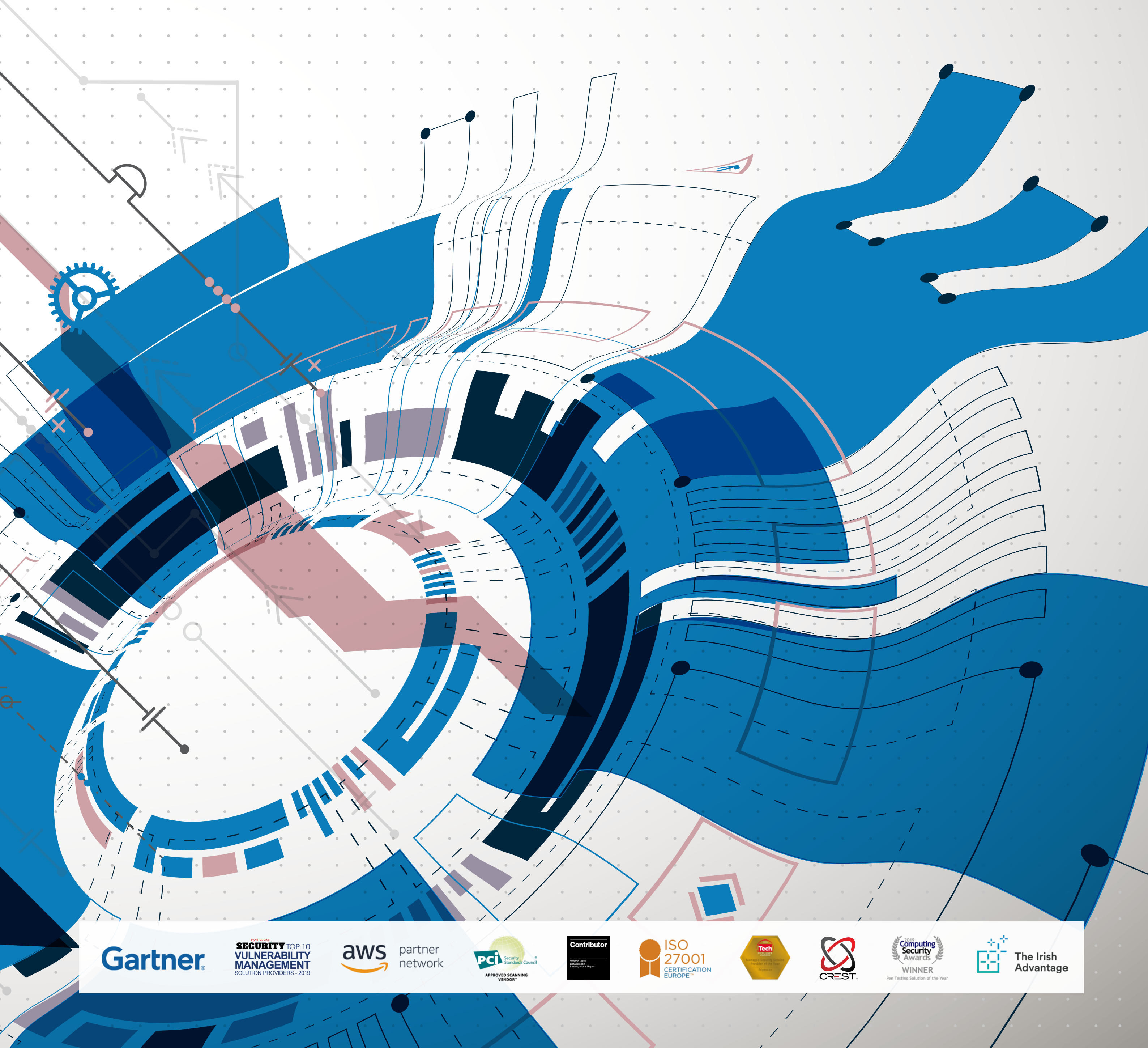
edgescan™

FULLSTACK VULNERABILITY MANAGEMENT™

The Edgescan API Journey

A COMPREHENSIVE STRATEGY TO SECURING YOUR APIs



Gartner

ENTERPRISE SECURITY TOP 10 VULNERABILITY MANAGEMENT SOLUTION PROVIDERS - 2019

aws partner network

PCI Security Standards Council APPROVED SCANNING VENDOR™

Contributor
Verizon 2019 Data Breach Investigations Report

ISO 27001 CERTIFICATION EUROPE™

Tech

CREST.

