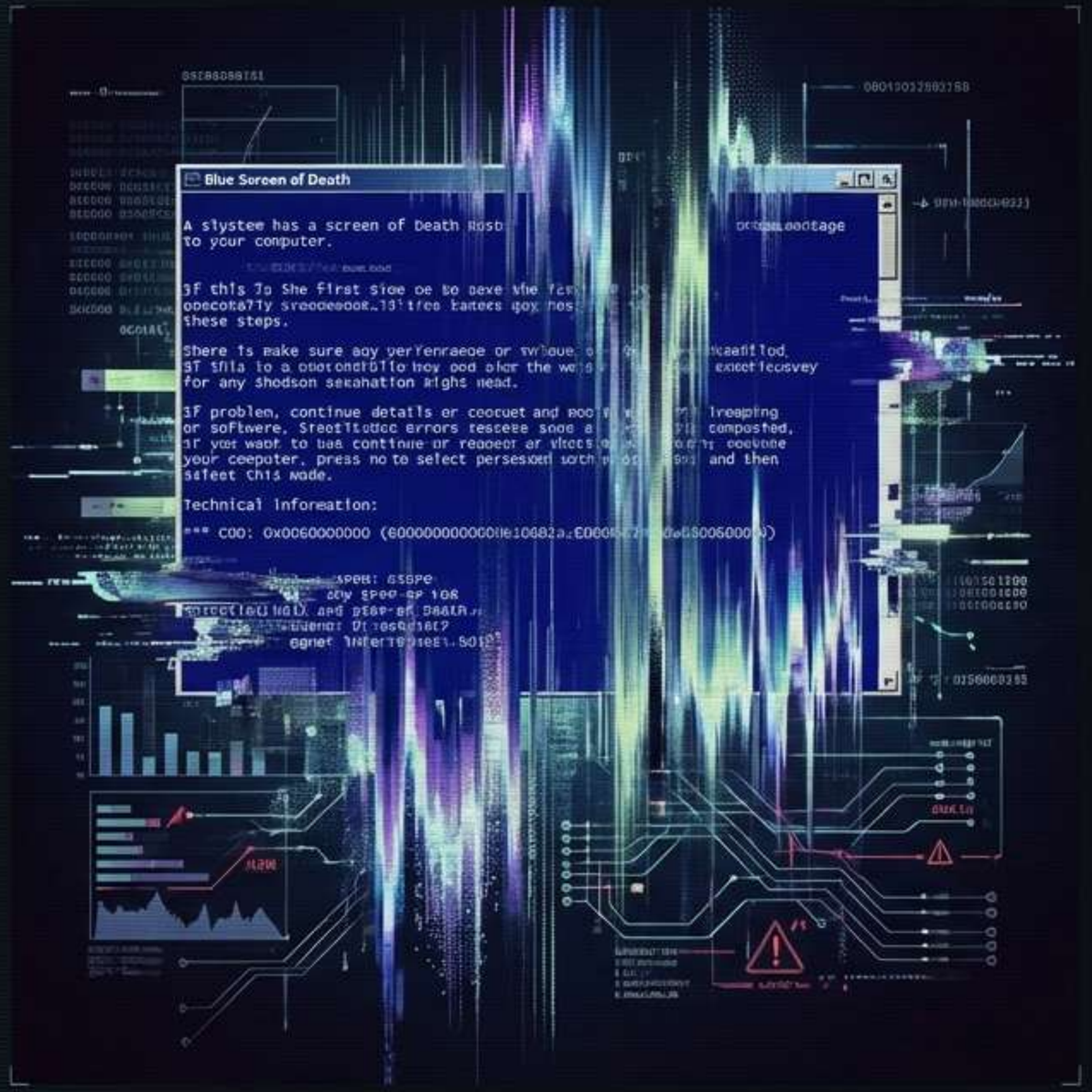
GARM: ARCHITEKTURA SUWERENNOŚCI CYFROWEJ

Izolacja Pre-OS i Ochrona w Środowisku Hostile Environment

[CONFIDENTIAL / DEEP TECH R&D]



ERA 'HOSTILE ENVIRONMENT' – SYSTEM OPERACYJNY TO POLE BITWY

- KATASTROFA 2024: Incydenty klasy CrowdStrike udowodniły kruchość systemów EDR działających wewnątrz OS.
- KOSZT WYCIEKU: Średni koszt wycieku danych: $4.88 mln. W sektorze finansowym: $6.08 mln.
- ZAGROŻENIE: Szpiegostwo przemysłowe (Insider Threats) kosztuje firmy średnio $17.4 mln rocznie.

