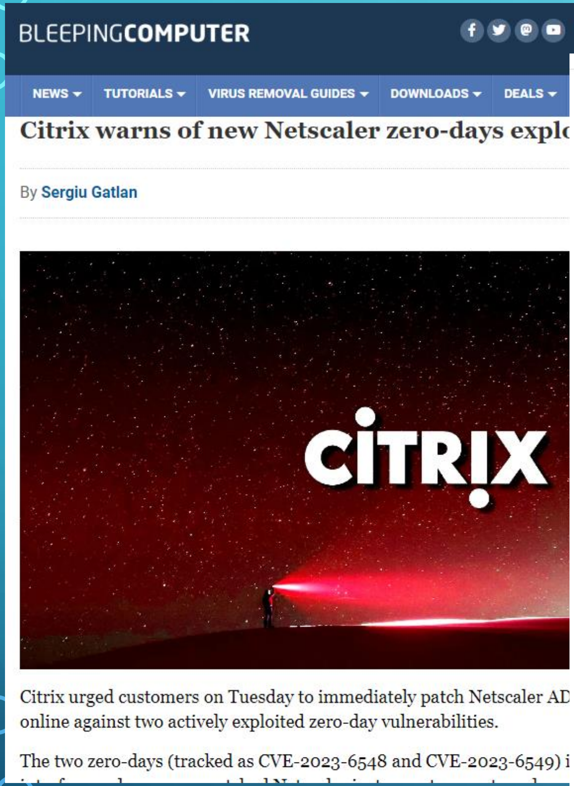
AI CYBER WATCHDOG

AN OPEN SOURCE PRIVATE AI SECURITY PROJECT

PROBLEM

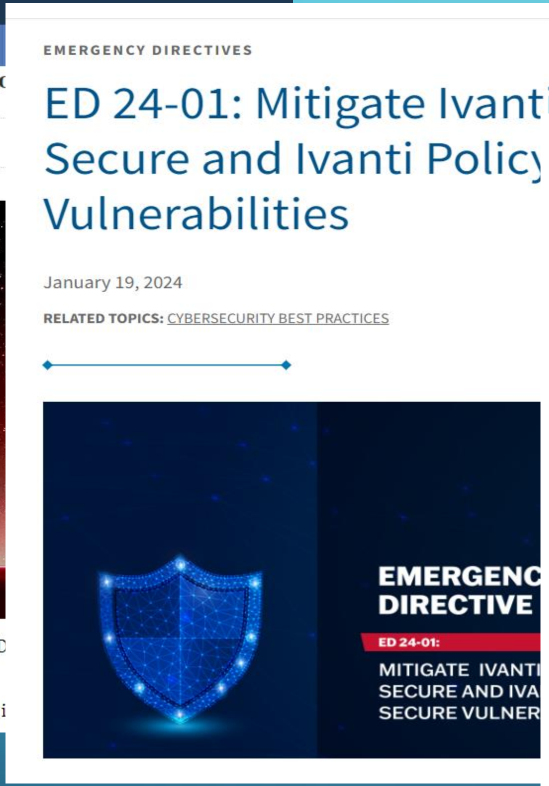


Citrix warns of new Netscaler zero-days explo

By Sergiu Gatlan

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

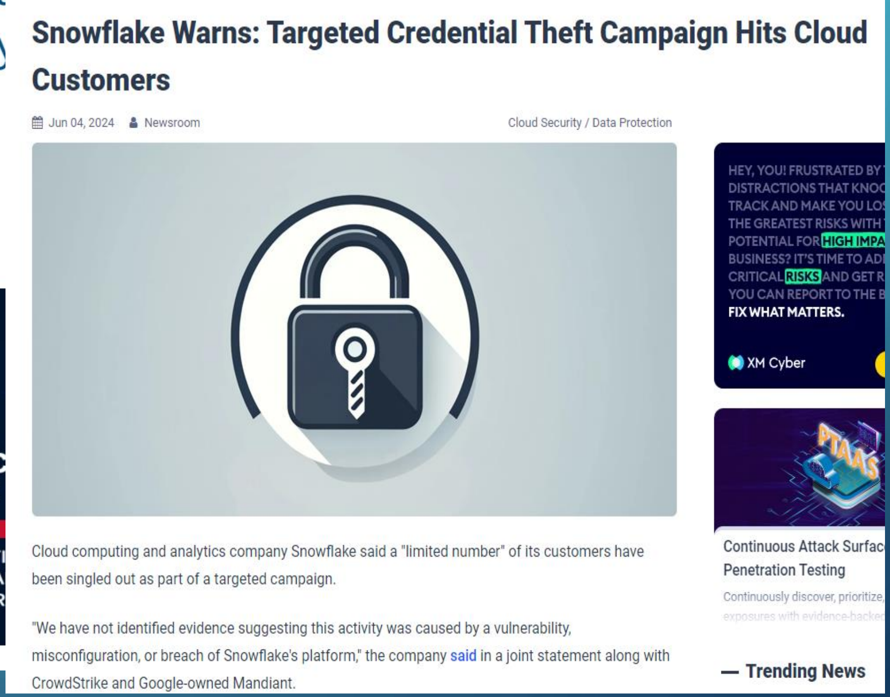
The two zero-days (tracked as CVE-2023-6548 and CVE-2023-6549) i



