Reducing Supply Chain Risk with SBOMs and Dependency-Track

OWASP Switzerland

21 June 2021

Reduce Supply Chain Risk

About

- Creator of OWASP Dependency-Track
- Chair of CycloneDX Core Working Group
- Leader and Co-Author of OWASP SCVS
- Contributor to Package URL Specification
- Multiple Software Transparency Working Groups
- Software Security Leadership at ServiceNow

- @stevespringett
- steve.springett@owasp.org
- https://stevespringett.com
- https://github.com/stevespringett

Background

- Flagship OWASP project – founded in 2013
- Highly mature
- Large community of contributors and adopters
  - Vibrant community on OWASP Slack workspace
  - 1M Docker pulls
- Open Source – Available under the Apache 2.0 license

Got SBOM?

Analogy

INGREDIENTS: Peanuts Roasted Salted (Peanuts, Sunflower Oil, Salt), Chocolate Peanuts Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Peanuts Blanched Roasted (Peanuts, Sunflower Oil)), Almonds, Chocolate Coffee Beans Naural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Coffee Beans Espresso Roasted), Pecans, Organic Dark Chocolate Drops (Organic Evaporated Cane Syrup, Organic Chocolate Liquor, Organic Cocoa Butter, Organic Soy Lecithin), Chocolate Almonds Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Almonds), Yogurt Almonds Natural (Yogurt Coating Natural (Evaporated Cane Syrup, Palm Kernel Oil, Yogurt Powder, Soy Lecithin (an Emulsifier), Lactic Acid, Natural Vanilla, Salt), Almonds)

CONTAINS PEANUTS, SOY, NUTS, MILK

Analogy

INGREDIENTS: Peanuts Roasted Salted (Peanuts, Sunflower Oil, Salt), Chocolate Peanuts Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Peanuts Blanched Roasted (Peanuts, Sunflower Oil)), Almonds, Chocolate Coffee Beans Naural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Coffee Beans Espresso Roasted), Pecans, Organic Dark Chocolate Drops (Organic Evaporated Cane Syrup, Organic Chocolate Liquor, Organic Cocoa Butter, Organic Soy Lecithin), Chocolate Almonds Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Almonds), Yogurt Almonds Natural (Yogurt Coating Natural (Evaporated Cane Syrup, Palm Kernel Oil, Yogurt Powder, Soy Lecithin (an Emulsifier), Lactic Acid, Natural Vanilla, Salt), Almonds)

