SSDF Attestation Form Guide and Evidence

# Purpose

Anchore Inc. provides this document as the evidence attachment for the [CISA Secure Software Development Attestation Form](https://www.cisa.gov/secure-software-attestation-form). The guide assumes Anchore Enterprise is used in the organization’s environment and is configured to scan the software in scope for the SSDF Attestation Form.

The [SSDF Attestation Form](https://www.cisa.gov/sites/default/files/2024-04/Self_Attestation_Common_Form_FINAL_508c.pdf) consists of three sections that must be completed. Sections I and II should be filled with organization-specific details. This documentation provides guidance and evidence specifically for Section III of the SSDF Attestation Form.

This document uses the official SSDF Attestation Form as the base template. Its intent is to help organizations complete Section III of the SSDF Attestation Form and easily transfer the information for final submission.

# Instructions

Texts highlighted in **YELLOW** should be updated with organizational-specific details.

*Before submitting this form, please replace all contents highlighted in* ***YELLOW*** *with your organization details.*

Texts highlighted in **GREEN** are Anchore’s advisory and comments for individual sections.

*Be sure to remove all contents highlighted in* ***GREEN*** *before submitting this form.*

The placeholder image shown below should be replaced with a screenshot of the evidence you are using as support for applicable responses:



Once this document is complete, please export the file in PDF format and attach it to the end of your official SSDF Attestation Form submission.

Once signed, this document in its entirety can be submitted to CISA.

*To submit the SSDF Attestation Form to CISA, an account must be created on the* [*Repository for Software Attestations and Artifacts (RSAA)*](https://softwaresecurity.cisa.gov/login?callbackUrl=https%3A%2F%2Fsoftwaresecurity.cisa.gov%2Fsoftware) *website.*

*If your organization is not listed in the “Software Producer” dropdown, you should email* [*central@cisa.dhs.gov*](mailto:central@cisa.dhs.gov) *requesting an addition. Please be advised this process will take a few days. You should plan on at least a week before the form can be submitted. Once an account exists, the SSDF Attestation Form can be submitted without any CISA intervention.*

Anchore also offers research information related to the SSDF attestation:

1. SSDF Attestation 101: A practical guide for Software Producers - [Download eBook](https://get.anchore.com/ssdf-attestation-101-ebook/)
2. Using the Common Form for SSDF Attestation: What Software Producers Need to Know - [Read Blog](https://anchore.com/blog/an-overview-ssdf-attestation-form/)
3. Automate NIST compliance and SSDF attestation with Anchore Enterprise - [Learn more](https://anchore.com/nist-compliance-and-ssdf-attestation/)

If you want to contact one of our experts, [please contact us](https://get.anchore.com/contact/).

***Remove everything above this line after this document has been completed and is ready for final submission***

**ORGANIZATION’s Evidence Attachments for Section III of SSDF Attestation Form**

# **SECTION 3.1**

The software is developed and built in secure environments. Those environments are secured by the following actions, at a minimum:

Section 3.1 covers controls specific to your environment. Anchore Enterprise does not directly impact this section. We are including guidance to help in collecting this evidence for your organization. If you have any questions or concerns, the [SSDF Attestation Form](https://www.cisa.gov/sites/default/files/2024-04/Self_Attestation_Common_Form_FINAL_508c.pdf) contains references to NIST 800-218 controls that can be consulted for more detailed information.

The following sections will include examples to guide responding to each requirement. These should be adjusted according to your environment.

## a) Separating and protecting each environment involved in developing and building software;

**(Example Response) Endpoint protection is deployed on all developer workstations.**



Evidence of security protection software should be included here. This could include screenshots of the system or a report from the system. Be sure to retract any sensitive details that could be included in the images and change this statement to cover whatever controls are in place for safeguarding developer environments (for example, if remote desktop environments are used to secure developers, that should be explained in place of the endpoint protection statement).

**(Example Response) The source code is stored in SCM.**



Evidence of a separate source code management system should be included here. Showing any protections enabled (for example, main branch protection or DCO checks) in the SCM are helpful details.

**(Example Response) All builds and testing are done via BUILD SYSTEM.**



Evidence of a separate build system should be included here. If code signing or other artifact attestation methods are in place, they should be specifically noted with specific examples here.