Źródło: IBM Cost of a Data Breach Report 2024

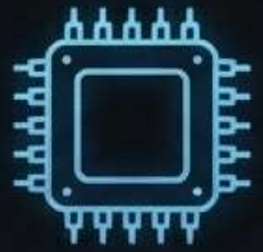
BEZPIECZEŃSTWO POZA SYSTEMEM

- NIEZALEŻNOŚĆ: Autorska izolacja na osi Ring-0. GARM operuje poniżej systemu operacyjnego.
- PRE-OS: Uruchomienie w warstwie UEFI, zanim malware przejmie kontrolę.
- IZOLACJA: Własny, wirtualny system plików (VFS) i renderowanie grafiki niezależne od API Windowsa.

INŻYNIERIA DEEP TECH – FUNDAMENT NIENARUSZALNOŚCI

RUST (RING-0)

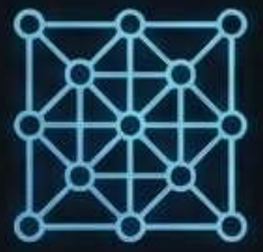
Bezpieczeństwo pamięci (Memory Safety) i wydajność. Eliminacja 80% narzutu obliczeniowego w porównaniu do rozwiązań legacy.



KERNEL DRIVERS (C++)

Niskopoziomowa kontrola nad sprzętem (Windows NT Driver Hooks).

Bezpośrednie zarządzanie przerwaniami PCI.



POST-QUANTUM CRYPTOGRAPHY

Gotowość na przyszłość: Algorytm Argon2id i architektura odporna na komputery kwantowe.

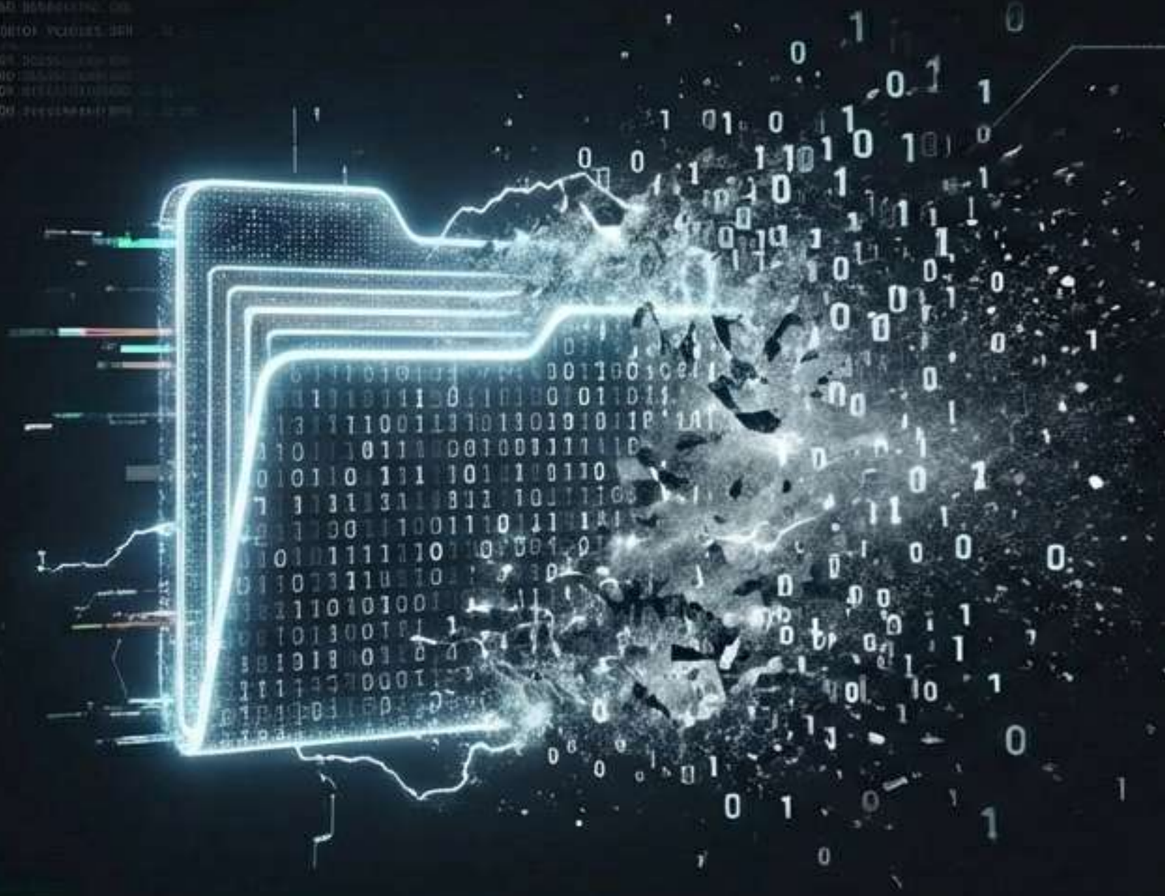
GHOST RENDERER – NIEWIDZIALNOŚĆ DLA SPYWARE

