3.2

Thursday, September 21, 2023 1:46 PM

trusted or measured boot process uses TPM at each stage of boot process to check hashes of system state data

Endpoint detection and response EDR real-time and historical vis into compromise, contains malware, and facilitates remediation

Secure cookies - help prevent session hijacking and data exposure

uses SetCookie header for sec

Server-level = host level

UEFI - Unified extensible firmware

UEFI - Unified extensible firmware interface

specification for software that connects pc firmware to OS

replacement for BIOS

BIOS - firmware used to manipulate settings on system

basic instructions on how sys should start up

does not support secure boot

hardware root of trust - known secure starting point by embed private key

Attestation - process of checking and validating system files

and validating system
during boot process

BitLocker - Windows full drive encryption

Windows firewall has rule for RDP
connections that can be disabled

VMs comm w/ each other through
virtual switch where HIPS can
prevent malicious traffic

HIPS does not update outdated services

Secure DevOps
- Continuous integration
- sec automation
- immutable systems w/ imaging

add device IDs to DLP