[CONFIDENTIAL / DEEP TECH R&D]

Hostile Environment Defense

GARM: Deep Tech Cybersecurity Architecture

Architektura Odporności w Erze Zero-Trust

Ring-0 Isolation // Rust Memory Safety // Sovereign Code

Świat się zepsuł, my go naprawimy.

Lekcja z CrowdStrike (Lipiec 2024)

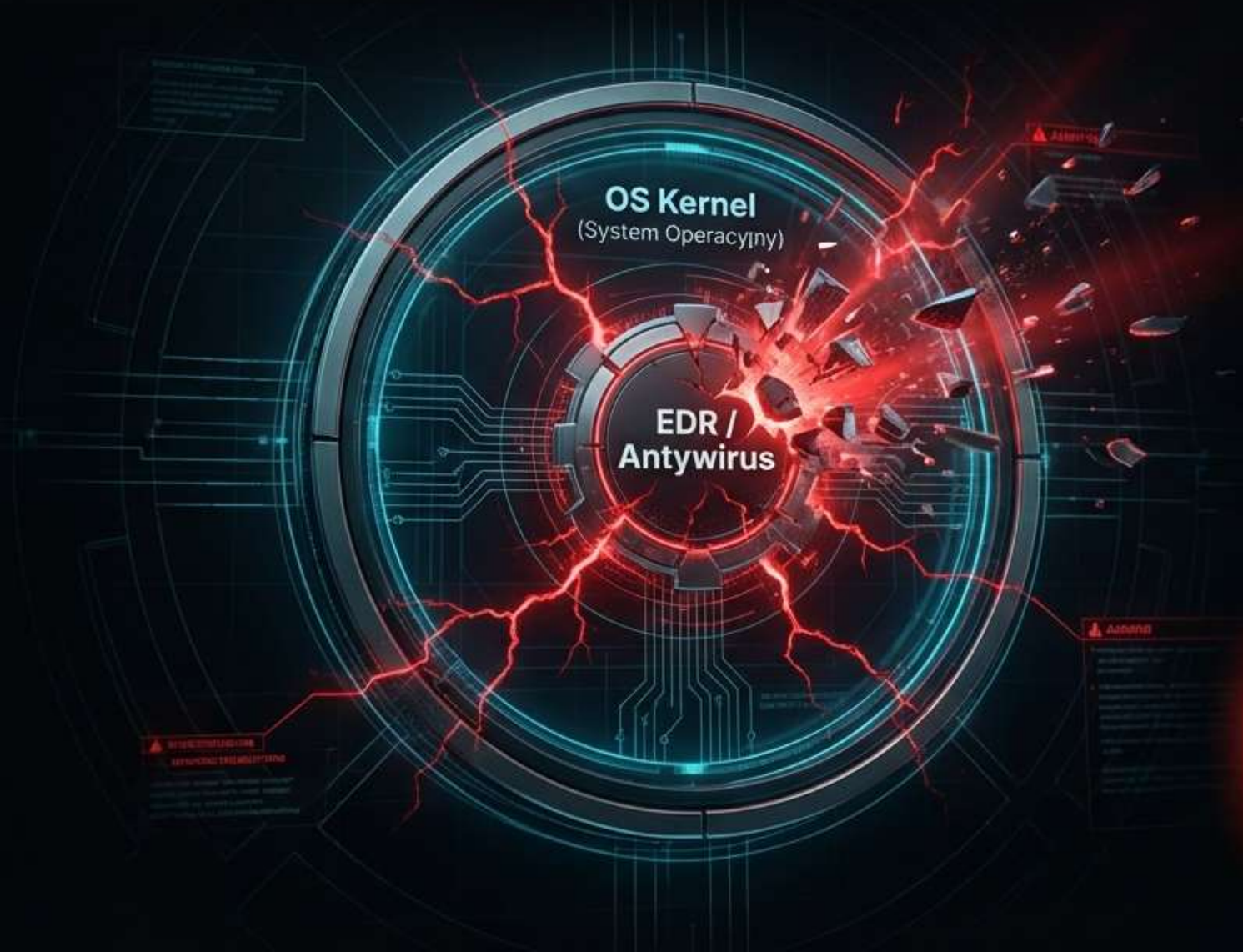
GARM to polisa ubezpieczeniowa na błędy dostawców bezpieczeństwa.

