DevSecOps – narzędzia, czy kultura organizacyjna i sposób pracy?

WOJCIECH TWARÓG

Nationale-Nederlanden

Wyzwanie

Organizacja w zmianie

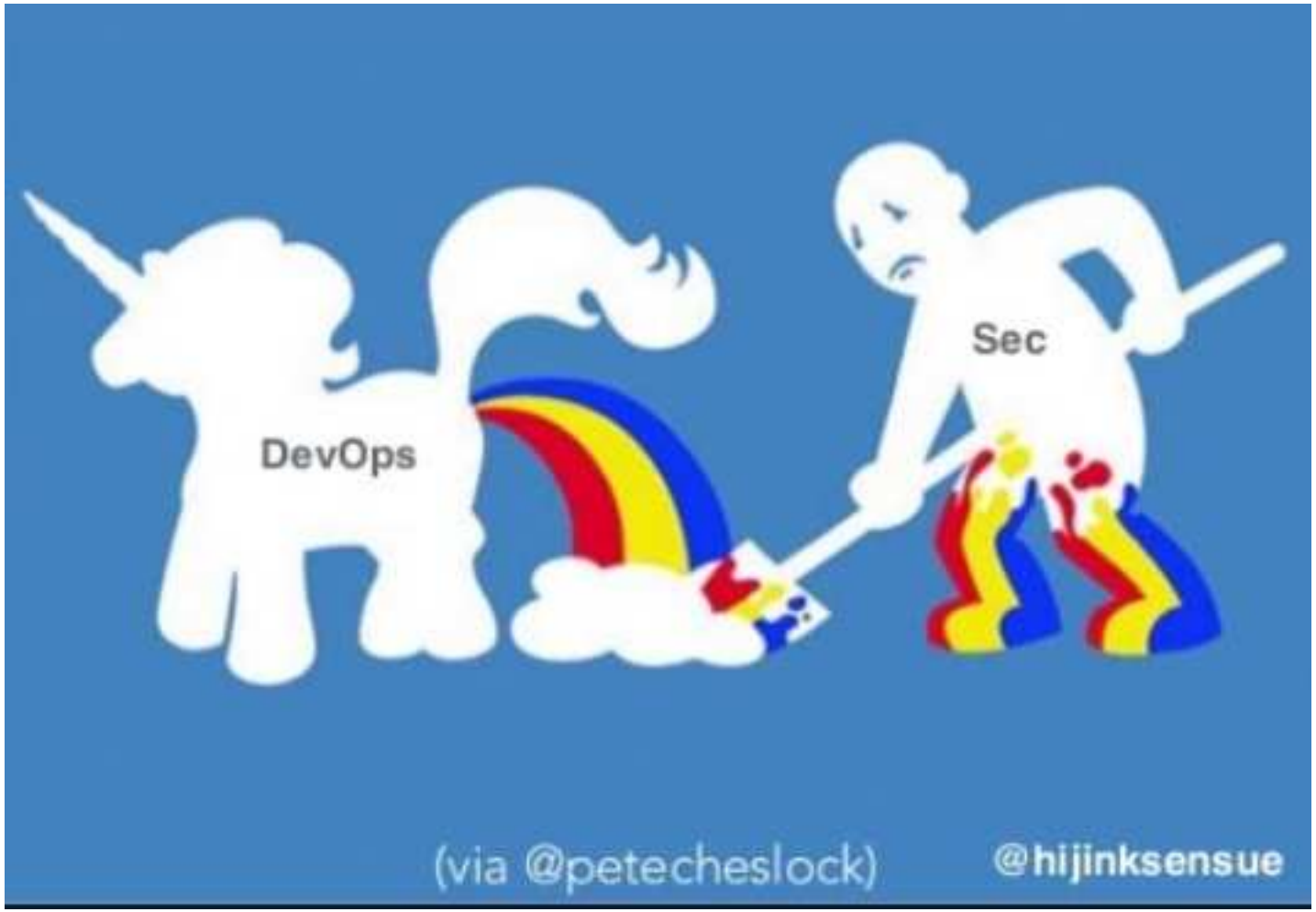
Raczkujący DevOps

Agile hype

Jesteśmy agile!

„Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan”

Co o tym myśli Security?



Security postrzegane jako hamulcowy

Security postrzegane jako hamulcowy


DEV
SEC
OPS

Wdrożenie

Wizja

Aplikacje tworzone bezpiecznie

Programiści i Inżynierowie Bezpieczeństwa współpracują

Bezpieczeństwo jest częścią cyklu życia i rozwoju aplikacji

Zmiana kulturowa - porzucenie postawy "my kontra oni"

Niezbędne jest…

Łap okazję - Transformacja Cyfrowa

Inspiracje

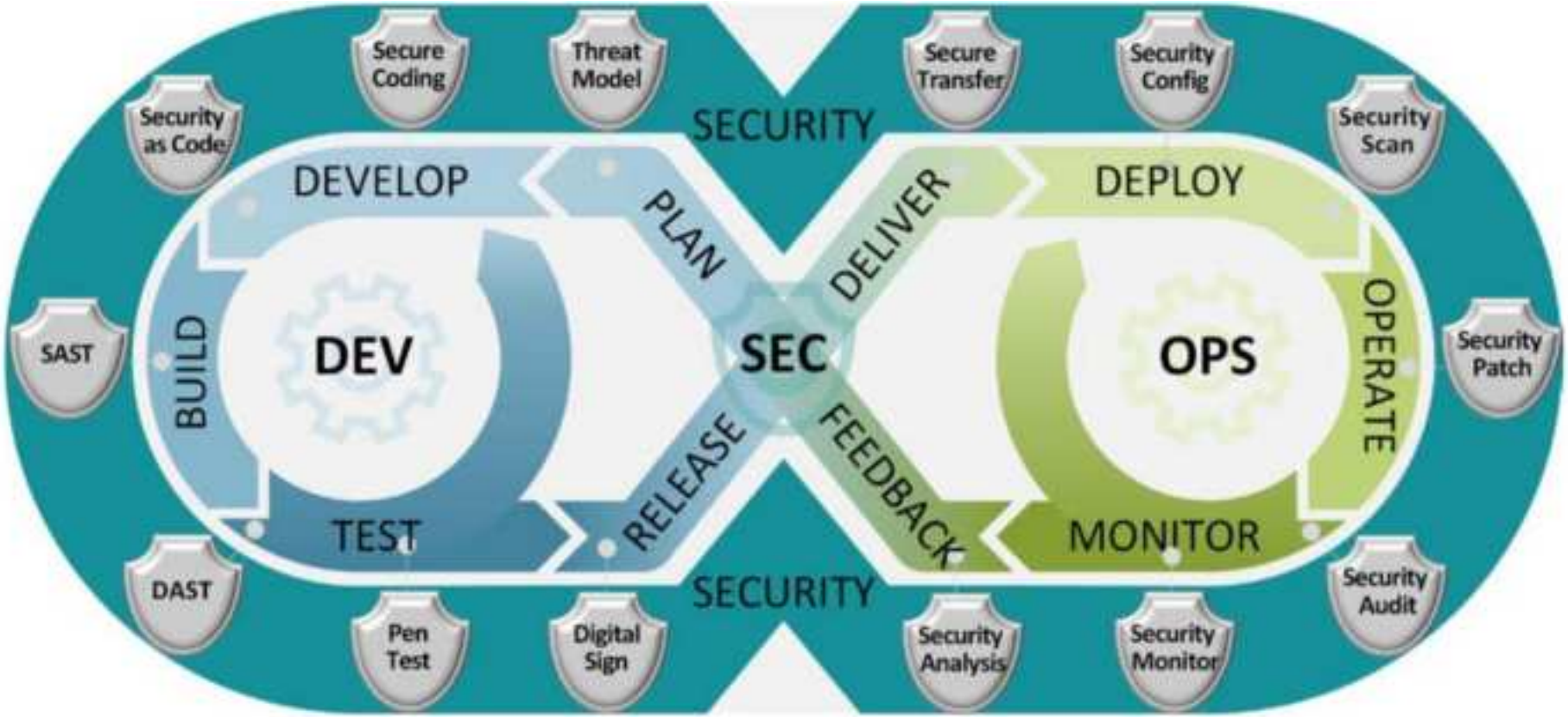
Microsoft

cisco

- Security needs to „come bearing gifts” – Netflix
- „Culture is top-down. Training is bottom-up” – Microsoft
- „Push to (…) as a Code needs to come from C-level” – Cisco
- „Everything we do is open source. The entire code and the entire Infrastructure as a Code is open to the public” - DoD

