cygint

Advanced Cybersecurity for Your Digital Assets

Modern Security Solutions for the Connected Enterprise

cygint.co / May 2025

cygint

About Us

Cygint (short for “Signal Intelligence”) is a specialised cybersecurity firm bringing together elite security professionals with decades of combined experience.

We deliver cutting-edge security solutions across IoT ecosystems, threat intelligence platforms, and specialised security testing services.

Our mission is to secure the evolving digital landscape through intelligence-driven approaches and adaptive security postures.

Our Core Values

- **Innovation**: Pioneering solutions for emerging threats
- **Precision**: Delivering targeted, effective security measures
- **Intelligence**: Data-driven insights for proactive defense
- **Integrity**: Trusted partnerships built on transparency

Founder

Nilesh Chaudhari

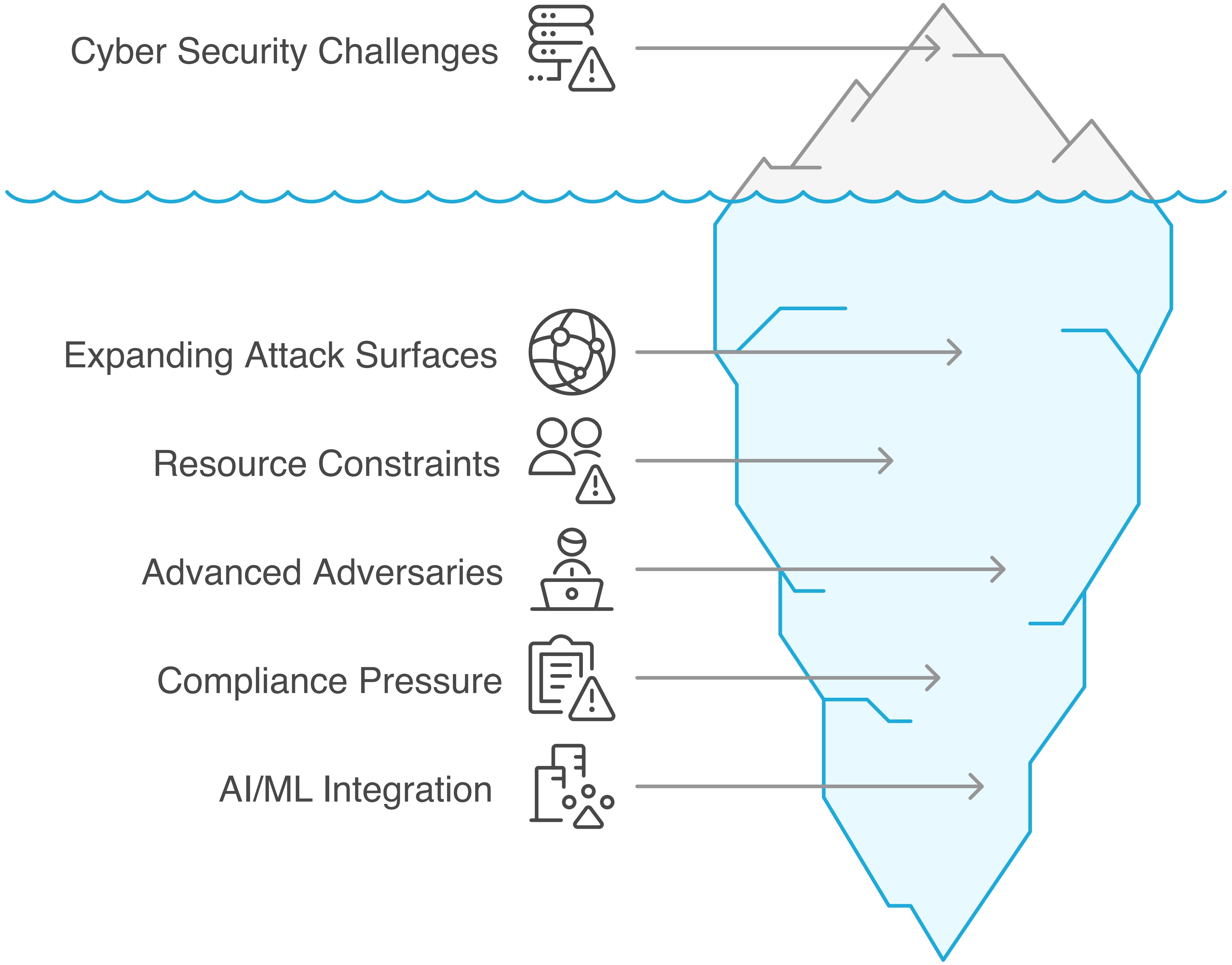
CCISO, CISSP, CBCP, CSM

- 24+ years of comprehensive cybersecurity leadership experience across enterprise risk management, business continuity, and security strategy development
- IP innovator and co-owner for multiple cyber security based patents (US and India)
- Experience leading global cybersecurity practices at major consulting companies including Wipro, Hewlett Packard Enterprise, Paladion (Atos Eviden), Infosys
- Expertise spans the full security spectrum: leadership, risk management, technical implementation, product development, and business growth

cygint

The Evolving Threat Landscape - 2025

- Expanding Attack Surfaces: The proliferation of IoT, cloud services, and interconnected systems has created unprecedented attack surface complexity
- Resource Constraints: Security teams are overwhelmed by alert volume and tool sprawl
- Advanced Adversaries: Threat actors are employing increasingly sophisticated techniques to bypass traditional security controls
- Compliance Pressure: Regulatory requirements continue to expand while becoming more technically specific
- AI/ML Integration: Both defenders and attackers are leveraging AI, creating new security paradigms



cygint

Our Core Services

Addressing the evolving Threat Landscape

IoT Security Solutions

End-to-end security for connected ecosystems, from design architecture to implementation and testing.

Full-stack approach

Specialised Security Testing

Advanced testing services including API Security, Assumed-Breach Testing, Adversary Simulation, and AI Platform Red Teaming.

Beyond conventional pentesting

Digital Exposure Management

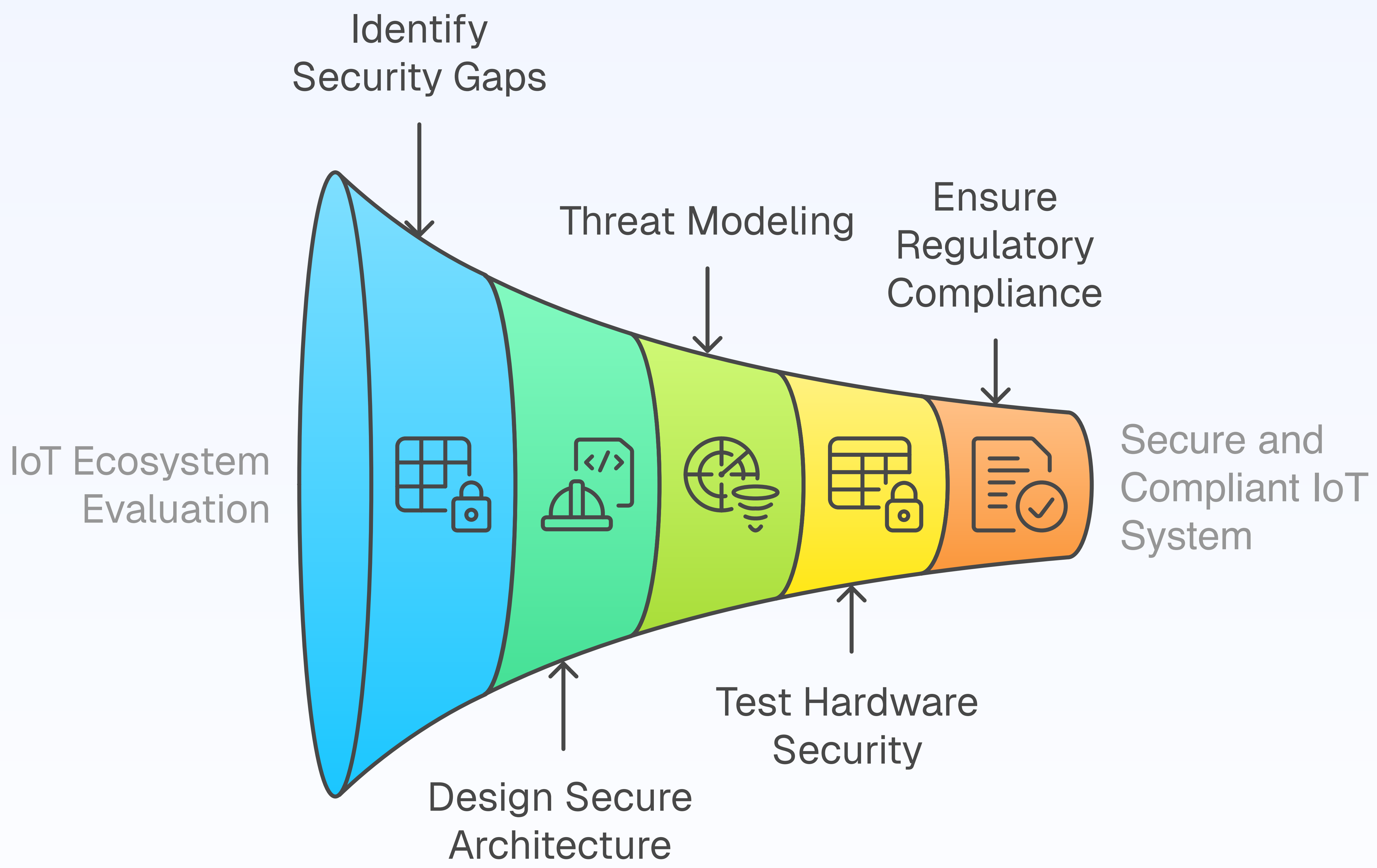
Agentic platform for external vulnerability detection and mitigation, with focus on team productivity.

