

15TH ITU ACADEMIC CONFERENCE

ITUKALEIDOSCOPE

NEW DELHI 2024

*Innovation and digital transformation
for a sustainable world*

21-23 October 2024
New Delhi, India



Generative AI Enabled Actionable Decision Support in Cybersecurity Operations for Enterprise Security

23 October 2024





Presenter: Sandeep Sharma,

Scientist – C & Team Leader (A) – AI Analytics

Co-authors: Saurabh Basu, Utkrisht Singh, Pankaj Kumar Dalela, Rajkumar Upadhyay

Centre for Development of Telematics (C-DOT), India



ITUKALEIDOSCOPE
NEW DELHI 2024

15TH ITU ACADEMIC CONFERENCE

The average cost of a data breach was **\$4.88 Million** in 2024



88% of cybersecurity breaches are caused by human error.



The average time to identify a breach is **194** days.



AI-based cybersecurity products was about **\$15 Billion** in 2021 and will surge to roughly **\$135 Billion** by 2030



55% of organizations plan to adopt GenAI solutions for cyber security in 2024

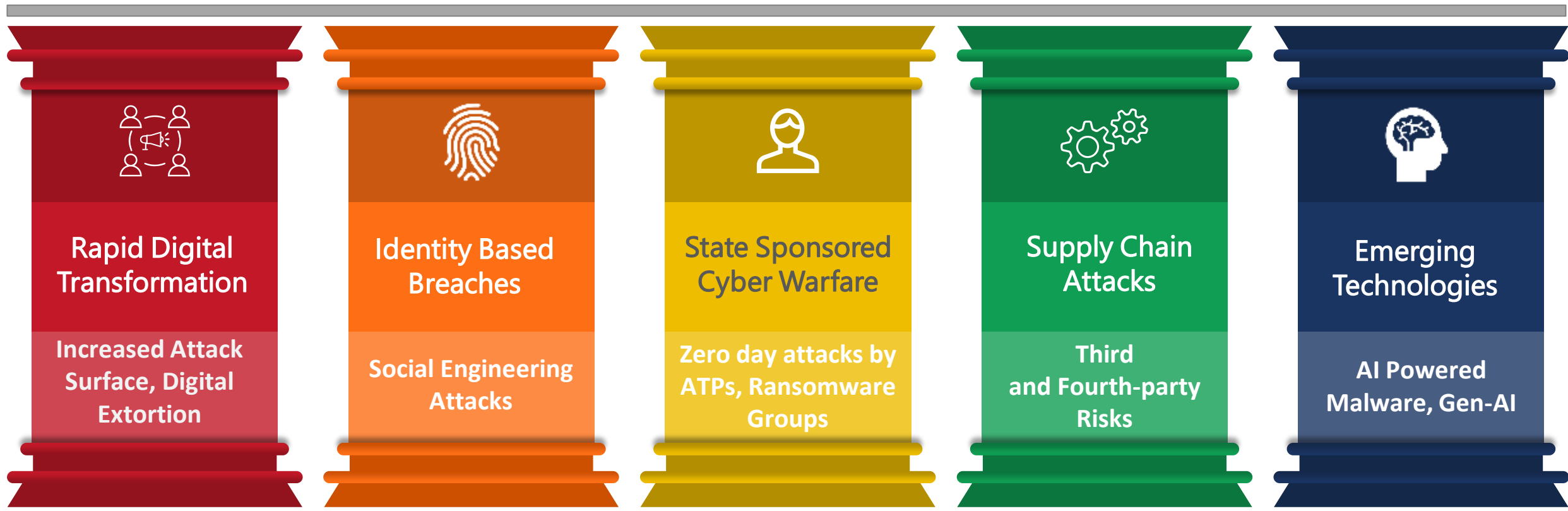


48% of professionals expressed confidence in their organization's ability to execute a strategy for leveraging AI in security.



