NGSOTI Project: 101127921 DIGITAL-ECCC-2022-CYBER-03 Learning from large-scale IPv4 blackhole: Behavioral analysis of SNMP traffic

Team CIRCL/NGSOTI

Co-funded by
the European Union

NGSOTI

CIRCL
Computer Incident
Response Center
Luxembourg

2025-11-30

Contents

1 Behavioral Analysis of the SNMP traffic **3**
1.1 Disclaimer . . . 3
1.2 Executive summary . . . 3
1.3 Acknowledgements . . . 4

2 Analysis scope **5**
2.1 Dataset . . . 5
2.2 Data lake setup . . . 5
2.3 General Statistical analysis . . . 7
2.3.1 SNMP Activity . . . 7
2.3.2 Country repartition . . . 8
2.3.3 SNMP version repartition . . . 13
2.3.4 SNMP Community . . . 15
2.3.5 Devices scanned. . . . 17
2.3.6 Vulnerabilities and exploits . . . 20
2.4 Anomalies investigation . . . 20
2.4.1 Palestinian Traffic . . . 20
2.5 Scanning vendor Traffic . . . 22
2.5.1 Censys . . . 22
2.5.2 NetSecScan . . . 25
2.5.3 Shadowserver . . . 25
2.5.4 ShadowForce . . . 25
2.5.5 Shodan . . . 25

3 TODO - TO REMOVE **25**
3.0.1 Vulnerabilities and exploits . . . 26
3.1 TO ANALYSE . . . 26
3.1.1 MISCONFIG . . . 26

4 Additional References **26**

5 Conclusions **26**

List of Figures

1 SNMP activity 7
2 Country repartition 8
3 IPv4 Repartition 9
4 Packet sent by BGP AS 10
5 Source IP per BGP AS 12
6 Version repartition 14
7 Community repartition 15
8 Devices to community 17
9 Top vendors 18
10 Scan Coverage 19

1 Behavioral Analysis of the SNMP traffic

1.1 Disclaimer

On 17/11/2025 This document is still a work in progress.

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

1.2 Executive summary

The missions of the european Project **NGSOTI** (Next Generation Security Operator Training Infrastructure), is to empower SOC operators and organisations across Europe with the knowledge, tools, and infrastructure needed to defend effectively against ever-evolving cyber threats. (restena.lu[1]). Within this scope the key objective is to enhance SOC operator capabilities.

SOCs carry the crucial mission of monitoring cybersecurity events and escalating any incidents or detections of malicious activity. While the task may seem straightforward, it is in fact increasingly complex. Attackers continuously evolve their techniques, thereby forcing SOC analysts to keep adapting.

These analysts are confronted with a dual challenge:

- On one hand, they must be versatile generalists, capable of responding across a wide spectrum of domains.
- On the other hand, the volume of alerts and information they must process frequently leads to cognitive fatigue.

This fatigue inevitably results in reduced alertness and motivation, which can lead to miss-detections of critical incidents.

Our sinkhole-based analysis is aligned with the core ambition of NGSOTI: to develop an open-source training infrastructure powered by real-world data that equips future SOC operators with advanced capabilities in network-related alert handling, incident response, log analysis, security operations management, threat intelligence, and communication. (restena.lu)

In this context, we target two complementary goals: Primarly, it will provide key insights and enriched data that enable SOC teams to understand threats to be able to detect attacks with finer granularity.

Secondly , our goal is to reduce operator fatigue by optimising the knowledge of background noise . I will help improving alerts prioritisation improving vigilance and training of SOC analysts.

[1] https://restena.lu/en/project/ngsoti Ngsoti project overview

By pursuing these complementary objectives, we aim to enhance both SOC performance and training quality within the NGSOTI framework.

1.3 Acknowledgements

We would like to express our gratitude to the RESTENA Foundation for providing the network infrastructure that made the creation of this dataset possible. We also thank the European Union for supporting the improvement of SOC operator training across Europe. Finally, we acknowledge the contributions and assistance of our project partners, whose support was essential to this work.

2 Analysis scope

This report is an analysis by CIRCL of traffic captured on his sinkhole. This analysis is valuable for SOC operator training, as it helps them understand how SNMP works, how it can be abused, and how background noise on the protocol can affect visibility and detection. It is focusing on the Simple Network Management Protocol (SNMP). SNMP is a standardized protocol used for monitoring, managing, and configuring networked devices such as routers, switches, servers, and IoT devices. It enables network administrators to collect information about device performance, network traffic, and operational status, as well as to remotely control certain device parameters.

