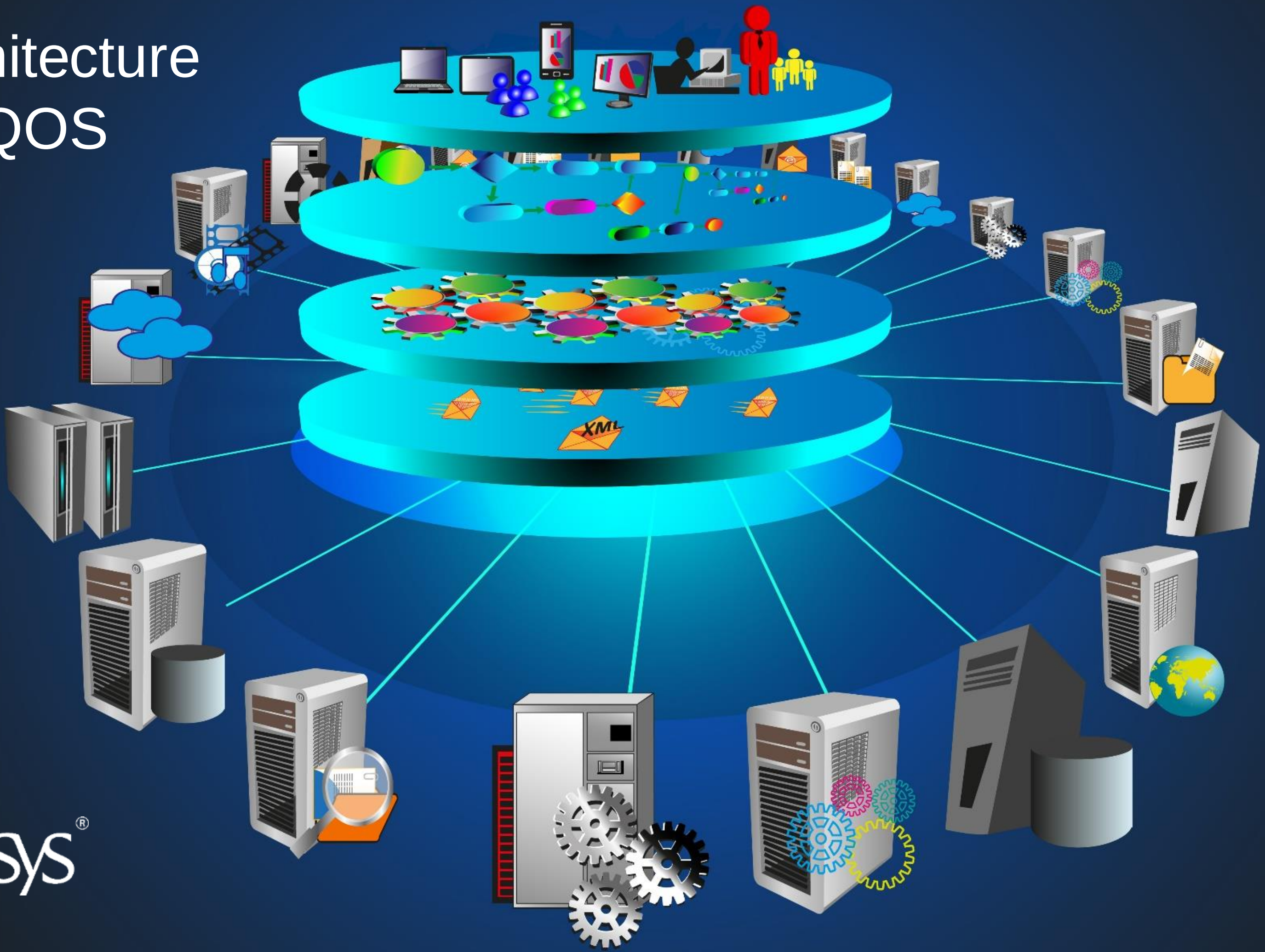
Architecture
QOS



Connect Architecture

Infosys®

Topics

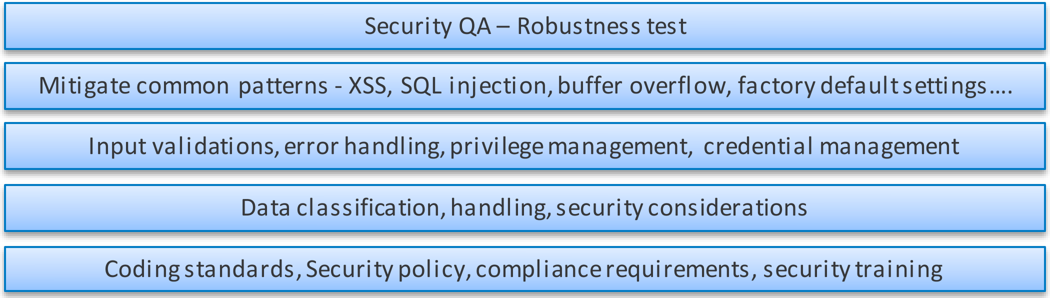
- QOS – what it means for Architecture
- Security - What to protect and How
- Incorporating Security in SDLC
- Design principles
- Integration of security with functional requirements
- Case Study

Business are continuously under threat, making security a functional requirement

1. Lack of awareness
2. State Sponsored attacks
3. Thefts/Financial Gains
4. To impact the Brand

What to protect & How

- Data
  - Business requirements and translations
  - Architecture and Code
  - Test Data
  - Changes, approvals, transfer and movement
  - Production data
- Brand
  - Business use cases and flow
  - internet facing applications/device



