
appFORT
Application Security
on appFORT
www.castellumlabs.com

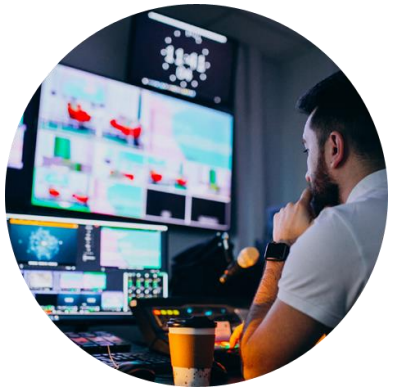
# About Us

**Rajeev Shukla, Founder**

- 25 years building IT products
- Leadership roles in Sun, CA, Quark and more
- Wide experience across US, India and Europe
- Founded Castellum Labs over three years back
- Commercially successful product/service portfolio

**Portfolio**

- Application Security & Governance
- Threat Intelligence & Threat Management
- SOC Monitoring (Managed Detection & Response)
- Cloud Security Solutioning and Cloud Security Operations



**Foundation for Design**

- Reporting is not Monitoring
- Data breaches don't hurt as much as ignorance
- Short-term service engagements deliver no real value
- Cybersecurity needs far more human intelligence than expected

watchOUT
Darkweb Monitoring

threatNIXD
Next Gen SOC Monitoring

appFORT
Continuous Application Security

# Manual VAPT: Meaningless, Noisy & Repetitive

*Adoption of CI/CD is taking place …*

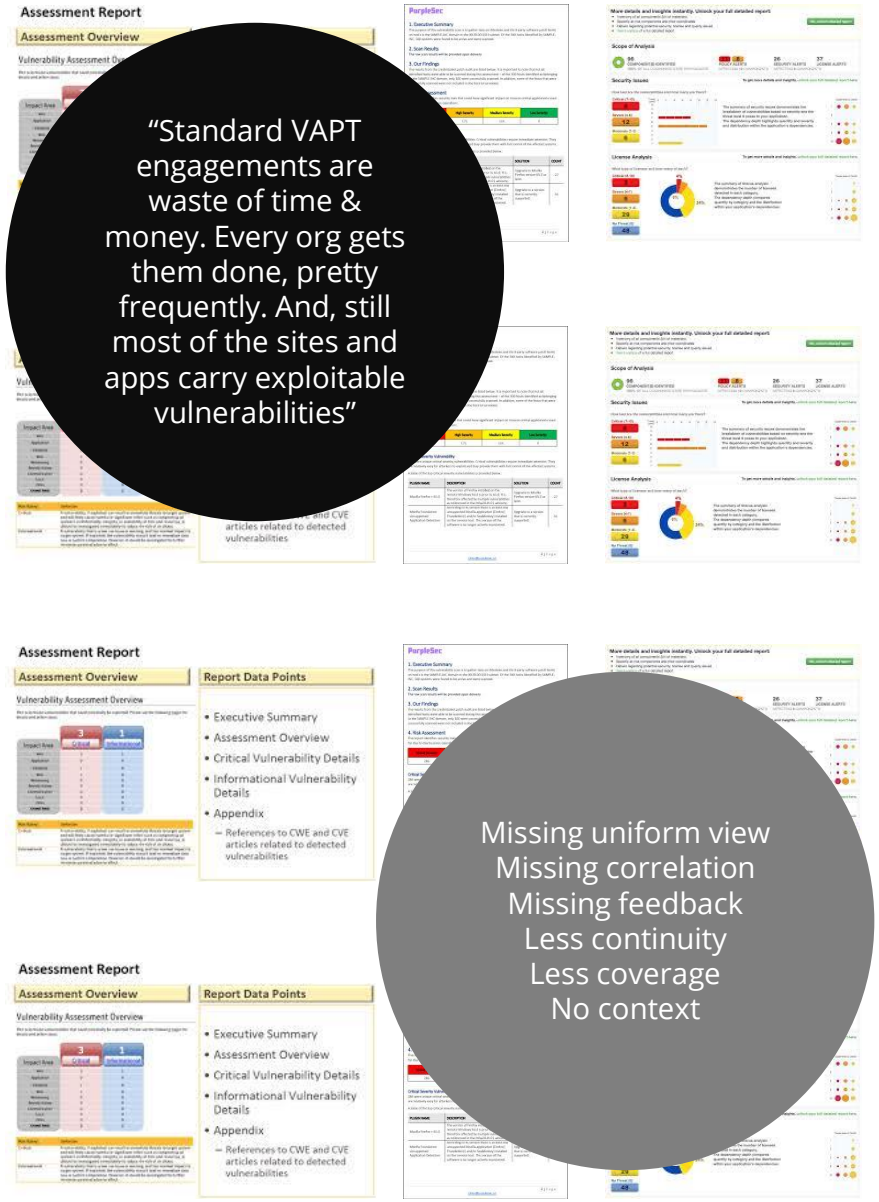
*"Rapid Release Cycle of Apps at Enterprise Customers"*