- OBEJŚCIE DWM: GARM rysuje interfejs bezpośrednio na buforach GPU, omijając Desktop Window Manager.
- EFEKT: Malware wykonujący zrzut ekranu widzi jedynie czarne piksele.
- ZERO-TRACE VFS: Brak pliku .exe w systemie. Dla Windowsa GARM jest niewidocznym szumem na dysku.

HARDWARE KILL-SWITCH & ANALIZA BEHAWIORALNA

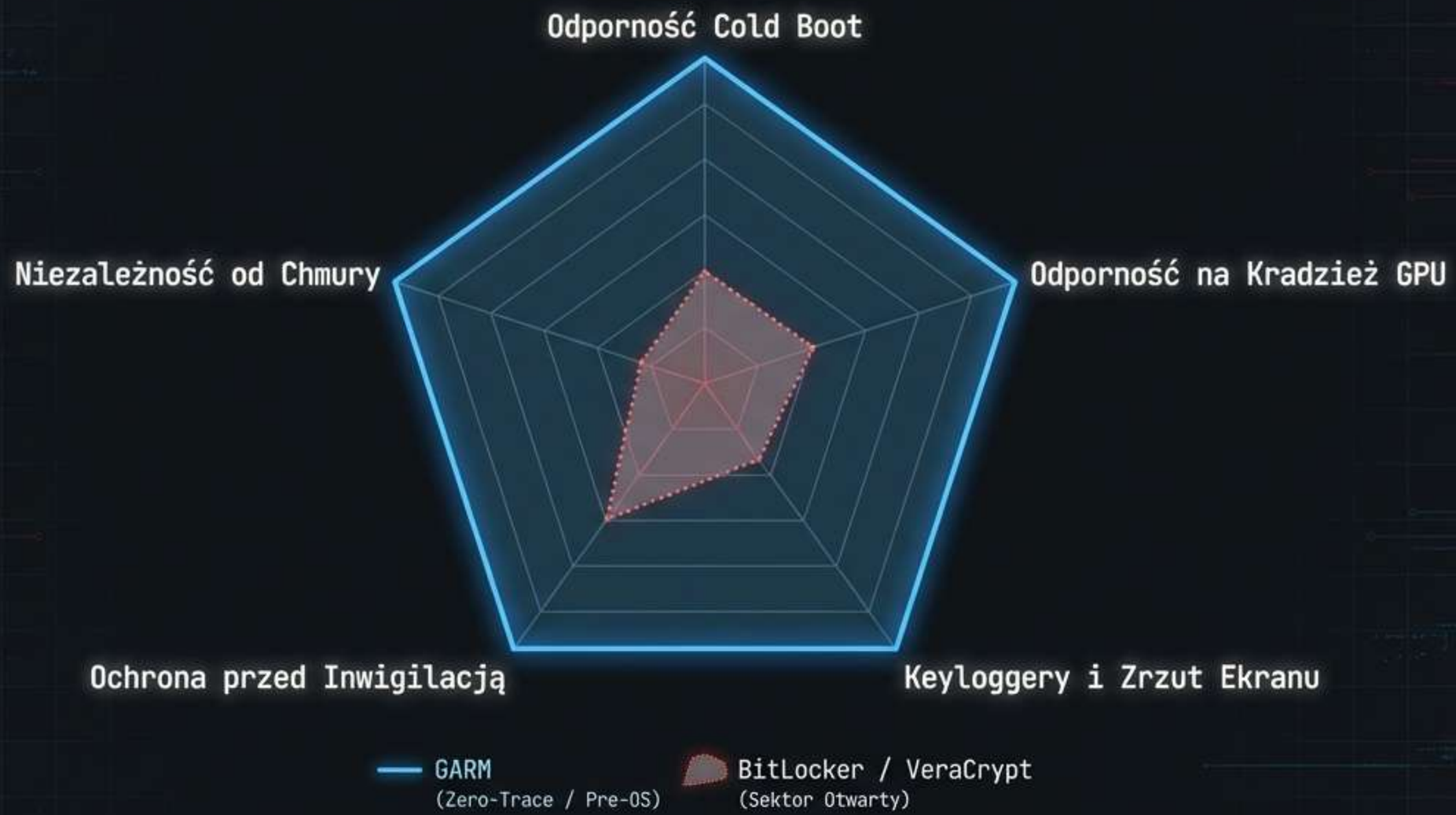
1. BLOKADA SPRZĘTOWA: Fizyczne odcięcie mikrofonu i kamery na poziomie sterowników PCI.
2. AI PROFILER: Lokalna sieć neuronowa (uruchamiana na CUDA) analizuje biometrię pisania i ruchów myszą.
3. WYKRYWANIE PRZYMUSU: Natychmiastowa reakcja na anomalie behawioralne sugerujące fizyczny przymus obsługi.

