

Cybersecurity Incident Tracking Database

A PostgreSQL-Based Design and Implementation Project

CSET 3300- Database Driven Websites

Jatin Sharma R01549954

1. Introduction

Cyber security attacks continue to be one of the most significant threats to modern organizations. Detecting, recording, and responding to these attacks requires not only technical skills but also proper data management.

Organizations often track cyber incidents across various teams, assets, and response workflows. Without a structured system, information can be scattered, incomplete, or inaccurate.

To address this need, this project implements a cyber-attack recording database built using PostgreSQL 18 and pgAdmin 4. The purpose of this system is to store cyber-attack events, track associated assets, record indicators of compromise (IOC's), and log responses taken by analysts.

The project demonstrates complete database design including:

- Entity-relationship modeling
- SQL DDL for database creation
- SQL DML for inserting dataset
- CRUD operations
- JOIN and aggregate report queries

This project demonstrates proficiency in designing and querying relational databases.

2. Problem Statement and Motivation

Security operation centers (SOC teams) require reliable systems to monitor and track security incidents. Without a dedicated database, organizations face the following challenges:

1. Inconsistent tracking of cyber-attack details.
2. Difficulty analyzing attack trends.
3. Harder to evaluate analyst response performance
4. No central repository of IOCs point
5. Scattered data across different tools.

A structured relational database system solves these issues by enabling accurate logging, response tracking, and well-defined reporting capabilities.

This project models a simplified SOC incident tracking system suitable for instructional and operational use.

3. System Requirements

Functional Requirements

- Classify attacks by vectors.
- Associate one or many assets affected by an attack
- Log responses taken by analysts
- Record cyber-attacks with the title, description, severity, status and action time
- Store indicators of compromise (IP, domain, hash, etc.)

Technical Requirements

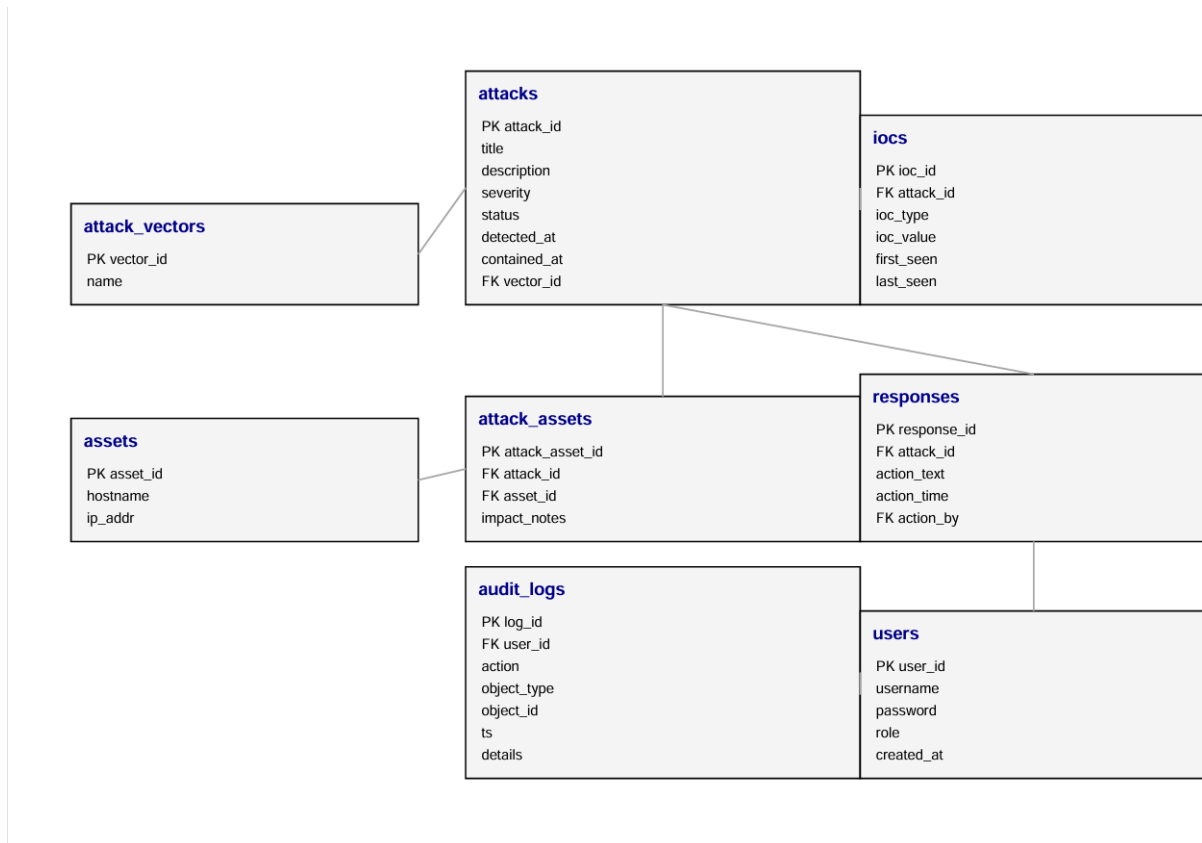
- PostgreSQL 18
- PgAdmin 4 for queries and visual interaction
- SQL DDL and DML

