CYBERMOKSH

ALERTNESS | KNOWLEDGE | WISDOM

Executive Brief

Cyberspace has been increasing and the cyber boundary for every country is no longer limited. In the past 7 years the growth of cyberattacks and taking control of cyber space has increased. Countries spend more time on creating a strong cyber arsenal as the threat landscape has changed drastically. No longer do we have novice hackers, but now we have specialist attackers for every domain. These specialists, understand the domain they are to hack and understand its day to day working style, and how the working style changes across countries. In these past 7 years, the quantum of cyberattacks has increased and also the quality and precision. New attack vectors, attack surfaces and techniques have come into existence. The technology shift is no longer yearly but literally daily.

These sudden developments have also increased the quantum of cyber incidents which Is leading to exponential growth of cyber incidents being reported and handled by organizations. These attacks are complex and no two attacks match 100%. Hackers are also no longer individuals, but now work as organizations and even state sponsored hacktivists. The need of the hour is automation.

Automation is the backbone of our solution which ensures that the end user is in control. Our custom algorithm allocates incidents based on past handing of incidents to the appropriate specialist. With the integration of 3rd party investigative tools the user gets the results from the tools and enabling them to take efficient decisions.

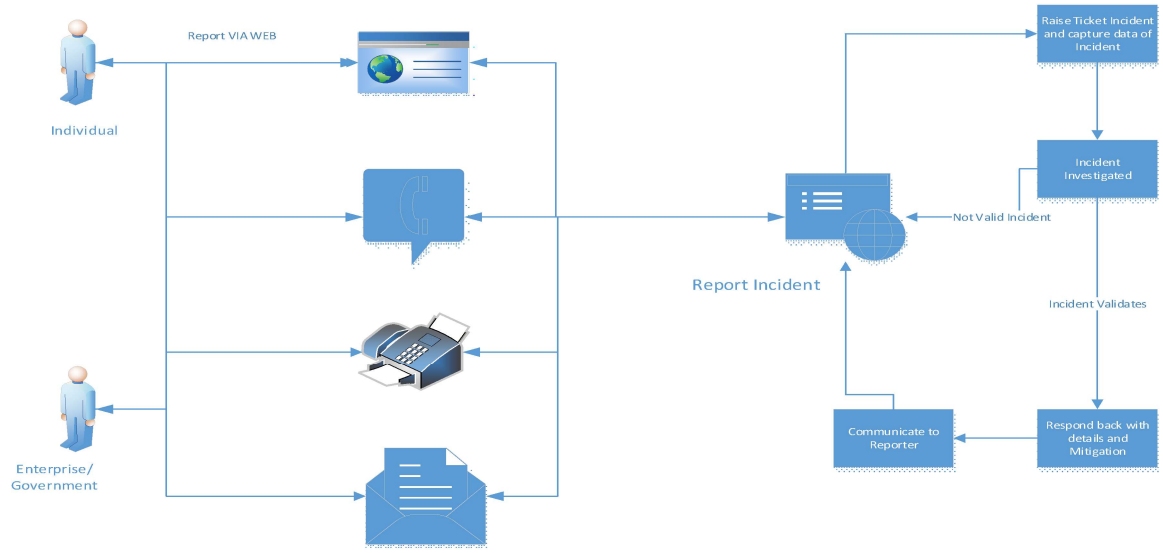
Incident Response Management- IRM

IRM, is an automated tool created to help Computer Security Incident Response team (CSIRT), CERTs and SOC's with capabilities to define the roles and responsibilities of Incident Response Stakeholders, to characterize incidents, and the relationships to policies and procedures and reporting requirements.

IRM's backbone is automation and the solution ensure that the lifecycle of each incident and details available to all users who are involved to resolve the incident.

CYBERMOKSH

ALERTNESS | KNOWLEDGE | WISDOM



High Level Overview of Incident Tracking System

The Key features of our solution are

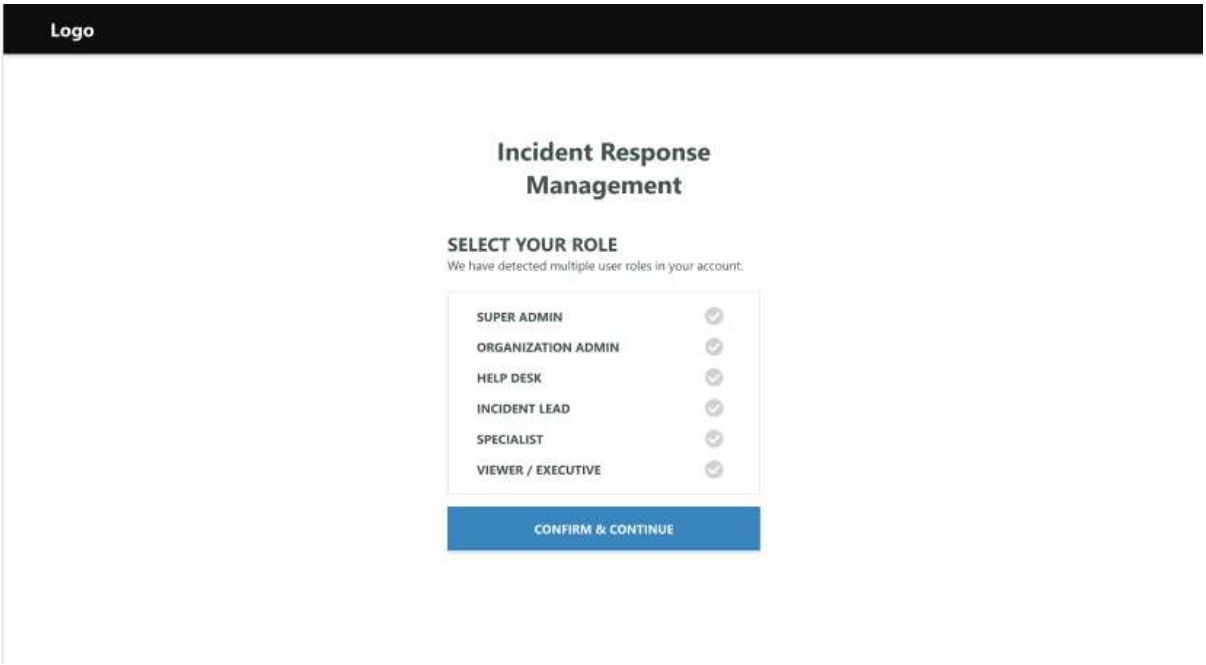
- Automated and semi-automated solution.
- Integration of 3rd tools like virus total, cuckoos' sandbox, WhoisAPI etc.
- Centralised Incident reporting, tracking and management system
- Automated allocation of Incidents
- Multiple methods for incident reporting
- Incident correlation with analysis
- Multi-Tenancy
- RBAC to ensure granular access control
- Enterprise ready
- Varied dashboards depending on user role
- Multiple methods of Incident reporting
- Incident Case Management
- Support for multiple incident categories and sub categories
- External Incident reporting page
- Built in custom algorithms to allocate incidents to team
- Using AI/ML to analyse incidents
- Supports MITRE Attack framework
- Built in Playbooks and allow user to create custom playbooks
- Ingest data from multiple sources

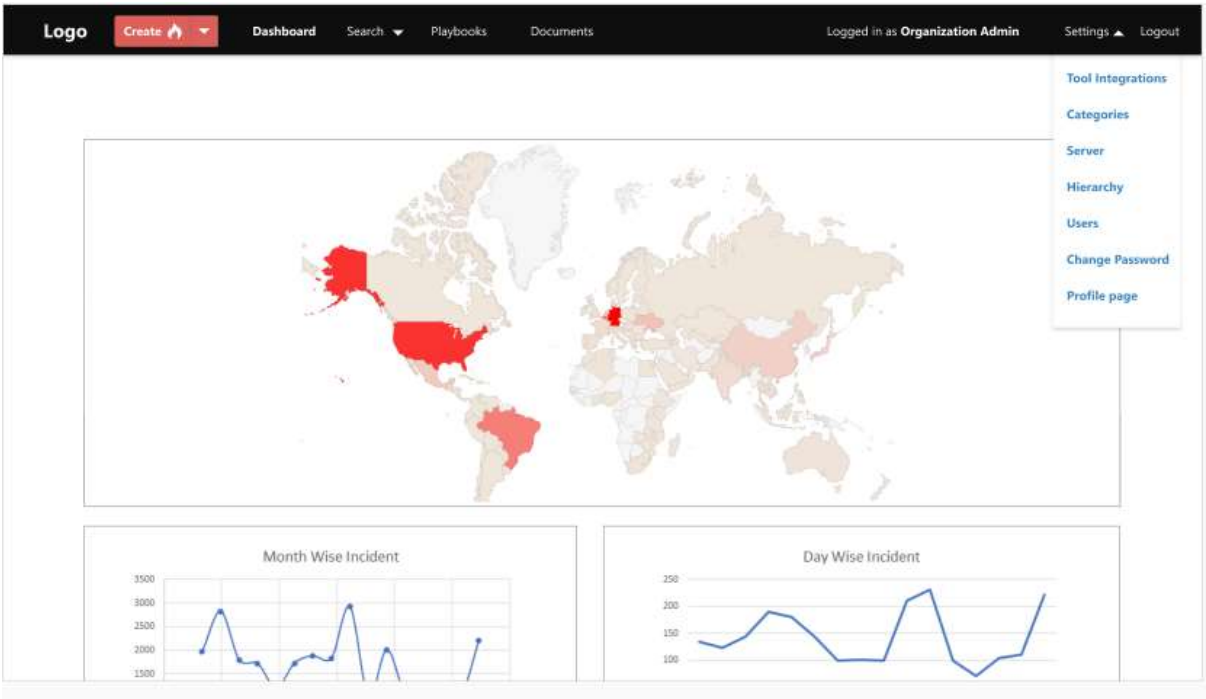
IRM, has a lot of checks and balances, like you need to mandatory create one (1) user for each role and category, else the solution would not allow any entry of incident data

Organization & Settings, Playbooks and Documents

In IRM, the user has an option to use a single tenancy as in the case for CERT's or CSIRTs or a multi-tenancy model for SOC's. The solution supports both models.

