➡ Patches often need to be validated

➡ Risk-based discovery, prioritization and remediation

➡ 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)

To Patch or Not to Patch …

To Patch or Not to Patch …

- Patches often need to be validated
- Risk-based discovery, prioritization and remediation
- 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)

Securing the Kernel