Proactive Detection of Network Security Incidents – A Study

Andrea Dufkova (ENISA)
Piotr Kijewski (CERT Polska/NASK)

FIRST 2012 Conference
21st June 2012, Malta

OUR TALK TODAY …

i. Links with ENISA work
ii. Facts about the study
iii. Dive into the research findings
iv. Impact of the study in Poland
v. Open questions
vi. Recommendations

Background information

ENISA CERT relations/operational security – focus in 2012 - studies

- Definition of baseline capabilities of national and governmental CERTs

- Training and exercises
- Cybercrime prevention
- Information sharing and alerting

- Early warning

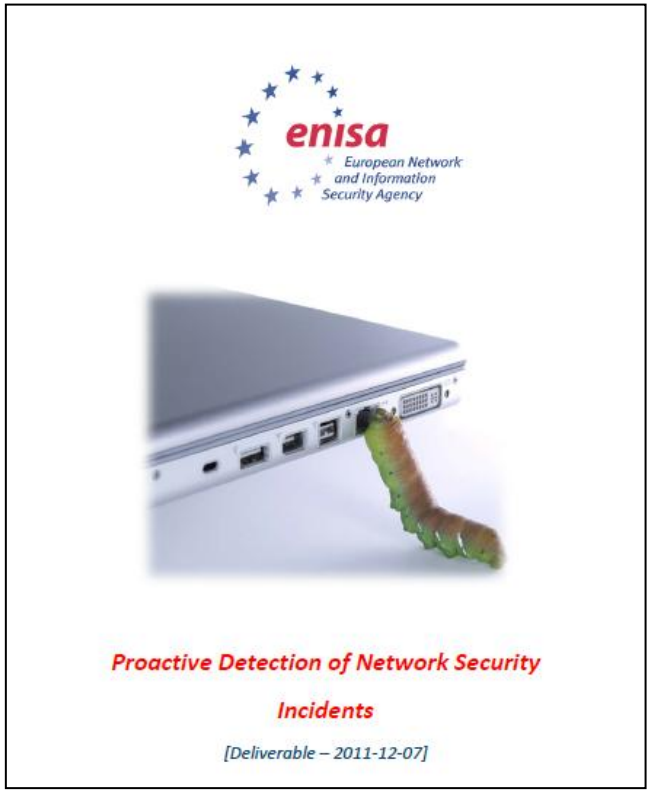
Some Facts

- Project ran for ½ year
- Study published in December 2011

… 133 pages to read, but…

- Inventory of services/tools and mechanisms (pages 27-98)
- 16 shortcomings – pages 108 - 127
- 35 recommendations - pages 128-132
- Where to get the study:

http://www.enisa.europa.eu/activities/cert/support/proactive-detection



Problem definition

- **Reactive approach**
  - **Wait for incoming incident reports (internal/external)**

vs

- **Proactive approach**
  - **Actively look for incidents taking place**
    - **Subscribe to external services informing about problems**
    - **Deploy internal monitoring tools / mechanisms**

- **Provide a sort of '*Early warning*' service from the constituent's (client's) perspective**

Objectives

- Inventory of available methods, activities and information sources for proactive detection of network security incidents
- Identify good practice and recommended measures
- What needs to be done to improve and by whom

Target audience

- National / governmental and other CERTs
- Abuse teams
- Data providers

new or already established ....

