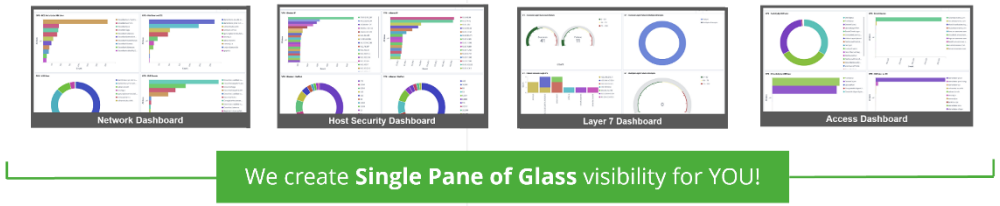
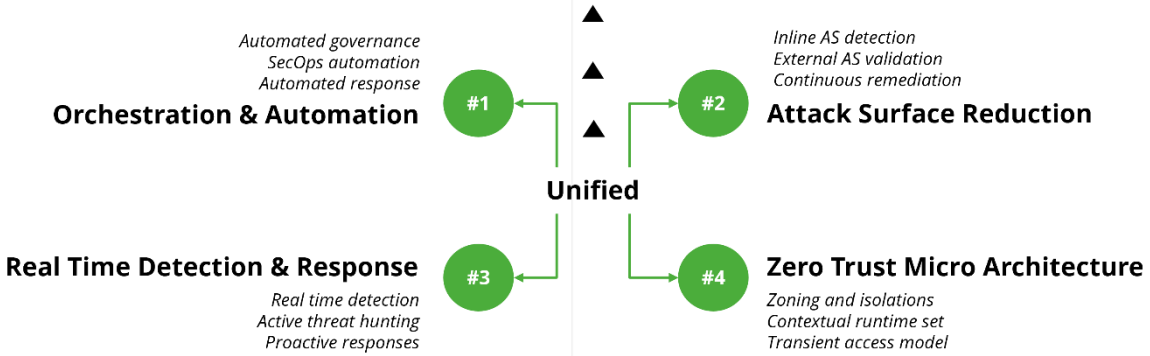
Castellum Labs





Castellum Labs

VAPT Engagement Service Description Deck

www.castellumlabs.com

About Castellum

Services delivered by Global Cyber Capability Center using advance Platforms

Based in Hyderabad, India with global customer base across India, US, Europe

Strong Handpicked Team of 50+ with (best of security talent globally)

Started by people with decades of product, services & deep tech experience

Subscription & annual contract modeled services delivered globally

Value + Impact from Day One, No Installation & No Deployment

Leadership Team

Rama

Advisor and Head – US Ops
(US based)

Senior business leader with 30 years of experience in US & India, across entire spectrum of IT industry in services & product companies

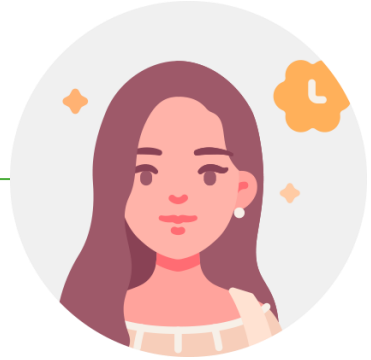
Head IT – Aryaka, Ex-PwC, Ex-IBM, Ex-VMWare, Ex-Malwarebytes, Ex-Infosys and Ex-NetApp

Rajeev Shukla

Founder & CEO
(India based)

Senior business leader with dozens of stints with MNCs for buding data center, networking & cyber security services and product businesses

Ex-VP CA Technologies, Director – Sun Microsystems, Ex-VP – Quark, Ex-CTO - Cygilant



Rinky (Sukriti Shukla)

Head of Strategic Sales
(India based)

Seasoned operational leadership from NGO sector, with experience across sales, HR, operations and legal

Started corporate journey with Castellum and handled variety of roles, HR, Pre-Sales & Sales

Some of Our Enterprise Customers

DSP MUTUAL FUND

Fidelity INVESTMENTS

Dr.Reddy's

STAR Health Insurance
Personal & Caring
The Health Insurance Specialist

CENTRE FOR GOOD GOVERNANCE
Knowledge • Technology • People

VIJAYA DIAGNOSTIC CENTRE

JT JOIN TOGETHER
Jersey Telecom

VIAPLUS

Quinnox
accelerate success

excelra

PRISM JOHNSON LIMITED

وزارة الصحة العامة
Ministry of Public Health
State of Qatar • دولة قطر

Some of Our Digital/Startup Customers

flodata ...anywhere

uprise

eduonix

Sub-K SAB KE LIYE SAMRUDDHI LAYE

FORMCEPT Your Analytics Platform

trica

ideaForge™ Create. Inspire

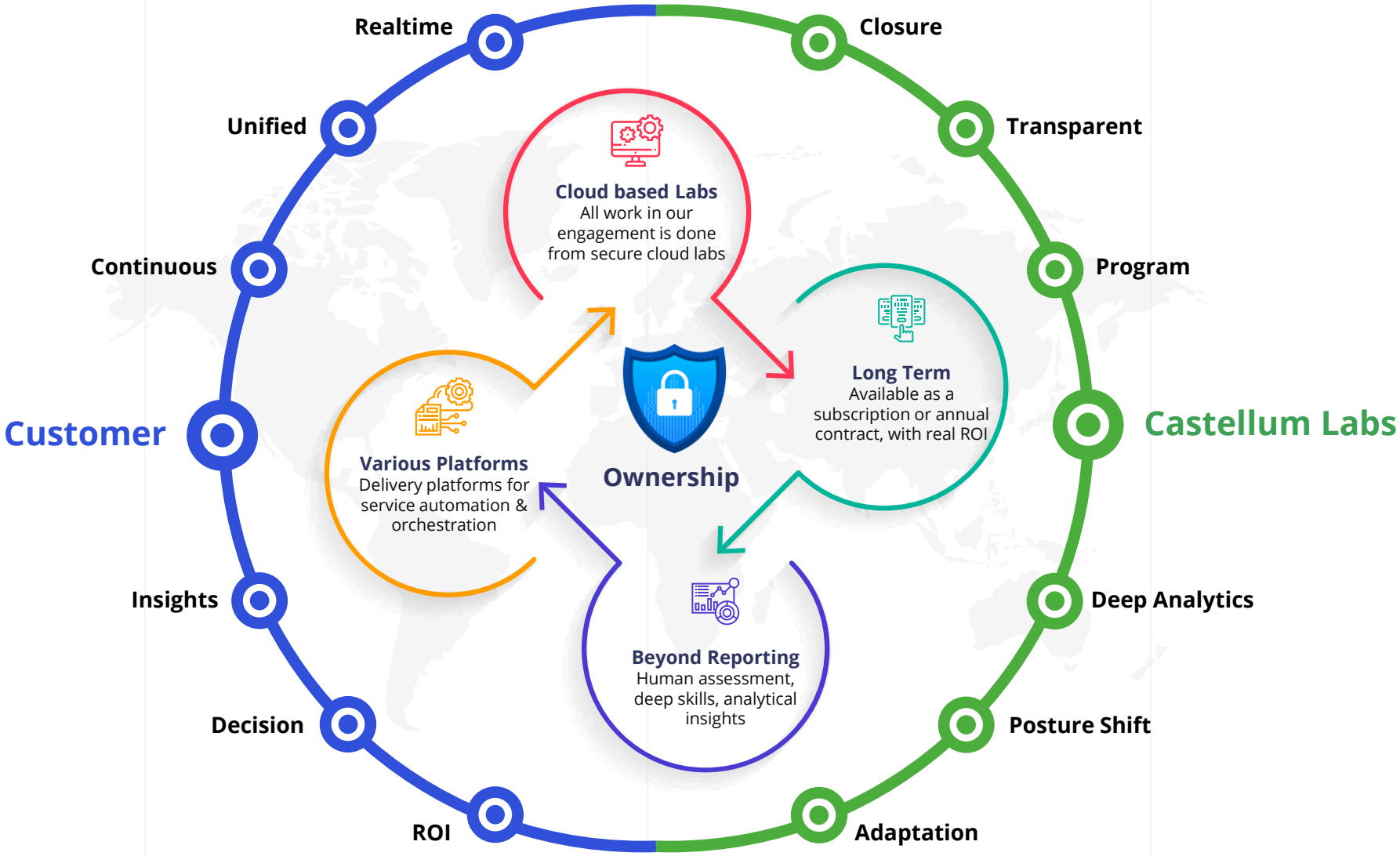
Spice money तो Life बनी

trustrace

NUTRABAY

AVANSE FINANCIAL SERVICES

Real Security, Not Transactional Projects



Standard VAPT: Noisy, Repetitive & Unclear

Adoption of CI/CD is taking place ...