4. Entity Descriptions

1. Users represent administrators and SOC analysts accessing the system.
2. Assets: These represent servers or systems targeted by the attackers.
3. Attack vectors: These represents categories of attack that include phishing, ransomware, DDoS, etc.

4. Attacks: These are the core entity recording each cyber-attack.
5. Attack_assets: These are many-to-many associations between attack and assets.
6. IOCs (Indicators of compromise) are technical indicators such as malicious IPs, domains, and file hashes.
7. Responses are the actions taken by analysts.
8. Audit logs tracks user's activities.

5. ER Diagram



6. Database Schema (DDL)

Below are the SQL statements used to create all tables in the attack_db database

6.1 Users

CREATE TABLE users

```
( user_id SERIAL PRIMARY KEY,  
  username VARCHAR(50) NOT NULL,  
  password VARCHAR(100) NOT NULL,  
  role VARCHAR(20) NOT NULL,  
  created_at TIMESTAMP NOT NULL DEFAULT NOW()  
);
```

6.2 Assets

```
CREATE TABLE assets  
( asset_id SERIAL PRIMARY KEY,  
  hostname VARCHAR(100) NOT NULL,  
  ip_addr VARCHAR(45) NOT NULL  
);
```

6.3 Attack Vectors

```
CREATE TABLE attack_vectors  
( vector_id SERIAL PRIMARY KEY,  
  name VARCHAR(50) NOT NULL  
);
```

6.4 Attacks

```
CREATE TABLE attacks  
( attack_id SERIAL PRIMARY KEY,
```

```
Title    VARCHAR(200) NOT NULL,  
description  VARCHAR(1000) NOT NULL,  
severity    INTEGER NOT NULL,  
status      VARCHAR(20) NOT NULL,  
detected_at  TIMESTAMP NOT NULL,  
contained_at  TIMESTAMP,  
vector_id    INTEGER NOT NULL,  
created_by   INTEGER NOT NULL,  
CONSTRAINT fk_attacks_vector  
FOREIGN KEY (vector_id)  
REFERENCES attack_vectors(vector_id),  
CONSTRAINT fk_attacks_user  
FOREIGN KEY (created_by)  
REFERENCES users(user_id)  
);
```

6.5 Attack_assets

```
CREATE TABLE attack_assets  
  
( attack_asset_id SERIAL PRIMARY KEY,  
  
attack_id INTEGER NOT NULL,  
  
asset_id INTEGER NOT NULL,  
  
impact_notes VARCHAR(500),  
  
CONSTRAINT fk_attack_assets_attack
```

```
FOREIGN KEY (attack_id)
REFERENCES attacks(attack_id),
CONSTRAINT fk_attack_assets_asset
FOREIGN KEY (asset_id)
REFERENCES assets(asset_id)
);
```