2019 Computing Security Awards WINNER
Pen Testing Solution of the Year

The Irish Advantage

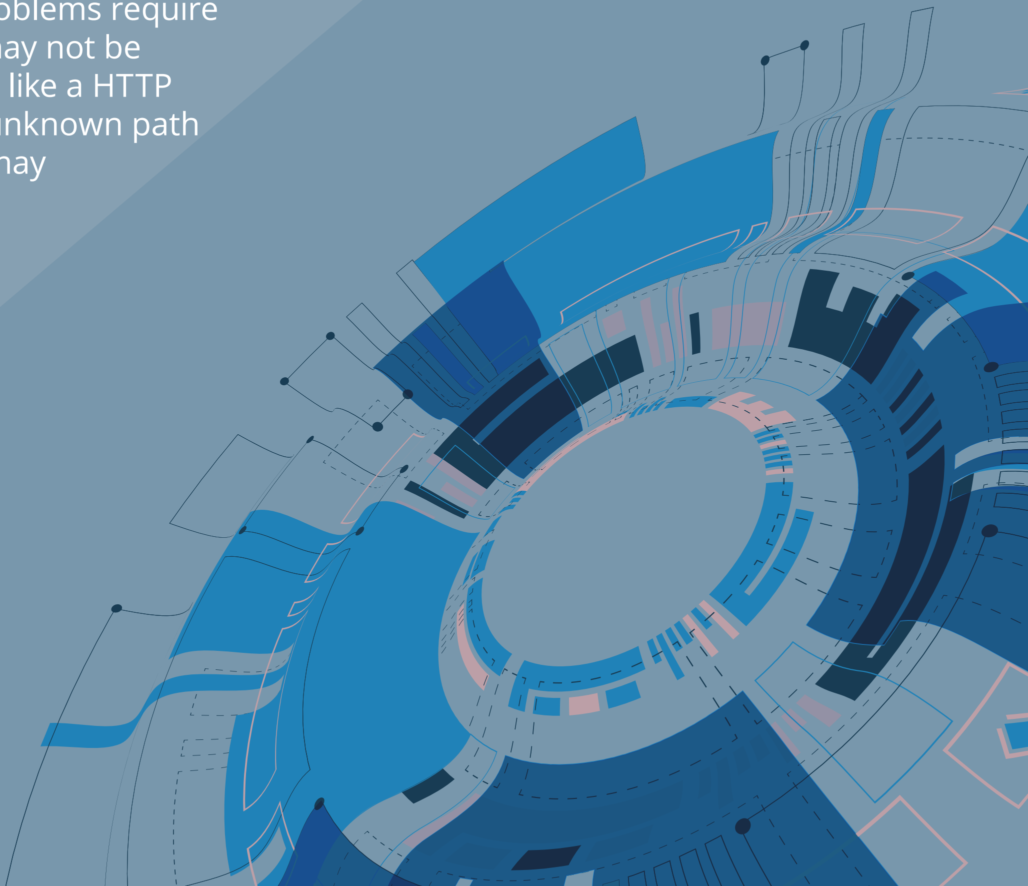
KEY PROBLEMS OF API ASSESSMENT?

- API Discovery. Continuous tracking and identification of exposed APIs across an organisation’s business estate can be difficult. Exposed APIs can lead to blind spots resulting in breach and data loss. This introduces additional risk to your business.

- API Uniqueness. Each new API represents a potentially unique attack vector into your systems. While there are similarities, API security configuration assessment is different to traditional vulnerability scanning.

- Insufficient API Threat Protection. API threat protection technology is not as mature as existing threat protection technology. Organisations need to be proactive about understanding security concerns associated with maintaining externally facing APIs.