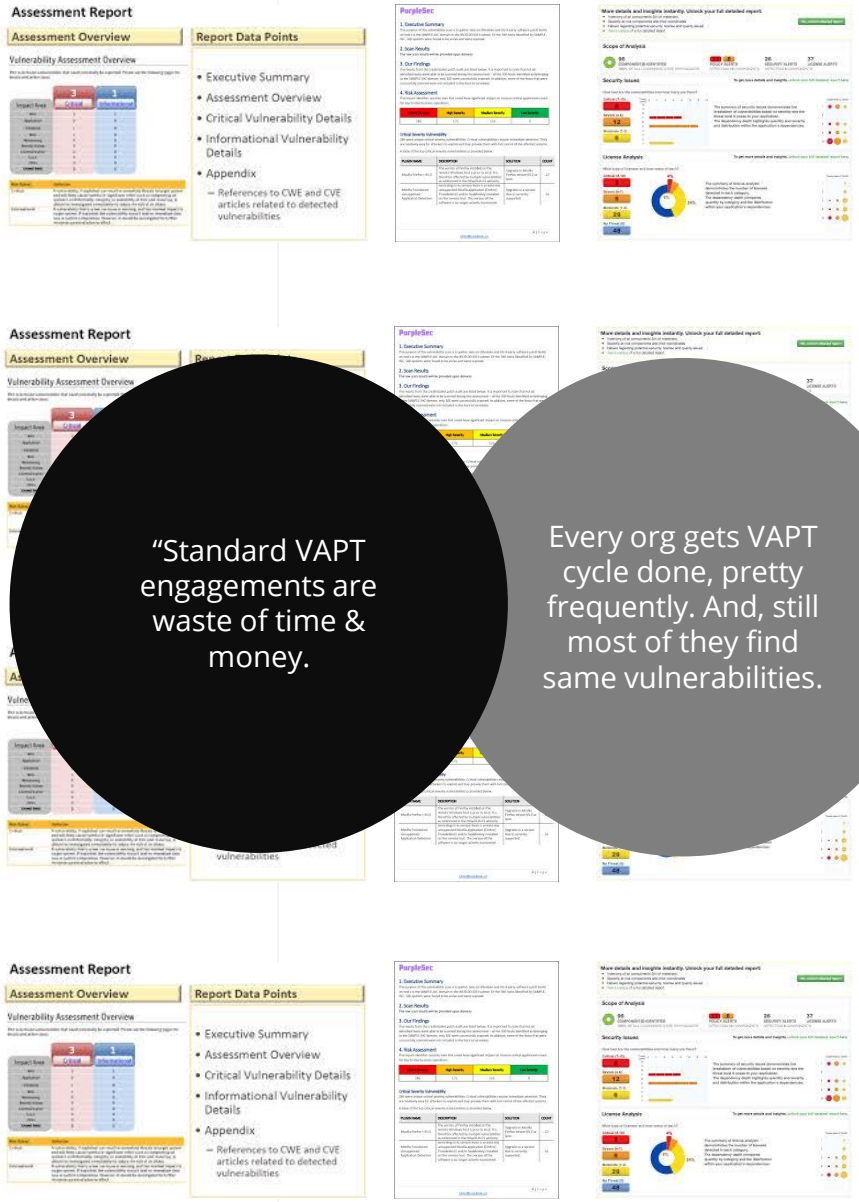
"Rapid Release Cycle of Apps & Changing IT at Enterprise Customers"

With manual security testing such as VAPT

"Very Limited Security Testing through Changes is Possible"

Tool based VAPT of software leads to

"Surface Risk Exposure Visibility is Unclear and Limited"



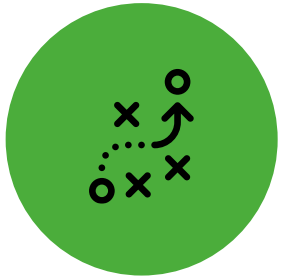
What VAPT Should Answer

#1

Which vulnerabilities occurred twice in a row across two cycles on same asset class in my cloud infrastructure?

#2

How many new vulnerabilities were found in this asset class in division 4, in three consecutive cycles?

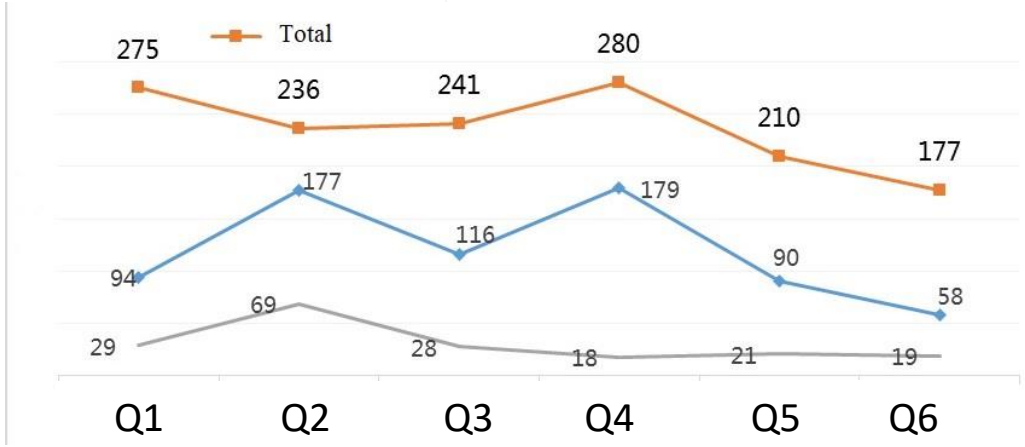


#3

Which part of my infrastructure has weakest operational practices on security, leading to introduction of new vulnerabilities

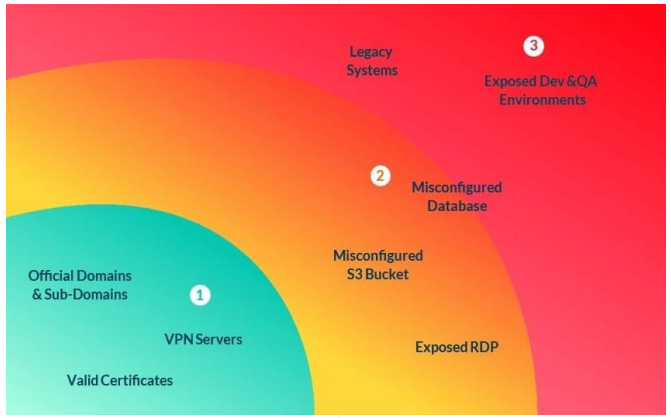
What VAPT Should Produce

Critical Asset Cluster



"Downward trend of vulnerabilities, in specific asset clusters across the enterprise IT"

Enterprise Attack Surface Q2



"Attack surface reduction representation over time for an enterprise IT footprint"

