TECHDEFENCELABS

CONTENTS

Disclaimer

This document is being submitted to SBAC BANK for describing Techdefence Labs (hereafter referred to as 'TD Labs' or 'We') to provide the services outlined herein. To describe our capabilities, TD Labs has disclosed certain proprietary and other sensitive information, which if disclosed to third parties, might harm TD Labs competitively. In consideration of receiving the disclosures, we request that SBAC BANK treat this document as confidential material.

This document shall remain the property of Techdefence Labs. The information in this document and any oral presentation conducted by TD Labs contains trade secrets and confidential and proprietary information of TD Labs. The disclosure of which would provide substantial benefit to our competitors. Accordingly, this document may not be disclosed, used, or duplicated—in whole or part—for any purpose other than evaluating TD Labs for purposes of awarding a contract.

Techdefence Labs retains the right to make changes to this document at any time without notice. Techdefence Labs makes no warranty for the use of this document & assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Copyright

Trademarks

Other product & corporate names may be trademark of other companies and are used only for explanation & to the owners benefit without intent to infringe.

Contact Details

COMPANY	Techdefence Labs Solutions Pvt. Ltd.
ADDRESS	5th Floor Swayam Complex, Opp. Vodafone House, Stadium Cross Road, Navrangpura – 380009

CONTACT NO	+91 79 40047405 | +91 756 786 7776
EMAIL	info@techdefencelabs.com
WEBSITE	www.techdefencelabs.com

1.Client Information

1.2 Statement of Work

Vulnerability Assessment and Penetration Testing for SBAC BANK is to be performed by Techdefence Labs. The aforesaid task includes all applications & servers provided by the client to be scrutinized for Security Testing.

The scope synopsis is given as below:

Security Assessment – Scope		
Sr. No	**In Scope Areas**	**Details**
1	ISO 27001	• Gap Analysis • Develop Policies, Procedures & Documentation • Statement of Applicability • Remediation Support • Risk Assessment • Internal Audit • Certification • Surveillance Audit • Awareness Training for 30 People • ISO Lead Auditor & Lead Implementer Training & Certification 05 Personnel
2	Vulnerability Assessment & Pen Testing	• Server 165 • Router 05 • NG Firewall 9 • Web Application Firewall 02 • Email Security Gateway 02 • Core Switch 04 • Total IP Address 300

Document Version – V 1.0		
Sr. No	**Key Personnel**	**Contact Details**
1	Mr. Sunny Vaghela - *Document Owner*	sunny@techdefencelabs.com
2	SBAC Bank&Designation	Client_Email

2.Overall Approach

2.1 Project Planning

Phase – I

Project Planning

This phase involves the activities pertaining to Project Plan activities. This will include formulating a project planning and project kick-off.

Activity 1 – Planning

This activity will entail proposed plan and finalize the tests

Activity 2 – Discussion with Technical Team and SBAC Bank's Team

Within this activity, the senior team at Techdefence Labs will conduct meeting with project team for scheduling activities, and co-develop a project plan, communication strategy and issue resolution process.

Also we ensure that there will be no effect on business and that any potential tests are carried out during non-working hours

2.2 Project Initiation

Phase – II

Project Initiation

This phase involves the activities pertaining to Project Management activities and resource mobilization. This will include formulating a project planning and project kick-off.

Activity 1 – Resource Mobilization

This activity will entail appointment and mobilization of project team *(SBAC Bank & TD Labs).*

Activity 2 – Project Planning and Kick-Off

Within this activity, the project team will conduct planning and scheduling activities, and co-develop a project plan, communication strategy and issue resolution process. Furthermore, TD Labs will conduct project kick-off meeting with the project steering committee to validate the scope of work and milestones/timelines for the activities.

Activity 3 – Project Plan Finalization

Prior to finalizing the project plan, we will discuss TD Labs tasks, milestones, dependencies with the concerned SBAC Bank's personnel and address any comments / suggestions as needed. Once finalized and approved by the authorities, the project plan will be used to execute and track project activities.

2.3 Project Execution

Phase III

Project Execution

This phase involves the following activities:

Activity 1 – Infra Security Review

This activity will entail security testing of the Network Infrastructure that includes by is not limited to the following areas:

- Infra Security review from Black Box / Grey Box penetration testing perspective.

2.4 Reporting & Knowledge Transfer

Phase IV

Reporting & Knowledge Transfer

This phase involves preparation of observations and close out focusing on the following areas:

- Identify remediation measures to be adopted & obtain agreement on the review findings and suggested remediation measures
- Conduct a close out meeting summarizing the agreed findings and action plans & Develop and provide the final report
- Conduct a knowledge transfer to the technical team.
- Present the findings to technical & management team.
- Hand over final set of deliverables to the client.

3. Detailed Methodology

3.1 IT Security Maturity Assessment :

3.1.1 IT Security Maturity Assessment Methodology

This is methodology that will talk about our understanding and the methodology we use to evaluate the maturity of the existing IT setup of an organization with a People, Process, Technology elements. The five levels of maturity, starting from Initial Stage where an organization is still in it's nascent stages of IT Security Maturity and most of the initiatives are ad hoc and reactive till a level 5 where it can boast it's practices to be extremely matured in line with the best in the industry across the globe, which it can further proudly mention in it's annual general reports for a higher investor assurance into the IT practices being followed within the organization.

Our controls are aligned to global best practices and compliance frameworks in context of Information Security & Risk Management. We have incorporated every control from ISO 27001:2013, PCI DSS 3.1, NIST SP 800-53, FISMA, HIPAA among others.

3.1.2 People Security Control Areas:

It is important for any organization to have right kind of people in the team. Policies de ned under this category will provide a security view to a recruiter, a manager as well as an employer.

Employment & Capacity Management Assessment

Employment & Capacity Management Assessment			
Existing Capacity of IT & IT Security Team Assessment	Technology Training Assessment	Learning, Development & Research Process Assessment	Employment Check & Background Verification Assessment

Employment & Capacity Management Assessment includes all the rules & regulations an employee is required to adhere to. It includes guidelines for an ideal recruitment process and an appropriate background verification checks, managing & evaluating the recruited people and ensure the capacity.

Existing Capacity of IT & IT Security Team Assessment

It includes the evaluation of the guidelines practiced for the technology training planning, management and evaluation of participants as per the business requirements.

Learning, Development & Research Process Assessment

It involves an analysis of the existing process of learning from previous incidents and accordingly developing the controls for the better security of the information and infrastructure of the organization.

Technology Training Assessment

It includes the evaluation of the guidelines practiced for the technology training planning, management and evaluation of participants as per the business requirements.

IS Awareness Assessment

IS Awareness Assessment			
IT Security Awareness Program Assessment	End Users & Top Management Awareness Programs	APT Simulation Test	Management & Strategy Training Program Assessment

Information Security Awareness Policy includes the guidelines for an ideal Security Awareness campaign and the activities needs to be performed such as social engineering drive, phishing trap, physical security break-in drive, various training programs on Fraud Investigation, Cyber Security Awareness, etc.

