
Qerberos
Pioneering AI-Powered Cybersecurity for Next Generation End Point Detection

Meet the team

Revolutionizing how organizations detect and respond to cyber threats using cutting-edge GenAI

Angus Chen (Director of Data Science)

Abubakar Zaidi (Python Developer)

Yamen Kashkash (Fullstack Developer)

Baria Mirza (Research Student)

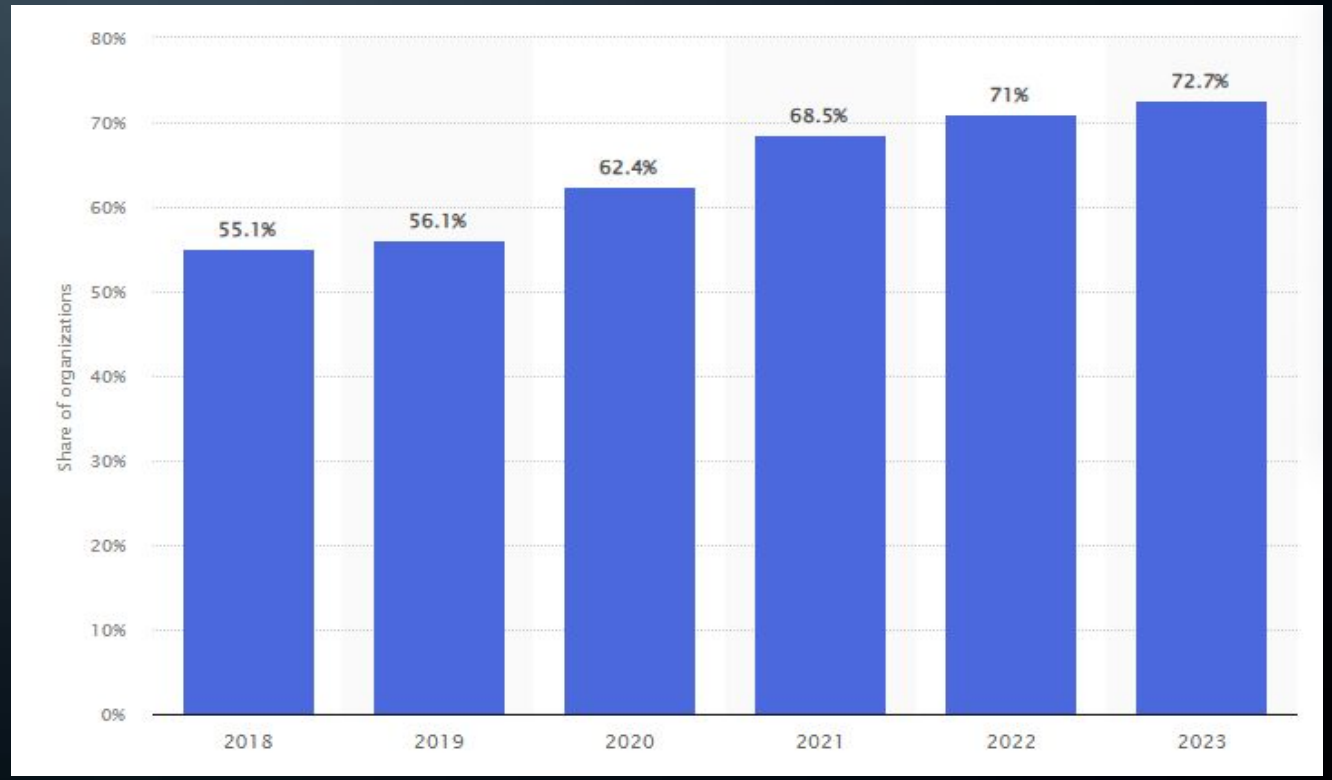
Blewuada Mawuli Y. (AI Enthusiast)

The Problem

- Hackers often install malicious services to maintain persistence on a compromised system.
- By creating a new service, the bad guys can ensure that their malware or backdoor starts automatically every time the system reboots.
- A malicious service can be used to escalate privileges on the system. If the service is configured to run with higher privileges, the attacker could gain greater control over the system.
- Attackers may use legitimate-looking services to avoid detection. By disguising their malicious service as a system or third-party service, they can fly under the radar of security monitoring tools.
- Detecting unauthorized service installations can be an early indicator of compromise, prompting further investigation.

Why Detect Unauthorized Services?

