ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Defensible 10 Standards

The creation model behind the ten domains

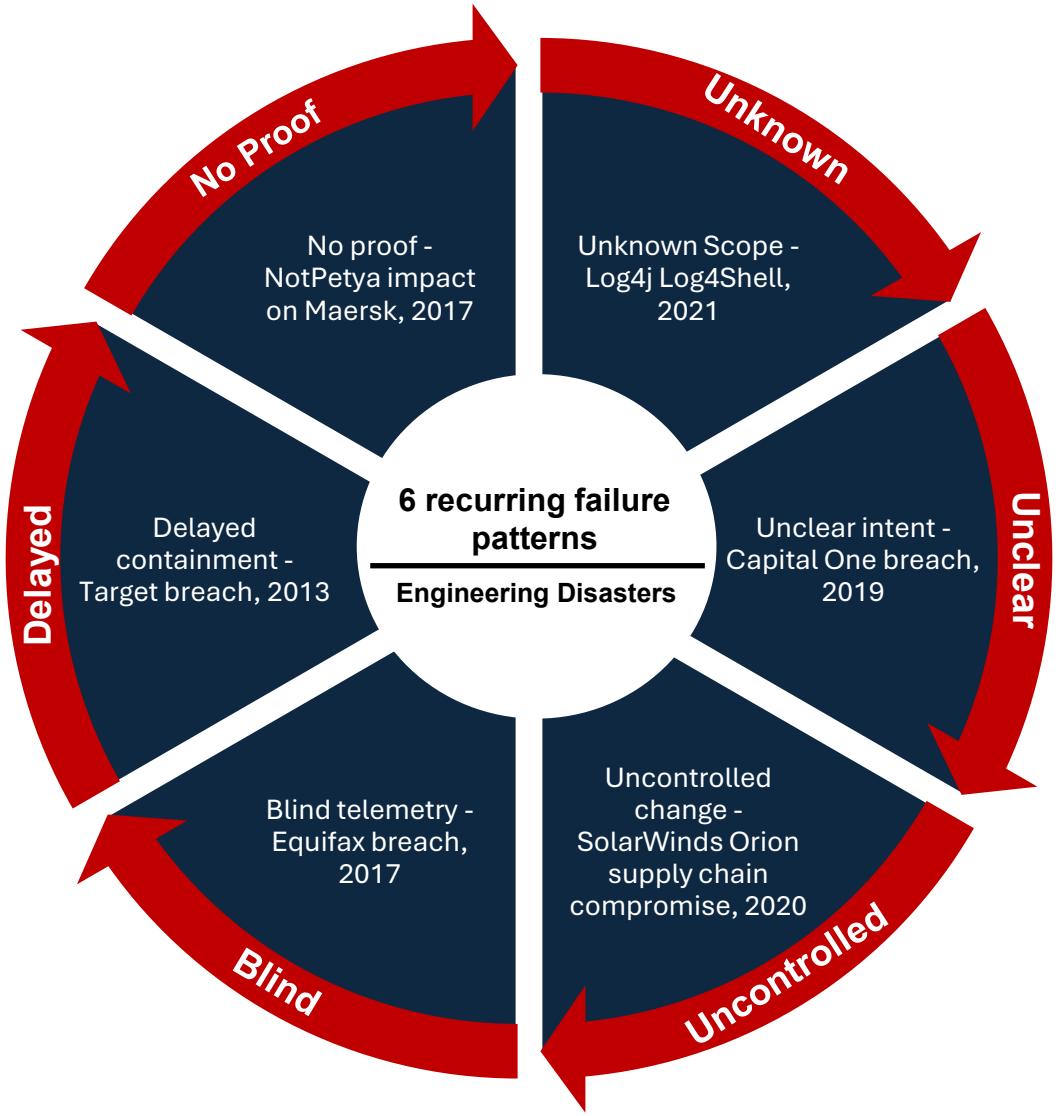
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Table of Contents

ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Six Failure Patterns

Across industries and architectures, major incidents repeat the same engineering failures:
Unknown scope. Unclear intent. Uncontrolled change. Blind telemetry. Delayed containment. No proof.



ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Unknown Scope

Incident: Log4j Log4Shell, 2021

Red lesson: Many organizations struggled to identify where the vulnerable component existed across their environments and dependencies, delaying containment and patching decisions.

Blue message: Define exists because you cannot protect what you cannot enumerate and bound.

ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Unclear Intent

Incident: Capital One breach, 2019

Red lesson: Regulators concluded the organization did not establish effective cloud risk assessment and did not implement appropriate design and implementation of key security controls in the cloud operating environment.

Blue message: Design exists because security intent must be explicit in architecture decisions, not implied by tools.

ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Uncontrolled Change

Incident: SolarWinds Orion supply chain compromise, 2020

Red lesson: The intrusion leveraged a compromised software build and distribution process, pushing trojanized updates through normal deployment channels.

Blue message: Deploy exists because change paths must be controlled, verifiable, and resilient to supply chain compromise.

ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Blind Telemetry

Incident: Equifax breach, 2017

Red lesson: A key monitoring control failed because of an expired digital certificate, leaving reduced visibility into data exfiltration activity.

Blue message: Detect exists because prevention assumptions fail, and visibility must be engineered and continuously verified.

ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Delayed Containment

Incident: Target breach, 2013

Red lesson: Congressional materials describe missed opportunities to act on warnings about attacker activity and exfiltration paths, contributing to the prolonged theft of payment data.

Blue message: Defend exists because response must be practiced, time bound, and operationally executable under pressure.

ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

No Proof

Incident: NotPetya impact on Maersk, 2017

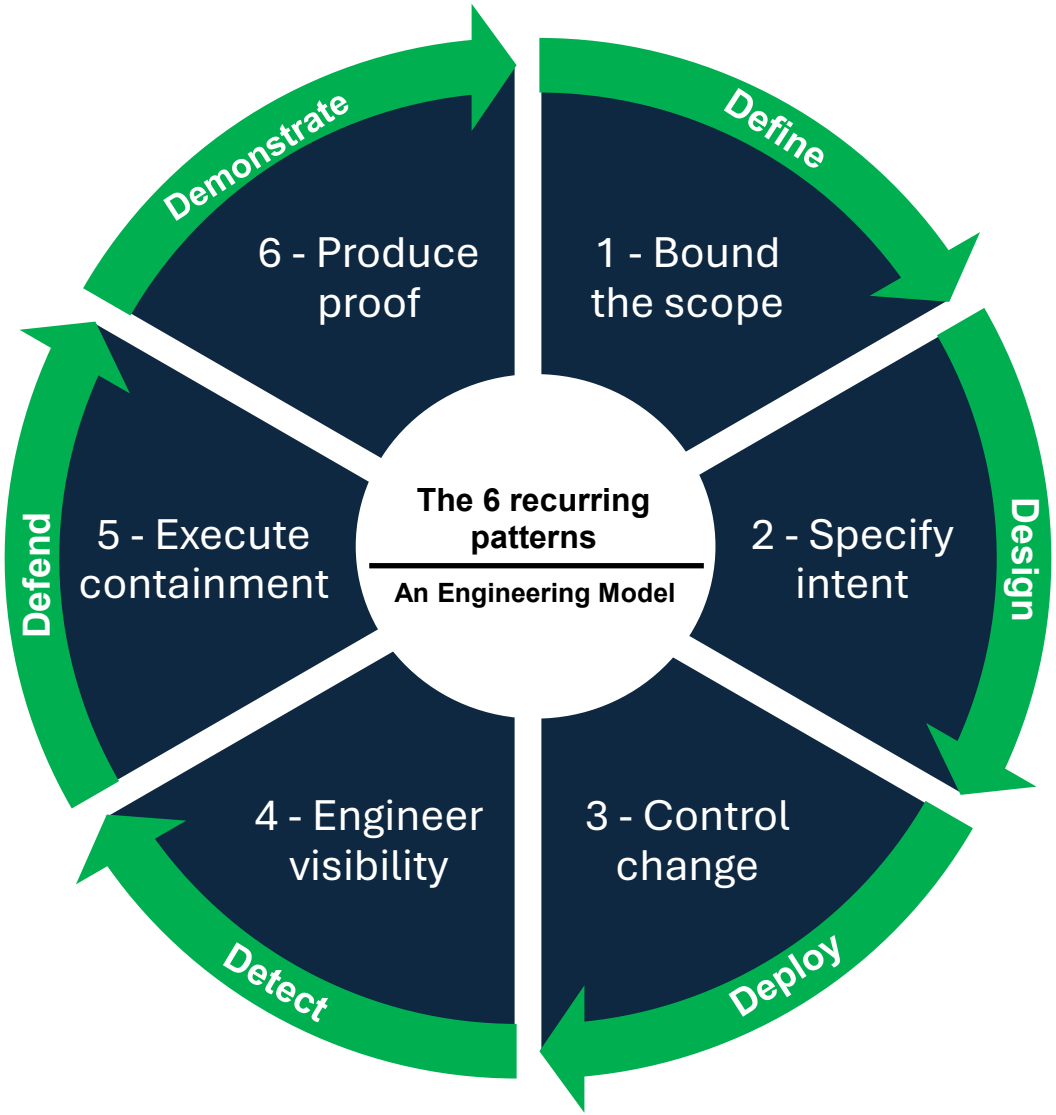
Red lesson: Recovery depended on a single surviving domain controller copy, highlighting how catastrophic recovery becomes when restoration and resilience are not demonstrably validated in advance.