End Users & Top Management Awareness Programs Assessment

It involves the analysis of existing guidelines to plan, execute and evaluate Awareness Programs designed specially for end users and top management.

IT Security Awareness Programs Assessment

It involves an analysis of the existing practice of conducting an ideal Security Awareness campaign and the activities that needs to be performed such as social engineering drive, phishing trap, physical security break-in drive etc. including various training programs on Cyber Security Awareness.

Management and Strategy Training Programs

It includes the analysis of existing guidelines for organizing the training programs for the awareness of top management and to train them to handle the adverse situations with right approach.

3.1.3 Process Security Control Areas:

Business process engineering is one of the most crucial elements of the successful IT implementation. Technology brings structure, but right kind of process needs be built around People and Technology element to ensure efficient, improved outcome. The set of policies under

process element helps organization defining what process are required and responsible to deliver the desired output.

Information Security Management System

Information Security Management System			
Risk Management	Vulnerability Management	Incident Response Management System	Log Management System
Fraud Investigation Policy & Process	Disaster Recovery & Business Process Continuity	Incident Response Management System	Teleworking Policies & Procedures
Document Control Policy	Compliance Management	Social Media Guidelines	Online Reputation Management

One of the most important element of the entire Security Governance Architecture is ISMS, Information Security Management System. It provides guidelines to an organization for managing and monitoring security issues by minimizing the risk and ensuring business continuity.

Compliance Management

This includes the assessment of various compliance being taken by the organization along with the assessment of organization's activities to manage and meet the internal, external or regulatory compliance requirements.

Disaster Recovery & Business Process Continuity

It includes the assessment of existing approach and plan de ned by the organization for the disaster recovery and business continuity during a disaster situation.

Document Control Policy

It includes the assessment of organization's practice for managing and controlling the documentation including the documentation of policies, processes, third party agreements etc.

Incident Response Management System

It includes the assessment of incident response management plan and approach de ned by the organization for the reporting and handling of any incident that might occur in the organization along with the assessment of business continuity plan in case of an incident.

Physical & Environmental Security

Physical & Environmental Security		
Access Control Policy	Clean Desk Policy	Information Disposal Policy
Information Storage & Retrieval Policy	Equipment Security Policy	Third Party Access Control

Organization managing the security of their physical infrastructure protects itself from thousands unknown, unseen attacks and breaches. It provides guidelines to manage the physical access controls, dispose the information, storing and retrieving the information securely and also to ensure the security of customer data.

Access Control Policy

It includes the assessment of the access controls implemented by the organization to secure the physical infrastructure of the organization and to protect the business critical data and devices from unauthorized physical access

Third Party Access Control

It includes the assessment of access controls implemented by the organization to secure its physical infrastructure from the third party.

3.1.4 Technology Security Control Areas:

In today's time, well de ned IT infrastructure plays a critical role in organization's business process. A well de ned and well maintained IT infrastructure ensures the security of digital communication, information availability as well as data sharing and data accessing, Identity and Access Management with appropriate password protection, Vulnerability Management and perimeter security with Firewalls and Intrusion Detection Systems.

Host

Servers and end user systems plays a very critical role when we talk about the security of business critical data and processes. Properly configured servers and end user systems ensures the security of business critical information whether it is in rest or in motion, le sharing, User management with proper authentication, data backup and restore, Risk management, vulnerability management and system security with firewalls and malware protection.

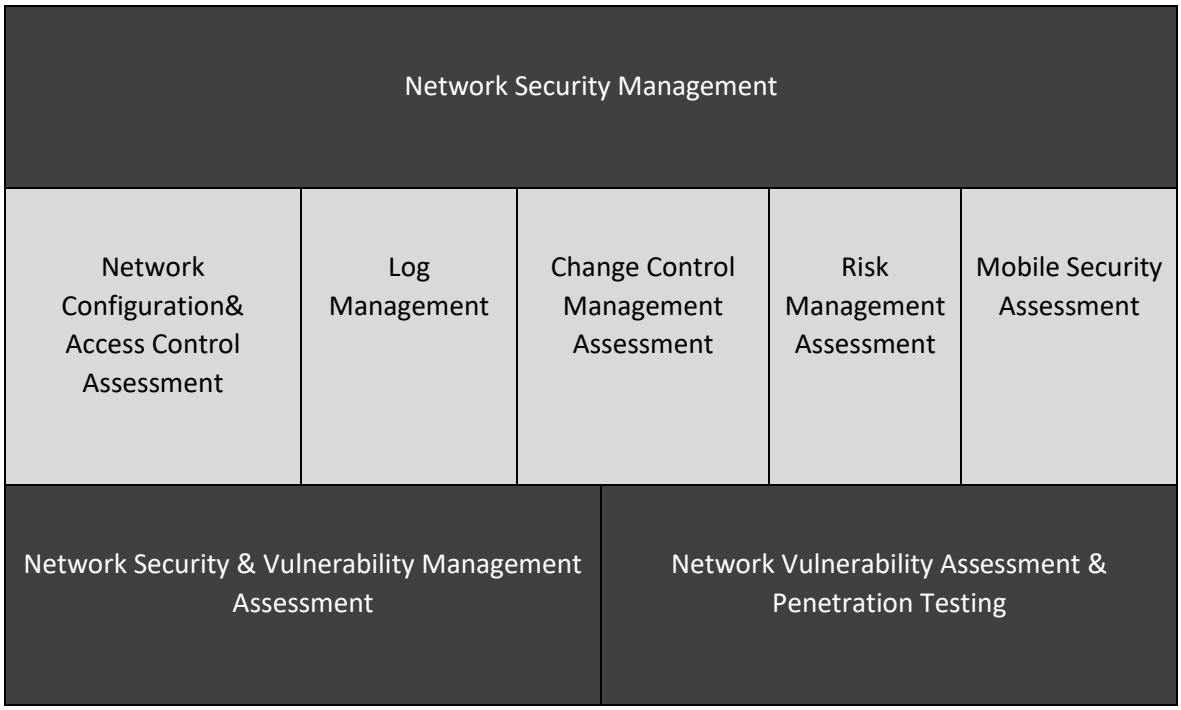
Application

Application Security plays a critical role in organization's business process. Secure and maintained applications ensures the security of organization's critical data, information availability as well as data sharing and data accessing, Identity and Access Management with appropriate password protection and Vulnerability Management.

