HORIZON 2020

Digital Security: Cybersecurity, Privacy and Trust
H2020-DS-2015-1

DS-04-2015 Information driven Cyber Security Management
Grant n° 700176

Secure Information Sharing Sensor Delivery event Network[†]

Deliverable D6.5:

Qualitative and Quantitative Assessment Report

Abstract: This document presents and essential assessment of both the qualitative and quantitative success and impact of the SISSDEN pilot.

Contractual Date of Delivery	April 30th, 2019
Actual Date of Delivery	April 20th, 2019
Deliverable Security Class	Public
Editor	Johannes Krupp (USAAR)
Contributors	All *SISSDEN* partners
Internal Reviewers	NASK, SHAD
Quality Assurance	Adam Kozakiewicz (NASK)

[†] The research leading to these results has received funding from the European Union Horizon 2020 Programme (H2020-DS-2015-1) under grant agreement n° 700176.

The *SISSDEN* consortium consists of:

Naukowa i Akademicka Sieć Komputerowa	Coordinator	Poland
Montimage EURL	Principal Contractor	France
CyberDefcon Limited	Principal Contractor	United Kingdom
Universitaet des Saarlandes	Principal Contractor	Germany
Deutsche Telekom AG	Principal Contractor	Germany
Eclexys SAGL	Principal Contractor	Switzerland
Poste Italiane – Sozietá per Azioni	Principal Contractor	Italy
Stichting the Shadowserver Foundation Europe	Principal Contractor	Netherlands

Table of Contents

1 Introduction

1.1 Aim of the document

This document aims to assess the overall success and impact of the SISSDEN Platform Pilot in terms of quantity and quality. SISSDEN proposed to address three impacts listed in work programme DS-4-2015 (Information driven Cyber Security Management):

1. *Facilitate the management of internal and external information sources related to cyber security management.*
2. *Better information management and appropriate dissemination.*
3. *Increase the level of awareness and preparedness of all stakeholders.*

In the SISSDEN Platform Pilot, these were addressed by (a) building a large-scale honeypot and data collection and analysis platform, (b) providing a curated reference data set to researchers, and (c) providing situational awareness to network operators and CERTs through daily remediation reports.

The impact and success of the SISSDEN Platform Pilot therefore depends directly on the quantity and quality of the data collected, the analyses developed, as well as the remediation reports sent.

1.2 Structure of the document

Sections 2 and 3 of this document are concerned with the data collected during the SISSDEN Platform Pilot operation. Section 2 gives a quantitative characterization of the different datasets while Section 3 provides an assessment of the quality of the collected data in terms of coverage and validity. Section 4 provides a quantitative description of the analysis results obtained from continuous analysis modules and Section 5 explores the impact of SISSDEN's remediation feeds with respect to the number of recipients reached as well as their utility, timeliness, and accuracy.

2 Datasets - Quantitative Analysis

During the operation of the SISSDEN pilot, data from multiple honeypots, darknets, and additional sources was collected. To provide a better understanding of the data collected, this section gives a quantitative characterization of the various datasets.

This characterization includes a description of the data, the total number of events that was collected from a source, the date that the source was added to SISSDEN, as well as a growth-rate in data. As the number of honeypots was continuously increased during the project, the growth rate is given as a total average over the entire collection period, but also as a rate considering just the last week of March. Furthermore, as different datasets are ingested through different means, the characterization also includes an average ingestion delay between the event and its appearance in the data collection.

Finally, this section also describes the actionable information that can be derived from a dataset, such as the number of distinct attacking IP addresses observed or the number of new malware samples collected by a sensor.

2.1 Honeypots

2.1.1 AmpPot

Description	Amplification DDoS events observed by AmpPot, including • Victim's IP address • Abused protocol • Timestamp of attack start • Timestamp of attack end
Start of collection	October 10th, 2017
No. of events (Mar 31st 2019)	3,977,420
Average ingestion rate (overall)	308 attacks per hour (7,400 per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	391 attacks per hour (9,382 per day)
Average ingestion delay	< 5 minutes
Types of actionable insights	IP addresses of DDoS victims
No. of actionable insights	2,068,210 distinct DDoS victims in 18,141 ASNs

2.1.2 CiscoASA

Description	Request events observed by a low interaction Cisco ASA honeypot. Events include • Attacker's IP address • Timestamp of request • Full HTTP request • Extracted exploit payload if this request exploits CVE-2018-0101
Start of collection	November 22nd, 2018
No. of events (Mar 31st 2019)	11,828
Average ingestion rate (overall)	91.5 events per day
Average ingestion rate (Mar 25th - Mar 31st 2019)	82.0 events per day
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	Attacker IP addresses, Request payloads
No. of actionable insights	1,322 distinct attackers in 340 ASNs using 183 different payloads

2.1.3 Conpot

Description	Request events observed by a low interaction industrial control system honeypot. Events include • Attacker's IP address • Timestamp of request • Attacked protocol (port number) • Request payload
Start of collection	May 11th, 2018
No. of events (Mar 31st 2019)	2,494,531
Average ingestion rate (overall)	320 events per hour (7,688 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	97.3 events per hour (2,335 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	Attacker IP addresses
No. of actionable insights	134,475 attackers in 8,370 ASNs

2.1.4 Cowrie

Description	Events observed and (malware) files captures by medium interaction Telnet and SSH honeypot. Events include • Attacker's IP address • Timestamp of begin of session • Timestamp of end of session • Attacked protocol (port number) • Credentials used for login • Commands sent during session • List of downloaded (malware) files
Start of collection	October 18th, 2017
No. of events (Mar 31st 2019)	Total: 414,916,048 SSH: 107,569,838 Telnet: 307,343,460
Average ingestion rate (overall)	9.07 events per second (783,235 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	36.9 events per second (3,184,814 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	Attacker IP addresses (=infected systems in many cases), Credentials used in attacks, Command sequences executed in devices
No. of actionable insights	SSH: 360,794 distinct sources in 10,808 ASNs, 1,200 distinct files Telnet: 1,956,266 distinct sources in 14,907 ASNs, 12,426 distinct files

2.1.5 Dionaea

Description	Events observed by low interaction honeypot dionaea. Events include • Attacker's IP address • Timestamp of request • Attacked protocol
Start of collection	Feb 18th, 2019
No. of events (Mar 31st 2019)	1,332,133

Average ingestion rate (overall)	22.3 events per minute (32,177 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	30.7 events per minute (44,145 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	Attacker IP addresses
No. of actionable insights	119,066 attackers in 7,110 ASNs. Events split by protocol: • smbd: 668,476 • mssqld: 234,685 • upnpd: 226,902 • mqttd: 81,517 • httpd: 78,891 • SipSession: 24,976 • mysqld: 13,252 • ftpd: 2,356 • pptpd: 476 • TftpServerHandler: 225 • Memcache: 218 • epmapper: 109 • mirrorc: 25 • mirrord: 25

2.1.6 ElasticPot

Description	Events observed by low-interaction Elasticsearch honeypot ElasticPot. Events include • Attacker's IP • Timestamp of request • Full body of elasticsearch query
Start of collection	Jan 9th, 2018
No. of events (Mar 31st 2019)	110,391
Average ingestion rate (overall)	10.3 events per hour (247 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	20.7 events per hour (496 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)

Types of actionable insights	Attacker's IP addresses, Request payloads used against Elasticsearch installations
No. of actionable insights	2,787 attackers in 440 ASNs,

2.1.7 Glastopf

Description	Events observed by web application honeypot Glastopf. Events include: • Attacker's IP • Timestamp of request • Full body of request • Classification of attack type for known patterns
Start of collection	May 11th, 2018
No. of events (Mar 31st 2019)	26,586,648
Average ingestion rate (overall)	56.9 events per minute (81,939 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	90.2 events per minute (129,899 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	Attacker's IP addresses, Request payloads used against web applications, Prevalence of attack patterns
No. of actionable insights	670,924 attackers in 14,905 ASNs. Attack split: • phpmyadmin: 7,799,501 • sqli: 1,325,134 • login: 710,273 • comments: 671,864 • head: 240,144 • style_css: 117,572 • robots: 81,185 • tomcat_manager: 37,725 • rfi: 33,985 • phpinfo: 33,251 • lfi: 15,631 • put: 5,126 • options: 2,610 • tomcat_status: 267 • unknown: 15,512,380

2.1.8 Heralding

2.1.8.1 Auth

Description	Login attempt events observed by low interaction honeypot heralding. Events include: • Attacker's IP • Timestamp of attempted login • Username • Password • attacked service (protocol)
Start of collection	Nov 21st, 2018
No. of events (Mar 31st 2019)	426,227,646
Average ingestion rate (overall)	37.8 events per second (3,267,178 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	57.6 events per second (4,975,757 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	Attacker's IP addresses, Login credentials
No. of actionable insights	470,505 attackers in 12,090 ASNs. Per service breakdown • telnet: 163,198,560 requests from 365,561 attackers • ssh: 158,832,465 requests from 94,144 attackers • vnc: 98,251,267 requests from 1,493 attackers • smtp: 3,223,025 requests from 3,744 attackers • http: 1,486,444 requests from 1,789 attackers • pop3: 741,936 requests from 142 attackers • https: 274,779 requests from 326 attackers • ftp: 120,515 requests from 4,265 attackers • imap: 76,632 requests from 11 attackers • postgresql: 22,010 requests from 10 attackers • pop3s: 7 requests from 5 attackers • imaps: 6 requests from 5 attackers 106,445 different usernames and 357,996 different passwords used.

2.1.8.2 Sessions

Description	Connections observed by low interaction honeypot heralding. A connection may have multiple authentication events captured in indices heralding-auth-*. Events include: • Attacker's IP • Timestamp of first packet • Duration of session • Attacked protocol
Start of collection	Nov 21st, 2018
No. of events (Mar 31st 2019)	566,305,498
Average ingestion rate (overall)	50.2 events per second (4,340,922 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	78.9 events per second (6,815,073 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	Attacker's IP addresses
No. of actionable insights	652,489 attackers in 14,582 ASNs

2.1.9 HoneyPy

Description	Events observed by low interaction honeypot honeypy. Events include • Attacker's IP address • Timestamp of request • Attacked protocol • Request payload
Start of collection	Mar 3rd, 2019
No. of events (Mar 31st 2019)	80,407,576
Average ingestion rate (overall)	39.6 events per second (3,420,364 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	47.7 events per second (4,120,284 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	Attacker IP addresses
No. of actionable insights	22,242 attackers in 2,941 ASNs

2.1.10 Micros

Description	Exploit attempts observed by medium interaction honeypot micros for CVE-2018-2636. Events include • Attacker's IP address • Timestamp of request • Full request • Parsed header information
Start of collection	Jan 9th, 2019
No. of events (Mar 31st 2019)	31,667
Average ingestion rate (overall)	16.2 events per hour (389 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	17.0 events per second (409 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	Attacker IP addresses, HTTP requests
No. of actionable insights	Request breakdown (top 10 out of 533 unique requests): • `GET / HTTP/1.1`: 19362 • `POST /cgi-bin/ViewLog.asp HTTP/1.1`: 3535 • `GET / HTTP/1.0`: 1717 • `GET /manager/html HTTP/1.1`: 862 • `HEAD /robots.txt HTTP/1.0`: 490 • `POST /tmUnblock.cgi HTTP/1.1`: 387 • `GET /favicon.ico HTTP/1.1`: 196 • `CONNECT api.ipify.org:443 HTTP/1.1`: 140 • `CONNECT www.google.com:443 HTTP/1.1`: 134 • `HEAD http://112.124.42.80:63435/ HTTP/1.1`: 128

2.1.11 Spam

Description	Spam mails received by SHAD spampot. Events include • Spam sender • Spam recipient • Message Subject • Message Content • Timestamp of message reception
Start of collection	Oct 10th, 2017
No. of events (Mar 31st 2019)	811,352,493
Average ingestion rate (overall)	17.5 events per second (1,510,484 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	5.22 events per second (451,144 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	
No. of actionable insights	

