UNIVERSITÄTS BIBLIOTHEK FRANKFURT AM MAIN

CI/CD/CDon't?

Deliberations on the threat model of continuous delivery systems

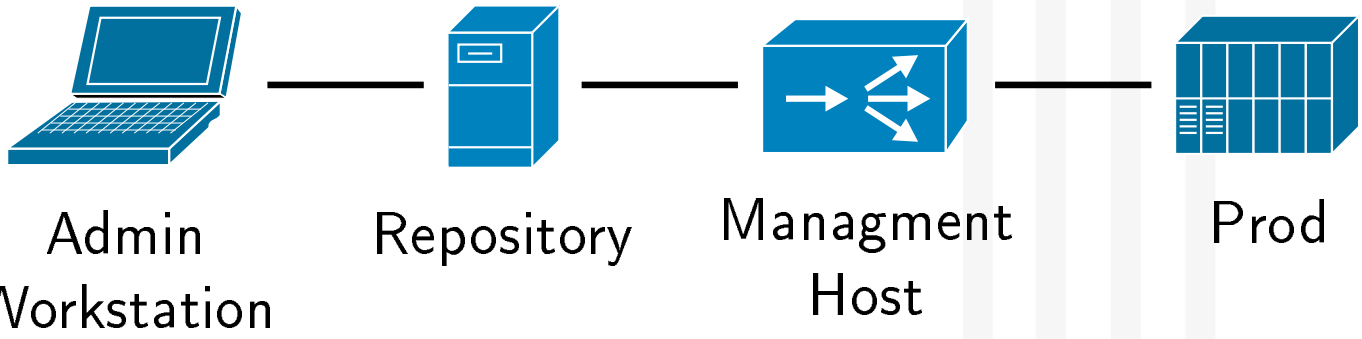
Jens Heinrich

