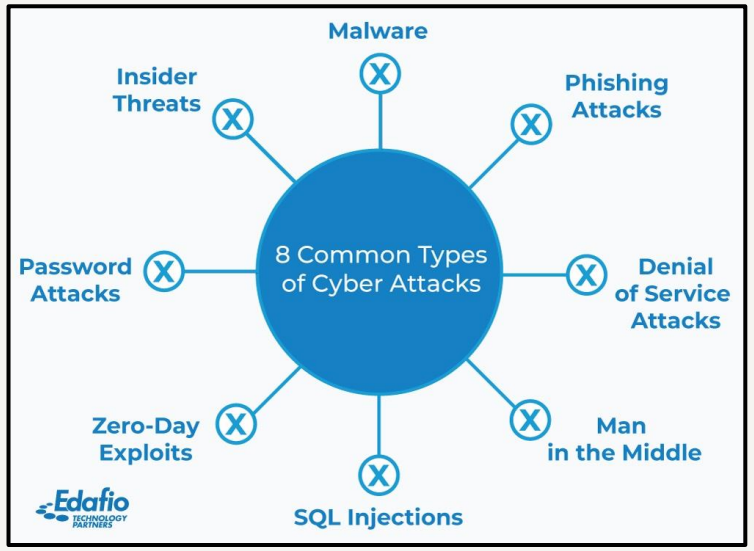
CyberGPT: Enhancing Cyber-threat Analysis using Generative-AI