2.1.12 Struts

Description	Requests observed by struts honeypot for CVE 2017-5638 attacks. Events include • Attacker's IP address • Timestamp of request • Full request • Parsed header information
Start of collection	Feb 27th, 2019
No. of events (Mar 31st 2019)	10,598
Average ingestion rate (overall)	13.6 events per hour (325 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	12.3 events per hour (295 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	Attacker IP addresses, Requests

No. of actionable insights	7,001 attackers in 1,954 ASNs. Request breakdown (top 10 out of 177 unique requests): • `GET / HTTP/1.1`: 6231 • `GET / HTTP/1.0`: 3073 • `GET /index.php HTTP/1.1`: 305 • `PROPFIND / HTTP/1.1`: 228 • `HEAD / HTTP/1.1`: 71 • `GET /index.php?s=/index/\thinkpp/invokefunction&function=call_user_func_array&vars[0]=md5&vars[1][]=HelloThinkPHP HTTP/1.1`: 55 • `POST /index.php?s=captcha HTTP/1.1`: 52 • `HEAD / HTTP/1.0`: 51 • `GET /index.php?lang=en HTTP/1.1`: 48 • `GET /?XDEBUG_SESSION_START=phpstorm HTTP/1.1`: 38

2.1.13 IoTLab

Description	Connections observed by USAAR IoTLab honeypot. Events include • Attacker's IP address • Timestamp of begin of session • Timestamp of end of session • Attacked protocol • Username • Password • Malware files downloaded during session
Start of collection	Jan 15th, 2019
No. of events (Mar 31st 2019)	1,288,222
Average ingestion rate (overall)	11.8 events per minute (17,038 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	9.64 events per minute (13,880 events per day)
Average ingestion delay	<10 minutes
Types of actionable insights	Attacker IP addresses, credentials used in login attempts, malware samples

No. of actionable insights	146,649 attackers trying 1,742 unique username/password combinations. Top 10 username/password combinations: • `admin:1234`: 10276 • `admin:admin`: 10216 • `root:vizxv`: 9615 • `root:aquario`: 9032 • `support:support`: 8881 • `root:xc3511`: 8875 • `root:admin`: 8830 • `root:root`: 8139 • `root:`: 7932 • `guest:12345`: 7900

2.1.14 Weblogic

Description	Requests observed by Weblogic honeypot for CVE-2017-10271 attacks. Events include • Attacker's IP address • Timestamp of request • Full request • Parsed header information
Start of collection	Jan 9th, 2019
No. of events (Mar 31st 2019)	3,333
Average ingestion rate (overall)	1.71 events per hour (41.0 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	3.44 events per hour (82.6 events per day)
Average ingestion delay	no delay (direct hpfeeds ingestion)
Types of actionable insights	Attacker IP addresses, Requests

No. of actionable insights	386 attackers in 125 ASNs, request breakdown (top 10 out of 151 unique requests): • `GET / HTTP/1.1`: 675 • `GET /favicon.ico HTTP/1.1`: 105 • `POST /wls-wsat/CoordinatorPortType HTTP/1.1`: 43 • `OPTIONS / HTTP/1.1`: 36 • `POST /console/j_security_check HTTP/1.1`: 36 • `GET /index.do HTTP/1.1`: 30 • `GET http://www.ip138.com/ HTTP/1.1`: 26 • `GET /FxCodeShell.jsp?view=FxxkMyLie1836710Aa&os=1&address=http://fid.hognoob.se/download.exe HTTP/1.1`: 24 • `GET /struts2-rest-showcase/orders.xhtml HTTP/1.1`: 20 • `OPTIONS / HTTP/1.0`: 18

2.2 Darknet

2.2.1 CYBE Top ASN

Description	Daily top ASNs observed in CYBE darknet. Events include • Day of observation • Protocol (TCP/UDP) • Port number • Id of darknet collector • ASN • Number of requests
Start of collection	Jan 22nd, 2018
No. of events (Mar 31st 2019)	145,475
Average ingestion rate (overall)	14.0 events per hour (335 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	11.9 events per hour (285 events per day)
Average ingestion delay	Between 0 and 24 hours (aggregated on daily basis)
Types of actionable insights	AS numbers of talkative autonomous systems
No. of actionable insights	1,830 ASNs. Top 10 (by number of events): • AS6939 Hurricane Electric, Inc.: 4552 • AS29073 Quasi Networks LTD.: 3940 • AS60781 LeaseWeb Netherlands B.V.: 3804 • AS4134 Chinanet: 2876 • AS14061 Digital Ocean, Inc.: 2542 • AS17974 PT Telekomunikasi Indonesia: 2501 • AS7552 Viettel Corporation: 1811 • AS10439 CariNet, Inc.: 1799 • AS45899 VNPT Corp: 1680 • AS4837 CNCGROUP China169 Backbone: 1573

2.2.2 CYBE Top IP

Description	Daily top IP addresses observed in CYBE darknet. Events include • Day of observation • Protocol (TCP/UDP) • Port number • Id of darknet collector • IP address • Number of requests
Start of collection	Jan 1st, 2018
No. of events (Mar 31st 2019)	282,623
Average ingestion rate (overall)	25.9 events per hour (621 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	19.3 events per hour (462 events per day)
Average ingestion delay	Between 0 and 24 hours (aggregated on daily basis)
Types of actionable insights	active IP addresses
No. of actionable insights	24,065 IPs. Top 10 (by number of events): • 185.94.111.1: 2905 • 134.147.203.115: 1824 • 185.200.63.56: 1064 • 184.105.139.67: 918 • 80.82.77.139: 906 • 80.82.77.33: 864 • 184.105.247.203: 746 • 184.105.247.199: 741 • 74.82.47.10: 733 • 184.105.247.211: 725

2.2.3 CYBE Top Net

Description	Daily top networks observed in CYBE darknet. Events include • Day of observation • Protocol (TCP/UDP) • Port number • Id of darknet collector • network prefix • Number of requests

Start of collection	Jan 1st, 2018
No. of events (Mar 31st 2019)	244,535
Average ingestion rate (overall)	22.4 events per hour (537 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	14.4 events per hour (346 events per day)
Average ingestion delay	Between 0 and 24 hours (aggregated on daily basis)
Types of actionable insights	Active networks
No. of actionable insights	24,065 IPs. Top 10 (by number of events): • 196.52.43.0/24: 9144 • 80.82.77.0/24: 8531 • 184.105.139.0/24: 6413 • 184.105.247.0/24: 4679 • 74.82.47.0/24: 4578 • 89.248.167.0/24: 4329 • 185.94.111.0/24: 4013 • 216.218.206.0/24: 3626 • 93.174.95.0/24: 3376 • 89.248.172.0/24: 3022

2.3 Malware

2.3.1 NASK

Description	Malware binaries ingested by NASK
Start of collection	Jul 26th, 2018
No. of samples (Mar 31st 2019)	3,810
Average ingestion rate (overall)	15.3 samples per day

2.3.2 VirusShare

Description	Malware binaries from VirusShare
Start of collection	Jun 10th, 2017
No. of samples (Mar 31st 2019)	884,228
Average ingestion rate (overall)	55.9 samples per hour (1,341 samples per day)

2.4 Varia

2.4.1 BadIP

Description	IP addresses with bad reputation observed by DTAG honeypots
Start of collection	Jan 11th, 2018
No. of events (Mar 31st 2019)	179,038,846
Average ingestion rate (overall)	4.66 events per second (402,811 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	5.62 events per hour (485,319 events per day)
Average ingestion delay	< 2 hours
Types of actionable insights	IP addresses
No. of actionable insights	10,224,391 unique IPs. Top 10 (by number of events): • 82.221.105.6: 7038 • 93.174.93.136: 7029 • 71.6.146.185: 7019 • 89.248.167.131: 7018 • 71.6.167.142: 7016 • 139.162.102.46: 7016 • 71.6.158.166: 7009 • 139.162.108.129: 7002 • 139.162.87.250: 6999 • 80.82.77.33: 6990

2.4.2 GData URLs

Description	Malicious URLs reported by GDATA
Start of collection	Jun 22nd, 2017
No. of events (Mar 31st 2019)	9,798,365
Average ingestion rate (overall)	10.5 events per minute (15,128 events per day)
Average ingestion rate (Mar 25th - Mar 31st 2019)	14.3 events per minute (20,625 events per day)
Average ingestion delay	< 4 hours (feed received and ingested every 4 hours)

Types of actionable insights	Malicious URLs
No. of actionable insights	3,503,773 distinct URLs

3 Datasets - Qualitative Analysis

Having established a rough description of the datasets collected in the previous section, this section focuses on the data contained therein regarding various aspects.

First, to evaluate the utility of deploying a wide range of different honeypots, the overlap between datasets is considered.

Afterwards, the geographic distribution of datasets is analysed to shed light onto the global coverage of the SISSDEN honeypot network.

Finally, in an attempt to verify the correctness and completeness of the data collected, a comparison is performed with open source data that is provided by third parties.

3.1 Data overlap

Analysing events occurred in the week Mar 25th - Mar 31st 2019, we can see the number of different IP addresses that attacked it, as shown in Figure 3.1.

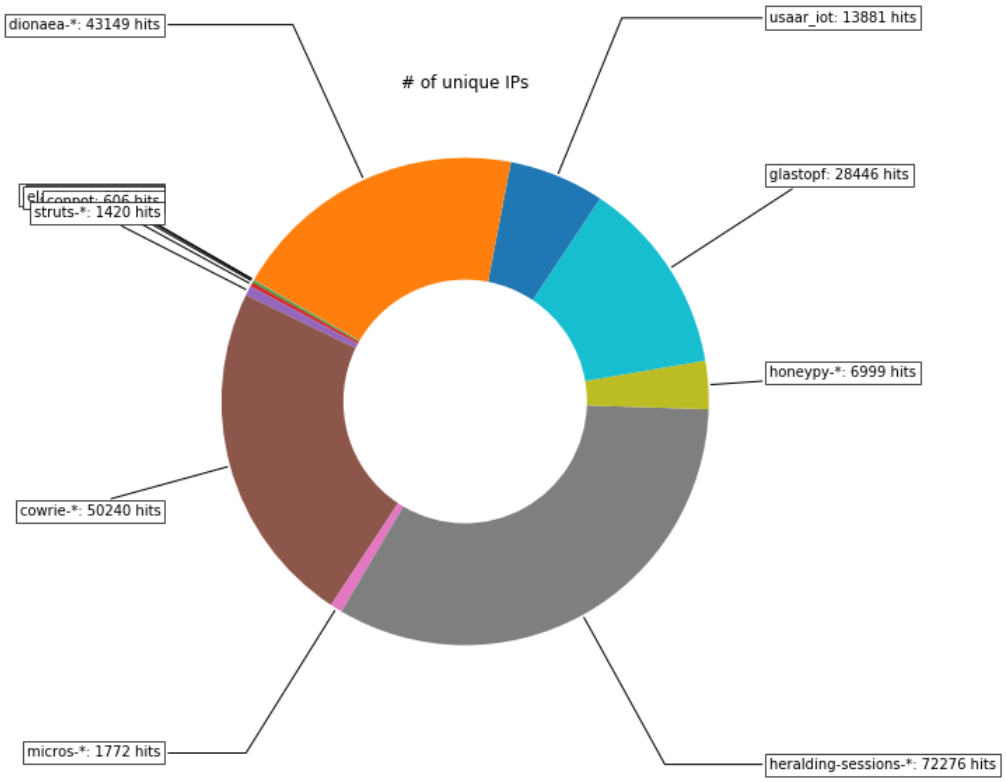

Figure 3.1: Distinct IP addresses per honeypot in a week of events

To better understand the contribution of every honeypot, the top 10’000 attacking IPs per honeypot are taken into consideration and those that are found in more than one kind of honeypot are removed. This leaves us with an indication of how many attackers are truly unique to that kind of honeypot, as shown in Figure 3.2.