Security QA – Robustness test

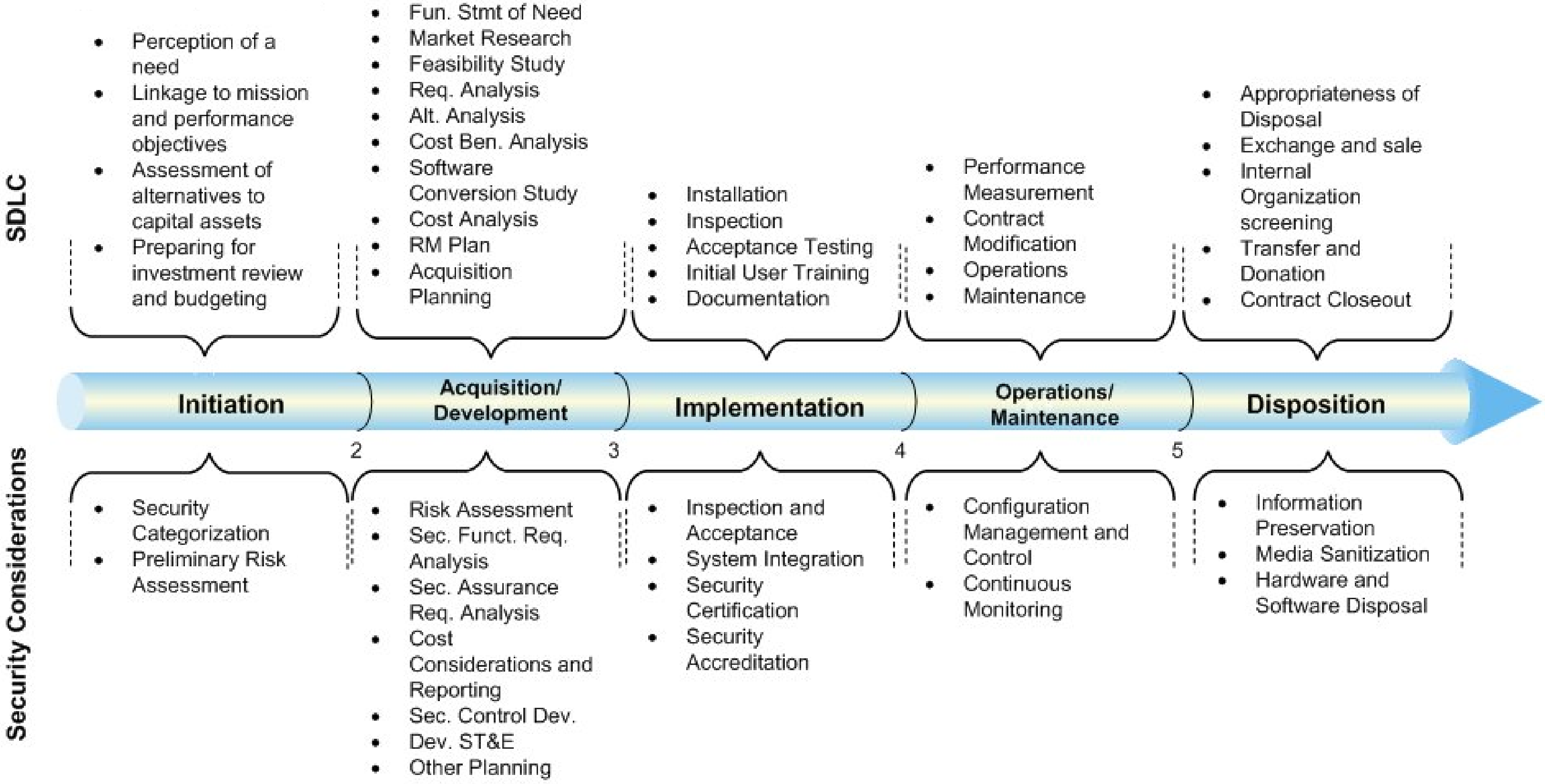
Mitigate common patterns - XSS, SQL injection, buffer overflow, factory default settings….

Input validations, error handling, privilege management, credential management

Data classification, handling, security considerations

Coding standards, Security policy, compliance requirements, security training

Security Considerations in SDLC



Initiation

SDLC:
- Perception of a need
- Linkage to mission and performance objectives
- Assessment of alternatives to capital assets
- Preparing for investment review and budgeting

Security Considerations:
- Security Categorization
- Preliminary Risk Assessment

Acquisition/ Development

SDLC:
- Fun. Stmt of Need
- Market Research
- Feasibility Study
- Req. Analysis
- Alt. Analysis
- Cost Ben. Analysis
- Software Conversion Study
- Cost Analysis
- RM Plan
- Acquisition Planning

Security Considerations:
- Risk Assessment
- Sec. Funct. Req. Analysis
- Sec. Assurance Req. Analysis
- Cost Considerations and Reporting
- Sec. Control Dev.
- Dev. ST&E
- Other Planning

Implementation

SDLC:
- Installation
- Inspection
- Acceptance Testing
- Initial User Training
- Documentation

Security Considerations:
- Inspection and Acceptance
- System Integration
- Security Certification
- Security Accreditation

Operations/ Maintenance

SDLC:
- Performance Measurement
- Contract Modification
- Operations
- Maintenance

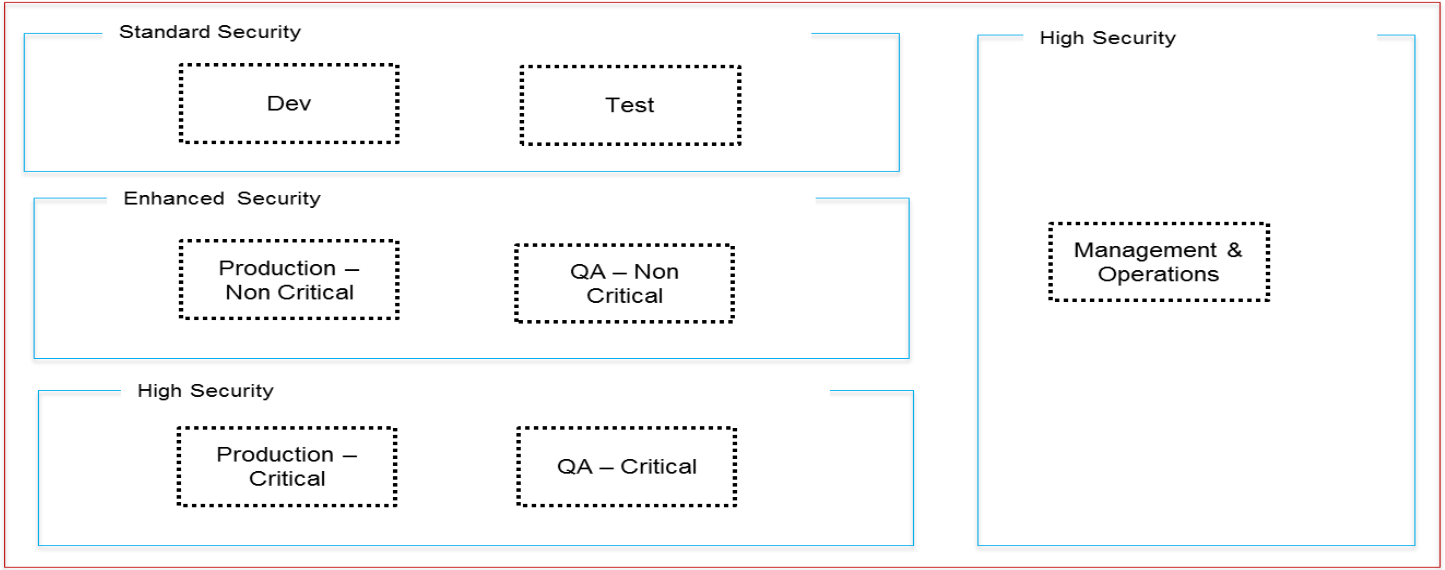
Security Considerations:
- Configuration Management and Control
- Continuous Monitoring

Disposition

SDLC:
- Appropriateness of Disposal
- Exchange and sale
- Internal Organization screening
- Transfer and Donation
- Contract Closeout

Security Considerations:
- Information Preservation
- Media Sanitization
- Hardware and Software Disposal

