Product Requirements Document (PRD)
CyberGraph Intelligence Platform (CGIP)

Multi-Tenant Cybersecurity Consulting Platform

Version: 2.0 (Revised for Consulting Services)
Date: October 26, 2025
Classification: Internal - Development
Prepared By: Product Management & Engineering
Status: Approved for Development

Executive Summary

The **CyberGraph Intelligence Platform (CGIP)** is a multi-tenant, enterprise-grade cybersecurity knowledge graph system designed specifically for cybersecurity consulting firms specializing in **Industrial Control Systems (ICS)**, **IEC 62443 compliance**, **ISO 57000 rail security**, **autonomous penetration testing**, and **comprehensive risk assessment services**.

Platform Focus

CGIP enables a small team of specialized consultants to deliver world-class security assessment, penetration testing, threat modeling, and compliance services across multiple client organizations with complete data segregation and shared threat intelligence capabilities.

Key Differentiators

- **Multi-Tenant Architecture**: Complete data isolation per client with shared threat intelligence baseline
- **IEC 62443 Native**: Built-in support for industrial control system security assessment and compliance
- **ISO 57000 Rail Standards**: Specialized support for rail system security and handover documentation
- **Agent Zero Integration**: Autonomous AI-powered penetration testing with knowledge graph access
- **Unified Cybersecurity Ontology**: Based on UCO with ICS/OT extensions
- **Automated Document Generation**: IEC 62443, ISO 57000, and industry-standard report templates
- **CMMS/RAMS Integration**: Link to asset management, maintenance, and reliability data
- **SOC-as-a-Service**: Third-party enrichment service for client Security Operations Centers

Business Model

CGIP serves as the central intelligence and workflow platform for consulting engagements, enabling:

- Rapid client onboarding with infrastructure discovery
- Automated risk assessment and gap analysis
- AI-assisted penetration testing at scale
- Standards-based compliance reporting (IEC 62443, ISO 57000)
- Continuous monitoring and threat intelligence as a service
- Multi-client portfolio management with executive dashboards

1. Product Overview

1.1 Product Vision

To empower cybersecurity consultants with AI-augmented knowledge graph technology that transforms complex multi-client industrial security assessments into efficient, repeatable, and defensible advisory services.

1.2 Product Scope

In Scope:

Multi-Tenancy & Client Management

- Per-client data segregation with row-level security
- Shared threat intelligence knowledge base (CVE, MITRE, standards)
- Client-specific dashboards and reporting
- Consultant role-based access across clients
- Project and engagement tracking

Industrial Control System Support

- IEC 62443 security level assessment and gap analysis
- Zone and conduit modeling and design
- SCADA, PLC, HMI, DCS device modeling
- OT network topology visualization
- Safety system (SIS) integration
- Industrial protocol analysis (Modbus, DNP3, OPC UA)

Standards and Compliance

- IEC 62443 parts 1-4 requirements database
- ISO 57000 series rail security standards

- MITRE ATT&CK for ICS
- Unified Cybersecurity Ontology (UCO) integration
- NIST Cybersecurity Framework mapping
- Automated compliance evidence collection

Knowledge Graph Construction

- Automated CVE/CWE/CAPEC/MITRE ATT&CK ingestion
- Client asset database integration
- ICS topology diagram parsing (PDF, Visio, images)
- OneKE-powered document extraction
- Entity resolution across heterogeneous sources
- Semantic alignment and concept normalization

Autonomous Penetration Testing (Agent Zero)

- KG query API for infrastructure reconnaissance
- Attack path discovery and ranking
- Exploit selection from CAPEC/CVE database
- Simulation engine for attack validation
- Learning feedback loop for path optimization
- Automated pentest report generation
- Tool recommendation engine

Threat Modeling and Risk Assessment

- STRIDE threat modeling framework
- MITRE ATT&CK technique mapping
- Attack scenario simulation
- Multi-factor risk scoring (CVSS, exploitability, asset criticality)
- Risk propagation through dependencies
- Attack surface analysis

Document Generation

- IEC 62443 gap analysis reports
- IEC 62443 control matrices
- Security level assessment documents
- Zone/conduit design documentation
- Penetration test reports
- Threat model documents
- ISO 57000 security reports

- ISO 57000 handover documentation
- Vulnerability assessment reports
- Executive summary dashboards

Integration Capabilities

- Client asset management database connectors
- CMMS (Computerized Maintenance Management System) integration
- RAMS (Reliability, Availability, Maintainability, Safety) data import
- SOC alert enrichment API (bi-directional)
- SIEM integration (Splunk, QRadar, Sentinel)
- STIX 2.1 export for threat intelligence sharing

Out of Scope (Future Phases):

- Active vulnerability scanning (use existing tools, import results)
- Automated patch deployment
- 24/7 SOC operations (enrichment only)
- Mobile application
- Public cloud marketplace offering (on-premises first)

1.3 Target Market

Primary Market: Small to medium-sized cybersecurity consulting firms (5-50 consultants) specializing in:

- Industrial control system security
- IEC 62443 compliance assessment
- Rail system security (ISO 57000)
- Operational technology (OT) security
- Penetration testing for critical infrastructure
- Threat modeling for ICS/SCADA environments

Client Industries:

- Manufacturing (discrete and process)
- Energy and utilities (power generation, transmission, distribution)
- Oil and gas (upstream, midstream, downstream)
- Rail transportation
- Water and wastewater treatment
- Chemical and pharmaceutical
- Food and beverage production

2. User Personas

2.1 Security Consultant (Sarah)

Role: Senior security consultant conducting client assessments
Experience: 8+ years in industrial security, IEC 62443 certified
Goals:

- Efficiently assess multiple client environments
- Document findings with evidence-based reports
- Deliver actionable remediation roadmaps
- Maintain consistent quality across engagements

Pain Points:

- Manual correlation of vulnerabilities to infrastructure
- Time-consuming report generation
- Inconsistent documentation across projects
- Difficulty visualizing complex ICS architectures

CGIP Usage:

- Import client infrastructure from diagrams and asset databases
- Run automated IEC 62443 gap analysis
- Generate compliance reports with one click
- Access shared threat intelligence for context

Success Metrics:

- 50% reduction in assessment time
- 90% report generation automation
- Zero documentation inconsistencies

2.2 IEC 62443 Assessor (Victor)

Role: IEC 62443 compliance specialist
Experience: 10+ years in industrial automation, ISA/IEC certified
Goals:

- Map client controls to IEC 62443 requirements
- Identify security level gaps by zone
- Generate audit-ready compliance documentation
- Track remediation progress over time

Pain Points:

- Manual control-to-requirement mapping
- Spreadsheet-based gap tracking
- Inconsistent zone definitions
- Difficulty demonstrating progress to auditors

CGIP Usage:

- Model client zones and conduits in knowledge graph
- Auto-map implemented controls to 62443 requirements
- Generate gap analysis reports by security level
- Track control implementation over time

Success Metrics:

- 70% faster gap analysis completion
- 100% audit trail coverage
- Real-time remediation tracking

2.3 Penetration Testing Lead (Marcus)

Role: Lead penetration tester for ICS environments
Experience: 12+ years, GIAC, OSCP, specialized in OT
Goals:

- Plan efficient penetration tests
- Discover realistic attack paths
- Validate exploitability safely
- Deliver comprehensive remediation guidance

Pain Points:

- Limited ICS exploit databases
- Difficult to model complex OT networks
- Time-consuming manual reconnaissance
- Hard to explain technical findings to non-technical clients

CGIP Usage:

- Visualize attack paths from KG
- Access CAPEC/CVE exploit database
- Generate pentest plans from templates
- Auto-document findings with context

Success Metrics:

- 40% faster reconnaissance phase

- 3x more attack paths identified
- 80% client satisfaction with reports

2.4 Autonomous Penetration Tester - Agent Zero (AI)

Role: AI agent performing autonomous security testing
Experience: Reinforcement learning trained on security datasets
Goals:

- Autonomously discover attack paths
- Select optimal exploits
- Validate vulnerabilities
- Learn from success/failure
- Update knowledge graph with findings

Capabilities:

- Query KG for infrastructure topology and vulnerabilities
- Reason about attack path feasibility
- Select tools and exploits dynamically
- Execute simulations in safe sandbox
- Provide feedback for path ranking improvement

CGIP Integration:

- REST API for KG queries (<500ms response)
- KG update API for discovered vulnerabilities
- Attack path ranking algorithm
- Exploit matcher with CAPEC/CVE database
- Simulation orchestration
- Learning feedback loop

Success Metrics:

- 10+ concurrent pentest simulations
- 90% exploit selection accuracy
- Continuous improvement through feedback

2.5 Threat Modeling Specialist (Tara)

Role: Threat modeling expert for ICS environments
Experience: 7+ years, STRIDE/MITRE practitioner
Goals:

- Model threats systematically (STRIDE)

- Map to MITRE ATT&CK techniques
- Simulate attack scenarios
- Prioritize mitigation strategies

Pain Points:

- Manual threat enumeration
- Difficult to track threat coverage
- Hard to keep models current
- Limited ICS-specific threat patterns

CGIP Usage:

- Build threat models in KG
- Auto-apply STRIDE categories
- Link to MITRE ICS techniques
- Simulate scenarios with KAG reasoning
- Generate threat model documents

Success Metrics:

- 60% faster threat modeling
- 100% MITRE technique coverage
- Continuous model updates

2.6 Security Architect (Andrea)

Role: Security architecture design for ICS/OT
Experience: 15+ years in industrial automation and security
Goals:

- Design secure zone/conduit architectures
- Validate designs against IEC 62443
- Model attack surfaces
- Document security controls

Pain Points:

- Complex zone boundary definitions
- Difficult to validate control coverage
- Manual architecture documentation
- Hard to communicate designs to operations teams

CGIP Usage:

- Model OT/IT architectures in KG

- Define zones, conduits, and security levels
- Validate against IEC 62443-3-3
- Auto-generate architecture documentation
- Visualize attack surfaces

Success Metrics:

- 50% faster architecture design
- Zero zone definition errors
- 90% stakeholder comprehension

2.7 Vulnerability Manager (Vijay)

Role: Vulnerability management across multiple clients
Experience: 6+ years in vulnerability management and asset management
Goals:

- Prioritize vulnerabilities by risk
- Track remediation across clients
- Link to asset databases
- Report on vulnerability trends

Pain Points:

- Overwhelming vulnerability volume
- Lack of context for prioritization
- Manual asset-CVE correlation
- Disconnected from asset management systems

CGIP Usage:

- Sync with client asset databases
- Auto-link CPE to CVEs
- Calculate context-aware risk scores
- Track remediation status
- Generate trend reports

Success Metrics:

- 70% improvement in prioritization accuracy
- 50% faster remediation
- Real-time asset-vulnerability mapping

2.8 Crisis Management / Incident Response (Carlos)

Role: Incident response coordinator
Experience: 10+ years in IR, GCIH, GCFA certified
Goals:

- Rapid threat context retrieval
- Access to IR playbooks
- Coordinate response teams
- Document incidents for lessons learned

Pain Points:

- Information overload during incidents
- Manual playbook lookup
- Difficult to track incident timeline
- Post-incident documentation time-consuming

CGIP Usage:

- Query KG for real-time threat context
- Retrieve IR playbooks by incident type
- Track incident timeline automatically
- Generate incident reports

Success Metrics:

- 40% faster MTTC (mean time to contain)
- 100% playbook adherence
- Automated incident documentation

