Artificial Intelligence In Cyber Security

By

Sanath Meshram

"Artificial intelligence is not a substitute for human intelligence; it is a tool to amplify human creativity and ingenuity."

1. Abstract

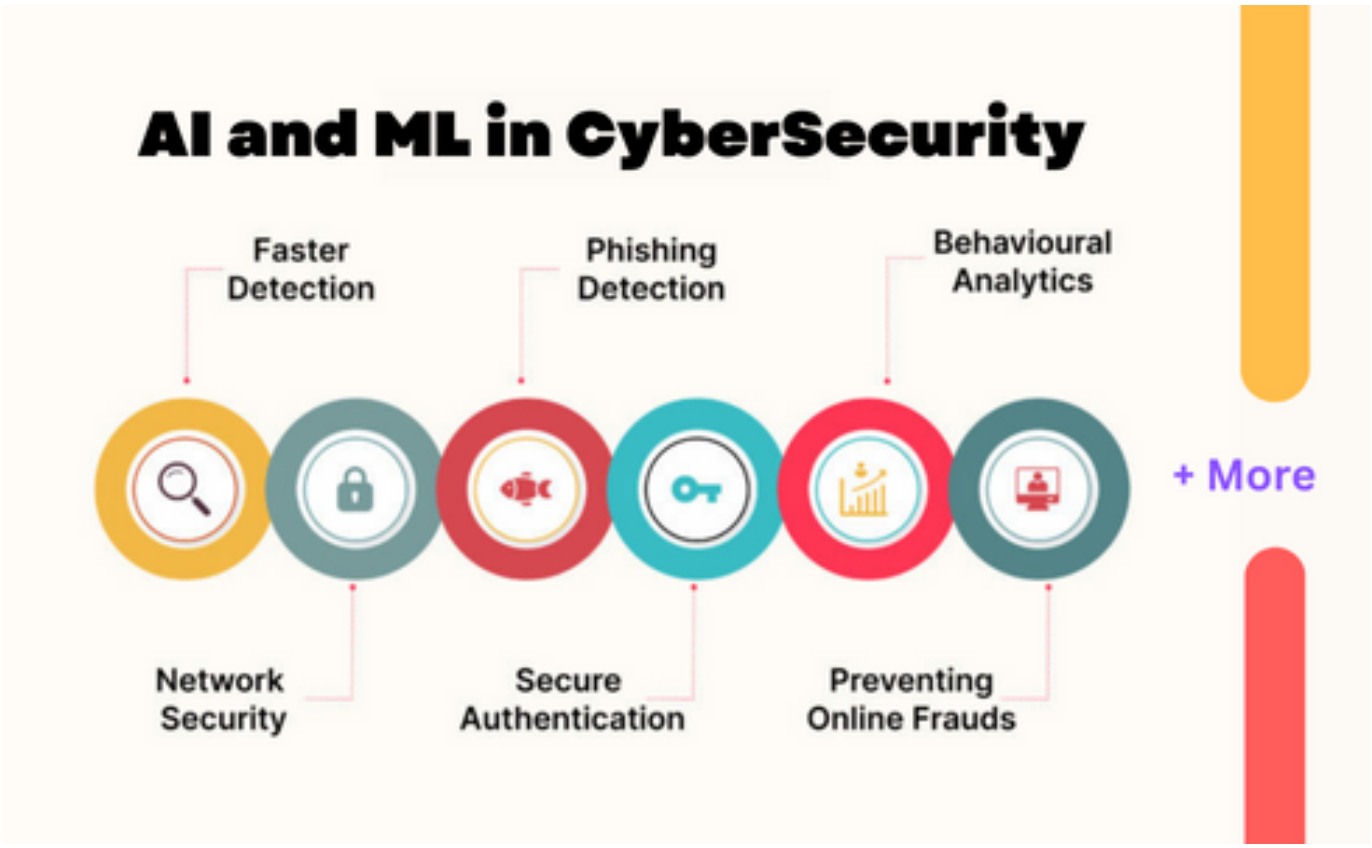
This abstract summarizes the pivotal role of Artificial Intelligence (AI) and Machine Learning (ML) in fortifying cybersecurity. The integration of AI and ML technologies significantly enhances threat detection, prevention, and response. From anomaly recognition and signature-based identification to behavioral analysis, phishing prevention, and adaptive access controls, these technologies bolster cybersecurity measures across various domains. The abstract also highlights the accelerated incident response, automated vulnerability management, and the role of AI in network security and threat intelligence. In conclusion, the paper underscores the transformative impact of AI and ML in fortifying cybersecurity against evolving threats.