*With manual security testing such as VAPT*

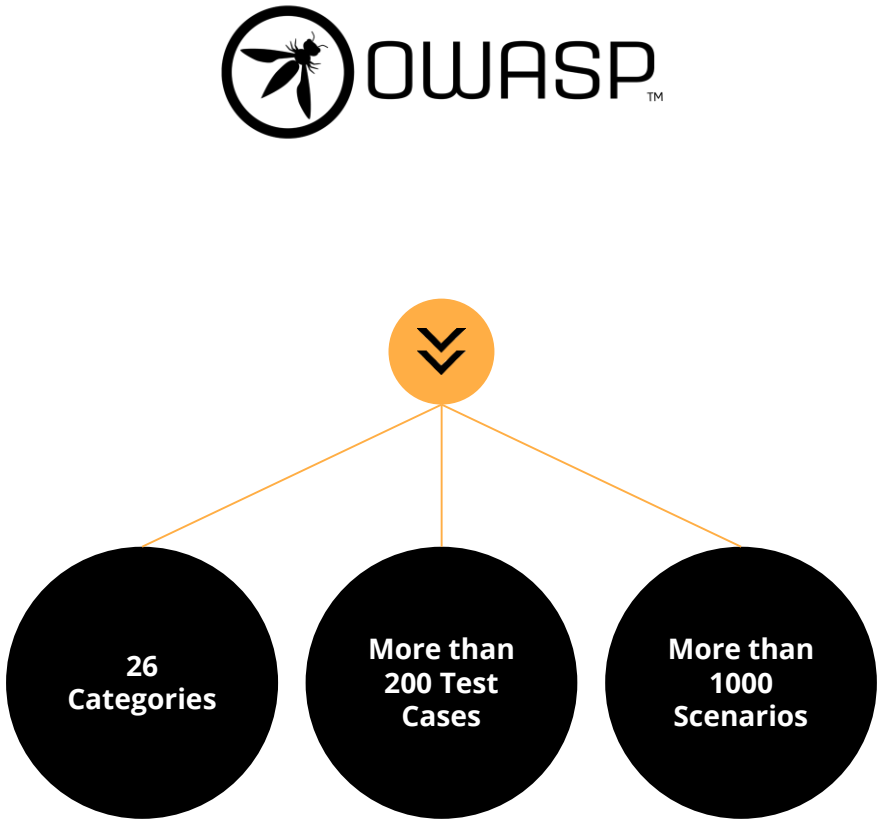
*"Limited Security Testing through Releases is Possible"*

*Tool based VAPT of software leads to*

*"Surface Risk Exposure Visibility is Unclear and Limited"*



# 360-Degree Security




- Penetration Testing (SAST / DAST / IAST)
- Software Composition Analysis (Libraries, Open Source Vuln)
- Code Scan & Code Review (Manual and Automated Scans)
- Design Security Assessment (Selective Security Components)
- Application Data Security Review (Database & Data Security)
- Container and Server Hardening (Config, Vuln & Run Time Hardening)

**Mobile**
iOS
Android
Abstracted Platform
HTML 5 & Native Applications

**Web Applications**
Java & .Net
Angular JS and Node JS
PHP and PHP Frameworks
Middleware Frameworks

**APIs**
SOAP
XML-RPC
JSON-RPC
REST

# AppSec Framework


## Comprehensive

- *Exceptional scenarios*
- *Threat modeling of apps*
- *Multi layer testing framework*
- *AppSec methodology risk reduction*

