Antivirus vs EDR vs XDR

ANTIVIRUS (AV)	EDR	XDR
Focus Detects and removes known malware like viruses, worms, and Trojans.	**Focus** Monitors and responds to advanced threats on individual devices (endpoints).	**Focus** Provides cross-platform, holistic threat detection and response.
Method Uses signature-based detection to identify known threats.	**Method** Behavioral analysis, threat hunting, and real-time monitoring.	**Method** Integrates data from multiple security tools (e.g., AV, EDR, etc) to correlate and detect threats.
Purpose Provides baseline protection against common malware.	**Purpose** Offers enhanced security by identifying and mitigating unknown and targeted threats.	**Purpose** Offers comprehensive security by connecting the dots between different security layers.
Scope Focuses on detecting and blocking known malware and viruses.	**Scope** Monitors and responds to suspicious activities and threats on individual endpoints.	**Scope** Integrates data and threat intelligence from multiple security sources, covering a broader range of endpoints and networks.
Usage Traditional protection against common threats but may struggle with advancedor unknown attacks.	**Usage** Offers deeper visibility and control, ideal for threat hunting and investigating incidents.	**Usage** Provides a holistic, cross-environment view for threat detection, response, and better protection against complex attacks.

MINISTRY OF SECURITY

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/cybersecurity/avedrxdr

Last update: **2023/11/04 11:50**