Business & Enterprise Systems

DAFITC 2024
Eagle Eye Enhances End to End Software Supply Chain Security

Mr. Larry Charbonneau, NH-04
Eagle Eye Lead Engineer
AFLCMC/GBE

Mr. Nick Mistry
SVP, CISO
Lineaje

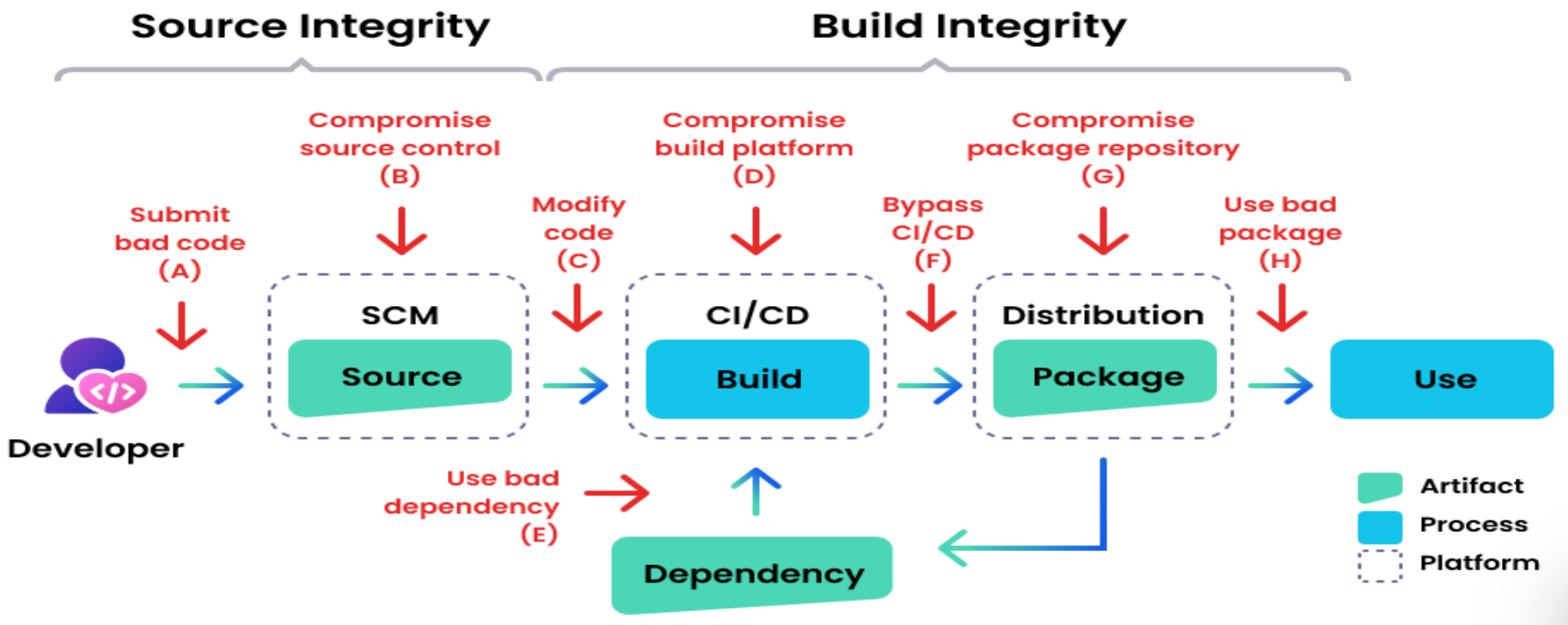
What is Eagle Eye?

