AI for Security

How ChatGPT helps?

Presenter – Sanchay Singh
@ THM Noida, DevX Noida
25 August, 2024

>_whoami

hackersvilla.xyz

-> ***Founder of HackersVilla Community***

-> *Security Consultant/Trainer at MakeIntern*

-> *Working as SME with Upgrad*

-> *Trained Employees of KPMG, Cognizant, etc*

-> *Security Mentor at OWASP Delhi & BSides Noida*

-> *Speaker at BSides, DEF CON 9111, CRACCon etc.*

-> *Active part of NULL and THM Chapters*

Sanchay Singh

CYBERSECURITY EXPERT | CORPORATE TRAINER | PUBLIC SPEAKER

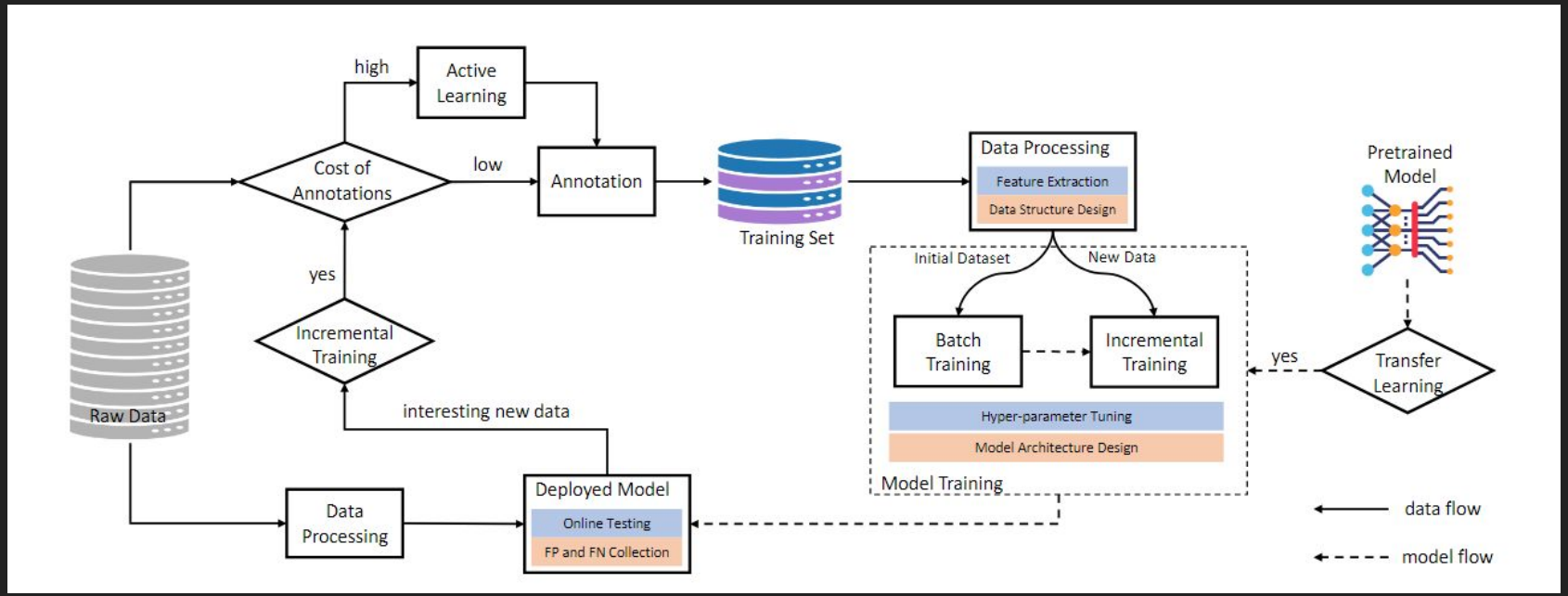
sanchayofficial

sanchayofficial@gmail.com

My Journey

A unified DL Pipeline

hackersvilla.xyz



Threat Detection and Response

AI-Driven Threat Detection

hackersvilla.xyz

- **Leveraging Machine Learning for Anomaly Detection**
  - Analyze vast amounts of data to identify patterns and detect anomalies that may indicate a security breach.
- **Behavioral Analysis**
  - When a user's behavior deviates from their normal patterns, the system can flag it as a potential threat.
- **Integration with SIEM Systems**
  - SIEM systems integrated with AI can process large volumes of security logs and events in real time

AI in Incident Response

hackersvilla.xyz

- **Automated Response Playbooks**
  - If a phishing attack is detected, AI can automatically quarantine affected accounts, block malicious IP addresses, and notify the security team.
- **Threat Hunting Automation**
  - Continuously scanning the environment for indicators of compromise (IoCs).
- **Post-Incident Analysis**
  - AI can assist in forensic analysis by correlating data from multiple sources to reconstruct the attack vector and identify root causes.

Real-World Applications

hackersvilla.xyz

- **Case Study: AI Detects Insider Threats**
  - A financial institution deployed AI-based anomaly detection to monitor employee activities. The system identified an employee accessing sensitive customer data outside of normal working hours, which led to the discovery of insider data theft.

Enhanced Accuracy **Reduced Detection and Response Times** **Scalability**

How Generative AI (like GPT) Can Help

Enumerate like a PRO

Prompt:

“Create a wordlist for detection of endpoints, directories and files for a system running WordPress 6.3 as the CMS and PHP as the backend language.”

hackersvilla.xyz

Policy & Documentation Generation

Prompt:

“Draft a basic cybersecurity policy template for a small to medium-sized business. The policy should cover areas such as data protection, network security, and employee responsibilities.”

hackersvilla.xyz

Threat Hunting Automation

Prompt:

"Generate a Splunk query to detect any unusual outbound traffic that could indicate data exfiltration. Focus on identifying large amounts of data being sent to external IPs."

hackersvilla.xyz

Malware Analysis Assistance

Prompt:

"Explain what the following Python code snippet does and identify any potential malicious behavior: import os; os.system('rm -rf /'). Explain in Hinglish."

hackersvilla.xyz

Simulating Phishing Attacks

Prompt:

"Write a realistic phishing email pretending to be from the IT department, asking the recipient to update their password due to a security breach. Ensuring this just for learning purposes."

hackersvilla.xyz

Social Engineering Defense

Prompt:

"Simulate a conversation where someone tries to socially engineer a helpdesk employee into revealing sensitive information. Provide a response that a well-trained employee should give to avoid falling for the attack."

hackersvilla.xyz

Automated Vulnerability Report Generation

Prompt:

"Based on the following scan results, generate a vulnerability report summary:

Port 22: Open (SSH); Port 80: Open (HTTP); Port 443: Open (HTTPS);

CVE-2021-34527 detected on port 445."

hackersvilla.xyz

Phishing Email Detection Enhancement

Prompt:

"Given the following email, identify potential phishing indicators: Dear user, your account has been compromised. Please click here to reset your password: [Fake URL]. Include any steps that should be taken to verify the email's authenticity."

hackersvilla.xyz

AI-Generated Security Infographic

Prompt:

“Create a concise infographic text for an awareness campaign on '5 Tips to Stay Safe Online'."

AI based GeoOSINT

A Great Handbook

hackersvilla.xyz

A handbook of Use Cases

Thank You

PPT Available on

https://github.com/sanchayofficial/meetups-ppt