Appendix II: CERT Survey Analysis

Proactive Detection of Network Security Incidents report

[December 2011]

Contents

1 Analysis of the results of the CERT survey

This appendix presents the results of the survey done as part of ENISA's (European Network and Information Security Agency) project 'Proactive detection of network security incidents'[1]. The survey was conducted by CERT Polska / NASK in April and May 2011.

1.1 Response ratio

The survey was sent to 105 potential respondents from the established list. The addresses were split for individuals' addresses (51) and generic CERT addresses (54), as there was not a known person to get in touch with in every case. In total we went through three rounds of reminders. Despite this, we did not receive any response from 11 individuals and received refusals from five individuals. In all, we obtained 45 completed surveys.

1.2 Respondent profile

The respondents were mainly from the area of government/public administration, academic organisations and ISPs. The group of organisations investigated is relatively varied. This is illustrated by the wide range in the number of incidents handled per organisation (stated as ranging from 10 to 2 million, although this may be due to differences in defining the term 'incident'), as well as the number of full-time equivalent employees at each surveyed CERT (from 0.5 to 41; average of 9 employees).

[1] Proactive detection of network security incidents, report: http://www.enisa.europa.eu/act/cert/support/proactive-detection/proactive-detection-report

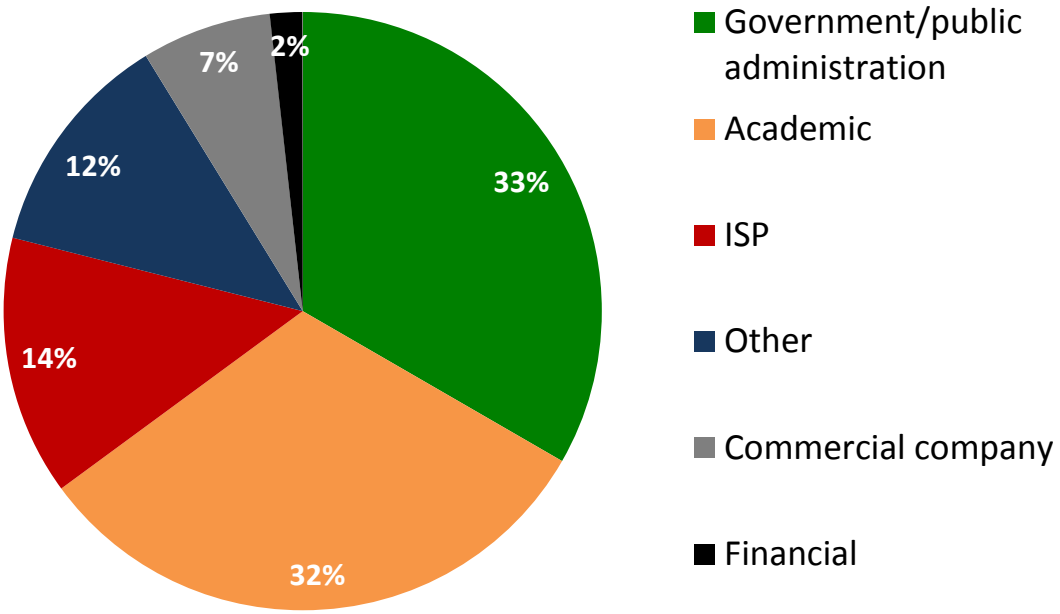

Figure 1: Respondents' organisation profile

Other:

1. *Foundation with governmental tasks*
2. *National CERT team*
3. *Telecom provider*
4. *Not-for-profit organisation*

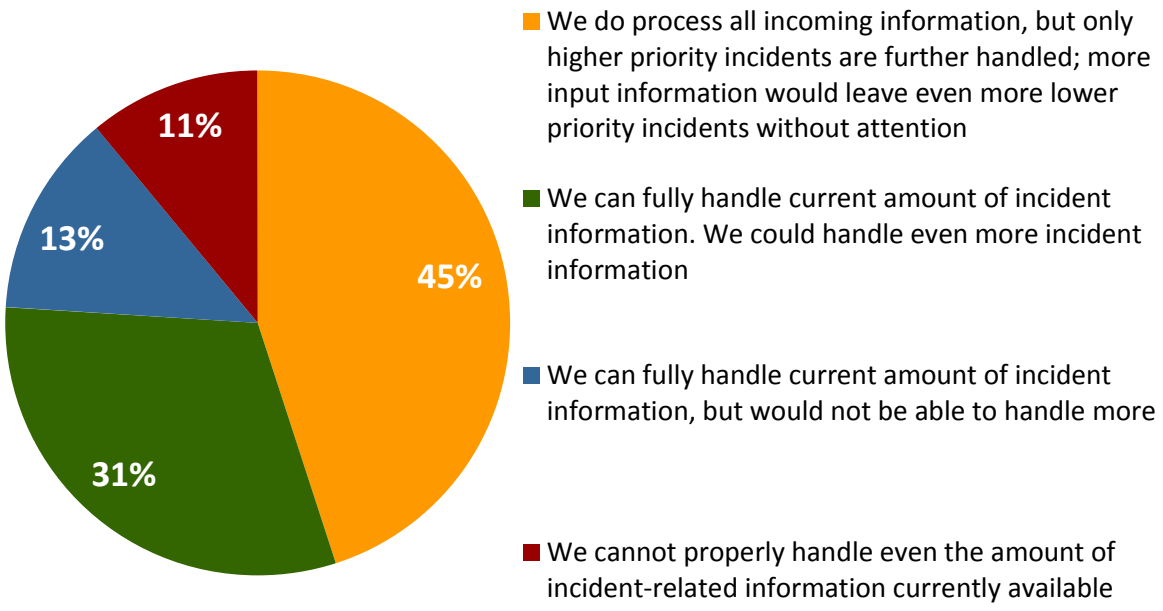

Figure 2: Resources available

Other comments about availability of resources include:

1. *How do we effectively measure whether we have enough resources? It is hard to find metrics to evaluate the effectiveness of the resources we use now. Most measures focus on quantity, not quality or effectiveness.*
2. *We're about to automate the incident handling as much as possible.*
3. *Besides our CSIRT (which consists of 3 people of whom 2 do this part time) we also have an abuse desk which consists of 0.5 FTE and handles most incidents every year.*
4. *We are short on manpower which we need in order to process all the information that we have (honeypots and darknets included).*
5. *Increase of incident information would require remake of some handling procedures to make the process more efficient.*
6. *It all depends how automated incident handling is; e.g. if we can send a list of infected IPs to each ISP and they know what to do with it, then it's easy. But now we are at the stage where we have to educate each ISP and to start collaboration with them. Therefore it takes much more resources than it should.*
7. *Some information sources (e.g C&C and Botnet) do not provide detail (e.g. pcap, log) for us to verify and we have to perform the test again ourselves.*
8. *Some resources (like the NSP-sec-community) are hard to get into. I understand the reasons for this although I do feel it's a waste of their information. That community has a lot of information teams could put to very good use, even though teams like us cannot contribute at the same level. I feel ambivalent about sources like that.*

9. *Our capabilities are restricted due to the volunteer nature of our team. Each member has a day job so our response capabilities are restricted by their availability. Should the number of incidents increase we will look at automating our responses for certain instances, increasing our pool of volunteers and ultimately with appropriate funding having FTE resources to cope with the demand.*
10. *The amount and organisation of IPs and information in the reports make some of them hard (even impossible) to handle without automation. Some of the information is stored in the incident DB to correlate with other reports but it is not processed.*
11. *We are working on the automatisation of notification and tracing or monitoring of open incidents, regarding phishing and malware distribution located in our country resources (domains or IP addresses).*
12. *Our activities can be split into three parts: group-related incidents, our customer-related incidents, and cyber fraud & research non-profit activities (phishing, malware, fast-flux, botnet, etc.).*
13. *As a side note, we don't process all incidents or events reported from those sources. We don't want to overload our constituency so we focus on the critical events.*
14. *Our incident levels are Low/Medium/High/Very High/Critical. We only manage incidents for High/Very High/Critical.*
15. *Current (reactive) working matches our resources.*
16. *Ongoing malware activity is monitored and handled mostly automatically, while higher priority incidents are handled manually, requiring strong human effort.*
17. *For proper handling of incident-related information it is important to have experienced IHO.*
18. *Always difficult to get additional resources (even if needed).*

1.3 Survey outcome

1.3.1 Sources of incident information

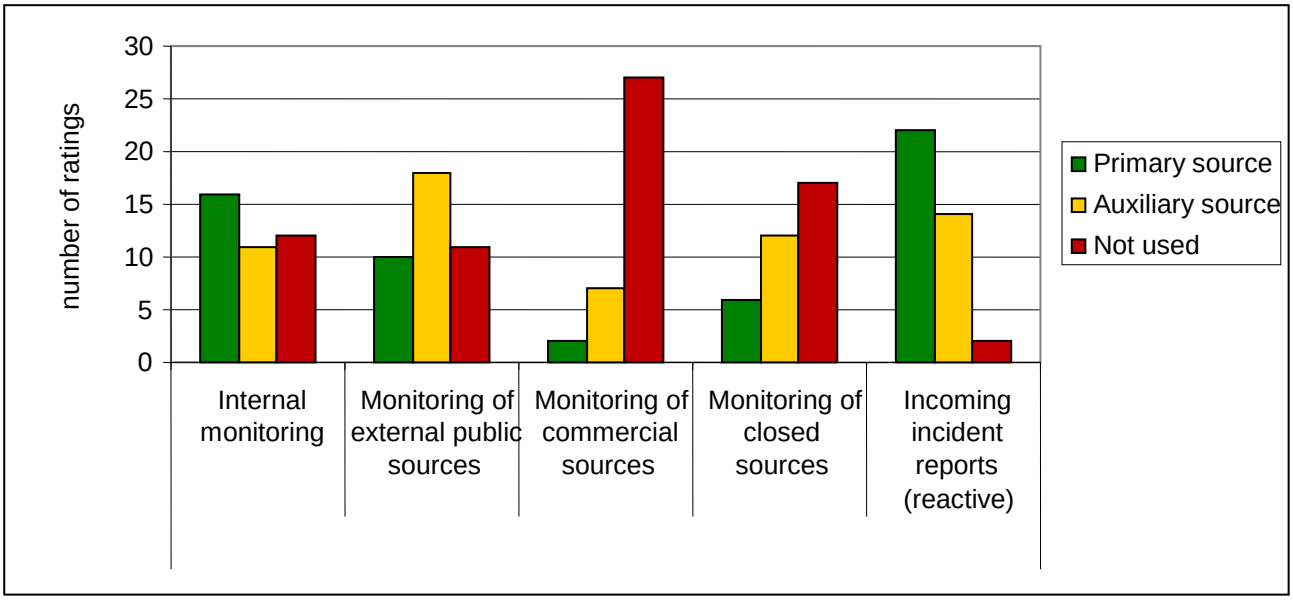

Figure 3: How do you obtain incident-related data about your constituency? [SPAM]

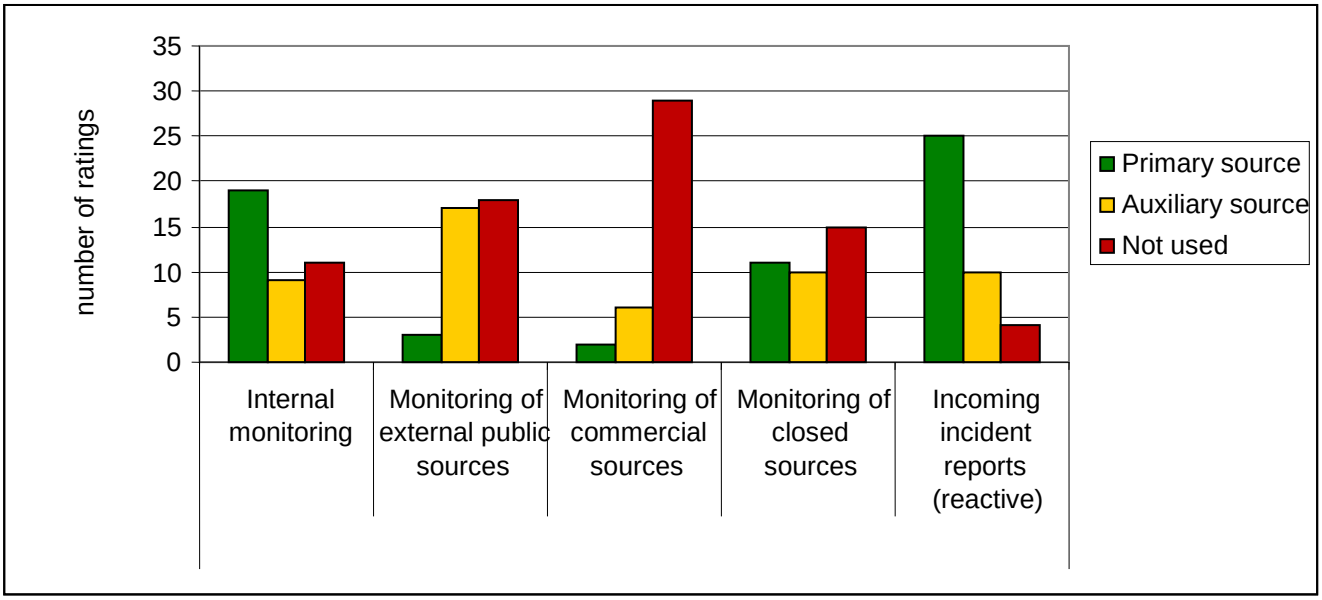

Figure 4: How do you obtain incident-related data about your constituency? [Scanning]

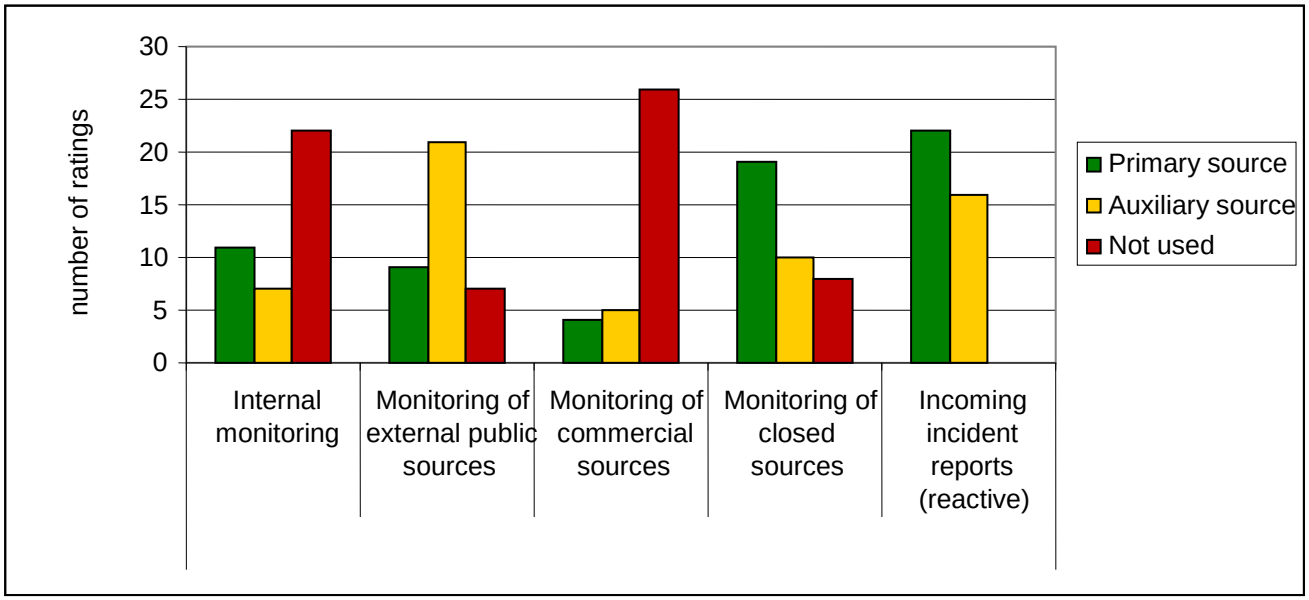

Figure 5: How do you obtain incident-related data about your constituency? [Botnet]

