Cybrella AppSec as a Service

VIP Cyber Crime Mystery Thriller

Nov 2021
Objectives

Cybrella Application Security Introduction

Cybrella Application Security Value Proposition

Next Steps - Enablement
Application security from the design stage

- It is known that identifying and fixing security vulnerabilities late in the development process cost much more than earlier identification.
- According to IBM, the cost of identification of security bug can even cost 100 times more when identification in maintenance stage rather than in earlier design stages.
- On average, over 70% of the IT security budget is spent on Infrastructure, yet over 75% of attacks happen at the Application level.
- According to Microsoft Research, only 1/3 of developers are confident that they write secure code.
AppSec – Cybrella Approach

Integrate Security into Your Product DNA

Cybrella's application security teams help the DevOps in any stage of the lifecycle that the application is in, from design/architecture to deployment.

Cybrella's applications security experts with a background in developing and coding in broad types of applications and domains - Web, Cloud, Mobile, IoT, Embedded, etc.

Cybrella works closely with the DevOps team to educate them in developing secure applications. We also build the controllers and assess the systems to identify and mitigate vulnerabilities and keep our clients' apps' confidence and one step ahead of the hackers.
Effective AppSec Program

Based on OWASP Open SAMM 2.0

SOFTWARE DEVELOPMENT

GOVERNANCE
- Strategy & Metrics
- Education & Guidance
- Policy & Compliance

CONSTRUCTION
- Threat Assessment
- Secure Architecture
- Secure Requirements

VERIFICATION
- Design Review
- Security Testing
- Implementation Review

OPERATIONS
- Issue Management
- Operational Enablement
- Environment Hardening
The Journey building the Secured Product by NIST

01 Requirements

Product Security Requirements
- Classify Application Business Risk (1-3)
- Establish Security Requirements
- Create Quality Gates / Bag Bars
- Security & Privacy Risk Assessments

02 Design

- Threat Modelling
- Analysis Attack Surface

03 Implement

- Implementation
  - Deprecate Unsafe Functions
  - Security Tests Based On Business Risk Classification
    - Static Analysis
    - Open Source Analysis
    - DAST
    - IAC
    - Containers

04 Verify

- Verification
  - Pentest
  - Attack Surface Review
  - CSPM

05 Release

- Release
  - Incident Respond Plan
  - Finale Security Review
  - Release Archive

06 Recover

- Recover
  - Recovery Planning improvements
  - Communications
Building SAST Program

Kick-Start – First Product/Project [6-8 Weeks]
- Information gathering
- Configure Users & Policies
- Initial Project onboarding
  - SDLC Integration
    - Architecture Review
    - Reporting Integration
    - Ticketing Integration
    - Training

For each project:
- Threat modeling + Architecture review
- Code Review
- Results review
- Results clean up
- Mitigation advice
- Rules tuning

Ongoing Support
- Consulting advised
- QBR quarterly
- Dedicated delivery manager – Weekly calls
- Results Review
- KPI Review
- Activity Reports

Program Management

POV

Discover
Integrate
Roll Out
Adoption

Continuous AppSec Improvement [Rest of the contract period] – Product/Month

Cybrella Cybersecurity Experts
Decentralized Approach – Key Players

- **AppSec Manager**
  - GRC
  - AppSec Expert
  - Security Architect
  - DevSecOps

**Sales/Product**
- Drive new Requirements

**Product Unit**
- Dev Team
- Security Champion
- Dev Team

**Product Unit**
- Dev Team
- Security Champion
- Dev Team

**Product Unit**
- Dev Team
- Security Champion
- Dev Team

**Product Unit**
- Dev Team
- Security Champion
- Dev Team

**Support for new Designs**

**Software Architects**

**System Architects**
Executive Directive and Alignment

Business Requirements
- Compliance
  - SOC2/ISO27001/GDPR
- SLA
- Liabilities

Prepare a Plan to address the Risks and Needs
- SDLC Program
- SecOps
- Compliance Standards (ISO/SOC2)

Management Alignment
- Set clear Policy to follow
- Assign Security Champion Program
- Resources and Budget
- Implementation & Execution
- KPI Tracking
Summary

Organizations accelerate to secure SDLC
Trusted partner to facilitate your security requirements

Experts in coding languages and frameworks
On hand to ensure your AppSec program is successful

Align with CI workflow without delays
Developers focus on security vulnerabilities and remediation

Developer Assistance on-demand
Remediate vulnerabilities earlier

Rapid ramp-up, setup and deploy
Fast-track your AppSec program
Contact us:

📍 Prudential Tower, 800 Boylston St., 16th Floor, Boston, MA 02199
📞 Tel: +1 857 453 6660 | Mobile: +1 857 636 1332
✉️ info@cybrella.io

Follow us on:

🔗 linkedin.com/company/cybrella
殛 facebook.com/cybrella
�性 @Cybrella_Cyber
_mail cybrella@gmail.com