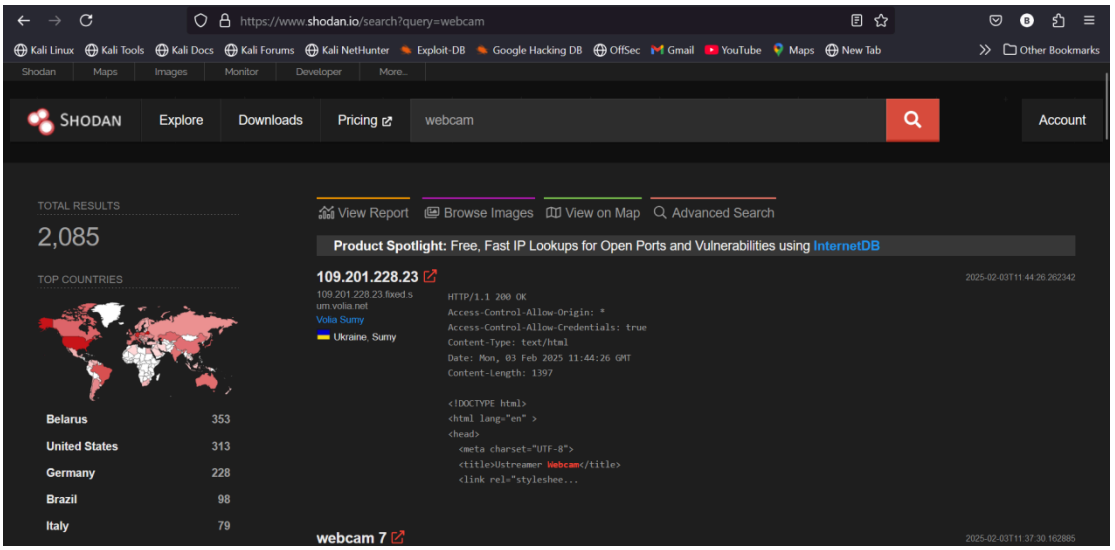
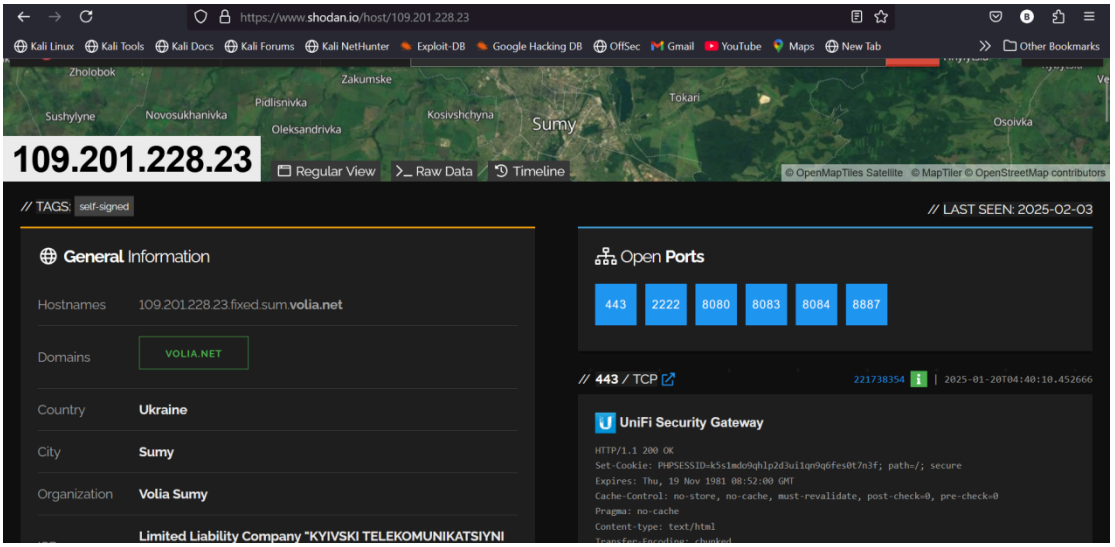
THREAT INTELLIGENCE USING OSINT

In this report we used shodan to look for vulnerabilities of IoT devices on the internet. Webcam results were more than two thousand. Each webcam has an ip address, city and country .