Data

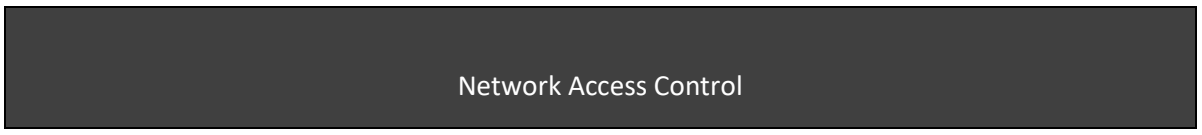
Data plays a critical role in organization's business process. Secure and monitoring data transfer ensures the security of organization's critical data, information availability as well as data sharing and data accessing.

Network Devices & Security System Assessment



In today's time, well defined IT infrastructure plays a critical role in organization's business process. A well defined and well maintained IT infrastructure ensures the security of digital communication, information availability as well as data sharing and data accessing, Identity and Access Management with appropriate password protection, Vulnerability Management and perimeter security with Firewalls and Intrusion Detection Systems.

Network Access Control Assessment



Network Assess Control Assessment	Firewall,IDS,IDPS,Management Assessment	Password Security Assessment	Remote Connections Access Control Assessment

It includes the assessment of the access controls implemented by the organization on technology infrastructure such as data, devices and tools owned by the organization.

Change Control Management

It includes the assessment of organization's approach to manage and control the changes required in the business processes as well as the technological environment along with the assessment of process defined to identify, calculate and mitigate the risks that might be introduced with the implementation of any change to the technological environment.

Email Access & Usage Management Assessment

It includes the assessment of configuration and management of email access of each employee working in the organization along with the assessment of guidelines defined for the secure usage of emails.

Firewall, IDS, IDPS Management

It includes the assessment of configurations of Security Systems such as firewall and Intrusion Detection System on the perimeter as well as between internal and external network and DMZ.

Mobility Security Assessment

It includes the assessment of the controls implemented by the organization for mobility - BYOD or CYOD, remote access, or usage of mobile devices in the organization network.

Internet Access & Usage Management Assessment

It includes the analysis of guidelines and procedure followed by the organization for permitting and assigning internet access to each needful user of the organization.

Log Management

It includes the assessment of existing process of retrieving and storing logs generated by each device participating in technology infrastructure for monitoring and further analysis.

Password Security Assessment

It includes the analysis of guidelines defined by the organization for the enforcement of a password policy to ensure the security of each user account, user device, business critical data and devices.

Server & End User System Assessment

System Configuration & Maintenance					
System Asset Management	Software Asset Management Assessment	System Configuration Management Assessment	User Management System Assessment	File Sharing Assessment	
System Access Control					
Firewall Configuration Management Assessment	Data Privacy & Protection Management Assessment	Password Security Assessment	Identity & Access Management Assessment		
System Security Management					
Removable Media Assessment	Log Management System Assessment	Malware Protection Assessment	Change Control Management Assessment	Data Backup and Restore Assessment	DC Security Assessment
System Security & Vulnerability Management Assessment	System Configuration & Access Control Management	Servers and EU Systems VAPT		Risk Management Assessment	

Servers and end user systems plays a very critical role when we talk about the security of business critical data and processes. Properly configured servers and end user systems ensures the security of business critical information whether it is in rest or in motion, le sharing, User management with proper authentication, data backup and restore, Risk management, vulnerability management and system security with firewalls and malware protection.

Asset Management Assessment

It includes the assessment of the process defined and practiced by the organization for the management and tracking of system assets.

Identity & Access Management Assessment

It includes assessment of process to manage the hierarchical access of each user working in the organization and also to ensure the availability of the data as per business requirement.

System Configuration Management Assessment

It includes the assessment of configuration defined and implemented by the organization for the hardening of systems for their security.

Malware Protection Assessment

Malware Protection Systems, perhaps one of the largest requirement for end user systems. It includes assessments of process to configure and maintain the malware protection systems on end user systems, servers as well as on the perimeter of the digital infrastructure.

File Sharing Assessment

It includes the configurations and management assessment of the le sharing for the easy data sharing between employees to avoid keeping sensitive data on the external environment or on the cloud.

Password Security Assessment

It includes the analysis of guidelines defined by the organization for the enforcement of a password policy to ensure the security of each user account, user device, business critical data and devices.

Application Security Assessment:

Application Security Management	
Application Vulnerability Assessment & Penetration Testing	Application Security & Vulnerability Management Assessment

Application Access Control Assessment	Change Control Management Assessment	Password Security Assessment	Log Management System Assessment
Vendor Management & Support Operations Assessment			

Application Security plays a critical role in organization's business process. Secure and maintained applications ensures the security of organization's critical data, information availability as well as data sharing and data accessing, Identity and Access Management with appropriate password protection and Vulnerability Management.

Secure Application Development Architecture Assessment

Secure Software Development Life Cycle	
Secure Application Development Architecture Assessment	Code Review Assessment

It includes assessment of guidelines defined by the organization to follow while developing application to ensure data security and availability.

Code Review Assessment
It includes the assessment of guidelines defined by organization to review code of each in-house or third party built application.

Application Access Control Assessment

It includes assessment of the access controls implemented by the organization in applications and applications access - such as data, devices and tools owned by the organization.

Change Control Management Assessment

It includes the assessment of organization's approach to manage and control the changes required in the applications as well as the technological environment along with the assessment of process defined to identify, calculate and mitigate the risks that might be introduced with the implementation of any change to the applications.

Application Vulnerability Assessment and Penetration Testing

It includes the assessment of organization's existing approach and process of performing periodic vulnerability assessment and penetration testing on the data, application and devices owned by the organization.

Data

<table>
<tr><td colspan="3">Data – At Rest</td></tr>
<tr><td colspan="2">Database Architecture Assessment</td><td>Database Access Controls Assessment</td></tr>
<tr><td colspan="3">Data – In Motion</td></tr>
<tr><td>Data Acquisition, Access & Sharing Policy</td><td>Support IT Assets – Support & Maintenance Policy</td><td>Log Management System</td></tr>
</table>

Data plays a critical role in organization's business process. Secure and monitoring data transfer ensures the security of organization's critical data, information availability as well as data sharing and data accessing.

Database Architecture Assessment

It includes assessment of the database architecture - tables - columns and even the way sensitive data has been stored. Data Acquisition, Access & Sharing Policy It includes the assessment of controls implemented by the organization to ensure data acquisition, access to data & sharing of the data.

Database Access Control

It includes the assessment of controls implemented by the organization to ensure and protect data from the unauthorized access.

3.1.5 Gap Analysis :

Techdefence Labs will perform Gap analysis and Risk Calculation which will further lead to the generation of the organizations overall IT Security Maturity Score Card.

