CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

As America's Cyber Defense Agency and the National Coordinator for Critical Infrastructure Security and Resilience, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

SECURE BY DEMAND

Agenda

- Secure by demand
- Why Now
- Key Definitions
- Core Principles
- Lifecycle Overview
- Lifecycle in Practice
- Top 10 Secure by Default Controls
- Next Session Questions
- Discussion & Q&A

Secure By Demand

Explanation: Combines two major approaches: Secure by Design & Default.

Goal: Bake in security so it's ready when demanded, not added later.

Objectives:

- Define Secure by Design, Default, Demand
- Explore lifecycle practices
- Learn top secure defaults
- Discuss adoption and governance

Why Now

- Breaches = Costly + Reputational damage
- Security debt compounds like financial debt
- Customers & Regulators expect strong security

Key Definitions

- **Secure By Design - Build security into architecture**
- **Secure By Default – Safe out of the box settings**
- **Secure by Demand- organizational ability to deliver secure outcomes rapidly**

Core Principles

Minimize attack surface: fewer doors open

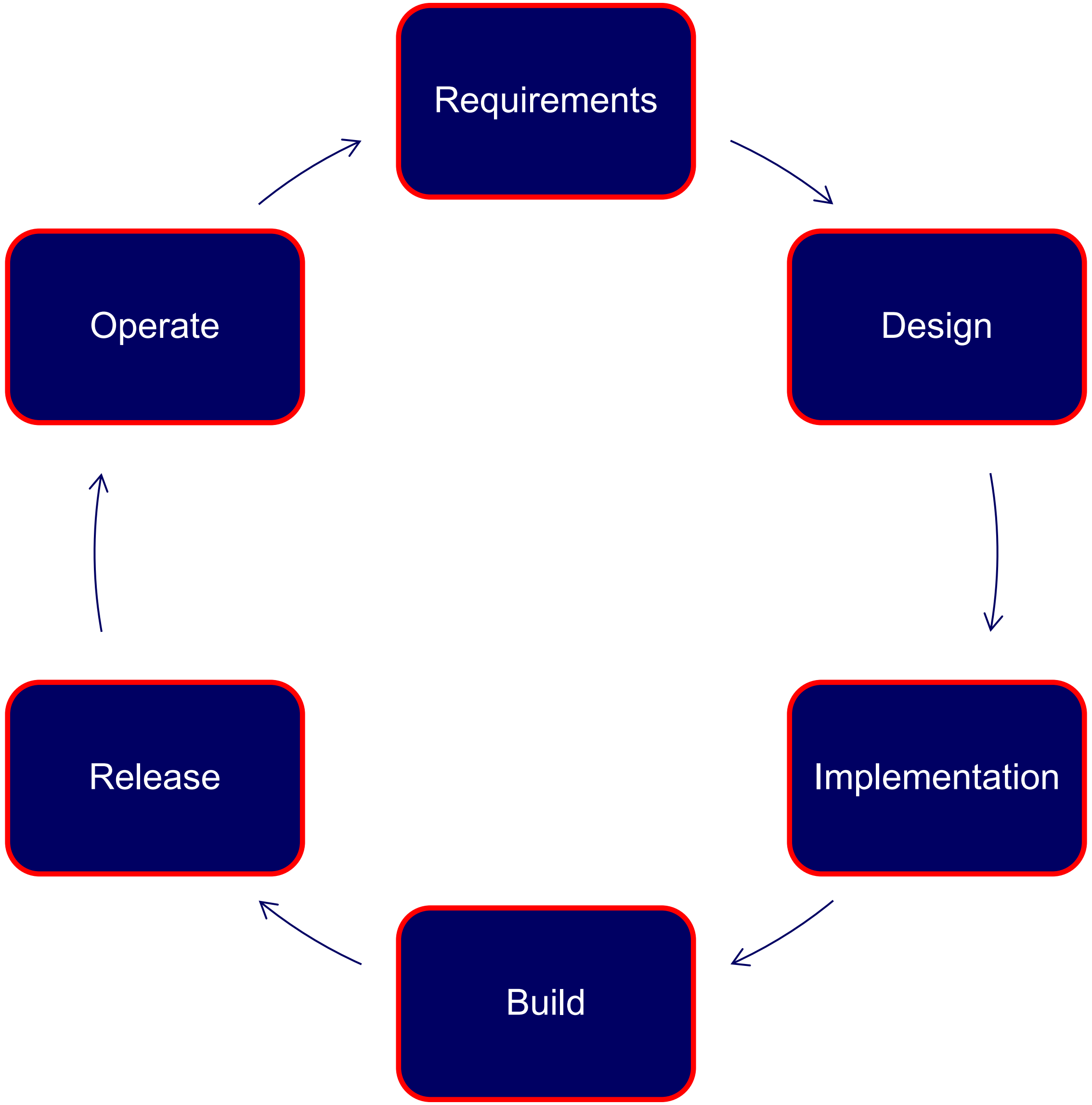
Assume compromise: design systems so that if breached, the damage is contained

Least privilege access: access need nothing more

Verified supply chain: trust but verify, know where your stuff come from

Observability & Recovery: always monitor and practice recovery so you can bounce back quickly

Lifecycle Overview



Lifecycle in Practice

Requirement: Security Stories and Abuse Cases

Design: Threat Modeling

Implementation: Safe Libraries, no hardcodes secrets

Build: software bill of materials (SBOM), artifact signing

Release: Ensuring safe delivery

Operate: Constant Monitoring and preparation for incident

Top 10 Secure by Default Controls

Multifactor Authentication: Makes stolen passwords difficult to use

Least Privilege: Reduces risk if accounts are compromised

Secure Transport Layer Security: Modern encryption standards protect data

Automatic Updates: prevent attackers from exploiting known bugs

Logging: Detects issues

Secrets Management: No passwords in the code

Sandboxing: isolates risky inputs

Dependency Allow list: prevents untrusted code from entering

Rate-Limits: stops abuse or brute force attacks

Customer Defaults: privacy and security turned on by default

For The Next Session

Non-Technical

1. How is leadership incentivizing adoption of secure by default practices across teams?
2. What training or awareness programs exist to help nontechnical staff understand secure by demand principles?
3. How do we communicate the value of secure by default to customers and stakeholders?
4. What governance or oversight structures ensure accountability for insecure defaults?
5. How do we balance user experience with stronger security defaults while maintaining customer trust?

Technical

1. How are we validating the integrity of build artifacts through cryptographic signing?
2. Do our pipelines enforce automated security scanning before deployments?
3. What mechanisms ensure secrets management across environments?
4. How are software bill of materials generated, maintained, and integrated into release processes?
5. What runtime protections are active and monitored?

For more information:
www.cisa.gov

Questions?

Email: William.Hicks@mail.cisa.dhs.gov
Phone: 202-809-4179
giovanni.williams@cisa.dhs.gov
Phone:202-503-5614

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Visit **CISA.gov** to learn more and see our mission in action at **cisa.gov/about/2023YIR**
or contact us at **central@cisa.dhs.gov**