- API Solutions. Modern problems require modern solutions. APIs may not be apparent and simply look like a HTTP service but in reality, an unknown path to business-critical data may be present.



WHAT IS EDGESCAN OFFERING?

Edgescan provides continuous API discovery and vulnerability management coupled with false-positive, free-risk intelligence.

Know your APIs, scan your APIs, test your APIs.
It's easy with Edgescan.

EDGESCAN API DISCOVERY

Find exposed APIs across an organisation's global estate.

Our **API Discovery** is part of the Edgescan Continuous Asset Profiling SaaS that allows you to understand the API topology within an estate.

With Edgescan's cataloguing and categorising correlation technology, it is possible to find the true inventory of exposed APIs and on the internet.

The proprietary discovery process runs at regular intervals across the entire estate, and reports the findings back to the end user.

EDGESCAN API VULNERABILITY SCANNING

Adopt a continuous approach to API security by running regular vulnerability scans against APIs. Include API security assessment and the creation and application of reusable API security policies.

Our **API Vulnerability Scanning** is part of the Edgescan Continuous Vulnerability Scanning SaaS that allows an ability to understand and detect security vulnerabilities with accuracy and keep pace with change.

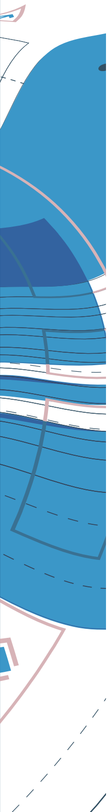
With Edgescan's security and vulnerability technology specifically designed for APIs, it is possible to have continuous security visibility of exposed APIs on the internet.

EDGESCAN API PENETRATION TESTING

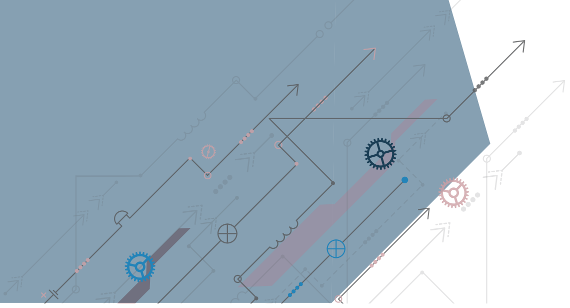
Achieve absolute confidence in the security of your APIs.

Our **API Penetration Testing** is part of the Edgescan API assessment service that allows a deep manual penetration test on an organisations's business critical APIs.

Combined with Edgescan API Discovery and API Vulnerability Scanning, it provides a comprehensive approach to securing APIs to whatever level is required.



