Global Next Consulting India Private Limited

GNCIPL

(Leader In Consulting)

GSTIN:09AALCG8170B1ZI

CIN: U62099UP2025PTC217716

📝 Software Project Details for Client Documentation

Section	Details
Project Title	**CyberSecOps Dashboard**-Global Cyber Defense Arc-GCDA – Single tool for Multiple Protection.
Client Name	Confidential
Project Manager	Ravi Kant (Technical Head)
Development Team	GNCIPL Internal Team
Start Date	16 July 2025
Expected Delivery	05 Aug 2025
Technology Stack	MERN Stack (MongoDB, Express, React, Node.js), Docker, Nginx
Hosting	DigitalOcean Cloud Server
Authentication	JWT, Role-based Access Control (RBAC), Okta OAuth
Frontend Features	Responsive UI, Dashboard Analytics, Role-based Access, Live Charts

Section	Details
Backend Features	REST APIs, MongoDB Integration, Scheduled Jobs, API Gateways
Security Tools Integrated	ServiceNow GRC, Splunk, QRadar, CrowdStrike, SentinelOne, Qualys, Tenable, Okta, OneTrust
Modules Implemented	1. User Management2. GRC Workflow3. SIEM Alert Viewer4. EDR Monitoring5. Vulnerability Dashboard6. DSAR & Privacy Handling7. Audit Logs8. KPI Analytics
Data Storage	MongoDB (Hosted via Docker container)
CI/CD	Docker Compose (Local), GitHub Actions (Optional)
SSL Enabled	Yes (via Let’s Encrypt & Nginx)
Maintenance Plan	Weekly backups, Monthly updates, Monitoring via UptimeRobot
Documentation	Admin Guide, User Manual, API Docs, Deployment Guide
Testing & QA	Manual Testing, API Testing (Postman), Unit Testing (Jest for backend, React Testing Library)
Support Period	[e.g., 3 Months Post-Deployment]
Contact for Support	Support@gncipl.com

Global Cyber Defense Arc (GCDA) – Single tool for Multiple Protection

🎯 1. Project Objective

To build a secure, modular, and scalable dashboard that enables cybersecurity analysts and GRC professionals to visualize and manage:

- Risk, policy, audit workflows (ServiceNow GRC)
- Security event monitoring (Splunk, QRadar)
- Endpoint detection & response (CrowdStrike, SentinelOne)

- Vulnerability findings (Qualys, Tenable, Rapid7)
- Identity & access management (Okta, CyberArk)
- Data privacy & DSAR handling (OneTrust, BigID)

🔍 2. Project Scope

✅ In-Scope

- MERN Stack App (React, Node, Express, MongoDB)
- User management with RBAC
- Integration with security APIs (ServiceNow, Splunk, etc.)
- Audit logging, email/Slack notifications
- Dockerized deployment on DigitalOcean
- Dashboard analytics

❌ Out-of-Scope

- Real-time SIEM log ingestion from local agents
- Custom development of native ServiceNow/Splunk plugins
- Full-featured mobile app (only responsive UI)

📦 3. Deliverables

Deliverable	Description	Due Date
Project Charter	Scope, goals, roles	Week 1
Wireframes & UI Designs	Approved Figma mockups	Week 2
Working Frontend	React UI with auth	Week 3
Working Backend	Node APIs + MongoDB models	Week 4
GRC Module	Risk, policy, audit flows	Week 5
SIEM & EDR Integration	Alert viewer, agent health	Week 7
Vulnerability Dashboard	CVE parser, scanner integration	Week 8
Privacy Module	DSAR form, consent tracker	Week 9
Docker Setup	Client, server, Mongo in Compose	Week 11

Deliverable	Description	Due Date
Live Deployment	Deployed to DigitalOcean	Week 13
Testing & UAT	Manual, API, security tests	Week 14
Final Handover	Docs, credentials, training	Week 16

🛠️ 4. Technology Stack

Component	Technology
Frontend	React, Redux, Axios, Chart.js
Backend	Node.js, Express, Mongoose
Database	MongoDB
Authentication	JWT, RBAC, Okta OAuth
API Integration	REST APIs (Splunk, ServiceNow, etc.)
Deployment	Docker, Nginx, DigitalOcean
CI/CD	GitHub Actions (optional)
Logging	Mongo AuditLog, Email, Slack