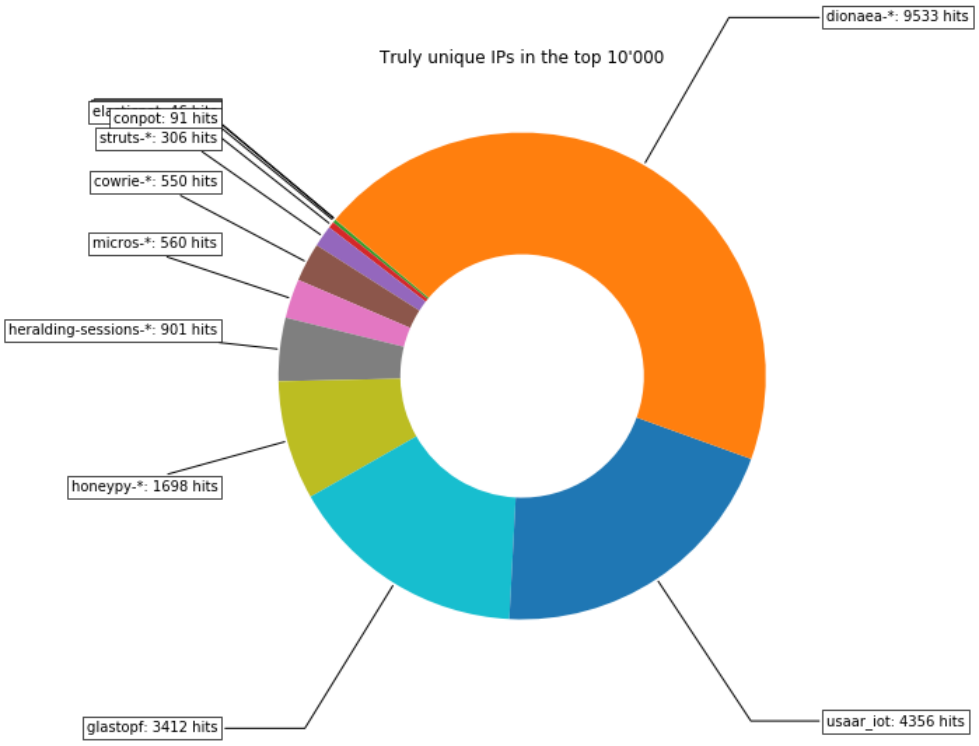

Figure 3.2: Truly unique attacking IPs in the top 10’000, per honeypot

3.2 Global coverage of datasets

3.2.1 AmpPot

AmpPot observed 3,977,420 events from different 224 countries, the vast majority of them targeted towards the USA (32.2%), which together with China, France and Saudi Arabia accounts for more than half (57.2%) of all attacks.

Top 10:

- USA: 1,279,330 (32.2%)
- CHN: 511,378 (12.9%)
- FRA: 276,887 (7.0%)
- SAU: 206,950 (5.2%)
- GBR: 175,806 (4.4%)
- DEU: 133,406 (3.4%)
- BRA: 125,252 (3.1%)
- POL: 118,387 (3.0%)
- HKG: 108,385 (2.7%)
- CAN: 105,013 (2.6%)

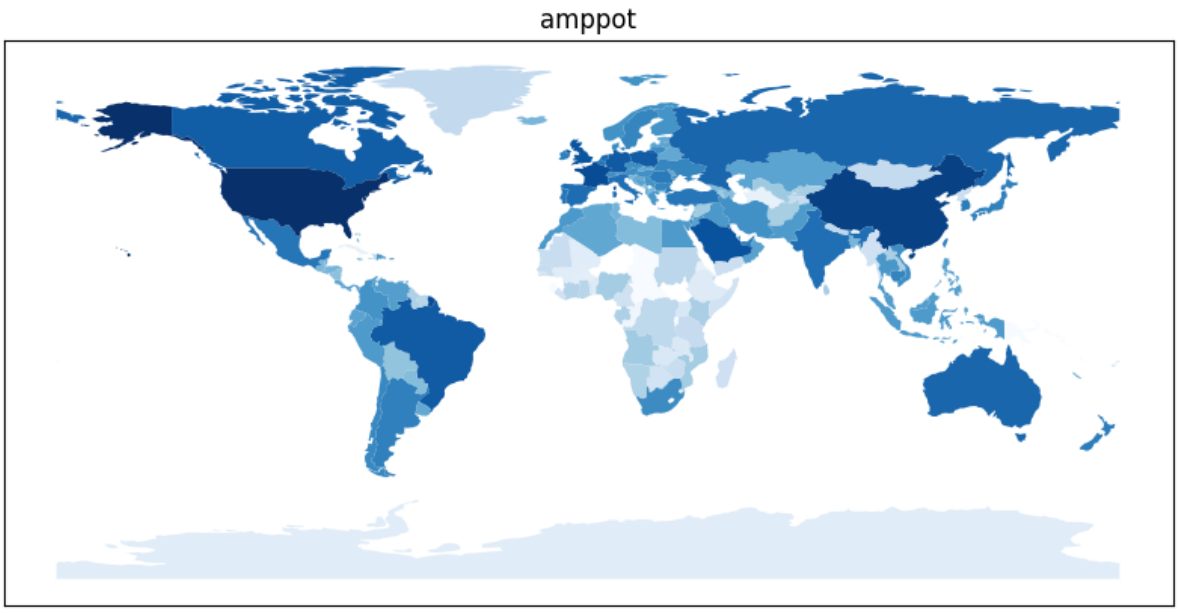

Figure 3.3: Global coverage of AmpPot

3.2.2 CiscoASA

CiscoASA observed 11,828 events from 68 different countries. More than half of these came from systems in the USA, followed by China and Russia with about 10% each.

Top 10:

- USA: 6,032 (51.0%)
- CHN: 1,386 (11.7%)
- RUS: 1,135 (9.6%)
- NLD: 879 (7.4%)
- DEU: 639 (5.4%)
- ROU: 152 (1.3%)
- FRA: 136 (1.1%)
- VNM: 127 (1.1%)
- NIC: 124 (1.0%)
- SGP: 91 (0.8%)

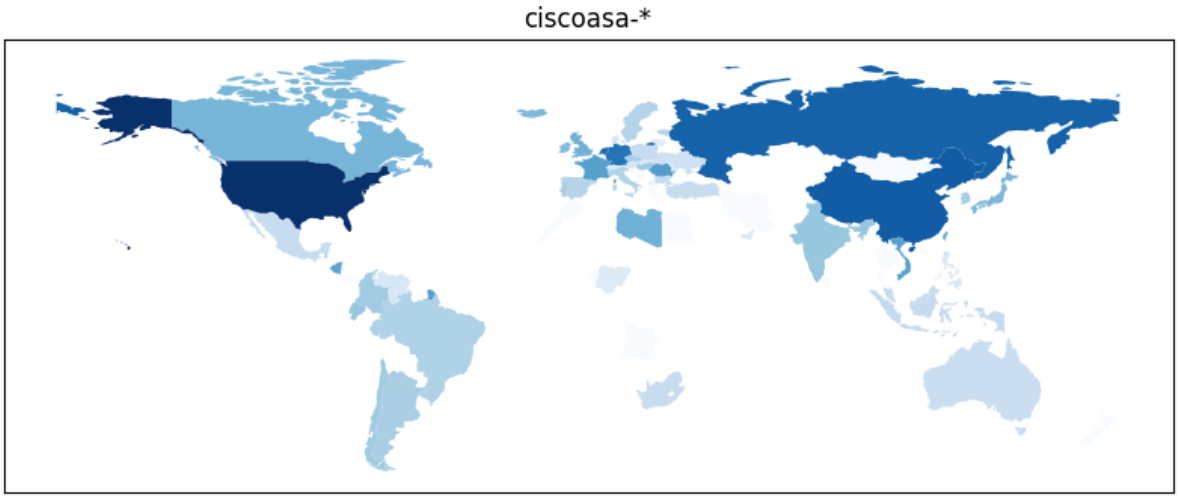

Figure 3.4: Global coverage of CiscoASA

3.2.3 Conpot

Conpot observed 2,494,531 events from 194 different countries. Contrary to before, almost half of these stem from China or Hong Kong, with the USA in third place.

Top 10:

- CHN: 791,505 (31.7%)
- HKG: 450,654 (18.1%)
- USA: 384,527 (15.4%)
- SYC: 130,100 (5.2%)
- NLD: 125,340 (5.0%)
- JPN: 45,942 (1.8%)
- RUS: 45,569 (1.8%)
- BRA: 44,466 (1.8%)
- FRA: 41,547 (1.7%)
- THA: 41,449 (1.7%)

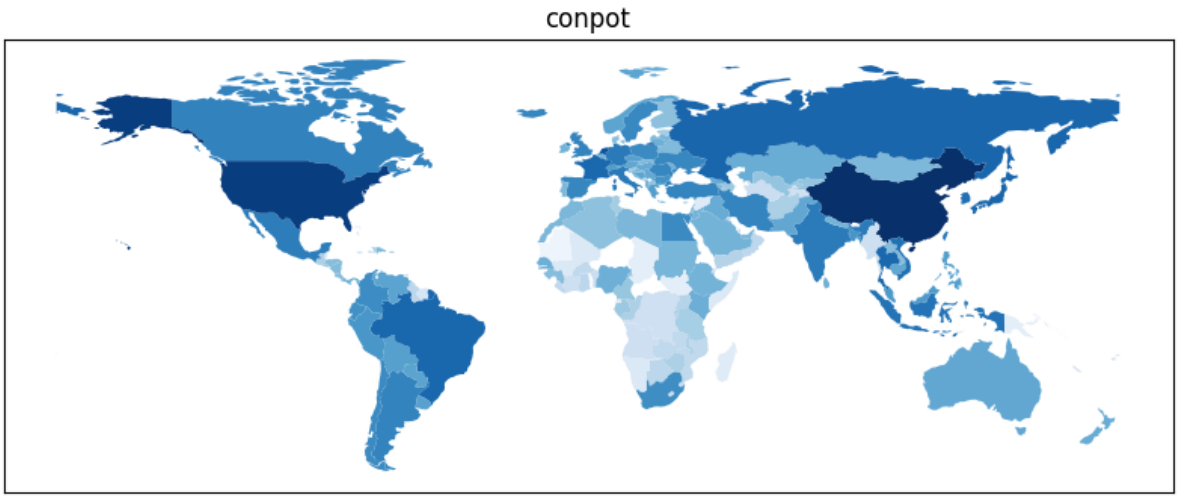

Figure 3.5: Global coverage of Conpot

3.2.4 Cowrie

Cowrie observed 414,916,048 events from 223 different countries. A third of these came from the USA, with Russia and Ireland in second and third place.

Top 10:

- USA: 144,580,682 (34.8%)
- RUS: 58,693,401 (14.1%)
- IRL: 33,168,359 (8.0%)
- NLD: 25,350,469 (6.1%)
- DEU: 21,332,936 (5.1%)
- ITA: 21,078,897 (5.1%)
- IND: 12,995,970 (3.1%)
- CHN: 12,509,525 (3.0%)
- CAN: 11,660,738 (2.8%)
- GBR: 11,000,910 (2.7%)

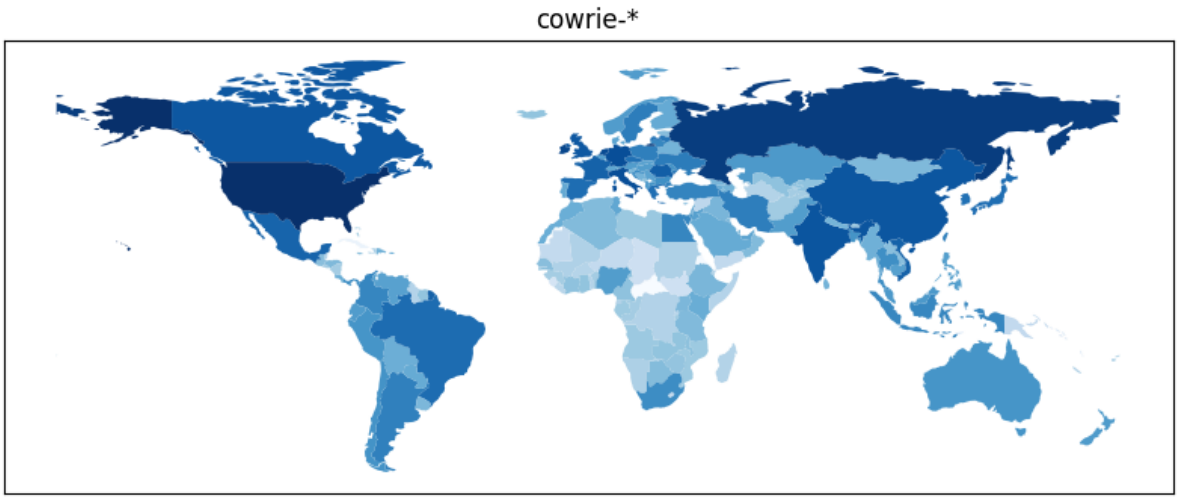

Figure 3.6: Global coverage of Cowrie

3.2.5 Dionaea

Dionaea observed 1,332,133 events from 190 different countries. Here, again China accounts for a good fifth of events, China, Brazil, and the USA together for more than half.