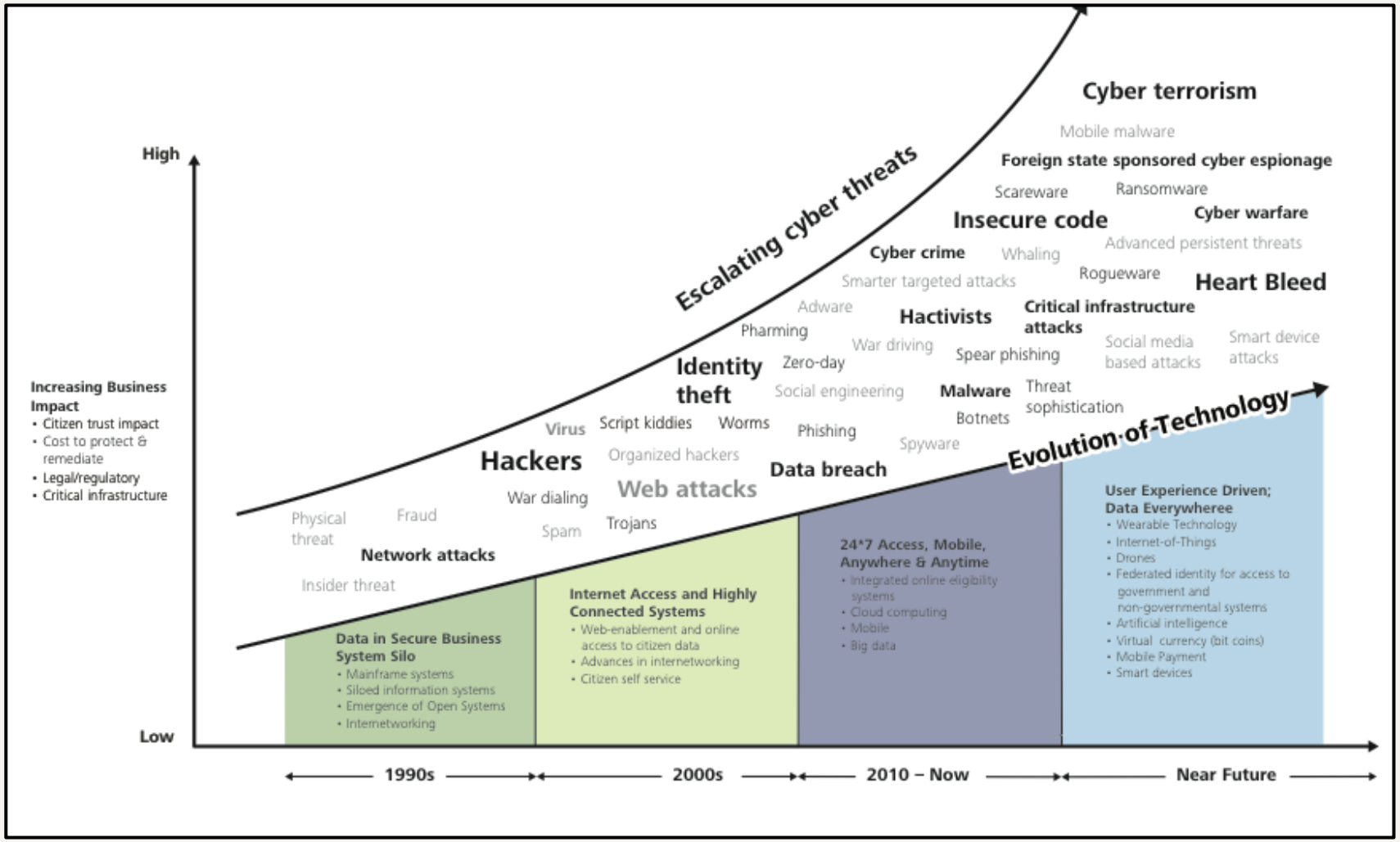
AI FOR BUSINESS - GROUP 5

- AKSHIT RAM PERSHAD
- HARITHA KARNA
- JOE ARUL SUSAI PRAKASH
- SHILPI KUMARI

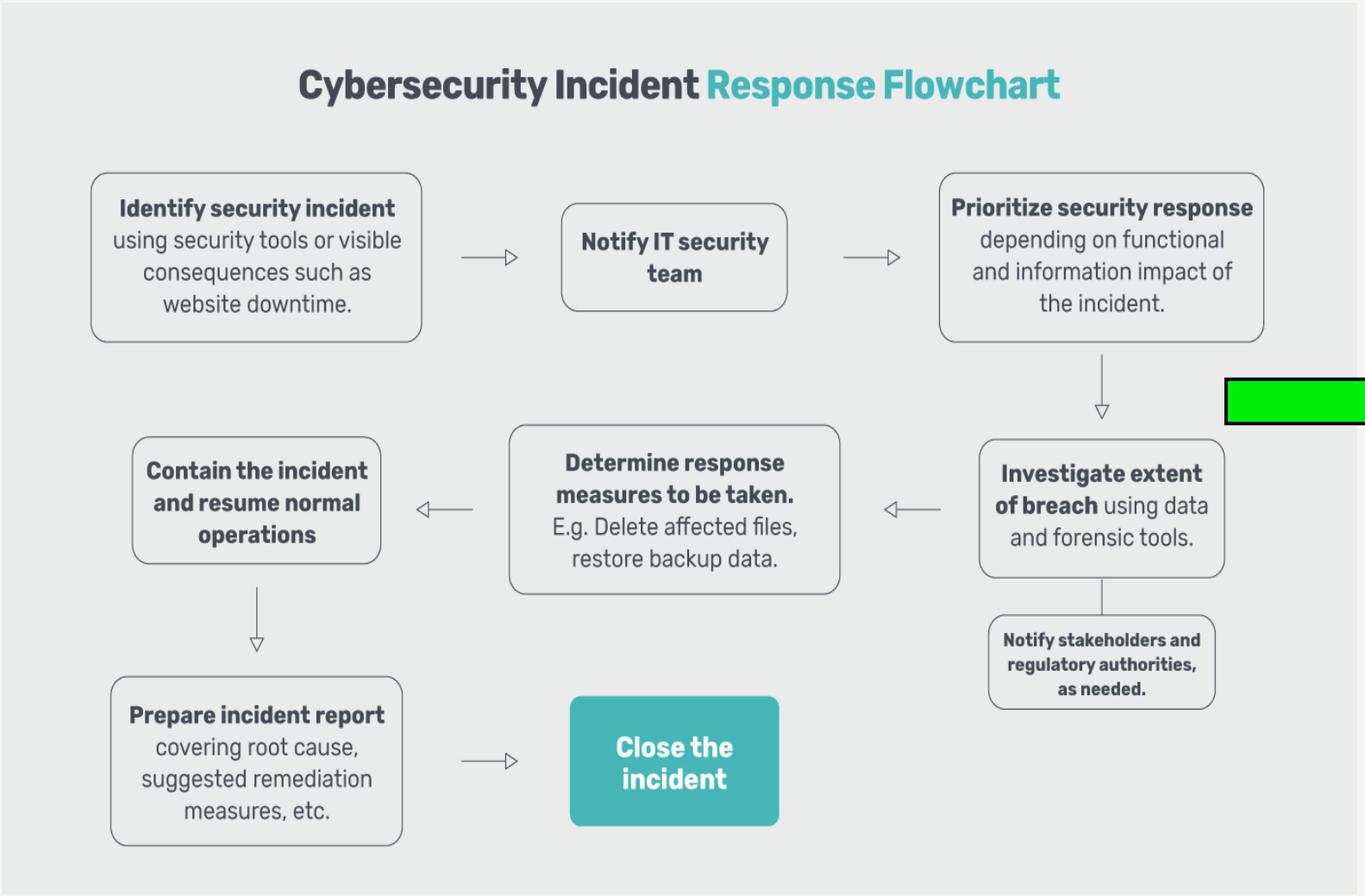
