

Enterprise IT and cloud environments are changing rapidly with addition of servers, laptops, wireless devices, web applications and cloud services almost on a daily basis. Software vendors are continuously releasing new versions of software and patches. New types of attacks and vulnerabilities are being uncovered continuously. It is difficult to keep up with all of this and ensure that the network, devices and web and cloud applications are not vulnerable to costly security compromises.

We recommend continuous monitoring and vulnerability management through a service such as Ebryx Detection and Response Services as a best practice. However, organisations at times need a clearer picture of their current security posture before opting for a SOC service. We strongly advise such customers to start with security assessments to identify critical gaps and address them immediately.

## Services Overview

Ebryx Security Assessment Services help you understand your current cybersecurity risk exposure throughout your organization. Besides the assessment of risk you get recommendations to remediate the vulnerabilities and threats. The service is based on industry best practices including NIST and SANS guidelines.

Our services cover the following components of your IT environment:



Depending on the customer requirement we can assess any one or all of the components of their IT environment.

Our security professional services include:

### Cybersecurity Policy Review

- Network and System configuration review
- Data protection policy
- Access control measures

### Security Architecture Review

- Defence-in-depth
- Logical segregations
- Evaluate security controls against business requirements

### Penetration Testing

- Identify and understand vulnerabilities in internal and external environment
- Simulate actions of a malicious actor targeting infrastructure, applications and third party connections

### Application Security Testing

- Secure your applications through static and dynamic security analysis

## Flexible Engagement

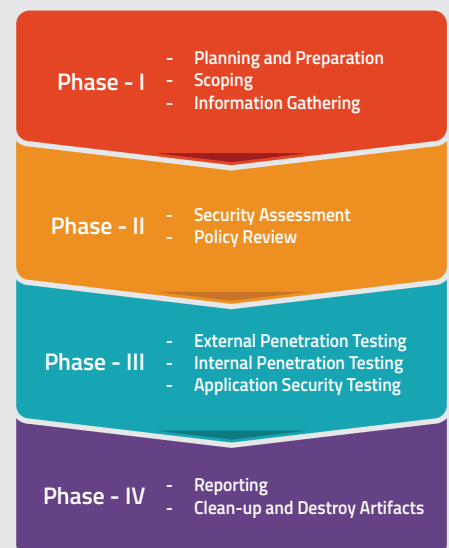
Customer can opt for an in-depth or a limited engagement depending on their requirement and budget.

### Enterprise Security Assessment

A comprehensive review of your IT environment to assess a system's configuration, security policy and architecture followed by vulnerability assessment and penetration testing. Our deliverables include detailed findings, list of recommendations and implementation guidelines.

## Our Methodology

The project management methodology followed by our team consists of the following phases:



### Penetration Testing

A limited engagement comprising vulnerability assessment of the environment followed by external penetration testing. Our deliverables include list of vulnerabilities, exposure to threats and attacks, and remediation guidance.

Service Feature	Penetration Testing	Enterprise Security Assessment
Scoping	✓	✓
Vulnerability Scanning	✓	✓
External Penetration Testing	✓	✓
Internal Penetration Testing	—	✓
SAST and DAST Analysis	—	✓
Security Policy Review	—	✓
Gap Analysis	—	✓
Configuration Review	—	✓
Business Logic Flaw Testing	—	✓
Risk Assessment	✓	✓
Assessment Report	✓	✓
Recommendations	✓	✓

### Service Delivery

Our services can be customized based on client requirements. This can be conducted for the whole IT environment or a specific component of it. You can avail the service on a one-time, periodic or continuous basis.

## Key Features and Benefits:

#### No Hassle:

- Zero disruption to operations during security assessment activity
- Scans can be scheduled to further ease operations

#### Great Value:

- Experienced team means recommendations are actionable with great impact on client's IT security
- Our team works with client IT team to further strengthen the security posture with technology and expertise

#### Best Practices:

- Technology and techniques used by our team are in line with global best practices and guidelines including NIST, PTES and OWASP

#### Compliance:

- Enterprises working in sectors where regulatory compliance mandates vulnerability assessment our service helps you meet this requirement

## Why Ebryx?

### Our Team

Ebryx has deep expertise in cybersecurity. Our team of security analysts is well-equipped through renowned industry certifications like GIAC Reverse Engineering Malware (GREM), GIAC Certified Forensic Examiner (GCFE), GIAC Certified Intrusion Analyst (GCIA) & Offensive Security Certified Professional (OSCP).

### Strong R&D Background

Our research and development services power some of the world's leading security products. We have contributed to several patents on malware classification and have been the first to uncover malware in consumer applications and services offered by some of the world's top companies.

### Clients and Partners

Some of the world's leading tech companies are using our services to help them improve their security posture. We are also value added resellers and implementation partners to some of the most innovative security tech companies around. These capabilities enable us to become your primary security partner.

### SMB Focused

One of our key value propositions is our focus on the SMB segment. We are sensitive to the budget constraints and the need to get the most out of limited resources. Our goal is to enable you to achieve robust security without putting you under undue financial strain.