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

January 19, 2024

RELATED TOPICS: CYBERSECURITY BEST PRACTICES



Snowflake Warns: Targeted Credential Theft Campaign Hits Cloud Customers

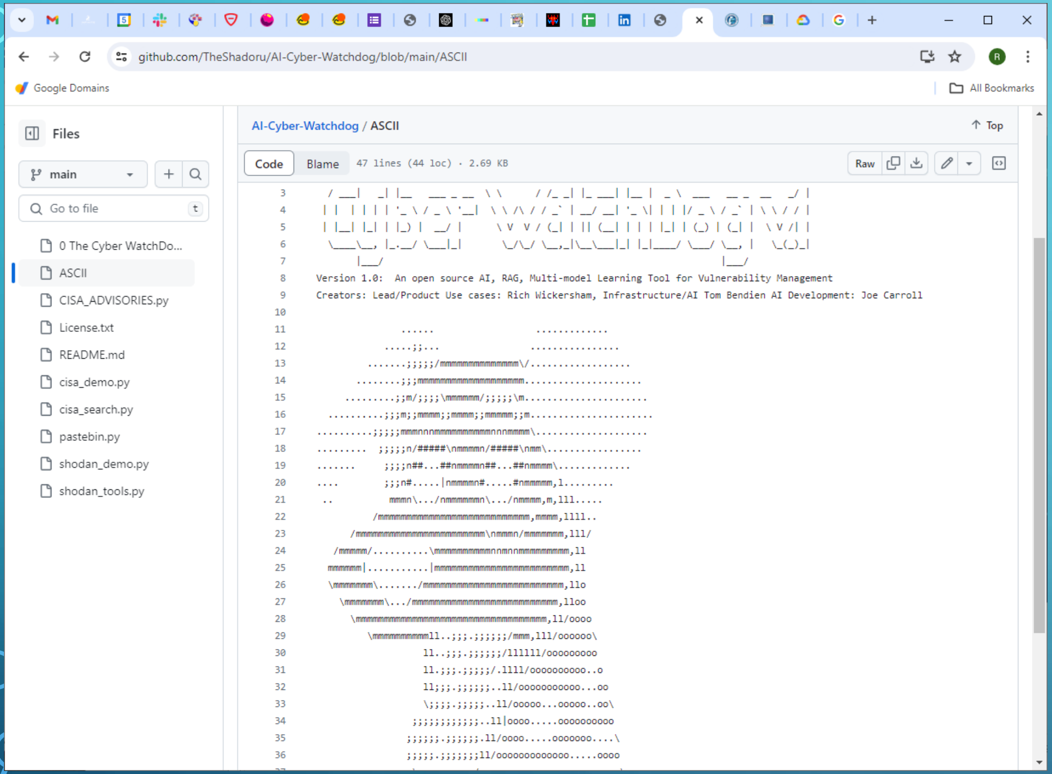
Jun 04, 2024 Newsroom Cloud Security / Data Protection

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.

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

SOLUTION



- 0 The Cyber WatchDo...
- ASCII
- CISA_ADVISORIES.py
- License.txt
- README.md
- cisa_demo.py
- cisa_search.py
- pastebin.py
- shodan_demo.py
- shodan_tools.py