6.6 IOCs (Indicators of Compromise)

```
CREATE TABLE iocs
( ioc_id SERIAL PRIMARY KEY,
  attack_id INTEGER NOT NULL,
  ioc_type VARCHAR(20) NOT NULL,
  ioc_value VARCHAR(255) NOT NULL,
  first_seen TIMESTAMP NOT NULL,
  last_seen TIMESTAMP,
  CONSTRAINT fk_iocs_attack
FOREIGN KEY (attack_id)
REFERENCES attacks(attack_id)
);
```

6.7 Responses

```
CREATE TABLE responses (
```

```
response_id SERIAL PRIMARY KEY,  
attack_id INTEGER NOT NULL,  
action_text VARCHAR(1000) NOT NULL,  
action_time TIMESTAMP NOT NULL,  
action_by INTEGER NOT NULL,  
CONSTRAINT fk_responses_attack  
FOREIGN KEY (attack_id)  
REFERENCES attacks(attack_id),  
CONSTRAINT fk_responses_user  
FOREIGN KEY (action_by)  
REFERENCES users(user_id)  
);
```

6.8 Audit Logs

```
CREATE TABLE audit_logs (  
log_id SERIAL PRIMARY KEY,  
user_id INTEGER NOT NULL,  
action VARCHAR(50) NOT NULL,  
object_type VARCHAR(50) NOT NULL,  
object_id INTEGER,  
ts TIMESTAMP NOT NULL DEFAULT NOW(),  
details VARCHAR(500),  
CONSTRAINT fk_audit_logs_user
```

FOREIGN KEY (user_id)

REFERENCES users(user_id)

);

7. Sample Data (DML)

The following commands were used to insert sample records into the database to simulate real-world cyber-attack scenarios

7.1 Insert Users

INSERT INTO users (username, password, role, created_at) VALUES

('admin', 'AdminPass123', 'Admin', NOW()),

('alice', 'Analyst1!', 'Analyst', NOW()),

('bob', 'Analyst2!', 'Analyst', NOW());

Data Output Messages Notifications						
Showing rows: 1 to 3 Page No: 1 of 1						
	user_id [PK] integer	username character varying (50)	password character varying (100)	role character varying (20)	created_at timestamp without time zone	
1	1	admin	AdminPass123	Admin	2025-10-30 14:43:54.919234	
2	2	alice	Analyst1!	Analyst	2025-10-30 14:43:54.919234	
3	3	bob	Analyst2!	Analyst	2025-10-30 14:43:54.919234	

7.2 Insert Assets

INSERT INTO assets (hostname, ip_addr) VALUES

('web-01', '10.0.0.11'),

```
('db-01', '10.0.0.21'),  
('mail-1', '10.0.0.31');
```

Data Output Messages Notifications				
Showing rows: 1 to 3				
	asset_id [PK] integer	hostname character varying (100)	ip_addr character varying (45)	
1	1	web-01	10.0.0.11	
2	2	db-01	10.0.0.21	
3	3	mail-1	10.0.0.31	

7.3 Insert Attack Vectors

```
INSERT INTO attack_vectors (name) VALUES  
('Phishing'),  
('Malware'),  
('Ransomware'),  
('DDoS'),  
('Privilege Escalation');
```

Data Output

Messages

Notifications

	<div>vector_id</div> <div>[PK] integer </div>	<div>name</div> <div>character varying (50) </div>
1	1	Phishing
2	2	Malware
3	3	Ransomware
4	4	DDoS
5	5	Privilege Escalation

7.4 Insert Attacks

INSERT INTO attacks

(title, description, severity, status, detected_at, contained_at, vector_id, created_by)
VALUES

('Credential harvest via email phishing', 'Phish email captured credentials for multiple users.', 3, 'Investigating', '2025-10-23 14:00:00', NULL, 1, 2),