Beyond attack surface management

cygint

IoT Security Solutions

Full-stack IoT security expertise from concept to implementation

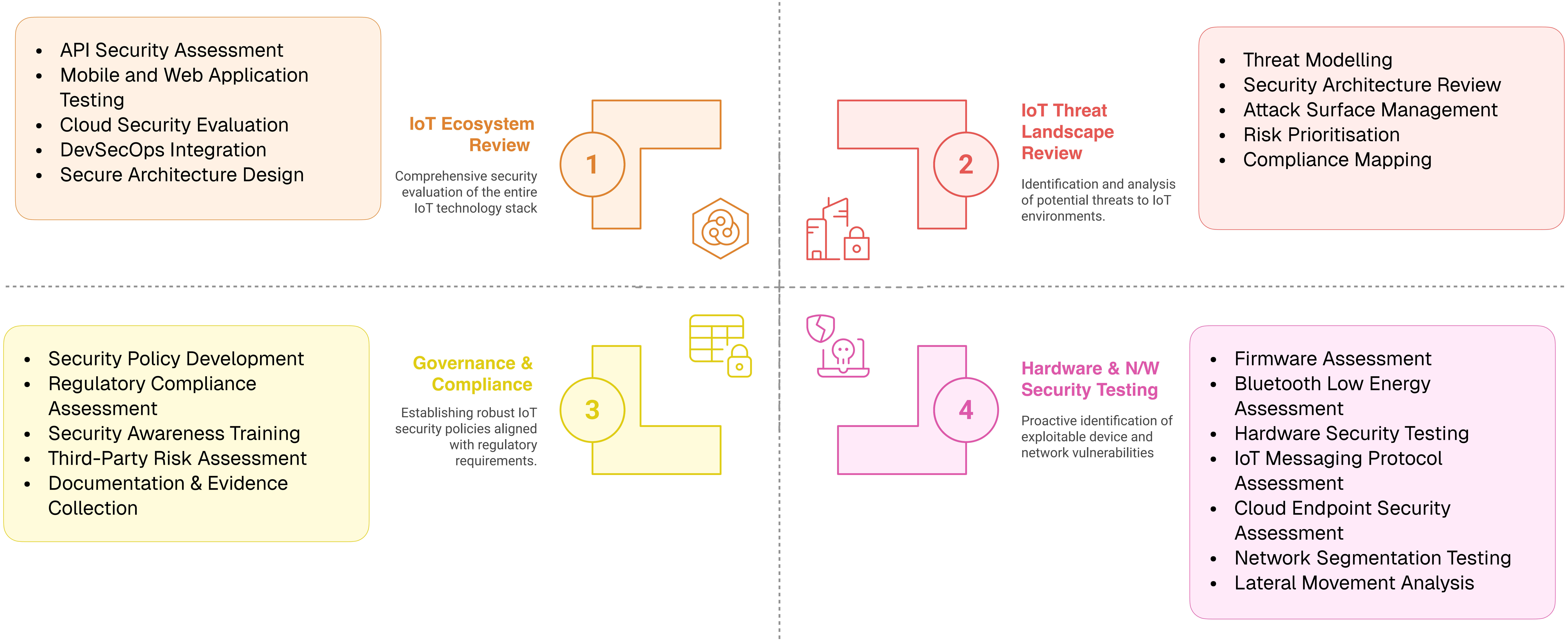

Identify Security Gaps
Threat Modeling
Ensure Regulatory Compliance
IoT Ecosystem Evaluation
Secure and Compliant IoT System
Test Hardware Security
Design Secure Architecture

- **Comprehensive IoT Assessment**: Evaluation of your IoT ecosystem, identifying security gaps across hardware, firmware, and communication protocols
- **Secure Architecture Design**: Building security into IoT deployments from the ground up
- **Threat Modeling**: Identifying and mitigating potential attack vectors specific to connected systems
- **Hardware & Firmware Security**: Rigorous testing of device security, including firmware vulnerability analysis
- **Regulatory Compliance**: Ensuring IoT products and services comply with relevant industry standards and regulations

cygint

Comprehensive IoT Security Service Offerings

End-to-End Protection for the Connected Enterprise



1

IoT Ecosystem Review

Comprehensive security evaluation of the entire IoT technology stack

- API Security Assessment
- Mobile and Web Application Testing
- Cloud Security Evaluation
- DevSecOps Integration
- Secure Architecture Design

2

IoT Threat Landscape Review

Identification and analysis of potential threats to IoT environments.

- Threat Modelling
- Security Architecture Review
- Attack Surface Management
- Risk Prioritisation
- Compliance Mapping

3

Governance & Compliance

Establishing robust IoT security policies aligned with regulatory requirements.

- Security Policy Development
- Regulatory Compliance Assessment
- Security Awareness Training
- Third-Party Risk Assessment
- Documentation & Evidence Collection