Universitätsbibliothek Johann Christian Senckenberg

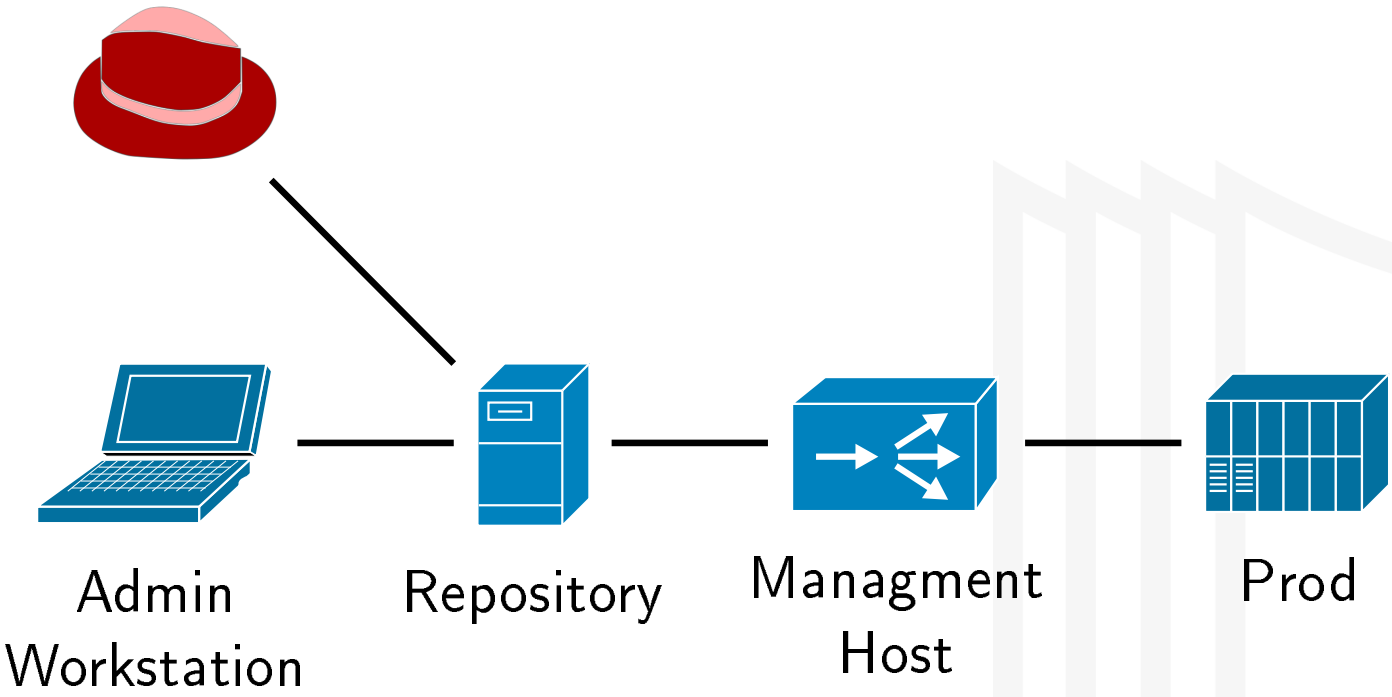
2020–03–14/15

CYBER CiderSecCon

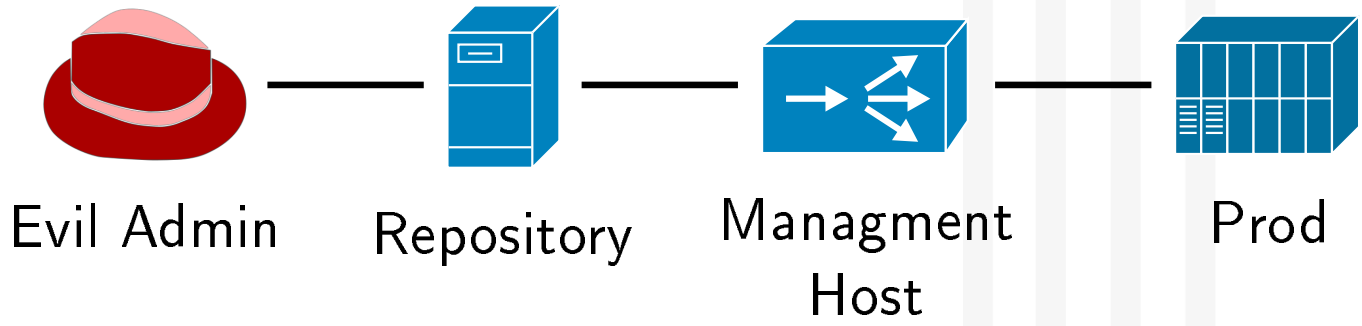
Concept-Pipeline