('Ransomware on db-01', 'Files encrypted and ransom note found.', 5, 'Contained', '2025-10-10 14:00:00', NULL, 3, 2),

('Web malware dropper', 'EDR flagged malicious dropper on web-01.', 4, 'New', '2025-10-28 14:00:00', NULL, 2, 3),

('DDoS against web-01', 'Traffic flood observed.', 2, 'Closed', '2025-10-15 14:00:00', '2025-10-15 17:00:00', 4, 3);

Data Output Messages Notifications						
Showing rows: 1 to 4 Page No: 1 of 1						
	attack_id [PK] integer	title character varying (200)	description character varying (1000)	detected_at timestamp without time zone	contained_at timestamp without time zone	
1	1	Credential harvest via em...	Phish email captured credenti...	2025-10-23 14:43:54.919234	[null]	
2	2	Ransomware on db-01	Files encrypted and note found	2025-10-10 14:43:54.919234	[null]	
3	3	Web malware dropper	EDR flagged dropper on web-01	2025-10-28 14:43:54.919234	[null]	
4	4	DDoS against web-01	Traffic flood observed	2025-10-15 14:43:54.919234	[null]	

7.5 Insert Attack-Asset Links

INSERT INTO attack_assets (attack_id, asset_id, impact_notes) VALUES

(1, 3, 'Mail account targeted'),

(2, 2, 'Database server encrypted'),

(3, 1, 'Web server compromised'),

(4, 1, 'Service degraded');

Data Output Messages Notifications					
Showing rows: 1 to 4					
	attack_asset_id [PK] integer	attack_id integer	asset_id integer	impact_notes character varying (500)	
1	1	1	3	Mail account targeted	
2	2	2	2	Database server encrypt...	
3	3	3	1	Web server compromised	
4	4	4	1	Service degraded	

7.6 Insert IOCs

INSERT INTO iocs (attack_id, ioc_type, ioc_value, first_seen, last_seen) VALUES

(1, 'Domain', 'login-secure-help.com', '2025-10-23 14:00:00', NULL),

(1, 'IP', '185.12.44.21', '2025-10-24 14:00:00', NULL),

(2, 'Hash', 'sha256:FAKEHASH123...', '2025-10-10 14:00:00', NULL),

(3, 'URL', '<http://malicious.example/dropper.exe>', '2025-10-28 14:00:00', NULL);

Data Output Messages Notifications						
Showing rows: 1 to 4 Page No: 1 of 1						
	ioc_id [PK] integer	attack_id integer	ioc_type character varying (20)	ioc_value character varying (255)	first_seen timestamp without time zone	last_seen timestamp without time zone
1	1	1	Domain	login-secure-help.com	2025-10-23 14:43:54.919234	[null]
2	2	1	IP	185.12.44.21	2025-10-24 14:43:54.919234	[null]
3	3	2	Hash	sha256:FAKEHASH123...	2025-10-10 14:43:54.919234	[null]
4	4	3	URL	http://malicious.example/dropper...	2025-10-28 14:43:54.919234	[null]

7.7 Insert Responses

INSERT INTO responses (attack_id, action_text, action_time, action_by) VALUES

(1, 'Forced password reset for affected users', '2025-10-24 14:00:00', 2),

(2, 'Isolated db-01 from network', '2025-10-11 14:00:00', 2),

(2, 'Restored from backup and rotated keys', '2025-10-12 14:00:00', 3),

(3, 'Quarantined infected process and patched', '2025-10-29 14:00:00', 3);

Data Output Messages Notifications					
Showing rows: 1 to 4 Page No: 1					
	response_id [PK] integer	attack_id integer	action_text character varying (1000)	action_time timestamp without time zone	action_by integer
1	1	1	Forced password reset for affected users	2025-10-24 14:43:54.919234	2
2	2	2	Isolated db-01 from network	2025-10-11 14:43:54.919234	2
3	3	2	Restored from backup and rotated keys	2025-10-12 14:43:54.919234	3
4	4	3	Quarantined infected process and patc...	2025-10-29 14:43:54.919234	3

8. Analytical Reports

This section presents the analytical SQL queries developed for the Cyber Attack recording database. The reports possess the ability to extract insights from the stored data using JOINS, filtering, ordering and aggregate functions.

