Cyber Threats Management System

Karl Xavier Layco
Student-ID: 922536937
GitHub: *BulbaWasTaken*

Checkpoint #	Date Submitted
Checkpoint I	9/17/2023
Checkpoint I v2	9/24/2023
Checkpoint II	9/30/2023
Checkpoint III	10/23/2023

Table of Contents

Project Description 4

Use Cases 5

1. Use Case: Real-time Threat Alert 5
2. Use Case: Threat Analysis Collaboration 5
3. Use Case: Threat Intelligence Sharing 6
4. Use Case: Threat Campaign Tracking 6
5. Use Case: Service Provider 7

Benefiting Software Tools/Products 7

Functional Database Requirements 8

1. User 8
2. Administrators 8
3. Registered Users 8
4. Employee 9
5. Teams 9
6. Company 9
7. Account 10
8. Profile 10
9. Report 10
10. Forum 10
11. Comments 11
12. Threat 11
13. Devices 11
14. Alert 12
15. Patterns 12
16. Solution 12
17. Threat Campaign 12
18. Malicious Actor 12
19. Attack Vector 13
20. Services 13
21. Vulnerability 13
22. Severity Level 13
23. Discovery Method 14

24. Status 14
Non-functional Database Requirements 15
1. Security 15
2. Storage 15
3. Performance 15
4. Data Integrity 15
5. Content 15
6. Legal 15
7. Organizational 16
8. Monitoring and Logging 16
9. Compatibility 16
10. System Requirements 16
11. Environmental 17
Entity Relationship Diagram (ERD) 18
Entity Description 19
Entity Establishment Relationship Diagram (EER) 24
Constraints Description 25

Project Description

Cyber Threats Database Management System aims to improve digital security and address the escalating challenges posed by cyber threats in today's digital landscape. The motivations behind this originates from the need to empower organizations to effectively manage and respond to cyber threats. The system aims to streamline the collection, analysis, and spreading of cyber threat intelligence, enabling you or any cybersecurity companies to make informed decisions, bolster their defenses, and proactively prevent cyberattacks. With a forum-like functionality, users can interact with other users and professionals in the industry. This is a centralized and user-friendly database system engineered for individuals or companies. The system is designed to collect and securely store diverse sources of threat intelligence data, including logs, external feeds, and incident reports. It is also designed to store solutions that companies innovated to help against the threats. Employing advanced data analytics, it discerns patterns and anomalies, offering actionable insights to its users. Ultimately, this system will significantly enhance your ability to detect, respond to, and mitigate cyber threats efficiently, contributing to a more secure digital landscape. This system distinguishes itself through some of its features. One of which is advanced threat analytics, which identifies emerging threat patterns and provides solutions. To improve user experience, we also have a feature of alerting users and professionals in real time. By having this, it is easier for the users and cybersecurity professionals to be ready or be informed of what the threat is. This system provides a customizable reporting feature where users can manually enter detailed information about past incidents and provide insights about the threat. Furthermore, it seamlessly integrates with existing security infrastructure, such as SIEM systems, augmenting an organization's threat detection and response capabilities. This system fosters collaboration by facilitating the secure

sharing of threat intelligence data with trusted partners, contributing to collective cybersecurity efforts. The system also allows any companies to keep track of employees to prevent insider attacks.

Use Cases

1. Use Case: Real-time Threat Alert

Actor: Splunk Employee (Homer)

Description: Homer is responsible for monitoring the security of his organization's network. He receives an alert on his system indicating a suspicious network activity pattern. With this system integrated into the Security information and event management (SIEM), Homer can swiftly investigate the alert. The system provides him with real-time information about the detected threat, its source, and potential impact. Homer can then take immediate action to mitigate the threat and prevent a potential breach. The Cyber Threats Management System enhances his ability to respond promptly to evolving threats, safeguarding his organization's sensitive data and infrastructure.

2. Use Case: Threat Analysis Collaboration

Actor: Security Analyst (Michael and Lenard), Splunk, CrowdStrike

Description: Michael, who works for Splunk, is responsible for conducting in-depth analyses of past security incidents to identify trends and vulnerabilities. Likewise, Lenard, who works for CrowdStrike was appointed to analyze reoccurring threats for the month. Using this system, Michael and Lenard can collaborate together and analyze the threats from the rich repository of reports from users of the system. They can request the

system to retrieve specific incident details. This system can help develop possible solutions by the collaboration of two companies.

3. Use Case: Threat Intelligence Sharing

Actor: Gamer (Alex), Riot Games

Description: Alex is a casual gamer that casually play games. One day, one of the players he is playing against DDoS attacked him to get an advantage. The enemy team won against his teammates, which enraged him. This occurrence happened to him multiple times afterwards. It happened to many other players as well, which makes this occurrence well-known within the community. Riot games, a company that develops games, is having a hard time in keeping track of reports. To improve their situation, they need a system where users, like Alex and other gamers, can report threats to companies and communicate with other users and companies. Riot Games needs a system where they can access reports from users so they can do something about the problem.

