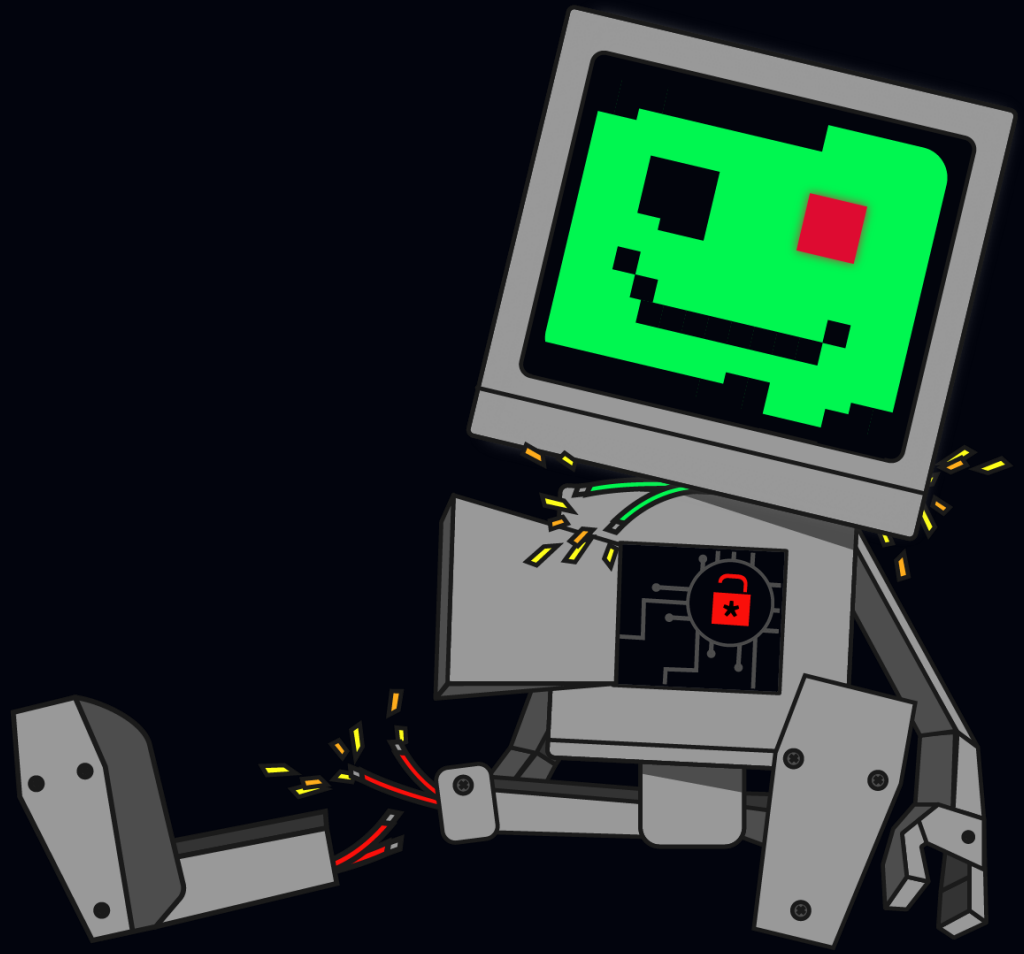
THE H@CK SUMMIT



C:\>

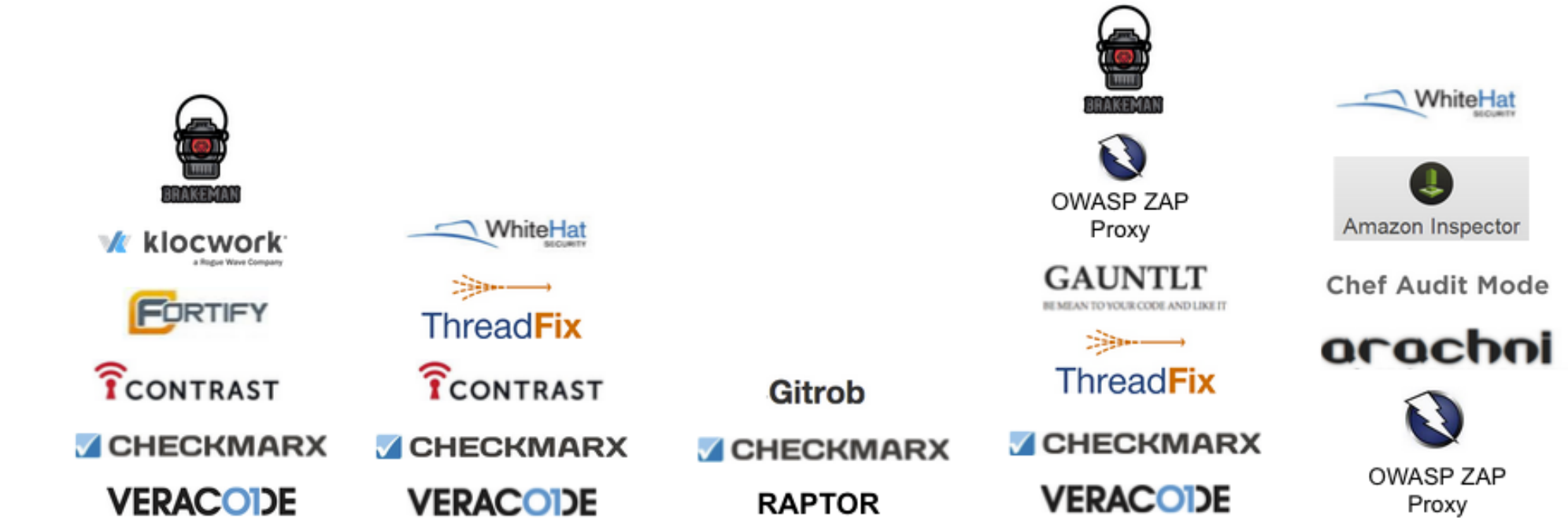
Jak wspierać deweloperów w bezpiecznym kodowaniu

Adrian Sroka
Software Security Architect

thehacksummit.com 13-14 października 2022 PGE Narodowy + Online

ORGANIZATORZY: Academic Partners Fundacja

Jak dbać o bezpieczeństwo?



https://owasp.org/www-project-appsec-pipeline/pipeline-tools

Kto najlepiej zadba o bezpieczeństwo aplikacji?

Deweloper

Dlaczego?

Ma największą wiedzę domenową i techniczną

Ale

Nie jest specjalista od bezpieczeństwa

Dev + Sec

Jak możemy pomóc deweloperom?

Szkolenie

Czy to brzmi znajomo?

1. Codzienna praca
2. Szkolenie bezpieczeństwa
3. Ekscytacja
4. Niewiele z tego pamięta

Automatyzacja

- DAST – mała wiedza o aplikacji
- SAST – wąski zakres zagrożeń
- SCA – wartościowe, ale nie sprawdza naszego kodu

Nie jest idealnie

Jaki deweloperzy mają problem z bezpieczeństwem?

- Deweloperzy nie czują się swobodnie
- Brak czasu, żeby poczuć bezpieczeństwo
- W konsekwencji nie stosują się do zasad

Jak więc pomóc developerom?

