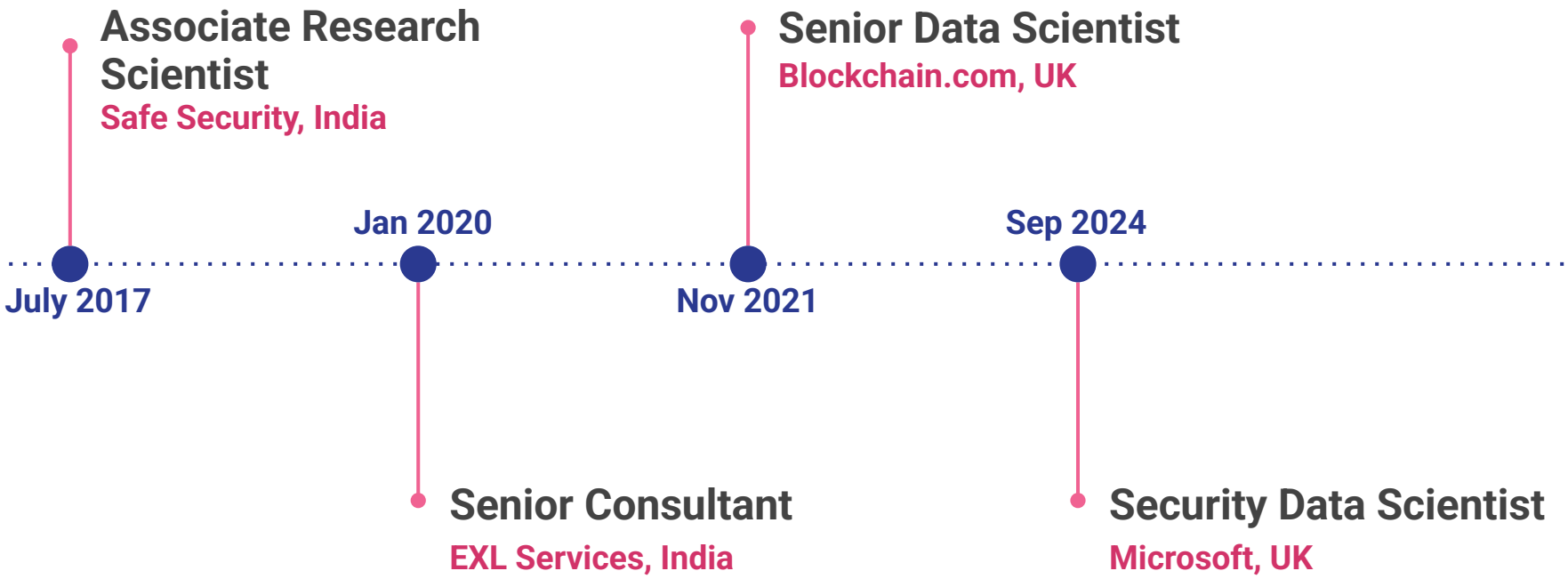
Agentic Cyber Defense with External Threat Intelligence

By Jyoti Yadav

About me

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Professional Journey



Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Slides & Code

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Slides and Code

https://github.com/jyotiyadav99111/PyDataLondon2025

Motivation

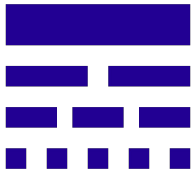
Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Overview

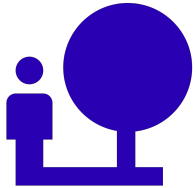
A conversational agent that autonomously investigates domain and IP threats—leveraging large language models, custom data-enrichment tools, and analyst feedback—to deliver rapid, contextual cybersecurity insights

Problem Statement

Thousands of new domains and IPs registered daily, many used in phishing or malware campaigns

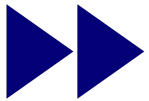


Static rule-based systems struggle with novel or obfuscated threats



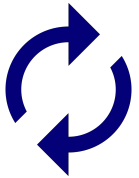
High false-positive/negative rates requiring expert intervention

