CyberGuard

Alec Nagal | 918485625 | itsmeAlec

Checkpoint #	Date Submitted
Milestone 1 Checkpoint 1	09/18/2023
Milestone 1 Checkpoint 2	10/03/2023

Table of Contents

Product Description

The motivation behind creating this database system is to address the pressing need for a comprehensive Threat Intelligence Platform that offers a holistic solution to the evolving cybersecurity landscape. I aim to provide organizations with a powerful tool to effectively manage and mitigate cybersecurity threats by consolidating and analyzing threat data from diverse sources. This platform seeks to solve the challenges of real-time threat monitoring, rapid incident response, and proactive threat intelligence sharing.

My Threat Intelligence Platform, tentatively named "CyberGuard," will serve as a centralized hub for collecting, analyzing, and disseminating threat intelligence data. It will utilize advanced AI and machine learning algorithms to identify emerging threats, vulnerabilities, and attack patterns. A unique feature of CyberGuard is its adaptive threat correlation engine, which continuously learns and adapts to new threat vectors, improving threat detection accuracy over time.

Five key use cases for CyberGuard include real-time threat detection and alerts, automated incident response orchestration, collaborative threat intelligence sharing among organizations, threat hunting and forensics, and compliance reporting. In each case, the platform's AI-driven threat analysis and automated workflows will play a crucial role in enhancing an organization's security posture.

Existing software tools or products in the market that would greatly benefit from integrating with CyberGuard include Security Information and Event Management (SIEM) solutions and Security Orchestration, Automation, and Response (SOAR) platforms. SIEM tools can leverage CyberGuard's enriched threat intelligence data to enhance their detection capabilities, while SOAR platforms can benefit from seamless integration for automated incident response workflows. The synergy between these tools and CyberGuard would significantly improve an organization's ability to detect, respond to, and mitigate cybersecurity threats.

Functional Requirements

User:

1.1. A user shall be able to register for a CyberGuard account.
1.2. A user shall log in securely using two-factor authentication.
1.3. A user shall reset their password if forgotten.
1.4. A user shall be assigned a unique user ID upon registration.
1.5. A user shall update their profile information, including contact details.
1.6. A user shall view their security dashboard upon login.
1.7. A user shall receive real-time threat alerts based on their preferences.
1.8. A user shall manage their subscription plan.

Administrator:

2.1. An administrator shall create user accounts.
2.2. An administrator shall manage user accounts.
2.3. An administrator shall define access levels for users.
2.4. An administrator shall define permissions for users.
2.5. An administrator shall approve new threat intelligence feeds.
2.6. An administrator shall monitor system health.
2.7. An administrator shall generate compliance reports.
2.8. An administrator shall manage system configuration settings.
2.9. An administrator shall configure automated incident response workflows.
2.10. An administrator shall manage integration with other security tools.

Threat Analyst:

3.1. A threat analyst shall investigate detected threats.
3.2. A threat analyst shall create custom threat detection rules.
3.3. A threat analyst shall manage custom threat detection rules.
3.4. A threat analyst shall collaborate with other analysts on threat analysis..
3.5. A threat analyst shall access historical threat data for analysis.
3.6. A threat analyst shall receive automated threat intelligence recommendations.
3.7. A threat analyst shall generate threat reports for stakeholders.
3.8. A threat analyst shall participate in threat intelligence sharing networks.

Integration Service:

4.1. The integration service shall ingest threat data from external sources.
4.2. The integration service shall normalize incoming threat data.
4.3. The integration service shall support various threat data formats (e.g., STIX/TAXII).
4.4. The integration service shall ensure data privacy during integration.
4.5. The integration service shall provide APIs for third-party tool integration.

4.6. The integration service shall automatically update threat indicators.

Alerting System:
5.1. The alerting system shall send real-time threat alerts to users.
5.2. The alerting system shall support alert filtering.
5.3. The alerting system shall use different communication channels (email, SMS, etc.).
5.4. The alerting system shall allow users to dismiss alerts.
5.5. The alerting system shall escalate critical alerts to designated personnel.
5.6. The alerting system shall record alert acknowledgment timestamps.

Threat Correlation Engine:
6.1. The threat correlation engine shall continuously analyze incoming threat data.
6.2. The threat correlation engine shall identify anomalies.
6.3. The threat correlation engine shall assign risk scores to detected threats.
6.4. The threat correlation engine shall correlate threats across different data sources.
6.5. The threat correlation engine shall provide visualizations of threat correlations.
6.6. The threat correlation engine shall adapt its correlation algorithms.

