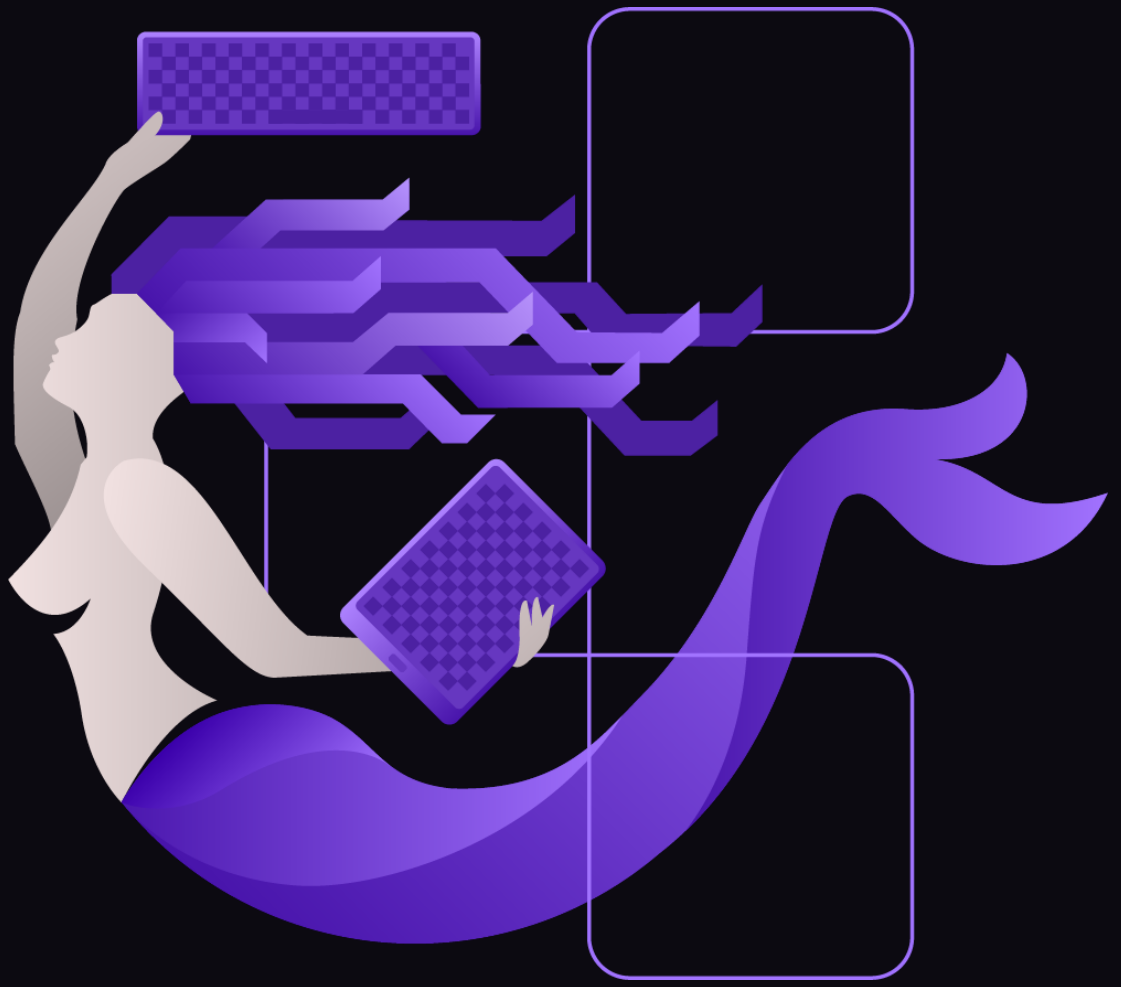
WARSZAWSKIE DNI INFORMATYKI



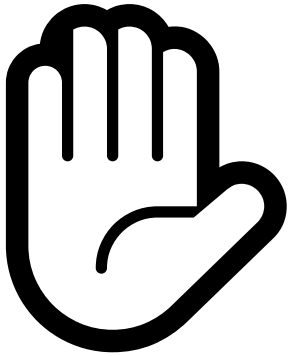
Supply Chain Security - czym właściwie jest i dlaczego to ważne?

