➡ Kernel Self-Protection (Linux)

➡ Kernel Patch Guard / Patch Protection (KPP) (Windows)

➡ Kernel Data Protection (Windows)

➡ System Coprocessor / Kernel Integrity Protection (MacOS)

➡ Pointer Authentication Codes (MacOS)

➡ Code integrity and signing

- Non-exhaustive. Often implemented at OS or hypervisor level (Virtualization Based Security)

Kernel Patch and Exploit Mitigations

Kernel Patch and Exploit Mitigations

- Kernel Self-Protection (Linux)
- Kernel Patch Guard / Patch Protection (KPP) (Windows)
- Kernel Data Protection (Windows)
- System Coprocessor / Kernel Integrity Protection (MacOS)
- Pointer Authentication Codes (MacOS)
- Code integrity and signing
- Non-exhaustive. Often implemented at OS or hypervisor level (Virtualization Based Security)

Endpoint Detection and Response