- Direct response to EO 14028
- Provide USAF with understanding the open-source components & dependencies by creating and analyzing SBOMS for all applications
- Provide a holistic review of CDT current pipeline
  - Assess the pipeline and scanning - code quality, security/vulnerability, etc. process
  - Identify threats within software supply chain against industry best practices
- Build and evolve concept of SBOM (Software Bill of Materials) generation and conduct initial analysis
  - Expand the SBOM analysis tool capability
    - Provide more data points for improved risk visibility
    - Utilize AI to help generate “get well” guidance for the CDTs
- Provide prioritized refactoring and secure coding fix consultation to CDT developers
- Establish initial source code escrow process
- Build and/or evolve an automated secure production pipeline for the CDT

Excerpt from Executive Order 14028

"...the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software"

Software Supply Chain Attack Vectors



Eagle Eye Approach

Assessments

- Both continuous assessments keys in on best practices that target supply chain attack vectors
- Assessment score is generated that reflects adherence to best practices – Similar to BES agile crawl, walk, run, fly measurement
- Two Areas
  - Pipeline
    - Focus on CDTs pipeline to help identify & mitigate supply chain attack vector risk
    - Assessment report will provide score, key findings for each best practice, and provide analysis feedback with remedy recommendations
  - Tool knowledge and use
    - Code Quality – Sonarqube, Security – Checkmarx, SBOM – Dependency Track (Soon Lineaje)
    - Focus on tool usage and the process that the CDT has in place to digest and address findings from the scan results
    - Assessment report will provide process key findings and provide analysis feedback with remedy recommendations
- Goal is to assess, track risk, monitor progress, and assist (both guidance and hands on)

Production Pipeline

- The goal of EE is to produce a common production pipeline template that address each of the attack vectors
  - Provide template for CDT's in maturing existing pipelines
    - Need CDT pipeline maturity integrated into all CI/CD pipelines (Assessments Focused)
  - Migrate CDT's production pipeline using this template
  - Produce a secure & trusted production pipeline that is managed by EE
    - EE will take over the CDT release branch

Future goal - the ONLY path to production will come from the EE production Pipeline

First Year - 2023

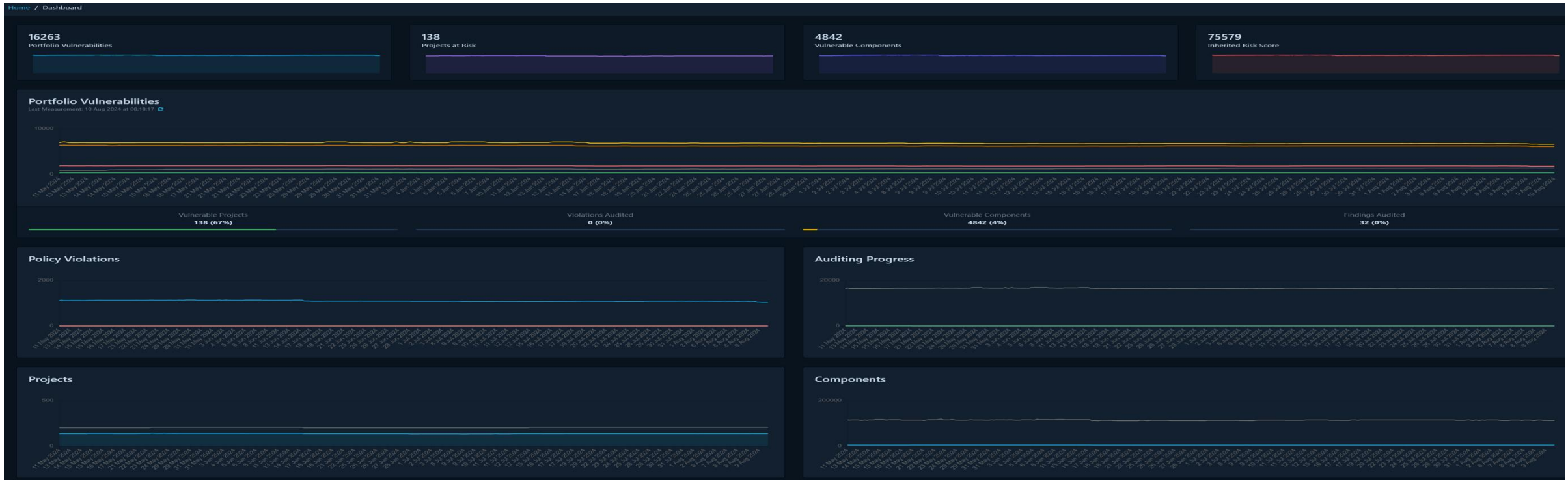
- There is no standardization across the CDT pipelines
  - Push to production is handled differently by every CDT
- CDTs might not have the needed dedicated resources
  - Team members often don't possess the in-depth knowledge of pipelines maintenance and security
- Scans are being ran but teams can find the tools difficult
  - Tools are used incorrectly producing bad/invalid results
  - Tools are used to "check the box" for compliance
  - Results are not understood and/or not integrated into the backlog
- Security/technical findings are submitted to Product Owner for consideration for backlog refinement; however, no new findings guardrails are in place by IA
- Few tools exist that are enterprise ready: SBOM analysis & scoring with enterprise-focus vs project level
- Foundation leg work must be done before developing an enterprise level "golden pipeline"

