



Security Assessment Services

Prepared by: Gani Riasudeen | eCyLabs

Executive Summary

Reducing the attack surface is crucial for any businesses navigating the challenges in the cloud era.

We, at eCyLabs, are committed to assess your overall status of cybersecurity readiness and guide through the remediation workflow.

This proposal outlines our services, approach, and the value we can bring to your organization.



Best,

Gani Riasudeen

Managing Director @ eCyLabs



Why eCyLabs?

Our Pentest product is special because it combines automatic scanning with expert advice like no other. [**Continuous vulnerability scanner + AI + Human Expert**]

- **Cloud Platform and AI**

The platform aggregates system findings to present a holistic view of organization-wide security status. You can manage discovered vulnerabilities, Prioritize the risks, AI Assisted patching and Risk Remediation workflow.

- **360 Degree Assessment**

Traditional vulnerability scanners are outdated. Modern applications are collection of services and our Toolkit provides security posture from code to cloud.

- **Compliance Dashboard**

Non-compliance can result in legal consequences and reputational damage. Compliance Dashboard helps to validate your status against various security standards.

- **Cybersecurity Expertise**

Best in Class Support. Get real time assistance from Security experts. Expertise is crucial for cyber security assessments and our team brings the benefits of security expertise from Global Enterprises.

Service Offering 1

Web Application Penetration Testing

- The Web Application Assessment can include scanning, testing or both.
- The test provides a deep security look at an application, which is of particular interest to a Customer.
- Dashboard provides organization wide security status across all the applications
- Vulnerability Assessment on all open ports
- Penetration testing for Web applications against the OWASP Top 10
- Crypto Flaws and PKI issue detection for SSL/TLS used in WebApps
- Code Scan to detect security gaps in open source libraries in the Project.
- URL Integrity, Broken Links, Blacklist and Malware Detection for URLs
- AI Model can help you with remediation and patching best practices.



API Penetration Testing

- OWASP API Top 10 Detections include scanning, testing or both.
- Upload your REST API Spec Files to provide deep inspection
- Dashboard for organization wide security status across all the applications
- Smarter Vulnerability Management
- Crypto Flaws and PKI issue detection for SSL/TLS used in WebApps
- Code Scan to detect security gaps in open source libraries in the Project.
- URL Integrity, Broken Links, Blacklist and Malware Detection for URLs
- AI Model can help you with remediation and patching best practices.



Service Offering 3

Cloud Security Assessment

- Our team of security experts conducts a comprehensive evaluation of your cloud security posture, examining internal practices to ensure adherence to best standards and assessing external defenses to safeguard against potential hacker threats.
- We assess and compare your cloud components security to industry benchmarks such as CIS benchmarks and OWASP, ensuring a thorough evaluation and adherence to globally recognized standards for robust security measures.
- We conduct a baseline security assessment by creating a standardized build configuration checklist, Our guidance includes implementing hardening methods in accordance with industry best practices.



