



Software Trust & Transparency: Artifacts

November 2021

Matt Fussa

Trust Strategy Officer

Artifacts

Evidence that demonstrates that an organization is:

- following a documented process or meeting a specific requirement;
- Are gathered and archived throughout the system development life cycle;
- are to be used as evidence in internal and/or external audits and assessments.

Secure Development Lifecycle



Cisco Secure Development Lifecycle.

Repeatable. Measurable. Resilient. Trustworthy.

- Rigorous, evolving product security baseline
- Minimizes vulnerabilities, enhances security
- Embeds security across the portfolio



NIST 800-53 SCRM Mapping

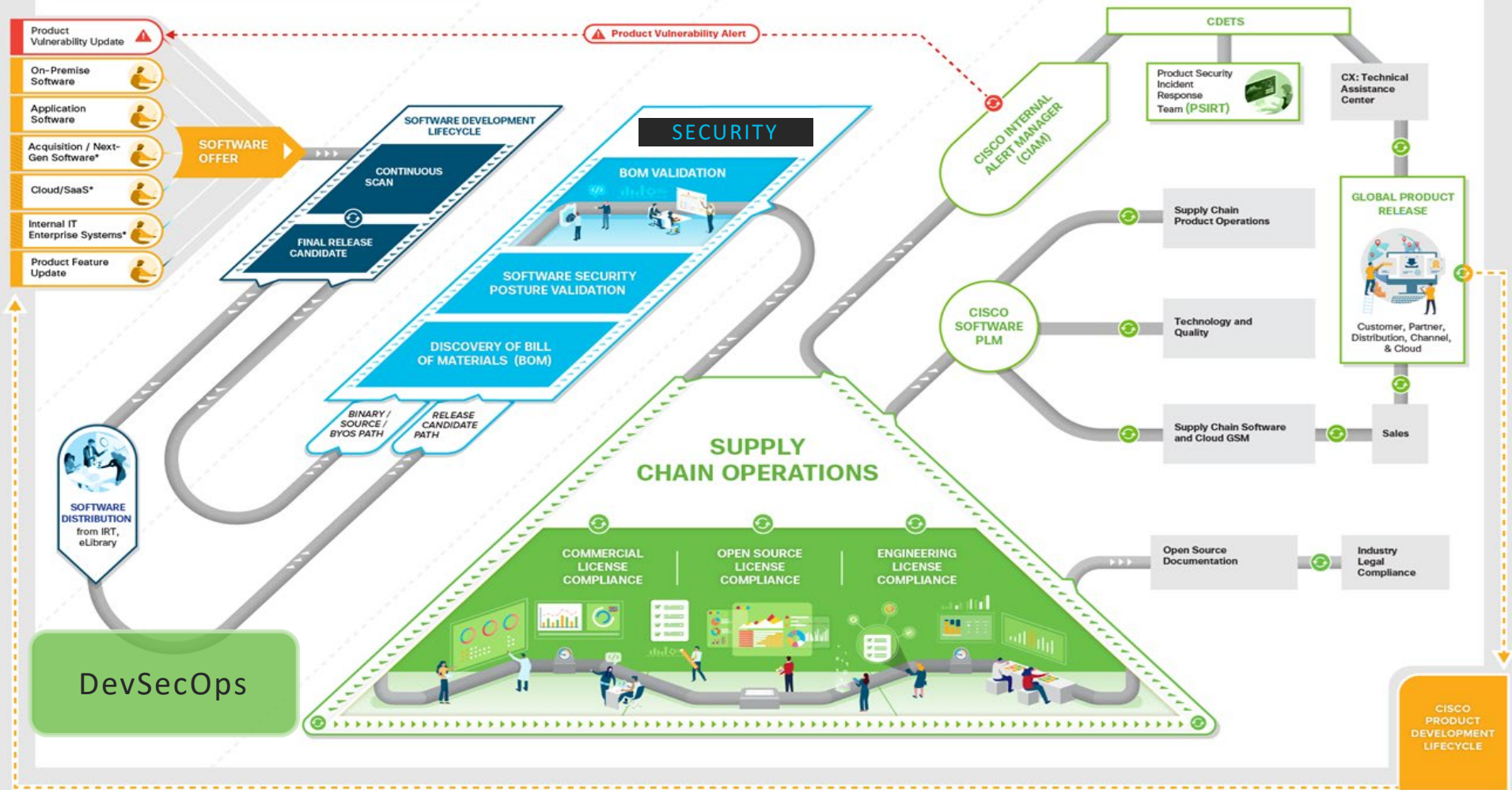
		Master Security Specification	Cisco Secure Development Lifecycle	Supply Chain Security Team	InfoSec	Acquisition & Integration Team	Secure Boot	Trust Anchor Module	Approved Vendor List	Supply Chain Resiliency Team	Quality Assurance	PSIRT	Brand Protection Team
Control	Name	Value Chain Security Architecture				Trustworthy Technology		Cisco Policies, Procedures, and Teams					
SR-1	Policy and Procedures	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
SR-2	Supply Chain Risk Management Plan	✓	✓	✓	✓					✓			
SR-2 (1)	Establish SCRM Team			✓	✓					✓			✓
SR-3	Supply Chain Controls and Processes	✓		✓	✓		✓	✓	✓	✓	✓		
SR-3-1	Diverse Supply Base			✓					✓	✓			
SR-3-2	Limitation of Harm			✓					✓	✓			✓
SR-3-3	Sub-Tier Flow Down	✓		✓	✓				✓	✓	✓		✓
SR-4	Provenance	✓	✓	✓	✓		✓	✓				✓	
SR-4-1	Identity	✓		✓	✓								✓
SR-4-2	Track and Trace	✓											
SR-4-3	Validate as Genuine and Not Altered	✓	✓	✓			✓	✓			✓		✓
SR-4-4	Supply Chain Integrity - Pedigree	✓		✓	✓		✓	✓					
SR-5	Acquisition Strategies, Tools, and Methods			✓	✓	✓			✓				
SR-5-1	Adequate Supply			✓		✓			✓	✓			
SR-5-2	Assessments Prior to Selection, Acceptance, Modification, or Update		✓	✓									✓
SR-6	Supplier Assessments and Reviews	✓		✓	✓				✓				
SR-6-1	Testing and Analysis	✓	✓		✓								
SR-7	Supply Chain Operations Security	✓		✓					✓				✓
SR-8	Notification Agreements	✓		✓	✓					✓			
SR-9	Tamper Resistance and Detection	✓		✓	✓		✓	✓					✓
SR-9-1	Multiple Stages of System Development Lifecycle	✓	✓				✓	✓					
SR-10	Inspection of Systems and Components	✓		✓									✓
SR-11	Component Authenticity	✓	✓	✓			✓	✓				✓	✓
SR-11-1	Anti-Counterfeit Training	✓		✓									✓
SR-11-2	Config Control for Component Service and Repair	✓		✓									
SR-11-3	Anti-Counterfeit Scanning	✓	✓	✓	✓		✓	✓			✓		✓
SR-12	Component Disposal	✓		✓									✓