Adrian Sroka
Security Architect, British Council

securitychampions.pl

ORGANIZATOR GŁÓWNY: Academic Partners FUNDACJA

KOMITET ORGANIZACYJNY: kilkadziesiąt organizacji z sektora IT / data science (pełna lista na stronie wydarzenia)



Kto wie, czym jest Supply Chain Security?

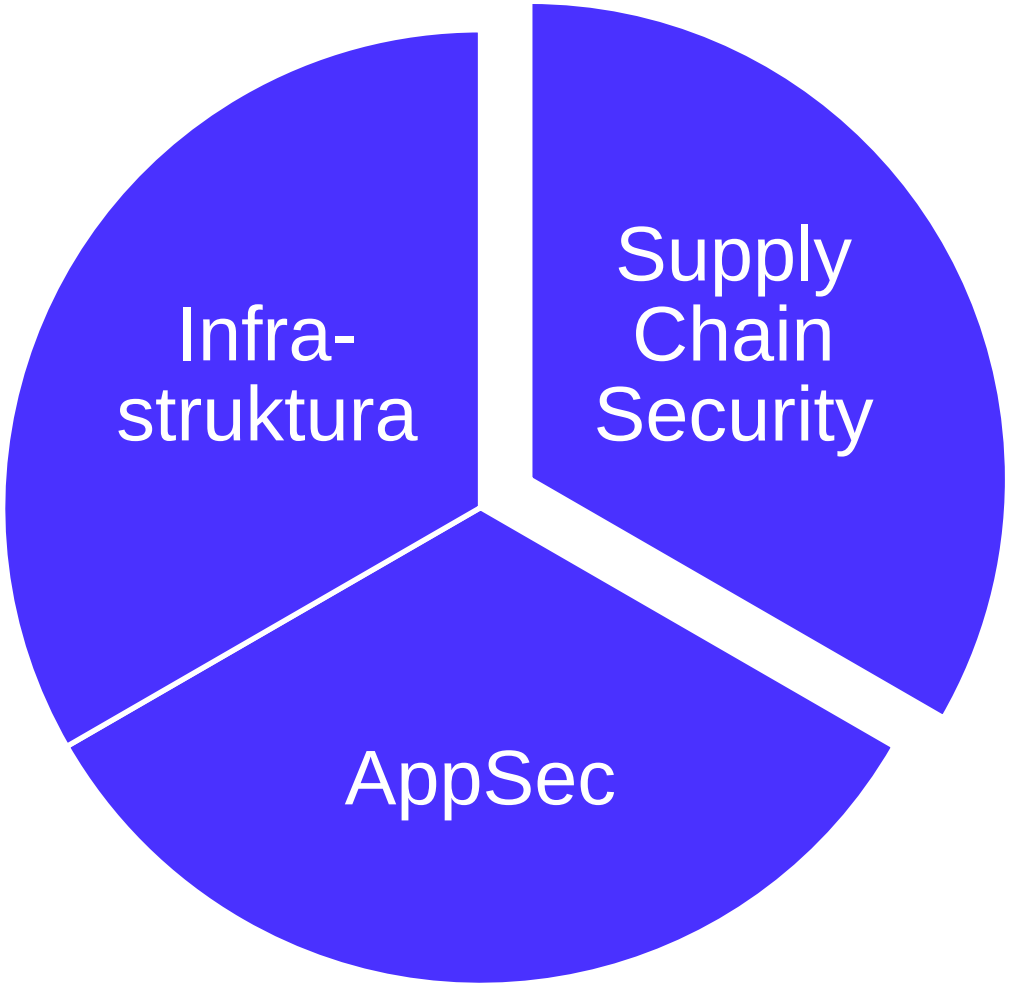
Dlaczego Supply Chain Security stało się ważne?

- AppSec rośnie w siłę

Atakujący ma 2 opcje:

- ścigać się dalej z obrońcami
- wybrać łatwiejszy łup - zamiast okradać bank, przejmijmy drukarnię

Supply Chain Security czym jest?



Czy to istotne?

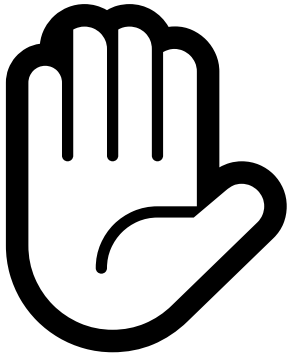
Sec. 4. Enhancing Software Supply Chain Security.