👥 5. Team & Roles

Role	Responsibility
Project Manager	Planning, coordination, client liaison
Frontend Developer	React UI implementation
Backend Developer	API, database, logic integration
DevOps Engineer	Docker setup, DigitalOcean deployment
QA Engineer	Testing, bug logging, UAT
Security Lead	OAuth, API hardening, role management
Documentation Lead	User manuals, handover package

📅 6. Timeline (High-Level Phases)

Phase	Weeks
Requirement Gathering	Week 1
UI/UX & Design Approval	Week 2
Development (Frontend/Backend)	Week 3–10
Integrations & Testing	Week 6–13
Deployment & QA	Week 13–15
Final Review & Handover	Week 16

⚠️ 7. Risks & Mitigation

Risk	Mitigation
API rate limits / failures	Use retries, log failures
Integration auth changes (e.g., Okta)	Store tokens securely, handle refresh logic
Delayed design/UI feedback	Weekly design demos
UAT bugs in final stages	Buffer 2 weeks for QA/fixes
Security vulnerability in backend	Code review + OWASP testing

---

📚 8. Documentation Plan

- 📖 Admin Guide (Managing modules, roles, configs)
- 🧑‍💼 User Manual (How to use dashboards, filters)
- ⚙️ API Docs (Postman collection + Swagger)
- 🧱 Deployment Guide (For rehosting)
- 📝 Testing Checklist & Bug Tracker

📎 Optional Add-ons

Feature	Description

Feature	Description
✅ MFA	Add TOTP-based MFA with Google Authenticator
✅ CI/CD	GitHub Actions → Docker Hub → Server
✅ Cloud Monitoring	Use UptimeRobot or Grafana
✅ Audit Compliance Export	CSV/PDF export of risk/audit logs

Detailed Module Description:

Module	Description	Frontend (React)	Backend (Node + Express + MongoDB)	Tool Integrations / APIs
User Authentication	Secure login/signup with role-based access control	React + Redux + JWT Auth Forms	Passport.js / JWT / bcrypt / RBAC middleware	Okta / CyberArk API for IAM/PAM
GRC Management	Risk, policy, compliance, and audit workflows	Risk register, policy viewer, audit checklist	REST API for CRUD on risks, policies, audits	ServiceNow GRC API
SIEM Integration	Real-time alerts and logs dashboard	Charts & logs from Splunk/QRadar	API calls and alert normalization	Splunk / IBM QRadar API
EDR/XDR Status	Endpoint threat detection and response status	Threat graphs, agent health views	Backend polling agents, webhooks	CrowdStrike / SentinelOne API
Vulnerability	Scan reports	Scan result	Import & parse	Qualys /

Module	Description	Frontend (React)	Backend (Node + Express + MongoDB)	Tool Integrations / APIs
Scanning	and vulnerability metrics	viewer, risk categorization	reports from scanners	Tenable / Rapid7 API
Privacy Governance	Data mapping, subject access request (DSAR) handling	DSAR form, data maps	Workflow engine, DSAR tracking backend	OneTrust / BigID API
Audit Logs & Notifications	Action tracking, notification alerts	Audit log table, alert modals	MongoDB audit log collection	Custom or external notification API
Dashboard & Analytics	KPI charts, threat heatmaps	D3.js / Chart.js dashboards	Aggregation pipelines	Combined analytics from tools

🔐 Features Implemented:

- Role-based access control (Admin, Analyst, Auditor)
- Token-based session management (JWT)
- OAuth SSO via Okta
- Log ingestion from Splunk/QRadar
- EDR insights via SentinelOne or CrowdStrike API
- GRC workflow CRUD via ServiceNow API
- CVE feed parsing from Tenable/Qualys
- Privacy management with OneTrust

🛡️ 1. User Authentication Module

🎯 Goal:

- Secure login/signup
- Role-based access (Admin, Analyst, Auditor)
- SSO via Okta