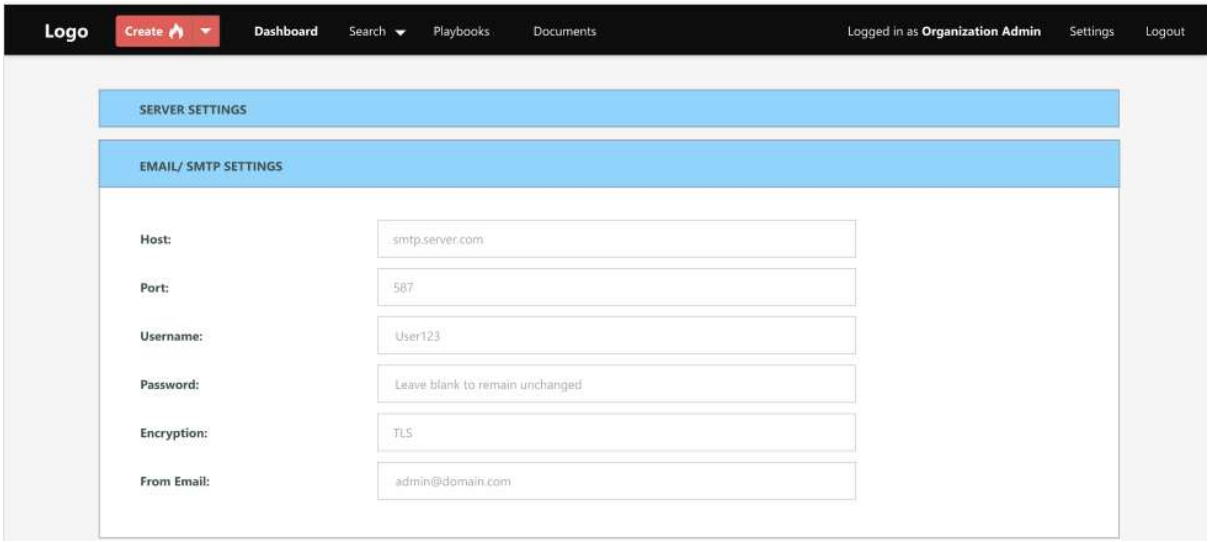
IRM has a built-in security and also enterprise ready with LDAP and email integration. The solution is delivered with default username (Admin) and default password (default1!) pre-fed. Once Logged in the Organization Admin can edit the organization details.

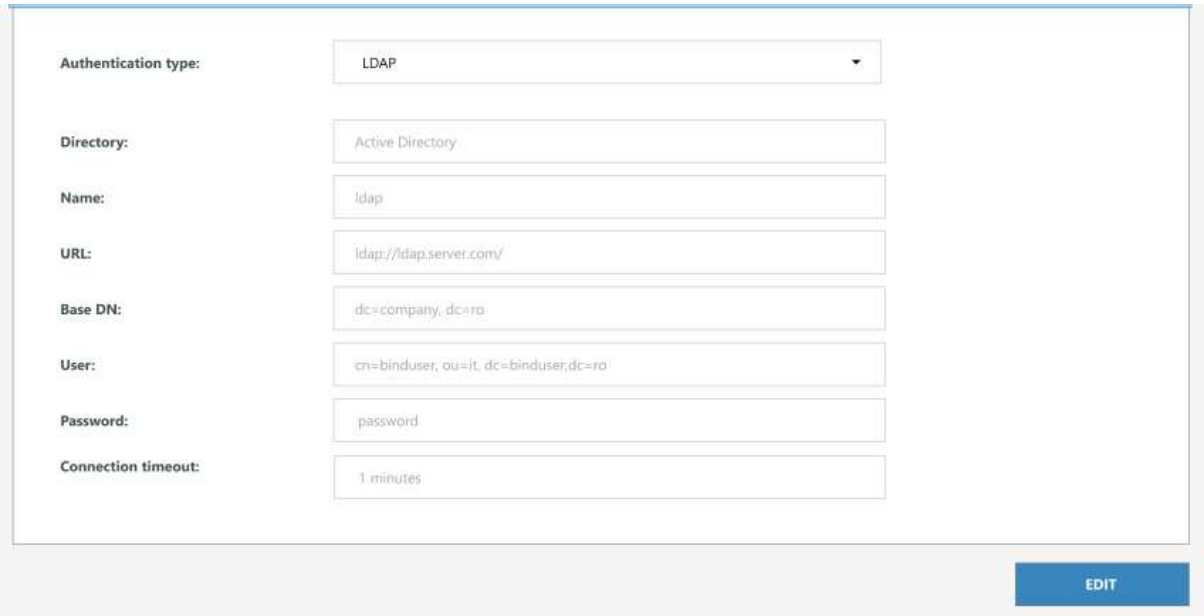




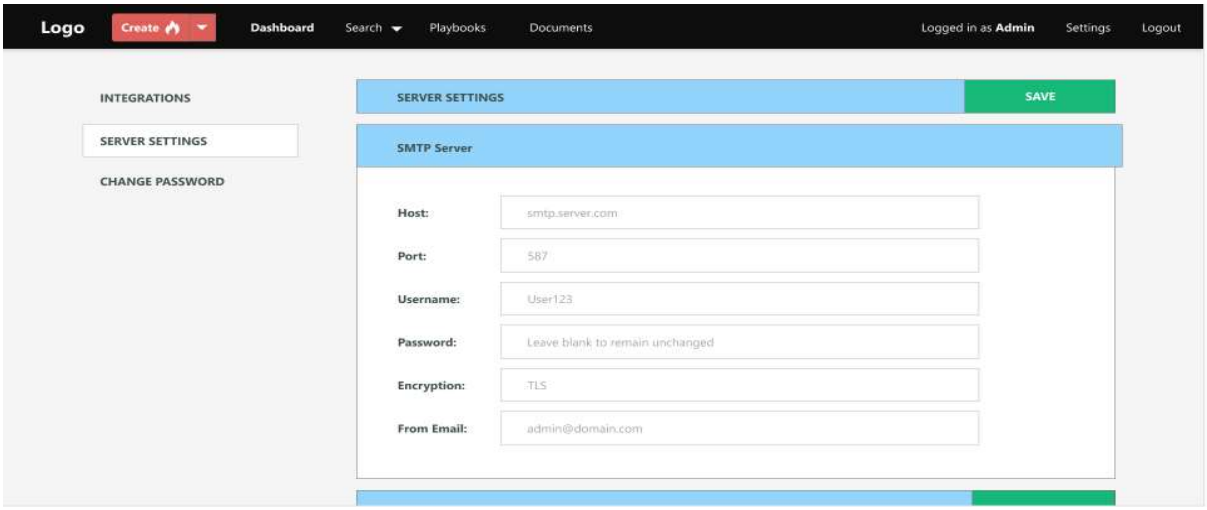
The Admin, has to enter the details pertaining to the Settings like

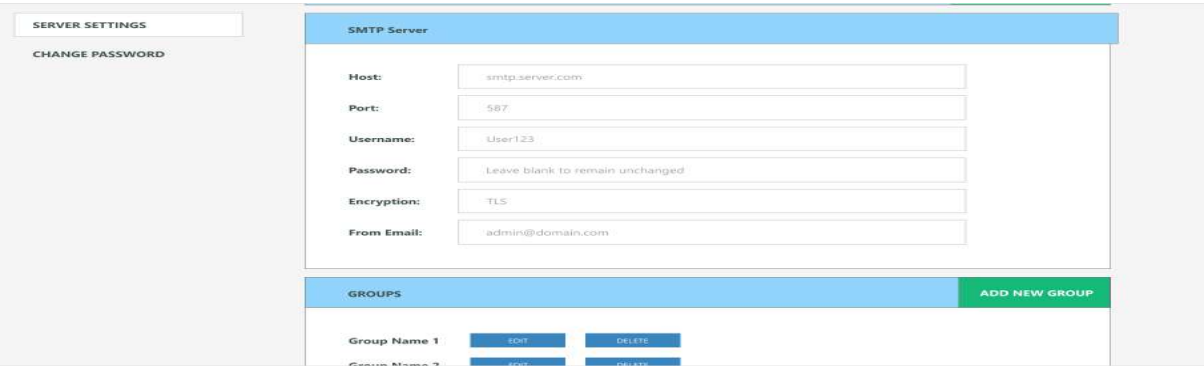
- LDAP settings
- Validating the availability of 3rd party tools (virus total, Cuckoos sandbox, WHOISAPI etc.,) and entering their API Keys.
- Creating specific groups
- Email server integration.

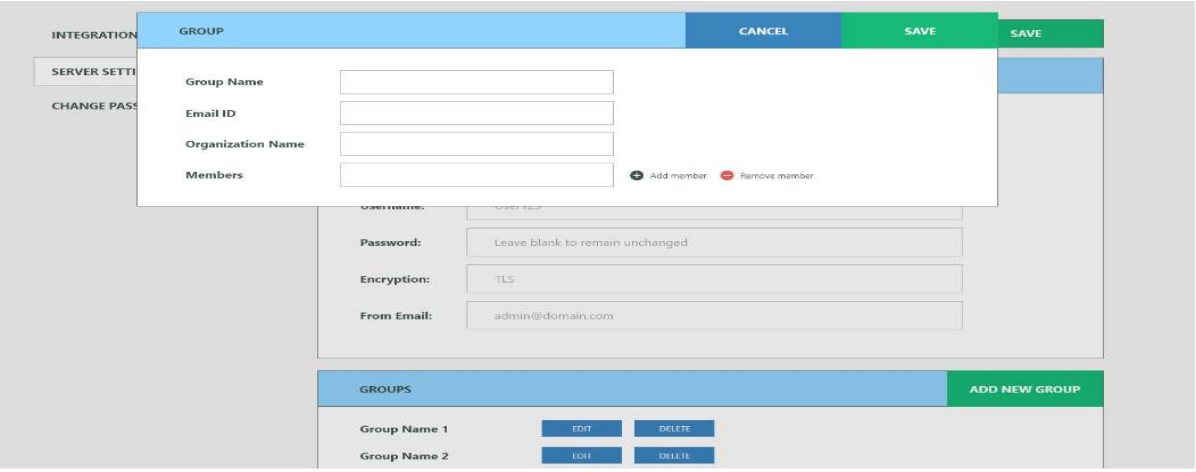




The Solution also allows the organization to create groups which may be required to create a Group to handle a specific investigation. Members can be added to the group.





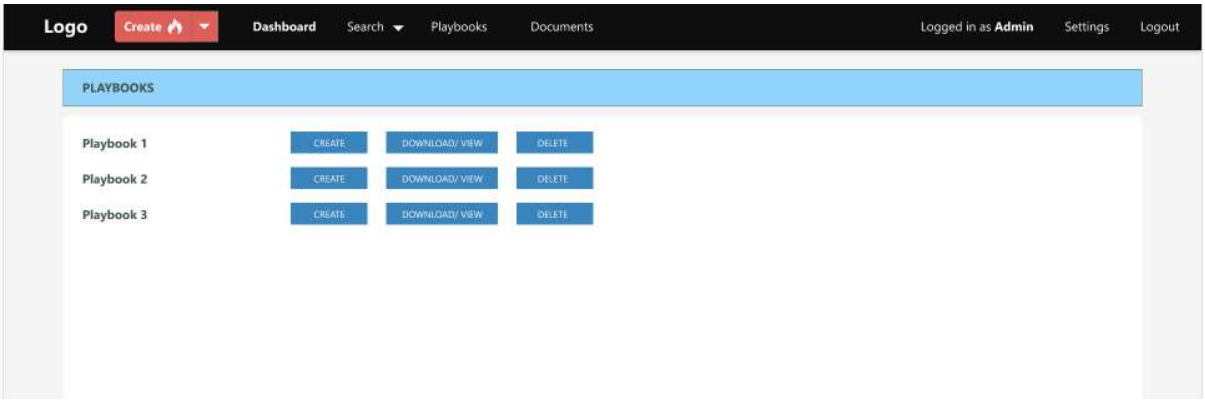

INTEGRATION
SERVER SETTI
CHANGE PASS
GROUP
CANCEL
SAVE
SAVE
Group Name
Email ID
Organization Name
Members
Add member
Remove member
Password:
Leave blank to remain unchanged
Encryption:
TLS
From Email:
admin@domain.com
GROUPS
ADD NEW GROUP
Group Name 1
EDIT
DELETE
Group Name 2
EDIT
DELETE

Playbooks

A Playbook is a very important tool used by organizations for managing Cyber Security Incidents.

