A project report submitted on

Business Development – Kratikal Tech. Pvt. Ltd.

Under the supervision of **Dr. Tiratha Raj Singh**

Submitted by

Medhavi Pokhriyal 161504

BACHELOR OF TECHNOLOGY IN BIOINFORMATICS

DEPARTMENT OF BIOTECHNOLOGY AND BIOINFORMATICS,
JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,
WAKNAGHAT, SOLAN 173234, HIMACHAL PRADESH, INDIA

STUDENT DECLARATION

I hereby declare that this submission is my own work carried out at Kratikal Tech. Pvt. Ltd. from 5th Feb, 2020 and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgement has been made in the text.

Place: JUIT, Solan, H.P. Signature : Medhavi Pokhriyal

Date : 07/06/2020 Name : Medhavi Pokhriyal

ACKNOWLEDGEMENT

Primarily, I would like to thank my highly respected & esteemed supervisor for his constant guidance, support & supervision. Also, I would like to show my gratitude to all the people around me, such as my superiors as well as my colleagues in the company. The valuable support of these people have led me to successfully complete my project & build up confidence.

I would also like to thank my manager in the company for his never ending assistance and helping me to correct my mistakes.

Signature : Medhavi Pokhriyal

Name: Medhavi Pokhriyal

Roll No.:161504

Date : 07/06/2020

Project Report Undertaking

I Mr. /Ms.____________Medhavi Pokhriyal________-Roll No.___ 161504_________ Branch______Bioinformatics_________is doing my internship with _Kratikal Tech. Pvt. Ltd. from 05/02/2020 to 07/06/2020.

As per procedure I have to submit my project report to the university related to my work that I have done during this internship.

I have compiled my project report. But due to COVID-19 situation my project mentor in the company is not able to sign my project report.

So I hereby declare that the project report is fully designed/developed by me and no part of the work is borrowed or purchased from any agency. And I'll produce a certificate/document of my internship completion with the company to TnP Cell whenever COVID-19 situation gets normal.

Signature : Medhavi Pokhriyal

Name:_Medhavi Pokhriyal_______

Date:07/06/2020_______________

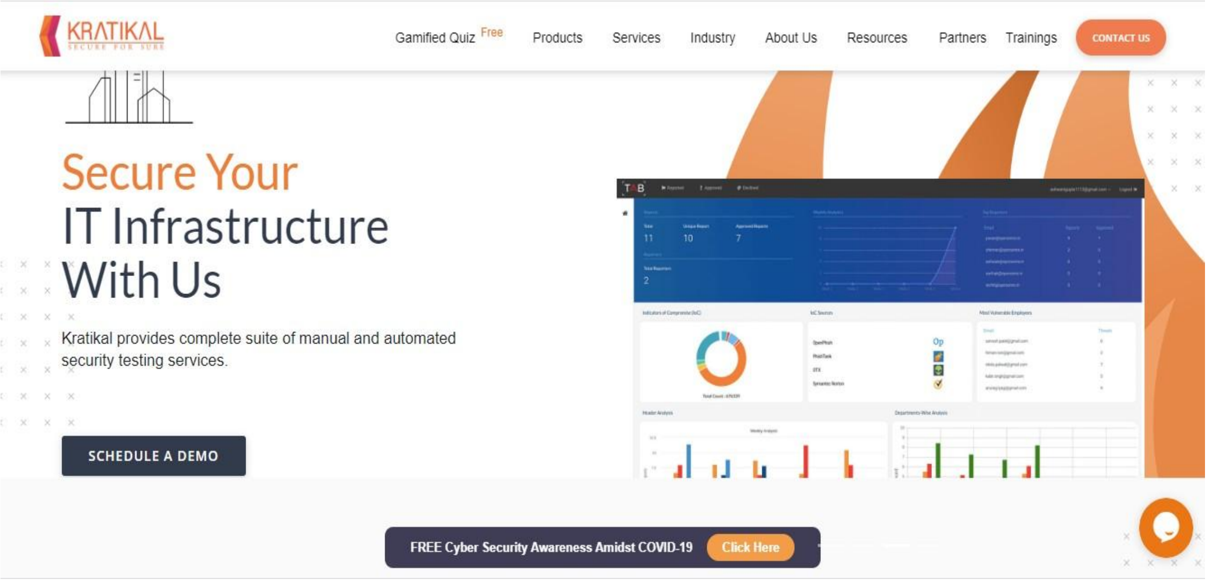
TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

Kratikal is a cyber security company, with more than 125+ clients such as PVR, ABCL, Fortis Healthcare, Max Life, GMR, Nykaa, etc. It was founded in the year 2013 with VAPT as a service. Furthermore, when the VAPT market was flooded, they came up with various other products for the protection of the organisations against cyber-attacks. Currently, it provides cyber security against the three most important pillars of any organisation i.e. people, process & technology.

In 2017, the flagship product ThreatCop was awarded as the “Top 10-Most innovative product” by DSCI NASSCOM. This was followed by gaining recognition as the “Top-3 Start-ups in India” by NASSCOM Product Conclave in 2018. Recently, Kratikal has also been awarded top cyber security startup at the 12th Top 100 CISO Awards.



Secure Your IT Infrastructure With Us

Kratikal provides complete suite of manual and automated security testing services.

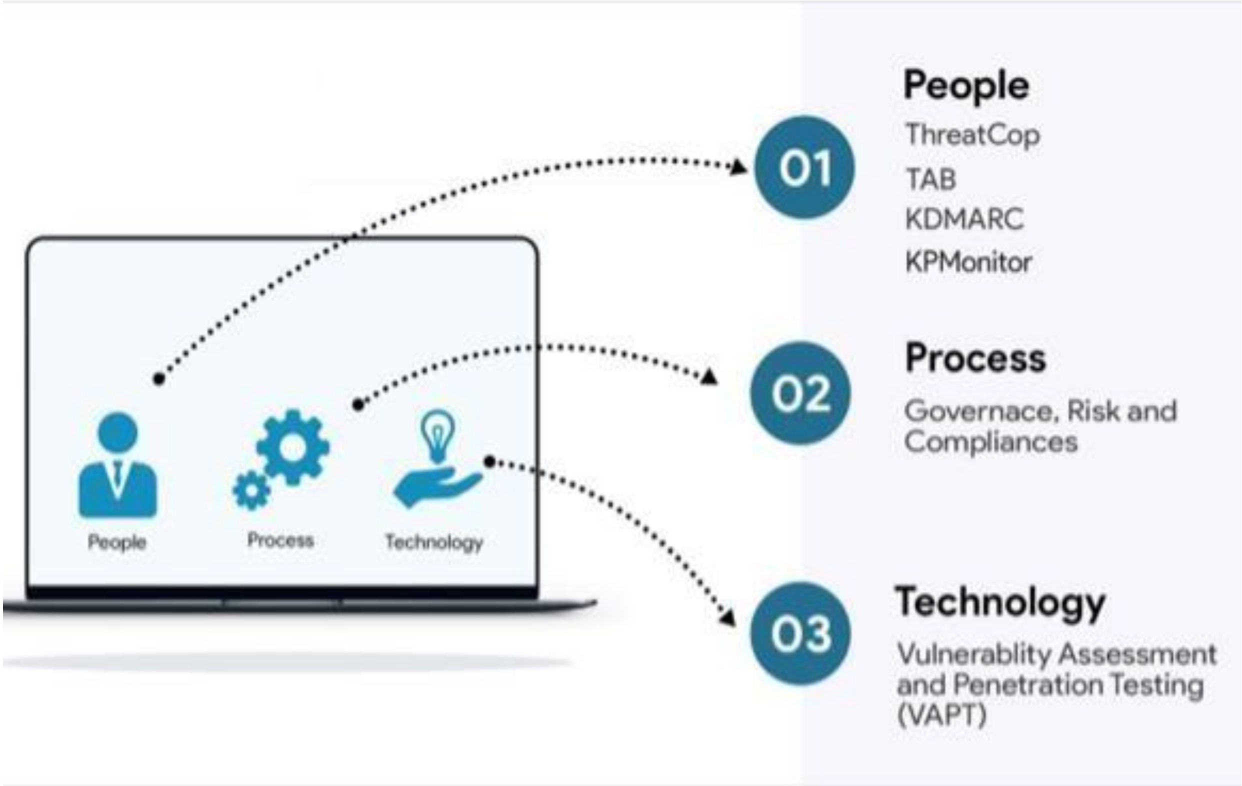
Kratikal aims to become a one stop solution for cyber security around the world. Besides, offering products & services, Kratikal also, believes in training people who have an interest in ethical hacking. Kratikal has a sister company called Krademy that majorly focuses on providing e-learning courses.

Kratikal not only helps an organisation become cybersecure but it also aids in, protecting by protecting their brand reputions. Tools & services offered by Kratikal usually include phishing simulation tool, response tool, email authentication tool, fraud monitoring tool, compliance management and VAPT.