4. Use Case: Threat Campaign Tracking

Actor: Cybersecurity Professional (John)

Description: John has started working for a Cybersecurity company. He is responsible for managing security teams and the corresponding threat campaign. The system can help John in various ways: (1) He can manage security teams and assign a threat campaign to each. (2) Upon selecting a specific campaign, John can view detailed information such as the campaign's name, description, objectives, and associated attack vectors. (3) For each campaign, John can access information about the threat actors involved, including their profiles, motivations, and tactics. (4) The system displays a list of systems targeted by the

campaign, enabling John to assess potential vulnerabilities. (5) The system can help John track the status of each track campaign. (6) The system can link individual reports from other users to a campaign.

5. Use Case: Service Provider

Actor: San Francisco State University Student (Sam)

Description: Sam recently bought a laptop for educational use. After setting it up, he noticed that the laptop did not come with an anti-virus. He searched the internet for anti-virus, but he was disappointed to learn that almost every anti-virus has an expensive subscription so he can use the basic functionality of it. Since he is only a college student that works part-time, he cannot afford majority of it. This system can help users, like Sam, to get good and affordable services. The system collects and stores information about good services users can get on the internet. The services that will be recommended by this system must be tested by administrators and employees. This system can also help Sam detect the vulnerability of the games he is playing.

Benefiting Software Tools/Products

The first one is Splunk. Splunk is an organization that is focused on solving problems in complex digital infrastructures. They are a leading provider of data analytics and security information and event management (SIEM) solutions. They can benefit from this system by leveraging its advanced threat analytics and real-time alerting capabilities. This integration enhances their ability to detect and respond to evolving threats more effectively.

Another one is CrowdStrike. a prominent cybersecurity company known for its endpoint detection and response (EDR) solutions. They can enhance their threat detection capabilities by

integrating with this system to access enriched threat intelligence data. This enables them to provide more accurate and proactive threat hunting and mitigation services to their clients.