Vulnerability Management Program

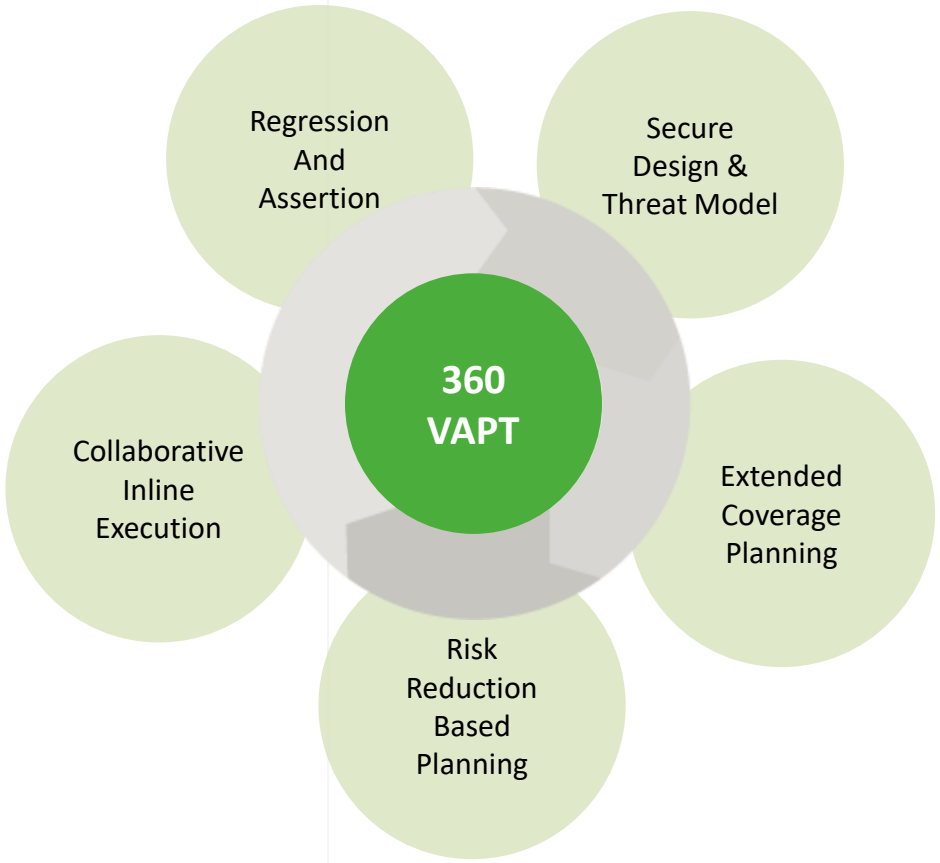
In today's digital infrastructure which are centered around dynamic provisioning, allocations and eliminations, traditional VAPT model which are based on asset scans are failing

VAPT Cycle Runs

Vulnerabilities Management Program

Focus Areas	VAPT Cycle	Vulnerability Mgmt Program
Detecting & Reporting Vuln	Yes	Yes
Remediation & Closure of Vuln	No	Yes
Using Intel for Advancing Detection	No	Yes
Mapping Detection Trends on Assets	No	Yes
Creating Feedback Loop for IT/Dev	No	Yes
Attack Surface Reduction	No	Yes
Reducing Avg Detection & Closure Time	No	Yes

360 Degree and Seamless



Comprehensive

- *Exceptional scenarios*
- *Threat modeling of assets*
- *Multi-layer testing framework*
- *Custom methodology risk reduction*

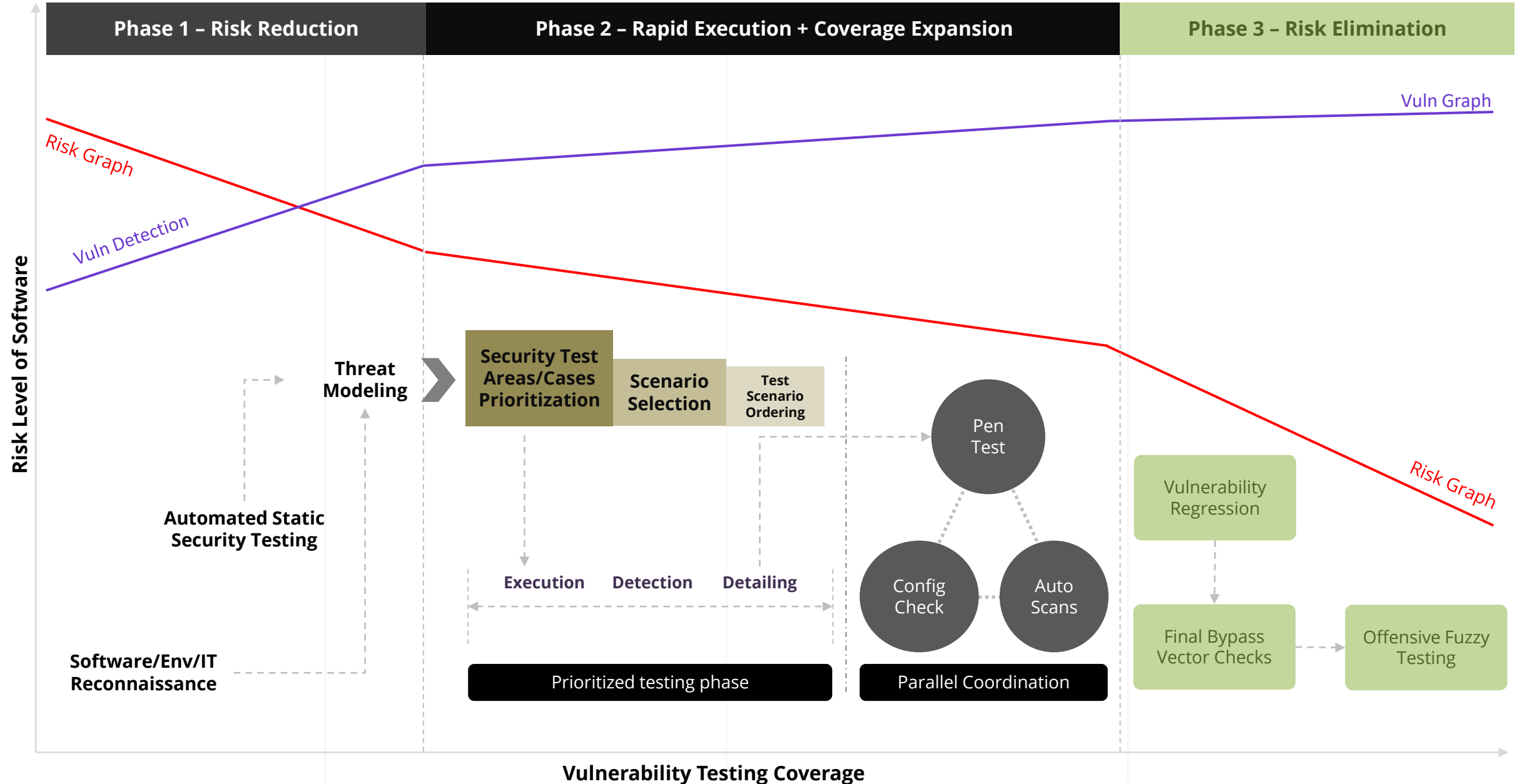
Inline Continuous

- *Designed continuity*
- *Across releases issue visibility*
- *Continuous test security execution*
- *Covering multiple asset change cycles*