2.9 SOC Integration Analyst (Sofia)

Role: Third-party SOC enrichment service provider
Experience: 5+ years in SOC operations and threat intelligence
Goals:

- Enrich client SOC alerts with context
- Provide threat intelligence
- Suggest response actions
- Demonstrate value of enrichment service

Pain Points:

- Limited context from client alerts
- Manual threat intelligence lookup

- Slow response to client queries
- Difficult to prove ROI

CGIP Usage:

- Receive alerts via API from client SOCs
- Query KG for asset and threat context
- Return enriched data with recommendations
- Track enrichment value metrics

Success Metrics:

- <5 second enrichment response time
- 80% alert context improvement
- Measurable reduction in client MTTD

2.10 Asset & RAMS Manager (Alan)

Role: Asset management and reliability engineering
Experience: 12+ years in asset management, CMMS, RAMS
Goals:

- Link assets to vulnerabilities
- Track critical safety items
- Integrate maintenance data
- Report on reliability metrics

Pain Points:

- Disconnected security and reliability systems
- Manual correlation of CVEs to assets
- Difficult to assess security impact on safety
- Spreadsheet-based critical item lists

CGIP Usage:

- Import asset database and CMMS data
- Auto-link assets to CVEs via CPE
- Track critical items with security context
- Display reliability metrics (MTBF, MTTR)

Success Metrics:

- 100% asset-vulnerability coverage
- Real-time critical item tracking
- Integrated security-reliability view

2.11 Client Project Manager (Patricia)

Role: Managing multiple client engagements
Experience: 8+ years in project management, PMP certified
Goals:

- Oversee all client projects
- Track deliverables and timelines
- Monitor consultant utilization
- Ensure client satisfaction

Pain Points:

- Visibility across multiple clients
- Manual status tracking
- Inconsistent deliverable quality
- Difficult to demonstrate value to clients

CGIP Usage:

- Multi-client executive dashboard
- Engagement tracking and timeline views
- Deliverable status monitoring
- Consultant assignment and utilization

Success Metrics:

- 100% on-time deliverable completion
- 95% client satisfaction score
- 30% improvement in consultant utilization

3. Functional Requirements

3.1 Multi-Tenancy and Client Management (Critical)

FR-001: Multi-Tenant Architecture

- **Description**: System shall implement multi-tenant architecture with complete data segregation between clients
- **Acceptance Criteria**:
  - PostgreSQL row-level security enforced at database layer
  - Neo4j multi-database support (one graph per client + shared graph)
  - Tenant context derived from JWT token
  - Automated tenant provisioning workflow

    - Zero data leakage verified through security audit
    - Cross-tenant query prevention with unit tests
- **Priority**: Critical
- **Phase**: Phase 1

FR-002: Per-Client Dashboards

- **Description**: Each client shall have dedicated dashboard with role-based views
- **Acceptance Criteria**:
    - Client users only see their organization's data
    - Configurable dashboard widgets per client
    - Support for client-specific branding
    - Role-based view permissions (read, write, admin)
    - Real-time data updates via WebSocket
- **Priority**: Critical
- **Phase**: Phase 7

FR-003: Shared Knowledge Base

- **Description**: Common threat intelligence shall be accessible across all clients
- **Acceptance Criteria**:
    - Shared graph database for CVE/CWE/CAPEC/MITRE data
    - Read-only access for all tenants
    - Updates to shared data do not impact tenant performance
    - Versioning for shared data with change tracking
- **Priority**: High
- **Phase**: Phase 5

3.2 Data Ingestion (Critical)

FR-004: Automated Threat Intelligence Ingestion

- **Description**: System shall automatically ingest CVE, CWE, CAPEC, and MITRE ATT&CK data
- **Acceptance Criteria**:
    - Daily synchronization with NVD JSON API
    - MITRE ATT&CK (Enterprise, ICS, Mobile) via STIX 2.1
    - Data lag < 6 hours from publication
    - Validation of data integrity with checksums
    - Error handling and retry logic
    - Monitoring dashboard for ingestion status

- **Priority**: Critical
- **Phase**: Phase 4

FR-005: IEC 62443 Standards Database

- **Description**: System shall integrate IEC 62443 standards (parts 1-4)
- **Acceptance Criteria**:
  - Complete requirements database from 62443-3-2 and 62443-3-3
  - Control descriptions and objectives
  - Security level mappings (SL 1-4)
  - Foundational requirements (FR) and system requirements (SR)
  - Technical control specifications
- **Priority**: Critical
- **Phase**: Phase 4

FR-006: ISO 57000 Rail Standards

- **Description**: System shall integrate ISO 57000 series rail security standards
- **Acceptance Criteria**:
  - ISO 57000 series requirements database
  - Mapping to rail system components
  - Compliance criteria definitions
  - Handover documentation templates
- **Priority**: High
- **Phase**: Phase 4

FR-007: Client Asset Database Integration

- **Description**: System shall import and sync client asset databases
- **Acceptance Criteria**:
  - REST/GraphQL API connectors for common CMDB systems
  - CSV/Excel import for manual data
  - Configurable sync schedule (real-time, daily, weekly)
  - Asset attribute mapping interface
  - Incremental updates with change detection
- **Priority**: Critical
- **Phase**: Phase 4

FR-008: ICS Topology Extraction

- **Description**: System shall extract ICS topology from diagrams and documents
- **Acceptance Criteria**:

    - PDF network diagram parsing with OneKE
    - Image recognition for Visio, draw.io, PNG, JPG
    - Device type classification (PLC, HMI, SCADA, DCS, RTU, IED)
    - Connection/relationship extraction
    - Manual correction interface for validation
    - Confidence scoring for extracted entities
- **Priority**: High
- **Phase**: Phase 4