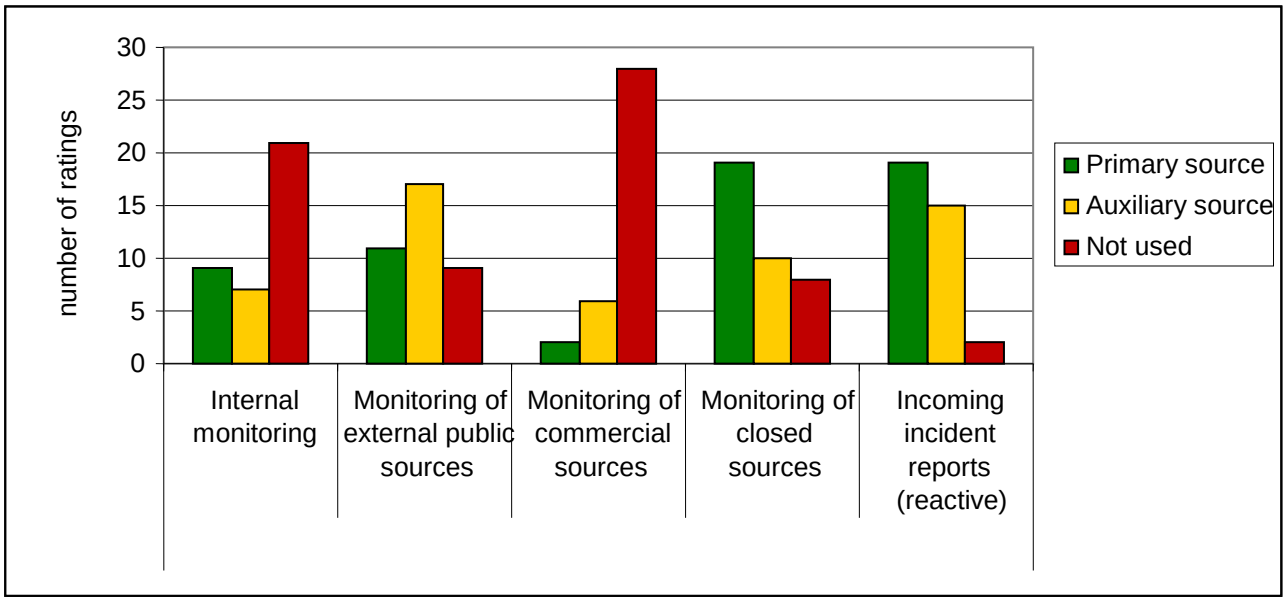

Figure 6: How do you obtain incident-related data about your constituency? [C&C]

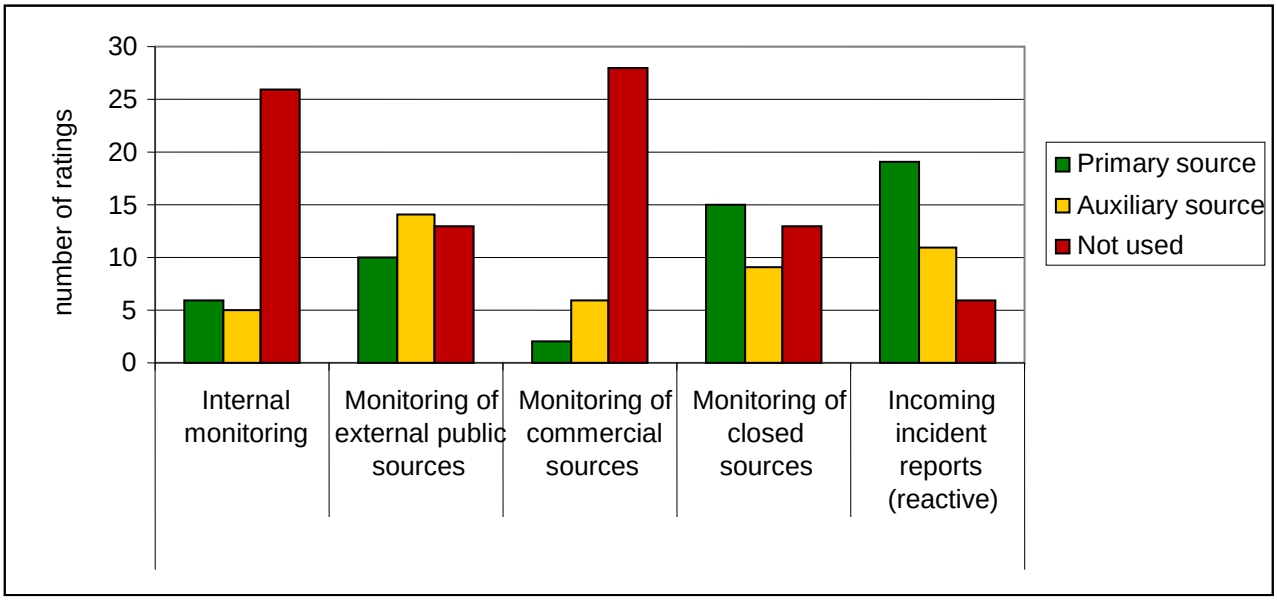

Figure 7: How do you obtain incident-related data about your constituency? [Fast-flux]

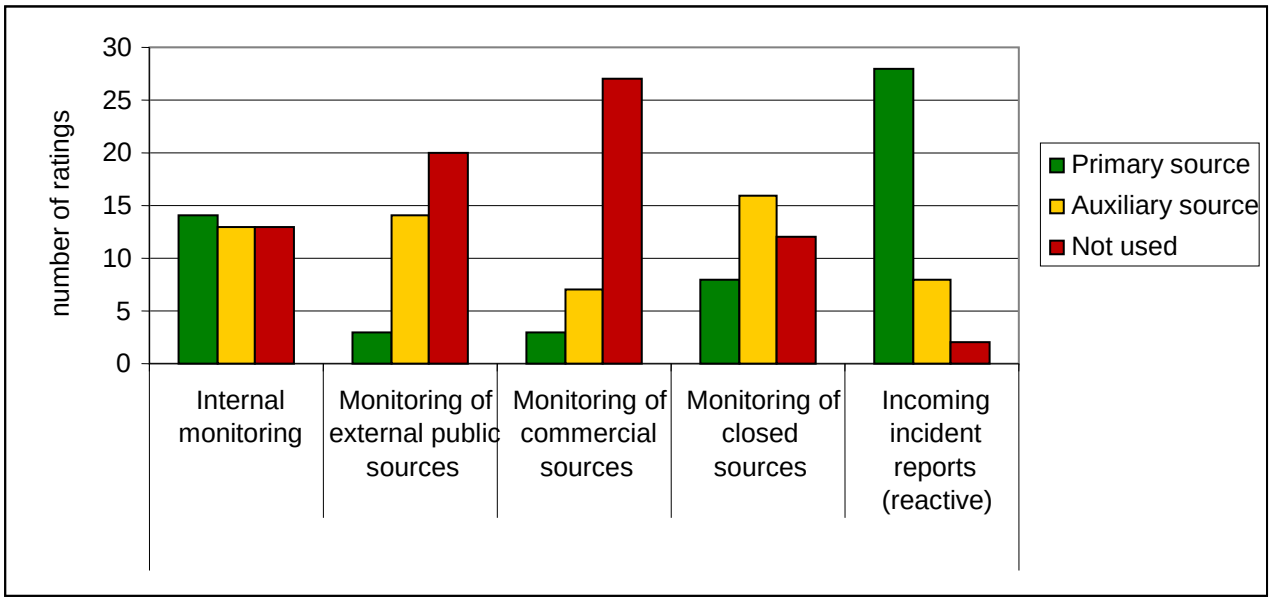

Figure 8: How do you obtain incident-related data about your constituency? [DDoS]

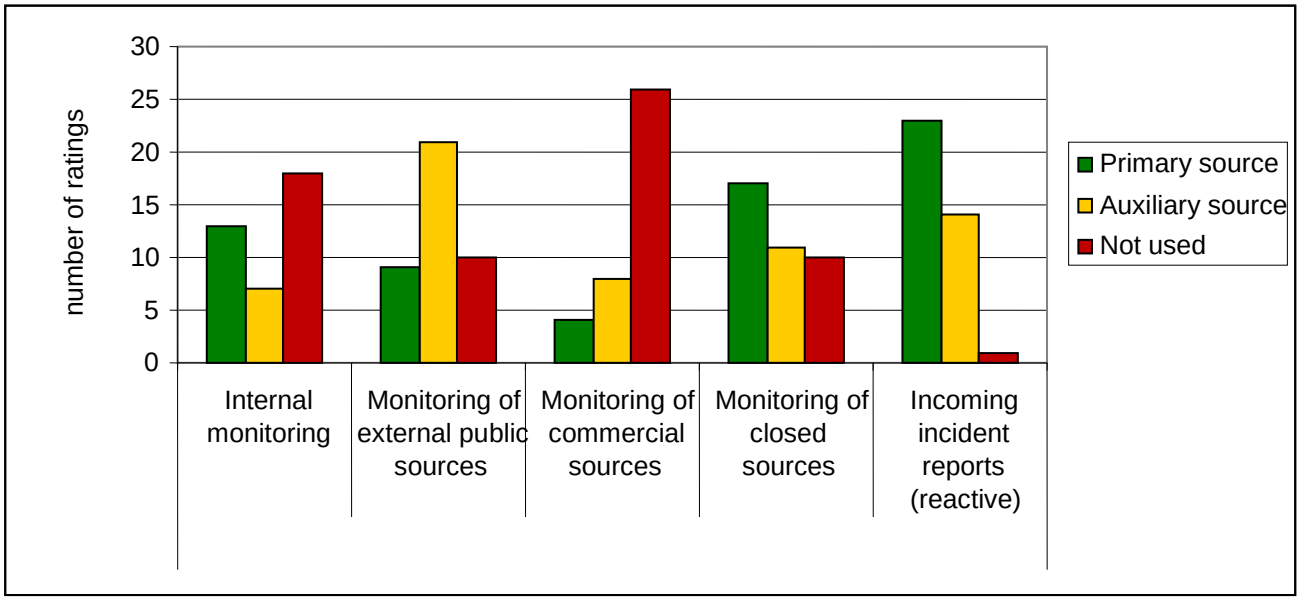

Figure 9: How do you obtain incident-related data about your constituency? [Malicious URLs]

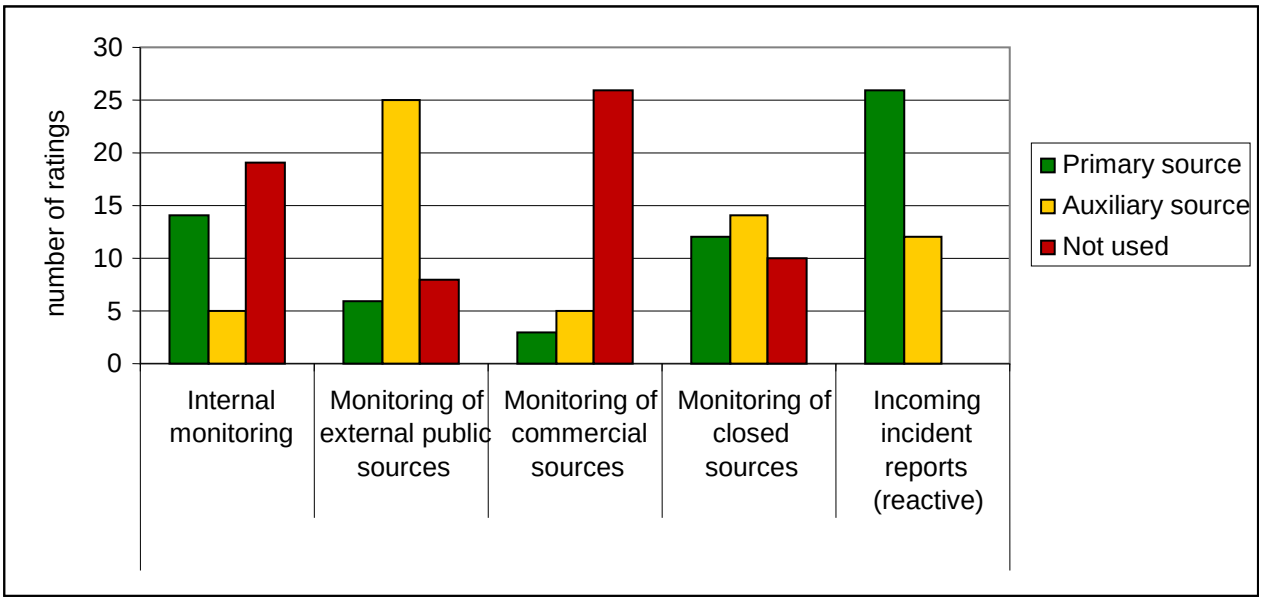

Figure 10: How do you obtain incident-related data about your constituency? [Phishing]

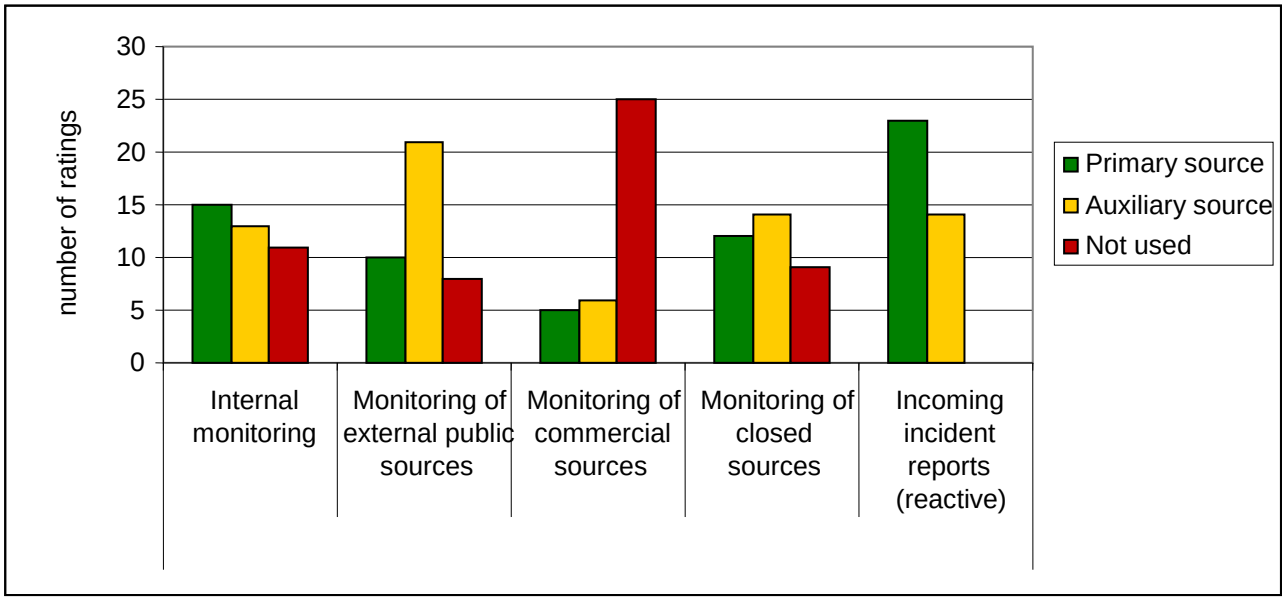

Figure 11: How do you obtain incident-related data about your constituency? [Malware]