AI-Cyber-Watchdog / ASCII

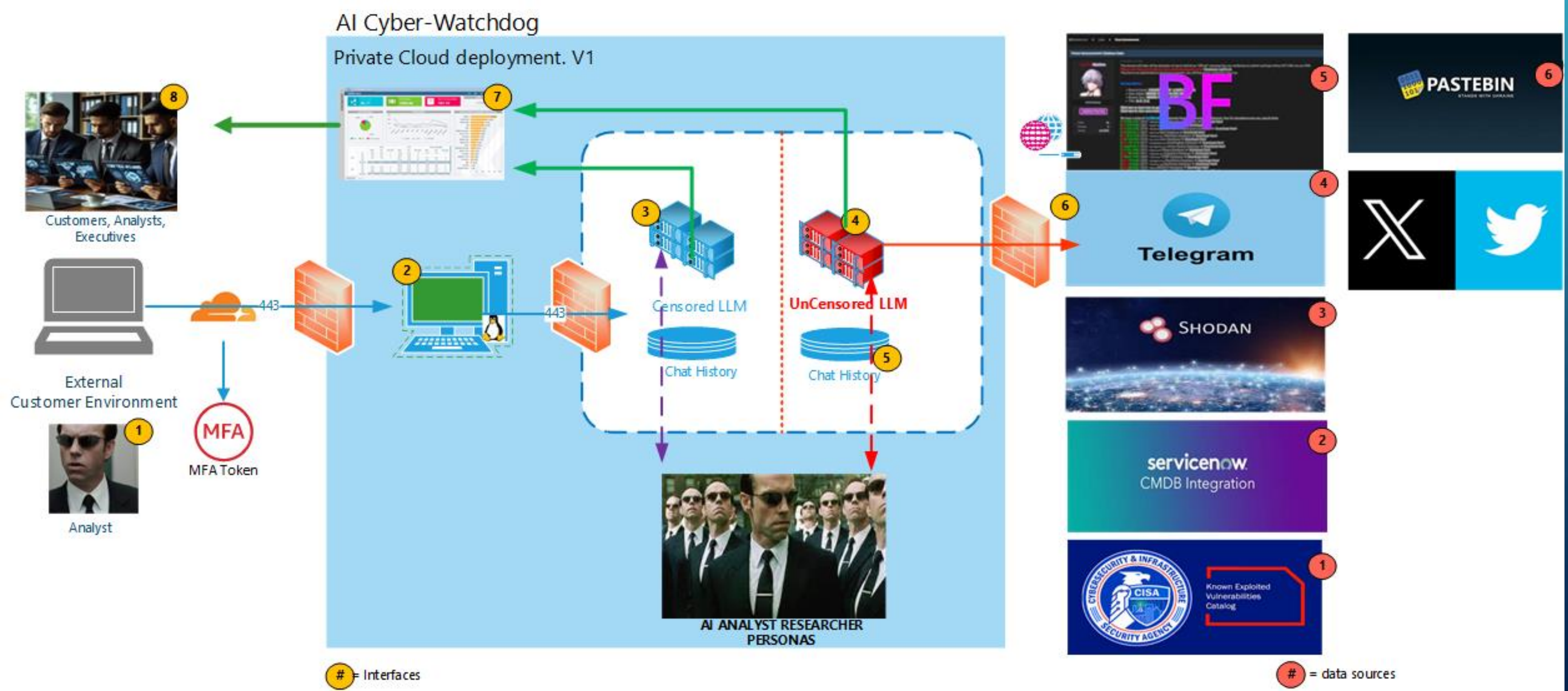
47 lines (44 loc) · 2.69 KB

```
  / ___|  _| |__   ___ _ __  \ \      / /_ _| |_ ___| |__ |  _ \  ___   __ _  __  _/ |
 | |  | | | | '_ \ / _ \ '__|  \ \ /\ / / _` | __/ __| '_ \| | | |/ _ \ / _` | \ \ / / |
 | |__| |_| | |_) |  __/ |      \ V  V / (_| | || (__| | | | |_| | (_) | (_| |  \ V /| |
  \____\__, |_.__/ \___|_|       \_/\_/ \__,_|\__\___|_| |_|____/ \___/ \__, |   \_(_)_|
       |___/                                                            |___/
Version 1.0:  An open source AI, RAG, Multi-model Learning Tool for Vulnerability Management
Creators: Lead/Product Use cases: Rich Wickersham, Infrastructure/AI Tom Bendien AI Development: Joe Carroll

               ......                 .............
             .....;;...              ................
          .......;;;;;/mmmmmmmmmmmmmm\/.................
        ........;;;mmmmmmmmmmmmmmmmmmm.....................
      .........;;m/;;;;\mmmmmm/;;;;;\m......................
   ..........;;;m;;mmmm;;mmmm;;mmmmm;;m.......................
 ..........;;;;;mmmnnnmmmmmmmmmmmnnnmmmm\....................
 .........  ;;;;;n/#####\nmmmmn/#####\nmm\.................
 .......     ;;;;n##...##nmmmmn##...##nmmmm\.............
 ....        ;;;n#.....|nmmmmn#.....#nmmmmm,l.........
  ..          mmmn\.../nmmmmmmn\.../nmmmm,m,lll.....
           /mmmmmmmmmmmmmmmmmmmmmmmmmmmm,mmmm,llll..
       /mmmmmmmmmmmmmmmmmmmmmmm\nmmmn/mmmmmmm,lll/
    /mmmmm/..........\mmmmmmmmmmnmnnmmmmmmmmm,ll
   mmmmmm|...........|mmmmmmmmmmmmmmmmmmmmmmmmm,ll
   \mmmmmmm\......./mmmmmmmmmmmmmmmmmmmmmmmmmm,llo
     \mmmmmmm\.../mmmmmmmmmmmmmmmmmmmmmmmmmmmm,lloo
       \mmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmm,ll/oooo
          \mmmmmmmmmmll..;;;.;;;;;;;/mmm,lll/oooooo\
                    ll..;;;.;;;;;;;/llllll/ooooooooo
                    ll.;;;.;;;;;/.llll/oooooooooo..o
                    ll;;;.;;;;;;..ll/ooooooooooo...oo
                    \;;;;.;;;;;..ll/ooooo...ooooo..oo\
                  ;;;;;;;;;;;;..ll|oooo.....oooooooooo
                 ;;;;;;.;;;;;;.ll/oooo.....ooooooo....\
                 ;;;;;.;;;;;;;ll/ooooooooooooo.....oooo
```