Blue message: Demonstrate exists because you need proof of recoverability and control effectiveness, not confidence statements.

ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

From Failure Patterns to Defensible Engineering

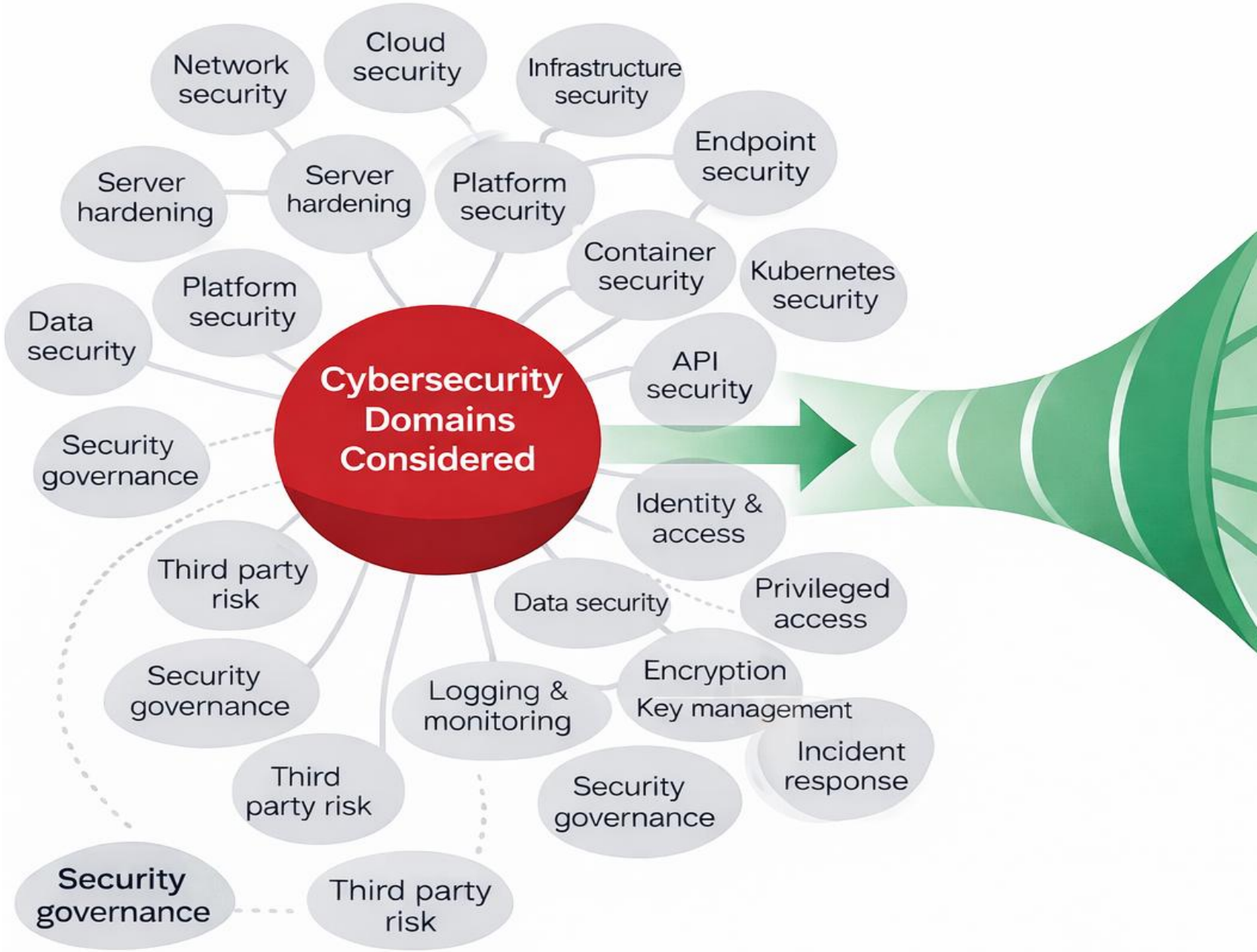
The Defensible Loop, a 6-phase engineering model that converts common incident breakdowns into disciplined security execution. The loop is designed to be repeated across any security domain and concludes with evidence that outcomes are real rather than assumed.



ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

From many cybersecurity domains to ten critical standards

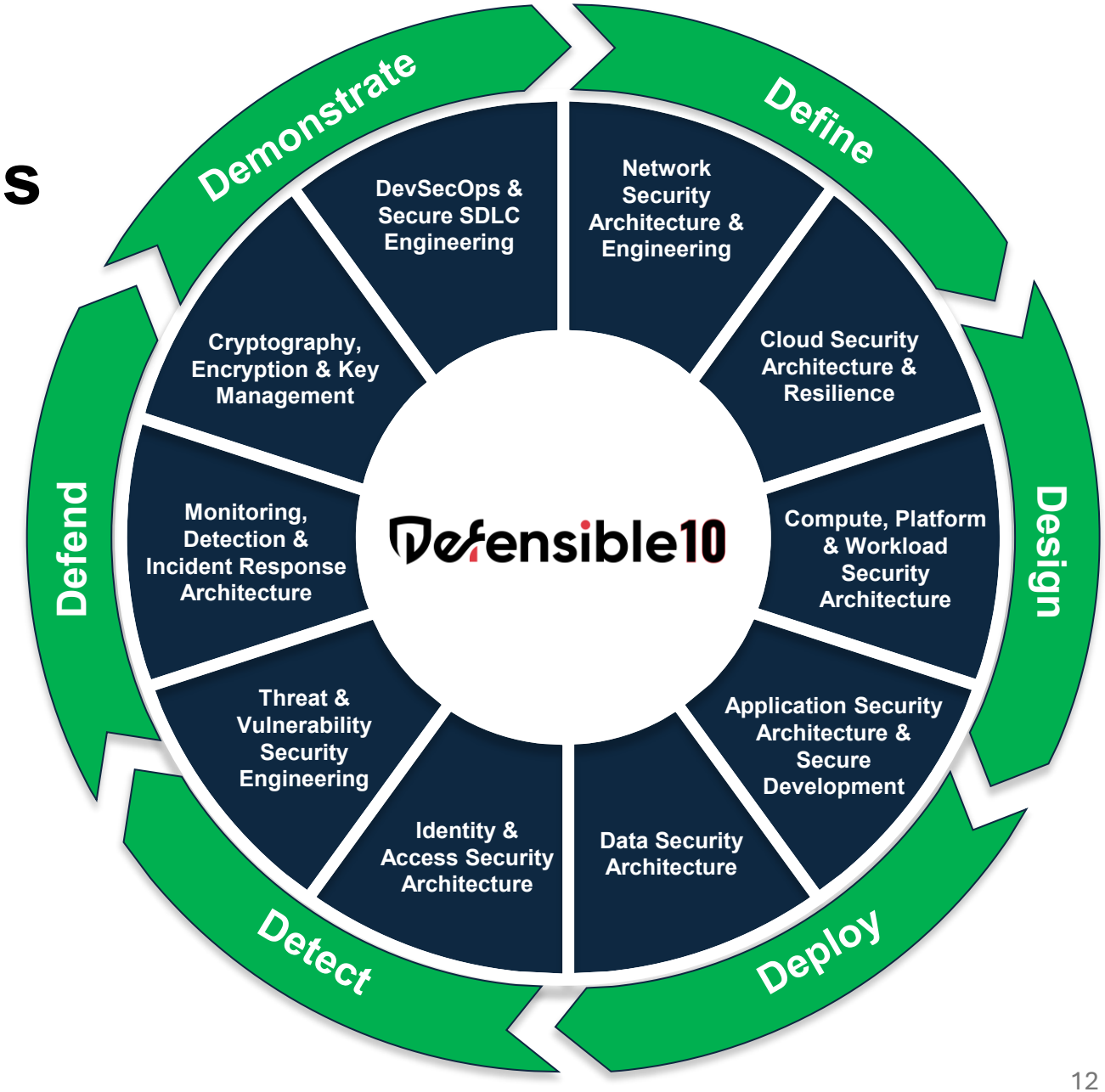
The Defensible Loop required a domain set that is complete, distinct, and measurable.



