

R-CITS

(Realtime Cybersecurity Incident Tracking)



R-CITS

The cyber threat landscape has changed exponentially & cyber-attacks are getting more and more sophisticated. It is no longer the individual traditional hacker, but now it's more organized, syndicated and even state sponsored. Trends indicate the discovery of large-scale vulnerabilities, data breaches, Spams, ATM Jackpotting, coordinated financial frauds, & many more sophisticated critical cyber-attacks.

R-CITS, gives each incident reported a digital persona. It enforces automation at every stage to ensure quick response time to incident and providing the user insights.

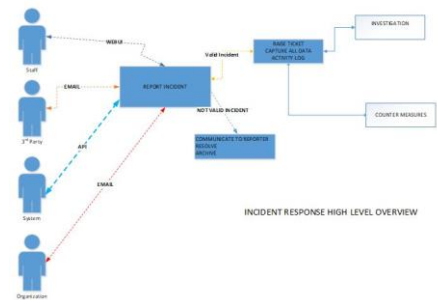
R-CITS, is automated and fits into your DevSecOps as it supports data ingestion from multiple sources.

R-CITS, helps your Incident Management team to respond & mitigate incidents quickly by providing them meaningful data.

R-CITS Key Features

- A centralised Incident reporting, tracking and management system
- Automated for sharing incident report
- Allow 3rd parties to report cyber incidents
- Provide capability to allow multiple automated and semi-automated methods of incident reporting
- Automated incident correlation
- Real-time information sharing and alerting mechanism in existing system.
- Provide advisories & Actionable intelligence
- Capability to conduct automated and manual root cause analysis
- Integrated with vulnerability management & incident detection

... & More



Roles

The solution has 6 roles defined (Super Admin, Group Admin, Service Desk, Incident Handler, Incident Analyst and Executive). Each role would be accessing the system using a user name (linked to their email ID). The Role Based Access Control (RBAC) mechanism to define the segregation of duties. The solution caters to creating a single organization only.

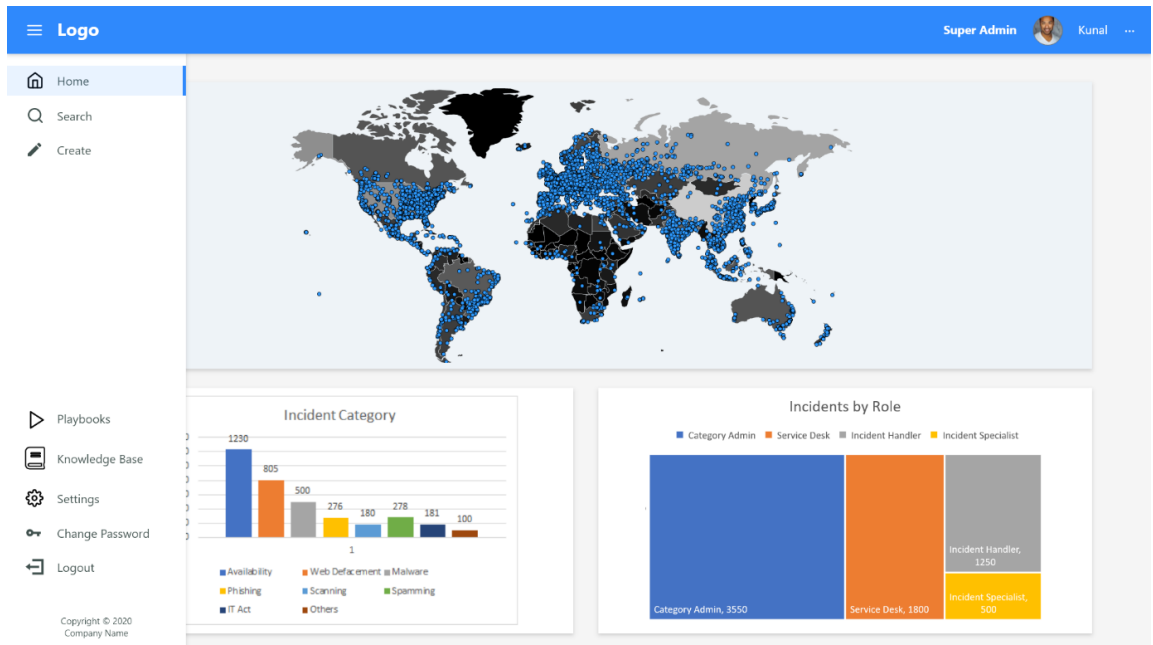
Organization Settings

The organization settings which need to be configured before starting the solution are LDAP (if required else it would use local authentication), SMTP (for email) & API keys for 3rd

R-CITS

(Realtime Cybersecurity Incident Tracking)

Features and Benefits



The 'Authentication Settings' page shows configuration for an LDAP directory. The 'Local Database' option is selected with a checkmark. The 'Active Directory' directory is configured with the following details:

- Directory: Active Directory
- Name: ldap
- URL: ldap://ldapserver.com
- Base DN: dc=company,dc=com
- User: cn=admin,dc=company,dc=com
- Password: password
- Connection timeout: 1 minute

The 'THIRD PARTY API CONFIGURATION' page displays a list of API integrations. Each entry includes the API name, a 'Test API Key' button, and an 'Active' status indicator.

API Name	Test API Key	Status
WebhookCloud	Test API Key	Active
API Key	Test API Key	Active
Google Ads Reporting	Test API Key	Active
API Key	Test API Key	Active
View Total	Test API Key	Active
API Key	Test API Key	Active
Security Tools	Test API Key	Active
API Key	Test API Key	Active
Threatminer	Test API Key	Active
API Key	Test API Key	Active
Abuse IP DB	Test API Key	Active
API Key	Test API Key	Active
Hostedness	Test API Key	Active
API Key	Test API Key	Active
Scyllion	Test API Key	Active
API Key	Test API Key	Active
URL Scan	Test API Key	Active
API Key	Test API Key	Active
Builtwith	Test API Key	Active
API Key	Test API Key	Active
Carbon Black	Test API Key	Active
API Key	Test API Key	Active
Shodan	Test API Key	Active
API Key	Test API Key	Active
VMTools	Test API Key	Active
API Key	Test API Key	Active
Zoom IT	Test API Key	Active
API Key	Test API Key	Active

R-CITS

Users

The SuperAdmin, would be responsible for creating and managing the users created. Dashboard & Landing page. The Group Admin can manage the users as required.

Dashboards

The Landing page and Dashboards would be based on the role and the access to specific resources.

Playbook & Documents

Pre-fed playbooks and allows user create their own playbook. Upload your documents like SOP, Knowledge Info etc.

Incident Reporting & Management

Our solution supports multiple methods for reporting an incident and has AI/ML to autoallocate an Incident. It follows the MITRE and SANS framework for Incident detection & management. With multiple tools integration it provides instant updates of the incident.