William Prado
08-01-2025

Review

1. Signature Based detection
   - Reactive
   - Good for common threats

Algorithm

A
B
C

Signature

A
B
C

Threat → Detection → Add Signature → Look for signature

2. Behavioral Based Detection
   - Action
   - Engine trained to spot baseline (normal) traffic or events
   - Disaventage - false positive

3. Heuristic - Static & Dynamic
   - multiple Behaviors

4 Anomaly - Based Detection
   - Location, Volume, frequency, etc.

5. Trend Analysis
   - Isolated events over time.

YTB: Roots of Trust overview

MS Tech Talk: Hardware root of Trust
- Hardware roof of Trust
  - Power on
  - Post
  - Device Boot
  - Load OS
  - Under Control

William Prado
09/01/2025

root kit.

Types of Root kits:

Type:	What it Targets:
Firmware	- Bios, hard drives, routers
Bootloader	- system startup process
Kernel	- core of the Operating system
Application	- Replaces or infects regular apps
Memory Based	- Lives in RAM (Temporary memory).

av cyber active

YTB- Trusted Platform Module (TPM) what is it?

Tpm= is a chip that is installed on the motherboard that is used to provide tamper-proof security-related functions.

- How do I determine if I have a TPM on my windows computer? tpm.msc

Prof. messer

YTB. Boot Integrity - SY0-601 CompTIA Sect: 3.2

YTB. What is Secure Boot?

GPS

1) Geo location
2) Geo Fencing
3) Geo Targeting
4) Geo Tagging

William Prado
09/01/2025

LDAP - 389
TLS over TCP - 636
UDP - 161

Note: if SNMP not used, change default configuration password & disable. i,e. just shut down if not being used

SMTP
25
mx DNS
"mailserver"

MSA
587

POPS
995

IMAPS
~~[redacted]~~
993

Vnseare Imaps
port 143.