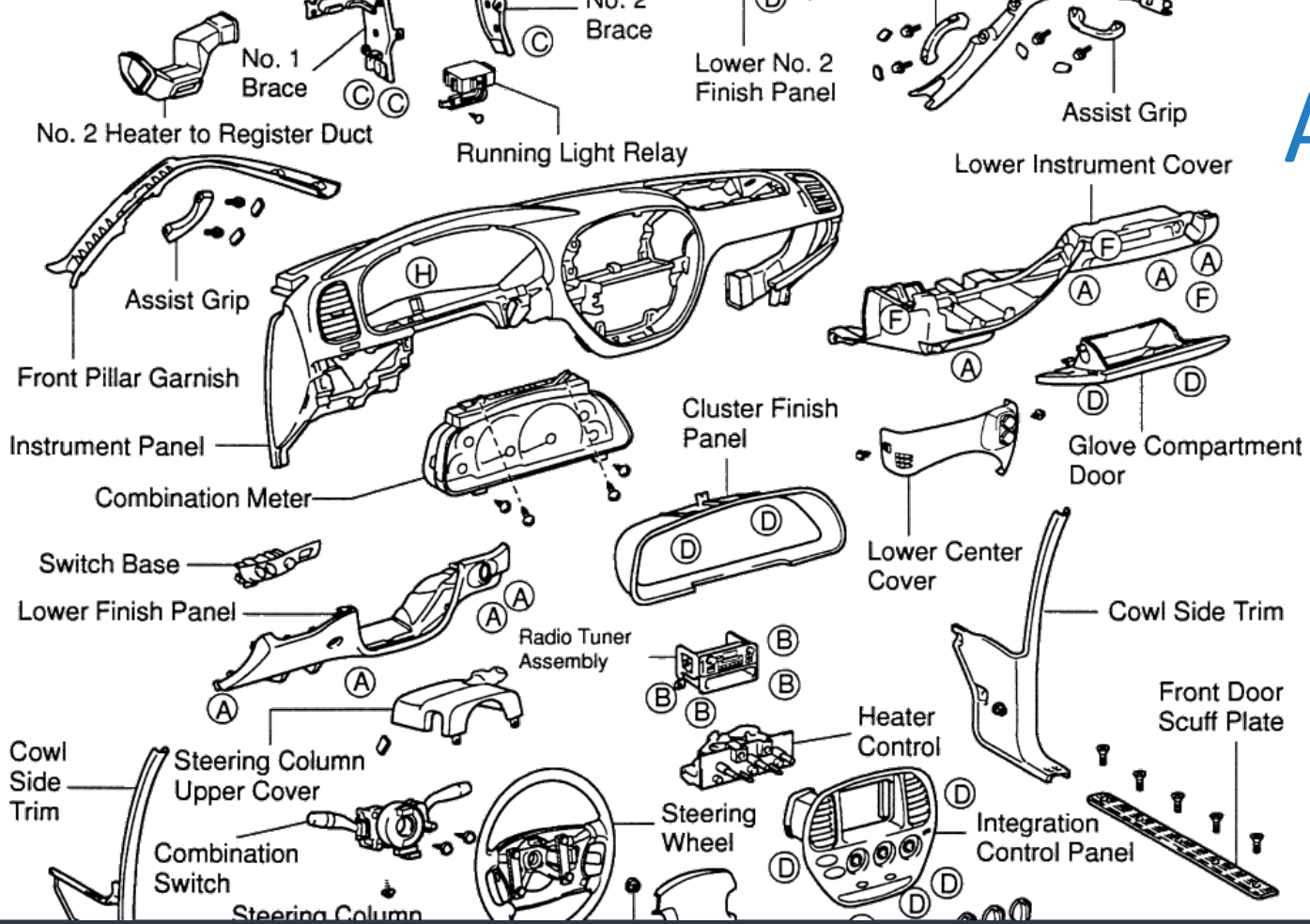
CONTAINS PEANUTS, SOY, NUTS, MILK

Analogy

INGREDIENTS: Peanuts Roasted Salted (Peanuts, Sunflower Oil, Salt), Chocolate Peanuts Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Peanuts Blanched Roasted (Peanuts, Sunflower Oil)), Almonds, Chocolate Coffee Beans Naural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Coffee Beans Espresso Roasted), Pecans, Organic Dark Chocolate Drops (Organic Evaporated Cane Syrup, Organic Chocolate Liquor, Organic Cocoa Butter, Organic Soy Lecithin), Chocolate Almonds Natural (Chocolate Coating Natural (Sugar, Palm Kernel Oil, Cocoa, Whey Powder (Milk), Cocoa Butter, Nonfat Milk Powder, Milk, Chocolate Liquor, Soy Lecithin (an Emulsifier), Natural Vanilla, Salt), Almonds), Yogurt Almonds Natural (Yogurt Coating Natural (Evaporated Cane Syrup, Palm Kernel Oil, Yogurt Powder, Soy Lecithin (an Emulsifier), Lactic Acid, Natural Vanilla, Salt), Almonds)

CONTAINS STRUTS

Analogy


No. 1 Brace
No. 2 Brace
Lower No. 2 Finish Panel
Assist Grip
No. 2 Heater to Register Duct
Running Light Relay
Lower Instrument Cover
Assist Grip
Front Pillar Garnish
Instrument Panel
Combination Meter
Cluster Finish Panel
Glove Compartment Door
Lower Center Cover
Switch Base
Lower Finish Panel
Radio Tuner Assembly
Cowl Side Trim
Front Door Scuff Plate
Heater Control
Cowl Side Trim
Steering Column Upper Cover
Steering Wheel
Integration Control Panel
Combination Switch
Steering Column

SBOM Formats

- CycloneDX
  - Security focused standard with origins in the OWASP community
- Software Package Data Exchange (SPDX)
  - License and IP focused standard created by Linux Foundation

About CycloneDX

- Flagship OWASP standards project
- Leading SBOM format
- Large ecosystem of official, community, and commercial tool support
- https://cyclonedx.org/
- https://owasp.org/cyclonedx

Contributing Factors

- Compliance
- Regulation
  - FDA and others
- Economic / Supply-Chain Management
  - Use fewer & better suppliers, use highest quality parts, track throughout lifecycle
- Market Forces
  - SDLC maturity, procurement, operational costs, risks, impact analysis
- Forensics
  - NTSB and others

What does Dependency-Track do?