Security layers



Primary environment

Legend

□ Physically secured/controlled

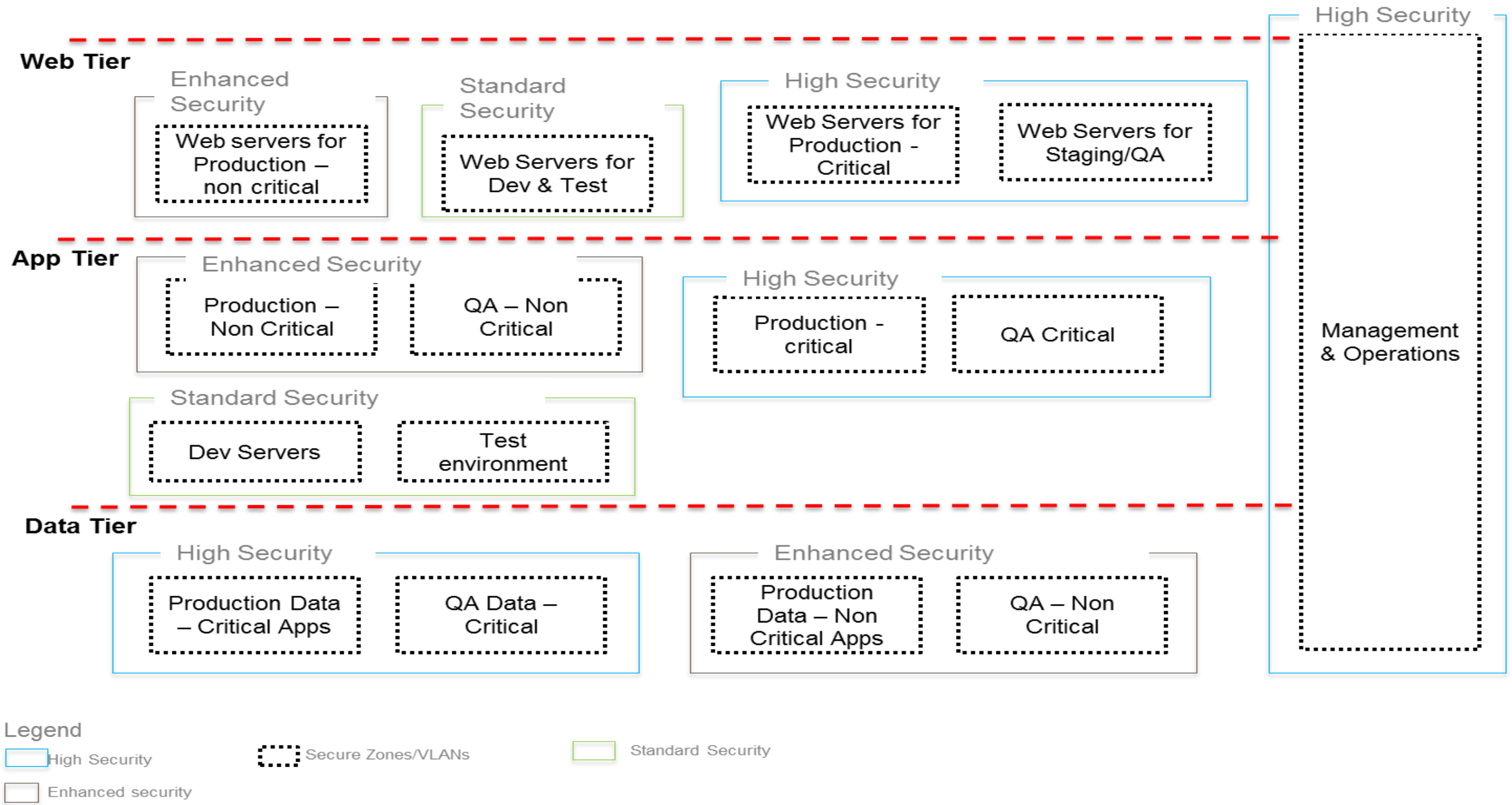
□ Physical, Air Gap instance of a collection of one or more logical environments

⬚ Environment

Key parameters influencing the architecture are -

1. Physical & environmental security
2. Technical controls within the infrastructure and processes
3. Security operations and management