Background and Motivation

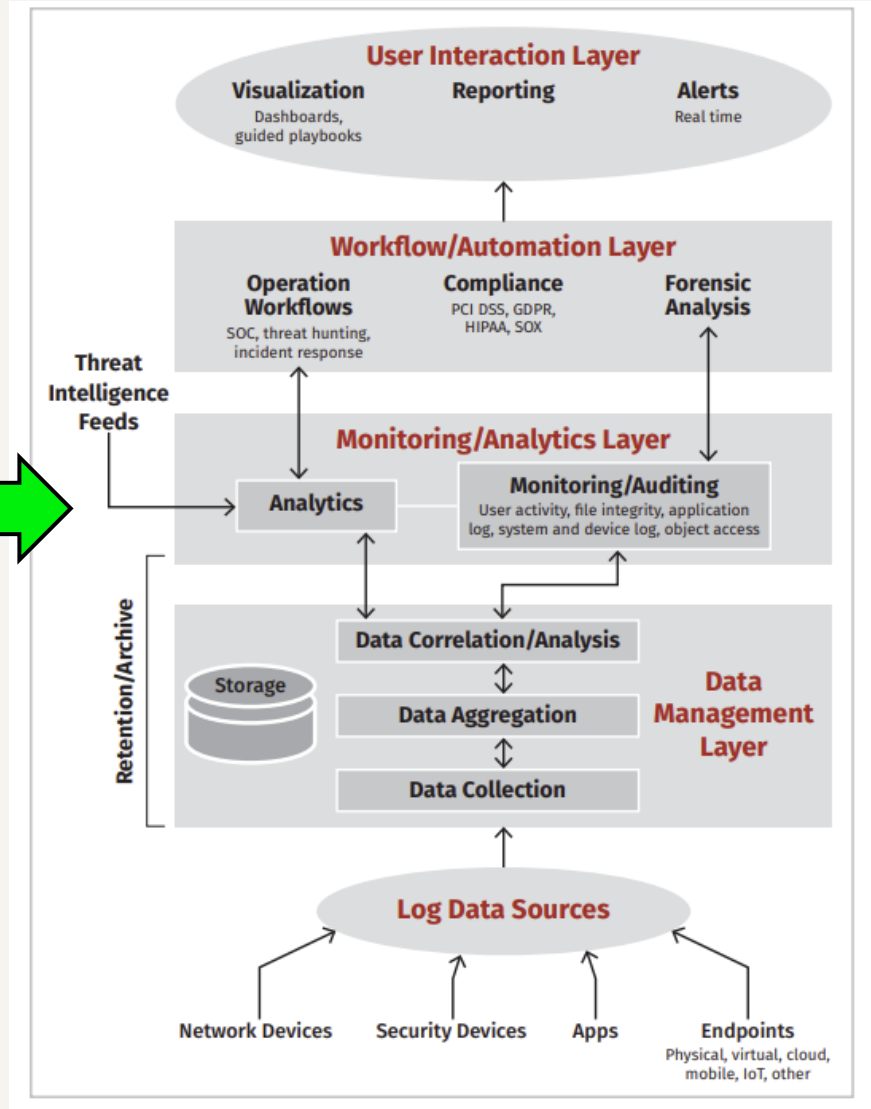


- Cyber Threat Overview
- Evolving Threat Landscape
- Technology Advancement
- Unification of technologies