Service Offering 4

Compliance Assessment & Advisory Services

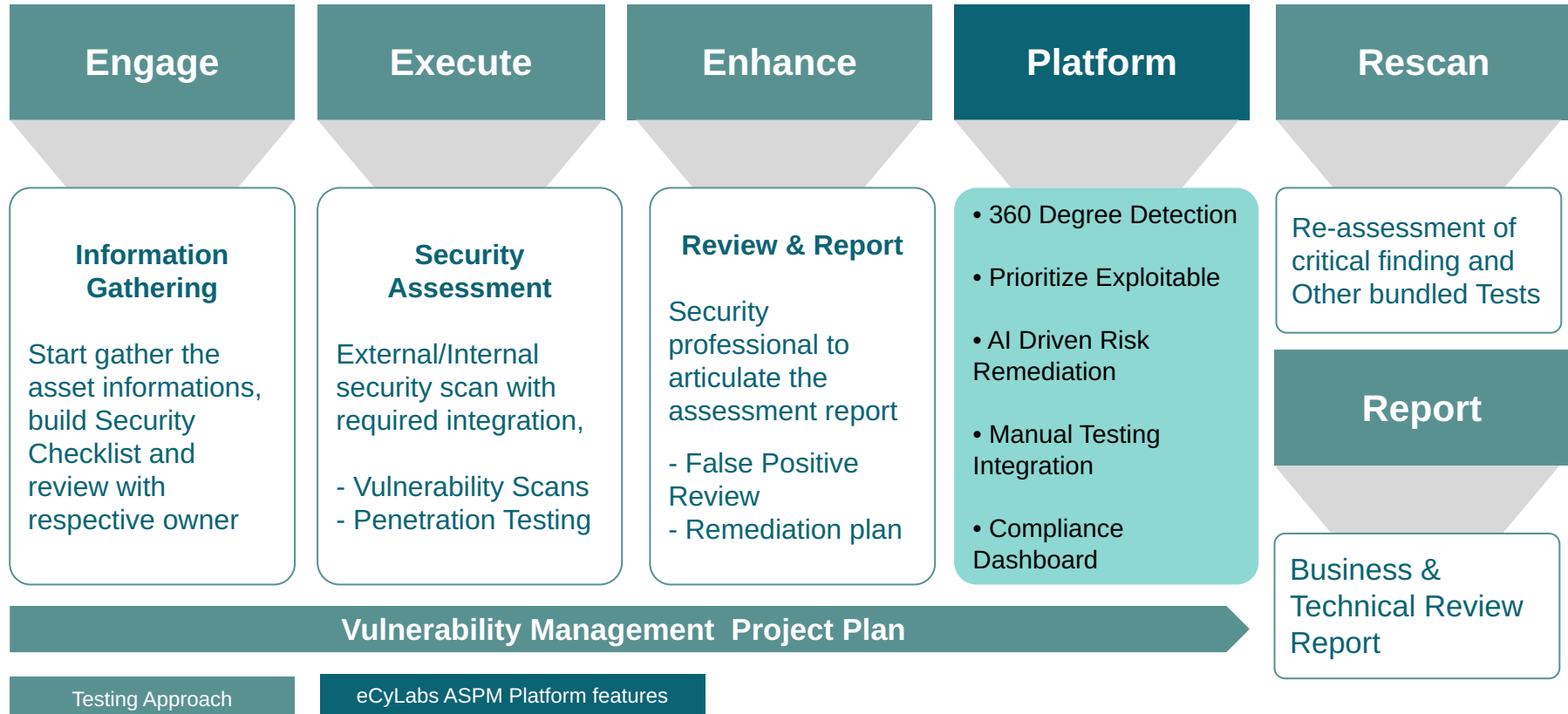
- **ISO 27001:2022 Readiness Assessment**

Our security experts guide you from audit readiness to final report so you get the assurance you deserve. Streamline ISO 27001 Certification Readiness with Robust Internal Auditing Procedures.

- **PCI DSS Readiness Assessment**

We benchmark your current processes and controls against the PCI DSS requirements so you can implement the proper processes and policies prior to the on-site assessment.

Our Approach



Refer to [Annex A](#) for more details about **How it Works**



Thank You!

We look forward to the opportunity to provide you with our Security Services. If you have any questions or require further clarification, please don't hesitate to contact us.



enquiry@ecylabs.com



+91 422 4959849



<http://www.ecylabs.com>



Annexure



Annexure A - How it Works



First step is to understand your application stack and your compliance requirements.

Onboard Application and its components to the Platform. [Read More](#) about ASPM Platform



Start Assessments with wide range of AppSec testing solutions. It includes Automated and Manual Testing methodology as many of the elements needs security expert attention.



Communication to Stakeholders for the vulnerabilities and the informations collected about application security risks and advisory to optimize an organization's application architecture.



Provide guidance to the technical team to **Prioritize and Remediate** the issues from code to the cloud by maximizing the effectiveness of a vulnerability management program.



We will act as Virtual CISO to **Continuously Monitor Application Security Posture** on mutual consent and ensure your application and organization is protected from Cyber Attacks.



Annexure B

Customer Responsibilities

- Remediation of vulnerabilities and fixing security misconfigurations identified
- Provide us with administrator or root-level access when required for some assessment.
- Ensure the availability of testing environments and obtain all required Change Management approvals for the tasks to be performed by eCyLabs
- External: Allow the traffic originating from the scanner (If required)
- Internal testing requires system from customer. We recommend the Ubuntu Linux VM OR Allow our remote access/funnel the data over the VPN interface.
- eCyLabs Support Coverage Encompasses 'Remote Location' and Operates on a 8x5 Basis During IST Business Hours. Modifications of Support Coverage can be discussed.

Annexure C



Tools & Technology

eCyLabs Vulnerability Management Platform

- **Cloud Platform**

eCyLabs Security Platform to provide 360 degree detection of your security posture from code to cloud.

- **AI Assistant**

AI Assistant in our Platform can help you with remediation steps and patching best practices.

- **Compliance Dashboard**

Compliance specific Dashboards with clear visibility and metrics for threat mitigation.

- **Exploitability Index**

With Exploitability Index, you get insight about how likely the vulnerability will get exploited and prioritize the items that demand immediate attention.



Refer to [Annex D](#) for more details about **Key Benefits** to your business

Annexure D

Key Benefits

- Identify known security exposures before attackers find them. **Assesses your security risk level**
- Establish a business risk/benefit curve and **Optimize security investments**
- Play a vital role in streamlining the **Cyber Insurance** underwriting process and offer more favorable rates.
- Achieve and maintain **Compliance Requirements** without duplicating efforts or incurring unnecessary costs.