ITUKALEIDOSCOPE
NEW DELHI 2024

Age of Digital Battleground, Need for Securing our Digital Future



Enterprises
employs
multitude of
security solutions
like **EDR**, **NDR**,
SIEM, **SOAR**,
UEBA and **DLP**

Security analysts
are inundated
with **Millions** of
security **event**
logs

Shortage of
dedicated and
skilled
manpower to
understand and
analyze security
events



Threat Detection



Contextual interpretation of complex log patterns and identification of emerging threats

Situational Awareness



Correlation of seemingly unrelated events to uncover complex attack patterns

Incident Response



Prioritized alerts based on severity and streamlined decision-making

Operational Efficiency



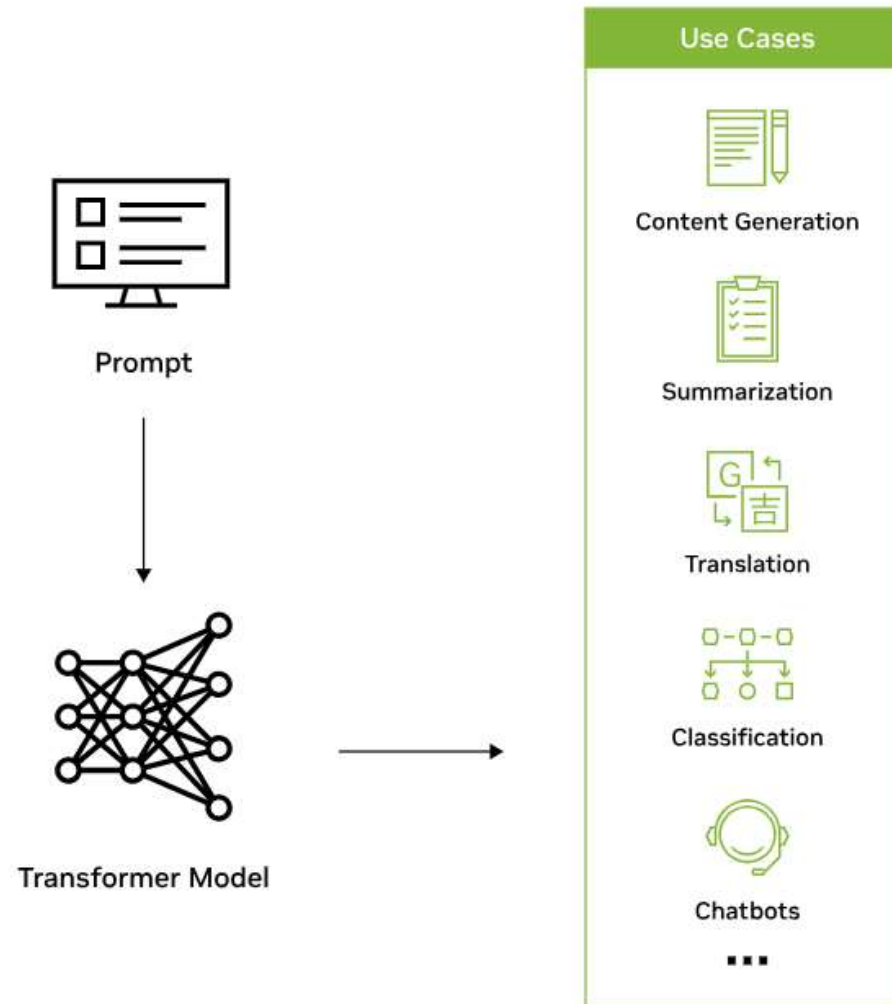
Reduction in manual log analysis workload and automated categorization of security events

Can GEN-AI help .. ?