Functional Database Requirements

1. User

1.1. A user is an unregistered user, registered user, administrator, or employee.

1.2. A user shall be able to create at most one account with a unique email.

1.3. A user shall be able to view many forums.

1.4. A user shall be harmed by many threats and vulnerabilities.

1.5. A user shall use many services.

2. Administrators

2.1. An administrator shall manage many forums.

2.2. An administrator shall manage many registered users, and employees.

2.3. An administrator shall be able to view many alerts.

2.4. An administrator is the only and only user that can edit information on the system.

2.5. An administrator is the only and only user that can edit the forums.

2.6. An administrator is able to add notes to an alert.

2.7. An administrator is able to ban or delete users who violates policies.

2.8. An administrator is able to communicate with other users.

2.9. An administrator shall be able to access many reports.

2.10. An administrator shall manage many teams.

3. Registered Users

3.1. A registered user shall be managed at least one administrator.

3.2. A registered user shall be able to login with at least one device.

3.3. A registered user shall be able generate many comments.

3.4. A registered user shall be able to submit many reports.

3.5. A registered user is able to communicate with other users.

4. Employee

4.1. An employee shall be assigned at most one team.

4.2. An employee shall work for one company.

4.3. An employee shall have one unique work id.

4.4. An employee shall be managed by at least one administrator.

4.5. An employee shall be able to access many reports.

4.6. An employee is able to add notes to an alert.

4.7. An employee is able to communicate with other users.

4.8. An employee shall produce many solutions.

4.9. An employee shall be able to view many alerts.

4.10. An employee shall analyze many threats and vulnerabilities.

4.11. An employee shall test many services.

5. Teams

5.1. A team shall be managed by one administrator.

5.2. A team shall analyze many threat campaigns.

5.3. A team shall have many employees.

5.4. A team shall only have one ID number.

5.5. A team shall have a team name.

6. Company

6.1. A company shall have many employees.

6.2. A company shall collaborate with many companies.

7. Account

7.1. An account shall belong to only one user.

7.2. An account shall have one profile.

7.3. An account shall have only one username.

7.4. An account shall have only one password.

7.5. An account shall have only one unique user id.

8. Profile

8.1. A profile shall be owned by one and only one account.

8.2. A profile shall have one alias.

9. Report

9.1. A report shall be submitted by one registered user.

9.2. A report shall have at least one threat or vulnerability.

9.3. A report shall be accessed by many employees, and administrators.

9.4. A report shall be displayed in many forums.

9.5. A report shall have only one unique ID.

9.6. A report shall have a date.

9.7. A report shall have descriptions.

9.8. A report shall have many malicious actors.

9.9. A report shall have many discovery methods.

9.10. A report shall have one and only one status.

9.11. A report shall report many threat campaigns.

10. Forum

10.1. A forum is a private forum or public forum.

10.2. A forum shall be viewed by many users.

10.3. A forum shall display many reports.

10.4. A forum shall display many solutions.

10.5. A forum shall display many services.

10.6. A forum shall have many comments posted.

10.7. A forum shall be managed by at least one administrator.

10.8. A forum shall have one publisher.

11. Comments

11.1. A comment shall be generated by many registered users.

11.2. A comment shall be posted in one forum.

12. Threat

12.1. A threat shall harm many users.

12.2. A threat shall infect many devices.

12.3. A threat shall have many solutions.

12.4. A threat shall contain many patterns.

12.5. A threat shall be analyzed by many employees.

12.6. A threat shall generate one alert.

12.7. A threat shall have many discovery methods.

12.8. A threat shall have one and only one status.

12.9. A threat shall have one and only one severity level.

12.10. A threat shall be in many reports.

12.11. A threat shall be in many threat campaigns.

13. Devices

13.1. A device shall login one registered user at a time.

13.2. A device shall be infected by many threats.

13.3. A device shall be attacked by many malicious actors.

14. Alert

14.1. An alert shall be generated by many threats and/or vulnerabilities.

14.2. An alert shall be viewed many administrators and employees.

15. Patterns

15.1. A pattern shall have at least one threat and/or vulnerability.

15.2. A pattern shall have a unique number.

16. Solution

16.1. A solution shall be generated by employees, but not other users.

16.2. A solution shall many threats and/or vulnerabilities.

16.3. A solution shall be displayed to many forums.

16.4. A solution shall have one unique id.

17. Threat Campaign

17.1. A campaign shall be analyzed by many teams.

17.2. A campaign shall be link from many reports.

17.3. A campaign shall have many attack vectors.

17.4. A campaign shall have many threats.

18. Malicious Actor

18.1. A malicious actor shall have one unique id.

18.2. A malicious actor shall have one alias.

18.3. A malicious actor shall be in many reports.

18.4. A malicious actor shall attack at least one device.

18.5. A malicious actor shall use at least one attack vector.

19. Attack Vector

19.1. An attack vector shall have one unique id.

19.2. An attack vector shall descriptions.

19.3. An attack vector shall have at least one malicious actor.

20. Services

20.1. A service shall be tested by at least one employee.

20.2. A service shall be viewed in many forums.

20.3. A service shall be used by many users.

21. Vulnerability

21.1. A vulnerability shall harm many users.

21.2. A vulnerability shall have many descriptions.

21.3. A vulnerability shall have one and one severities level.

21.4. A vulnerability shall a publication date.

21.5. A vulnerability shall have one and only one status.

21.6. A vulnerability shall be in many reports.

21.7. A vulnerability shall have many solutions.

21.8. A vulnerability shall contain many patterns.

21.9. A vulnerability shall be analyzed by many employees.

21.10. A vulnerability shall generate one alert.

21.11. A vulnerability shall have many discovery methods.

22. Severity Level

22.1. A Severity level is low, medium, high, or critical.

22.2. A Severity level shall have one level id.

22.3. A Severity level shall have many vulnerabilities and/or threats.

23. Discovery Method

23.1. A discovery method shall discover at least one vulnerability and/or threats.

23.2. A discovery method shall have one unique id.

23.3. A discovery method shall be in many reports.

24. Status

24.1. A status is open, closed, mitigated, or under investigation.

24.2. A status shall indicate the status of many vulnerabilities.

24.3. A status shall indicate the status of many threats.

24.4. A status shall indicate the status of many reports.

Non-functional Database Requirements

1. Security

1.1. Only encrypted passwords shall be supported by the database.

1.2. Only authorized users and employees can access the database.

1.3. Data shall be encrypted during transmission to protect sensitive information.

2. Storage

2.1. Regular automated backups of the database shall be performed every day at 11:59 p.m.

2.2. The database system shall assign at least 15 MB of memory per table.

3. Performance

3.1. The system shall be able to process a minimum of 100,000 security events per second.

3.2. Database queries for threat data retrieval shall have a response time of under 3 seconds.

4. Data Integrity

4.1. The database shall implement data integrity constraints to prevent unauthorized or accidental data modifications.

4.2. Audit logs shall track all changes made to the database to maintain data accountability.

5. Content

5.1. The system shall ensure that the data stored in the database is accurate and up to date.

5.2. Users should be able to easily search for and find relevant content within the system using efficient search algorithms and filters.

6. Legal

6.1. The system shall comply with relevant data protection and privacy regulations.

6.2. The system shall implement data retention policies in accordance with legal requirements.

7. Organizational

7.1. The system shall define role-based access controls to restrict access to sensitive threat data based on user or employee roles.

7.2. Companies shall ensure that employees handling threats are adequately trained.

8. Monitoring and Logging

8.1. The system shall have built-in monitoring and logging capabilities to track database performance, errors, and security events.