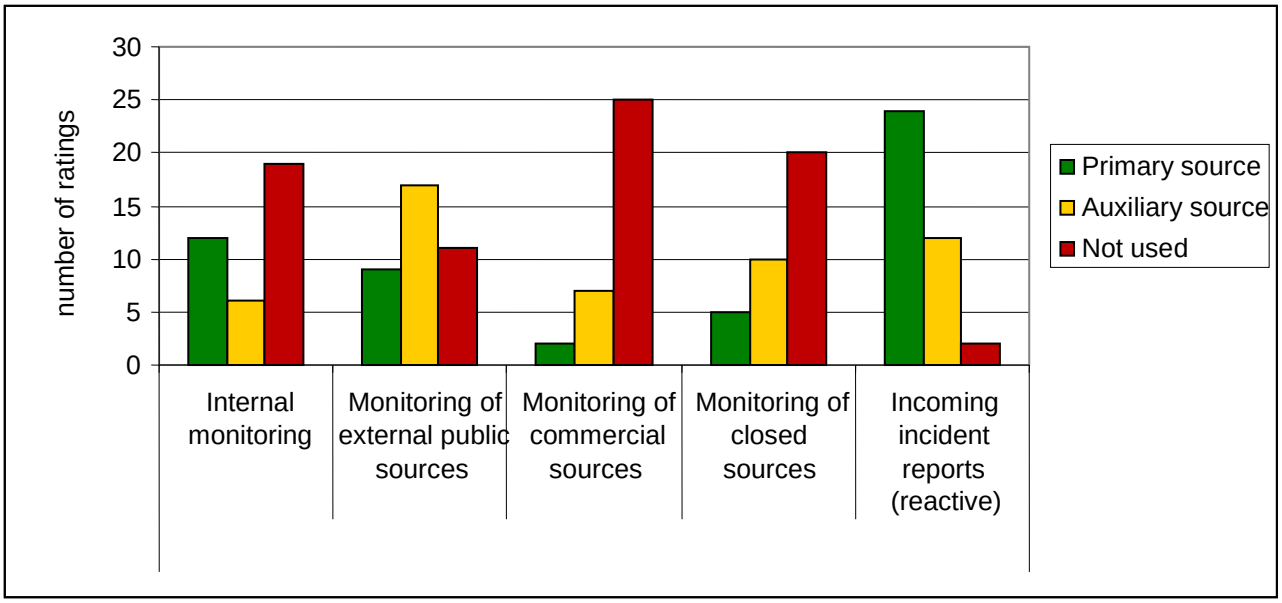

Figure 12: How do you obtain incident-related data about your constituency? [Defacements]

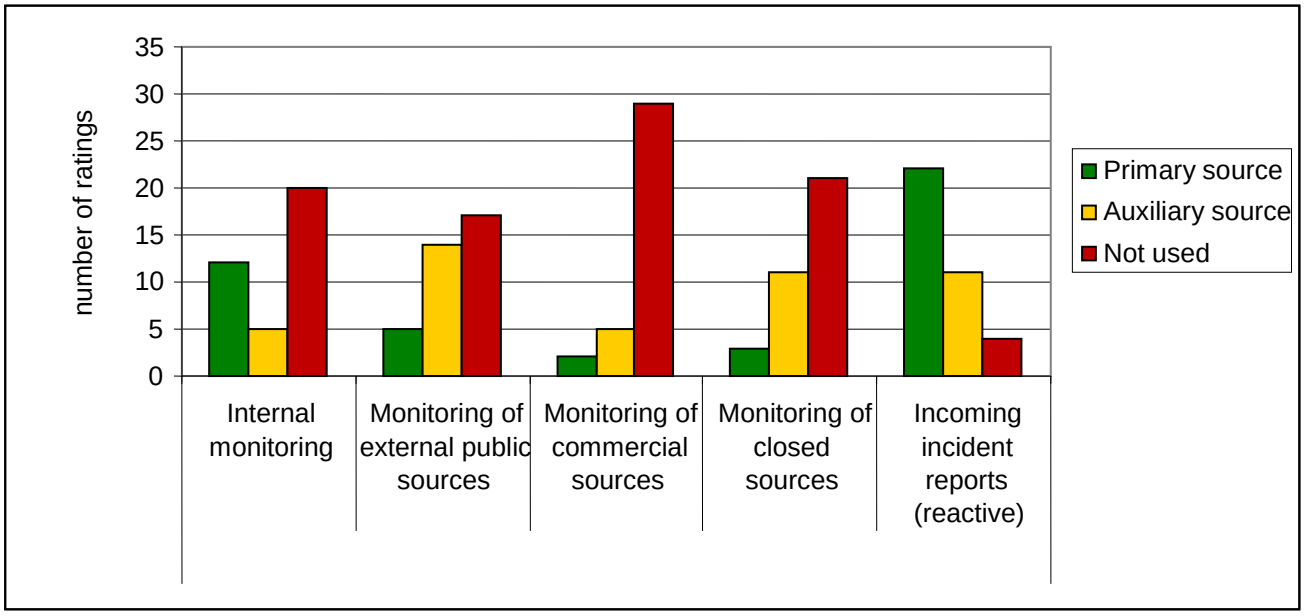

Figure 13: How do you obtain incident-related data about your constituency? [Mass (SQL) injection]

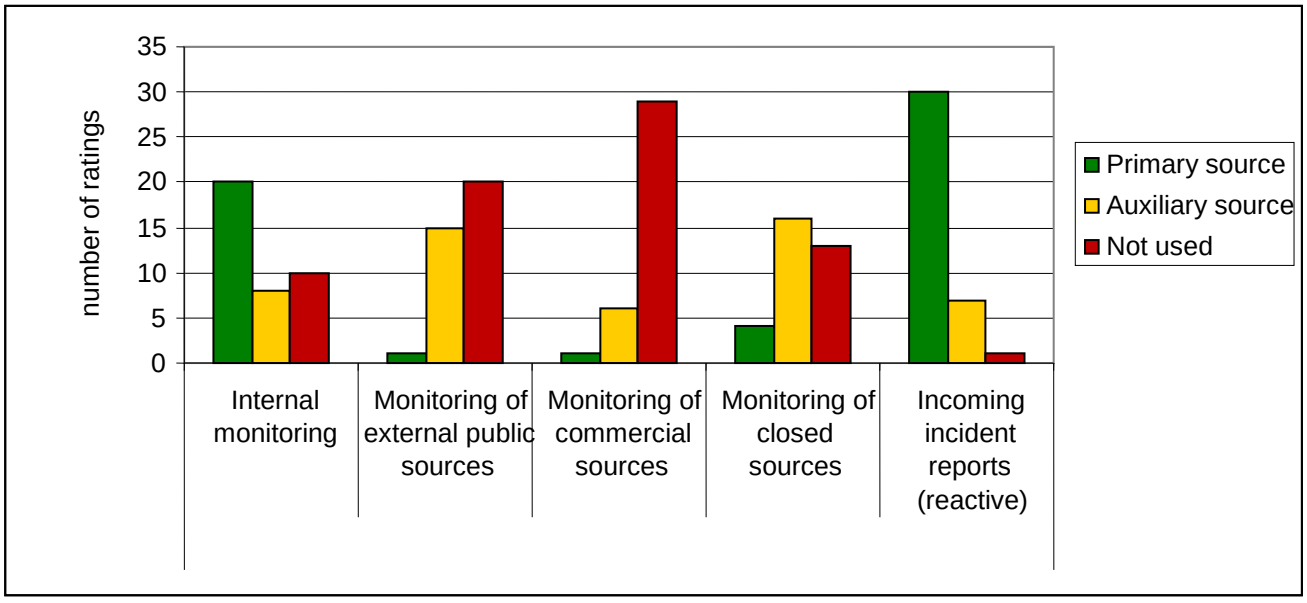

Figure 14: How do you obtain incident-related data about your constituency? [Intrusions]

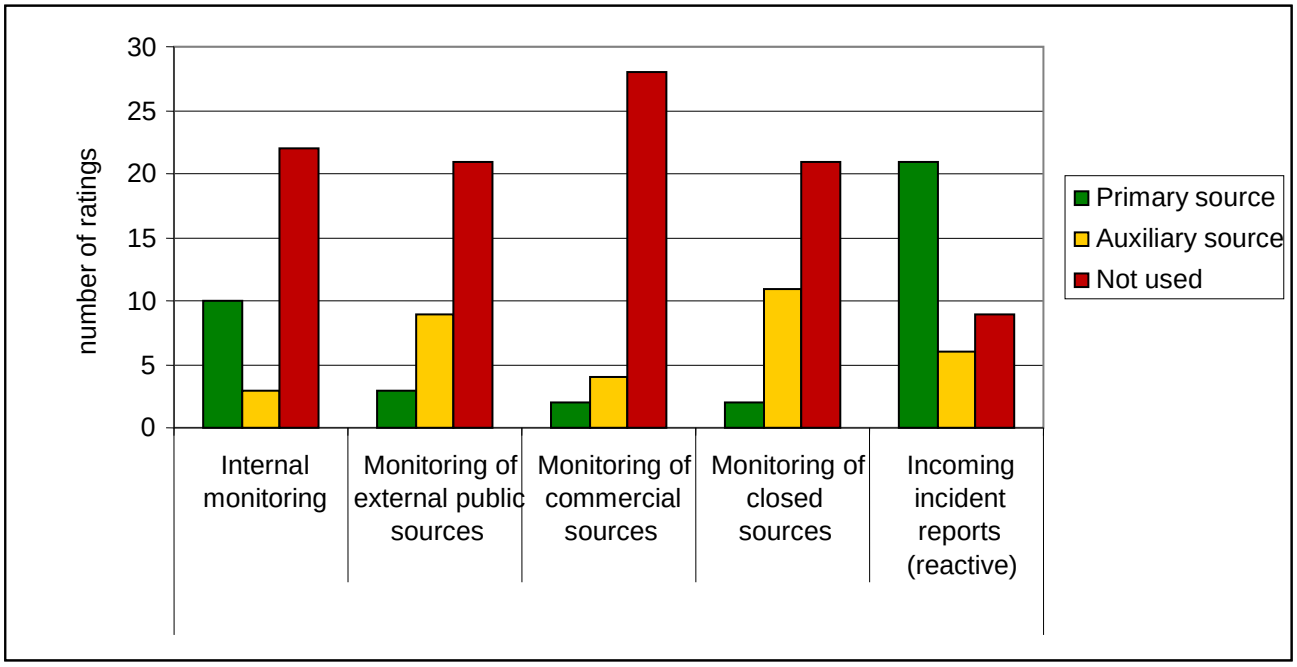

Figure 15: How do you obtain incident-related data about your constituency? [APT]

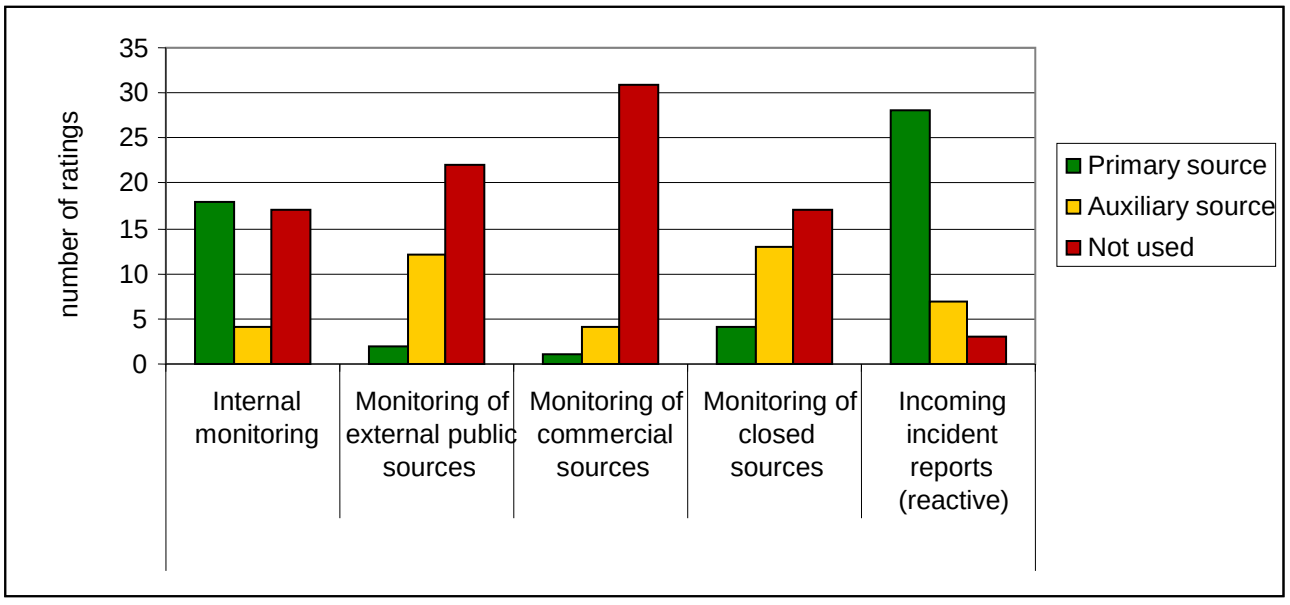

Figure 16: How do you obtain incident-related data about your constituency? [Brute-force]

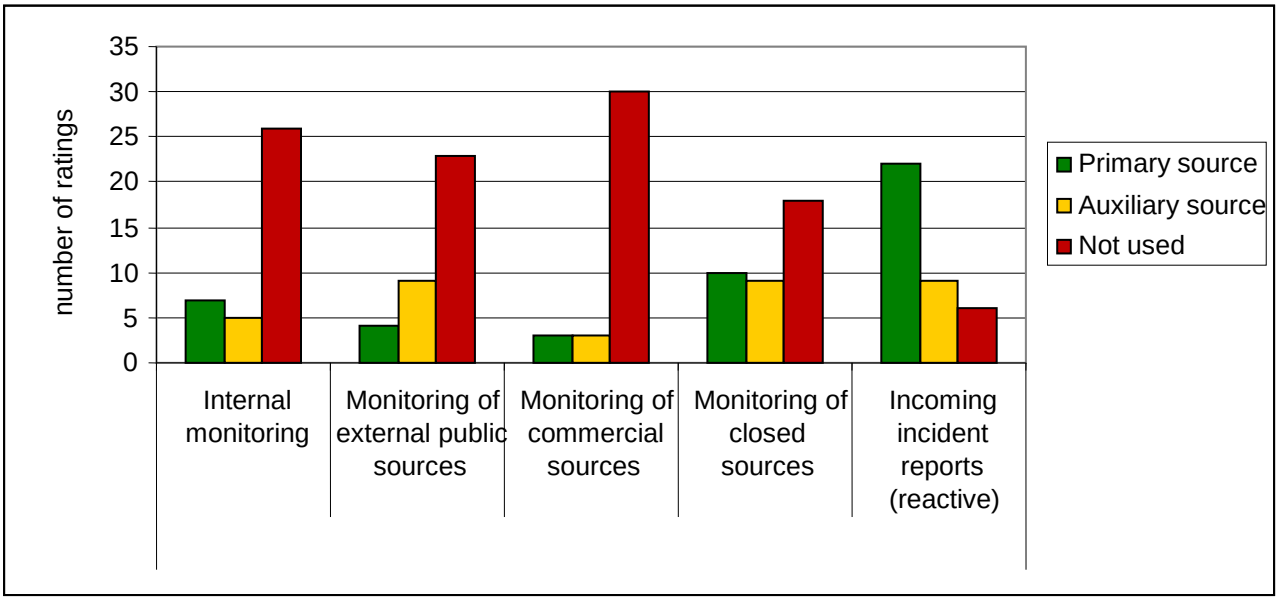

Figure 17: How do you obtain incident-related data about your constituency? [Open resolvers]

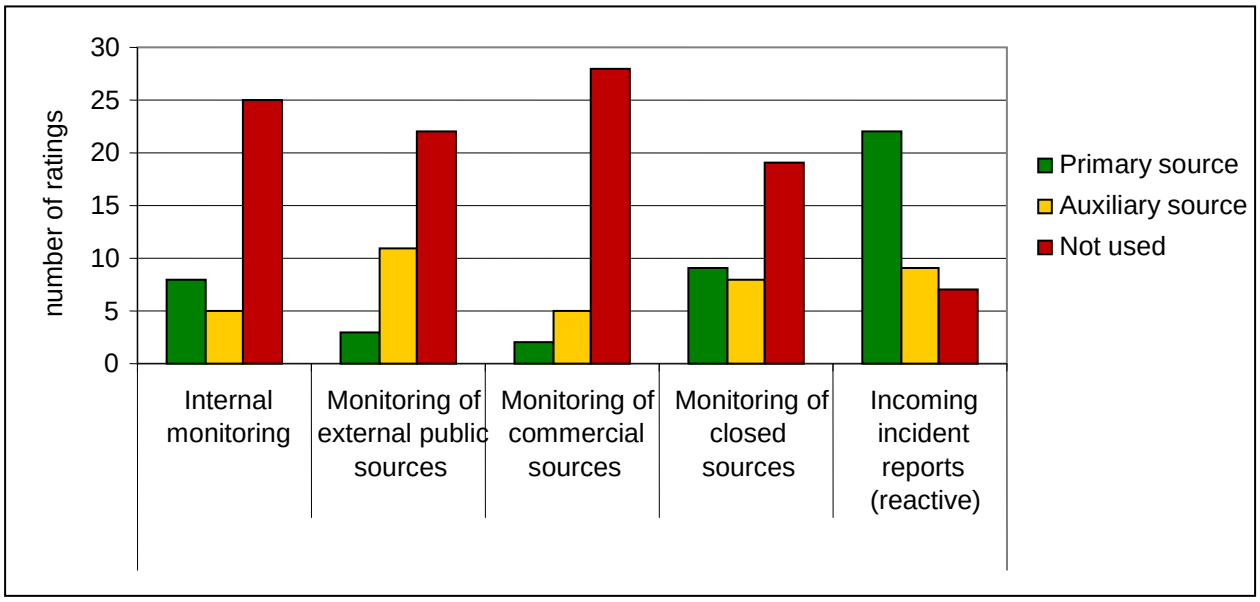

Figure 18: How do you obtain incident-related data about your constituency? [Open proxy]