## b) Regularly logging, monitoring, and auditing trust relationships used for authorization and access: i) to any software development and build environments; and ii) among components within each environment;

**(Example Response) Both SCM and BUILD SYSTEM capture audit logs, which are reviewed as needed.**



Example log entries should be included here. If logs are stored in a centralized location, that should be noted here with evidence included. Be sure to redact any sensitive log details.

## c) Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk;

**(Example Response) ORGANIZATION enforces MFA via SSO.**



Include evidence that MFA is enabled for the organization. This could include screenshots of an administrative interface such as Okta or OneLogin. Any services that have MFA also enabled should include screenshots as evidence.

## d) Taking consistent and reasonable steps to document, as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;

**(Example Response) SCM and BUILD SYSTEM are the only environments used for the development and building of software for release and testing.**



This answer will need to be tailored to your environment. Whatever applications are used to develop your software should be noted here. The above sections should contain evidence that these services are configured and secured properly. Documentation examples such as descriptions and diagrams would be helpful.

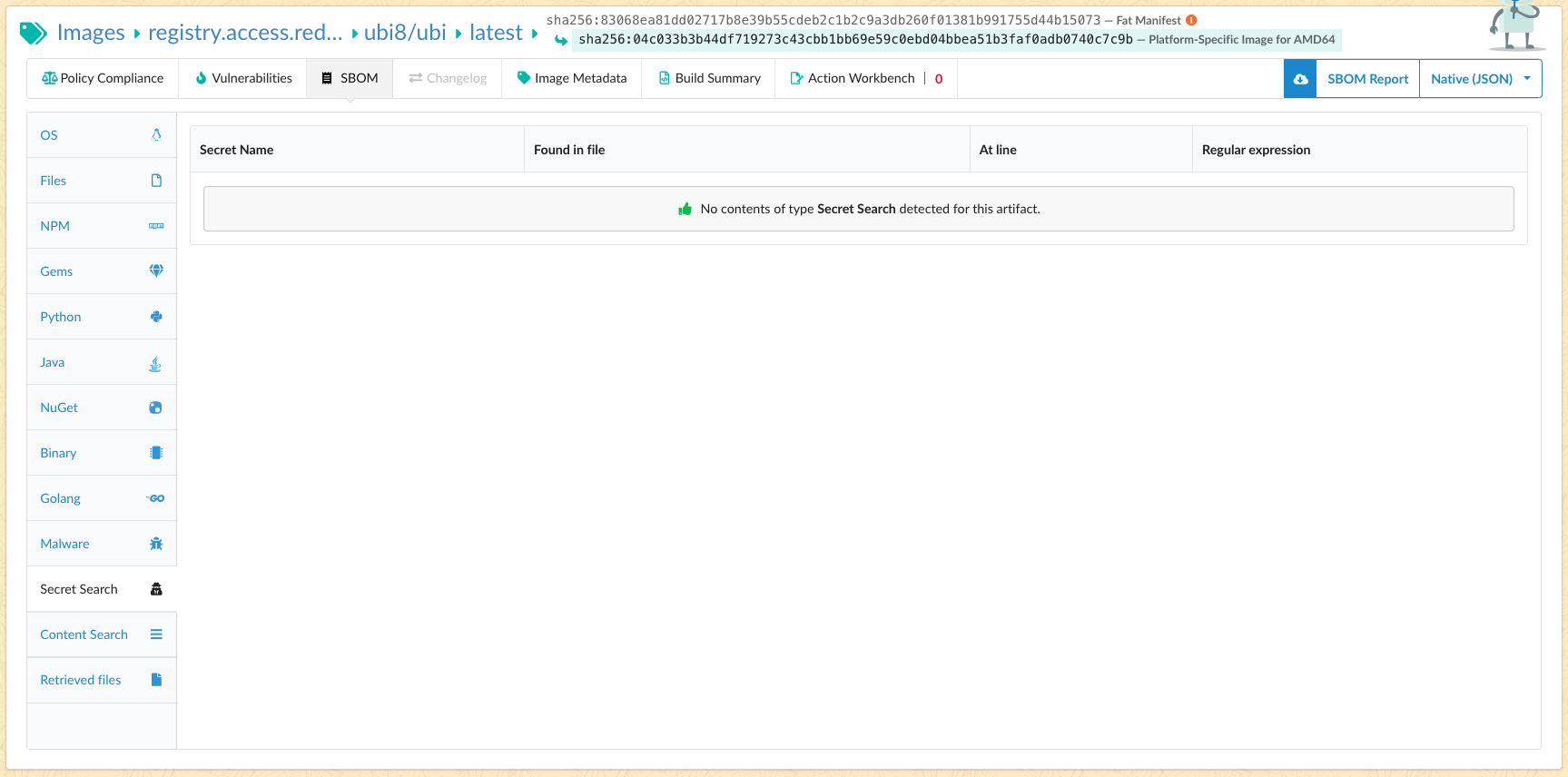
## e) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk;