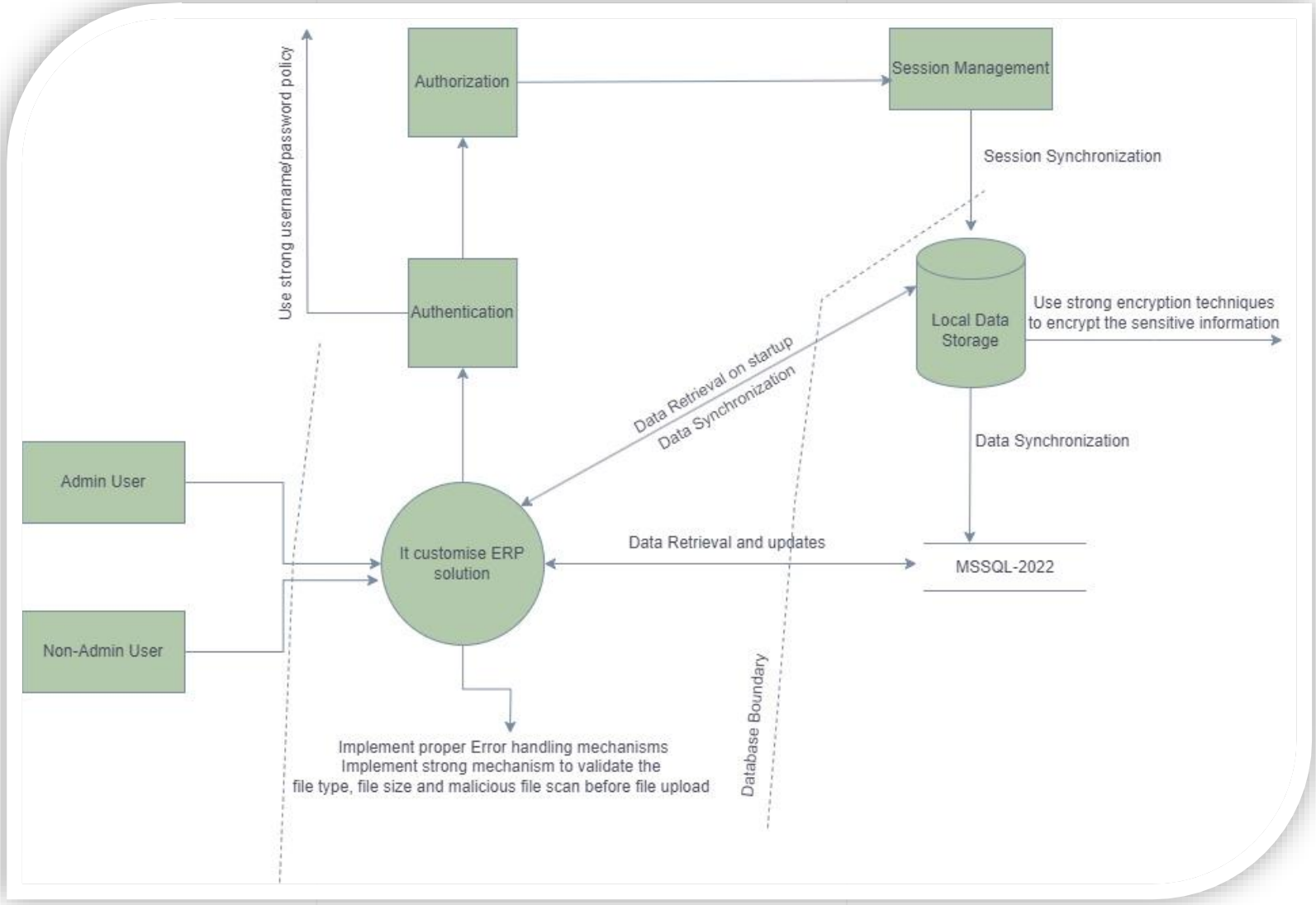
Automated

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

Advanced Cyber Security Frameworks



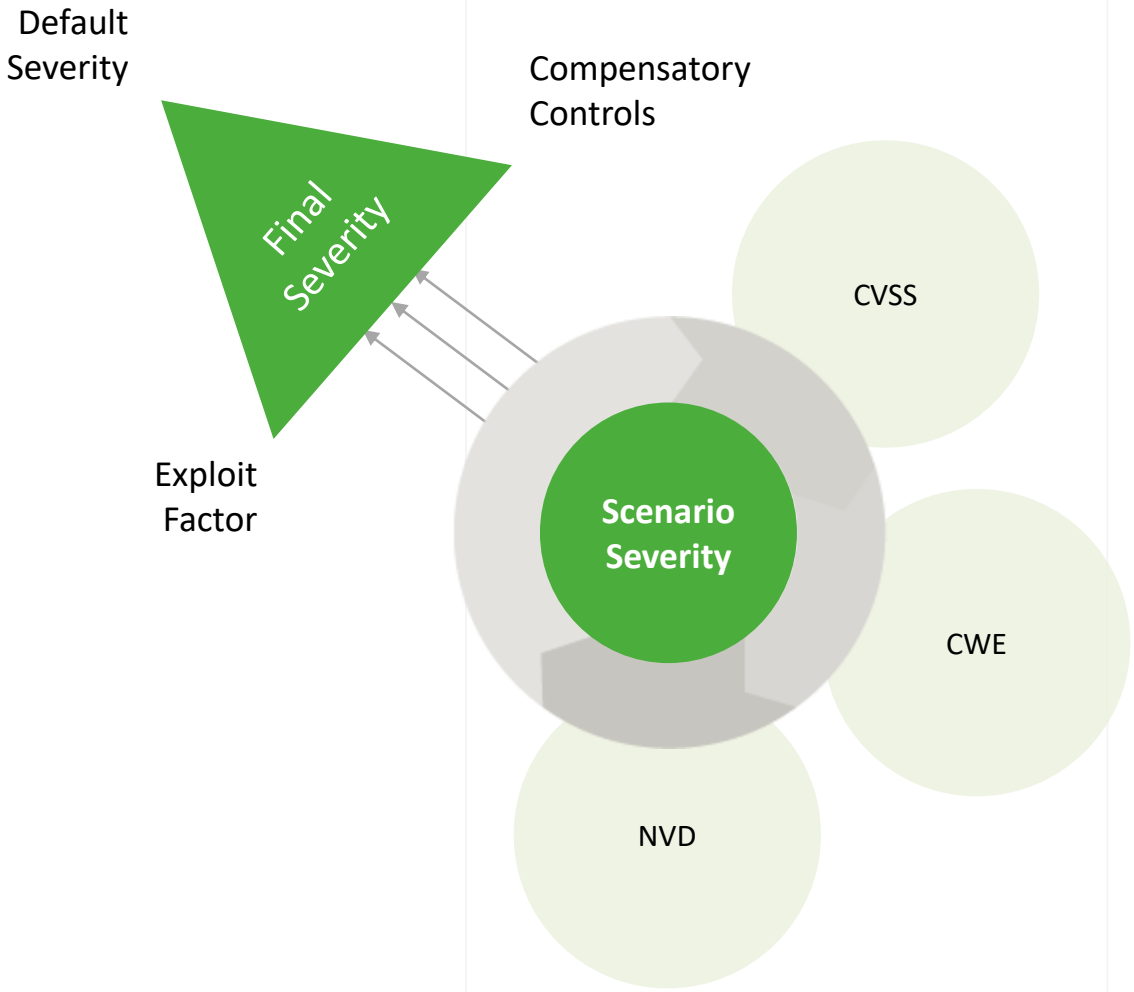
Threat Model for Precise Execution



Vulnerabilities Detailing Model

Detailing Phase Name	Key Objectives
Recon & Info Intel	*Survey*
	Element Scans
	Threat Model to be Used
Vulnerability & Exploit	*Vulnerability Finding*
	Scans for Weak Points
	Exploit Establishments
Exploit Verification	*Logic Exploitation*
	Route Exploitation
	Information Exploitation
Evidence Establishment	*Evidential Data*
	Data Aggregation
	Security & Risk Analysis
Risk and Exposure Analysis	*Vulnerability Impact*
	Compensatory Controls Analysis
	Impact Analysis for Final Score
Remediation Analysis and Detailing	*Vulnerability Remediation Analysis*
	Bypass Vectors Analysis