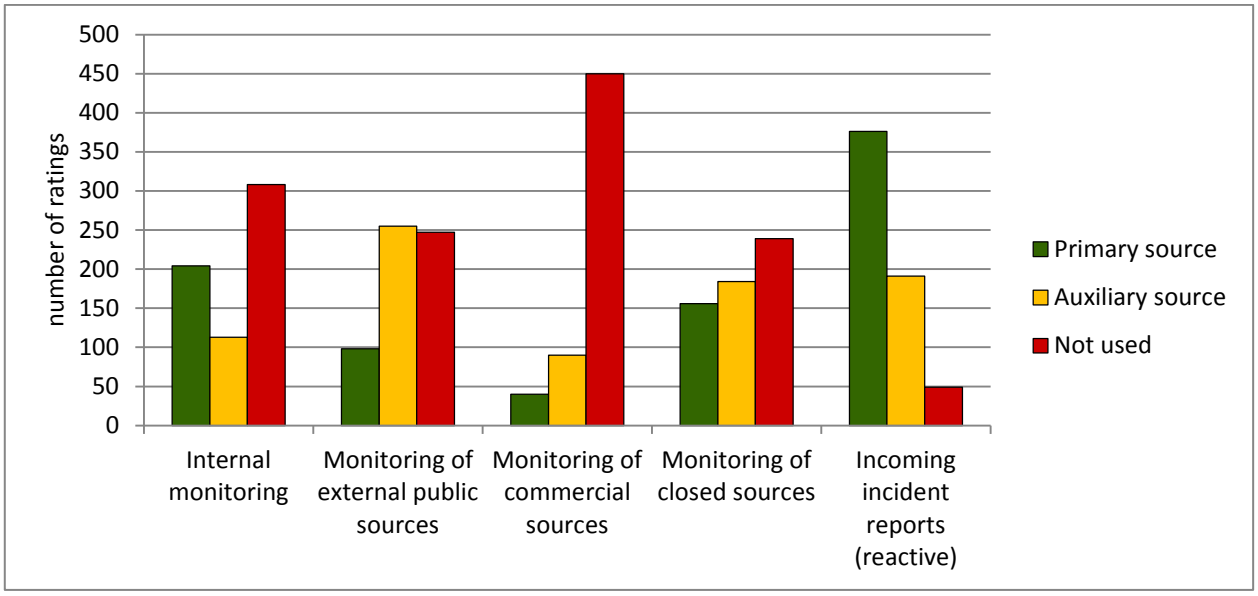

Figure 19: How do you obtain incident-related data about your constituency? [All incident types added together]

1.3.2 Satisfaction with current sources

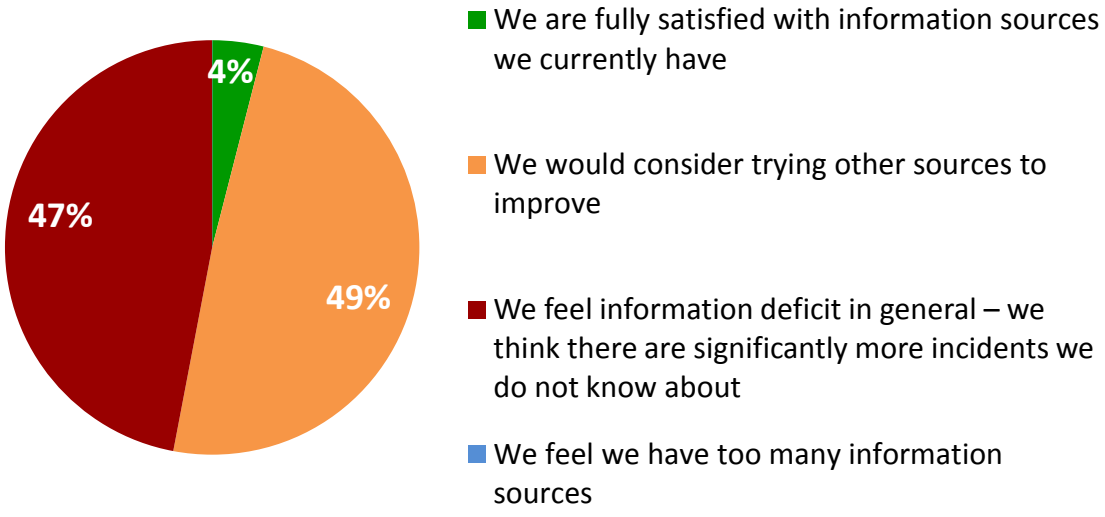

Figure 20: General feelings regarding information sources currently used

Additional feelings and comments regarding information sources that the respondents use:

1. *The cost of sharing information is high. By cost, I do not mean just the cost in dollars/euros. Building effective relationships to share quality information in a scalable way is difficult. There is always room for improvement, and we feel there is still a long way to go.*
2. *Semantics and reliability are often unclear (e.g. was there a three-way handshake or might the address have been spoofed?) There are many variants of each malware, each with many different names. That makes it difficult if not impossible to get accurate information (e.g. what DNS queries does it issue, which addresses does it connect to?).*
   Postmaster.live.com's snds provides useful data, but there's no way to ask questions. As an example, the FAQ states that the snds is on the PST (Pacific standard time) time zone, but our own observations seem to show that the timestamps are in UTC (coordinated universal time). Makes almost no difference where dynamic addresses are involved.
   many of these categories are just no problem (any more) in our net (open resolvers) or at least do not deserve any special handling (open proxies – they just pop up as spam sources, fast flux, C&C).
   Classification is a problem by itself:
   ** do you look at the symptom or at the cause (which is mostly unknown or at least uncertain)*
   ** do you look at it from the perspective of us as attacker or as the one being attacked, or both (in particular with intrusion/bruteforce that is an issue)*
   ** what's the classification's purpose? Statistics & detection of trends or decision about how to handle the incident?*
   ad 8) Phishing) Do you mean phishing sites we host or phishing attacks against our constituency? In their essence, phishing sites are == defacement == malware hosted on a

(web) server.

ad 9) Why is 'too many information sources' last in the list?

3. *We should get more budget to monitor our ISP networks more closely; we don't even have netflow enabled.*
4. *We are in the process of adding new sources of information to our IM system and it takes time and effort to adopt them, to write needed scripts, etc. Systems/processes are far from being automated.*
5. *We have a couple of information sources in various formats (log, website content, RSS feeds and csv file) and do not have a tool to consolidate it automatically. Since each data source has its own naming convention and data format, it is difficult to normalise it and store into the database.*
6. *We feel there is more information than we can handle. We would like to automate processing even more. A wide use of ARF would facilitate this.*
7. *Sources that we use are a combination of closed sources, publicly available information and issues reported to us by those within our constituency and outside it. As a small CERT we cannot afford any commercial services and therefore would like information on other useful services, be they public or closed, that we could use.*
8. *We need to improve internal monitoring / sources.*
9. *If possible standard reports format should be used by the sources (IODEF, X-ARF), which allows the teams to automate the handling of the information provided. Repository of sources (both public and commercial) would be useful for beginners.*
10. *We need to gather more and more information from external resources, because we don't manage our own network or AS.*
11. *More information could be shared among CERTs.*
12. *In general we do not disclose information about the sources of our incident reports. We use a mix of monitoring, external open and commercial sources. Most handled incidents are reported to us (reactive) though we have an incline towards more proactive handling of incidents due to better tooling.*
13. *We handle incidents from internal sensors, requests from within our constituency and international contacts.*
14. *All sources have to be rated by reliability.*
15. *Harmonised formats would improve automation.*

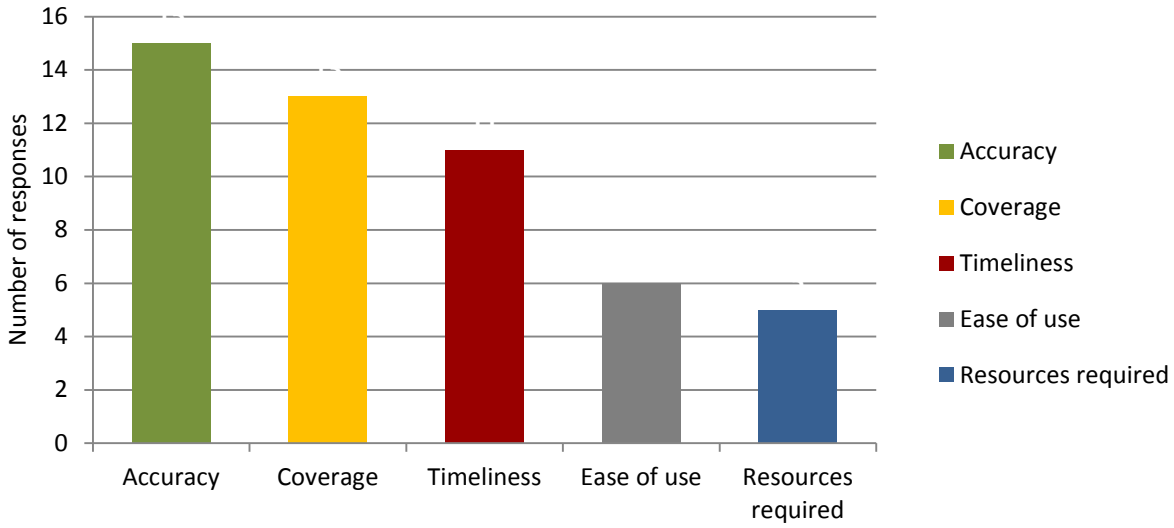

Figure 21: What would you like to improve when trying new sources to obtain information about security incidents in your constituency?

1.3.3 External sources

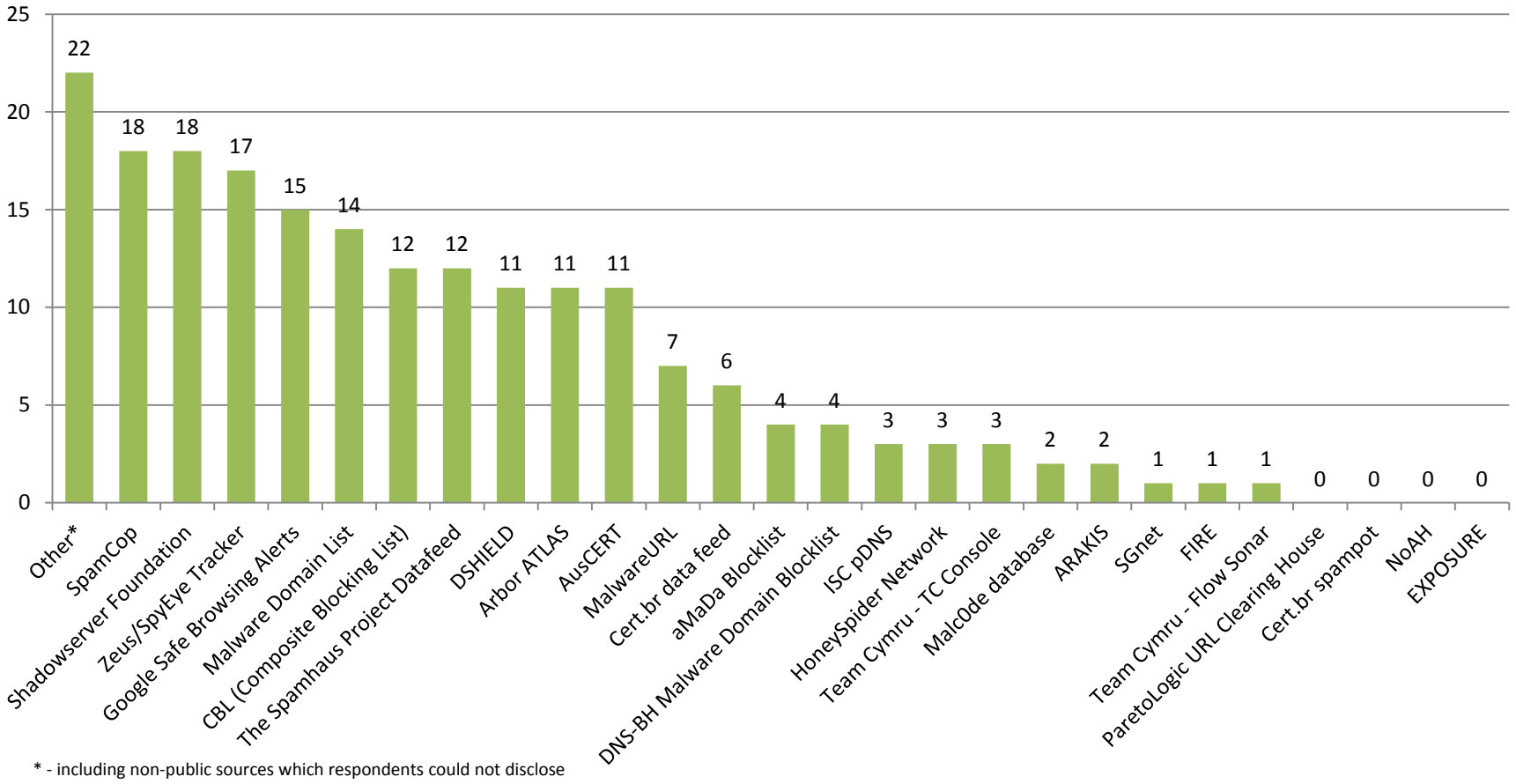

Figure 22: External sources providing information on malicious or problematic URLs, IP numbers or domains that respondents monitor for entries from their constituency

Numbers on vertical axis represents the number of respondents monitoring the specific source.

Below are some responders' answers for questions about other sources, not included in the list. Some responders declared that they cannot disclose their sources.