2. ABOUT THE COMPANY

Kratikal Tech. Pvt. Ltd. is among one of the leading cyber security start-ups in India, known for its distinctive products & services with an aim to become a one stop solution for cyber security around the world. Being a SaaS based hi-tech security solutions providing organisation, it is recognised by Oracle, MicrosoftBiz, IBM, IndiaMobileCongress & is also, awarded by Data Security Control of India, NASSCOM, 100 CISO Platform. Thus, assisting a diverse range of industries such as E-commerce, Financial Services, BFSI, NBFC, Telecom, Consumer Internet, Cloud Service Platforms, Manufacturing & Healthcare

Kratikal provides security along the three most important pillars of any organisation, i.e. People, Process & Technology & acts as a trusted standard for companies and individuals acquiring services to protect their brands, businesses and dignity from baffling Cyber-attacks. Famous for its state-of-the-art security solutions such as a real time cyber-attack simulation and awareness tool, phishing incident response tool, email authentication tool, fraud monitoring & take-down tool, risk detection and threat analysis as well as source codereview.


People
Process
Technology
01
People
ThreatCop
TAB
KDMARC
KPMonitor
02
Process
Governace, Risk and Compliances
03
Technology
Vulnerablity Assessment and Penetration Testing (VAPT)

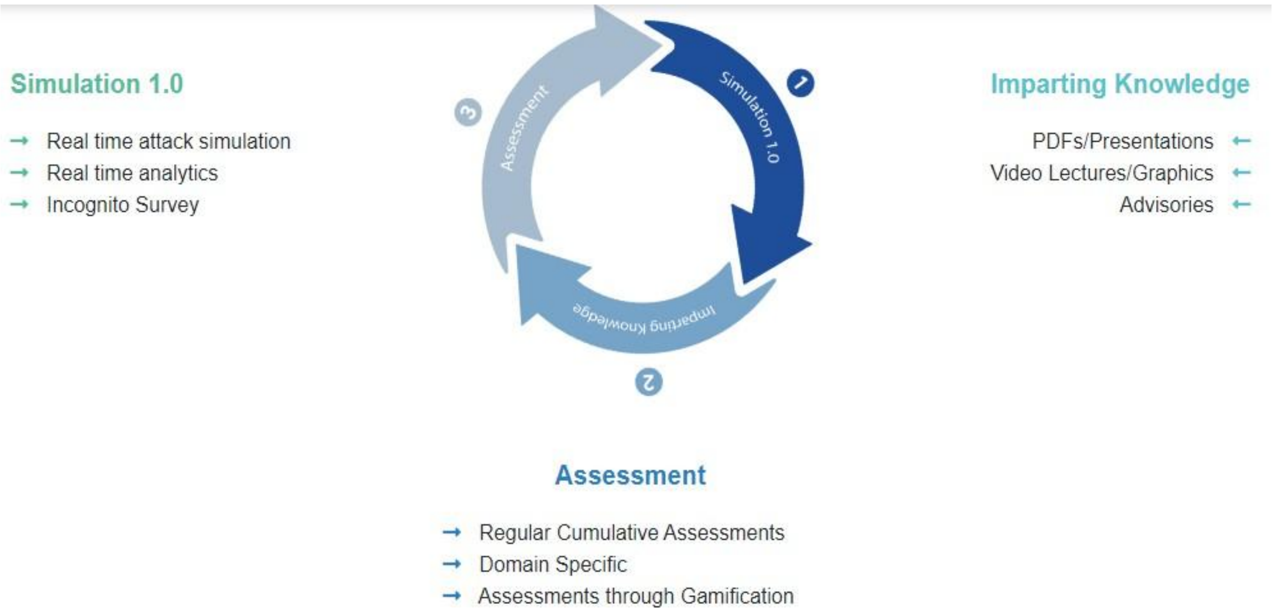
3. PRODUCTS & SERVICES

PRODUCTS

A. ThreatCop

ThreatCop is an Artificial Intelligence/Machine Learning tool that assesses the real time threat posture of an organisation.

The tool majorly focuses on the employees, thus securing the People Pillar of any organisation. The employees can be the weakest link if not provided with cyber security awareness. Thus, ThreatCop helps your employees by calculating an Employee Vulnerability Score(EVS), followed by instantaneous knowledge imparting and lastly, assessing the employee awareness through regular assessments or gamifications.



ThreatCop covers 6 different types of cyber-attack vectors:

i. Phishing : A type of a cyber-attack using a disguised email to obtain sensitive information from a person.

ii. Smishing : A type of a cyber-attack using a disguised SMS to obtain sensitive information from a person.

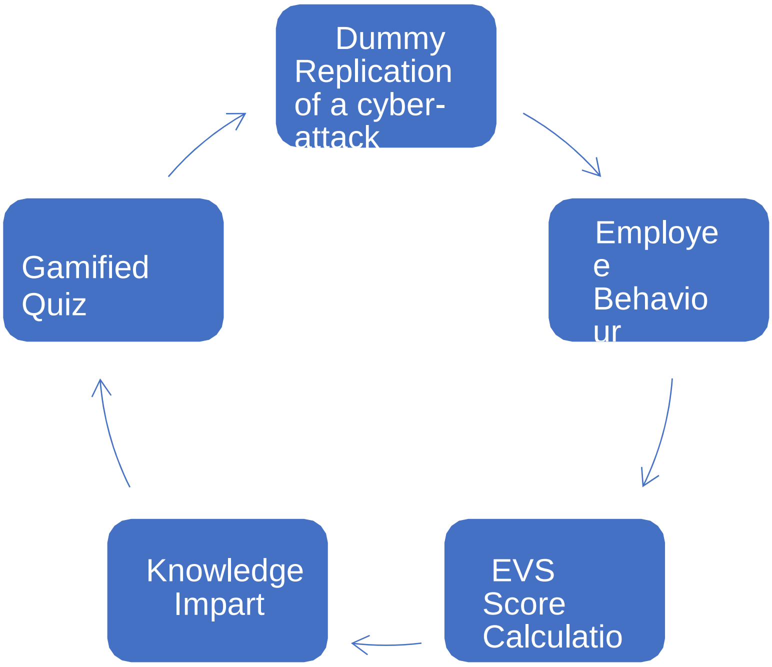
iii. Vishing : A type of a cyber-attack using a disguised call to obtain sensitive information from a person.

iv. Ransomware : A malicious software corrupts the system until the desired ransom is paid.
v. Risk of Removable Media : Higher risk of data loss if the media is lost.
vi. Cyber scam : Tricking people by deception on the internet.

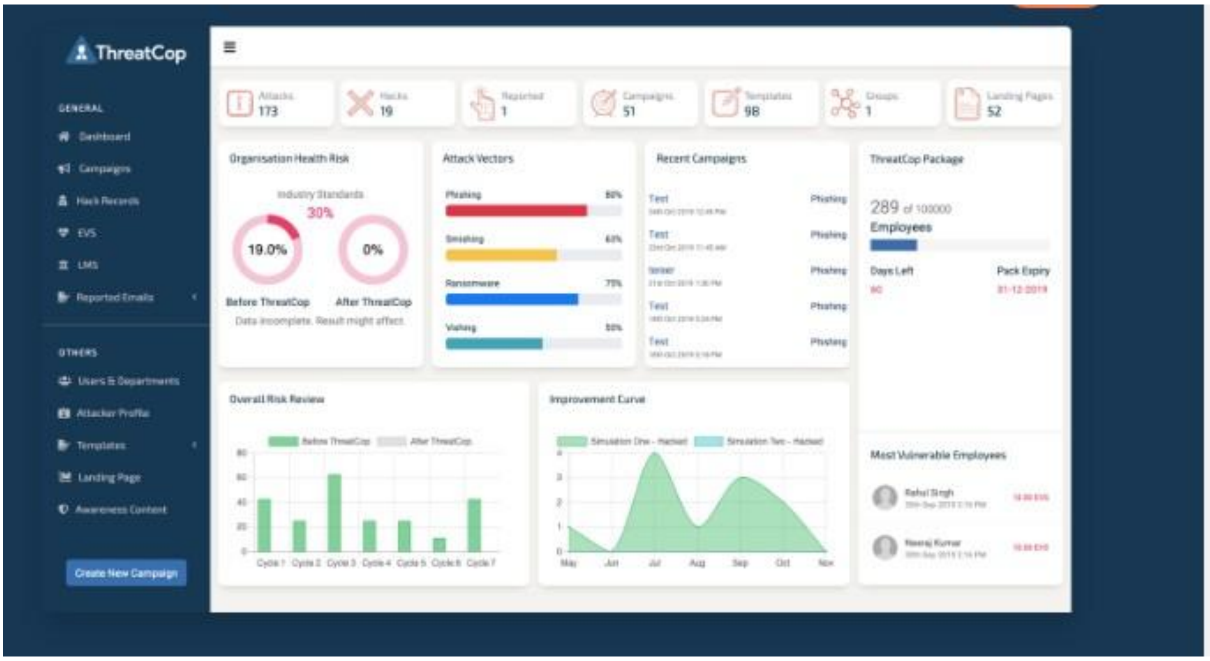
Being a real time attack simulation tool, it involves real time analytics along with incognito survey assessment, cumulative assessments and domain specific assessments through gamified quizzes. Hence, it is believed to be a complete solution for all the security needs of any organization at employee level as it discovers all the possible ways by which an individual can be compromised. Thus, reducing the cyber risk in any organisation by 90%. Access to the ThreatCop dashboard, gives you an overall threat analysis with unlimited number of cyber-attack simulations as well as attack campaigns that can be run to build a cyber secure environment.