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

SOLUTION = AI-WATCHDOG ANALYST



SOLUTION AND REQUIREMENTS

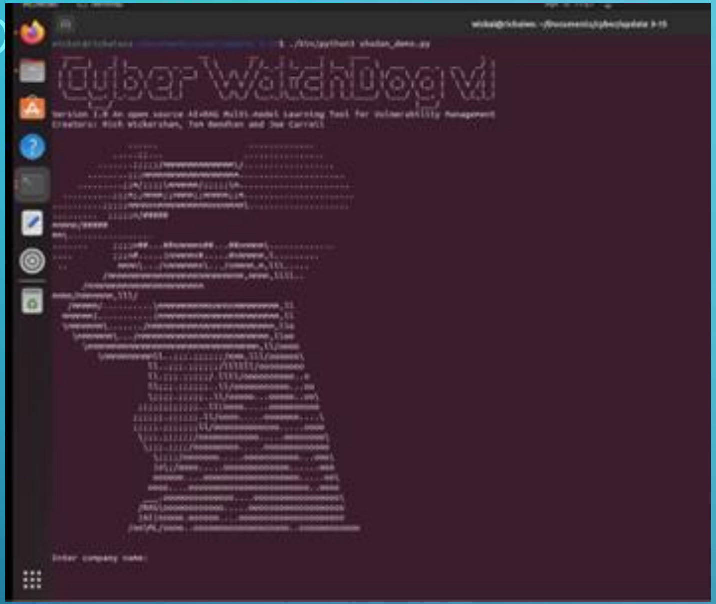
- The AI Cyber Watchdog Project will provide actionable intelligence quickly for Known Exploitable Vulnerabilities
- Watchdog will Determine our exposure by looking both internally and externally
- Watchdog will Utilize RAG to pull in data from multiple sources(CMDB, Shodan, X, Telegram, etc) CREATE 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 by(CISA) to initiate the project
- **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)
- The Analyst wants a detailed report on inventory, patch level and likelihood of breach
- 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/ devices or software in our clients enterprise environment and validate via OSINT data and dark web data whether we have an issue.

