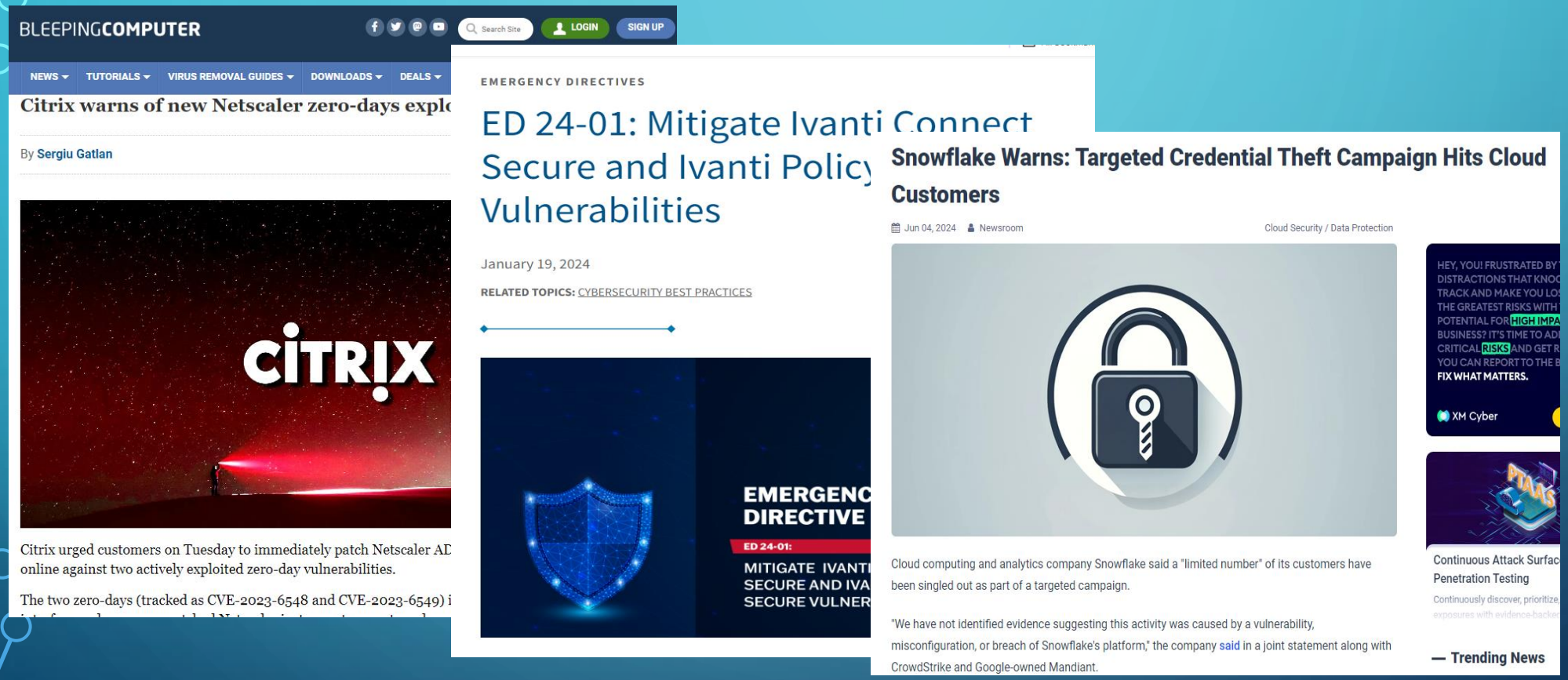
AI CYBER WATCHDOG

AN OPEN SOURCE PRIVATE AI SECURITY PROJECT

HTTPS://GITHUB.COM/THESHADORU/AI-CYBER-WATCHDOG

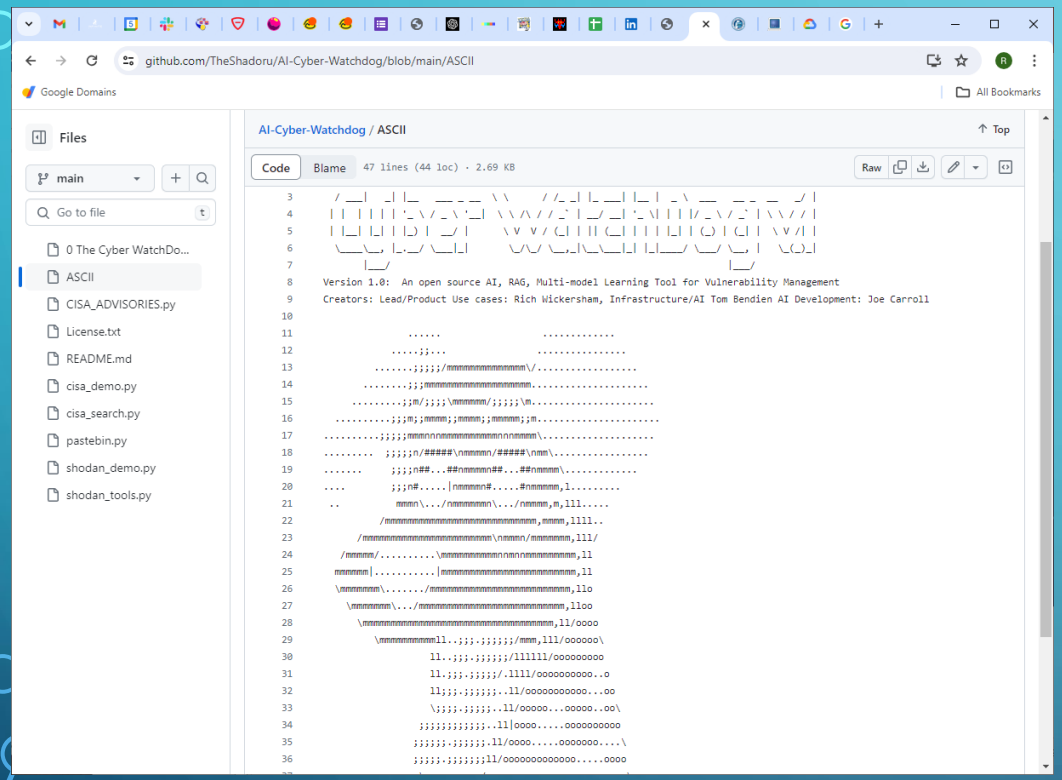
Rich Wickersham 2024
X: @richwickersham

PROBLEM



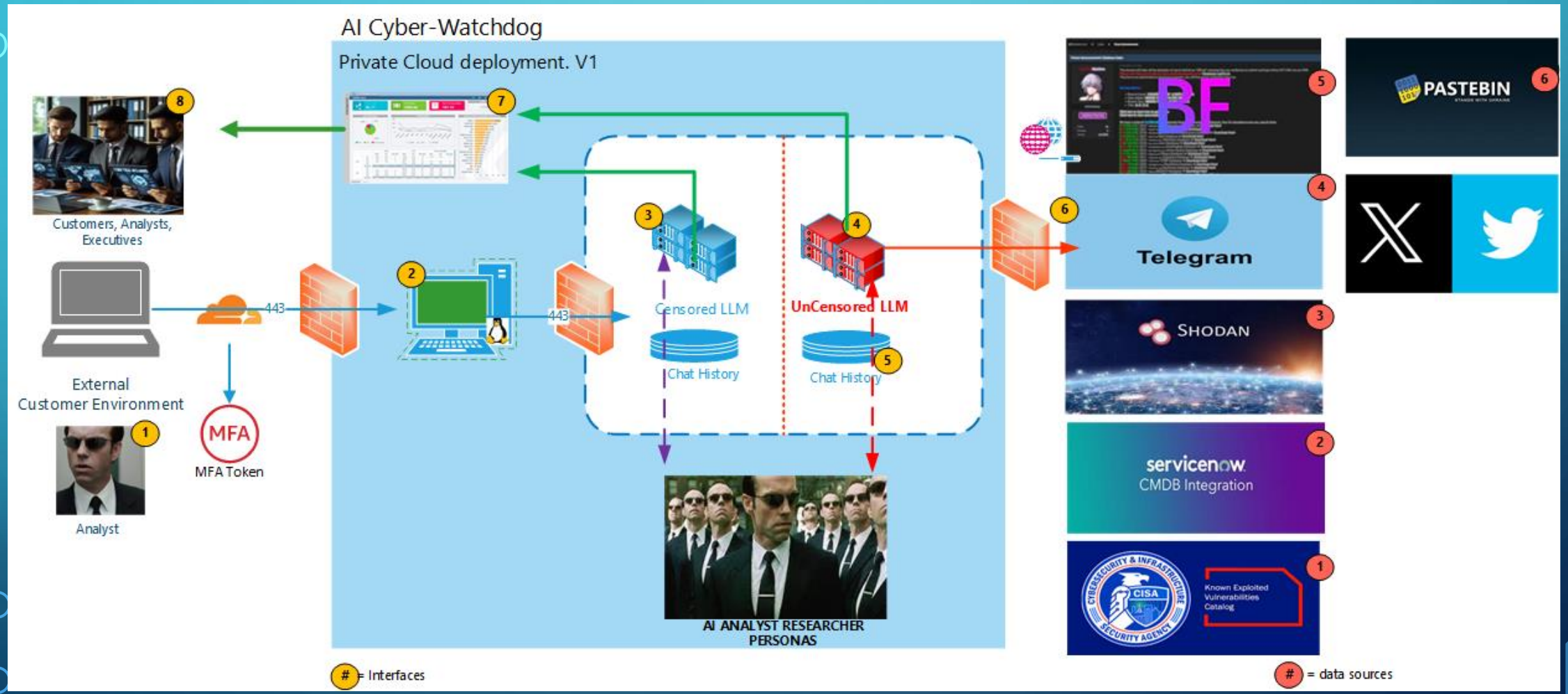
Across the private and public sector we still fail to react quickly to Zero Days or Known Exploitable Vulnerabilities, while TTE/TTKE decreases.

SOLUTION



AI Cyber-Watchdog: **https://github.com/TheShadoru/AI-Cyber-Watchdog**

DESIGN = AI-WATCHDOG ANALYST



v.1- Wickersham

SOLUTION AND REQUIREMENTS

- The AI Cyber Watchdog Project will provide actionable intelligence quickly for Known Exploitable Vulnerabilities
- Watchdog will Determine our exposure by looking both internally and externally
- Watchdog will Utilize RAG to pull in data from multiple sources(CMDB, Shodan, X, Telegram, etc) CREATE SUMMARY DATA and WRITE FILES TO VECTOR DB for further document chat/analyst interrogation.

In a world where the adversary space is speeding up we need to be faster!