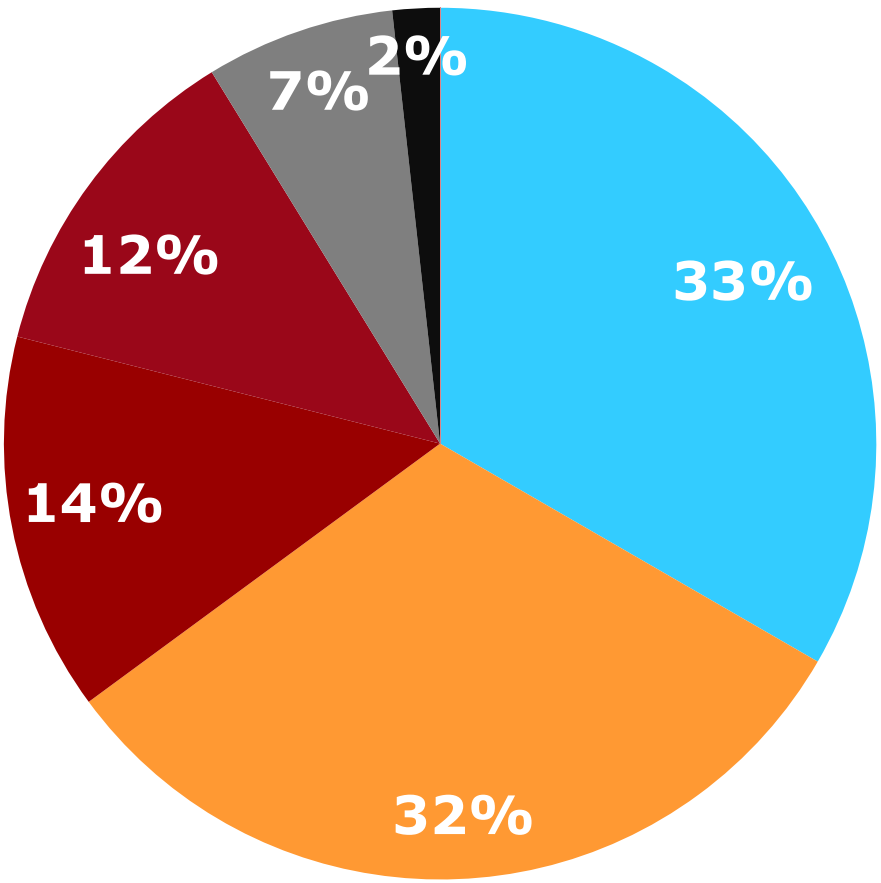
Approach

- **Authors of the study – ENISA experts and CERT Polska / NASK (contractor)**

- **Main steps:**
  - **Desktop research**
  - **Survey among CERTs (>100 invitations, 45 responses)**
  - **Analysis**
  - **Expert group (active survey participants, other experts)**
    - **Meeting**
    - **Mailing list**

Survey

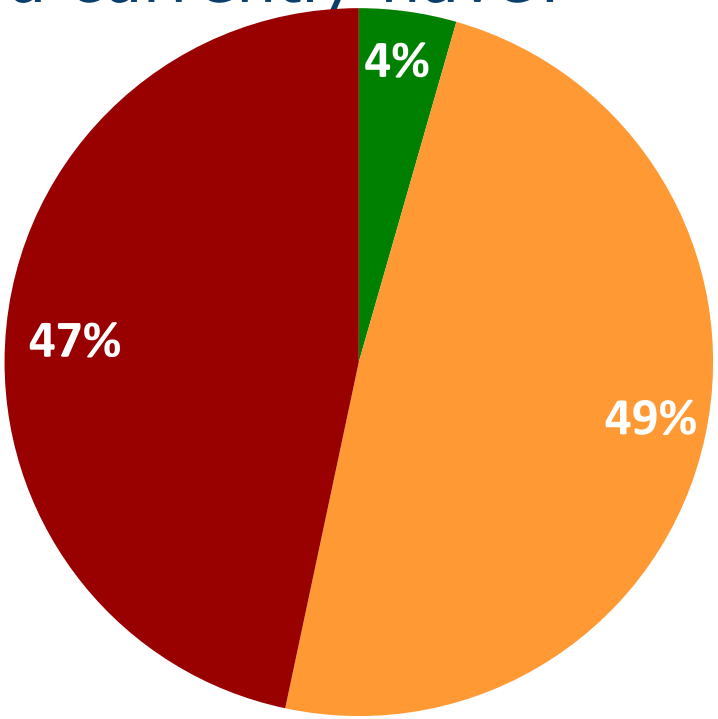
Respondent profile



- Government/public administration
- Academic
- ISP
- Other(please specify)
- Commercial Company
- Financial