(a) The security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions. The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The security and integrity of "critical software" — software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources) — is a particular concern. Accordingly, the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.

Biden Administration's Executive Order

Czym właściwie jest Supply Chain Security?

Biblioteki Open Source



Kto w swojej pracy ma narzędzie do weryfikacji bezpieczeństwa zależności?

Ciekawostka:

- npm domyślnie wyświetla informacje o bezpieczeństwie wykorzystywanych paczek

```
C:\xampp3\htdocs\projects\cms\roocket> npm install

up to date, audited 1138 packages in 6s

59 packages are looking for funding
  run `npm fund` for details

44 vulnerabilities (43 moderate, 1 high)

To address issues that do not require attention, run:
  npm audit fix

To address all issues (including breaking changes), run:
  npm audit fix --force

Run `npm audit` for details.
```

Co tu jest źle?

```
"dependencies": {
    "rollup": "~2.75.0",
    "rxjs": "^6.6.7",
    "selenium-webdriver": "3.5.0",
    "semver-dls": "^1.0.1",
    "shelljs": "^0.8.5",
    "sourcemap": "0.7.4",
    "source-map-support": "0.5.21",
    "sourcemap-codec": "^1.4.8",
    "start-server-and-test": "^1.10.11",
    "systemjs": "0.18.10",
    "terser": "^5.8.0",
    "tmp": "0.2.1",
    "todomvc-app-css": "^2.3.0",
    "todomvc-common": "^1.0.5",
    "tsickle": "0.38.1",
    "tslib": "^2.3.0",
    "tslint": "6.1.3",
    "typescript": "~4.7.2",
    "webtreemap": "^2.0.1",
    "xhr2": "0.2.1",
    "yargs": "^17.2.1"
  },
```

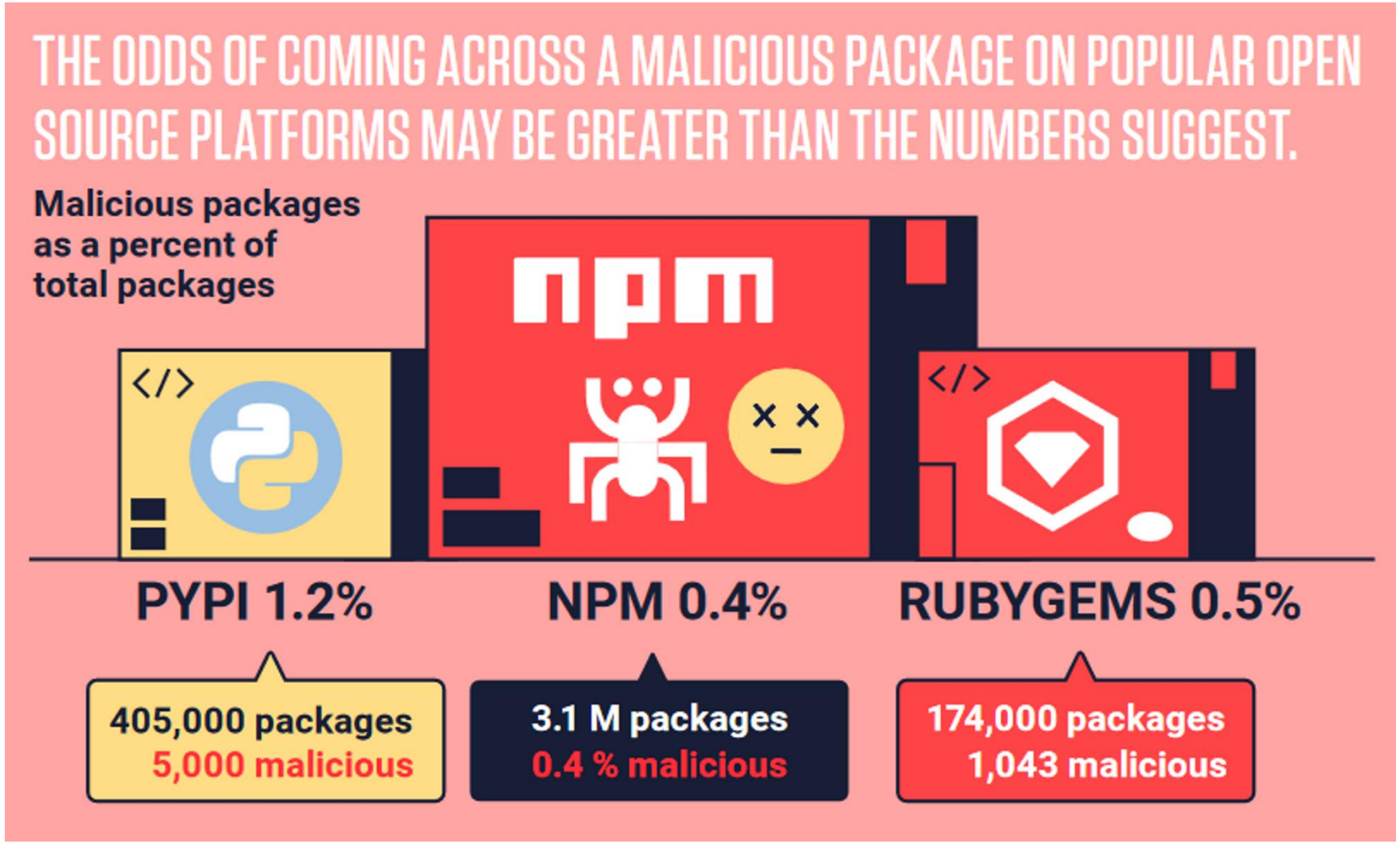
Co tu jest źle?