This Year – 2024 progress

- Added 5 more CDTs into EE (still in progress)
- Took last years assessments and made improvements
  - Pipeline
    - Increased the questions from 14 to over 30
    - Added more detailed scoring question with validation – Trust but verify!
    - Enhanced scoring categories and cleaner overall score
  - Tools
    - Improved scoring and more verification here as well
- Adding Lineaje as new SBOM analysis tool (will be more details and demo)
- Production Pipeline template is undergoing second revision and will be in place by years end.

SBOM Update

- Have seen increased SBOM generation and analysis
- Dependency Track has over 30 CDT Projects with over 100 SBOMS



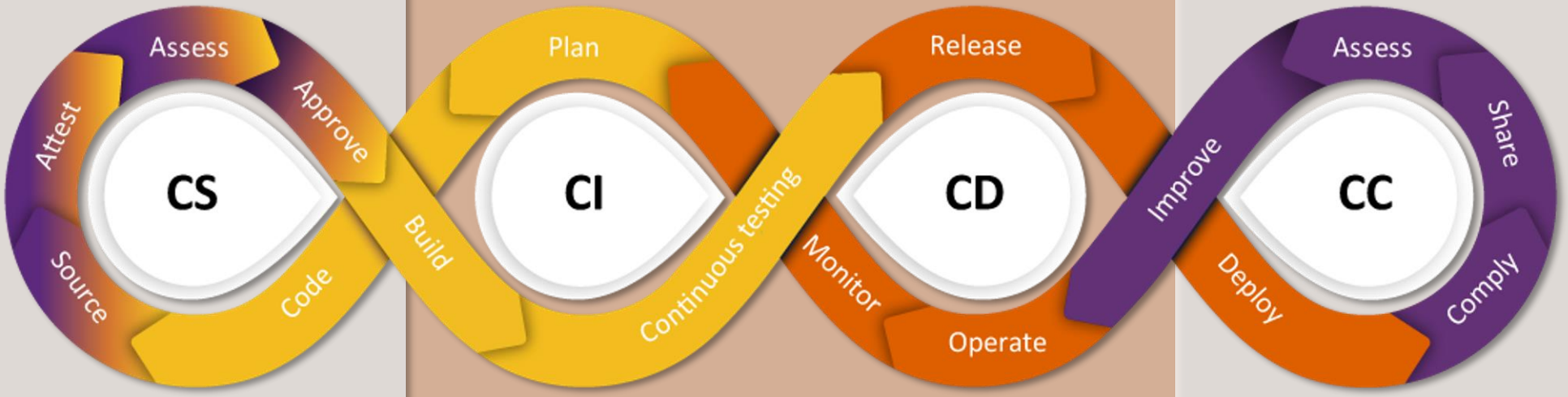
Improved SBOM Capability

- Eagle Eye is bringing new SBOM capability
  - Standing up instance in the DSO C1D space now
  - Using isolated tenant in Lineaje SaaS offering with four EE scrubbed SBOMS

To Address the Challenges of the Modern Vulnerability Management We Need to Shift Left of Shift Left and Automate Compliance Right

Shift Left of "Shift-Left"
proactively identify and mitigate supply chain risks

Automate Compliance
ensure security is integrated into every software release



Continuous Sourcing	Continuous Integration	Continuous Deployment	Continuous Compliance
70-90% of software is open-source which is opaque & tamperable	**95% of Vulnerabilities** are found **in open-source** **56% vulnerabilities have no fixes** in open-source	One third of **developers spend 50% of their time patching vulnerabilities** in open-source	In modern software development **a million releases a day is not uncommon**

Lineaje's Comprehensive Solution to Software Supply Chain Risks

PURPOSE BUILT TO ADDRESS SUPPLY CHAIN CHALLENGES

At Lineaje, we designed unique solutions and capabilities purpose-built to address these challenges head-on.