Survey

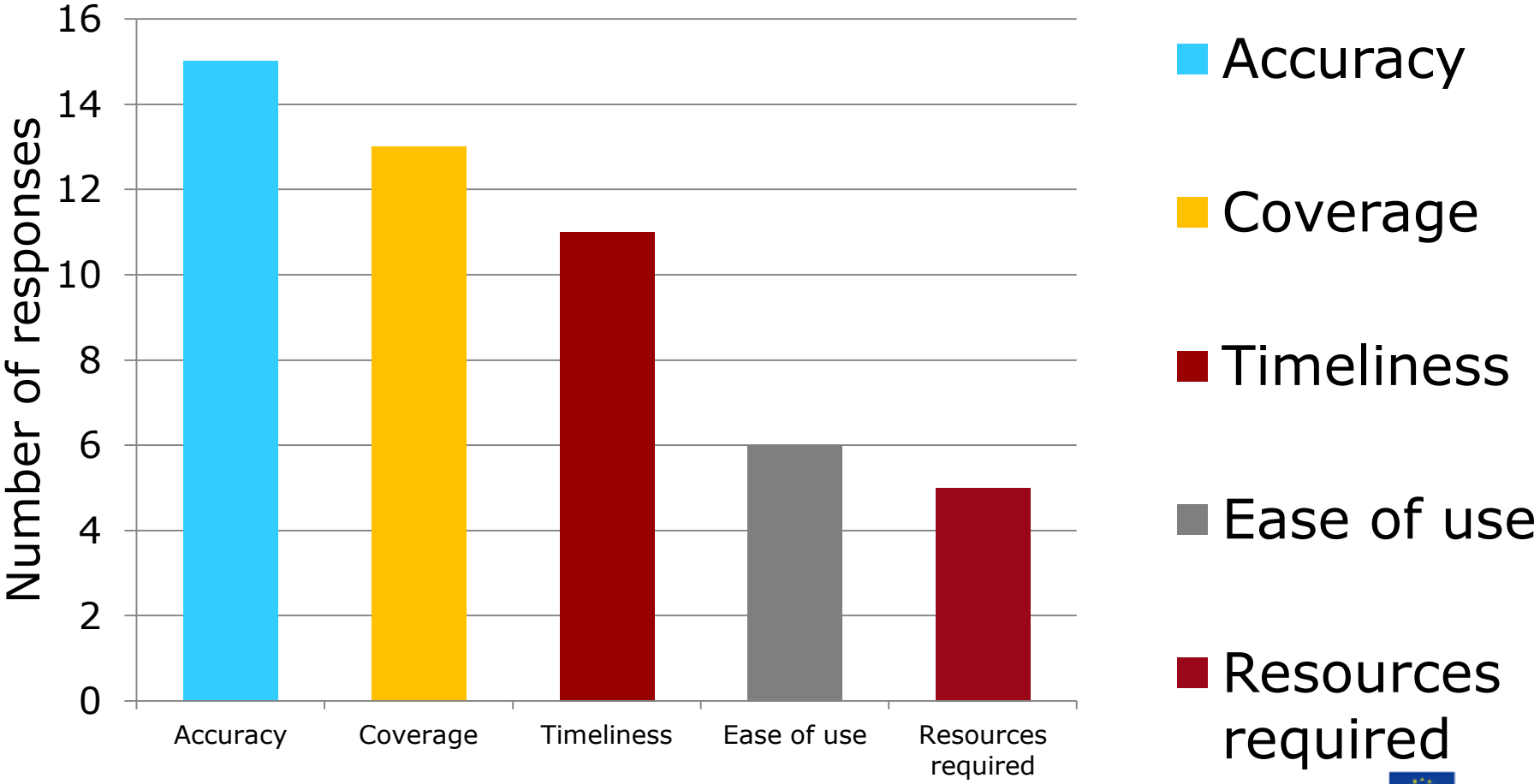
How do you feel with the incident information sources you currently have?



