



Application Security Posture Management

Redefined security solution for modern application architecture.

ecylabs.com

enquiry@ecylabs.com

in.linkedin.com/ecylabs



eCyLabs ASPM Overview

eCyLabs is a Security Advisory and Consulting firm that brings the benefits of security expertise from securing the **Global Enterprise Applications**.

Application Security Posture Management service is focused on securing the applications and its architecture. eCyLabs will act as a responsible service provider to implement your application security to ensure applications are protected from Cyber Attacks.



ASPM Platform

Application Security Posture Management provides 360 degree view of application security posture from code to cloud. It is designed to automate application security processes within an organization.



Managed Services

eCyLabs **Managed Security Services** are provided by knowledgeable professionals with deep expertise on application security. We provide security solutions as a integral part of your organization.

Danger of Outdated Security Solutions



Recent attacks are around the third-party integration of cloud applications



Traditional vulnerability scanners are outdated and they were invented before cloud era.



New solution required to Secure collection of services in Modern application architecture.

How to Secure Web from code to cloud ?



**Application
Security Posture
Assessment
Services provides
360 degree view
of application
security posture
from code to
cloud.**



Detection Logics in ASPM v1

Automated

Manual

Web Architecture

- Blacklist Detection
- DNS / FW Status
- Access Control
- Risk Ports
- Domain Security
- Web Vulnerabilities

- Architecture Review
- Firewall Audit
- Third Party Review
- SSO Audit

Application Services

- Malware Infection
- Broken Links
- Code Analysis
- URL Integrity
- Crypto Flaws(ssl)
- Load Time and More

- Database Security
- Dependency Mapping
- Baseline Compliance

OWASP Top 10 for Web & API

- Injection Attacks
- Broken Authentication
- Data Exposure
- XSS and XXE
- Security Misconfigurations
- Insufficient Logging
- API Vulnerabilities
- API Authorization
- API Encryption
- Improper Assets and More

Regulatory and Compliance

Validate the Application against **PCI-DSS, HIPAA, NIST, CIS** and More

Server Hardening against compliance requirements for variety of baselines.
(Windows, Linux and More)

Detect gaps in open source libraries in the Project.

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.

Connect with our Security Advisor & Get Started



<https://ecylabs.com/calendar>



enquiry@ecylabs.com



<https://lnkd.in/gaEe6G29>



+91 4224959849

Thank You!