NETFLIX

Inspiracje – DoD USA



Inspiracje – Deming and Toyota Lean Manufacturing

ADVANCED THREAT SUMMIT

- Pozyskuj materiały od najlepszych dostawców
- Pozyskuj tylko najlepsze części od najlepszych dostawców
- Śledzenie użycia części w całym procesie produkcyjnym
- BOM by można było przeprowadzać akcje serwisowe wadliwych części

- Korzystanie z zaufanych repozytoriów artefaktów
- Używanie zatwierdzonych artefaktów o wysokiej reputacji
- Śledzenie użycia podpisanych artefaktów (obrazów platformy
- SBOM by móc wycofać z użycia wadliwe artefakty

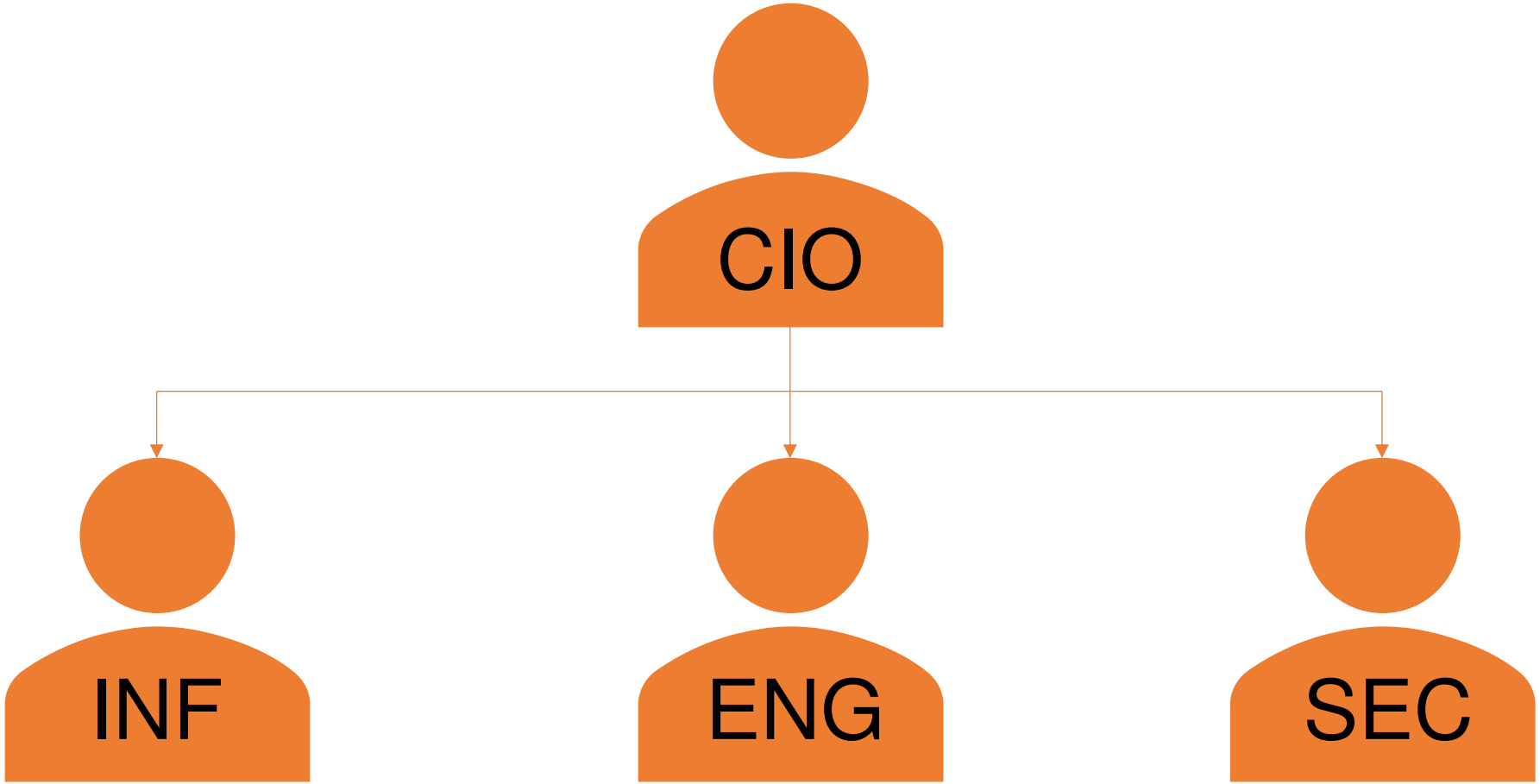
ADVANCED
THREAT
SUMMIT

Strategia

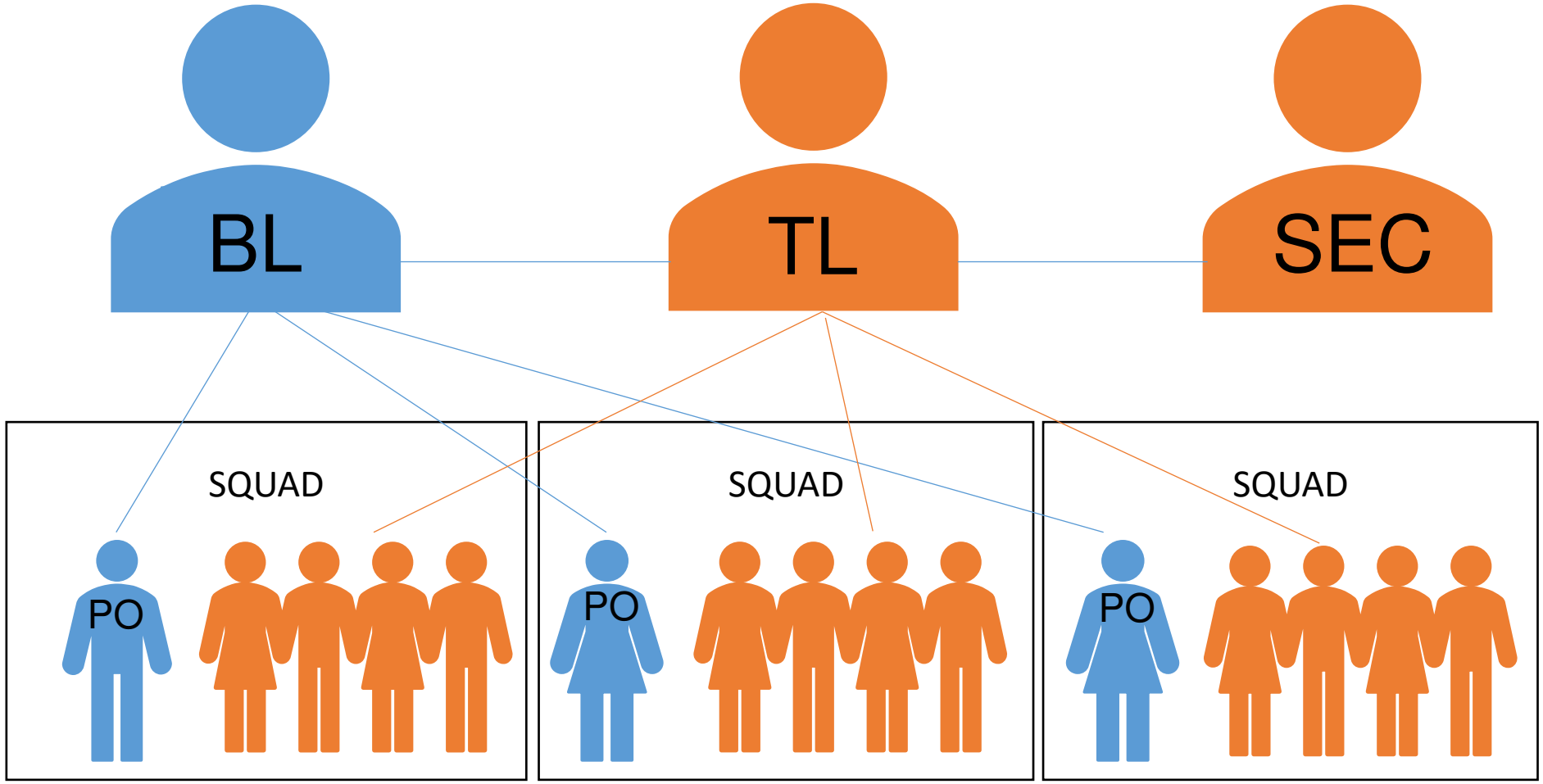
Nowy model operacyjny

				
Strumienie Wartości podzielone wg segmentów	3 jednostki wspierające • IT Governance • Cyberbezpieczeństwo • Infrastruktura	Zaangażowanie Cyberbezpieczeństwa • Co najmniej 0.5 FTE na Strumień Wartości	Wspólne inicjatywy • SRE • Cloud community	Docelowy model raportowania Sec • Matrycowo do Szefa Cyberbezpieczeństwa • … za wiele lat

Organizacja IT



Organizacja – zespoły wytwórcze



Zmiana kulturowa

ADVANCED THREAT SUMMIT

- Szkolenia i dzielenie się wiedzą
- Otwartość i sztuka kompromisu
- Budowanie zaufania
- Bezpieczeństwo wspiera merytorycznie
- Wolność i odpowiedzialność
- Hackowanie – to się dzieje naprawdę

Budowa zespołu SRE

- Entuzjaści z różnych obszarów
- Budowanie narzędzi „dla siebie”
- Cel nr 1 - Wypracowanie MVP
- Przestrzeń na testy i wybuchy
- Czas na rozwój i utrzymanie CI/CD