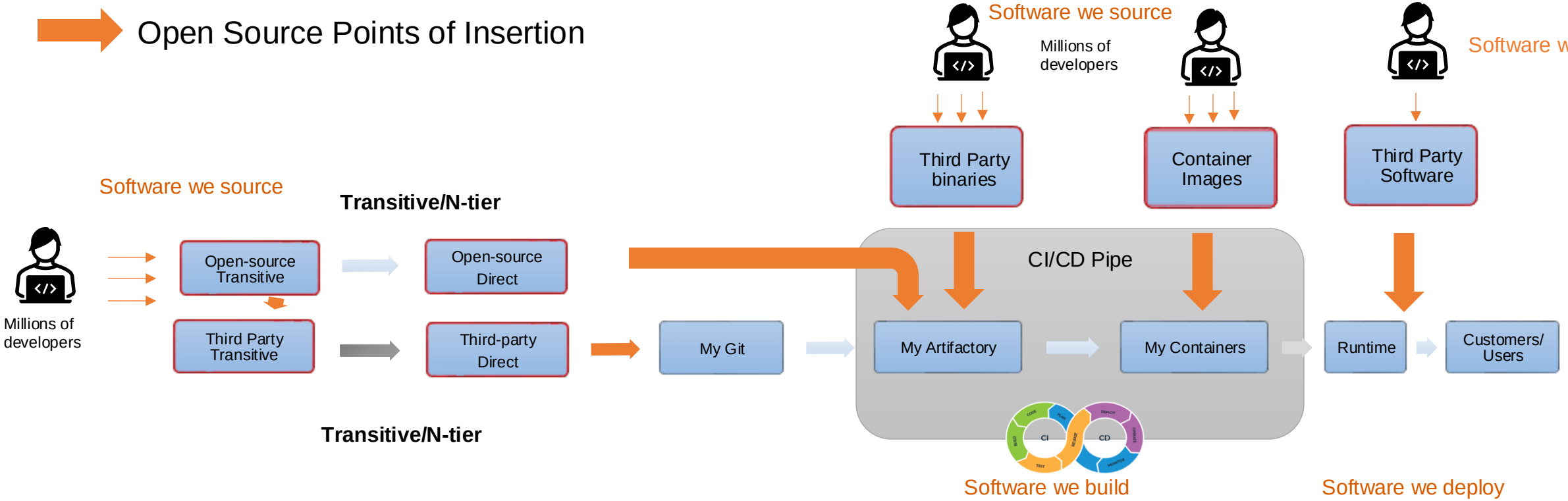
LINEAJE PLATFORM

CHALLENGE	BUSINESS IMPLICATIONS	LINEAJE SOLUTION CAPABILITY
The Software Supply Chain is Opaque	Invisible components in software you source, build, deploy or buy (e.g., log4j)	**100% Supply Chain Illumination**: ***Crawlers*** automate discovery of 100% of the components in your software, including all dependencies and transitive dependencies.
Unknown Risks Inherent in the Software Supply Chain	Dev teams introduce risky components because they lack visibility into the unknown risks in open-source	**Open-Source Risk Reputations**: Automated assessment including code quality, security posture, provenance, and vulnerabilities for inherent risks.
95% Of Vulnerabilities Are in Open Source	Over $13B annually spent on vulnerability management in the US	**Smart Patching:** Automate compatibility analysis and patch without breaking your software.
56% Of Vulnerabilities Lack Viable Solutions	Extensive resources expended to address vulnerabilities through increased monitoring, manual interventions, and work-arounds	**AI-Enabled OSS Remediation:** Automate fixing "unfixed" open-source code and contribute back to the ecosystem for components used in your software.
600% Increase in Supply Chain Attacks	Supply chain attacks such as SolarWinds and 3CX have resulted in millions of dollars in losses for affected businesses	**Supply Chain Threat Detection**: Attest the integrity of the supply chain including open-source, build, third-party COTS, and deployed software.

