CI/CD/CDon't?

Deliberations on the threat model of continuous delivery systems
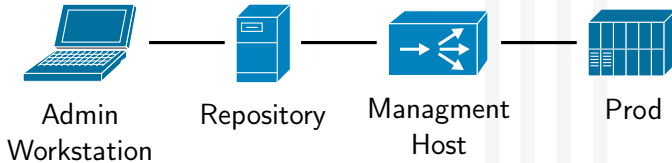
Jens Heinrich

Universitätsbibliothek Johann Christian Senckenberg
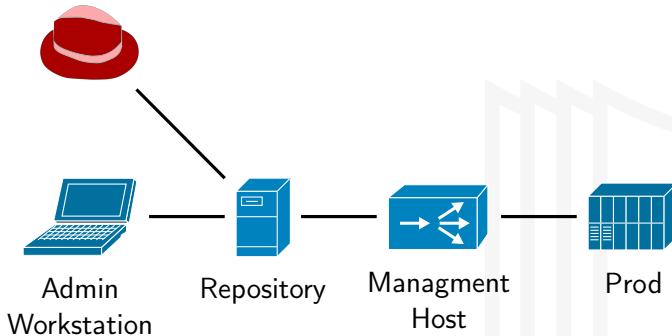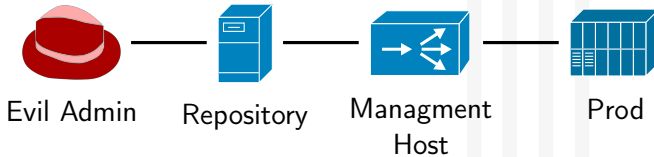
2020–03–14/15
CYBER CiderSecCon

Admin
Workstation

Repository

Managment
Host

Prod

Admin
Workstation

Repository

Managment
Host

Prod

Attack Vectors-Evil Admin

Evil Admin — Repository — Managment Host — Prod

Admin
Workstation

Repository

Managment
Host

Prod

Admin
Workstation

Repository

Managment
Host

Prod

Admin
Workstation

Repository

Managment
Host

Prod

Mitigations-Impersonation

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

Admin Workstation Repository Managment Host Prod
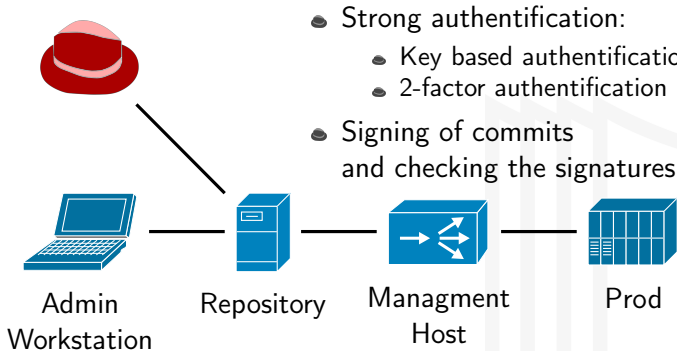
- Privilege Separation:
  - 2-man-rule
  - Enforced tests

Evil Admin   Repository   Managment Host   Prod

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

Admin
Workstation
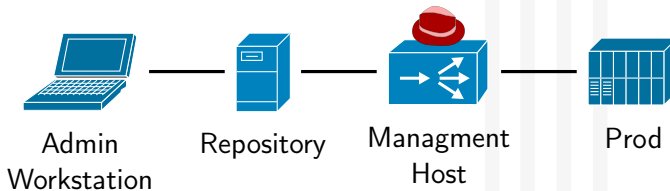
Repository

Managment
Host

Prod
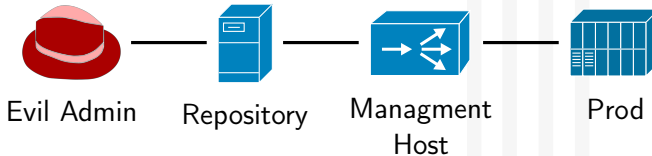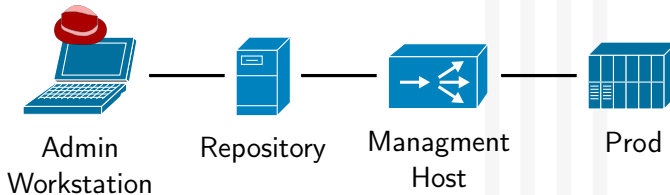
Mitigations-Compromised Repository

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

Admin Workstation   Repository   Managment Host   Prod

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

Admin Workstation — Repository — Managment Host — Prod

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

Admin Workstation — Repository — Managment Host — Prod
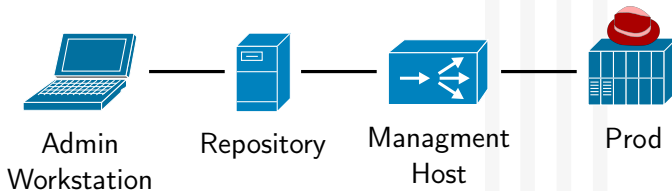
You may contact me

- via eMail J.Heinrich@ub.uni-frankfurt.de

- via GitHub github.com/ubffm/cicdcdont-lightning

- via Twitter @JensHeinrichFFM