RUNSAFE LYNX PARTNERSHIP

Technology Overview

September 2022

Harden mission critical systems to operate through the most common and devasting exploits w/ RunSafe's DoD-proven, automated protection software

- Increase cyber resilience and mission assurance by reducing the attack surface 60-90%

- Employ moving-target-defense to eliminate attackers' asymmetric advantage

- Streamline cyber mitigation efforts, without changing code or schedule.

Proven via successful implementations with NAVSEA, Marine Corps Systems Command, and AF PlatformOne as well as commercial deployments (see appendix for logos)

RunSafe program success with multiple DoD weapon systems, including:

NAVSEA
- 100% of mission applications protected with no change to system functionality
- Operational Deployment (TRL 9) scheduled for 2023 based on successful program testing

Marine Corps SYSCOM
- Successful integration into tactical C2 applications
- Providing forward protection when in theater systems can't be patched
- Protecting Linux Open Source packages

AF PlatformOne
- Approved for use in PlatformOne Pipelines
- Integrated into SkiCAMP & ThunderCamp SW factories
- Flew as part of SkyBorg flight test 2021

Current practices of scanning and patching alone leave weapon systems vulnerable to the most common and most devastating cyber attacks

- Addressing scan results slows down your development teams, and doesn't address key vulnerabilities

- Zero Days, newly discovered vulnerabilities, continue despite scanning and other practices

- 15 minutes after a vulnerability disclosure, attackers are attempting exploits, far ahead of patching (if even available)

Labor intensive vulnerability mitigation is disruptive, reactive and insufficient, distracting from warfighter priorities and increasing cost to support.

RunSafe Security's Core Offerings

3 Ways to Fill the Software Security Gap

ALKEMIST CODE

- RunSafe immunization technology inserts protections at build time and so your software is secure at runtime.
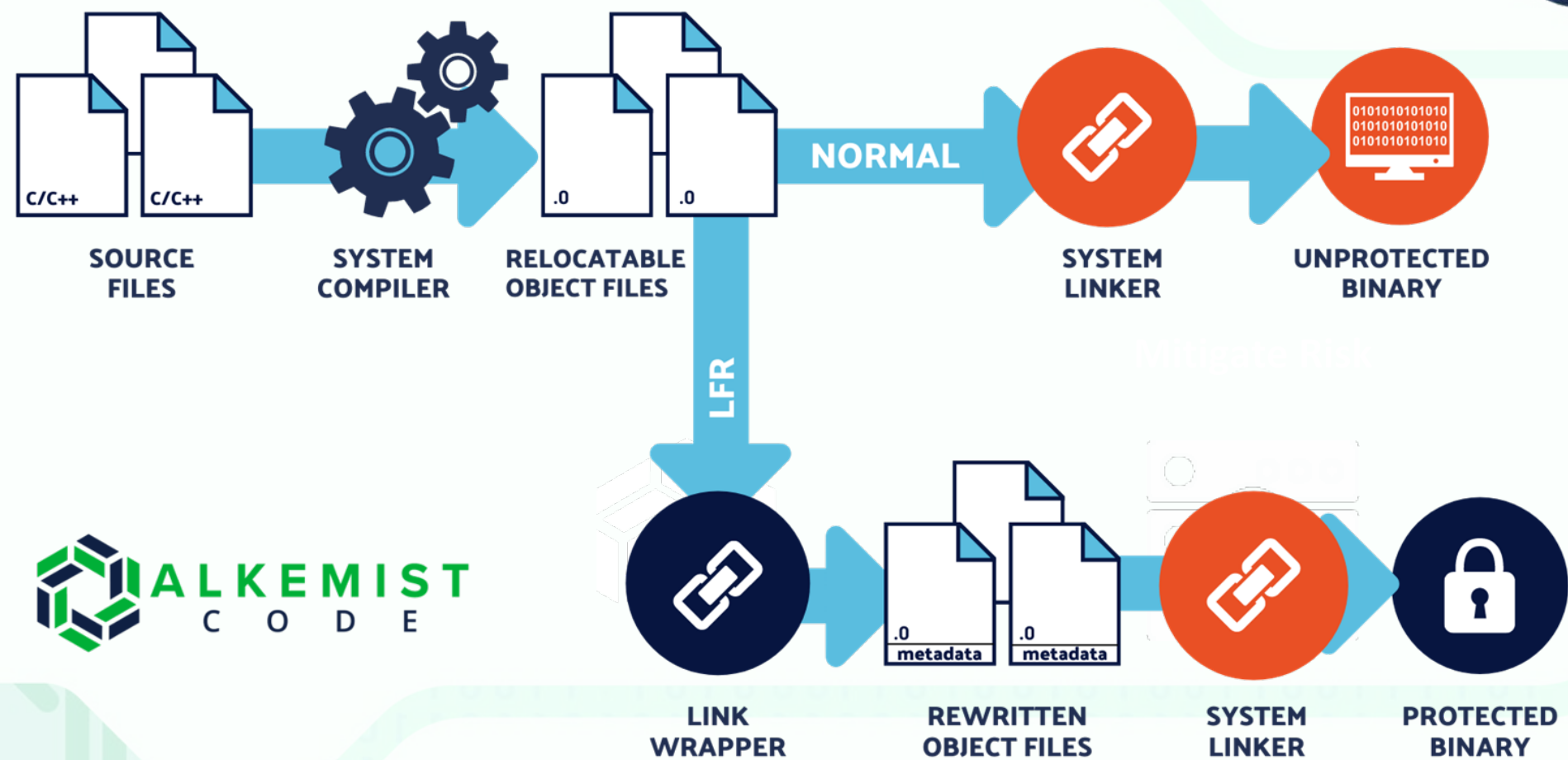
ALKEMIST REPO

- RunSafe automated hardening of open-source packages, components, and libraries in your software supply chain.