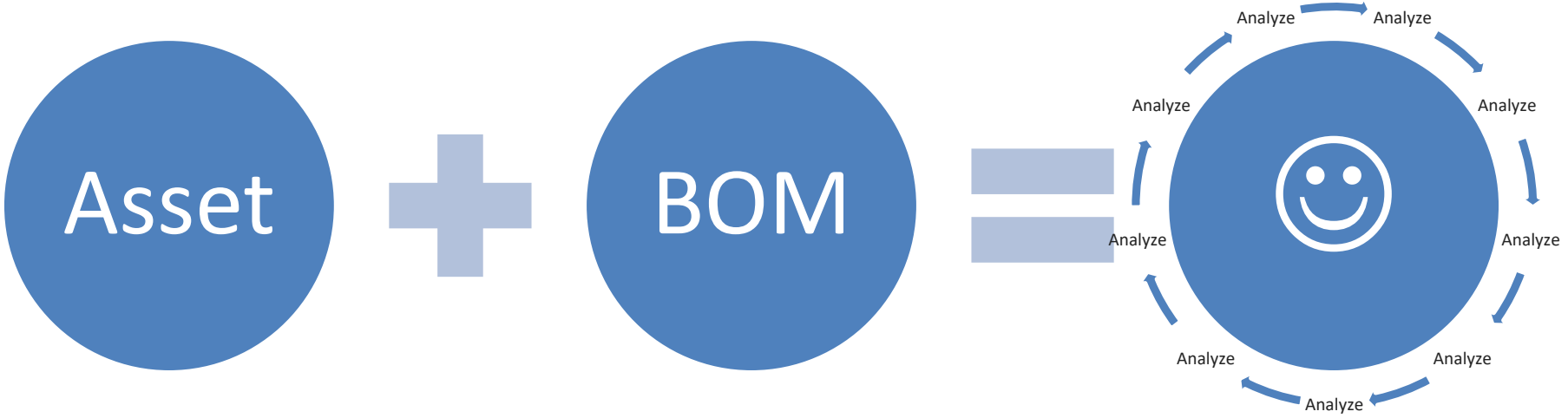
Consumes, analyzes, and produces SBOMs at high velocity

Ideal for use in modern build pipelines

Ideal for procurement and M&A

Quickly answer:
What is affected, and where

Conceptually



Conceptually

SBOM Production
Software Bill-of-Materials created during CI/CD or acquired from suppliers

SBOM Analysis
Analyzes components for security, operational, and license risk

Intelligence Streams
Produces real-time analysis and security events delivering actionable findings to external systems

SBOM Ingestion
SBOMs published to Dependency-Track via REST, Jenkins plugin, or uploaded through web interface

Continuous Monitoring
Continuously analyzes portfolio for risk and policy compliance

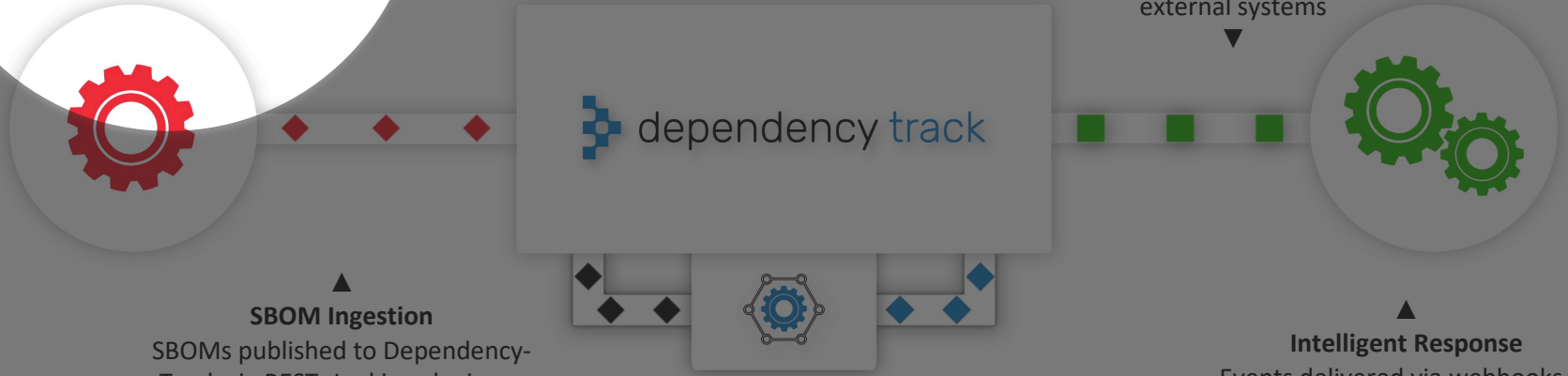
Intelligent Response
Events delivered via webhooks or chat-ops and findings published to risk management and vulnerability aggregation platforms