4

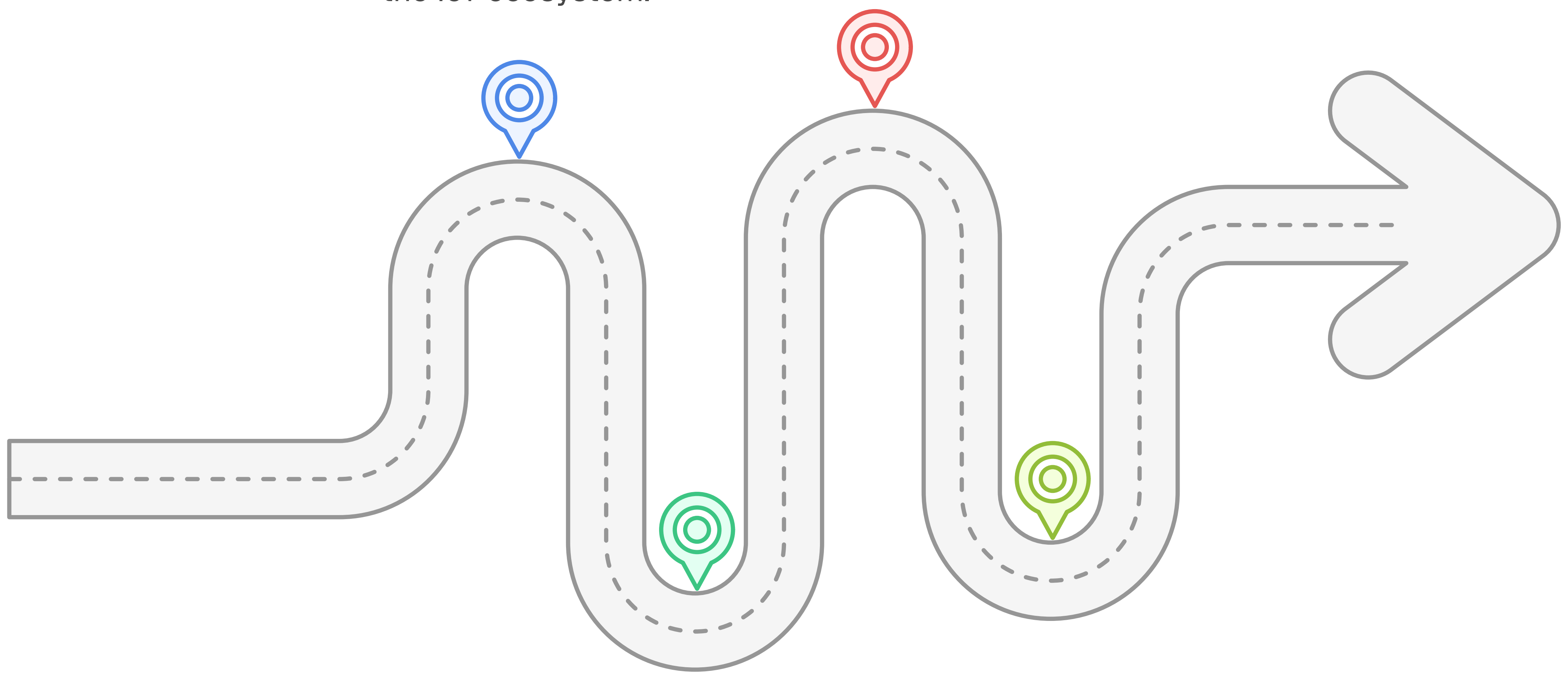
Hardware & N/W Security Testing

Proactive identification of exploitable device and network vulnerabilities

- Firmware Assessment
- Bluetooth Low Energy Assessment
- Hardware Security Testing
- IoT Messaging Protocol Assessment
- Cloud Endpoint Security Assessment
- Network Segmentation Testing
- Lateral Movement Analysis

IoT Security Testing Methodology

Aligned with OWASP IoT Security Testing Guidelines



Reconnaissance

Setting objectives and gathering information about the IoT ecosystem.

Exploitation

Testing the resilience of IoT devices against attacks.

Vulnerability Analysis

Examining IoT devices and networks for weaknesses.

Reporting and Validation

Documenting findings and providing remediation guidance.

1. Reconnaissance

- **Objective Setting**: Scope of the penetration test, including specific devices, networks, and systems to be examined.
- **Information Gathering**: Gather information about the target IoT ecosystem. This includes device specifications, firmware versions, network architectures, and application interfaces.

2. Vulnerability Analysis

- **Static Analysis**: Examine the IoT device's firmware and software without executing them, looking for vulnerabilities like hardcoded credentials, insecure configurations, and known vulnerable components.
- **Dynamic Analysis**: Interact with the IoT device and its ecosystem in real-time, attempting to exploit potential vulnerabilities in its operating environment, such as weak encryption, buffer overflows, and authentication bypasses.
- **Network Analysis**: Analyse the network communications to and from IoT devices for weaknesses, including sniffing network traffic to identify unencrypted data transmission and analysing protocols for vulnerabilities.

3. Exploitation

- **Developing Exploits**: Based on identified vulnerabilities, develop or use existing exploits to test the IoT device's resilience against attacks. This includes attempting to gain unauthorised access, escalate privileges, or execute remote code.
- **Impact Assessment**: Evaluating the impact of successful exploits on the device's functionality, data integrity, and user privacy. This step helps understand the real-world implications of vulnerabilities.

4. Reporting and Validation

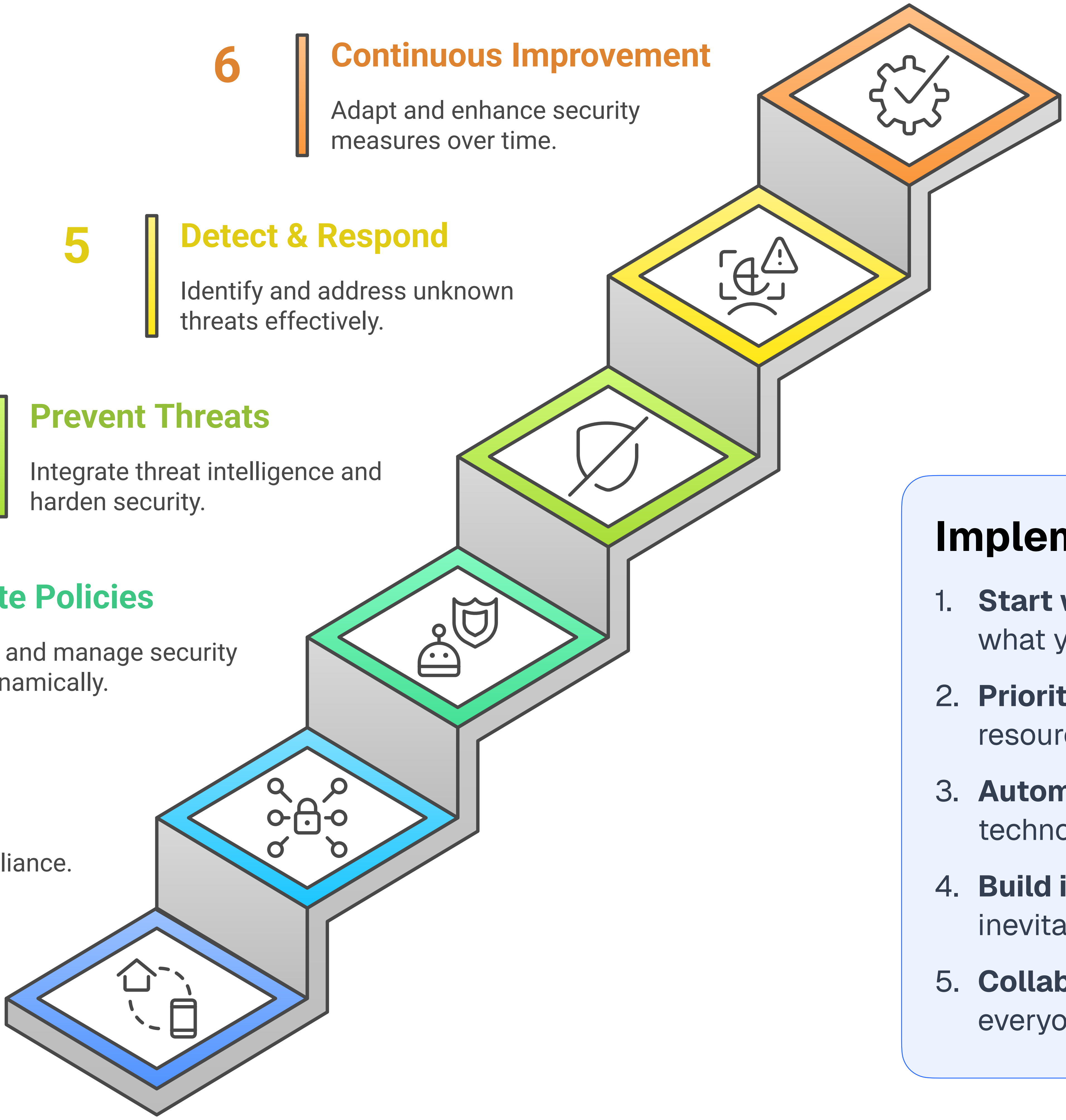
- **Comprehensive Reporting**: Detailed report that outlines the vulnerabilities discovered, the methods used to exploit them, the potential impact, and recommendations for mitigation.
- **Remediation Guidance**: Specific actionable advice for addressing identified vulnerabilities, such as

IoT Security Lifecycle Management

Our Comprehensive Approach to Securing the IoT Ecosystem

Benefits

- **Holistic security**: Addresses all aspects of IoT ecosystem protection
- **Reduced attack surface**: Minimizes potential entry points for threats
- **Regulatory compliance**: Meets industry and government requirements
- **Business enablement**: Securely enables IoT innovation and adoption
- **Operational resilience**: Maintains business continuity despite threats



1 **Understand Assets**

Catalog and map all IoT devices and connections.

