Software Bill of Materials im Konfigurationsmanagement

Niklaus Hofer

Software Bill of Materials

1. September 2023

Übersicht

- Begriffserklärung (Was ist ein SBOM?)
- Arbeiten mit SBOM
- Integration mit weiteren Werkzeugen

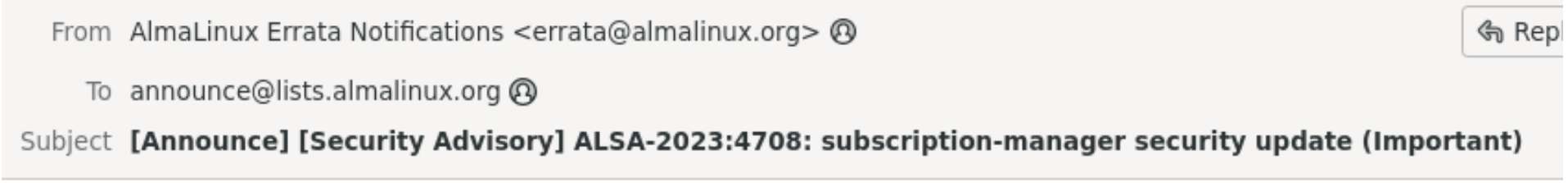
Begriffserklärung (Was ist ein SBOM?)

SBOM Begriffserklärung

- Software Bill of Materials
  - In Anlehnung an ein BOM / Bill of Materials aus der Fertigung
  - Auch als Stückliste bekannt
- Liste aller auf einem System installierter Software
  - Maschinenlesbar

Sicherheitsmeldungen

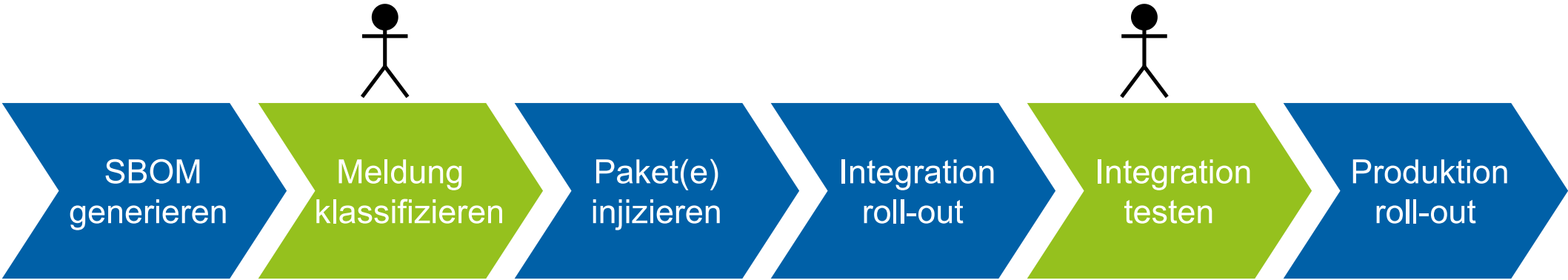
- Meldungen zu Sicherheitslücken
  - Von den Softwarelieferanten
  - Via E-Mail



- In den SBOMs nachschauen, ob wir die Software nutzen

Arbeiten mit SBOM

Übersicht des Ablaufs



SBOM Generierung

- SBOM wird auf jedem Server erstellt
  - 1-Mal am Tag
  - Für den Kunden einsehbar (noch in Arbeit)
- Mit der Software *syft*
- Im Format *cyclonedx-json*
- SBOMs werden zentral gesammelt

Klassifizierung

- Vier Stufen:
  - Low
    - "[...] unlikely [...] to be able to be exploited, or where a successful exploit would give minimal consequences."
  - Moderate
    - "[...] difficult to exploit but could still lead to some compromise of the confidentiality, integrity or availability of resources under certain circumstances."
  - Important
    - "[...] compromise the confidentiality, integrity or availability of resources."
  - Critical
    - "[...] exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) [...]"