SNMP operates in a client-server model: managed devices run an SNMP agent that exposes management data, while a network management system (NMS) queries these agents or receives unsolicited notifications (traps) to monitor the network. Data is structured in the form of Object Identifiers (OIDs), which represent specific metrics such as CPU load, interface status, or memory usage. This Traffic is using UDP (Unified Datagram Protocol) therefore it give relevant informations even if no host are listening and responding to.

SNMP supports three versions:

- `v1` and `v2c`: Basic functionality with community strings for authentication, but limited security.
- `v3`: Adds cryptographic security with authentication and encryption.

2.1 Dataset

The dataset is an extract of the SNMP traffic captured by the blackhole network collected by CIRCL from November 1st to October 31th, 2025. Each record of the dataset represents a single SNMP packet received by the blackhole. It includes packet reception timestapm, source and destination IPs and ports, SNMP version, requested OIDs, community string (if applicable), and the reference pcap file. The sinkhole is a /18 containing 16382 IPv4 addresses, on a range which is only 1 bit away from a private RFC1918 range. This network allowing not only to capture standard scanning and exploits activity but also to catch misconfigurations or “typo” traffic targeting nearby private network spaces. This dataset provides insights into automated scanning campaigns as well as opportunistic reconnaissance behavior observed in the first half of 2025.

2.2 Data lake setup

The SNMP traffic was extracted from raw pcaps files using Suricata 7.0.3, an open-source network threat detection engine capable of parsing protocols in real time. Suricata generated structured metadata, including SNMP version, community strings, requested OIDs, source and destination IPs and ports, and timestamps.

Theses extracted metadata were ingested into ClickHouse 25.9.3.1. Clickhouse is a high-performance columnar database optimized for analytical workloads. Since ClickHouse allows fast aggregation and querying of large datasets, it is ideal for statistical analysis of SNMP traffic, such as tracking scanning patterns, frequent OIDs, and temporal trends in probing activity.

The final data lake contains the following structure;

	name	compressed_size	uncompressed_size	ratio
1.	version	331.43 MiB	1.18 GiB	3.65
2.	file	465.48 MiB	107.46 GiB	236.4
3.	dest_ip	2.43 GiB	8.89 GiB	3.66
4.	src_ip	1.71 GiB	8.42 GiB	4.92
5.	oids	3.21 GiB	36.20 GiB	11.28
6.	src_port	958.68 MiB	1.18 GiB	1.26
7.	dest_port	11.83 MiB	1.18 GiB	102.23
8.	community	187.06 MiB	4.07 GiB	22.29
9.	timestamp	151.82 MiB	2.36 GiB	15.93

- `version`, is the snmp version could be 1,2 or 3.
- `file` reference the pcap original file where the packet is stored
- `dest_ip` the destination ipv4
- `scr_ip` the source ipv4
- `oid` is an array of requested oids in the snmp frame
- `src_port` the udp source port
- `dest_port` the udp destination port
- `Community` is the SNMP community string
- `timestamp` the timestamp of the data frame.

2.3 General Statistical analysis

2.3.1 SNMP Activity

2.3.1.1 Methodologie

We leveraged the volumetric information available in the data lake to quantify the activity associated with each source IP. To enrich this view, we correlated all source IP addresses with their corresponding BGP Autonomous Systems using network WHOIS data. for this and Country-level attribution we used the historical IP-to-ASN mapping service provided by the CIRCL D4 project, specifically the (IPASN-History dataset][2])

2.3.1.2 Results

The year-long analysis reveal that the IPv4 /18 sinkhole was contacted via SNMP by 153,045 distinct IPv4 sources, generating a total of 6.34 billion queries. The diagram below illustrates the daily volume.

Figure 1: SNMP activity

[2] [https://github.com/D4-project/IPASN-History] CIRCL D4 project IPASN-History

The frequency analysis highlights clear spikes of more than 3.5 billion SNMP queries per day on the following dates:

– Late November 2024 and early October 2024
– 14 January 2025
– 2–3 June 2025
– 29 October 2025

2.3.2 Country repartition

To visualise the source of the snmp traffic we used two different criterias, packet volume and different ip volume per country.