2 **Assess Risks**

Monitor and evaluate vulnerabilities and compliance.

3 **Automate Policies**

Implement and manage security policies dynamically.

4 **Prevent Threats**

Integrate threat intelligence and harden security.

5 **Detect & Respond**

Identify and address unknown threats effectively.

6 **Continuous Improvement**

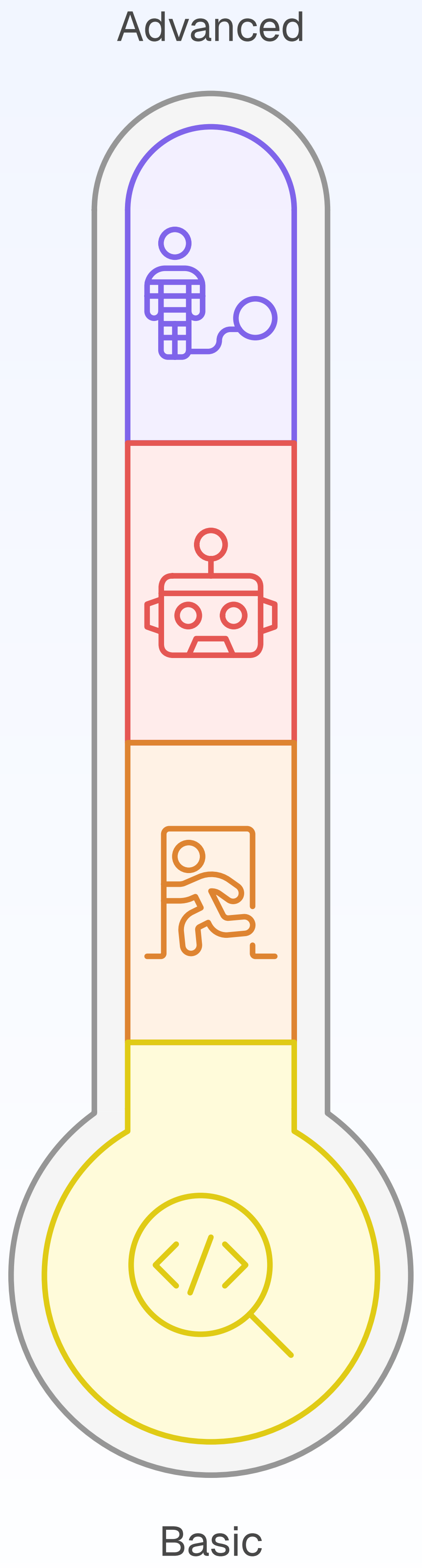
Adapt and enhance security measures over time.

Implementation Strategy

1. **Start with visibility**: You can't secure what you can't see
2. **Prioritise based on risk**: Focus resources on critical vulnerabilities
3. **Automate where possible**: Leverage technology to scale security efforts
4. **Build in resilience**: Prepare for inevitable security incidents
5. **Collaborate across teams**: Security is everyone's responsibility

Specialised Security Testing Services

Testing methodologies that go beyond conventional approaches



Advanced

Beyond-Pentest Simulation

Mimics advanced attacks, evades security controls.

AI Platform Red Teaming

Assesses AI systems, identifies unique AI vulnerabilities.

Assumed-Breach Testing

Simulates attacker movement, finds escalation paths.

API Security Testing

Assesses API security, tests for common vulnerabilities.

Basic

- **API Security Testing**: Comprehensive assessment of API security posture, testing against OWASP API Security Top 10, business logic flaw identification, and authentication bypass testing
- **Assumed-Breach Penetration Testing**: Identifies lateral movement opportunities, privilege escalation paths, and evaluates detection capabilities
- **AI Platform Red Teaming**: Specialised security assessment for AI systems and models, identifying vulnerabilities like prompt injection, model poisoning, and alignment failures
- **RedMirror Recon**™ (Beyond-Pentest Adversary Simulation): Next-level adversary drill for 'already-assessed' organisations. Sophisticated multi-vector attack chains, evasion of existing security controls, and realistic exfiltration scenarios

API Security Testing

Comprehensive assessment against OWASP API Guidelines

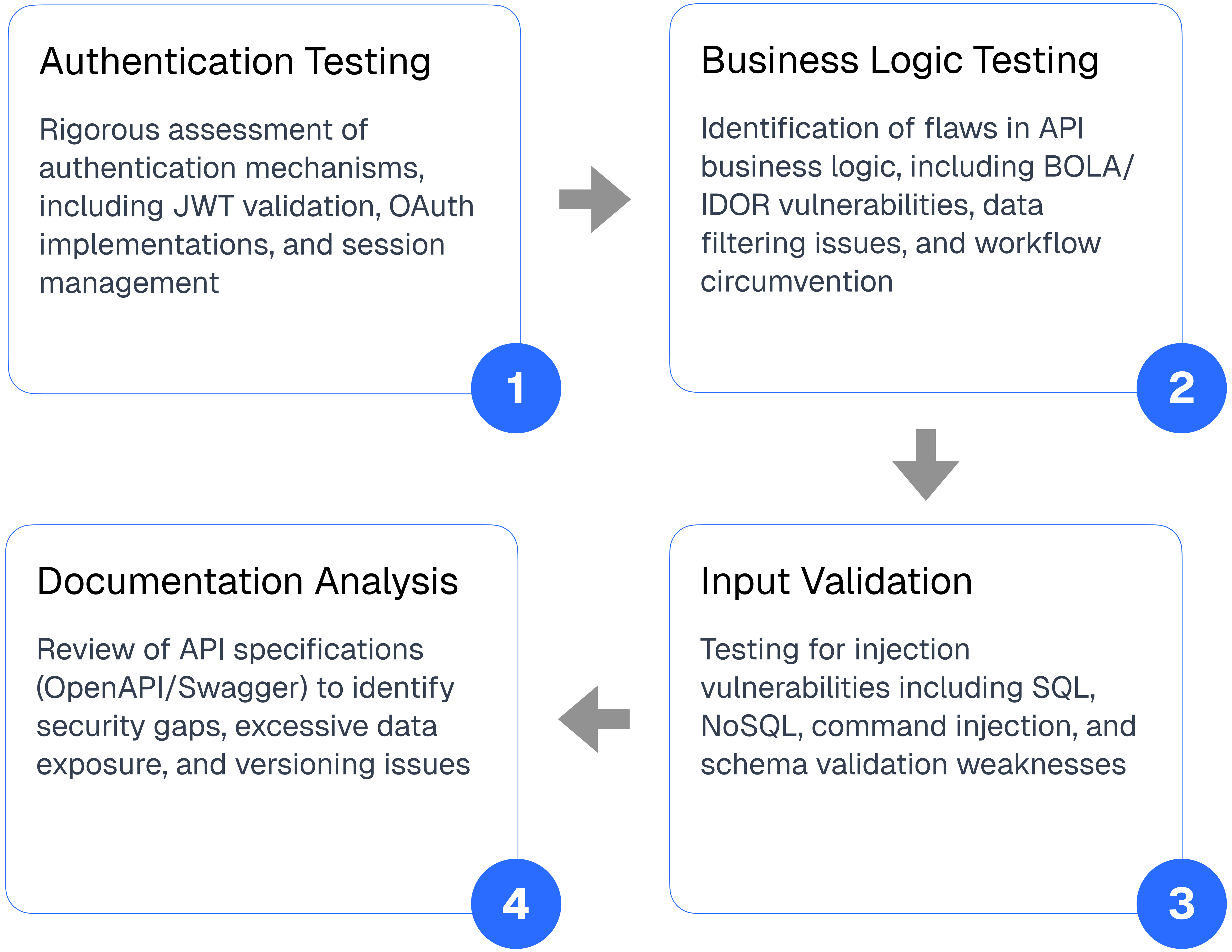
Purpose

- Identify vulnerabilities across your API ecosystem
- Prevent data breaches and unauthorised access
- Ensure compliance with security standards
- Protect critical business functionality
- Validate security controls throughout API lifecycle

Differentiators

- API-specific testing methodology
- Full-stack API security assessment
- Custom tools for modern API patterns
- Developer-friendly remediation guidance

Methodology



1 Authentication Testing

Rigorous assessment of authentication mechanisms, including JWT validation, OAuth implementations, and session management

2 Business Logic Testing

Identification of flaws in API business logic, including BOLA/IDOR vulnerabilities, data filtering issues, and workflow circumvention

3 Input Validation

Testing for injection vulnerabilities including SQL, NoSQL, command injection, and schema validation weaknesses

4 Documentation Analysis

Review of API specifications (OpenAPI/Swagger) to identify security gaps, excessive data exposure, and versioning issues

Attack Vectors Covered

BOLA
Exploiting flaws in object-level authorization schemes.

