ActiveState

Why SAST DAST & IAST Are Not Enough

And How to Cover your Software Supply Chain Ass

ActiveState

Introductions

Nicole Schwartz

Security Product Manager
ActiveState

Dana Crane

Product Marketing Mgr
ActiveState

ActiveState

Housekeeping

- We will host 2 polls during the webinar
- We will be emailing everyone the slides after the webinar
- Submit your questions in the Q&A tab and we will answer at the end

ActiveState

Our Mission

- Purpose
  - Create technology that just works: open source software that's easy to use and safe for Enterprises to adopt.
- What We Deliver
  - A secure open source software supply chain for the modern enterprise

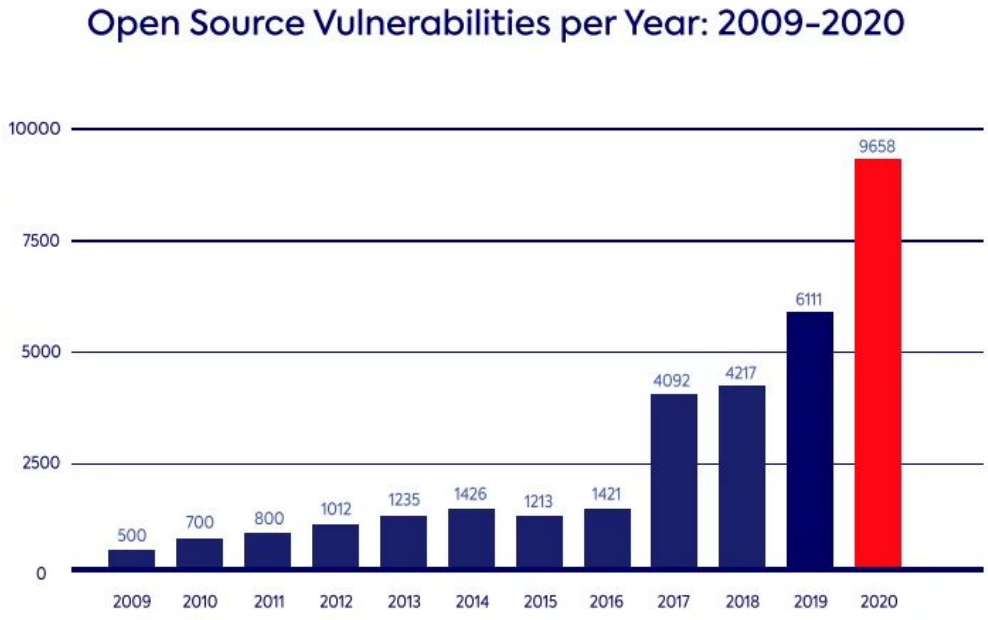
ActiveState

Traditional AppSec

- SAST - identify source code vulnerabilities
- DAST - identify running code vulnerabilities
- IAST - identify vulnerabilities in code that are exploitable at runtime
- SCA - identify vulnerabilities in open source packages
- IaC - Infrastructure as Code scanning