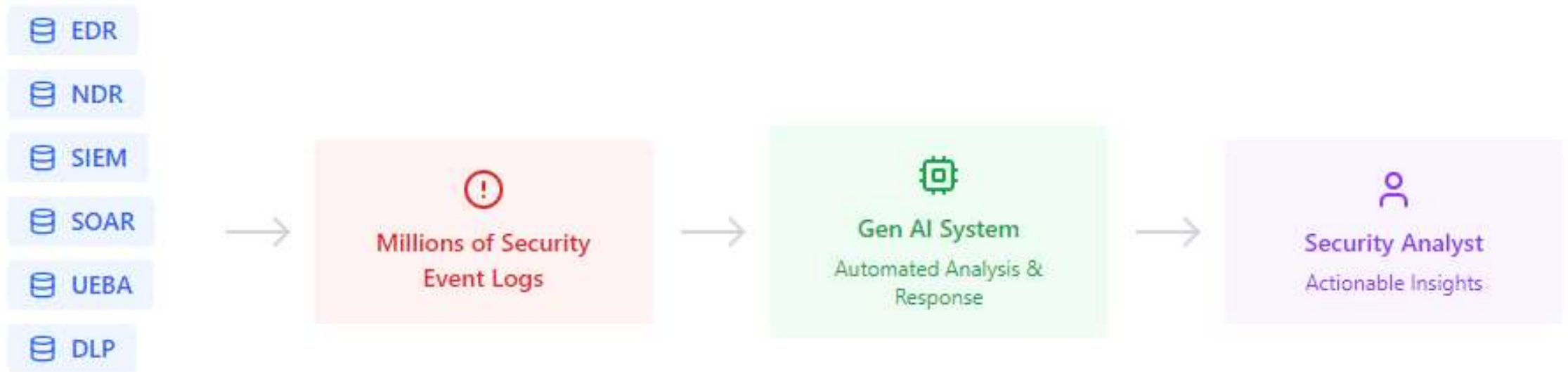


LARGE LANGUAGE MODELS

Large language models are advanced artificial intelligence system trained on vast amounts of text data to understand and generate human understandable language.



GEN-AI for Automated Security Event Response



Multiple Security Solutions
deployed by Organizations

Implementation Details

Dataset Collection

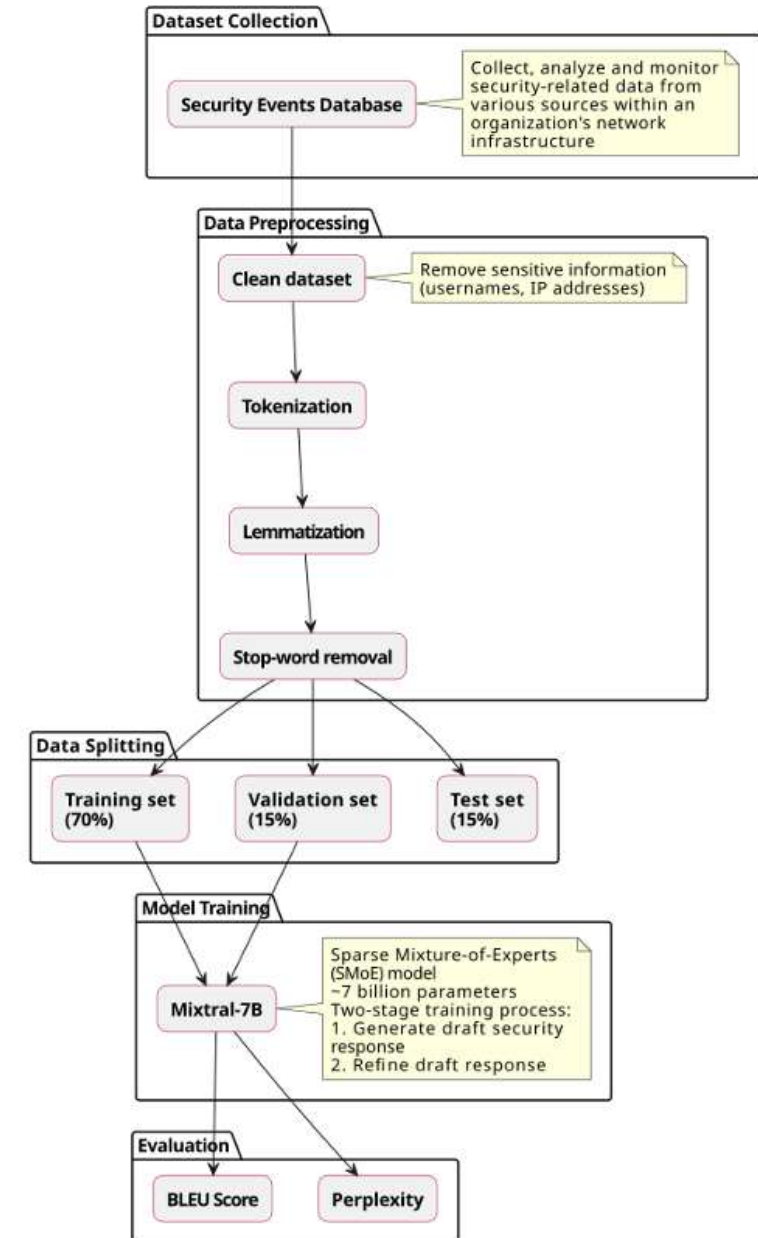
Real-world dataset of 1 million security event logs consumed from ELK (Elasticsearch, Logstash, and Kibana) stack based on SIEM solutions[1].