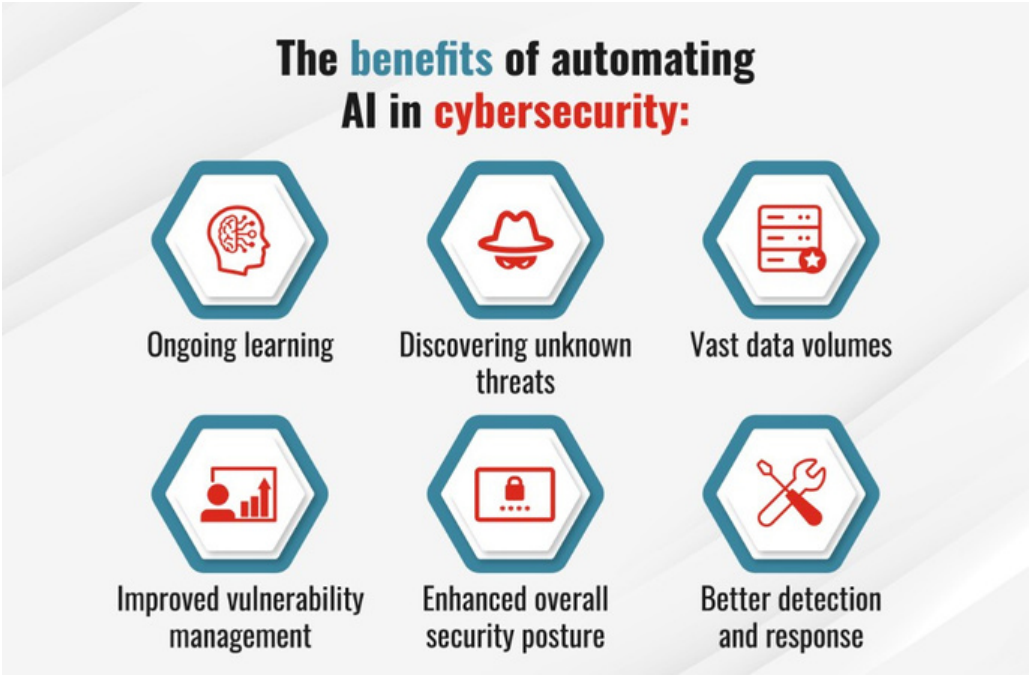
2. Introduction

As the digital landscape evolves, the sophistication and diversity of cyber threats continue to pose formidable challenges to organizations worldwide. In response to this dynamic threat environment, the integration of Artificial Intelligence (AI) and Machine Learning (ML) has emerged as a cornerstone in the realm of cybersecurity. This paper provides a succinct exploration of how AI and ML technologies contribute to fortifying cybersecurity measures. From advanced threat detection mechanisms to proactive prevention strategies and expedited incident response, the following sections delineate the transformative impact of these technologies across diverse domains, underscoring their pivotal role in safeguarding against contemporary cyber threats.

Cyber security is important because it encompasses everything that relates to protecting our data from cyber attackers who want to steal this information and use it to cause harm. This can be sensitive data, governmental and industry information, personal information, personally identifiable information (PII), intellectual property, and protected health information (PHI). Therefore, they are obviously vulnerable to cyber attacks. A cyber attack is an attack launched from one or more computers against cyber attacks is either to disable the target computer, or take the services offline, or get access to the target computer’s data. In response to the issues, artificial intelligence tools are commonly implemented to deal with cyber threats. Artificial intelligence (AI) has helped more organizations to improve the security posture effectively and reduce the breach risks. Machine learning and artificial intelligence are the essential tools in technology for information security as it helps companies and individuals to check and analyze the threats posed to the organization .

- **General Flow**





- # Problem Statements :

In the face of an ever-evolving digital landscape, the escalating complexity and diversity of cyber threats pose a critical challenge to the security of organizations. Traditional cybersecurity measures, while effective to a certain extent, often fall short in rapidly detecting, preventing, and responding to sophisticated attacks. The pressing need for innovative solutions has given rise to a significant problem in contemporary cybersecurity—how to adapt to and combat advanced and dynamic cyber threats effectively. This problem statement underscores the urgency for integrating Artificial Intelligence (AI) and Machine Learning (ML) technologies as a transformative approach to address the shortcomings of conventional cybersecurity measures and fortify organizations against the relentless and evolving nature of cyber threats.