ActiveState

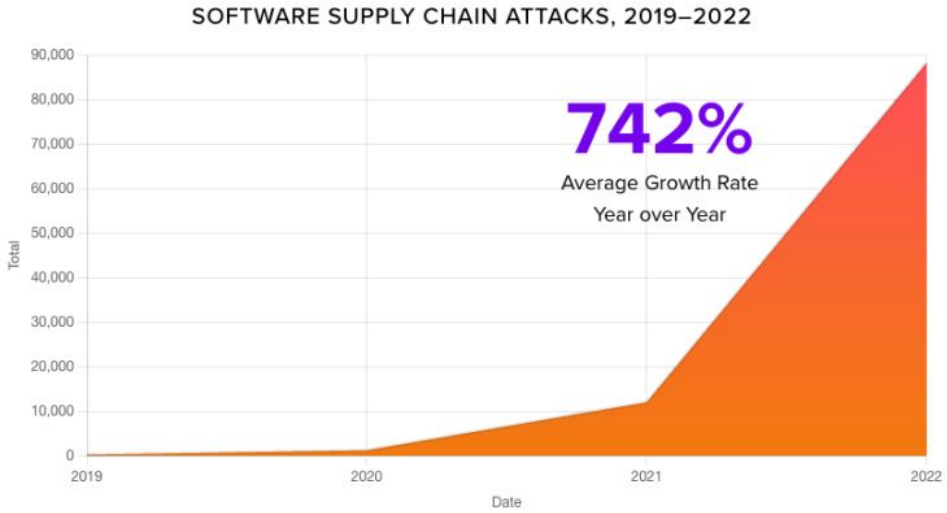
Vulnerabilities are Growing



Source: mend.io

ActiveState

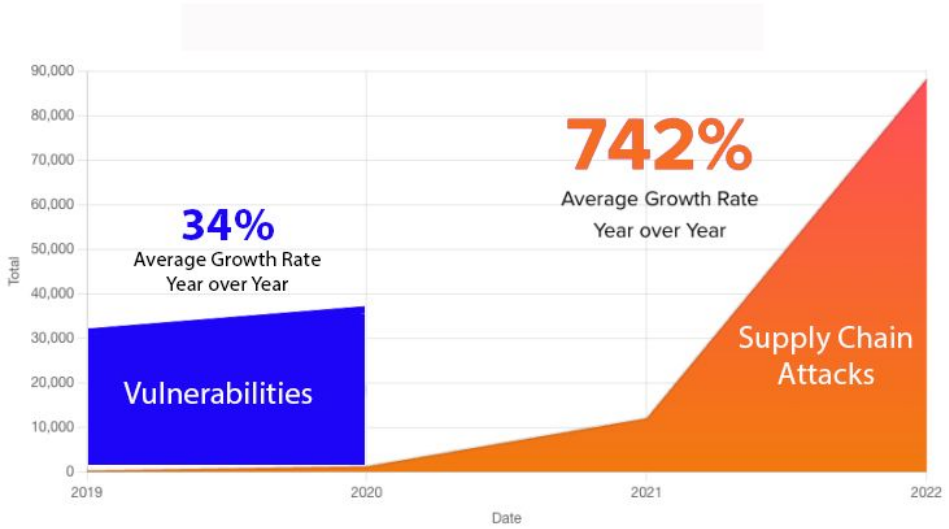
But Software Supply Chain Attacks are also Growing



Source: Sonatype State of the Software Supply Chain

ActiveState

Supply Chain Attacks vs Vulnerabilities



ActiveState

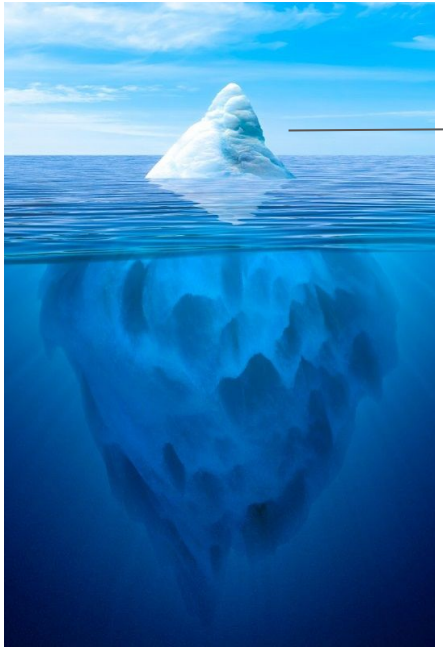
Traditional AppSec Not Enough

74% of IT pros believe technologies like static and dynamic application security testing [SAST & DAST] are important, but feel that those technologies aren't enough to protect them from supply chain threats

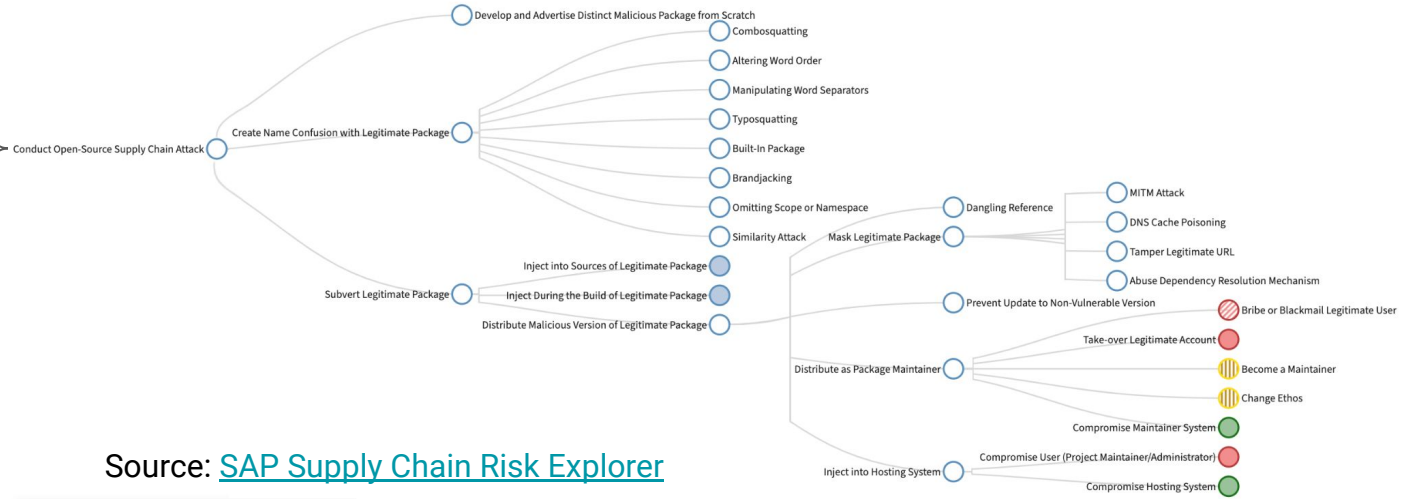
Source: ReversingLabs Software Supply Chain Risk Survey