Działamy na poziomie, który pozwala odzyskać kontrolę, nawet gdy EDR wywoła krytyczny błąd jądra (Kernel Panic).

$5.4 mld strat w jeden dzień.

[CONFIDENTIAL / DEEP TECH R&D]

To nie był atak hakerski. To był błąd architektury zaufania.



Old Model

- Obecna ochrona (EDR) działa wewnątrz jądra systemu (In-Kernel).
- Kiedy upada jądro, antywirus staje się bezużyteczny.

Systemy bezpieczeństwa stały się pojedynczym punktem awarii (Single Point of Failure).

[CONFIDENTIAL / DEEP TECH R&D]

GARM to nie kolejny antywirus. To cyfrowy układ odpornościowy.

Antywirus

- GARM to "Plan B", który działa poniżej poziomu katastrofy.
- Nie walczymy z wirusami. Izolujemy krytyczne dane od skompromitowanego systemu.
- Hostile Environment: Zakładamy, że system operacyjny jest już stracony.

[CONFIDENTIAL / DEEP TECH R&D]

Deep Tech: Dominacja w Ring-0.

Malware nie widzi tego, czego nie może dosięgnąć. Startujemy przed systemem Windows (Pre-OS).

Windows OS + Apps + EDR

UEFI / Boot

GARM Hypervisor (Ring-0 / VT-x)

- Sprzętowa izolacja rdzenia (Hyper-V)
- Invisible to OS

Hardware (CPU / RAM)

[CONFIDENTIAL / DEEP TECH R&D]

Technologiczny Elityzm: Rust & Memory Safety.

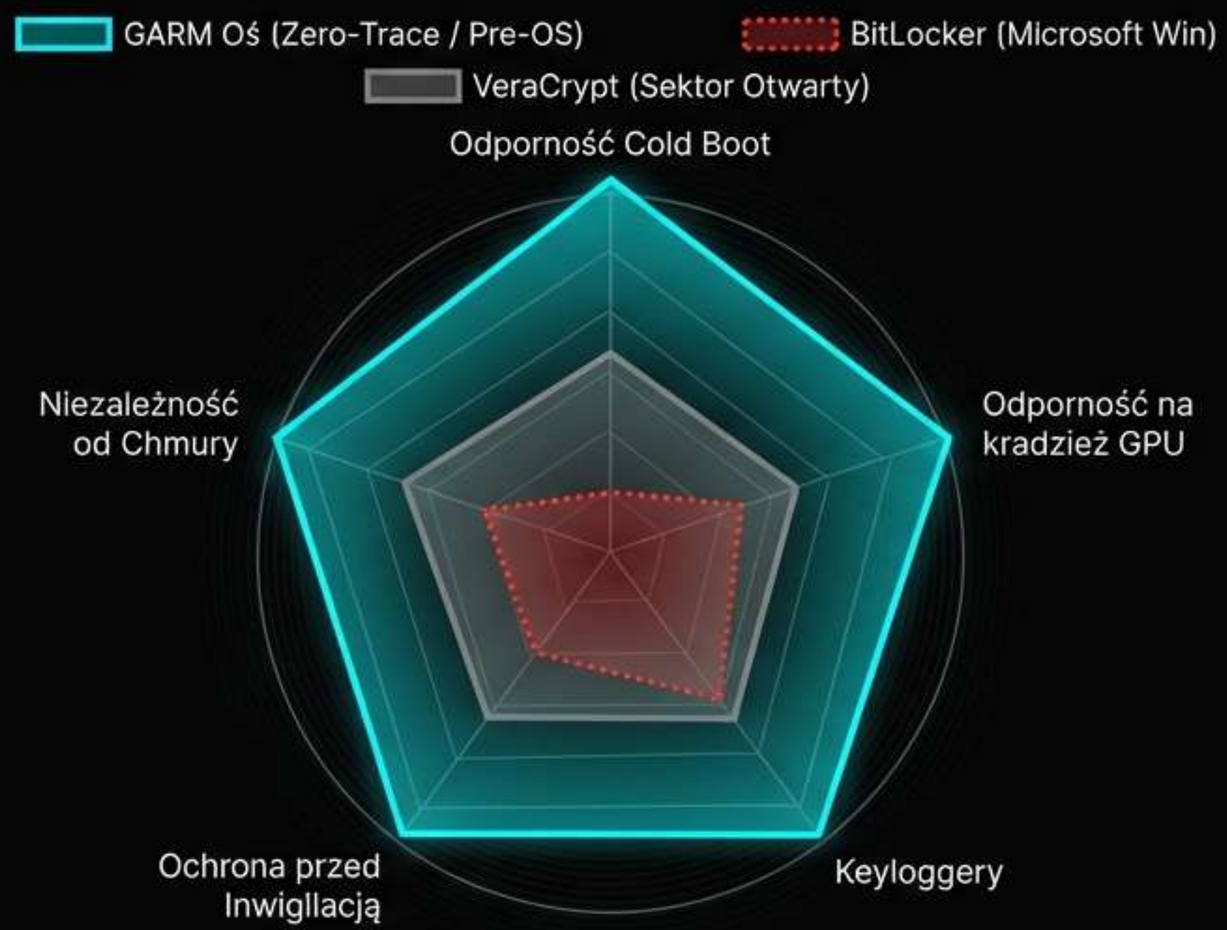
Eliminujemy 70% błędów bezpieczeństwa pamięci (Buffer Overflow).