Top 10:

- CHN: 282,130 (21.2%)
- BRA: 258,176 (19.4%)
- USA: 134,225 (10.1%)
- VNM: 112,325 (8.4%)
- IND: 70,573 (5.3%)
- RUS: 65,796 (4.9%)
- IDN: 60,161 (4.5%)
- PHL: 24,118 (1.8%)
- TWN: 22,542 (1.7%)
- THA: 22,238 (1.7%)

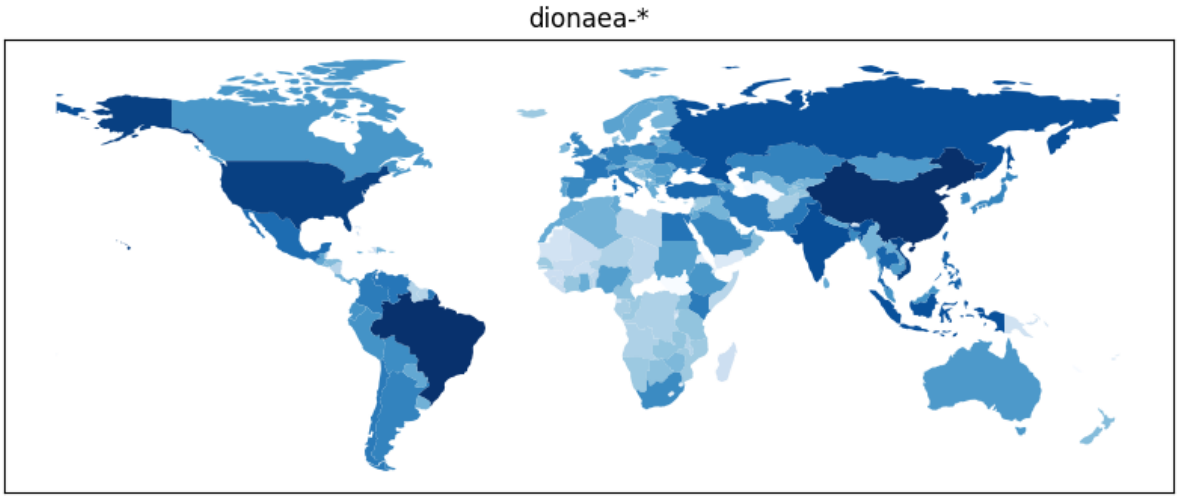

Figure 3.7: Global coverage of Dionaea

3.2.6 ElasticPot

ElasticPot observed 110,391 events from 91 different countries. The overwhelming majority of events is from the USA, followed by China and Hong Kong.

Top 10:

- USA: 60,751 (55.0%)
- CHN: 11,664 (10.6%)
- HKG: 8,918 (8.1%)
- SYC: 4,648 (4.2%)
- ROU: 4,199 (3.8%)
- NLD: 3,390 (3.1%)
- RUS: 2,969 (2.7%)
- IND: 2,182 (2.0%)
- DEU: 1,586 (1.4%)
- FRA: 1,272 (1.2%)

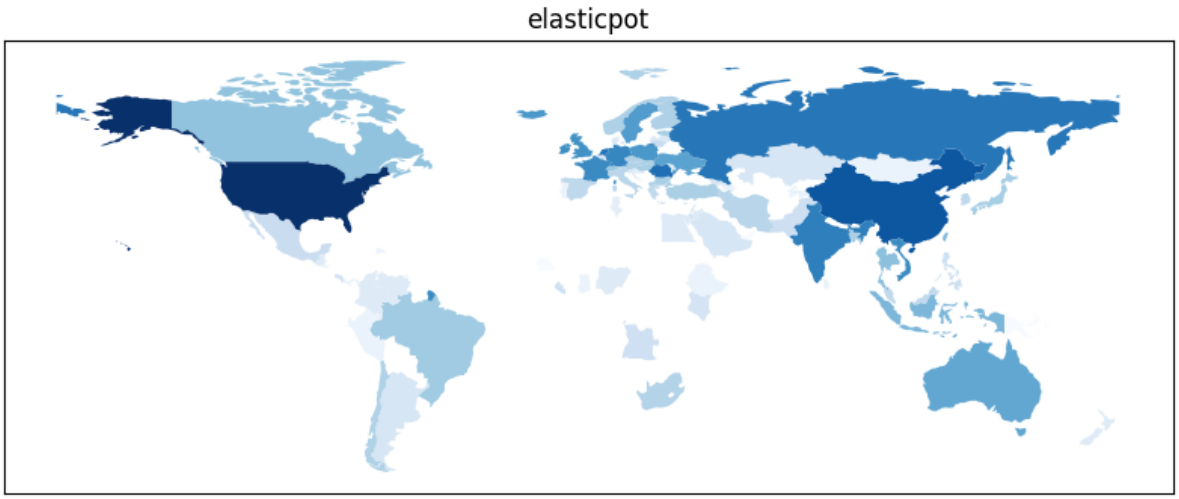

Figure 3.8: Global coverage of ElasticPot

3.2.7 Glastopf

Glastopf observed 26,586,648 events from 224 different countries. Interestingly, a quarter of these originates from Canada, more than from the USA or China. Top 10:

- CAN: 6,635,879 (25.0%)
- USA: 5,239,380 (19.7%)
- CHN: 4,181,870 (15.7%)
- RUS: 1,782,597 (6.7%)
- DEU: 1,363,121 (5.1%)
- FRA: 1,146,182 (4.3%)
- UKR: 964,580 (3.6%)
- ITA: 497,472 (1.9%)
- HKG: 496,708 (1.9%)
- NLD: 363,144 (1.4%)

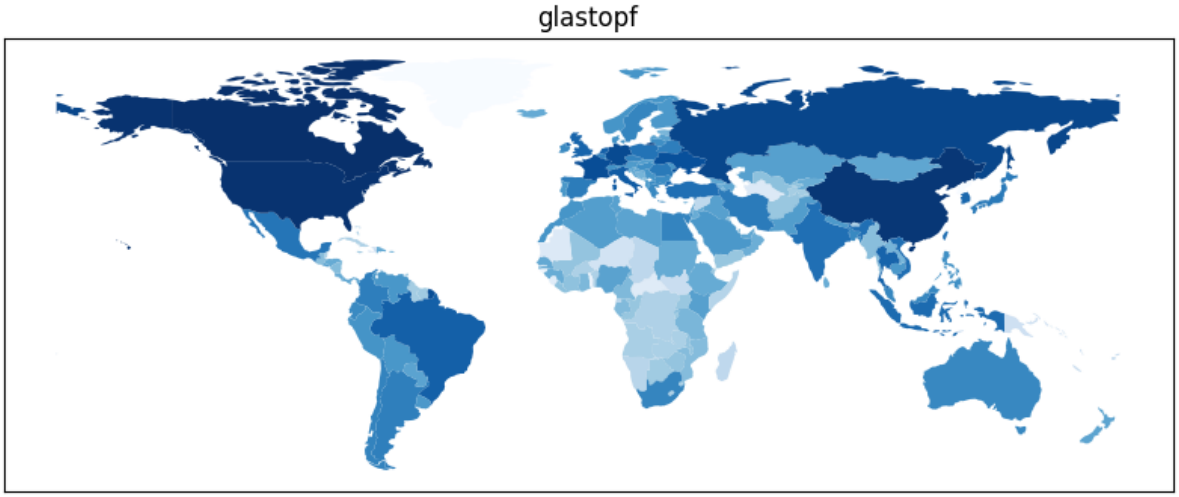

Figure 3.9: Global coverage of Glastopf

3.2.8 Heralding

Heralding observed 566,305,498 events from 219 different countries. Half of these from China or Russia. The number of events from Poland even pushes the USA out of the top 3.

Top 10:

- CHN: 160,829,323 (28.4%)
- RUS: 140,128,188 (24.7%)
- POL: 58,147,993 (10.3%)
- USA: 57,321,231 (10.1%)
- NLD: 15,909,345 (2.8%)
- IND: 12,239,215 (2.2%)
- FRA: 11,160,630 (2.0%)
- BRA: 9,829,114 (1.7%)
- GBR: 9,532,187 (1.7%)
- DEU: 7,721,306 (1.4%)

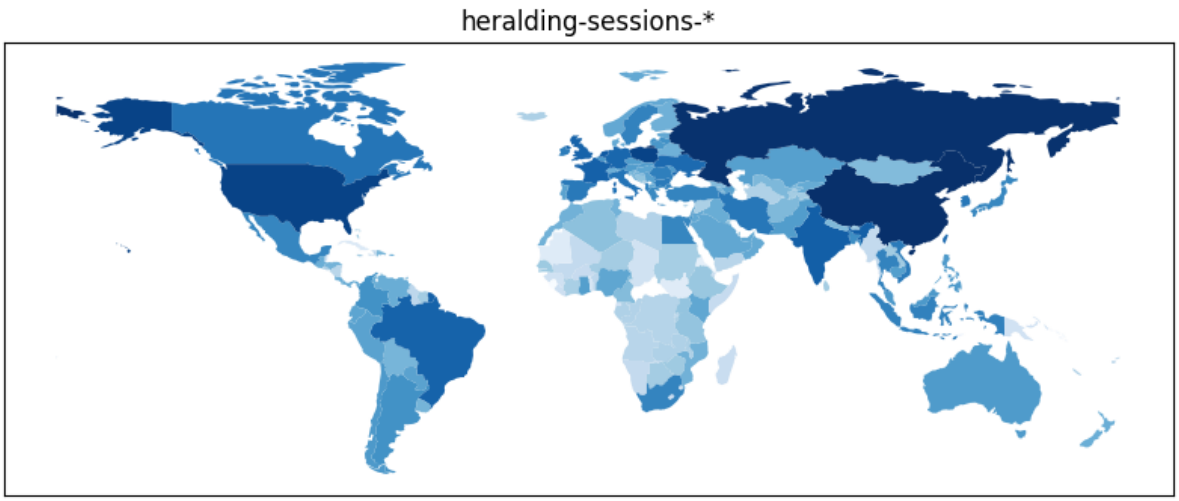

Figure 3.10: Global coverage of Heralding sessions

3.2.9 HoneyPy

HoneyPy observed 80,407,576 events from 163 different countries. Almost exactly half of all events originate from China, and 3 out of 4 events coming from either China, the USA or Russia.