Figure 2: Country repartition

Top 10 of total hits per country.

Rank	Country	distinct IPs	total_packets
1	ID	2383	248.491.546
2	CN	96762	243.813.326
3	PS	2	98.002.656
4	CL	4750	88.763.504
5	US	7088	85.706.798
6	DE	2829	71.712.610

Rank	Country	distinct IPs	total_packets
7	CO	3255	33.193.630
8	BR	1057	27.132.990
9	RU	146	23.517.254
10	JP	977	22.577.496

Many interesting informations are revealed by this output.
- Indonesia is the first nation in term of packet emited just before China with 50x less source IP's.
- Palestine emitted 98 Billions of packets using only two IP's. This behaviour is analysed in the chapter Anomalies Investigation / Palestinian traffic.

Figure 3: IPv4 Repartition

Rank	Country	Distinct IPs
0	CN	96762
1	US	7088
2	CL	4750
3	IN	4233
4	CO	3255
5	DE	2829

Rank	Country	Distinct IPs
6	SG	2740
7	SE	2495
8	ID	2383
9	TH	1981
10	MY	1783

Figure 4: Packet sent by BGP AS

Splitting the load across BGP Autonomous System makes it possible to distinguish traffic originating from countries other than China, Indonesia, and Palestine. This analysis highlights additional countries that generate substantial volumes of SNMP traffic, such as Germany, Japan, Russia, Chile, and several others.

Rank	Country	AS name	Packet send
1	ID	QUANTUMNET-AS-ID PT Quantum Tera Network	143779568
2	CN	CHINANET-BACKBONE No.31,Jin-rong Street	133905880

Rank	Country	AS name	Packet send
3	PS	PALTEL-AS PALTEL Autonomous System	98002656
4	ID	GRAHANET-AS-ID PT.Graha Telekomunikasi Indonesia	94598288
5	DE	DTAG Internet service provider operations	45130112
6	CN	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	31525886
7	CL	Orbyta S.A.	31167900
8	DE	LUENECOM-AS	18456158
9	RU	PROVODOV_NET-AS	16996588
10	JP	ASAHI-NET Asahi Net	16344656
11	CO	Colombia Movil	15037450
12	SE	TELENOR-SE former Utfors Bredband AB & Telenor AB	14628176
13	CN	CHINAMOBILE-CN China Mobile Communications Group Co., Ltd.	14538808
14	CN	CMNET-V4SHANGHAI-AS-AP Shanghai Mobile Communications Co.,Ltd.	13641050
15	JP	NETSURF-AS-	13194946

It is more instructive to examine the traffic of BGP Autonomous System (AS) by distinct used IP source. This perspective reveals which networks us the more IP's for the SNMP scanning activity. Beyond major operators such as ChinaNet Backbone N31 and hosting providers like DigitalOcean, a significant

portion of the traffic originates from mobile networks and domestic netwok operator. Many of these AS appear to rely on ORB nodes (Open Relay Boxes), which are commonly used to conduct large-scale distributed scanning. Examples include HI3G, COMUNICACIÓN CELULAR S.A., Comcel S.A., and several others.

Figure 5: Source IP per BGP AS

Rank	AS name	Distinct IPs
1	CHINANET-BACKBONE No.31,Jin-rong Street	6219
2	DIGITALOCEAN-ASN	2419
3	HI3G	2136
4	TELEFONICA CHILE S.A.	1723
5	ENTEL CHILE S.A.	1678
6	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	1511
7	BHARTI-MOBILITY-AS-AP Bharti Airtel Ltd. AS for GPRS Service	1327
8	ALPHASTRIKE-RESEARCH	1268
9	AKAMAI-LINODE-AP Akamai Connected Cloud	1262

Rank	AS name	Distinct IPs
10	COMUNICACION CELULAR S.A. COMCEL S.A.	1230
11	DTAG Internet service provider operations	1073
12	VIL-AS-AP Vodafone Idea Ltd	1033
13	CHINAMOBILE-CN China Mobile Communications Group Co., Ltd.	918
14	TELKOMNET-AS-AP PT Telekomunikasi Indonesia	853
15	WATANIYATELECOM-AS	783

2.3.3 SNMP version repartition

2.3.3.1 Methodology

The methodology used to produce the SNMP version repartition is straightforward: each SNMP packet observed in the sinkhole traffic, whether it is a request, response, or trap, is parsed to extract the SNMP version field. All captured frames containing SNMP data are processed individually, and the version identifiers are aggregated to compute their distribution. This ensures that the graph reflects an accurate representation of the protocol versions present in the observed background noise.