Each report contains the SQL query, a short explanation of the result and a screenshot of the query and output in pgAdmin.

8.1 Report 1- Open Attacks

SQL Query:

```
SELECT attack_id, title, severity, status, detected_at  
  
FROM attacks WHERE status <> 'Closed'  
  
ORDER BY severity DESC, detected_at ASC;
```

Explanation:

This report displays all the cyber-attacks that are still active and require further investigation.

Screenshot:

Data Output Messages Notifications						
Showing rows: 1 to 3 Page No: 1						
	attack_id [PK] integer	title character varying (200)	severity integer	status character varying (20)	detected_at timestamp without time zone	
1	2	Ransomware on db-01	5	Contained	2025-10-10 14:43:54.919234	
2	3	Web malware dropper	4	New	2025-10-28 14:43:54.919234	
3	1	Credential harvest via em...	3	Investigating	2025-10-23 14:43:54.919234	

8.2 Report 2: Most Common Attack Vectors (last 90 days)

SQL Query:

SELECT

```
v.name AS attack_vector,  
  
COUNT(*) AS total_attacks  
  
FROM attacks a  
  
JOIN attack_vectors v  
  
ON a.vector_id = v.vector_id  
  
WHERE a.detected_at >= NOW() - INTERVAL '90 days'  
  
GROUP BY v.name  
  
ORDER BY total_attacks DESC, v.name ASC;
```

Explanation:



This report displays which type of attack vectors have been used most frequently in the past 90 days.

Screenshot:

Data Output

Messages

Notifications

	attack_vector character varying (50) 	total_attacks bigint 
1	DDoS	1
2	Malware	1
3	Phishing	1
4	Ransomware	1

8.3 Report 3- Top Targeted Assets

SELECT

s.hostname AS asset,

COUNT(*) AS total_attacks

FROM attack_assets aa

JOIN assets s

ON aa.asset_id = s.asset_id

GROUP BY s.hostname

ORDER BY total_attacks

DESC, s.hostname ASC;

Explanation:

This report identifies which organizational assets have been attacked most frequently.

Screenshot:

Data Output

Messages

Notifications

<

8.4 Report 4- Open Attacks with Vectors and Asset Details

SQL Query:

SELECT

a.attack_id,

a.title,

v.name AS attack_vector,

```

s.hostname AS asset,

a.status,

a.detected_at

FROM attacks a

JOIN attack_vectors v

ON a.vector_id = v.vector_id

JOIN attack_assets aa

ON a.attack_id = aa.attack_id

JOIN assets s

ON aa.asset_id = s.asset_id

WHERE a.status <> 'Closed'

ORDER BY a.attack_id ASC, s.hostname ASC;

```

Explanation:

The multi-table JOIN report consolidates the attack details, attack vectors, and the affected assets.

Screenshot:

Data Output Messages Notifications						
	attack_id integer	title character varying (200)	attack_vector character varying (50)	asset character varying (100)	status character varying (20)	detected_at timestamp without time zone
1	1	Credential harvest via em...	Phishing	mail-1	Investigating	2025-10-23 14:43:54.919234
2	2	Ransomware on db-01	Ransomware	db-01	Contained	2025-10-10 14:43:54.919234
3	3	Web malware dropper	Malware	web-01	New	2025-10-28 14:43:54.919234

8.5 Report 5- IOC (Indicator of Compromise)

SQL Query

```
SELECT
a.attack_id,
a.title,
i.ioc_type,
i.ioc_value,
i.first_seen,
i.last_seen
FROM iocs i
JOIN attacks a
ON i.attack_id = a.attack_id
WHERE a.status <> 'Closed'
ORDER BY a.attack_id ASC, i.ioc_type ASC;
```

Explanation:

This report shows all the IOCs related to active cyber-attacks, including malicious domains, IP addresses, URLs, and file hashes. This helps the analysts detect ongoing threats and track attacker behavior.

