User Stories V4

1. Use Case 1: Real-Time Collaboration: Secure Chat

US1: As an **admin**, I want to be able to create a chat room for every case and add the assigned members to that case.

US2: As a **DFIR team member**, I want to chat in real-time with other analysts or team members assigned to the same case, so that we can collaboratively investigate and resolve incidents efficiently without leaking information.

US3: As an **External Collaborator**, I want secure communication channels so that I can provide expertise and receive case updates without compromising confidentiality.

Acceptance Criteria:

For an admin

- An admin must be able to create a chat room.
- An admin must be able to delete a chat room.
- An admin must be able to update a chat room (*??)
- An admin must be able to add DFIR team members to their respective chat rooms.
- An admin must be able to remove DFIR team members to their respective chat rooms.
- An admin should be able to view all chat rooms.
- An admin must be able to view all users added to a chat room.

For a DFIR team member

- A DFIR team member must be added to a case-specific chat room only if they are assigned to the case.

For an External collaborator

- External Collaborators must be able to join a case via a link shared by an administrator.
- An external collaborator must have access to a chat for a limited amount of time based on a token that expires after a set period of time.

For all chat members

- All messages sent by chat members must be end-to-end encrypted.
- All chat participants must be able to send and receive real-time updates and notifications.
- Plain text messages and evidence attachments must be supported.
- Chat members should be able to read all the messages in the chat.
- Chat members must be able to delete their own messages

2. Use Case 2: Real-Time Collaboration: Discussion Threads

US1: As a **DFIR Team Member**, I want to create and discuss detailed annotation threads on specific evidence files so that I can document my analysis, track insights or discrepancies, and collaborate effectively with other assignees on complex findings.

US2:**As a Lead DFIR Investigator**, I want to review and manage annotation threads so that I can ensure analysis quality and coordinate team efforts.

US3: **As an External Collaborator**, I want to contribute distinctly identifiable annotations so my specialised input is visible while maintaining evidence integrity.

Acceptance Criteria:

<u>For a DFIR Team member and any member with access to a case</u>

- A DFIR team member must be able to create annotation threads on specific evidence files.
- A DFIR team member must be able to reply to, edit, and delete their own annotations.
- A DFIR team member must be able to tag collaborators in the annotation threads.
- DFIR team members must be able to view all annotations related to their assigned cases.
- A DFIR team member can approve (or react to) all annotations.

<u>For a Lead DFIR Investigator</u>

- A lead DFIR Investigator can additionally delete annotations created by other DFIR team members.
- Can approve or reject annotations for final review.
- A lead DFIR Investigator should be able to add a case collaborator to participate in the thread.
- A lead investigator should be able to update a thread priority.

<u>For an External Collaborator</u>

- Annotations that are made by external collaborators must be marked with their role, “External Collaborator” for easy identification.

3. Use Case 3: Automated Logging

US1: As a **compliance officer**, I want all critical actions to be logged and immutable so that I can verify the integrity of the investigation and enforce chain-of-custody

US2: As a **DFIR Administrator**, I want to be able to access and view comprehensive automated logging of all system activities so that I can monitor team progress and ensure proper evidence handling procedures.

US3:As a **DFIR Team Member**, I want my analysis activities to be automatically logged so that I can focus on investigation work without manual documentation overhead.

Acceptance Criteria:

For a Compliance Officer

- All sensitive actions (e.g., logins, uploads, deletions, approvals) must be automatically logged.
- Each log entry must include a timestamp, action, actor (user ID) and IP address.
- Each log entry must be tamper-proof and cannot be altered post-creation.
- All logs must be retained and stored for legal and compliance auditing.

For an administrator

- All user actions must be automatically logged and must include a timestamp, action, actor (user ID) and IP address.
- An admin must be able to view logs and filter them depending on the user, case, date or the type of action performed.
- An admin must be able to download or export logs for reporting and auditing purposes.

For a DFIR team member

- All actions performed by a DFIR team member such as viewing evidence, interactions in the annotations must be logged automatically.
- Every team member must be able to view their own action history or logs.

4. Use Case 4: Graphical Evidence Mapping

US1: As a **DFIR Team Member**, I want to visually map relationships between evidence items, so that I can easily identify connections, dependencies, or patterns in the investigation.

US2: As a **Lead DFIR Investigator**, I want to organize nodes and links in an evidence map, so that I can present the investigative findings in a structured visual format.

US3: As an **External Collaborator**, I want to view the evidence map and highlight connections I contribute to, without altering the base structure.

Acceptance Criteria:

For a DFIR Team Member**:**

- Must be able to create nodes representing evidence items.
- Must be able to link evidence items visually.
- Must be able to comment or annotate connections between evidence items.
- Must be able to view the entire evidence map.

For a Lead DFIR Investigator:

- Must be able to edit or remove nodes and links.
- Must be able to highlight key evidence connections for reports or presentations.
- Must be able to export the evidence map for external review.