2.3.3.2 Results

Figure 6: Version repartition

The final dataset contains 328 billion of SNMP packets. The analysis of SNMP versions shows that only about 2% of queries use SNMPv3. This low adoption is expected, as SNMPv3 secures the communication channel through authentication and encryption, making it less attractive for uncontrolled scanning activities. In contrast, SNMPv1 and SNMPv2c are simple, weak, and widely deployed, and their lack of security controls allows unauthorized actors to retrieve information easily. As a result, these

legacy versions constitute the overwhelming majority of the background scanning traffic observed.

2.3.4 SNMP Community

2.3.4.1 Methodology

The methodology for this representatio consists of extracting SNMP community strings from all SNMPv1 and SNMPv2c packets present in the dataset. These versions expose the community field in clear text, making it directly observable and suitable for statistical analysis. SNMPv3 packets were intentionally excluded from this extraction step, as their authentication and encryption mechanisms prevent community or credential data from being visible in clear text. The analysis is thus limited to v1 and v2c, where the community string is present and readable in every captured frame. Empty snmp community were redacted to 'Empty' for being visible in the cloudword.

2.3.4.2 Results

Figure 7: Community repartition

Numerous community strings are expected when examining traffic generated for discovery-oriented scanning activities.

- PUBLIC, is the historical default SNMP read only community.

- CANON_ADMIN[3] is the documented default community for canon printers.

- PRIVATE is also a commonly documented configuration for read write access. For example this configuration isn is with cisco[^3] devices

More interestingly, this highlights the presence of others community string 'internal' as well as numerous variants of 'public'. These observations provide insight into how commonly these weak or guessable strings are used across unsolicited SNMP traffic.

The following graph depict the relations between the snmp hardware and the requested v1 & v2 community. it cleardy demonstrate that beside public, there is a clear focus on certain oid for certain devices. This reveal abuse for default snmp community however most of the non public ones discovered in this dataset are not documented

[3] https://oip.manual.canon/USRMA-0219-zz-SS-enUS/contents/10040030.html Default SNMP configuration

Figure 8: Devices to community

2.3.5 Devices scanned.

2.3.5.1 Methodology

To analyze the SNMP sinkhole dataset, we focus on the Object Identifiers (OIDs) queried by IP sources. Since each SNMP packet may contain multiple OIDs, we flatten the data to handle them individually. Some oids are common on each platform, however some of them are vendor related. We then extract the vendor-specific prefix of each OID, identified by the `1.3.6.1.4.1.x` pattern, where `x` corresponds to a particular vendor. By counting the frequency of queries for each vendor prefix and ranking them, we can identify which vendors' devices are most commonly targeted or scanned. This methodology allows us to uncover trends in attacker behavior, highlight reconnaissance activity, and detect potential focus on specific device types in the wild.

2.3.5.2 Results

Figure 9: Top vendors

Figure 10: Scan Coverage

It is noteworthy that several device families do not exhibit continuous scanning activity throughout the year. For example, Cisco devices appear only between March and May 2025, while Lite-One Technology Corp. devices are observed from January through July. This irregularity suggests that scanning campaigns may be driven by factors other than broad, systematic reconnaissance.

A valuable follow-up investigation would be to examine whether publicly disclosed SNMP exploitation techniques, proof-of-concept releases, or newly identified SNMP-related vulnerabilities emerged during these same periods. Correlating vendor-specific scanning activity with vulnerability disclosure timelines could help determine whether the observed traffic aligns with opportunistic exploitation attempts or with more general background scanning activity.

