SOFTWARE BILL OF MATERIAL

Aanleiding tot het opzetten van SBOM

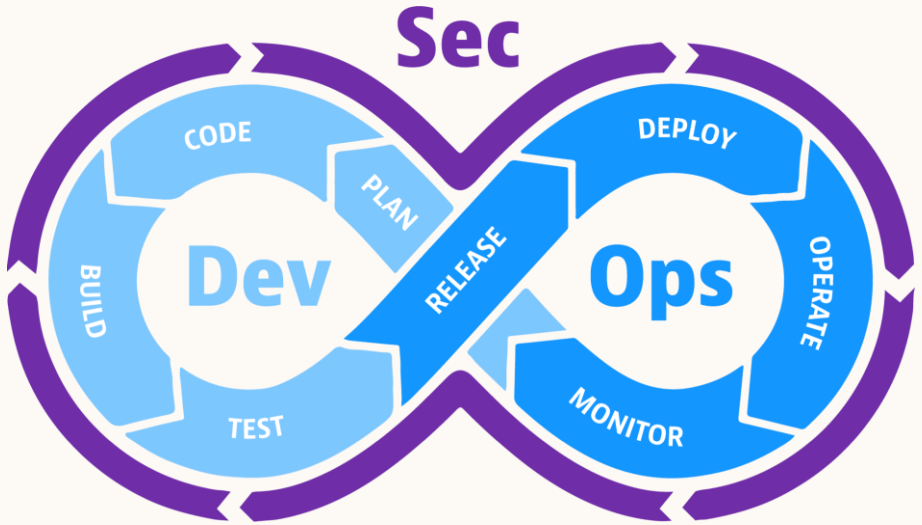
- Project Cyber Security Noord Nederland

  Doel - MKB Cyber weerbaarder maken
- Provincie en gemeente Groningen / TNO / RUG /Hanze hogeschool
- Lectoraat Digitale Transformatie - New Business &ICT

This presentation was written as part of the Cyber Security Noord Nederland Program.
The Program Cyber Security Noord Nederland has received funding from the RSP of the Province of Groningen and the municipality of Groningen.