Conceptually

SBOM Production
Software Bill-of-Materials created during CI/CD or acquired from suppliers

SBOM Analysis
Analyzes components for security, operational, and license risk

Intelligence Streams
Produces real-time analysis and security events delivering actionable findings to external systems



SBOM Ingestion
SBOMs published to Dependency-Track via REST, Jenkins plugin, or uploaded through web interface

Continuous Monitoring
Continuously analyzes portfolio for risk and policy compliance

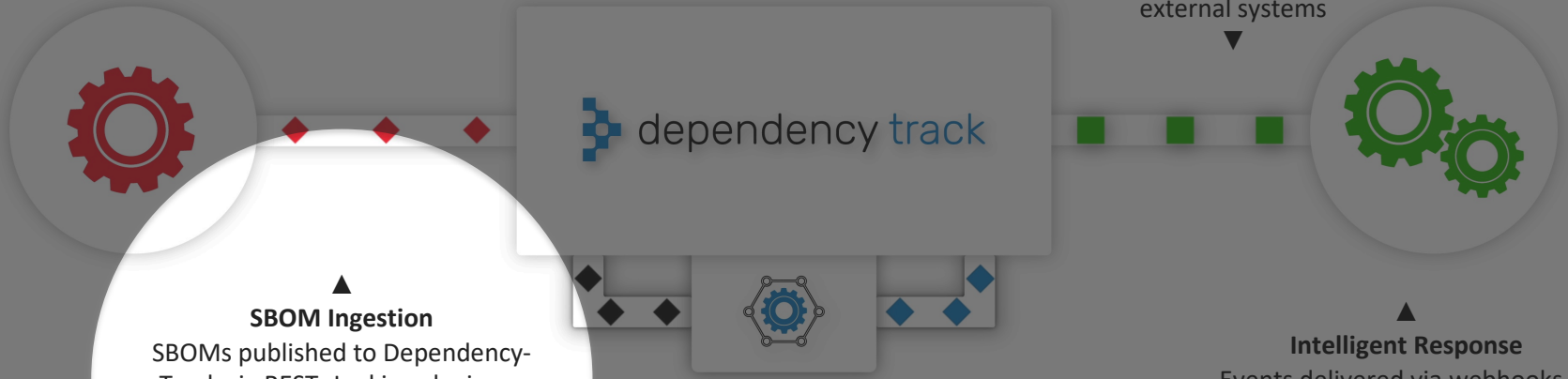
Intelligent Response
Events delivered via webhooks or chat-ops and findings published to risk management and vulnerability aggregation platforms

Conceptually

SBOM Production
Software Bill-of-Materials created during CI/CD or acquired from suppliers

SBOM Analysis
Analyzes components for security, operational, and license risk

Intelligence Streams
Produces real-time analysis and security events delivering actionable findings to external systems



SBOM Ingestion
SBOMs published to Dependency-Track via REST, Jenkins plugin, or uploaded through web interface

Continuous Monitoring
Continuously analyzes portfolio for risk and policy compliance

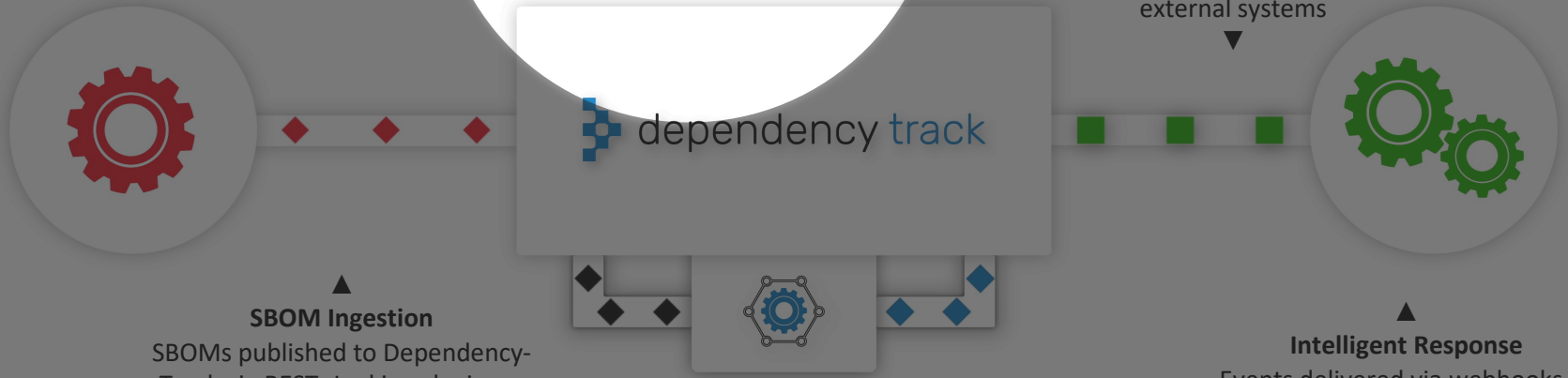
Intelligent Response
Events delivered via webhooks or chat-ops and findings published to risk management and vulnerability aggregation platforms

