CERT.PL>_

Protecting country-sized constituencies

2024-03-27, TRUST aWARE workshop



What a National CSIRT does?

- NIS defines a baseline for national CSIRTs ... but implementation varies significantly
- Poland case: 3 national-level teams
 - GOV: central government + critical infrastructure
 - MOD: military-related
 - NASK \rightarrow CERT.PL: everything else



Our constituents (simplified)

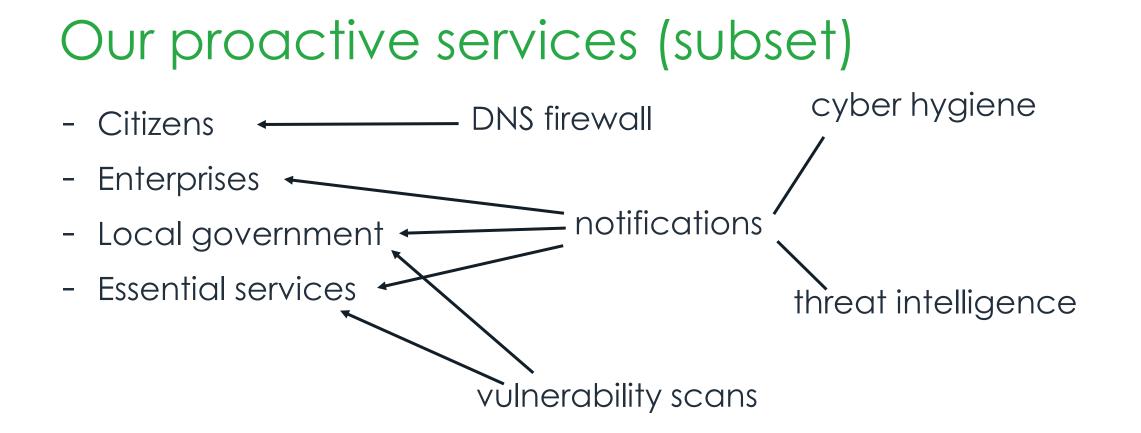
- Citizens
- Enterprises
- Local government
- Essential services



Common threats (subset)

- Enterprises ransomware
- Local government
- Essential services espionage







What are we looking for?

- Information: CTI, vulnerable devices, anything relevant
- Tools supporting our work = force multiplier
- Products for our constituents:
 - advisories
 - best practices
 - free tools, services



conte (ves): cenge.min_points + (challenge.max_points - challenge.min_points) /
(max(0, solves - 1) / 11.92201) ** 1.206069))) hallenge, flag): ent_session.is_authenticated: ChallengesService.UserNotAuthenticated() est = repository.contests['by_slug'][challenge.contest] log.info('incorrect flag', {'challenge': challenge, 'flag': flag)) not challenge.flag.strip() == flag.strip(): WrongFlagException() solve = Solve db.session.add(sc challenge, 'flag': flag}) db.session.commit log.info('correct fl except (IntegrityError, eAlreadySolved() db.session.rollb raise Chall*

urn

CERT.PL>_ NASK

Thank you for attention.

https://cert.pl/en/

https://github.com/CERT-Polska/