		Liklihood				
		Rare Event may occur in exceptional Cases	Unlikely Event could occur once in Six months	Moderate The event could occur once in quarter	Likely The event could occur every month	Certain The event could occur daily
	LEVEL	1	2	3	4	5
Minimal – Small gap, No Financial Losses	1	1	2	3	4	5
Minor – Small gap, Moderate Financial Loss	2	2	4	6	8	10
Moderate Moderate Gap, Moderate financial Loss	3	3	6	9	12	15
Major Major gap Major financial Loss	4	4	8	12	16	20
FATAL Critical gap, Major Financial loss for longterm	5	5	10	15	20	25

Risk Score	Risk Level	Maturity	Description
0	Minimul	Optimising	No Financial Impact If Exploited
1-3	Low	Fully Managed	May or May not have financial Impact If Exploited
4-7	Medium	Partially Managed	Modrared Financial Imact If Exploited
8-14	High	Defined	Probability of Reputation Loss, High, Potential financial risk if exploited
15-25	Critical	Initial	High Probability of Reputation Loss, high, potential financial risk if exploited

3.1.6 MATURITY Level Definition:

Initial (0-1)

Basic Infrastructure Security setup, ad-hoc activities, initial executive awareness, undocumented process; changing capability may be in place with some technology and tools; limited local processes; limited organizational support.

Defined (1-2)

Defined capability is in place with significant technology and tools for some key resources and people; processes defined for some regions and/ or business units; organizational guidance and support is in place for some key regions and/or business units.

Partially Managed (2-3)

Partial capability is in place with a combination of some technology and tools; key resources and people, local processes covering some regions/business units or processes are repeatable but may not be good practice or maintained; limited organizational support to implement good practice.

Fully Managed (3-4)

Mature capability is in place with advanced technology and tools for most key resources and governance body; consistent processes exist for most regions and/or business units; some governance is in place (accountability/responsibility/metrics).

Optimizing (4-5)

Advanced capability is in place which is leading-edge technology and tools for all key resources and people; consistent process across regions and business units; effective governance is in place (accountability /responsibility/continual monitoring for improvement).

3.1.7 MATURITY Assessment Process:

Techdefence Labs will begin assessment of the scoped elements under People, Process and Technology to understand and identify Gaps in existing business process and also by performing Vulnerability Assessment & Penetration Testing on business-critical Servers, Applications as well as Network Devices.

Step 1: Face to Face Interviews: Identify key stakeholders & conduct face to face interviews.
Step 2: Document Screening: Identify & obtain key documents to understand the present policies & regulations.
Step 3: Onsite Assessment: Based on the documents & the reviews obtained in the previous stages, assessment of the organization is conducted across People, Process & Technology.
Step 4: Gap Identification: Based on the assessment gaps are identified.

Step 5: Project Delivery & Security Roadmap Design: Based on Assessment, Project report containing maturity score for different parameter to be submitted along with Security Maturity Enhancement Roadmap.

3.1.7 IT Security Maturity Assessment Deliverables:

Techdefence Labs will submit detailed maturity assessment report along with compliance status of o rganization based on NIST, HIPPS, SANS, FISMA & ISO 27001:2013 Standard.

3.1.8 IT Security Maturity Enhancement Roadmap:

Techdefence Labs will share all the reports and a CXO summary with pinpointed actionable items along with guidelines of what exactly needs to be done to them in order to enhance the maturity level.

1. **Information Security Policy Formulation**
2. **Training Calendar Designing**
3. Based on the existing maturity level, Techdefence Labs will provide fixes for all the gaps as,

- Long Term Fix
- Short Term Fix

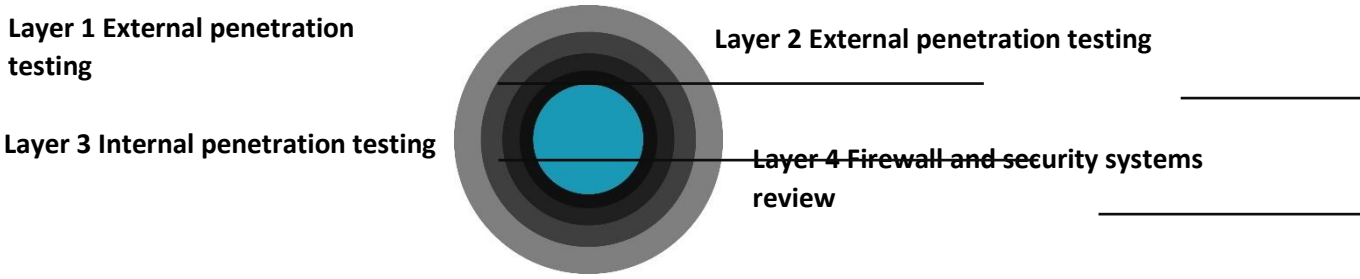
Both the fixes will be further categorized as,

- Free of Cost Solutions & Commercial Solutions
- **90 Days Cover to implement free of cost solutions.**

3.2 Infrastructure Security Testing

To facilitate the provision of this service to our clients, we have designed an approach that identifies the most serious risks and security flaws first and then focuses on less obvious areas as the project proceeds. This can be illustrated by the onion skin model. Our model illustrates how we first test the client network for vulnerabilities from the outside. Initially, we will conduct this test assuming the point of view of an uninformed attacker. We then gradually move on until we assume the role of a trusted user of the network trying to access an unauthorised resource or service. The following list gives some more detail as to the specifics of each level.

3.2.1 Layered Approach



Layer 1 External penetration testing (naive hacker)

• Establish whether unauthorised logical access can be gained via the external network interfaces by a 'naive' hacker who has limited and/or no previous knowledge of your network.

Layer 2 External penetration testing (supplier/customer level access)

• Establish whether unauthorised logical access can be gained, via external network components by a hacker who has the same level of access as your customers and suppliers, to the target production environment and other key systems.

Layer 3 Internal penetration testing (unauthorised user)