- 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

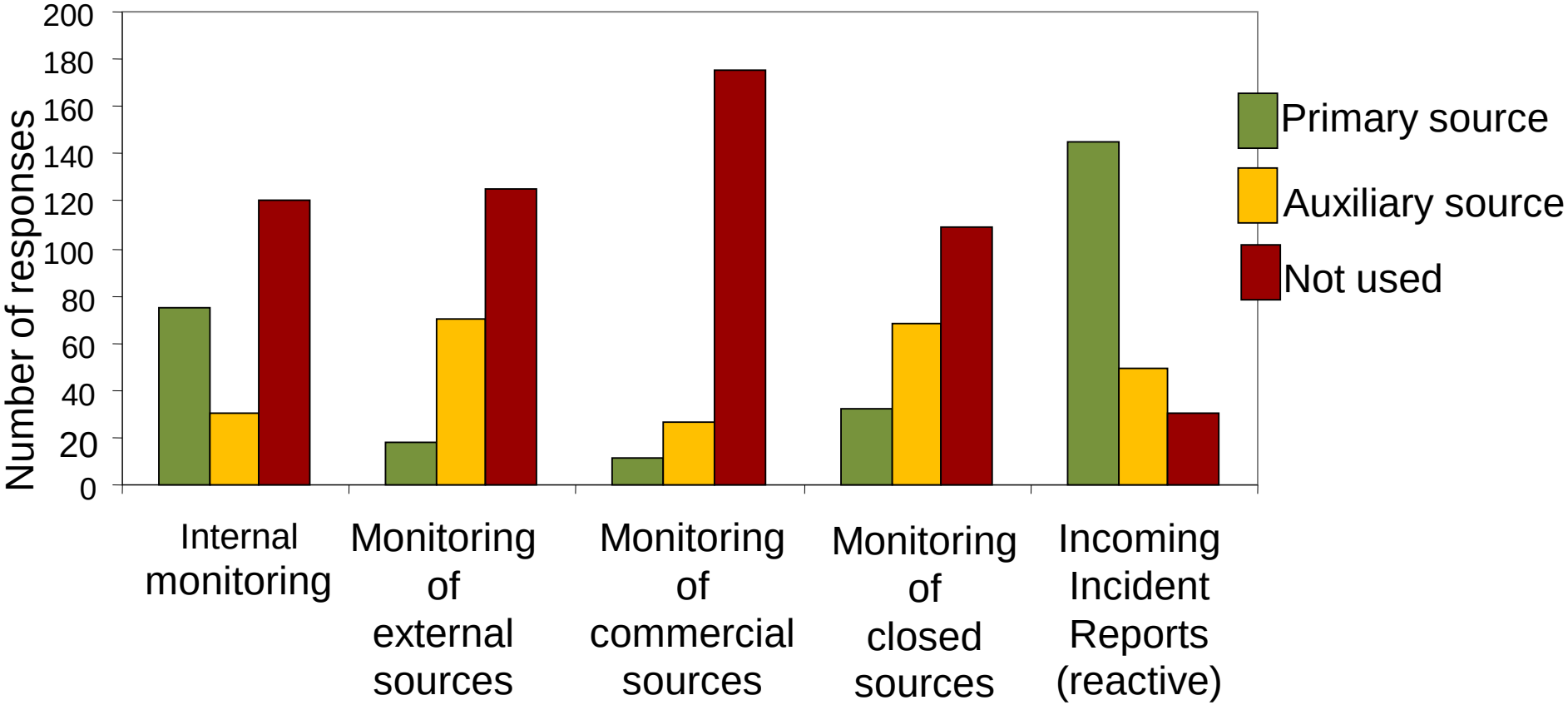
Survey

What you would like to improve?