A Playbook is a linear style checklist of required steps and actions required to successfully respond to specific incident types and threats. Incident Response Playbooks provide a simple step-by-step, top-down approach to orchestration. They help to establish formalized incident response processes and procedures within investigations and can ensure that required steps are systematically followed, which can help to meet and comply with regulatory frameworks or the way a particular incident category is to be addressed.

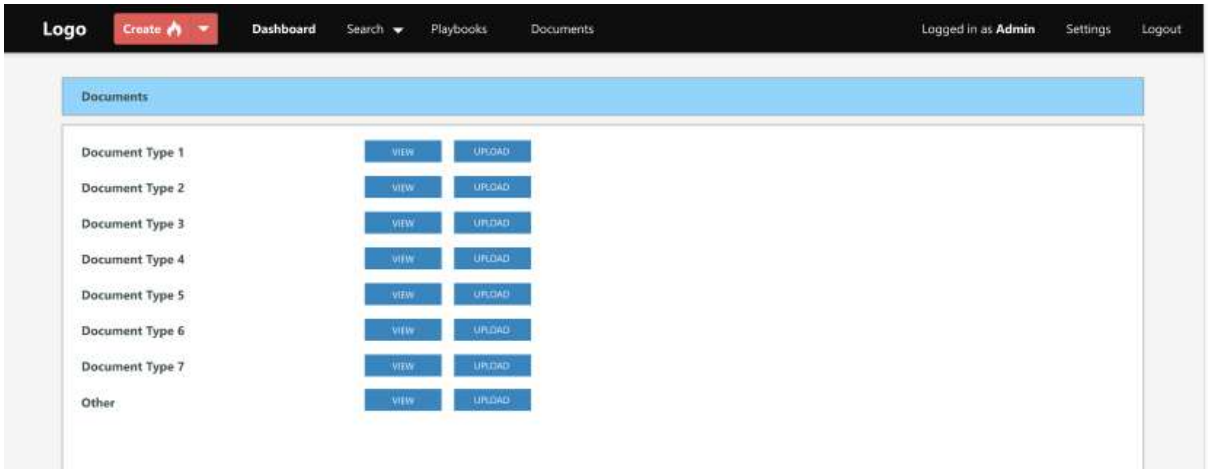
IRM has pre-fed playbooks which cover the major incident types present. The Admin and the Team Lead can create new playbooks, while all other roles can only view or download playbooks. A record of the user request for playbook download is maintained.

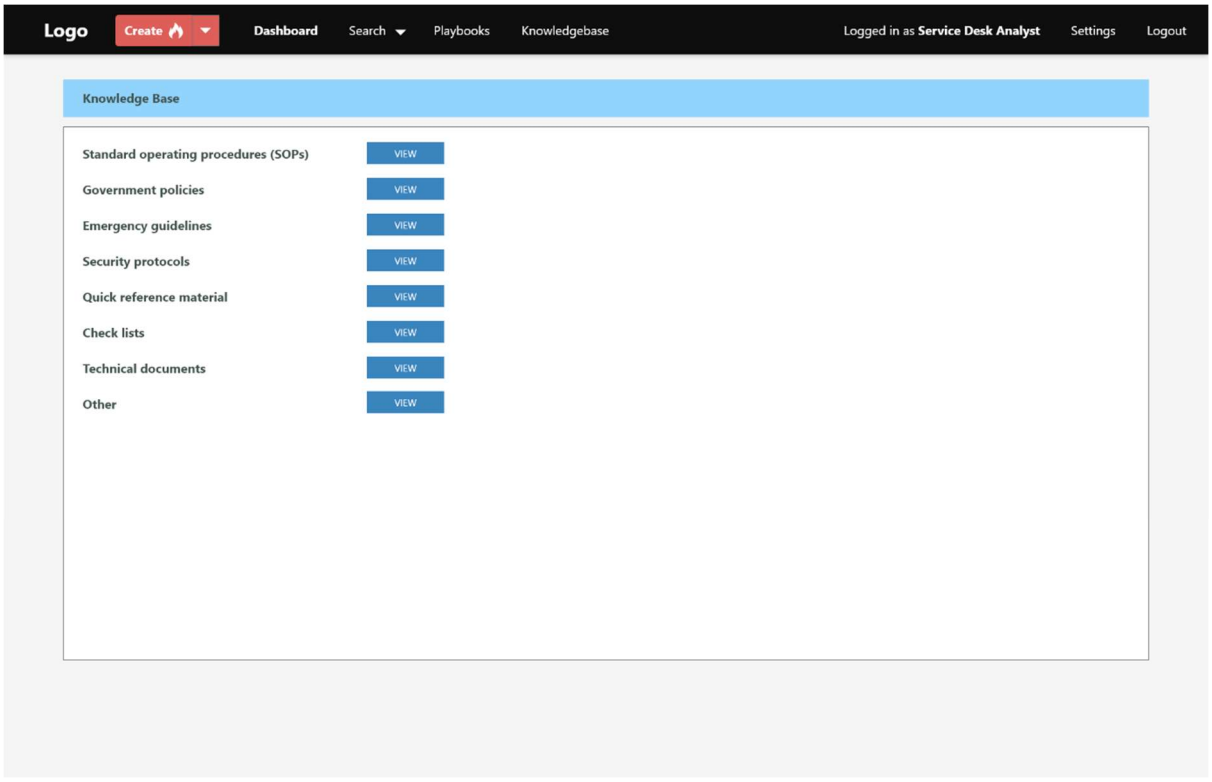


The Playbook would be stored in raw format in the backend database. When a request is made for download, the tool would capture the details of the user and download as a PDF and emboss the customer logo. One can create custom playbooks and the solution checks if a user is creating a playbook with an existing name.

Documents

The Documents section is the central repository where the organization can store its key information like Operating Procedures, Policies, Best Practices etc... The Admin is the only role allowed to upload documents.





Roles, Incident categories & Users

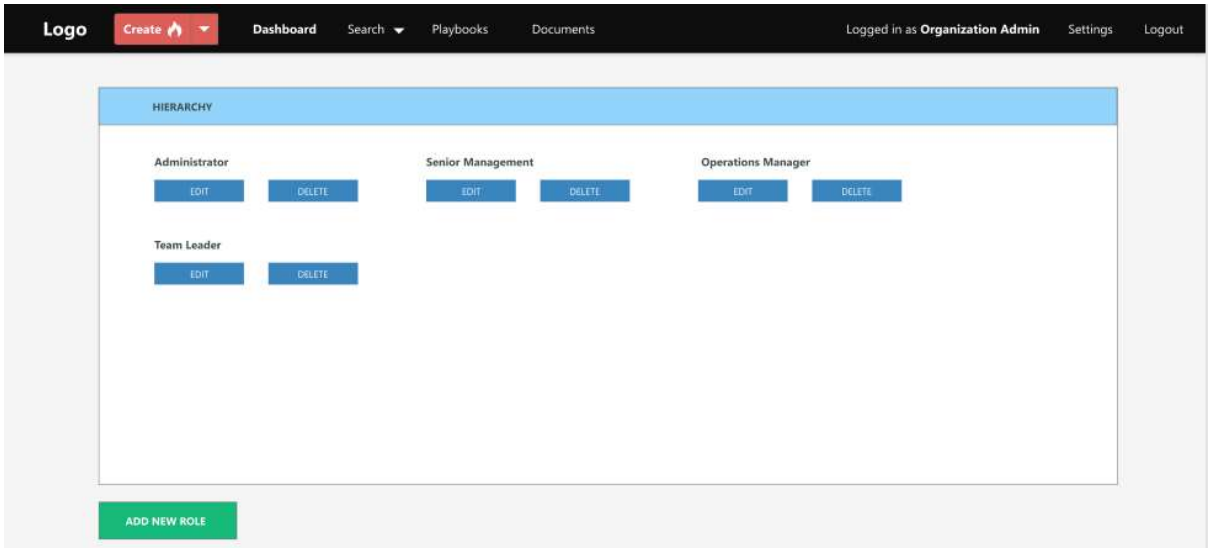
The solution uses two methods for Authentication. The organization can integrate the solution with their existing LDAP or can use local authentication of the solution.

Roles

We have defined multiple roles which are mapped to Incident categories. Till the time each user is not defined and mapped to an incident, one cannot start reporting/recording

incidents. The roles are clearly defined with their responsibilities and follow the role-based access control. Below is a list of roles including the external reporting entity.

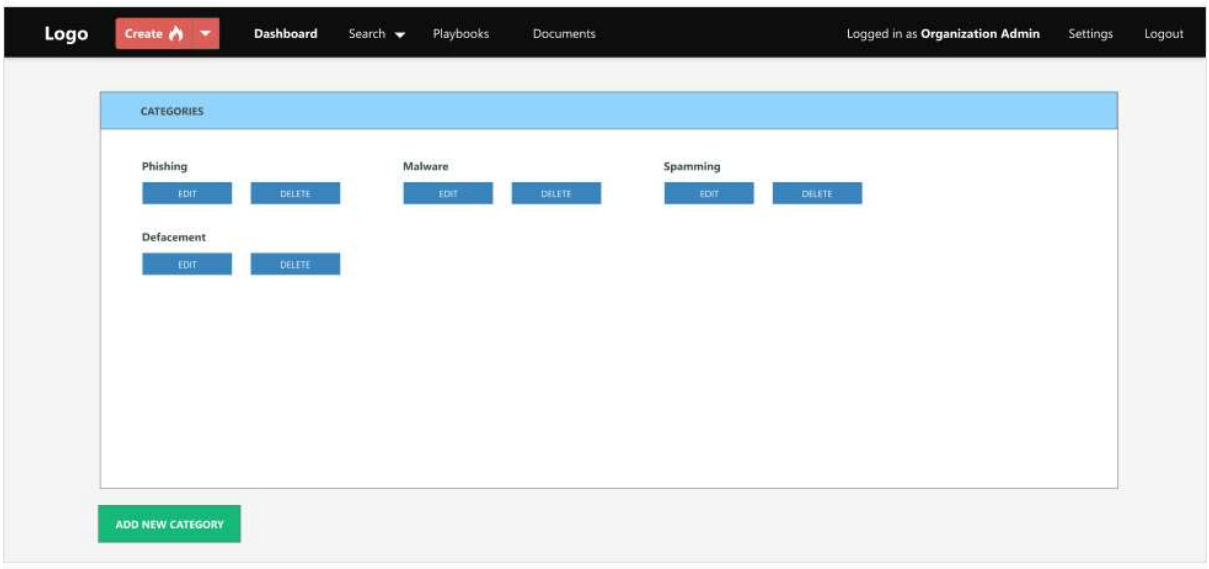
Role	Description
Administrator-Admin	Admin has complete control of every aspect in terms of editing the organization details, add/edit users, add/edit /upload documents and playbooks etc. Admin is not allowed to create incidents but can only view incidents.
Team Lead (TL)	Team Lead Is the manager of the Team. The Team Lead can be the lead for a single incident category or multiple incident categories. Team Lead can create a lead and also edit any lead at any stage or reallocate a lead to another user provided the person is the team lead for the role.
Help Desk (HD)	First point where Incident Reporters can report their incidents via a call, email, SMS or FAX. Help Desk is responsible for basic validation of any incident reported.
Incident Lead (IL)	Incident Lead is a member of a single incident category only. Once the lead is assigned by the Help Desk the Incident Lead analyses & validates the data to ascertain the incident type and also provide a remediation/solution
Specialist (SP)	A specialist who is a member of 1 incident category Team only. Once the lead is assigned by the lead, the Specialist analyses the data to ascertain the incident type and also provide a remediation/solution
Executive (EXE)	A senior management who only views the data



Incident Categories

Incident categories are pre-defined in the solution. IRM supports multiple incident categories and sub-categories which will allow the user to bifurcate the incidents granularly to extract more meaningful data.