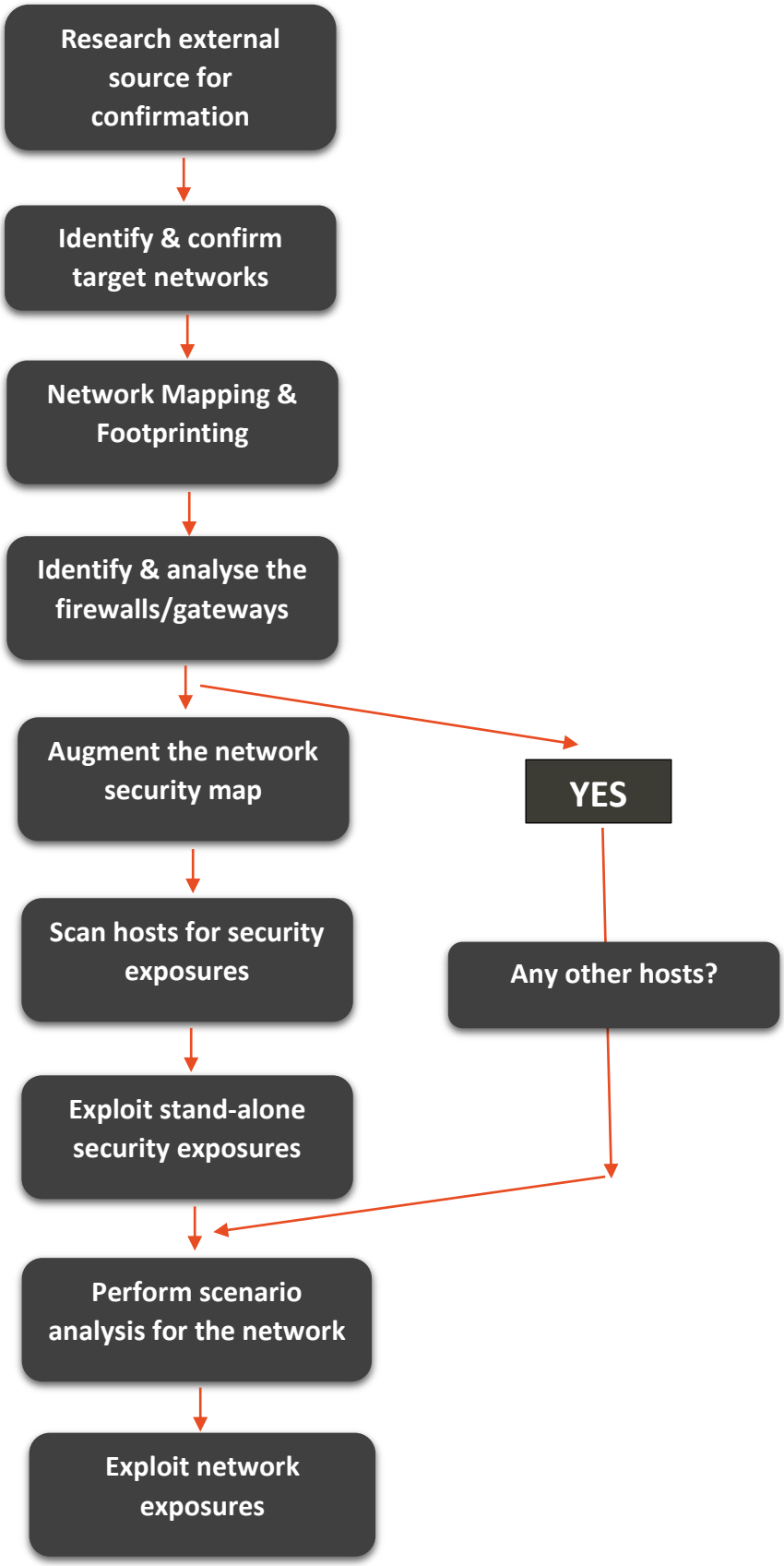
• Ascertain whether unauthorised access can be gained via internal penetration and audit testing of your systems by exploiting loopholes in your networks services and resources.
• Determine whether it is possible to manipulate key controls implemented for the protection of your system(s).
• Assess whether existing procedures for responding to such a breach of security are adequate and effective.
• Assess the security of certain sensitive servers and workstations.

Layer 4 Firewall and security systems review

• Analyse the effectiveness of the policies employed by your firewalls and the infrastructure in place for administration. Review the operating system configuration for a secure implementation.
• Review your procedures and processes for monitoring and reporting of incidents on the firewall. Review network and host security components, for example, IDS.

The consistent deployment of this approach is ensured using cutting edge technology, and our policy to only use highly specialized staff that works in this area with the use of comprehensive work-programs to enhance our quality control procedures.

3.5.2 Infrastructure Security Testing Process



Retrieve and document information about your organisation and systems from:

- The Domain Name Service (DNS);
- The Internet registration database (RIPE);
- Bulletin boards, forums and other social media;

• The web;
• Other relevant sources.

Identify and analyse the front-end router for:
• Active ports;
• Login ports for remote access;
• SNMP (if active);
• Finger (if active);
• Supported routing protocols

Identify and analyse the firewall by:
• Identifying all active TCP ports;
• Identifying all active UDP ports;
• Establishing the security rule base;
• Testing for known security flaws.

Iteratively identify and analyse accessible machines in front of and behind the firewall which can be identified as a host;
• Have an active TCP session established;
• Have an active UDP port identified;
• Be tested for known security flaws.

Iteratively identify and exploit vulnerable systems using: public vulnerability information;
• Configuration errors;
• Design errors.

Conduct a series of scenario analysis over the entire network to establish:
• What unauthorised traffic can be passed to the local area network (LAN);
• What security exposures can be exploited on the target systems.

3.2.3 Infrastructure Security Testing tools

Commercial Tools

- Tenable Nessus

Free Tools

- Metasploit
- Nmap
- Nikito
- Kali Linux
- Wireshark

4. Project Deliverables

4.1 Deliverables

Management Summary

Techdefence labs submits management report end of the testing process which includes followings

- High Level Findings
- High Level Recommendations
- Graphical Summary

Technical Report

We will submit comprehensive developer report which includes followings

- Title of the finding
- Severity Rating
- Ease of Exploitation
- Vulnerability Classification (OWASP/WASC)
- Description & Analysis

Conclusion

- Overall assessment of the security, of organization, & statements summarizing our opinion of the security levels as per defined standards.

4.2 Tools

Commercial Tools

- Burpsuite Pro
- Nessus

Open Source Tools

Metasploit	Nmap suite	Wireshark
Kali linux	Nikto	Pwdump
Brutos	SSLScan	WordPress scan
Pen-Test tools	APK Tool	Dex2jar
JD GUI	Dexplorer	MobSF
Cycript	Clutch2	0tool

5. Project Management & Quality Assurance

We have strong project management process to undertake large-scale security integration projects. Our process includes quality management, risk management, issue resolution, activity and milestone tracking and communication management.

5.1 Project Organization

5.1.1 Techdefence Labs Team:

- Our Project Team will be headed by senior resource designated as project lead, who will be responsible for successful project execution including management activities.
- Project lead will be primary contact between Techdefence Labs and Client Team. He will have sufficient authority to take decisions on behalf of company for scope of work defined.
- Project lead will report to CTO / COO at Techdefence Labs, who will also provide him/her guidance to measure performance of project.
- Project team will comprise of resources as per tasks/milestone to be achieved in each phase that will be committed to the phase throughout its duration.

5.1.2 Client Team

- Client will provide Project Lead from their end which holds final responsibility for achieving the project deliverables. He/she should have appropriate authority to resolve issues, approve and change project plan. He will also provide overall direction and decision making for the project from client's end.
- A project co-ordinator will work with the project team to facilitate information collection, interaction within client organization and coordinating with all activities done by Project team from Techdefence and Client team.
- Depending upon complexity of project, there may be requirement for project staff for administrative related activities.

5.2 Project Plan

Techdefence Labs team will prepare final project plan at the beginning of the project that will list down set of tasks and timeline for achieving the same.