Incident Response Workflow:
7.1. The incident response workflow shall automatically trigger actions based on threat severity.
7.2. The incident response workflow shall initiate containment actions (e.g., isolating affected systems).
7.3. The incident response workflow shall create incident tickets for tracking.
7.4. The incident response workflow shall notify relevant personnel about ongoing incidents.
7.5. The incident response workflow shall document actions taken during incident response.
7.6. The incident response workflow shall provide post-incident analysis reports.

Data Privacy and Compliance:
8.1. The system shall encrypt sensitive threat data at rest.
8.2. The system shall encrypt sensitive threat data in transit.
8.3. The system shall support data anonymization techniques.
8.4. The system shall provide audit logs for compliance reporting.
8.5. The system shall support user consent management for data sharing.

Customizable Threat Intelligence Feeds:
9.1. Users shall manage various threat intelligence feeds.
9.2. Users shall customize threat feed configurations..
9.3. Users shall specify threat feed sources.
9.4. Users shall enable/disable specific threat indicators from feeds.
9.5. Users shall receive timely updates on changes to threat intelligence feeds.

Collaborative Threat Analysis:
10.1. Users shall collaborate on threat analysis by sharing insights.
10.2. Users shall engage in threaded discussions on specific threats.
10.3. Users shall collectively prioritize threats based on consensus.
10

.4. Users shall have access to shared threat analysis reports.
10.5. Users shall be able to assign threat analysis tasks to team members.

Historical Threat Data Analysis:
11.1. Users shall query historical threat data using various filters.
11.2. Users shall visualize historical threat trends.
11.3. Users shall export historical threat data for offline analysis.
11.4. Users shall conduct statistical analysis on historical data.
11.5. Users shall compare current threat data.
11.5. Users shall compare historical threat data.

Subscription Management:
12.1. Users shall manage their subscription plans.
12.2. Users shall view billing history.
12.3. Users shall cancel or suspend their subscription as needed.
12.4. Users shall receive automated subscription renewal reminders.
12.5. Users shall update payment information securely.

APIs for Third-Party Integrations:
13.1. The system shall provide well-documented APIs for integration with other security tools.
13.2. APIs shall support real-time data exchange.
13.3. Users shall generate API keys for secure integration.
13.4. API usage shall be monitored for security.

Real-time Threat Intelligence Recommendations:

14.1. Users shall receive AI-driven recommendations for mitigating specific threats.
14.2. Recommendations shall be based on threat severity.
14.3. Users shall have the option to automate recommended actions.
14.4. Users shall provide feedback on the effectiveness of recommendations.
14.5. Users shall track the status of actions initiated from recommendations.

Customizable Compliance Reports:

15.1. Users shall generate compliance reports tailored to specific regulations.
15.2. Reports shall include data on threat detection, incident response, and user access.
15.3. Users shall schedule automated report generation.
15.4. Reports shall be exportable in various formats (e.g., PDF, CSV).
15.5. Users shall archive compliance reports for historical reference.

Advanced Threat Indicator Search:

16.1. Users shall perform advanced searches on threat indicators using complex queries.
16.2. Users shall save search queries.
16.3. Users shall visualize search results using interactive charts.
16.4. Users shall export search results for further analysis.
16.5. Users shall set up alert notifications based on saved search criteria.

Collaborative Threat Intelligence Sharing:

17.1. Users shall participate in threat intelligence sharing communities.
17.2. Users shall submit threat intelligence to share with trusted partners.
17.3. Users shall access shared threat intelligence reports.
17.4. Users shall rate the quality of shared threat intelligence.
17.5. Users shall collaborate on joint threat response actions.

Data Export and Integration with SIEM:

18.1. Users shall export threat reports to third-party SIEM solutions.
18.2. Integration with SIEM shall support standardized formats (e.g., CEF, JSON).
18.3. Users shall configure data mappings for SIEM integration.
18.4. Users shall monitor the status of data export to SIEM.
18.5. SIEM integration shall enhance real-time security monitoring.

Customizable Dashboards and Widgets:

19.1. Users shall personalize their security dashboards with widgets of their choice.
19.2. Widgets shall display real-time threat data, analytics, and charts.

19.3. Users shall arrange widgets according to their preference.
19.4. Users shall share customized dashboards with team members.
19.5. Widgets shall support drill-down capabilities for in-depth analysis.

Machine Learning Model Training:
20.1. Administrators shall initiate machine learning model training sessions.
20.2. Model training shall utilize historical threat data for accuracy.
20.3. Users shall monitor the progress status of model training.
20.4. Trained models shall continuously improve threat detection accuracy.
20.5. Users shall validate model training results.