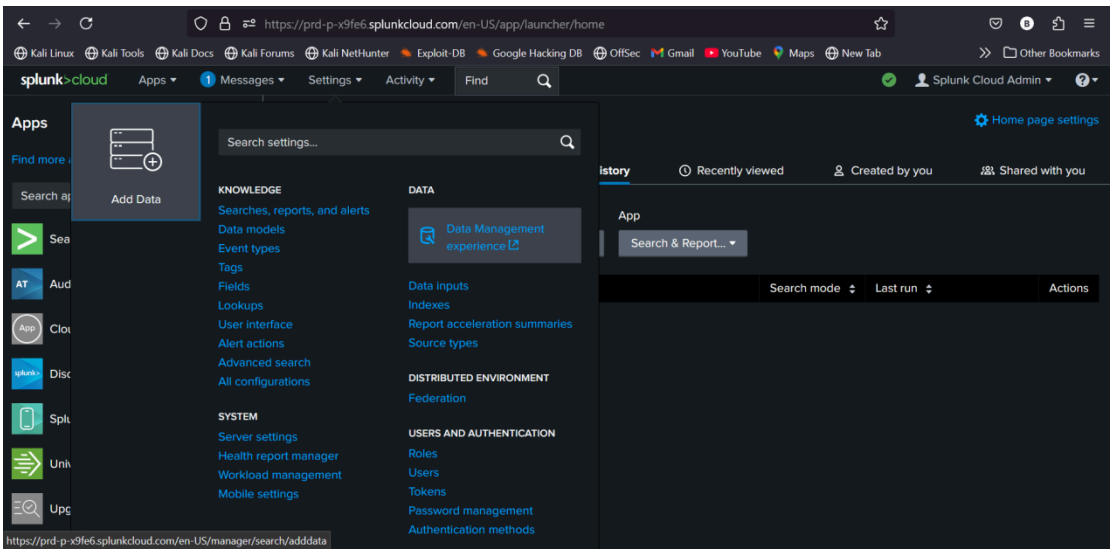


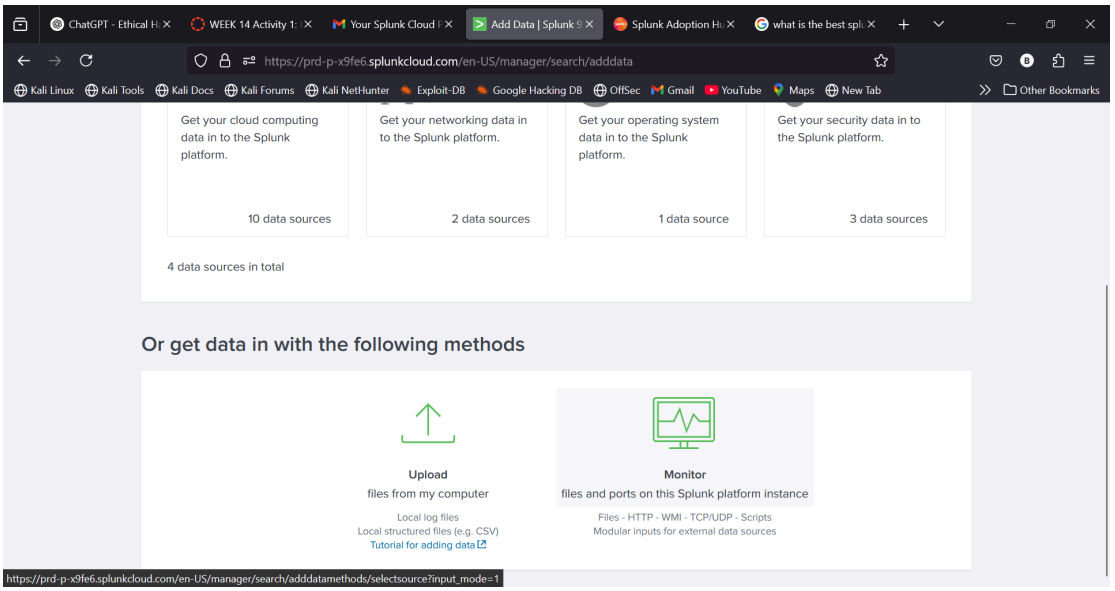
Upon clicking the first IP address, it displayed, open ports and status of the ssl certificate.