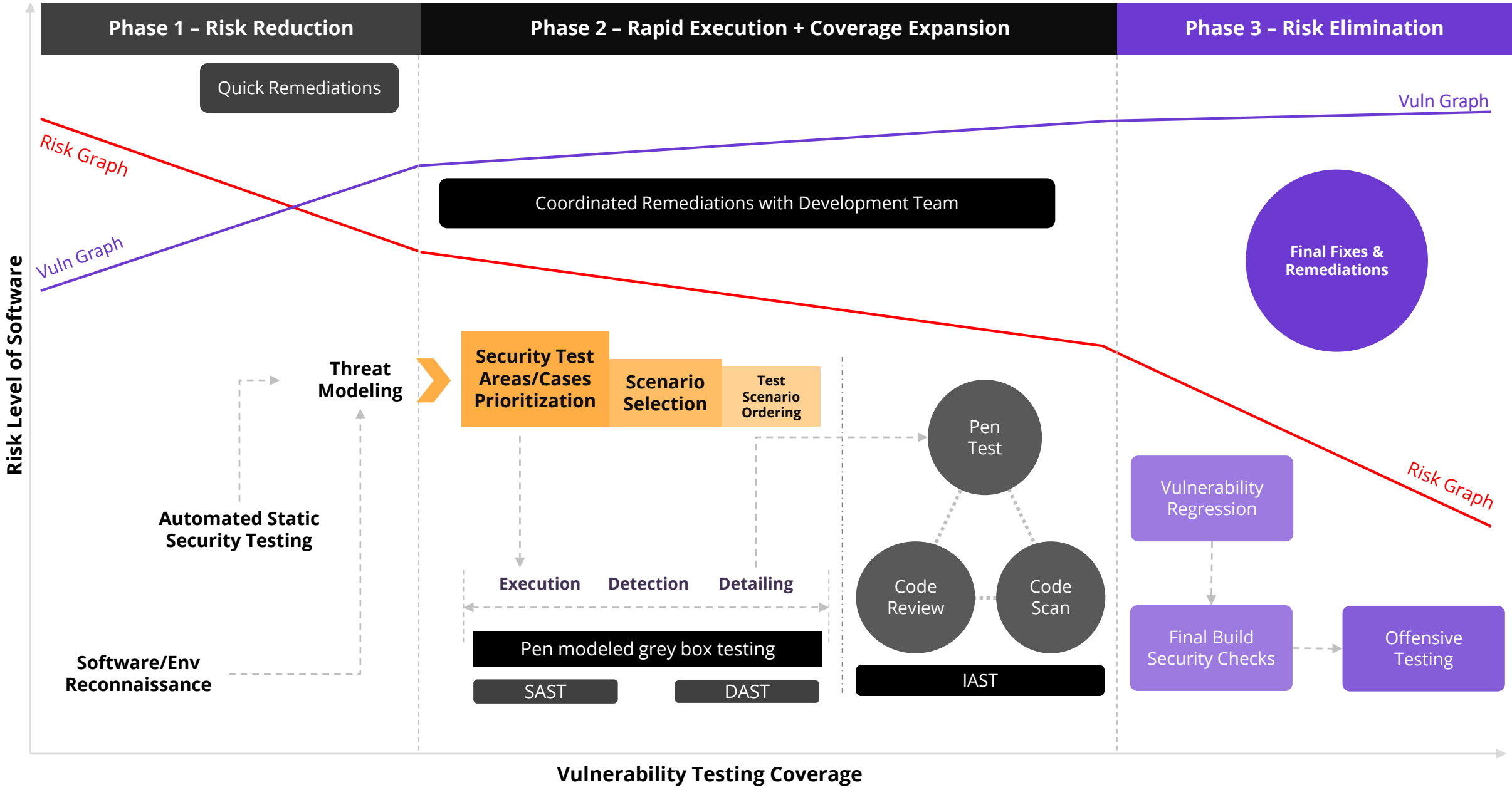
## Inline Continuous

- *Designed continuity*
- *Across releases issue visibility*
- *Continuous app security execution*
- *Covering multiple apps release trains*