1. *http://postmaster.live.com/snds*
2. *Network sensors and exchange information with CSIRTs*
3. *http://www.projecthoneypot.org*
4. *Norman sandbox reporter (timeliness: fair, accuracy of results: fair, ease of use: fair, coverage: fair, resources required: good)*
5. *Ikaka (timeliness: fair, accuracy of results: good, ease of use: fair, coverage: fair, resources required: good) http://site.ikaka.com*
6. *We use about 30 spam-oriented ARF-based feedback loops we set up with other providers and/or mass-mailers.*
   In general: timeliness: fair, accuracy: fair, ease of use: excellent (we automated processing and generation of feedback, that's why we like ARF) coverage: fair, resources required: good
7. *www.zone-h.org (timeliness: fair, accuracy: good, ease of use: good, coverage: fair, resources: good)*
8. *Emerging threats-botnet (http://rules.emergingthreats.net/blockrules/emerging-botcc.rules). The main problem with this source is they don't provide information about port/channel being used by the C&C. The amount of checks and false positives sometimes is high.*
9. *Different reports from industry but it is private.*
10. *Netcraft Toolbar (timeliness: good, accuracy: excellent, ease of use: excellent, coverage: excellent, resources: excellent)*
    Phishtank (timeliness: good, accuracy: fair, ease of use: good, coverage: good, resources: fair)
    Phishintel UAB (timeliness: excellent, accuracy: good, ease of use: poor, coverage: good, resources: fair).
11. *A side note: Dshield has different kind of data sources (trending, top100, daily and a block list) and their quality can vary a lot.*
12. *Fortinet Antispam Panda URL Filtering.*
13. *Other CERT team.*

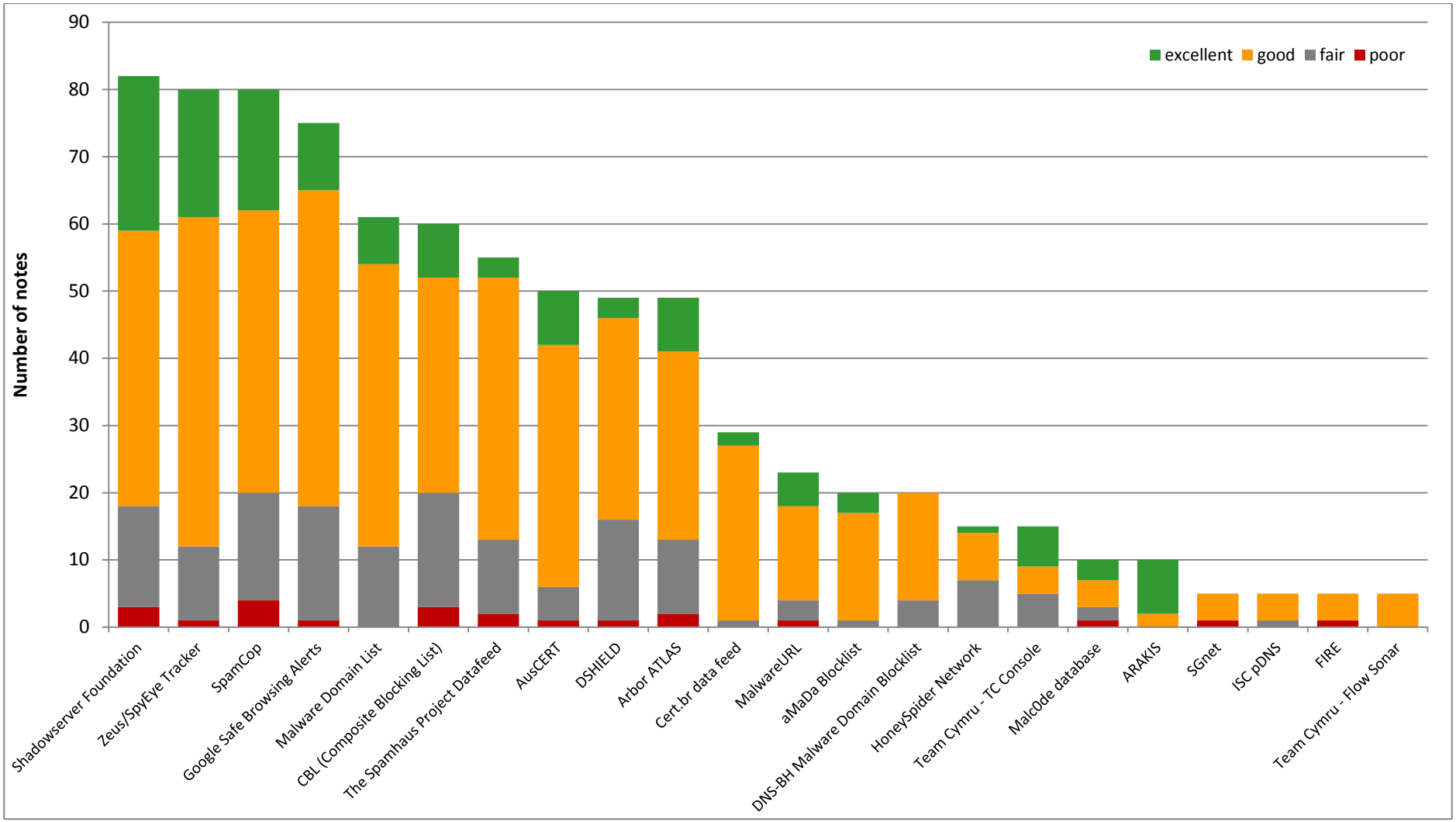

Figure 23: Evaluation of sources providing information on malicious or problematic URLs, IPs or domains

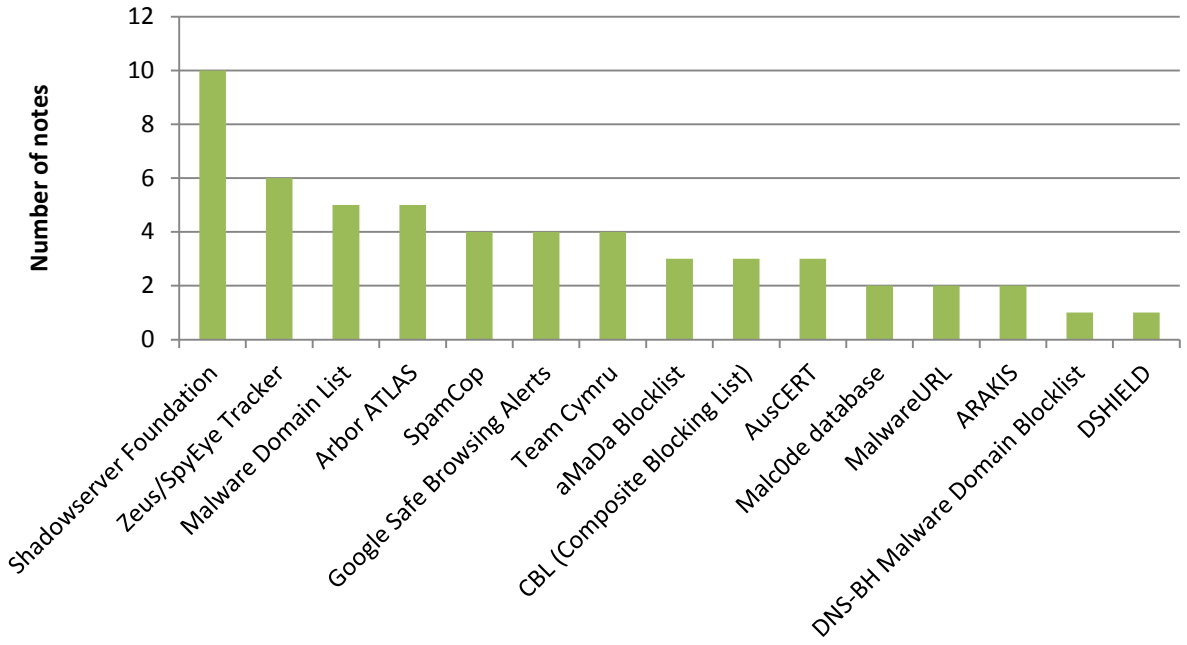

Figure 24: Top 3 best sources for gathering information

Other sources that were mentioned by respondents as being in their top 3:

- BFK
- cleanmx
- EGC
- Netflows (nfsen, homegrown tools)
- live.com/snds
- sgnet
- Our own ARF-based feedbackloop system
- Complaints received by the CERT-team and the Abuse-desk
- isc.sans.org
- Other CSIRTs Feeds Honeypot/Honeynet data
- Fastflux monitoring
- Netcraft
- Phishintel UAB
- RSA
- Blocklist and BGP Ranking (a mix of different sources).
- IBM.ISS Secunia Deepsight Symantec
- Twitter

1.3.4 Closed sources

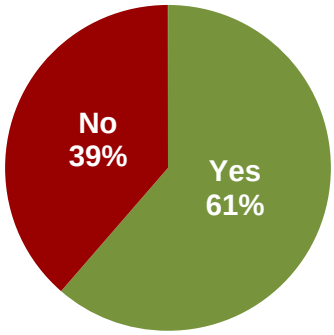

Figure 25: Do you use any closed sources of information you cannot disclose?

What kind of information do the closed sources of information provide? Can you describe the source in a few words?

1. *Timely indicators of previously unknown incident activity.*
2. *Information including malware infections, malware URLs, bruteforce, DDoS, defacements, fastflux, openresolvers, phishing, openproxies, scanning, spam.*
3. *A closed mailing list of law enforcement, CERTs, ISPs and others in the field.*
4. *Specific information for our constituency.*
5. *Information related to security threats, vulnerabilities and incidents, e.g. web defacements, network monitoring data.*
6. *Malicious URLs.*
7. *Same kind of incident reports as Shadowserver.*
8. *Malicious URLs, related to client-side attacks. Websites compromised and with iframes or malicious javascripts. Exploit kit websites. Malicious code distribution sites. Information about infected machines related to a botnet C&C taken down.*
9. *Reliable and proven information among trusted participants.*
10. *Intrusions, basically.*
11. *We use some internal passive DNS dataset and source from private dionaea installation.*
12. *Vulnerabilities, malware, report.*
13. *We do not disclose our external sources.*
14. *Respondent treats all of his sources as confidential and has NDAs in place specifically to protect the confidentiality of sources.*
15. *Sources are for internal use only.*
16. *Local and international contacts.*
17. *Incident notification about phishing, malware and DDoS targeting the financial industry.*
18. *Suspicious hosts from our constituency.*
19. *C&C and fastflux.*

How does the quality of such sources compare with the public ones?

Respondents unanimously stressed superior accuracy, timeliness, reliability and quality of information gathered from closed sources in comparison to the public ones. They claim that closed sources relay the information before those available publicly. Nevertheless it was mentioned that information received from closed sources is sometimes less frequent.

1.3.5 Internal tools

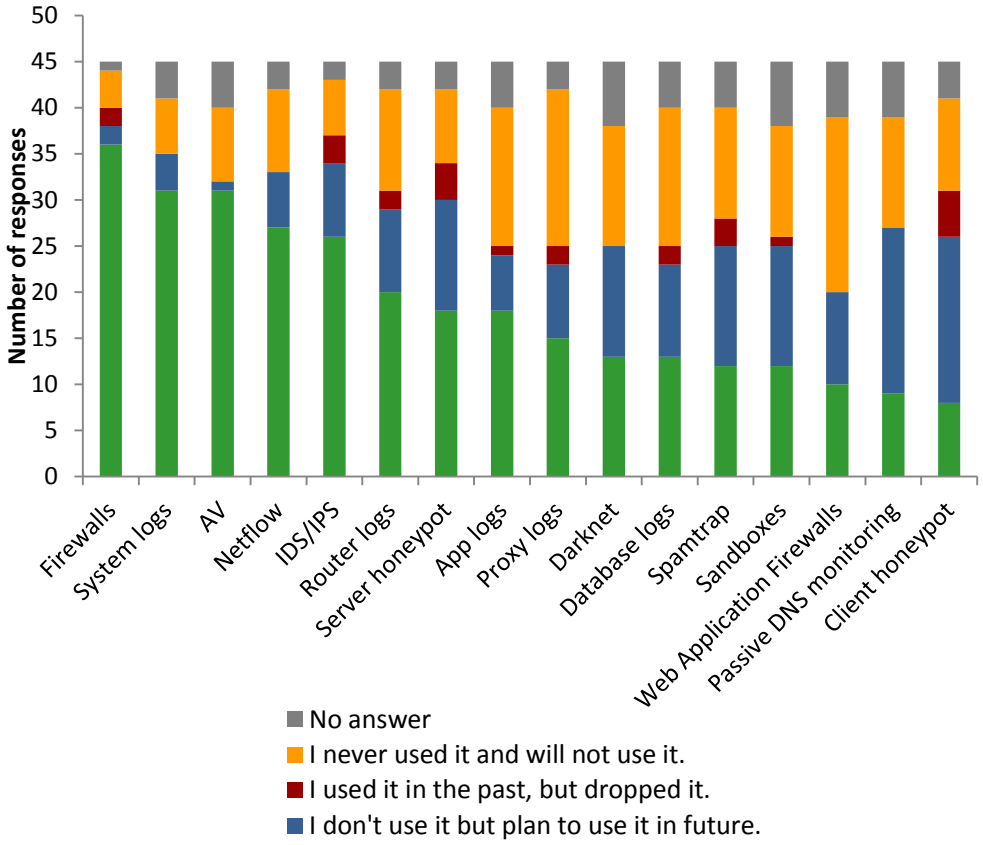

Figure 26: Categories of tools for gathering information from the network

Below are other types of tools for gathering information from the network not included in the list that respondents mentioned:

1. *Recursive DNS logs*
2. *SNMP logs (timeliness: excellent, accuracy: good, coverage: good, required resources: fair, scalability: good, extensibility: good)*
3. *Tracker – Tracking the fastflux domains http://honeynet.org.au/?q=node/10 (timeliness: good, accuracy of results: good, coverage: fair, required resources: good, scalability: fair, extensibility: fair)*

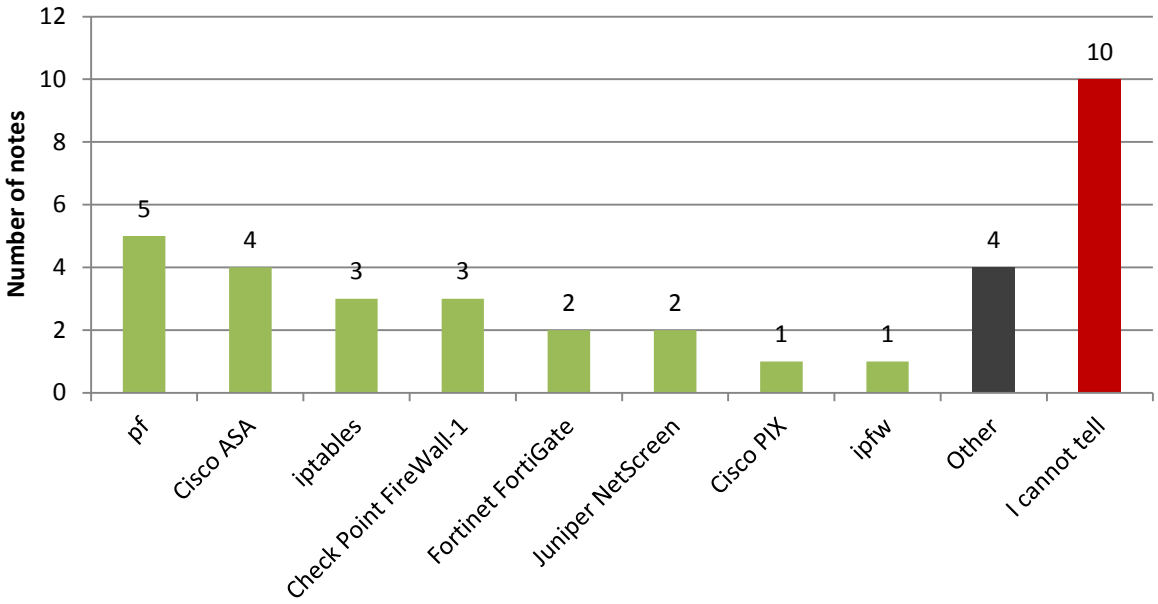

Figure 27: Which firewall do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

Others:

1. *Zorp*
2. *Cisco IOS ACL*
3. *Diferent technologies depend on Public Administrations*
4. *GeNUA GeNUScreen*

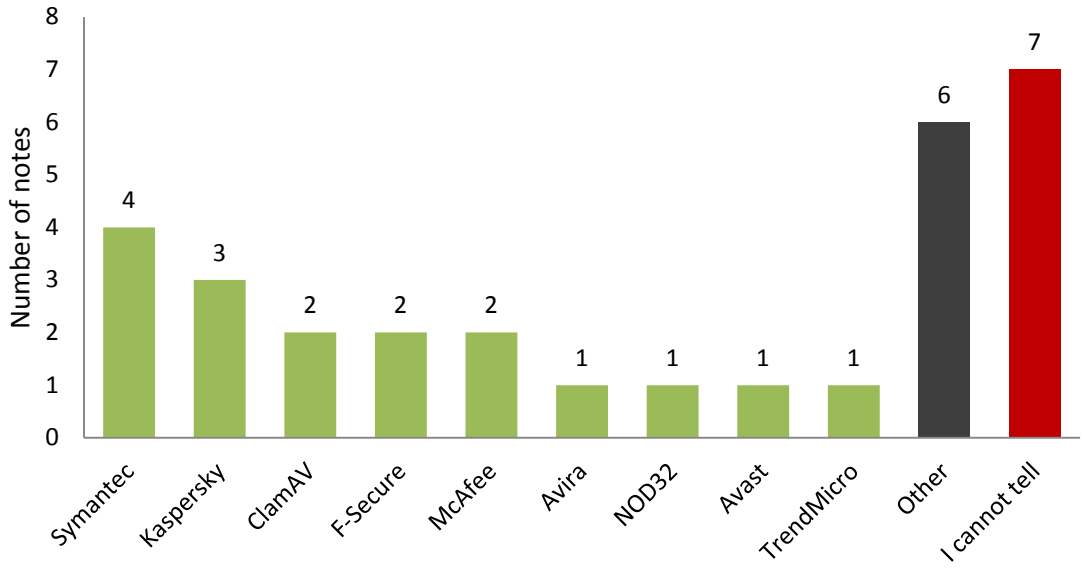

Figure 28: Which antivirus solution do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