Reduce Analysis and Remediation timeline from weeks to hours

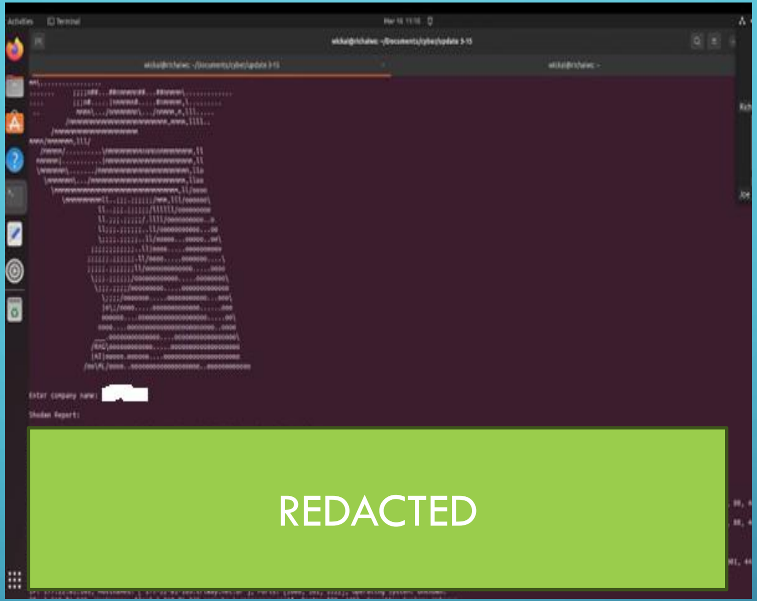
DEMO PLACEHOLDER- SHODAN-CISA-PASTEBIN



```
$ ./bin/python3 shodan_demo.py
Cyber WatchDog v1
Version 1.0 An open source AI+RAG Multi-Model Learning Tool for Vulnerability Management
Creators: Rich Wickersham, Tom Bandhan and Joe Carroll

Enter company name:
```

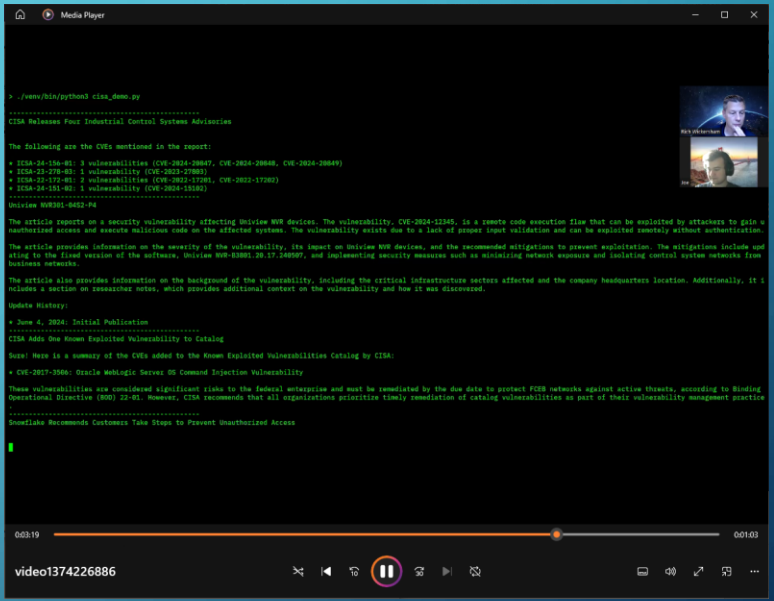
WatchDOG!



```
Enter company name: [redacted]
Shodan Report:
```

REDACTED

SHODAN



```
> ./venv/bin/python3 cisa_demo.py

-----------------------------------------------
CISA Releases Four Industrial Control Systems Advisories


The following are the CVEs mentioned in the report:

* ICSA-24-156-01: 3 vulnerabilities (CVE-2024-20847, CVE-2024-20848, CVE-2024-20849)
* ICSA-23-278-03: 1 vulnerability (CVE-2023-27803)
* ICSA-22-172-01: 2 vulnerabilities (CVE-2022-17201, CVE-2022-17202)
* ICSA-24-151-02: 1 vulnerability (CVE-2024-15102)
-----------------------------------------------
Uniview NVR301-04S2-P4

The article reports on a security vulnerability affecting Uniview NVR devices. The vulnerability, CVE-2024-12345, is a remote code execution flaw that can be exploited by attackers to gain u
nauthorized access and execute malicious code on the affected systems. The vulnerability exists due to a lack of proper input validation and can be exploited remotely without authentication.

The article provides information on the severity of the vulnerability, its impact on Uniview NVR devices, and the recommended mitigations to prevent exploitation. The mitigations include upd
ating to the fixed version of the software, Uniview NVR-B3801.20.17.240507, and implementing security measures such as minimizing network exposure and isolating control system networks from
business networks.

The article also provides information on the background of the vulnerability, including the critical infrastructure sectors affected and the company headquarters location. Additionally, it i
ncludes a section on researcher notes, which provides additional context on the vulnerability and how it was discovered.

Update History:

* June 4, 2024: Initial Publication
-----------------------------------------------
CISA Adds One Known Exploited Vulnerability to Catalog

Sure! Here is a summary of the CVEs added to the Known Exploited Vulnerabilities Catalog by CISA:

* CVE-2017-3506: Oracle WebLogic Server OS Command Injection Vulnerability

These vulnerabilities are considered significant risks to the federal enterprise and must be remediated by the due date to protect FCEB networks against active threats, according to Binding
Operational Directive (BOD) 22-01. However, CISA recommends that all organizations prioritize timely remediation of catalog vulnerabilities as part of their vulnerability management practice
.
-----------------------------------------------
Snowflake Recommends Customers Take Steps to Prevent Unauthorized Access
```