Security segregation – Layers & Tiers, Applications and Data



Web Tier

Enhanced Security

Web servers for Production – non critical

Standard Security

Web Servers for Dev & Test

High Security

Web Servers for Production - Critical

Web Servers for Staging/QA

App Tier

Enhanced Security

Production – Non Critical

QA – Non Critical

High Security

Production - critical

QA Critical

Standard Security

Dev Servers

Test environment

Data Tier

High Security

Production Data – Critical Apps

QA Data – Critical

Enhanced Security

Production Data – Non Critical Apps

QA – Non Critical

High Security

Management & Operations

Legend

□ High Security

⬚ Secure Zones/VLANs

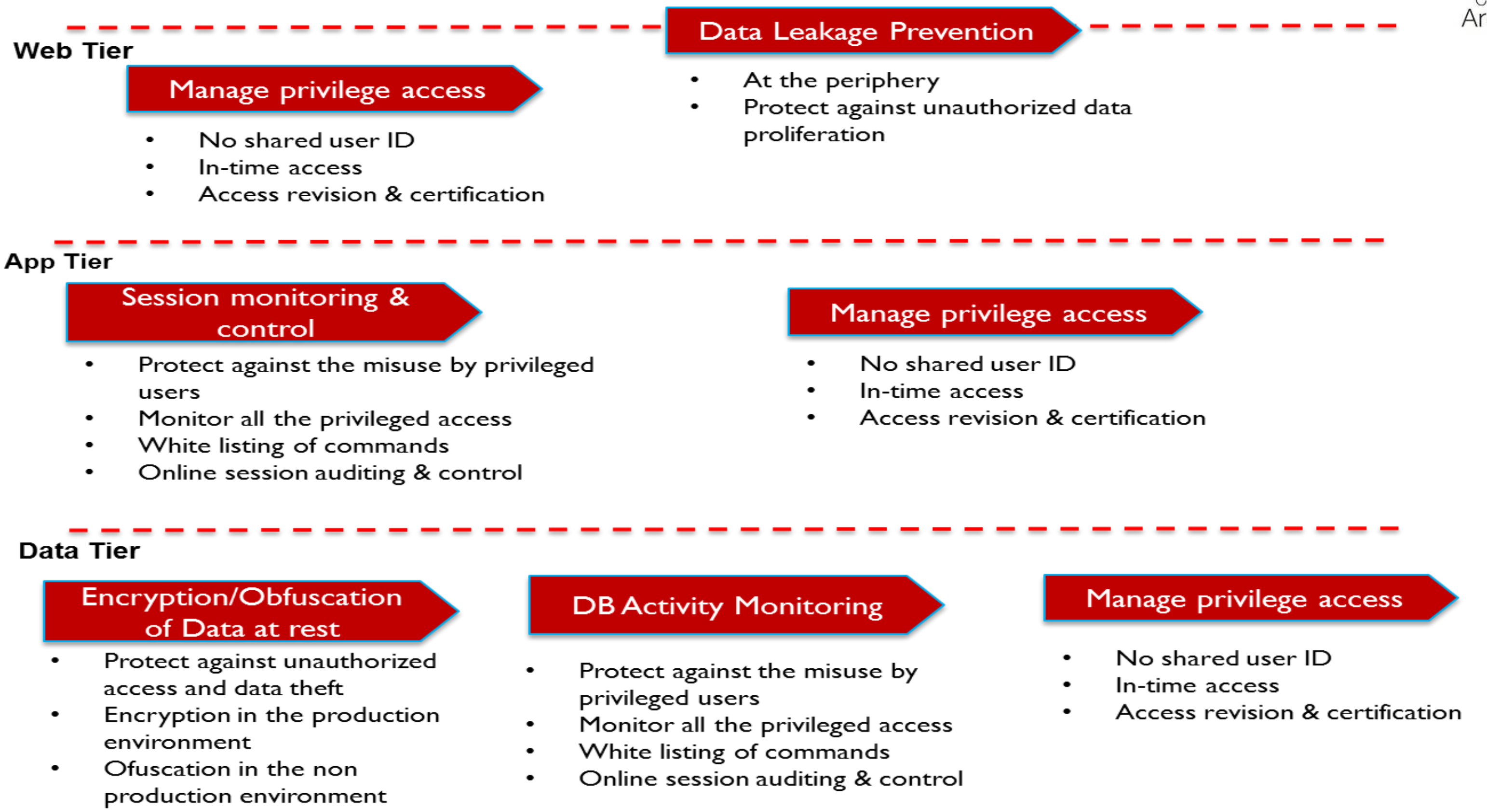
□ Standard Security

□ Enhanced security

Design Principles for the development team

1. Ensure the critical applications should be positioned in High Security Zone and/or in specific server pools.
2. Based on the criticality of data, logical/physical segregation, test data management needs to handled appropriately
3. No direct access from external to internal critical systems/data
4. Never use “factory default” settings
5. Integrating the security architecture (understand this architecture from your project’s security architect) within each functional tier
6. Security QA must be done along with regular QA
7. Design decisions, exceptions must be approved and documented

Data Security controls at leach Tier



Web Tier

Data Leakage Prevention

- At the periphery
- Protect against unauthorized data proliferation

Manage privilege access

- No shared user ID
- In-time access
- Access revision & certification

App Tier

Session monitoring & control

- Protect against the misuse by privileged users
- Monitor all the privileged access
- White listing of commands
- Online session auditing & control

Manage privilege access

- No shared user ID
- In-time access
- Access revision & certification

Data Tier

Encryption/Obfuscation of Data at rest

- Protect against unauthorized access and data theft
- Encryption in the production environment
- Ofuscation in the non production environment

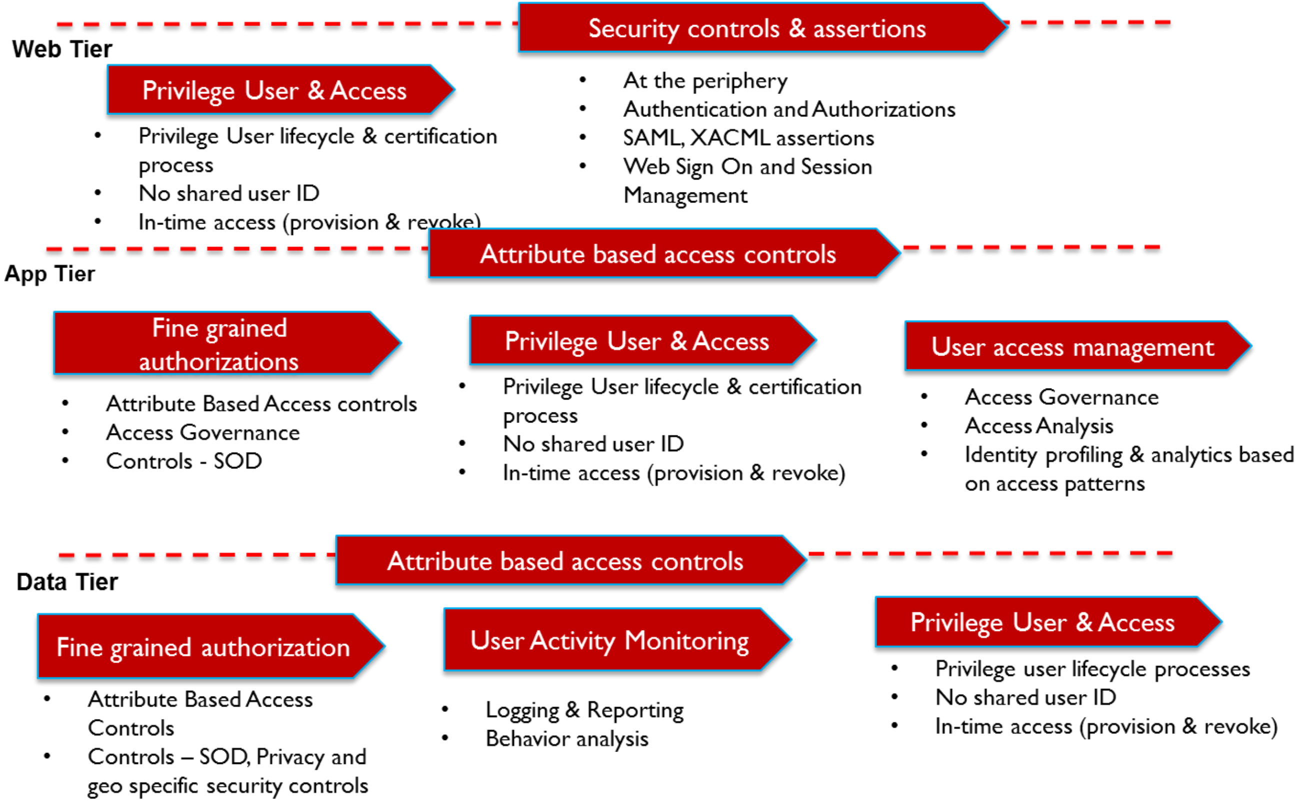
DB Activity Monitoring

- Protect against the misuse by privileged users
- Monitor all the privileged access
- White listing of commands
- Online session auditing & control

Manage privilege access

- No shared user ID
- In-time access
- Access revision & certification

Access controls at each Tier



Web Tier

Security controls & assertions

- At the periphery
- Authentication and Authorizations
- SAML, XACML assertions
- Web Sign On and Session Management

Privilege User & Access

- Privilege User lifecycle & certification process
- No shared user ID
- In-time access (provision & revoke)

App Tier

Attribute based access controls

Fine grained authorizations

- Attribute Based Access controls
- Access Governance
- Controls - SOD

Privilege User & Access

- Privilege User lifecycle & certification process
- No shared user ID
- In-time access (provision & revoke)

User access management

- Access Governance
- Access Analysis
- Identity profiling & analytics based on access patterns

Data Tier

Attribute based access controls

Fine grained authorization

- Attribute Based Access Controls
- Controls – SOD, Privacy and geo specific security controls