Bomber


BOMBER
DKFM - DevOps Kung Fu Mafia
https://github.com/devops-kung-fu/bomber
Version: 0.4.4
Ecosystems detected: rpm
Scanning 1023 packages for vulnerabilities...
Vulnerability Provider: OSV Vulnerability Database (https://osv.dev)
Files Scanned
esa-int-002.json (sha256:b2b2b3e291c94e25b
Licenses Found: ImageMagick, MIT, ISC, GPL-2.0-o
0 AND Zlib, BSD-3-Clause, Unicode-DFS-2016 AND BSD
lic-Domain, IJG, Zlib, libtiff, BSD-2-Clause-Paten
only, BSD-2-Clause AND ISC AND MIT, LGPL-2.1-or-la
No vulnerabilities found using the osv provider
NOTE: Just because bomber didn't find any vulnerab
not mean that there are no vulnerabilities. Please
supports (osv, ossindex)
BOMBER

Integration mit weiteren Werkzeugen

Pakete injizieren

- Im Normalbetrieb werden alle Softwarequellen zu Monatsbeginn eingefroren
- Im Falle kritischer Updates, müssen wir die aktualisierten Pakete trotzdem ergänzen

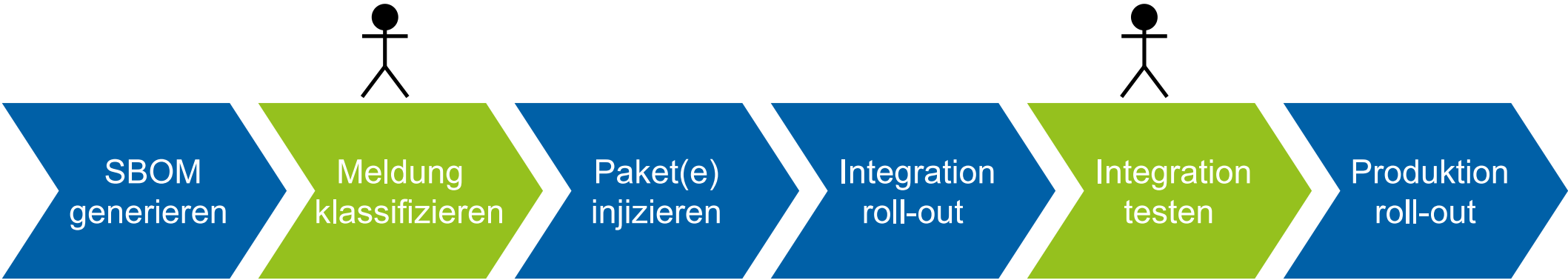
Roll-out

- Liste der Systeme erhalten wir aus den SBOMs
- Installation der aktualisierten Paketen
- Wo immer möglich - Tests auf den Integrationssystemen
- Bei Unsicherheiten oder Neustarts: Koordination mit dem Kunden