**(Example Response) The CI and SCM systems store all credentials in a way that cannot be extracted.**



Include screenshots that provide evidence that secrets are stored in a way that users cannot extract them. This could be part of the SCM build system or an external vault system. Be sure no important secret information is included in the screenshots.

**(Response) The product is scanned for secrets via Anchore Enterprise before release or deployment.**



Ensure Anchore Enterprise's secret scan feature is configured for your environment. Details on this configuration can be found [here](https://docs.anchore.com/current/docs/compliance_management/policy_overview_ctl/policy_checks/#gate-secret_scans).

## f) Implementing defensive cybersecurity practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents;

**(Example Response) Systems are monitored using MONITORING SYSTEMS.**



Evidence of monitoring systems should be included here. This should include any deployed logging systems such as Elasticsearch or Splunk. Proof of any alerts configured in build systems, SCM, endpoint protection, etc., should also be included here.

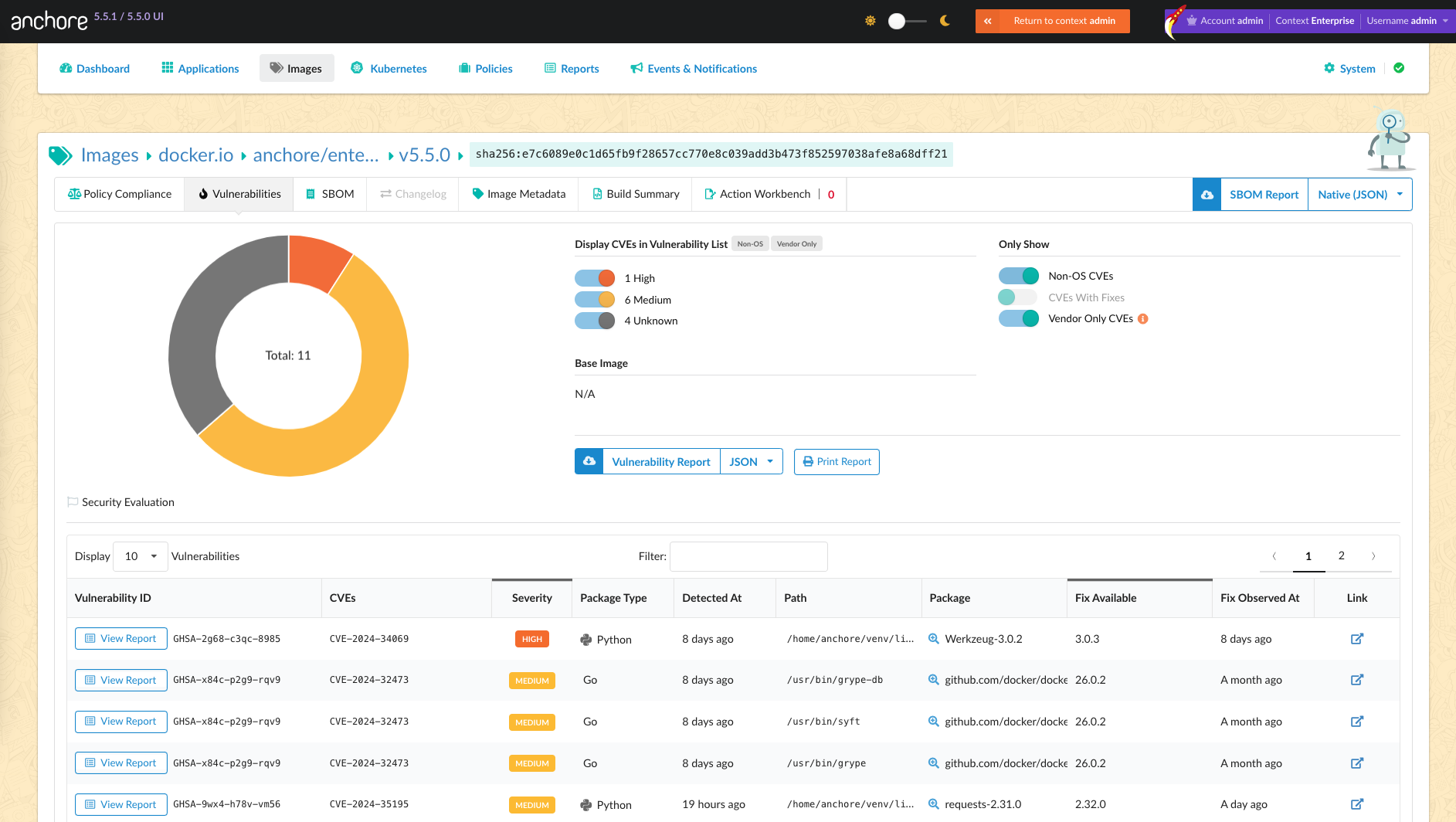
# **SECTION 3.2**

## The software producer makes a good-faith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;

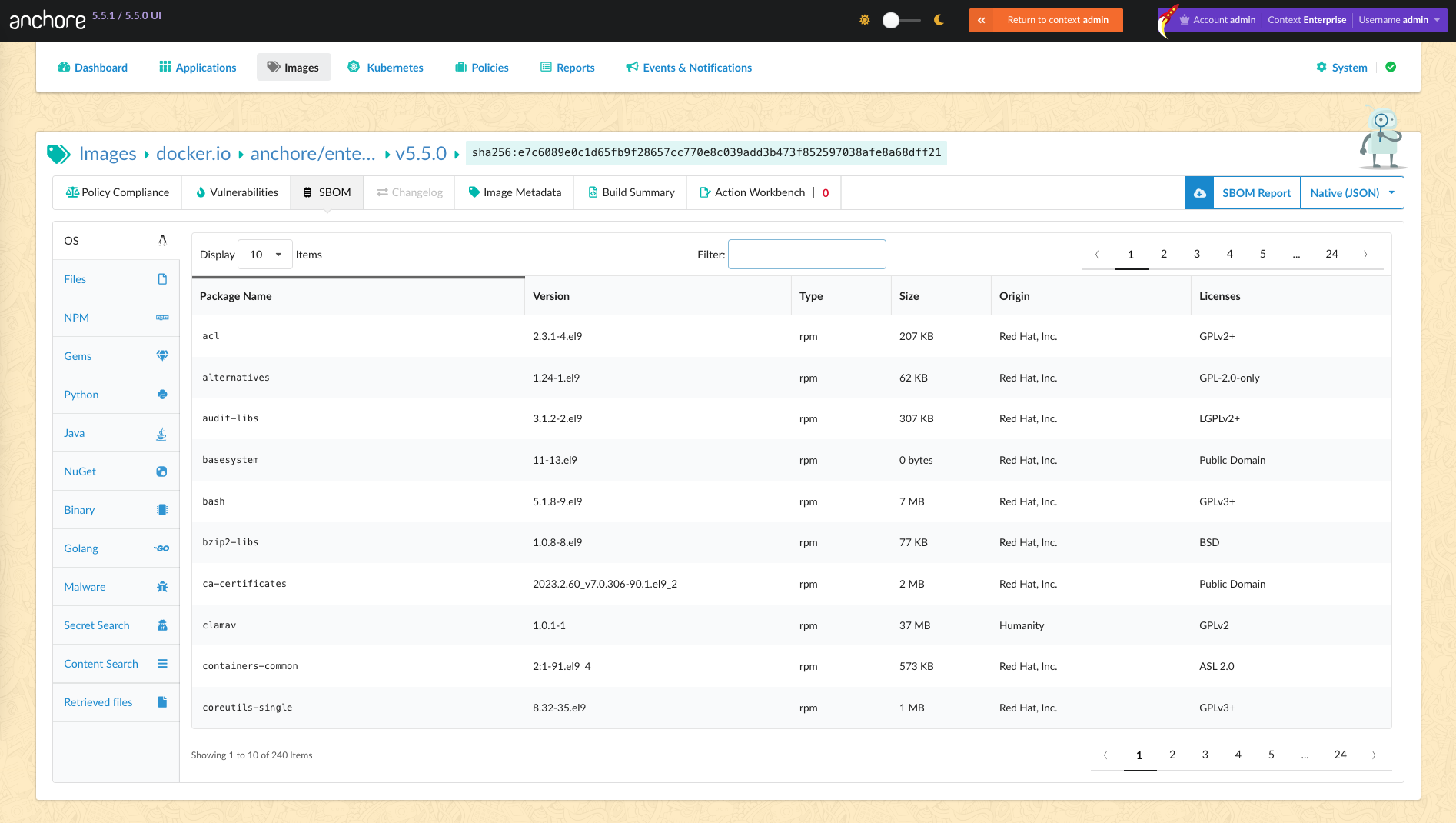
Anchore Enterprise provides the evidence needed for much of sections 3.2-3.4. The answers and screenshots below should be modified as needed but should be suitable for submission as-is for evidence. If desired, new screenshots specific to your deployment can be captured.

**(Response) Anchore Enterprise is used to scan and monitor all SOFTWARE/ORGANIZATION artifacts. The tool monitors all 3rd party components included within the system. All built versions of the SOFTWARE/ORGANIZATION artifacts are scanned automatically.**

**Anchore Enterprise vulnerability view showing vulnerabilities affecting the artifact:**



**Anchore Enterprise SBOM view listing 3rd party components:**

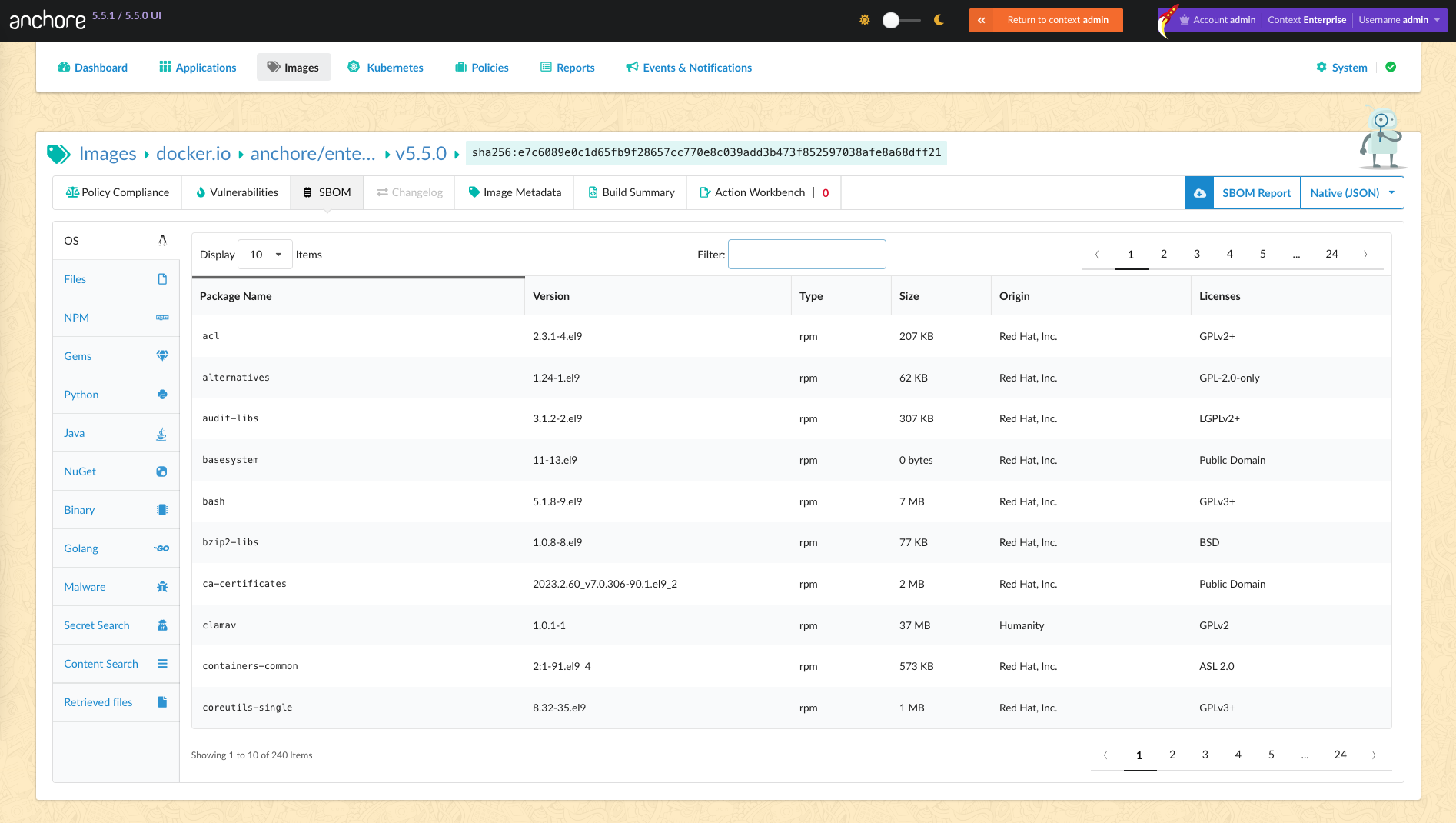


# **SECTION 3.3**

## The software producer maintains provenance for internal code and third-party components incorporated into the software to the greatest extent feasible;

**(Response) All software components are tracked via Anchore Enterprise as SBOM content, which is tied to specific digests of artifacts. All artifacts are automatically scanned, and the SBOM is immutably stored in Anchore Enterprise.**

**Anchore Enterprise SBOM view:**



**Provenance can be shown by comparing stored SBOM data of artifacts. By analyzing image digests and file checksums, the provenance can be traced back to the source of the package data.**

**Example of SBOM content containing file checksums:**



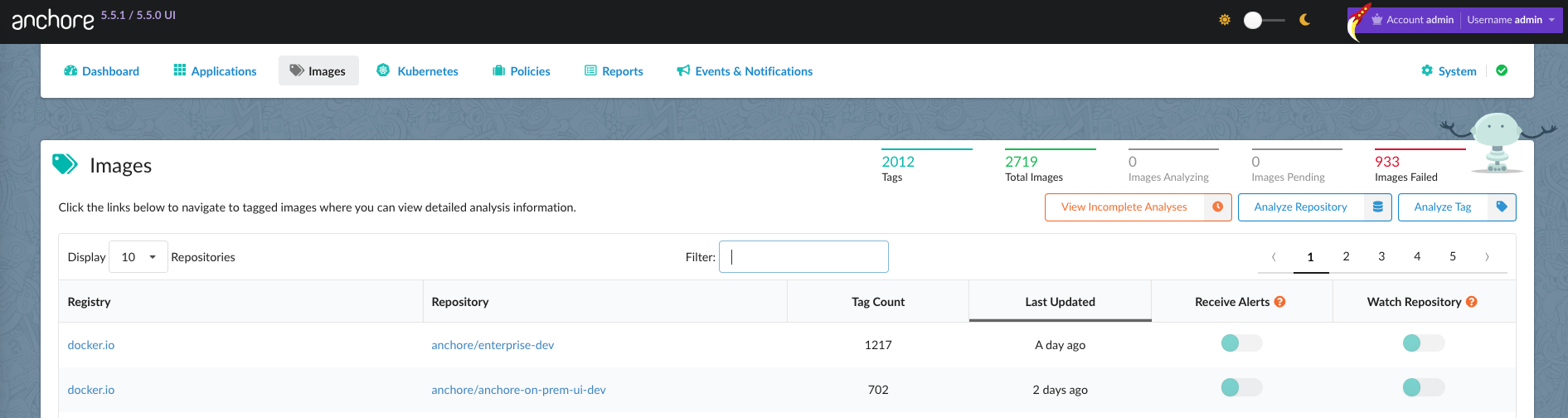
# **SECTION 3.4**

## The software producer employs automated tools or comparable processes that check for security vulnerabilities. In addition:

## a) The software producer operates these processes on an ongoing basis and prior to product, version, or update releases;

**(Response) Anchore Enterprise scans all stored SBOMs every 2 hours for policy violations and vulnerabilities. When new images are added to a registry, they are automatically detected and scanned.**

**Anchore Enterprise image view showing images with recent updates:**



## 

## b) The software producer has a policy or process to address discovered security vulnerabilities prior to product release; and

## c) The software producer operates a vulnerability disclosure program and accepts, reviews, and addresses disclosed software vulnerabilities in a timely fashion and according to and timelines specified in the vulnerability disclosure program or applicable policies.

This section will need to be tailored for your organization. The text and screenshot included are specific to Anchore but are included to serve as an example to get you started. The included text also covers sections 3.4b and 3.4c. If your evidence does not cover both sections, adjust as needed.

**(Example Response) Anchore has a vulnerability handling process documented in the secure development policy:**