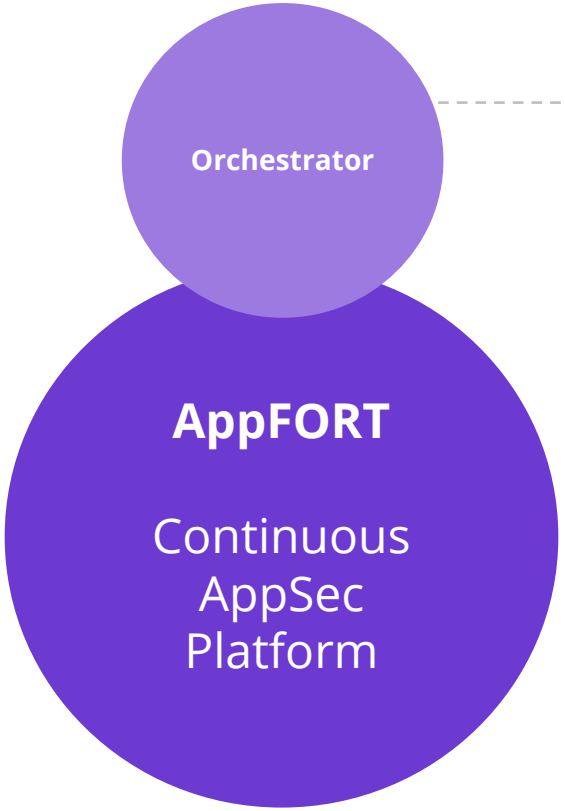
## Automated

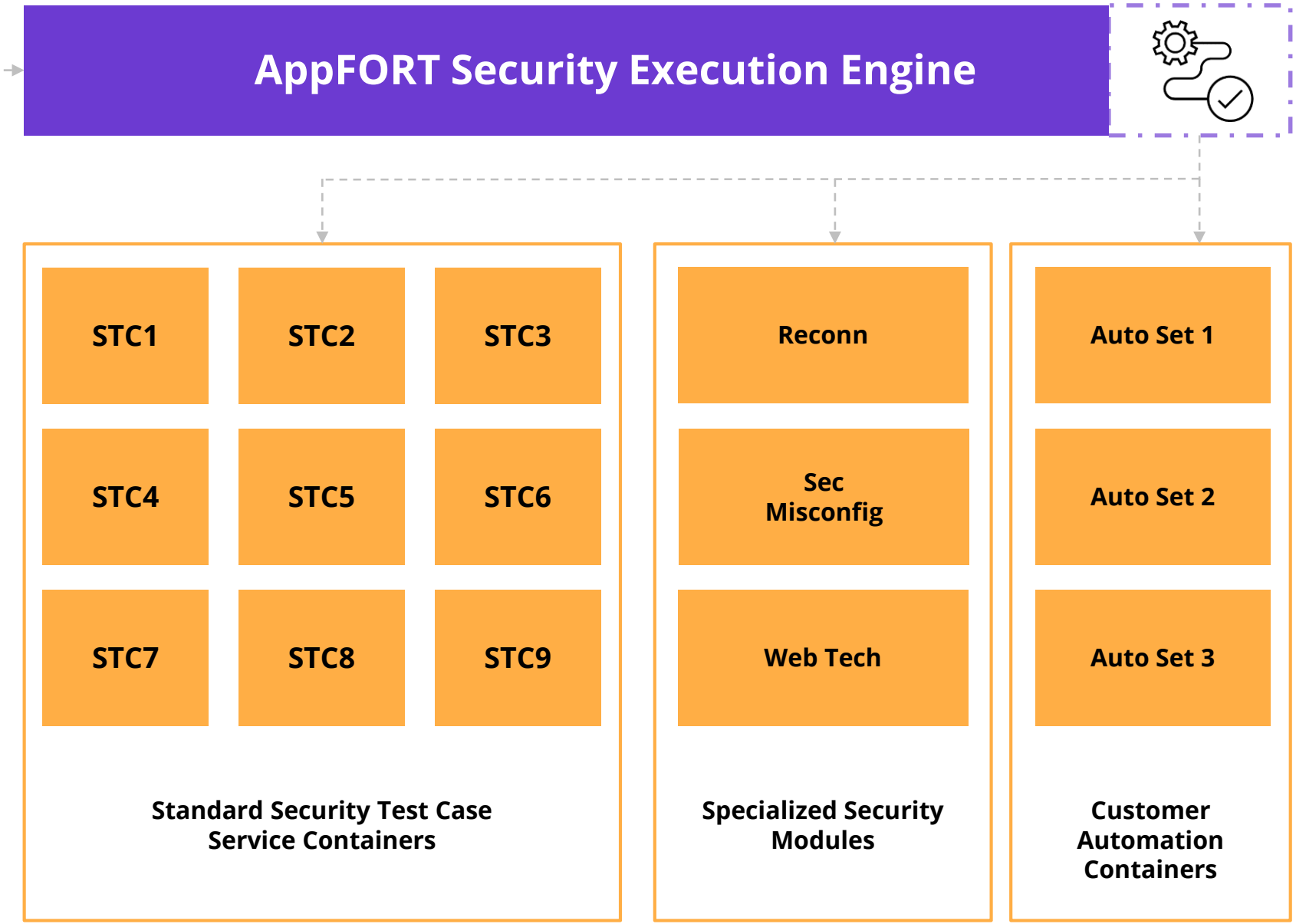
- *Simplified remote automation*
- *In-built automation for security testing*
- *Orchestrated execution of automated routines*
- *Stated reduction of overall security cost for apps*