- Sprawmy, żeby bezpieczeństwo weszło im w krew

Ale…

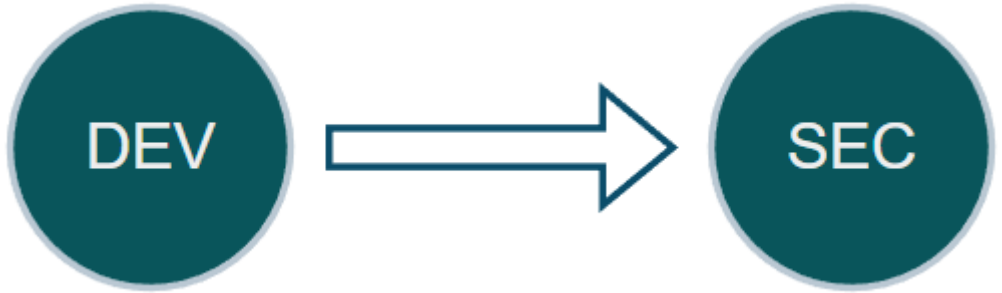
- Łatwo powiedzieć trudniej zrobić

5 metod jak pomóc deweloperom

To może być proste

Ostrzeżenie

- Bazuje to na doświadczeniu i eksperymentach
- Subiektywne



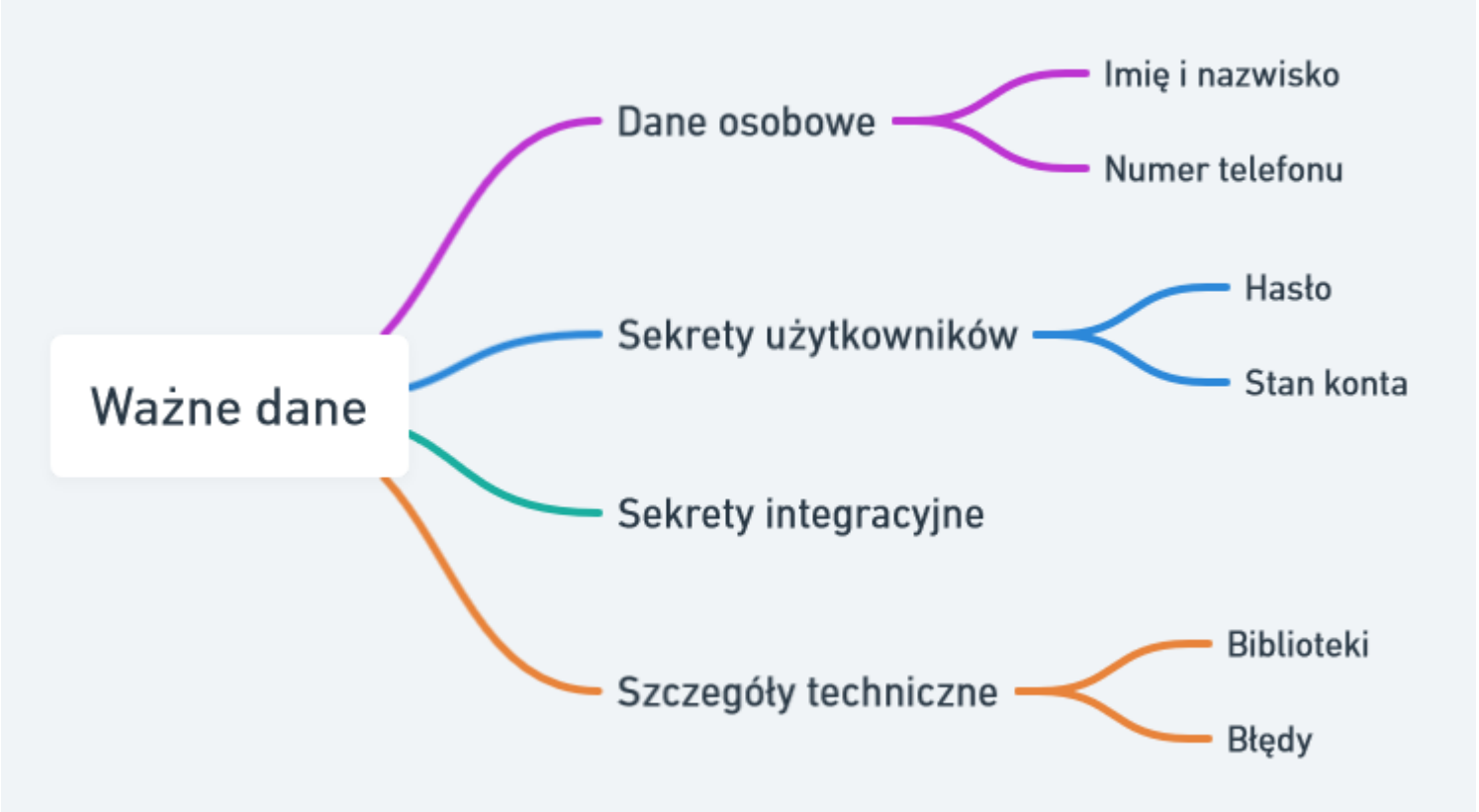
1. Zbudowanie świadomości ważnych obszarów