The Plan will contain following:

1. Project Phases,
2. Objectives and client expectations.
3. Implementation plan with milestones.

5.3 Information Management

Our Information Management process will cover following aspects:

5.3.1 Project Management Flow

To manage information to and from the project team, we will setup common mail id which will act as central point for requesting information, collecting information and sharing information between project teams.

5.3.2 Document Management

The Project team will setup document library to facilitate collection, organize and retrieval project documents including scope details, reports, project plans, execution plans

5.3.3 Client Communication

Our formal project communication will consist of

Progress Report:

Techdefence Labs team will deliver progress report at regular interval for client's management on agreed upon schedules throughout the life cycle of project

Progress Meeting:

Techdefence Labs will conduct weekly progress meeting with Project lead (Client Team) and Coordinator to share details about project status, resolution of issues, next week agenda.

Executives Presentation:

Techdefence Labs will prepare and deliver presentation on Project Status, brief about findings of vulnerabilities to be shared with top management during and after completion of the project

5.4 Project Completion

Projects are formally closed to ensure that all deliverables meet client expectations and those which are defined during initial phase. The process involved is

Project Sign-off: A formal sign-off is obtained from client as per the form which captures objectives, expectations and timelines of project execution.

Project Feedback form: The client's experience in interacting with project team and the quality of deliverables is formally measured through client's feedback form.

5.5 Project Support

We believe in continuous relationship with client and therefore provide strong after-project support.

The support extends

- Knowledge transfer to client team.
- Technical query resolution.
- Periodic reviews of security initiatives.

Periodic training to understand current trends, emerging risks and security solutions.

6. Information Security Consultant Profiles

6.1

Name: Nikhil Srivastava **Designation: VP Information Security**	
Profile Summery	Nikhil is VP- Global Information Security at Techdefence Labs. His area of expertise includes vulnerability assessment, Penetration Testing, Source Code Reviews, Information Security Trainings.
Educational Qualifications	B.Tech in Information Technology from Rajasthan University , India
Professional Experience	6+ Years
Certifications	Certified Ethical Hacker – EC-council, USA EC-council security Analyst – EC-council, USA Licensed Penetration Tester- EC-council, USA License No. KS12-502

Technology Summary

Security Tools	Burp Suite, Acunetix, IBM Rational Scanner, W3af, Iron WASP, Scanda, Dominator, Swfscan, Nmap, DirBuster, xenotix, Xcat, Echo mirage, Java snoop, Tessercap, Reflector, BurpJDser, Curl, Ldapblindexplorer, Nikto, paimei, afd, SQLmap, Metasploit framework, Ollydbg, Windbg.
Firefox Add-on	Hack bar, Tamper data, Live Http headers, Cookie manager+, Firebug, No-redirect, Wappalyzer, Ghostery, and Elite Proxy Switcher.
Programming Languages	C, C++, Perl, Php, Python, Java, Ruby
Server Software Configuration	Apache, DNS, DHCP, Ldap
Internet Technology	Html, Html 5, XML, Ajax, JavaScript, SOAP, REST,WSDL, Angular, ECMA
Database	Mysql, MSSQL, Oracle, Sybase, Postgresql
Operating System	Windows, Linux, Mac

Project Execution Summary

Project Executed	**He has successfully completed projects across below verticals** • Telecom Service Providers • Medical Centers • Banking & Financial Sector

	• Stock Trading Applications • WAF Testing • Online Media • Online Professional Services • Startups • Job Portals

Information Security Research

Security Research Advisories	His research folio includes following: 1. **Discovered 0day Vulnerability in WordPress 3.6** - The Advisory has been published earlier under secunia and available at www.secunia.com/community/advisories/54803 CVE details: CVE-2013-5738 http://osvdb.org/show/osvdb/97214 **2. Discovered Cubecart Online Shopping-Cart 0-day Vulnerability** - The advisory has been published under http://forums.cubecart.com/topic/47719-cubecart-524-released/ . CVE-ID details: CVE-2011-4550 **3. Discovered 0day in Tiki Wiki CMS Groupware version 11.0** – The advisory has been published under http://www.kb.cert.org/vuls/id/450646 CVE Details: CVE-2013-6022 **4. Discovered 0day Vulnerability in Cs-Cart** –The advisory has been published under http://www.kb.cert.org/vuls/id/405942 CVE details: CVE-2013-7317 **5. Magento E-COM Security Advisory** – The advisory has been published under https://magento.com/security/patches/supee-7405 **6. Umbraco CMS Remote Code Execution:** A remote code execution vulnerability discovered in Umbraco CMS (http://umbraco.com/) The advisory has been published under http://issues.umbraco.org/issue/U4-5901 **7. Vertical Privilege Escalation in Umbraco CMS – The advisory has been published under** http://issues.umbraco.org/issue/U4-5891 **8. PHPMyFAQ Multiple Vulnerabilities**

	SQL Injection vulnerability: CVE-ID: CVE-2014-6045 Incorrect enforcement of privilege restrictions: CVE-ID: CVE-2014-6047 Direct request to the URL of an attachment: CVE-ID: CVE-2014-6048 Multiple CSRF vulnerability: CVE-ID: CVE-2014-6046 Insecure direct object reference vulnerability : CVE-ID: CVE-2014-6049 Insecure captcha implementation: CVE-ID: CVE-2014-6050 **9. Discovered 0day Vulnerability in WordPress Plugin WordFence Security.** The advisory has been published under CVE details:CVE-2014-4932
Hall of Fame	Tesla Security Researcher Acknowledgement https://www.teslamotors.com/about/security Telekom Security Acknowledgement A program by Deutsche CERT, Reported multiple high and medium severity vulnerabilities. For more info http://www.telekom.com/security/acknowledgements Barracuda Network Security Acknowledgement Found Multiple Serious Vulnerabilities in Barracuda Services, as a token, they rewarded me with huge bounty and provided with highest level (MASTER) in their wall of fame. https://barracudalabs.com/research-resources/bug-bounty-program/bug-bounty-hall-of-fame-2/ Wordpress Multisite Multiple Vulnerabilities (Stored Cross Site Scripting, Reflected Cross site scripting, SQL injections) rewarded with 1000$ and Security researcher acknowledgement here https://managewp.com/white-hat-reward Microsoft Security Researcher Acknowledgement for finding Flash based cross site scripting issue on msn.com, researcher acknowledgement here http://technet.microsoft.com/en-us/security/cc308575 11. Coinbase Security Researcher Acknowledgement for finding Flash based Cross Site Scripting issue and Cloud Flare cache hitting issue with their web application. https://coinbase.com/whitehat 12. Blackberry Security Researcher Acknowledgement for finding Stored Cross site scripting and Cross site request forgery in blackberry USA web application. http://us.blackberry.com/business/topics/security/incident-response-team/collaborations.html 13. Adobe Security Researcher Acknowledgement for finding SQL injection and Flash based Cross site scripting issue in Adobe Web