2.3.6 Vulnerabilities and exploits

TO ANALYSE

MISCONFIG

```
Frame 421698: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits)
Ethernet II, Src: AristaNetwor_c6:33:eb (60:6b:5b:c6:33:eb), Dst: ConnectAs_cd:82:21 (00:00:24:cd:82:21)
Internet Protocol Version 4, Src: 113.222.191.216, Dst: [redacted].8
User Datagram Protocol, Src Port: 35661, Dst Port: 161
Simple Network Management Protocol
  version: version-1 (0)
  community: internal
  data: set-request (3)
    set-request
      request-id: 4004
      error-status: noError (0)
      error-index: 0
      variable-bindings: 4 items
        1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0: "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=IMAGE;HOST=192.168.2.182:54925;APPNUM=1;DURATION=360;CC=1;"
          Object Name: 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 (iso.3.6.1.4.1.2435.2.3.9.2.11.1.1.0)
          Value (OctetString): "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=IMAGE;HOST=192.168.2.182:54925;APPNUM=1;DURATION=360;CC=1;"
        1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0: "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=OCR;HOST=192.168.2.182:54925;APPNUM=3;DURATION=360;CC=1;"
          Object Name: 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 (iso.3.6.1.4.1.2435.2.3.9.2.11.1.1.0)
          Value (OctetString): "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=OCR;HOST=192.168.2.182:54925;APPNUM=3;DURATION=360;CC=1;"
        1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0: "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=EMAIL;HOST=192.168.2.182:54925;APPNUM=2;DURATION=360;CC=1;"
          Object Name: 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 (iso.3.6.1.4.1.2435.2.3.9.2.11.1.1.0)
          Value (OctetString): "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=EMAIL;HOST=192.168.2.182:54925;APPNUM=2;DURATION=360;CC=1;"
        1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0: "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=FILE;HOST=192.168.2.182:54925;APPNUM=5;DURATION=360;CC=1;"
          Object Name: 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 (iso.3.6.1.4.1.2435.2.3.9.2.11.1.1.0)
          Value (OctetString): "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=FILE;HOST=192.168.2.182:54925;APPNUM=5;DURATION=360;CC=1;"
```

```
5267… 252.982609   45.227.237.38   19 SNMP   586 set-request 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 1.3.6.1.4.1.2435.2.3.9.2.1
35006 18.050112    223.150.224.…    8 SNMP   534 set-request 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 1.3.6.1.4.1.2435.2.3.9.2.1
```

```
snmpV2-trap
  request-id: 2152803
  error-status: noError (0)
  error-index: 0
  variable-bindings: 7 items
    1.3.6.1.2.1.1.3.0: 4044259023
      Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
      Value (Timeticks): 4044259023
    1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.4.1.9.9.41.2.0.1 (iso.3.6.1.4.1.9.9.41.2.0.1)
      Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0)
      Value (OID): 1.3.6.1.4.1.9.9.41.2.0.1 (iso.3.6.1.4.1.9.9.41.2.0.1)
    1.3.6.1.4.1.9.9.41.1.2.3.1.2.208159: "SFF8472"
      Object Name: 1.3.6.1.4.1.9.9.41.1.2.3.1.2.208159 (iso.3.6.1.4.1.9.9.41.1.2.3.1.2.208159)
      Value (OctetString): "SFF8472"
    1.3.6.1.4.1.9.9.41.1.2.3.1.3.208159: 4
      Object Name: 1.3.6.1.4.1.9.9.41.1.2.3.1.3.208159 (iso.3.6.1.4.1.9.9.41.1.2.3.1.3.208159)
      Value (Integer32): 4
    1.3.6.1.4.1.9.9.41.1.2.3.1.4.208159: "THRESHOLD_VIOLATION"
      Object Name: 1.3.6.1.4.1.9.9.41.1.2.3.1.4.208159 (iso.3.6.1.4.1.9.9.41.1.2.3.1.4.208159)
      Value (OctetString): "THRESHOLD_VIOLATION"
    1.3.6.1.4.1.9.9.41.1.2.3.1.5.208159: "Twe1/0/7: Rx power high warning; Operating value:   1.1 dBm, Threshold value:   1.0 dBm."
      Object Name: 1.3.6.1.4.1.9.9.41.1.2.3.1.5.208159 (iso.3.6.1.4.1.9.9.41.1.2.3.1.5.208159)
      Value (OctetString): "Twe1/0/7: Rx power high warning; Operating value:   1.1 dBm, Threshold value:   1.0 dBm."
    1.3.6.1.4.1.9.9.41.1.2.3.1.6.208159: 4044259023
      Object Name: 1.3.6.1.4.1.9.9.41.1.2.3.1.6.208159 (iso.3.6.1.4.1.9.9.41.1.2.3.1.6.208159)
      Value (Timeticks): 4044259023
```