🧩 Frontend:

- React + Redux
- Pages: Login, Signup, Forgot Password, Profile
- Form validation with Formik or React Hook Form
- Role-based route protection using PrivateRoute

🔧 Backend:

- Express + MongoDB
- Passport.js for local strategy + JWT
- Roles stored in MongoDB
- API: /auth/signup, /auth/login, /auth/verifyToken, /auth/profile

🔐 Integration:

- Okta OAuth 2.0 / OpenID Connect
- Use Okta SDK to support enterprise SSO login

📜 2. GRC Management Module

🎯 Goal:

- Manage risks, policies, audits
- Workflow for compliance

🧩 Frontend:

- Risk Register Table
- Policy Document Viewer
- Audit Plan Form (create/assign/complete)

🔧 Backend:

- Models: Risk, Policy, Audit
- Routes: /grc/risks, /grc/policies, /grc/audits

- Add timeline/history logs on updates

🔐 Integration:

- ServiceNow REST API (Table API)
- Push/pull GRC data via secure API tokens

📊 3. SIEM Integration Module

🎯 Goal:

- Show real-time security alerts/logs
- Normalize logs from Splunk/QRadar

🧩 Frontend:

- Alerts Table with filters
- Real-time WebSocket feed
- Charts: top sources, affected assets

🔧 Backend:

- Normalize log structure: { timestamp, severity, message, source }
- Use WebSockets for live alerts
- Schedule CRONs to poll logs every X mins

🔐 Integration:

- Splunk Search API
- IBM QRadar Offense API

🧿 4. EDR/XDR Status Module

🎯 Goal:

- View agent status
- Map threats to endpoints

🧩 Frontend:

- Endpoint list with health status
- Threat detail modal
- Geo-location map using Leaflet.js

🔧 Backend:

- Models: Device, Threat
- Routes: /edr/devices, /edr/threats
- Webhooks for real-time threat updates

🔐 Integration:

- SentinelOne / CrowdStrike APIs
- Requires API token, query endpoints regularly

🛡️ 5. Vulnerability Scanning Module

🎯 Goal:

- Upload + view scan results
- Map to CVE database

🧩 Frontend:

- File Upload (CSV/JSON)
- Vulnerability Table by severity
- CVE Detail Page

🔧 Backend:

- Parse file, extract vulnerabilities
- Enrich using NIST CVE DB / Qualys API
- Routes: /vuln/upload, /vuln/list, /vuln/:id

🔐 Integration:

- Qualys / Tenable API
- CVE Feed from https://cve.circl.lu/

🔏 6. Privacy Governance Module

🎯 Goal:

- Handle DSARs, consent, data map

🧩 Frontend:

- DSAR Form
- Consent Management
- Data Mapping (PII, Sensitive)

🔧 Backend:

- Models: DSAR, Consent, DataAsset
- Routes: /privacy/dsar, /privacy/consent

🔐 Integration:

- OneTrust API to sync DSARs
- BigID for auto-tagged PII

🧠 7. Audit Logs & Notifications

🎯 Goal:

- Log user actions + alert security events

🧩 Frontend:

- Admin panel for logs
- Notifications (toaster, popup)

🔧 Backend:

- MongoDB schema for AuditLog
- Middleware to auto-log actions

🔐 Integration:

- Email (NodeMailer) or Slack alerts
- Custom webhook for external SIEM input

📈 8. Dashboard & Analytics Module

🎯 Goal:

- Unified dashboard with KPIs

🧩 Frontend:

- D3.js / Chart.js visualizations
- Filters by date/user/module

🔧 Backend:

- Aggregation pipelines for metrics
- Caching with Redis for performance

🔐 Integration:

- Data from all modules
- External API aggregation (e.g., threat count from EDR, CVE stats)

📦 Tech Stack Recap

Layer	Tech
Frontend	React, Redux, Axios, D3.js, Chart.js, Socket.IO
Backend	Node.js, Express, MongoDB, Mongoose, JWT, Passport.js
Auth/Security	JWT, Okta, RBAC, OAuth2, Helmet, CORS
API Integration	Okta, ServiceNow, Splunk, QRadar, CrowdStrike, SentinelOne, Qualys, Tenable, OneTrust, BigID
DevOps	Docker, GitHub Actions, Nginx reverse proxy, PM2

Here's a detailed **Project Milestone Table** for the **CyberSecOps Dashboard** MERN full-stack project. This structure is ideal for **client documentation**, project planning, or reporting.