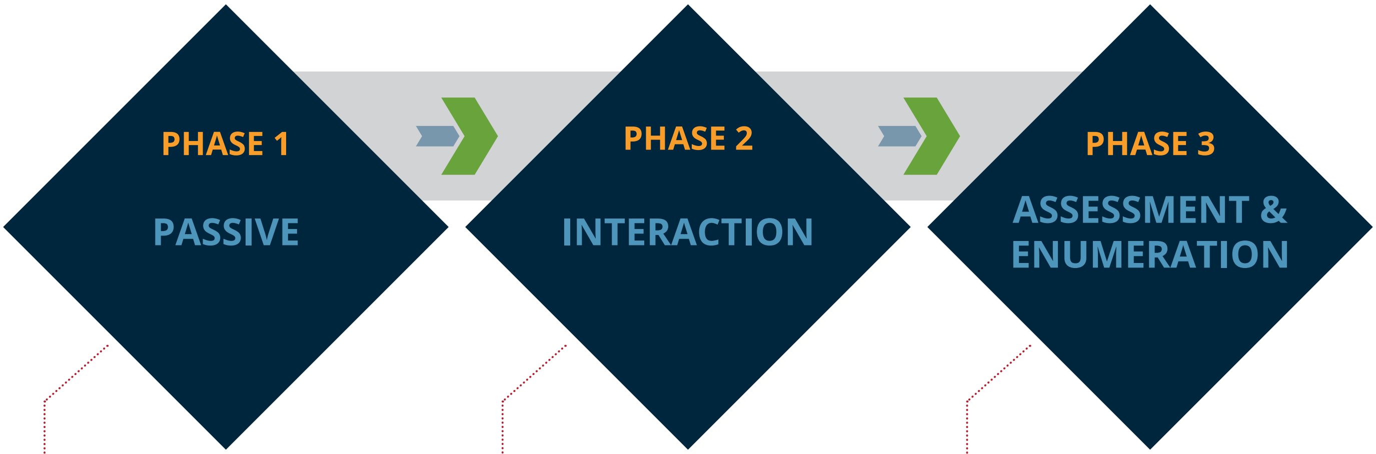
STEP 1: API Discovery



EDGESCAN PROVIDES VISIBILITY AND SECURITY

- API Discovery is part of the Edgescan Continuous Asset Profiling SaaS. It allows an understanding of the API topology within an estate.
- Our proprietary discovery process runs continuously across an organisation's entire estate, 24 hours a day, all year around.
- With Edgescan's cataloguing and categorising correlation technology, it is possible to find a true inventory of APIs and exposures facing the public Internet
- In conjunction with the Edgescan Continuous Asset Profiling service, users get real-time visibility of all hosts, services and APIs exposed to the internet.

EDGESCAN API DISCOVERY METHODOLOGY



PHASE 1

PASSIVE

PHASE 2

INTERACTION

PHASE 3

ASSESSMENT & ENUMERATION

PHASE 1: PASSIVE

Simply share the organisation's external estate with Edgescan. Edgescan will analyse the data looking for indicators of APIs.

PHASE 2: INTERACTION

Edgescan continuous asset profiler runs against all available external addresses provided. Edgescan's multi-layered checks are applied on all live services, resulting in discovery of unknown and shadow APIs.

Historically this was complex but we've cracked it!

PHASE 3: ASSESSMENT & ENUMERATION

After API discovery has been completed, Edgescan will run custom API security assessments against all live services.

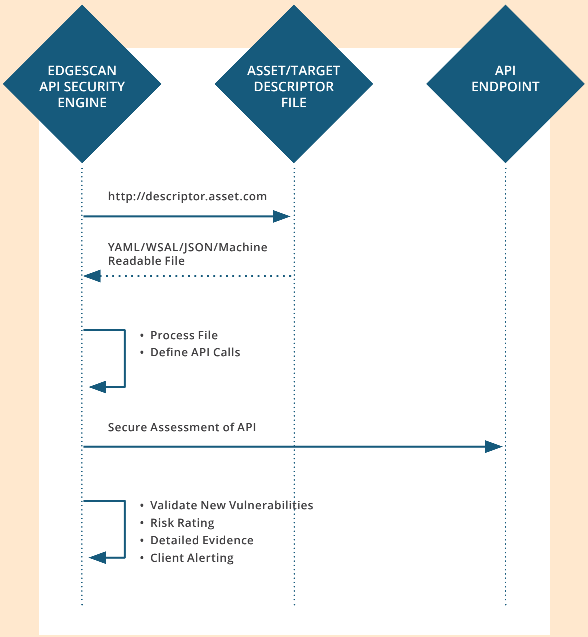
These are specific API security checks to determine the security posture of the discovered APIs.

edgescan™

HOW IT WORKS

Our multi-layered approach to discovering APIs results in a confidence interval describing if an API is actually present.

API discovery works by applying specialised probing traffic across each endpoint and evaluating the results. This multi-layered approach results in detection of APIs based on responses to the probes sent.