8.2. The system shall log all relevant security events, and reports.

9. Compatibility

9.1. The system shall be compatible with various operating systems, including Windows, macOS, and Linux.

9.2. The system shall be compatible with various browsers, such as Chrome, Mozilla, and Opera

10. System Requirements

10.1. The system shall be available 24/7 to ensure constant monitoring and threat detection.

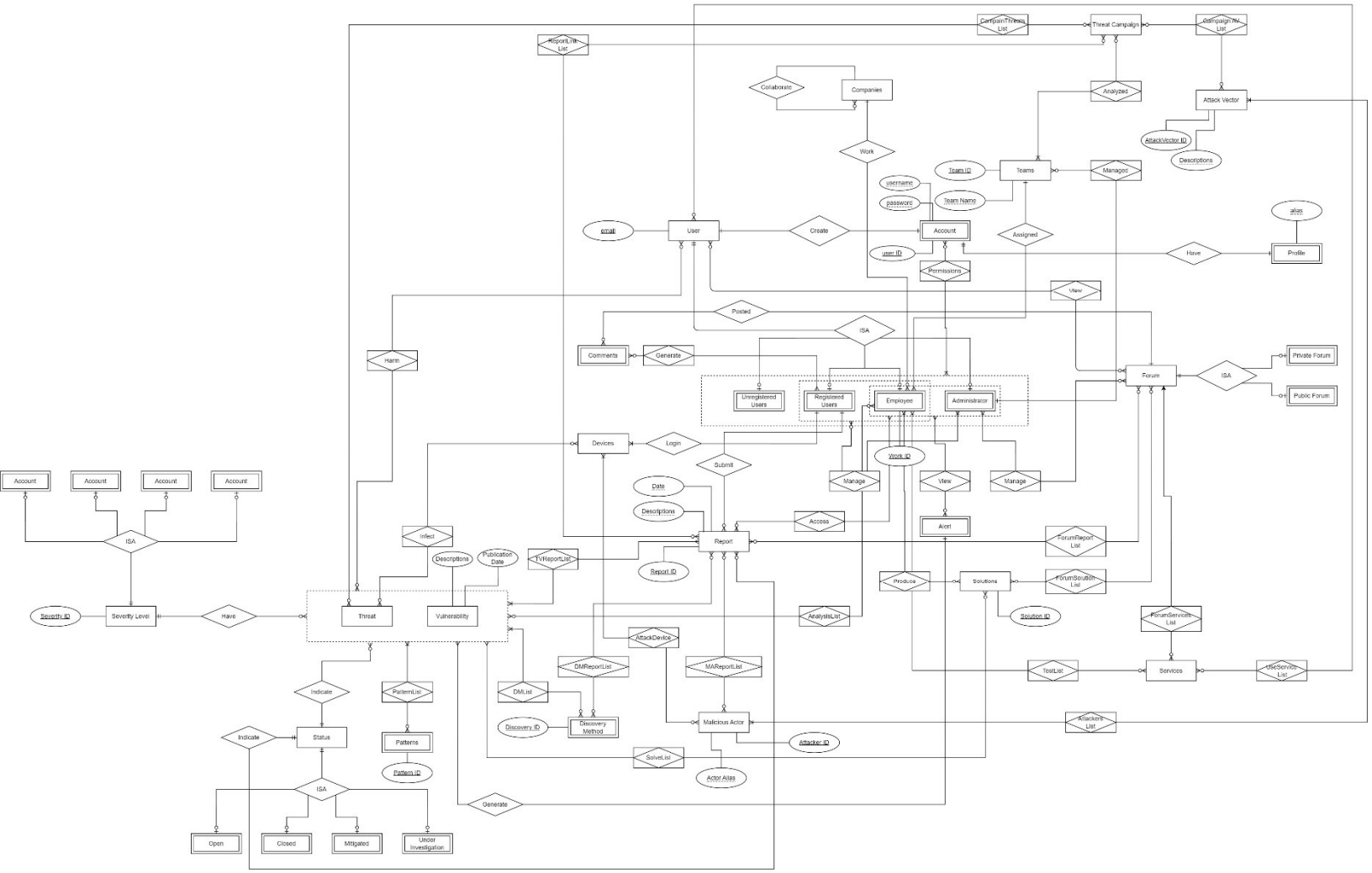
10.2. The system shall have a high degree of reliability to minimize down time and data loss.

11. Environmental

11.1. The system shall maintain redundant network connections to ensure uninterrupted data flow and database access in case of network failures.

