William Prado
07/31/2025
- Implement Endpoint sec.
- Addendum.

YTB. Behavioral Based Detection
UEBA - user and entity behavior analytics
NTA - Network Traffic Analysis

Signature	Behavior
"pattern"	Predetermined actions

YTB-IBM-User Behavioral Analytics

Heuristic	Anomaly	Trend
-static -dynamic	Isolated event	

WAF

YTB: Web filtering using defender for endpoint
Firewall = defender.

* Microsoft 365 defender has attack simulation training.

End Point Management
Controls: • inventory • Patching • remote wipe
• sec Policy • Encryption • Log tracking

AI is like a super-smart analyst - it reads data, find patterns, and makes decisions.
Gen AI is like a creative partner - it takes what it's learned + builds something new from scratch.

William Prado
07/31/2025
- Implement endpoint sec.
- Addendum

MDR:
MAAGED service 3rd party
EDR/XDR provider

XDR • integrate EDRs • Network Based

IBM YTB: SIEM or XDR
Security Information and event management (SIEM).
Extended Detection & Response (XDR).

YTB: What is SOAR? Automation & Orchestration explained.

Playbooks help teams respond to incidents like ransomware attacks or data breaches w/ coordinated strategies. It is like your strategy guide.
Runbooks ensure consistency in tasks like isolating infected systems, restoring backups, or rotating credentials. It's like your cheat sheet for button combos.

* Host-based Intrusion Detection/Prevention
* Hardening Techniques
* Hardware Root of Trust
* Trusted Platform Module (TPM)