semver-dsl

source-map

```
"dependencies": {
    "rollup": "~2.75.0",
    "rxjs": "^6.6.7",
    "selenium-webdriver": "3.5.0",
    "semver-dls": "^1.0.1",
    "shelljs": "^0.8.5",
    "sourcemap": "0.7.4",
    "source-map-support": "0.5.21",
    "sourcemap-codec": "^1.4.8",
    "start-server-and-test": "^1.10.11",
    "systemjs": "0.18.10",
    "terser": "^5.8.0",
    "tmp": "0.2.1",
    "todomvc-app-css": "^2.3.0",
    "todomvc-common": "^1.0.5",
    "tsickle": "0.38.1",
    "tslib": "^2.3.0",
    "tslint": "6.1.3",
    "typescript": "~4.7.2",
    "webtreemap": "^2.0.1",
    "xhr2": "0.2.1",
    "yargs": "^17.2.1"
  },
```

Ile bibliotek jest złośliwych?



Źródło: [The State of Software Supply Chain Security]

Ataki z użyciem bibliotek

- GrubHub – @grubhubprod/cookbook – atak w konkretną firmę, kradzież danych
- CoPay – flatmap-stream – wyciek kluczy prywatnych (haseł do kryptoportfeli) z aplikacji wykorzystujących zarówno bibliotekę event-stream, jak i copay-dash.
- Twilio – twilio-npm – reverse – shell

Biblioteki Open Source
Rekomendacje

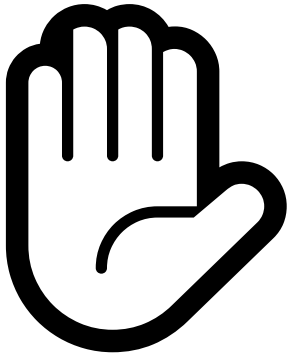
- SBOM
- Narzędzia do skanowania zależności
- Version pinning
- CSP - hash validation

Zewnętrzni dostawcy

Zewnętrzni dostawcy

- Ufamy im
- Wymieniamy z nimi dane
- Dostajemy od nich dane
- Są w stanie wykonywać akcje

- Są jak użytkownicy



W czyjej firmie przeprowadzany jest audyt bezpieczeństwa dostawców oprogramowania?

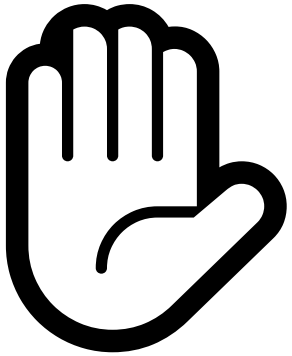
Zewnętrzni dostawcy
Ataki

- Atlassian – atak na single sign-on (SSO) – kompromitacja setek zależnych aplikacji
- Target – 70 mln danych osobowych i 40 mln danych kart płatniczych – wyciek sekretów u zewnętrznego dostawcy

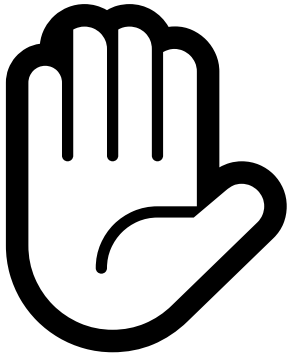
Zewnętrzni dostawcy
Rekomendacje

- Weryfikacja bezpieczeństwa dostawców (co najmniej tak bezpieczni jak my)
- Zasada ograniczonego zaufania (zero trust)

Złośliwe obrazy



Kto używa konteneryzacji?