11.2. The system shall minimize energy consumption and support power-saving modes for devices where applicable.

Entity Relationship Diagram (ERD)



Entity Description

1. User (Strong)
    - user_id: key, numeric
    - name: composite, alphanumeric
    - email: valid email
    - dob: multi-value, timestamp
    - user_type: enumeration
    - accounts_id: key, numeric
2. Administrators (Weak)
    - admin_id: key, numeric
    - admin_password: alphanumeric
3. Registered Users (Weak)
    - registered_user_id: key, numeric
4. Employee (Weak)
    - employee_id: key, numeric
    - user_id: key, numeric
    - company: key, numeric
    - team_id: key, numeric
5. Teams (Strong)
    - team_id: key, numeric
    - team_name: alphanumeric
    - admin_managed: key, numeric
6. Company (Strong)

- company_id: key, numeric
- name: alphanumeric
- email: valid email
- collab: key, numeric

7. Account (Weak)
    - account_id: key, numeric
    - username: alphanumeric
    - password: alphanumeric
8. Profile (Weak)
    - account_id: key, numeric
    - profile_id: key, numeric
    - alias: alphanumeric
9. Report (Strong)
    - report_id: key, numeric
    - title: alphanumeric
    - submitted_by: key, numeric
    - threat: key, numeric
    - vulnerability: key, numeric
    - publication_date: multi-value, timestamp
    - description: alphanumeric
    - status: key, numeric
10. Forum (Strong)
    - forum_id: key, numeric

- forum_title: alphanumeric
- forum_description: alphanumeric
- publisher: key, numeric

11. Comments (Weak)
    - comment_id: key, numeric
    - posted_forum: key, numeric
    - publisher: key, numeric
    - comment: text
12. Threat (Strong)
    - threat_id: key, numeric
    - threat_name: alphanumeric
    - status: key, numeric
    - severity_level: key, numeric
13. Devices (Strong)
    - device_id: key, numeric
    - user_log: key, numeric
14. Alert (Weak)
    - alert_id: key, numeric
    - threats: key, numeric
    - vulnerabilities: key, numeric
    - alert_date: multi-value, timestamp
15. Patterns (Weak)
    - pattern_id: key, numeric

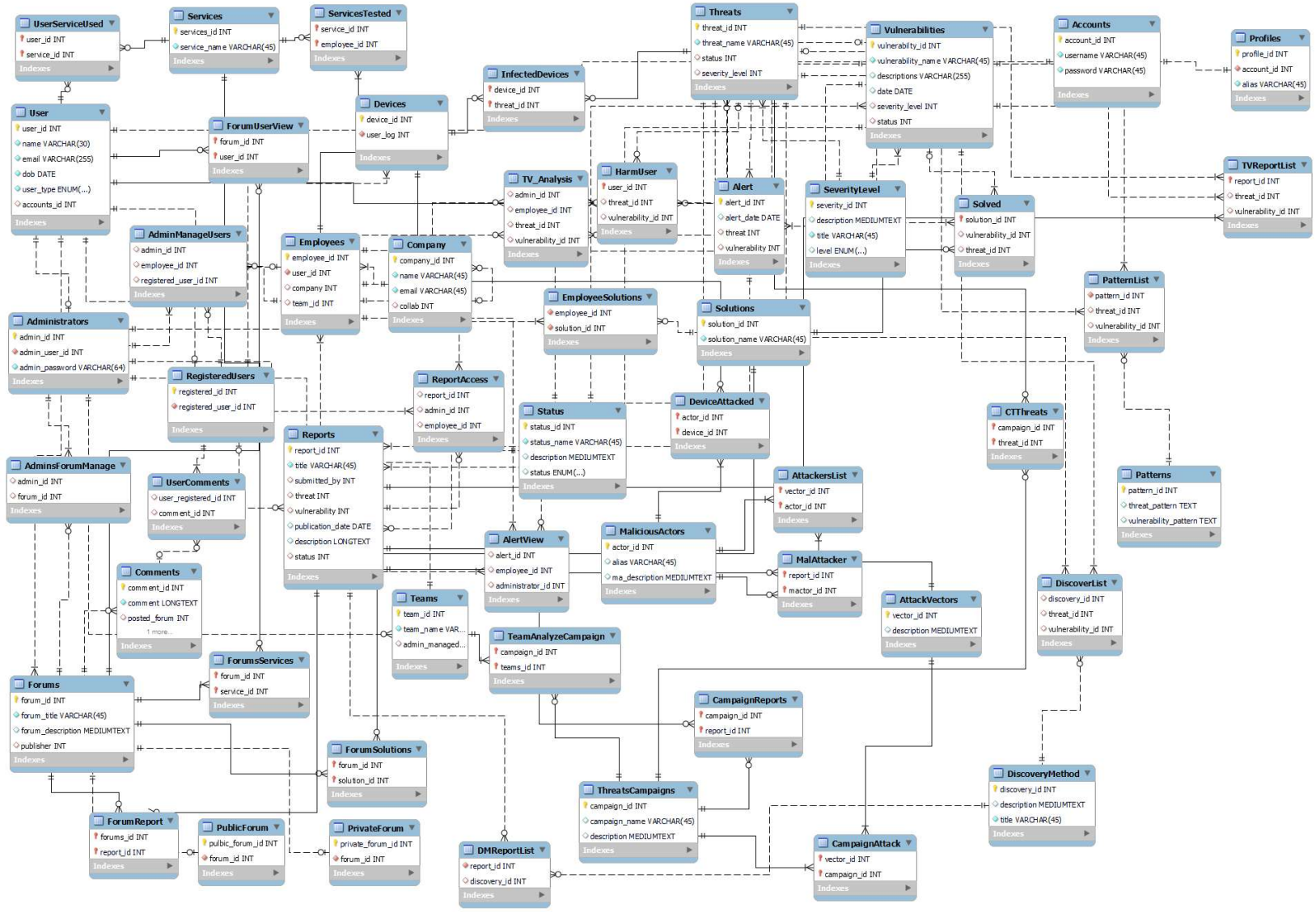
- threat_pattern: text
- vulnerability_pattern: text