3.3 Knowledge Graph Construction (Critical)

FR-009: UCO Integration

- **Description**: System shall integrate Unified Cybersecurity Ontology (UCO)
- **Acceptance Criteria**:
    - UCO 2.1 classes and properties in SPG-Schema
    - Mapping to OpenSPG entity types
    - Support for UCO observable objects, actions, and relationships
    - Compatibility with STIX 2.1 for threat intelligence
- **Priority**: Critical
- **Phase**: Phase 3

FR-010: Custom ICS Ontology

- **Description**: System shall implement custom ICS ontology extending UCO
- **Acceptance Criteria**:
    - IEC 62443 concepts (zones, conduits, security levels)
    - ICS device types (PLC, SCADA, HMI, DCS, SIS, RTU, IED)
    - Industrial protocols (Modbus, DNP3, OPC UA, PROFINET)
    - Zone/conduit relationships and boundaries
    - Security level attributes per zone
- **Priority**: Critical
- **Phase**: Phase 3

FR-011: Entity Resolution

- **Description**: System shall resolve entities across multiple sources
- **Acceptance Criteria**:
    - Fuzzy matching for entity names with configurable threshold
    - Confidence scoring for merge candidates

    - Manual review workflow for low-confidence matches
    - Provenance tracking for merged entities
    - Duplicate detection with similarity metrics
- **Priority**: High
- **Phase**: Phase 5

FR-012: Semantic Alignment

- **Description**: System shall align concepts and terminology across sources
- **Acceptance Criteria**:
    - Concept normalization using SPG-Schema
    - Synonym mapping and resolution
    - Reduction of duplicate concept nodes
    - Preservation of source terminology in metadata
- **Priority**: High
- **Phase**: Phase 5

3.4 IEC 62443 Compliance (Critical)

FR-013: Control Mapping

- **Description**: System shall map client controls to IEC 62443 requirements
- **Acceptance Criteria**:
    - Control-to-requirement relationship modeling
    - Coverage analysis by foundational requirement (FR)
    - Gap identification for unmapped requirements
    - Evidence attachment for implemented controls
    - Audit trail for control changes
- **Priority**: Critical
- **Phase**: Phase 5

FR-014: Security Level Gap Analysis

- **Description**: System shall analyze gaps against target security levels
- **Acceptance Criteria**:
    - Gap analysis by zone and security level (SL 1-4)
    - Missing control identification
    - Remediation effort estimation
    - Gap trend tracking over time
    - Export gap analysis reports

- **Priority**: Critical
- **Phase**: Phase 6

FR-015: Zone and Conduit Modeling

- **Description**: System shall model IEC 62443 zones and conduits
- **Acceptance Criteria**:
  - Visual zone/conduit editor in UI
  - Zone attribute assignment (SL, criticality, purpose)
  - Conduit modeling with security requirements
  - Boundary validation and conflict detection
  - Export to Visio/PDF
- **Priority**: High
- **Phase**: Phase 5

3.5 Penetration Testing (Critical)

FR-016: Attack Path Discovery

- **Description**: System shall discover attack paths through infrastructure
- **Acceptance Criteria**:
  - Shortest path algorithm from source to target assets
  - Multi-hop attack chain enumeration
  - Weighting by exploitability and exposure
  - Filtering by attacker profile (insider, external, advanced)
  - Visualization of attack graphs
- **Priority**: Critical
- **Phase**: Phase 6

FR-017: Exploit Database

- **Description**: System shall maintain exploit database with CAPEC pattern matching
- **Acceptance Criteria**:
  - CAPEC attack pattern database
  - Exploit-to-CVE linking
  - Exploit-to-technique (MITRE ATT&CK) mapping
  - Exploitability scoring
  - Tool availability indicators
  - Exploit search and filtering
- **Priority**: Critical

- **Phase**: Phase 6

FR-018: Penetration Test Plan Generation

- **Description**: System shall generate pentest plans from templates
- **Acceptance Criteria**:
  - Template-based plan generation (ICS-specific)
  - Scope definition with asset selection from KG
  - Timeline estimation based on scope
  - Rule of engagement template
  - Test case generation from attack paths
  - Export to PDF/DOCX
- **Priority**: High
- **Phase**: Phase 7

3.6 Agent Zero Integration (Critical)

FR-019: Agent Zero KG Query API

- **Description**: Agent Zero shall query knowledge graph for infrastructure data
- **Acceptance Criteria**:
  - REST API endpoint: GET /api/v1/agent-zero/query
  - Query by asset, vulnerability, attack path, technique
  - JSON response with graph data and relationships
  - Response time < 500ms for p95
  - Rate limiting to prevent abuse
  - Authentication with API key
- **Priority**: Critical
- **Phase**: Phase 6

FR-020: Agent Zero KG Update API

- **Description**: Agent Zero shall update knowledge graph with findings
- **Acceptance Criteria**:
  - REST API endpoint: POST /api/v1/agent-zero/update
  - Submit discovered vulnerabilities, successful exploits
  - Validation of submitted data against schema
  - Audit trail for AI-generated updates
  - Response time < 200ms for p95
  - Conflict resolution for concurrent updates

- **Priority**: Critical
- **Phase**: Phase 6

FR-021: Attack Path Selection

- **Description**: Agent Zero shall receive optimal attack path recommendations
- **Acceptance Criteria**:
  - REST API endpoint: POST /api/v1/agent-zero/select-path
  - Input: target asset ID, attacker constraints
  - Output: ranked attack paths with success probability
  - Algorithm considers difficulty, stealth, impact
  - Response time < 1 second for complex paths
  - Explainable path ranking
- **Priority**: Critical
- **Phase**: Phase 6

FR-022: Simulation Engine

- **Description**: Agent Zero shall simulate attacks in sandbox environment
- **Acceptance Criteria**:
  - REST API endpoint: POST /api/v1/agent-zero/simulate
  - Execute attack simulations safely
  - Return success/failure with telemetry
  - Timeout protection for long-running simulations
  - Resource isolation per simulation
- **Priority**: High
- **Phase**: Phase 6