CISA

Increased productivity and efficiency are achieved with AI

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

Pre AI Workflow(Current State)

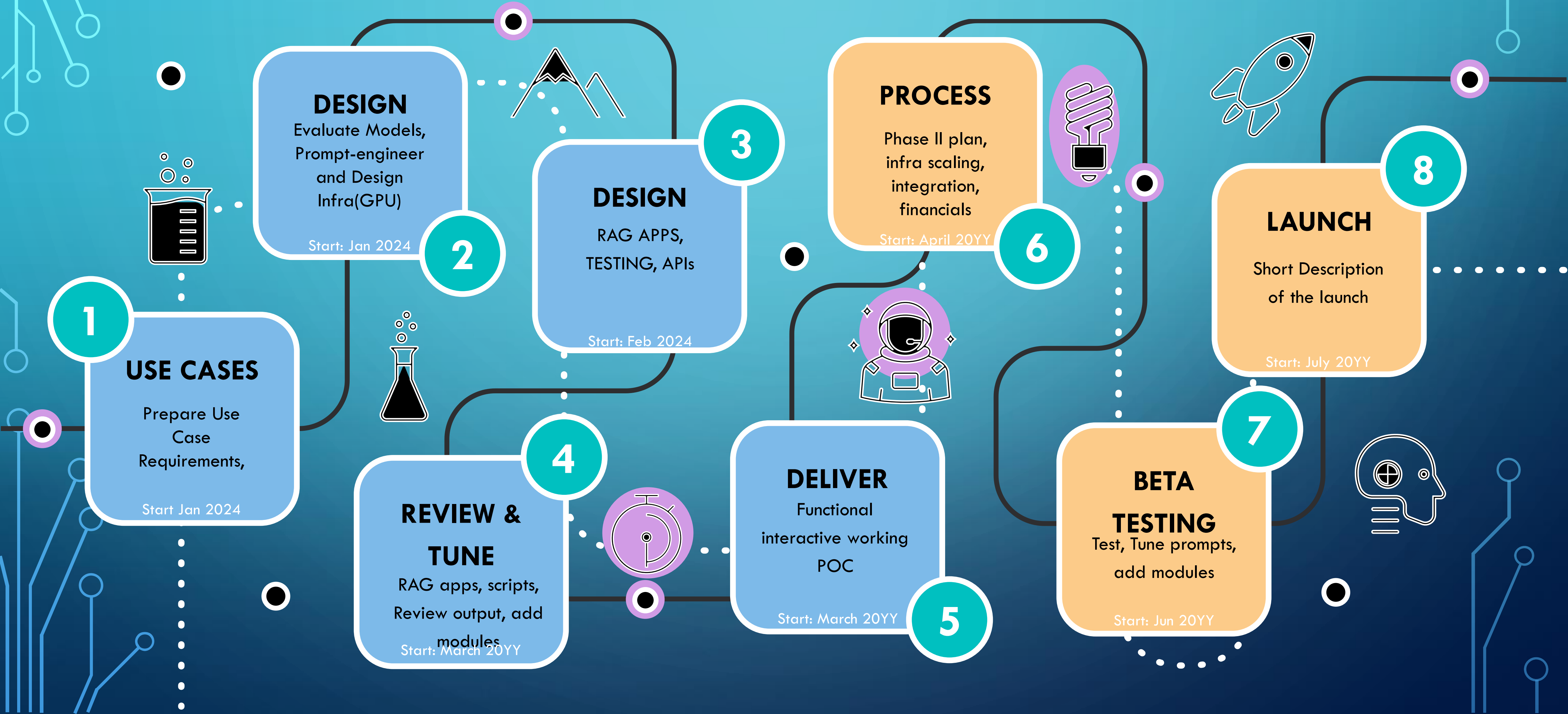
- 3 hours to assess the impact of a CVE(KEV)
- 1 hour to prepare the deliverable
- 1 hour to orchestrate response
- Process REPEATS for all KEV CVE or critical misconfigurations

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