PROTOKOŁY PANIC WIPE – GDY WSZYSTKO INNE ZAWIEDZIE



- CRYPTOGRAPHIC ERASE: Błyskawiczne nadpisanie kluczy szyfrujących w RAM. Dane stają się cyfrowym szumem w milisekundach.
- DECOY VAULTS: Fałszywe hasła otwierające 'czyste' konto-pułapkę (Plausible Deniability).
- OCHRONA NA GRANICACH: Rozwiązanie problemu wymuszonego dostępu przez służby celne lub grupy przestępcze.

GARM VS. STANDARD RYNKOWY – ELIMINACJA PUNKTÓW AWARII



Tradycyjne szyfrowanie (BitLocker) nie chroni przed atakami w czasie rzeczywistym (Runtime).

ODPOWIEDŹ NA REGULACYJNE TRZĘSIENIE ZIEMI (EU 2027)

- CYBER RESILIENCE ACT: Nowe wymogi unijne. Kary do 15 mln EUR lub 2.5% obrotu za brak compliance.
- SUWERENNOŚĆ: Budowa Europejskiej Architektury Referencyjnej niezależnej od gigantów z USA.
- DUAL-USE: Technologia podwójnego zastosowania – krytyczna dla biznesu i sektora obronnego.

ZDYWERSYFIKOWANE ŹRÓDŁA PRZYCHODU

B2B SAAS ENTERPRISE

Model subskrypcyjny (Per-Seat) dla korporacji, Family Offices i funduszy Hedge.

B2G & DUAL-USE

Kontrakty rządowe, sektor obronny i infrastruktura krytyczna.

WHITE-LABEL API (PAAS)

Udostępnianie silnika szyfrującego dla Fintechów i banków.

PLAN AKCELERACJI: FAZA I & II (TRL 3 → TRL 5)

MVP & CORE ARCHITECTURE

Miesiąc 1 | Miesiąc 2 | Miesiąc 3 | Miesiąc 4 | Miesiąc 5 | Miesiąc 6 | Miesiąc 7 | Miesiąc 8 | Miesiąc 9

CORE TEAM

Rekrutacja inżynierów Senior Rust/Kernel.