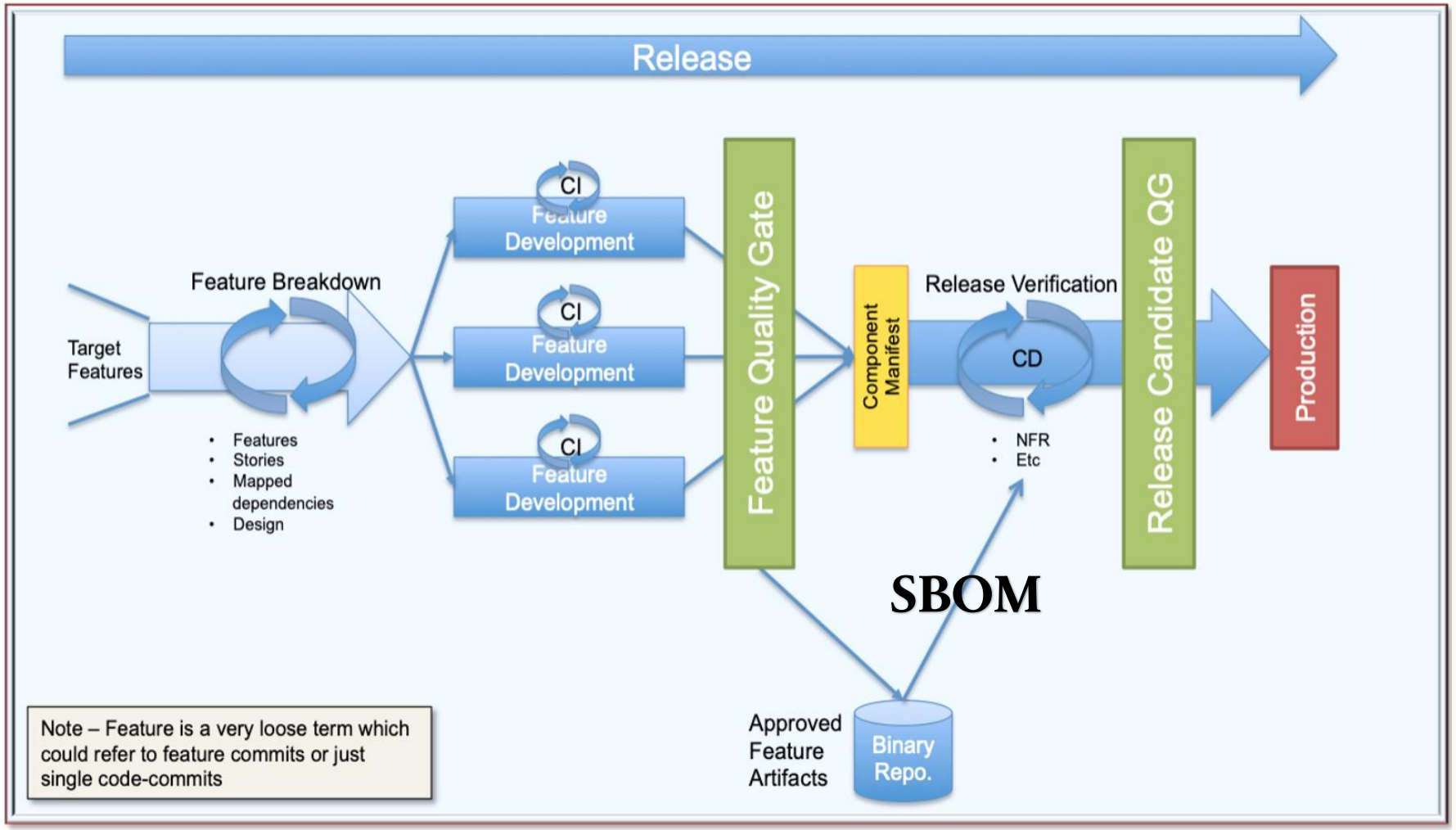
Aanleiding tot het opzetten van SBOM

- Realiseren door:
  - Tooling
  - Handreikingen en best practices
- Deel project – DevSecOps maturity models



This presentation was written as part of the Cyber Security Noord Nederland Program.
The Program Cyber Security Noord Nederland has received funding from the RSP of the Province of Groningen and the municipality of Groningen.

Dev(Sec)Ops pipeline



https://github.com/tpayne/devops-coord-framework/tree/master/devops-framework-pipeline/examples

PROGRAMMA CYBERSECURITY NOORD-NEDERLAND

This presentation was written as part of the Cyber Security Noord Nederland Program.
The Program Cyber Security Noord Nederland has received funding from the RSP of the Province of Groningen and the municipality of Groningen.

Hanzehogeschool Groningen
University of Applied Sciences

JESSE LOURENS

- 24 jaar
- Passie voor IT
  - Aan apparaten sleutelen
  - Jongs af aan geïnteresseerd
- Student Hanze hogeschool Groningen
  - Stage bij Digital Society Hub
  - Software Bill of Materials opdracht

STAGE OPDRACHT

- Behoefte aan kennis rondom SBOM vanuit MKB Noord-Nederland
- Wetgeving rondom Software Bill Of Materials
- Tooling rondom Software Bill Of Materials