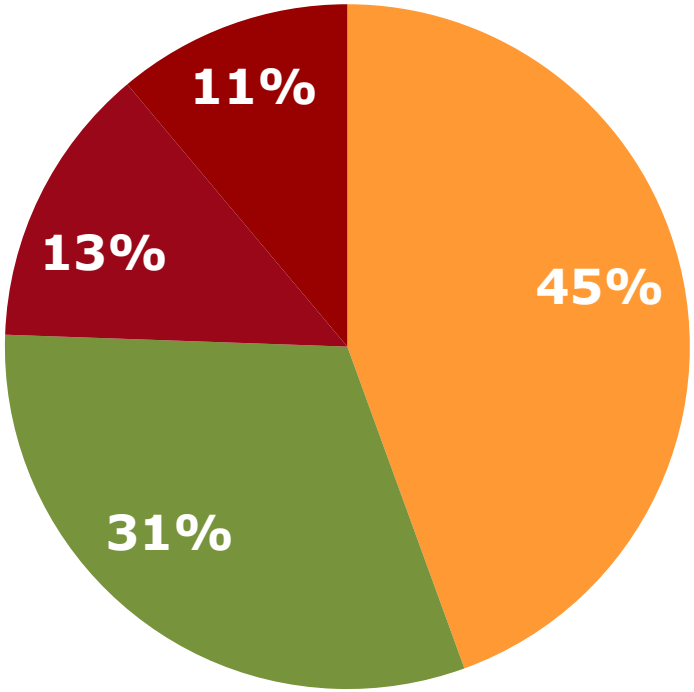
Survey

How do you obtain incident related data about your constituency?