Conceptually

SBOM Production
Software Bill-of-Materials created during CI/CD or acquired from suppliers

SBOM Analysis
Analyzes components for security, operational, and license risk

Intelligence Streams
Produces real-time analysis and security events delivering actionable findings to external systems



SBOM Ingestion
SBOMs published to Dependency-Track via REST, Jenkins plugin, or uploaded through web interface

Continuous Monitoring
Continuously analyzes portfolio for risk and policy compliance

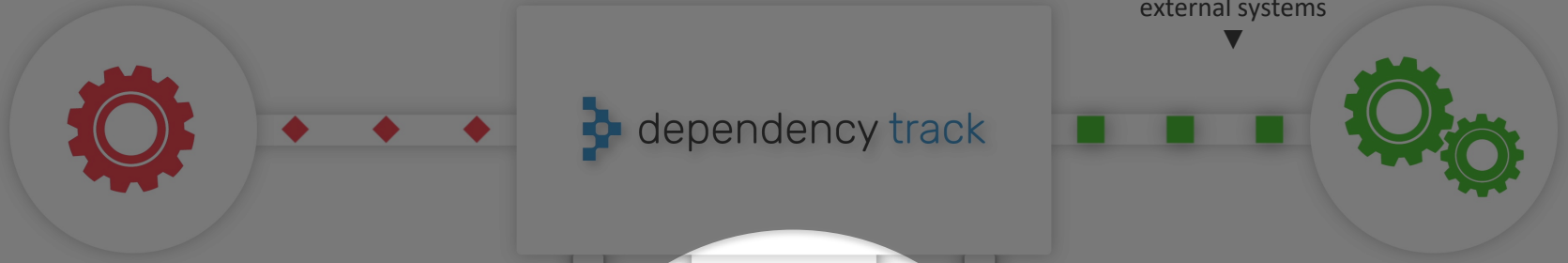
Intelligent Response
Events delivered via webhooks or chat-ops and findings published to risk management and vulnerability aggregation platforms

Conceptually

SBOM Production
Software Bill-of-Materials created during CI/CD or acquired from suppliers

SBOM Analysis
Analyzes components for security, operational, and license risk

Intelligence Streams
Produces real-time analysis and security events delivering actionable findings to external systems



SBOM Ingestion
SBOMs published to Dependency-Track via REST, Jenkins plugin, or uploaded through web interface

Continuous Monitoring
Continuously analyzes portfolio for risk and policy compliance

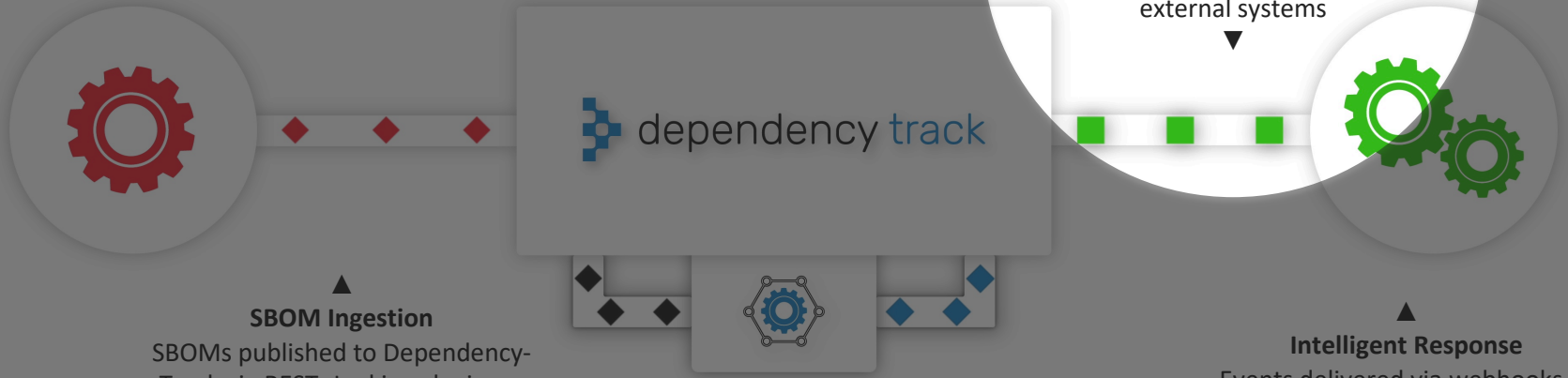
Intelligent Response
Events delivered via webhooks or chat-ops and findings published to risk management and vulnerability aggregation platforms

