Securing Diverse Supply Chains

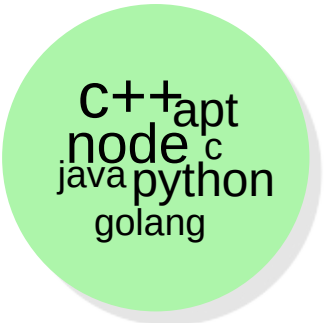
across Interconnected Systems

Wayne Starr
Aaron Creel
01 February 2023

The Problem

> Synergizing activities across an organization for Large Software Systems can be difficult and time consuming.

Teams



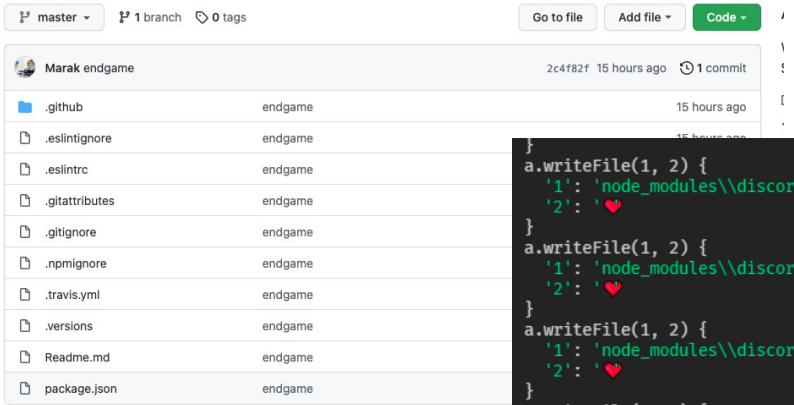
Ecosystems

Environments

One Software Project*

* Not including containers, web or infrastructure components

Why Solve This?



Solutions

Policy

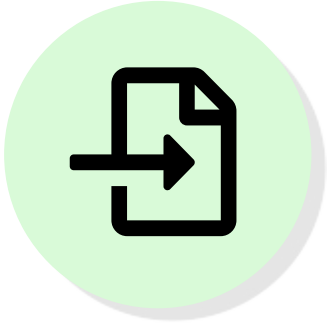
Implement organizational standards to capture data consistently