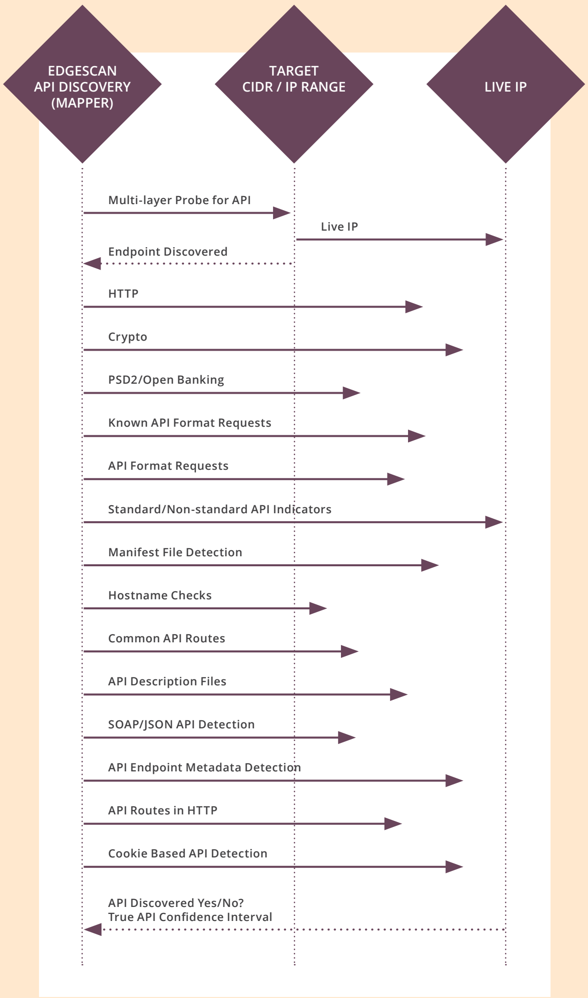

EDGESCAN API SECURITY ENGINE
ASSET/TARGET DESCRIPTOR FILE
API ENDPOINT
http://descriptor.asset.com
YAML/WSAL/JSON/Machine Readable File
• Process File
• Define API Calls
Secure Assessment of API
• Validate New Vulnerabilities
• Risk Rating
• Detailed Evidence
• Client Alerting

DevSecOps - API Assessment made easy:

- CI/CD Integration
- On demand via API or Edgescan portal
- WSDL/YAML/Swagger/JSON Metadata based API navigation
- Validated results
- “All-you-can-eat” assessments
- Fullstack coverage

Detection probes include:

- Known API format requests
- HTTP status type checks
- TLS Certificate checks
- API format Requests (SOAP/JSON etc)
- Standard and Non-Standard API indicators
- Manifest file detection
- Hostname checks
- Cert common name checks
- Common API routes detection
- API description files (Swagger/WADL)
- SOAP protocol detection
- JSON/XML response analysis
- API endpoints Metadata detection
- API routes in HTTP attributes
- Cookie based API detection



STEP 2: API Scanning

EDGESCAN SECURITY AND VULNERABILITY SCANNING

- Edgescan API Scanning is a critical part of securing an organisation's estate
- Parameters and attributes are enumerated and included in the assessment
- Edgescan technology supports most RESTful and RPC APIs
- In order to provide the greatest level of depth and rigour, it is advised that a machine readable manifest be made available to the assessments team
- This will allow legitimate use of the in-scope API to be recorded and any authentication controls to be understood

HOW IT WORKS

Our multi-engine approach to scanning APIs results in a deep technical assessment of and organisation's APIs.

DevSecOps - API Assessment made easy:

- CI/CD Integration
- On demand via API or Edgescan portal
- WSDL/YAML/Swagger/JSON Metadata based API navigation
- Validated results
- "All-you-can-eat" assessments
- Fullstack coverage

Tests are designed and configured for each endpoint.

Assessment includes:

- Broken Object Level Authorisation
- Broken Authentication
- Excessive Data Exposure
- Resource and Rate Limiting Tests
- Broken Function Level Authorisation
- Mass Assignment
- Security Misconfigurations
- Injection Based Vulnerabilities