Non-Functional Requirements

Performance:

1.1. The database system shall support high concurrent user access, with a minimum of 1,000 simultaneous users.
1.2. Response times for threat data queries shall be consistently under 500 milliseconds.
1.3. The database system shall provide efficient indexing and query optimization techniques to enhance query performance.
1.4. The system shall maintain historical threat data for a minimum of five years without significant degradation in query performance.

Storage:

2.1. The database system shall allocate sufficient storage to accommodate at least 100 million threat indicators and associated metadata.
2.2. Data compression techniques shall be employed to optimize storage efficiency.
2.3. The system shall provide options for both on-premises and cloud-based storage.
2.4. The database shall support automated data archiving and purging to manage storage growth efficiently.

Security:

3.1. All user data, including threat intelligence feeds and user profiles, shall be encrypted at rest using industry-standard encryption algorithms.
3.2. User authentication shall require strong, multi-factor authentication (MFA) mechanisms.
3.3. Data access control shall be role-based, with fine-grained permissions.
3.4. Audit logs shall capture all database transactions and access attempts for security monitoring.
3.5. Threat data ingested from external sources shall undergo validation and sanitization to prevent injection attacks.
3.6. The database shall enforce data consistency and integrity through referential constraints and data type validation.
3.7. Regular security assessments and penetration testing shall be conducted to identify and address vulnerabilities.

Scalability:

4.1. The database system shall support horizontal scaling to accommodate increased data and user load.
4.2. The system shall allow for the addition of new threat intelligence feeds and integration services without significant disruption.

4.3. Scalability shall be achieved through load balancing and distributed database architecture.
4.4. Performance shall linearly scale with the addition of hardware resources or nodes.
4.5. The system shall provide auto-scaling capabilities to handle sudden spikes in traffic.

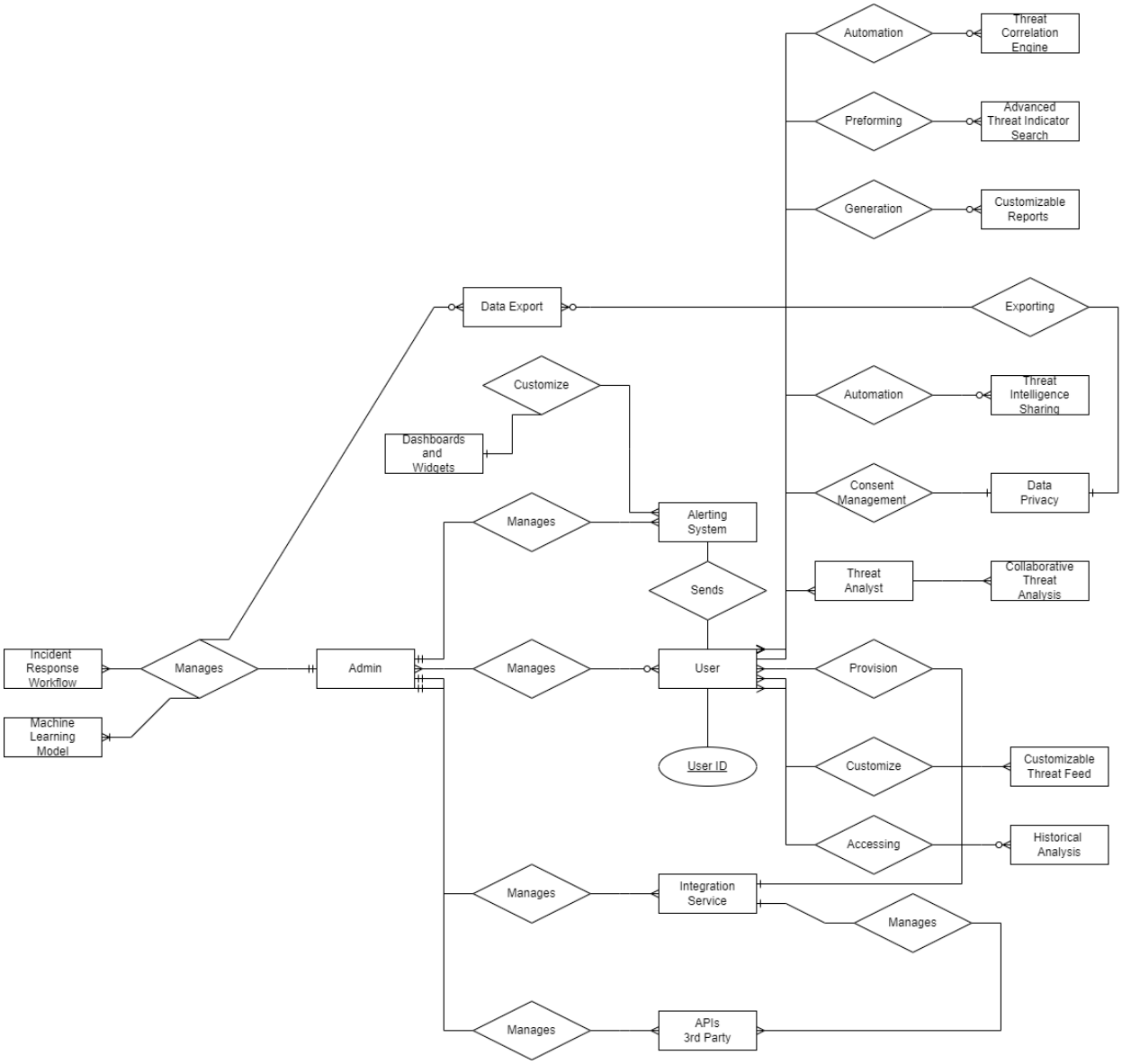
Availability and Reliability:
5.1. The database system shall provide 99.9% uptime availability for core services.
5.2. High availability (HA) and failover mechanisms shall be implemented to minimize service interruptions.
5.3. Regular maintenance and updates shall be performed during scheduled maintenance windows to minimize downtime.
5.4. The database shall support automated backup and disaster recovery procedures.
5.5. Data redundancy and replication shall ensure data availability in the event of hardware failures.