Data Preprocessing

Extracted relevant fields (event type, severity level, MITRE technique, description) from the SIEM logs and then Cleaned dataset via removing sensitive information (usernames, IP addresses)

Data Splitting

Split the dataset into three subsets: training, validation and test sets. The training set (70% of the data) is used to fine-tune the Mistral-7B model.



Implementation Details

Model Selection

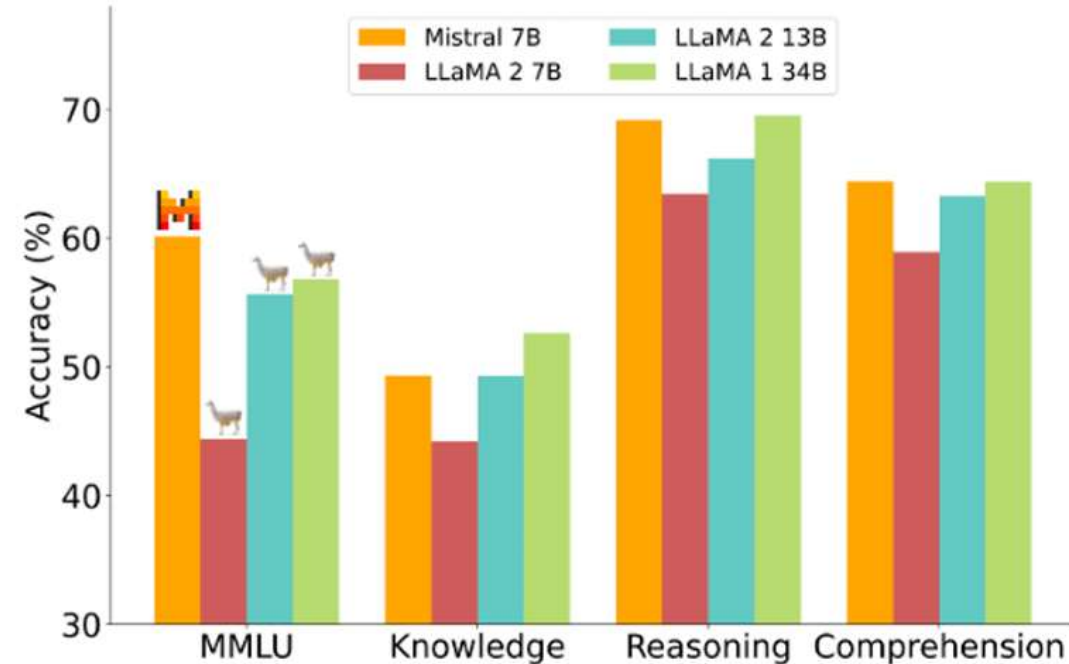
Mistral-7B leverages a Sparse Mixture-of-Experts architecture[2]. It is best 7B large language model capable of capturing relationships within natural language data*.