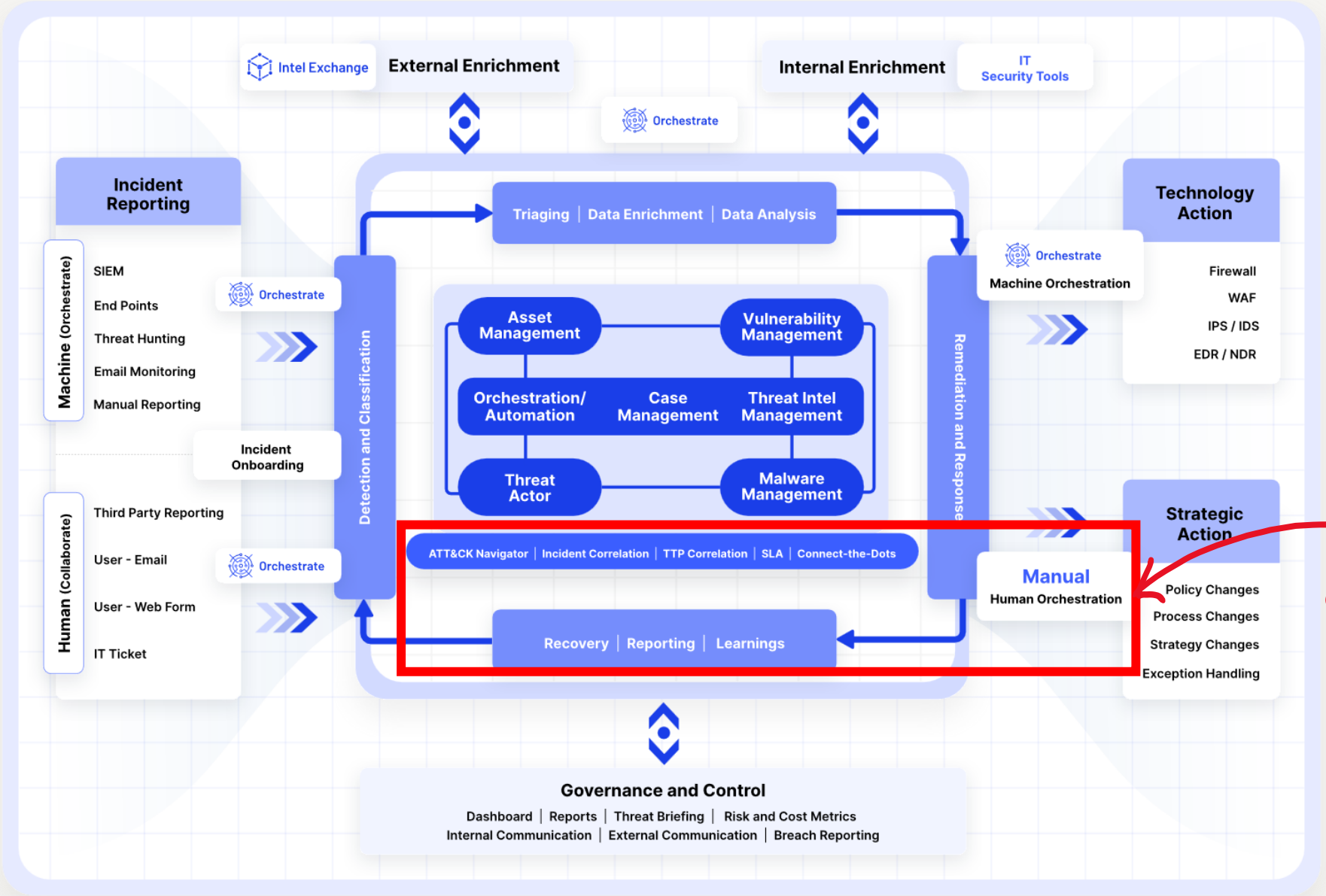


THREAT *DETECTION-ANALYSIS-RESPONSE* PROCESS (PROBLEM SPACE)