Incident Category	Description
Availability	Attacks intended to put systems out of service, to cause damage to productivity and/or the image of the institutions being attacked.
Indian IT ACT	Covers under the Indian IT Act
Intrusions/Defacement	Attacks intended to exploit design, operation or configuration vulnerabilities in different technologies, in order to enter an organisation's systems fraudulently.
Malware	Software intended to infiltrate or damage a computer, server or other network device, without its manager or user finding out, for a variety of purposes.
Phishing	Attacks intended to collect fundamental information in order to launch more sophisticated attacks, through social engineering or identification of vulnerabilities.
Scanning	Attacks intended to collect fundamental information in order to launch more sophisticated attacks, through social engineering or identification of vulnerabilities.
Spamming	Incidents which lead to fraudulent actions, loss of money, reputation etc. in all its variants.
Others	Here all the ones that are not covered are put in this category

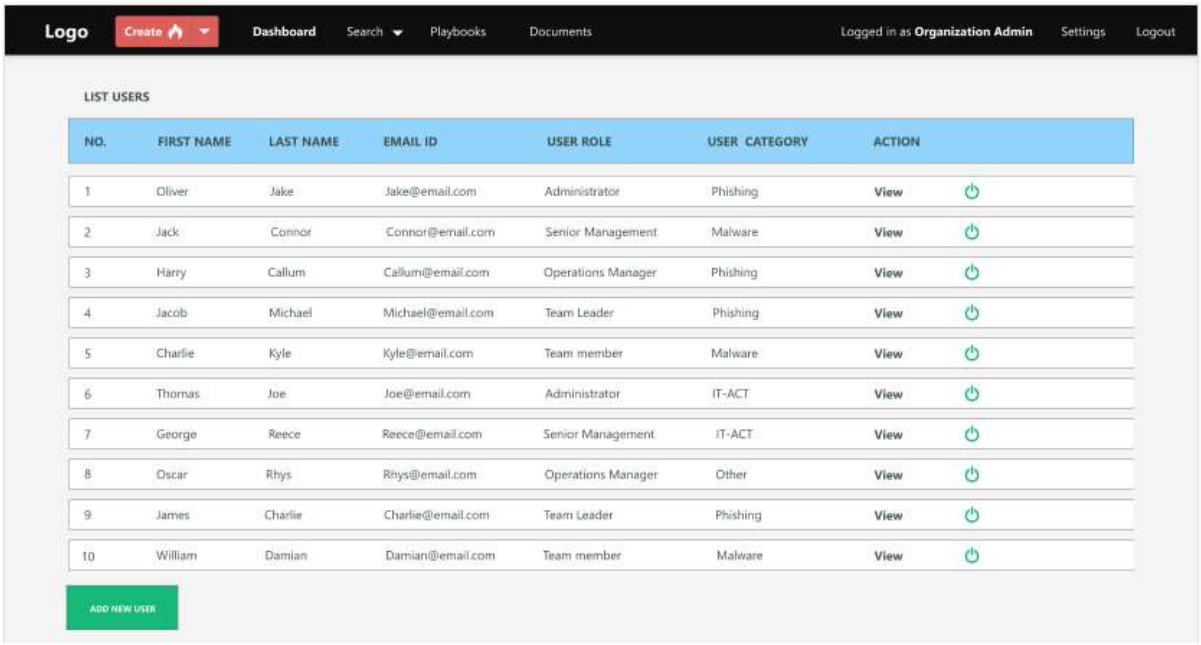


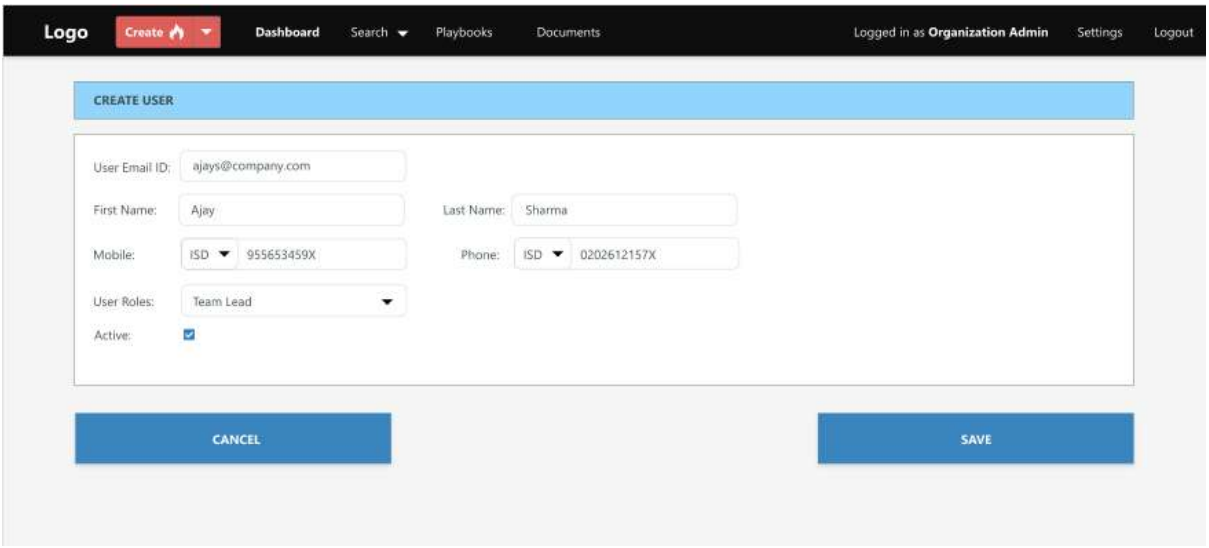
Users

Before proceeding to enter Incident details, the organization needs to create users. The User role categories have been defined in previous section. For each Incident category and role, a user has to be associated. If the same is not created the system would not allow you to make entry for incident reporting.

Each user would be assigned to an incident group.

- Admin- There is only One (1) Admin in the organization. Admin's is not given access to create an incident. Admin responsibilities are clearly defined and is responsible for managing the settings, creating /editing groups & users.
- Team Lead- a Team lead heads a particular team and can create, edit, re-allocate any incident. Team Lead can be a Team Lead for multiple Incident Categories, but an Incident Category cannot have more than One (1) Team Lead assigned to it.
- Help Desk- a member of this group would be associated with all incident categories. However, the Help Desk Associate can only view the incident category which they have been allocated
- Incident Lead- a member of this group would be associated with just 1 incident category. The member can only access/view data relevant to the member only
- Specialist- a member of this group would be associated with just 1 incident category. The member can only access/view data relevant to the member only
- Solution also has capability to create groups for specific tasks
- The External reporting entity would not have access to the internal portal but a front-end portal which would be external facing only.



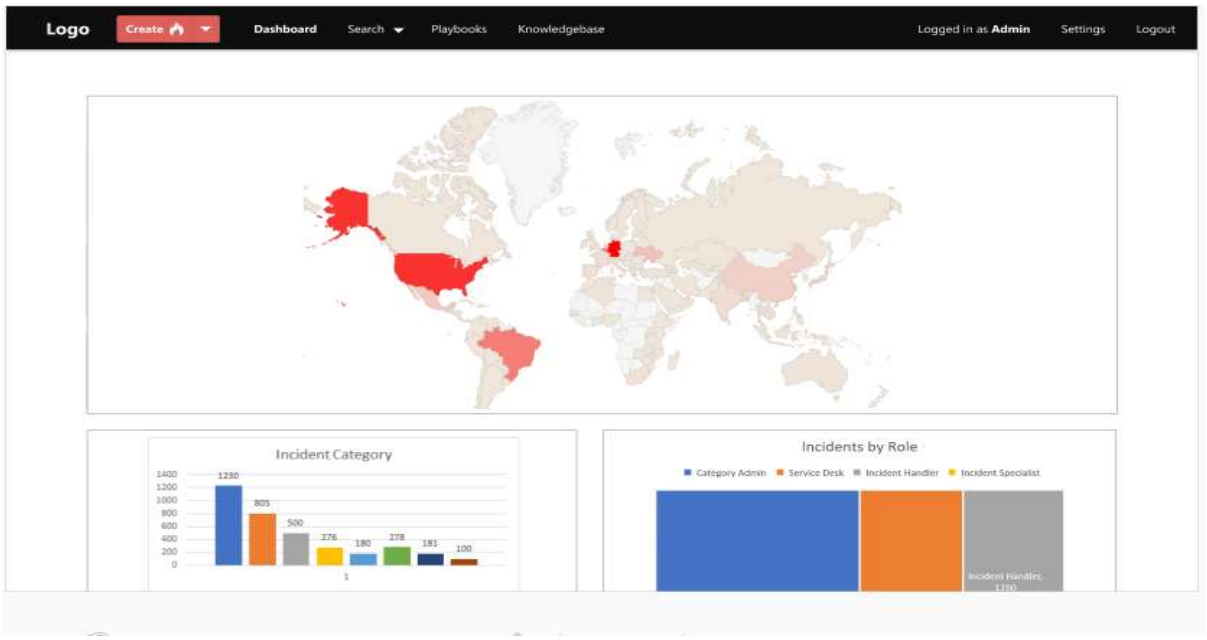

Logo
Create
Dashboard
Search
Playbooks
Documents
Logged in as Organization Admin
Settings
Logout
CREATE USER
User Email ID:
ajays@company.com
First Name:
Ajay
Last Name:
Sharma
Mobile:
ISD
955653459X
Phone:
ISD
0202612157X
User Roles:
Team Lead
Active:
CANCEL
SAVE

Dashboard & Landing page, Search Features

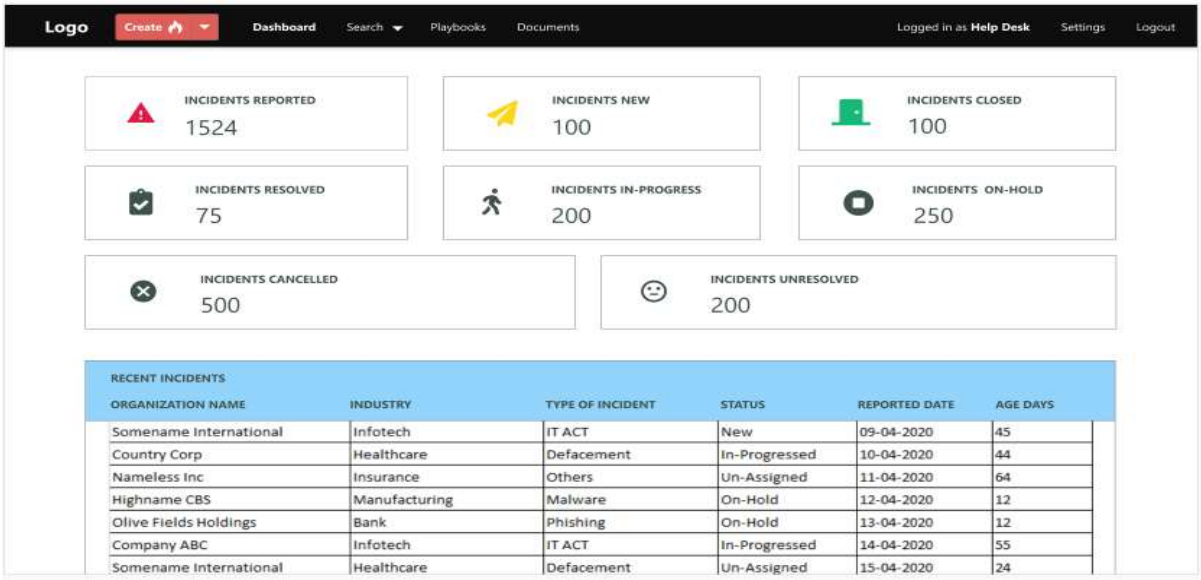
Based on the user role, the user would land on the relevant landing page. The landing page for each role is different and based on the user and role the relevant data would be displayed.

