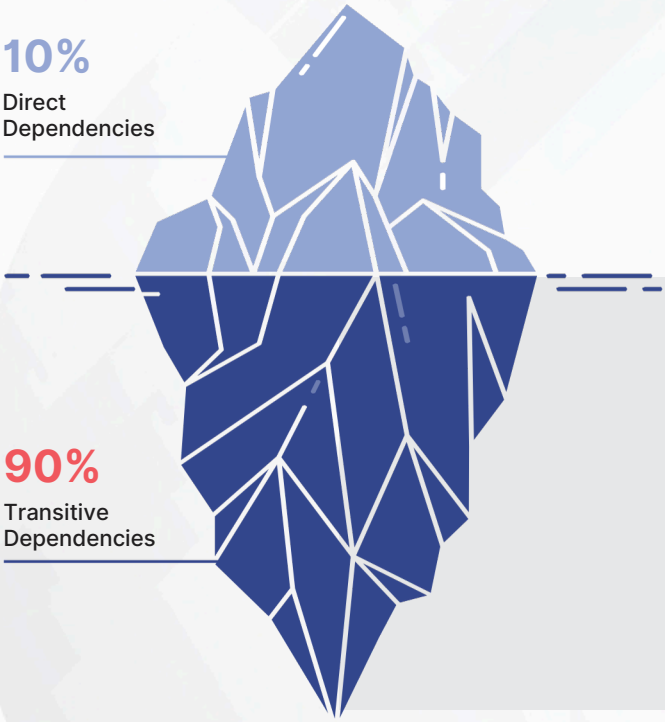
US Air Force Eagle Eye Program

Detecting and Eliminating Software Supply Chain Threats in Software You Source, Build, Buy, and Deploy

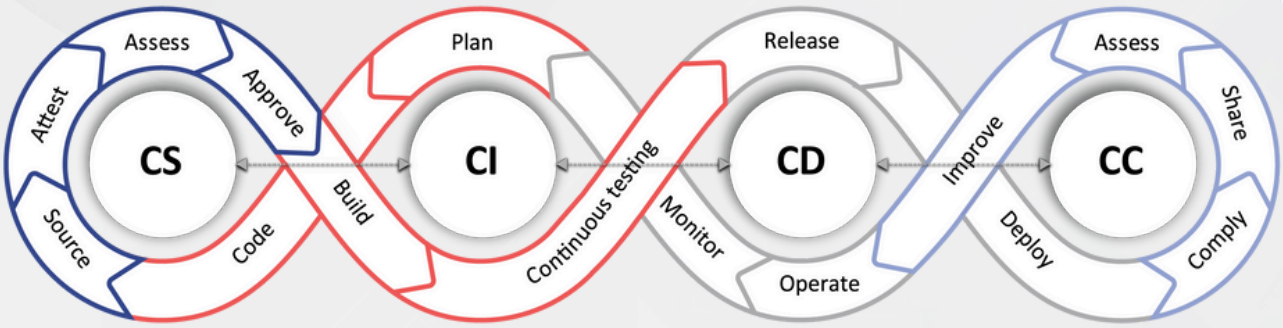


Traditional security approaches are fundamentally incapable of keeping pace with the complexity and speed of modern software development. **Near-Peer adversaries exploit these vulnerabilities** through increasingly sophisticated attacks, concealing compromised software **buried 20-30 layers deep across extensive lines of code.**

- 600% YoY increase in software supply chain attacks.
- Recent cyber assaults, such as SolarWinds, Log4j, and XZ highlight significant vulnerabilities in the software supply chain.
- Hidden vulnerabilities are buried within millions of lines of code, masquerading as authentic code, making detection nearly impossible.

US Air Force's Eagle Eye Addresses These Challenges with Lineaje:

Lineaje is providing end-to-end visibility, proactive threat detection, automated compliance reporting, and AI-driven vulnerability remediation, all within a unified platform. Deployed on the USAF Cloud One platform, Lineaje SBOM360 ensures a secure, scalable, and efficient approach to DevSecOps, tailored to the rigorous demands of military operations.



Software Supply Chain Challenges	**Hidden Risks in Open Source** 600% YoY increase in Software Supply Chain Attacks. 70-90% of Software is comprised of Open Source.	**Vast Majority of Vulnerabilities Hav No Fix** Over 56% of open source vulnerabilities have no fixes.	**Significant Costs of Vulnerability Management** One-third of developers spend over half their time patching open source vulnerabilities.	**Increased Regulatory and Compliance Mandates** Regulatory response is growing with EO14028, FDA, NIST CSF, EU CRA, CMMC, and FedRAMP, require Software Supply Chain Risks controls
Lineaje Platform	Lineaje "crawls" open-source and identifies tamper risks to the software supply chain. Lineaje continuously monitors for unauthorized changes to detect software supply chain compromises and attacks.	Lineaje AI identifies all vulnerabilities and inherent risks. Proactively recommends more secure open source compatible with your application tech stack but has fewer vulnerabilities.	Lineaje AI, Bombots identify vulnerabilities and automate tasks of vulnerability remediations, without breaking your application.	Lineaje automates SBOM generation and compliance verification for EO14028 and NIST SSDF requirements for every software release. Centrally manages SBOMs and all evidentiary artifacts for compliance with each SBOM.

CRITICAL OPEN SOURCE PROJECTS

What lies within the top 44 critical open-source software is worth exploring.

What's in your Open Source Software?

- 5120 Components in Software Supply Chain
- 977,597 Contributors across components
- 66 Countries with contributions
- 17,477,917 Commits across components
- 9,901,629 LOC scanned across component
- 169 languages scanned across components

Where is your Open Source coming from?

Country	Gold	Silver	Bronze	Tally
United States	2584	319	546	3908
Russia	1430	680	653	4180
United Kingdom	550	328	258	2017
Brazil	285	263	696	2344
China	159	40	52	577
Germany	72	230	348	1858
India	29	33	38	232
Canada	21	1930	566	3270
New Zealand	9	8	11	67
Iran	2	0	0	4

Highest code contributor in a component

Second highest code contributor in a component

Third highest code contributor in a component

Lineaje is at DAFITC 2024

Montgomery, AL from August 26-28, 2024.

Talk to us and know where your innovations and risks come from. We are in **Booth 271.**

How risky is your Open Source Software?

Vulnerable Components	Component Count
Exploitable**	16
Critical	98
High	200
Medium	173

Vulnerability Distribution	Vulnerability Count
Exploitable**	16
Critical	196
High	474
Medium	413

** CISA Known Exploited Vulnerabilities