VRAGEN

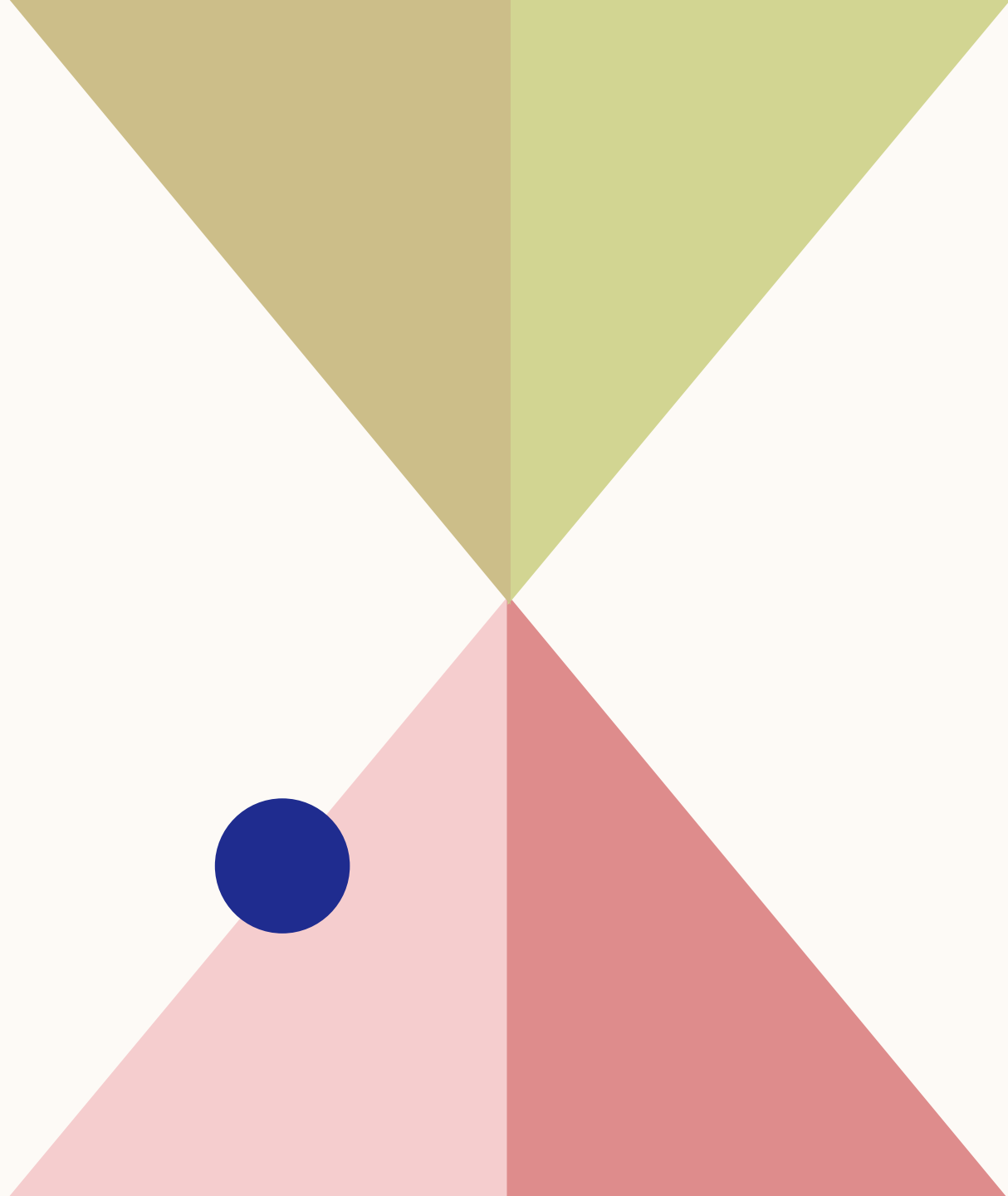
Wie kent de Software Bill of Materials?

VRAGEN

Wie kent de Vulnerability Exploitability Exchange (VEX)?