Compliance:
6.1. The database system shall comply with industry-specific cybersecurity standards (e.g., NIST, ISO 27001).
6.2. Compliance reports and audit trails shall be readily available for regulatory assessments.
6.3. Data retention policies shall align with data protection regulations, ensuring lawful data handling.

Usability and Accessibility:
7.1. The database system shall provide a user-friendly and intuitive web-based interface.
7.2. The platform shall be accessible from a variety of devices and browsers.
7.3. User documentation and online help resources shall be comprehensive and accessible.
7.4. Accessibility features shall comply with WCAG 2.1 guidelines for users with disabilities.

Data Backup and Recovery:
8.1. Daily automated data backups shall be performed, and backups shall be retained for a minimum of 30 days.
8.2. Backup and recovery procedures shall be tested regularly to ensure data integrity and availability.
8.3. Point-in-time recovery shall be supported to restore the database to a specific state in case of data corruption or errors.

Entity Relation Diagram



Entity Descriptions

1. User (Strong)

- user_id: Primary key, numeric
- username: Alphanumeric
- email: Alphanumeric, email domain
- password_hash: Alphanumeric (hashed for security)
- two_factor_enabled: Boolean
-last_login: Timestamp

2. Administrator (Strong)

- admin_id: Primary key, numeric
- username: Alphanumeric
- email: Alphanumeric, email domain
- password_hash: Alphanumeric (hashed for security)
- last_login: Timestamp
- access_level: Alphanumeric (e.g., 'Admin', 'Super Admin')

3. Threat Analyst (Strong)

- analyst_id: Primary key, numeric
- username: Alphanumeric
- email: Alphanumeric, email domain
- password_hash: Alphanumeric (hashed for security)
- last_login: Timestamp
- department: Alphanumeric (e.g., 'Security Operations', 'Threat Intelligence')

4. Integration Service (Strong)

- service_id: Primary key, numeric
- name: Alphanumeric (e.g., 'Data Ingestion Service', 'API Gateway')
- description: Alphanumeric
- integration_type: Alphanumeric (e.g., 'External Data Source', 'Internal API')
- last_updated: Timestamp

5. Alerting System (Strong)

- system_id: Primary key, numeric
- name: Alphanumeric (e.g., 'Real-time Alerting', 'Notification Engine')
- description: Alphanumeric
- communication_channels: Alphanumeric (e.g., 'Email', 'SMS', 'Push Notification')
- last_triggered: Timestamp
- acknowledged: Boolean

6. Threat Correlation Engine (Strong)
- engine_id: Primary key, numeric
- name: Alphanumeric (e.g., 'Correlation Engine', 'Risk Scoring Engine')
- description: Alphanumeric
- correlation_algorithm: Alphanumeric (e.g., 'Pattern Matching', 'Behavior Analysis')
- last_run: Timestamp
- risk_score: Numeric

7. Incident Response Workflow (Strong)
- workflow_id: Primary key, numeric
- name: Alphanumeric (e.g., 'Automated Incident Response', 'Manual Workflow')
- description: Alphanumeric
- status: Alphanumeric (e.g., 'Active', 'Completed')
- start_time: Timestamp
- end_time: Timestamp

