“Zero Wing” by Tapolan & Williams Electronics, 1991

“Zero Wing” by Tapolan & Williams Electronics, 1991

Eddie Knight, Sonatype

CRob, Linux Foundation

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The year was 2000…

- The topic was well known
- A rallying call was made
- The community responded in force

Animation
Bad_CRC

CATS : ALL YOUR BASE ARE BELONG TO US.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

FINOS
Fintech
Open Source
Foundation

CLOUD NATIVE
COMPUTING FOUNDATION

OpenJS
Foundation

The year was 2024...

- The topic was well known
- A rallying call was made
- The community responded in force

Open Source Project Security Baseline

GRC Engineering Model for Automated Risk Assessments

Gemara

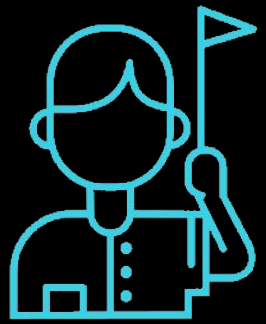
Effective Cybersecurity Guidance

- Topically Broad
- Widely Recognized
- Outcome Oriented

Effective Cybersecurity Controls

- Threat Informed
- Technology Specific
- Machine Readable

Open Source Project Security Baseline



Guidance

Controls

Gemara Layer 2 Adopter

OSPS-BR-06 - Produce all released software assets with signatures and hashes

All released software assets MUST be signed or accounted for in a signed manifest including each asset's cryptographic hashes.

OSPS-BR-06.01

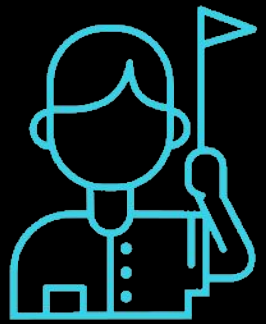
Requirement: When an official release is created, that release MUST be signed or accounted for in a signed manifest including each asset's cryptographic hashes.

Recommendation: Sign all released software assets at build time with a cryptographic signature or attestations, such as GPG or PGP signature, Sigstore signatures, SLSA provenance, or SLSA VSAs. Include the cryptographic hashes of each asset in a signed manifest or metadata file.

- Maturity Level 2
- Maturity Level 3

External Framework Mappings

- SSDF: PO5.2, PS2.1, PW6.2



Guidance

FINOS COMMON CLOUD CONTROLS

Gemara Layer 2 Adopter

Controls

CCC.TH05 - Data is Corrupted During Replication

Data may become corrupted, delayed, or deleted during replication processes across regions or availability zones due to misconfigurations or unintended disruptions. This could lead to compromised data integrity and availability, potentially affecting recovery processes and system reliability.

Impacted Capabilities:

Source	Capability
CCC	CCC.F08
CCC	CCC.F12
CCC	CCC.F21

Related Mappings:

Source	Mapping
MITRE-ATT&CK	T1485
MITRE-ATT&CK	T1565
MITRE-ATT&CK	T1491
MITRE-ATT&CK	T1490

CCC.TH06 - Data is Lost or Corrupted

Data loss or corruption may occur due to accidental deletion, or misconfiguration. This can result in the loss of critical data, service disruption, or unintended exposure of sensitive information.

Impacted Capabilities:

Source	Capability
CCC	CCC.F11
CCC	CCC.F18

Related Mappings:

Source	Mapping
MITRE-ATT&CK	T1485
MITRE-ATT&CK	T1565
MITRE-ATT&CK	T1491

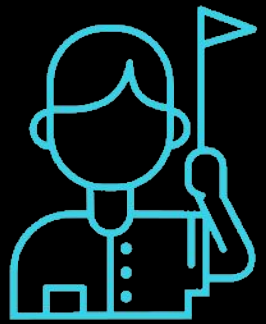
FINOS
COMMON
CLOUD
CONTROLS

Effective Cybersecurity Policies

- Specific to Business Units
- Informed by Business Risk Profiles
- Isolated to Services or Architectures
- Mapped to Control Catalogs

GRC Engineering Model for Automated Risk Assessments

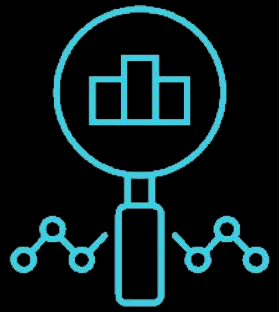
Gemara



Guidance

LFX

Gemara Layer 4 Adopter



Evaluation

LFX

LFX Insights | Search projects, repositories... ⌘+K | Collections | Open Source Index | Documentation

Argo / argo-cd | Share

Overview | Contributors | Popularity | Development | Security & Best Practices

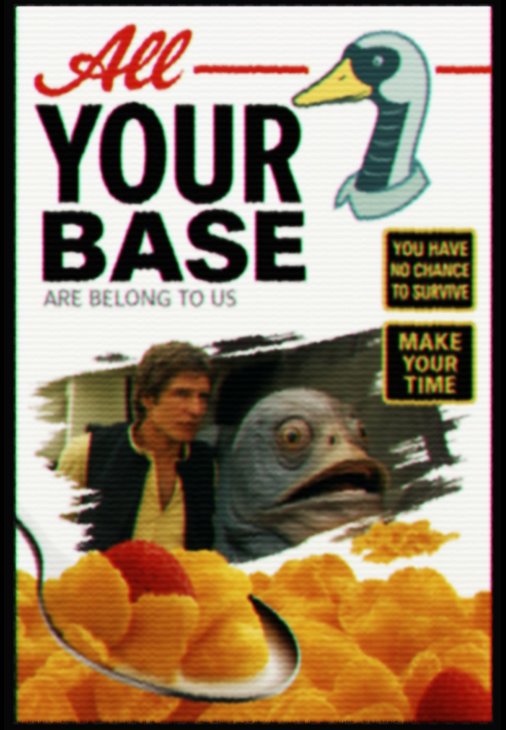
Governance 100%

Governance defines policies and processes to guide decisions and community actions, ensuring readiness for risks and growth.

Legal 100%

Legal ensures code is under a valid open source license, reducing IP risks and ensuring proper licensing and distribution.

Requirement ID: OSPS-LE-02.01 Needs review	While active, the license for the source code MUST meet the OSI Open Source Definition or the FSF Free Software Definition.
Requirement ID: OSPS-LE-03.01 Passed	While active, the license for the source code MUST be maintained in the corresponding repository's LICENSE file, COPYING file, or LICENSE/ directory.
Requirement ID: OSPS-LE-03.02 Passed	While active, the license for the released software assets MUST be included in the released source code, or in a LICENSE file, COPYING file, or LICENSE/ directory alongside the corresponding release assets.



Security Insights

- Enables Baseline & Related Assertions from Projects
- Ingested by Evaluators to determine facts about a project

Security Assessments

- Closes project-specific gaps that automation can't reliably cover
- Equips maintainers and stewards to design more secure software

Eddie Knight, Sonatype

CRob, Linux Foundation

OpenSSF
OPEN SOURCE SECURITY FOUNDATION