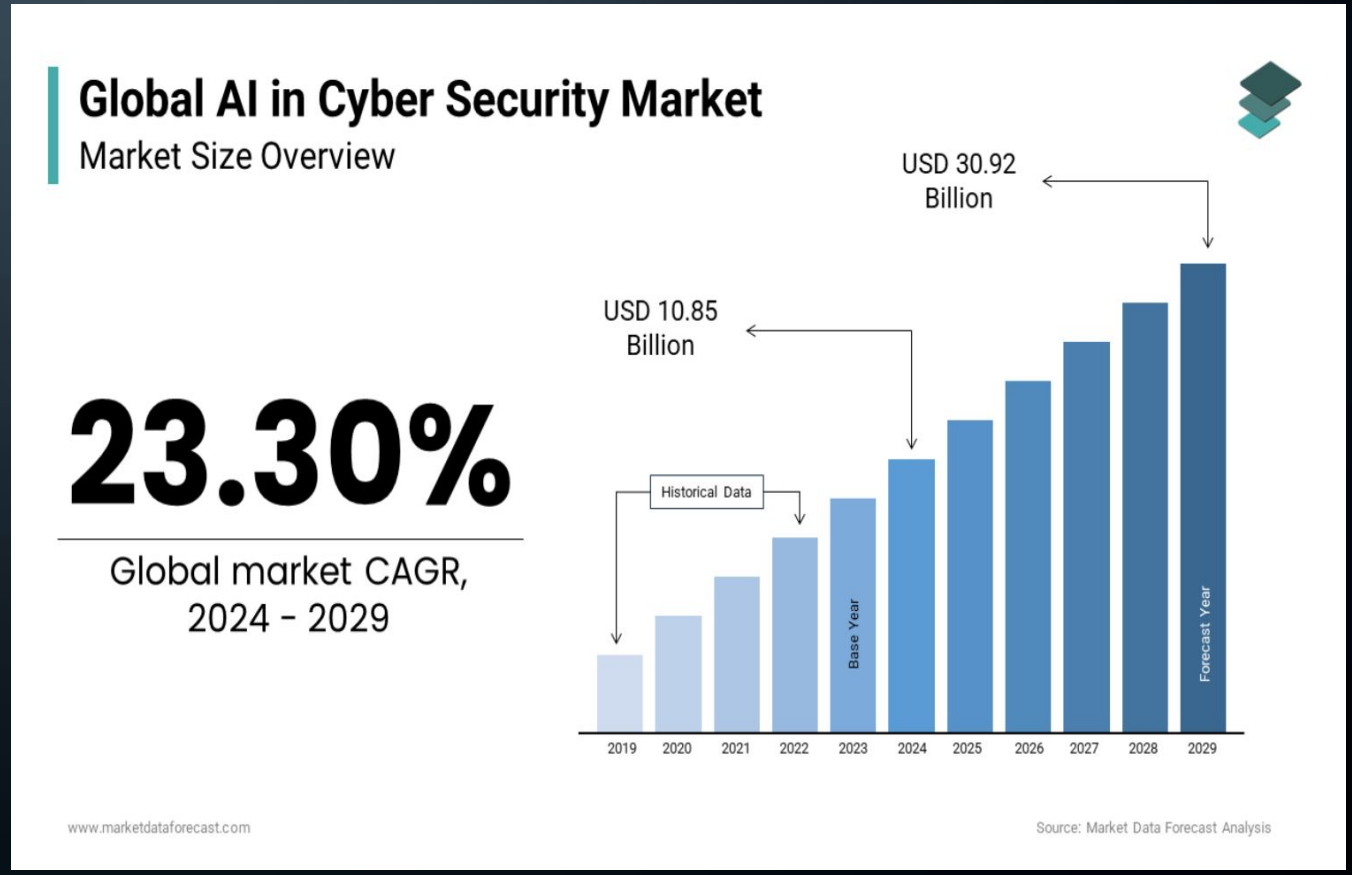
- Detecting unauthorized service installations is an early sign of a compromise, prompting immediate investigation.
- By identifying and disabling these services, the organization can prevent attackers from gaining higher levels of control.
- Early detection helps in identifying sophisticated attacks that might evade other forms of detection.



Annual share of organizations affected by cyber attacks worldwide from 2018 to 2023 are shown in the figure.

Market Overview

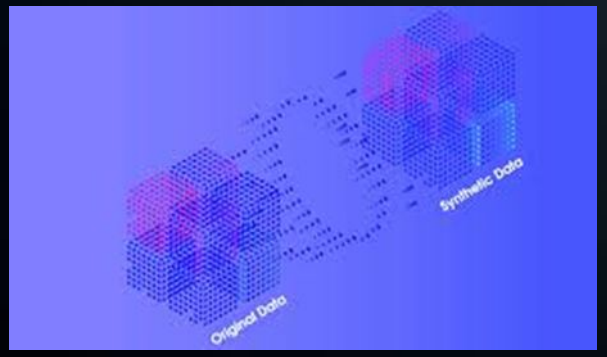
- Increasing demand for AI-driven security solutions, especially for endpoint security, due to the rise of remote work and sophisticated cyber threats.
- The global AI in cybersecurity market was valued at $16.5 billion in 2021 and is expected to grow to $91.7 billion by 2032, with a CAGR of 16.2%.
- The endpoint security market is projected to grow at a CAGR of 9% from 2024 to 2031.