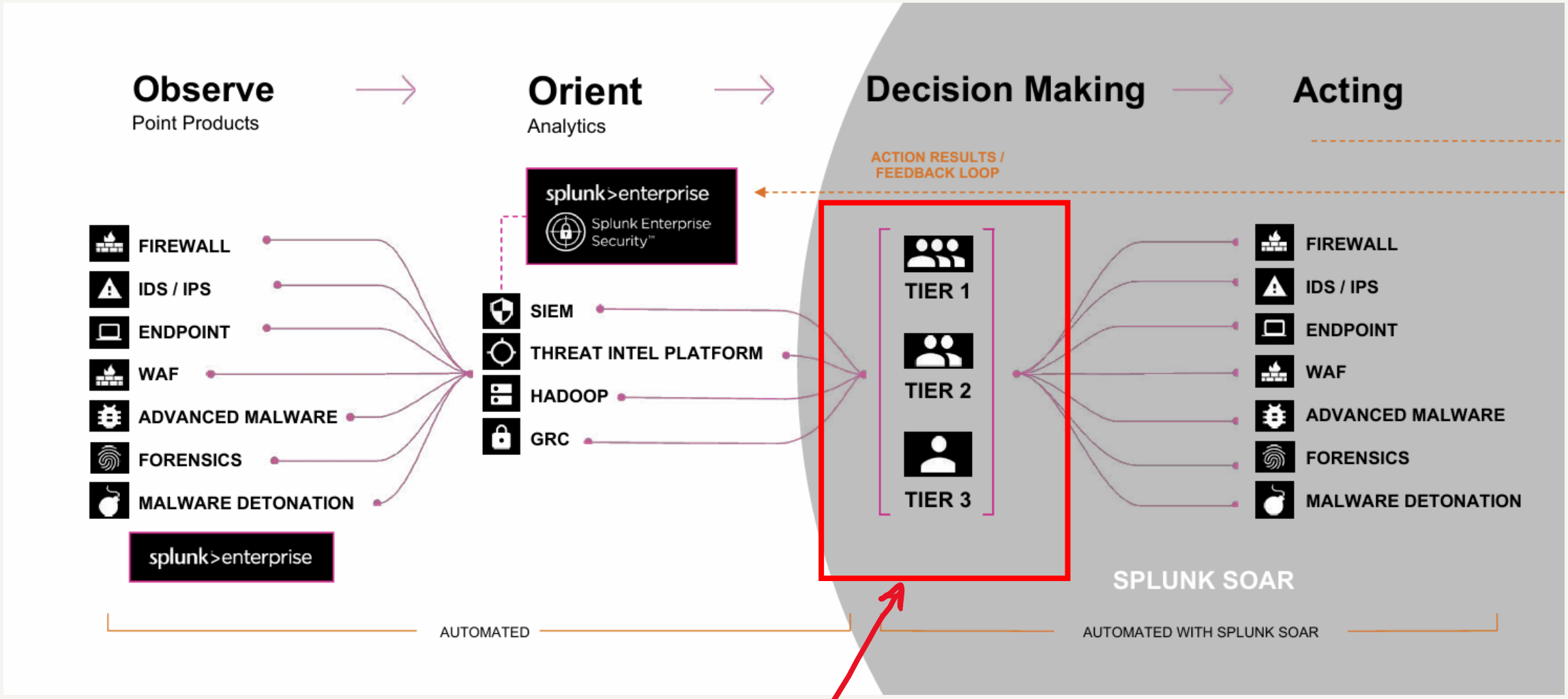
CURRENT STATE OF THREAT INTELLIGENCE (PROB. SPACE)