- # How AI is used in cybersecurity :

Artificial intelligence in cybersecurity is considered to be a superset of disciplines like machine learning and deep learning cyber security, but it does have its own role to play. AI at its core is concentrated on “success” with “accuracy” carrying less weight. Natural responses in elaborate problem-solving are the ultimate goal. In a true execution of AI, actual independent decisions are being made. Its programming is designed for finding the ideal solution in a situation, rather than just the hard-logical conclusion of the dataset .

To further explain, it’s best to understand how modern AI and its underlying disciplines work currently. Autonomous systems are not within the scope of widely mobilized systems, especially in the field of cybersecurity. These self-directed systems are what many people commonly associate with AI. However, AI systems that either assist or augment our protective services are practical and available.

The ideal role of AI in cybersecurity is the interpretation of the patterns established by machine learning algorithms. Of course, it's not yet possible for modern-day AI to interpret results with the abilities of a human yet. Work is being done to help develop this field in pursuit of humanlike frameworks, but true AI is a distant goal that requires machines to take abstract concepts across situations to reframe them. In other words, this level of creativity and critical thought is not as close as the AI rumors would like you to believe.

- # How machine learning is used in cybersecurity :

Machine learning security solutions are different from what people envision to be of the artificial intelligence family. That said, they are easily the strongest cybersecurity AI tools we have to-date. In the scope of this technology, data patterns are used to reveal the likelihood that an event will occur — or not.

Machine learning security solutions are different from what people envision to be of the artificial intelligence family. That said, they are easily the strongest cybersecurity AI tools we have to-date. In the scope of this technology, data patterns are used to reveal the likelihood that an event will occur — or not.

ML is somewhat opposite to that of true AI in some respects. Machine learning is particularly “accuracy” driven, but not as focused on “success.” What this means is that ML proceeds intending to learn from a task-focused dataset. It concludes by finding the most optimal performance of the given task. It will pursue the only possible solution based on the given data, even if it’s not the ideal one. With ML, there is no true interpretation of the data, which means this responsibility still falls on human task forces.

Machine learning excels at tedious tasks like data pattern identification and adaptation. Humans are not well suited to these types of tasks due to task fatigue and a generally low tolerance for monotony. So, while the interpretation of data analysis is still in human hands, machine learning can assist in framing the data in a readable, dissection-ready presentation. Machine learning cybersecurity comes in a few different forms, each with its own unique benefits:

Data classifying

Data classifying works by using preset rules to assign categories to data points. Labeling these points is an important part of building a profile on attacks, vulnerabilities, and other aspects of proactive security. This is fundamental to the intersection of machine learning and cyber security.

Data clustering

Data clustering takes the outliers of classifying preset rules, placing them into “clustered” collections of data with shared traits or odd features. For example, this can be used when analyzing attack data that a system is not already trained for. These clusters can help determine how an attack happened, as well as, what was exploited and exposed.

- # Market / Business Need Assessment :

Cybersecurity faces a myriad of threats that are constantly evolving as technology advances. Leveraging Artificial Intelligence (AI) and Machine Learning (ML) can significantly enhance the ability to detect, prevent, and respond to these threats. Here are some potential threats in the field of cybersecurity and how AI/ML can help address them:

Malware and Ransomware:

Threat: Malicious software and ransomware attacks can compromise systems and data integrity, leading to unauthorized access or data encryption.
AI/ML Solution: AI can analyze patterns, behaviors, and anomalies in real-time, detecting new and previously unknown malware. ML algorithms can improve the accuracy of identifying malicious code and behaviors, enabling proactive defense mechanisms.

Phishing Attacks:

Threat: Phishing attacks target individuals through deceptive emails or messages, aiming to trick them into revealing sensitive information.
AI/ML Solution: AI-powered email filtering systems can analyze content, sender behavior, and historical data to identify and block phishing attempts. ML models can learn from patterns and continuously adapt to new phishing tactics.

Insider Threats:

Threat: Insider threats involve malicious actions or negligence from employees or authorized users, leading to unauthorized access or data leaks.
AI/ML Solution: Behavioral analysis using ML helps establish a baseline of normal user behavior. AI systems can detect anomalies, identifying potential insider threats and providing alerts for further investigation.

Zero-Day Exploits:

Threat: Zero-day exploits target vulnerabilities in software that are unknown to the vendor or unpatched, making them particularly challenging to defend against.
AI/ML Solution: ML algorithms can analyze network and system behaviors to identify unusual patterns that may indicate a zero-day exploit. AI can also assist in the rapid development and deployment of patches or mitigations.

DDoS Attacks:

Threat: Distributed Denial of Service (DDoS) attacks overwhelm a system or network with traffic, causing service disruption.
AI/ML Solution: AI can analyze network traffic in real-time to identify patterns associated with DDoS attacks. ML models can distinguish between legitimate and malicious traffic, enabling automated response mechanisms to mitigate the impact.