Dashboard & Landing page

Landing pages are segregated for the user type and segregated for Admin, Team lead and executive and Help desk, Incident Lead & specialist separately.



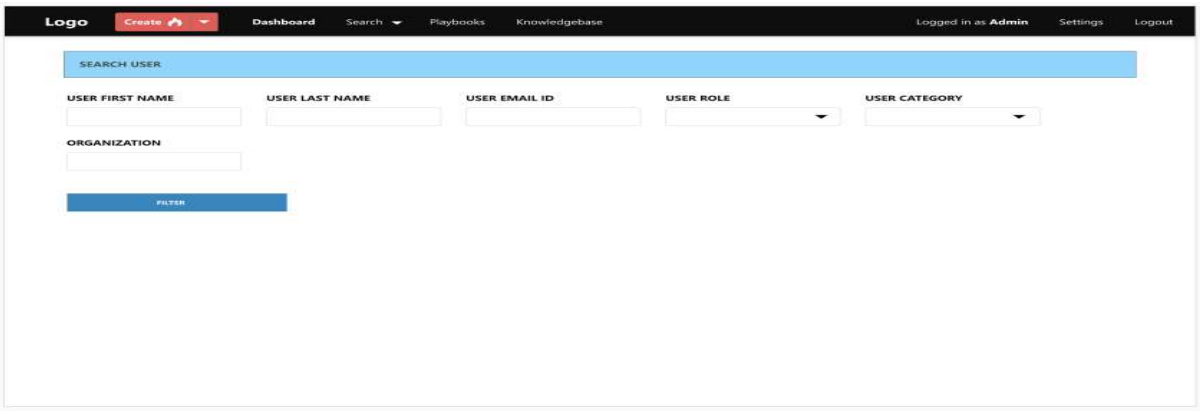
Landing page for Help Desk, Incident Lead and Specialist would be as below



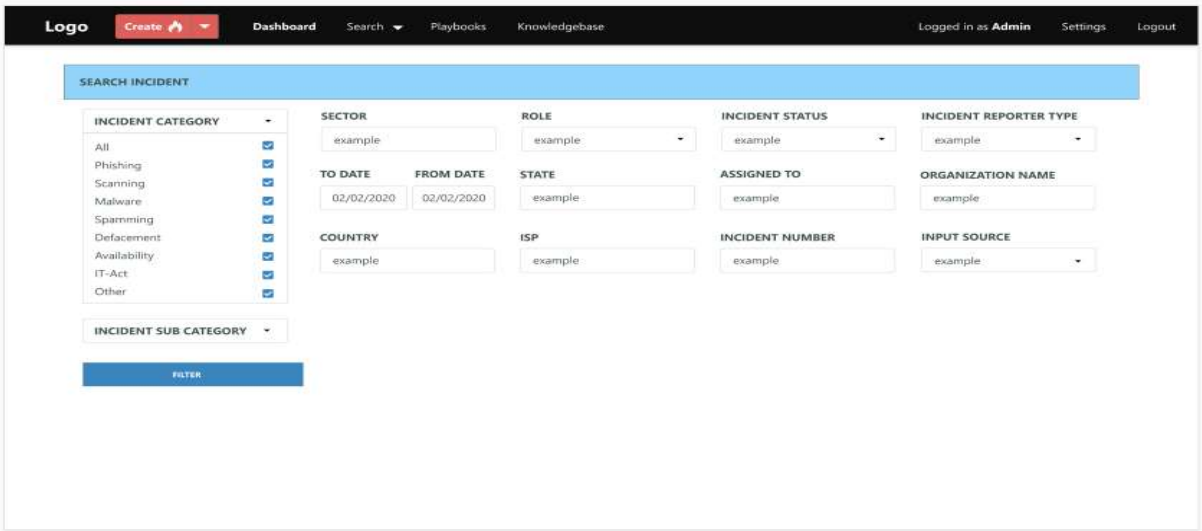
ORGANIZATION NAME	INDUSTRY	TYPE OF INCIDENT	STATUS	REPORTED DATE	AGE DAYS
Somename International	Infotech	IT ACT	New	09-04-2020	45
Country Corp	Healthcare	Defacement	In-Progressed	10-04-2020	44
Nameless Inc	Insurance	Others	Un-Assigned	11-04-2020	64
Highname CBS	Manufacturing	Malware	On-Hold	12-04-2020	12
Olive Fields Holdings	Bank	Phishing	On-Hold	13-04-2020	12
Company ABC	Infotech	IT ACT	In-Progressed	14-04-2020	55
Somename International	Healthcare	Defacement	Un-Assigned	15-04-2020	24

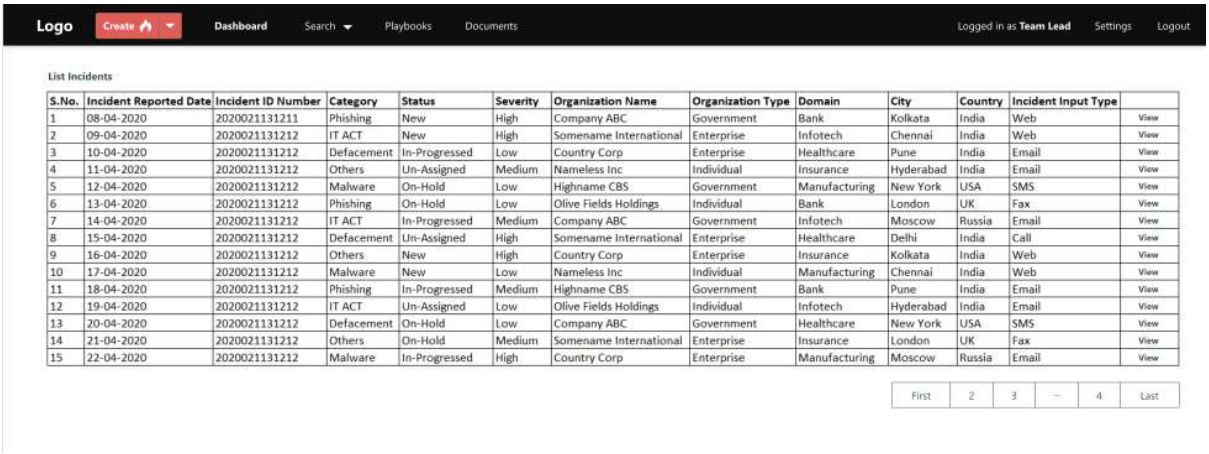
Search

The Search feature would render information based on the role. For example- the Admin can search & edit any Users & any Incidents, whereas the Team Lead can search & edit for only users who are part of the team or search for Incident which belongs to the category for the user is the Team Lead. Similarly, the Help Desk. Incident Lead and the Specialist, can only search for incidents for which they are assigned, and will not be able to view anyone else lead.



IRM also provides multiple combinations of search criteria parameters like Incident Categories, Sector, Incident Status etc.



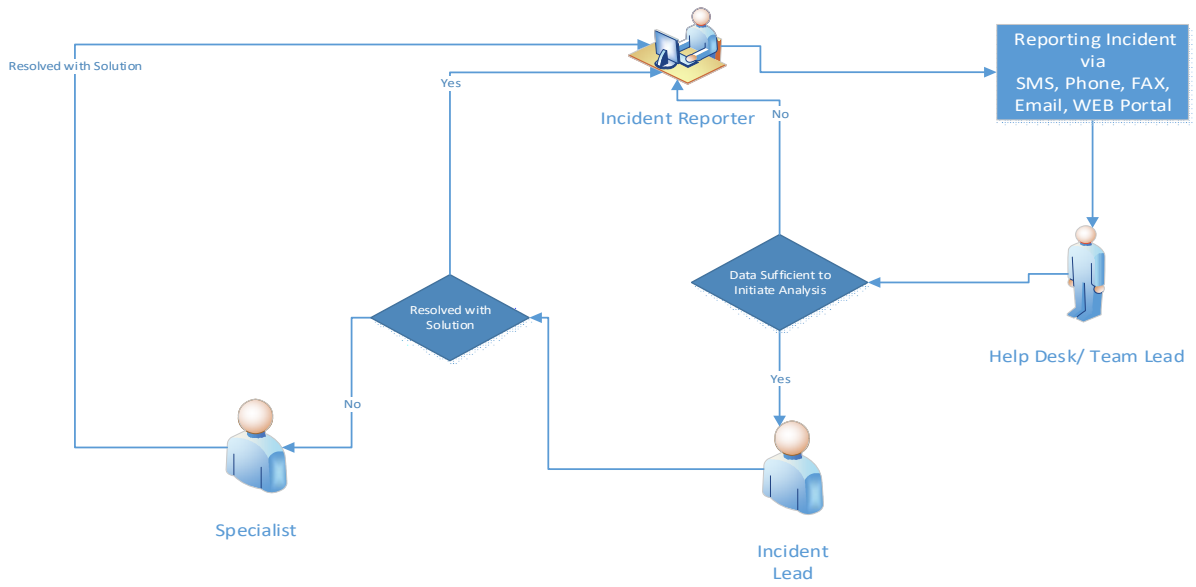


S.No.	Incident Reported Date	Incident ID Number	Category	Status	Severity	Organization Name	Organization Type	Domain	City	Country	Incident Input Type	
1	08-04-2020	2020021131211	Phishing	New	High	Company ABC	Government	Bank	Kolkata	India	Web	View
2	09-04-2020	2020021131212	IT ACT	New	High	Somename International	Enterprise	Infotech	Chennai	India	Web	View
3	10-04-2020	2020021131212	Defacement	In-Progressed	Low	Country Corp	Enterprise	Healthcare	Pune	India	Email	View
4	11-04-2020	2020021131212	Others	Un-Assigned	Medium	Nameless Inc	Individual	Insurance	Hyderabad	India	Email	View
5	12-04-2020	2020021131212	Malware	On-Hold	Low	Highname CBS	Government	Manufacturing	New York	USA	SMS	View
6	13-04-2020	2020021131212	Phishing	On-Hold	Low	Olive Fields Holdings	Individual	Bank	London	UK	Fax	View
7	14-04-2020	2020021131212	IT ACT	In-Progressed	Medium	Company ABC	Government	Infotech	Moscow	Russia	Email	View
8	15-04-2020	2020021131212	Defacement	Un-Assigned	High	Somename International	Enterprise	Healthcare	Delhi	India	Call	View
9	16-04-2020	2020021131212	Others	New	High	Country Corp	Enterprise	Insurance	Kolkata	India	Web	View
10	17-04-2020	2020021131212	Malware	New	Low	Nameless Inc	Individual	Manufacturing	Chennai	India	Web	View
11	18-04-2020	2020021131212	Phishing	In-Progressed	Medium	Highname CBS	Government	Bank	Pune	India	Email	View
12	19-04-2020	2020021131212	IT ACT	Un-Assigned	Low	Olive Fields Holdings	Individual	Infotech	Hyderabad	India	Email	View
13	20-04-2020	2020021131212	Defacement	On-Hold	Low	Company ABC	Government	Healthcare	New York	USA	SMS	View
14	21-04-2020	2020021131212	Others	On-Hold	Medium	Somename International	Enterprise	Insurance	London	UK	Fax	View
15	22-04-2020	2020021131212	Malware	In-Progressed	High	Country Corp	Enterprise	Manufacturing	Moscow	Russia	Email	View