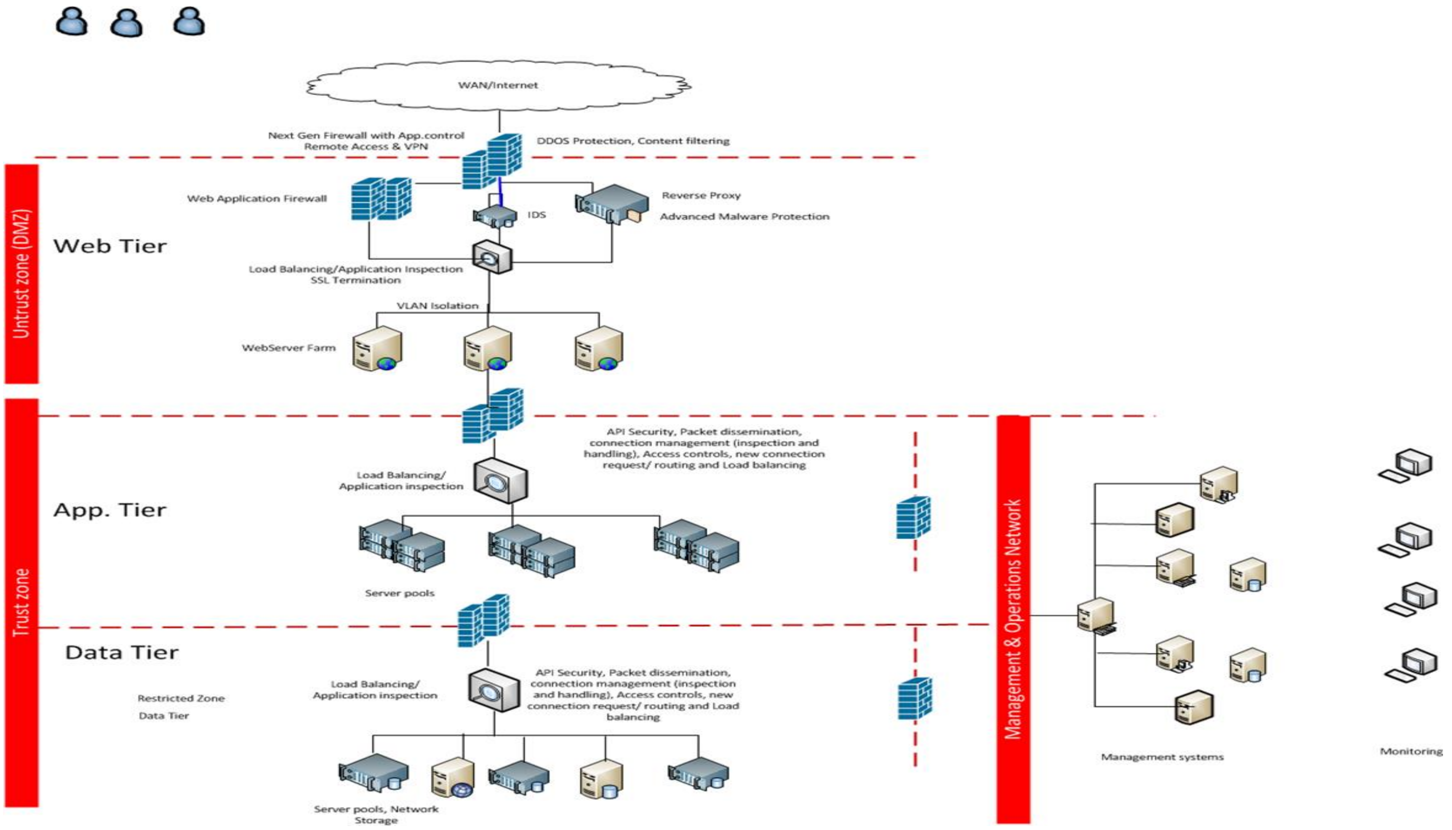
User Activity Monitoring

- Logging & Reporting
- Behavior analysis

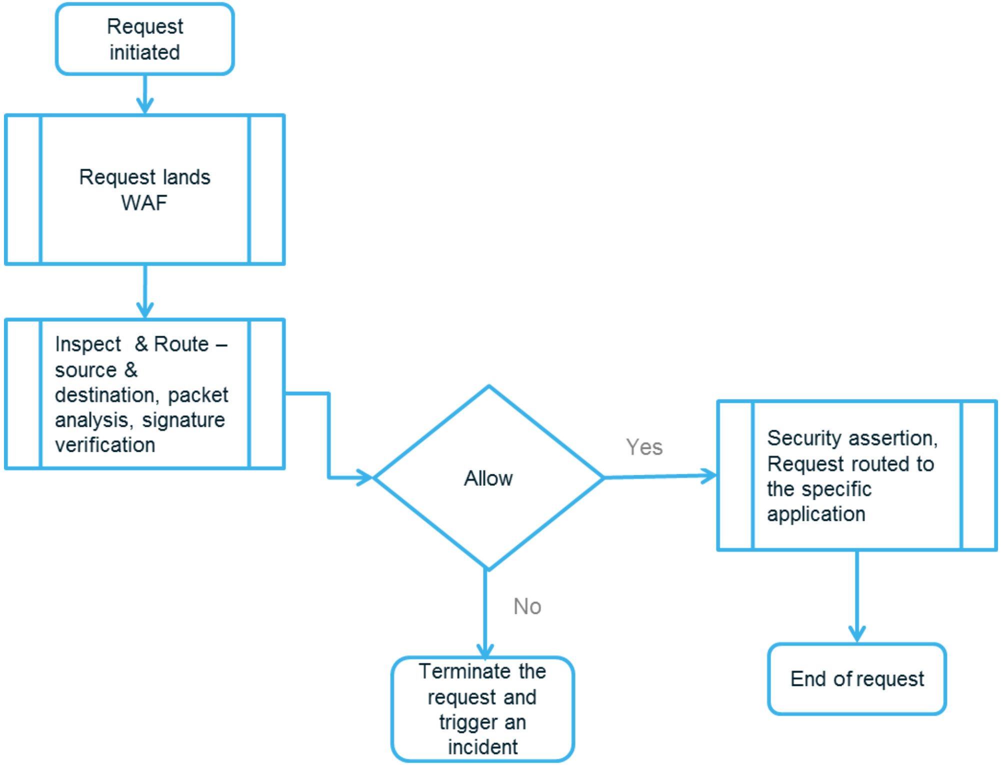
Privilege User & Access

- Privilege user lifecycle processes
- No shared user ID
- In-time access (provision & revoke)

Secure communication – a Sample flow


WAN/Internet
Next Gen Firewall with App.control
Remote Access & VPN
DDOS Protection, Content filtering
Untrust zone (DMZ)
Web Tier
Web Application Firewall
IDS
Reverse Proxy
Advanced Malware Protection
Load Balancing/Application Inspection
SSL Termination
VLAN Isolation
WebServer Farm
Trust zone
App. Tier
API Security, Packet dissemination, connection management (inspection and handling), Access controls, new connection request/ routing and Load balancing
Load Balancing/
Application inspection
Server pools
Data Tier
Restricted Zone
Data Tier
Load Balancing/
Application inspection
API Security, Packet dissemination, connection management (inspection and handling), Access controls, new connection request/ routing and Load balancing
Server pools, Network Storage
Management & Operations Network
Management systems
Monitoring

Data Flow – Request handling (Standard Security)



