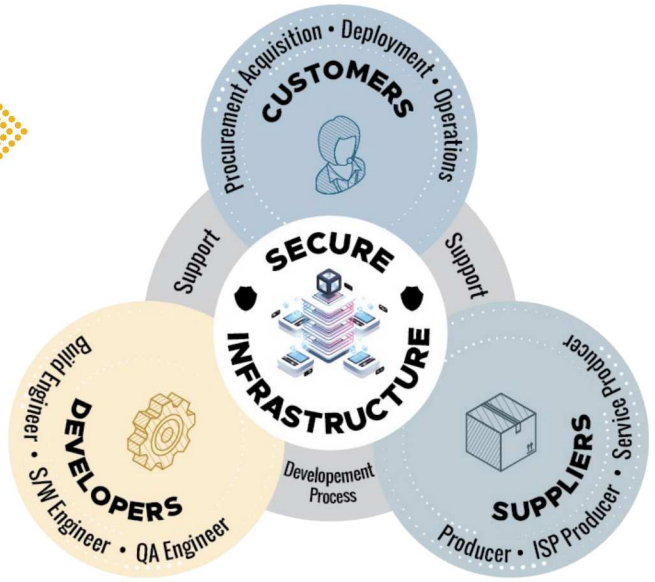
SECURING THE SOFTWARE SUPPLY CHAIN

CUSTOMERS



User Organizations (i.e. the Customer) follow a series of key phases in the acquisition, deployment, and operation of software products.

Customer teams specify to and rely on vendors for providing key artifacts (e.g. SBOM) and mechanisms to verify the software product, its security properties, and attest to the SDLC security processes and procedures.

Processes Involved in the Key Phases

- Requirements Definition
- Supply Chain Risk Management
- Product Evaluation and Selection
- Contracting Deployment/Integration
- IT Operations
- Security Operations

Post procurement, the customer evaluates the product, plans for integration and roll out, and then performs necessary functions and steps for deploying the software into the environment.

Part of the roll out process includes coordination with security operations, oversight boards, and the internal user community. Deployment processes incorporate procedures for product updates, upgrades, and End of Life (EOL) or removal. Finally, the customer implements procedures, processes, controls, and policies on the use and operations of the software product.

THREATS

- Product (or product update/upgrade)
  - Undocumented features, malicious or risky code/functionality, vulnerable code or components
  - Changes in functionality or security assumptions between evaluation and deployment
- Vendor
  - Change in ownership can impact risk assessment of product (control, geo location, ownership, security incidents)
  - Poor enterprise and/or development security hygiene

RECOMMENDED BEST PRACTICES

- Require and verify attestation (e.g. SBOM) for the product
- Perform Security, Environmental, and Functionality tests on the software product
- Check integrity mechanisms (e.g., product file hashes, config file hashes) during deployment
- Require notification from supplier
  - Changes of ownership/control, geo location, 3rd parties to software product)
  - Cyber incidents and investigations and
  - Mitigations/impacts to product or development environment of the product at time of delivery
- Require self-attestation of cybersecurity hygiene of the vendor/supplier development process and the infrastructure supporting the development of their product to inform the risk management determination by the user organization
- Continuous Security Monitoring of product as part of Security Operations