With all Edgescan assessment we include the application/API layers as well as the infrastructure/ network layer providing vulnerability intelligence on the full stack. Edgscan's assessment taxonomy includes coverage for common API and Web application vulnerabilities including the OWASP API Top 10.*

edgescan™

*https://owasp.org/www-project-api-security/

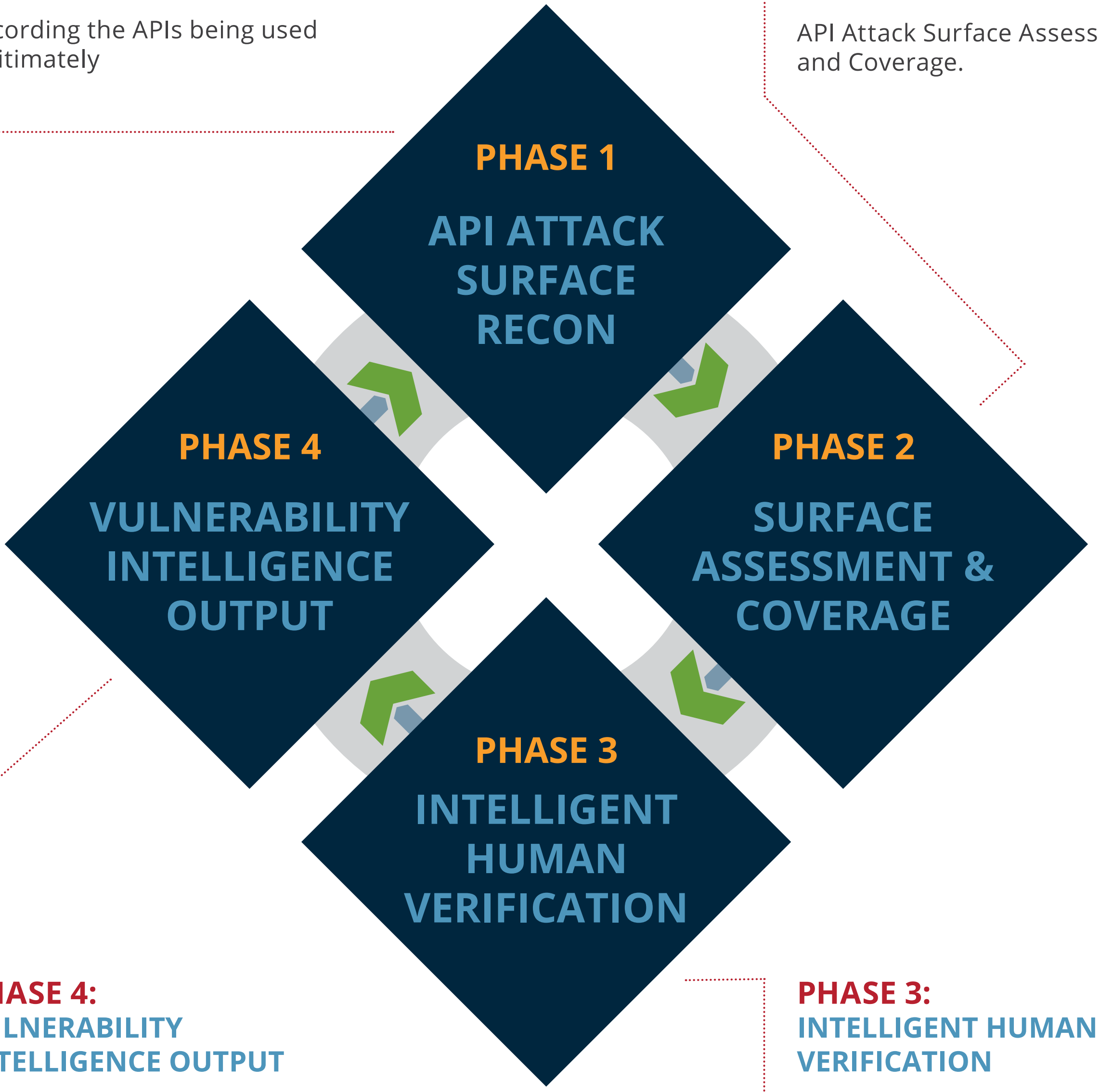
EDGESCAN API SCANNING METHODOLOGY

PHASE 1:
API ATTACK SURFACE RECON

Recording the APIs being used legitimately

PHASE 2:
ASSESSMENT & COVERAGE

API Attack Surface Assessment and Coverage.