Request initiated

Request lands WAF

Inspect & Route – source & destination, packet analysis, signature verification

Allow

Yes

Security assertion, Request routed to the specific application

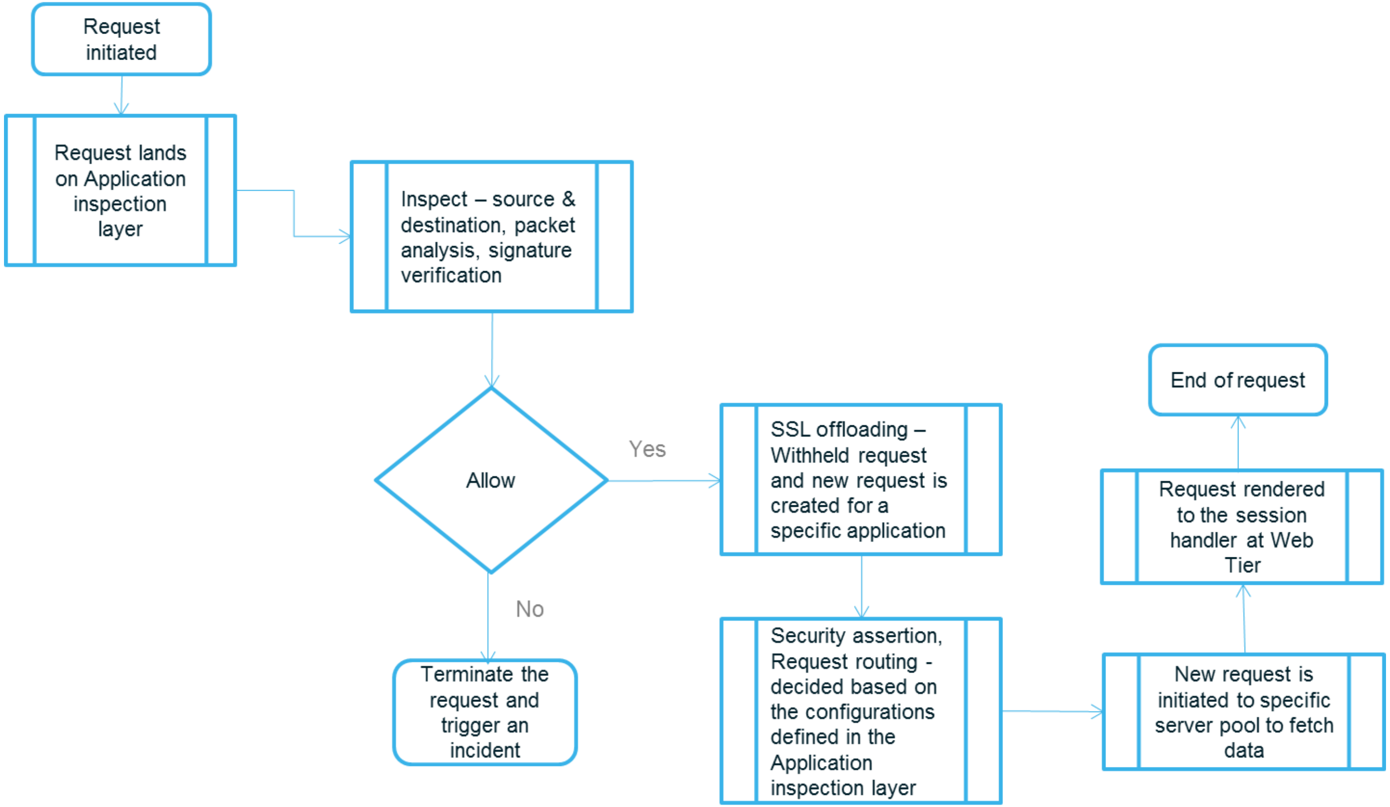
End of request

No

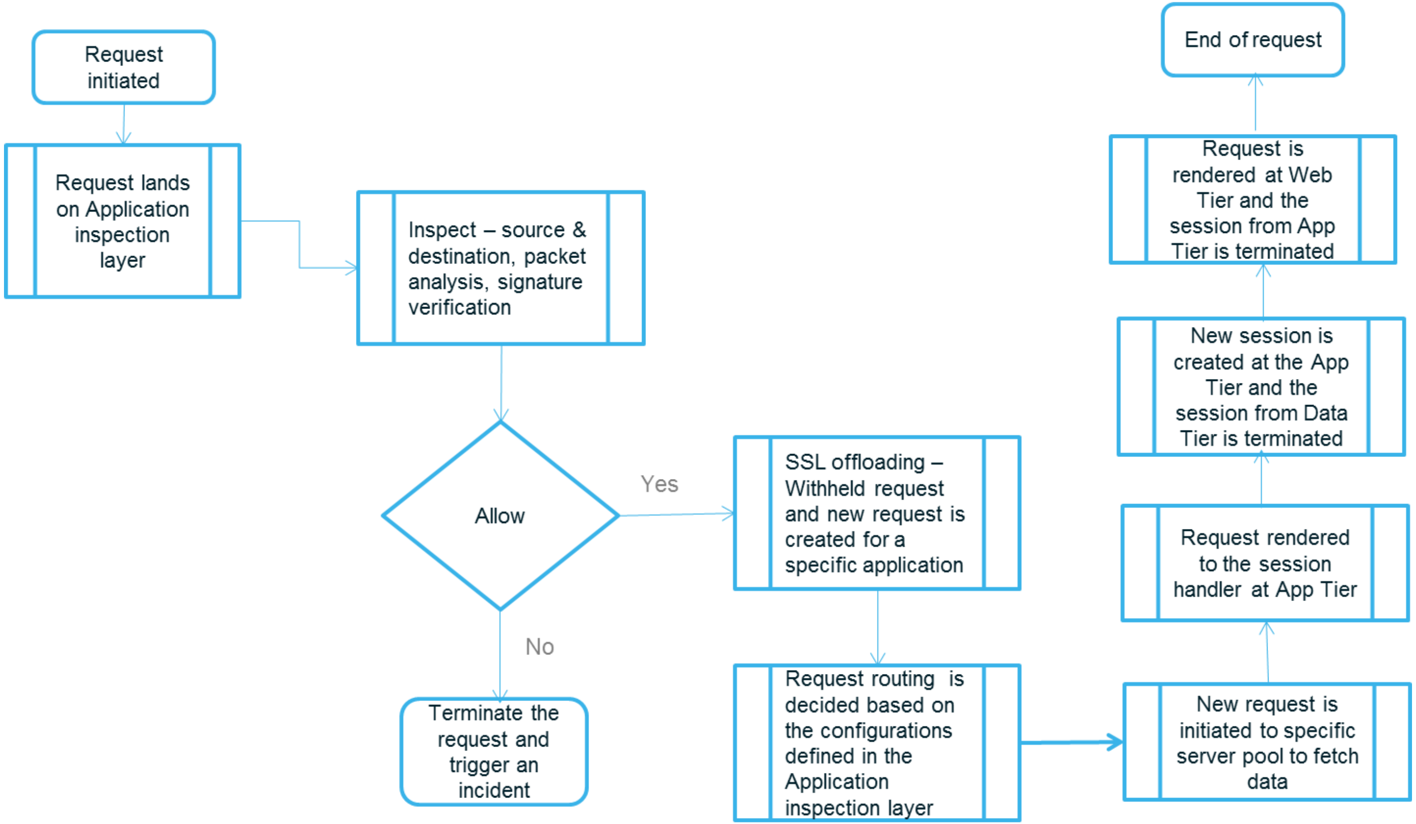
Terminate the request and trigger an incident

Data Flow – Request handling (Enhanced Security)

Connect Architecture


Request initiated
Request lands on Application inspection layer
Inspect – source & destination, packet analysis, signature verification
Allow
Yes
No
Terminate the request and trigger an incident
SSL offloading – Withheld request and new request is created for a specific application
Security assertion, Request routing - decided based on the configurations defined in the Application inspection layer
New request is initiated to specific server pool to fetch data
Request rendered to the session handler at Web Tier
End of request