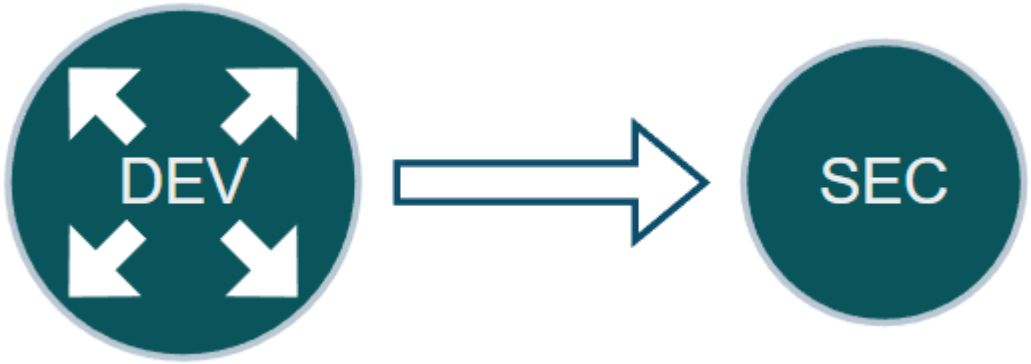
Nie muszę wiedzieć jak sobie z tym poradzić, wystarczy wiedzieć w jakich przypadkach mam dopytać

Zbudowanie świadomości ważnych obszarów

Budowa mapy tego co ważne:

- obszary
- dane
- funkcjonalności





2. Ułatwienie decyzji

Nawet gdy nie wiem, co będzie najlepsze, wiem gdzie znajdę pomoc

Ułatwienie decyzji

Rodzaje decyzji

- wybór technologii
- biblioteki
- algorytmy
- dobre praktyki

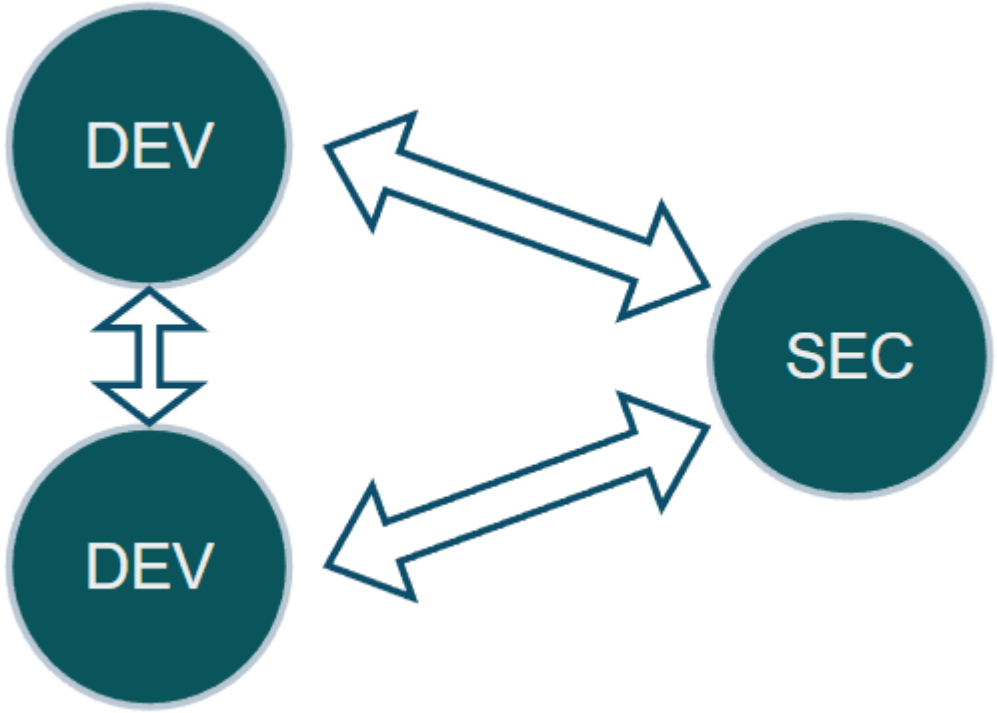
Ułatwienie decyzji

Automatyzuj decyzje tak samo jak automatyzujesz testy

Narzędzia:

- checklisty
- bazy wiedzy
- modele myślowe
- polityki – krótkie

Jeżeli funkcjonalność dotyczy...	**... oraz ...**	**... zadaj następujące pytania**
Backend	Pliki	• Czy walidujemy pliki podczas uploadu? ◦ Czy sprawdzamy wielkośc, rozszerzenie, content type? • Czy pliki podlegają skanowaniu antywirusowemu? File Upload Cheatsheet



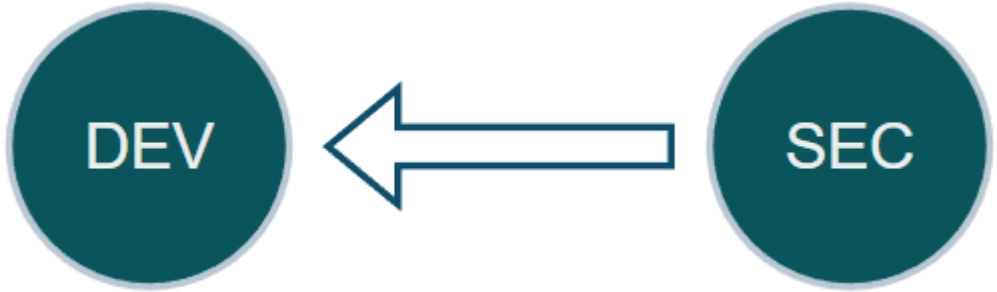
3. Miejsce do dyskusji

Zawsze mam się do kogo odezwać z moim problemem

Miejsce do dyskusji

Tworzenie społeczności

- w ramach zespołu
- Security Champions

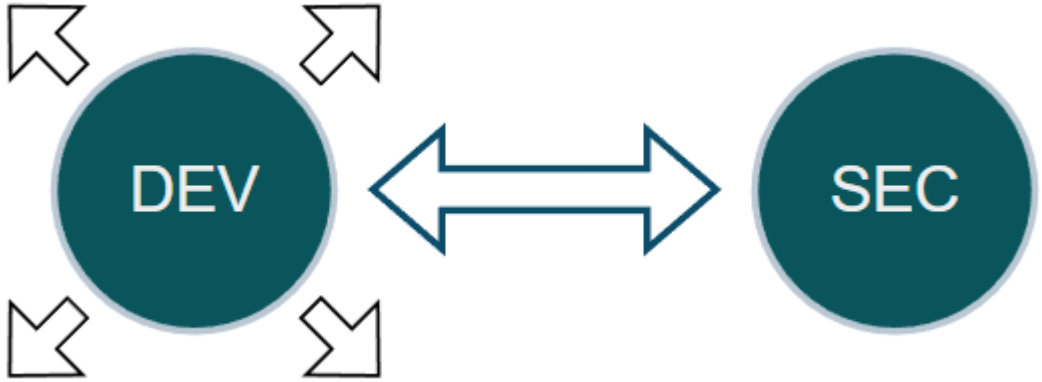


4. Regularna ekspozycja

Systematycznie słyszę o bezpieczeństwie i o tym, co się dzieje w tym temacie w firmie

Regularna ekspozycja

- Przypomnienia
- Newslettery
- Transparencja działań



5. Zaangażowanie

Regularnie mogę zweryfikować moją wiedzę i testować nowe pomysły

Zaangażowanie

- Możliwości sprawdzenia się
- Wspólne wyzwania
- Włączenie w decyzje
- Hackatony
- Ćwiczenia

5 kluczowych aspektów

1. Zbudowanie świadomości ważnych obszarów
2. Ułatwienie decyzji
3. Miejsce do dyskusji
4. Regularna ekspozycja
5. Zaangażowanie

Wspólny mianownik

- Komunikacja
- Security Champions

Security Champions

- Społeczność ludzi zainteresowanych bezpieczeństwem

Jakie problemy rozwiązuje?

