

Subject: Combined functionalities and use cases of the integrated RAG Q/A system and Cyber Dashboard in one application

1. Introduction

The integrated application combines two complementary cybersecurity capabilities in one platform:

- a **Retrieval-Augmented Generation (RAG) Question/Answer system**, designed to let users ask natural-language questions over cybersecurity documents, free text, and STIX intelligence
- a **Cyber Dashboard**, designed to validate, explore, prioritize, score, store, and visualize STIX2.1 threat intelligence data

Together, these two components create a unified cyber threat intelligence workspace. In the same application, users can ingest structured and unstructured threat data, explore it visually, verify its quality, query it conversationally, and extract actionable insights for both operational and management use.

2. Main Objective

The objective of the integrated application is to transform raw cybersecurity information into readable, searchable, explorable, and actionable intelligence. Instead of separating document analysis, intelligence verification, graph exploration, and question-answering into different tools, the application centralizes them into one workflow.

This allows users to:

- ingest PDF advisories, pasted intelligence text, and STIX bundles
- validate and review STIX before approval
- query content in natural language
- visualize entities and relationships
- prioritize incidents and intelligence
- support both analyst workflows and leadership reporting

3. Combined Functional Scope

The application combines the following major capabilities:

- PDF ingestion and question answering
- pasted text ingestion and question answering
- STIX JSON ingestion and question answering
- STIX bundle verification before import
- incident exploration and intelligence analysis
- graph and 3D relationship visualization
- database-backed intelligence storage
- executive overview and threat prioritization

This makes the platform usable both as:

- an **analyst workbench**
- and a **decision-support platform**

4. Main Use Cases

4.1 Document-Based Threat Intelligence Q/A

The RAG Q/A component allows users to upload PDF reports such as advisories, incident reports, or technical analyses, then ask natural-language questions such as:

- How did the attackers gain initial access?
- Which CVEs are mentioned?
- What indicators of compromise are listed?
- Which MITRE ATT&CK techniques are referenced?

This use case helps analysts quickly extract facts from long documents without manually reading the full report.

Business value: Faster intelligence extraction, reduced analyst workload, and easier access to critical information from lengthy cybersecurity documents.

4.2 Pasted Intelligence Text Analysis

Users can paste copied incident summaries, analyst notes, detection findings, or CTI observations directly into the system and query them immediately. This is useful when working with fragmented intelligence that is not yet stored as a document or STIX object.

Example questions:

- What malware is mentioned in the text?
- Which IPs or domains appear as indicators?
- What techniques are associated with the incident?

Business value: Supports quick triage and investigation without requiring formal document preparation.

4.3 STIX-Based Natural Language Question Answering

The integrated application supports STIX JSON ingestion as a searchable source. Instead of only visualizing STIX, users can also ask questions such as:

- What indicator is present in the STIX bundle?
- Which vulnerability is described?
- Which ATT&CK technique is referenced?
- Summarize this STIX bundle in one paragraph.

This bridges the gap between structured threat intelligence and natural-language consumption.

Business value: Makes STIX easier to understand and query for both analysts and non-specialists.

4.4 Executive Overview and Risk Prioritization

The Cyber Dashboard provides an overview page showing the most important incidents and highlighting the top-risk intelligence item. This supports quick identification of:

- the highest-priority threat
- the actor, victim, or attack pattern involved
- the justification for prioritization
- related supporting context such as malware, vulnerability, or campaign linkage

Combined with the RAG assistant, a user can move from a dashboard insight to direct questioning of its supporting evidence.

Business value: Improves decision-making and supports leadership reporting with both dashboard summaries and explainable evidence.

4.5 STIX Bundle Verification Before Import

Before adding intelligence into the persistent platform, users can paste a STIX 2.1 bundle into the verification page. The system:

- validates the bundle structure
- extracts incidents, objects, and relationships
- calculates decision and confidence scores
- highlights warnings for weak or incomplete data
- allows approval before import

After this step, the same intelligence can also be queried through the Q/A system.

Business value: Improves data quality and prevents invalid or low-value intelligence from polluting the repository.

4.6 Raw STIX 3D Visualization

The dashboard includes a 3D STIX visualizer that enables users to:

- paste raw STIX JSON
- upload a STIX file
- open the current verification preview in 3D
- inspect entities and links visually
- filter by STIX object type
- search specific entities
- understand the structure of actors, indicators, malware, campaigns, and vulnerabilities

This complements the Q/A system: the dashboard shows the graph visually, while the Q/A interface explains it conversationally.

Business value: Improves interpretability, stakeholder communication, and visual validation of complex threat intelligence.

4.7 Incident Exploration

The Incident Explorer page supports detailed incident review by allowing users to:

- inspect a single incident record
- review linked STIX objects
- analyze connected relationships
- understand the object distribution inside the incident

The integrated assistant can then answer follow-up questions about the incident using the same evidence base.

Business value: Supports operational incident review while adding conversational analysis on top of structured data.

4.8 Threat Actor Intelligence Analysis

The Attacker Intelligence page supports actor-centric analysis by helping users:

- analyze threat actor characteristics
- review related malware, tools, and techniques
- understand targeting patterns
- support profiling and long-term monitoring

The Q/A system can complement this by explaining actor behavior in natural language using related intelligence sources.

Business value: Supports deeper adversary profiling and improves understanding of attacker behavior across cases.