Vulnerability Severity Scoring



Multi
Mapping

ISO

CIS Center for Internet Security®

OWASP®

NIST

Managed <> Vulnerability to Resolution

Detect & Report

Assisted Remediation

Closure

1. Guided Vulnerability Filing System

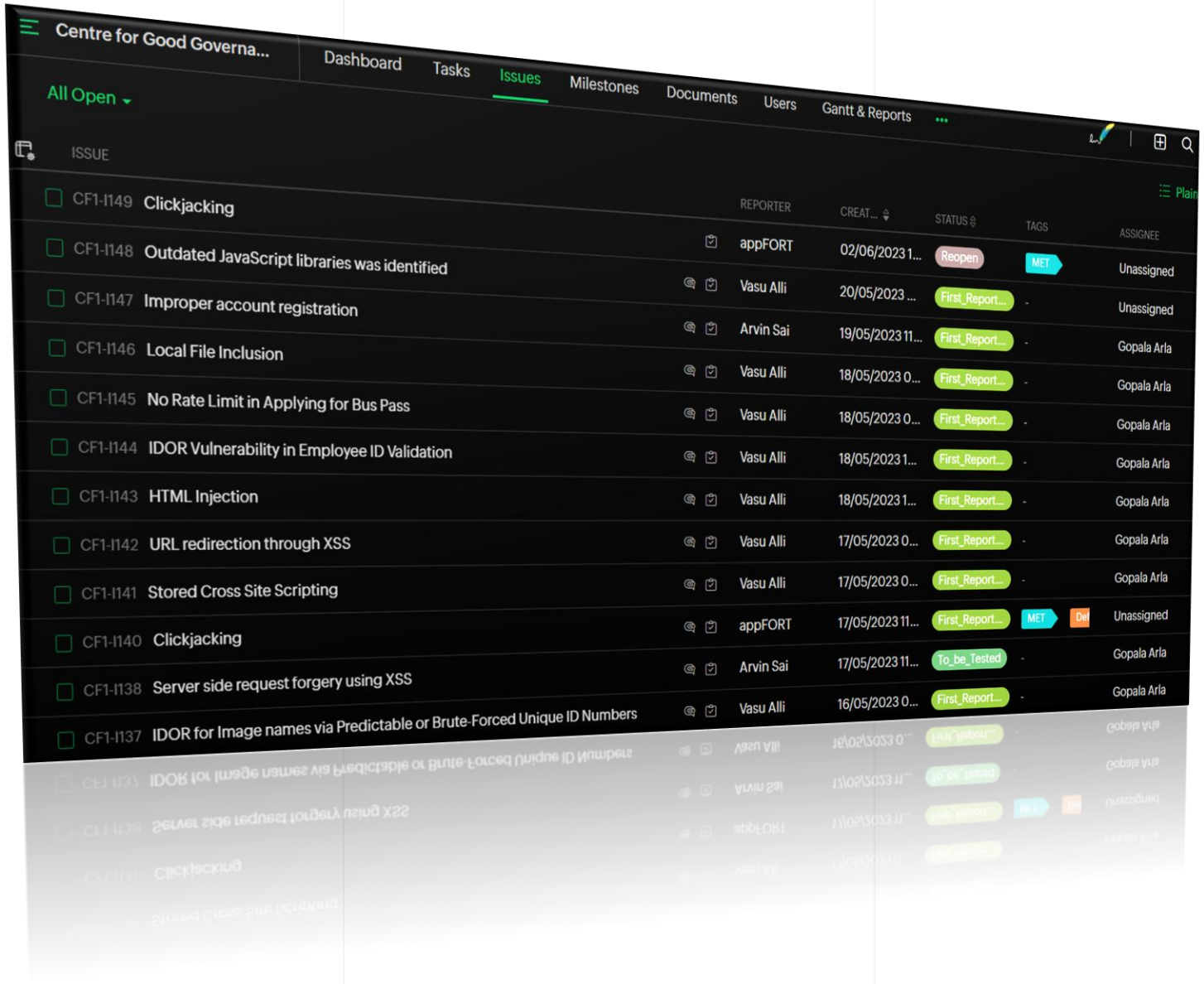
2. Auto Allocation IT/Developer

3. Vulnerability Reproduction Steps

4. Researched Remediation Steps

5. Vulnerability Closure Triaging

Unified View <> Single Window



- “One” security portal
- All collaboration on one portal
- Unified security window for customers

Exceptional Customer Set of Reports

4.0 Executive Summary

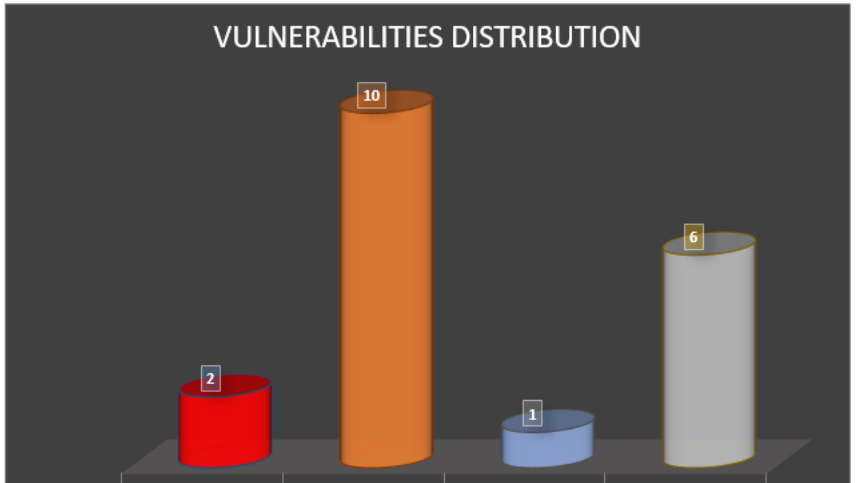
Castellum Labs was engaged to perform a penetration test for GOCL. This report discusses the results from the assessment. During the engagement for security testing and assessment, Castellum Labs covered good security practice while aiming to determine if:

- The systems were suitably configured in line with good security practice
- Communications within network were suitably protected from interception & intervention
- Customer systems were suitably protected against unauthorized activity from authorized users
- Systems were suitably securely configured against malicious activity from un-authorized users

4.1 Vulnerabilities Findings Summary

Castellum was able to achieve the goal of this security assessment, and identified number of high severity and high impact findings during the assessment, including following high priority ones.

Finding Category (Vulnerability Category)	Place
Sensitive Service Exposure	**3 Servers / 3 Storage Device**
Vulnerable & Outdated Service/Software	**3 Server / 3 Storage / 3 DBs / 2 EPs**
Insecure Authentication with FTP	**2 Endpoints**



Castellum Labs
VAPT Security Testing and Vuln Assessment Report

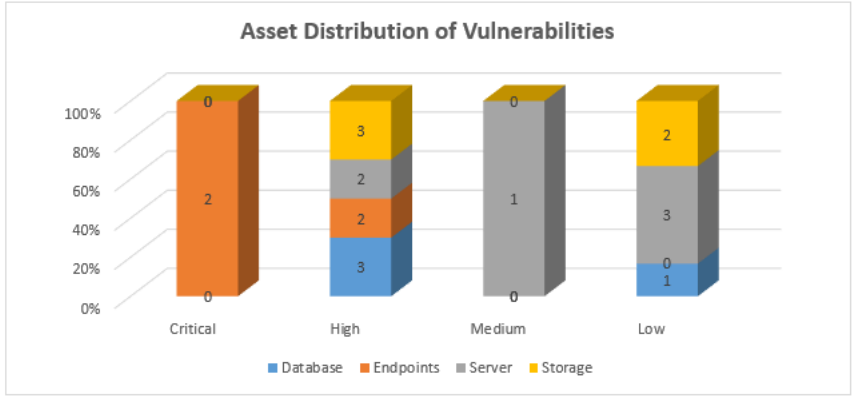
Technical aspect of this security assessment was conducted over a period of 20 days, while remaining time was spent on access provisioning, reconnaissance and preparation. Several serious security issues and challenges were detected within the network, including use of outdated software versions, lack of security best practices, lack of patching, insufficient controls for web applications.

4.2 Asset Distribution of Vulnerabilities

Among all of the assets considered and included in the security testing and assessment, VM images and web applications carried maximum number of vulnerabilities. Considering that these same VM images are hosting web applications, a combination of these vulnerabilities can be critical.