For an External Collaborator:

- Can view the evidence map in read-only mode unless explicitly granted temporary edit access.
- Annotations made by external collaborators must be marked as such.

5. Use Case 5: Case Timeline Management

US1: As a **DFIR Team Member**, I want to enter investigative events in a chronological timeline and link related evidence to each event, so that I can track the sequence of incidents and their relationships.

US2: As a **Lead DFIR Investigator**, I want to review, update, and reorganize events in the timeline, so that the investigation chronology is accurate and clear.

Acceptance Criteria:

For a DFIR Team Member:

- Must be able to add events to the timeline with date/time and description.
- Must be able to link evidence items to specific events.
- Must be able to view all events and their associated evidence.

For a Lead DFIR Investigator:

- Must be able to edit, remove, or reorder events.

- Must be able to approve events and their evidence links for final review.

- Must be able to filter or search timeline events by date, type, or involved evidence.

6. **Use Case 6: Case Report Generation**

   US1: As a DFIR Team Member, I want to generate structured reports for a case including evidence, annotations, timelines, and visual maps, so that I can share findings in a professional and organized format.

   US2: As a Lead DFIR Investigator, I want to customize the report content, layout, and format, so that it meets organizational or legal standards.

   Acceptance Criteria:

   For a DFIR Team Member:

   - Must be able to generate a case report including all evidence, annotations, linked timeline events, and graphical maps.
   - Must be able to preview the report before exporting.

   For a Lead DFIR Investigator:

   - Must be able to include or exclude specific sections or evidence.
   - Must be able to export the report in multiple formats (PDF, DOCX).
   - Must be able to add an executive summary or custom notes to the report.

TABLE SUMMARY OF CONTENTS

Use Case	User Story	Role	Acceptance Criteria
1. Real-Time Collaboration: Secure Chat	**US1: Create a case-specific chat room**	**Admin**	**- Must be able to create a chat room.- Must be able to delete a chat room.- Must be able to update a chat room.- Must be able to add or remove DFIR team members.- Must be able to view all chat rooms and their members.**
	US2: Chat in real-time with case members	**DFIR Team Member**	**- Must be added to a chat room only if assigned to the case.- Must be able to send and receive real-time messages.- Plain text and attachments must be supported.- Must be able to**

			read all messages.- Must be able to delete own messages.
	US3: Secure communication as external collaborator	External Collaborator	- Must join via link shared by admin.- Access limited by token expiration.- Must send and receive encrypted messages.- Messages and contributions must be visible to others.
2. Real-Time Collaboration: Discussion Threads	US1: Create and discuss annotation threads	DFIR Team Member	- Can create threads on specific evidence files.- Can reply, edit, delete own annotations.- Can tag collaborators.- Can view all annotations related to assigned cases.- Can approve/react to annotations.
	US2: Review and manage annotation threads	Lead DFIR Investigator	- Can delete annotations by others.- Can approve/reject annotations.- Can add collaborators to threads.- Can update thread priority.
	US3: Contribute identifiable annotations	External Collaborator	- Annotations must be marked “External Collaborator”.
3. Automated Logging	US1: Log all critical actions	Compliance Officer	- Automatically log sensitive actions (login, upload, delete, approve).- Include timestamp, action, actor, IP.- Tamper-proof logs.- Retain logs for auditing.
	US2: Access and view logs	DFIR Administrator	- Log all user actions with timestamp, actor, IP.- Can filter logs by user, case, date, or action type.- Can download/export logs for reporting/auditing.

	US3: Automatic logging of own actions	DFIR Team Member	- Actions (viewing evidence, annotation interactions) logged automatically.- Can view own action history/logs.
4. Graphical Evidence Mapping	US1: Visual mapping of evidence	DFIR Team Member	- Can create nodes for evidence items.- Can link evidence visually.- Can comment/annotate connections.- Can view entire map.
	US2: Organize nodes and links	Lead DFIR Investigator	- Can edit/remove nodes and links.- Can highlight key connections.- Can export evidence map for external review.
	US3: View and highlight contributions	External Collaborator	- Read-only view unless temporary edit access granted.- Annotations must be marked as external contributions.
5. Case Timeline Management	US1: Enter events and link evidence	DFIR Team Member	- Can add events with date/time and description.- Can link evidence to events.- Can view all events and associated evidence.
	US2: Review and manage timeline	Lead DFIR Investigator	- Can edit, remove, reorder events.- Can approve events and evidence links.- Can filter/search by date, type, or evidence.
6. Case Report Generation	US1: Generate structured reports	DFIR Team Member	- Can generate reports including evidence, annotations, timeline, graphical maps.- Can preview reports before exporting.

US2: Customize and export reports	**Lead DFIR Investigator**	**- Can include/exclude specific sections or evidence.- Can export in multiple formats (PDF, DOCX).- Can add executive summary or custom notes.**
US3: suggest AI generated information regarding the case	**DFIR team member**	**-Can press a button that suggests text well suited for case.**