# AppSec Framework



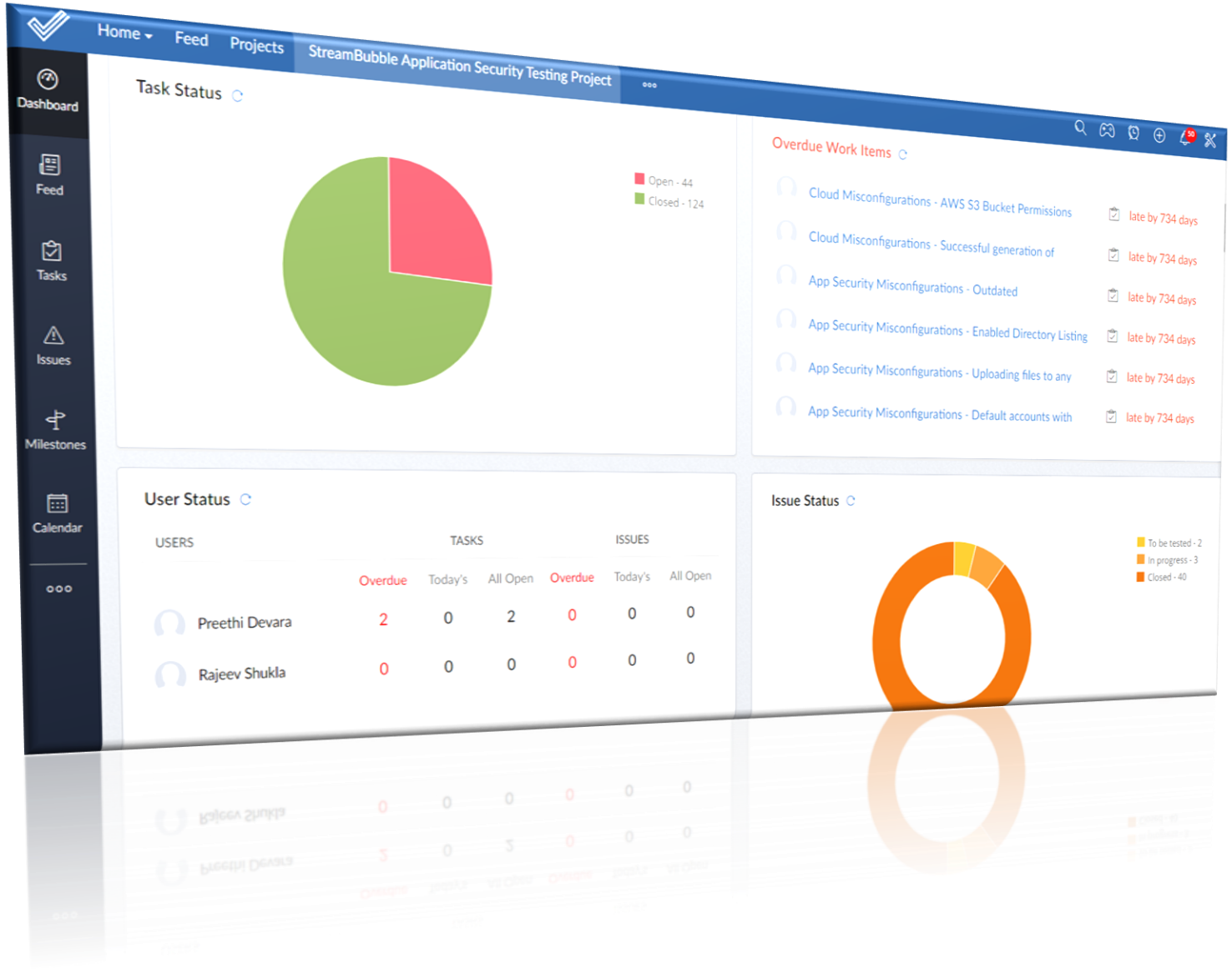
# Orchestrated Application Security




**AppFORT**, a cloud based platform
- For Security Automation
- For Execution Coordination
- For Continuous AppSec

# AppSec Customer Portal




Project portal with task, milestone and other details

---

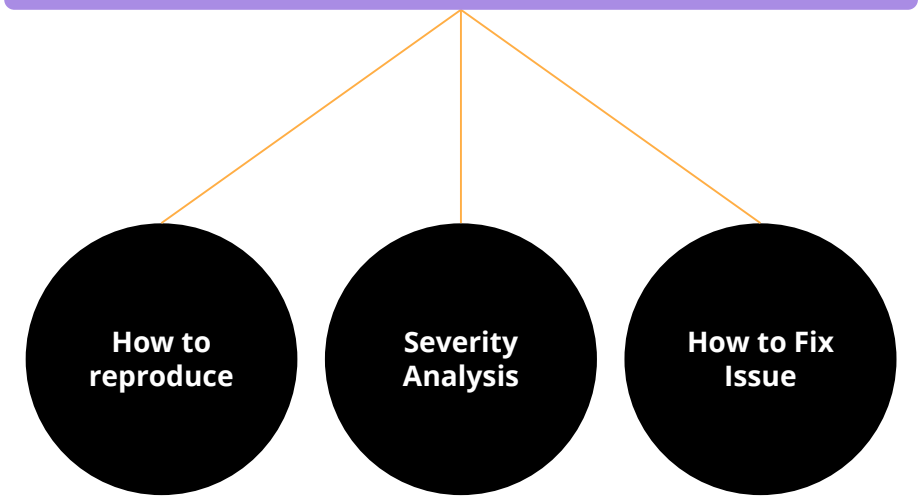
Customers are given an access to portal for all s/w projects