Our Solution: GenAI Based Detection

- Our GenAI-based model detects unauthorized services using event logs on endpoint devices with high accuracy, providing early warning of potential cyber threats.
- The solution is designed to be lightweight and can be deployed to edge devices without disrupting existing processes.

 Real-time Detection

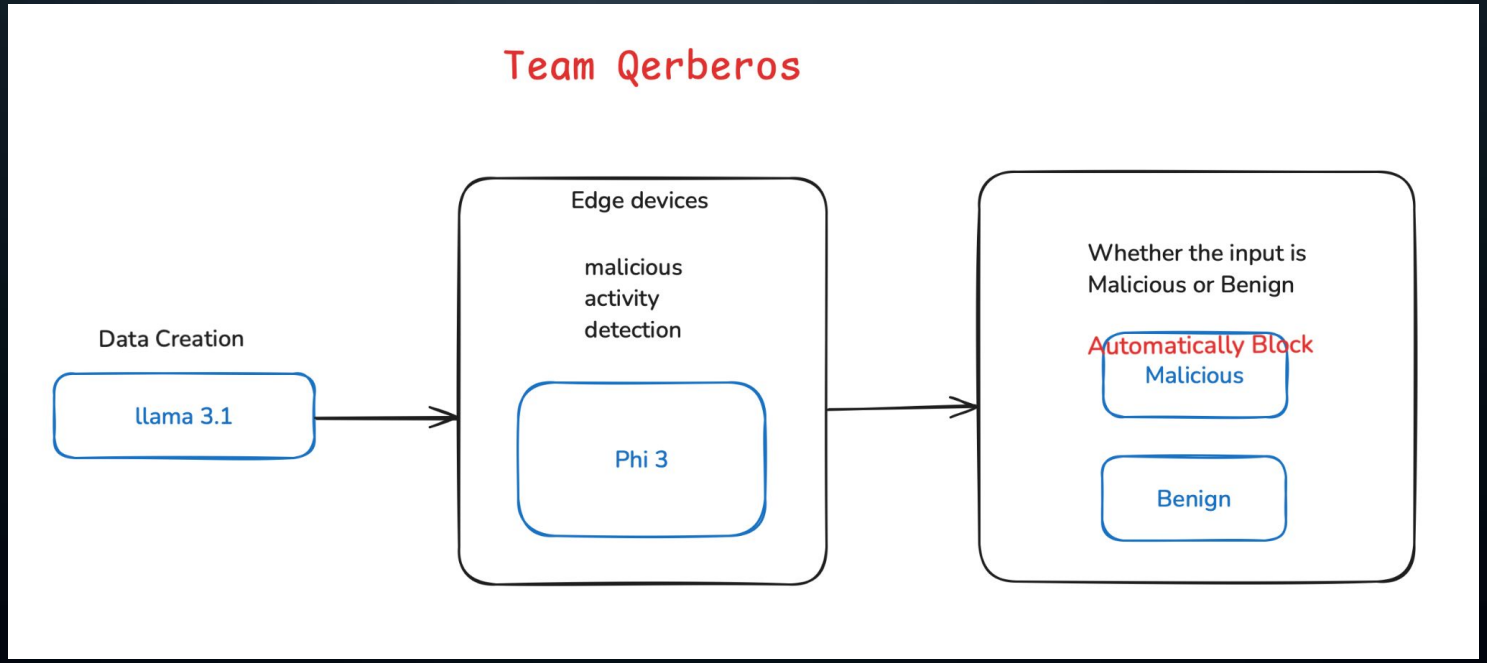


 Low Latency

 Edge Deployment

Technical Approach

- Utilized LLMs like Llama 3.1 for synthetic data generation and Phi 3 for model deployment on edge devices.
- Trained the model on both real and synthetic data to enhance accuracy.
- The architecture includes data creation, and malicious activity detection.



Market Potential and Business Model

> Projected market size USD 298.5 billion by 2028*

> Broad Target Audience

> Expanding Revenue Streams:

- SaaS Model
- Licensing
- Professional Services

Source: https://www.secureitworld.com

The Prototype and key Features

Vision and Roadmap

As a leading AI-powered cybersecurity company, we protect digital assets of organizations worldwide from advanced and evolving threats.