Learning Management System is an automated training campaign that aims to create cyber awareness about the various security attack vectors amongst the employees using PDFs/Presentations, Video Lectures, Infographics & Advisories. The LMS is followed by a periodic assessment of employees i.e. the employees fill a questionnaire on the basis of their learning/knowledge gained. Knowledge imparted is usually on the basis of the different attack vectors. For instance, if an email-based phishing attack is simulated then the employees will be trained specifically for email parameters that will help him identify a phishing email or a genuine email. The assessment followed by the knowledge imparting really helps in analysing the learning curve (level of awareness) of the employees. The dashboard keeps a real time tracking of the assessment's result, progress and provides the user with analytics and metrics of the campaign run. However, the overall health of an organization can be analysed by comparing pre-ThreatCop deployment and post phishing simulation campaign results.

The user is able to create, import & customize the vector templates so as to make the phishing simulation more real. Besides, the user has been given full control/ access over the design, date and time and is able to schedule the attack campaign as per his convenience. Another, distinctive feature of ThreatCop is to intimate the user about the hack record of the employees in third party apps as it aids in extracting the hack history of the employees. Thus, providing the user with in-depth analysis of the employee's vulnerability level. At the running time of simulated phishing campaign a geolocation tag of the employees is tagged.

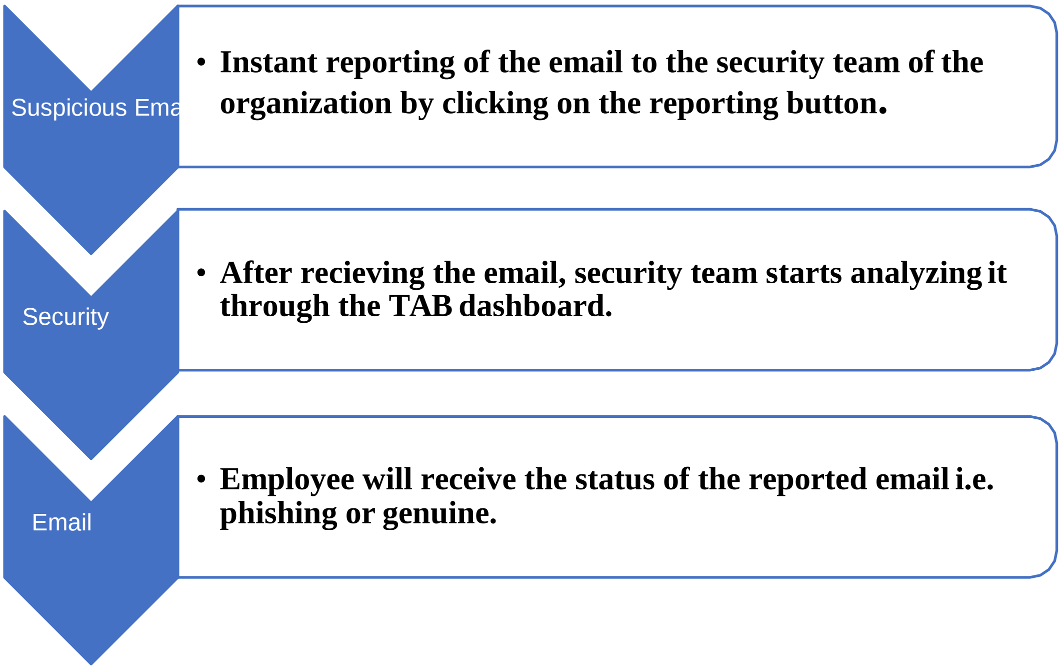


The above figure demonstrates the working of ThreatCop, cyber-attack simulation & people awareness tool.



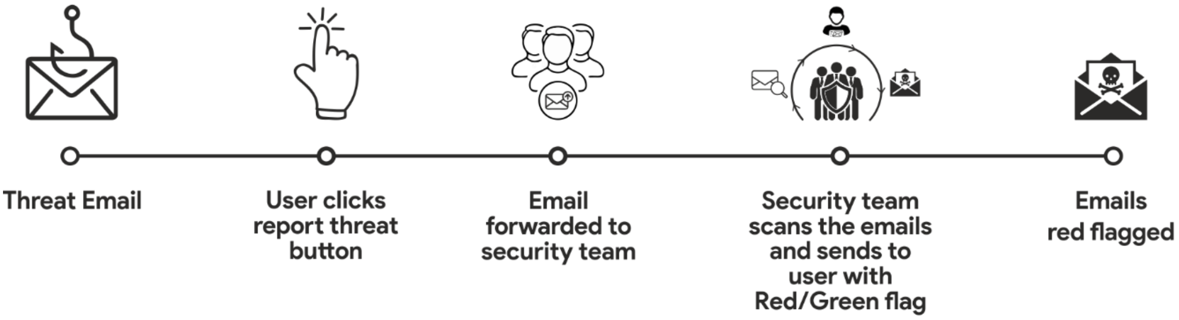
B. Threat Alert Button(TAB)

Threat Alert Button is a phishing incident response tool that empowers the employees against the incoming phishing emails. Each employee is given the ability to report any kind of suspicious looking email with a help of a reporting button. If a suspicious email lands in the employee’s inbox and he faces trouble in determining whether the email is genuine or phishing, he can directly report it with the help of TAB. Thus, preventing the attack to happen in future. After reporting, the suspicious email is removed from the inbox of all the employees and, is sent to the security team to analyse the different parameters by which one can catagorise a genuine & phishing emails. If the email is found to be genuine, the email is directly sent back into the inbox of all the employees. If not, the email permanently stays in the spam folder, thus, reporting by one employee can save the whole organisation from a cyber-attack.

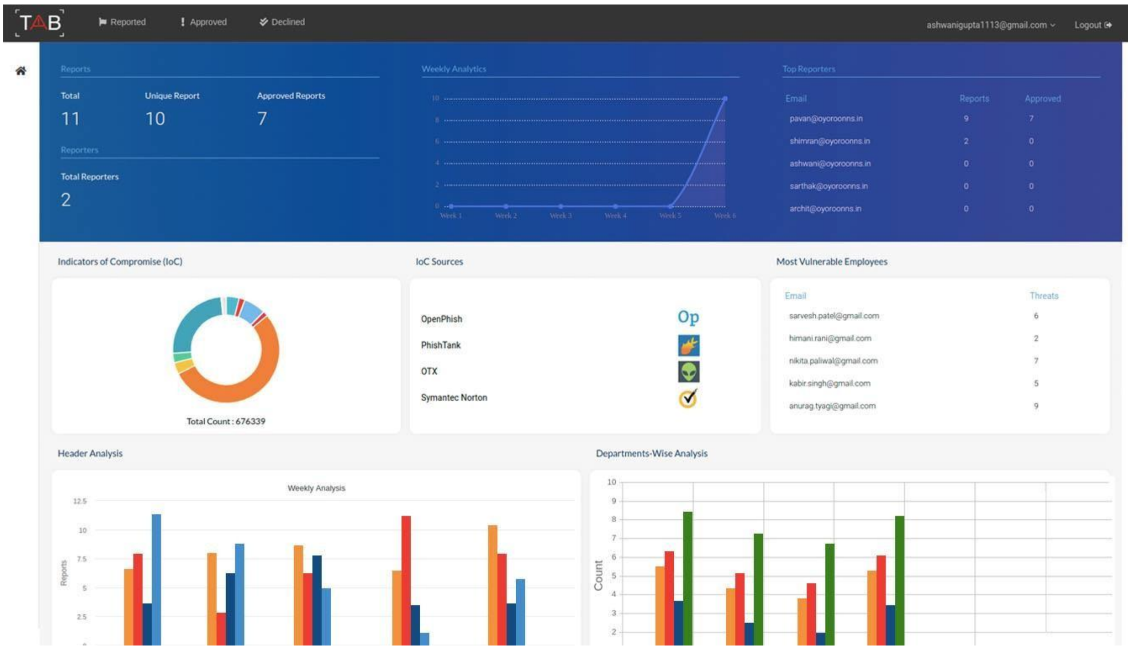


- **Instant reporting of the email to the security team of the organization by clicking on the reporting button.**
- **After recieving the email, security team starts analyzing it through the TAB dashboard.**
- **Employee will receive the status of the reported email i.e. phishing or genuine.**

Among many promising features of this tool, the ability to automatically move the reported email to spam from the inbox of all the employees really creates a significant difference as it helps in saving the whole organisation. Besides, instant reporting TAB also helps in analysing the reported email through GCTX. GCTX is a database containing millions of Indicators of Compromise such as IP addresses, Domains, Hostnames (subdomains), Email, URL, File Hashes such as SHA1, SHA256, MD5, PEHASH, IMPHASH, CIDR Rules, File Paths, MUTEX name, CVE number etc. which updated every hour for best possible results. Thus, when the reported email's indicators are run or compared with the indicators in GCTX database, the threat actors present in a fraudulent email are detected and give accurate results.