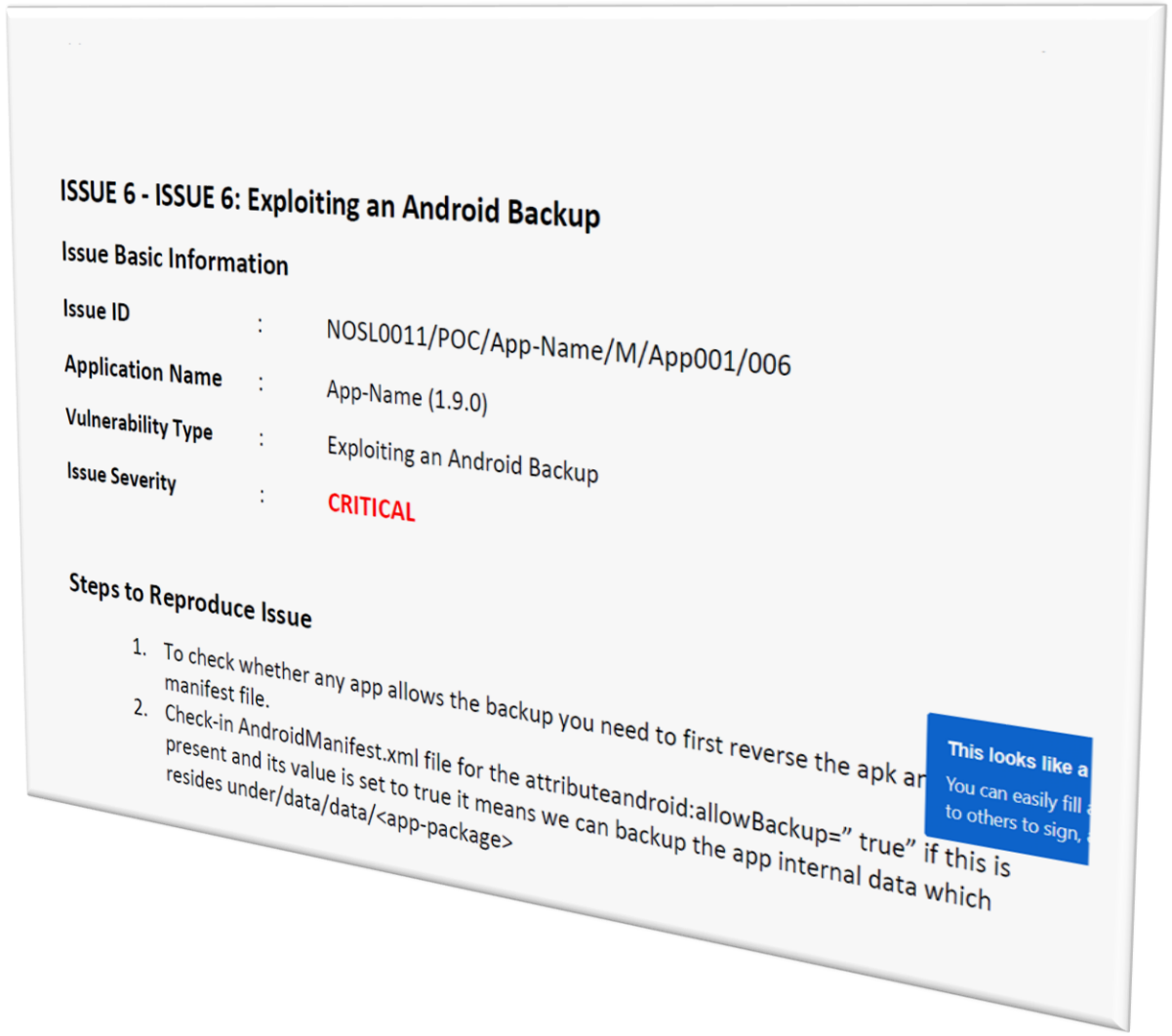
---

Real time access to project statuses and execution details

# Closing the loop

"Every issue detected by our team is reported via an IDR (Issue Details Report)"



**ISSUE 6 - ISSUE 6: Exploiting an Android Backup**

**Issue Basic Information**

| | | |
|---|---|---|
| Issue ID | : | NOSL0011/POC/App-Name/M/App001/006 |
| Application Name | : | App-Name (1.9.0) |
| Vulnerability Type | : | Exploiting an Android Backup |
| Issue Severity | : | CRITICAL |

**Steps to Reproduce Issue**

1. To check whether any app allows the backup you need to first reverse the apk ar
   manifest file.
2. Check-in AndroidManifest.xml file for the attributeandroid:allowBackup=" true" if this is present and its value is set to true it means we can backup the app internal data which resides under/data/data/<app-package>

This looks like a
You can easily fill
to others to sign,

# Run Plan Example

## Security Execution Visibility

| | | |
|---|---|---|
| Static Testing | Dynamic Testing | Interactive Testing | Greybox Testing |
| Code Scan | Code Review | Composition Analysis | Code and Composition Review |
| Design Review | Remediation Expl | Dev Training | Design & Regression |
| Sec Issue Fixing | Regression Cycle | Server Hardening | Remediation Phase |

| First Security Testing Run (120 Apps) | | | Apr | | | | | | | May | | | | | | | Jun | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Application Category** | **Size** | **Count of Apps** *(by Size)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* | *(4 Days)* |
| **Critical Applications** | Large Apps | 5 | | | | | | | | | | | | | | | | | | | | | | |
| | Medium Apps | 24 | | | | | | | | | | | | | | | | | | | | | | |
| | Small Apps | 19 | | | | | | | | | | | | | | | | | | | | | | |
| **High Priority Applications** | Large Apps | 14 | | | | | | | | | | | | | | | | | | | | | | |
| | Medium Apps | 29 | | | | | | | | | | | | | | | | | | | | | | |
| | Small Apps | 29 | | | | | | | | | | | | | | | | | | | | | | |

