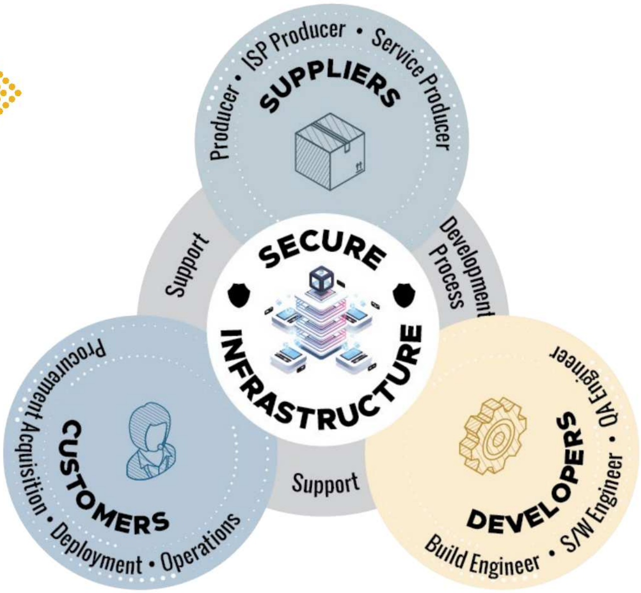
SECURING THE SOFTWARE SUPPLY CHAIN

SUPPLIERS


SUPPLIERS
Producer • ISP Producer • Service Producer
Development Process
DEVELOPERS
QA Engineer • S/W Engineer • Build Engineer
Support
CUSTOMERS
Procurement Acquisition • Deployment • Operations
Support
SECURE INFRASTRUCTURE

Software suppliers (i.e. vendors) act as a liaison between the customer and the software development team; ensuring software is developed in a secure environment and delivered via secure channels.

- The Supplier has overall organizational policy and management responsibility for secure software development. As such, the Supplier should work in close coordination with both internal software development and third party software sources.
- Supplier responsibilities from the customer's perspective include ensuring the integrity and security of software releases and updates, providing notifications of and remedies for vulnerabilities in accordance with contractual agreements.
- To ensure a more secure software supply chain, Suppliers should seek to identify threats that could compromise the organization, software development, software itself, and software delivery (i.e. on-premise or Software-as a-Service (SaaS)) environments and implement associated mitigations.
- NIST's Secure Software Development Framework (SSDF) offers foundational guidance for software producers and ensures secure development processes. Suppliers are responsible for secure delivery to the end customer.

THREATS

Potential introduction of exploitable elements (i.e. code, scripts, etc.)

- Use of potentially vulnerable software libraries
- Introduction of methods that adversaries can co-opt for exploitation
- Adversaries may inject vulnerabilities during transactions

RECOMMENDED BEST PRACTICES

- Verifiable software release process from development - emphasis on software integrity
- Secure packaging and delivery methods to customer (e.g., SBOM, cryptographic, Hashing, Code Signing, etc.)
- Methods for customer to verify releases, patches, and updates
- Secure delivery of updates and patches to customer
- Monitor emerging threats and address vulnerabilities with updates
- Provide education and training to improve secure development and delivery process
- Artifacts that articulate secure architecture