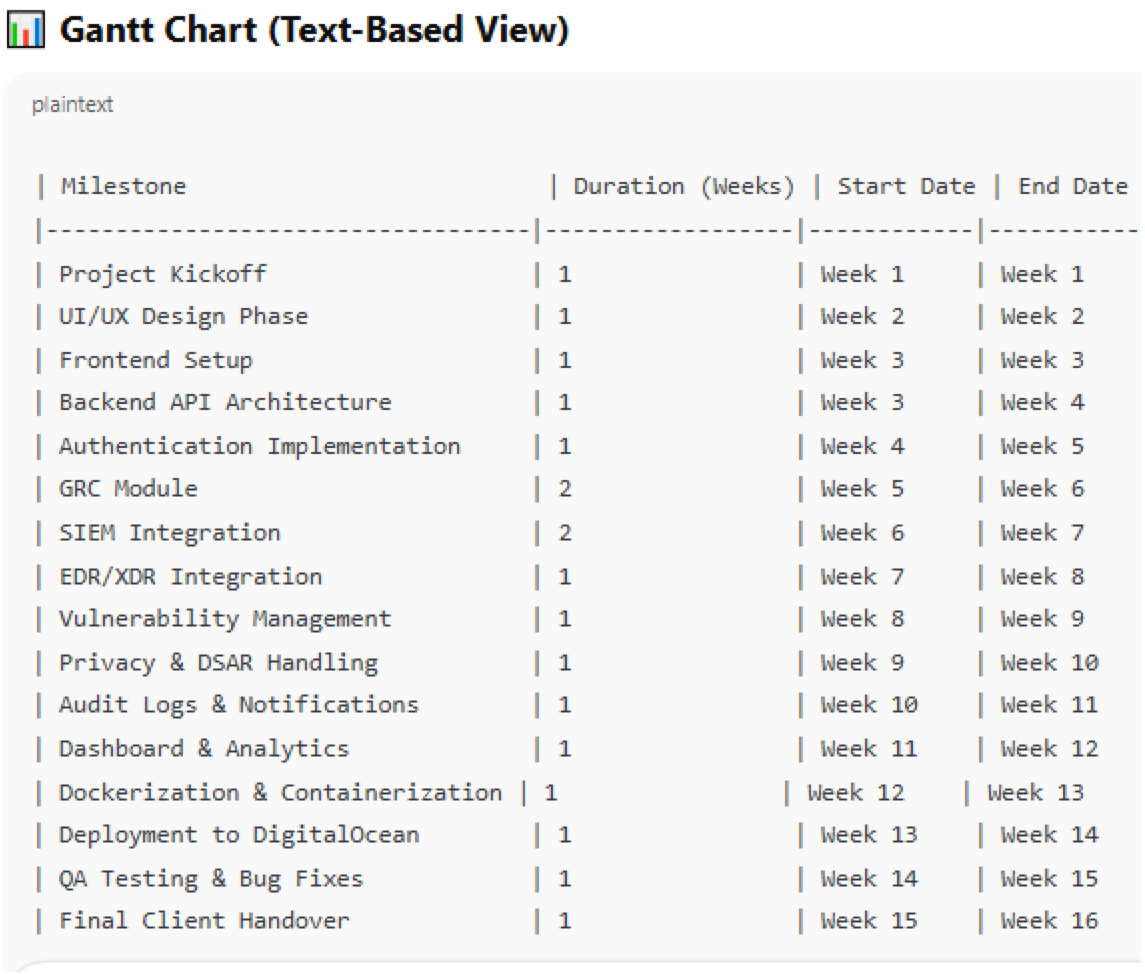
📅 **CyberSecOps Dashboard – Project Milestones**