16. Solution (Strong)
    - solution_id: key, numeric
    - solution_name: alphanumeric
    - solution: alphanumeric
17. Threat Campaign (Strong)
    - campaign_id: key, numeric
    - campaign_name: alphanumeric
    - description: alphanumeric
18. Malicious Actor (Strong)
    - actor_id: key, numeric
    - alias: composite, alphanumeric
    - ma_description: alphanumeric
19. Attack Vector (Strong)
    - vector_id: key, numeric
    - description: alphanumeric
20. Services (Strong)
    - services_id: key, numeric
    - service_name: alphanumeric
21. Vulnerability (Strong)
    - vulnerability_id: key, numeric
    - vulnerability_name: alphanumeric

- descriptions: alphanumeric
- severity_level: key, numeric
- date: multi-value, timestamp
- status: key, numeric

22. Severity Level (Strong)
    - severity_id: key, numeric
    - description: alphanumeric
    - title: alphabetic
23. Discovery Method (Strong)
    - discovery_method_id: key, numeric
    - description: alphanumeric
    - title: alphanumeric
24. Status (Strong)
    - status_id: key, numeric
    - status_name: alphabetic
    - description: alphanumeric

Entity Establishment Relationship Diagram (EER)



Constraints Description

Table	*Foreign Key*	*ON UPDATE*	*ON DELETE*	*Comment*
User	account_id	CASCADE	CASCADE	If the user deletes the account, the user will hold no account until a new one is assigned
UserServiceUsed	usu_user_id_fk	CASCADE	CASCADE	If user is deleted, then the user that used the services will be deleted as well
UserServiceUsed	service_id_fk	CASCADE	CASCADE	If the service is deleted, the rows will be deleted as well.
ForumServices	fs_forum_id_fk	CASCADE	CASCADE	If the forum is deleted, the services posted in the forum will be deleted as well.
ForumServices	fs_service_id_fk	CASCADE	CASCADE	If the service is deleted, the forum will be deleted as well.
ServiceTested	st_service_id_fk	CASCADE	CASCADE	If the service is deleted, the tested service by an employee will be deleted as well.
ServiceTested	st_employee_id_fk	CASCADE	CASCADE	If the employee is deleted, the services the employee tested will be deleted as well.
ForumUserView	fuv_user_id_fk	CASCADE	CASCADE	If the user is deleted, the user's access to

				the forum will be deleted as well.
ForumUserView	fuv_forum_id_fk	CASCADE	CASCADE	If the forum is deleted, the user will not be able to view the forum.
AdminManageUsers	am_admin_id_fk	CASCADE	CASCADE	If the administrator is deleted, the users managed will hold no value until a new one is assigned.
AdminManageUsers	am_emp_id_fk	CASCADE	SET NULL	If the employee is deleted, the employees managed by the admin will hold no value until assigned a new one.
AdminManageUsers	am_reg_id_fk	CASCADE	SET NULL	If the registered user is deleted, the administrator will manage no one until a new user is assigned.
Employees	uid_fk	CASCADE	CASCADE	If the user is deleted, the employee will be deleted as well.
Employees	company_fk	CASCADE	SET NULL	If the company is deleted, the employee will not be in a company until assigned to a new one.
Registered Users	reg_id_fk	CASCADE	CASCADE	If the user is deleted, the registered user