4.9 Campaign Intelligence Tracking

The Campaign Intelligence page helps users study campaigns and their links to incidents, threat actors, and malware. It supports:

- grouping related malicious activity
- identifying recurring patterns
- understanding campaign targets and scope
- assisting attribution and campaign monitoring

The integrated application can then be used to ask questions over those campaigns in a more accessible way.

Business value: Improves visibility into coordinated malicious activity and helps move beyond isolated incident analysis.

4.10 Relationship Intelligence Analysis

The Relationship Intelligence page focuses on the links between STIX entities. It can be used to:

- review relationships such as uses, targets, indicates, and attributed-to
- evaluate graph completeness and relationship density

- identify weak or missing intelligence linkage
- support graph-based intelligence analysis

This is especially powerful when combined with RAG Q/A, because users can both visualize the relationships and ask explanatory questions about them.

Business value: Strengthens intelligence quality analysis and improves the usability of relationship-rich STIX data.

4.11 Database-Backed Intelligence Management

The dashboard uses PostgreSQL for persistent storage of incidents, STIX objects, and relationships. This supports:

- repeated querying and dashboard reuse
- live refresh after import
- long-term growth of an internal intelligence repository

The RAG Q/A component can be extended to query against that same stored intelligence base instead of only temporary session memory.

Business value: Creates a reusable cyber intelligence platform rather than a one-time analysis interface.

4.12 Analyst Knowledge Assistance

The integrated platform supports both structured exploration and guided explanation. Junior analysts, interns, or non-experts can use it to:

- summarize attack chains
- explain evidence behind exploitation claims
- identify the most important indicators
- understand how STIX entities connect
- move from graph exploration to direct question-answering

Business value: Improves onboarding, learning, and productivity within a startup security team.

4.13 Management and Client-Facing Reporting

The application can support supervisors, startup leadership, or external stakeholders by:

- highlighting top-priority incidents
- summarizing attack narratives
- presenting supporting evidence
- visualizing connected intelligence
- making technical CTI easier to present and understand

Business value: Strengthens communication between technical teams and non-technical decision-makers.

5. Target Users

The integrated application is suitable for:

- Cyber threat intelligence analysts
- SOC analysts
- Security engineers
- Incident response teams
- Startup security teams
- Product or security managers
- Leadership stakeholders who need high-level threat summaries
- Junior analysts or interns who need guided analysis

6. Business Value of the Integrated Application

The combination of RAG Q/A and the Cyber Dashboard creates significantly more value than either component alone because it joins:

- **natural-language access to intelligence**
- with **structured visualization and validation**

This gives the startup a platform that can:

- improve readability of raw intelligence
- reduce manual effort in document review and STIX validation
- accelerate incident understanding and prioritization
- centralize verification, querying, analysis, and visualization
- support both operational and executive use cases
- provide a foundation for a future internal or client-facing cyber intelligence product

7. Key Performance Indicators (KPIs)

7.1 Intelligence Quality KPIs

- Number of valid STIX bundles submitted
- Number of invalid bundles rejected
- Number of bundles accepted with warnings
- Average decision score per imported bundle
- Average confidence score per imported bundle
- Number of missing fields detected in submitted intelligence
- Percentage of bundles containing useful supporting context such as malware, indicators, vulnerabilities, and campaigns

7.2 Threat Visibility KPIs

- Total number of incidents stored
- Total number of STIX objects stored
- Total number of relationships stored
- Number of distinct threat actors tracked
- Number of active campaigns identified
- Number of incidents linked to vulnerabilities
- Number of incidents linked to malware or tooling
- Relationship density per incident or per bundle

7.3 Operational Monitoring KPIs

- Top-risk incident currently identified by the platform
- Number of high-priority incidents above a selected score threshold
- Number of incidents affecting critical sectors
- Number of incidents with complete relationship mapping
- Frequency of new intelligence imports over time
- Time between STIX submission and analyst approval/import

7.4 Q/A and Retrieval KPIs

- Number of questions asked per source type
- Average answer latency
- Retrieval precision and recall
- Percentage of answers with cited evidence
- Number of successful answers over indexed documents or STIX sources
- Number of unanswered or insufficient-evidence queries

7.5 Visualization and Workflow KPIs

- Number of bundles reviewed in 3D before import
- Number of searches/filter actions in the visualizer
- Most frequently explored STIX object types
- Number of incidents reviewed through the dashboard
- Number of imported bundles that result in new top-risk incidents

8. Current Limitations

- The current Q/A prototype works best with the currently indexed evidence base.

- Multi-source memory and source-aware retrieval can still be improved.
- Retrieval precision and answer consistency need further optimization.
- STIX relationship reasoning can be expanded for more advanced graph-aware analysis.
- Integration between persistent dashboard storage and conversational retrieval can be strengthened in future versions.

9. Recommended Next Steps

- Connect the Q/A system to the persistent database used by the dashboard
- Improve source-aware multi-document and multi-STIX retrieval
- Strengthen evaluation metrics for answer precision and retrieval performance
- Extend STIX relationship support for deeper graph reasoning
- Add exportable summaries or analyst-ready reports
- Continue refining UI/UX for operational and presentation scenarios

10. Conclusion

The integrated RAG Q/A and Cyber Dashboard application represents a complete cybersecurity intelligence workspace. It combines document understanding, free-text analysis, STIX validation, database-backed intelligence management, relationship exploration, and natural-language question answering in a single platform.