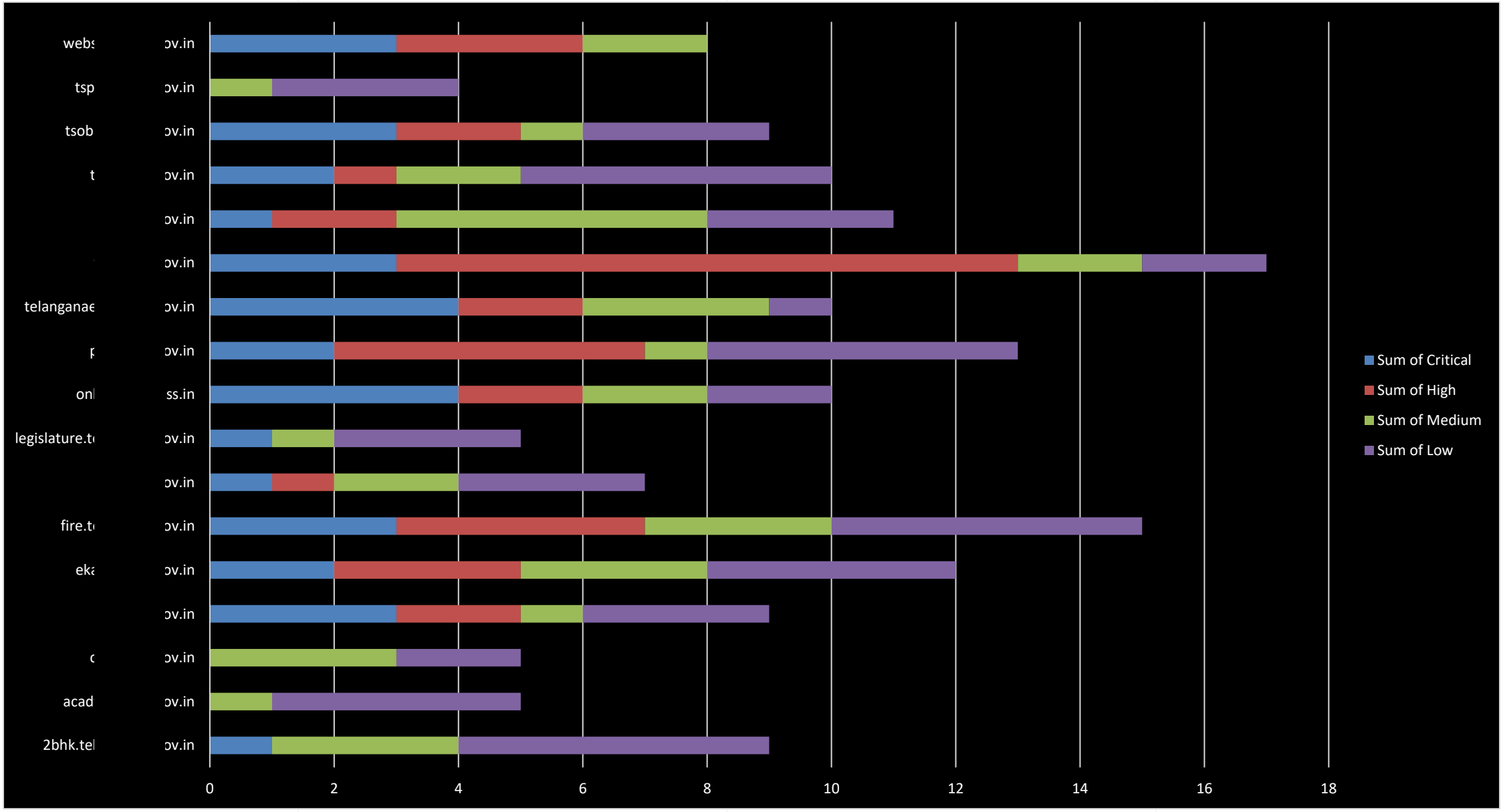
Asset with Top Density of Vulnerabilities	
Server	**Storage Devices**
6 Vulnerabilities (H-2, M-1, L-3)	5 Vulnerabilities (H-3, L-2)

A distribution of the vulnerabilities on all the internal assets within GOCL is presented below. This distribution is indicative of the internal attack surface of the company.

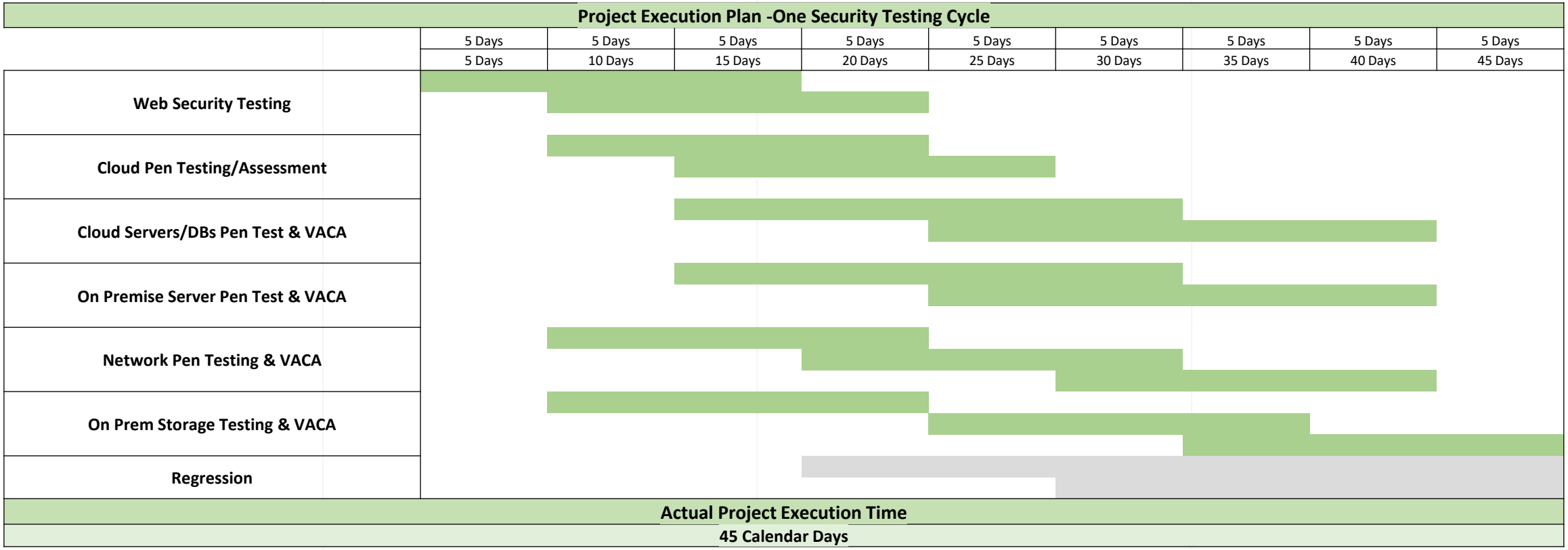


Vulnerabilities summary representation above contains vulnerabilities across all of the network and server infrastructure and also included web application hosted within the network. These vulnerabilities are spread across categories, such as critical service exposure, cryptographical failures, insecure file upload functionality, unauthorized access to network, insecure software and libraries, unnecessarily open ports, vulnerable service

Across Cycle Vulnerability Patterns



Timeline for VAPT Engagement Cycles



20 Days

Small to mid size infra
(50 to 75 assets)

30 Days

Mid size infra
(75 to 150 assets)