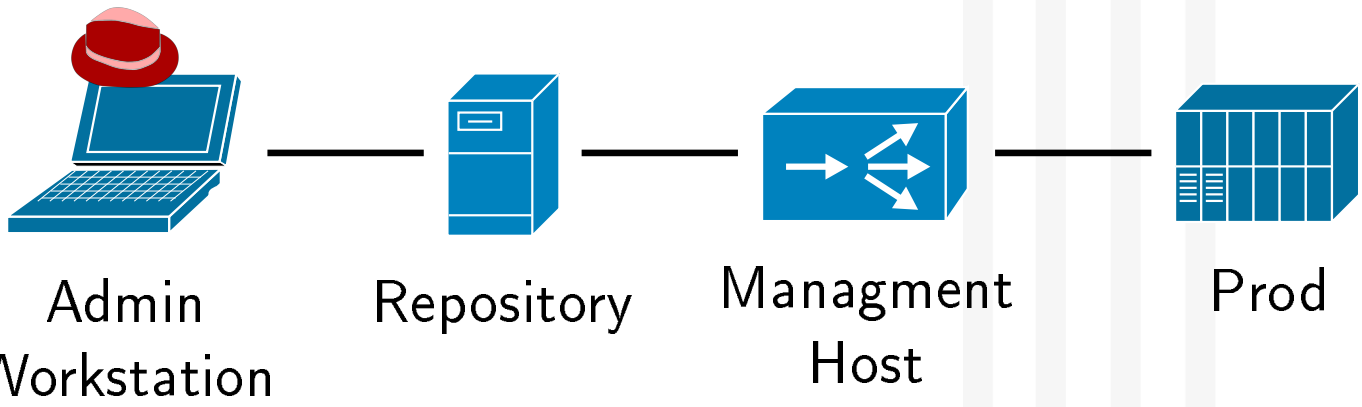
Attack Vectors-Impersonation



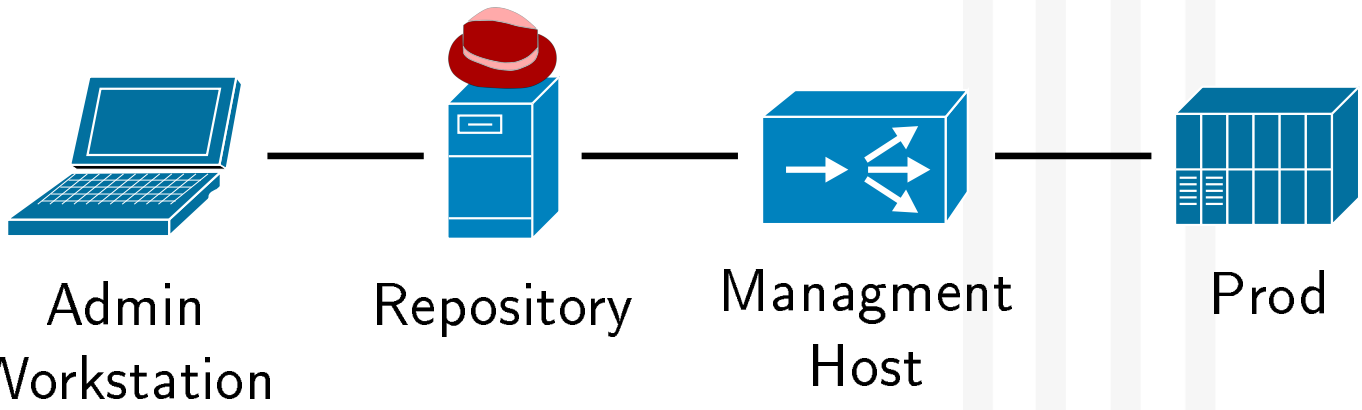
Attack Vectors-Evil Admin



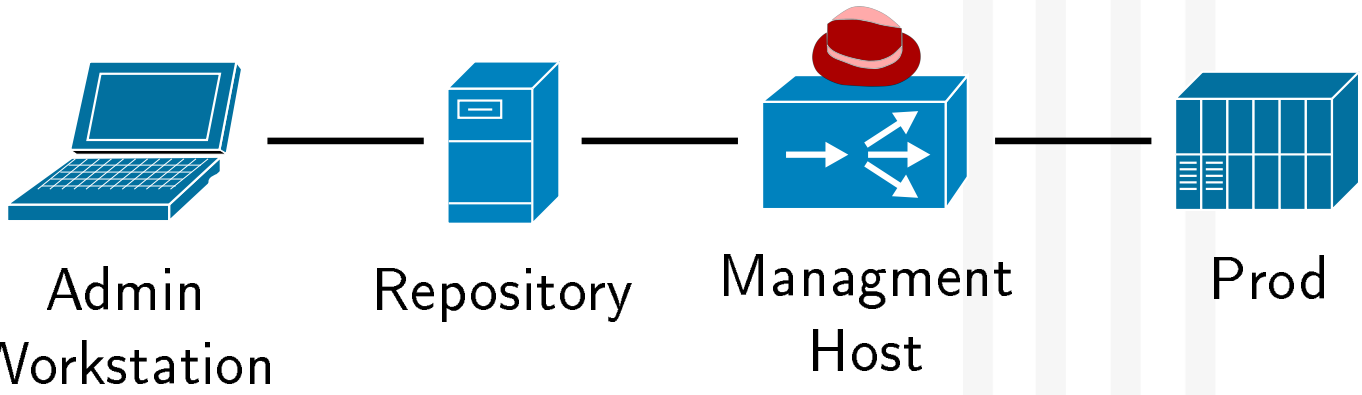