Credential Theft:

Threat: Attackers often steal usernames and passwords, either through phishing or other means, t o gain unauthorized access.
AI/ML Solution: AI-driven systems can detect abnormal user behavior patterns, identifying potential unauthorized access. ML models can continuously learn and adapt to new tactics used by attackers in stealing and using credentials.

Data Exfiltration:

Threat: Unauthorized extraction of sensitive data from an organization's network.
AI/ML Solution: AI can monitor network traffic for unusual data transfer patterns and behaviors. ML models can identify anomalies indicative of data exfiltration and trigger alerts for immediate investigation.

IoT Vulnerabilities:

Threat: Insecure Internet of Things (IoT) devices can serve as entry points for cyber attacks.
AI/ML Solution: AI can monitor and analyze the behavior of IoT devices, detecting unusual activities that may indicate a security compromise. ML can provide predictive maintenance by identifying potential vulnerabilities in IoT devices.

Supply Chain Attacks:

Threat: Attackers compromise the software supply chain to introduce malicious code into trusted applications or systems.
AI/ML Solution: AI can analyze code repositories and detect anomalies or malicious patterns during the software development life cycle. ML can assist in identifying and mitigating potential threats within the supply chain.

Evasive Tactics:

Threat: Attackers often use evasive tactics to bypass traditional security measures.
AI/ML Solution: AI-driven systems can adapt to evolving threats by learning from historical data and identifying new attack patterns. ML models can continuously update their knowledge to stay ahead of sophisticated evasion techniques.
In summary, AI and ML play pivotal roles in strengthening cybersecurity defenses by providing advanced threat detection, automated response mechanisms, and continuous adaptation to emerging threats. Combining these technologies with traditional cybersecurity measures creates a robust defense strategy against the evolving threat landscape.

In summary, AI and ML play pivotal roles in strengthening cybersecurity defenses by providing advanced threat detection, automated response mechanisms, and continuous adaptation emerging threats. Combining these technologies with traditional cybersecurity measures creates a robust defense strategy against the evolving threat landscape

.

- # Business Model In Cybersecurity :

In the field of cybersecurity, various business models exist, ranging from traditional product and service offerings to more modern, subscription-based models. The complexity and dynamic nature of]cybersecurity threats have led to the development of diverse business models to address the evolving needs of organizations. Here are several business models commonly found in the cybersecurity industry:

Consulting and Advisory Services:

- **Description:** Cybersecurity consulting firms provide expert advice and guidance to organizations regarding their cybersecurity posture. This includes risk assessments, compliance audits, and strategic planning.
- **Revenue Model:** Hourly consulting fees, project-based fees, or retainer contracts.

Managed Security Services (MSSP):

- **Description:** MSSPs offer ongoing monitoring, management, and response to security incidents. They often provide services such as intrusion detection, firewall management, and threat intelligence.
- **Revenue Model:** Subscription-based fees, with pricing tiers based on the level of services offered.

Security Software Development:

- **Description:** Companies develop and sell cybersecurity software solutions, including antivirus programs, firewalls, encryption tools, and threat detection platforms.
- **Revenue Model:** License fees, subscription-based models, or a combination of both.

Incident Response Services:

- **Description:** Organizations specializing in incident response provide rapid assistance to clients facing cybersecurity incidents, helping them contain, analyze, and recover from security breaches.
- **Revenue Model:** Hourly rates for incident response services, retainer contracts, or subscription-based models.

Security Hardware Manufacturing:

- **Description:** Companies design and manufacture hardware devices dedicated to cybersecurity, such as firewalls, intrusion prevention systems, and secure networking equipment.
- **Revenue Model:** Sales of hardware devices, with additional revenue from maintenance contracts or software updates.

Security Training and Education:

- **Description:** Organizations provide cybersecurity training programs, workshops, and certifications to individuals and corporate teams to enhance their knowledge and skills.
- **Revenue Model:** Tuition fees, certification exam fees, and customized training packages.

Cybersecurity Insurance:

- **Description:** Insurance companies provide cybersecurity insurance policies that cover financial losses resulting from security breaches, data breaches, or other cyber incidents.
- **Revenue Model:** Premiums paid by organizations based on the level of coverage and assessed risk.

Biometric Security Solutions:

- **Description:** Companies develop and offer biometric authentication solutions, including fingerprint recognition, facial recognition, and iris scanning, to enhance access control and identity verification.
- **Revenue Model:** Sales of biometric devices, licensing fees, and subscription-based services.