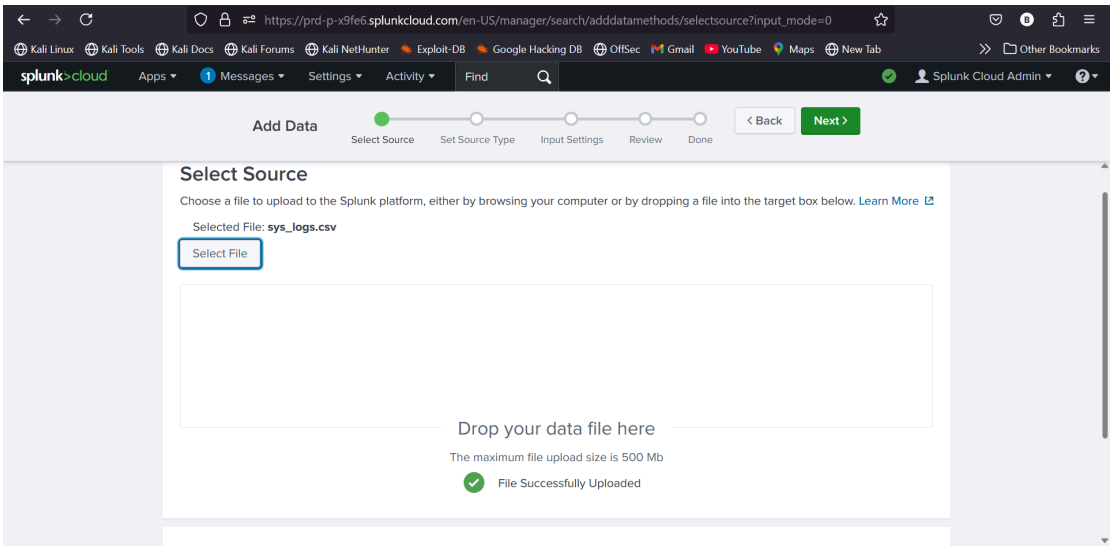


COLLECTING AND ANALYZING DATA USING SPLUNK

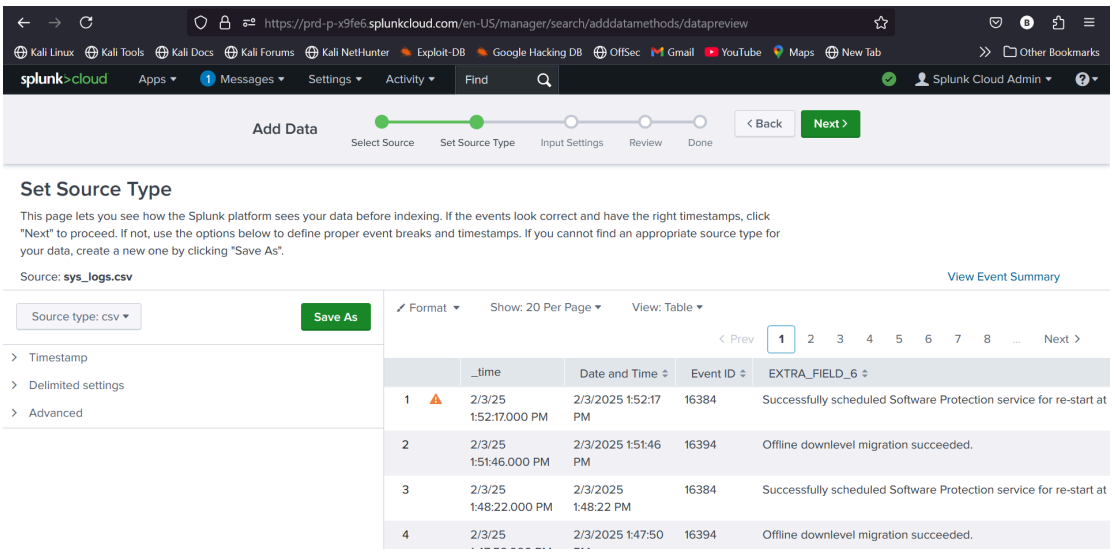
In this report I used splunk cloud to perform log analysis. After creating an instance I logged into my cloud instance and added data that contained already saved event logs from my pc.



