EPSS vs. CVSS 4.0 :

Core Characteristics

Factor	EPSS	CVSS 4.0
Purpose	Predicts likelihood of exploitation within 30 days	Measures severity and impact of vulnerabilities
Score Range	O to 1 (0% to 100% probability of exploitation)	O to 10 (Severity-based ranking)
Update Frequency	Daily (Real-time threat updates)	Rarely updated (Static unless reassessed)
Core Calculation	Machine learning model using logistic regression + XGBoost, trained on real-world attack data	Weighted formula based on exploitability, impact, and business/environmental modifiers
Key Inputs	• Threat intelligence (Fortinet, Shadowserver, GreyNoise) • Exploit databases (Metasploit, Exploit DB, GitHub) • Vulnerability scanning detections (Nuclei, Jaeles) • Social media signals (Twitter, dark web) • IDS/IPS exploit tracking	• Vulnerability characteristics (Attack Vector, Complexity, Privileges Required) • Business impact (Confidentiality, Integrity, Availability) • Environmental & Threat Metrics (NEW in CVSS 4.0) • Supplemental Metrics (Safety, Automation, Urgency)
Use Case	Threat-driven vulnerability prioritization	Severity-based classification, compliance reporting
Best For	Security teams prioritizing immediate threats	Compliance, audits, business risk assessment