	application. http://www.adobe.com/support/security/bulletins/securityacknowledgments.html 14. Nokia Security Research Acknowledgement for finding SQL injection, Stored Cross site scripting and flash Based Cross site scripting in Nokia. Nokia rewarded with token as Nokia Lumia 920 and acknowledgement. http://www.nokia.com/global/security/acknowledgements/ 15. PayPal Security Wall of fame https://www.paypal.com/us/webapps/mpp/security-tools/wall-of-fame-honorable-mention 16. Google Security Researcher Acknowledgement for finding Cross site request forgery issue in Google Product and services. (2 Times) http://www.google.com/about/appsecurity/hall-of-fame/distinction/ 17. Apple Security researcher Acknowledgement for finding Reflected Cross site scripting issue. http://support.apple.com/kb/HT1318 18. Help-Scout Security Acknowledgement and reward https://www.helpscout.net/security/#reporting
Achievements	Microsoft Security Response Center TOP 100 hackers in world Rank - #96 Salesforce TOP 5 Researchers in the world – Rank - #5 Hackerone TOP 100 Researchers in the world – Rank #52 Cobalt TOP 100 Researchers in the world – Rank #8 Google Security Research Acknowledgement Program – Rank #274

6.2

Name: Kalpesh Jha **Designation: Senior Security Analyst**	
Profile Summery	Kalpesh is Security Analyst at Techdefence Labs. His area of expertise includes vulnerability assessment, Penetration Testing, Source Code Reviews, Information Security Trainings.

Educational Qualifications	Masters In Computer Science (Information Technology)
Professional Experience	+3 Years
Certifications	• Certified Network Defender (CND) • Certified Cyber Security Expert(CCSE) • Certified Ethical Hacker(CEH)

Technology Summary

Security Tools	Burp Suite, Nmap, DirBuster, xenotix, Nikto, SQLmap, Metasploit framework, Ollydbg, Nessus, Immunity Debugger, Nessus, Accunetix, Core Impact,Hopper, IDA Pro.
Firefox Add-on	Hack bar, Live Http headers, Cookie manager+, Firebug, No-redirect, Wappalyzer.
Programming Languages	C, C++, Php, Python, Android
Server Software Configuration	Apache, DNS, DHCP
Internet Tech	Html, Html 5, XML, Ajax, JavaScript, SOAP
Database	Mysql, MSSQL, Oracle
Operating System	Windows, Linux, Unix

Project Execution Summery

Project Executed	He has successfully completed 30+ projects across below verticals • Banking & Financial Sector • Stock Trading Applications • WAF Testing • Online Media • Online Professional Services

	• Startups • Job Portals • E-Learning Portals • HRMS Platform • Block chain • E-commerce Platforms

6.3

Name: Maulik Vaidh **Designation: Senior Security Analyst**	
Profile Summery	Maulik is Information Security Analyst at Techdefence Labs. His area of expertise includes vulnerability assessment, Penetration Testing, Source Code Reviews, Information Security Trainings.
Education Qualifications	Master in Cyber Security from SRM University
Experience	3+ Years
Certifications	• Certified Ethical Hacking Expert - CEHE • Certified Cyber Security Expert - CCSE • Certified Web Application Security Expert - CWASE

Technology Summary

Security Tools	Burp Suite, Acunetix,Nmap, DirBuster, xenotix, Nikto,SQLmap, Metasploit framework, Ollydbg,Nessus,Nexpose,MobSF,Appie.
Firefox Add-on	Hack bar, Tamper data, Live Http headers, Cookie manager+, Firebug, No-redirect, Wappalyzer and Elite Proxy Switcher.
Programming Languages	C, C++, Perl, Php, Python, Ruby
Server Software Configuration	Apache, DNS, DHCP

Internet Technology	Html, Html 5, XML, Ajax, JavaScript, SOAP
Database	Mysql, MSSQL, Oracle
Operating System	Windows, Linux

Project Execution Summery

Project Executed	He has successfully completed 30+ projects across below verticals • Banking & Financial Sector • Stock Trading Applications • WAF Testing • Online Media • Online Professional Services • Startups • Job Portals • E-Learning Portals & HRMS Platform

7. About Techdefence Labs

7.1 Introduction

Techdefence Labs is an information security based innovation center developed by Techdefence Labs Solutions Pvt. Ltd. Techdefence Labs is based out of Ahmedabad, India and was established in

2009. Starting from the small awareness programs on cyber security to conducting training sessions for the Corporates, Educational institutions & Law Enforcement Agencies, Techdefence Labs has encapsulated its growth in multiple fields of expertise. With multi-fold growth in training and consulting for information security solutions, Techdefence Labs has now proudly marched into Information Security Solutions and Services.

Techdefence Labs initiation in providing the best tool for security testing has led to the core conclusion of "The Best Way to Secure Yourself is to hack it yourself." Techdefence Labs strongly recommends and enforces the manual testing over tools and proprietary platforms. A rigorous manual testing supported with equivalent synchronized testing by proprietary platforms developed at Techdefence Labs, promises a 100% secure solution with expert auditing.

A state-of-the-art R&D innovation center at the pinnacle of its growth, Techdefence Labs cultivates an environment of creativity and passion amongst its super industrious team of individuals. The innovation is driven by the hardcore belief of "Where you see the solutions, we see the flaws." A meticulous out-of-the box thinking induced among the very foundation of the firm has led to break through of unmatched solutions to satisfactory customers like Cyberoam, Sulekha.com, Dealcloud , Logmeonce, HPCL, Indian Oil and many others..

Main Goal

Techdefence Labs main goal is to reciprocate to the innumerable market & industry requirements for the best solution to ensure a secure cyber space. We have built our vision, mission and values to support the very basis of our goal.

Our Mission

To provide the secure most solutions and best-in-class products for ensuring a smooth run of business for the clients through perseverance and sheer innovation while delivering supreme quality service and assistance.

Our Vision

Techdefence Labs shall be the renowned pinnacle of cyber security solutions and services, along with spreading a culture of passion and innovation with satisfied clients and a safe guarded cyber space.