ActiveState

Vulnerabilities are the Tip of the Threat Iceberg



Vulnerabilities



Source: [SAP Supply Chain Risk Explorer]

ActiveState

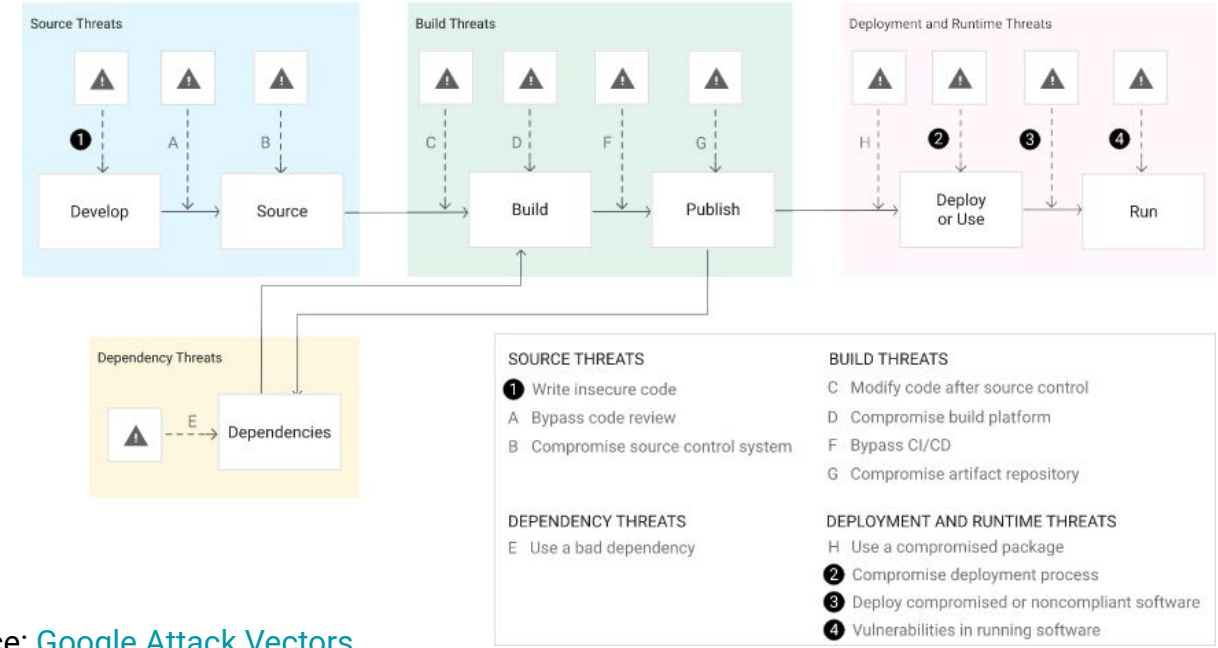
Poll: Which issues do you currently prioritize?