PRE-ENTRY

DISCOVERY

REGISTRATION

COMPLIANCE



SW Development: Robust Process = Substantive Artifacts

Build Environment Security Standard

- Inventory & Attribution
- Hardening
- Vulnerability Management
- Logging and Monitoring
- Segmentation
- Access
- Superuser guardrails
- Source Requirements
- Build Requirements
- Provenance Requirements

EO 14028 – Section 4, Enhanced Software Supply Chain Security

- (A) using administratively separate build environments;
- (B) auditing trust relationships;
- (C) establishing multi-factor, risk-based authentication and conditional access
- (D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;
- (E) employing encryption for data; and
- (F) monitoring operations and alerts and responding to attempted and actual cyber incidents;
- (ii) providing artifacts that demonstrate conformance to subsection (e)(i)
- (iii) employing automated tools/processes to maintain trusted source code supply chains
- (iv) employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them.
- (v) providing artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv)
- (vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components tools, and services present in software development processes through audits
- (vii) providing a purchaser a Software Bill of Materials (SBOM)
- (viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;
- (ix) attesting to conformity with secure software development practices; and
- (x) ensuring and attesting to the integrity and provenance of open source software used within any portion of a product.

People - Process – Technology - Policy

Artifacts from Secure SW Development

- Identified and accountable SW Security Lead
- Two-person review before commits
- Attribution down to developer
- Documented Policy & Process
- Security assessment of build environment
- Security Assessment of 3d party code
- Use of approved base images
- Approved code library
- Use of antimalware solution in build environment
- Use of encryption within build environment
- Use & follow vulnerability management standard
- Security & visibility
- Secure logging standards
- Build environment/production environment segmentation
- Source code management system
- SBOM

SLSA Security Levels



1

Basic Protection



2

Medium Protection



3

Advanced Protection



4

Maximum Protection

Sharing Artifacts

The Trust Center

Introducing the New Trust Standard

It's more than a gut feeling.

[Read report](#)



New Trust
Standard



2021 Consumer
Privacy Survey



Cybersecurity
Awareness

[Key Topics](#)

[Featured Content](#)

[Innovation](#)

[For Sellers](#)

[Resources](#)

[Trust Portal](#)

[Protecting the Cisco Enterprise](#)

[Security Ad](#)

<https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/>

<https://www.cisco.com/c/en/us/about/trust-center.html>

The Trust Center /

Trust Portal

Access to security, data privacy, and compliance content.