Others:

1. *Sophos*
2. *Panda Security*
3. *We use several solutions*
4. *Different technologies depend on Public Administrations*

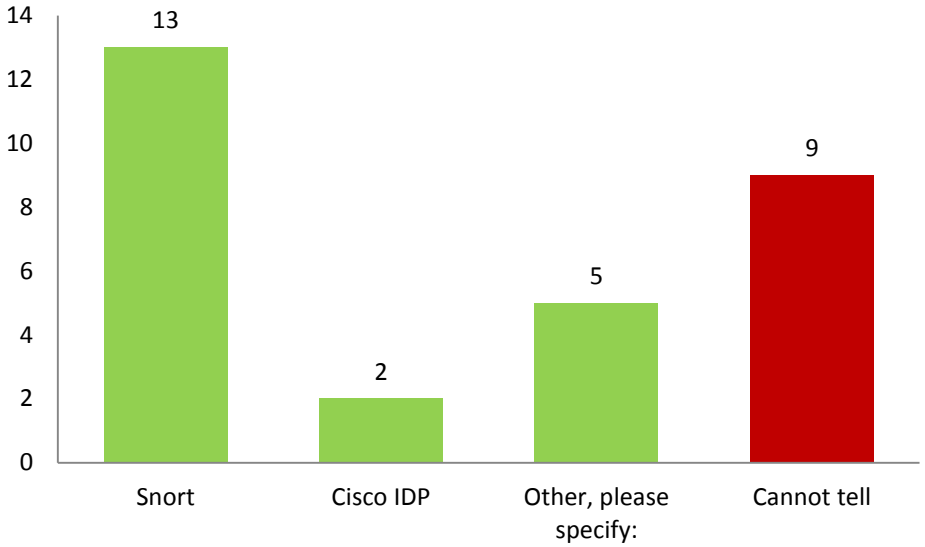

Figure 29: Which IDS/IPS do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

Others:

1. *Peakflow SP, Peakflow X*
2. *Bro*
3. *HP Tippingpoint*
4. *Dragon*

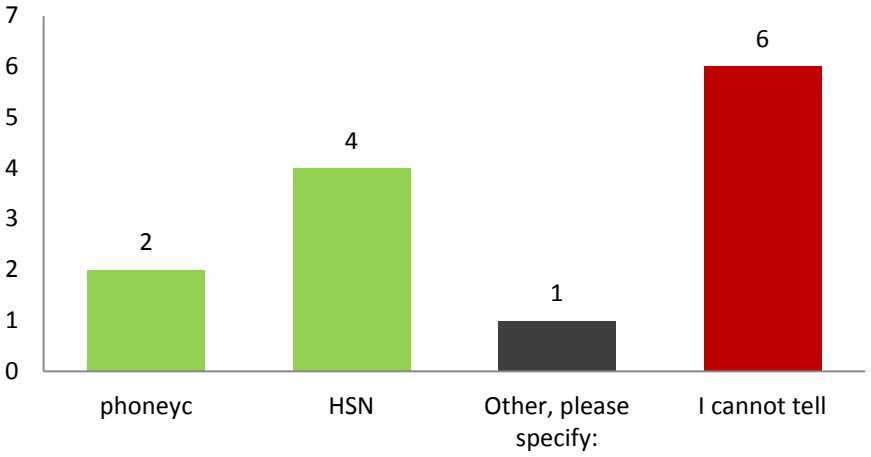

Figure 30: Which client honeypot do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

Other: *Argos*

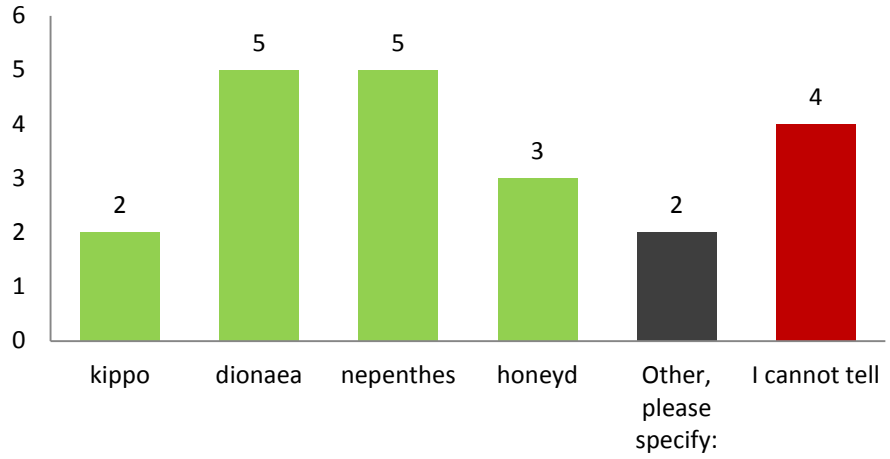

Figure 31: Which server honeypot do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

Other:

1. *SURFids*
2. *We use several types of honeypots: amun, dionea, kippo, nephentes, argos*

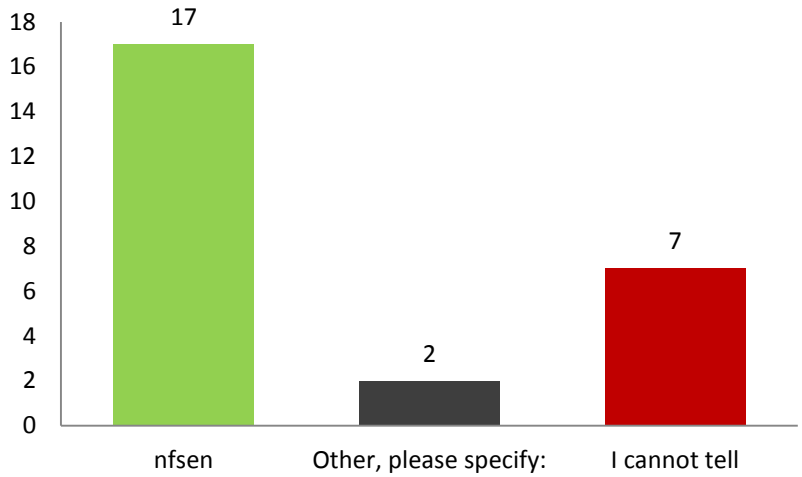

Figure 32: Which netflow collector/analyser do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

Others:

1. *Arbor Peakflow*
2. *We are working on it*

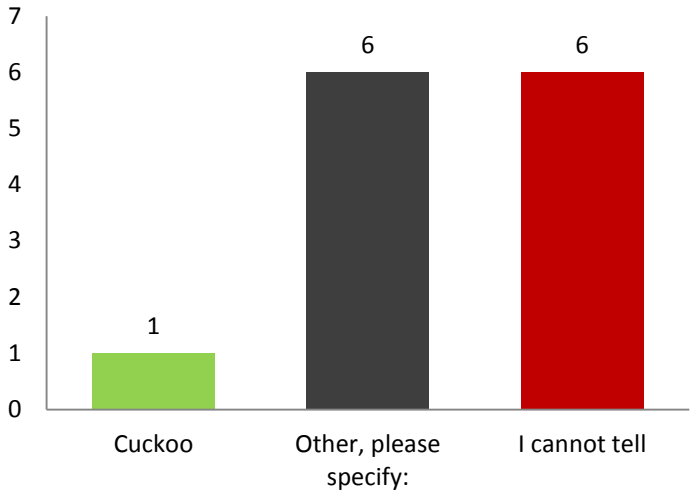

Figure 33: Which sandbox do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

Others:

1. *Truman*
2. *iDefense*
3. *Sandboxie*
4. *Norman*
5. *Real PC*

1.3.6 Sharing of information with others

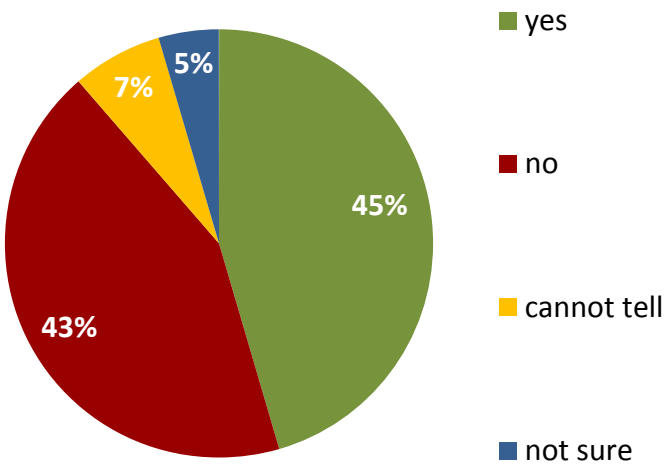

Figure 34: Do you collect information from your internal tools about incidents related to other constituencies?

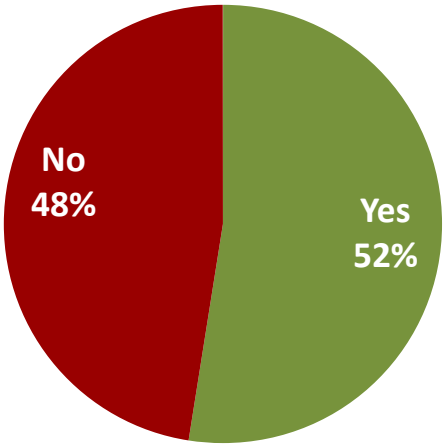

Figure 35: Do you share the data? [that you collect about other constituencies]

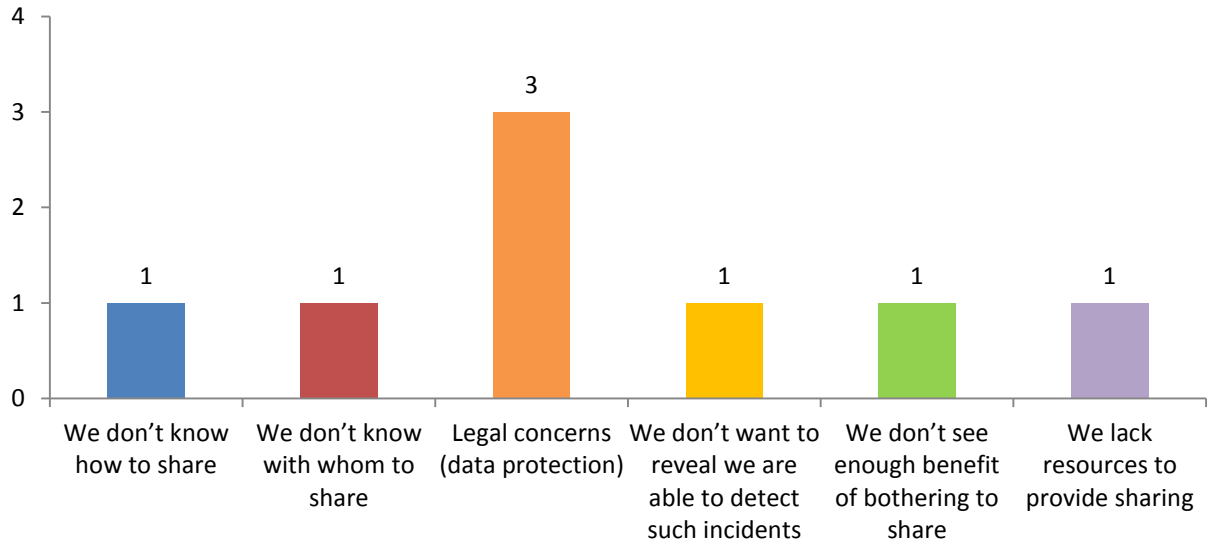

Figure 36: Why aren't you sharing the data?

What information do you share with others?

1. *Depends on the situation, who the other party is and what they want.*
2. *All information required for understanding and handling the (potential) security problem.*
3. *Information regarding incidents.*
4. *Spam traps; information about brute force attacks (logs); information about specific attacks (logs).*
5. *Information relevant to them.*
6. *Spam sources spamming our spam traps.*
7. *Incidents reported to us.*

8. *Defacements; phishing.*
9. *Malicious domains; phishing attempts.*
10. *All the information related to the issue.*
11. *Incident data.*
12. *Possible intrusions mostly.*
13. *When a specific incident is discovered, we usually share it with other CSIRTs.*
14. *Currently none.*
15. *Security bulletins.*
16. *Time stamped IPs if possible within limits of data protection laws.*
17. *Inside the public administration.*
18. *Information relevant to the constituency.*
19. *Suspected hosts (compromised), compromised websites (URL), malware.*
20. *Compromised machines.*

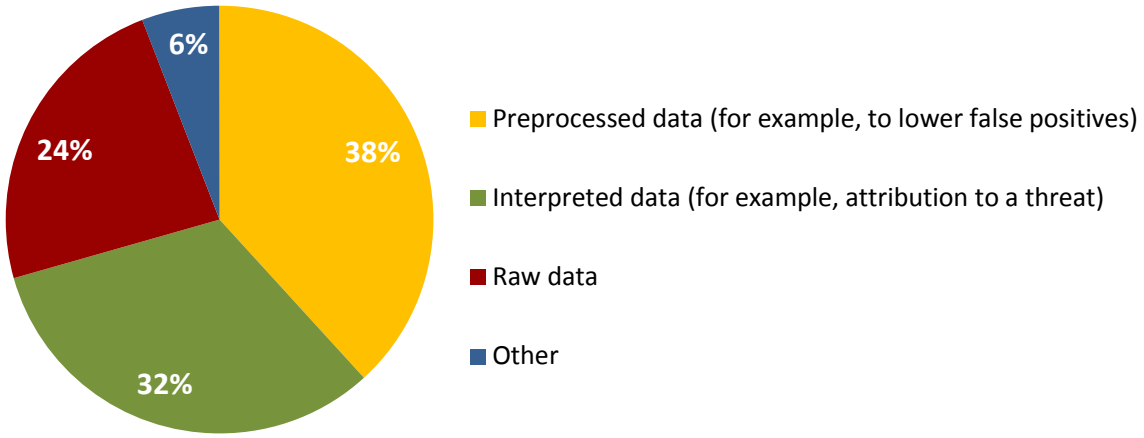

Figure 37: In what form do you share information with others?

Other: *ARF, report*

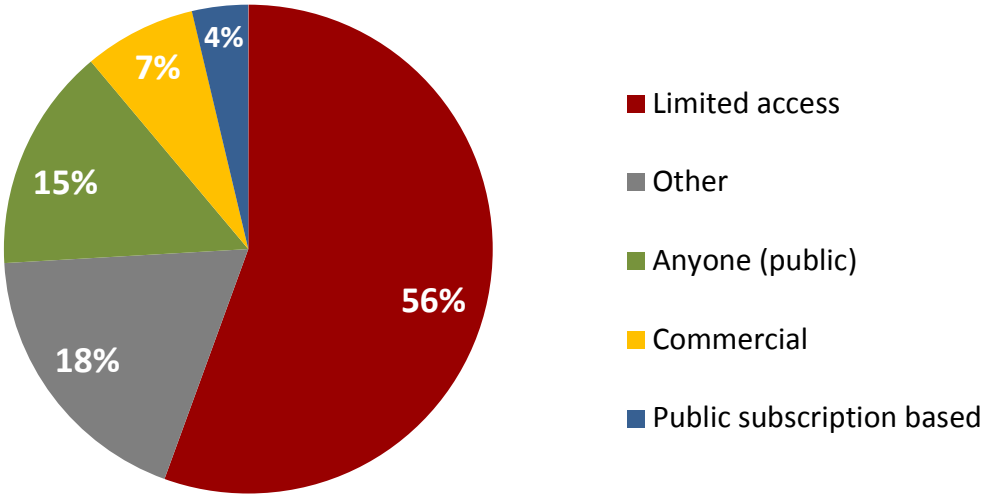

Figure 38: Under what conditions do you share information?