AGENDA

- Vroeger & Nu
- Wat is de SBOM
  - (Aankomende) Wetgeving
  - Standaarden
- Wat is VEX
- Tools



VROEGER

- Opensource code stond in zijn kinderschoenen
- Free software movement
    - GNU Project (1983)
- Probleemspecifieke oplossingen

NU

- Opensource code
- Frameworks
- Libraries

- Kortom: Proces versimpeld en versneld

HUIDIGE PROBLEEM

- Proces versimpeld en versneld
- Software steeds complexer
- Verschillende library versies

HUIDIGE PROBLEEM

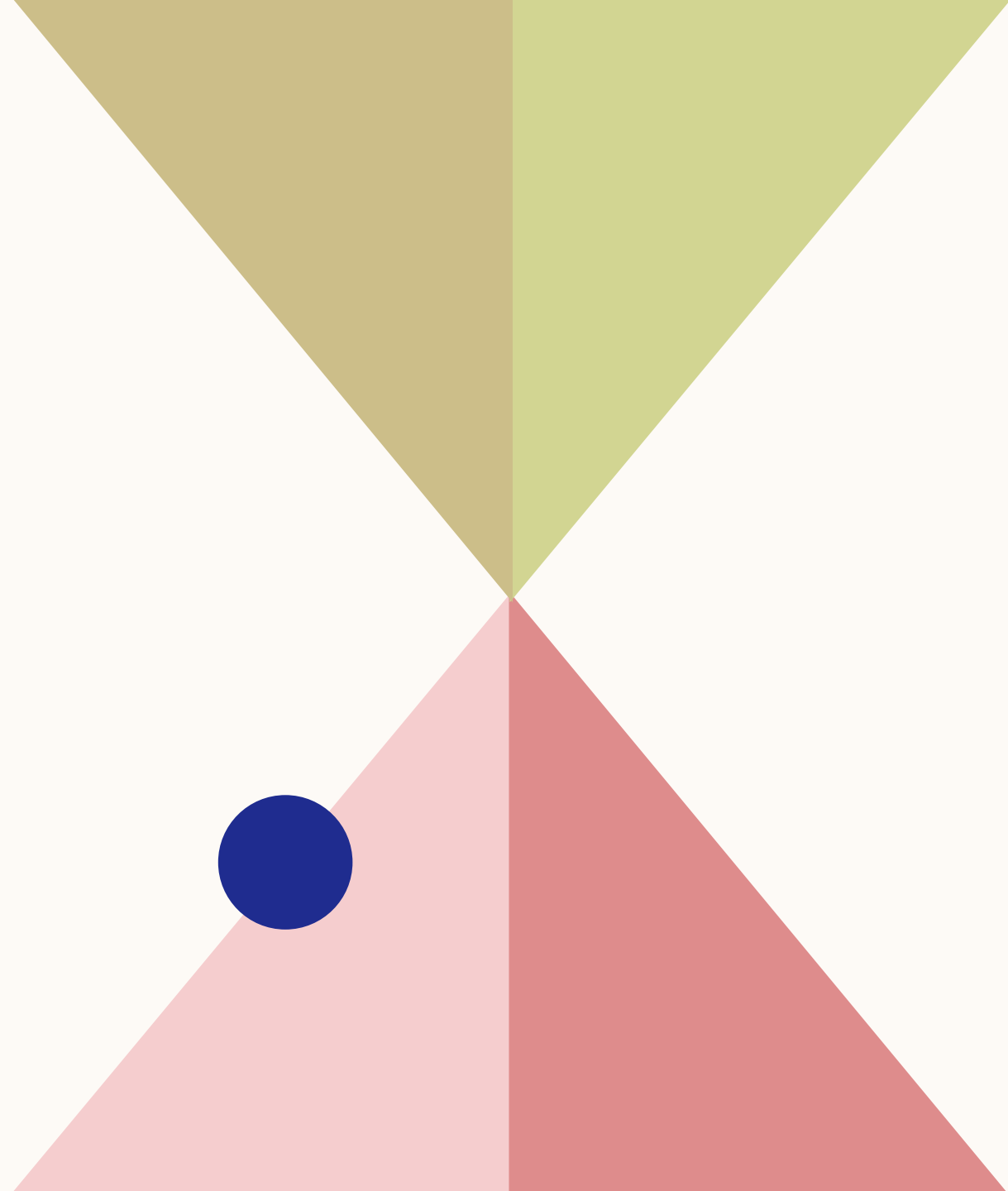
- Log4J
  - Log tool
  - 10 miljoen pogingen per uur
  - Grote jongens
    - Intel
    - Dell
    - IBM
    - GitHub
- SolarWinds - Orion
  - Solarwinds123
  - Github
  - 90 miljoen dollar (CRN)
  - Raakt Amerikaanse overheid
- Hoe nu verder?