UNCLASSIFIED

Eagle Eye Provides Visibility, Scanners, and Remediations End to End

Open Source Points of Insertion



DISCOVER

- Dependencies
- Deep Transitive Dependencies
- Provenance
- Geo-provenance
- Authors / Contributors
- Age
- Integrity / Tamper Risks
- Dubious Origin Components
- Tampered Components
- Unknown Components

DETECT

- Vulnerability Scan
- Exploitability
- Reachability
- Licenses
- SAST Scan
- DAST Scan
- Code Quality Scan
- Security Posture Scan
- Binaries In Code
- Exposed Credentials / Tokens
- Suspicious Contributors
- Malware Scan
- Build Pipeline Integrity

PLAN

- AI Smart Remediation Planning
- Well Maintained Open Source Projects and Available Fixes
- Unmaintained Open Source Projects With No Fixes
- Incompatible Versions
- Unmaintained Transitive Dependencies
- Banned Components
- EOL Components

FIX

AI-Remediation

- Compatible Plan (developer instructions with fixes that will not break your software)
- Minor Plan (developer instructions with fixes that may introduce some breaking changes)
- Major Plan (developer instructions to forlk /

SEARCH

- **Natural Language Search**
  Perform intricate queries to find and assess risks by simply asking questions in everyday language