First | 2 | 3 | ... | 4 | Last

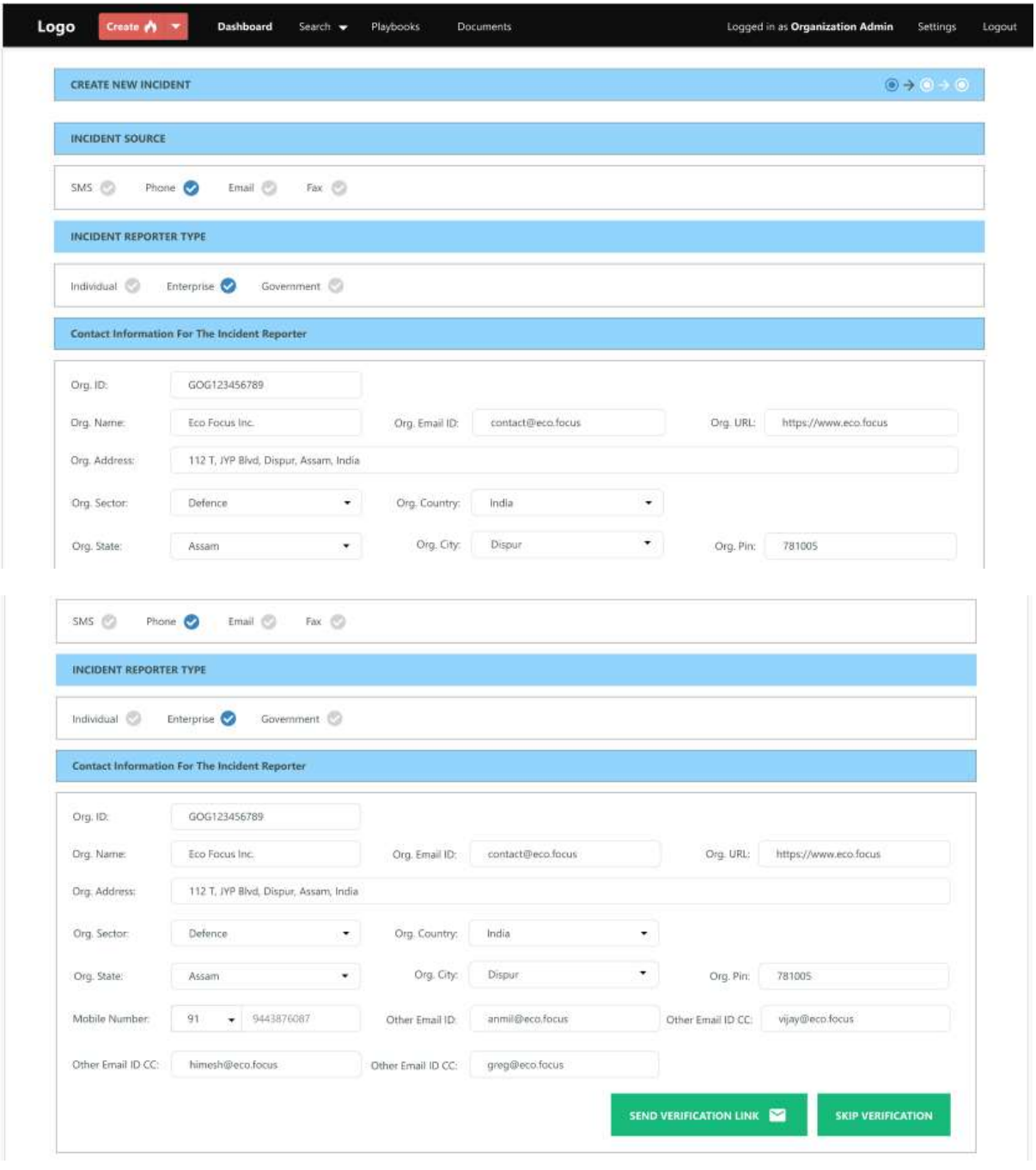
Incident Reporting & Management

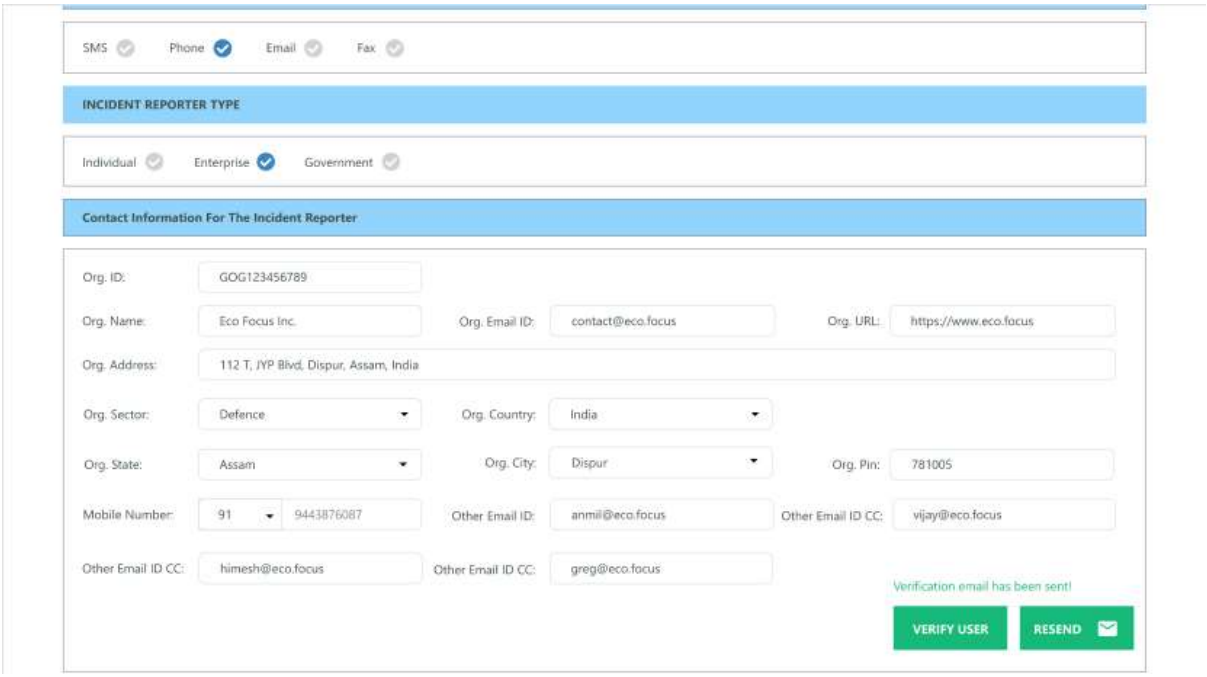
Reporting a cyber incident and documenting the facts is a very important aspect. Incorrect information entered could result in incorrect resolutions and compromises. **IRM** ensures that the user be it the Help Desk or the Team Lead capturing the incident details, verifies the reporter and the data before initiating a request for data analysis. Our solution ensures supports multiple methods of recording a cyber incident are supported. It also segregates whether the incident has been reported by an individual, a government body or an enterprise. It also supports segregating the governments into central and state governments and has pre-fed data of government organizations.