Top 10:

- CHN: 40,175,047 (50.0%)
- USA: 14,367,616 (17.9%)
- RUS: 6,015,454 (7.5%)
- HKG: 3,544,571 (4.4%)
- BEL: 3,076,946 (3.8%)
- IND: 2,798,968 (3.5%)
- SGP: 2,430,811 (3.0%)
- THA: 1,740,726 (2.2%)
- SRB: 1,083,838 (1.3%)
- COL: 867,430 (1.1%)

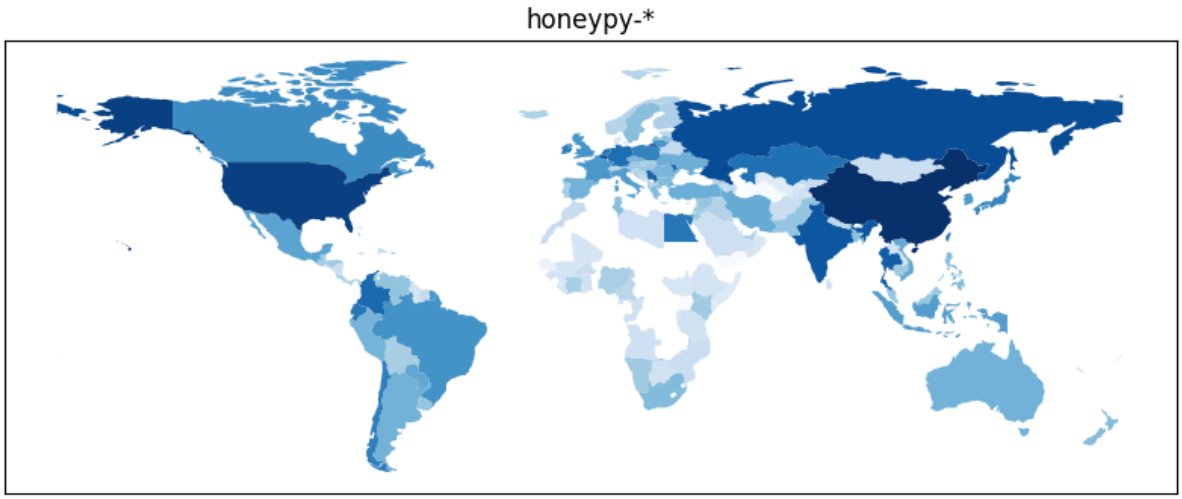

Figure 3.11: Global coverage of HoneyPy

3.2.10 Micros

Micros observed 31,667 events from 163 different countries.

Top 10:

- BRA: 5,579 (17.6%)
- USA: 4,412 (13.9%)
- CHN: 2,428 (7.7%)
- RUS: 2,188 (6.9%)
- IND: 1,328 (4.2%)
- IRN: 1,201 (3.8%)
- EGY: 1,098 (3.5%)
- UKR: 847 (2.7%)
- NLD: 846 (2.7%)
- IDN: 811 (2.6%)

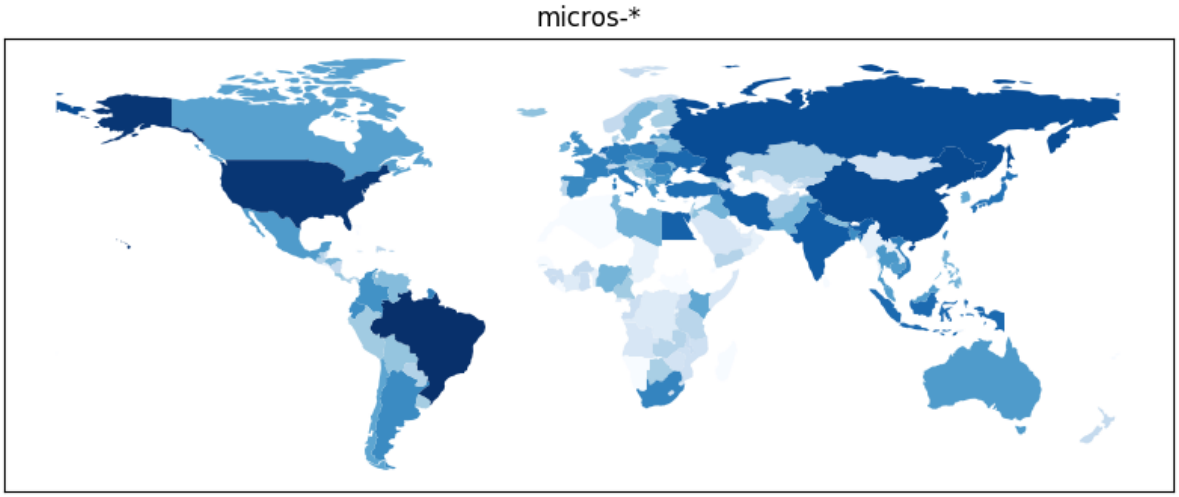

Figure 3.12: Global coverage of Micros

3.2.11 Struts

Struts observed 10,598 events from 142 different countries. Top 10:

- BRA: 1,427 (13.5%)
- USA: 1,256 (11.9%)
- RUS: 1,202 (11.3%)
- CHN: 947 (8.9%)
- UKR: 430 (4.1%)
- IRN: 389 (3.7%)
- DEU: 384 (3.6%)
- IND: 337 (3.2%)
- NLD: 273 (2.6%)
- TWN: 271 (2.6%)

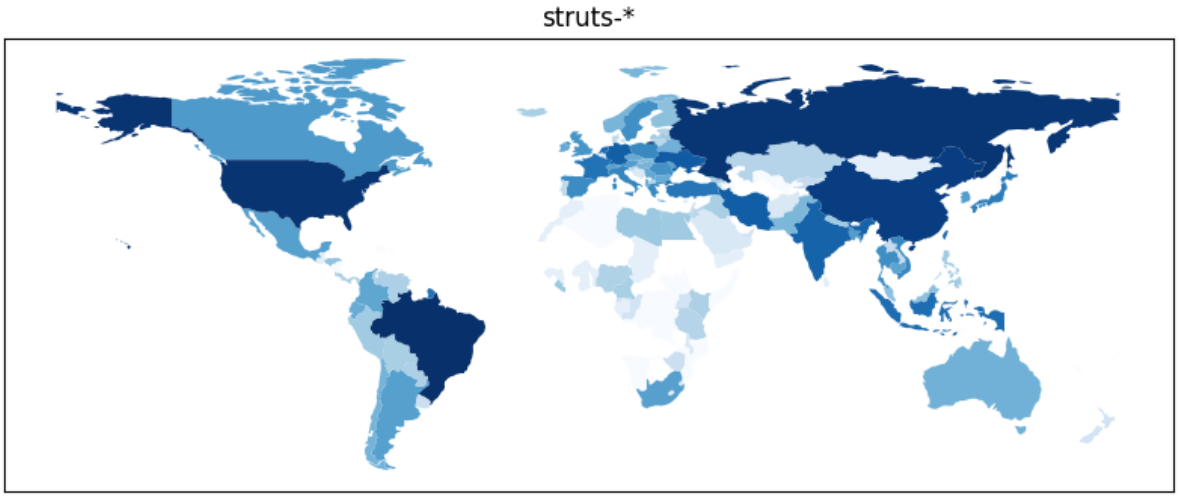

Figure 3.13: Global coverage of Struts

3.2.12 Weblogic

Weblogic observed 3,333 events from 30 different countries. Top 10:

- JPN: 352 (10.6%)
- USA: 341 (10.2%)
- CHN: 307 (9.2%)
- COL: 128 (3.8%)
- MDA: 108 (3.2%)
- NLD: 96 (2.9%)
- RUS: 49 (1.5%)
- KOR: 32 (1.0%)
- HKG: 30 (0.9%)
- VNM: 27 (0.8%)

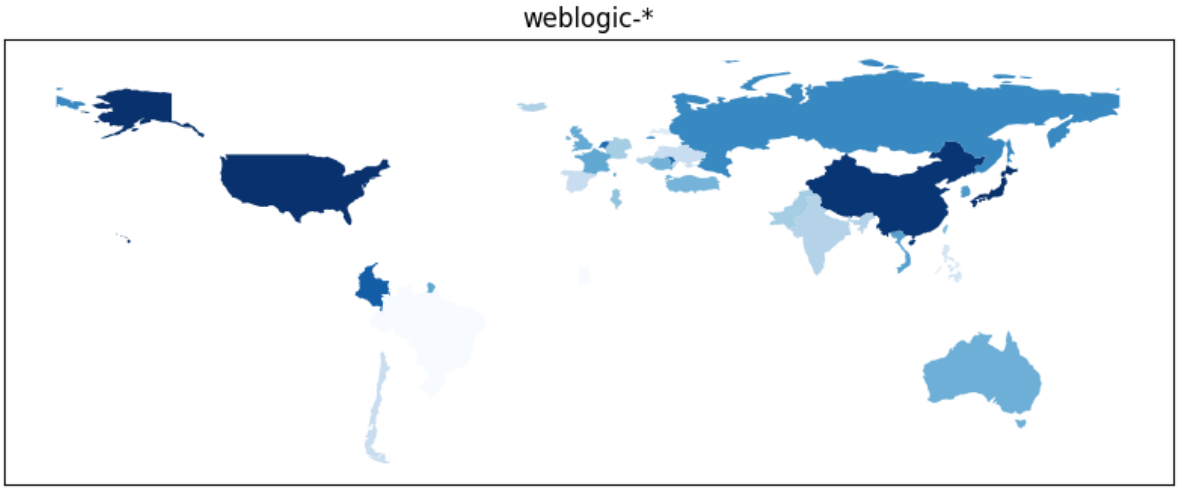

Figure 3.14: Global coverage of Weblogic

3.2.13 Conclusion

While the exact traffic distribution differs between honeypots types, every honeypot observes events all around the globe. In total, SISSDEN datasets cover 245 out of the 249 country codes defined by ISO 3166-1.

3.3 Comparison with OSInt data

3.3.1 NoThink! Honeypots

NoThink! Honeypots periodically publishes lists of statistics from a honeypot network. The lists cover various time ranges and protocols. Starting with data from the SSH protocol for the year 2019, 2888 individual IPs are listed (as of 10 April 2019). Matching with SISSDEN data, we can see that most had a match, missing only 53 (1.84%). Figure 3.15 illustrates matches across honeypot indices.

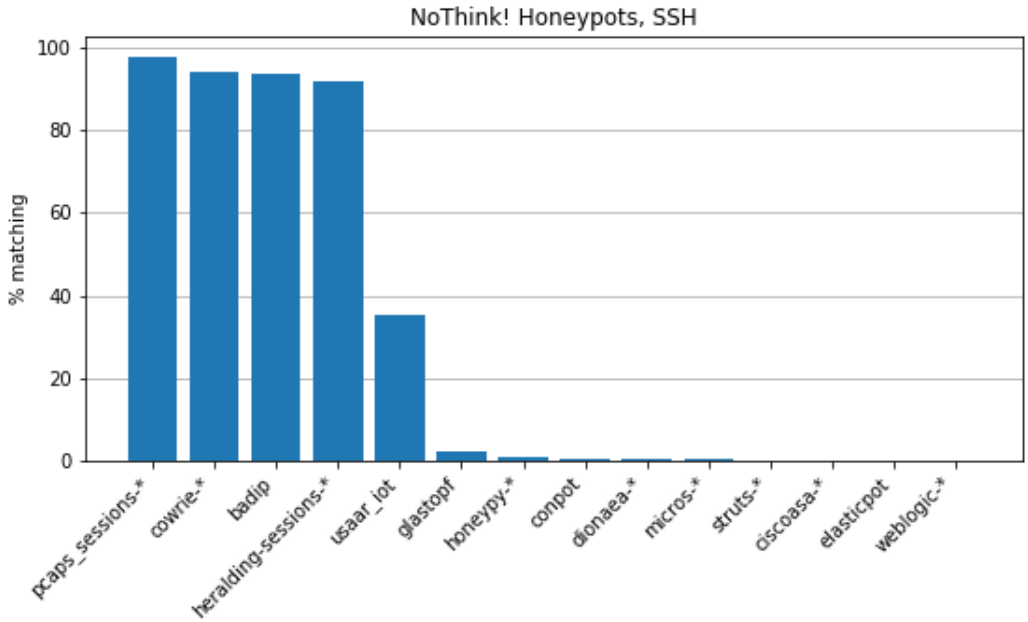

Figure 3.15: Percentage of matched IPs with NoThink! Honeypots data, SSH protocol

Performing the same analysis with Telnet data, 3469 events are listed from NoThink! Honeypots, of which 541 (15.6%) didn't appear in SISSDEN data. Results are shown in Figure 3.16.