opportunity for Gen-AI

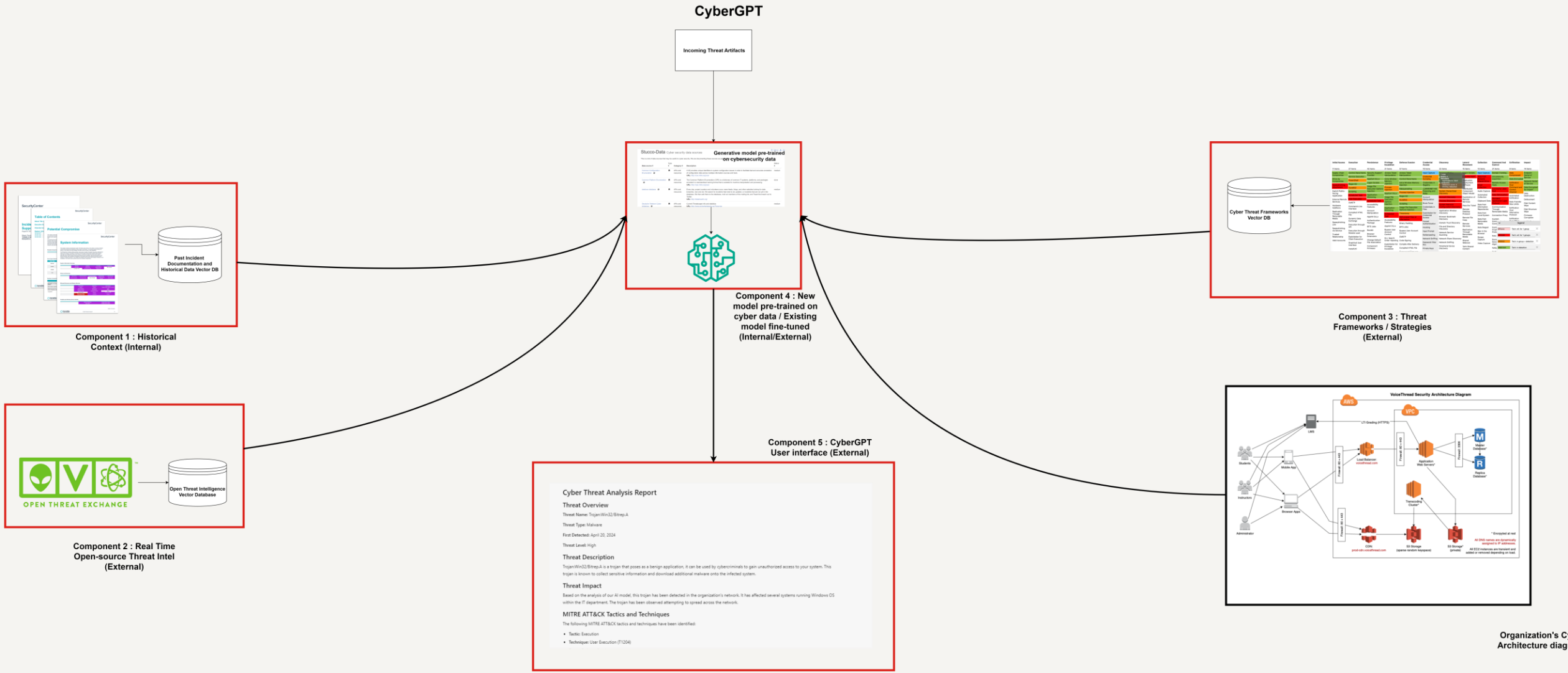
UNIFIED SECOPS CASE STUDIES (PROBLEM SPACE)

SPLUNK MISSION CONTROL, MICROSOFT SENTINEL, IBM QRADAR

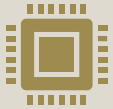


Opportunity for Gen AI

CyberGPT Machine Design (Solution Space)



Generative AI methods used in CyberGPT (Solution Space)



Pre-training / Fine-tuning of LLMs: Training a new model on Cyber data & Fine-tuning an existing model using techniques like PEFT and QLora help make the Gen-AI model more accurate in analyzing cybersecurity problems.

