EPSS and CVSS 4.0 :
What Are They Both Missing?

Missing Factor	EPSS	CVSS 4.0	Why it Matters?
Automatically Adjusts for Business Risk	❌ No	❌ No (Requires Manual Adjustments)	Vulnerability impact varies by organization; prioritization should reflect business-critical assets.
Accounts for Security Controls & Network Segmentation	❌ No	❌ No (Environmental Score Must Be Manually Set)	Security posture affects exploitability —firewalls, EDR, segmentation can mitigate risk.
Exploit Chaining Awareness	❌ No	❌ No	Attackers chain multiple vulnerabilities to achieve deeper access, which neither scoring system models.
Zero-Day & Emerging Threat Awareness	❌ No (Depends on Public Data)	❌ No (Lacks Live Intelligence)	Both systems rely on known data, meaning unknown or developing threats remain unaccounted for.
Predictive Threat Actor Intent	❌ No	❌ No	Threat actors shift tactics, but neither EPSS nor CVSS predicts which vulnerabilities they will weaponize next.
Real-Time Risk Scoring Based on Organizational Context	❌ No	❌ No	Risk changes daily—both lack continuous scoring adjustments based on evolving attack surface.
Automation of True Risk-Based Prioritization	❌ No	❌ No	Organizations must manually combine EPSS, CVSS, business context, and security controls, which is time-consuming and inconsistent.
Automatically Adjusts for Business Risk	❌ No	❌ No (Requires Manual Adjustments)	A vulnerability on a production database is far riskier than one on a test machine—but neither system accounts for that automatically.
Accounts for Security Controls & Network Segmentation	❌ No	❌ No (Environmental Score Must Be Manually Set)	Firewalls, EDR, NAC, WAFS, and micro-segmentation reduce exploitability, but EPSS & CVSS assume all vulnerabilities are equally exposed.

Missing Factor	EPSS	CVSS 4.0	Why it Matters?
Exploit Chaining Awareness	❌ No	❌ No	Attackers don't exploit just one vulnerability—they chain multiple together (e.g., initial access → privilege escalation → lateral movement). Neither model accounts for attack paths.
Zero-Day & Emerging Threat Awareness	❌ No (Depends on Public Data)	❌ No (Lacks Live Intelligence)	Both systems rely on disclosed vulnerabilities, meaning nation-state, APT, or ransomware operator tactics using zero-days are missed.
Predictive Threat Actor Intent	❌ No	❌ No	What vulnerabilities are attackers likely to target next? Neither system forecasts future exploit trends based on adversary behavior or dark web activity.
Real-Time Risk Scoring Based on Organizational Context	❌ No	❌ No	Attack surfaces change daily—newly exposed assets increase risk, while patched systems lower it. Neither EPSS nor CVSS dynamically adjusts to an organization's real-time security posture.
Integration with MITRE ATT&CK TTPs	❌ No	❌ No	SecOps relies on MITRE ATT&CK to map vulnerabilities to real-world adversary tactics—but neither EPSS nor CVSS correlates vulnerabilities with known attack techniques.
Asset Criticality & Data Sensitivity Awareness	❌ No	❌ No	A high-EPSS, low-CVSS vulnerability on a crown jewel system (e.g., Active Directory, customer database) is more critical than one on a low-value asset—but neither score reflects that.
Security Debt & Exposure Trend Analysis	❌ No	❌ No	SecOps needs to know: Is our risk getting worse over time? Neither system provides historical trend analysis on vulnerability backlog growth, remediation efficiency, or recurring exposures.
Automated Attack Surface Prioritization	❌ No	❌ No	Without automated asset discovery and risk mapping, both EPSS and CVSS require manual correlation with CMDBs, attack surface management tools, and vulnerability scanners.

Missing Factor	EPSS	CVSS 4.0	Why it Matters?
Remediation Complexity & Patch Workload Awareness	❌ No	❌ No	Some vulnerabilities require days/weeks of testing before patching (e.g., ERP systems, industrial control systems), but neither EPSS nor CVSS helps SecOps assess patch feasibility or risk of operational disruption.
Integration with XDR/SIEM for Active Threat Correlation	❌ No	❌ No	If a vulnerability is actively being exploited in an environment, SecOps needs to correlate it with real-time alerts from EPSS & CVSS do not provide automated detection-driven prioritization.
Cloud-Specific Vulnerability Prioritization	❌ No	❌ No	Neither system differentiates between traditional IT vulnerabilities vs. cloud-native risks (e.g., misconfigurations in AWS IAM, Kubernetes RBAC, or serverless functions).
End-of-Life (EOL) Software Awareness	❌ No	❌ No	If a vulnerable system can't be patched because it's end-of-life (EOL) (e.g., Windows Server 2008, legacy SCADA systems), SecOps needs mitigation recommendations—but neither EPSS nor CVSS provides this context.
Threat Actor- Specific Targeting Patterns	❌ No	❌ No	Some vulnerabilities are more likely to be exploited by specific APTs, ransomware groups, or cybercriminals—but neither system provides threat actor mapping or IOC enrichment.