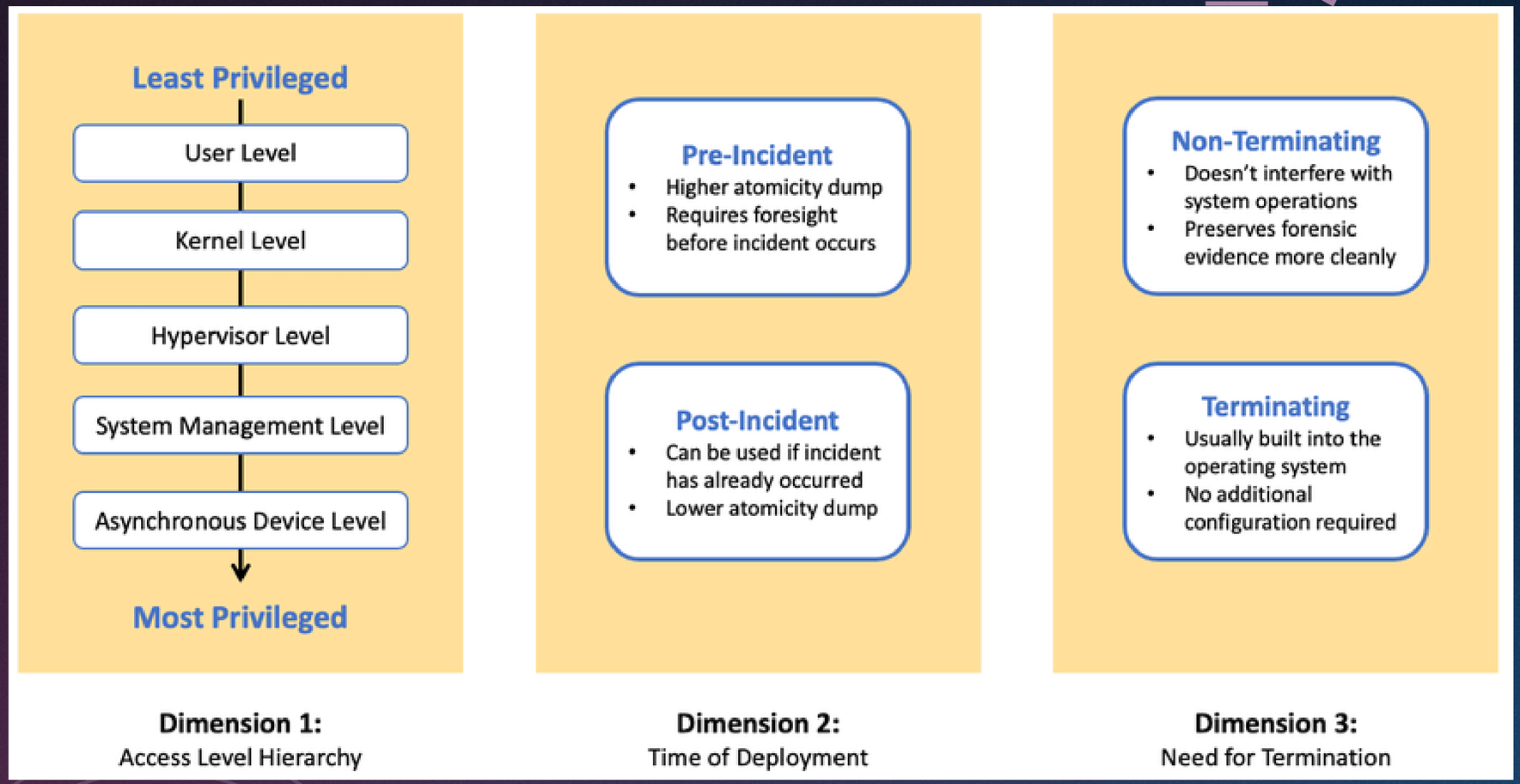
The Evolution of Volatile Memory Forensic

2540125384 – Benedicto Marvelous Alidajaya
2540118933 – John Orlond
2540124702 – Matthew Kurniawan