Threat Email
User clicks report threat button
Email forwarded to security team
Security team scans the emails and sends to user with Red/Green flag
Emails red flagged

The TAB aims to automate mitigation of cyber attacks by blacklisting the fraudulent e-mail sender's address from every employee's email ID within the organization. The primary objective of the tool, TAB is to empower employees by giving them the power of reporting. A single vigilant employee can protect the entire organization against cyber-attacks by just reporting a suspicious email. If the email is proved to be a malicious email, the whole organization can be benefitted as not every employee is usually cyber aware & majority of fraudulent emails usually remain undetected. Considering the current pandemic situation, most of the organizations are working from home & email is a major point of contact between the organizations and customers. And since, entire businesses are being run over emails, it has become a necessity for organizations to be cyber-secure in order to safeguard confidential data.



Reports

Total	Unique Report	Approved Reports
11	10	7

Reporters

Total Reporters

2

Top Reporters

Email	Reports	Approved
pavan@oyoroonns.in	9	7
shimran@oyoroonns.in	2	0
ashwani@oyoroonns.in	0	0
sarthak@oyoroonns.in	0	0
archit@oyoroonns.in	0	0

Indicators of Compromise (IoC)

Total Count : 676339

IoC Sources

OpenPhish

PhishTank

OTX

Symantec Norton

Most Vulnerable Employees

Email	Threats
sarvesh.patel@gmail.com	6
himani.rani@gmail.com	2
nikita.paliwal@gmail.com	7
kabir.singh@gmail.com	5
anurag.tyagi@gmail.com	9

Header Analysis

Departments-Wise Analysis

C. KPMonitor

Most phishing activities not only put customers' financial details as well as assets at risk but also the company's brand reputation. Phishing can be of websites, domains as well as mobile applications. Brand reputation takes years & years to build in the market, yet, can be destroyed in a matter of seconds.

KPMonitor is a phishing & fraud monitoring tool that aims to protect your brand reputation by securing it from brand misuse, defamatory attacks, and malicious entities. Brand protection service is a process of protecting intellectual property (IP) of companies along with their associated brands.

Further, it provides protection against the counterfeiters, copy pirating, IP violations i.e. patents, design rights, trade dress, and color mark, etc. Rendering this service causes the company to not only protect the reputation, image & value but also, protect the revenue loss of the organization, thus, proving to be all the more effective.

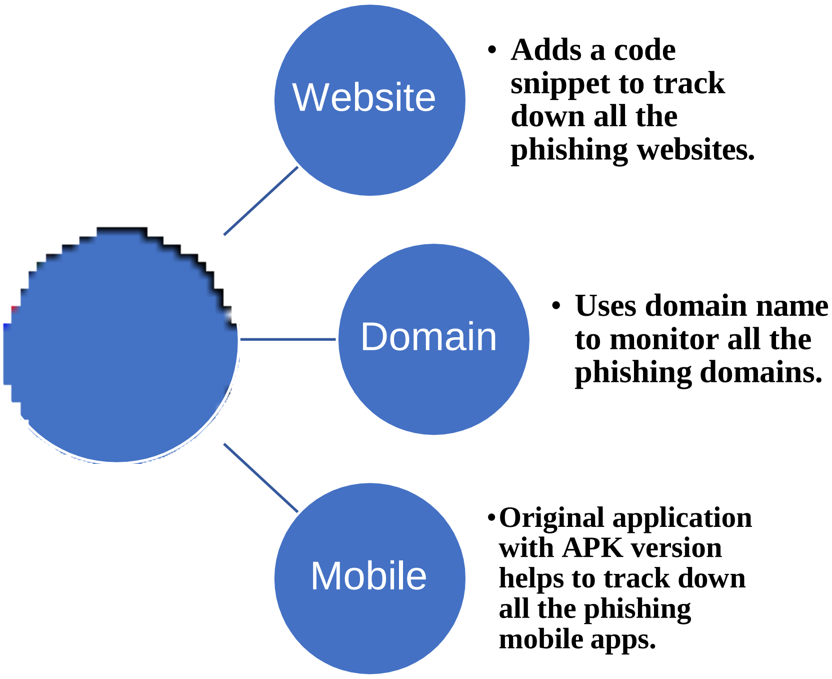
Fundamentally, the brand protection service prevents brand abuse by securing the digital assets and hence, safeguarding against brand breach with the help of right tools deployed in the right place.

Many organisation have more than one domain and managing them simultaneously gets very tedious. Similarly, protecting an organisation's image & brand reputation isn't so easy because it needs daily monitoring of domains, web & mobile applications with more than one resource to be deployed to protect it from misuse & infringement.

Hence, to ease this problem Kratikal brings in a tool which focuses on both of the important parameters, developed with an innovative software with a new technology approach called KPMonitor.

KPMonitor is a tool which is designed to monitor/ track phishing and fraudulent activities of websites, domains as well as mobile applications, developed by Kratikal that intends to protect the corporate brands from vicious activities. It ensures that the domains of the organisation are being managed and protected by offering a brand protection service and tracking down the attempts of misuse of an organisation's website, domain and mobile applications in real-time.

Works differently for websites, domains & Applications :

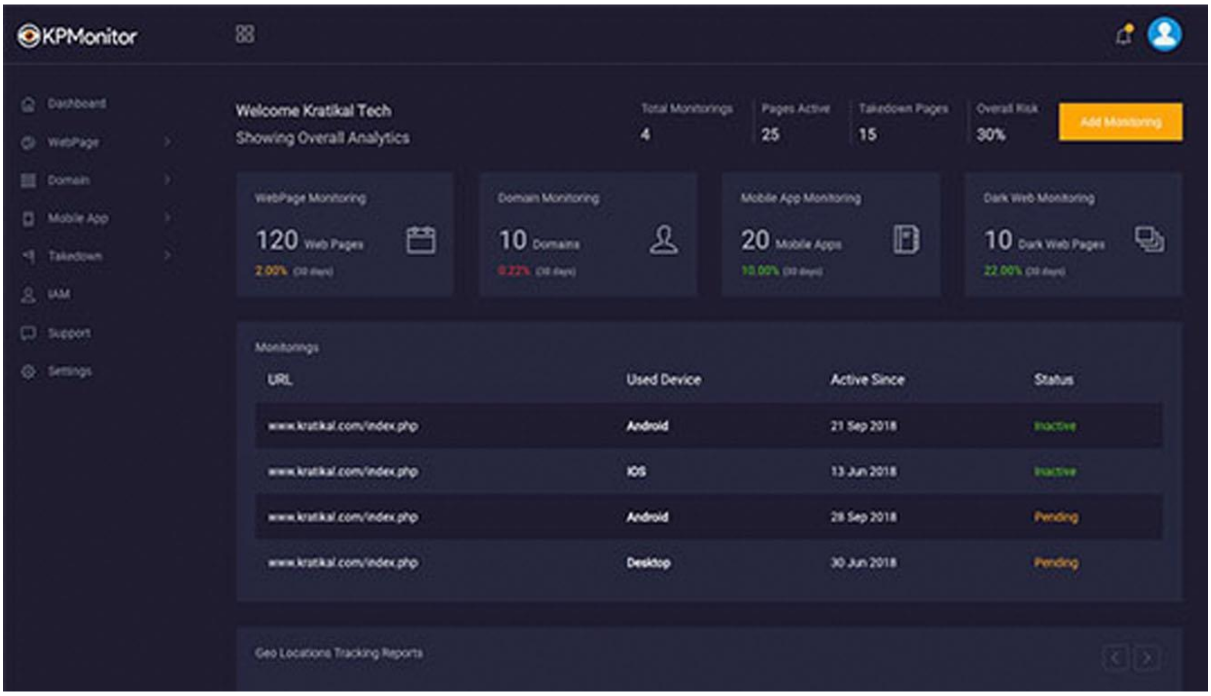

Website
Adds a code snippet to track down all the phishing websites.
Domain
Uses domain name to monitor all the phishing domains.
Mobile
Original application with APK version helps to track down all the phishing mobile apps.

Three distinguishing features of KPMonitor :

1. **Blacklisting:** Blacklists the IP of the individual who attempts to maliciously use the website, domain or mobile application.
2. **Permanent takedown:** External services such as Indian Copyright Act & different ISPs aid in permanently taking down the spoofed domains.
3. **Instant takedown:** A promising feature that takes down the spoofed website and mobile applications with just one-click.

With these distinctive features, the exponential yet silent upsurge of brand counterfeiting is drastically decreased.

Kratikal, the first company in India to design & develop a phishing and fraud monitoring tool with a feature of instantaneous takes down of spoofed domains, mobile applications and websites. Hence, taking another step towards a cyber secure India.