- Skalowanie - Specjaliści bezpieczeństwa nie mogą być w każdym zespole
- Eliminuje dystans – zbliża deweloperów i bezpieczeństwo

Security Champions – jak to zrobić dobrze

https://github.com/c0rdis/security-champions-playbook/blob/master/assets/img/playbook.png

Security Champions – jak to zrobić dobrze

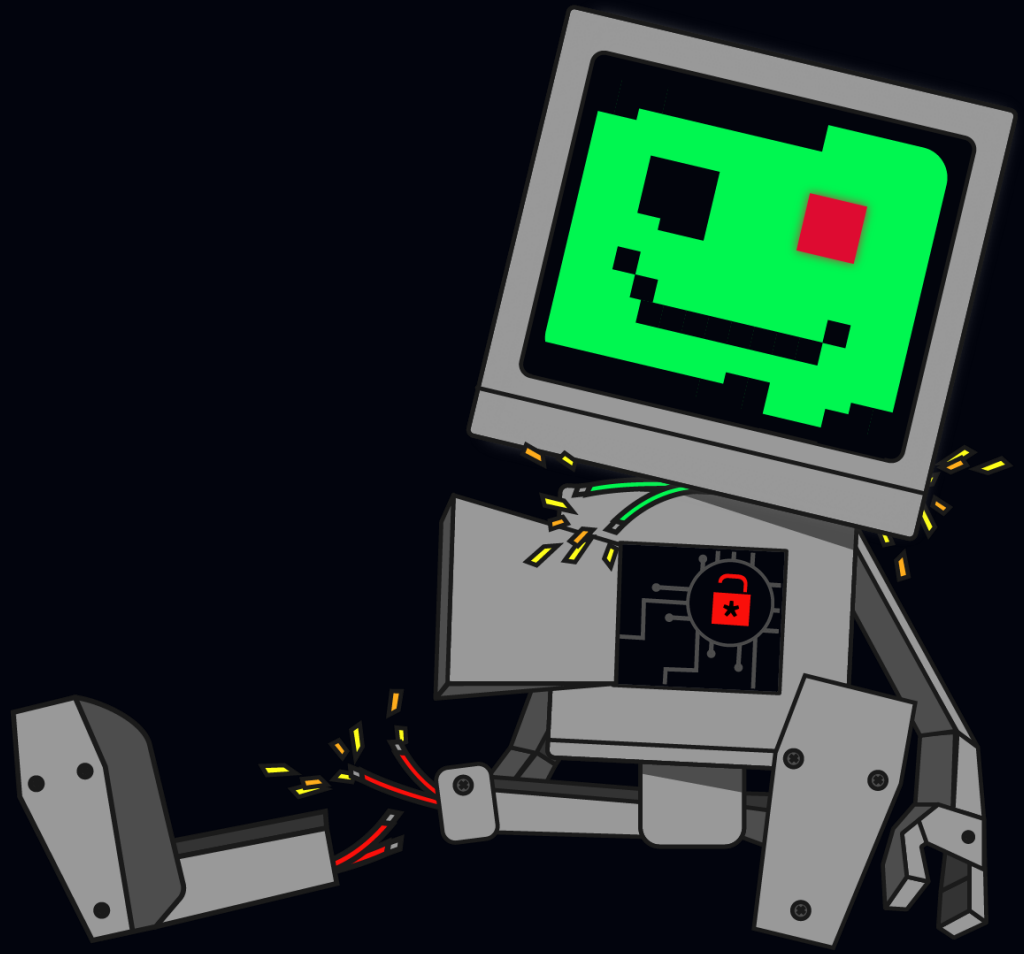
Jak utrzymać zainteresowanie?

- Są na bieżąco z tym co się dzieje w firmie
- Wiedzą więcej niż inni
- Mają większe możliwości

THE H@CK SUMMIT

Dziękujemy za uwagę!

Zapraszamy do **zadawania pytań**
oraz **oceny wystąpienia**
pod nagraniem.



Dla tych, którzy mnie uważnie słuchali - konkurs:
https://www.diwebsity.com/devsec

thehacksummit.com | 13-14 października 2022 | PGE Narodowy + Online

ORGANIZATORZY: Academic Partners Fundacja | Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni