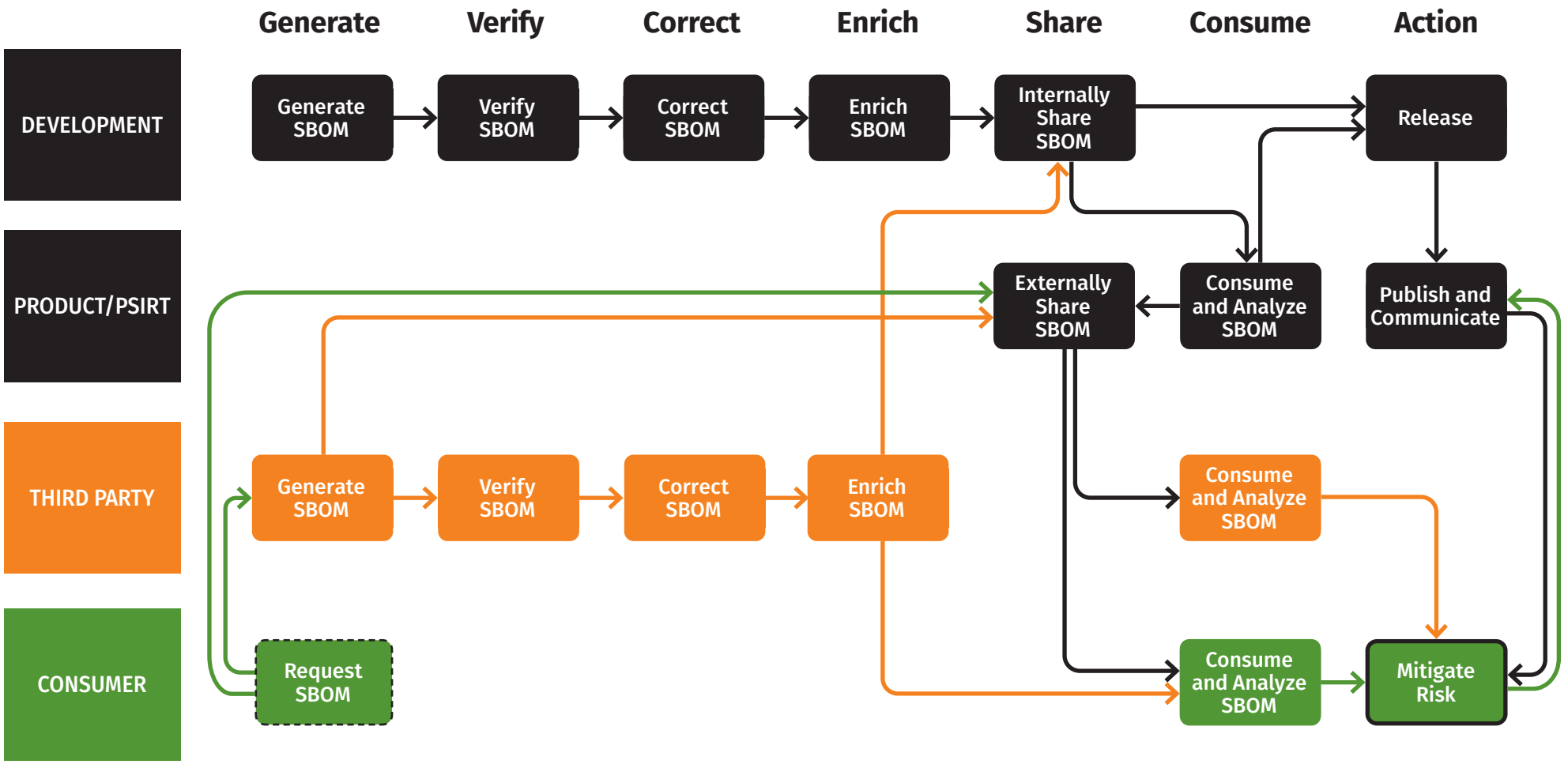
SBOM Maturity and Process Flow:

Enhancing Supply Chain Security with Effective SBOM Management

SANS CYBER DEFENSE

This process flow diagram illustrates the lifecycle of a Software Bill of Materials (SBOM) through various stages and participants, including Development, Product/PSIRT, Third Party (representing SBOM consultants and tool providers), and Consumer. Each stage is aligned with key actions: Generate, Verify, Correct, Enrich, Share, Consume, and Action. In programs just getting started, Verify, Correct, and Enrich activities typically are not performed until higher maturity in the process is achieved. Here's a detailed breakdown of the process.



DEVELOPMENT

Generate SBOM

The development team generates the initial SBOM, listing all components, libraries, and dependencies. Ideally, an automated process, but when you are just getting started, this might be performed manually.

Verify SBOM *(Higher Maturity)*

At higher maturity levels, the SBOM is verified for accuracy and completeness. This involves checking for correct component versions, licensing information, dependency relationships, and conformance to data specifications and quality.

Correct SBOM *(Higher Maturity)*

Errors identified during verification, such as missing components or license information, are corrected, ensuring the SBOM accurately represents the software.

Enrich SBOM *(Higher Maturity)*

Additional information, such as security attributes or metadata, is added to enhance the SBOM's usefulness.

Internally Share SBOM

The SBOM is shared within the organization, allowing various teams to use it for security and compliance.

Consume and Analyze SBOM

The SBOM is analyzed to understand its contents and identify potential risks or dependencies that need attention.

Release

The product, along with its SBOM, is released. The SBOM is available for external parties needing it for their processes. SBOMs might be issued as part of release management or as part of other out-of-band processes, such as using SBOM data exchanges or offering via API.

Publish and Communicate

The SBOM is published and communicated to relevant stakeholders, ensuring transparency and facilitating trust in the software supply chain.

PRODUCT/PSIRT

Externally Share SBOM

The SBOM is shared externally with partners, customers, or regulatory bodies to help them understand the software's composition and security posture.

Consume and Analyze SBOM

PSIRT ensures the SBOM is suitable for external sharing so that external parties can analyze it for risks, compliance, and dependency management.

THIRD PARTY (SBOM CONSULTANTS AND TOOL PROVIDERS)

Generate or Request SBOM

Third parties, including consultants and tool providers, either generate their own SBOMs using proprietary tools and methods or request SBOMs from suppliers, ensuring a complete inventory for analysis or integration. Their role is to support suppliers, consumers, or both. Multiple third parties may be engaged. In some cases, this involves complex legal agreements such as non-disclosure agreements and licensing for SBOM data to establish shareability.

Verify SBOM *(Higher Maturity)*

Verification by third parties ensures the SBOM's accuracy, enhancing trust and reliability in the supply chain.

Correct SBOM *(Higher Maturity)*

Corrections are made if any issues are found during verification, maintaining the integrity of the SBOM data.

Enrich SBOM *(Higher Maturity)*

Enrichment adds valuable context and metadata, making the SBOM more useful for analysis and decision-making. In many instances, this enrichment is a key differentiator for the third party by introducing additional threat and vulnerability intelligence into the SBOM process.

Consume and Analyze SBOM

Third parties analyze SBOMs to provide insights, support compliance, and recommend mitigations, identifying consumer risks.

Mitigate Risk

Based on the analysis, third parties recommend actions to mitigate identified risks, enhancing the software's security and resilience. Typically, they cannot directly influence the software's security posture except to make recommendations.

CONSUMER

Request SBOM

Consumers request SBOMs from their suppliers or third-party service providers to gain visibility into the software's composition. This becomes a challenge for scaling the request and follow-ups, or "vendor chasing," similar to a vendor risk assessment process. Since contractual terms may vary, SBOM frequency, fidelity, and format rules may deviate significantly, and conformance to contractual terms becomes necessary. The use of third-party tools can reduce the burden.

Consume and Analyze SBOM

Consumers analyze the SBOMs to understand potential risks, verify compliance, and manage dependencies. Ideally, this analysis will be correlated against the install base for the software, but this does require correlation against asset inventories, something that is rarely done with current tools.

Mitigate Risk

Actions are taken to mitigate identified risks based on the SBOM analysis, ensuring software security and integrity. This mitigation tends to be bifurcated into internal and external activities. It may involve requesting security patches be created, as well as designing and implementing virtual patching strategies until a patch can be made and deployed.

KEY FLOWS

Development to Product/PSIRT

The SBOM is generated, verified, corrected, enriched, and internally shared before being externally shared and consumed. Suppliers ensure the SBOM is suitable for sharing, is shared in conformance with contractual terms, and engages stakeholders throughout the process.

Third Party Involvement

Third parties (consultants and tool providers) play a crucial role in generating, verifying, correcting, enriching, and consuming SBOMs, providing expertise and tools to support SBOM capabilities. In many cases, supplier- or consumer-centric SBOM processes can be offloaded to third parties in a hybrid managed services fashion to streamline the process.

Consumer Interaction

Based on the insights gained, consumers request, consume, and analyze SBOMs to mitigate risks. Focusing on outcomes ensures that SBOM investments yield meaningful security returns.