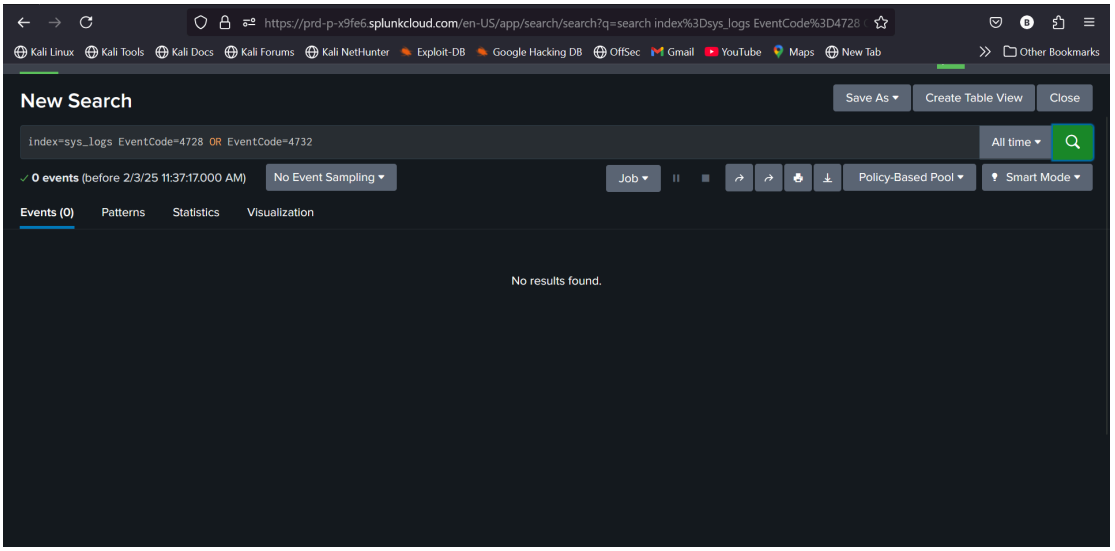




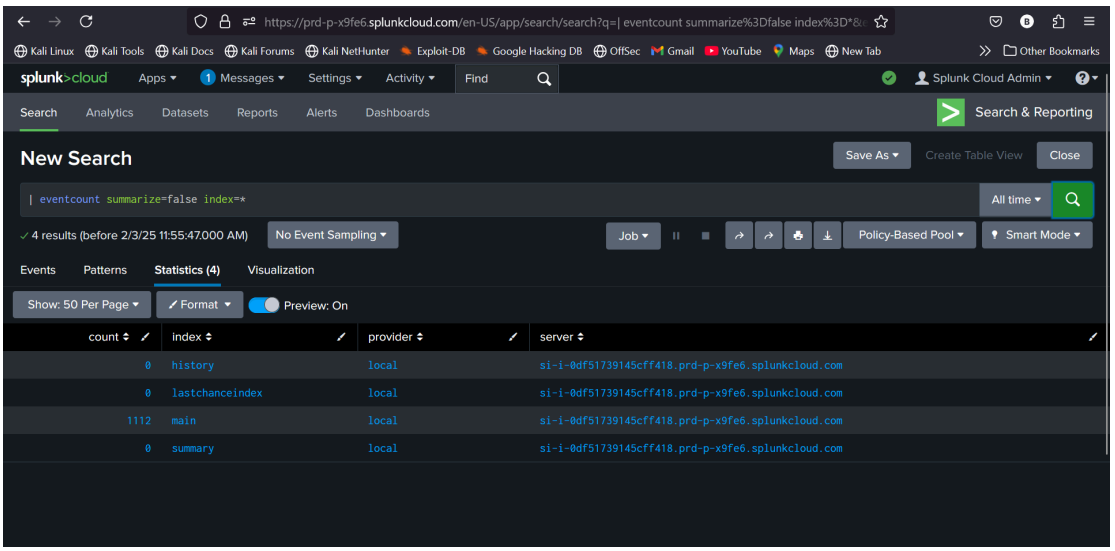
The file containing the logs was already saved in .cvs. The next step was to ensure the configurations are correct. Splunk automatically detects the source type, index and time stamp setting.