Kto ma pewność, że jego obrazy bazowe są bezpieczne?

Złośliwe obrazy

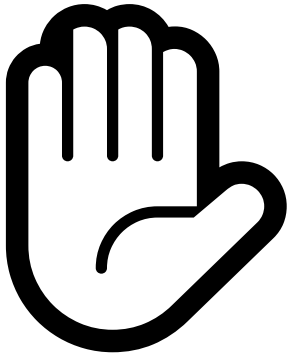
Image Name	Image Digest	Downloads
vibersastra/ubuntu	81b850230c2a9ea155aa06adda5537f5e01a4ec2b0209aaa24c23e06161ff385	10,000+
vibersastra/golang	a6af08adbcf9eba00e3ea15f8a67a7766465fb387868efd43ab77f7668a8dc46	6,900
ynprpagamentitk/liferay	3978fb1b4d9581fddbd44f44901e87f9f8baf7942c74d5820c573c06cc83f861	281
arrghgluiistk/drupal	9ab7485664242c00db8ec6e0ea2b829320a7762107527a8c66d1754ec730c8b8	213
eiprtvchdcom/drupal	c7490c9e2a437e111968e96529cef80bc0d92a7040b656e2404114837e270941	131
vesnpsexga/joomla	3978fb1b4d9581fddbd44f44901e87f9f8baf7942c74d5820c573c06cc83f861	118
ganodndentcom/drupal	380898334e75e10cc1e5cf4c574d46e57f8b32f52552924fc1f5c158a7fb3291	55
dogigeronracom/drupal	50c1685bfcd67435188e74c8b5321de32f44f0c613fc2eebdbff3020273e690a	37
pumevnezdiroorg/drupal	bf9c24747d7c2903cf931a0a321f37c44fe6236dc40679d4cec3743384943e40	31

Źródło: 2022 Sysdig Cloud-Native Threat Report

Złośliwe obrazy
Rekomendacje

- Skanowanie bezpieczeństwa obrazów
  - BOM
  - Dockerfile - audyt
- Aktualizacje
- Akceptacja bazowych obrazów

Narzędzia developerskie



Kto robił hotfixa bezpośrednio na produkcji lub obchodząc polityki akceptów?

Co może być złego w narzędziach?

Release server

- Kto może zreleasować aplikację?
- Kto może zreleasowac aplikację z dowolnego brancha?

Pipeline

- Czy zmiany w pipeline są audytowane?

Budowa aplikacji

- Czy build jest zautomatyzowany/powtarzalny?
- Kto ma dostęp do build serwerów?
- Jak często aktualizujemy build serwery tym agenty?

Repozytoria

- Kto może skasować brancha?
- Kto może zmergować sie z `main` bez akceptacji?
- Czy jesteśmy w stanie wyśledzić kto dokonał zmiany wymagań akceptacji?
- Czy w repozytorium nie ma sekretów?

Serwery

- Kto ma dostęp do serwera produkcyjnego?

Ataki na narzędzia deweloperskie

- SolarWinds – złośliwy kod wykonany przez zainfekowanie platformy, z której korzystało wiele aplikacji – zainfekowanie procesu kompilacji
- Codecov – atak na narzędzie do budowania obrazów

Narzędzia deweloperskie
Rekomendacje

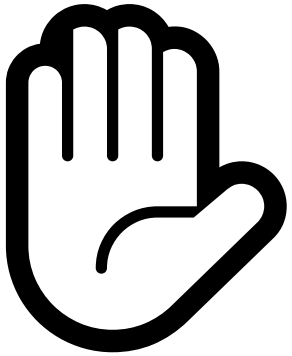
- Hardening
- Least privilige principle

Ludzie

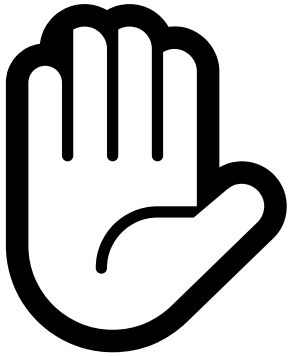
Ludzie
Co nam grozi?