Welcome Kratikal Tech
Showing Overall Analytics

Total Monitorings	Pages Active	Takedown Pages	Overall Risk
4	25	15	30%

WebPage Monitoring
120 Web Pages
2.00% (30 days)

Domain Monitoring
10 Domains
0.22% (30 days)

Mobile App Monitoring
20 Mobile Apps
10.00% (30 days)

Dark Web Monitoring
10 Dark Web Pages
22.00% (30 days)

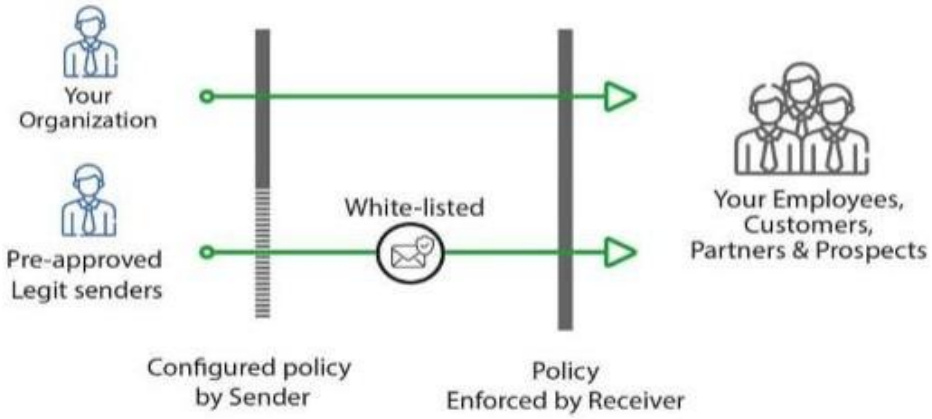
Monitorings

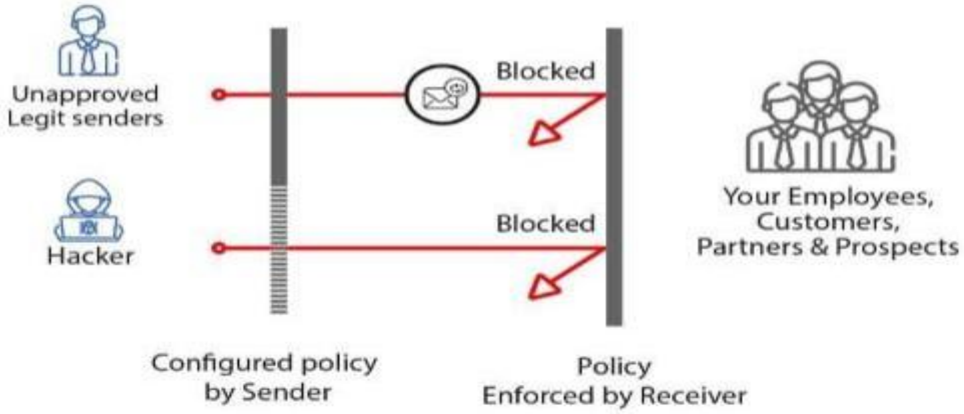
URL	Used Device	Active Since	Status
www.kratikal.com/index.php	Android	21 Sep 2018	Inactive
www.kratikal.com/index.php	IOS	13 Jun 2018	Inactive
www.kratikal.com/index.php	Android	28 Sep 2018	Pending
www.kratikal.com/index.php	Desktop	30 Jun 2018	Pending

Geo Locations Tracking Reports

D. KDMARC

Advancements in the email-based attacks are leading to an increase in compromise of major security vulnerabilities as the traditional email security lack in labelling the flaws. Thus, Kratikal put an effort to rectify this and came up with a tool called KDMARC which aims to build client's and employee's confidence to gain trust in their mailbox. A tool that analyses the email authentication reports so as to, identify the nature of the incoming emails. This tool majorly focuses on the incoming flow of emails & thus, builds an employee's confidence to trust his own inbox.


Your Organization
Pre-approved Legit senders
White-listed
Your Employees, Customers, Partners & Prospects
Configured policy by Sender
Policy Enforced by Receiver

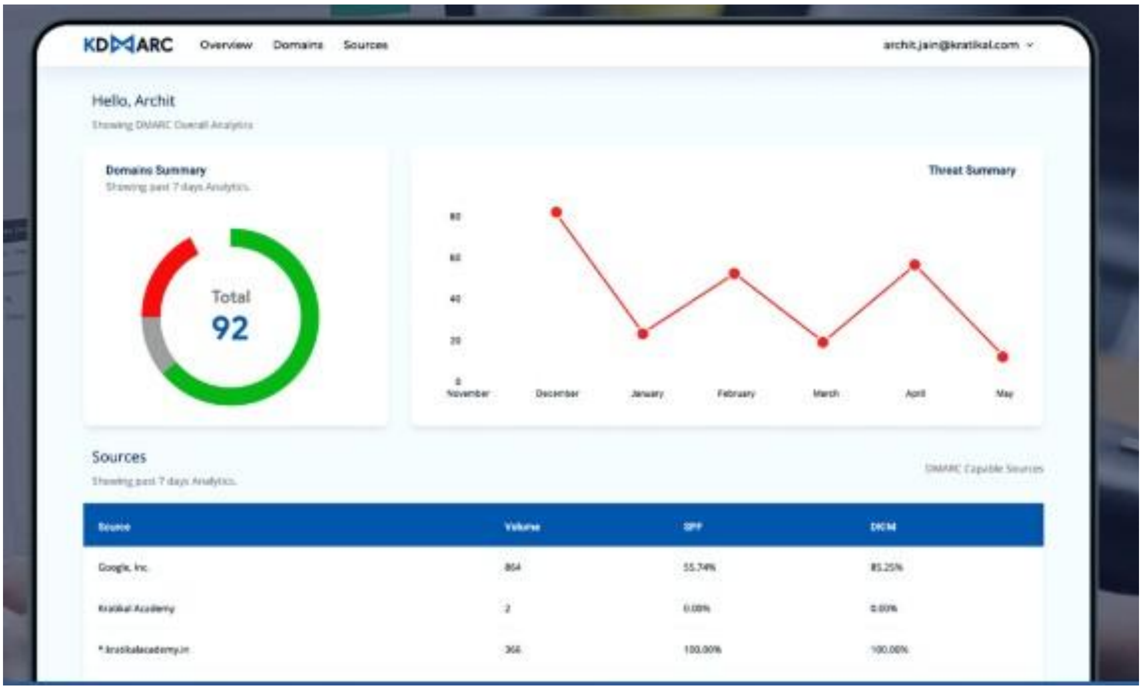


The tool majorly focuses on the outbound flow of emails & so, it checks for whitelisted Ids depending upon SPF & DKIM. If the Ids from which the mails are sent, is whitelisted the email will land in your inbox but if, the Ids is not whitelisted the email might land according the policy you have set. There are three types of policies i.e. none, quarantine, reject.

None - Email lands in Inbox.

Quarantine - Email lands in Spam.

Reject – Email is directly deleted from the server.



Hello, Archit

Showing DMARC Overall Analytics

Showing past 7 days Analytics.

Sources

Showing past 7 days Analytics.

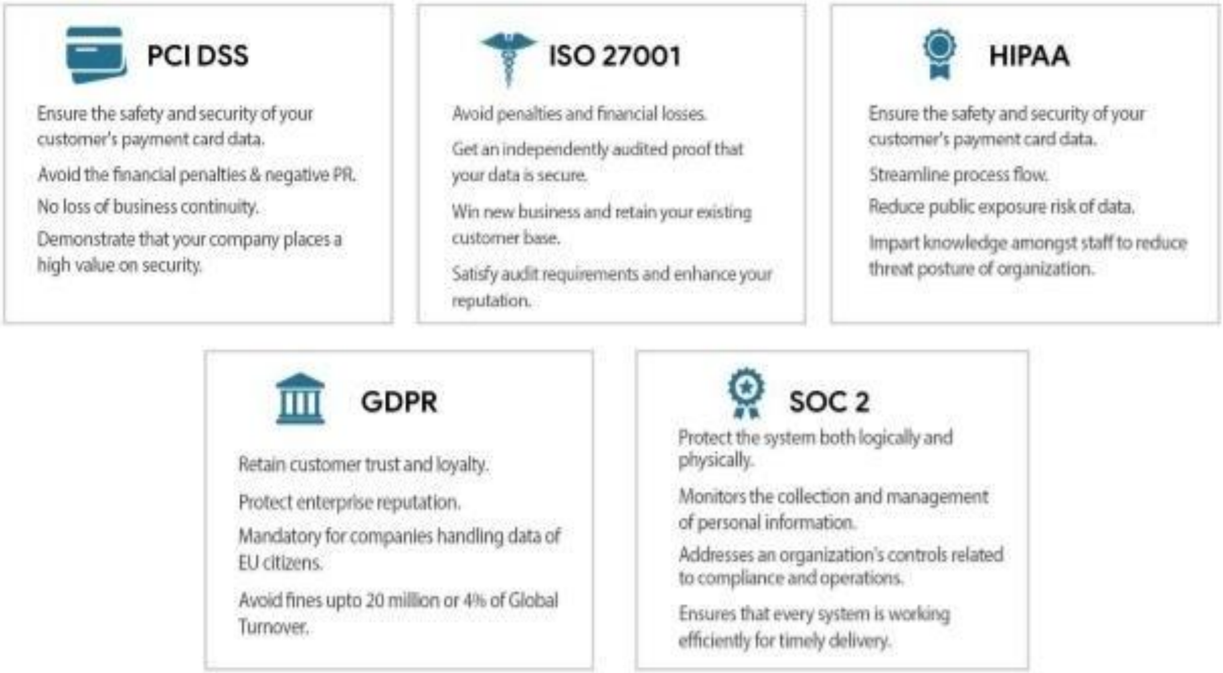
Source	Volume	SPF	DKIM
Google, Inc.	864	55.74%	85.25%
Kratikal Academy	2	0.00%	0.00%
*.kratikalacademy.in	366	100.00%	100.00%

COMPLIANCES

Besides developing various products, Kratikal also does compliance management. A regulatory compliance is a standard set of rules that describes the goals of the organizations that they desire to achieve by putting in efforts. A quality standard is described as a detail of the specifications, requirements along with various characteristics & guidelines in order to meet the quality of the product.