Conceptually

SBOM Production
Software Bill-of-Materials created during CI/CD or acquired from suppliers

SBOM Analysis
Analyzes components for security, operational, and license risk

Intelligence Streams
Produces real-time analysis and security events delivering actionable findings to external systems



SBOM Ingestion
SBOMs published to Dependency-Track via REST, Jenkins plugin, or uploaded through web interface

Continuous Monitoring
Continuously analyzes portfolio for risk and policy compliance

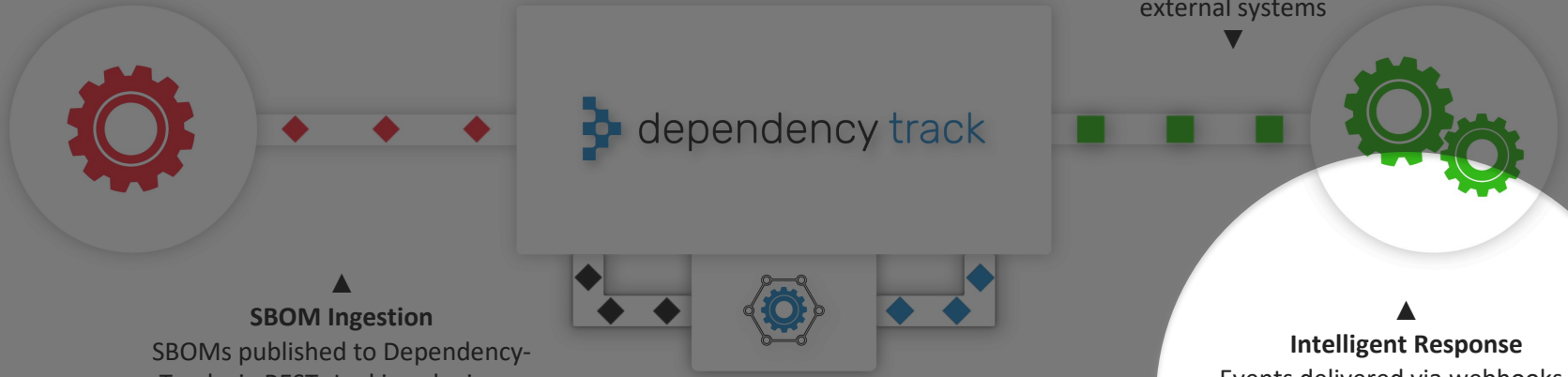
Intelligent Response
Events delivered via webhooks or chat-ops and findings published to risk management and vulnerability aggregation platforms

Conceptually

SBOM Production
Software Bill-of-Materials created during CI/CD or acquired from suppliers

SBOM Analysis
Analyzes components for security, operational, and license risk

Intelligence Streams
Produces real-time analysis and security events delivering actionable findings to external systems



SBOM Ingestion
SBOMs published to Dependency-Track via REST, Jenkins plugin, or uploaded through web interface

Continuous Monitoring
Continuously analyzes portfolio for risk and policy compliance

Intelligent Response
Events delivered via webhooks or chat-ops and findings published to risk management and vulnerability aggregation platforms

Conceptually

SBOM Production
Software Bill-of-Materials created during CI/CD or acquired from suppliers

SBOM Analysis
Analyzes components for security, operational, and license risk

Intelligence Streams
Produces real-time analysis and security events delivering actionable findings to external systems

SBOM Ingestion
SBOMs published to Dependency-Track via REST, Jenkins plugin, or uploaded through web interface

Continuous Monitoring
Continuously analyzes portfolio for risk and policy compliance

Intelligent Response
Events delivered via webhooks or chat-ops and findings published to risk management and vulnerability aggregation platforms

DEMO

Isn’t this SCA?


oh
Hell
no!