ALKEMIST FLARE

- RunSafe Monitoring to capture software crashes enhancing code quality and identify vulns other tools & methods miss.

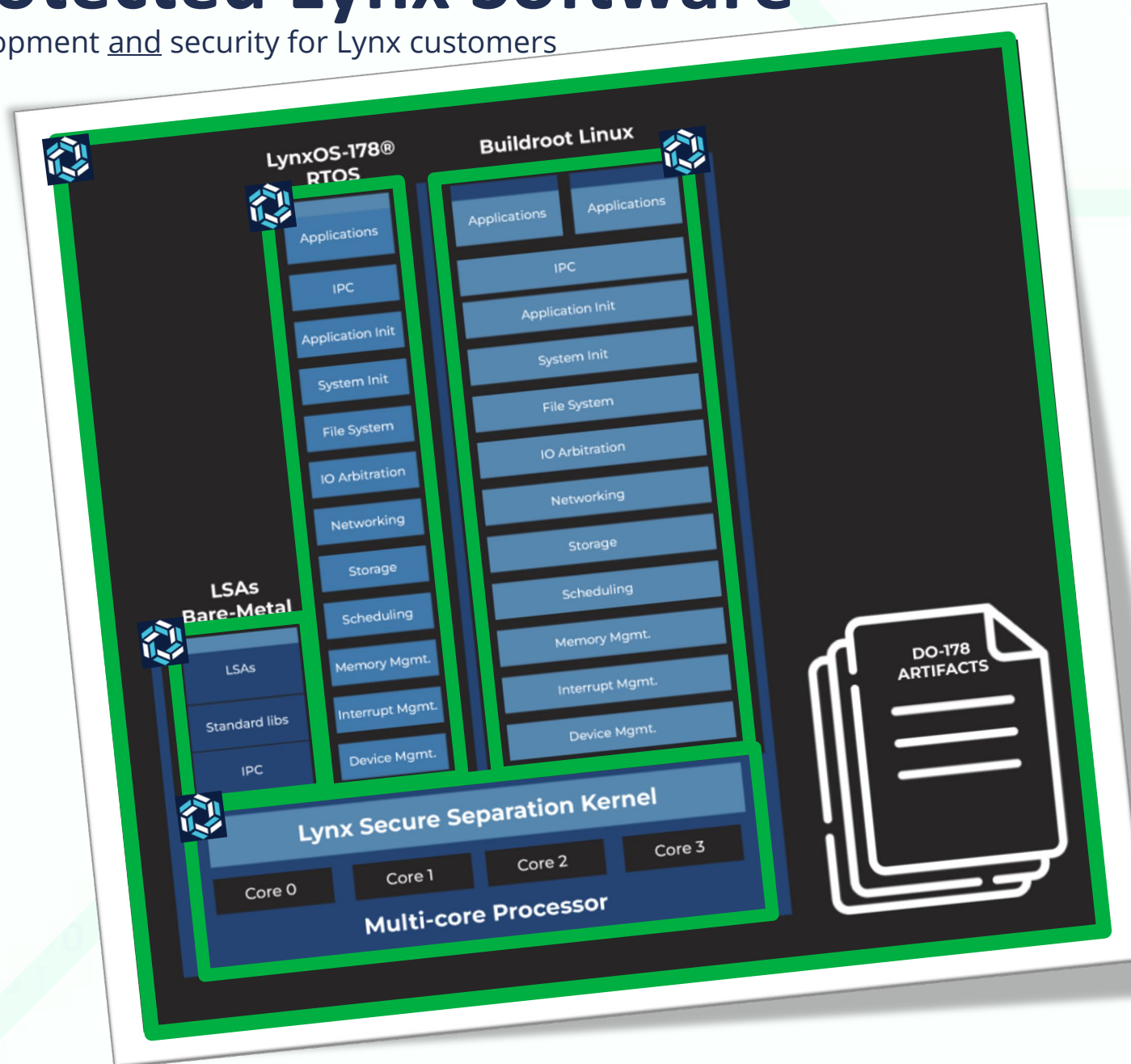# Alkemist:Code Implementation Flow

RunSafe Protected Lynx Software

Change economics of development <u>and</u> security for Lynx customers

Protect
- LynxOS-178
- LynxSecure
- LynxElement
- Buildroot Linux

Reduce security cost and time risk for Lynx customers