PHASE 1

API ATTACK SURFACE RECON

PHASE 2

SURFACE ASSESSMENT & COVERAGE

PHASE 3

INTELLIGENT HUMAN VERIFICATION

PHASE 4

VULNERABILITY INTELLIGENCE OUTPUT

PHASE 4:
VULNERABILITY INTELLIGENCE OUTPUT

Reporting – integrations – vulnerability intelligence output.

PHASE 3:
INTELLIGENT HUMAN VERIFICATION

Automation and intelligent human verification. Automation for scale. Expert validation for rigour.

STEP 3: API Penetration Testing

EDGESCAN API PENETRATION TESTING

- Edgescan API scanning technology has the ability to find vulnerabilities in all types of APIs
- Edgescan's automated API scanning uses the best scannning tools to cover the parts of an organisation's APIs that are simple to enumerate
- With API penetration testing, our security experts go the extra mile for our client's most critical assets.
- Manual penetration testing allows for the full suite of tests to be performed in order to break the business logic of the application

HOW IT WORKS

- Recording the APIs being used legitimately
- Recorded requests are analysed for parameters which may result in a security issue
- RESTful HTTP requests – Parameters are examined and marked for assessment
- HTTPS: Assessment of HTTPS layer employed
- Access Control:
  - JWT (JSON Web Tokens)
  - API Keys
- HTTP Methods (GET, PUT, POST, DELETE) – Assessment is performed
- **Input Validation:** Assessment of parameters ensure Input validation is appropriate
- **Content Type:** Assessment of content types to ensure payloads can only be used as intended
- **Error handling:** Detection of error response codes ensure no data leakage.
- **Security Headers:** Check to see if correct content type headers are employed.
- Technical Vulnerabilities are discovered with Edgescan Automation. Typical examples are Injection attacks (XML, SQLI, RCE, CMDI, XXE)
- Swagger enabled API's

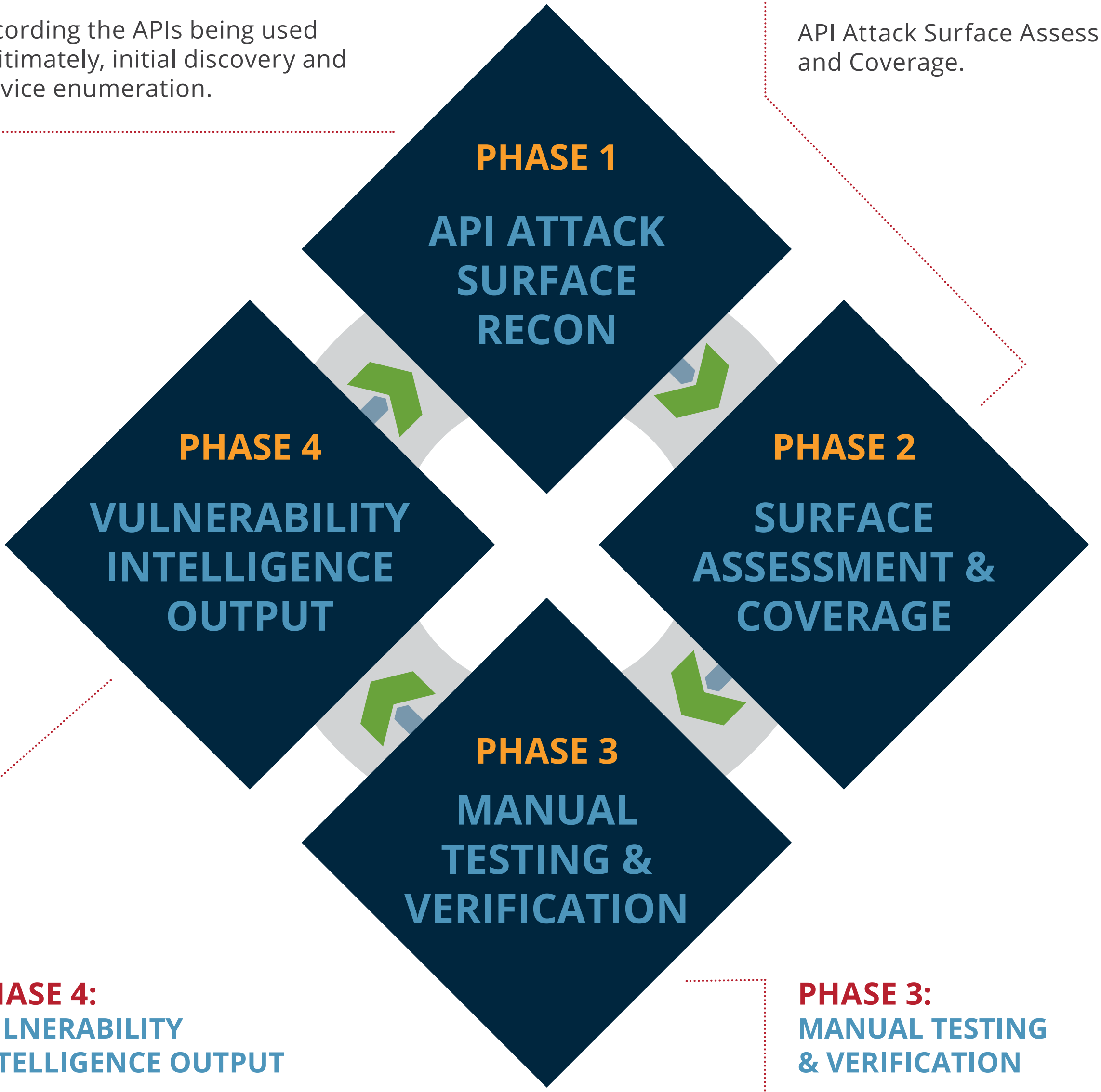
EDGESCAN API PENETRATION TESTING METHODOLOGY