# Continuous CISO View

## Software Risk Exposure

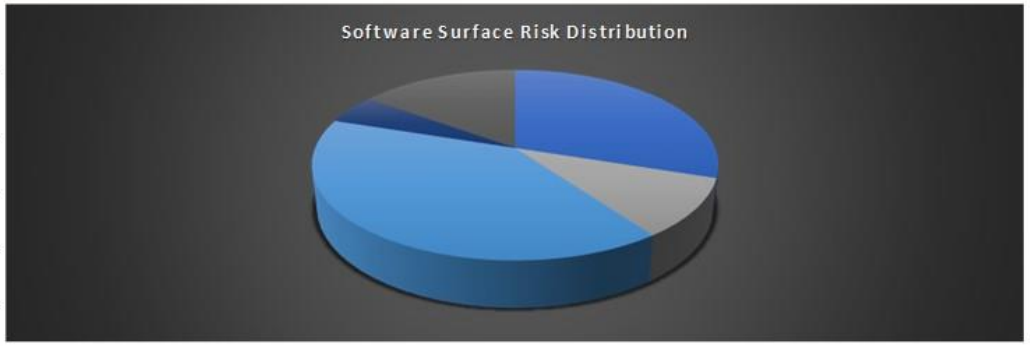
## Enterprise Software Risk Board

| Current Software Surface Risk Index |
|---|
| 4.4 |

| Risk Levels | Low | High |
|---|---|---|
| Highly Insecure | 1 | 3 |
| Insecure | 4 | 5 |
| Secure /Dev Gaps | 6 | 7 |
| Secure /Audit Gaps | 7 | 8 |
| Secure | 9 | 9 |
| Fully Secure | 10 | 10 |

| Risk Rating Criterion | |
|---|---|
| Accessibility of S/W | *Remote/Local* |
| Location of Software | *Internal/External/DMZ* |
| Usage Profile of S/W | *High/Medium/Low Tx* |
| User Profile of S/W | *Internal/External/Cust* |
| Auth Model of S/W | *App/AD/MFA* |
| Static Vuln Scan Output | *Various Counts* |

| Risk Rating | Count of Apps |
|---|---|
| Highly Insecure Apps | 6 |
| Insecure Software | 2 |
| Secure but Gaps | 8 |
| Secure Software/Apps | 1 |
| Fortified Software | 3 |




| Application Name | Business Criticality | Current Risk Rating<br>*Weighted Scale*<br>*1 to 10*<br>*1 High - 10 Low* | Application Posture<br>Current (As Is) | Application Posture<br>Targeted | Targeted Risk Rating<br>*Weighted Scale*<br>*1 to 10*<br>*1 High - 10 Low* | Does Internal Team do Some AppSec? | Does Provider do Some AppSec? |
|---|---|---|---|---|---|---|---|
| CRM Application | High | 3 | Highly Insecure | Secure | 6 | Yes | Yes |
| Sales Management S/W | High | 3 | Highly Insecure | Secure | 8 | Yes | No |
| Supply Chain Software | High | 5 | Insecure | Secure | 6 | No | No |
| CRM Mobile Application | High | 6 | Secure | Highly Secure | 8 | Yes | Yes |
| Biometric Attendance Web | Low | 8 | Highly Secure | Secure | 7 | No | Yes |
| Financial Software | Medium | 10 | Fully Hardened | Fully Hardened | 10 | Yes | Yes |
| Cash Management Software | Low | 10 | Fully Hardened | Fully Hardened | 10 | Yes | Yes |
| Facility Mgmt Mobile App | Low | 9 | Highly Secure | Highly Secure | 9 | No | Yes |
| Partner API (Treade Platform) | High | 6 | Secure | Secure | 8 | Yes | Yes |