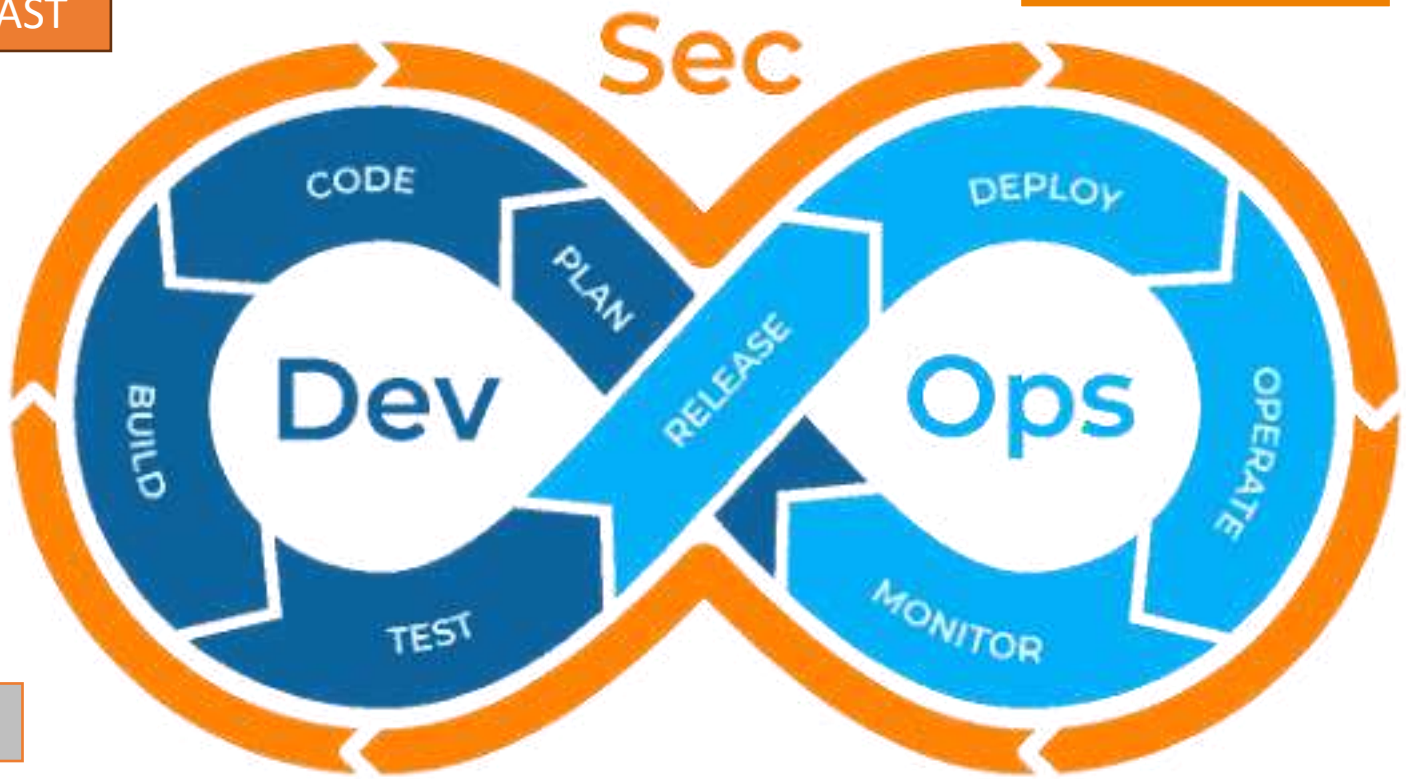
MVP

Code review

Threat Modeling

Secrets Management

SAST



Container and Host Security

DAST

Penetration testing

Security Monitoring

Źródło grafiki:https://srilaguduva.com/blog/devsecops-way/

Faza 2

Code review

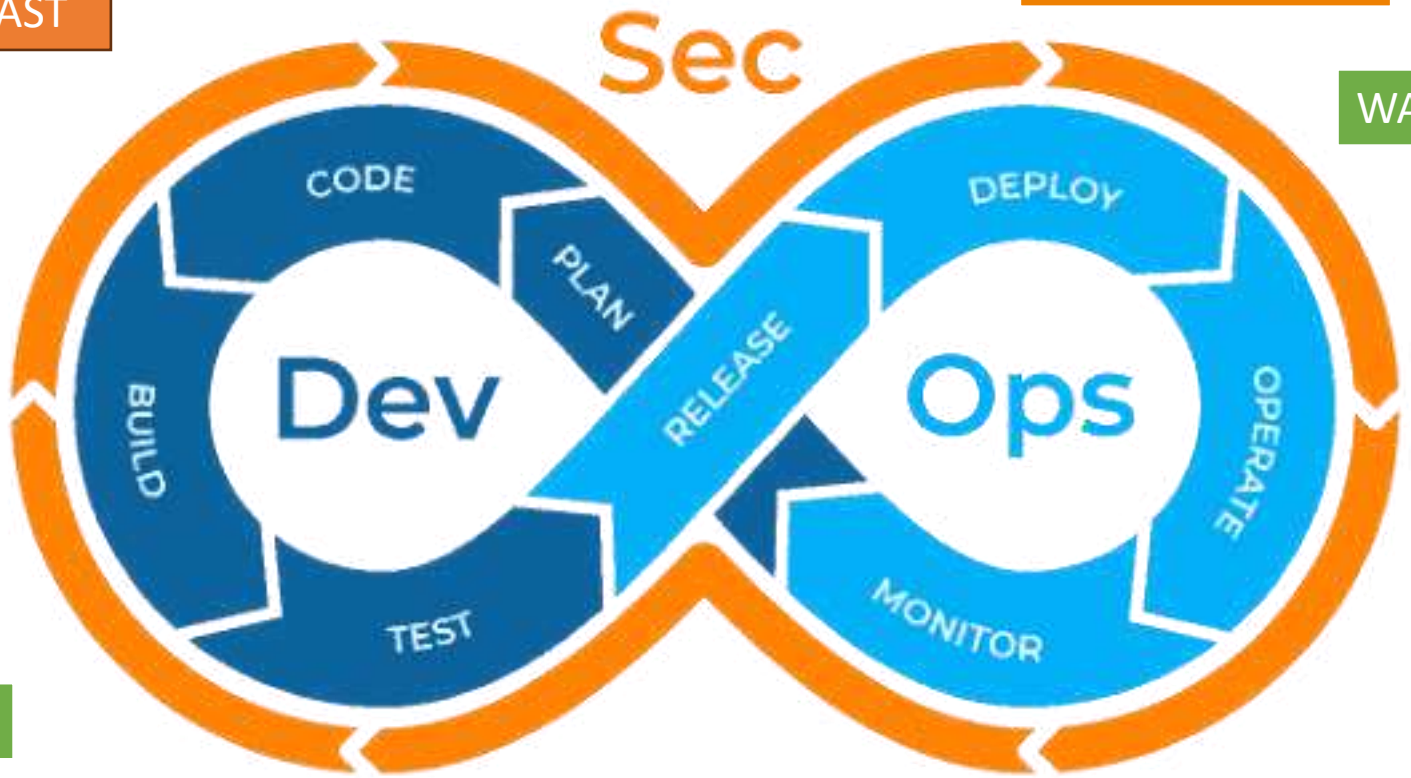
Threat Modeling

Secrets Management

SAST

WAF rules

Repo Scan



Dependency Check

Container and Host Security