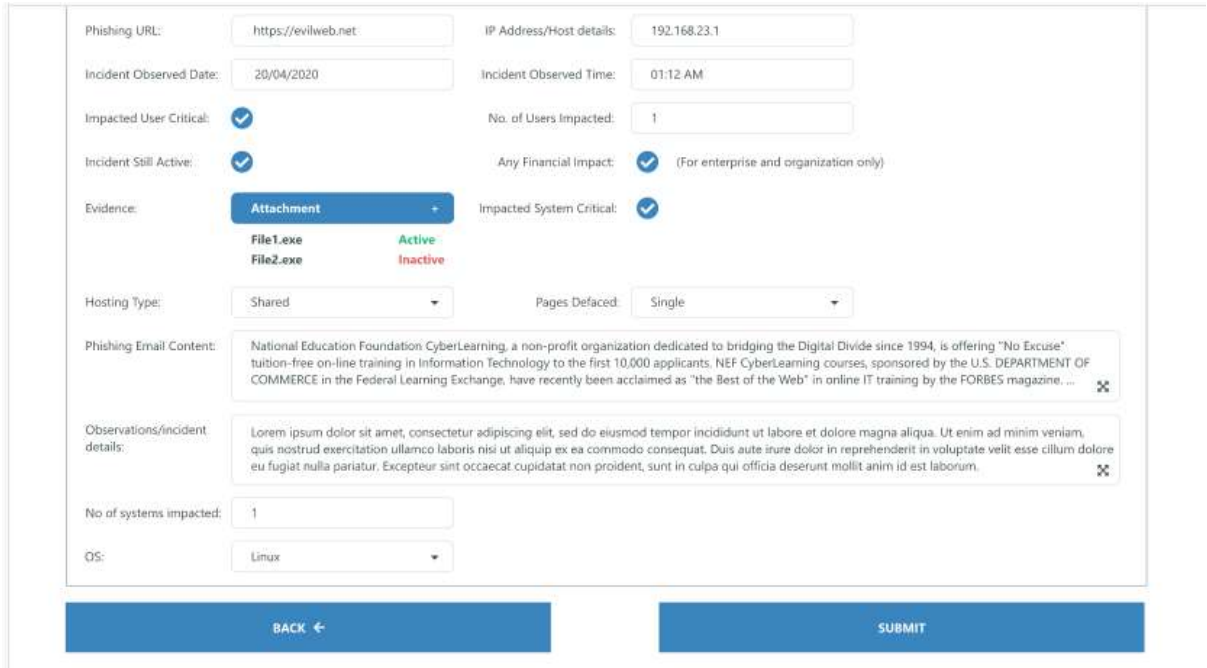


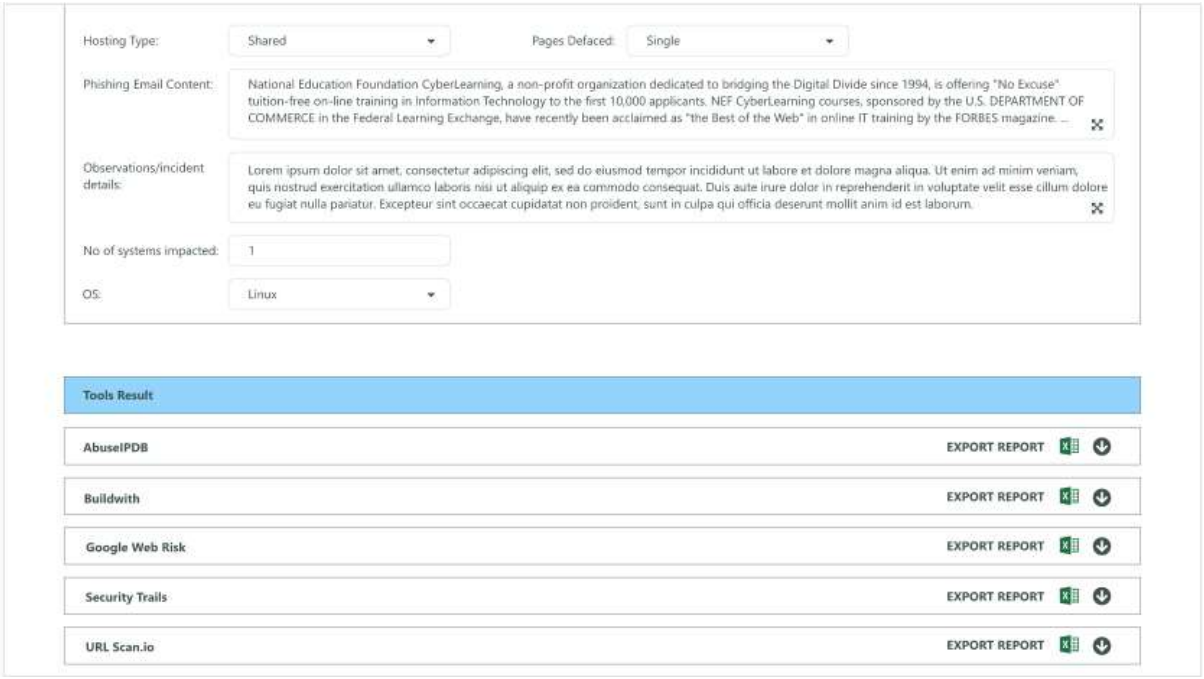
INCIDENT FLOW

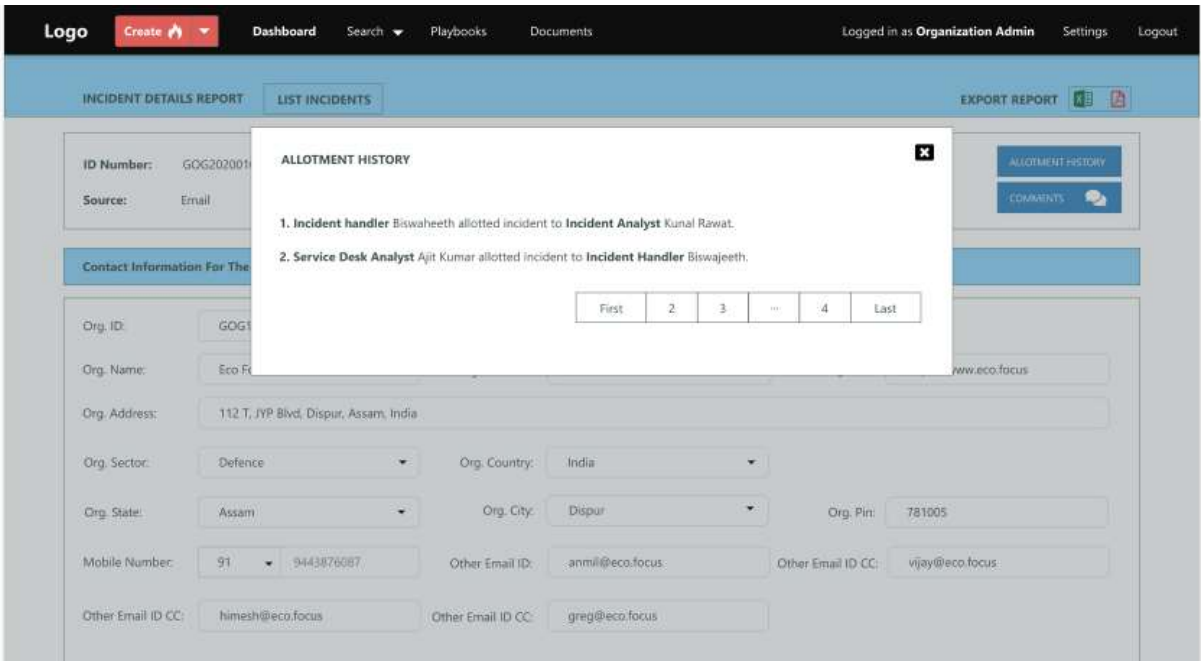
The lifecycle of the incident can be tracked from its method of reporting, which enables organisations to map their resources better. The solution also incorporates ML & AI to be able to correlate incidents providing better insights into the attacks. A new incident can only be created by the Help Desk member or the Team Lead member. Other roles like Incident Lead and Specialist would be allocated leads from the Help Desk or Team Lead. These would appear as new leads for them.

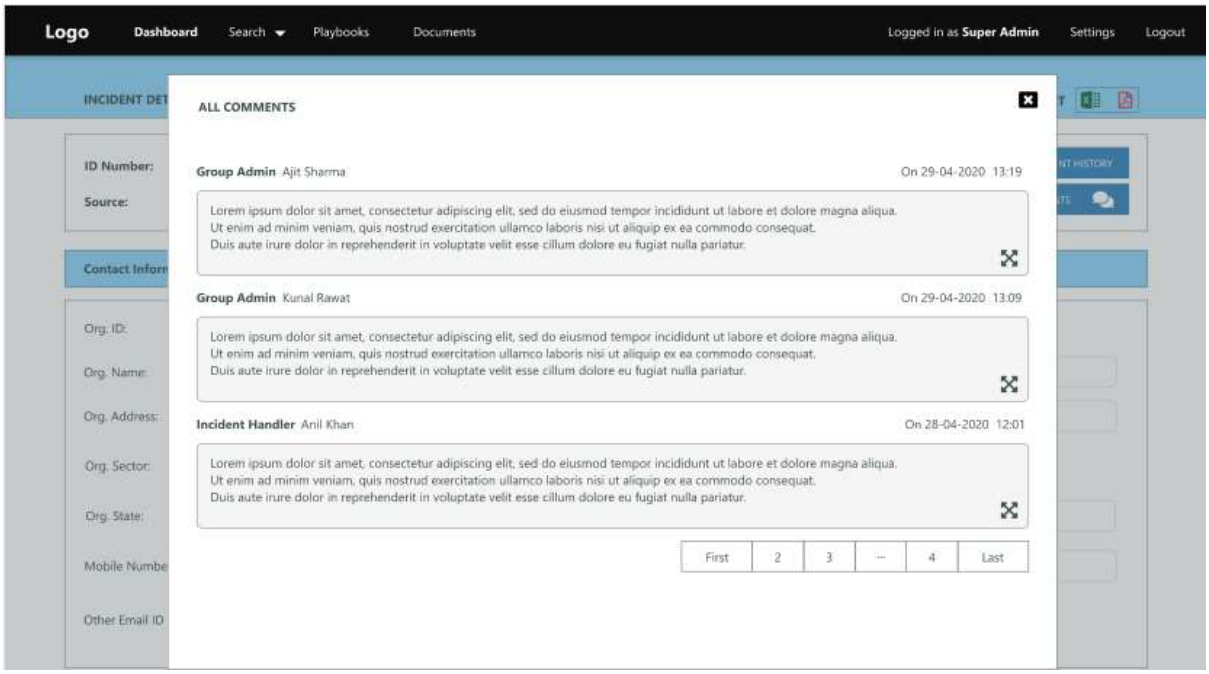


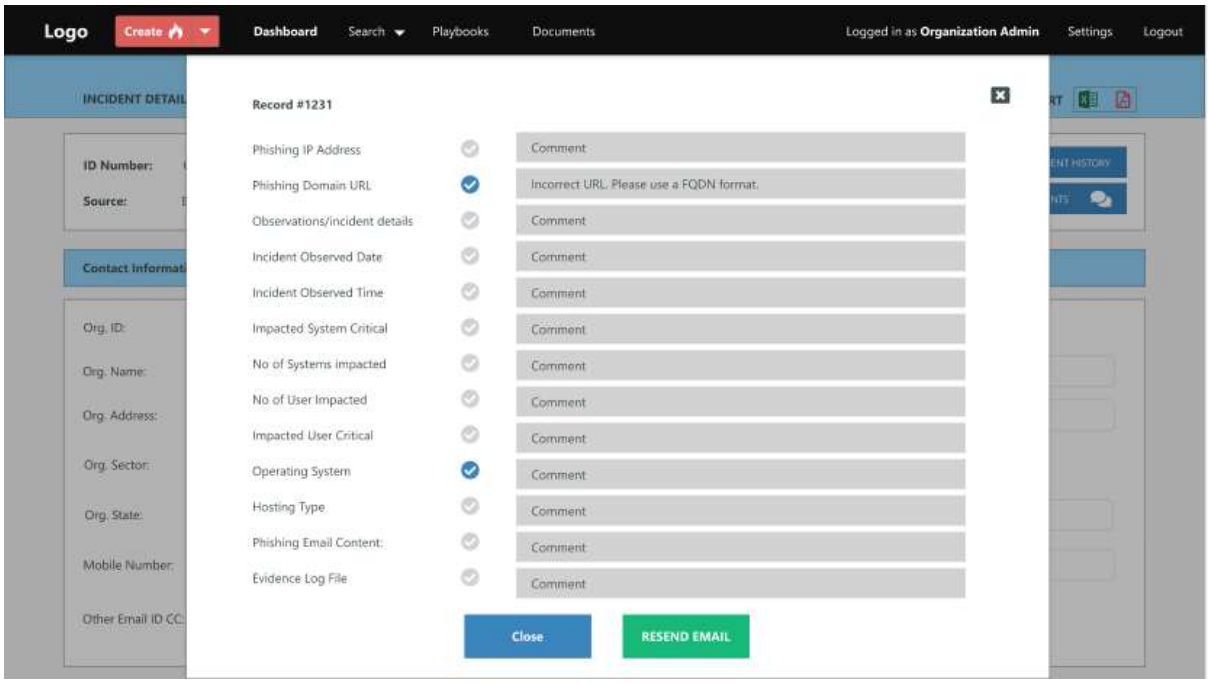

SMS
Phone
Email
Fax
INCIDENT REPORTER TYPE
Individual
Enterprise
Government
Contact Information For The Incident Reporter
Org. ID: GOG123456789
Org. Name: Eco Focus Inc.
Org. Email ID: contact@eco.focus
Org. URL: https://www.eco.focus
Org. Address: 112 T, JYP Blvd, Dispur, Assam, India
Org. Sector: Defence
Org. Country: India
Org. State: Assam
Org. City: Dispur
Org. Pin: 781005
Mobile Number: 91 9443876087
Other Email ID: anmil@eco.focus
Other Email ID CC: vijay@eco.focus
Other Email ID CC: himesh@eco.focus
Other Email ID CC: greg@eco.focus
Verification email has been sent!
VERIFY USER
RESEND