Authentication
Exploiting weaknesses in authentication processes.

Data Exposure
Sensitive data being revealed unintentionally.

Mass Assignment
Modifying object properties without proper authorization.

Injection Attacks
Injecting malicious code into API requests.

SSRF
Abusing server-side requests to access internal resources.

Business Logic Abuse
Exploiting flaws in the API's business logic.

Fuzzing & Manipulation
Sending invalid data to trigger unexpected behavior.

cygint

Assumed-Breach Penetration Testing

Start where attackers land, finish where your defences fail

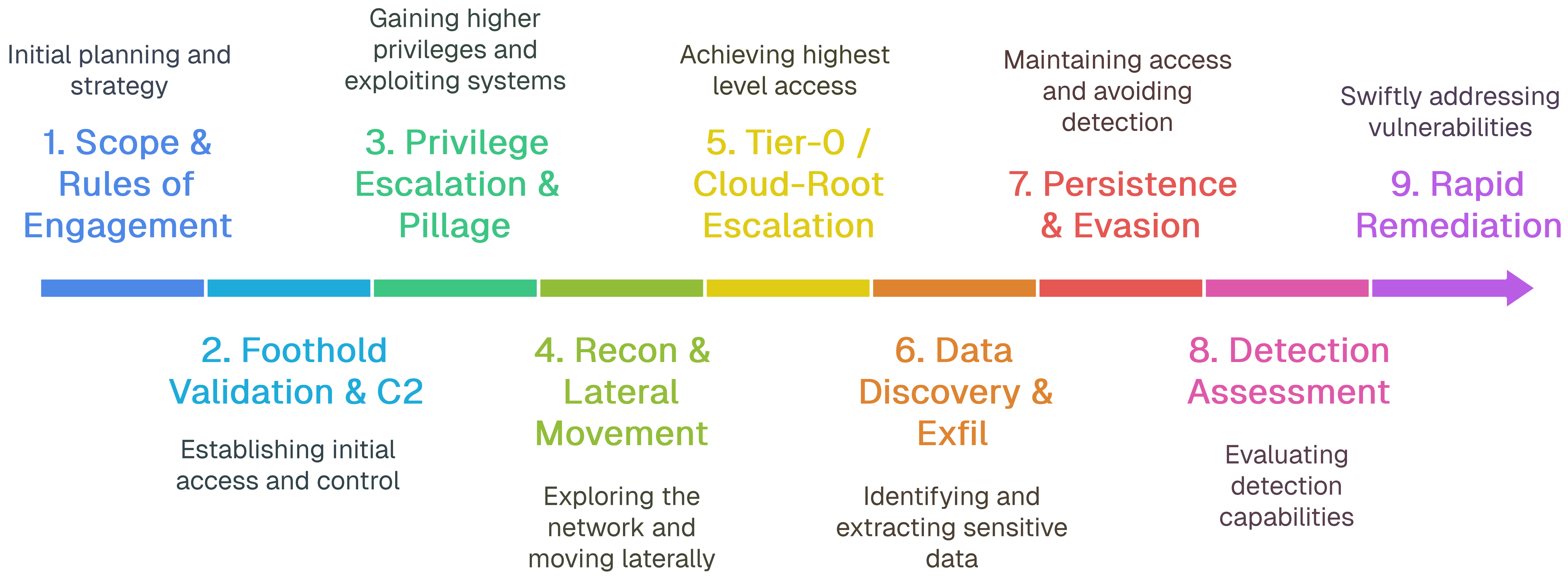
Purpose

- Measure reach, speed, detection, and impact
- Evaluate the effectiveness of detection, response, and containment capabilities once attackers are inside
- Prioritise security investments based on actual attack paths and techniques that succeeded

Differentiators

- Assumed foothold mirrors real incidents
- Business-first risk scoring
- Exploit-ready code deliverables
- Purple-team DNA
- Metrics that matter

Methodology



1. Scope & Rules of Engagement

Initial planning and strategy

2. Foothold Validation & C2

Establishing initial access and control

3. Privilege Escalation & Pillage

Gaining higher privileges and exploiting systems

4. Recon & Lateral Movement

Exploring the network and moving laterally

5. Tier-0 / Cloud-Root Escalation

Achieving highest level access

6. Data Discovery & Exfil

Identifying and extracting sensitive data

7. Persistence & Evasion

Maintaining access and avoiding detection

8. Detection Assessment

Evaluating detection capabilities

9. Rapid Remediation

Swiftly addressing vulnerabilities

Attack Vectors Covered

On-Prem & Azure AD

Exploits targeting on-premises and Azure Active Directory environments.

Hybrid / Multicloud

Pivoting techniques across hybrid and multi-cloud infrastructures.

SaaS token abuse

Exploiting vulnerabilities in SaaS token authentication mechanisms.

EDR evasion

Techniques used to bypass Endpoint Detection and Response systems.

OT / IoT attacks

Network attacks targeting Operational Technology and IoT devices.

Ransomware & Insider

Simulations of ransomware attacks and insider threat scenarios.