Other:

1. *Alerts sent to our constituent's security contact. Occasionally we send notifications to other CERTs.*
2. *Data owners.*
3. *Traffic light protocol.*
4. *Stakeholders under the traffic light protocol and other national CERTS.*
5. *Within incident handling process (related CERTs).*

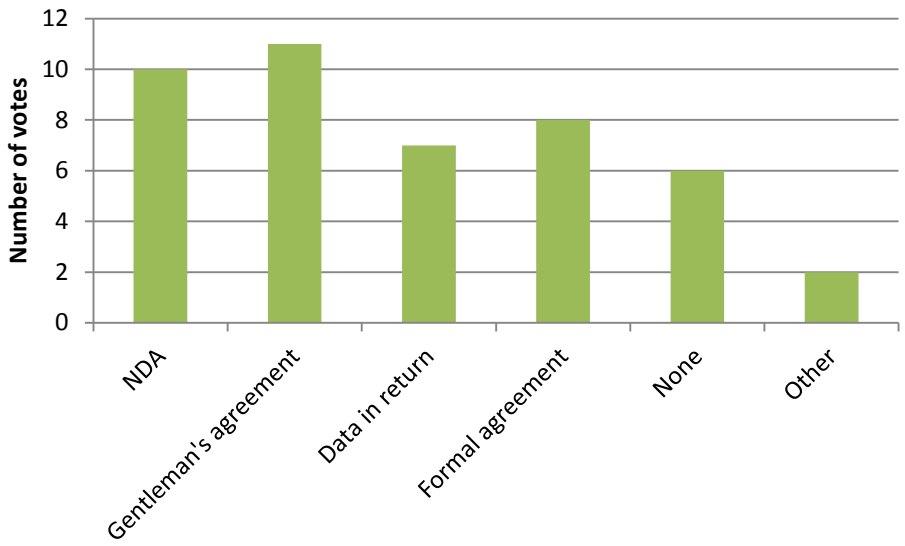

Figure 39: Do you require any sort of agreement or peer-sharing information in return?

Other:

1. *GPG*
2. *Traffic Light Protocol*

1.3.7 Correlation

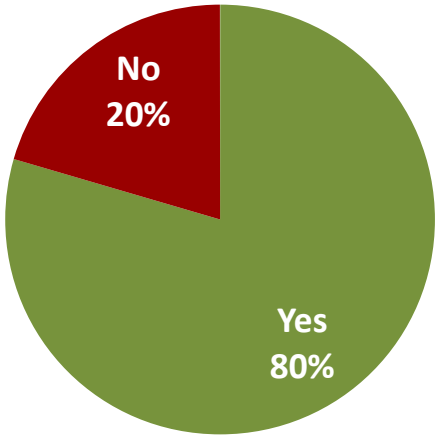

Figure 40: Do you correlate information from multiple sources in order to generate/confirm incidents?

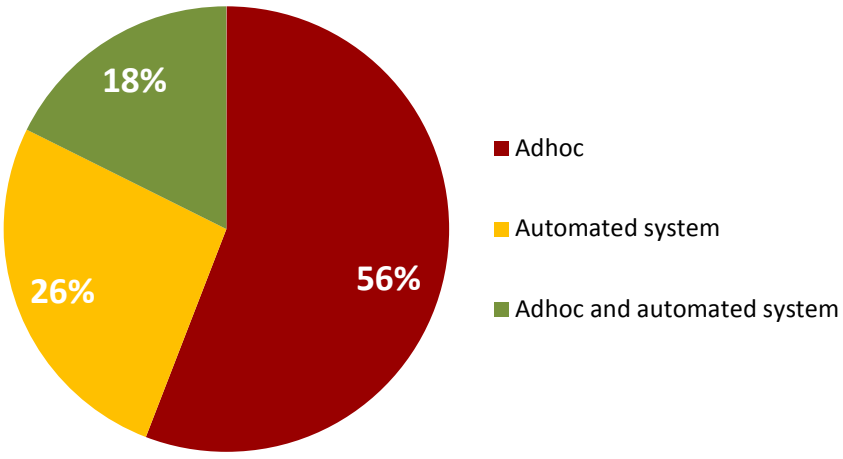

Figure 41: How do you correlate information from multiple sources?

If you use any tool for correlation what is its/their name(s)? What are their main strengths and weaknesses?

1. *AbuseHelper, loghound, SEC.*

2. *Own developed system and Megatron by Sitic Strengths: able to process a lot of information sources. Weaknesses: if something changes development is needed.*
3. *We use internally developed tools.*
4. *OSSIM: It's open source, but it requires a lot of maintenance.*
5. *We are about to include a correlation tool.*
6. *Cisco MARS.*
7. *Internally developed tool.*
8. *They are mostly self generated scripts.*
9. *BGP Ranking is used to confirm the activities of a specific ISP. But we still lack a good approach for the validation or trust ranking of the data sources. When correlating certain data sources, some might have a bigger impact but it's usually due to a 'false positive' result. If CSIRTs were able to share their ranking of data source, it could improve the whole process of confirming incidents.*
10. *Arcsight: strength: very powerful tool; weaknesses: hard to manage.*

1.3.8 Sharing of tools

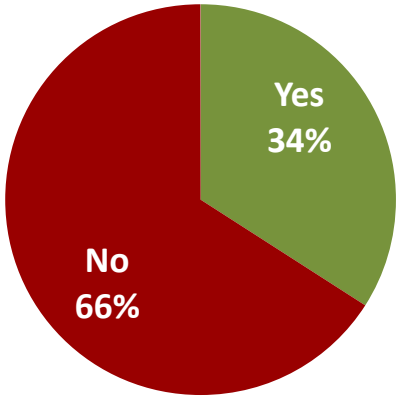

Figure 42: Have you developed your own tools for detection of threats?

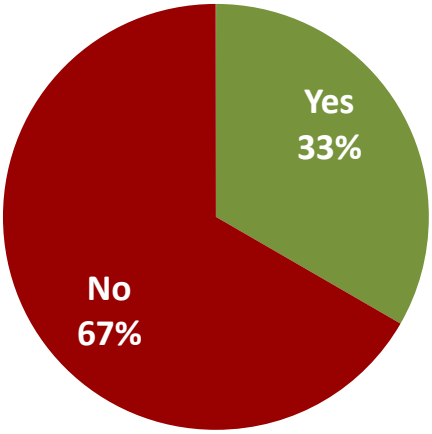

Figure 43: Have you tried to share the tool? (replies from those who tried to develop a tools)

1.3.9 What is missing

What kinds of tools do you think are missing for the detection of incidents?

1. *Visualisers.*
2. *Sensor network – will be taking place from the second half of 2011.*
3. *We are focusing now on tools to automate as much of the incident analysis process as possible. We believe too much valuable analyst time is wasted performing tasks that can be automated.*
4. *In our organisation: Netflow.*
5. *A centralised tool for management of information received from multiple sources.*
6. *DNS monitoring, automated log analysis.*
7. *A universal data container to consolidate the information to provide a correlation analysis.*
8. *Tools and sources are available or can be made available; however the automation for processing is lacking. Manual processing is not scalable.*
9. *Tools to detect p2p activity, live SQLl injection attempts.*
10. *Host integrity tools are underdeveloped and underutilised.*
11. *Advanced Anomaly Detection on netflow data (based on data mining algorithms, learning patterns, etc.). Tools for correlation of information.*
12. *It's not a question of missing tools, but of human resources (time) and no such directions given by our constituency upper-level management.*
13. *Ticketing tools.*
14. *Usually a lot of sites are lacking a good baseline and profile of network traffic before incidents, that would help the compromised sites to easily differentiate traffics during incidents.*
15. *IDS/IPS.*

16. *Better probes/IDS-based tools. Interaction between tools needs to be improved: result from analysing tools should be fed into IDS/IPS or DNS /blacklisting. Better reporting facilities on tools. Fast traffic analyses for dDoS. Reporting and visualisation tools.*
17. *Something that can correlate events more easily.*
18. *Integrated incident reporting tools in the user's desktop software.*
19. *Omni – database for incident correlation.*
20. *Honeynet – Planned.*

What kinds of services do you think are missing for the detection of incidents?

1. *Information sharing with other teams.*
2. *Easy ability of a trusted community to effectively share indicator information.*
3. *A global communication framework.*
4. *Log analysis.*
5. *A shared anonymous proxy server pool for running client honeypot in order to hide the source.*
6. *Remote monitoring services.*
7. *Standardised protocols for data exchanging between teams. Anonymous sharing of information service.*
8. *IT and infrastructure mapping.*
9. *Malware analysis, forensics.*
10. *A better approach to rank the incident data sources among CSIRTs.*
11. *Standardisation of exchange formats. Clearinghouse services of incident data.*
12. *Automated drill-down of network events.*
13. *Incident management workflow.*
14. *No comment.*

1.3.10 Underreported incidents

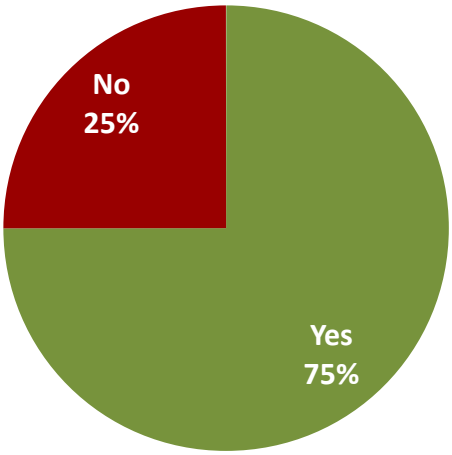

Figure 44: Do you think that some incidents are underreported?

What kinds of incidents in your opinion are underreported?

1. *Ones that an organisation deems are not important, but might be important to another party. Ones not detected or analysed due to lack of resources or lack of capability.*
2. *If only I knew that!*
3. *DoS, Data Leakage, Server compromise.*
4. *Failed DoS-attacks. Even a failed attempt to cause impact is of use. The source should be observed with caution.*
5. *Those not disclosing personal information or that will at some stage become public knowledge. A large number of incidents are occurring but are not reported, which in turn impacts on our ability to analyse the attacks so we can better defend against them.*
6. *Those that relate to the image of the organisation involved.*
7. *P2P, web defacements.*
8. *Application level incidents, service unavailability and incidents solved by administrator within constituency.*
9. *Data loss incidents.*
10. *Outbound attacks: network scanning, DoS/DDoS incoming phishing, brute force.*
11. *APT.7*
12. *Viruses, worms, intrusion, theft of data, data leakage.*
13. *Internal or local incidents in some public or private organisations.*
14. *Specific targeted attacks or espionage-related. Detection of viruses is handled locally, so correlation with other incidents is not possible Idem for DDoS attacks.*
15. *Targeted Trojans APTs Private Sector attacks.*
16. *Internationally there is still some reticence to share timely and accurate information regarding actual incidents; this is an area of ongoing concern in the CERT community.*

17. *Local low-impact incidents on client systems.*
18. *Incidents from internal adversaries which are not detected by any sensor.*
19. *Ones that have occurred as a result of user activity.*
20. *Intrusion data leak.*
21. *Spam, attacks from out hosts.*

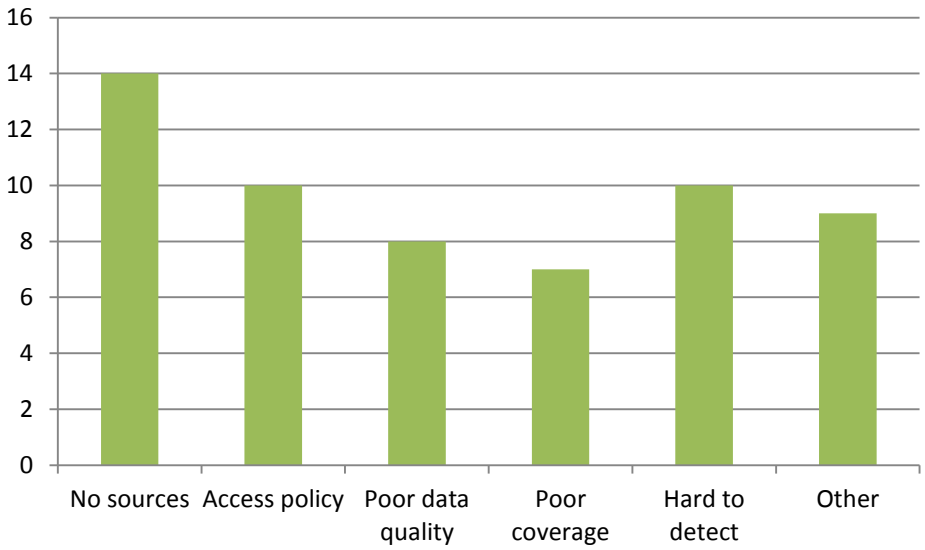

Figure 45: What is the reason why these kinds of incidents are underreported?

Other:

1. *Could be commercial/reputational damage to the organisation.*
2. *No incident report obligation.*
3. *Lack of security awareness and lack of willingness on part of management.*
4. *Data privacy issues.*
5. *Not even detected.*
6. *Locally handled and not reported.*
7. *Complex problem space.*
8. *Poor involvement of end-user in reporting incidents / poor awareness.*

1.3.11 What other problems do you have in obtaining incident information?

1. *Political issues impede sharing. Trust issues impede sharing. Lack of resources impedes sharing.*
2. *Blocking outgoing port 25 prevents spam, but hides the bots from us. Dynamic addresses and NAT prevent us from tracking incidents.*
3. *Some source information has restrictions on no. of daily access, e.g. Google Safe Browsing.*
4. *Insufficient knowledge and/or sense of urgency outside our team.*

5. *Getting details of root cause of incident, cost resulting from the incident and actors behind the attacks*
6. *Access to logs, etc., as the CSIRT does not access or have control over affected systems.*
7. *Collaboration between security teams, mainly from private sector, because they have a lot of information but sometimes are very wary of sharing.*
8. *Legal issues.*
9. *Invalid information about ISPs in the databases of Regional Internet Registrars.*
10. *There is an additional issue; that is, the privacy regulations usually consider IP addresses as personal data.*
11. *Data protection issues.*
12. *Security incident management is not integrated into the incident management process.*
13. *Awareness of users.*
14. *Sheer amount of data.*
15. *Incident reporting is often put aside in favour of production priorities.*

2 The survey questionnaire

1. Your name:
[ ]

2. Your e-mail address (optional). We will use it only to ask about details or clarifications of your answers.
[ ]

3. Name of your organisation:
[ ]

4. Size of your (host) organisation:
( ) <10 employees
( ) 10-49 employees
( ) 50-99 employees
( ) 100-299 employees
( ) 300+ employees

5. What is the profile of your organisation?
[ ] Academic
[ ] ISP
[ ] Government/public administration
[ ] Financial
[ ] Vendor
[ ] Commercial Company
[ ] Other(please specify) [ ]

6. How many incidents per year do you handle? (approx.)

[ ]

7. How many people (FTE) are assigned to your CERT?

[ ]

8. How do you obtain incident related data about your constituency?

Please, use the table below to indicate all sources you monitor or use to get information about the listed categories of incidents.

Explanation of source types:

- Internal monitoring - Systems deployed internally, such as firewalls, IPS or antivirus software.
- Monitoring of external public sources - Information feeds from public sources that you actively monitor or subscribe to, e.g. blacklists, ZeusTracker etc.
- Monitoring of commercial sources - Information feeds with access/subscription fees
- Monitoring of closed sources - Information feeds which require verification, recommendation or use other trust mechanisms to restrict access
- Incoming incident reports (reactive) - Incident related data sent to you without any subscriptions, contracts or your active looking for it (e.g. SpamCop reports fall in this category)
- Note: You can choose more than one primary source in each category.

	Internal monitoring			External public sources			Commercial sources			Closed sources			Incoming incident reports (reactive)		
	Not used	Primary source	Auxiliary source	Not used	Primary source	Auxiliary source	Not used	Primary source	Auxiliary source	Not used	Primary source	Auxiliary source	Not used	Primary source	Auxiliary source
Spam	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Scanning	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Botnet	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
C&C	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Fast-flux	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
DDoS	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Malicious URLs	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Phishing	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Malware	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Defacements	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Mass (SQL) injection	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Intrusions	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
APT	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Brute-force	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Open resolvers	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Open proxy	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

9. Please choose the answer which best matches your general feelings regarding information sources you use to obtain information about security incidents in your constituency:

[ ] We are fully satisfied with information sources we currently have

[ ] We would consider to try other sources to improve

[ ] We feel information deficit in general - we think there are significantly more incidents we do not know about

[ ] We feel we have too many information sources

10. Here you can put any other feelings or comments regarding information sources that you use:

[ ]

11. What would you like to improve when trying new sources in obtaining information about security incidents in your constituency?