Retrieval Augmented Generation: Historical Incident Documentation, Open-Source Threat Intelligence and Threat Strategy data is vectorized and stored in vector databases like LlamaIndex to provide richer context to LLMs at the time of generation.

Prompting: The LLMs are continually prompted by the CyberGPT manager from different angles to obtain a detailed, well-thought response which helps SOC analysts take appropriate steps to combat the threat.

Human Behavior Design

- Our chat interface, powered by generative AI and fine-tuning models, enables cyber analysts to engage with an AI solution, enhancing understanding and responsiveness to cybersecurity queries and threats.
- The AI leverages historical incident data, organizational architecture insights, and open threat intelligence databases to analyze, suggested response playbooks and respond to emerging threats effectively.

Benefits for Cyber Analysts:

- Empowers analysts with comprehensive historical insights and real-time threat intelligence.
- Streamlines threat analysis and resolution processes.
- Enhances collaboration and decision-making within cybersecurity teams.
- The interface prioritizes simplicity and user-friendliness, facilitating easy navigation, interaction, and access to essential functionalities such as inputting threat details, viewing historical data, and receiving recommendations.

Requirements to build the solution (Implementation Cycle)

- Component 1 – Past incident documentation and historical data : Unavailable
- Component 2 – Open Threat Intelligence Repositories : Available, needs to be vectorized (Open Threat Exchange)
- Component 3 – Threat Response Frameworks / Strategies : Available, needs to be vectorized (MITRE Attack)
- Component 4 – Model trained on Cybersecurity datasets : Available (ZySec AI on Huggingface)
- Component 5 – User Interface to access CyberGPT : Needs to be built
- Organizational cybersecurity architecture : Unavailable

Implications of Generative AI in Cybersecurity Incident Response

Enhanced Threat Detection	Streamlined Incident Response	Addressing Black Swan Events
• **Generative AI** can significantly improve threat detection by analyzing patterns and anomalies in data that might be missed by traditional methods. • The integration of AI with **XDR** and **SIEM** tools can lead to earlier and more accurate detection of potential threats.	• By automating the response process, **SOAR** tools augmented with AI can reduce the time between detection and response, minimizing potential damage. • AI can assist in creating dynamic playbooks that adapt to new threats, ensuring a swift and appropriate response to incidents.	• Generative AI can help in understanding and responding to '**black swan**' incidents by providing recommendations based on similar historical events and patterns. • This reduces the reliance on manual scouring of documentation and consultation, leading to faster resolution times
Cost Reduction	**Continuous learning and Improvement**	**Ethical privacy considerations**
• Faster incident response and resolution can significantly reduce the financial impact of cyber-attacks. • AI-driven automation can also decrease the workload on cybersecurity analysts, allowing them to focus on more complex tasks.	• Generative AI systems can learn from each incident, improving their recommendations and responses over time. • This leads to a continuously evolving cybersecurity posture that can adapt to the ever-changing threat landscape.	• Implementing AI in cybersecurity must be done with consideration for ethical issues and privacy concerns. • Ensuring that AI systems are transparent and accountable is crucial for maintaining trust and compliance.

Thank You!

References

Background:

- Cyber-evolution: https://www.researchgate.net/publication/374156044_Evolution_of_the_Cyber_Security_Threat_An_Overview_of_the_Scale_of_Cyber_Threat
- Threat D&R to Intelligence: https://blogs.idc.com/2023/08/24/evolving-from-threat-detection-and-response-to-threat-intelligence/

Problem Space:

- AI/ML in Security Automation: https://www.techscience.com/iasc/v28n2/42057/html
- SIEM to SOAR: https://correlatedsecurity.com/soar-critical-success-factors/
- Next-generation SIEM systems: https://www.sans.org/media/vendor/evaluator-039-s-guide-nextgen-siem-38720.pdf
- MITRE attack framework: https://www.recordedfuture.com/threat-intelligence-101/tools-and-technologies/mitre-attack-framework

Case Studies:

- Microsoft Sentinel: https://learn.microsoft.com/en-us/azure/sentinel/
- Splunk Mission Control: https://www.splunk.com/en_us/products/mission-control.html
- Cyware Platform: https://cyware.com/products/incident-analysis-threat-response-platform