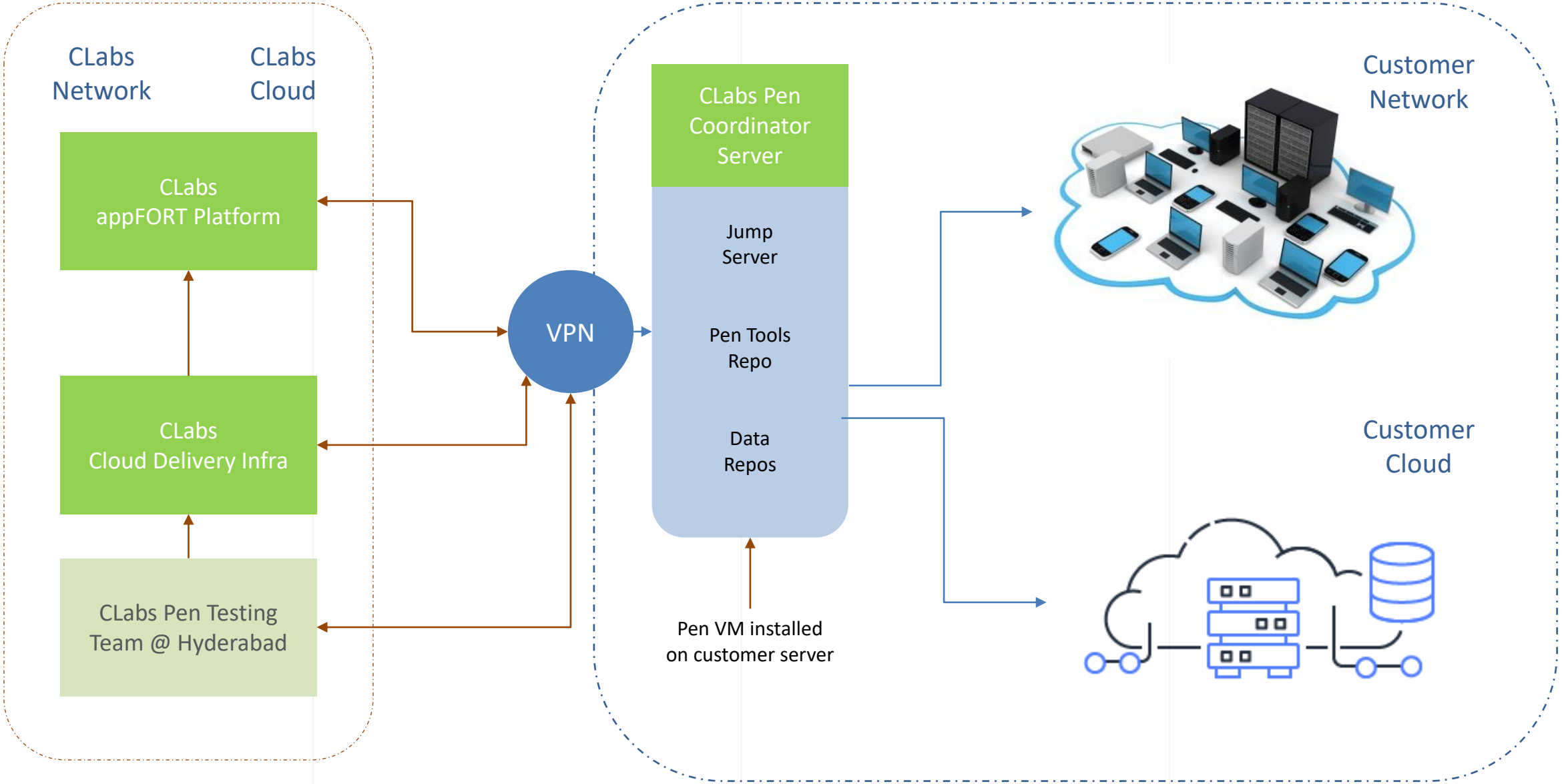
45 Days

Large size infra
(150 to 300 assets)

60 Days

Very Large size infra
(300 to 1000 assets)

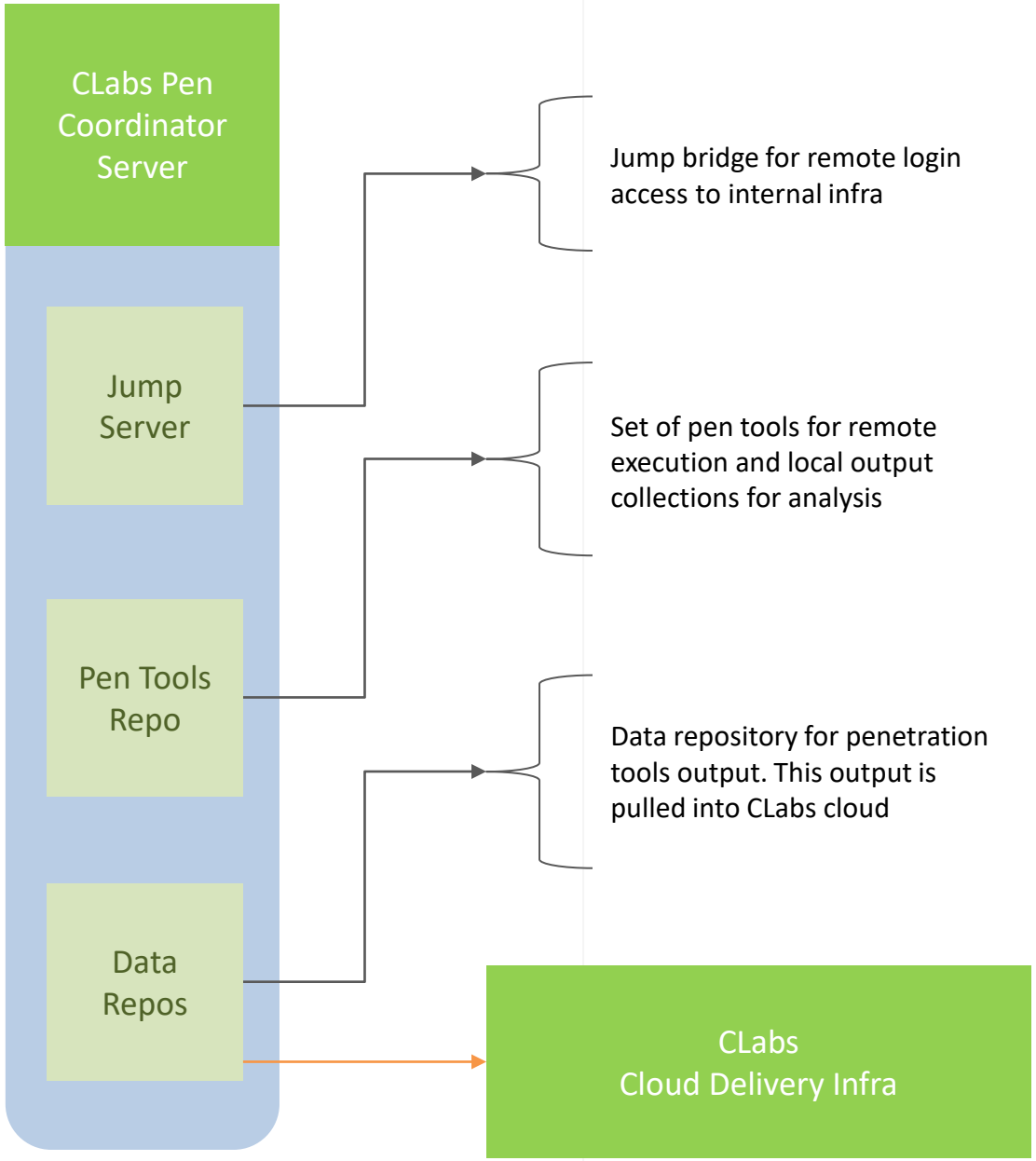
Castellum VAPT Execution Infra



Hardened Pen Coordinator Image

A super hardened VM with pre-installed tool sets for remote execution.