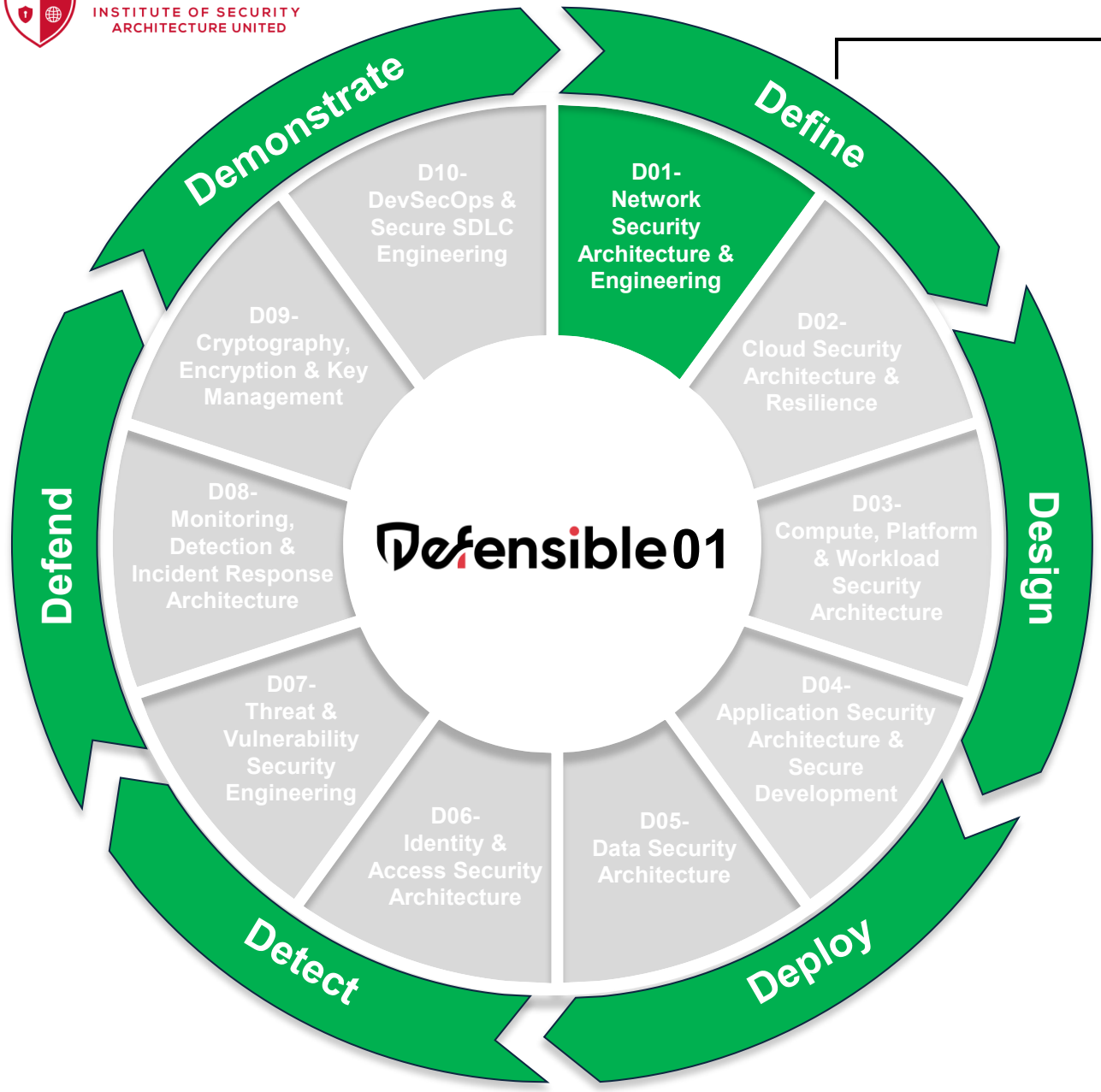
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

10 Cybersecurity Domains Driven by 1 Engineering Loop

The Defensible 10 Standards define 10 core cybersecurity domains in which architecture and engineering work must be defined, implemented, and verified. These domains were derived by consolidating overlapping cybersecurity elements into 10 critical parent domains, each with distinct control objectives and evidence requirements. Each domain standard is driven by the same Defensible Loop, ensuring repeatable execution and measurable proof.



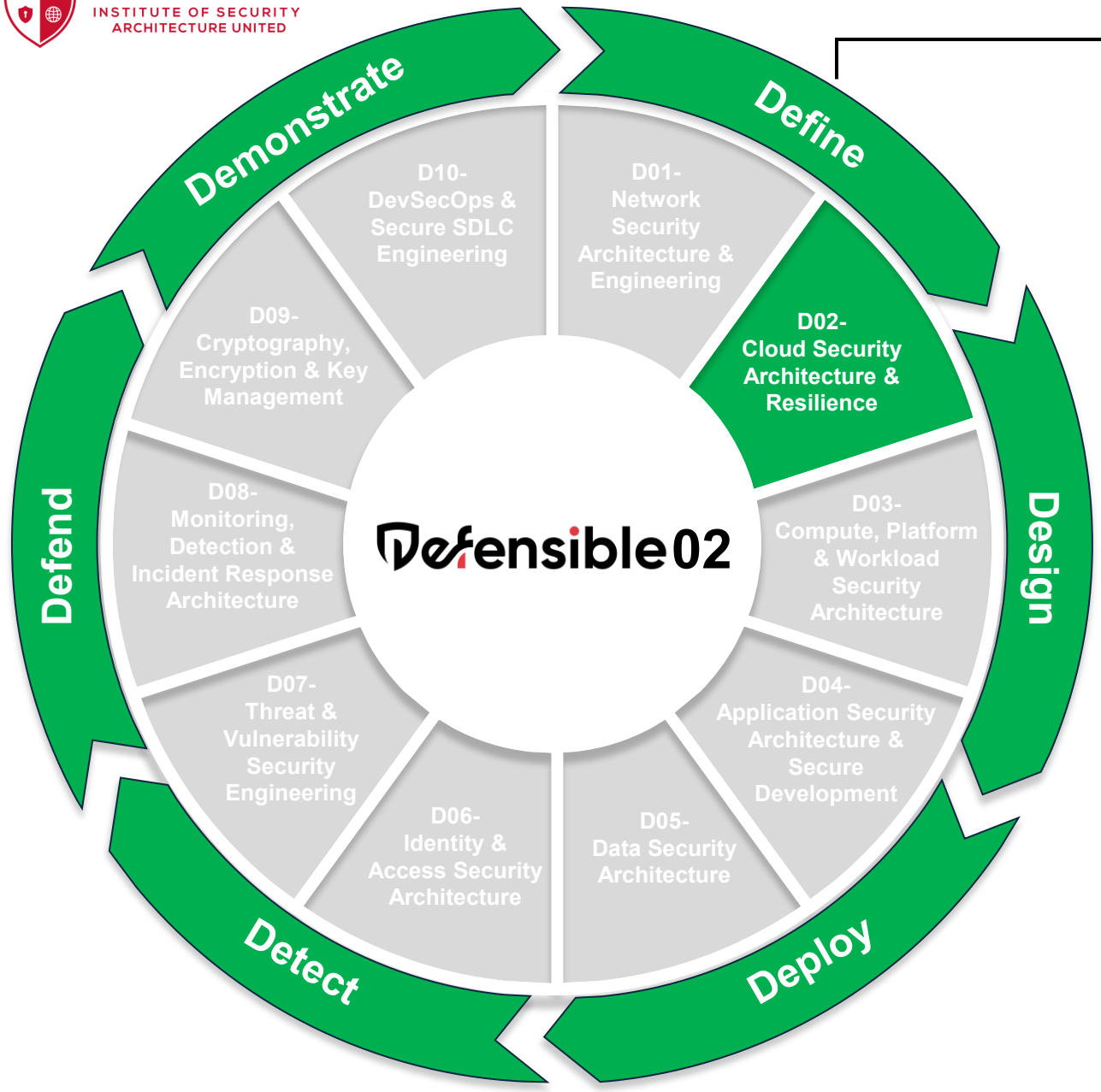
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED



D-Loop Phase	D01 - Network Security Architecture and Engineering
Define	Scope: Zones, boundaries, and traffic paths
Design	Blueprint: Segmentation and boundary policy design
Deploy	Build: Enforced network policy baseline
Detect	Signals: Flow, DNS, and boundary telemetry
Defend	Shield: Isolation and containment actions
Demonstrate	Proof: Path tests and rule validation

D01 Network Security Architecture and Engineering - defines measurable expectations for network segmentation, boundary control, secure connectivity, and resilient traffic enforcement. The Defensible Loop is applied to ensure networks are designed with clear trust boundaries, operated with engineered visibility, and validated with proof.

