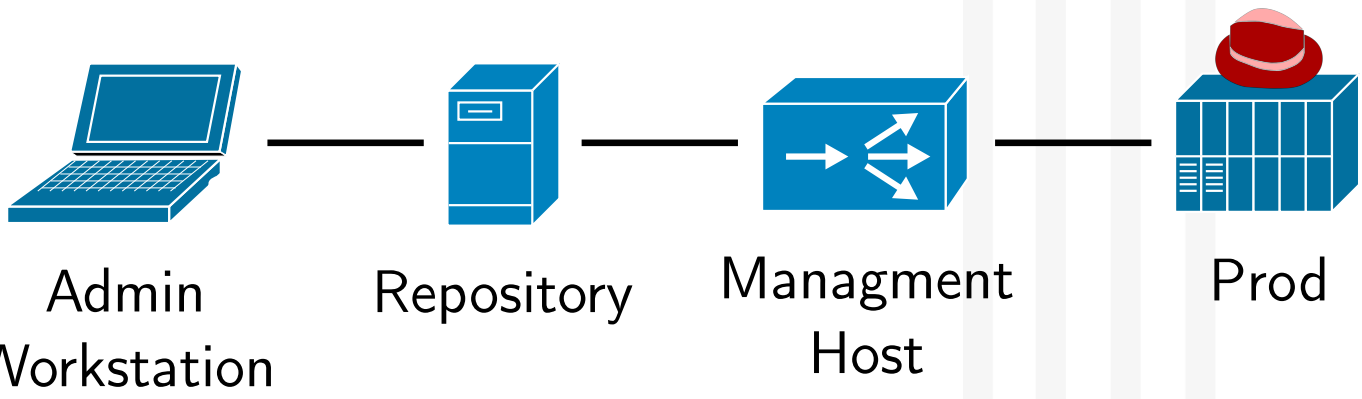
Attackvectors-Compromised Repository



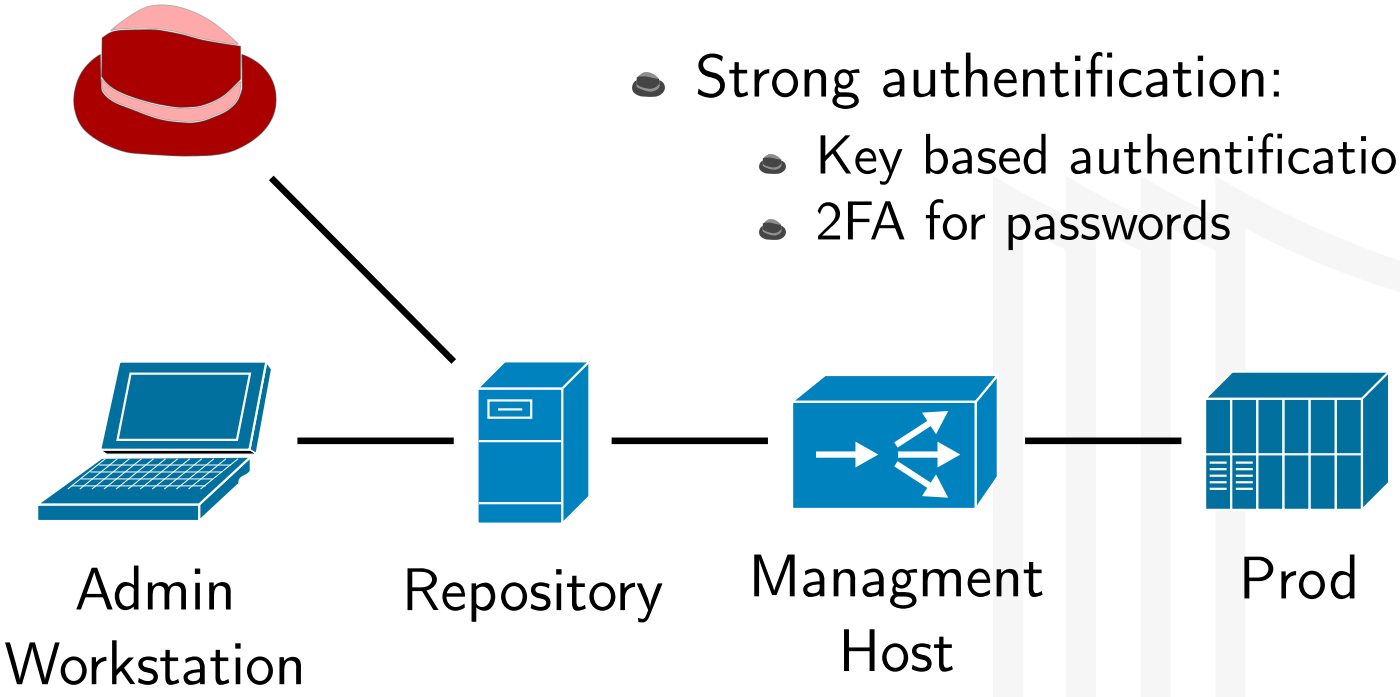
Attackvectors-Compromised Managment Host



