

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 .

The screenshot shows the Shodan search results page for the query 'webcam'. The page displays a total of 2,085 results. A world map highlights the top countries: Belarus (353), United States (313), Germany (228), Brazil (98), and Italy (79). The first result is for IP address 109.201.228.23, located in Sumy, Ukraine. The page also shows a 'Product Spotlight' for 'Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB'. The search bar at the top shows the query 'webcam' and the 'Account' button.

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

The screenshot shows the Shodan host details page for IP address 109.201.228.23. The page displays a map of the location (Sumy, Ukraine) and a list of open ports: 443, 2222, 8080, 8083, 8084, and 8887. The 'General Information' section shows the hostnames (109.201.228.23.fixed.sum.volia.net), domains (VOLIA.NET), country (Ukraine), city (Sumy), and organization (Volia Sumy). The 'Open Ports' section shows the status of the ports (443/TCP). The 'UniFi Security Gateway' section shows the status of the gateway (HTTP/1.1 200 OK).

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 first screenshot shows the Splunk Cloud 'Add Data' menu. The 'Data' section is expanded, showing options like 'Data Management experience', 'Data inputs', 'Indexes', 'Report acceleration summaries', and 'Source types'. The 'SYSTEM' section includes 'Server settings', 'Health report manager', 'Workload management', and 'Mobile settings'. The 'DISTRIBUTED ENVIRONMENT' section includes 'Federation'. The 'USERS AND AUTHENTICATION' section includes 'Roles', 'Users', 'Tokens', 'Password management', and 'Authentication methods'.

The second screenshot shows the 'Add Data' wizard. It displays four data sources: '10 data sources', '2 data sources', '1 data source', and '3 data sources', totaling 4 data sources. Below this, it lists two methods: 'Upload' (files from my computer) and 'Monitor' (files and ports on this Splunk platform instance). The 'Upload' method is selected, showing options for 'Local log files' and 'Local structured files (e.g. CSV)'. A link to 'Tutorial for adding data' is provided.

The third screenshot shows the 'Select Source' step of the 'Add Data' wizard. The 'Selected File' is 'sys_logs.csv'. A 'Select File' button is visible. Below the file selection area, there is a 'Drop your data file here' section with a note: 'The maximum file upload size is 500 Mb'. A green checkmark indicates 'File Successfully Uploaded'.

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

← → ↻ https://prd-p-x9fe6.splunkcloud.com/en-US/manager/search/adddatamethods/datapreview

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Gmail YouTube Maps New Tab

splunk>cloud Apps Messages Settings Activity Find Splunk Cloud Admin

Add Data Select Source Set Source Type Input Settings Review Done < Back Next >

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **sys_logs.csv** [View Event Summary](#)

Source type: csv **Save As**

Timestamp
Delimited settings
Advanced

Format Show: 20 Per Page View: Table

< Prev 1 2 3 4 5 6 7 8 ... Next >

	_time	Date and Time	Event ID	EXTRA_FIELD_6
1	2/3/25 1:52:17.000 PM	2/3/2025 1:52:17 PM	16384	Successfully scheduled Software Protection service for re-start at
2	2/3/25 1:51:46.000 PM	2/3/2025 1:51:46 PM	16394	Offline downlevel migration succeeded.
3	2/3/25 1:48:22.000 PM	2/3/2025 1:48:22 PM	16384	Successfully scheduled Software Protection service for re-start at
4	2/3/25	2/3/2025 1:47:50	16394	Offline downlevel migration succeeded.

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

← → ↻ https://prd-p-x9fe6.splunkcloud.com/en-US/app/search/search?q=search index%3Dsys_logs EventCode%3D4728

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Gmail YouTube Maps New Tab

New Search Save As Create Table View Close



Index=sys_logs EventCode=4728 OR EventCode=4732 All time




0 events (before 2/3/25 11:37:17.000 AM) No Event Sampling Job


Events (0) Patterns Statistics Visualization

No results found.




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.



← → ↻ https://prd-p-x9fe6.splunkcloud.com/en-US/app/search/search?q=|eventcount summarize%3Dfalse index%3D*&...  

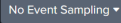





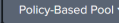
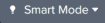
splunk>cloud Apps  Settings  Find 

Search Analytics Datasets Reports Alerts Dashboards 


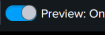
New Search



| eventcount summarize=false index=*  




✓ 4 results (before 2/3/25 11:55:47.000 AM)        


Events Patterns **Statistics (4)** Visualization

Show: 50 Per Page  




count	index	provider	server
0	history	local	si-i-0df51739145cff418.prd-p-x9fe6.splunkcloud.com
0	lastchanceindex	local	si-i-0df51739145cff418.prd-p-x9fe6.splunkcloud.com
1112	main	local	si-i-0df51739145cff418.prd-p-x9fe6.splunkcloud.com
0	summary	local	si-i-0df51739145cff418.prd-p-x9fe6.splunkcloud.com



← → ↻ https://prd-p-x9fe6.splunkcloud.com/en-US/app/search/search?q=|eventcount summarize%3Dfalse index%3D*&...  

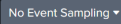





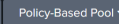
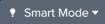
splunk>cloud Apps  Settings  Find 

Search Analytics Datasets Reports Alerts Dashboards 


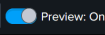
New Search



| eventcount summarize=false index=*  




✓ 4 results (before 2/3/25 11:55:47.000 AM)        


Events Patterns **Statistics (4)** Visualization

Show: 50 Per Page  


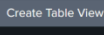

count	index	provider	server
0	history	local	si-i-0df51739145cff418.prd-p-x9fe6.splunkcloud.com
0	lastchanceindex	local	si-i-0df51739145cff418.prd-p-x9fe6.splunkcloud.com
1112	main	local	si-i-0df51739145cff418.prd-p-x9fe6.splunkcloud.com
0	summary	local	si-i-0df51739145cff418.prd-p-x9fe6.splunkcloud.com



← → ↻ https://prd-p-x9fe6.splunkcloud.com/en-US/app/search/search?q=search index%3Dmain | stats count by src_ip | s...  

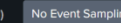





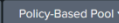
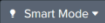
splunk>cloud Apps  Settings  Find 

Search Analytics Datasets Reports Alerts Dashboards 

New Search

index=main | stats count by src_ip | sort -count | head 5  

✓ 1,112 events (before 2/3/25 12:04:46.000 PM)        

Events Patterns Statistics (0) Visualization

Your search did not return any events because you are in Smart Mode.
[Search in Verbose Mode to view events.](#)

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 brute force or rainbow attack. The passwords should also be strong ones that include special characters, numerals, 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.