Inventory

Assembly

Provenance

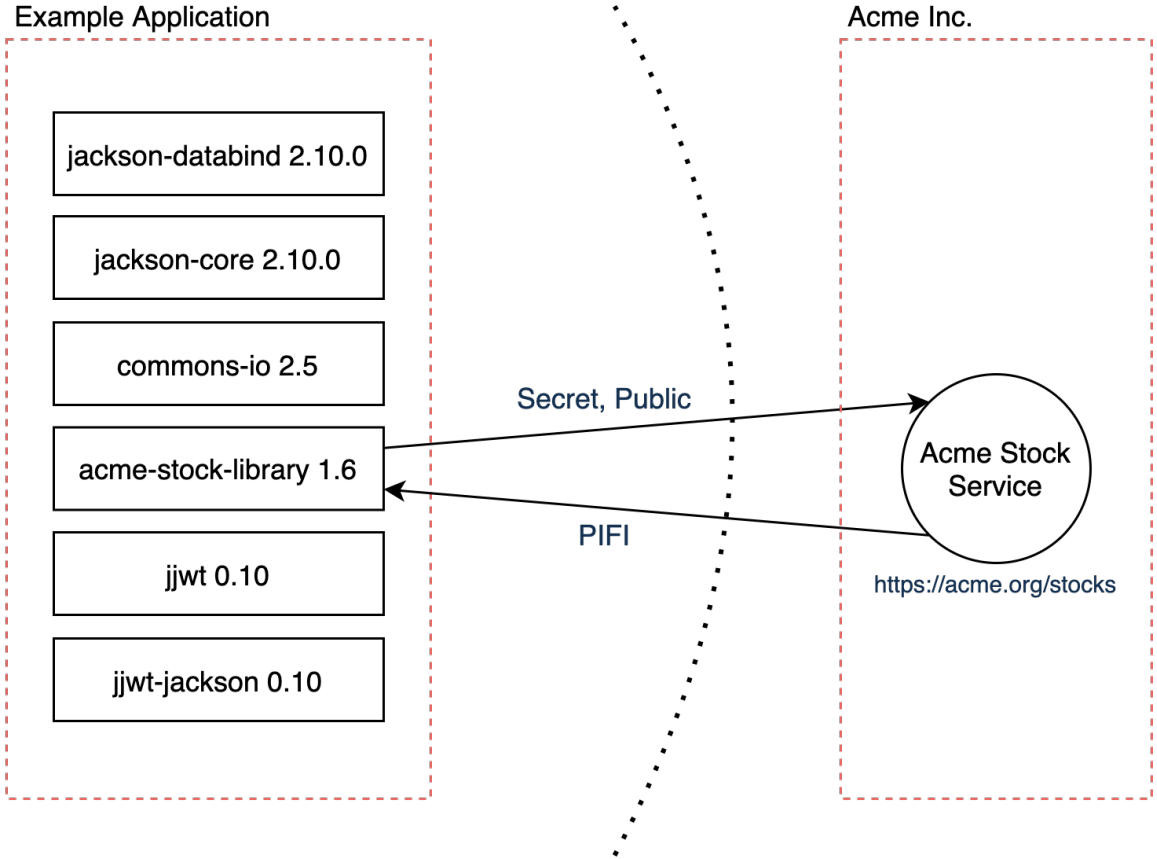
Pedigree

Packaging and distribution

Remediation and disclosure

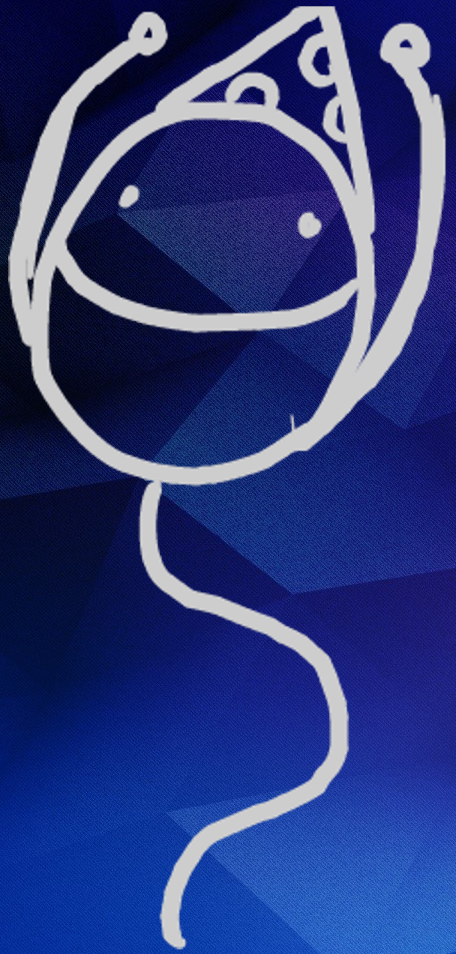
Hardware

Services

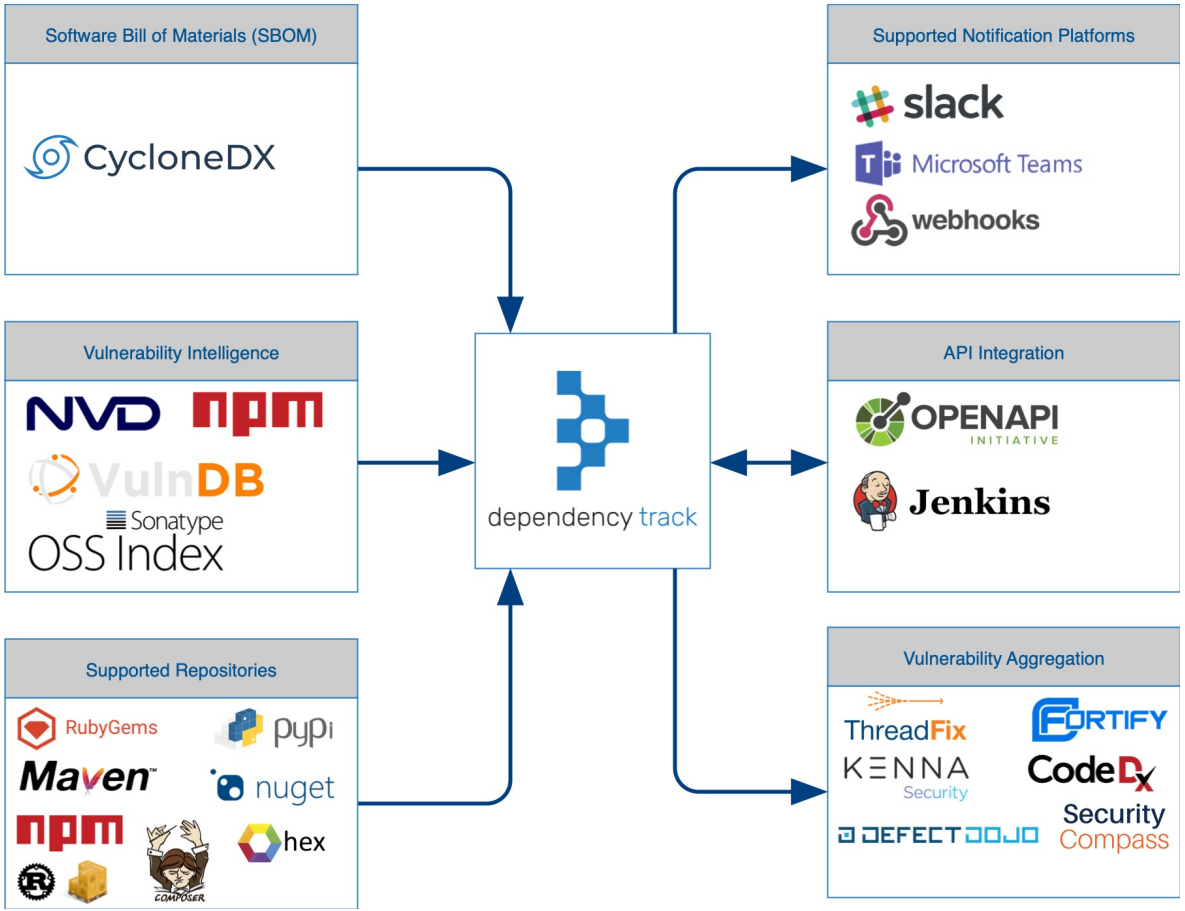


Services

- Describes the provider
- Endpoint URIs
- Data classifications
- Directional flow of data
- Authentication requirements
- Trust boundary traversal
- License
- External references



oh yes!



Integrations

- Ingest BOMs during CI/CD
- Analyzes continuously
- Notifications on
  - New vulnerability
  - New vulnerable dependency
  - Audit decision changes
  - Outdated versions
    BOM consumed and processed
  - Policy violations
- Monitor activity (slack, teams)
- Automate response (webhooks)
- Part of organizations risk metrics

Project Info

- GitHub
  - https://github.com/DependencyTrack
- Social Media
  - https://twitter.com/DependencyTrack
  - https://www.youtube.com/c/OWASPDependencyTrack
- Documentation
  - https://docs.dependencytrack.org
- Website
  - https://dependencytrack.org

Thank You