Attack Vectors-Compromised Workstation



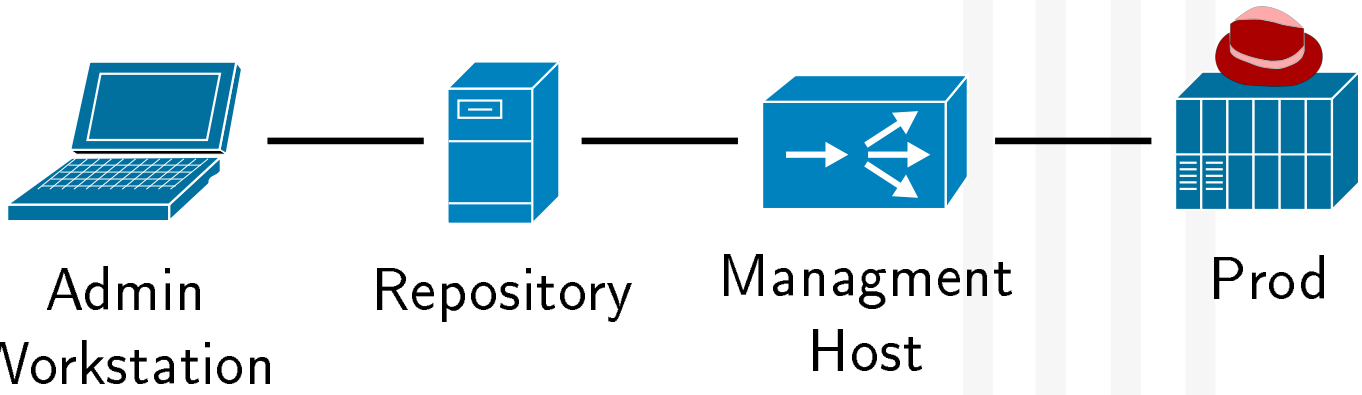
Attack Vectors-Compromised Repository



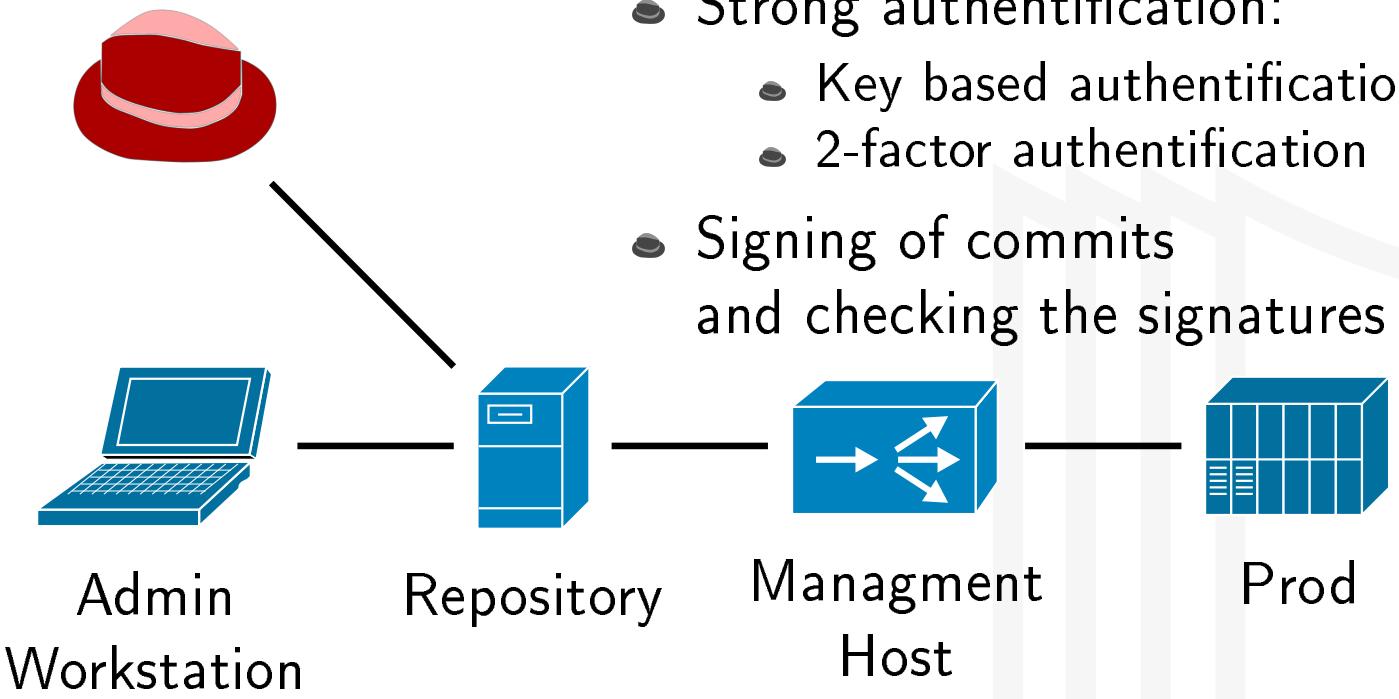
Attack Vectors-Compromised Managment Host