**ONE**
**Uniform**
**Continuous**

# Engagement Models

#1

### Managed AppSec Program

Recurrence based Program Structure

#2

### AppSec with Automation

Recurrence based Program Structure

Remote Automated Security Execution

#3

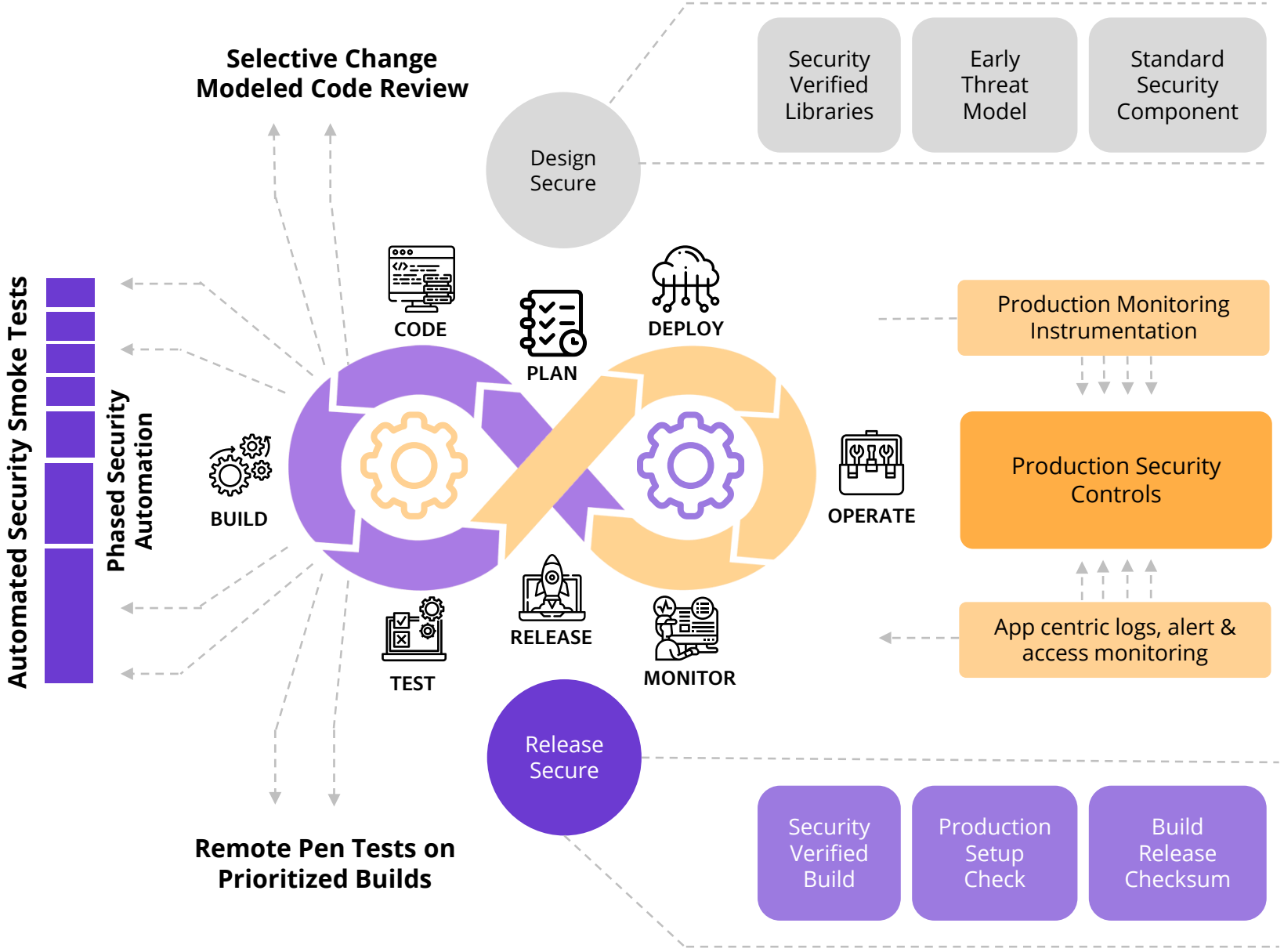
### AppSec for DevSecOps

Continuous Program Structure

Remote Automated Security Execution

End-to-End Security Automation

# Continuous App Sec: Progression to DevSecOps



# Partial Customer List

| Name of Customer | Sector | Country | Area of Service |
|---|---|---|---|
| TrusTrace | SaaS Supply Chain | SWEDEN | Application Security |
| StreamBubble | Media Platform | DUBAI | Application Security |
| ChefDesk | Retain POS Products | INDIA | Application Security |
| Decathlon | Retail | INDIA | AppSec |
| Eduonix | Online Learning | INDIA | AppSec |
| DSPIM | Investment Mgmt | India | AppSec |
| Vijaya Diagnostics | Pathology Labs | India | AppSec |
| Uprise | SaaS Platform | Australia | AppSec/Cloud |
| Star Health | Insurance | INDIA | AppSec/WatchOUT |
| External A Ministry | Govt | QATAR | Network Security |
| Jersey Telecom | Telecom | UK | Network Sec / AppSec |
| Dr. Reddy's Lab | Pharmaceuticals | INDIA | Threat Intelligence |
| DarwinBox | SaaS HR Company | INDIA | WatchOUT |

appFORT

# Keep In Touch.

+91 99807 80365

enquiry@castellumlabs.com

www.castellumlabs.com