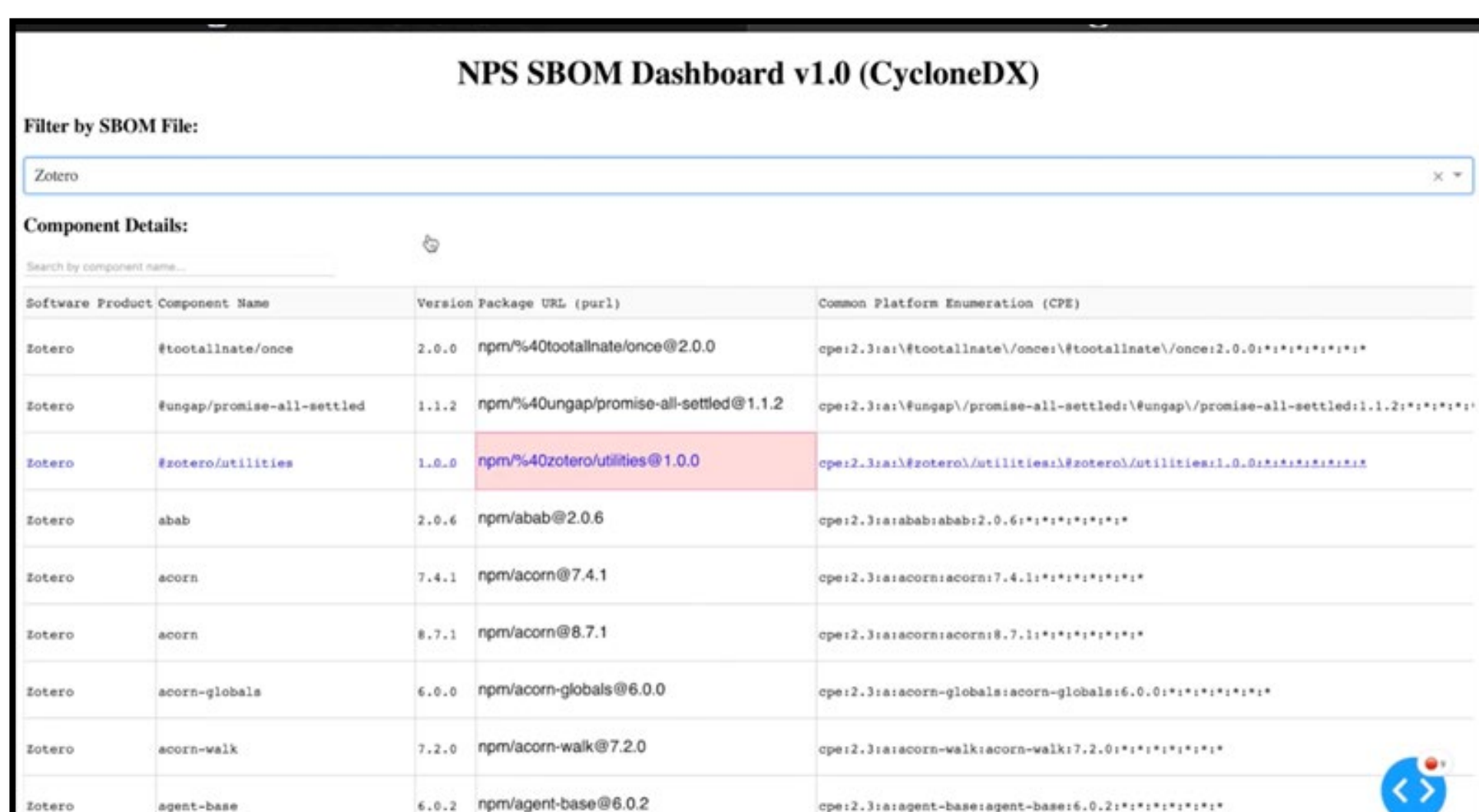


Abstract

This Innovation Capstone Project explored the DOD's software supply chain. We validated the problem statement, pinpointed solutions, and made recommendations. By adopting SBOMs, we believe the DOD can enhance software risk management, strengthen contractor cybersecurity accountability, and safeguard national security data, fortifying the nation's cyber defenses. We created a minimum viable product (MVP) utilizing AI, generated a system dynamics (SD) model, and engaged with the DOD CIO to collaborate on a pilot program centered on SBOMs within the USAF.



Software Product Component Name	Version	Package URL (purl)	Common Platform Enumeration (CPE)
zotero	2.0.0	npm/%40totalrate/once@2.0.0	cpe:2.3:a1/totalrate/once/totalrate/once:2.0.0:*:*:*:*
zotero	1.1.2	npm/%40ungap/promise-all-settled@1.1.2	cpe:2.3:a1/ungap/promise-all-settled/ungap/promise-all-settled:1.1.2:*:*:*:*
zotero	1.0.0	npm/%40zotero/utilities@1.0.0	cpe:2.3:a1/zotero/utilities/zotero/utilities:1.0.0:*:*:*:*
zotero	2.0.6	npm/abab@2.0.6	cpe:2.3:a1/abab/abab:2.0.6:*:*:*:*
zotero	7.4.1	npm/acorn@7.4.1	cpe:2.3:a1/acorn/acorn:7.4.1:*:*:*:*
zotero	8.7.1	npm/acorn@8.7.1	cpe:2.3:a1/acorn/acorn:8.7.1:*:*:*:*
zotero	6.0.0	npm/acorn-globals@6.0.0	cpe:2.3:a1/acorn-globals/acorn-globals:6.0.0:*:*:*:*
zotero	7.2.0	npm/acorn-walk@7.2.0	cpe:2.3:a1/acorn-walk/acorn-walk:7.2.0:*:*:*:*
zotero	6.0.2	npm/agent-base@6.0.2	cpe:2.3:a1/agent-base/agent-base:6.0.2:*:*:*:*