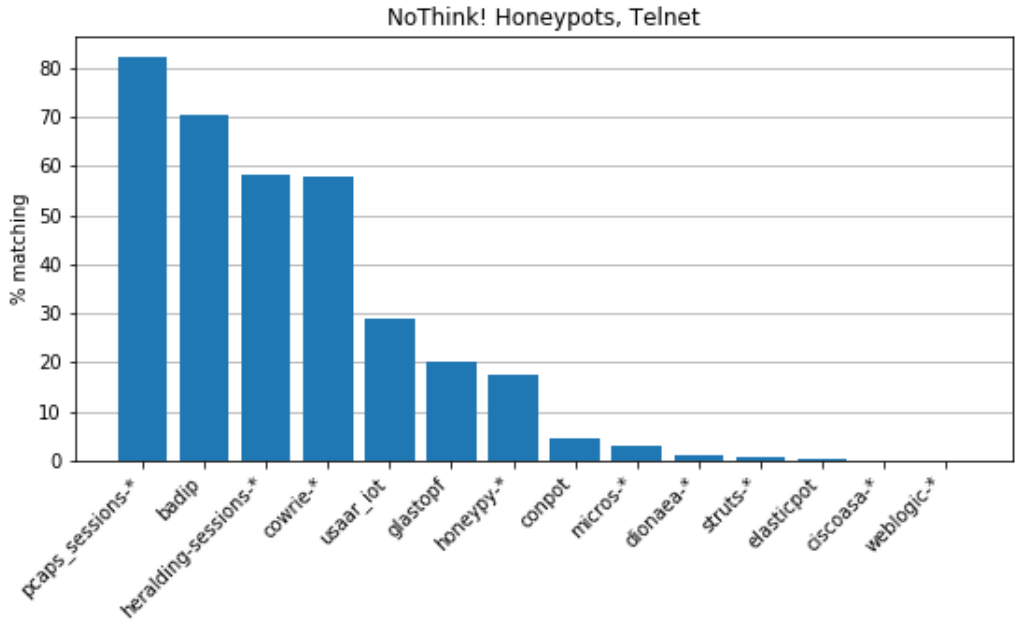

Figure 3.16: Percentage of matched IPs with NoThink! Honeypots data, Telnet protocol

For the SNMP protocol, only 137 IPs are listed, with 2 (1.46%) without a match. Results across honeypot indices are shown in Figure 3.17.

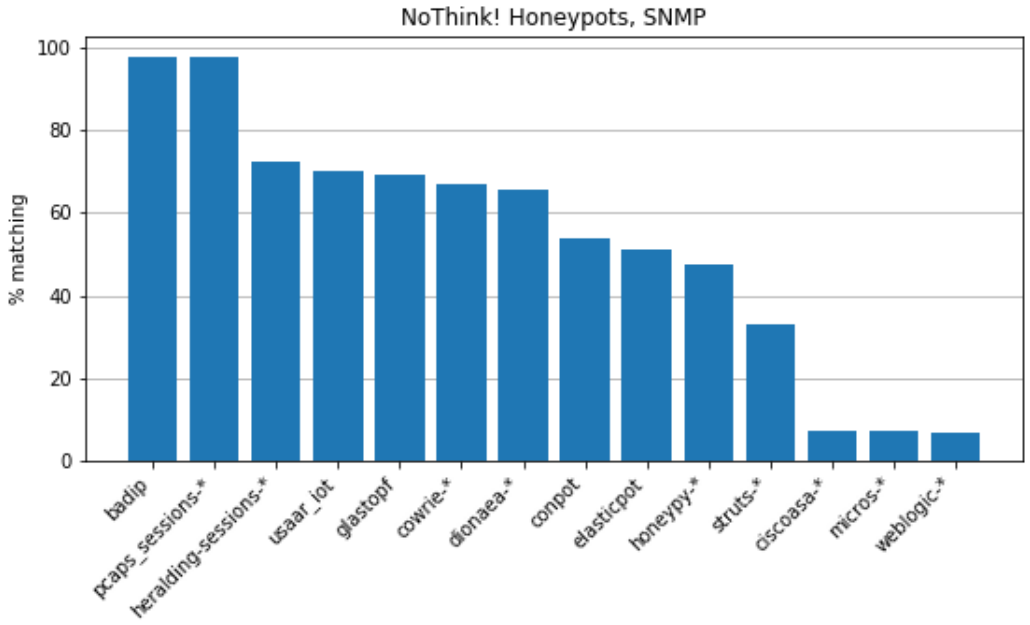

Figure 3.17: Percentage of matched IPs with NoThink! Honeypots data, SNMP protocol

NoThink! Honeypots also has a section dedicated to DNS amplification attacks. At the time of writing, this dataset lists 396 attacked IPs, but taking into consideration only records after 10th October 2017 (the day Amppot first started collecting data), this number falls to 28, of which only 1 didn't have a match.

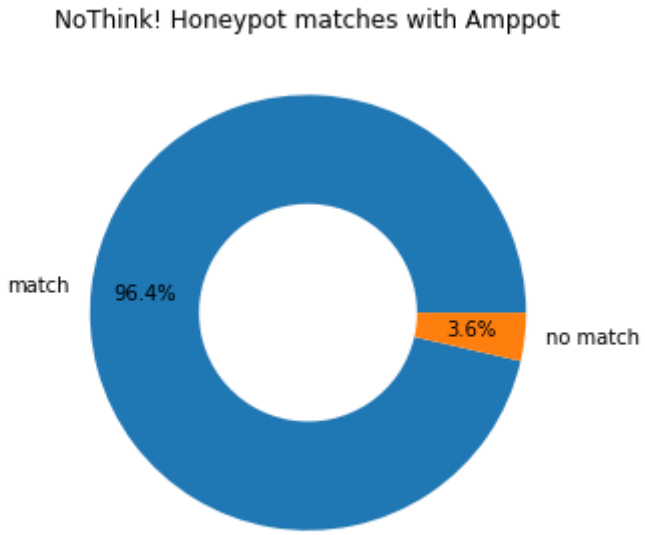

Figure 3.18: Amppot matches with NoThink! Honeypot DNS amplification attacks

Taking into consideration all events collected by AmpPot in the same time range, we can see that the number of distinct attacked IP addresses greatly outnumbers that of NoThink! Honeypots.

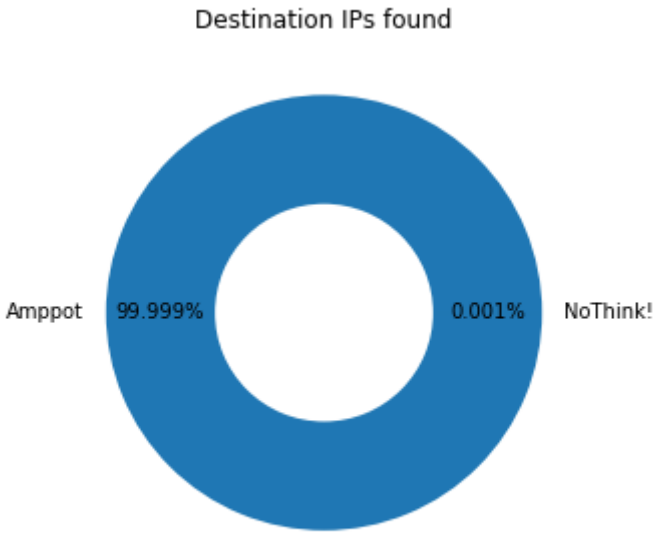

Figure 3.19: Comparison between distinct IPs collected by AmpPot vs NoThink!

3.3.2 Green Snow

Green Snow publishes an IP blacklist originating from “attacks of any kind except for spam”. On 10th April 2019 the list contained 3771 records, with no time reference about when each record was registered. Matching with data collected by SISSDEN resulted in Figure 3.20. 1198 IPs didn’t have any match.

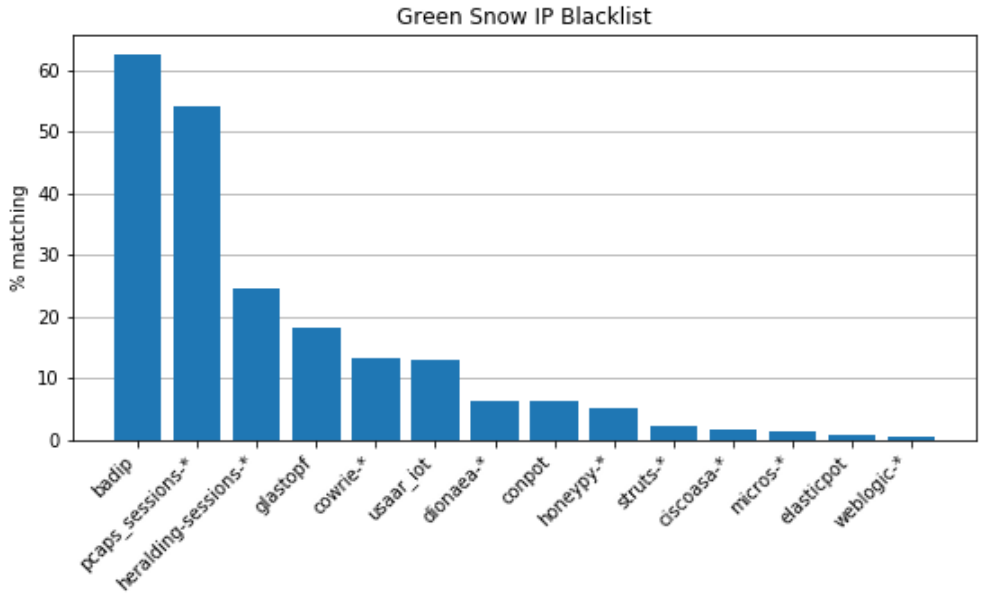

Figure 3.20: Percentage of matched IP addresses with Green Snow’s IP blacklist

3.3.3 Talos Intelligence

Talos Intelligence from CISCO publishes an IP Blacklist. At the time of writing (9th April 2019) the list contains 1604 records. No information is given about the time each record was registered. 660 IPs were found to be unique to this list, while the others had a match in data collected by SISSDEN in the percentages shown in Figure 3.21.

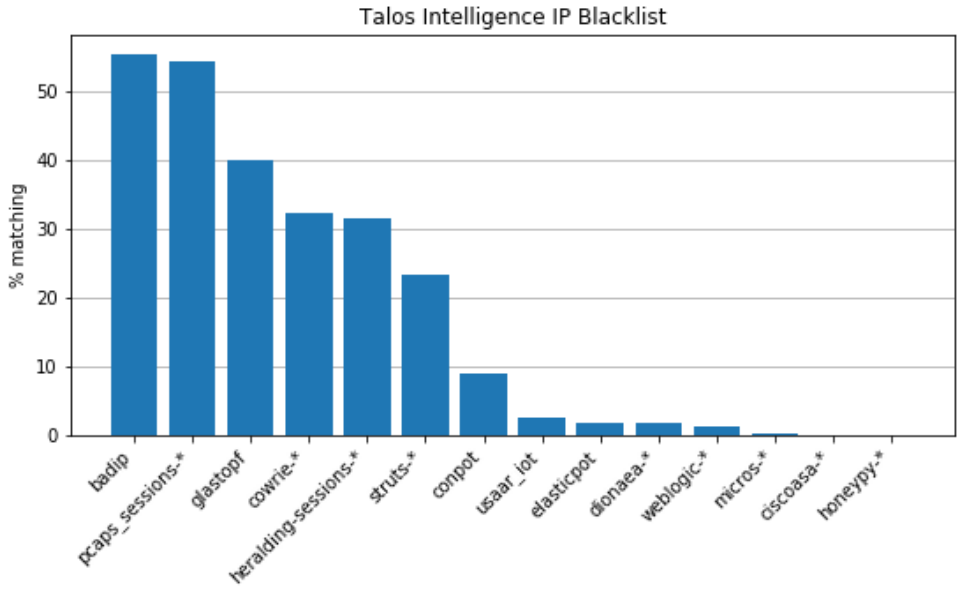

Figure 3.21: Percentage of matched IP addresses with Talos Intelligence’s IP Blacklist

3.3.4 BruteForceBlocker SSH login probes

This dataset lists IP addresses that tried and failed to login via SSH. On the 9th April 2019, the dataset was downloaded. It contained 961 IPs collected over the period ranging 10th March - 9th April 2019. Searching for the existence of the given IPs in the data collected by SISSDEN, only 9 addresses didn't have a match. Figure 3.22 illustrates the number of matched IP addresses per index taken into account.