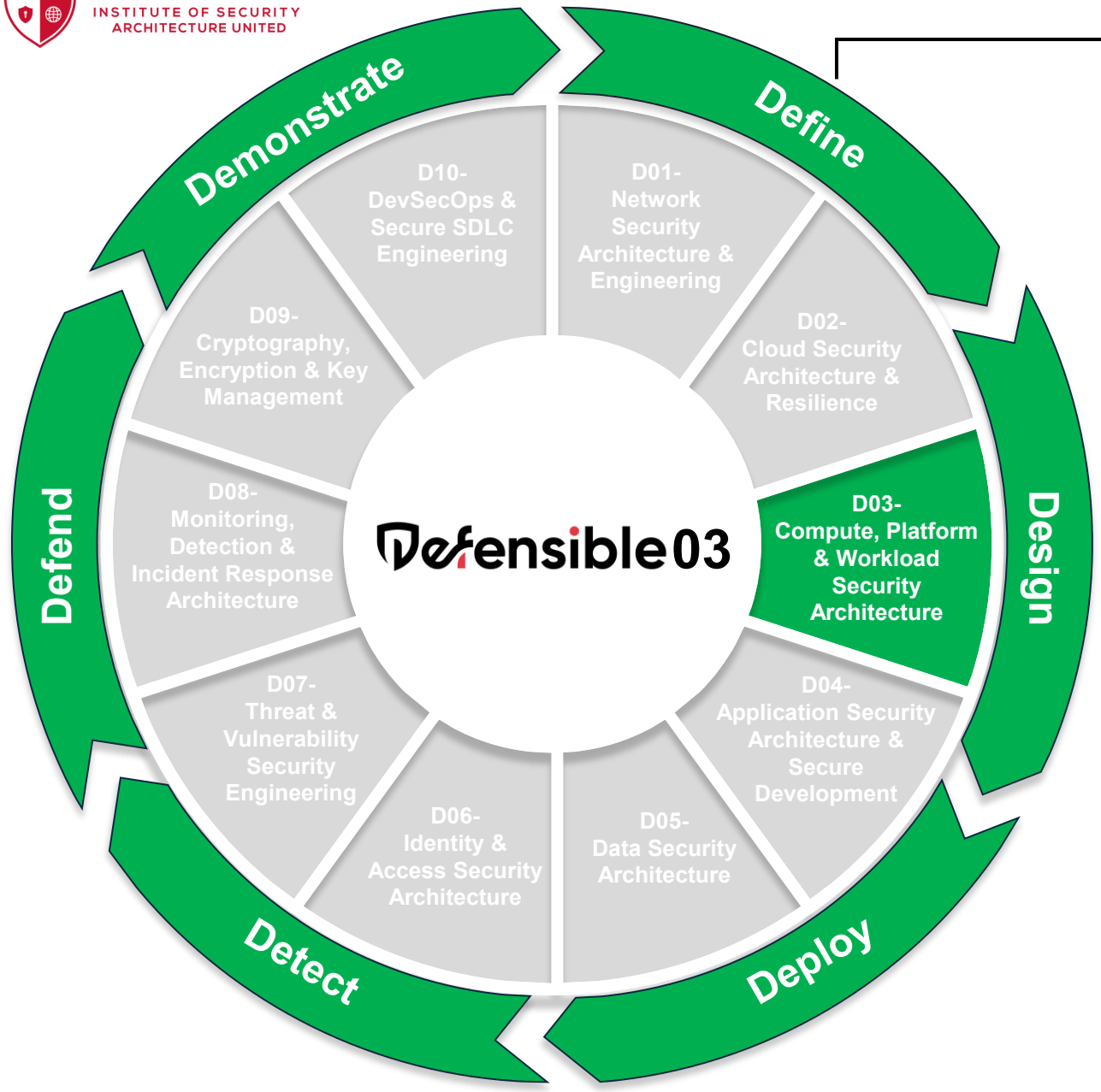
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED



D-Loop Phase	D02 - Cloud Security Architecture and Resilience
Define	Scope: Tenants, regions, and service inventory
Design	Blueprint: Landing zone guardrails and resilience intent
Deploy	Build: Automated policy and configuration baselines
Detect	Signals: Audit, drift, and identity telemetry
Defend	Shield: Guardrail blocks and recovery actions
Demonstrate	Proof: Drift evidence and recovery tests

D02 Cloud Security Architecture and Resilience - defines measurable expectations for secure cloud foundations, policy guardrails, identity and network controls, and resilience through recovery and continuity. The Defensible Loop is applied to engineer cloud security from landing zone design through validated evidence of enforcement and recoverability.

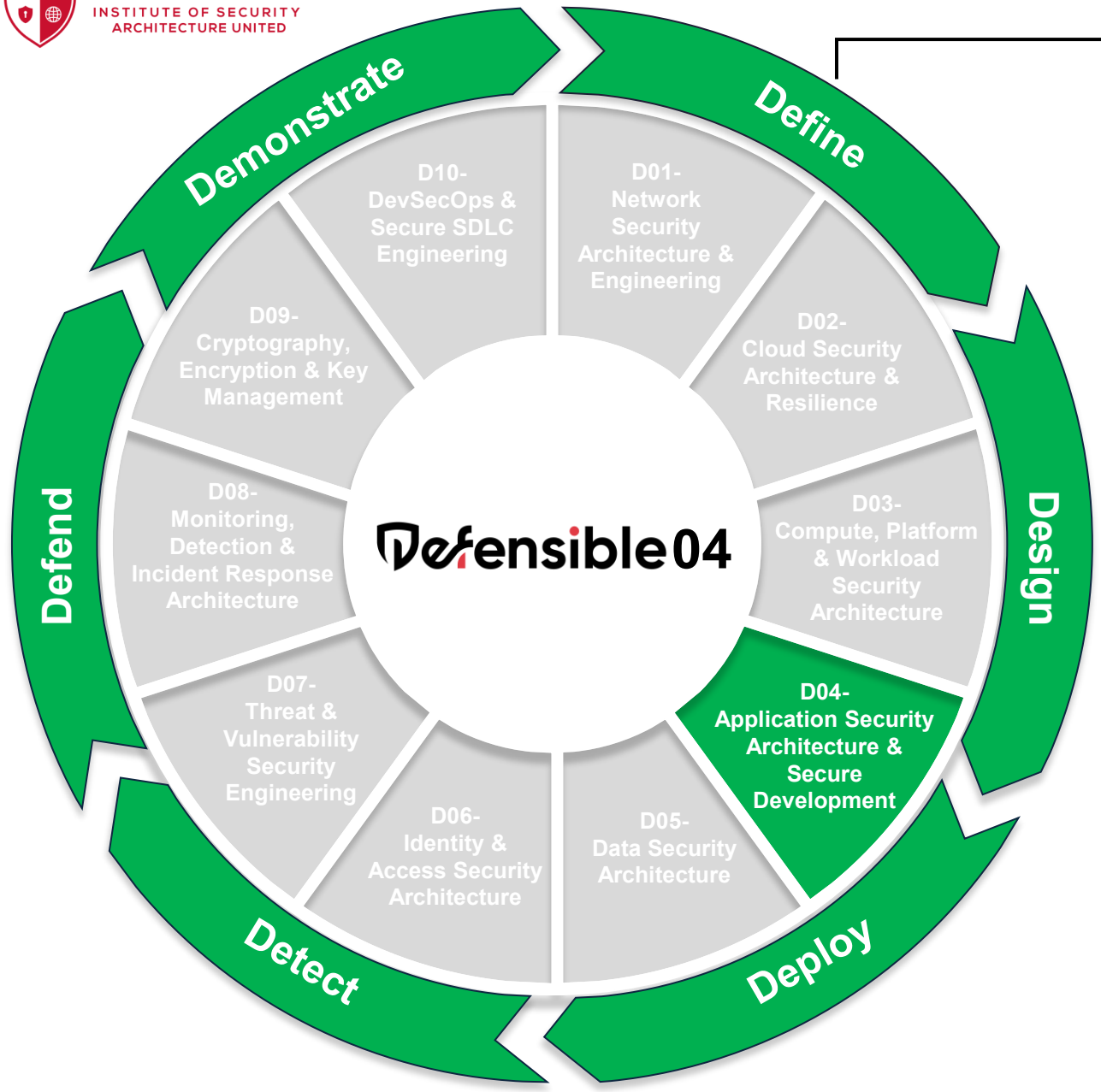
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED



D-Loop Phase	D03 - Compute, Platform, and Workload Security Architecture
Define	Scope: Workload classes and privileged pathways
Design	Blueprint: Hardening and isolation design intent
Deploy	Build: Golden images and runtime enforcement
Detect	Signals: Integrity and privileged activity signals
Defend	Shield: Quarantine, rollback, and remediation actions
Demonstrate	Proof: Baseline conformance verification

D03 Compute, Platform, and Workload Security Architecture - defines measurable expectations for secure workload baselines, platform hardening, isolation boundaries, and controlled privileged pathways across compute environments. The Defensible Loop is applied so workloads are built from known baselines, continuously monitored for integrity, and validated with proof.

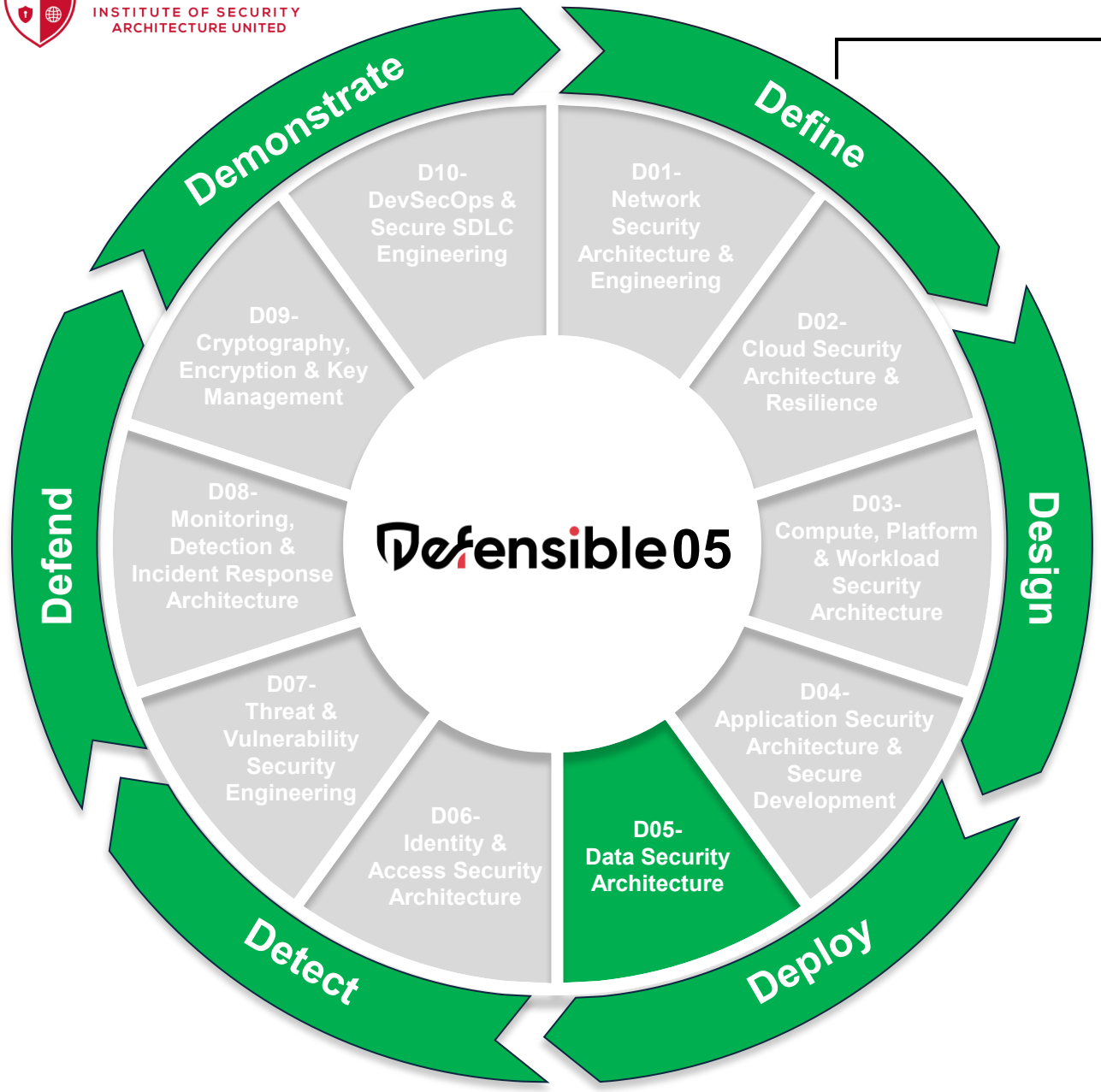
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED



D-Loop Phase	D04 - Application Security Architecture and Secure Development
Define	Scope: Application surface and trust boundaries
Design	Blueprint: Threat informed authorization design
Deploy	Build: Build gates and dependency governance
Detect	Signals: Authentication, API, and app security events
Defend	Shield: Runtime controls and remediation actions
Demonstrate	Proof: Test results and gate evidence

D04 Application Security Architecture and Secure Development - defines measurable expectations for secure application design, authorization, and API protection, secure development practices, and software supply chain integrity. The Defensible Loop is applied so security requirements become build gates, runtime visibility, and verified evidence before release.

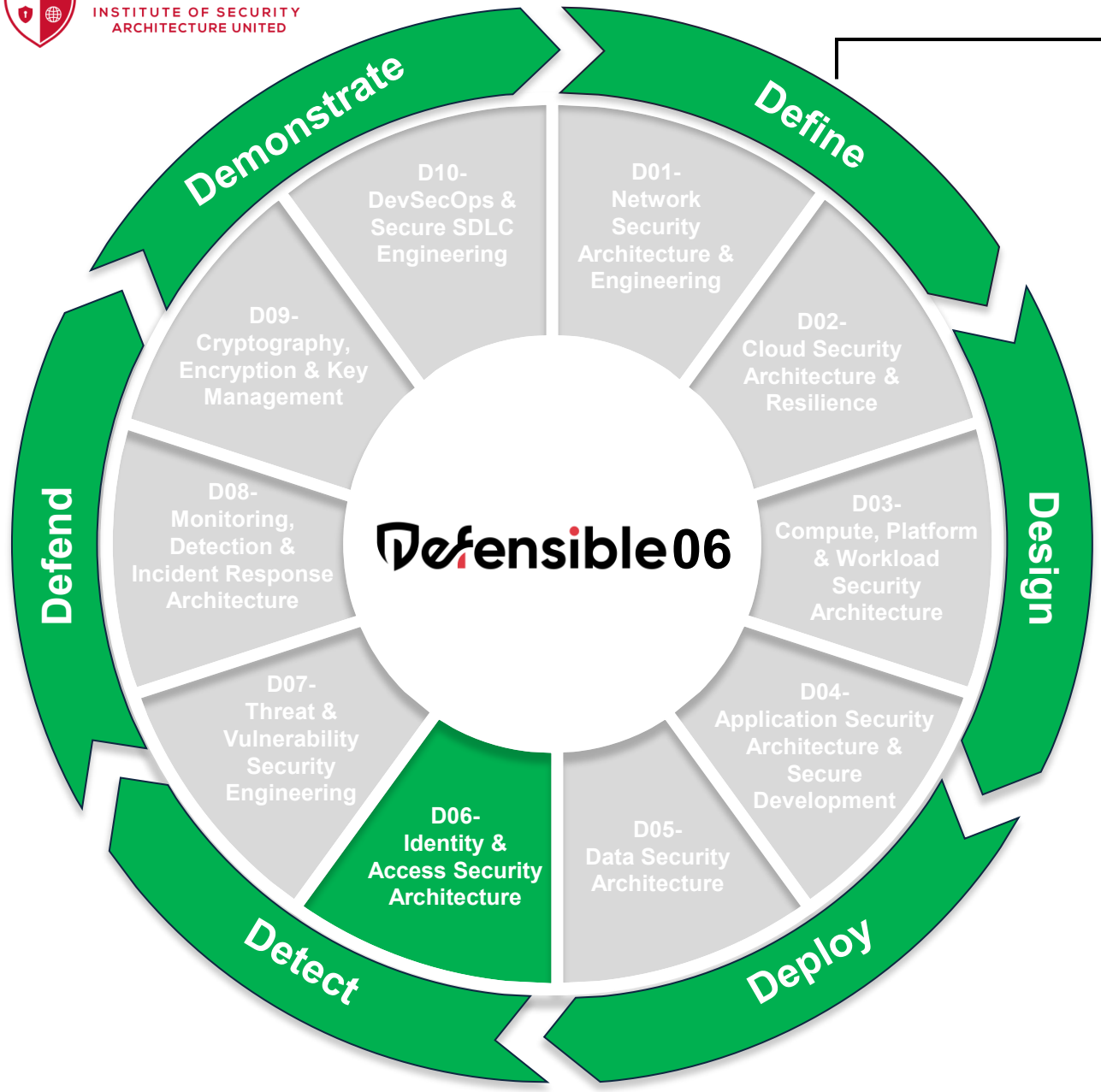
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED



D-Loop Phase	D05 - Data Security Architecture
Define	Scope: Data domains, flows, and storage locations
Design	Blueprint: Access, encryption, and movement intent
Deploy	Build: Policy enforcement and encryption baselines
Detect	Signals: Access and movement anomaly signals
Defend	Shield: Exfiltration blocks and rapid revocation
Demonstrate	Proof: Access reviews and crypto verification

D05 Data Security Architecture - defines measurable expectations for data classification, governed data flows, access enforcement, encryption and integrity protections, and prevention of unauthorized movement. The Defensible Loop is applied so data controls are engineered end-to-end and validated with proof.

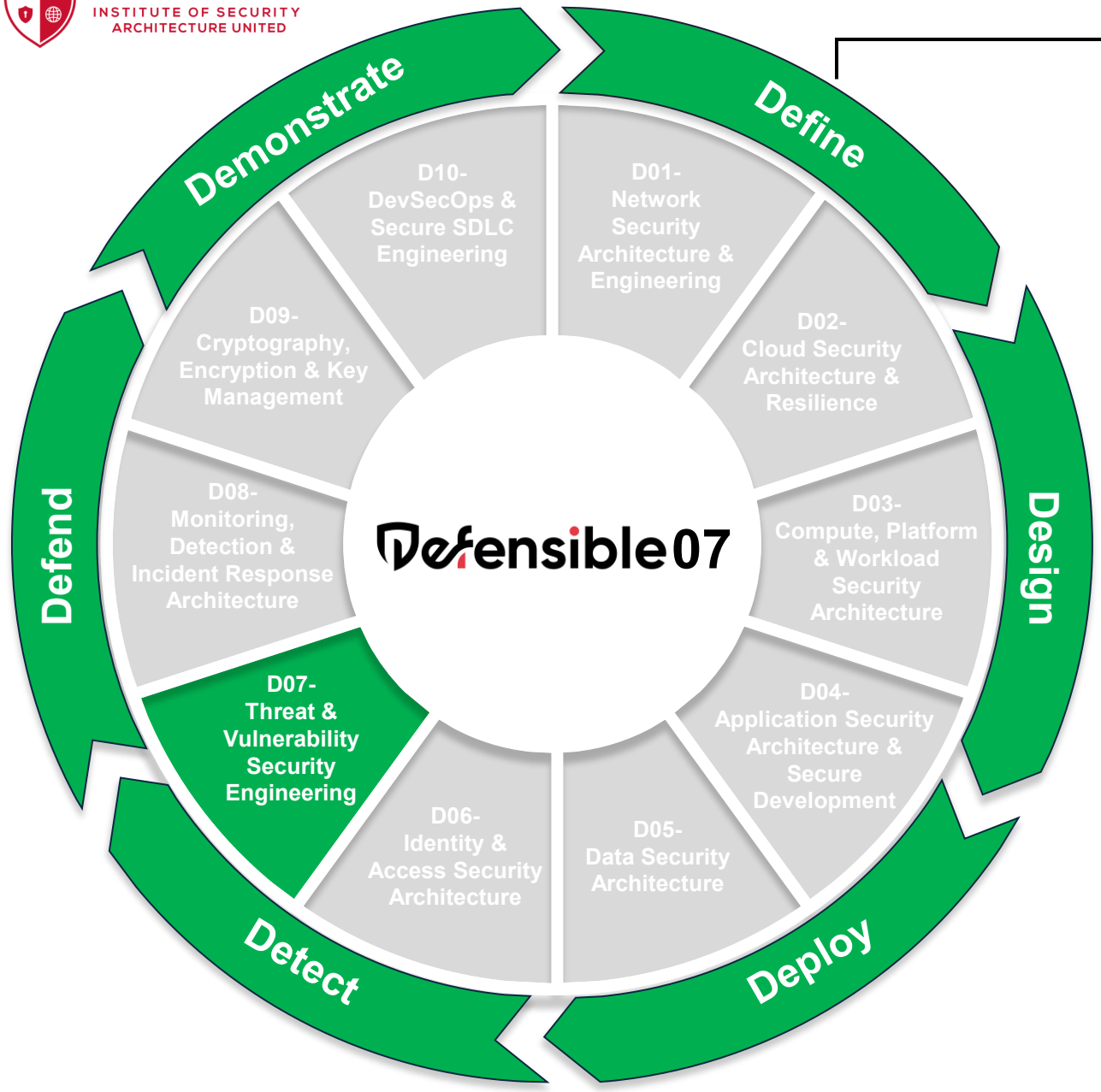
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED



D-Loop Phase	D06 - Identity and Access Security Architecture
Define	Scope: Identity types, roles, and privilege tiers
Design	Blueprint: Authentication and authorization design
Deploy	Build: Strong authentication and privileged workflows
Detect	Signals: Sign in and privilege telemetry
Defend	Shield: Session containment and credential revocation
Demonstrate	Proof: Entitlement reviews and policy validation

D06 Identity and Access Security Architecture - defines measurable expectations for authentication strength, authorization strategy, privileged access boundaries, and lifecycle control of identities and entitlements. The Defensible Loop is applied to ensure access decisions are enforced consistently, observed continuously, and validated with evidence.