IoT Security Solutions:

- **Description:** Businesses focus on securing Internet of Things (IoT) devices and networks, providing solutions to address the unique cybersecurity challenges associated with IoT.
- **Revenue Model:** Sales of IoT security software, consulting fees, and subscription-based services.

Cybersecurity Analytics and Threat Hunting:

- **Description:** Companies leverage advanced analytics and threat hunting techniques to identify and respond to cybersecurity threats proactively.
- **Revenue Model:** Subscription-based fees for access to analytics platforms and threat hunting services.

Selecting the appropriate business model often depends on factors such as the organization's core competencies, the target market, and the specific cybersecurity challenges it aims to address. Many cybersecurity companies also adopt a combination of these models to provide comprehensive solutions and meet the diverse needs of their clients.

- # Concept Generation :

Concept generation in the field of AI/ML in cybersecurity involves ideating innovative solutions, tools, or approaches that leverage artificial intelligence and machine learning to enhance security measures. Here are several concept ideas to inspire innovation in AI/ML cybersecurity:

1. **Adaptive Threat Intelligence Platform:**
   - **Concept:** Develop an AI-driven threat intelligence platform that dynamically adapts to emerging cyber threats. The system should continuously analyze global threat data, learn from new attack patterns, and update defenses in real-time.
   -
2. **Explainable AI for Security Decisions:**
   - **Concept:** Create AI models that provide clear explanations for their security decisions. This concept enhances transparency and trust in AI-driven security systems, making it easier for cybersecurity professionals to understand and validate the rationale behind automated decisions.
   -
3. **Behavioral Biometrics Authentication:**
   - **Concept:** Implement machine learning algorithms that continuously analyze user behavior patterns to enhance authentication. This could include keystroke dynamics, mouse movement, and other behavioral biometrics for more secure and user-friendly authentication
   - .
4. **Predictive Cyber Risk Scoring:**
   - **Concept**: Develop an AI-based system that predicts an organization's cyber risk score based on historical data, current vulnerabilities, and threat intelligence. This proactive approach helps organizations prioritize and mitigate potential risks.
   -
5. **AI-Powered Threat Hunting Bot:**
   - **Concept:** Create an autonomous threat hunting bot that uses machine learning to analyze network logs, identify anomalies, and proactively hunt for potential threats. The bot could work in conjunction with security analysts to enhance the efficiency of threat detection.
   -
6. **Dynamic Network Segmentation:**
   - **Concept:** Implement an AI-driven network segmentation solution that dynamically adjusts access controls based on real-time threat assessments. This concept enhances the ability to contain and isolate potential security breaches.

7 **Automated Incident Response with AI Orchestration:**
   - **Concept:** Develop an AI-driven incident response system that automates the initial stages of threat containment and mitigation. The system could integrate with various security tools and orchestrate responses based on predefined playbooks.

- # Concept Development :

- **AI-Driven Threat Intelligence Fusion:**
  Concept: Develop an AI system that aggregates and analyzes diverse threat intelligence feeds, providing real-time insights and proactive defense against emerging cyber threats.

- **Behavioral Biometrics for User Authentication:**
  Concept: Implement machine learning algorithms to analyze and authenticate users based on unique behavioral patterns, enhancing security and usability simultaneously.

- **Explainable AI in Security Decisions:**
  Concept: Create AI models that provide transparent and understandable explanations for their security decisions, fostering trust and aiding cybersecurity professionals in validation.

- **Predictive Cyber Risk Scoring:**
  Concept: Utilize AI to predict an organization's cyber risk score, leveraging historical data, vulnerability assessments, and threat intelligence for proactive risk management.

- **Automated Incident Response with AI Orchestration:**
  Concept: Develop an AI-driven incident response system that automates initial threat containment and mitigation, orchestrating responses through integration with various security tools.

- **Federated Learning for Collaborative Threat Detection:**
  Concept: Explore federated learning approaches for collaborative threat detection, allowing organizations to collectively train models without sharing sensitive data, enhancing collaboration.

- **Homomorphic Encryption for Secure ML Training:**
  Concept: Apply homomorphic encryption to secure sensitive data during machine learning model training, enabling organizations to leverage AI models without compromising data privacy.

- **AI-Powered Anomaly Detection in ICS:**
  Concept: Extend AI-driven anomaly detection to Industrial Control Systems (ICS), providing early detection of abnormal behavior for enhanced cybersecurity in critical infrastructure.

- **Zero-Trust AI Network Access Control:**
  Concept: Implement a zero-trust network access control system that leverages AI to continuously assess user and device behavior, minimizing trust assumptions within the network.