FR-023: Learning Feedback Loop

- **Description**: Agent Zero shall submit feedback to improve path selection
- **Acceptance Criteria**:
  - REST API endpoint: POST /api/v1/agent-zero/feedback
  - Submit path ID and outcome (success/failure, time, stealth)
  - Update path ranking model with feedback
  - Response time < 100ms
  - Feedback aggregation and model retraining
- **Priority**: High
- **Phase**: Phase 6

3.7 Threat Modeling (High)

FR-024: STRIDE Framework

- **Description**: System shall support STRIDE threat modeling
- **Acceptance Criteria**:
  - STRIDE categories (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
  - Apply categories to data flows and components
  - Threat enumeration by STRIDE category
  - Integration with MITRE ATT&CK techniques
- **Priority**: High
- **Phase**: Phase 6

FR-025: Threat Scenario Simulation

- **Description**: System shall simulate threat scenarios using MITRE techniques
- **Acceptance Criteria**:
  - Select MITRE ATT&CK techniques for scenario
  - Model attacker capabilities and objectives
  - Simulate technique execution against defenses
  - Identify successful attack chains
  - Generate threat model reports
- **Priority**: High
- **Phase**: Phase 6

3.8 Risk Assessment (Critical)

FR-026: Multi-Factor Risk Scoring

- **Description**: System shall calculate risk scores using multiple factors
- **Acceptance Criteria**:
  - CVSS base score integration
  - Exploitability weighting (public exploit availability)
  - Asset criticality factor (business impact)
  - Exposure factor (internal vs. external, network segmentation)
  - Aggregated risk score formula
  - Configurable weighting per client
- **Priority**: Critical
- **Phase**: Phase 6

FR-027: Risk Propagation

- **Description**: System shall calculate cascading risk through dependencies
- **Acceptance Criteria**:
  - Graph algorithms for dependency traversal
  - Risk score propagation through relationships
  - Blast radius calculation for vulnerabilities
  - Critical path identification
  - Visualization of risk propagation
- **Priority**: Critical
- **Phase**: Phase 6

3.9 Asset Management (Critical)

FR-028: Asset-Vulnerability Linking

- **Description**: System shall link assets to applicable vulnerabilities
- **Acceptance Criteria**:
  - CPE matching for asset-to-CVE linking
  - Fuzzy matching for incomplete CPE data
  - Version-aware vulnerability assignment
  - Bulk linking with validation
  - Real-time updates on new CVEs
- **Priority**: Critical
- **Phase**: Phase 5

3.10 RAMS Integration (High)

FR-029: CMMS Integration

- **Description**: System shall integrate with CMMS for maintenance data
- **Acceptance Criteria**:
  - REST API connector for common CMMS systems
  - Import maintenance schedules, work orders
  - MTBF (Mean Time Between Failures) calculation
  - MTTR (Mean Time To Repair) tracking
  - Link maintenance events to security incidents
- **Priority**: High
- **Phase**: Phase 4

3.11 Document Generation (Critical)

FR-030: IEC 62443 Report Templates

- **Description**: System shall generate IEC 62443 assessment reports
- **Acceptance Criteria**:
  - Templates: Gap Analysis, Control Matrix, Security Level Assessment
  - Auto-populate from KG data
  - Customizable report sections
  - Export to PDF, DOCX
  - Evidence attachment support
  - Version control for templates
- **Priority**: Critical
- **Phase**: Phase 7

FR-031: ISO 57000 Handover Documentation

- **Description**: System shall generate ISO 57000 handover documents
- **Acceptance Criteria**:
  - Templates: Security Report, Handover Documentation, Evidence Package
  - Rail-specific requirement mapping
  - Automated evidence collection from KG
  - Export to PDF, DOCX, ZIP
  - Digital signature support
- **Priority**: Critical
- **Phase**: Phase 7

3.12 SOC Integration (High)

FR-032: Bi-Directional SOC Integration

- **Description**: System shall integrate with client SOCs for alert enrichment
- **Acceptance Criteria**:
  - REST API endpoint for SOC alert ingestion
  - Query KG for asset and threat context
  - Return enriched alert data with recommendations
  - WebHook for proactive threat notifications
  - Support for Splunk, QRadar, Sentinel formats
- **Priority**: High
- **Phase**: Phase 8

3.13 Crisis Management (High)

FR-033: Incident Response Knowledge Base

- **Description**: System shall provide IR playbooks and context
- **Acceptance Criteria**:
  - IR playbook library by incident type
  - Link playbooks to MITRE techniques
  - Query KG for real-time threat context during incidents
  - Incident timeline tracking
  - Lessons learned documentation
- **Priority**: High
- **Phase**: Phase 8

3.14 Reasoning and Analytics (Critical)

FR-034: Multi-Hop Reasoning

- **Description**: System shall answer queries requiring 3+ relationship hops
- **Acceptance Criteria**:
  - KAG-Solver logical form decomposition
  - Support for complex security questions
  - Response time < 5 seconds for standard queries
  - Explainable reasoning with path visualization
  - Natural language query interface
- **Priority**: Critical
- **Phase**: Phase 6

4. Non-Functional Requirements

4.1 Performance

NFR-001: Graph Query Performance

- **Requirement**: Graph queries shall return within 2 seconds for 90th percentile
- **Acceptance Criteria**: Load testing shows p90 < 2s for standard query patterns
- **Priority**: Critical

NFR-002: Knowledge Graph Scale

- **Requirement**: Support minimum 50 million nodes and 200 million relationships
- **Acceptance Criteria**: Stress testing with target scale maintains performance