				will be deleted as well.
Administrators	user_id_fk	CASCADE	CASCADE	If the user is deleted, the administrator will be deleted as well.
Device Attacked	da_actor_id_fk	CASCADE	CASCADE	If the actor is deleted, the information on the table will be deleted as well.
Device Attacked	da_device_id_fk	CASCADE	CASCADE	If the device is deleted, the information on the table will be deleted as well.
Devices	device_user_id_fk	CASCADE	CASCADE	If the user is deleted, the device will be deleted as well.
InfectedDevices	threats_id_fk	CASCADE	CASCADE	If the threat is deleted, the rows with the threat will be deleted as well.
InfectedDevices	device_id_fk	CASCADE	CASCADE	If the device is deleted, the rows with the threat will be deleted as well.
UserComments	uc_ru_id_fk	CASCADE	SET NULL	If the user is deleted, the comments will remain and will hold no user.
UserComments	uc_comments_id_fk	CASCADE	CASCADE	If the comment is deleted, the column will be deleted as well.
Forum	forum_user_id_fk	CASCADE	SET NULL	If the user is deleted, the forum will remain.
AdminsForumManage	afm_admin_id_fk	CASCADE	CASCADE	If the admin is deleted, the

				forum will hold no administrators until a new one is assigned
AdminsForumManage	afm_forum_id_fk	CASCADE	CASCADE	If the If the forum is deleted, the admin will stop managing that forum.
PrivateForum	privforum_id_fk	CASCADE	CASCADE	If the forum is deleted, the private forum will be deleted as well
PublicForum	pubforum_id_fk	CASCADE	CASCADE	If th If the forum is deleted, the public forum will be deleted as well
Company	company_id_fk	CASCADE	CASCADE	If the company is deleted, the collaboration on other companies will be deleted as well.
Comments	posted_forum_id_fk	CASCADE	CASCADE	If the forum is deleted, all comments will be deleted as well.
Reports	registered_user_id_fk	CASCADE	SET NULL	If the user is deleted, the report will hold no publisher.
Reports	rep_status_id_fk	CASCADE	SET NULL	If the status is deleted, the report will hold no status until assigned a new one.
Reports	threat_id_fk	CASCADE	SET NULL	If the threat is deleted, the report will hold no threat.

Reports	Vulnerability_id_fk	CASCADE	SET NULL	If a vulnerability is deleted, the report will hold no vulnerability.
ForumReport	forumRep_id_fk	CASCADE	CASCADE	If the forum is deleted, the report shall be deleted as well.
ForumReport	freport_report_id_fk	CASCADE	CASCADE	If the report is deleted, the forum will be deleted as well.
MalAttacker	ma_report_id_fk	CASCADE	CASCADE	If the report is deleted, the column will be deleted as well.
MalAttacker	ma_actor_id_fk	CASCADE	CASCADE	If the actor is deleted, the column shall be deleted as well.
CampaignReports	cr_campaign_id_fk	CASCADE	CASCADE	If the campaign is deleted, the rows are deleted as well.
CampaignReports	cr_report_id_fk	CASCADE	CASCADE	If the report is deleted, the campaign will hold no report until assigned a new one.
CampaignAttack	ca_vector_id_fk	CASCADE	CASCADE	If the attack vector is deleted, the campaign will be deleted as well.
CampaignAttack	ca_campaign_id_fk	CASCADE	CASCADE	If the campaign is deleted, the column shall be deleted as well.
TeamAnalyzeCampaign	ta_campaign_id_fk	CASCADE	CASCADE	If the campaign is deleted, no team can analyze the campaign.
TeamAnalyzeCampaign	ta_teams_id_fk	CASCADE	CASCADE	If the team is deleted, no

				campaign can be analyzed.
Threats	status_id_fk	CASCADE	SET NULL	If status is removed, threat holding the status will hold no status until a new one is assigned
Threats	severity_id_fk	CASCADE	SET NULL	If severity level is removed, threat holding the level will hold no levels until a new one is assigned.
Vulnerabilities	severity_level_id_fk	CASCADE	SET NULL	If severity level is removed, the vulnerability holding the level will hold no levels until a new one is assigned.
Vulnerabilities	vul_status_id_fk	CASCADE	SET NULL	If status is removed, the vulnerability holding the status will hold no status until a new one is assigned.
Profiles	prof_account_id_fk	CASCADE	CASCADE	If the account is deleted, the profile shall be deleted as well.
TV_Analysis	tva_admin_id_fk	CASCADE	SET NULL	If admin is deleted, the column will hold no admins until a new one is assigned.
TV_Analysis	tva_emp_id_fk	CASCADE	SET NULL	If an employee is deleted, the column will hold no

				employees until a new one is assigned.
TV_Analysis	tva_threat_id_fk	CASCADE	SET NULL	If a threat is deleted, the column will hold no threats until a new one is assigned.
TV_Analysis	tva_vul_id_fk	CASCADE	SET NULL	If a vulnerability is deleted, the column will hold no vulnerability until a new one is assigned.
HarmUser	hu_user_id_fk	CASCADE	CASCADE	If the user is deleted, the column shall be deleted as well.
HarmUser	hu_threat_id_fk	CASCADE	CASCADE	If the threat is deleted, the rows holding the threats will hold no threats until a new one is assigned.
HarmUser	hu_vul_id_fk	CASCADE	CASCADE	If the vulnerability is deleted, the rows holding the vulnerability will hold no vulnerability until a new one is assigned.
Alert	threat_id	CASCADE	SET NULL	If the threat is deleted, the rows holding the threats will hold no threats until a new one is assigned.
Alert	vulnerability_id	CASCADE	SET NULL	If the vulnerability is deleted, the rows

