

AI CYBER WATCHDOG

AN OPEN SOURCE PRIVATE AI SECURITY PROJECT

[HTTPS://GITHUB.COM/THESHADORU/AI-CYBER-WATCHDOG](https://github.com/theshadoru/ai-cyber-watchdog)

Rich Wickersham 2024

X: @richwickersham

PROBLEM



Search Site

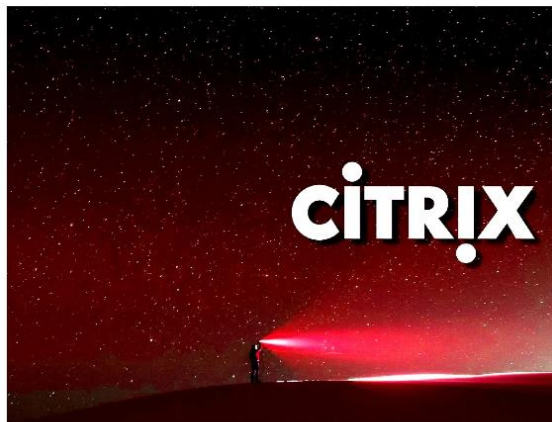
LOGIN

SIGN UP

NEWS TUTORIALS VIRUS REMOVAL GUIDES DOWNLOADS DEALS

Citrix warns of new Netscaler zero-days exploited

By Sergiu Gatlan



Citrix urged customers on Tuesday to immediately patch Netscaler ADCs online against two actively exploited zero-day vulnerabilities.

The two zero-days (tracked as CVE-2023-6548 and CVE-2023-6549) i

EMERGENCY DIRECTIVES

ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

January 19, 2024

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#)



Snowflake Warns: Targeted Credential Theft Campaign Hits Cloud Customers

Jun 04, 2024 Newsroom

Cloud Security / Data Protection



Cloud computing and analytics company Snowflake said a "limited number" of its customers have been singled out as part of a targeted campaign.

"We have not identified evidence suggesting this activity was caused by a vulnerability, misconfiguration, or breach of Snowflake's platform," the company said in a joint statement along with CrowdStrike and Google-owned Mandiant.

HEY, YOU! FRUSTRATED BY DISTRACTIONS THAT KNOCK TRACK AND MAKE YOU LOSE THE GREATEST RISKS WITH POTENTIAL FOR HIGH IMPACT BUSINESS? IT'S TIME TO ADDRESS CRITICAL RISKS AND GET READY YOU CAN REPORT TO THE BOARD. FIX WHAT MATTERS.

XM Cyber



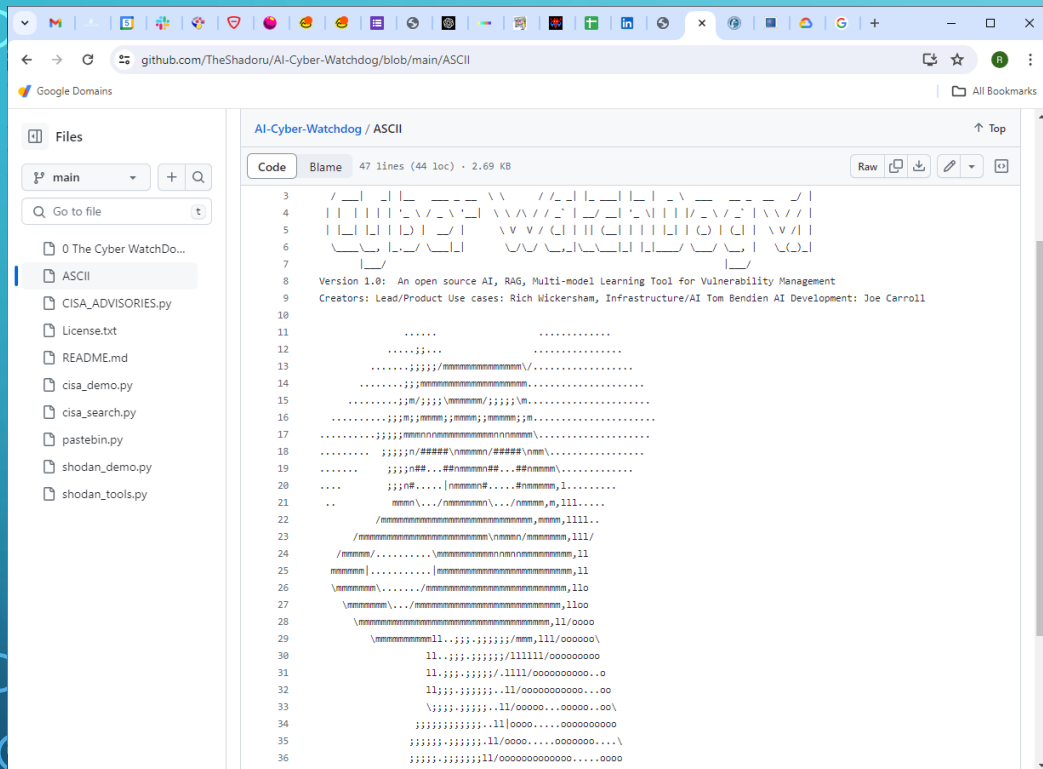
Continuous Attack Surface Penetration Testing