SOFTWARE BILL OF MATERIALS

Wat is het eigenlijk?

SOFTWARE BILL OF MATERIALS

- Ingrediëntenlijst
- Waarom nu?



WETGEVING

- Disclaimer
- Cyber Resilience Act – Europese Unie
- Executive Order 14028 – Verenigde Staten
- Doel: ICT infrastructuur weerbaarder

EUROPESE UNIE

- Voorlopige versie
- “Een formeel document met details en de onderlinge relaties van componenten die in de software-elementen van een product zitten.” – CRA (voorlopige versie)

VERENIGDE STATEN

- “A formal record containing the details and supply chain relationships of various components used in building software” – National Institute of Standards & Technology

VERENIGDE STATEN

- Barrière verlagen voor informatiedeling
- Moderniseren van cybersecurity standaarden
- Verbeteren van software supply chain beveiliging
- Pilot met MDS2
  - Medisch apparatuur
  - FDA
- Verkoop van software aan Amerikaanse overheid entiteiten.

TOEKOMSTBEELD

- Wetgeving wordt uitgebreid
- Handvaten bieden rondom SBOM
- Use cases uitbreiden

DATA VELDEN

#	Naam
1	Auteur
2	Leverancier
3	Component naam
4	Versie
5	Component hash
6	Other Unique Identifier
7	Relatie
8	Timestamp

- Wat voor unieke identifier van de component
  - PURL
  - SWID

PRAKTIJK

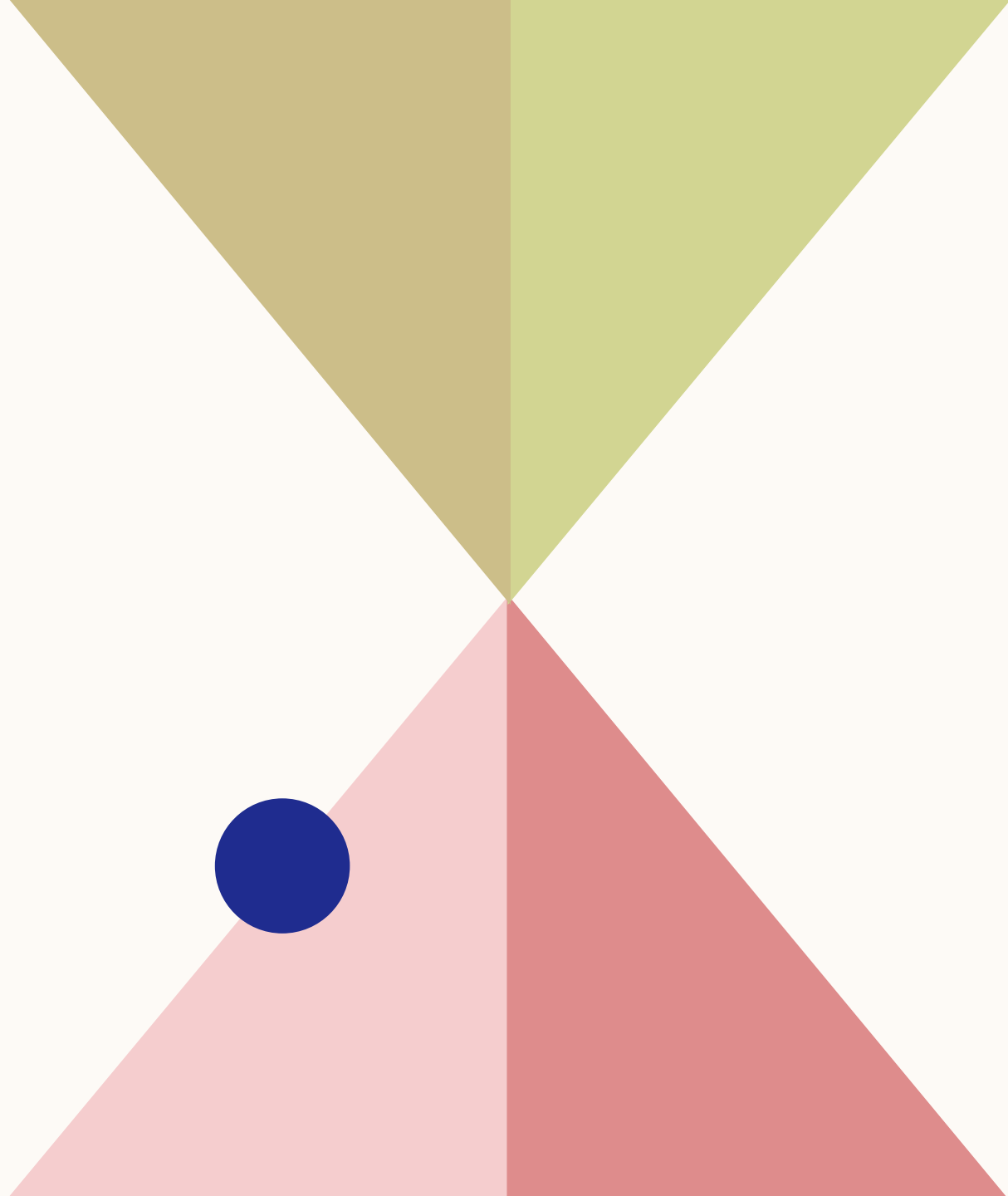
JSON Example


```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.4",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "components": [
    {
      "type": "application",
      "name": "Acme Application",
      "version": "9.1.1",
      "cpe": "cpe:/a:acme:application:9.1.1",
      "swid": {
        "tagId": "swidgen-242eb18a-503e-ca37-393b-cf156ef09691_9.1.1",
        "name": "Acme Application",
        "version": "9.1.1",
        "text": {
          "contentType": "text/xml",
          "encoding": "base64",
          "content": "PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiID8+
        }
      }
    },
    {
      "type": "library",
      "group": "org.apache.tomcat",
      "name": "tomcat-catalina",
      "version": "9.0.14",
      "purl": "pkg:maven/org.apache.tomcat/tomcat-catalina@9.0.14"
    }
  ]
}
```