Matematyczna pewność kodu.

Zero-cost Abstractions
Ownership & Borrowing
Type System

To jest inżynieria wojskowa, nie startup studencki.

Eliminacja Punktów Awarii.



BitLocker nie chroni przed atakami fizycznymi (DMA/Cold Boot).

GARM: Pełna ochrona kluczy szyfrujących w izolowanej enklawie.

[CONFIDENTIAL / DEEP TECH R&D]

Europejska Suwerenność Cyfrowa.

Supply Chain Security: Gwarantujemy, że infrastruktura krytyczna UE nie zależy od zamkniętego kodu z USA czy Azji.

Brak ukrytych furtek (No Backdoors).

Nasz, lokalny, polski kod. Tarcza, której nie można wyłączyć zza oceanu.

[CONFIDENTIAL / DEEP TECH R&D]

Pieniądze i Strach: Instrument Przetrwania.

DORA + NIS2: Złoty standard dla sektora bankowego.

Groźba kar do
15 mln €
lub 2.5% globalnego obrotu.

Odpowiedzialność karna zarządów.

Nie tylko chronimy dane.
Chronimy kapitał i licencje bankowe.

[CONFIDENTIAL / DEEP TECH R&D]

Plan Taktyczny: Skalowalność i Certyfikacja

Q3 2025

1

Finalizacja jądra w **Rust** (Core Completion)

Q1 2026

2

Pierwszy zamknięty pilotaż (MVP / Closed Beta)

Q3 2026

3

Inicjacja certyfikacji **Common Criteria** (EAL) - Klucz do sektora Gov

2027

4

Pełna zgodność z **Cyber Resilience Act** (CRA)

[CONFIDENTIAL / DEEP TECH R&D]

Alokacja Kapitału (R&D Focus)

40%

Inżynierowie Deep Tech & Elite AI (Rust/Kernel) JetBrains Mono

UI/UX

Tauri / B2B Web OS

Audyty

Prawne i Certyfikacja (CRA/Patent)

Inwestujemy w twardą technologię, nie w marketing.

[CONFIDENTIAL / DEEP TECH R&D]

Zespół Deep Tech DNA.

Senior Rust Architects.
Eksperci od Ring-0 i
Inżynierii Wstecznej.

“Nie jesteśmy web-developerami. Jesteśmy architektami jąder systemowych.”

Security Researchers.
Audytorzy kodu i
Red Teaming.

GARM: Architektura Nieufności

Dołącz do budowy nowego europejskiego standardu bezpieczeństwa.

[CONFIDENTIAL / DEEP TECH R&D]