Memory Acquisition Method

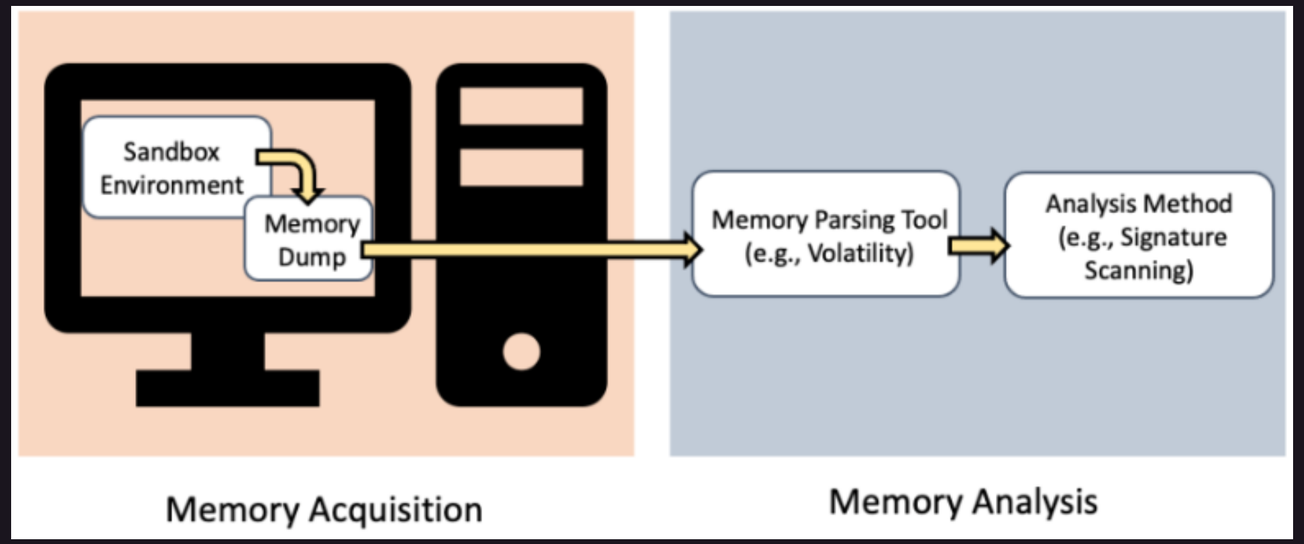


Acquisition Techniques

- User Level : Menggunakan software emulator
- Kernel Level : Mengimplementasi tool sebagai kernel drivers, mengenerate crash dumps atau file hibernasi, dan debugger pada exe
- Hypervisor Level : Menggunakan tools seperti HyperSleuth, Vis, Cheng. Tool yang disediakan oleh VMware adalah cmss2core.exe dan dump-memmory pada LibVMI.
- System Management Level : Tools yang digunakan oleh blueteam untuk melakukan forensic pada level BIOS seperti SmmBackdoor.
- Asynchronous Level : Bisa direct memmory access menggunakan PCILeech atau inception, Hardware Thread Control Block menggunakan Snipsnap atau built-in cold boot.

Memory Analysis

- Setelah memory dump diperoleh, ada beberapa metode untuk menganalisis memory dump dan mengetahui keberadaan suatu malware.
- Parsing memory dump -> mendapatkan useful information dan kemudian menggunakan informasi tersebut dalam pendekatan analisis tertentu.
- Alat seperti *Volatility* dan *Rekall* dibuat untuk mengurai memory dump.



Scanning Methods

Signature Scanning

- Mencari signature dari known malware dengan konten memory dump files dari sistem yang terinfeksi, biasanya berupa *byte pattern* dan *strings* yang unik untuk jenis malware.
- *YARA matching engine* membandingkan sample tertentu dengan sample besar database setiap signature yang masing-masing mewakili jenis malware atau malware family.

Heutristic Scanning

- Metode yang mendeteksi ancaman menggunakan rules dan algoritma untuk mencari perintah atau instruksi yang mungkin mengindikasi ke malicious intent.
- Lebih dapat di generalisir daripada signature, memungkinkan heuristik untuk mengidentifikasi malware yang tidak terlihat sebelumnya yang memiliki karakteristik yang sama dengan malware yang diidentifikasi sebelumnya.

Dynamic Analysis within a Sandbox

Virtualized Environment

Software Emulators

Sandbox Tools