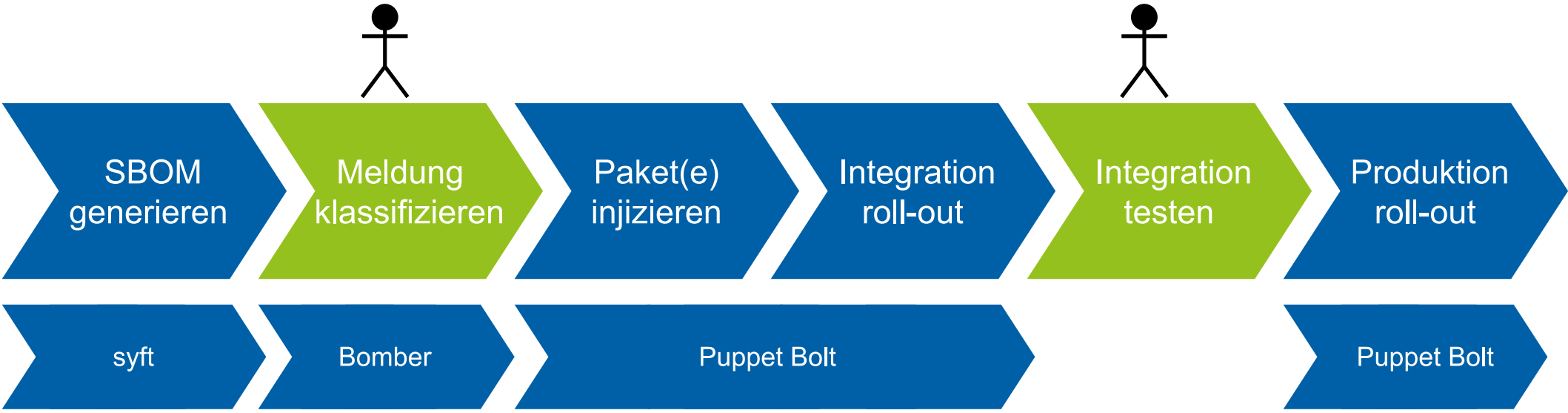
Puppet Bolt

- Verbesserung der Automatisierung
  - Paket-Injizierung
  - Einspielen der Updates
- Bessere Zuverlässigkeit bei Tasks zu Randzeiten

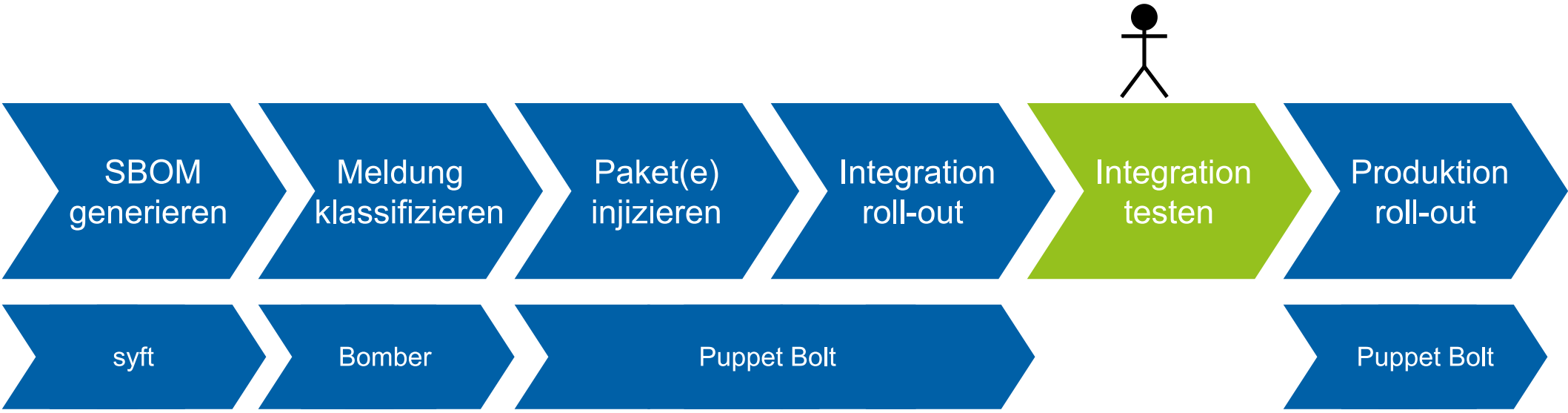
Übersicht des Ablaufs



Übersicht des Ablaufs



Übersicht des Ablaufs



Zukunft

- Fertigstellung der zuvor erwähnten Punkte
  - Puppet Bolt, Bomber
- Integration der Software-Stacks unserer PaaS-Kunden
  - Schrittweiser Ausbau in den kommenden Monaten
- Verbesserte Transparenz
  - Kunden erhalten Zugriff auf die SBOMs ihrer VMs
- SBOM Standardisierung
  - Hier ist das letzte Wort noch nicht gesprochen

Fragen?

Links

- https://www.stepping-stone.ch/
- https://www.stoney-backup.com/
- https://www.stoney-cloud.com/
- https://www.stoney-mail.com/
- https://www.stoney-meet.com/
- https://www.stoney-office.com/
- https://www.stoney-services.com/
- https://www.stoney-storage.com/
- https://www.stoney-wiki.com/

stepping stone AG
Wasserwerkgasse 7
CH-3011 Bern

Telefon: +41 31 332 53 63
www.stepping-stone.ch
info@stepping-stone.ch