Attack Vectors-Compromised Prod



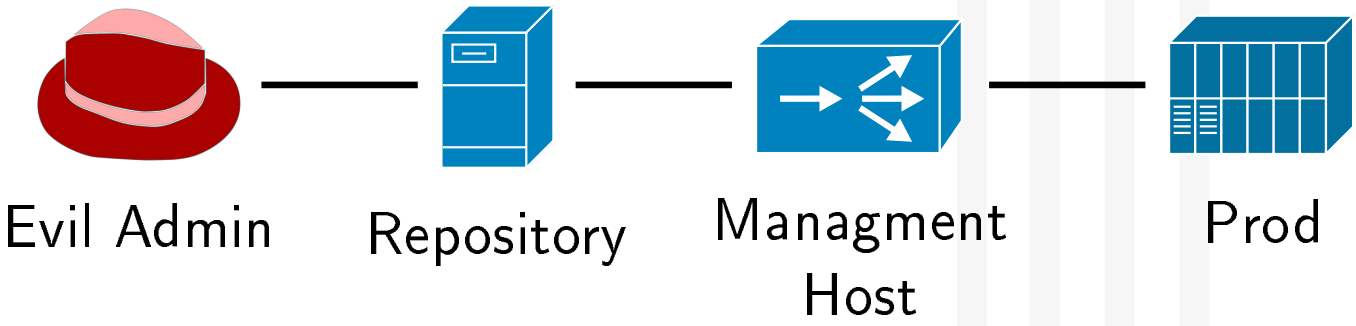
Mitigations-Impersonation



- Strong authentification:
  - Key based authentification
  - 2-factor authentification
- Signing of commits
  and checking the signatures