SBOM

DAST

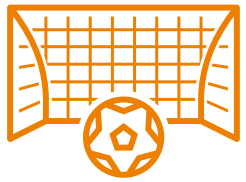
Penetration testing

Security Monitoring

Źródło grafiki:https://srilaguduva.com/blog/devsecops-way/

Wynik

Wynik

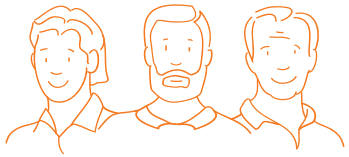


Gramy do jednej bramki

Bezpieczeństwo angażowane jest na początku inicjatyw

Kultura bezpieczeństwa wbudowana w organizację

Wynik



Zespoły dzielą się wiedzą i szkolą nawzajem

Znacząco wzrosła jakość produkowanych aplikacji

Szybciej i częściej dostarczamy zmiany

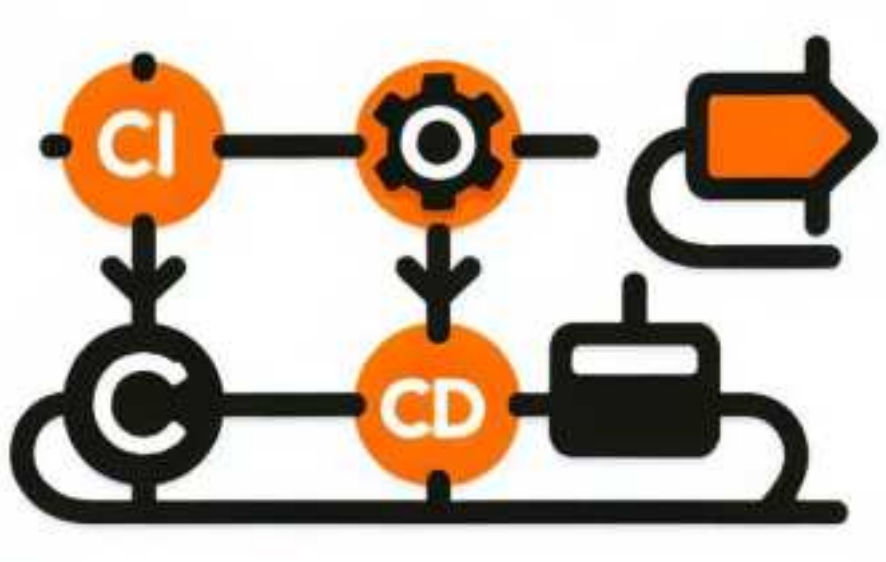
Mamy CI/CD pipeline, z wbudowanymi bramkami bezpieczeństwa

Wnioski

Kultura zjada strategię na śniadanie

DevSecOps, to ludzie...
...i trochę narzędzi

Nieustanna edukacja jest koniecznością



Standaryzacja pipeline’u przynosi realne korzyści

Utrzymanie wysokiej dojrzałości procesu, kosztuje

Warto było!