Phishing URL: https://evilweb.net
IP Address/Host details: 192.168.23.1
Incident Observed Date: 20/04/2020
Incident Observed Time: 01:12 AM
Impacted User Critical:
No. of Users Impacted: 1
Incident Still Active:
Any Financial Impact:
(For enterprise and organization only)
Evidence:
Attachment
Impacted System Critical:
File1.exe Active
File2.exe Inactive
Hosting Type: Shared
Pages Defaced: Single
Phishing Email Content: National Education Foundation CyberLearning, a non-profit organization dedicated to bridging the Digital Divide since 1994, is offering "No Excuse" tuition-free on-line training in Information Technology to the first 10,000 applicants. NEF CyberLearning courses, sponsored by the U.S. DEPARTMENT OF COMMERCE in the Federal Learning Exchange, have recently been acclaimed as "the Best of the Web" in online IT training by the FORBES magazine. ...
Observations/incident details: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
No of systems impacted: 1
OS: Linux
BACK
SUBMIT

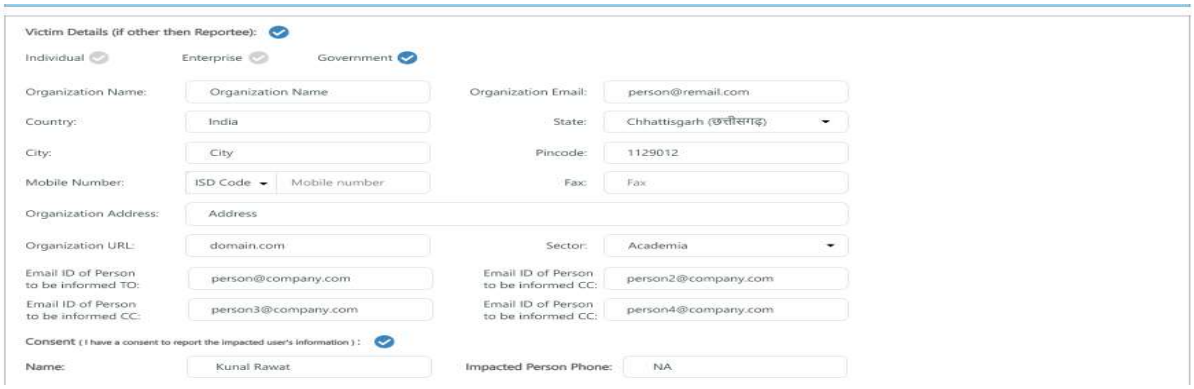

Hosting Type:
Shared
Pages Defaced:
Single
Phishing Email Content:
National Education Foundation CyberLearning, a non-profit organization dedicated to bridging the Digital Divide since 1994, is offering "No Excuse" tuition-free on-line training in Information Technology to the first 10,000 applicants. NEF CyberLearning courses, sponsored by the U.S. DEPARTMENT OF COMMERCE in the Federal Learning Exchange, have recently been acclaimed as "the Best of the Web" in online IT training by the FORBES magazine. ...
Observations/incident details:
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
No of systems impacted:
1
OS:
Linux
Tools Result
AbuseIPDB
EXPORT REPORT
Buildwith
EXPORT REPORT
Google Web Risk
EXPORT REPORT
Security Trails
EXPORT REPORT
URL Scan.io
EXPORT REPORT

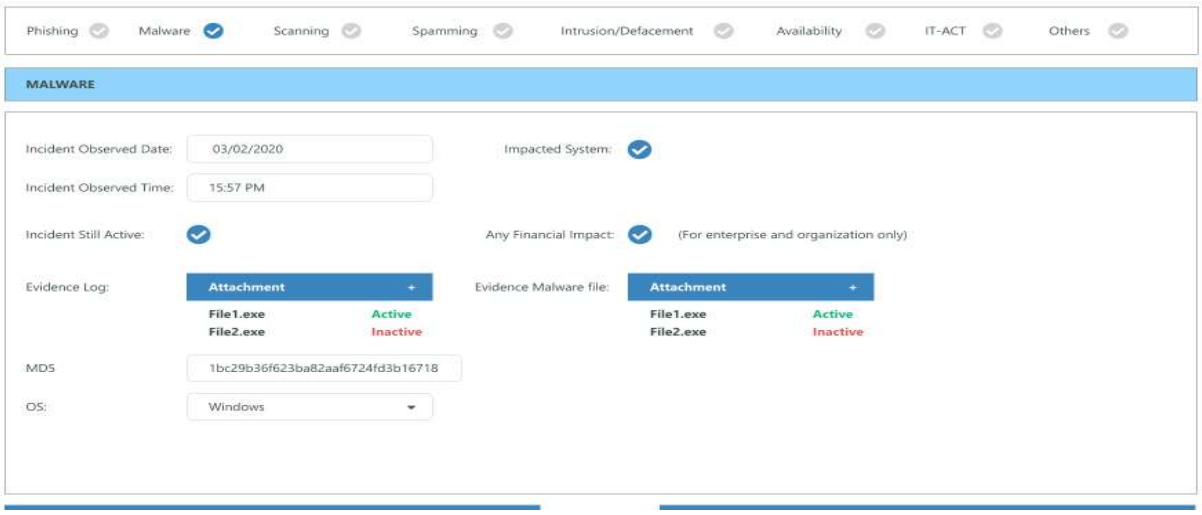

Logo
Create
Dashboard
Search
Playbooks
Documents
Logged in as Organization Admin
Settings
Logout
INCIDENT DETAILS REPORT
LIST INCIDENTS
EXPORT REPORT
ID Number:
Source:
Email
ALLOTMENT HISTORY
1. Incident handler Biswaheeth allotted incident to Incident Analyst Kunal Rawat.
2. Service Desk Analyst Ajit Kumar allotted incident to Incident Handler Biswajeeth.
First
2
3
4
Last
ALLOTMENT HISTORY
COMMENTS
Contact Information For The
Org. ID:
Org. Name:
Org. Address:
112 T, JYP Blvd, Dispur, Assam, India
Org. Sector:
Defence
Org. Country:
India
Org. State:
Assam
Org. City:
Dispur
Org. Pin:
781005
Mobile Number:
91
9443876087
Other Email ID:
anmil@eco.focus
Other Email ID CC:
vijay@eco.focus
Other Email ID CC:
himesh@eco.focus
Other Email ID CC:
greg@eco.focus

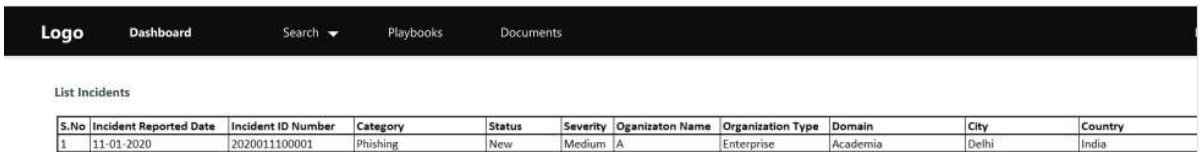




The solution captures critical incident details like - data of the person reporting the incident, affected entity details, systems affected, evidence details etc. The evidence for an incident can be shared via email. Once received the Help Desk associate can upload the same for investigation.

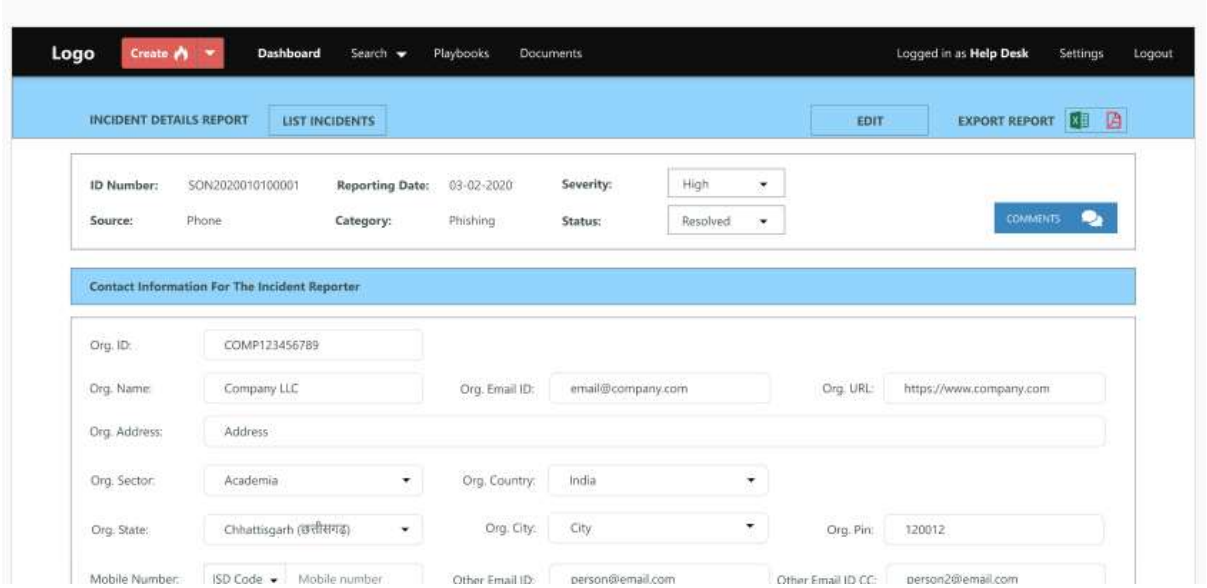






The Help desk associate once satisfied allots the Incident to an Incident Lead. On allotment it would appear as a new lead on their dashboard.

The solution maintains a chain of custody of the incident. A comment section in provided which captures the comments made by the users who were handing the incident prior to it being allotted to them. The User can also download the incident report as a CSV, HTML, DOC/DOCX, or a PDF File.


Logo
Create
Dashboard
Search
Playbooks
Documents
Logged in as Help Desk
Settings
Logout
INCIDENT DETAILS REPORT
LIST INCIDENTS
EDIT
EXPORT REPORT
ID Number:
SON2020010100001
Reporting Date:
03-02-2020
Severity:
High
Source:
Phone
Category:
Phishing
Status:
Resolved
COMMENTS
Contact Information For The Incident Reporter
Org. ID:
COMP123456789
Org. Name:
Company LLC
Org. Email ID:
email@company.com
Org. URL:
https://www.company.com
Org. Address:
Address
Org. Sector:
Academia
Org. Country:
India
Org. State:
Chhattisgarh (छत्तीसगढ़)
Org. City:
City
Org. Pin:
120012
Mobile Number:
ISD Code
Mobile number
Other Email ID:
person@email.com
Other Email ID CC:
person2@email.com