Milestone #	**Milestone Title**	**Description**	**Deliverables**
1	Project Kickoff	Initial meeting with stakeholders to finalize scope and requirements	Project charter, requirement doc, tech stack finalization
2	UI/UX Design Phase	Wireframes, mockups, and design system development	Figma mockups, design approval from client
3	Frontend Setup	React app setup with routing, layout, and initial components	Basic React project with header/sidebar layout

Milestone #	Milestone Title	Description	Deliverables
4	Backend API Architecture	Node.js + Express setup, MongoDB connection, base API structure	Working backend with folder structure and DB connection
5	Authentication Implementation	Login, registration, JWT tokens, role-based access (RBAC), Okta SSO	Auth APIs + UI integration
6	GRC Module	Risk, policy, and audit workflow features	CRUD for risks/policies/audits, linked user roles
7	SIEM Integration	Integration with Splunk/QRadar for alerts and logs	Live alert dashboard, normalized alert API
8	EDR/XDR Integration	Integration with CrowdStrike / SentinelOne APIs for endpoint monitoring	Endpoint health status, threat viewer
9	Vulnerability Management	Uploading scans, parsing CVEs, integration with Qualys/Tenable	Vuln dashboard, CVE detail pages
10	Privacy & DSAR Handling	DSAR form, consent logs, OneTrust integration	DSAR submission flow, status tracking
11	Audit Logs & Notifications	Tracking user actions, sending notifications via email/web	Mongo audit logs, email/slack alerts
12	Dashboard &	KPI dashboard for risks,	Chart.js/D3.js

Milestone #	Milestone Title	Description	Deliverables
	Analytics	alerts, audits, vulnerabilities	visualizations
13	Dockerization & Containerization	Dockerfiles for frontend/backend, MongoDB service, Docker Compose	Working local Docker setup
14	Deployment to DigitalOcean	Setup server, SSL, firewall, environment variables	Live application on cloud with HTTPS
15	QA Testing & Bug Fixes	Manual + API testing, UAT, performance checks	Bug report, fixed builds
16	Final Client Handover	Final walkthrough, credentials, documentation, training session	Project report, user/admin guide, support handoff

***Detailed Timeline (may vary based on client requirement).**



📊 Gantt Chart (Text-Based View)

plaintext

```
| Milestone                         | Duration (Weeks) | Start Date | End Date
|-----------------------------------|------------------|------------|-----------
| Project Kickoff                   | 1                | Week 1     | Week 1
| UI/UX Design Phase                | 1                | Week 2     | Week 2
| Frontend Setup                    | 1                | Week 3     | Week 3
| Backend API Architecture          | 1                | Week 3     | Week 4
| Authentication Implementation     | 1                | Week 4     | Week 5
| GRC Module                        | 2                | Week 5     | Week 6
| SIEM Integration                  | 2                | Week 6     | Week 7
| EDR/XDR Integration               | 1                | Week 7     | Week 8
| Vulnerability Management          | 1                | Week 8     | Week 9
| Privacy & DSAR Handling           | 1                | Week 9     | Week 10
| Audit Logs & Notifications        | 1                | Week 10    | Week 11
| Dashboard & Analytics             | 1                | Week 11    | Week 12
| Dockerization & Containerization | 1                | Week 12    | Week 13
| Deployment to DigitalOcean        | 1                | Week 13    | Week 14
| QA Testing & Bug Fixes            | 1                | Week 14    | Week 15
| Final Client Handover             | 1                | Week 15    | Week 16
```

File Organization structure

🗂 File Organization (in project repo or drive):

```
/docs/
├── 01_project_charter.pdf
├── 02_requirements_spec.docx
├── 03_ui_ux_design_guide.pdf
├── 04_architecture_diagram.png
├── 05_erd.pdf
├── 06_api_documentation.yaml
├── 07_admin_guide.pdf
├── 08_user_manual.pdf
├── 09_deployment_guide.md
├── 10_ci_cd.md
├── 11_security_checklist.xlsx
├── 12_test_report.pdf
├── 13_training_notes.pdf
├── 14_release_notes.md
├── 15_backup_disaster_plan.pdf
```

Global Next Consulting (India) Pvt. Ltd.
GNCIPL