Model Fine -Tuning

Input to the model consists event type, severity level, source and textual description of the event and desired output is concise and interpretable security response message.

Model Evaluation

Fine-tuned model demonstrated impressive BLEU score of 0.85 and low perplexity score of 12.7 indicates that generated responses are highly coherent

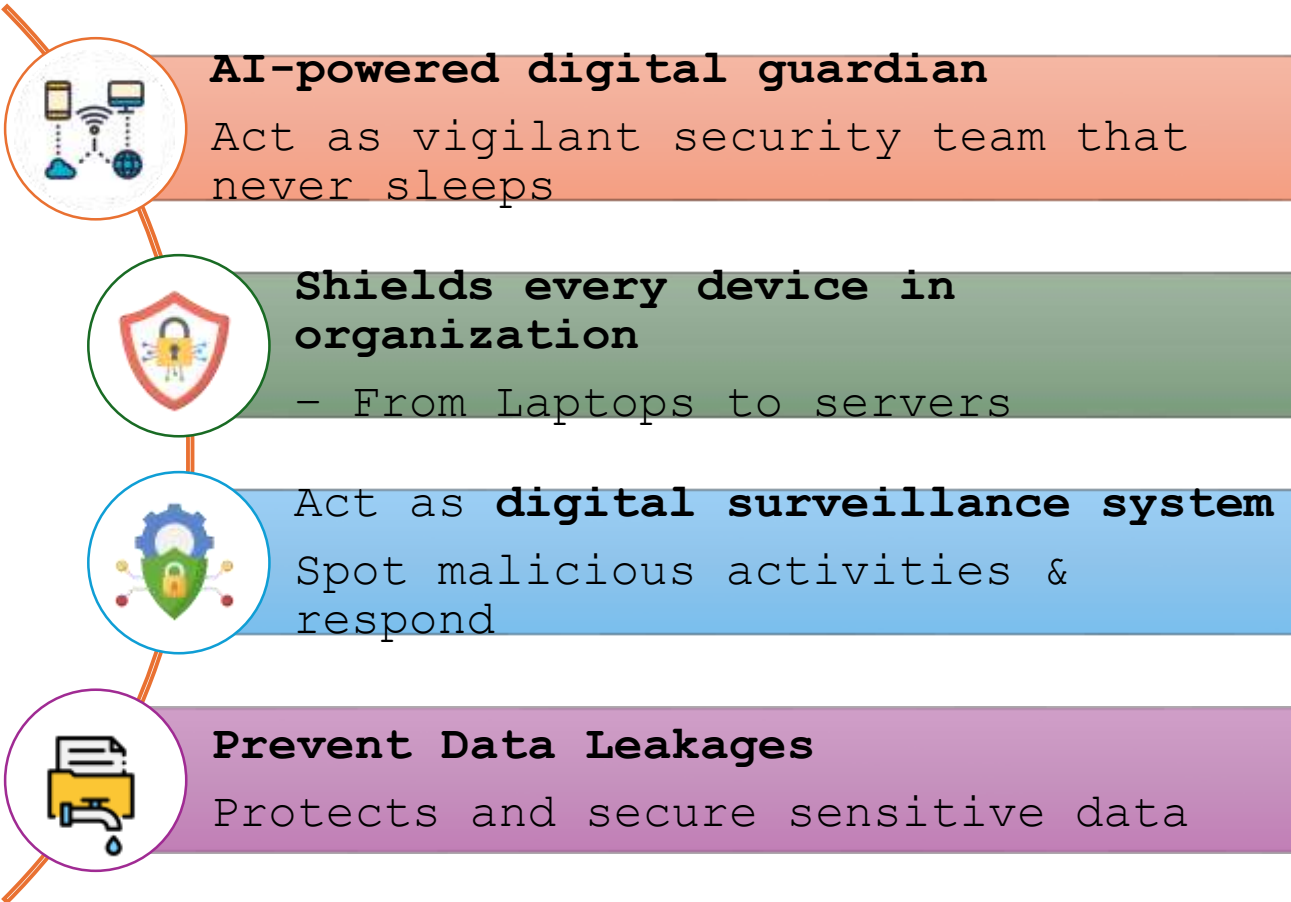


[2] A. Q. Jiang, A. Sablayrolles, A. Mensch, C. Bamford, D.S.Chaplot, D.D.L.Casas, et al., "Mistral 7B," arXiv preprint arXiv:2310.06825, 2023.

*This research is conducted on April 2024 and it is compared with multiple open source large language model Llama, Mistral, Vicuna, BERT etc.

TRINETRA End-to-End Enterprise Cyber Security Solution

Facilitates establishment of **security command & control center** to **monitor end-points, identify security vulnerabilities & potential gaps, detect anomalies & suspicious activities, & helps to mitigate the same**



Unified Endpoint Management (UEM) | Endpoint Detection and Response (EDR) | Security Information and Event Management (SIEM) | Security Orchestration and Automated Response (SOAR)

User and Entity Behavior Analytics (UEBA) | Data Loss Prevention (DLP) | Network Detection & Response (NDR) | Security Audit Benchmark and Compliance (SABC)