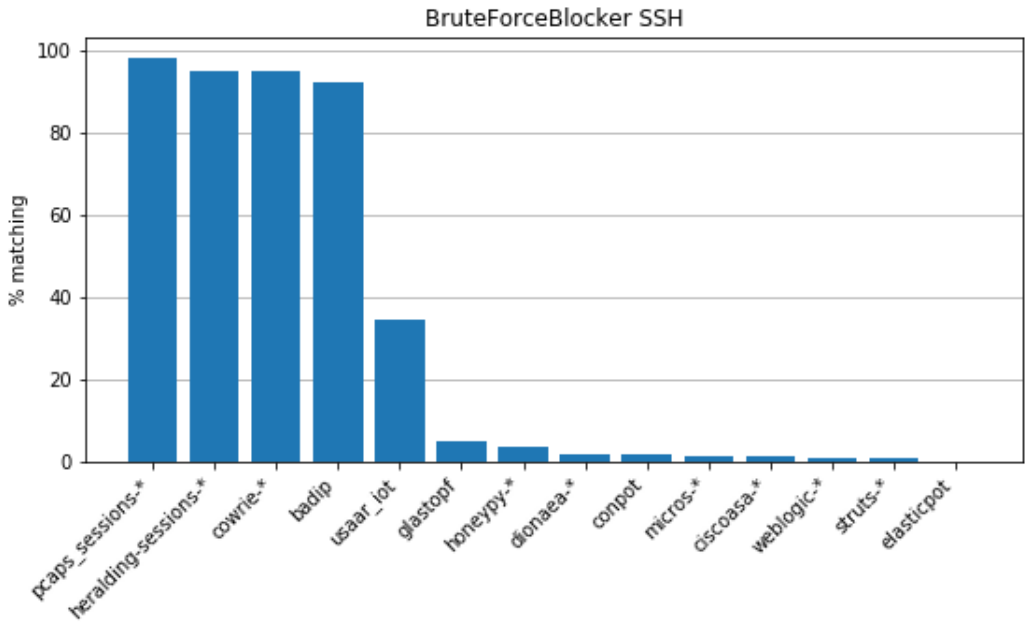

Figure 3.22: Percentage of matched IP addresses with BruteForceBlocker data

Also, note that for the same time range, SISSDEN's network collected 2,637,102 distinct attacking sources.

3.3.5 Blocklist.de

Blocklist.de exposes the IP addresses of the last 25 reported attacks and the top 15 attackers. For both lists, only 2 addresses (the same ones) did not match SISSDEN data. Figures 3.23 and 3.24 illustrate the results.

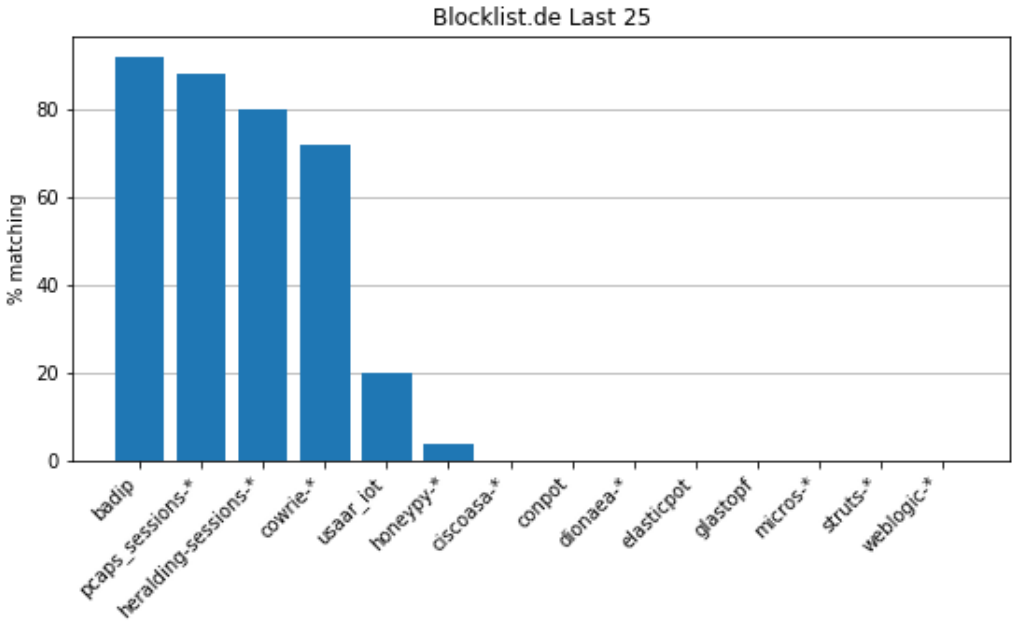

Figure 3.23: Percentage of matched IP addresses with the last25 list provided by Blocklist.de

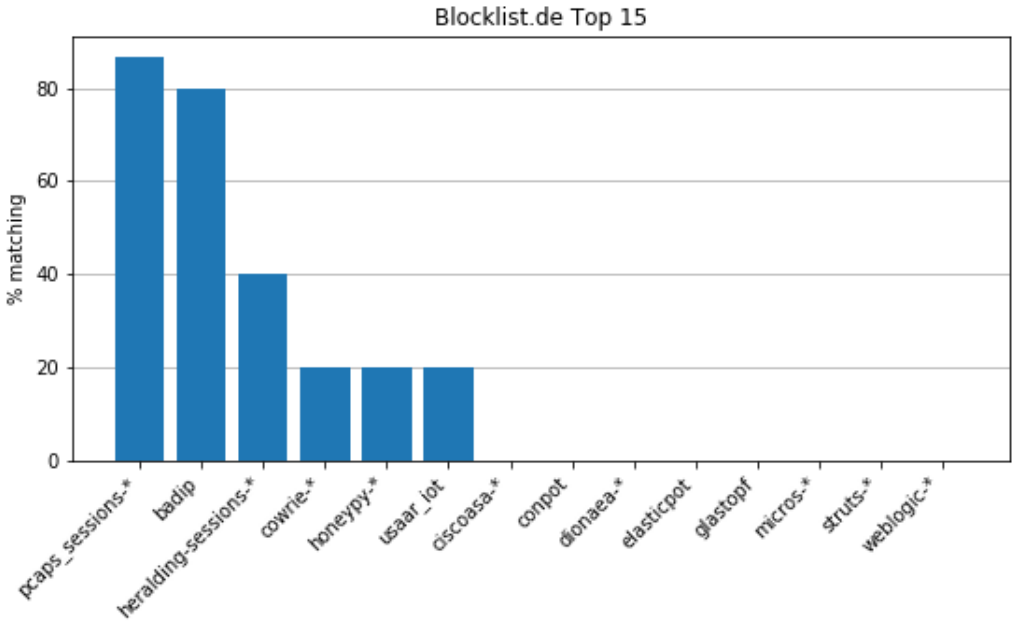

Figure 3.24: Percentage of matched IP addresses with the top15 list provided by Blocklist.de

4 Continuous Analytical Modules

Next to the extensive data collection, another key feature of the SISSDEN Platform Pilot is the analytical platform and its analytical modules that fuse and extract insights from the data collected. This section hence gives a quantitative assessment of the data produced by these analytical modules.

In general, analytical modules developed in WP 5 as part of the analytical platform follow one of two possible execution strategies:

1. **One-off on demand execution**: These modules can be queried by an analyst on specific data to further examine an incident.
2. **Continuous execution**: These modules are run in a continuous fashion, either on a fixed periodic interval or as soon as new data is available.

As the former type of analysis only produces results on an as-needed basis, these analyses are excluded from the quantitative characterization given in this section as the amount of results they produce strongly depends on their use by analysts. This section thus only describes modules running continuously which regularly produce new results as new events are ingested into the platform.

For every analytical module, this section lists the date the module was enabled in the SISSDEN Platform Pilot, a short description of the events produced by the module, as well as the number of events produced and their average rate.

For a full description of all analytical modules, please refer to D5.3 “Final Data Analysis Results”.

4.1 Anomaly Detection Alerts

Description	Anomaly Detection Alerts
Start of analysis	Feb 6th, 2019
No. of events (Apr 15th 2019)	16,266
Average event rate	238 events per day

4.2 HoneyPy Droppers

Description	Dropper scripts extracted from attacks against HoneyPy
Start of analysis	Mar 26th, 2019
No. of events (Apr 15th 2019)	110,184
Average event rate	224 events per hour (5,365 events per day)

4.3 Cowrie URLs

Description	Download URLs extracted from attacks against cowrie
Start of analysis	Mar 27th, 2019
No. of events (Apr 15th 2019)	218,200
Average event rate	468 events per hour (11,227 events per day)

4.4 PGA Analyzer

Description	PGA signatures observed in NASK darknet
Start of analysis	Apr 15th, 2018
No. of events (Apr 15th 2019)	65,625,002
Average event rate	2.08 events per second (179,648 events per day)

4.5 SMTP Analyzer

Description	Results of SMTP dialect analyser on spam mails received by spampot
Start of analysis	May 8th, 2018
No. of events (Apr 15th 2019)	335,365
Average event rate	979 events per day

4.6 Darknet Event

Description	Malicious Events identified in NASK darknet traffic
Start of analysis	Apr 26th, 2018
No. of events (Apr 15th 2019)	7,802,356,269
Average event rate	254.83 events per second (22 million events per day)

4.7 USAAR Sandbox

Description	Malware analysis results from USAAR sandbox. Analysis results include a full network capture of the malware's network traffic, a reduced flow description of the traffic, a screenshot, as well as a classification label for known malware. Sandbox environment are provided for Windows malware, Linux malware, IoT malware, and Mobile (Android) malware.
Start of analysis	Jun 12th, 2017
No. of events (Apr 15th 2019)	781,547
Average event rate	48.44 events per hour (1,163 events per day)

4.8 C2 Extraction

Description	Traffic recorded during sandbox execution is filtered for known pattern of C2 communication. If such communication is identified, the IP address and port information of the C2 server is extracted.
Start of analysis	Jun 12th, 2017
No. of events (Apr 15th 2019)	259,855
Average event rate	16.1 events per hour (387 events per day)

4.9 Scanner Fingerprinting

Description	Attacks observed by AmpPot honeypots are analysed for identifying information of the system that scanned for reflectors as attack preparation. Using this information, it is possible to link back an attack to its reconnaissance phase.
Start of analysis	Oct 10th, 2017
No. of events (Apr 15th 2019)	1,267,503
Average event rate	1.59 events per minute (2,294 events per day)

5 Remediation Reports

Besides the collected data sets and analysis modules, the SISSDEN pilot has also been of impact to the community through remediation reports. This section quantifies the number of events that has been reported to network operators and organizations as well as the impact these reports had had based on the results of a survey conducted among the recipients.

5.1 Reports

SISSDEN remediation reports help network operators and organizations by providing situational awareness of activities regarding their networks. Reports are sent out via Shadowserver's daily remediation feed, through which 100 National CSIRTs and over 4100 network owners, at least 1100 of which are EU network owners, are reached. During the SISSDEN pilot, 5 new report types have been established:

5.1.1 Drone Brute Force[1]

Name	Drone Brute Force
Description	The Drone Brute Force report reports login attempts observed by cowrie and heralding honeypots against telnet and ssh services.
Established	April 2018 (first test operation since April 2017)
No. of events reported (Apr 16th 2019)	6,429,800 events

5.1.2 HTTP Scanners[2]

Name	HTTP Scanners
Description	The HTTP Scanners report reports scan activity observed by HTTP-based service honeypots Glastopf and ElasticPot.
Established	September 2018
No. of events reported (Apr 16th 2019)	1,338,039 events

[1] https://sissden.eu/blog/brute-force

[2] https://sissden.eu/blog/http-scanners-report

5.1.3 ICS Scanners[3]

Name	ICS Scanners
Description	The ICS Scanners report reports scan events against industrial control systems as observed by the Conpot honeypot.
Established	September 2018
No. of events reported (Apr 16th 2019)	142,188 events

5.1.4 Amplification DDoS Victim[4]

Name	Amplification DDoS Victim
Description	The Amplification DDoS Victim report reports DDoS attack victims observed by AmpPot honeypots.
Established	October 2018
No. of events reported (Apr 16th 2019)	36,730 events

5.1.5 Darknet[5]

Name	Darknet
Description	The Darknet report reports general scanning activity observed in darknets, enriched with output of the PGA analysis.
Established	October 2018
No. of events reported (Apr 16th 2019)	23,272,041 events

5.2 Report Recipient Survey

To validate the utility of the reports established during the SISSDEN pilot operation and thereby evaluate the impact of SISSDEN to network operators, a survey was conducted among report recipients. While the full survey can be found in D2.6, this section puts a focus specifically on those questions regarding the utility and impact of SISSDEN remediation reports.