Attackvectors-Compromised Prod



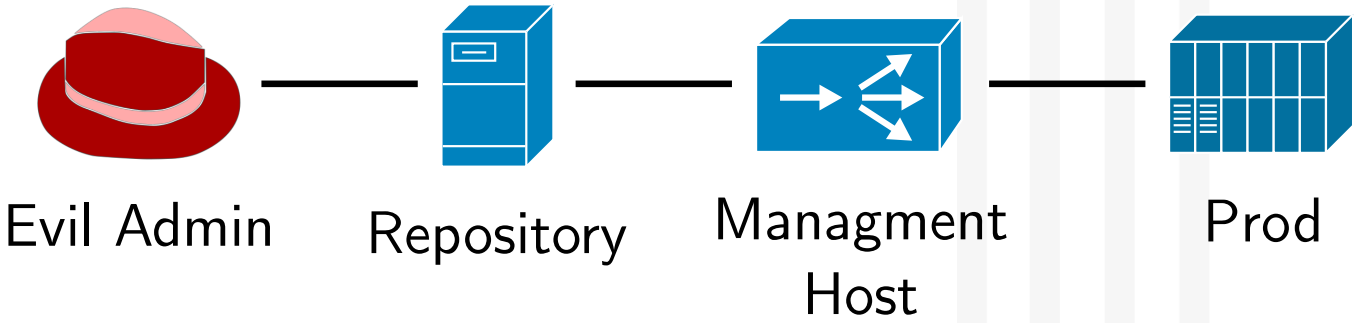
Mitigations-Impersonation



- Strong authentification:
  - Key based authentification
  - 2FA for passwords

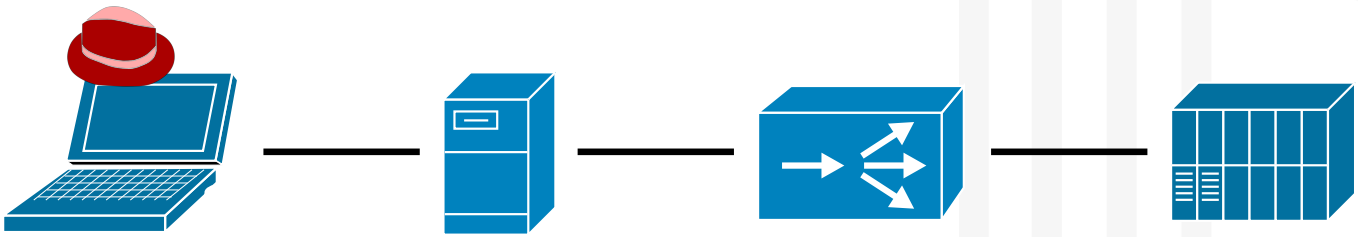
Mitigations-Evil Admin

- Privilege Separation:
  - 2-man-rule
  - enforced tests



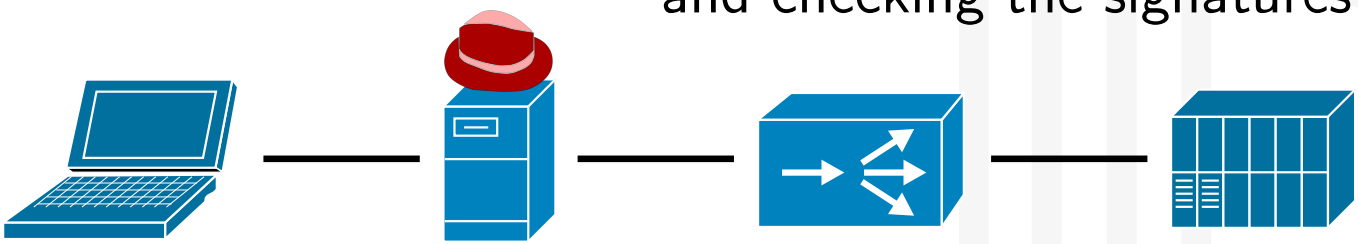
Mitigations-Compromised Workstation

- Hardening measures:
  - using dedicated hardware
  - using hardware security modules



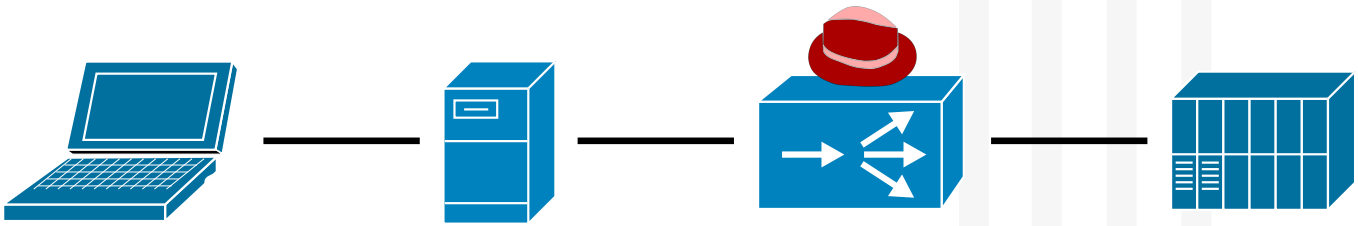
Mitigations-Compromised Repository

- Privilege Separation:
  - enforced offsite/offline backups