Automation

Check dependencies and vulnerabilities with automated tooling

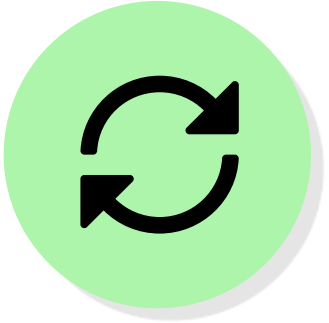
Policy

Standard Checkpoints



On Import

Check packages when they enter the dev environment



On Integration

Check packages on build or in continuous integration

On Deployment

Check packages as they are deployed to production

The Stale Shelf

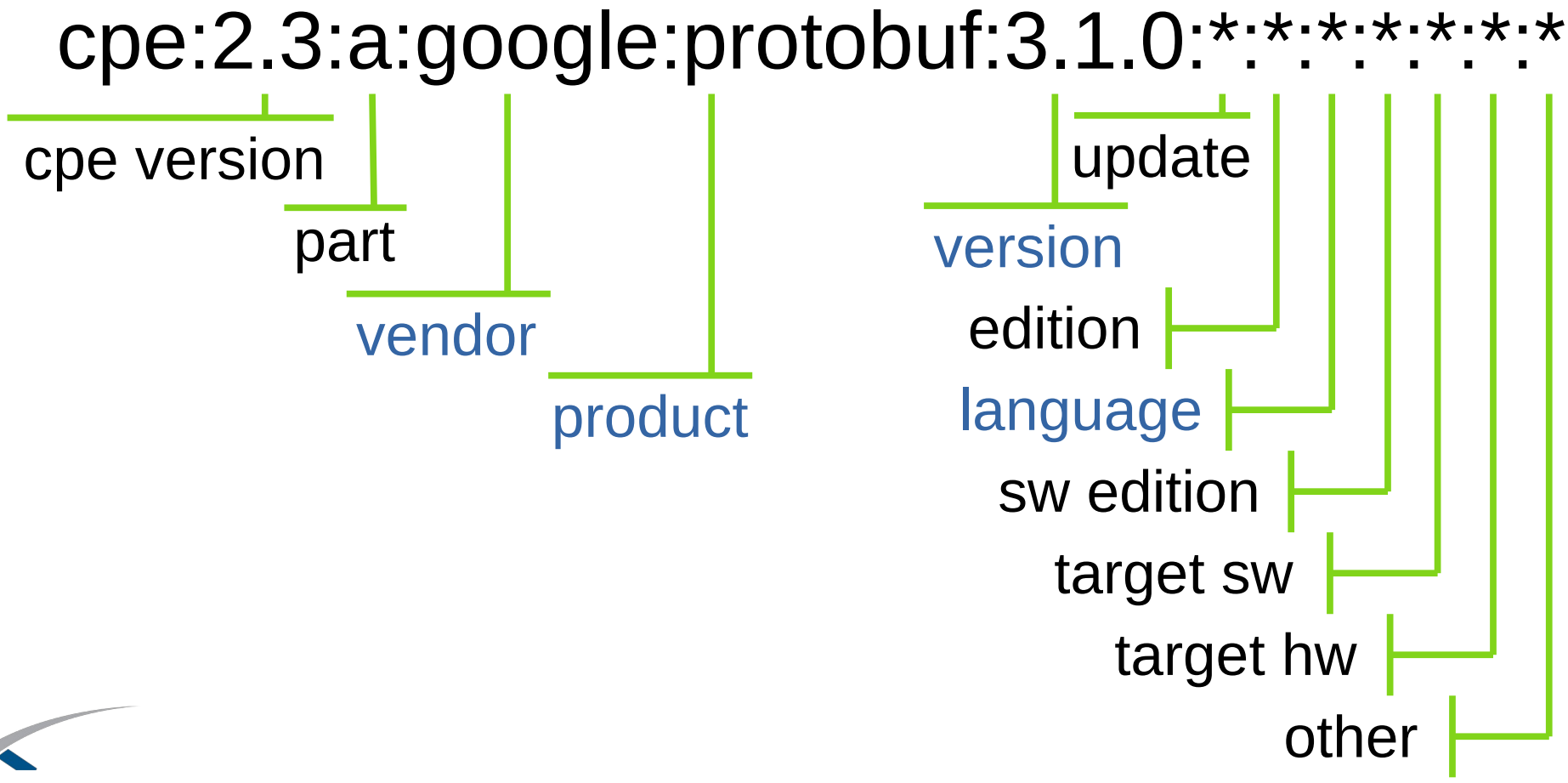
> In addition to common checkpoints you must continuously evaluate the products that you have running in production.
>
> Vulnerabilities never stop being discovered and you must be prepared to respond when updates are required.

Keep Things Simple

> Reduce developer friction through standardized / templated tooling within the enterprise
>
> Tighten feedback loops within the environment developers use today to provide feedback quickly

Automation

Package Identification



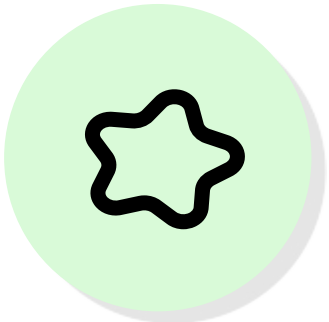
Analysis Considerations

Is this package on disk or in a requirements file?

Is this package publicly available or private?

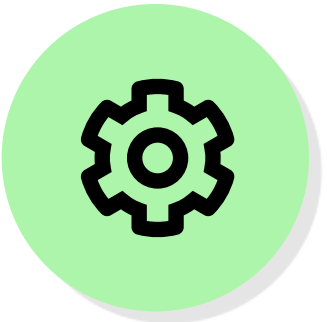
Is this package actually in use by the application?

Shortcomings



Consistency

Tooling can be inconsistent or not provide required information across package ecosystems



Configurability

SBOM utilities sometimes lack the configurability needed to run within large (slow) codebases

Management

Once data is collected, managing data and keeping things together can be difficult

Demo

Questions