ISO is one of the most accepted set of quality standards adopted by a vast number of firms around the world. Provided, a company fails to meet the quality standard of the compliances, resulting in loss of the customer trust and henceforth, the market share.

Kratikal provides various security auditings like **ISO 27001, PCI DSS, HIPAA, GDPR and SOC2.**



PCI DSS

Ensure the safety and security of your customer's payment card data.

Avoid the financial penalties & negative PR.

No loss of business continuity.

Demonstrate that your company places a high value on security.

ISO 27001

Avoid penalties and financial losses.

Get an independently audited proof that your data is secure.

Win new business and retain your existing customer base.

Satisfy audit requirements and enhance your reputation.

HIPAA

Ensure the safety and security of your customer's payment card data.

Streamline process flow.

Reduce public exposure risk of data.

Impart knowledge amongst staff to reduce threat posture of organization.

GDPR

Retain customer trust and loyalty.

Protect enterprise reputation.

Mandatory for companies handling data of EU citizens.

Avoid fines upto 20 million or 4% of Global Turnover.

SOC 2

Protect the system both logically and physically.

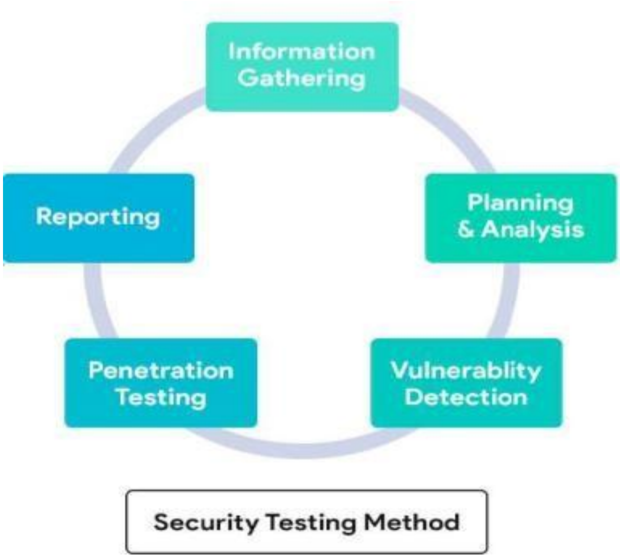
Monitors the collection and management of personal information.

Addresses an organization's controls related to compliance and operations.

Ensures that every system is working efficiently for timely delivery.

VAPT

Vulnerability Assessment & Penetration Testing(VAPT) allows an organisation to secure their applications against security bugs by finding out the entry points for various attackers. In an organisation, there can be many forms of security testing such as Application security testing, Network penetration testing, server security testing, Infrastructure penetration testing, Cloud security testing, IOT security testing & secure code review.



Methodology:

Information Gathering – This stage involves exploring of the organisation's application, architecture, features as well as security controls.

Planning analysis – This stage consists of planning on how to conduct the VAPT, using the information collected. Thus, this stage involves devising a "Red Team" approach to mimic real time attacks with an intention of minimising the impact of the attack. The attack is usually done on a dummy environment or at the time of lowest traffic.

Vulnerability Assessment – A stage in which we try to look for all the possible vulnerabilities with help of vulnerability scanners related to the platform, APIs, technology framework etc.

Penetration testing – This stage focuses on running exploits to evaluate the security of an organisation's applications/network/server/cloud/IOT or the overall infrastructure. Using more than 250 test cases, open source exploits as well as in-house tools. Penetration testing can be of 2 types i.e. Automatic & Manual, the latter is used for a higher degree of penetration.

Reporting – This stage focuses on generating concise reports containing the number of vulnerabilities discovered as well as its nature, impact, threat level and lastly, the recommendation to remove the vulnerability. Reports can be customised according to the requirements of the organisation.

Also, Kratikal carries out comprehensive discussions to help the organisation's fix the bugs to remove vulnerabilities & harden the application. Thus, helping various organisations to be secured against cyber-crimes.

4. ROLE OF BUSINESS DEVELOPMENT

Business development deals with various tasks and processes to bring in opportunities within and between various organizations. It deals with creating a requirement/need for products offered by your company by pitching & probing. Business development also creates a long-term value for an organization by building good relationships with the customers.

The business developer is responsible for the analytical preparation of potential growth opportunities for higher management, also plays a role in monitoring its implementation. In both, development phase and implementation phase a business developer plays a vital role by building rapport & maintaining an already built relationship. Sales ensures that the organization is self-sufficient in implementing the growth opportunity.

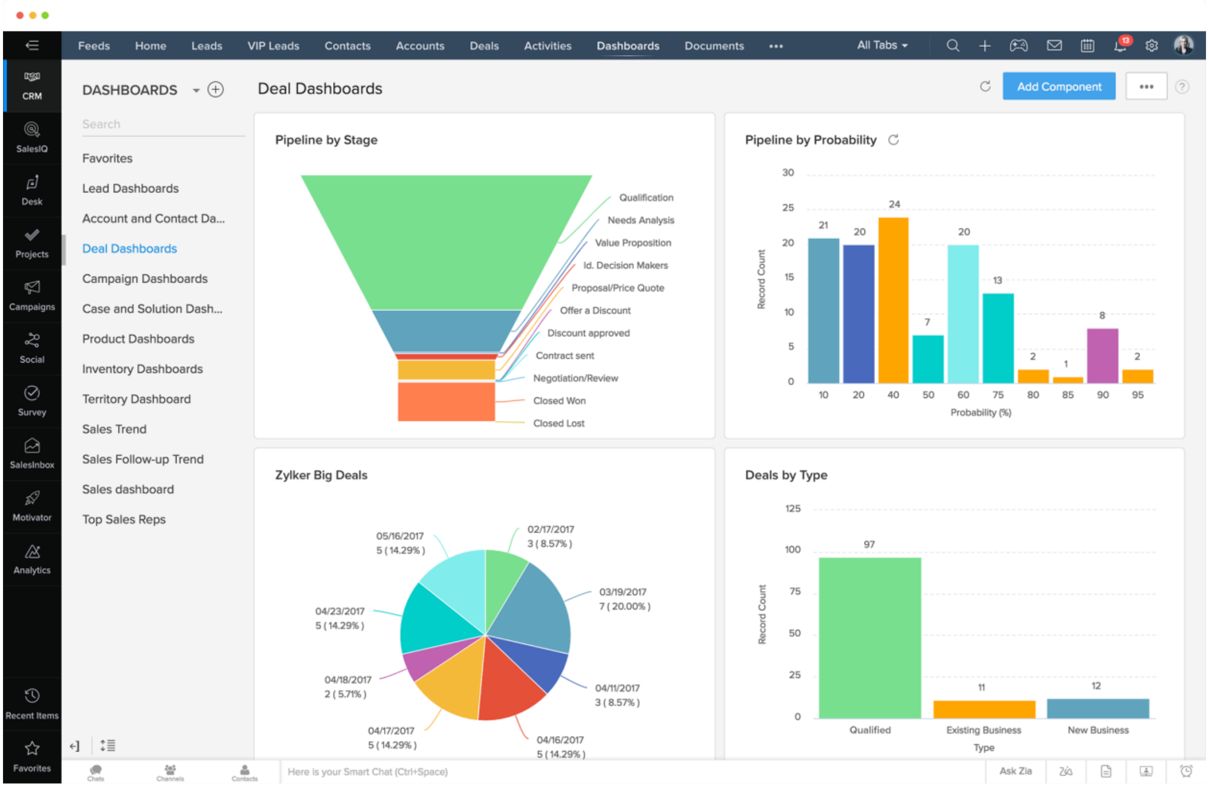
A pipeline containing recent prospects is created and is assigned to the business development staff. This is followed by the calculation of percentage chance of success along with attached projected sales-volumes. Usually, organizations support pipelines with some customer relationship management(CRM) tool, implemented as a web-based solution or an in-house system. CRM helps in managing & analysing leads to draw sales management information.

