APEX STANDARDS

Cybersecurity Analysis Platform with Critical Cross-Referencing Capabilities

Whitepaper
Next-Gen Cyber Defense
ASS-80 Software Update

Introducing Apex Standards Cybersecurity Analysis Platform (ASS-80)

Trusted by top cybersecurity teams, the Apex Standards Cybersecurity Analysis Platform (ASS-80) empowers your organization with cutting-edge capabilities, informed by the latest insights from RSA Conference 2024 and leveraging advancements in Large Language Model (LLM) AI for the next generation cyber defense.

Key Features & Strategic Benefits

High Automation Levels and Critical Cross-Checking Capabilities: ASS-80 harnesses the power of AI to automate vulnerability identification, assessment, and prioritization, freeing up valuable time for your security team to focus on strategic initiatives. Its cross-checking functionalities ensure the accuracy and reliability of the results, minimizing the risk of overlooking critical threats.

Multi-Dimensional Vulnerability Analysis: ASS-80 goes beyond basic CVSS scores, providing a granular, multi-dimensional analysis of vulnerabilities across various factors, including exploitability, impact, and temporal trends. This enables your team to gain deep insights into the potential risks associated with each vulnerability and make informed decisions about remediation efforts.

Reverse Cross-Reference with IETF Capabilities (ASS-35): ASS-80 seamlessly integrates with our IETF Analysis Platform (ASS-35) to provide a reverse cross-reference of vulnerabilities against relevant IETF standards and best practices. This helps identify potential misconfigurations and deviations from industry standards, further strengthening your security posture.

CVE Cross-Reference with Software Bill of Materials (SBOM): ASS-80 enables you to cross-reference CVEs against your software bill of materials (SBOM) and CPE data, identifying vulnerabilities in third-party components and libraries and pinpointing affected vendors and products, ensuring comprehensive security across your entire software supply chain. *Receive real-time alerts for newly discovered vulnerabilities related to your SBOM.*

Prioritized Response Based on EPSS and KEV: ASS-80 leverages the Exploit Prediction Scoring System (EPSS) to identify vulnerabilities with the highest likelihood of exploitation, cross-referencing them with the Known Exploited Vulnerabilities (KEV) catalog to prioritize those potentially being exploited in the wild. This strategic approach empowers your team to focus on the most critical threats, enabling proactive mitigation and reducing the risk of attacks.