[Getting Started](#)

[Download](#) | [Share](#) | [Add to my collection](#) | [View my collection](#)

Search

Filters

[Clear filter](#)

☐ Trust Packages

Document Type

Search by document type

☐ BCP/DR

☐ C5

☐ CAIQ

☐ CSA STAR

[Show 23 More](#)

Solution Category

Select from the list to 'Download', 'Share', or 'Add to my collection'

1-25 of 397 results

Document	Document type
☐ AppDynamics CAIQ	CAIQ
☐ AppDynamics Disaster Recovery Plan	BCP/DR
☐ AppDynamics GDPR FAQ	FAQ
☐ AppDynamics GovAPM FedRAMP	FedRAMP
☐ AppDynamics SIG	SIG
☐ AppDynamics SOC 2	SOC
☐ AppDynamics SaaS Products Privacy Data Sheet	Privacy Data Sheet
☐ AppDynamics Security Compliance (6)	-
TRUST PACKAGE - Use this content to address security and privacy compliance questions regarding AppDynamics.	
☐ AppDynamics Security and Privacy Standard - Security Brief	Security Brief
☐ Assessment Checklist for Financial Institutions in the EU - Cisco Webex Meetings and Teams	EBA Risk Assessment

Example: Trust Package

Duo Security Compliance

Use this content to address security and privacy compliance questions regarding Duo.

Trust Package last update: Sep 24, 2021

☐ Select full Trust Package

Document	Document type
☐ Duo CAIQ  New	CAIQ
☐ Duo ISMS Statement of Applicability – ISO 27001 	ISO
☐ Duo Letter of Attestation 	Penetration Test
☐ Duo Letter of Work Performed 	Penetration Test
☐ Duo Privacy Data Sheet Updated	Privacy Data Sheet
☐ Duo Security Brief	Security Brief
☐ Duo Security Business Continuity and Disaster Recovery Plan BCP/DR  Updated	BCP/DR
☐ Duo Security C5 Report  New	C5
☐ Duo Security ISO 27001:2013	ISO
☐ Duo Security SOC 2 	SOC
☐ Duo Security SOC 3 Report	SOC

Generic Security Vision for “Guided Experiences”

Suggestion:
Add Tiles to Trust
Portal Homepage
to initiate “Guided
Experiences”



The screenshot shows the Cisco Trust Portal homepage. At the top is the Cisco logo and navigation links: Products, Support & Learn, Partners, and Events & Videos. The main header area is dark blue with the text "The Trust Center /" and "Trust Portal" in large white font. Below this is a sub-header "Access to security, data privacy, and compliance content." and a "Getting started" button. A red box highlights three blue tiles with white text: "Conduct Supplier Security Assessment", "Conduct Product/Offer Security Due Diligence", and "Partners with Customer Security Questions". Below the tiles is a search bar and a list of documents. The list includes "AppDynamics CAIQ", "AppDynamics Disaster Recovery Plan", "AppDynamics GDPR FAQ", and "AppDynamics GovAPM FedRAMP". The "AppDynamics GovAPM FedRAMP" item has a "New" tag.

Products Support & Learn Partners Events & Videos

The Trust Center /

Trust Portal

Access to security, data privacy, and compliance content.

Getting started

Conduct Supplier Security Assessment

Conduct Product/Offer Security Due Diligence

Partners with Customer Security Questions

Download Share Add to my collection View my collection

Select from the list to 'Download,' 'Share,' or 'Add to my collection.'

1-25 of 361 results

Document	Document type
☐ AppDynamics CAIQ	CAIQ
☐ AppDynamics Disaster Recovery Plan	BCP/DR
☐ AppDynamics GDPR FAQ	FAQ
☐ AppDynamics GovAPM FedRAMP	FedRAMP

Vision for SW Security “Guided Experiences”

Suggestion:
Add Tiles to Trust
Portal Homepage
to initiate “Guided
Experiences” for
SW Security



The screenshot shows the Cisco Trust Portal homepage. At the top is the Cisco logo and navigation links: Products, Support & Learn, Partners, and Events & Videos. The main header area is dark blue with the text "The Trust Center /" and "Trust Portal" in large white font. Below "Trust Portal" is the subtitle "Access to security, data privacy, and compliance content." and a "Getting started" button. A red box highlights three blue tiles in the middle section:

- Conduct Supplier SW Security Assessment
- SW Security Process, Policy & Controls
- SW Security Evidence (logs, records, data)

Below the tiles is a search bar with a magnifying glass icon. To the right of the search bar are links: Download, Share, Add to my collection, and View my collection. Below these links is a table of results:

Document	Document type
☐ AppDynamics CAIQ	CAIQ
☐ AppDynamics Disaster Recovery Plan	BCP/DR
☐ AppDynamics GDPR FAQ	FAQ
☐ AppDynamics GovAPM FedRAMP	FedRAMP

At the bottom left of the screenshot is a sidebar with a search bar and filters. The filters section includes "Select Solution Category" and "Select Product & Services" dropdown menus.