Data Flow – Web request handling (High Security)



Request initiated

Request lands on Application inspection layer

Inspect – source & destination, packet analysis, signature verification

Allow

Yes

No

Terminate the request and trigger an incident

SSL offloading – Withheld request and new request is created for a specific application

Request routing is decided based on the configurations defined in the Application inspection layer

New request is initiated to specific server pool to fetch data

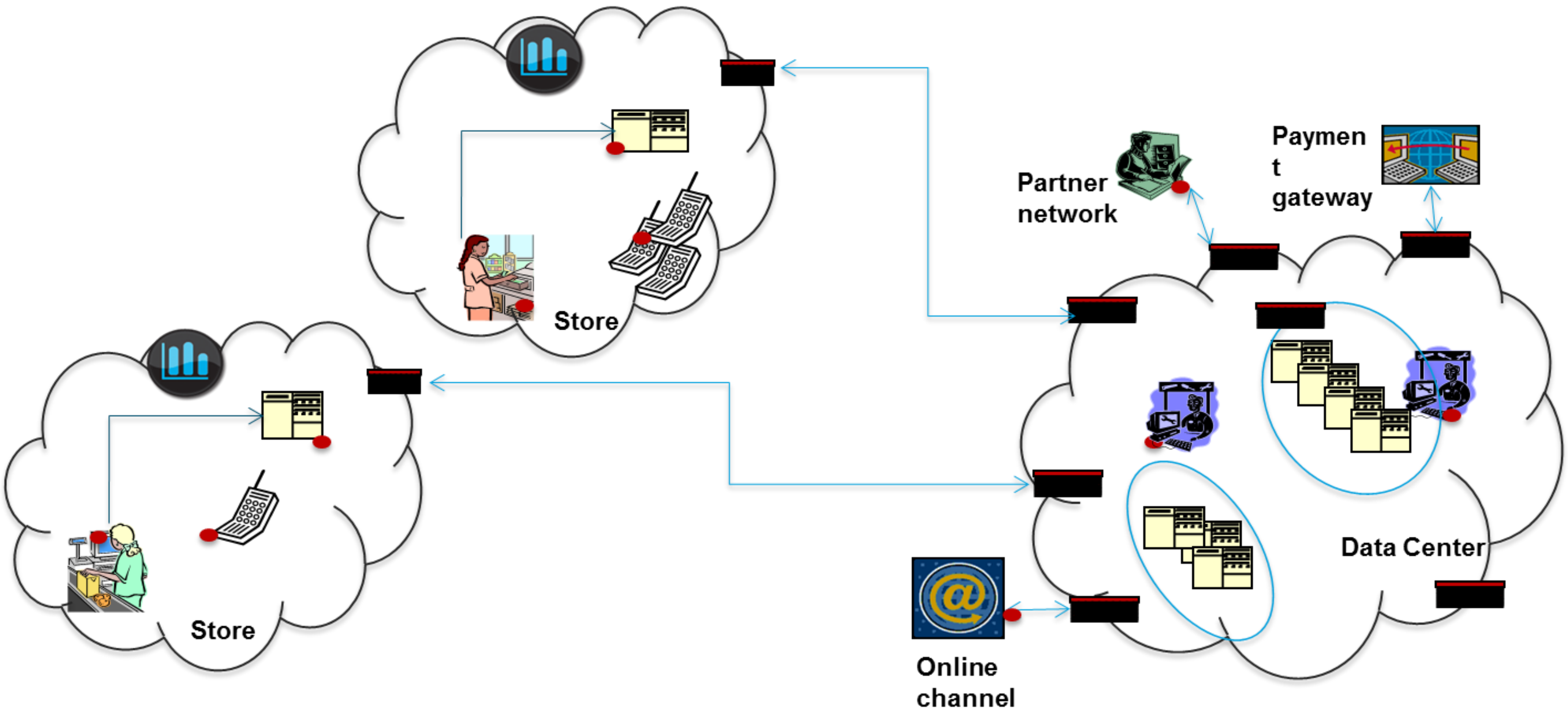
Request rendered to the session handler at App Tier

New session is created at the App Tier and the session from Data Tier is terminated

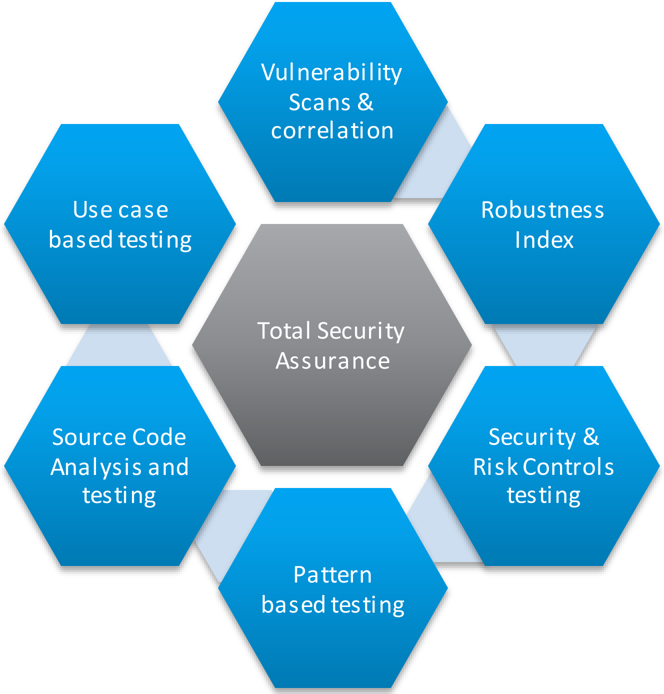
Request is rendered at Web Tier and the session from App Tier is terminated

