2023

ISAUnited Defensible Architecture (IDA) Methodology

A Threat-based Approach to Designing Security Architecture

ISAUnited
International Security Architects

Defensible Architecture

Methodology Outline
ISAUnited Defensible Architecture

Introduction

Our commitment to security architecture has resulted in ISAUnited supporting dedicated teams of security architects focused on advancing architectural security posture. We designed this teachable approach to deliver a security architecture foundation for organizations to institute a proper security architecture methodology to address business requirements and solve problems.

ISAUnited has developed this approach into a complete architectural methodology and process framework. With great pride, we're excited to introduce this to a wider audience as the ISAUnited Defensible Architecture methodology. We know that organizations see value in a structured approach to security architecture, which is why ISAUnited developed the Defensible Architecture methodology.

This methodology allows any enterprise security team to develop a secure architecture using a formulated, accountable, and comprehensive process and to help security practitioners explain, develop, mature their security posture, and align with security best practices. Through our process, architects can accurately capture and record business requirements and convert these into tangible security solutions.

ISAUnited Security-by-Design Phased Approach Methodology

1. Pre-Design Phase

- Intake - Read the problem statement document.
- Intake - Read the proposed solution document.
- Intake - Business requirements document

2. Discovery Phase

- Complete the SARS document (IDA-Template-01):
    - Intake - Diagrams, DFD's, and workflows
    - Intake - Components and systems
    - Intake - Data classifications
    - Intake - Integrations, APIs, and technologies

3. Design Development Phase

- *Concept Design*
    - Develop the HLA Design Security Report consisting of (IDA-Template-02):
        - Create HLA design drawings or workflows or flow charts or DFDs.
        - Develop the baseline security controls (IDA-Template-03)
        - Write and complete the HLA Design security analysis.
    - Deliver the above HLA Design analysis.

- *Technical Design*
    - Develop the DLA Design Security Report consisting of (IDA-Template-04):
        - Develop the threat and vulnerability analysis report that consists of (IDA-Template-05):
            - Identify Threats
            - Discover Vulnerabilities
            - Create Threat map.
        - DLA design drawings or workflows or flow charts or DFDs
        - Curate the technical security controls (IDA-Template-06)
        - After DLA Design is finalized, write the DLA Design security report.
    - Deliver the above DLA Design report.

4. Post-Design Phase

- Handoff to Engineering and Operations
- Continuous security architecture oversight during implementation
- Continuous security analysis oversight during implementation
- Deliver the Security Standard artifact (IDA-Template-07)
- Close out the project.