7.2 Clientele

Company Type	Company Name	Services Delivered
Enterprises	**Cyberoam** - Largest Security Solutions Provider	VA, PT, Training
	Sandesh – Leading Media House based in Gujarat	VA, PT
	APSEZ – Adani Group	VA, PT
	PharmEasy	VA, PT
	Schoogle	VA,PT
	Sanghi Cement	VA, PT
	ADANI Power Limited	VA,PT
	ADANI Wilmar Limited	VA,PT
	ADANI Enterprises Limited	VA,PT
	ADANI Atreco	VA,PT
	ADANI Mining	VA,PT
	ADANI Green Energy	VA,PT
	ADANI PORT	VA,PT
	ADANI Gas Limited	VA, PT, WAF Implementation & Monitoring
	SRK Export – Second largest diamond export manufacturer	VA, PT, Training
	Kalupur Bank	VA, PT
	Jivan Bank, Rajkot	VA,PT, Information Security Policy Formulations
	Texco Bank, Surat	VA,PT,Cyber Forensics, Information Security Policy Formulations
	Oneworldexpress – United kingdom based Logistics Provider	VA, PT
	Future Group – Leading Retail Group	Training
	Master Capital – Capital & Security Services Provider	VA, PT
Government	**Essel group -** most prominent business house with a diverse portfolio of assets in media, packaging, entertainment, technology-enabled solutions provider	VA, PT
	Aakash – Leading Education institute for competitive Exams	VA, PT

	Sulekha – Largest Classified Portal based in India	VA, PT
	Indian Oil – Largest Commercial Enterprises into Petroleum industry based In India	Training, PT
	HPCL – Second Largest Commercial Enterprises into Petroleum industry based in India	Training, PT
	Ncode Solutions - is a Certifying Authority licensed to issue Digital Certificates in India.	Audit, PT
	Ministry of Home affairs, Malaysia	Training
	Reserve Bank of India	Training
	IT Cell, Chief Ministers Office, Gujarat -	Training
Ecommerce **Startups**	**Cyber Crime Cells –** Gujarat, Maharashtra, Rajasthan, Tamilnadu	Training
	SABOskirt – Online Apparel Store based in Australia	VA, PT
	Almostfree – Online Coupons / Deals portal based in India	VA, PT
	Quicko – Online Income-tax E-filing portal based in India	VA, PT
	Onfido – Background checks Portal based in UK	VA, PT
	Juspay – Online Payment Gateway Service based in India	VA, PT
	Tripoto – Online Travel Portal based in India	VA, PT
	Myles – Self Rental Car Portal based in India	VA, PT
	Inncerchef – Online food ordering platform based in India	VA, PT
	Swiggy – Online food ordering platform based in India	VA, PT
	Exotel – Cloud based Telephony Platform based in India	VA, PT
	Resumonk – Online CV Builder Portal based in India	VA, PT
	Sun Telematics	VA,PT
	Mintzip	VA,PT, Cloud Config Review
	Thelittle news – Online news media App	VA, PT
Online Services	**Anytime Doctor –** Online doctor appointment booking portal based in India	VA, PT
	Youth4work – Online Job Portal	VA, PT

	CAPITA World – Online Money Lending Platform based in Middle-East	VA, PT
	Logmeonce – Single click Sign-on Service based in USA	VA, PT

7.3 Differentiators

Techdefence Labs has kept itself upbeat to every challenge by outperforming from their targets consistently with rigorous endeavours. This very culture distinguishes Team Techdefence Labs in a different and a better genre of cyber security professionals. From R&D, design, development, smart engineering which inculcate core technical values to the enjoyable and lively knowledge enriching seminars, Techdefence Labs has stood out par excellence in serving the needs of clients and society altogether.

7.3.1 Experienced Certified Professionals

Techdefence Labs pursues and believes in strong in-depth knowledge. Hence, 95% of employees at Techdefence Labs are thoroughly complete in following certifications and many other IT related certifications/degrees.

CCNA- Cisco Certified Network Associate

CEH – Certified Ethical Hacker

CCSE – Certified Cyber Security Expert

ECSA – EC Council Certified Security Analyst

LPT - Licensed Penetration Tester

ISO 270001 Lead Auditor and Implementer

7.3.2 State of the art R&D Lab

Techdefence Labs perseverance towards excellence knows no boundaries and its expansion within itself is a result of cumulative growth of the company. The state-of-the-art R&D innovation center also known as **Techdefence Labs,** setup specially to cater to the needs of project requirements.

7.3.3 Commitment to Security Research

Generating a thinking process in a free-for-all mode, Techdefence Labs researchers expand to the horizons in the vast cyber space, looking for learning and expertise. Our globally renowned researchers have found various vulnerabilities and loopholes in following famous sectors of cyber space like **Microsoft, Google, Facebook, Yahoo!, Tesla, Wordpress, Magento, Mozilla, Adobe, Apple, Nokia, Blackberry** and Hall of Fame are thronged with such endeavours. Our researchers are also listed in MSRC (Microsoft Security Response Centre) **TOP 100 Security Researchers** in world.

7.3.4 Flexible Service Approach

With the focus on people, process and technology aspects of security coupled with flexible delivery capabilities based on company's priority, business value and business risk.

7.3.5 Associations and Collaboration

Techdefence Labs is in association with many cyber security firms and communities across the world building ties for knowledge sharing, competency and support from different domain experts.

Our solution seekers scour through these communities and stay up to date with latest trends and techniques, helping nurture the best and competitive product and service from Techdefence Labs.

7.3.6 Proprietary Tools

The industrious and creative team at Techdefence Labs never stops at a single solution and neither does it stop at enhancing the power of tools and proprietary platforms which are of utmost importance. We have developed our own platforms like Appdefence – Web and Mobile for identifying vulnerabilities in Web and Mobile applications.

7.3.7 Standard Based Approach

Techdefence Labs Follows standards based approach for its services. Our consultants are well versed with globally accepted standards for security.

NIST standard for Risk Management
OWASP – Open Web application Security Project
OSSTMM – Open Source Security Testing Methodology Manual
ISSAF – Information Security System Assessment Framework
ISO27001 for Information Security Management Systems

7.3.8 Knowledge sharing through Research Papers and Seminars

Techdefence Labs has involved itself with knowledge sharing activities since the very beginning. Techdefence Labs believes that information is knowledge and knowledge is power. Techdefence Labs has published numerous articles and papers in various international journals, magazines. Conducting seminars to a wide range of audiences and educated professionals over cyber security at International conferences, Techdefence Labs has expanded its reach and voice through various media for educating the world of the cyber space

7.4 Benefits to the Organization

Plugging the gaps

The Issues identified by security assessment will highlight the existing weakness in applications / network / infrastructure that could lead to data breaches, malicious infiltration or worse. The countermeasures will definitely suggest software and hardware changes and also do amendments your security protocols.

Ensuring Continuity

24/7 communications and customer or user access are essential to your business operations. Any disruption will have negative impact on your organization. Security Assessment can throw up potential threats to all these areas and help ensure that your business doesn't suffer from downtime and inaccessibility issues.

Meeting Compliance

Industry and legal requirements dictate that a certain level of penetration testing is compulsory. Security Assessment can definitely help manage risk proactively and meeting compliance.

Enhanced Trust

Any organization's commitment to conduct assessment and act on recommendations enhances trust to customers and stakeholders.

Enhance Quality Assurance

IT dependent organization with secure production environment subjected to regular pen testing and assessment will enhance organization's standing in market and assures buyers of consistent and high standard.

Develop Information Security Strategy

Security Assessment will help develop information security strategy by identifying focus and growth areas, as well as best practices in implementation of the same strategy.