Rodzaje problemów:

- (sensacyjny) konkurencja
- (złośliwy) jak kogoś zwolnimy
- (realny) zwykły ludzki błąd



Kto wie, że w jego firmie przeprowadza się screening nowych pracowników?



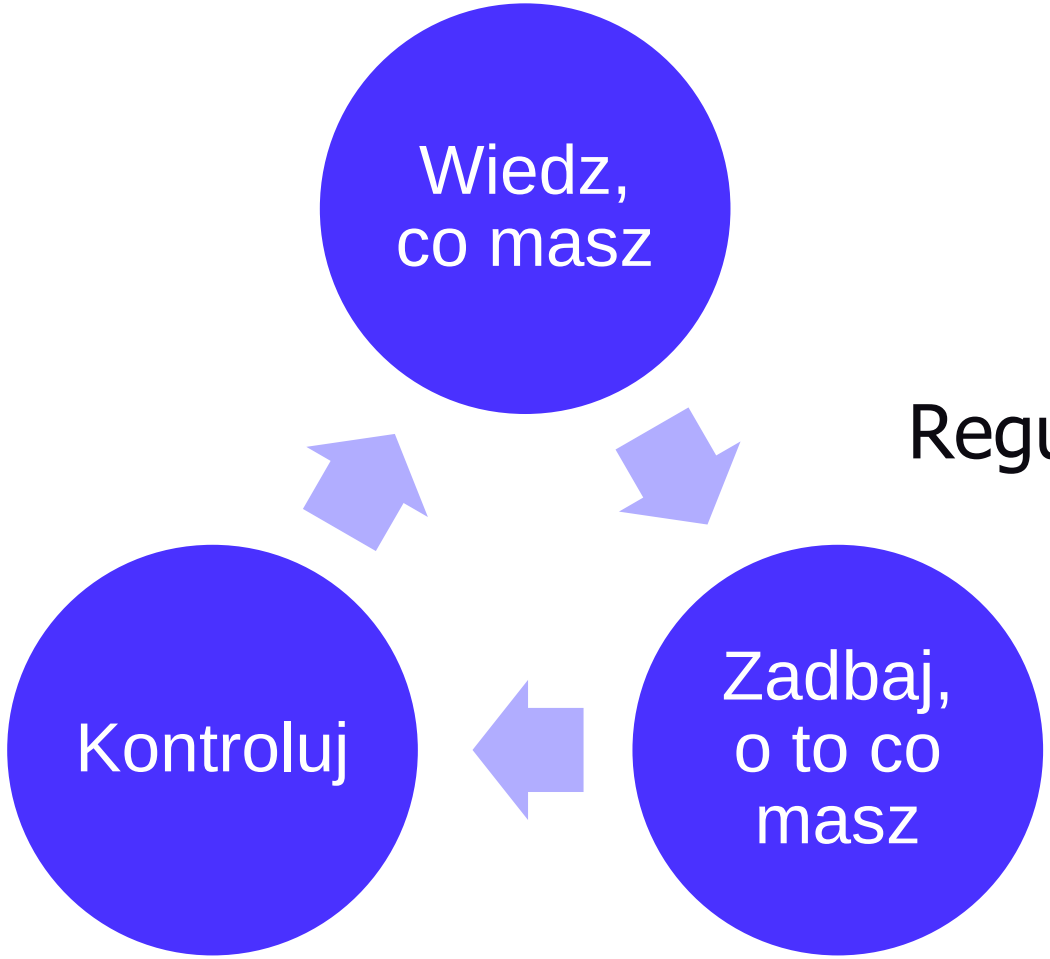
Kto przeprowadzał analizę ryzyka ze strony deweloperów?