[ ] Timeliness of provided incident data

[ ] Accuracy

[ ] Coverage

[ ] Ease of use

[ ] Resources required

[ ] Other (please specify) [ ]

12. Resources available:

[ ] We can fully handle current amount of incident information. We could handle even more incident information

[ ] We can fully handle current amount of incident information, but would not be able to handle more

[ ] We do process all incoming information, but only higher priority incidents are further handled, more input information would leave even more lower priority incidents without attention

[ ] We cannot properly handle even the amount of incident related information currently available

13. Here you can put any additional comments about availability of resources:

[ ]

14. Please specify what external sources providing information on malicious or problematic URLs, IPs or domains you monitor for entries from your constituency:

[ ] aMaDa Blocklist

[ ] DNS-BH Malware Domain Blocklist

[ ] Malc0de database

[ ] Malware Domain List

[ ] MalwareURL

[ ] ParetoLogic URL Clearing House

[ ] Zeus/SpyEye Tracker

[ ] CBL (Composite Blocking List)

[ ] SpamCop

[ ] The Spamhaus Project Datafeed

[ ] DSHIELD

[ ] Arbor ATLAS

[ ] Shadowserver Foundation

[ ] Cert.br data feed

[ ] Cert.br spampot

[ ] SGnet

[ ] AusCERT

[ ] ISC pDNS
[ ] NoAH
[ ] FIRE
[ ] EXPOSURE
[ ] HoneySpider Network
[ ] ARAKIS
[ ] Google Safe Browsing Alerts
[ ] Team Cymru - TC Console
[ ] Team Cymru - Flow Sonar
[ ] Other, including non-public sources which you can disclose

In the following questions we ask you to rate the information sources you are using. Please use the following scheme:

| Timeliness - how far is the data feed behind actual events?
| - Poor - delay of more than 7 days
| - Fair - delay between 24 hours and 7 days
| - Good - delay is lower than 24 hours
| - Excellent - data is provided (almost) live
|
| Accuracy of results - how often do you experience false positives/negatives?
| - Poor - there seems to be no quality control; data is almost unusable
| - Fair - data should not be used as a sole source, can be used for correlation of events
| - Good - occasional false positives/negatives; the feed can be generally used as a main source of data with human supervision
| - Excellent - (almost) no false positives/negatives; data can be fully trusted
|
| Ease of use - how easy is it to access and parse the data?
| - Poor - fancy mechanisms are used for access control making it hardly usable on many systems and/or data format is very hard to parse
| - Fair -
| - Good -

| - Excellent - data is easy to access and parse for both human and automats
|
| Coverage
| - Poor - the data feed covers only small fragments of constituency
| - Fair - the are significant gaps in coverage of the constituency by the data feed
| - Good - most of the constituency is covered by the data feed
| - Excellent - whole constituency is covered by the data feed
| |
| Resources required
| - Poor - the data source requires large amount of financial and/or human resources for adoption and usage
| - Fair - the data source requires significant amount of resources for adoption and/or usage
| - Good - the data source requires significant amount of resources for adoption but less for usage
| - Excellent - the amount of resources required to adopt and use the data source is negligible
+----------+

15. Please rate aMaDa Blocklist timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
aMaDa Blocklist	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

16. Please rate DNS-BH Malware Domain Blocklist timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
DNS-BH Malware Domain	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Blocklist

17. Please rate Malc0de database timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
Malc0de database	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

18. Please rate Malware Domain List timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
Malware Domain List	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

19. Please rate MalwareURL timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
MalwareURL	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

20. Please rate ParetoLogic URL Clearing House timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
ParetoLogic URL Clearing House	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

21. Please rate Zeus/SpyEye Tracker timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
Zeus/SpyEye Tracker	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

22. Please rate CBL (Composite Blocking List) timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
CBL (Composite Blocking List)	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

23. Please rate SpamCop timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
SpamCop	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

24. Please rate The Spamhaus Project Datafeed timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
The Spamhaus Project Datafeed	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

25. Please rate DSHIELD timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
DSHIELD	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

26. Please rate Arbor ATLAS timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
Arbor ATLAS	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

27. Please rate Shadowserver Foundation timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
Shadowserver Foundation	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

28. Please rate Cert.br data feed timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
Cert.br data feed	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

29. Please rate Cert.br spampot timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
Cert.br spampot	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

30. Please rate SGnet timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
SGnet	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

31. Please rate AusCERT timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
AusCERT	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

32. Please rate ISC pDNS timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
ISC pDNS	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

33. Please rate NoAH timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
NoAH	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

34. Please rate FIRE timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
FIRE	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

35. Please rate EXPOSURE timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
EXPOSURE	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

36. Please rate HoneySpider Network timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
HoneySpider Network	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

37. Please rate ARAKIS timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
ARAKIS	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

38. Please rate Google Safe Browsing Alerts timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
Google Safe Browsing Alerts	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

39. Please rate Team Cymru - TC Console timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
Team Cymru - TC Console	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

40. Please rate Team Cymru - Flow Sonar timeliness, accuracy of results, ease of use, coverage and resources required:

	Timeliness				Accuracy of results				Ease of use				Coverage				Resources required			
	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent	poor	fair	good	excellent
Team Cymru - Flow Sonar	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

41. If you are aware of other sources, not included in the list above, please list them here and, if possible, rate them using the

criteria of timeliness, accuracy of results, ease of use, coverage and resources required.

[ ]

42. Do you use any closed sources of information you cannot disclose?

[ ] Yes

[ ] No

43. What kind of information do the closed sources of information provide? Can you describe the source in a few words?

[ ]

44. How does the quality of such sources compare with the public ones?

[ ]

45. Provide a list of TOP 3 best sources for gathering information from according to you:

[ ]

46. Do you use the following tools to gather information from your network:

	I use it	I used it in the past, but dropped it.	I never used it and will not use it.	I don't use it but plan to use it in future.
Firewalls	[ ]	[ ]	[ ]	[ ]
Web Application Firewalls	[ ]	[ ]	[ ]	[ ]
AV	[ ]	[ ]	[ ]	[ ]
IDS/IPS	[ ]	[ ]	[ ]	[ ]
Client honeypot	[ ]	[ ]	[ ]	[ ]
Server honeypot	[ ]	[ ]	[ ]	[ ]
Netflow	[ ]	[ ]	[ ]	[ ]
Router logs	[ ]	[ ]	[ ]	[ ]
Sandboxes	[ ]	[ ]	[ ]	[ ]
System logs	[ ]	[ ]	[ ]	[ ]
Database logs	[ ]	[ ]	[ ]	[ ]
App logs	[ ]	[ ]	[ ]	[ ]
Spamtrap	[ ]	[ ]	[ ]	[ ]
Proxy logs	[ ]	[ ]	[ ]	[ ]
Darknet	[ ]	[ ]	[ ]	[ ]
Passive DNS monitoring	[ ]	[ ]	[ ]	[ ]

| In the following questions we ask you to rate the information sources you are using.
|
| Please use the following scheme:
|
| Timeliness - how far is the data feed behind actual events?
| - Poor - delay of more than 7 days
| - Fair - delay between 24 hours and 7 days
| - Good - delay is lower than 24 hours
| - Excellent - data is provided (almost) live
|
| Accuracy of results - how often do you experience false positives/negatives?
| - Poor - there seems to be no quality control; data is almost unusable
| - Fair - data should not be used as a sole source, can be used for correlation of events
| - Good - occasional false positives/negatives; the feed can be generally used as a main source of data with human supervision
| - Excellent - (almost) no false positives/negatives; data can be fully trusted
|
| Ease of use - how easy is it to access and parse the data?
| - Poor - fancy mechanisms are used for access control making it hardly usable on many systems and/or data format is very hard to parse
| - Fair - signifcant effort is required to access and parse the data in order to integrate them with other systems
| - Good - data is easy to access but requires some effort to be readable for humans and/or automats
| - Excellent - data is easy to access and parse for both humans and automats
|
| Coverage
| - Poor - the data feed covers only small fragments of constituency
| - Fair - the are significant gaps in coverage of the constituency by the data feed
| - Good - most of the constituency is covered by the data feed
| - Excellent - whole constituency is covered by the data feed
|
| Resources required

| - Poor - the data source requires large amount of financial and/or human resources for adoption and usage
| - Fair - the data source requires significant amount of resources for adoption and/or usage
| - Good - the data source requires significant amount of resources for adoption but less for usage
| - Excellent - the amount of resources required to adopt and use the data source is negligible
|
| Scalability - ability to scale to smaller/larger networks or data volumes
| - Poor - (almost) no possibility to scale
| - Fair - scaling is not possible without extensive changes/customisation
| - Good - scaling is possible with some
| - Excellent - scaling is easy and requires negligible amount of resources
|
| Extensibility - ability to extend the functionality
| - Poor - closed architecture, (almost) no possibility to extend
| - Fair - open/modular architecture, but requires lots of custom coding to extend
| - Good - open/modular architecture; can be extended with existing plugins, but customisation requires significant effort
| - Excellent - modular architecture; easy to extend with existing or customised plugins
|

47.If you use other types of tools to gather information from your network not included in the list above, please list them here and, if possible, rate them using the criteria of timeliness, accuracy of results, coverage, required resources, scalability, extensibility.

NOTE: If you have developed your own tools, do not list them here. They will be covered by questions later in the survey.

[ ]

48. Which firewall do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

[ ] I cannot tell
[ ] pf
[ ] ipfw
[ ] ipf
[ ] iptables
[ ] Check Point FireWall-1
[ ] Fortinet FortiGate
[ ] Juniper NetScreen
[ ] Juniper SRX
[ ] Cisco ASA
[ ] Cisco PIX
[ ] Cisco FWSM
[ ] Other, please specify: [ ]

49. How would you rate this firewall in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

50. Which web application firewall do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

[ ] I cannot tell

[ ] mod_security
[ ] AQTRONIX WebKnight
[ ] Trustwave WebDefend
[ ] FirtiNet FortiWeb
[ ] Cisco ACE
[ ] Imperva SecureSphere
[ ] f5 BIG-IP
[ ] integrated with web application
[ ] Other, please specify: [ ]

51. How would you rate this web application firewall in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

52. Which antivirus solution do/did you use as a source of incident data?

(If you use more than one, please select the one which you consider most valuable)

[ ] I cannot tell
[ ] AVG
[ ] Avast
[ ] Avira
[ ] BitDefender
[ ] ClamAV
[ ] F-Prot
[ ] F-Secure
[ ] Fortinet
[ ] Kaspersky
[ ] McAfee
[ ] NOD32
[ ] Norman
[ ] Symantec
[ ] TrendMicro
[ ] Other, please specify: [ ]

53. How would you rate the specific implementation of this antivirus solution as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

54. Which IDS/IPS do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

[ ] Cannot tell
[ ] Snort
[ ] Suricata
[ ] OSSEC
[ ] AIDE
[ ] Prelude IDS
[ ] Check Point IPS-1
[ ] Cisco IDP
[ ] Other, please specify: [ ]

55. How would you rate the specific implementation of this IDS/IPS as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

56. Which client honeypot do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

[ ] I cannot tell
[ ] HSN

[ ] phoneyc

[ ] jsunpack

[ ] Capture-HPC

[ ] Other, please specify: [ ]

57. How would you rate the specific implementation of this client honeypot as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

58. Which server honeypot do/did you use as a source of incident data?
(If you use more than one, please select the one which you consider most valuable)

[ ] I cannot tell
[ ] honeyd
[ ] nepenthes
[ ] dionaea
[ ] kippo
[ ] kojoney
[ ] VoIP Honey
[ ] Other, please specify: [ ]

59. How would you rate the specific implementation of this server honeypot as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

60. Which netflow collector/analyzer do/did you use as a source of incident data?

(If you use more than one, please select the one which you consider most valuable)

[ ] I cannot tell

[ ] nfsen

[ ] Other, please specify: [ ]

61. How would you rate the specific implementation of this netflow collector/analyzer as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

62. Which sandbox do/did you use as a source of incident data?

(If you use more than one, please select the one which you consider most valuable)

[ ] I cannot tell

[ ] Zero Wine

[ ] Cuckoo

[ ] Other, please specify: [ ]

63. How would you rate the specific implementation of this sandbox as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

64. How would you rate the specific implementation of monitoring of router logs as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

65. How would you rate the specific implementation of monitoring of system logs as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

66. How would you rate the specific implementation of monitoring of database logs as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

67. How would you rate the specific implementation of monitoring of proxy logs as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

68. How would you rate the specific implementation of monitoring of application logs as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

69. How would you rate the specific implementation of using spamtraps as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

70. How would you rate the specific implementation of darknets as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

71. How would you rate the specific implementation of passive DNS monitoring as the source of incident data in your organisation in the following categories:

	Rate			
	Poor	Fair	Good	Excellent
Timeliness of provided incident data	[ ]	[ ]	[ ]	[ ]
Accuracy of results	[ ]	[ ]	[ ]	[ ]
Ease of use	[ ]	[ ]	[ ]	[ ]
Coverage	[ ]	[ ]	[ ]	[ ]
Required Resources	[ ]	[ ]	[ ]	[ ]
Scalability	[ ]	[ ]	[ ]	[ ]
Extensibility	[ ]	[ ]	[ ]	[ ]

72. Have you customized any tool you listed in questions 48 to 71 (including writing scripts to parse data)?

[ ] Yes

[ ] No

73. What was the reason for customizing a tool/tools?

[ ]

74. Have you developed your own tools for detection of threats?

[ ] Yes

[ ] No

75. Please describe shortly what the tool does and how it works.

[ ]

76. Why and how can this customized or developed tool be potentially useful for other teams? (if not clear from the answer to the previous question)

[ ]

77. Have you tried to share the tool?

[ ] Yes

[ ] No

78. With whom did you try to share the tool and what was their feedback?

[ ]

79. Provide a list of TOP 3 best tools for gathering information according to you:

[ ]

80. Do you collect information about incidents related to other constituencies?

[ ] yes

[ ] no

[ ] not sure

[ ] cannot tell

81. Do you share the data?

[ ] Yes -> jump to 83

[ ] No

82. Why aren't you sharing the data?
[ ] Accuracy of our data is not sufficient to share
[ ] We don’t know how to share
[ ] We don’t know with whom to share
[ ] Legal concerns (data protection)
[ ] We don’t think anyone needs more data
[ ] We don’t want to reveal we are able to detect such incidents
[ ] We don’t see enough benefit of bothering to share
[ ] We stopped sharing the data, because the other side did not act on it (ie, problems reported were not fixed)
[ ] We lack resources to provide sharing
[ ] Other, please specify: [ ]
-> jump to 87

83. What information do you share with others?
[ ]

84. In what form do you share information with others?
[ ] Raw data
[ ] Preprocessed data (for example, to lower false positives)
[ ] Interpreted data (for example, attribution to a threat)
[ ] Other, please specify: [ ]

85. Under what conditions do you share information?
[ ] Anyone (public)
[ ] Public subscription based
[ ] Limited access
[ ] Commercial
[ ] Other, please specify: [ ]

86. Do you require any sort of agreement or peers sharing information in return?

[ ] NDA
[ ] Gentleman's agreement
[ ] Data in return
[ ] Formal agreement
[ ] None
[ ] Other, please describe: [ ]

87. Do you correlate information from multiple sources in order to generate/confirm incidents?

[ ] Yes
[ ] No

88. How do you correlate information from multiple sources?

[ ] Adhoc
[ ] Automated system

89. If you use any tool for correlation what is its/their name(s)? What are their main strengths and weaknesses?

[ ]

90. What kinds of tools do you think are missing for the detection of incidents?

[ ]

91. What kinds of services do you think are missing for the detection of incidents?

[ ]

92. Do you think that some incidents are underreported?

[ ] Yes
[ ] No

93. What kind of incidents in your opinion are underreported?

[ ]

94. What is the reason that those kind of incidents are underreported?

[ ] No sources
[ ] Access policy
[ ] Poor data quality
[ ] Poor coverage
[ ] Hard to detect
[ ] Other: [ ]

95. What other problems you have in obtaining incident information?

[ ]

96. Additional comments to this survey

[ ]