Continuously discover, prioritize, exposures with evidence-backed

Trending News

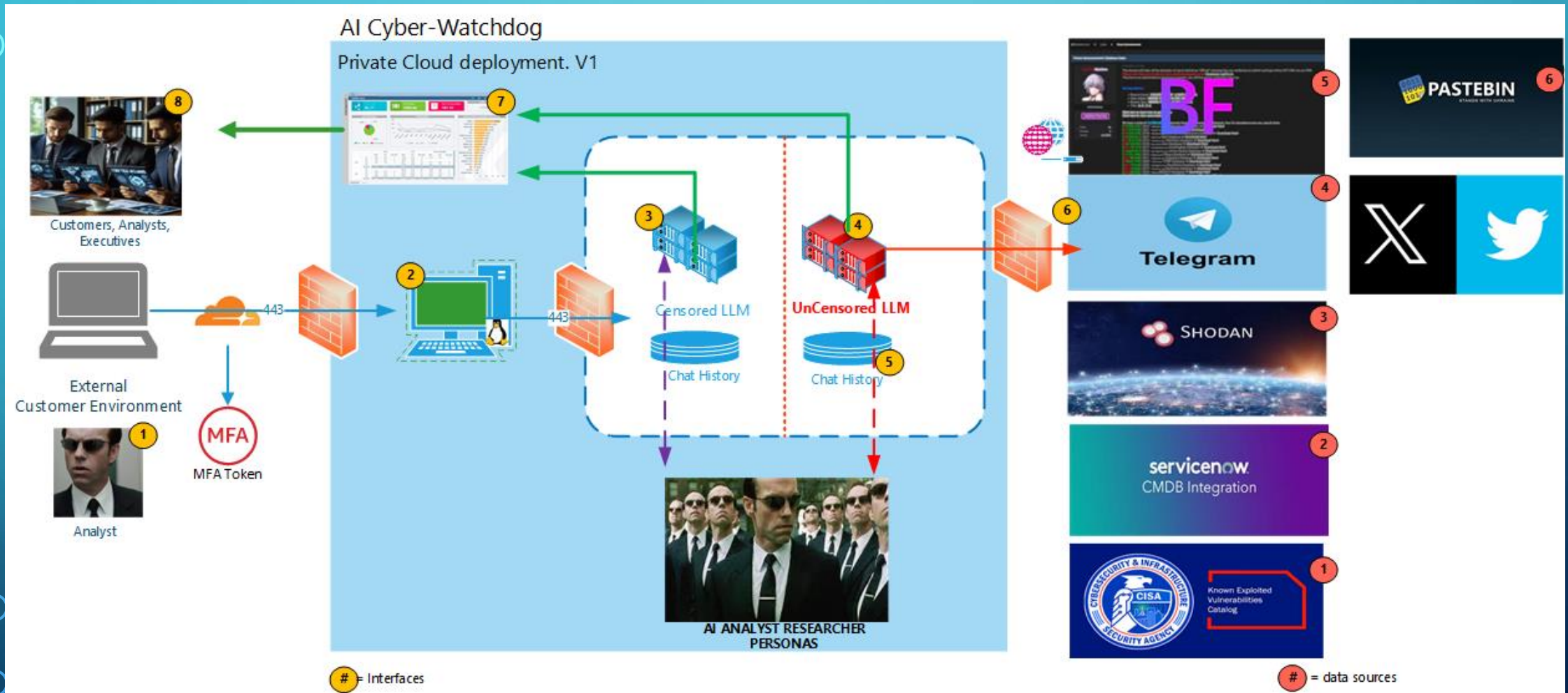
Across the private and public sector we still **fail to react quickly** to Zero Days or Known Exploitable Vulnerabilities, while TTE/TTKE decreases.