PHASE 1:
API ATTACK SURFACE RECON

Recording the APIs being used legitimately, initial discovery and service enumeration.

PHASE 2:
ASSESSMENT & COVERAGE

API Attack Surface Assessment and Coverage.


PHASE 1
API ATTACK SURFACE RECON
PHASE 2
SURFACE ASSESSMENT & COVERAGE
PHASE 3
MANUAL TESTING & VERIFICATION
PHASE 4
VULNERABILITY INTELLIGENCE OUTPUT

PHASE 4:
VULNERABILITY INTELLIGENCE OUTPUT

Reporting – integrations – vulnerability intelligence output.

PHASE 3:
MANUAL TESTING & VERIFICATION

Automation and Manual Verification. Automation for scale. Expert validation for rigour.

SERVICE DEFINITIONS

EDGESCAN API DISCOVERY

Our **API Discovery** is part of the Edgescan Continuous Asset Profiling SaaS that allows an understanding of the API topology within an estate. With Edgescan's cataloguing and categorising correlation technology, it is possible to reveal the true inventory of APIs and exposures on the internet. The proprietary discovery process runs at regular intervals across the entire estate, and reports the findings back to the end user.

EDGESCAN API VULNERABILITY SCANNING

Our **API Vulnerability Scanning** is part of the Edgescan Continuous Vulnerability Scanning service that allows an understanding of common security vulnerabilities which may be present throughout an estate. With Edgescan security and vulnerability scanning engines specifically designed for APIs, it is possible to have continuous security visibility of your API exposures on the internet.

EDGESCAN API PENETRATION TESTING

Our **API Penetration Testing** is part of the Edgescan API Testing service that allows you to get a deep manual penetration test on your business critical APIs. Combined with Edgescan API Discovery and API Vulnerability Scanning, it provides a comprehensive approach to securing your APIs to whatever level is needed.

edgescan™

FULLSTACK VULNERABILITY MANAGEMENT™
www.edgescan.com

IRL: +353 (0) 1 6815330
UK: +44 (0) 203 769 0963
US: +1 646 630 8832

Sales and general enquiries:
sales@edgescan.com

@edgescan