Different tasks as a Business Development Intern:

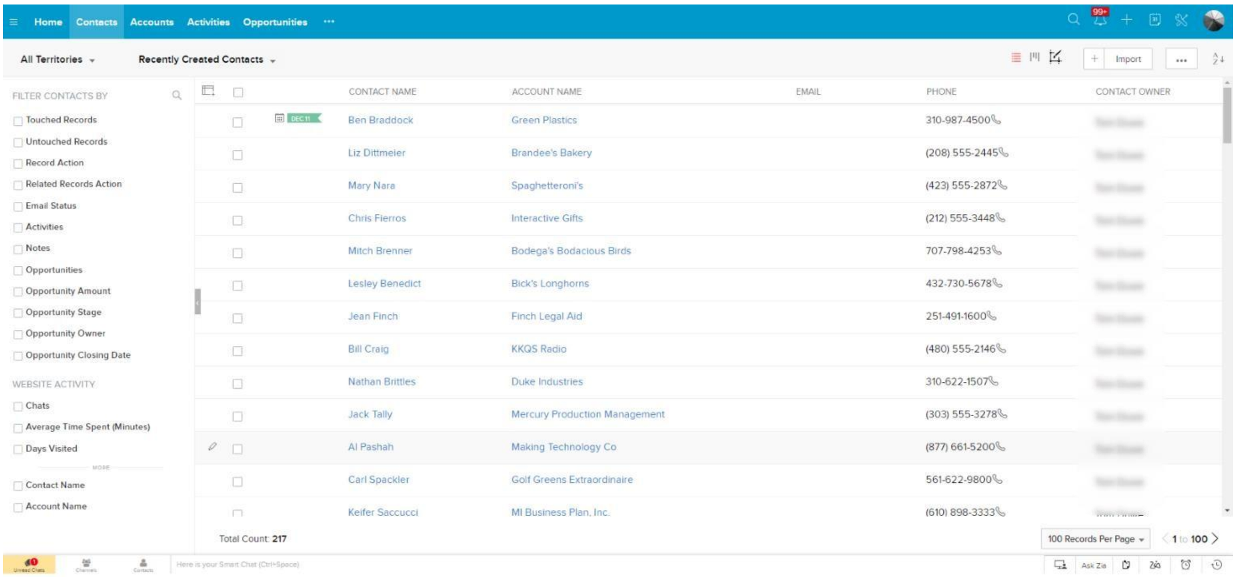
A. Learning ZOHO CRM for Lead Management

Nowadays, majority of the companies use CRM tools to manage their leads, qualified leads so as to keep a track of the number of inbound & outbound leads. This CRM tool helps in analysing the total number of data, the data that is being qualified, out of that qualified data the amount of data gets converted into deals. The CRM also helps organisations in keeping a track of an employee’s daily work as well as analysing the performances of each employee. In Kratikal, the CRM tool used is ZOHO. Hence, it aids in managing a company's interaction with current as well as prospects by analysing clients' history with the company, thus improving business relationships with the existing clients & their retention.

However, the main function of business development is also to create a room for long-term opportunities. To be at the paramount in business development, one needs to good at building strong relationships with prospect & clients. Zoho CRM helps recognise the loopholes in our endeavours so that one can change in order to gain better results.



Leads Updation in Zoho CRM ensures that the uploaded is correctly mapped. Excel sheets can also be imported from the computer to the CRM and thus, proves to be time-efficient. The leads generated have a specific parameters in the excel sheet which are mapped with the corresponding parameters present in Zoho CRM.



CONTACT NAME	ACCOUNT NAME	EMAIL	PHONE	CONTACT OWNER
Ben Braddock	Green Plastics		310-987-4500	
Liz Dittmeier	Brandee's Bakery		(208) 555-2445	
Mary Nara	Spaghetteroni's		(423) 555-2872	
Chris Fierros	Interactive Gifts		(212) 555-3448	
Mitch Brenner	Bodega's Bodacious Birds		707-798-4253	
Lesley Benedict	Bick's Longhorns		432-730-5678	
Jean Finch	Finch Legal Aid		251-491-1600	
Bill Craig	KKQS Radio		(480) 555-2146	
Nathan Brittles	Duke Industries		310-622-1507	
Jack Tally	Mercury Production Management		(303) 555-3278	
Al Pashah	Making Technology Co		(877) 661-5200	
Carl Spackler	Golf Greens Extraordinaire		561-622-9800	
Keifer Saccucci	MI Business Plan, Inc.		(610) 898-3333	

Total Count: 217

100 Records Per Page 1 to 100

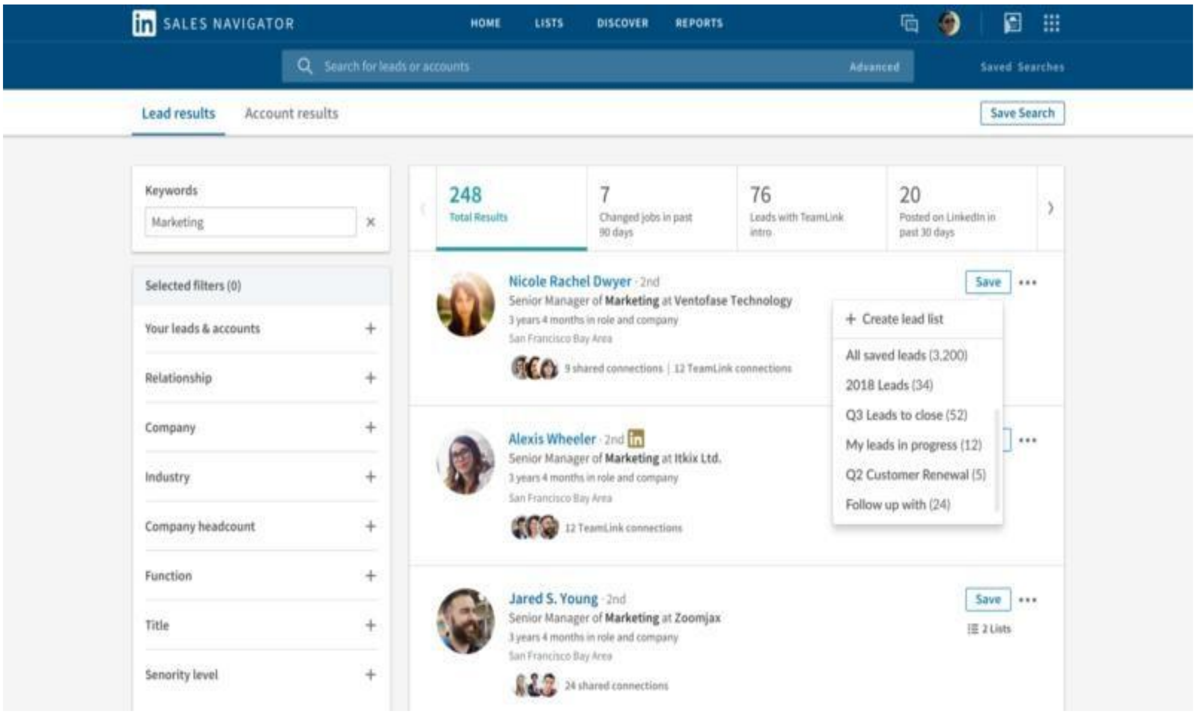
B. Data Mining

Data Mining is a process of extracting data from various sources. In business development, the data that is typically mined consists of Company names, the person who has relevant experience in cyber-security i.e. CISO/CIO/CTO, email id, phone number, head count of the company, LinkedIn profiles, cities and many more.

Usually it is easy find all the parameters except for email ids & phone numbers. There are various tools that help one find relevant data about the industries. One such tool is LinkedIn Sales Navigator.

LinkedIn Sales Navigator:

LinkedIn Sales Navigator helps in building the perfect list of customers by segmenting the most relevant leads on the basis of the applied filters for your business. The applied filters helps in narrowing down your search and find an ideal customer profile thus, improving the probability of conversion. Hence, segmenting a vast amount of data down to the relevant leads can really be beneficial for you as well as the organisation.