- **Priority**: High

NFR-003: Natural Language Query Performance

- **Requirement**: Natural language queries shall return within 5 seconds
- **Acceptance Criteria**: Benchmarking with KAG-Solver shows p90 < 5s
- **Priority**: Critical

4.2 Scalability

NFR-004: Concurrent Consultant Support

- **Requirement**: System shall support 50+ concurrent consultants across clients
- **Acceptance Criteria**: Load testing with 50 users maintains <3s response times
- **Priority**: Critical

NFR-005: Parallel Penetration Testing

- **Requirement**: Agent Zero shall handle 10+ parallel pentest simulations
- **Acceptance Criteria**: 10 Agent Zero instances running concurrently without degradation
- **Priority**: High

4.3 Multi-Tenancy

NFR-006: Data Isolation

- **Requirement**: Data isolation enforced at database and application layers
- **Acceptance Criteria**: Security audit confirms zero cross-tenant data leakage
- **Priority**: Critical

NFR-007: Shared Data Updates

- **Requirement**: Shared knowledge base updates must not impact tenant performance
- **Acceptance Criteria**: Updates complete within 1 hour with zero tenant impact
- **Priority**: High

4.4 Availability

NFR-008: System Uptime

- **Requirement**: System uptime of 99.5% during business hours (7 AM - 7 PM)
- **Acceptance Criteria**: Monitoring demonstrates 99.5% uptime over 30 days
- **Priority**: Critical

4.5 Security

NFR-009: Encryption at Rest

- **Requirement**: All client data encrypted at rest using AES-256
- **Acceptance Criteria**: Security scan confirms encryption for all databases
- **Priority**: Critical

NFR-010: Encryption in Transit

- **Requirement**: All API communications encrypted using TLS 1.3
- **Acceptance Criteria**: SSL Labs test achieves A+ rating
- **Priority**: Critical

NFR-011: Multi-Factor Authentication

- **Requirement**: MFA required for all user accounts
- **Acceptance Criteria**: MFA enforced, tested with security audit
- **Priority**: Critical

NFR-012: Tenant Separation

- **Requirement**: Client data must be logically or physically separated
- **Acceptance Criteria**: Architecture review confirms tenant separation
- **Priority**: Critical

4.6 Compliance

NFR-013: Audit Log Retention

- **Requirement**: Audit logs retained for minimum 7 years (regulatory compliance)
- **Acceptance Criteria**: Retention verified, logs searchable for 7+ years
- **Priority**: Critical

NFR-014: IEC 62443 Evidence Trails

- **Requirement**: Automated compliance evidence collection for IEC 62443
- **Acceptance Criteria**: Evidence trails maintained for all assessments
- **Priority**: Critical

4.7 Usability

NFR-015: Consultant Workflow Efficiency

- **Requirement**: UI shall support <3 clicks to access common tasks
- **Acceptance Criteria**: User testing validates 3-click access to top 10 tasks
- **Priority**: Medium

4.8 Maintainability

NFR-016: Code Coverage

- **Requirement**: Backend services shall have minimum 80% test coverage
- **Acceptance Criteria**: SonarQube/Codecov reports show 80%+ coverage
- **Priority**: High

4.9 Reliability

NFR-017: Backup and Recovery

- **Requirement**: Automated backup every 12 hours with 90-day retention
- **Acceptance Criteria**: Backup restoration test successful, RPO < 12 hours
- **Priority**: Critical

4.10 Agent Zero Integration

NFR-018: Agent Zero API Performance

- **Requirement**: Agent Zero API must have <500ms response time for KG queries
- **Acceptance Criteria**: API performance testing shows p95 < 500ms
- **Priority**: Critical

5. Technical Architecture

5.1 Multi-Tenant Architecture

Data Segregation Strategy:

- **Option 1 (Recommended)**: Schema-per-tenant in PostgreSQL + Multi-database in Neo4j
- **Option 2**: Row-level security with tenant_id column
- **Shared Data**: Separate graph database for CVE/MITRE/standards accessible to all tenants

Tenant Context:

- JWT token contains tenant_id claim
- Middleware extracts and validates tenant context
- All database queries automatically scoped to tenant
- Shared data accessed via separate connection

5.2 Knowledge Graph Architecture

Storage Layer:

- Neo4j 5.x Enterprise with multi-database support
- One database per client (tenant isolation)
- Shared database for common threat intelligence
- Graph algorithms via Neo4j GDS

Schema Layer:

- OpenSPG SPG-Schema for domain modeling
- UCO 2.1 base ontology
- Custom ICS extension ontology
- IEC 62443 concept definitions

Construction Layer:

- OpenSPG SPG-Builder for ETL
- OneKE for document extraction
- Custom ICS topology parsers
- Entity resolution pipeline

Reasoning Layer:

- KAG-Solver for logical reasoning
- Custom attack path algorithms
- Risk propagation models
- STRIDE threat modeling engine

5.3 Agent Zero Integration Architecture

Agent Zero ⟷ CGIP Communication:

```
Agent Zero
  ↓ Query Infrastructure
[KG Query API] → OpenSPG/Neo4j
  ↓ Return Graph Data
Agent Zero
  ↓ Select Attack Path
[Attack Path Selector] → KAG-Solver
  ↓ Return Ranked Paths
Agent Zero
  ↓ Get Exploits
[Exploit Matcher] → CAPEC/CVE Database
  ↓ Return Exploits
Agent Zero
  ↓ Simulate Attack
```

```
[Simulation Engine] → Sandbox Environment
  ↓ Return Results
Agent Zero
  ↓ Update KG
[KG Update API] → OpenSPG/Neo4j
  ↓ Submit Feedback
[Learning Feedback] → ML Model
```

5.4 Document Generation Pipeline

Template Engine:

- Jinja2 for document templates
- Docxtpl for DOCX generation
- WeasyPrint for PDF generation
- Custom rendering engine for IEC 62443/ISO 57000 formats