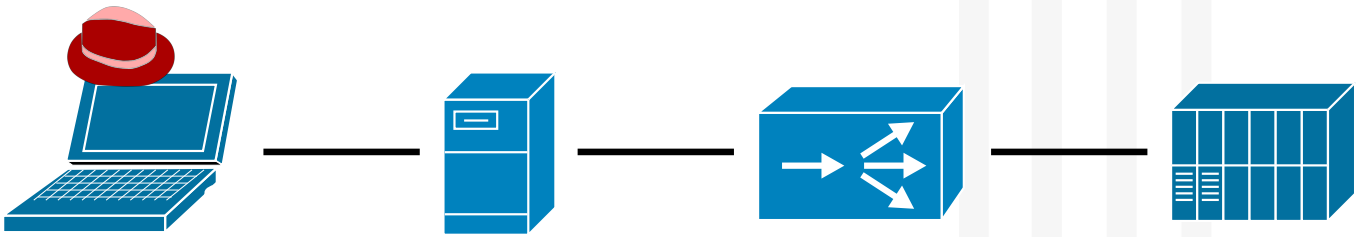
Mitigations-Evil Admin

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



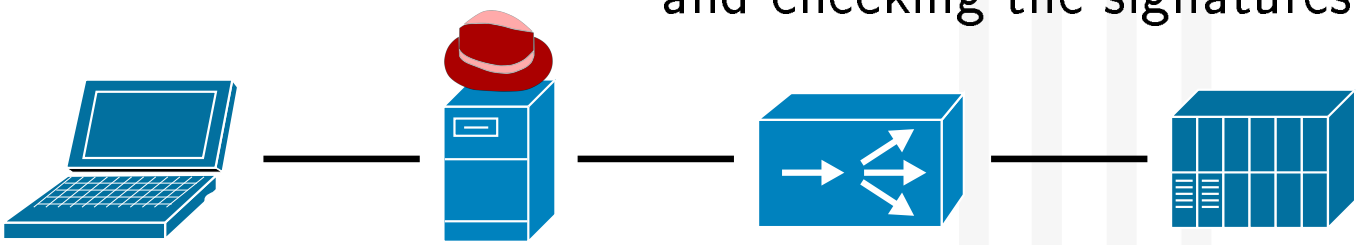
Mitigations-Compromised Workstation

- Hardening measures:
  - Using dedicated hardware
  - Using hardware security modules for storage



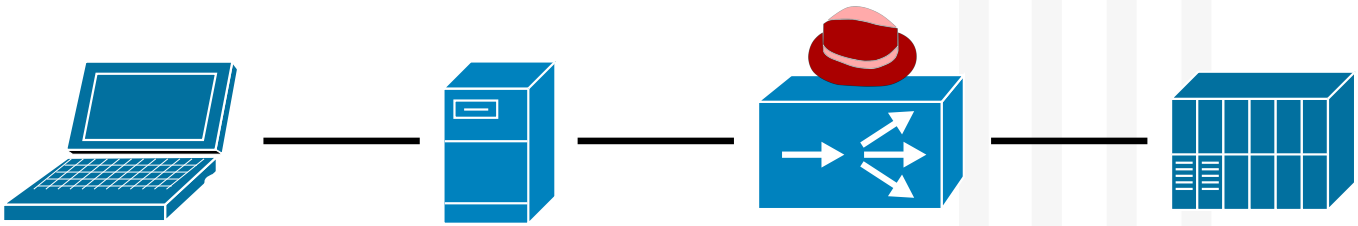
Mitigations-Compromised Repository

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



Mitigations-Compromised Managment Host

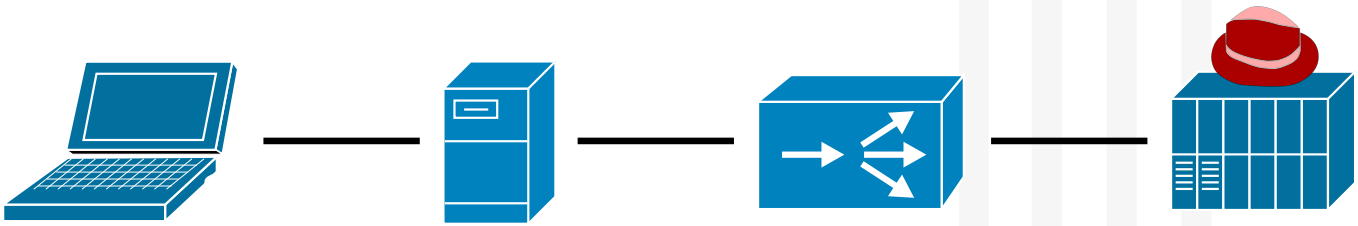
- Privilege Separation:
  - Enforced offsite/ offline backups
  - Splitting the infrastructure in groups
  - Regular self checks/ deploys



Admin Workstation — Repository — Managment Host — Prod

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
- via GitHub github.com/ubffm/cicdcdont-lightning
- via Twitter @JensHeinrichFFM

Sources I