- **Blockchain-Enabled Threat Intelligence Sharing:**
  Concept: Develop a blockchain-based platform for secure and decentralized sharing of threat intelligence, ensuring integrity and transparency in collaborative cybersecurity efforts.

These concise concepts highlight the application of AI/ML in cybersecurity, addressing key areas such as threat intelligence, user authentication, risk management, incident response, and collaboration among organizations.

- # Final AI Service Prototype :

Creating a final AI service prototype requires a comprehensive understanding of the specific concept or solution you want to develop. Since we've discussed various AI/ML cybersecurity concepts, I'll provide a generic outline for building a final AI service prototype, incorporating elements from the previously discussed concepts. Let's consider an AI-Driven Threat Intelligence Fusion platform as an example:

- **AI-Driven Threat Intelligence Fusion Platform Prototype**

1. **Concept Overview**:
Develop a centralized platform that aggregates, analyzes, and provides real-time insights into cyber threats by fusing diverse threat intelligence feeds.

2**. Key Functionalities**:

a. ***Data Ingestion:***
- Integrate with multiple threat intelligence feeds, including open-source feeds, commercial feeds, and proprietary sources.
- Develop connectors or APIs for seamless data ingestion.

b. ***Data Processing and Enrichment:***
- Apply natural language processing (NLP) and machine learning algorithms to process and enrich threat data.
- Extract relevant entities, relationships, and contextual information from unstructured data.

c. ***Anomaly Detection:***
- Implement machine learning models for anomaly detection to identify unusual patterns or trends in incoming threat data.
- Utilize clustering algorithms to group similar threats and identify potential attack campaigns.

d. ***Real-time Threat Intelligence Dashboard:***
- Design a user-friendly dashboard that provides real-time visualizations of threat intelligence data.
- Include dynamic charts, graphs, and maps to highlight emerging threats and historical trends.

e. ***Explainable AI Interface:***
- Implement an explainable AI interface to provide clear explanations for threat assessments and prioritization.
- Allow users to understand the rationale behind threat scores and recommendations.

f. ***Collaboration Tools:***
- Integrate collaboration features, such as secure chat or discussion forums, to facilitate communication among cybersecurity teams.

- Enable sharing of insights and collaborative decision-making.

3. ***Technical Architecture:***

Illustrate the technical architecture through a schematic diagram:

Display data flow from various threat feeds to the central platform.

Highlight components such as data processing modules, machine learning models, and the user interface.

Showcase integration points with external cybersecurity tools.

4. ***User Interface Mockups:***

Develop interactive user interface mockups using prototyping tools.

Include screens for threat dashboards, threat details, collaboration features, and explainable AI interfaces.

Focus on creating an intuitive and user-friendly experience.

5. ***Security and Compliance:***

Implement security measures to protect the platform and its data.

Utilize encryption for data in transit and at rest.

Ensure compliance with relevant data protection regulations .

6. ***Testing and Validation:***

Conduct rigorous testing, including:

Unit testing for individual components.

Integration testing to ensure seamless interaction between modules.

User acceptance testing to gather feedback from potential users.

7. ***Feedback and Iteration:***

Collect feedback from cybersecurity professionals, threat analysts, and stakeholders.

Iterate on the prototype based on feedback, addressing any identified issues or areas for improvement.

8. ***Documentation:***

Provide comprehensive documentation, including user guides, system architecture documentation, and any necessary training materials.

9. ***Deployment Plan:***

Develop a deployment plan for the AI service prototype.