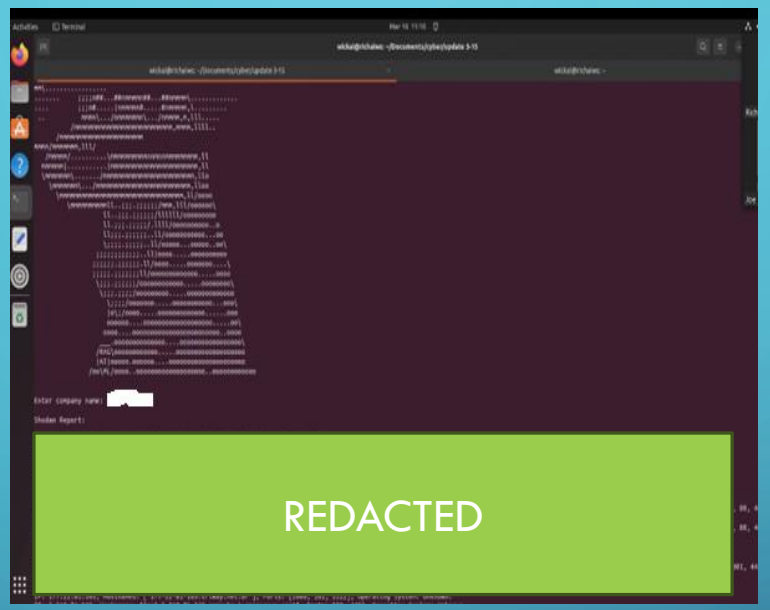
ENTERPRISE VULNERABILITY WATCH DOG

- **KEV:** A Known Exploitable Vulnerability is published (CISA RSS) to initiate the use case
- **CMDB:** Determine whether have the vulnerable infrastructure in our environment(e.g. Cisco, Citrix, Ivanti) via CMDB
- **OSINT:** The Analyst wants to search across OSINT sources, tools, Social (Shodan, Pastebin, Telegram X, etc)
- **Dark Web:** The Analyst wants to search on cybercrime forums(company mentions, code, vuln)
- **Analysis:** The Analyst wants a detailed report on inventory, patch level and likelihood of breach
- **Analysis:** The analyst will ask the AI to recommend remediation priority steps, priority and deliver summary reports
- **Retrieval Augmented Generation:**
  - Connect to Multiple sources, deliver immediate answers and save pulled data for further document chat
  - Prompt engineering will: Retrieve all potentially vulnerable hosts/infra or software in our clients enterprise environment and validate externally via OSINT data and Dark Web data.

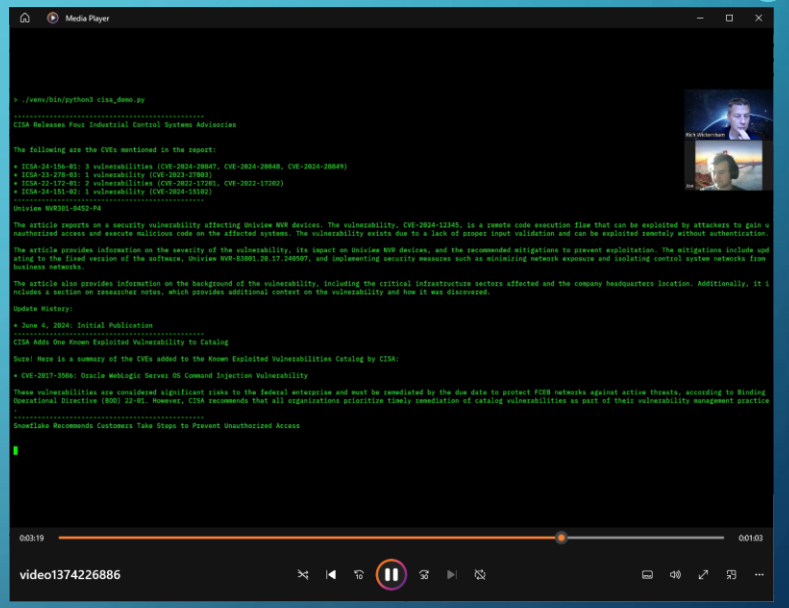
Reduce Analysis and Remediation timeline from weeks to hours

DEMO PLACEHOLDER- SHODAN-CISA-PASTEBIN

WatchDOG!



SHODAN



CISA

Increased productivity and efficiency are achieved with AI

EVALUATE A USE CASE **PRE** AND **POST AI**

Pre AI Workflow(Current State)

- 3 hours to assess the impact of a CVE(KEV)
- 1 hour to prepare the deliverable
- 1 hour to orchestrate response
- Process REPEATS for all KEV CVE or critical misconfigurations

Post AI Workflow(Target State)

- 15 minutes to generate an virtual analyst assessment
- 15 minutes for analysis
- Zero day response is accelerated!

Increased productivity and efficiency are achieved with AI

AI CYBER WATCHDOG PROCESS

1

USE CASES

Prepare Use Case Requirements,

Start Jan 2024

2

DESIGN

Evaluate Models, Prompt-engineer and Design Infra(GPU)

Start: Jan 2024

3

DESIGN

RAG APPS, TESTING, APIs

Start: Feb 2024

4

REVIEW & TUNE

RAG apps, scripts, Review output, add modules

Start: March 20YY

5

DELIVER

Functional interactive working POC

Start: March 20YY

6

PROCESS

Phase II plan, infra scaling, integration, financials

Start: April 20YY

7

BETA TESTING

Test, Tune prompts, add modules

Start: Jun 20YY

8

LAUNCH

Short Description of the launch

Start: July 20YY