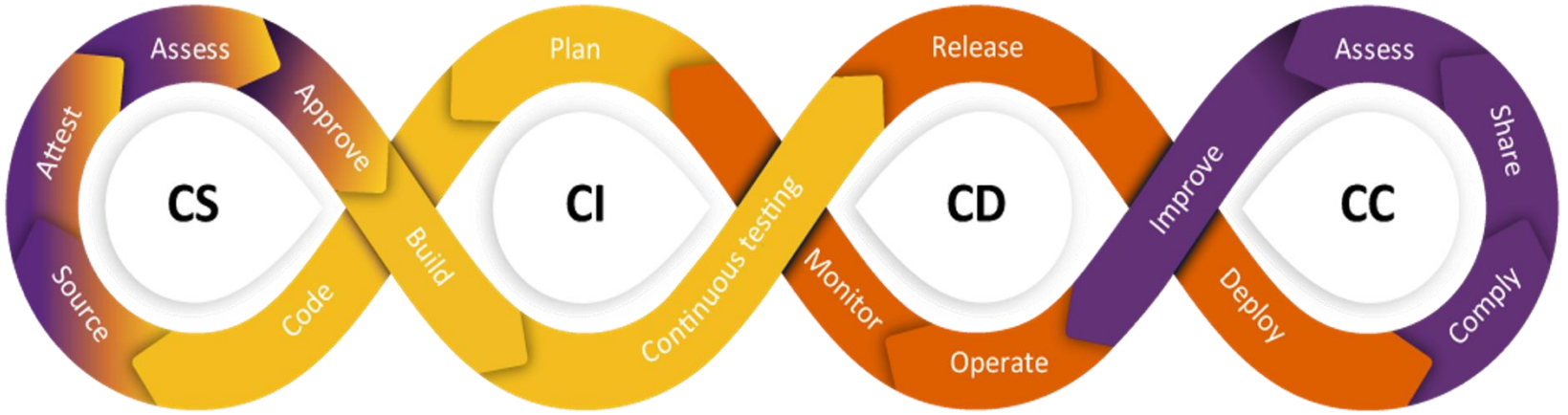
GOVERN

- **Automated Policies**

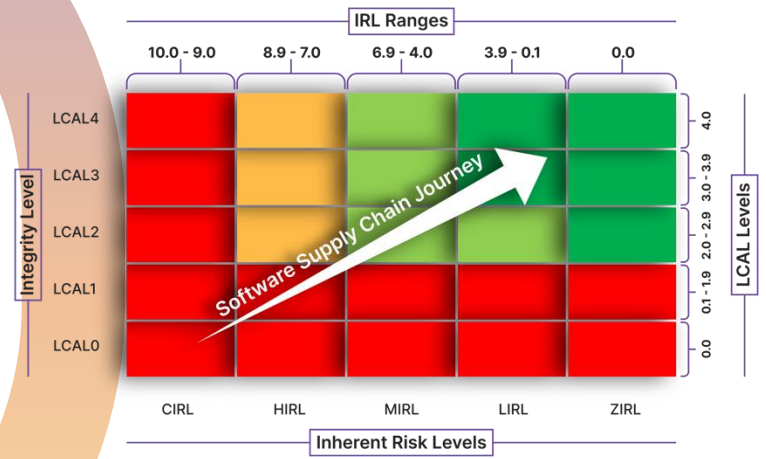
- Lifecycle stages and gates
- Polices defined by functions (legal, AppSec, Compliance, Dev, etc.)

Lineaje Platform enables Find-to-Fix Capabilities

Dependency Crawler | Scanner Hub | Fingerprint Based Attestation | Policy Based Risk Prioritization | Supply Chain Threat Detection



AI Plan

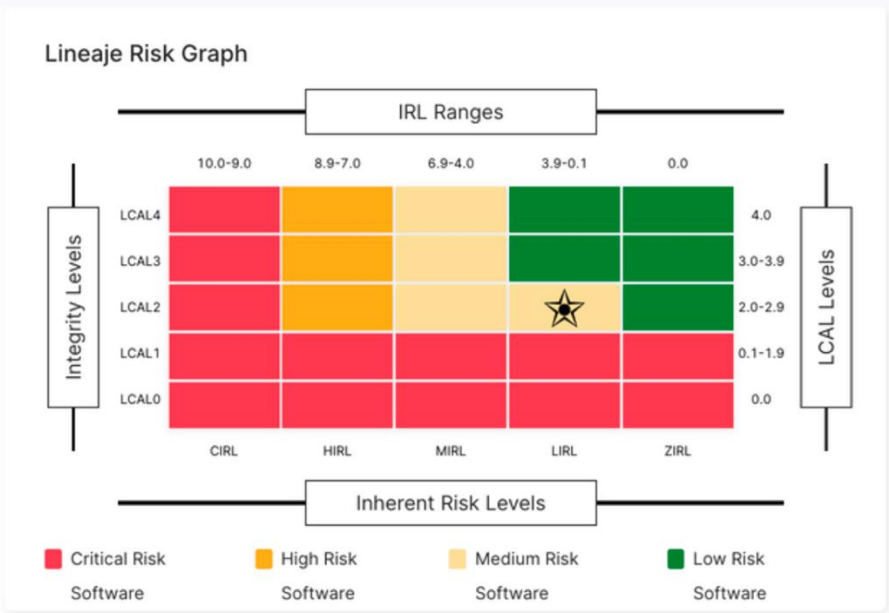


AI Assign

SBOM Manager to Govern and Privately Share all SBOMs

Compliance Remediation | Compliance Hub | Cross Org Remediation

How Risky is Each Project?



Number of Components: 1283

Mean Inherent Risk Level of Components (IRL) (Low 0.6)

Mean Component Attestation Level (Attested 2.6)

In Lineage Risk Graph Aggregate Risk Score based on Inherent Risk Level (IRL) and Lineage Component Attestation Level (LCAL) offers organizations a robust framework for assessing and mitigating risks associated with their software projects.

Aggregate Risk Score based on Inherent Risk Level (IRL):
Comprehensive Risk Assessment: By analyzing inherent risk across 170 dimensions, the Lineage Risk Graph provides a comprehensive assessment of potential risks associated with each component in the software project.

Lineage Component Attestation Level (LCAL):
Identification of Software Integrity Risks: LCAL provides insights into the software integrity or "tamperability" risks associated with the project's components. This helps in identifying vulnerabilities and weaknesses that could compromise the integrity of the software.

Showtime!

Questions…