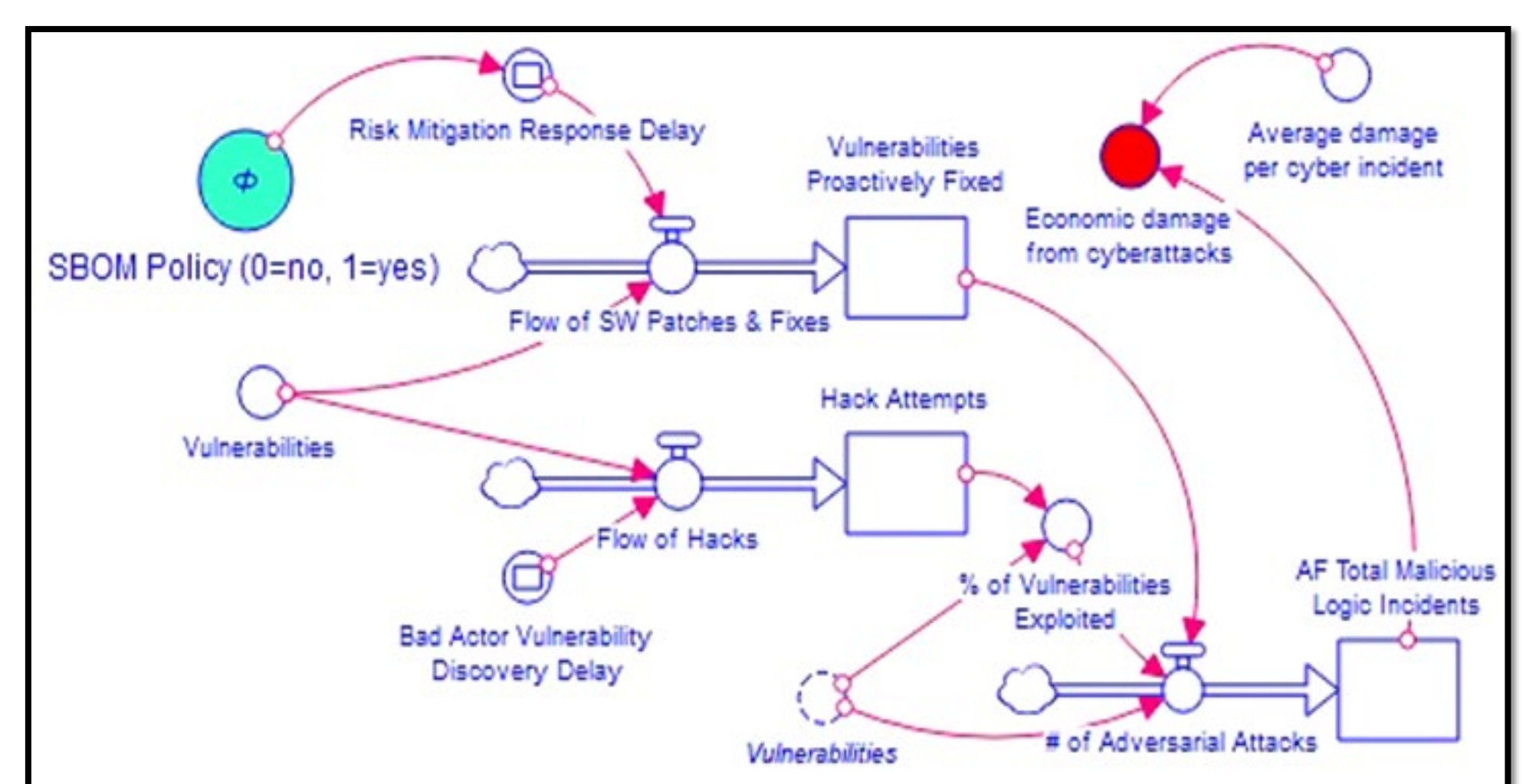
NPS Dashboard V1.0 interface

Methods

- Hacking for Defense: Conducted stakeholder interviews, in-depth research, driven by sponsor feedback, and multiple MVP iterations to form the validated problem statement.
- Working Groups: Engagement with diverse stakeholders, including the Enterprise Information as a Service (EITaaS) team, DOD and DAF CIO, for SBOM utilization and integration into DOD SCRM processes.
- Goals, Decisions, Signals, and Data Model: We mapped the EITaaS program's goals and decisions to the essential data within SBOMs, which create signals for risk, optimizing software supply chain risk management.
- SD: Assessed the quantifiable impact of an SBOM policy on the AF, creating a causal loop diagram to model the relationships between key SBOM variables in the USAF's information technology (IT) software supply chain and modeling the economic impact of an USAF SBOM policy implementation.

Results & Their Impact

- MVP established a basic, zero-dollar SBOM procedure, covering SBOM generation, storage, scanning, and vulnerability identification.
- SD model showed an SBOM policy could potentially save \$7B over 10 years, reducing economic damage from cyberattacks from 5% to 2% of the total USAF IT cost.



Cyberattacks and Economic Damage Model (ISEE Systems, Stella Software ©)

Recommendations

- Elevate understanding and awareness of SBOMs among DOD internal stakeholders as a foundational step for effective implementation.
- Encourage collaboration between the EITaaS program, DAF CIO, and DOD CIO for a pilot program to experiment with SBOM management processes and demystify its significance in mitigating software risk.
- Draw from industry standards to create an inclusive SBOM standard and pragmatic approach to SBOM collection and implementation, encompassing the entire SBOM lifecycle.
- Adoption of best practices for software supply chain risk management, easing implementation, and allowing for risk mitigation while refining the risk management framework.