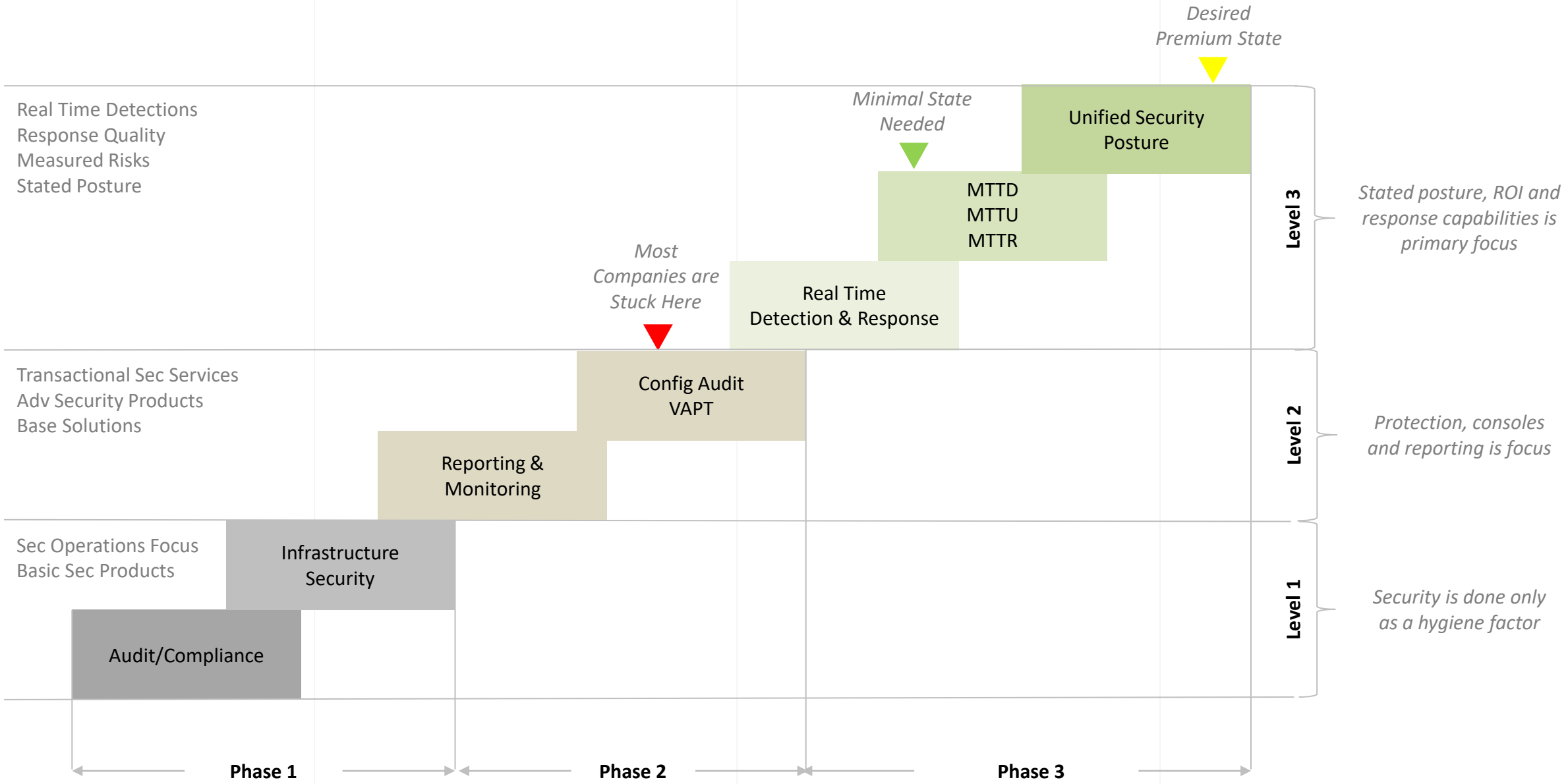
- ✓ Hardened Kali Linux image
- ✓ Scoped user for pen tools execution
- ✓ Process hardening for known set execution
- ✓ Network hardening for bounded communication
- ✓ Data pipe definition to restrict comm to CLabs cloud
- ✓ Extensive logging of the execution activities
- ✓ Auto deletion of outputs after ingestion
- ✓ Login access to customer as well



Execution of Scenarios/TCs

appFORT	Clabs Cloud Infra for Delivery	Clabs Pen Coord. Server	Read Only Account in Customer Cloud
Remote and over VPN execution on web, mobile and API	Remote pen execution on public IP surface of customer	Local pen execution on internal network devices/servers In cloud pen execution on internal network devices/servers	Use of cloud native scan and test tools for selective pen vectors

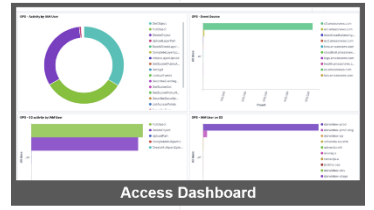
Operational to Strategic Posture



Keep in Touch.

+91 8639953505 enquiry@castellumlabs.com www.castellumlabs.com

CLabs' Vision is "Clarity" & "Defense in Depth"



We create **Single Pane of Glass** visibility for YOU!

Automated governance
SecOps automation
Automated response

Orchestration & Automation #1

Inline AS detection
External AS validation
Continuous remediation

Attack Surface Reduction #2

Unified

Real Time Detection & Response #3

Real time detection
Active threat hunting
Proactive responses

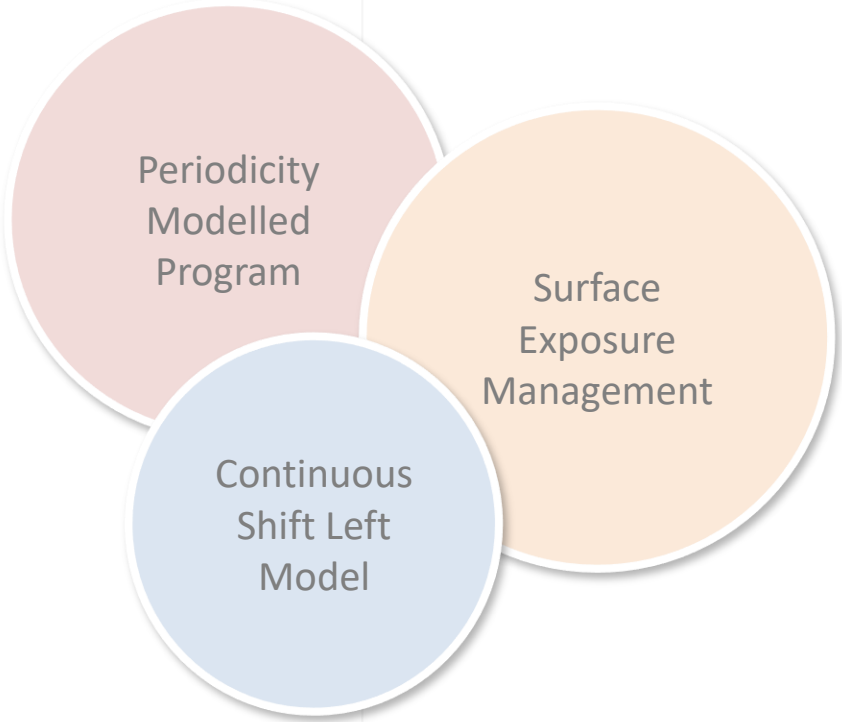
Zero Trust Micro Architecture #4

Zoning and isolations
Contextual runtime set
Transient access model

Programs & Transformation Services

VAPT/VACA Programs

Red Team <> Blue Team Modeled
Annual Program for Vuln Management



Threat Intel & Hunt

Counter Intelligence Powered
Quarterly or Monthly Hunt/Runs

DevSecOps

AppSec Programs & DevSecOps
Transformational Project for Shift Left

Privacy Engineering

Adoption, Engineering & Compliance
Transformation Project for Continuous Privacy

Security Services (Projects) Portfolio

Cloud Workload & DC Hardening

Infrastructure Security

Simulations for Defense Capability

Breach & Attack Simulation

Assessments & Optimizations

SOC / SIEM Streamlining

ISO 27K and SOC 2 Type 1/2

Cyber Certifications

Employee Awareness

Phishing and Emp Awareness

Incident Response

Runbooks, Process & Breach Handling

Security Assessments

Gap, Audit and Maturity

Automations & Insight

Security Data Lake & SecOps