- CycloneDX voorbeeld
- Elk standaard ziet er iets anders uit

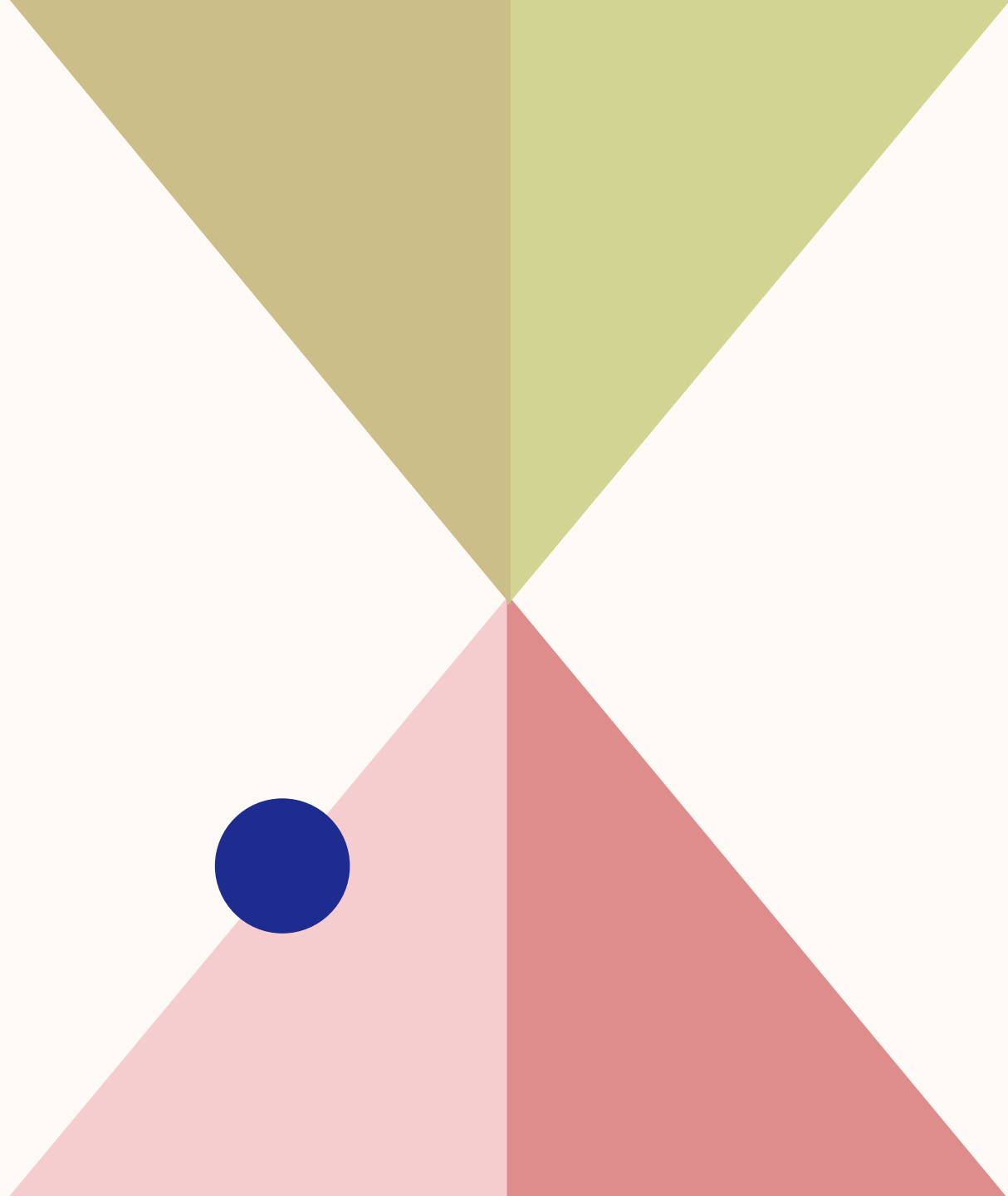
AUTOMATISERING

- Creëren
- Analyseren
- Delen
- Standaarden



STANDAARDEN

- National Telecommunications and Information Administration
- SPDX
  - 2011 – licentie informatie opslaan
  - Software development doeleinden
- CycloneDX
  - Specifiek gemaakt voor SBOM
  - Lichtgewicht voor machine



VULNERABILITY EXPLOITABILITY EXCHANGE

VEX

- Kwetsbaarheden details
- Kwetsbaarheid bruikbaar voor kwaadwillende?
- Oplossing
- Verbeterd de focus op wat daadwerkelijk tegen je gebruikt kan worden
- Combinatie met SBOM

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2023-1389	TP-Link	Archer AX21	TP-Link Archer AX-21 Command Injection Vulnerability	2023-05-01	TP-Link Archer AX-21 contains a command injection vulnerability that allows for remote code execution.	Apply updates per vendor instructions.	2023-05-22	https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware

- Ideale situatie: bijhouden van VEX

TOOLS

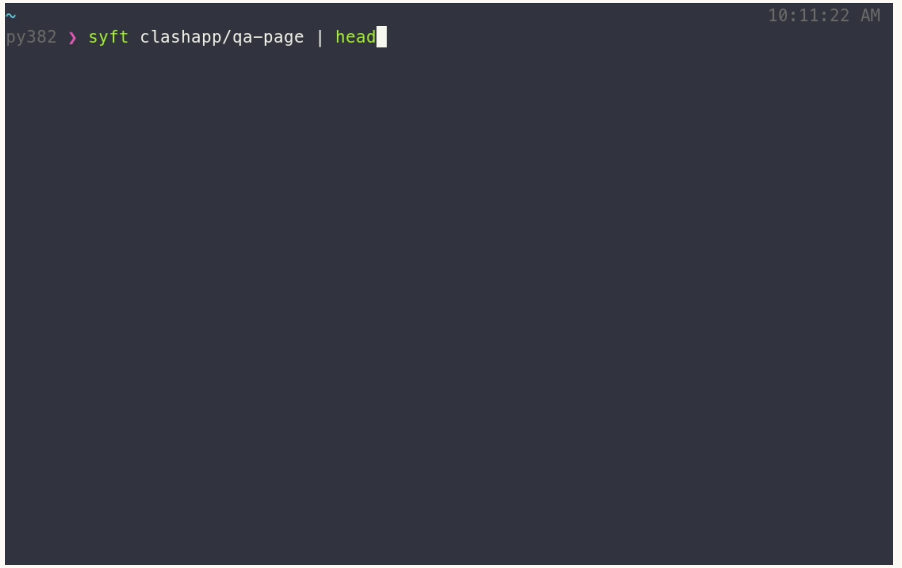
SBOM creëren & analyseren

TOOLS

- Programmeer taal
- Use case
- Open source tools

TOOLS - SYFT

- Gemaakt door Anchore
- SBOM genereer tool
- Command Line Interface



TOOLS - BOMBER

Vulnerability Details

pkg:pypi/certifi@2022.9.24

Vulnerabilities

Certifi removing TrustCor root certificate

Severity: **MODERATE**

EPSS: 15%

Reference Documentation

Certifi 2022.12.07 removes root certificates from “TrustCor” from the root store. These are in the process of being removed from Mozilla’s trust store.

TrustCor’s root certificates are being removed pursuant to an investigation prompted by media reporting that TrustCor’s ownership also operated a business that produced spyware. Conclusions of Mozilla’s investigation can be found here.

Severity: **UNSPECIFIED**

EPSS: 15%

Reference Documentation

Certifi is a curated collection of Root Certificates for validating the trustworthiness of SSL certificates while verifying the identity of TLS hosts. Certifi 2022.12.07 removes root certificates from “TrustCor” from the root store. These are in the process of being removed from Mozilla’s trust store. TrustCor’s root certificates are being removed pursuant to an investigation prompted by media reporting that TrustCor’s ownership also operated a business that produced spyware. Conclusions of Mozilla’s investigation can be found in the linked google group discussion.

TOOLS - MICROSOFT

- Open source gemaakt
- Automatiseringen mogelijkheden bij build time
    - Azure DevOps pipeline
    - GitHub Actions

Dependency graph

Dependencies | Dependents

Export SBOM

Search all dependencies

hexdump >= 3.3
Detected automatically on Nov 05, 2019 (pip) · panda/setup.py

libusb1 1.6.6
Detected automatically on Nov 05, 2019 (pip) · panda/setup.py · GPL-3.0-or-later

pycrypto >= 2.6.1
Detected automatically on Nov 05, 2019 (pip) · panda/setup.py

requests
Detected automatically on Nov 05, 2019 (pip) · panda/setup.py

tqdm >= 4.14.0
Detected automatically on Nov 05, 2019 (pip) · panda/setup.py

cffi 1.11.4
Detected automatically on Dec 13, 2019 (pip) · panda/requirements.txt · MIT

flake8 3.7.9

CONCLUSIE

- Combineren tools
- Geen heilige graal
- Toekomst

THANK YOU

Jesse Lourens
j.lourens@st.hanze.nl