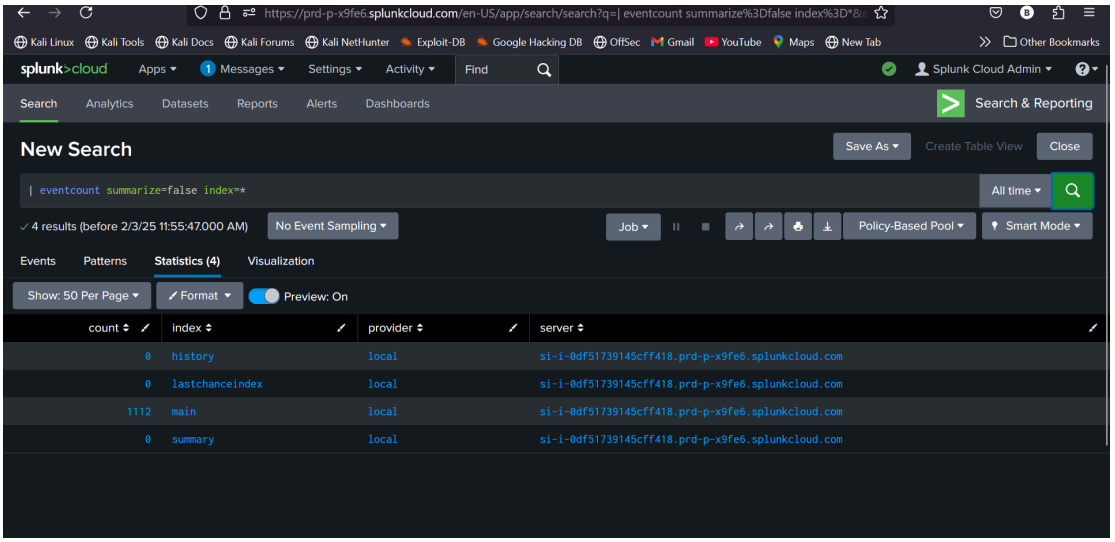


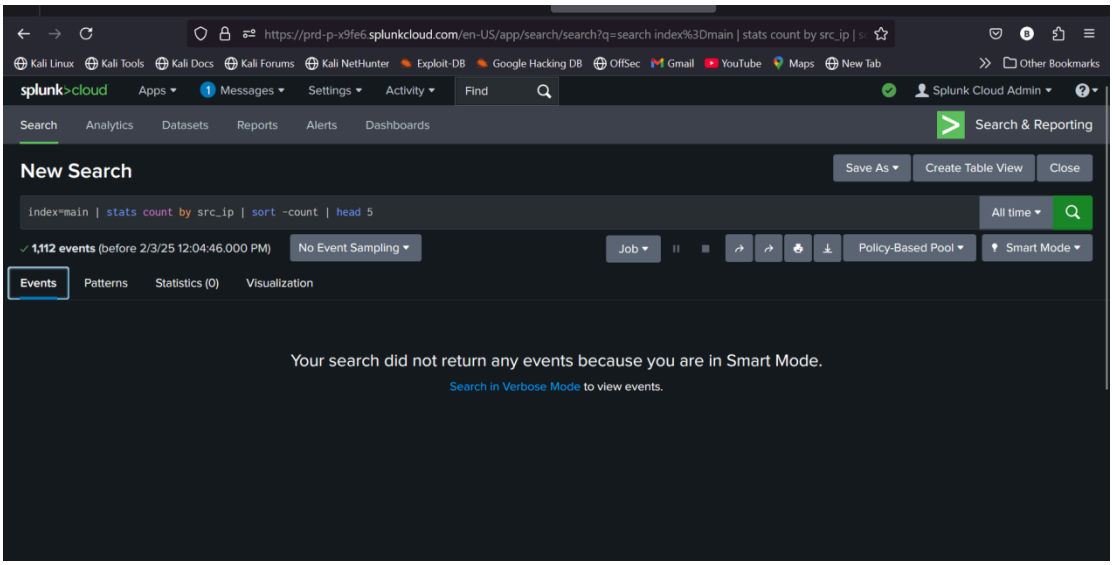
After the events were ready to be analyzed , I tried searching if there was privilege escalation but there was none.



To find out what indexes I will use according to how splunk has ingested my file, I ran the command | ‘eventcount summarize=false index=*’. The index was main since splunk automatically allocated a general index of main because I did not configure the indexes when uploading. There was no brute-force attempt or login from a different region. No privilege escalation attempt was made.







How to improve security in a network system

- Using firewalls - using network firewalls to block unauthorized traffic is essential in filtering malicious traffic. Firewalls also have a feature of blacklisting and whitelisting making it a good tool to protect a given network.
- Network segmentation - separating internal networks, guests and IoT networks is a good practice that prevents escalation of attacks or even DDOs attack.
- Using VPNs - VPNs enables protected remote access of a network by masking the IP address of a user.
- Multi-factor authentication - use of passwords, biometrics and OTPs to log into a network prohibits successful bruteforce or rainbow attack. The passwords should also be strong ones that include special characters, numericals, lowercase and uppercase letters and they should be long.
- Least privilege - this includes role-based access control where a user has the minimum access to data that is necessary. It also includes separation of roles where a user is given one role and cannot do roles he or she is not supposed to.
- Encryption - implementing SSL/TLS on data in transit helps protect it from man-in-the-middle attack.
- Regular updates and patches - network devices should be up to date to prevent attackers from making use of the vulnerabilities that have already been patched by the manufacturer.
- Regular security audits- this is to ensure vulnerabilities are patched on time.
- Awareness and training - sensitizing employees to ensure they uphold the security standards required to secure networks and not to fall victims of social engineering.