8. Data Privacy and Compliance (Strong)
- compliance_id: Primary key, numeric
- name: Alphanumeric (e.g., 'Data Encryption', 'Consent Management')
- description: Alphanumeric
- compliance_type: Alphanumeric (e.g., 'Encryption', 'Data Anonymization')
- audit_logs_enabled: Boolean
- last_audit_timestamp: Timestamp

9. Customizable Threat Intelligence Feeds (Strong)
- feed_id: Primary key, numeric
- name: Alphanumeric (e.g., 'Custom Threat Feeds', 'External Threat Data')
- description: Alphanumeric
- feed_type: Alphanumeric (e.g., 'RSS', 'API')
- last_updated: Timestamp
- enabled: Boolean

10. Collaborative Threat Analysis (Strong)
- analysis_id: Primary key, numeric
- title: Alphanumeric
- description: Alphanumeric
- status: Alphanumeric (e.g., 'Open', 'Closed')
- priority: Alphanumeric (e.g., 'High', 'Low')
- created_at: Timestamp
- assigned_to: Alphanumeric

11. Historical Threat Data Analysis (Strong)
- analysis_id: Primary key, numeric
- date: Timestamp
- analysis_type: Alphanumeric (e.g., 'Trend Analysis', 'Statistical Analysis')
- result_summary: Alphanumeric
- created_by: Alphanumeric
- data_exported: Boolean
- export_format: Alphanumeric (e.g., 'CSV', 'PDF')

12. Subscription Management (Strong)
- subscription_id: Primary key, numeric
- user_id: Foreign key, numeric (relating to the User entity)
- plan_name: Alphanumeric (e.g., 'Basic', 'Premium')
- billing_history: Alphanumeric
- subscription_status: Alphanumeric (e.g., 'Active', 'Suspended')
- renewal_reminder_sent: Boolean
- payment_information: Alphanumeric (e.g., Credit Card, PayPal)

13. APIs for Third-Party Integrations (Strong)
- api_id: Primary key, numeric
- api_name: Alphanumeric
- description: Alphanumeric
- integration_type: Alphanumeric (e.g., 'REST API', 'Webhooks')
- documentation_link: Alphanumeric (URL)
- api_key_generation: Boolean
- usage_monitoring: Boolean

14. Real-time Threat Intelligence Recommendations (Strong)
- recommendation_id: Primary key, numeric
- user_id: Foreign key, numeric (relating to the User entity)
- threat_type: Alphanumeric
- severity: Alphanumeric (e.g., 'Critical', 'Low')
- recommended_action: Alphanumeric
- action_status: Alphanumeric (e.g., 'Pending', 'Completed')
- feedback_rating: Numeric (e.g., 1-5)
- action_timestamp: Timestamp

15. Customizable Compliance Reports (Strong)
- report_id: Primary key, numeric
- report_name: Alphanumeric
- regulation_type: Alphanumeric (e.g., 'GDPR', 'HIPAA')
- generation_schedule: Alphanumeric (e.g., 'Weekly', 'Monthly')
- export_format: Alphanumeric (e.g., 'PDF', 'CSV')
- archived: Boolean
- archived_timestamp: Timestamp

16. Advanced Threat Indicator Search (Strong)
- search_id: Primary key, numeric
- user_id: Foreign key, numeric (relating to the User entity)
- query: Alphanumeric
- saved: Boolean
- visualization_type: Alphanumeric (e.g., 'Charts', 'Graphs')
- notification_enabled: Boolean
- notification_criteria: Alphanumeric

17. Collaborative Threat Intelligence Sharing (Strong)
- sharing_id: Primary key, numeric
- community_name: Alphanumeric
- user_id: Foreign key, numeric (relating to the User entity)
- shared_content: Alphanumeric
- quality_rating: Numeric
- shared_timestamp: Timestamp
- collaboration_status: Alphanumeric (e.g., 'Active', 'Inactive')

18. Data Export and Integration with SIEM (Strong)
- export_id: Primary key, numeric
- user_id: Foreign key, numeric (relating to the User entity)
- siem_system: Alphanumeric (e.g., 'Splunk', 'QRadar')
- export_status: Alphanumeric (e.g., 'Enabled', 'Disabled')
- data_format: Alphanumeric (e.g., 'CEF', 'JSON')
- data_mapping_configuration: Alphanumeric
- export_timestamp: Timestamp
- enhancement_enabled: Boolean

19. Customizable Dashboards and Widgets (Strong)
- dashboard_id: Primary key, numeric
- user_id: Foreign key, numeric (relating to the User entity)