Screenshot:

Data Output Messages Notifications						
<div> <div> <div>SQL</div> <div>Showing rows: 1 to 4</div> <div>Page No: 1 of 1</div> </div> </div>						
	attack_id integer	title character varying (200)	ioc_type character varying (20)	ioc_value character varying (255)	first_seen timestamp without time zone	last_seen timestamp with
1	1	Credential harvest via em...	Domain	login-secure-help.com	2025-10-23 14:43:54.919234	[null]
2	1	Credential harvest via em...	IP	185.12.44.21	2025-10-24 14:43:54.919234	[null]
3	2	Ransomware on db-01	Hash	sha256:FAKEHASH123...	2025-10-10 14:43:54.919234	[null]
4	3	Web malware dropper	URL	http://malicious.example/dropper....	2025-10-28 14:43:54.919234	[null]

9. Evidence of Work









This section contains all the visual proof that the database was successfully created, populated, and is able to execute the queries using pgAdmin 4.

9.1 Database Structure (Table List)

This contains the full list of tables in the attack_db under public schema.

> 1..3 Sequences

✓ Tables (8)

- >  assets
- >  attack_assets
- >  attack_vectors
- >  attacks
- >  audit_logs
- >  iocs
- >  responses
- >  users

9.2 Table Data Screenshots

This section shows the data stored in each table after running the DML inserts

9.2.1 Users Table

Data Output Messages Notifications

Showing rows: 1 to 3 Page No: 1 of 1

	user_id [PK] integer	username character varying (50)	password character varying (100)	role character varying (20)	created_at timestamp without time zone
1	1	admin	AdminPass123	Admin	2025-10-30 14:43:54.919234
2	2	alice	Analyst1!	Analyst	2025-10-30 14:43:54.919234
3	3	bob	Analyst2!	Analyst	2025-10-30 14:43:54.919234

9.2.2 Assets Table

Data Output Messages Notifications

Showing rows: 1 to 3 Page No: 1 of 1

	asset_id [PK] integer	hostname character varying (100)	ip_addr character varying (45)
1	1	web-01	10.0.0.11
2	2	db-01	10.0.0.21
3	3	mail-1	10.0.0.31

9.2.3 Attack Vectors Table

Data Output

Messages

Notifications

Showing rows: 1 to 5

Page No: 1

	<div>vector_id</div> <div>[PK] integer<div></div></div>	<div>name</div> <div>character varying (50)<div></div></div>
1	1	Phishing
2	2	Malware
3	3	Ransomware
4	4	DDoS
5	5	Privilege Escalation

9.2.4 Attacks Table

Data Output

Messages

Notifications

Showing rows: 1 to 4

Page No: 1

of 1

	attack_id [PK] integer	title character varying (200)	description character varying (1000)	detected_at timestamp without time zone	contained_at timestamp without time zone	closed_at timestamp without time zone
1	1	Credential harvest via em...	Phish email captured credenti...	2025-10-23 14:43:54.919234	[null]	[null]
2	2	Ransomware on db-01	Files encrypted and note found	2025-10-10 14:43:54.919234	[null]	[null]
3	3	Web malware dropper	EDR flagged dropper on web-01	2025-10-28 14:43:54.919234	[null]	[null]
4	4	DDoS against web-01	Traffic flood observed	2025-10-15 14:43:54.919234	[null]	[null]

9.2.5 Attacks_assets Table

Data Output Messages Notifications

	attack_asset_id [PK] integer	attack_id integer	asset_id integer	impact_notes character varying (500)
1	1	1	3	Mail account targeted
2	2	2	2	Database server encrypt...
3	3	3	1	Web server compromised
4	4	4	1	Service degraded