Why Agentic AI



Automates multi-step investigations in seconds

Leverages LLMs to synthesize diverse signals into coherent analysis



Continuous Feedback Ingestion making it dynamically Responsive

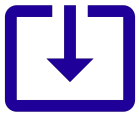
Model Components

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

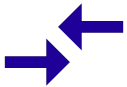
Data Collection Tools

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Whois



Local DB



API

example.com

WHOIS Information

IP Address: 23.192.228.84

Whois | RDAP | DNS Records | Uptime | Diagnostics | Refresh Data

Registrar Information

Registrar
RESERVED-Internet Assigned Numbers Authority

WHOIS Server
whois.iana.org

Referral URL
http://res-dom.iana.org

Important Dates

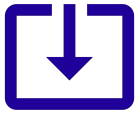
Created
1/1/1992

Updated
8/14/2024

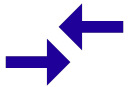
Expires
8/13/2025

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

GeoIP



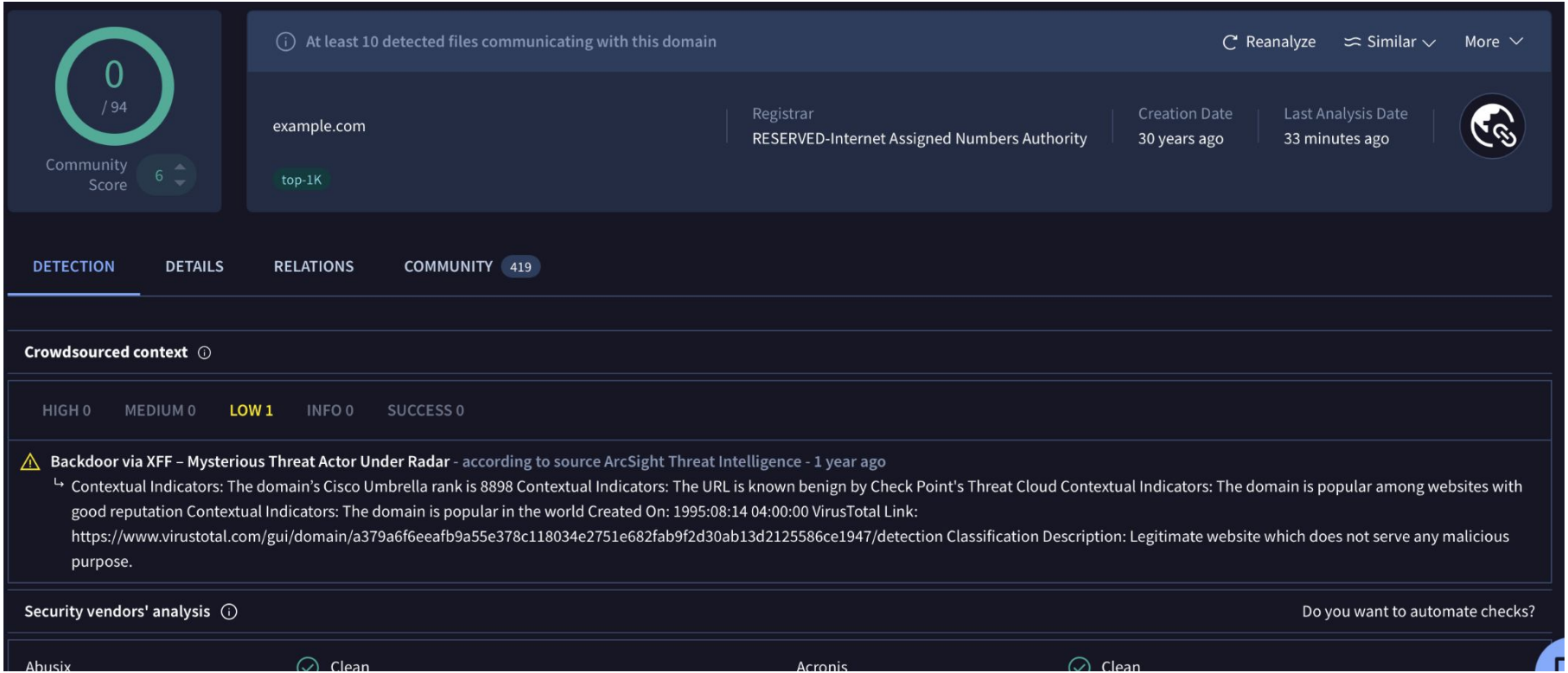
Local DB



API


```
{"status":"success","country":"United
States","countryCode":"US","region":"CA","regionName":"California","cit
y":"San
Jose","zip":"95141","lat":37.3388,"lon":-121.8916,"timezone":"America/L
os_Angeles","isp":"Akamai International B.V.","org":"Akamai
Technologies, Inc.","as":"AS20940 Akamai International
B.V.","query":"23.192.228.84"}
```

