

This is the export of a building block from the TMC Threat Library. This project aims to propose mitigations for relevant threats to reusable building blocks of modern tech systems. For more information about the project visit <https://threat-modeling.net/library/>

Build processes

Gains

-  [Team2] Turn code into magic/product - by TMC DACH
-  [Team2] Prepare build artifacts for shipping - by TMC DACH
-  [Team2] Reproducible build, not on developer machine - by TMC DACH

System Model

-  Developer - by TMC DACH
-  Architect - by TMC DACH
-  Manager / PO - by TMC DACH
-  Tester - by TMC DACH
-  Security Engineer - by TMC DACH
-  Infrastructure admin - by TMC DACH
-  [Team2] Developer - by TMC DACH
-  [Team2] Vibe coder - by TMC DACH
-  [Team2] Agent - by TMC DACH
-  [Team2] Merge requestor - by TMC DACH
-  [Team2] Reviewer - by TMC DACH
-  [Team2] Project lead - by TMC DACH
-  3rd party system - by TMC DACH
-  Build environment - by TMC DACH

-  Compiler - by TMC DACH
-  Version Control - by TMC DACH
-  Artifact repository - by TMC DACH
-  Test environment - by TMC DACH
-  [Team2] Unit tests - by TMC DACH
-  [Team2] SAST (Static application security testing) / DAST (Dynamic ...) - by TMC DACH
-  [Team2] Dependency checks / SCA (Software composition analysis) - by TMC DACH
-  [Team2] Version control - by TMC DACH
-  [Team2] IAM (Identity Access Management) - by TMC DACH
-  [Team2] Build server - by TMC DACH
-  Source Code - by TMC DACH
-  3rd party library - by TMC DACH
-  Pipeline definition - by TMC DACH
-  Artifacts - by TMC DACH
-  Build pipeline - by TMC DACH
-  [Team2] Code - by TMC DACH
-  [Team2] Third party dependencies - by TMC DACH
-  [Team2] Version history - by TMC DACH
-  [Team2] Secrets (tokens, ...) - by TMC DACH
-  [Team2] Build artifacts - by TMC DACH
-  [Team2] Build IDs - by TMC DACH
-  Source code enters build environment - by TMC DACH
-  Artifact is stored in repository - by TMC DACH
-  Infrastructure admin changes build environment + connections to the outside - by TMC DACH
-  Artifacts flows from repository to prod environment - by TMC DACH

 **More info**

⚡ Threats and ☂️ Mitigation Ideas

*Confidentiality? Integrity? Availability? / Usability? Privacy? Safety? €\$? ...
→ Protect? Detect? Respond? → Follow-up threats?*

⚡ Artifact integrity/authenticity - by TMC DACH

☂️ Signing of artifacts - by TMC DACH

⚡ Supply Chain Attack - by TMC DACH

☂️ Dependency pinning - by TMC DACH

☂️ Vuln scans - by TMC DACH

☂️ Delayed updates - by TMC DACH

☂️ CVE/dependency firewall - by TMC DACH

⚡ Build environment authenticity - by TMC DACH

☂️ Trusted environments - by TMC DACH

☂️ Signed environments - by TMC DACH

☂️ Zero Trust environments - by TMC DACH

⚡ Code integrity / authenticity - by TMC DACH

☂️ Code signing - by TMC DACH

☂️ protected branches - by TMC DACH

☂️ Commit discipline - by TMC DACH

⚡ Version control integrity / authenticity - by TMC DACH

⚡ Mutating version updates - by TMC DACH

⚡ Rouge developers: malware/backdoor injection - by TMC DACH

☂️ Reviews & 4 eyes principle - by TMC DACH

☂️ Code scanning - by TMC DACH

☂️ protected branches - by TMC DACH

 Approval of unsaved artifacts - by TMC DACH

 4 eyes principle (e.g. by security engineer) - by TMC DACH