				holding the vulnerability will hold no vulnerability until a new one is assigned.
Solved	solved_sol_id_fk	CASCADE	CASCADE	If solution is deleted, the rows holding the solution will be deleted as well
Solved	solved_vul_id_fk	CASCADE	SET NULL	If the vulnerability is deleted, the rows holding the vulnerability will hold no vulnerability until a new one is assigned.
Solved	solved_threat_id_fk			If the threat is deleted, the rows holding the threats will hold no threats until a new one is assigned.
TVReportList	tvl_report_id_fk	CASCADE	CASCADE	If the report is deleted, the rows holding the reports shall be deleted as well.
TVReportList	tvl_threat_id_fk	CASCADE	SET NULL	If the threat is deleted, the rows holding the threats will hold no threats until a new one is assigned.
TVReportList	tvl_vul_id_fk	CASCADE	SET NULL	If the vulnerability is deleted, the rows holding the vulnerability will hold no vulnerability

				until a new one is assigned.
EmployeeSolutions	es_employee_id_fk	CASCADE	CASCADE	If an employee is deleted, the column holding the employee shall be deleted as well.
EmployeeSolutions	es_solution_id_fk	CASCADE	CASCADE	If a solution is deleted, the column holding the solution shall be deleted as well.
PatternList	pl_pattern_id_fk	CASCADE	CASCADE	If a pattern is deleted, the column holding the pattern shall be deleted as well.
PatternList	pl_threat_id_fk	CASCADE	SET NULL	If the threat is deleted, the rows holding the threats will hold no threats until a new one is assigned.
PatternList	pl_vul_id_fk	CASCADE	SET NULL	If the vulnerability is deleted, the rows holding the vulnerability will hold no vulnerability until a new one is assigned.
CTThreats	ctt_campaign_id_fk	CASCADE	CASCADE	If a campaign is deleted, the column holding the campaign shall be deleted as well.
CTThreats	ctt_threat_id_fk	CASCADE	CASCADE	If a threat is deleted, the column holding the threat shall

				be deleted as well.
ReportAccess	ra_report_id_fk	CASCADE	CASCADE	If a report is deleted, the column holding the report shall be deleted as well
ReportAccess	ra_admin_id_fk	CASCADE	SET NULL	If an admin is deleted, the rows holding the admin will hold no admin until a new one is assigned.
ReportAccess	ra_emp_id_fk	CASCADE	SET NULL	If the employee is deleted, the rows holding the employee will hold no employees until a new one is assigned.
AttackersList	vector_id_fk	CASCADE	CASCADE	If the attack vector is deleted, the rows holding the vector shall be deleted as well.
AttackersList	mactor_id_fk	CASCADE	CASCADE	If the actor is deleted, the rows holding the actor shall be deleted as well.
AlertView	av_alert_id_fk	CASCADE	CASCADE	If the alert is deleted, the rows holding the alert shall be deleted as well
AlertView	av_emp_id_fk	CASCADE	SET NULL	If an employee is deleted, the rows holding the employee will hold no employees until

				a new one is assigned.
AlertView	av_admin_id_fk	CASCADE	SET NULL	If an admin is deleted, the rows holding the admin will hold no admins until a new one is assigned.
DiscoverList	dl_disc_id_fk	CASCADE	CASCADE	If a discovery method is deleted, the rows holding the method shall be deleted as well
DiscoverList	dl_threat_id_fk	CASCADE	SET NULL	If a threat is deleted, the rows holding the threat will hold no threats.
DiscoverList	dl_vul_id_fk	CASCADE	SET NULL	If a vulnerability is deleted, the rows holding the vulnerability will hold no vulnerabilities.
Teams	admins_id_fk	CASCADE	SET NULL	If an admin is deleted, the rows holding the admin will hold no admin until a new one is assigned.
Teams	employee_id_fk	CASCADE	SET NULL	If an employee is deleted, the rows holding the employee will hold no employees until a new one is assigned.
ForumSolutions	forum_sol_id_fk	CASCADE	CASCADE	If a forum is deleted, the rows holding the forum shall be deleted as well.

ForumSolutions	fs_solution_id_fk	CASCADE	CASCADE	If a solution is deleted, the rows holding the solution shall be deleted as well
DMReportList	report_id_fk	CASCADE	CASCADE	If a report is deleted, the rows holding the reports shall be deleted as well
DMReportList	discovery_id_fk	CASCADE	CASCADE	If a discovery method is deleted, the rows holding the method shall be deleted as well