AI Platform Red Teaming

Specialised security assessment for AI systems and models

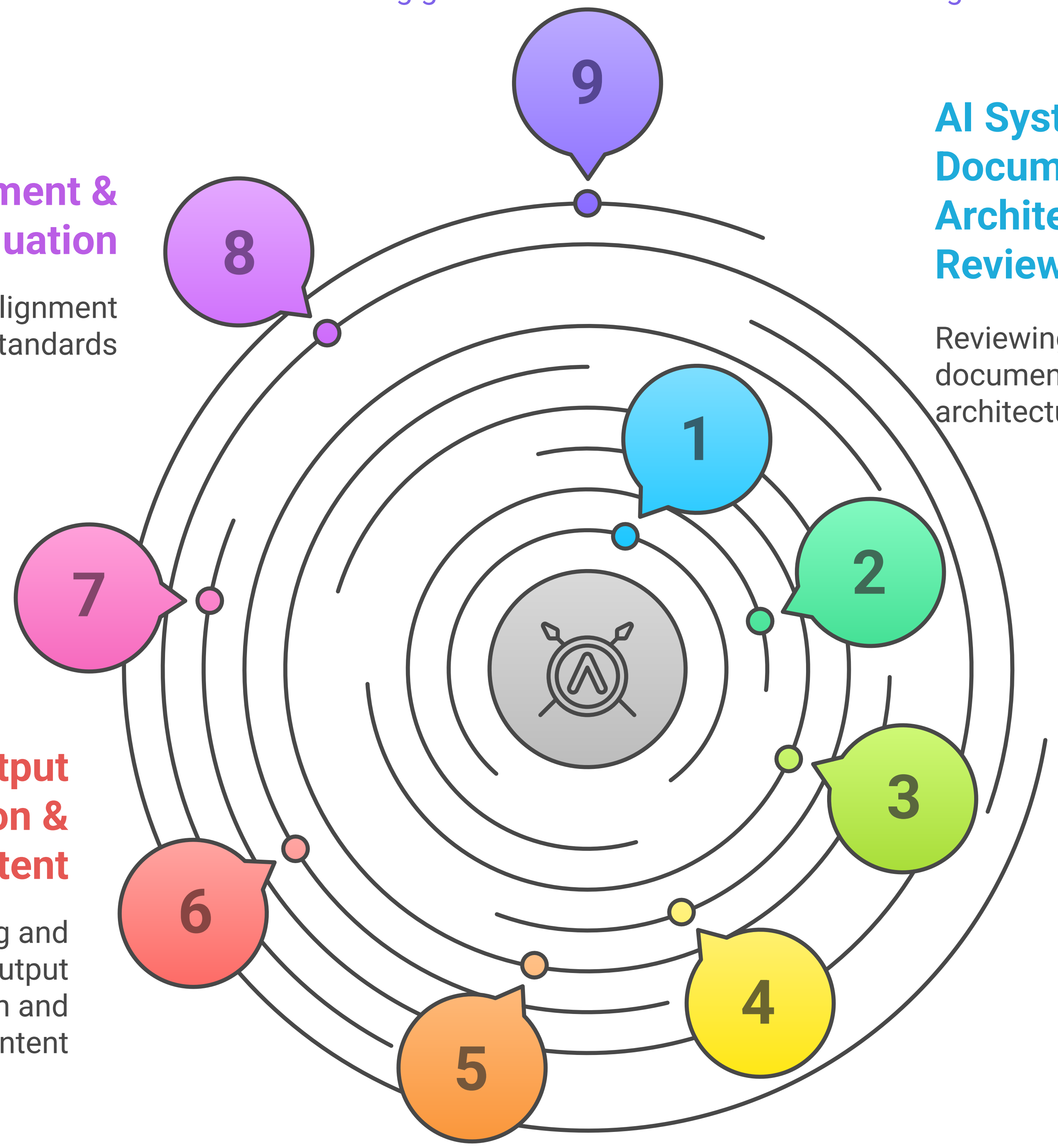
Purpose

- Identify vulnerabilities specific to AI/ML systems
- Evaluate alignment with ethical standards and policies
- Test resilience against prompt attacks and model manipulation
- Ensure data privacy and IP protection
- Validate security controls for AI infrastructure
- Measure real-world impact of potential AI exploitation

Differentiators

- AI-native security expertise
- Combination of prompt & technical attacks
- Specialized in proprietary & open-source models
- Testing across model types (text, image, multimodal)
- Real-world impact assessment

Methodology



Remediation Guidance & Hardening

Providing guidance for remediation and hardening

AI System Documentation & Architecture Review

Reviewing system documentation and architecture

Model Type & Surface Area Analysis

Analyzing model types and potential vulnerabilities

Prompt Injection & Jailbreaking Assessment

Assessing vulnerabilities to prompt injection and jailbreaking

Model Boundary Testing & Edge Cases

Testing model boundaries and handling edge cases

Data Extraction & Privacy Controls

Evaluating data extraction risks and privacy controls

Output Manipulation & Harmful Content

Identifying and mitigating output manipulation and harmful content

Infrastructure & Integration Security

Ensuring security of infrastructure and integration

Alignment & Safety Evaluation

Evaluating alignment with safety standards

Attack Vectors Covered

Prompt Injection

Injecting malicious prompts to manipulate model.

System Leakage

Extracting sensitive system instructions from the model.

Parameter Inference

Inferring model parameters through crafted queries.

Model Extraction

Stealing the model architecture and weights.

Data Poisoning

Corrupting training data to manipulate model behavior.

Model Inversion

Reconstructing training data from model outputs.

Adversarial Examples

Crafting inputs to cause model misclassification.

Chain Manipulation

Manipulating chain-of-thought reasoning process.

Plugin Vulnerabilities

Exploiting vulnerabilities in plugins or extensions.

Model DoS

Overloading the model to cause denial of service.

cygint

RedMirror Recon™

Beyond-Pentest Adversary Simulation for 'already-assessed' organisations

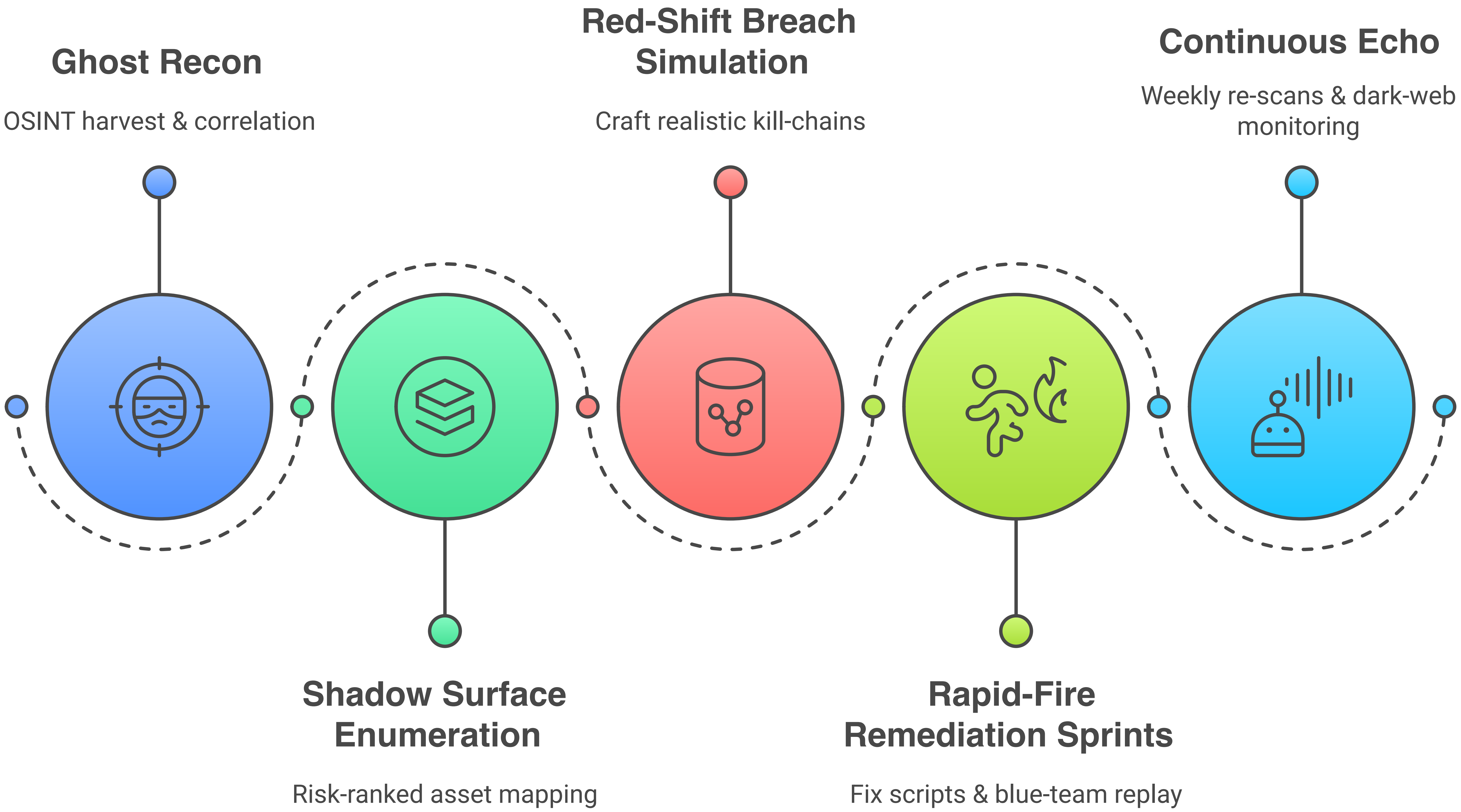
Purpose

- Next-level adversary drill for 'already-assessed' organisations.
- Blends deep OSINT, automated attack-surface mapping & human exploitation.
- Validates real-world breach paths that routine pentests miss.

Differentiators

- Targets firms relying on recent audits—'Already-Assessed ≠ Already-Safe'.
- Business-risk scoring mapped to revenue, regulation, kill-chain stage.
- Exploit-ready, containerised PoCs for developer reproduction.
- Executive metrics: time-to-breach vs industry peers.