2.4 Anomalies investigation

2.4.1 Palestinian Traffic

According to the volumetry analysis the Palestinian Autonomous System 12975 have emited 41.8 Billions of packets.

	ip	as_number	as_name
1.	213.6.137.78	12975	PALTEL-AS PALTEL Autonomous System
2.	213.6.173.227	12975	PALTEL-AS PALTEL Autonomous System

It appear that the traffic was only generated by the host 213.6.137.78 from at least 1st of January to the 19th of May. This IP did not have any PTR associated DNS records and is not known in our passive DNS database.

For each destination, two different scans are performed. Each scans are performed 3 times and retried every 3 seconds.

For the first type of scan, it do a SNMP get request and ask the following generic SNMP Oids;
- 1.3.6.1.2.1.2.2.1 ifEntry
- 1.3.6.1.2.1.4.20.1 ipAddrTable
- 1.3.6.1.2.1.4.22.1 ipNetToMediaTable

Then finally the unknown regitered vendor 9999 oid
- 1.3.6.1.2.1.9999.1.1.6.4.1

This last scan may be related to microtiK os devices as documented here And seems to allows determination of internal IP's.

```
snmpwalk [redacted] -v1 -c public 1.3.6.1.2.1.9999.1.1.6.4.1 | head
Error: OID not increasing: iso.3.6.1.2.1.9999.1.1.6.4.1.4.192.168.33.99
 >= iso.3.6.1.2.1.9999.1.1.6.4.1.4.172.31.33.144

iso.3.6.1.2.1.9999.1.1.6.4.1.4.192.168.33.99 = INTEGER: 2
iso.3.6.1.2.1.9999.1.1.6.4.1.4.172.31.33.144 = INTEGER: 2
```

The second scan is also a SNMP get request on; * 1.3.6.1.2.1.25.3.3.1.2 hrProcessorEntry * 1.3.6.1.2.1.25.2.3.1.2 hrStorageEntry

For all the request, no payload are present.

Example in c0bb49e788964718af4dfea4c0ab898c-2025-04-27-174644

No.	Time	Source	Destination	Protocol	Length	Info
2052…	*REF*	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.3.3.1.2
2052…	0.000154	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.2.3.1.1
2053…	0.000217	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.2.3.1.2
2110…	3.001044	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.3.3.1.2
2110…	3.001120	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.2.3.1.1
2110…	3.001269	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.2.3.1.2
4417…	144.008254	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.2.2.1
4417…	144.008330	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.20.1
4417…	144.008509	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.22.1
4417…	144.008654	213.6.137.78	1	SNMP	88	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1
4467…	147.008987	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.2.2.1
4467…	147.009116	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.20.1
4467…	147.009395	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.22.1
4467…	147.009590	213.6.137.78	1	SNMP	88	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1
4517…	150.021936	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.2.2.1
4517…	150.022000	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.20.1
4517…	150.022040	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.22.1
4517…	150.022202	213.6.137.78	1	SNMP	88	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1

Example in c0bb49e788964718af4dfea4c0ab898c-2025-03-16-011212

No.	Time	Source	Destination	Protocol	Length	Info
77873	*REF*	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.2.2.1
77874	0.000117	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.20.1
77875	0.000325	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.22.1
77876	0.000550	213.6.137.78	33	SNMP	89	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1
84696	3.008617	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.2.2.1
84697	3.008956	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.20.1
84698	3.009134	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.22.1
84700	3.009339	213.6.137.78	33	SNMP	89	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1
89161	6.022444	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.2.2.1
89162	6.022497	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.20.1
89163	6.022573	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.22.1
89164	6.022643	213.6.137.78	33	SNMP	89	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1
5457…	224.964692	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.3.3.1.2
5515…	227.968957	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.3.3.1.2
5774…	238.984735	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.2.3.1.1
5774…	238.985045	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.2.3.1.2
5820…	241.985373	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.2.3.1.1
5820…	241.985542	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.2.3.1.2

This schema is observable for all destination IP's.

2.5 Scanning vendor Traffic

By resolving the pointers record it is convenient to find out some scanning solutions vendors or foundation.