Ataki na deweloperów

Zabezpieczenie ludzi
Rekomendacje

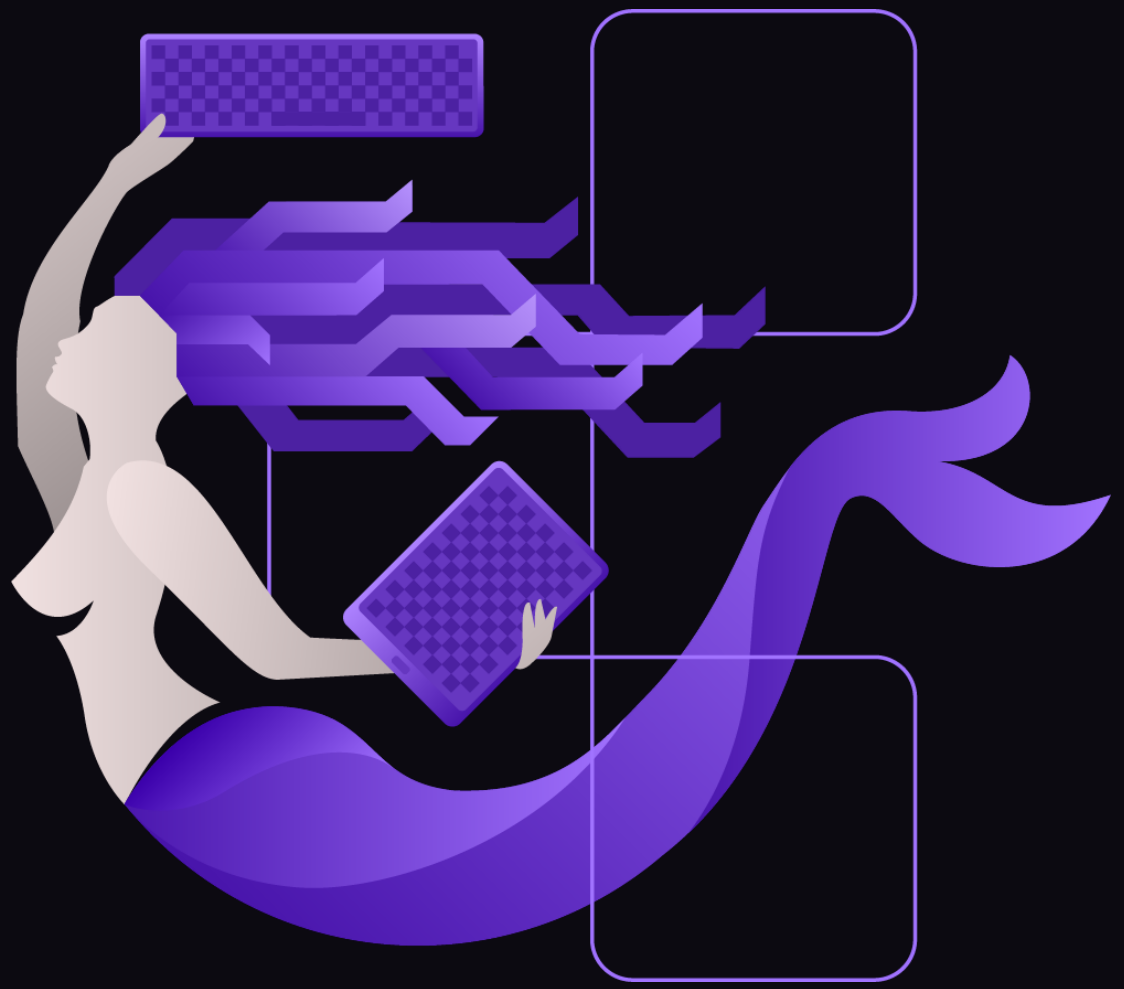
- Nauka ludzi - awareness
- Least privilige principle

Supply Chain Security
Co możemy zrobić?



Regularnie powtarzaj

WDI WARSZAWSKIE DNI INFORMATYKI



Dziękujemy za oglądanie!

Zapraszamy do zadawania pytań
oraz oceny prelekcji pod nagraniem.

Konkurs

https://www.diwebsity.com/wdi

Biuletyn Bezpieczeństwa Aplikacji

https://securitychampions.pl/

www.WarszawskieDniInformatyki.pl | 31 marca - 1 kwietnia 2023 | Politechnika Warszawska + online

ORGANIZATOR GŁÓWNY: Academic Partners FUNDACJA

KOMITET ORGANIZACYJNY: kilkadziesiąt organizacji z sektora IT / data science (pełna lista na stronie wydarzenia)