Methodology



Ghost Recon

OSINT harvest & correlation

Shadow Surface Enumeration

Risk-ranked asset mapping

Red-Shift Breach Simulation

Craft realistic kill-chains

Rapid-Fire Remediation Sprints

Fix scripts & blue-team replay

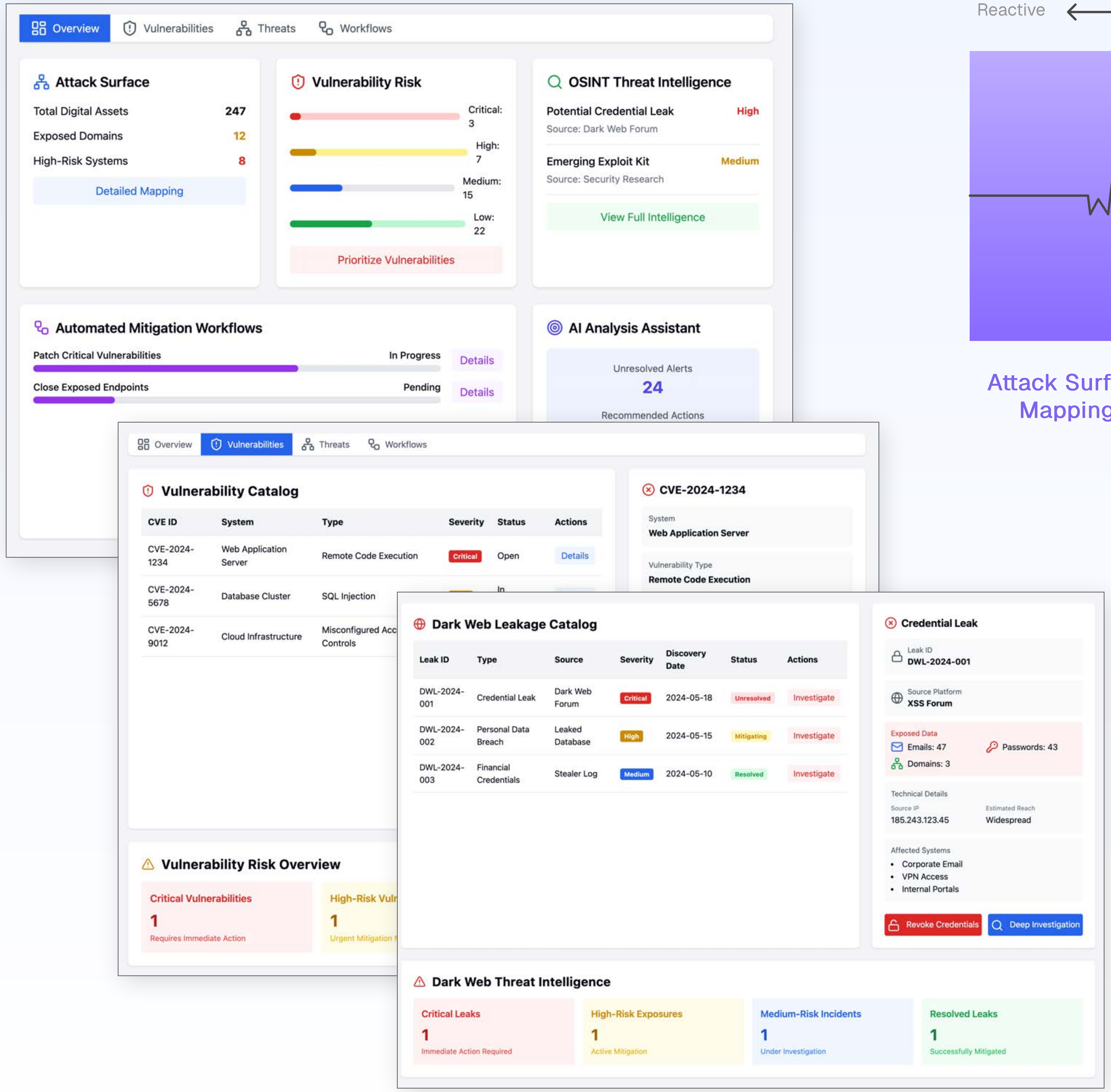
Continuous Echo

Weekly re-scans & dark-web monitoring

cygint

Digital Exposure Management Platform

Our agentic platform transforms external threat detection and response



Attack Surface

Total Digital Assets	247
Exposed Domains	12
High-Risk Systems	8

Detailed Mapping

Vulnerability Risk

Critical: 3

High: 7

Medium: 15

Low: 22

Prioritize Vulnerabilities

OSINT Threat Intelligence

Potential Credential Leak — High

Source: Dark Web Forum

Emerging Exploit Kit — Medium

Source: Security Research

View Full Intelligence

Automated Mitigation Workflows

Patch Critical Vulnerabilities — In Progress — Details

Close Exposed Endpoints — Pending — Details

AI Analysis Assistant

Unresolved Alerts

24

Recommended Actions

Vulnerability Catalog

CVE ID	System	Type	Severity	Status	Actions
CVE-2024-1234	Web Application Server	Remote Code Execution	Critical	Open	Details
CVE-2024-5678	Database Cluster	SQL Injection		In	
CVE-2024-9012	Cloud Infrastructure	Misconfigured Acc Controls			

CVE-2024-1234

System

Web Application Server

Vulnerability Type

Remote Code Execution

Vulnerability Risk Overview

Critical Vulnerabilities

1

Requires Immediate Action

High-Risk Vul

1

Urgent Mitigation

Dark Web Leakage Catalog

Leak ID	Type	Source	Severity	Discovery Date	Status	Actions
DWL-2024-001	Credential Leak	Dark Web Forum	Critical	2024-05-18	Unresolved	Investigate
DWL-2024-002	Personal Data Breach	Leaked Database	High	2024-05-15	Mitigating	Investigate
DWL-2024-003	Financial Credentials	Stealer Log	Medium	2024-05-10	Resolved	Investigate