Assuming the same level of criticality, which would you prioritize first?:

- Threats posed by flaws in proprietary source code
- Threats found in running applications
- Threats posed by vulnerabilities in open source packages
- Threats posed by software supply chain security attacks

ActiveState

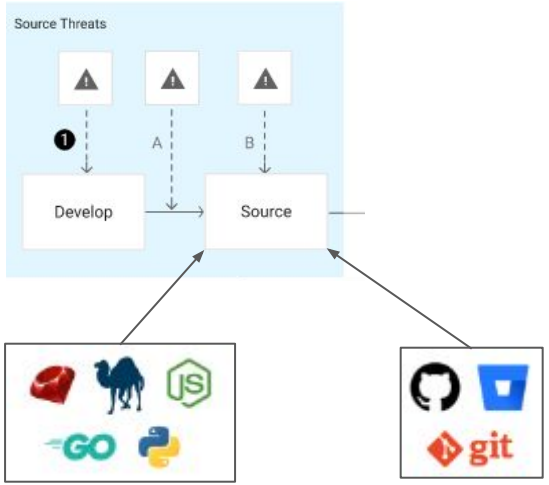
Threat Detection & Enforcement Points



Source: [Google Attack Vectors]

ActiveState

Threat Detection & Enforcement Points



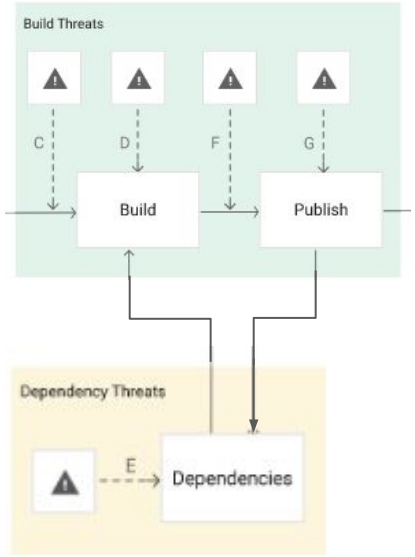
Open source code

Proprietary code

Source	Version Controlled	✓
	Verified History	✓
	Retained Indefinitely	✓
	Two-Person Reviewed	✓

ActiveState

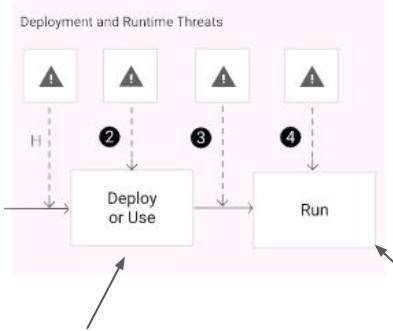
Threat Detection & Enforcement Points



Build	Scripted	✓
	Build Service	✓
	Ephemeral Environment	✓
	Isolated	✓
	Parameterless	✓
	Hermetic	✓
	Reproducible	✓

ActiveState

Threat Detection & Enforcement Points



Validation on install

Signed artifacts

ActiveState

SLSA Spells “Control”

Source Threats:	Provenance Attestations
Build Threats:	Secure Build Service
Dependency Threats:	Verification Summary Attestations (VSAs)
Deployment/Runtime Threats:	Signing
	Verification at deployment

ActiveState

Poll: Your Best Practices

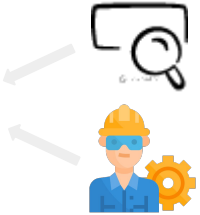
How many supply chain controls do you implement in your dev process? Check all that apply:

- We check all proprietary code
- We check all open source code
- We build all dependencies from source code
- Our builds are repeatable
- We create and/or validate Attestations
- We sign all our artifacts

ActiveState

ActiveState Platform Demo

CATALOG



ActiveState

We crawl the web for Open Source. Our Build Engineers clean, fix and augment the data. (example add C dependencies)

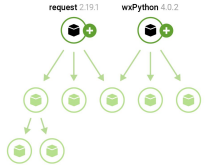
DEPENDENCY MANAGER

Teams organize their build requirements into projects

+ request 2.19.1
+ wxPython 4.0.2

SOLVER

Our universal Solver computes **all needed dependencies** based on the catalog at a fixed point in time and submits the required SBOM to the Build Cluster

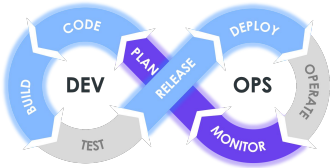


BUILD CLUSTER

Build Manager coordinates parallel builds in the cluster. Build nodes draw existing artifacts if available, build new artifacts in hermetically sealed containers and record result in the Artifact Store

ARTIFACT STORE

Various distribution methods exist to deploy artifacts and complete reproducible environments (runtimes) to various points in your SLDC



ActiveState

Q&A

ActiveState

Next Steps

Schedule a demo with our product experts:
https://www.activestate.com/solutions/contact-sales/

Take our Supply Chain Security Survey & find out how you rate:
https://www.surveymonkey.com/r/BNGZPH6

Try the ActiveState Platform for free:
https://platform.activestate.com/