The blackhole was reached by; * Cencys * NetSecScan * Shadowserver * ShadowForce * Shodan * onyphe.net (TODO) *

2.5.1 Censys

Censys scanners are originating from BGP AS;
* 398324
* 398722

We identified in our dataset 65 IP's with a censys DNS related PTR record
* 16 scanner-001.hk2.censys-scanner.com
* 16 scanner-007.ch1.censys-scanner.com
* 1 scanner-011.ch1.censys-scanner.com
* 16 scanner-11.ch1.censys-scanner.com
* 16 scanner-14.ch1.censys-scanner.com

And and additional 16 Ip's from these AS responding to the PTR unused-space.coop.net.

The footprint of these 81 Ip's.

Packets per day for selected PTR IPs
SPC_IP
Day
Packets
0
20
40
60
80
100
120
140

From this frequencial analysys we could see that Censys never exceed a total of 350 SNMP paquets per hours and spread the load in a really efficient manner keeping a footprint of the dataset very ligth.

Additionnaly during this timeframe, all these request were using SNMPv3 query, which impair us to determine the queried OID and Versions.

```
▸ Frame 493080: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
▸ Ethernet II, Src: AristaNetwor_c6:33:eb (60:6b:5b:c6:33:eb), Dst: ConnectAs_cd:82:21 (00:00:24:cd:82:21)
▸ Internet Protocol Version 4, Src: 162.142.125.87, Dst: [redacted].55
▸ User Datagram Protocol, Src Port: 48845, Dst Port: 161
▾ Simple Network Management Protocol
    msgVersion: snmpv3 (3)
  ▸ msgGlobalData
    msgAuthoritativeEngineID: <MISSING>
    msgAuthoritativeEngineBoots: 0
    msgAuthoritativeEngineTime: 0
    msgUserName:
    msgAuthenticationParameters: <MISSING>
    msgPrivacyParameters: <MISSING>
  ▾ msgData: plaintext (0)
    ▾ plaintext
        contextEngineID: <MISSING>
        contextName:
      ▾ data: get-request (0)
        ▾ get-request
            request-id: 1875005265
            error-status: noError (0)
            error-index: 0
            variable-bindings: 0 items
```

It should be mentionned that besides SNMP, a Single scanners scans for 74 other TCP ports and 12 UDPs

2.5.2 NetSecScan

2.5.3 Shadowserver

2.5.4 ShadowForce

2.5.5 Shodan

3 TODO - TO REMOVE

-» TODO * Volume of XX bytes of raw network capture * graph scan vendor * new oid / month * analyse agnov * snmp community (grep -v tuple (1ipvs1pt)) * trouver vulns * todo donner les donnees / notebook. * outcome -> liste * grouper par token les srcip(cable, adsl, vpn, scan) parametre. * Semaines pattern (sur un byte) * month sur un byte