Credential Leak

Leak ID

DWL-2024-001

Source Platform

XSS Forum

Exposed Data

Emails: 47

Passwords: 43

Domains: 3

Technical Details

Source IP

185.243.123.45

Estimated Reach

Widespread

Affected Systems

- Corporate Email
- VPN Access
- Internal Portals

Revoke Credentials

Deep Investigation

Dark Web Threat Intelligence

Critical Leaks

1

Immediate Action Required

High-Risk Exposures

1

Active Mitigation

Medium-Risk Incidents

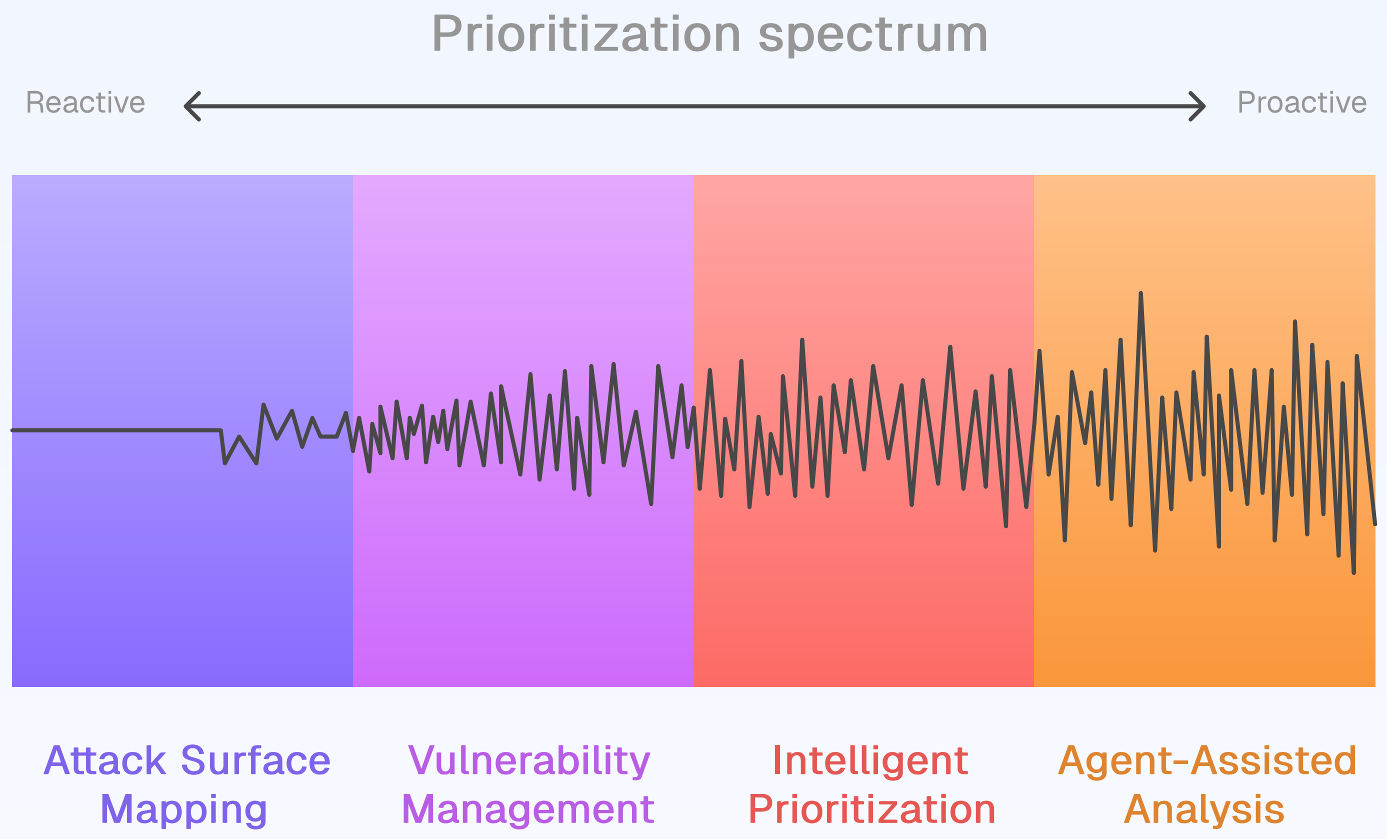
1

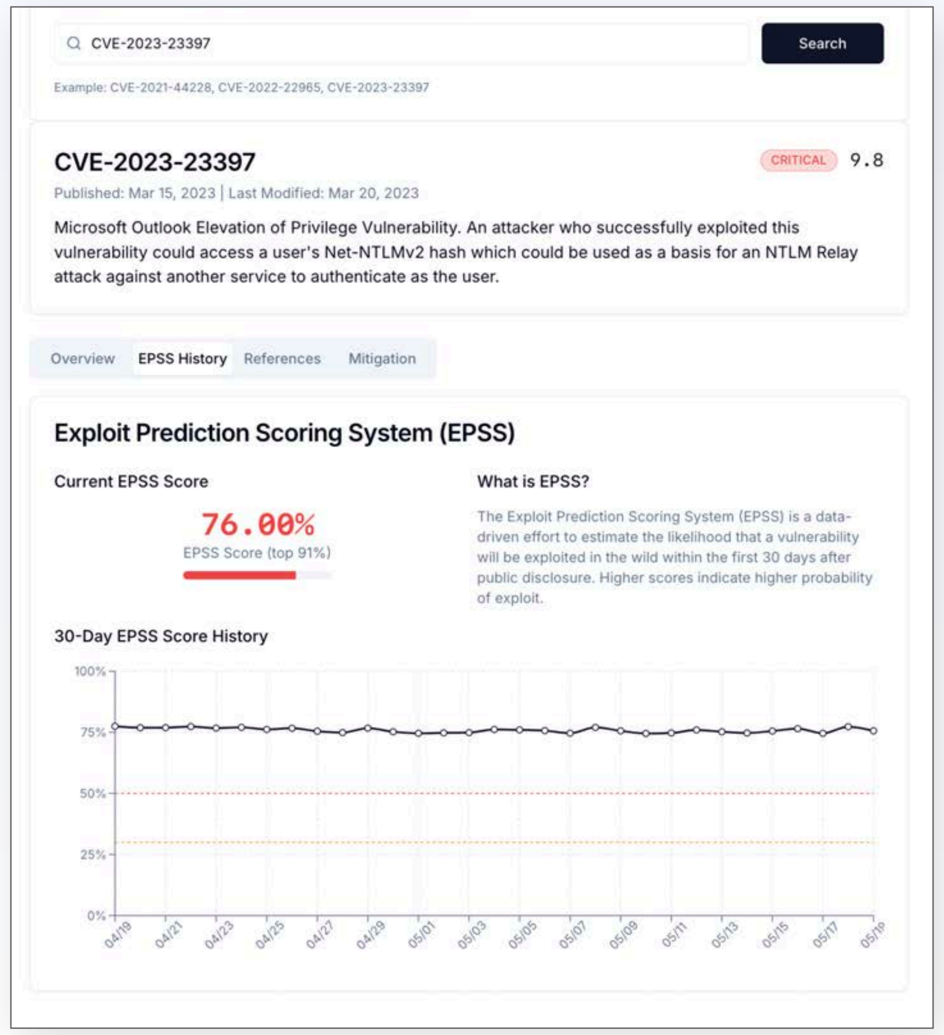
Under Investigation

Resolved Leaks

1

Successfully Mitigated





Example: CVE-2021-44228, CVE-2022-22965, CVE-2023-23397

CVE-2023-23397

CRITICAL 9.8

Published: Mar 15, 2023 | Last Modified: Mar 20, 2023

Microsoft Outlook Elevation of Privilege Vulnerability. An attacker who successfully exploited this vulnerability could access a user's Net-NTLMv2 hash which could be used as a basis for an NTLM Relay attack against another service to authenticate as the user.

Exploit Prediction Scoring System (EPSS)

Current EPSS Score

76.00%

EPSS Score (top 91%)

What is EPSS?

The Exploit Prediction Scoring System (EPSS) is a data-driven effort to estimate the likelihood that a vulnerability will be exploited in the wild within the first 30 days after public disclosure. Higher scores indicate higher probability of exploit.

30-Day EPSS Score History

- **Advanced Attack Surface Mapping**: Automatically discover and map your entire digital footprint, from IPs to domains and beyond
- **Vulnerability Management**: Continuous scanning with risk-based prioritisation to identify and address vulnerabilities before they can be exploited
- **Intelligent Prioritisation**: AI-driven risk scoring ensures you focus on the vulnerabilities that pose the greatest risk to your business
- **OSINT Integration**: Leveraging open-source intelligence to identify emerging threats before they materialise
- **Agent-Assisted Analysis**: AI-powered assistants that enhance analyst productivity and reduce alert fatigue
- **Automated Mitigation Workflows**: Streamlined processes for addressing external exposures

Credentials & Skillsets

Seasoned security professionals with varied backgrounds

- **Risk-driven approach to security management**
  It is impossible to eliminate all security threats entirely, but instead, security efforts should be targeted at reducing and mitigating the most significant risks based on their potential impact and probability of occurrence.
- **Experienced and Qualified Team**
  Background in Offensive Security Research, threat intelligence, IoT/ embedded systems security, Cloud security architecture, AI/ML Security, Enterprise Security Operations
- **Industry alignment**
  The team has worked extensively in the BFSI, Manufacturing, Telecom and Retail industries.
- **Vendor neutral**
  Vendor-neutral advisory with in-depth knowledge of solutions from major security technology suppliers

C|CISO™
Certified | Chief Information Security Officer

CISSP® Certified Information Systems Security Professional

CISM® Certified Information Security Manager® An ISACA® Certification

Information Security Management System ISO 27001 Certified Lead Auditor

International Organization for Standardization ISO 3100 Risk-Management

C|EH Certified | Ethical Hacker

OFFENSIVE® security OSCP

OffSec OSEP

Responsible Disclosures

Cygint team members have identified security vulnerabilities in 15+ brands and enabled them to secure their products and infrastructure.

ORACLE

aruba NETWORKS

TESLA

FCA FIAT CHRYSLER AUTOMOBILES

Skyscanner

Etsy

Thank you

Nilesh Chaudhari
Director, Cygint

Email: nilesh@cygint.co
Mobile: +91-9902713002