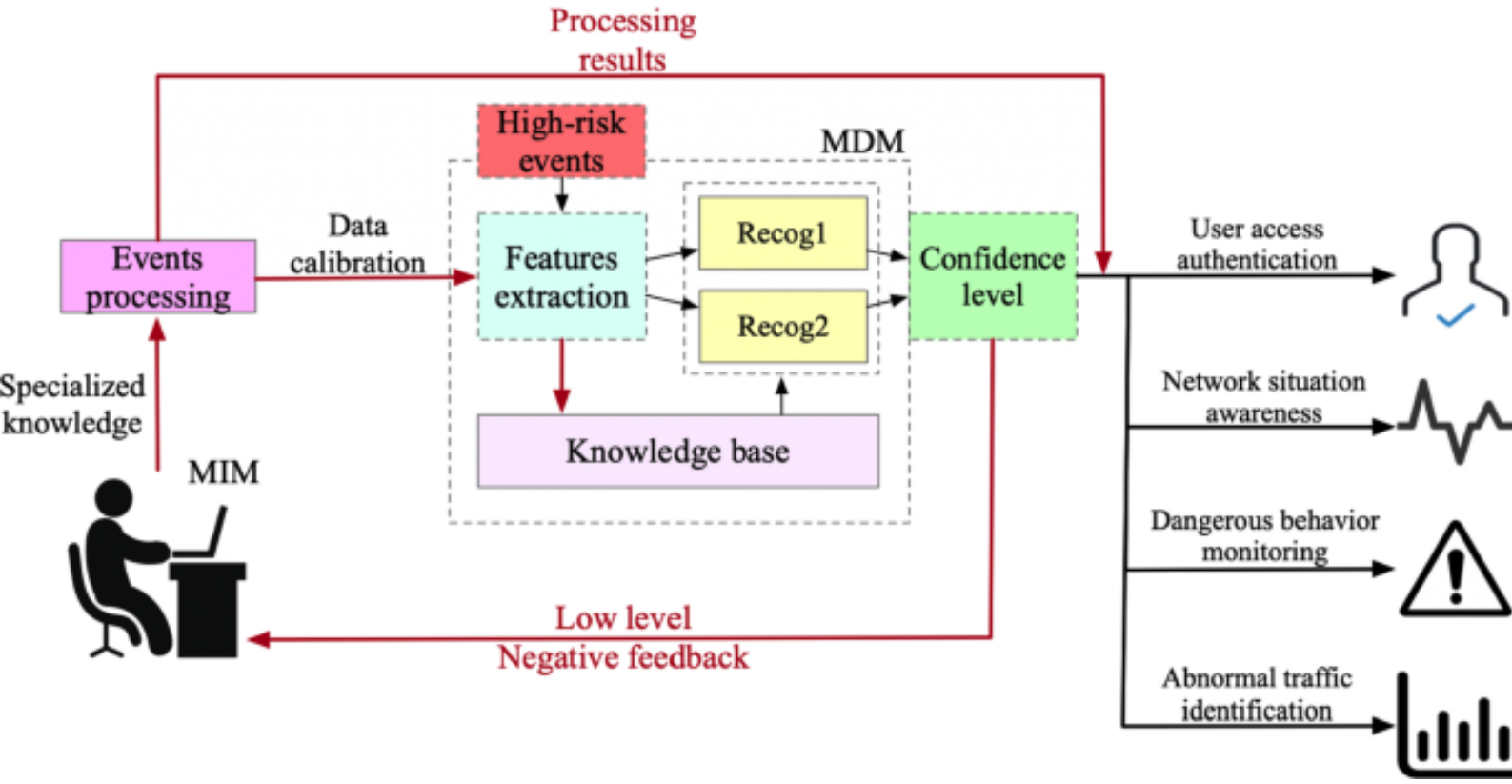
Consider whether it will be deployed on-premises or in the cloud, and outline the necessary steps for deployment.

10. ***Monitoring and Maintenance:***

Implement monitoring tools to track the performance of the AI service prototype.

Develop a maintenance plan for regular updates, bug fixes, and enhancements.

Building a final AI service prototype involves collaboration between AI developers, cybersecurity experts, and UX/UI designers. The iterative nature of the development process ensures that the prototype aligns with the envisioned AI-driven threat intelligence fusion platform, providing a practical solution for enhancing cybersecurity measures.


Processing results
High-risk events
MDM
Events processing
Data calibration
Features extraction
Recog1
Recog2
Confidence level
User access authentication
Specialized knowledge
Network situation awareness
Knowledge base
MIM
Dangerous behavior monitoring
Low level
Negative feedback
Abnormal traffic identification


6 WAYS TO IMPROVE CYBERSECURITY WITH AI AND ML
Enhance threat hunting
Detect intrusions and malware
Discover code vulnerabilities
Enhance network security
Detect phishing
Predict breach risks

• Technical specifications & Team required to develop

Developing an AI-driven Threat Intelligence Fusion Platform, as outlined in the previous response, requires a multidisciplinary team with expertise in various domains. Here are the technical specifications and the roles of the team members needed for the development of such a platform:

- **Technical Specifications:**

1. ***Programming Languages:***

Backend Development:

Python for machine learning model development and backend services.

Java, Node.js, or Python for building the core backend infrastructure.

Frontend Development:

JavaScript (React, Angular, or Vue.js) for creating a dynamic and interactive user interface.

Database:

MongoDB, PostgreSQL, or another suitable database for storing threat intelligence data.

Integration:

RESTful APIs for integrating with external threat intelligence feeds and cybersecurity tools.