Keywords: Marketing

Selected filters (0)

- Your leads & accounts +
- Relationship +
- Company +
- Industry +
- Company headcount +
- Function +
- Title +
- Senority level +

248 Total Results | 7 Changed jobs in past 90 days | 76 Leads with TeamLink intro | 20 Posted on LinkedIn in past 30 days

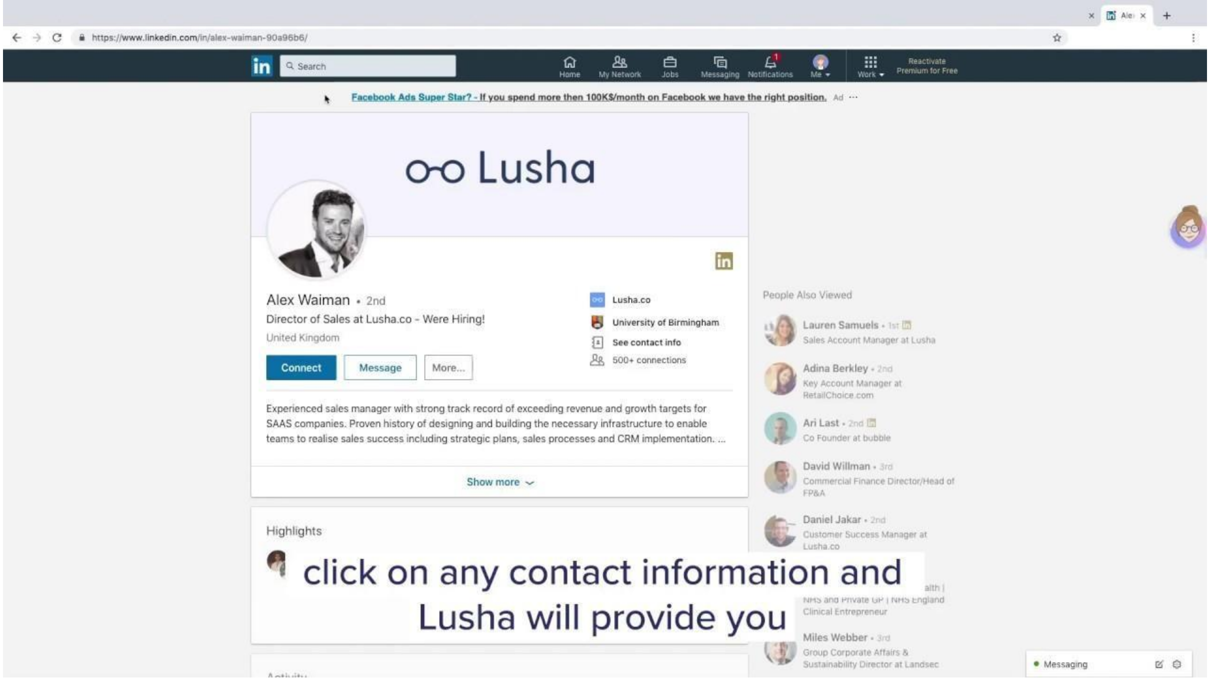
Nicole Rachel Dwyer · 2nd
Senior Manager of **Marketing** at Ventofase Technology
3 years 4 months in role and company
San Francisco Bay Area
9 shared connections | 12 TeamLink connections

Alexis Wheeler · 2nd
Senior Manager of **Marketing** at Itkix Ltd.
3 years 4 months in role and company
San Francisco Bay Area
12 TeamLink connections

Jared S. Young · 2nd
Senior Manager of **Marketing** at Zoomjax
3 years 4 months in role and company
San Francisco Bay Area
24 shared connections

Lusha:

Lusha is a software providing unique & high quality premium data in order to increase the number of clients/prospects. It uses various algorithms to extract the data such as emails and phone numbers hence, helping many sales & marketing professionals to boost their organisations' campaigns by improving their revenue and business growth.



https://www.linkedin.com/in/alex-waiman-90a96b6/

Facebook Ads Super Star? - If you spend more then 100K$/month on Facebook we have the right position. Ad

Alex Waiman • 2nd
Director of Sales at Lusha.co - Were Hiring!
United Kingdom

Lusha.co
University of Birmingham
See contact info
500+ connections

Experienced sales manager with strong track record of exceeding revenue and growth targets for SAAS companies. Proven history of designing and building the necessary infrastructure to enable teams to realise sales success including strategic plans, sales processes and CRM implementation. ...

People Also Viewed

Lauren Samuels • 1st
Sales Account Manager at Lusha

Adina Berkley • 2nd
Key Account Manager at RetailChoice.com

Ari Last • 2nd
Co Founder at bubble

David Willman • 3rd
Commercial Finance Director/Head of FP&A

Daniel Jakar • 2nd
Customer Success Manager at Lusha.co

alth | NHS and Private GP | NHS England Clinical Entrepreneur

Miles Webber • 3rd
Group Corporate Affairs & Sustainability Director at Landsec

click on any contact information and
Lusha will provide you

C. Cold Calling

After extracting the data into the sheet, it is updated on the Zoho CRM as leads. One the leads have been updated in the Zoho CRM, the lead generation process starts. Initially, calling is the form through which we reach-out after sending a LinkedIn request. The calling is done to get familiar with each other's organisation as well as build a relationship. Besides, building relationship another objective is to create a need for our product & services in their organisation. How effectively can you pitch really depends on the impact you create on somebody's mind.

If you are successful in creating a need & then you pitch the solution to the problem mentioned. This will convince the other individual to let you expand on your organisations' offerings to their company.

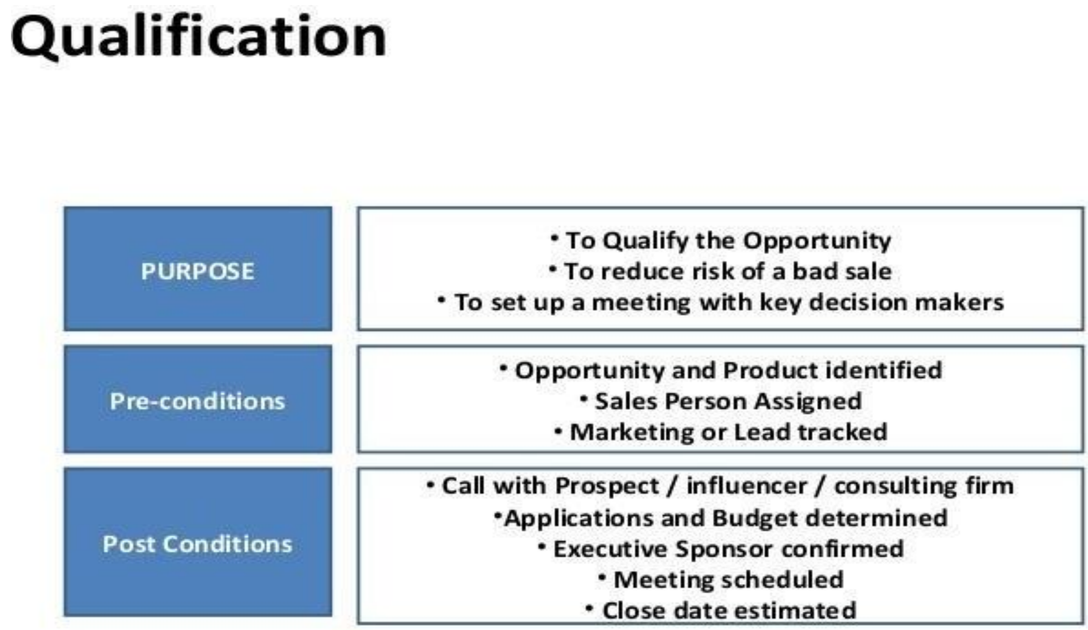
After the meeting has been fixed, the pre-sales take the meeting thus elaborating the products even more. This helps the prospect to make an informed decision that is most likely to convert into a deal.

D. Meetings

Usually, the meetings are taken by the pre-sales employees. The conversion majorly depends on how well a business development individual can present the company in a meeting. The ultimate goal of a meeting is to get converted into a deal. For a meeting to get converted into a deal there are a lot of parameters that should be taken into consideration such as –

a. excellent communication skills
b. good rapport building skills
c. probing
d. pitching

Up until now, I have been a part of more than 15 meetings including face-to-face discussions as well as scheduled web call meetings that have taught me various factors such as pitching, probing, rapport building.



Qualification

PURPOSE	• To Qualify the Opportunity • To reduce risk of a bad sale • To set up a meeting with key decision makers
Pre-conditions	• Opportunity and Product identified • Sales Person Assigned • Marketing or Lead tracked
Post Conditions	• Call with Prospect / influencer / consulting firm •Applications and Budget determined • Executive Sponsor confirmed • Meeting scheduled • Close date estimated

5. CONCLUSIONS

Business Development plays a major role in creating new opportunities in business. Hence, the growth of the company depends upon business development staff. A Business Developer works to improve an organization's market position and achieve financial growth. This person job is to work with the internal team, marketing staff, and managers to increase sales opportunities and thereby, maximize revenue for their organization. There are three main components that forms the base of business development: markets, customers, and relationships. In order to grow a business beyond its current state, it is important to focus on one or more of these areas.

6. REFERENCES

1. Company Website - https://www.kratikal.com/

2. Threat Cop - https://www.threatcop.ai/

3. TAB - https://www.threatalertbutton.com/

4. KPMonitor- https://www.kpmonitor.com/

5. KDMARC- https://kdmarc.com/

6. Sales Navigator - https://www.linkedin.com/premium/products/?intentType=FIND_LEADS&upsellOrderOrigin=guest_login_sales_nav

7. Lusha - https://www.lusha.co/

8. ZOHO CRM - https://www.zoho.com/in/crm/

9. Compliance - https://www.kratikal.com/security-compliance-management.php

10. VAPT - https://www.kratikal.com/managed-security-services.php