Data Flow:

1. User selects report template
2. Query KG for required data
3. Populate template with data
4. Render to DOCX/PDF
5. Store in document repository
6. Provide download link

5.5 Technology Stack

Frontend:

- Next.js 14+ (App Router)
- shadcn/ui components
- Tailwind CSS
- Zustand for state management
- React Query for server state

Backend:

- FastAPI (Python 3.11+)
- PostgreSQL 16+ (application data, multi-tenant)
- Pydantic for data validation
- SQLAlchemy for ORM
- Alembic for migrations

Knowledge Graph:

- OpenSPG 0.5.x
- Neo4j 5.23+ Enterprise
- OneKE 1.0+
- KAG Framework 0.4+

AI/ML:

- OpenAI API / Azure OpenAI / Local LLM
- Agent Zero (latest)
- Milvus/Qdrant for vector search

Infrastructure:

- Docker Compose (development)
- Kubernetes (production)
- Kafka/RabbitMQ (event streaming)
- Redis (caching)
- Nginx (reverse proxy)
- Prometheus + Grafana (monitoring)
- ELK Stack (logging)

6. Use Cases

6.1 UC-001: IEC 62443 Risk Assessment

Actor: IEC 62443 Assessor
Goal: Assess client infrastructure against IEC 62443, identify gaps, generate compliance reports

Preconditions:

- Client tenant provisioned
- Client assets imported
- IEC 62443 standards loaded

Main Flow:

1. Assessor logs into client tenant
2. Imports client asset database or network diagrams
3. System extracts ICS topology and devices
4. Assessor models zones and conduits
5. Assigns target security levels (SL) per zone
6. System maps implemented controls to 62443 requirements
7. System performs gap analysis against target SL

8. Assessor reviews gap analysis results
9. System generates gap analysis report
10. Assessor delivers report to client

Postconditions:

- Client infrastructure modeled in KG
- Gap analysis documented
- Compliance report generated

Deliverables:

- IEC 62443 Gap Analysis Report
- Control Matrix
- Remediation Roadmap

6.2 UC-002: Autonomous Penetration Testing

Actor: Agent Zero (AI)
Goal: Autonomously discover attack paths, simulate attacks, document findings

Preconditions:

- Client tenant configured
- Infrastructure modeled in KG
- Agent Zero authorized for tenant

Main Flow:

1. Agent Zero queries KG for client infrastructure
2. System returns network topology and asset data
3. Agent Zero identifies potential entry points
4. Agent Zero requests attack path recommendations
5. KAG-Solver returns ranked attack paths
6. Agent Zero selects optimal path
7. Agent Zero queries exploit database for matching exploits
8. System returns applicable exploits with metadata
9. Agent Zero simulates attack in sandbox
10. Simulation engine returns success/failure results
11. Agent Zero updates KG with findings
12. Agent Zero submits learning feedback
13. System generates pentest report

Postconditions:

- Attack paths documented
- Vulnerabilities validated
- KG updated with findings
- Learning model improved

Deliverables:

- Penetration Test Report
- Exploited Vulnerabilities List
- Attack Path Diagrams
- Remediation Recommendations

6.3 UC-003: Threat Modeling for ICS

Actor: Threat Modeling Specialist
Goal: Model threats using STRIDE/MITRE, simulate scenarios, identify high-risk paths

Preconditions:

- Client infrastructure modeled
- MITRE ATT&CK for ICS loaded

Main Flow:

1. Specialist accesses threat modeling interface
2. Selects client infrastructure components
3. Applies STRIDE categories to data flows
4. System suggests MITRE ATT&CK techniques per STRIDE category
5. Specialist selects relevant techniques
6. System simulates attack scenarios using KAG-Solver
7. System identifies successful attack chains
8. Specialist reviews threat model
9. System generates threat model document
10. Specialist delivers to client

Postconditions:

- Threat model documented
- Attack scenarios identified
- Mitigation strategies proposed

Deliverables:

- Threat Model Document
- Attack Tree Diagrams

- Risk Register
- Mitigation Strategies

6.4 UC-004: SOC Alert Enrichment

Actor: SOC Integration Analyst
Goal: Enrich client SOC alerts with KG context, provide threat intelligence

Preconditions:

- SOC integration configured
- Client KG populated

Main Flow:

1. Client SOC sends alert to CGIP API
2. System extracts IoCs and asset identifiers
3. System queries KG for matching entities
4. System identifies related threats, vulnerabilities, assets
5. System calculates potential impact using risk propagation
6. System retrieves response recommendations
7. System returns enriched alert data to SOC
8. SOC analyst reviews enriched data
9. SOC takes action based on recommendations

Postconditions:

- Alert enriched with context
- Response recommendations provided
- Value metrics tracked

Deliverables:

- Enriched Alert Data
- Threat Context
- Response Recommendations

6.5 UC-005: Vulnerability Management

Actor: Vulnerability Manager
Goal: Link assets to CVEs, prioritize by risk, track remediation

Preconditions:

- Client assets in KG
- CVE database synchronized

Main Flow:

1. System syncs with client asset database
2. System matches asset CPE to CVEs
3. System calculates risk scores (CVSS + exploitability + criticality)
4. Manager reviews vulnerability list
5. Manager prioritizes remediation based on risk
6. Manager assigns remediation tasks
7. System tracks remediation status
8. System generates vulnerability reports

Postconditions:

- Vulnerabilities prioritized
- Remediation tracked
- Trends analyzed

Deliverables:

- Vulnerability Prioritization List
- Remediation Tracking Dashboard
- Risk Trend Reports

6.6 UC-006: Crisis Management / Incident Response

Actor: Crisis Management / IR
Goal: Support incident response with threat intel, playbooks, context

Preconditions:

- Client KG available
- IR playbooks loaded

Main Flow:

1. Incident alert triggers IR workflow
2. IR coordinator queries KG for threat context
3. System returns related threats, techniques, affected assets
4. System retrieves relevant IR playbooks
5. IR team executes playbook steps
6. System tracks incident timeline
7. IR team documents actions taken
8. System generates incident report
9. Team conducts lessons learned review

Postconditions:

- Incident contained
- Timeline documented
- Lessons learned captured

Deliverables:

- Incident Timeline
- Root Cause Analysis
- Lessons Learned Report
- Playbook Updates

6.7 UC-007: Security Architecture Design

Actor: Security Architect
Goal: Design secure zone/conduit architecture, validate against IEC 62443

Preconditions:

- Client requirements gathered
- IEC 62443 standards available

Main Flow:

1. Architect models OT/IT architecture in KG
2. Defines zones based on criticality and function
3. Defines conduits between zones
4. Assigns security levels (SL) per zone
5. Maps controls to IEC 62443-3-3 requirements
6. System validates control coverage
7. System identifies missing controls
8. Architect refines design
9. System generates architecture documentation
10. Architect presents to client

Postconditions:

- Architecture documented
- IEC 62443 compliance validated
- Design approved

Deliverables:

- Security Architecture Diagram

- Zone/Conduit Design
- Control Specification
- Design Review Report

6.8 UC-008: ISO 57000 Compliance (Rail)

Actor: IEC 62443 Assessor
Goal: Map rail systems to ISO 57000 requirements, generate handover docs

Preconditions:

- Rail system inventory available
- ISO 57000 standards loaded

Main Flow:

1. Assessor imports rail system components
2. System maps components to ISO 57000 requirements
3. Assessor documents implemented controls
4. System assesses compliance gaps
5. Assessor gathers evidence artifacts
6. System generates security report
7. System generates handover documentation
8. Assessor delivers to owner/operator

Postconditions:

- Compliance assessed
- Handover documentation complete
- Evidence package ready

Deliverables:

- ISO 57000 Security Report
- Handover Documentation
- Evidence Package
- Compliance Matrix

7. Success Metrics

7.1 Consultant Productivity

- **Time per IEC 62443 Assessment**: Reduce from 40 hours to 20 hours (50% improvement)
- **Report Generation Time**: Reduce from 8 hours to 30 minutes (93% improvement)
- **Consultant Utilization**: Increase billable hours by 30%

7.2 Client Satisfaction

- **Net Promoter Score (NPS)**: Target > 60
- **Client Retention Rate**: > 90%
- **Repeat Engagement Rate**: > 75%

7.3 Technical Performance

- **Query Response Time**: p90 < 2 seconds
- **Knowledge Graph Scale**: 50M+ nodes per shared database
- **System Uptime**: 99.5% during business hours
- **Agent Zero API Performance**: p95 < 500ms

7.4 Business Impact

- **New Client Onboarding**: < 2 days from contract to first assessment
- **Assessment Accuracy**: 95% validation rate on findings
- **Remediation Tracking**: 100% visibility into client remediation progress

8. Project Timeline

Phase	Duration	Milestone
Phase 0: Initiation	2 weeks	Team assembled, standards approved
Phase 1: Infrastructure	3 weeks	Docker environment, CI/CD operational
Phase 2: Backend Core	4 weeks	FastAPI + PostgreSQL + Auth complete
Phase 3: KG Schema	4 weeks	UCO + ICS ontology defined
Phase 4: Data Ingestion	5 weeks	CVE/MITRE/IEC/Asset ingestion working
Phase 5: KG Construction	5 weeks	Entity resolution, control mapping active
Phase 6: Reasoning/Agent	4 weeks	KAG-Solver + Agent Zero integration
Phase 7: Frontend	6 weeks	Next.js UI with all features
Phase 8: Integration	4 weeks	SOC/CMMS/RAMS integrations complete
Phase 9: Security/RBAC	3 weeks	Multi-tenant security validated
Phase 10: Testing/QA	4 weeks	All testing complete

Phase	Duration	Milestone
Phase 11: Documentation	2 weeks	User docs + training delivered
Phase 12: Deployment	2 weeks	Production go-live

Total Duration: 48 weeks (~12 months)

9. Risks and Mitigation

9.1 Technical Risks

Risk	Probability	Impact	Mitigation
OpenSPG performance issues at scale	Medium	High	Early load testing, Neo4j fallback
Agent Zero integration complexity	High	Medium	Incremental development, API versioning
Multi-tenant data leakage	Low	Critical	Security audits, penetration testing
ICS topology extraction accuracy	Medium	Medium	Manual review workflow, confidence scoring

9.2 Business Risks

Risk	Probability	Impact	Mitigation
Consultant adoption resistance	Medium	High	Early user involvement, comprehensive training
Client data sensitivity concerns	High	High	Strong security controls, audit trails
Scope creep from consultants	High	Medium	Strict change control, phased approach

Appendices

Appendix A: Ontology References

- **Unified Cybersecurity Ontology (UCO)**: https://github.com/Ebiquity/Unified-Cybersecurity-Ontology
- **MITRE ATT&CK STIX Mapping**: https://documentation.eccenca.com/23.3/build/tutorial-how-to-link-ids-to-osint/lift-data-from-STIX-2.1-data-of-mitre-attack/
- **IEC 62443 Automation Ontology**: Knowledge-based Engineering of Automation Systems using Ontologies (Glawe et al.)

Appendix B: Standards References

- **IEC 62443**: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- **ISO 57000 Series**: Rail applications - Cybersecurity standards
- **NIST Cybersecurity Framework**: https://www.nist.gov/cyberframework

Document Approval

Role	Name	Signature	Date
Product Manager			
Technical Lead			
Principal Consultant			
Security Architect			

This document is confidential and proprietary. Distribution restricted to authorized personnel.