idées * congés pattern

3.0.1 Vulnerabilities and exploits

3.1 TO ANALYSE

3.1.1 MISCONFIG

```
▸ Frame 421698: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits)
▸ Ethernet II, Src: AristaNetwor_c6:33:eb (60:6b:5b:c6:33:eb), Dst: ConnectAs_cd:82:21 (00:00:24:cd:82:21)
▸ Internet Protocol Version 4, Src: 113.222.191.216, Dst: [redacted].8
▸ User Datagram Protocol, Src Port: 35661, Dst Port: 161
▾ Simple Network Management Protocol
    version: version-1 (0)
    community: internal
  ▾ data: set-request (3)
    ▾ set-request
        request-id: 4004
        error-status: noError (0)
        error-index: 0
      ▾ variable-bindings: 4 items
        ▾ 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0: "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=IMAGE;HOST=192.168.2.182:54925;APPNUM=1;DURATION=360;CC=1;"
            Object Name: 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 (iso.3.6.1.4.1.2435.2.3.9.2.11.1.1.0)
            Value (OctetString): "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=IMAGE;HOST=192.168.2.182:54925;APPNUM=1;DURATION=360;CC=1;"
        ▾ 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0: "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=OCR;HOST=192.168.2.182:54925;APPNUM=3;DURATION=360;CC=1;"
            Object Name: 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 (iso.3.6.1.4.1.2435.2.3.9.2.11.1.1.0)
            Value (OctetString): "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=OCR;HOST=192.168.2.182:54925;APPNUM=3;DURATION=360;CC=1;"
        ▾ 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0: "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=EMAIL;HOST=192.168.2.182:54925;APPNUM=2;DURATION=360;CC=1;"
            Object Name: 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 (iso.3.6.1.4.1.2435.2.3.9.2.11.1.1.0)
            Value (OctetString): "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=EMAIL;HOST=192.168.2.182:54925;APPNUM=2;DURATION=360;CC=1;"
        ▾ 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0: "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=FILE;HOST=192.168.2.182:54925;APPNUM=5;DURATION=360;CC=1;"
            Object Name: 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 (iso.3.6.1.4.1.2435.2.3.9.2.11.1.1.0)
            Value (OctetString): "TYPE=BR;BUTTON=SCAN;USER="DELL";FUNC=FILE;HOST=192.168.2.182:54925;APPNUM=5;DURATION=360;CC=1;"
```

```
5267… 252.982609   45.227.237.38   19 SNMP   586 set-request 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 1.3.6.1.4.1.2435.2.3.9.2.1
35006 18.050112    223.150.224.…    8 SNMP   534 set-request 1.3.6.1.4.1.2435.2.3.9.2.11.1.1.0 1.3.6.1.4.1.2435.2.3.9.2.1
```

```
  ▾ snmpV2-trap
      request-id: 2152803
      error-status: noError (0)
      error-index: 0
    ▾ variable-bindings: 7 items
      ▾ 1.3.6.1.2.1.1.3.0: 4044259023
          Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
          Value (Timeticks): 4044259023
      ▾ 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.4.1.9.9.41.2.0.1 (iso.3.6.1.4.1.9.9.41.2.0.1)
          Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0)
          Value (OID): 1.3.6.1.4.1.9.9.41.2.0.1 (iso.3.6.1.4.1.9.9.41.2.0.1)
      ▾ 1.3.6.1.4.1.9.9.41.1.2.3.1.2.208159: "SFF8472"
          Object Name: 1.3.6.1.4.1.9.9.41.1.2.3.1.2.208159 (iso.3.6.1.4.1.9.9.41.1.2.3.1.2.208159)
          Value (OctetString): "SFF8472"
      ▾ 1.3.6.1.4.1.9.9.41.1.2.3.1.3.208159: 4
          Object Name: 1.3.6.1.4.1.9.9.41.1.2.3.1.3.208159 (iso.3.6.1.4.1.9.9.41.1.2.3.1.3.208159)
          Value (Integer32): 4
      ▾ 1.3.6.1.4.1.9.9.41.1.2.3.1.4.208159: "THRESHOLD_VIOLATION"
          Object Name: 1.3.6.1.4.1.9.9.41.1.2.3.1.4.208159 (iso.3.6.1.4.1.9.9.41.1.2.3.1.4.208159)
          Value (OctetString): "THRESHOLD_VIOLATION"
      ▾ 1.3.6.1.4.1.9.9.41.1.2.3.1.5.208159: "Twe1/0/7: Rx power high warning; Operating value:   1.1 dBm, Threshold value:   1.0 dBm."
          Object Name: 1.3.6.1.4.1.9.9.41.1.2.3.1.5.208159 (iso.3.6.1.4.1.9.9.41.1.2.3.1.5.208159)
          Value (OctetString): "Twe1/0/7: Rx power high warning; Operating value:   1.1 dBm, Threshold value:   1.0 dBm."
      ▾ 1.3.6.1.4.1.9.9.41.1.2.3.1.6.208159: 4044259023
          Object Name: 1.3.6.1.4.1.9.9.41.1.2.3.1.6.208159 (iso.3.6.1.4.1.9.9.41.1.2.3.1.6.208159)
          Value (Timeticks): 4044259023
```

4 Additional References

5 Conclusions

This analysis provides valuable insights and constitutes a meaningful contribution to operational security practice. The newly derived MISP warning lists offer SOC operators additionnal classification mechanisms that help reduce operational fatigue by filtering out predictable or low-value SNMP scanning activity. At the same time, the characterization of SNMP traffic enables analysts to better understand protocol behaviors and to discriminate between benign background scanning and events that warrant closer investigation. Together, these outcomes strengthen the operator's ability to prioritize relevant signals and maintain effective situational awareness.