[3] https://sissden.eu/blog/ics-scanners-report

[4] https://sissden.eu/blog/amplification-ddos-victims-report

[5] https://sissden.eu/blog/darknet-report

5.2.1 General Report Reception

In a first question, survey participants were asked to rank SISSDEN remediation reports regarding three aspects: usefulness, timeliness, and accuracy. Answers could be given on a scale from “very low” to “excellent”.

In total, 121 participants answered this question. 114 participants (94.2%) considered the SISSDEN remediation reports’ usefulness as “good” or “excellent”, 107 participants (88.4%) described the reports’ timeliness as “good” or “excellent” timeliness, and 108 participants (89.3%) assessed the reports’ accuracy as “good” or “excellent”.

	very low	low	ok	good	excellent
Usefulness	0 (0%)	2 (1.7%)	5 (4.1%)	58 (47.9%)	56 (46.3%)
Timeliness	1 (0.8%)	1 (0.8%)	12 (9.9%)	46 (38.0%)	61 (50.4%)
Accuracy	1 (0.8%)	0 (0%)	12 (9.9%)	55 (45.5%)	53 (43.8%)

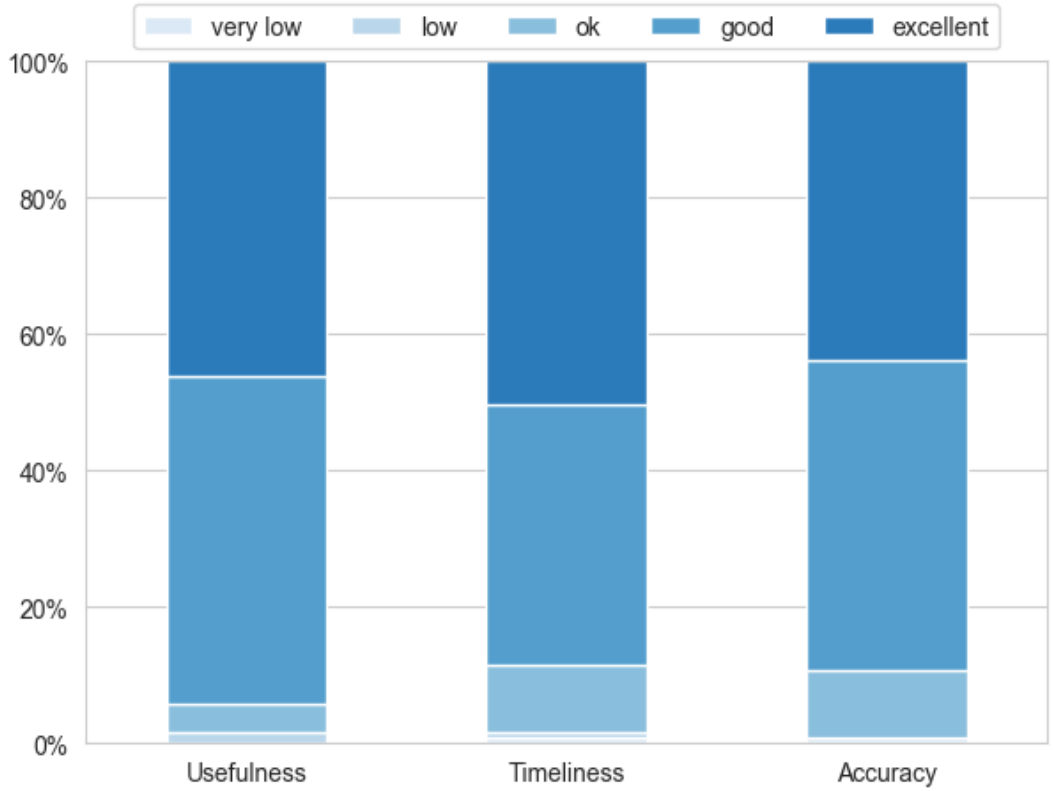

Figure 5.1: Distribution of user evaluations of general report reception

5.2.2 Per Report Reception

A second question asked participants to rate the individual reports on a five-point scale from “not useful” to “invaluable”.

As recipients only receive reports regarding their networks the number of answers differs between reports, ranging from 96 (Darknet report) to 108 (DDoS Victim report). 76 of 103 participants (73.8%) considered the Drone Brute Force report “very useful” or higher, as did 80 of 107 participants (74.8%) for the HTTP scanner report. The ICS scanners report was given a rating of “very useful” or higher by 68 of 99 participants (68.7%), the Amplification DDoS Victim report was given the same grades by 79 of 108 participants (73.1%), and the Darknet report was considered “very useful” or “invaluable” by 67 of 96 participants (69.8%).

	not useful	somewhat useful	fairly useful	very useful	invaluable
Drone Brute Force	0 (0%)	6 (5.8%)	21 (20.4%)	64 (62.1%)	12 (11.6%)
HTTP Scanners	0 (0%)	7 (6.5%)	20 (18.7%)	66 (61.7%)	14 (13.1%)
ICS Scanners	0 (0%)	6 (6.1%)	25 (25.3%)	56 (56.6%)	12 (12.1%)
Amplification DDoS Victim	2 (1.9%)	7 (6.5%)	20 (18.5%)	61 (56.5%)	18 (16.7%)
Darknet	2 (2.1%)	6 (6.3%)	21 (21.9%)	52 (54.2%)	15 (15.7%)

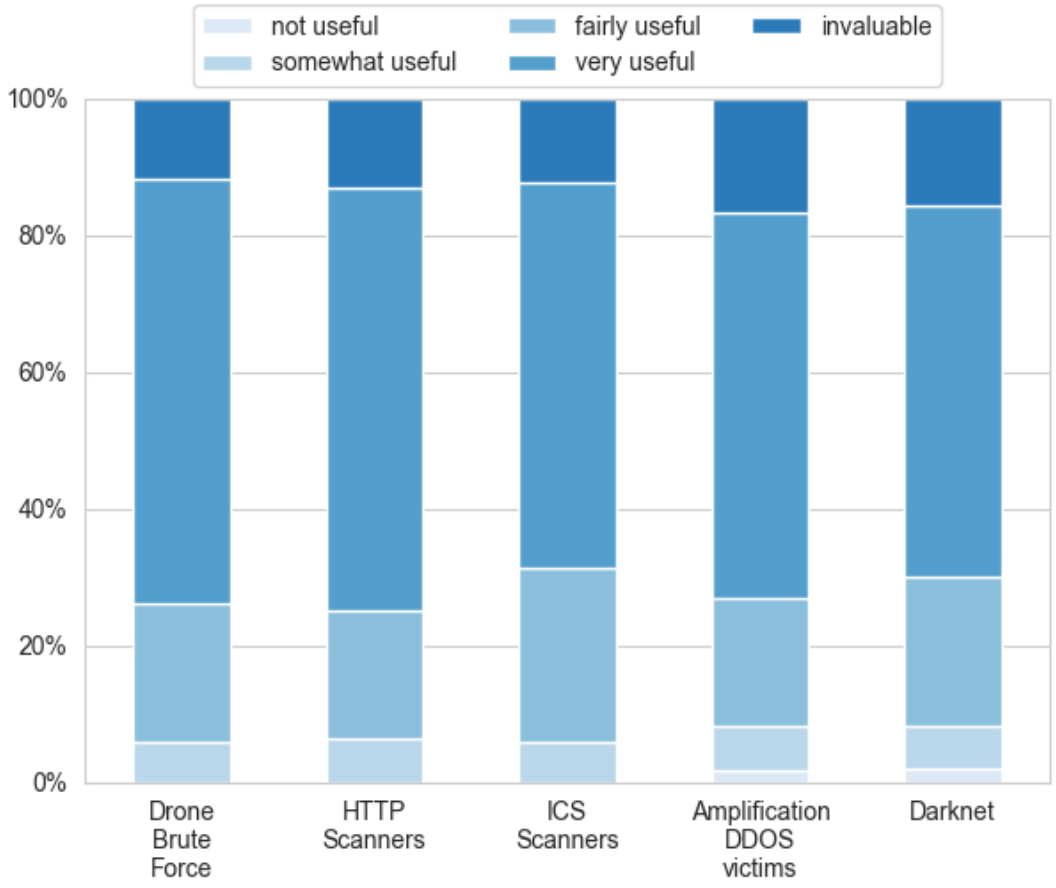

Figure 5.2: Distribution of user evaluations of per report reception

5.2.3 Remediation Impact

To assess the impact of remediation efforts, participants were also questioned to estimate the percentage of incidents reported by SISSDEN they were able to remediate.

This question received 111 replies. While 25 participants (22.5%) stated they were able to remediate only 20% or less of reported incidents, 56 participants (50.4%) reported remediation rates of 60% and above.

	0-10%	10-20%	20-40%	40-60%	60-80%	80-100%
remediation rate	10 (9.0%)	15 (13.5%)	16 (14.4%)	14 (12.6%)	27 (24.3%)	29 (26.1%)

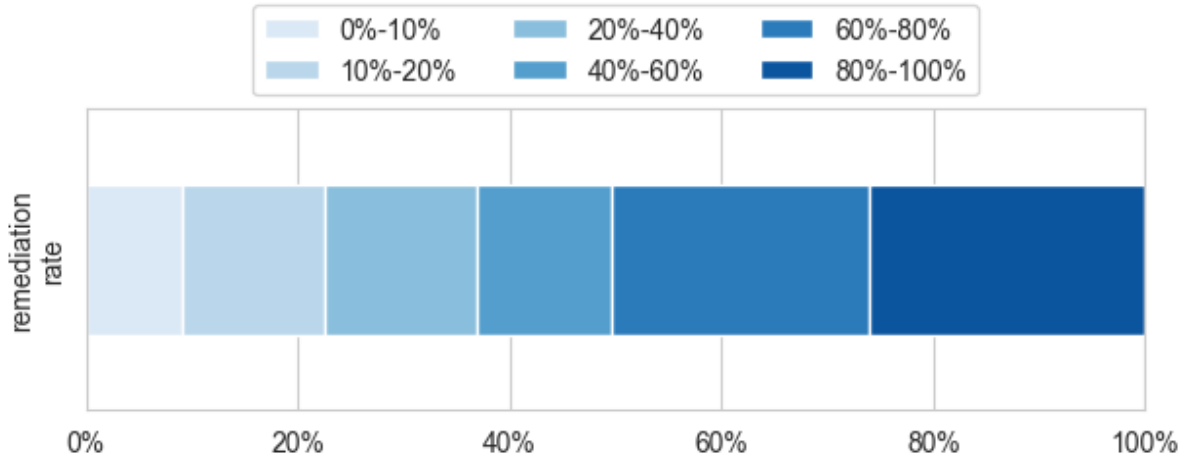

Figure 5.3: Distribution of user evaluations of remediation rate

5.3 Conclusion

In conclusion, the five SISSDEN remediation reports sent out through Shadowserver reach a great number of CERTs and network operators. They are considered useful, timely, and accurate by an overwhelmingly large fraction of recipients. In addition, about half of the survey participants reported remediation rates of 60% and higher on the reported incidents.