- Signing of commits
  and checking the signatures



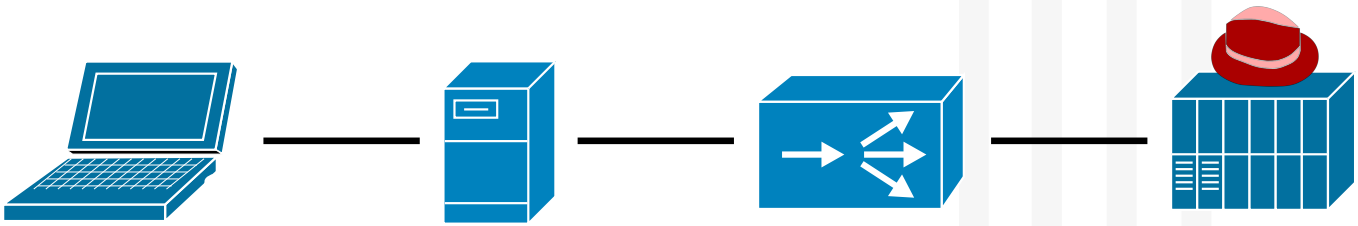
Mitigations-Compromised Managment Host

- Privilege Separation:
  - enforced offsite/offline backups
  - splitting the infrastructure in groups
  - regular self checks/deploys



Mitigations-Compromised Prod

- Privilege Separation:
  - enforced offsite/offline backups
- Reproducable builds
  - JUST REDEPLOY AND RESTORE



UNIVERSITÄTS BIBLIOTHEK FRANKFURT AM MAIN

You may contact me

- via eMail `J.Heinrich@ub.uni-frankfurt.de`
- our GitHub `github.com/ubffm/cicdcdont-lightning`
- personally on the conference