Applying GenAI on Generated Security Events

Time ▾ _source

Apr 29, 2024 @ 12:15:34.758 input.type: log agent.ip: 192.168.1.130 agent.name: DESKTOP-T06VA5V agent.id: 265 manager.name: trinetra3 data.win.eventdata.image: C:\\Program Files (x86)\\Microsoft Visual Studio\\Installer\\resources\\app\\ServiceHub\\Services\\Microsoft.VisualStudio.Setup.Service\\BackgroundDownload.exe data.win.eventdata.processGuid: {885cc6c7-4208-662f-350c-000000005300} data.win.eventdata.processId: 9084 data.win.eventdata.utcTime: 2024-04-29 06:45:39.812 data.win.eventdata.targetFilename: C:\\Users\\ADMIN\\AppData\\Local\\Temp\\m5n2udw3.suz\\xnrt4y2t.json data.win.eventdata.ruleName: technique_id=T1047,technique_name=File System Permissions Weakness data.win.eventdata.creationUtcTime: 2024-04-29 06:45:39.812 data.win.eventdata.user: DESKTOP-T06VA5V\\ADMIN data.win.system.eventID: 11 data.win.system.keywords: 0x8000000000000000 data.win.system.providerGuid: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} data.win.system.level: 4 data.win.system.channel: Microsoft-Windows-Sysmon/Operational data.win.system.opcode: 0 data.win.system.message: "File created:

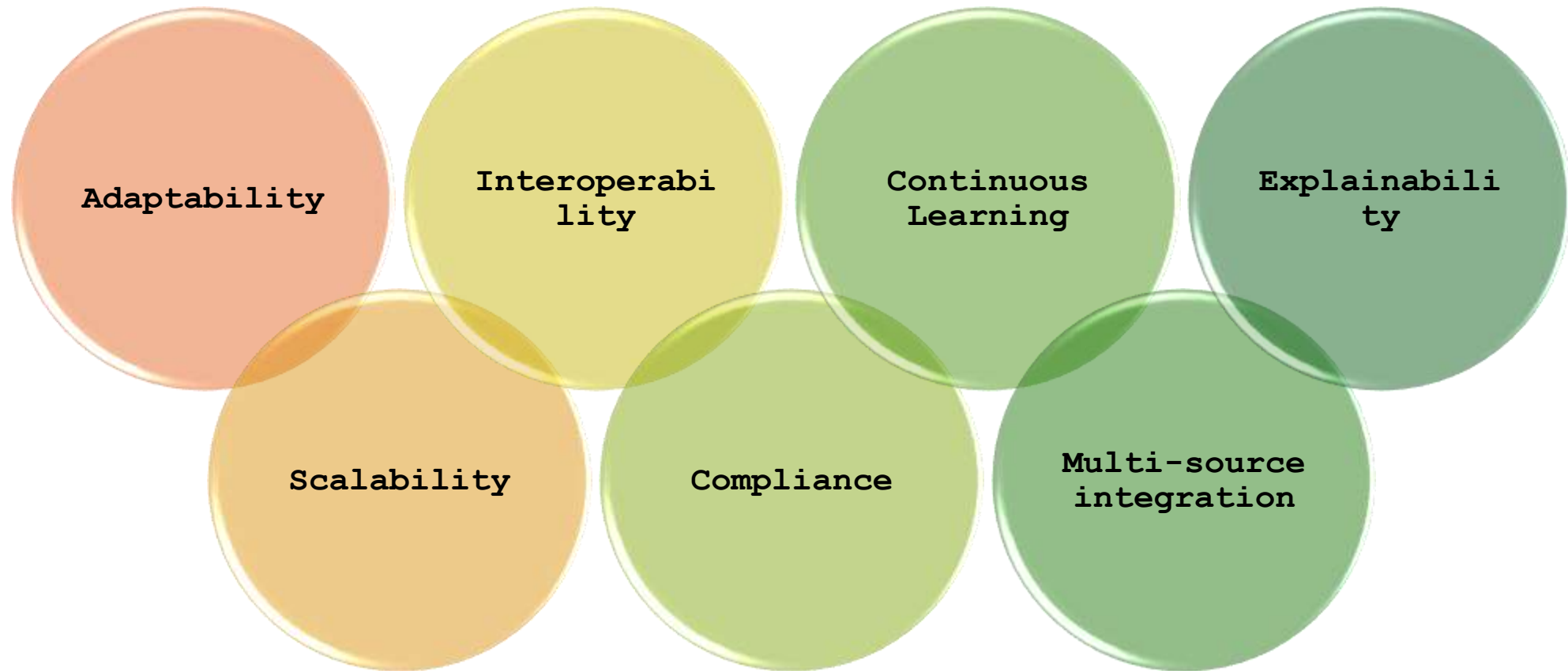
Expanded document

[View surrounding documents](#) [View single document](#)

Table	JSON
f _index	trinetra-alerts-4.x-2024.04.29
f agent.id	265
f agent.ip	192.168.1.130
f agent.name	DESKTOP-T06VA5V
f data.win.eventdata.creationUtcTime	2024-04-29 06:45:39.812
f data.win.eventdata.image	An event with ID 11 occurred on your system at 2024-04-29 06:45:39.812. This event is related to the creation of a file. The file was created by an application with the process ID 9084 and image name "C:\\Program Files (x86)\\Microsoft Visual Studio\\Installer\\resources\\app\\ServiceHub\\Services\\Microsoft.VisualStudio.Setup.Service\\BackgroundDownload.exe". The target filename for this file is "C:\\Users\\ADMIN\\AppData\\Local\\Temp\\m5n2udw3.suz\\xnrt4y2t.json". This event was logged by the Microsoft-Windows-Sysmon provider with a level of 15. To prevent similar events from occurring in the future, you can take the following actions: - Review the permissions for the application that created the file. If the permissions are not necessary for the application to function correctly, consider removing or limiting those permissions. - Implement a file access control policy that restricts unauthorized users or applications from creating or modifying files in sensitive areas of your system. - Regularly review the event logs on your system to identify and investigate any suspicious events or patterns that may indicate potential security vulnerabilities or threats. - Keep all software, operating systems and applications up-to-date with the latest patches and security updates to help protect against known vulnerabilities and exploits.

Way ahead . . .

Need for Thoughtful Implementation and Strategic Effort . . .



Thank you!