VirusTotal

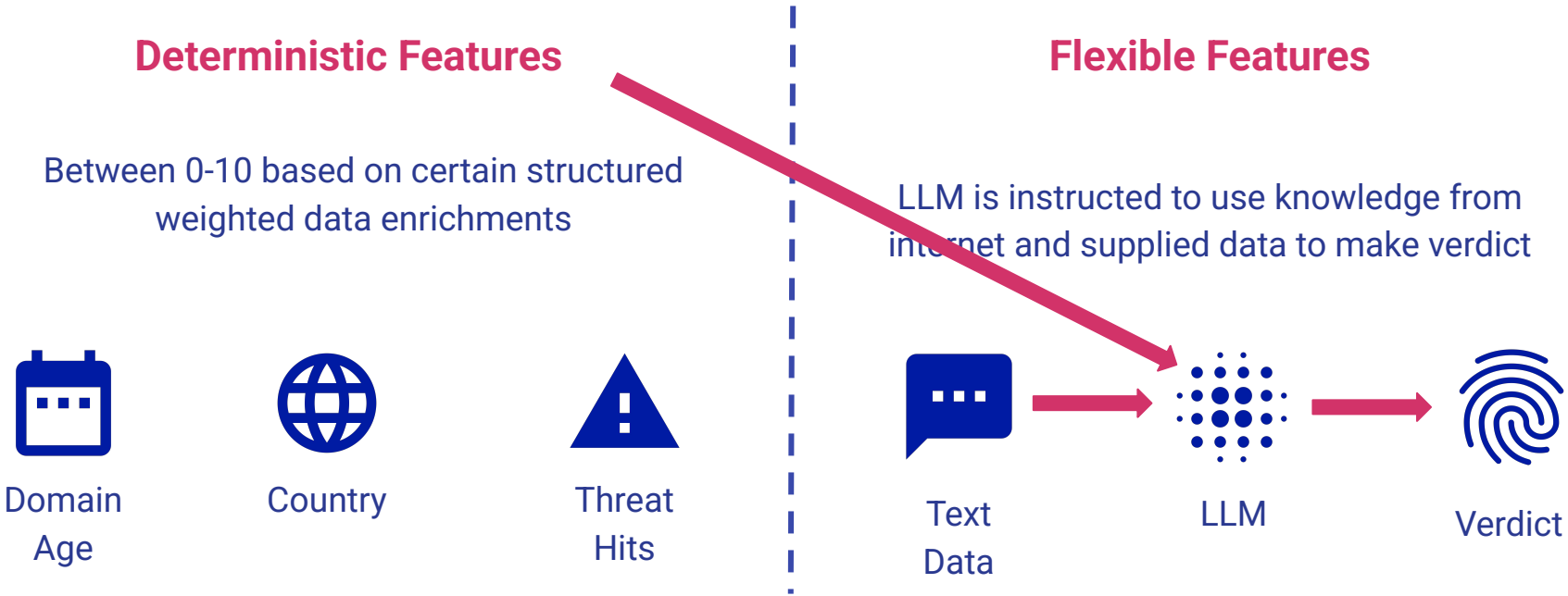


Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Explanation & Scoring Tools

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Verdict: Malicious or Not? why?

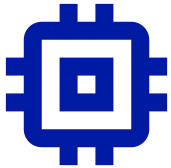


Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Feedback and Memory Tools

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Continuous Learning and Recency



Memory Access Tool

- What were the last domains I checked?
- How does this domain compares to the last domains I checked?
- etc