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

The image features a blue background with white circuit-like lines and a central white text area. The text area contains the title "DEMO PLACEHOLDER- SHODAN-CISA-PASTEBIN" and a list of items: "WatchDOG!", "SHODAN", "CISA", and "PASTEBIN". The "SHODAN" item is highlighted with a red background. Below the list, a white text box contains the sentence "Increased productivity and efficiency are achieved with AI".

DEMO PLACEHOLDER- SHODAN-CISA-PASTEBIN

A screenshot of a terminal window displaying the output of the WatchDog v1 tool. The output shows a list of vulnerabilities found on a target system, including CVE-2024-12345, CVE-2024-12346, and CVE-2024-12347. The terminal also shows the tool's version and the user's input.

WatchDOG!

A screenshot of the SHODAN search results page. The page displays a list of search results, including the IP address 192.168.1.1 and the domain www.example.com. The results are sorted by relevance and show the number of hits for each search term.

REDACTED

SHODAN

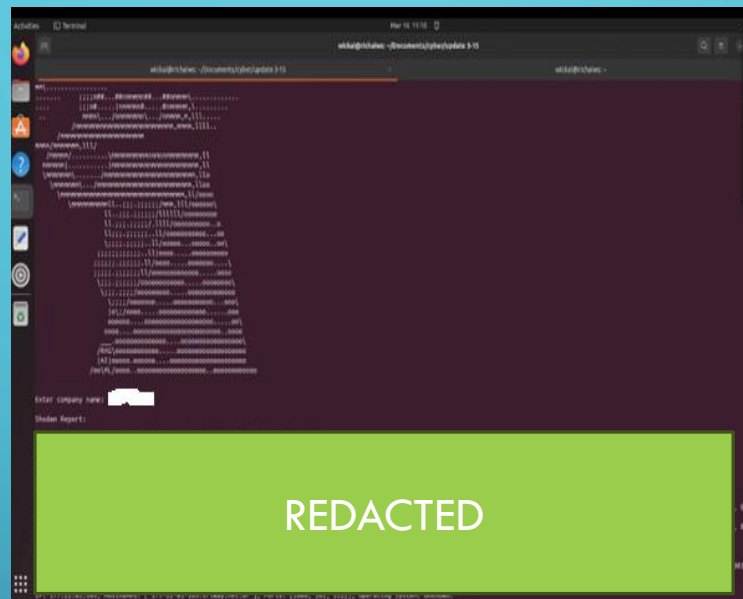
A screenshot of the CISA website displaying a vulnerability advisory. The advisory is titled "CISA Releases Four Industrial Control System Advisories" and lists four vulnerabilities: CVE-2024-12345, CVE-2024-12346, CVE-2024-12347, and CVE-2024-12348. The advisory also includes a summary of the vulnerabilities and a list of affected systems.

CISA

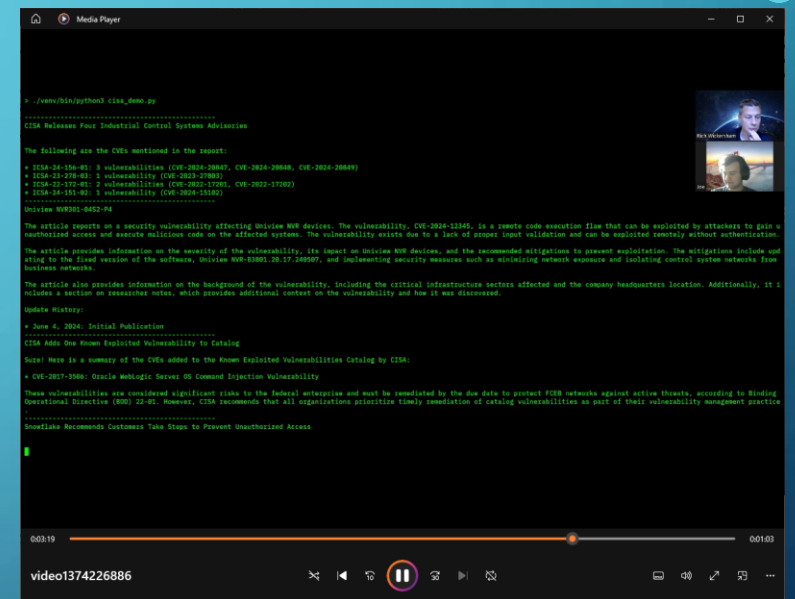
Increased productivity and efficiency are achieved with AI



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