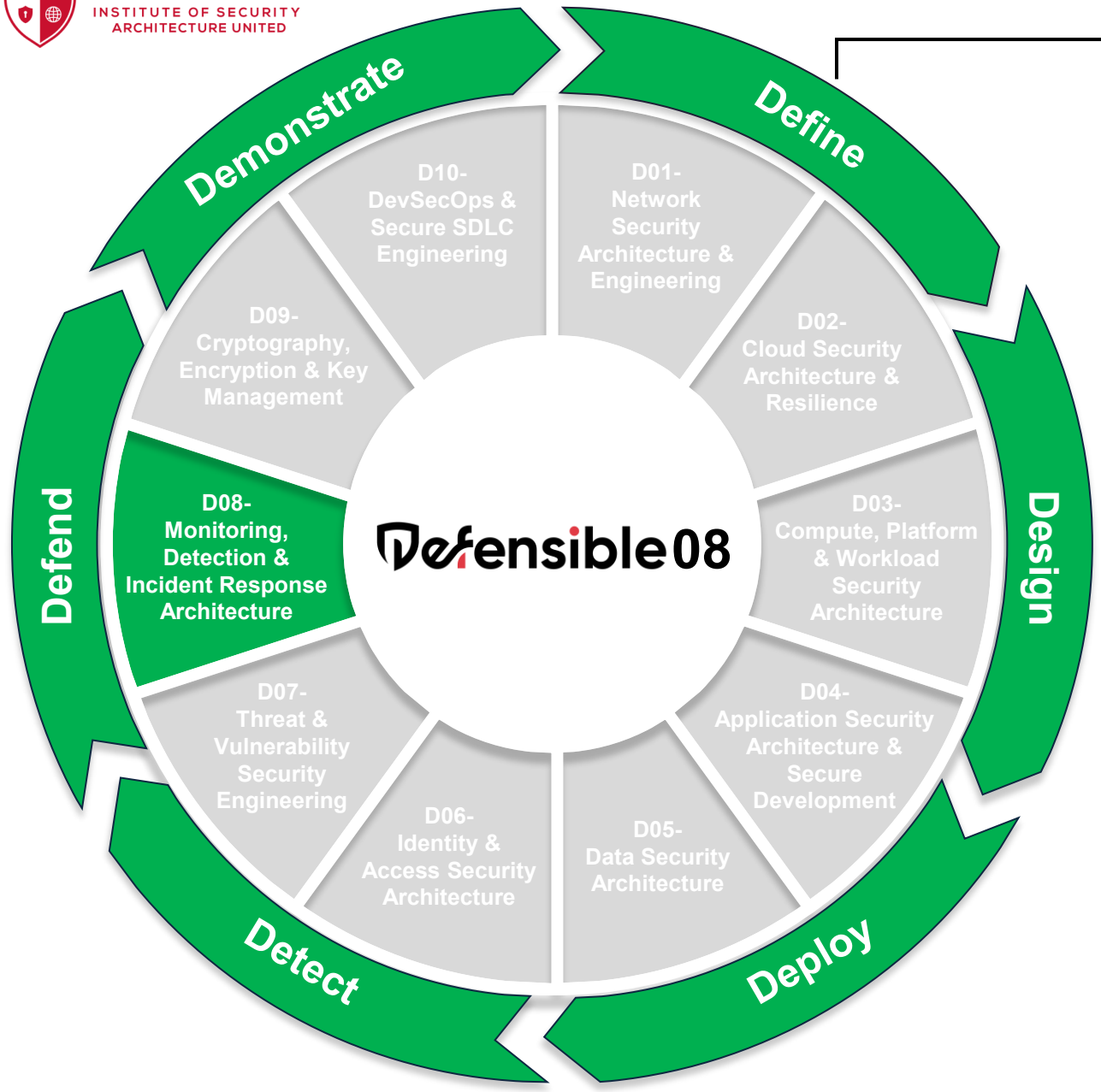
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED



D-Loop Phase	D07 - Threat and Vulnerability Security Engineering
Define	Scope: Exposure inventory and threat assumptions
Design	Blueprint: Triage and mitigation strategy
Deploy	Build: Assessment cadence and remediation workflow
Detect	Signals: Vulnerability state and exploit signals
Defend	Shield: Emergency mitigations and compensating controls
Demonstrate	Proof: Closure validation and risk reduction

D07 Threat and Vulnerability Security Engineering - defines measurable expectations for exposure visibility, vulnerability intake and prioritization, remediation engineering, and compensating controls when immediate fixes are not possible. The Defensible Loop is applied to ensure that risk reduction is operational, time-bound, and validated with evidence.

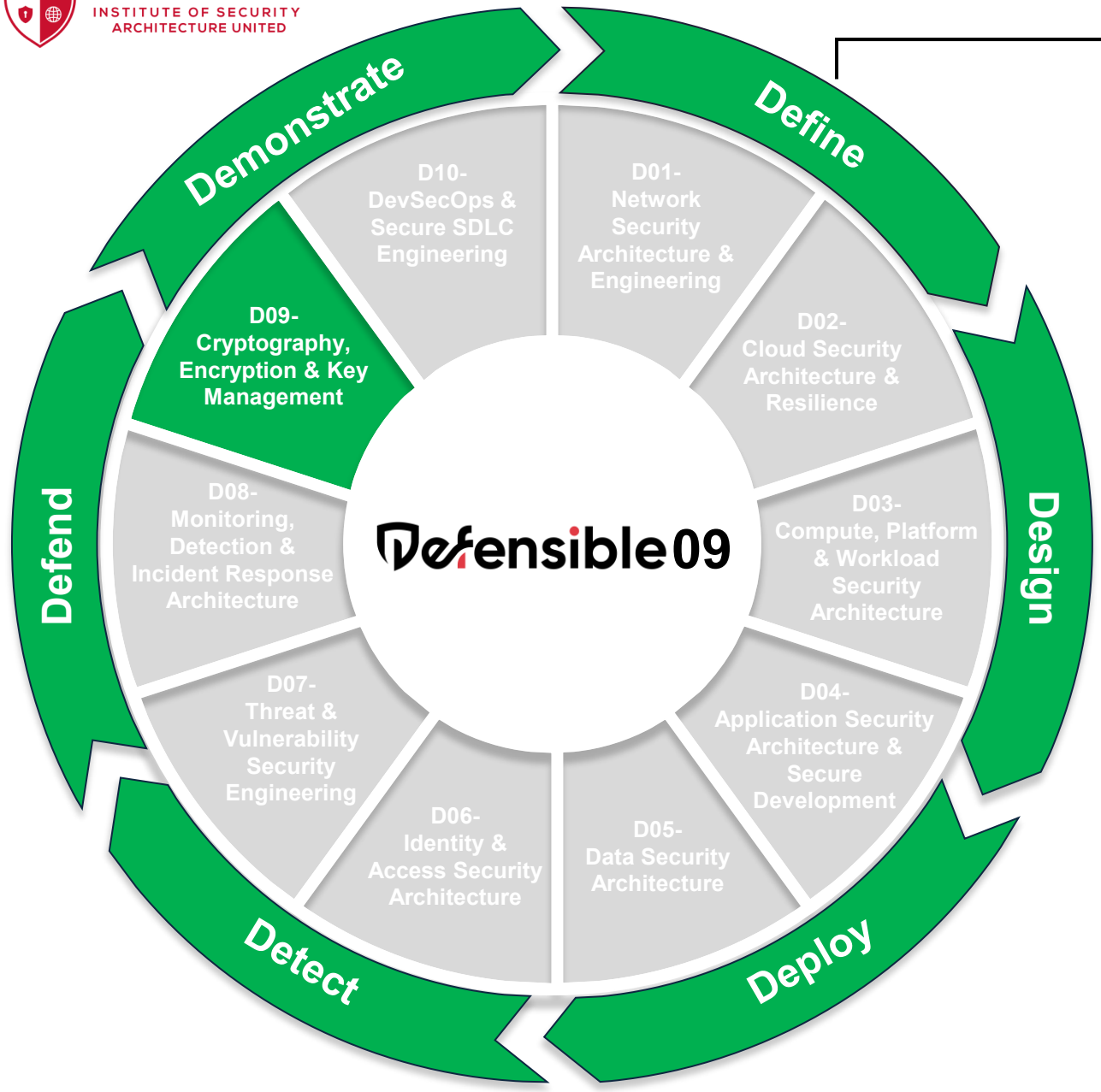
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED



D-Loop Phase	D08 - Monitoring, Detection, and Incident Response Architecture
Define	Scope: Monitoring scope and incident severity model
Design	Blueprint: Telemetry and response workflow design
Deploy	Build: Pipelines, normalization, and alert routing
Detect	Signals: Correlation logic and coverage signals
Defend	Shield: Containment, eradication, and recovery actions
Demonstrate	Proof: Exercises and incident evidence

D08 Monitoring, Detection, and Incident Response Architecture - defines measurable expectations for telemetry architecture, detection engineering, alert fidelity, incident response workflows, and recovery execution. The Defensible Loop is applied so monitoring produces decisions, response produces containment, and outcomes are validated with proof.