Feedback Ingestion Tool

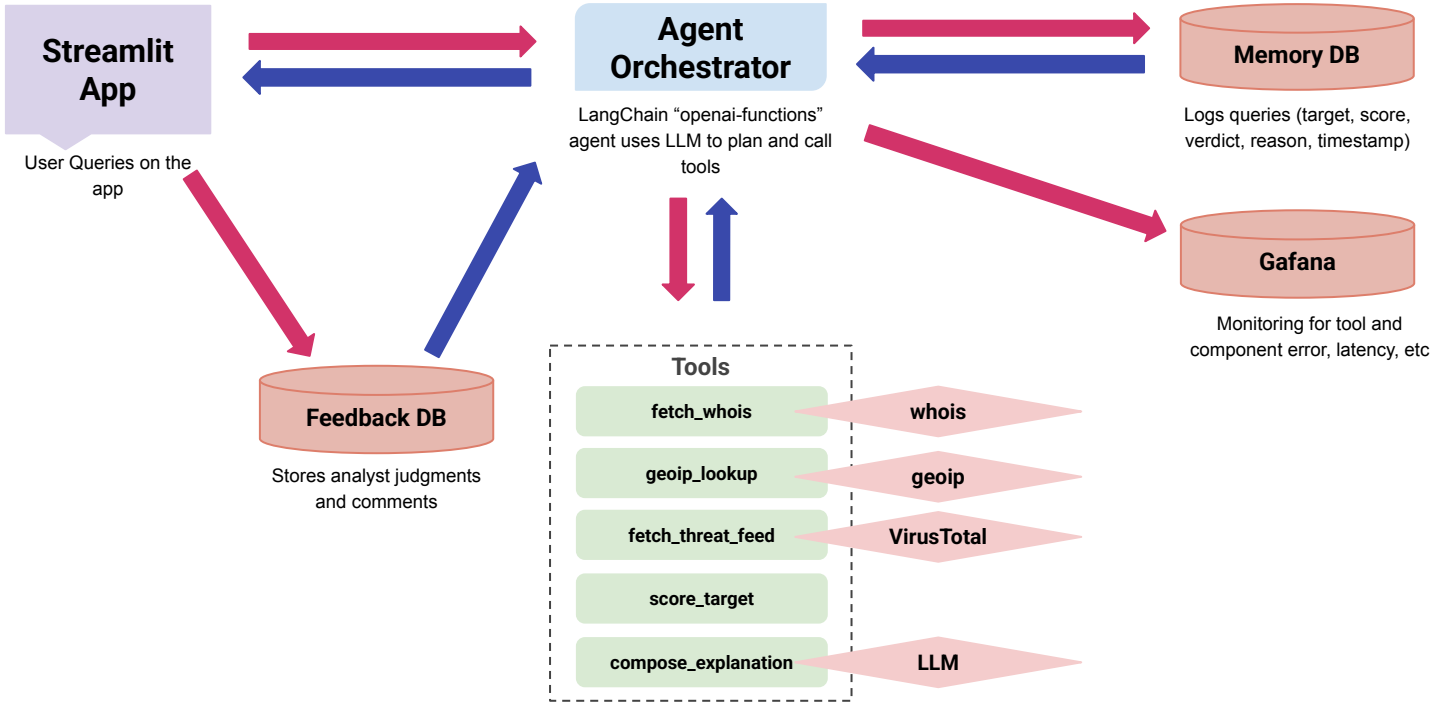
Auto ingestion of feedback for further feature adjustments for next query

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Architecture

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Architecture



Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

DEMO…

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Considerations

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft

Integration & Deployment Options

- **Packaging Options:**
  - **Streamlit App:** Quick deployment for analysts, minimal code changes, ideal for demos
  - **FastAPI Service:** Production-grade REST API, integrates with SIEMs and webhooks
  - **CLI Tool:** Lightweight scripting integration for automation pipelines
- **Containerization & Infrastructure:**
  - **Dockerfile Best Practices:** small base image, multi-stage builds, environment variables, secrets management
  - **Orchestration:** Kubernetes deployment (Helm charts), auto-scaling, health probes
  - **Serverless:** Cloud based Functions for event-driven execution
- **CI/CD Pipeline:**
  - **Automated Testing:** Unit tests for tools, integration tests for agent flows
  - **Build & Release:** GitHub Actions or Jenkins to build images, run linting, deploy to staging/production
- **Scaling & Observability:**
  - **Prometheus Metrics:** track query volume, latency, error rates
  - **Alerting:** Grafana or Alertmanager to notify on anomalies (e.g. high error rate)
  - **Logging & Tracing:** Structured logs (JSON), distributed tracing (OpenTelemetry)

Integration & Deployment Options

- **Data Privacy & Governance:**
  - No personally identifiable information (PII) or sensitive data logged in memory/feedback DBs
  - Data retention policies: automatic purge or archival of queries after defined period
  - Encryption at rest and in transit (TLS for APIs, AES for DB files)
- **API Key & Secret Management:**
  - Store OpenAI keys in environment variables or secret vaults (HashiCorp Vault, Cloud Key Manager)
  - Rotate keys regularly and audit access logs
- **OpenAI Usage Monitoring & Cost Control:**
  - Track token consumption per model via Prometheus metrics or OpenAI Usage API
  - Implement hard limits or alerts on monthly spend
  - Use lower-cost models (e.g., GPT-3.5) for less-critical workflows
- **Access Controls & Audit Logging:**
  - Role-based access control (RBAC) for the UI and API endpoints
  - Log every action (queries, feedback submissions, admin changes) with timestamps and user IDs
  - Integrate with SIEM for real-time security alerts

Thank You!

Jyoti Yadav

Cyber Security Data Scientist at Microsoft | Ex-Blockchain.com | Ex-EXL | Ex-Lucidian |...

Disclaimer: All the tools used or recommended in the presentation are author's own suggestions and are not officially endorsed by Microsoft