PROOF OF CONCEPT

Ożywienie "GARM-Core" i architektury VFS.

GHOST WINDOW

De-kompilacja sterowników Windows i wdrożenie izolacji graficznej.

EKSPANSJA: FAZA III & IV (TRL 6 → TRL 8)

SCALING & COMMERCIALIZATION

EDGE-AI PROFILER

Implementacja modeli behawioralnych na kartach CUDA.

AUDYTY RED-TEAM

Zewnętrzna weryfikacja bezpieczeństwa (np. Cure53).

COMMERCIAL RELEASE

Gotowość rynkowa i sprzedaż licencji.

KONSORCJUM R&D – ELITA INŻYNIERII

STRUKTURA ORGANIZACYJNA I KOMPETENCJE

CEO

Ekspert ds. compliance, funduszy UE i zarządzania ryzykiem.

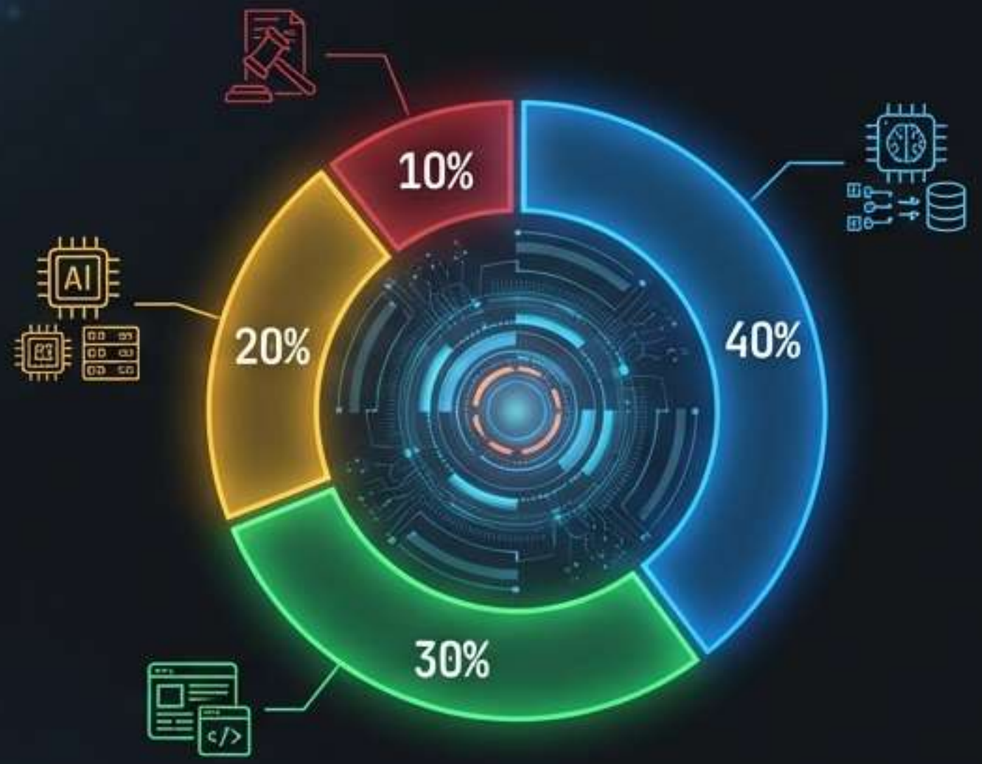
CTO / ARCHITEKT

Twórca architektury Zero-Trust, ekspert Ring-0 i Threat Modeling.

ZESPÓŁ DEEP TECH

Specjaliści Rust, C++ Kernel Drivers, AI Data Scientists.

STRUKTURA ALOKACJI KAPITAŁU (R&D)



CEL: 400,000 PLN

ALOKACJA:

- 40% - Deep Tech Engineers & Elite AI
- 30% - Web UI / Tauri Framework
- 20% - AI Training & Hardware
- 10% - Audyty Prawne


GARM: PRZYSZŁOŚĆ JEST PRYWATNA
Zapraszamy do współtworzenia nowego standardu bezpieczeństwa w Europie.
kontakt@garm-project.eu | www.garm-project.eu
NotebookLM