Real-World Impact

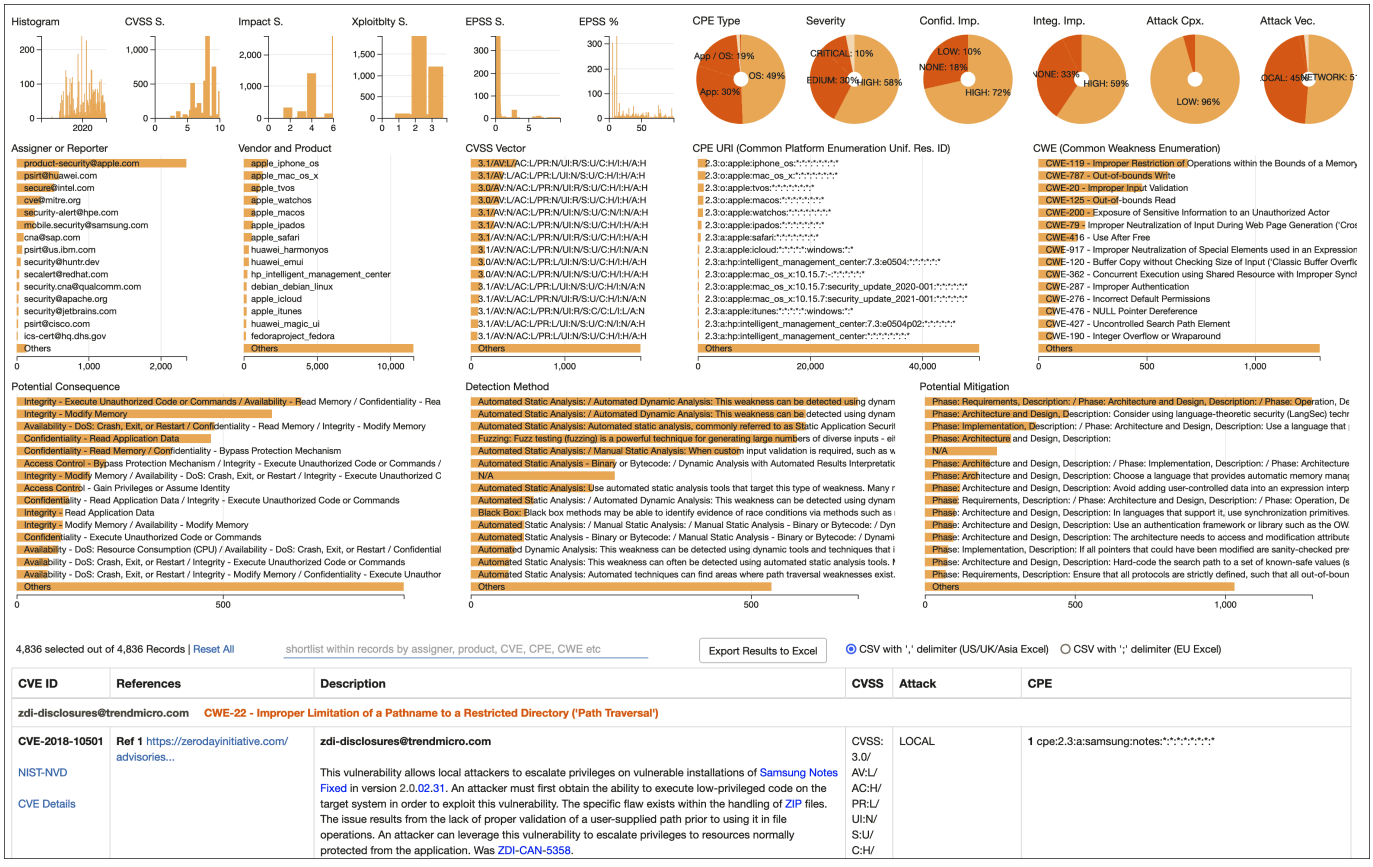
Leading organizations, including S&P 500 companies, critical infrastructure managers, Small and Midsize Enterprise (SMEs), and Chief Information Security Officers (CISOs), rely on ASS-80 to stay ahead of the curve in the ever-evolving threat landscape. By automating vulnerability analysis, prioritizing response efforts, and ensuring compliance with industry standards, ASS-80 empowers these organizations to strengthen their cybersecurity posture and protect their most valuable assets.

Embrace Next-Gen Cybersecurity with ASS-80

Join the ranks of top cybersecurity teams who trust Apex Standards to safeguard their organizations against sophisticated cyber threats. Visit **www.apexstandards.com** or contact us at support@apexstandards.com to learn more about how ASS-80 can help you achieve a new level of security and resilience.

Abbreviations and Sources

1. **CVE**: Common Vulnerability and Exposure (https://nvd.nist.gov/)
2. **CWE**: Common Weakness Enumeration (https://cwe.mitre.org/)
3. **CPE**: Common Platform Enumeration (https://nvd.nist.gov/)
4. **CVSS**: Common Vulnerability Scoring System (https://nvd.nist.gov/)
5. **EPSS**: Exploit Prediction Scoring System (https://www.first.org/epss/model)
6. **KEV**: Known Exploited Vulnerabilities (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)



The intuitive dashboard offers a comprehensive, multi-dimensional view of your cybersecurity landscape, enabling efficient cross-checking and filtering of vulnerability metrics and categories across CVE, CWE, CVSS, EPSS, CPE, and other critical factors. This holistic approach empowers you with in-depth insights and granular control over potential threats.