9.2.6 IOCs Table

	ioc_id [PK] integer	attack_id integer	ioc_type character varying (20)	ioc_value character varying (255)	first_seen timestamp without time zone	last_seen timestamp without time zone
1	1	1	Domain	login-secure-help.com	2025-10-23 14:43:54.919234	[null]
2	2	1	IP	185.12.44.21	2025-10-24 14:43:54.919234	[null]
3	3	2	Hash	sha256:FAKEHASH123...	2025-10-10 14:43:54.919234	[null]
4	4	3	URL	http://malicious.example/dropper....	2025-10-28 14:43:54.919234	[null]

9.2.7 Responses Table

	response_id [PK] integer	attack_id integer	action_text character varying (1000)	action_time timestamp without time zone	action_by integer
1	1	1	Forced password reset for affected users	2025-10-24 14:43:54.919234	2
2	2	2	Isolated db-01 from network	2025-10-11 14:43:54.919234	2
3	3	2	Restored from backup and rotated keys	2025-10-12 14:43:54.919234	3
4	4	3	Quarantined infected process and patc...	2025-10-29 14:43:54.919234	3

9.2.8 Audit Logs table

	log_id [PK] integer	user_id integer	action character varying (50)	object_type character varying (50)	object_id integer	ts timestamp without time zone	details character varying (1000)
--	------------------------	--------------------	----------------------------------	---------------------------------------	----------------------	-----------------------------------	-------------------------------------

9.3 Report Outputs

9.3.1 Report 1- Open attacks

	attack_id [PK] integer	title character varying (200)	severity integer	status character varying (20)	detected_at timestamp without time zone
1	2	Ransomware on db-01	5	Contained	2025-10-10 14:43:54.919234
2	3	Web malware dropper	4	New	2025-10-28 14:43:54.919234
3	1	Credential harvest via em...	3	Investigating	2025-10-23 14:43:54.919234

9.3.2 Report 2- Attack Vectors (Last 90)

	attack_vector character varying (50)	total_attacks bigint
1	DDoS	1
2	Malware	1
3	Phishing	1
4	Ransomware	1

9.3.3 Report 3- Top Targeted Assets

	asset character varying (100)	total_attacks bigint
1	web-01	2
2	db-01	1
3	mail-1	1

9.3.4 Report 4- Multi-Table JOIN Output

	attack_id integer 🔒	title character varying (200) 🔒	attack_vector character varying (50) 🔒	asset character varying (100) 🔒	status character varying (20) 🔒	detected_at timestamp without time zone 🔒
1	1	Credential harvest via em...	Phishing	mail-1	Investigating	2025-10-23 14:43:54.919234
2	2	Ransomware on db-01	Ransomware	db-01	Contained	2025-10-10 14:43:54.919234
3	3	Web malware dropper	Malware	web-01	New	2025-10-28 14:43:54.919234

9.3.5 Report 5- IOCs for Active Attacks

	attack_id integer 🔒	title character varying (200) 🔒	ioc_type character varying (20) 🔒	ioc_value character varying (255) 🔒	first_seen timestamp without time zone 🔒	last_seen timestamp without time zone 🔒
1	1	Credential harvest via em...	Domain	login-secure-help.com	2025-10-23 14:43:54.919234	[null]
2	1	Credential harvest via em...	IP	185.12.44.21	2025-10-24 14:43:54.919234	[null]
3	2	Ransomware on db-01	Hash	sha256:FAKEHASH123...	2025-10-10 14:43:54.919234	[null]
4	3	Web malware dropper	URL	http://malicious.example/dropper....	2025-10-28 14:43:54.919234	[null]

10. Conclusion

This project built a fully working cyber-attack incident management database using PostgreSQL and pgAdmin 4.

All the tables were created, sample data was added, and the queries ran successfully, proving that the system works as intended.

The database helps track attacks, affected assets, users, response actions, and indicators of compromise. The reports show how this data can be used to monitor open incidents, see trends, and support basic security decision making

Overall. The project met its goals and clearly demonstrates how a well-structured database can help organize and manage cybersecurity information.