End of request

Integration of Security with Functional requirements



Infosys Application Security Assurance Framework



Total Security Assurance

Vulnerability Scans & correlation

Robustness Index

Security & Risk Controls testing

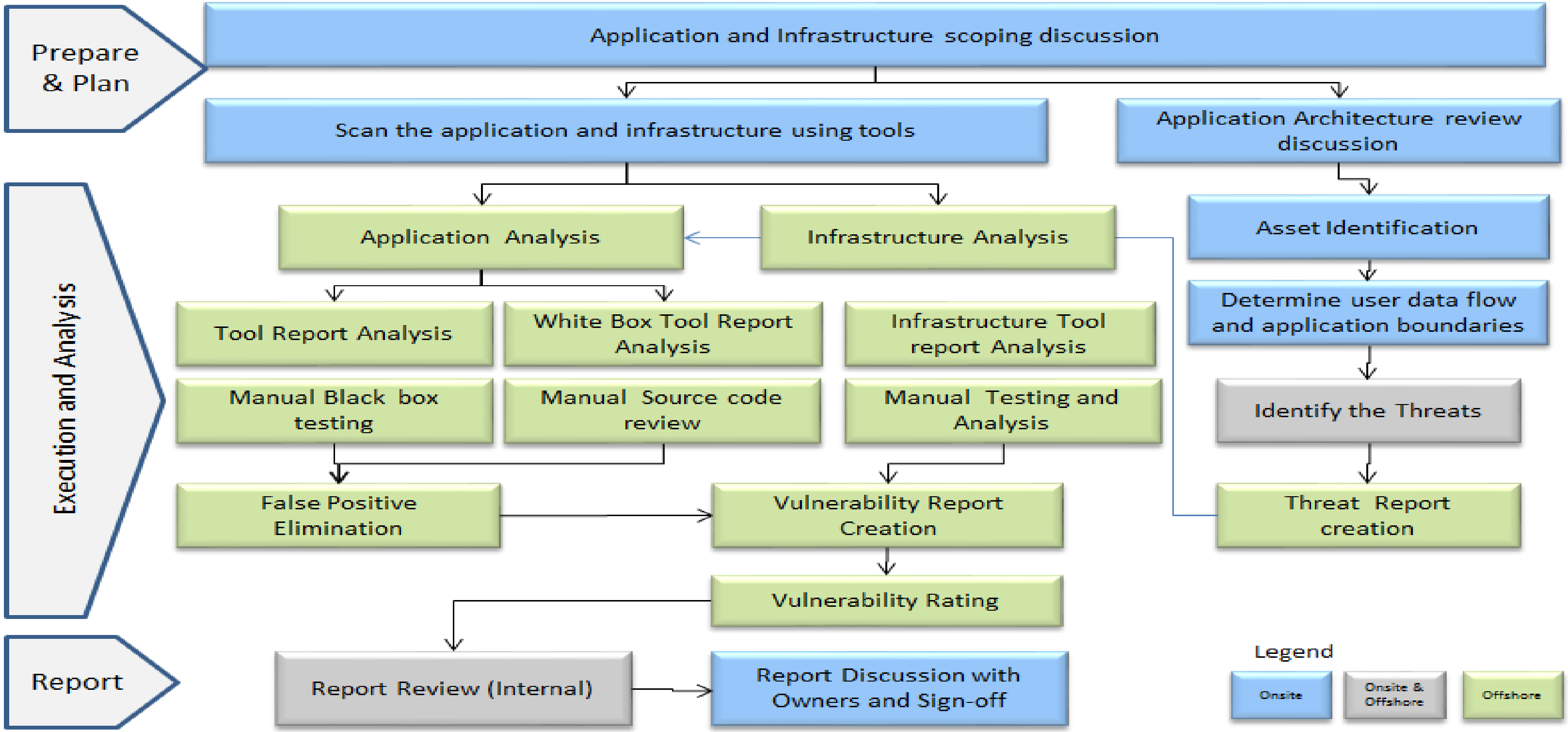
Pattern based testing

Source Code Analysis and testing

Use case based testing

- Vulnerability assessments of the environment, applications, use cases, data and processes
- Robustness Index based on negative Scenarios and strength of code, strength of the environment, security controls and underlying platform
- Minimum Baselined Security Controls required for the environment is tested. These controls are defined based on the Domain, Geo, Regulatory and Privacy requirements
- Security Platform & Service Standardization for Security QA
- Derived patterns based on past vulnerabilities, threat actions, process gaps. These patterns are used in defining new test scenarios and also to strengthen security and Risk Governance processes

Security Testing approach


Prepare & Plan
Application and Infrastructure scoping discussion
Scan the application and infrastructure using tools
Application Architecture review discussion
Execution and Analysis
Application Analysis
Infrastructure Analysis
Asset Identification
Tool Report Analysis
White Box Tool Report Analysis
Infrastructure Tool report Analysis
Determine user data flow and application boundaries
Manual Black box testing
Manual Source code review
Manual Testing and Analysis
Identify the Threats
False Positive Elimination
Vulnerability Report Creation
Threat Report creation
Vulnerability Rating
Report
Report Review (Internal)
Report Discussion with Owners and Sign-off
Legend
Onsite
Onsite & Offshore
Offshore

Sample deliverables

Web Security
Check List

Web Application
curity Analysis Brie

Summary Report
(Sample)

Case Studies

Case Study 1: Application security assurance & testing for a Leading Pharmaceutical Company

Approach

- Contextualize Infosys security assurance framework – testing controls and metrics to client's business processes and applications which needed to be tested
- Executions –
  - external and internal penetration test
  - Scanning – applications (web and enterprise)
  - Source code analysis
- Security posture creation - risk identification and scoring, gaps with security, regulatory and privacy controls
- Remediation roadmap and business case definition

Solution

- Manual and tool based analysis of identified set of applications
- Contextualized outcome of the analysis with use cases and by applying security controls
- Segregated security gaps by processes and configurations
- Remediate the gaps based on the approved roadmap and milestone definitions
- Retest and certify
- Appended Metrics and added testing controls to be part of Security QA for application onboarding

Result

- Security posture, Risk score of the gaps
- Business case development
- Gap remediation, retest and certify applications for security
- Provided specific security testing controls to be added into Client's QA process

Case study 2: Pre-audit security assessment for a US based Bank

Connect Architecture

Context

- ❑ The client is one of the worlds leading multinational bank, situated in USA
- ❑ It operates in over 130 countries around the globe
- ❑ Its subsidiaries and affiliates offer banking services, credit services and advisory fraud protection services to its worldwide customers

Drivers

- ❑ Customer was not satisfied by risk assessment done internally or by other third party vendor involved especially in the manual validation of Vulnerabilities.
- ❑ Even after security testing done, there were high rate of vulnerabilities found at production stage. This could make customer web application vulnerable to intrusion even after assessment.
- ❑ The customer was in need to comply to security compliance mandate for their web applications before release.
- ❑ There was no co-ordination between the security assessment team and the project development teams to fix the findings.

Challenges

- ❑ Unavailability of web-application & the testing could not be down due to unplanned downtime of customer test environment
- ❑ This hit reduced our deadline, which could not be extended since it would hit the overall project delivery schedule
- ❑ Unavailability of in-depth briefing about the application been tested. It was the highest challenge to understand the application and its logic before manual testing
- ❑ Understand the user code and business logic to disclose any vulnerabilities not detected by black box testing.
- ❑ Generating high quality and accurate reports in the first iteration of assessment.

Case study 2: Pre-audit security assessment for a US based Bank

Connect Architecture

Approach

- ❑ Infosys offered the Global Delivery Model to the customer to assess the web-applications.
- ❑ The already available Source code analysis scan setup with the customer was used to acquire source code scan result for code analysis for white box testing.
- ❑ Coupled with all the reports, Infosys offshore team conducted the manual security testing for validating and exposing the truly known vulnerabilities.
- ❑ These findings are then peer reviewed and built into a report for customer development team.
- ❑ The development team is then briefed with the findings and helped in fixing or understanding the vulnerability if required.

Solution

- ❑ Infosys built a team of security analysts offshore to assess the applications and a very small project management team for client interfacing at onsite. This reduced the total cost of engagement for the customer while enhancing the quality of deliverables.
- ❑ Infosys team scanned the application using various tools and rigorous manual testing, these reports are then analyzed and filtered for false positives.

Result

- ❑ Remove false positives by manual validation of findings from the tool scan.
- ❑ Highly technical and accurate security findings to assist development team in remediation & effective delivery through an assembly line model
- ❑ Designing & Creating customized technical reports and test case documents and reports
- ❑ Fast turn-out time even for large application assessment so that overall project delivery time is not hampered.
- ❑ Provide recommendations in the reports that could help development team in their future design and development work.

Thank You

Acknowledgements : Saritha Auti