2. ***Machine Learning and AI:***

Frameworks:

TensorFlow or PyTorch for developing machine learning models.

Scikit-learn for machine learning utilities.

Natural Language Processing (NLP):

NLTK or spaCy for text processing and NLP tasks.

Clustering Algorithms:

K-means or hierarchical clustering for grouping similar threats.

Explainable AI:

Implementing techniques to provide clear explanations for AI-driven decisions.

3. ***Security and Compliance:***

Encryption:

Utilize TLS/SSL for securing data in transit.

Implement encryption mechanisms for data at rest.

Access Control:

Role-based access control (RBAC) for managing user permissions.

Compliance:

Ensure compliance with data protection regulations (GDPR, HIPAA, etc.).

4. ***User Interface:***

Prototyping Tools:

Figma, Sketch, or Adobe XD for creating interactive user interface mockups.

Frontend frameworks (React, Angular, or Vue.js) for developing the actual user interface.

5. ***Infrastructure:***

Cloud Services:

AWS, Azure, or Google Cloud Platform for scalable and flexible cloud infrastructure.

Containerization:

Docker for containerization of application components.

Kubernetes for container orchestration.

6. ***Collaboration and Communication:***

Collaboration Tools:

Slack, Microsoft Teams, or similar tools for team communication.

Jira or Trello for project management and task tracking.

Team Structure:

1. ***Project Manager:***
   Oversees the entire project, ensuring it stays on schedule and within budget.
   Communicates with stakeholders and coordinates the efforts of the development team.
2. ***AI/ML Enginee***r:
   Specialized in machine learning and artificial intelligence.
   Develops and fine-tunes machine learning models for threat detection and anomaly analysis.
3. ***Backend Developers:***
   Build the core infrastructure, including data processing pipelines, APIs, and integration with external systems.
4. ***Frontend Developers:***
   Design and develop the user interface based on the provided mockups.
   Ensure a seamless and intuitive user experience.
5. ***Security Engineer:***
   Focuses on implementing security measures throughout the platform.
   Conducts security assessments and ensures compliance with data protection regulations.
6. ***Database Administrator:***
   Manages the database infrastructure, ensuring data integrity and availability.
   Optimizes database performance for efficient querying.
7. ***DevOps Engineer:***
   Responsible for the deployment, scaling, and monitoring of the application in a cloud environment.
   Implements CI/CD pipelines for automated testing and deployment.
8. ***UX/UI Designer:***
   Designs the user interface, ensuring a visually appealing and user-friendly experience.
   Creates interactive prototypes for user testing.
9. ***Data Scientist:***
   Works closely with the AI/ML engineer to preprocess and analyze data for training machine learning models.
   Assists in feature engineering and optimization.
10. ***QA/Test Engineer:***
    Conducts thorough testing of the entire platform, including unit testing, integration testing, and user acceptance testing.
    Identifies and reports bugs for resolution.
11. ***Legal and Compliance Specialist:***
    Ensures that the platform adheres to relevant data protection and privacy regulations.
    Provides guidance on legal considerations in the development process.

Collaboration and Workflow:

Agile Methodology:

Adopt an agile development methodology for flexibility and iterative improvements.
Regular Sprints and Stand-ups:
Conduct regular sprint planning meetings and daily stand-ups for effective communication within the team.

Continuous Integration/Continuous Deployment (CI/CD):

Implement CI/CD pipelines to automate testing and deployment processes.
Building a successful AI-driven Threat Intelligence Fusion Platform requires collaboration, communication, and expertise across these roles. The team should work cohesively to deliver a prototype that meets the requirements and provides valuable insights into the evolving cybersecurity landscape.

- Conclusion :

Conclusion In a scenario where malicious intelligence and cyber threats are rising exponentially, sophisticated cybersecurity strategies cannot be ignored. Also, security against large-scale threats, with very minimal resources, has been demonstrated from experience in DDoS prevention if smar approaches are used. Publications reviews indicate that studies into artificial neural networks offer findings of AI most widely relevant to cybersecurity. Neural network implementations continue on cybersecurity. For many fields where neural networks weren't the most appropriate technologies, sophisticated cybersecurity approaches are still desperately needed. Such fields include decision support, understanding of the situation, and control of information. The most interesting in this scenario is expert machine development. Too fast general artificial intelligence has advanced cannot be known, but a possibility remains that the perpetrators will exploit a new form of artificial intelligence as long as it is accessible. This is not obvious. In addition, the latest technology in the understanding, interpretation, and management of information, particularly in the area of computer learning, would significantly improve systems' cybersecurity capabilities.