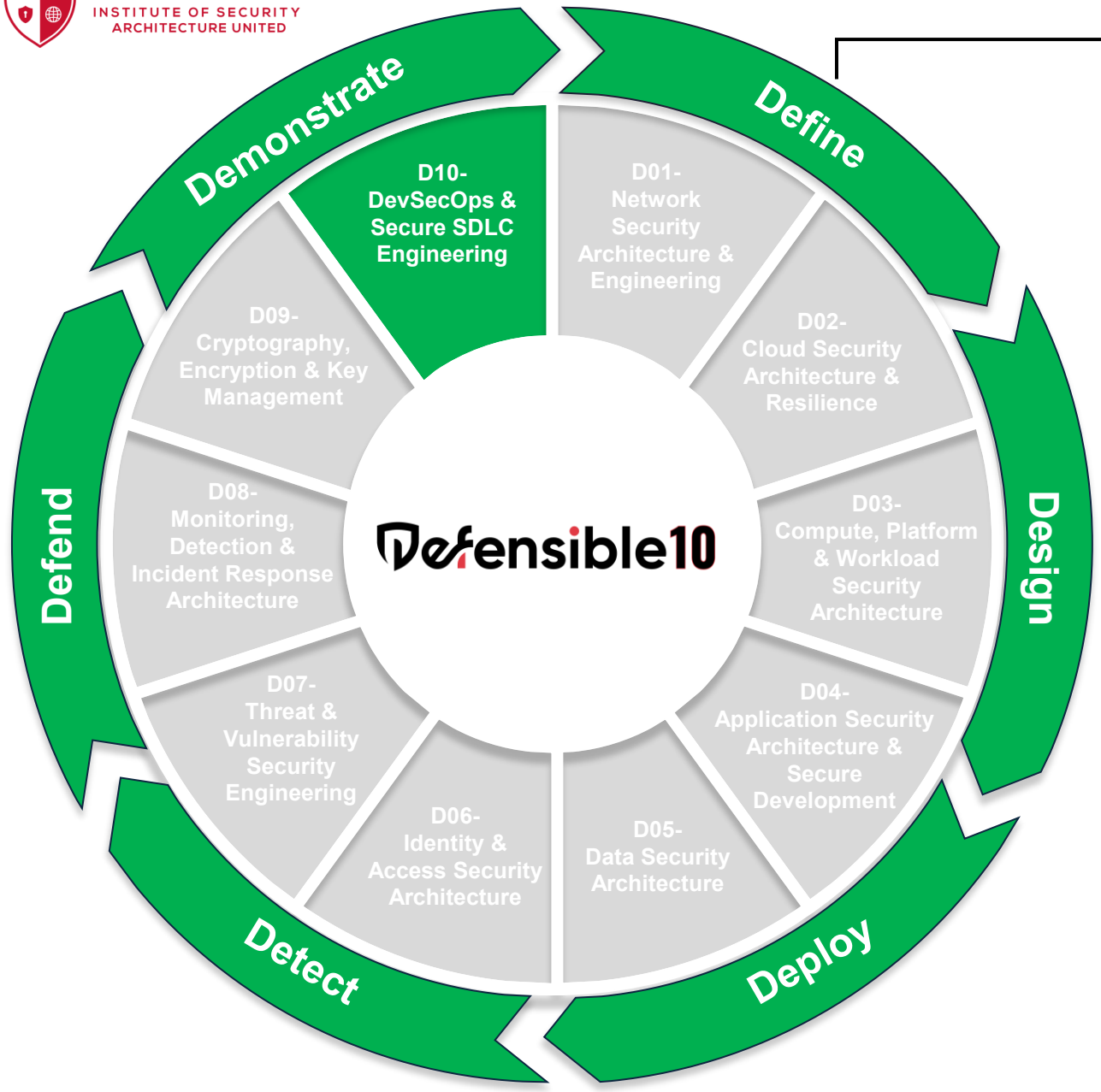
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED



D-Loop Phase	D09 - Cryptography, Encryption, and Key Management
Define	Scope: Crypto inventory and trust anchors
Design	Blueprint: Algorithm policy and key lifecycle design
Deploy	Build: Key storage, rotation, and certificate baseline
Detect	Signals: Key usage anomalies and policy violations
Defend	Shield: Revocation, rotation, and compromise handling
Demonstrate	Proof: Crypto verification and rotation proof

D09 Cryptography, Encryption and Key Management – defines measurable expectations for cryptographic policy, key lifecycle architecture, certificate management, rotation and revocation, and protection of data in transit and at rest. The Defensible Loop is applied so that cryptographic controls are implemented consistently and validated with proof.

ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED



D-Loop Phase	D10 - DevSecOps and Secure SDLC Engineering
Define	Scope: Pipeline stages and release boundaries
Design	Blueprint: Secure pipeline and provenance design
Deploy	Build: Gates, signing, and controlled deployments
Detect	Signals: Gate outcomes and integrity signals
Defend	Shield: Rollback and artifact revocation actions
Demonstrate	Proof: Attestations and deployment trace proof

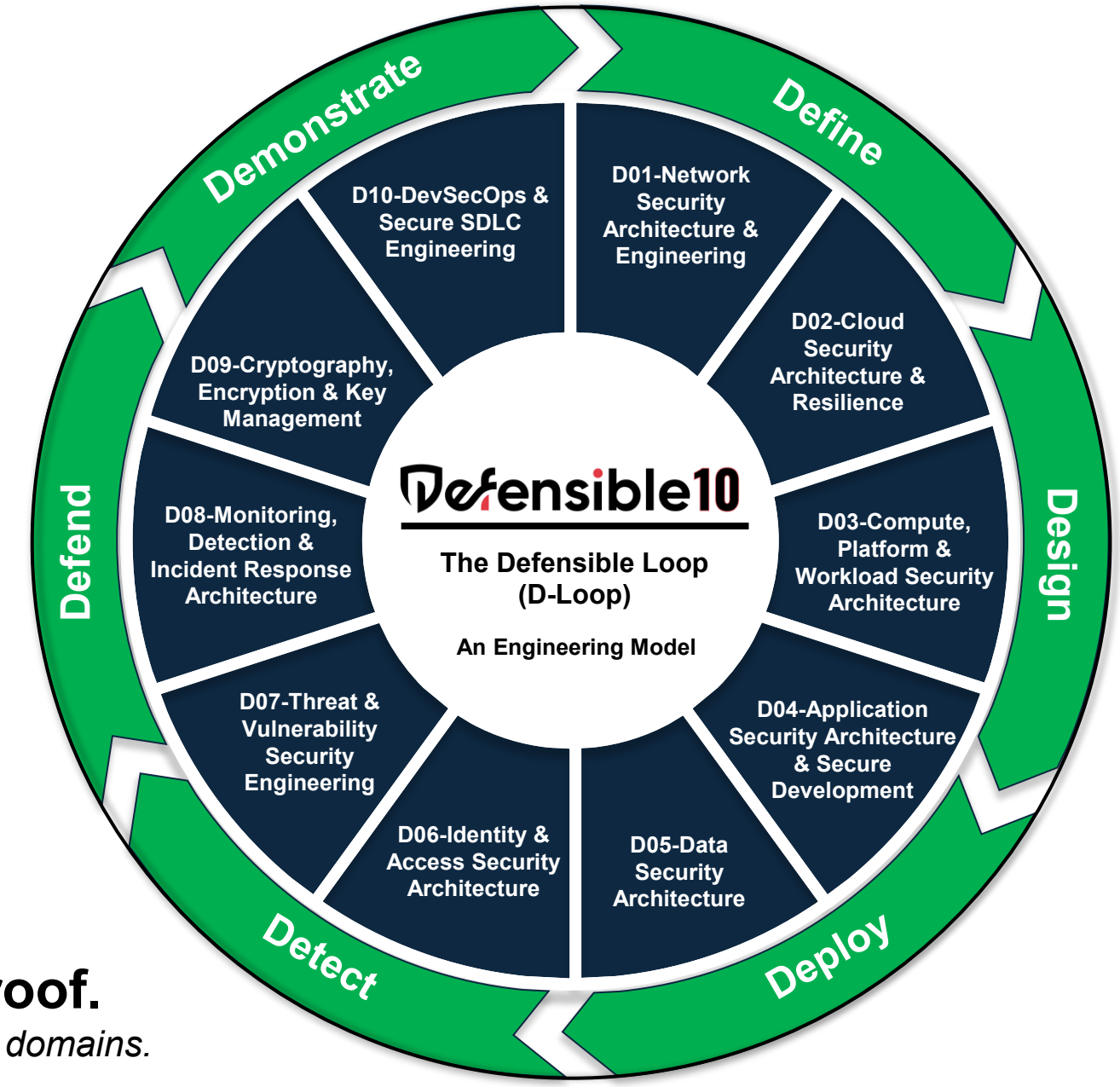
D10 DevSecOps and Secure SDLC Engineering - defines measurable expectations for secure pipeline architecture, non-bypassable gates, artifact integrity and provenance, controlled deployments, and rapid rollback and revocation. The Defensible Loop is applied so that software delivery produces verifiable outcomes and ends with proof.

ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

The Defensible 10 Standards

1 engineering loop, executed across 10 cybersecurity domains.

This wheel represents the complete Defensible 10 Standards framework. Each numbered domain, D01 - D10, applies the same Defensible Loop: Define, Design, Deploy, Detect, Defend, and Demonstrate, so cybersecurity work is consistent, measurable, and ends with proof.



Start with the loop. End with proof.

Join the standards community and help refine the domains.