Survey

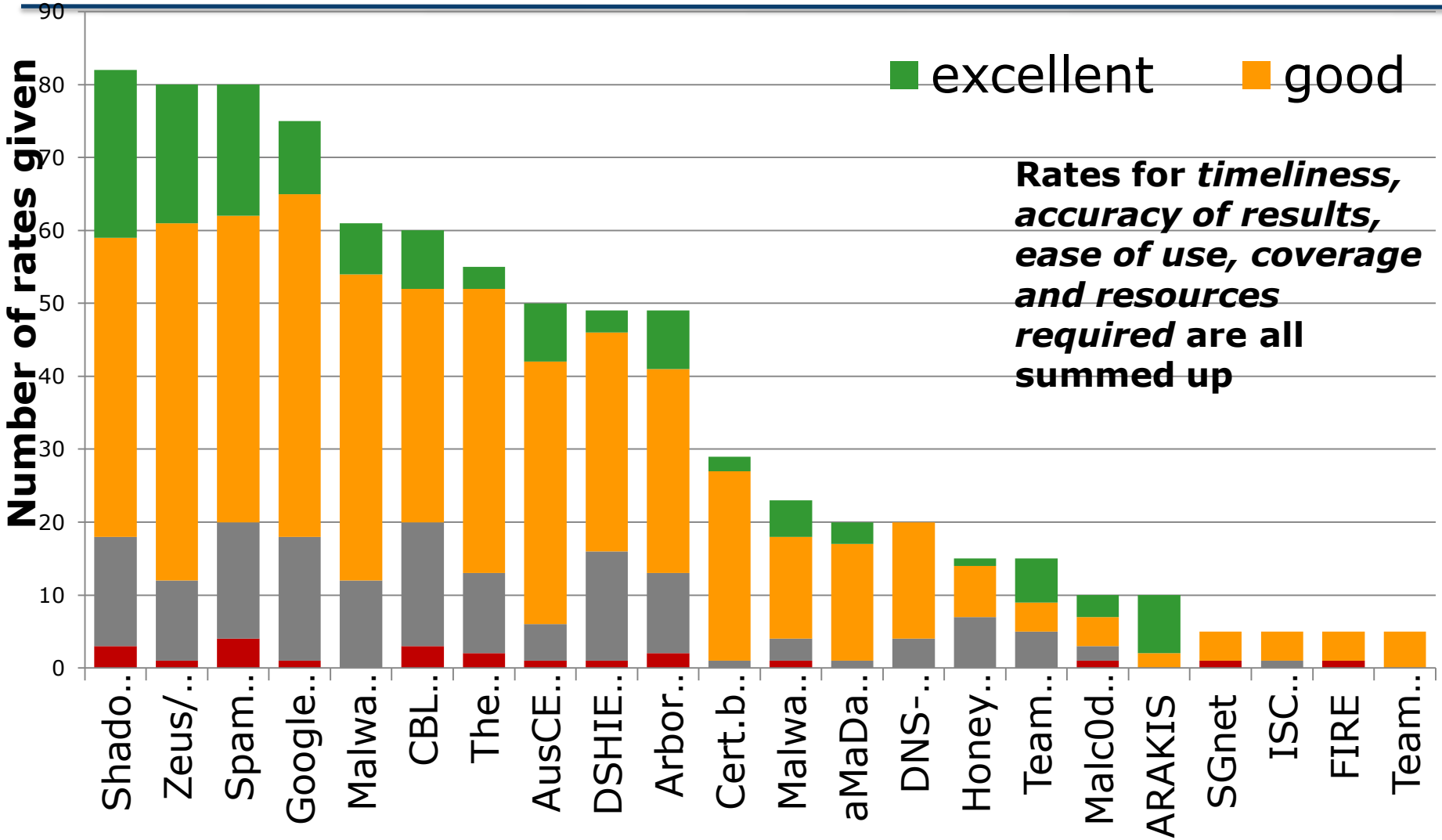
Resources available



- 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 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 cannot properly handle even the amount of incident related information currently available

Survey

External sources of information



Survey

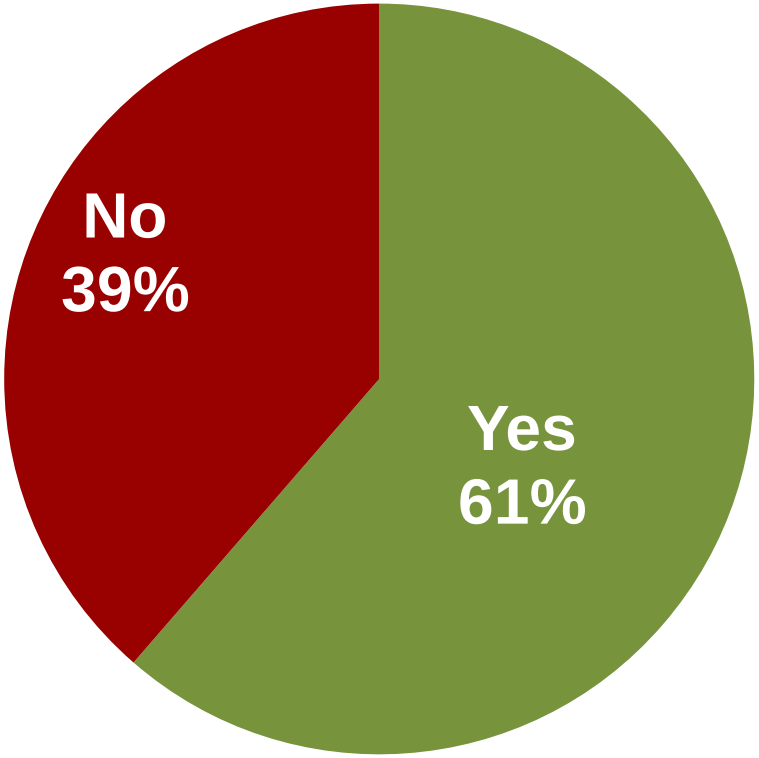
CERTs that use most popular source (Shadowserver)

40%

Survey

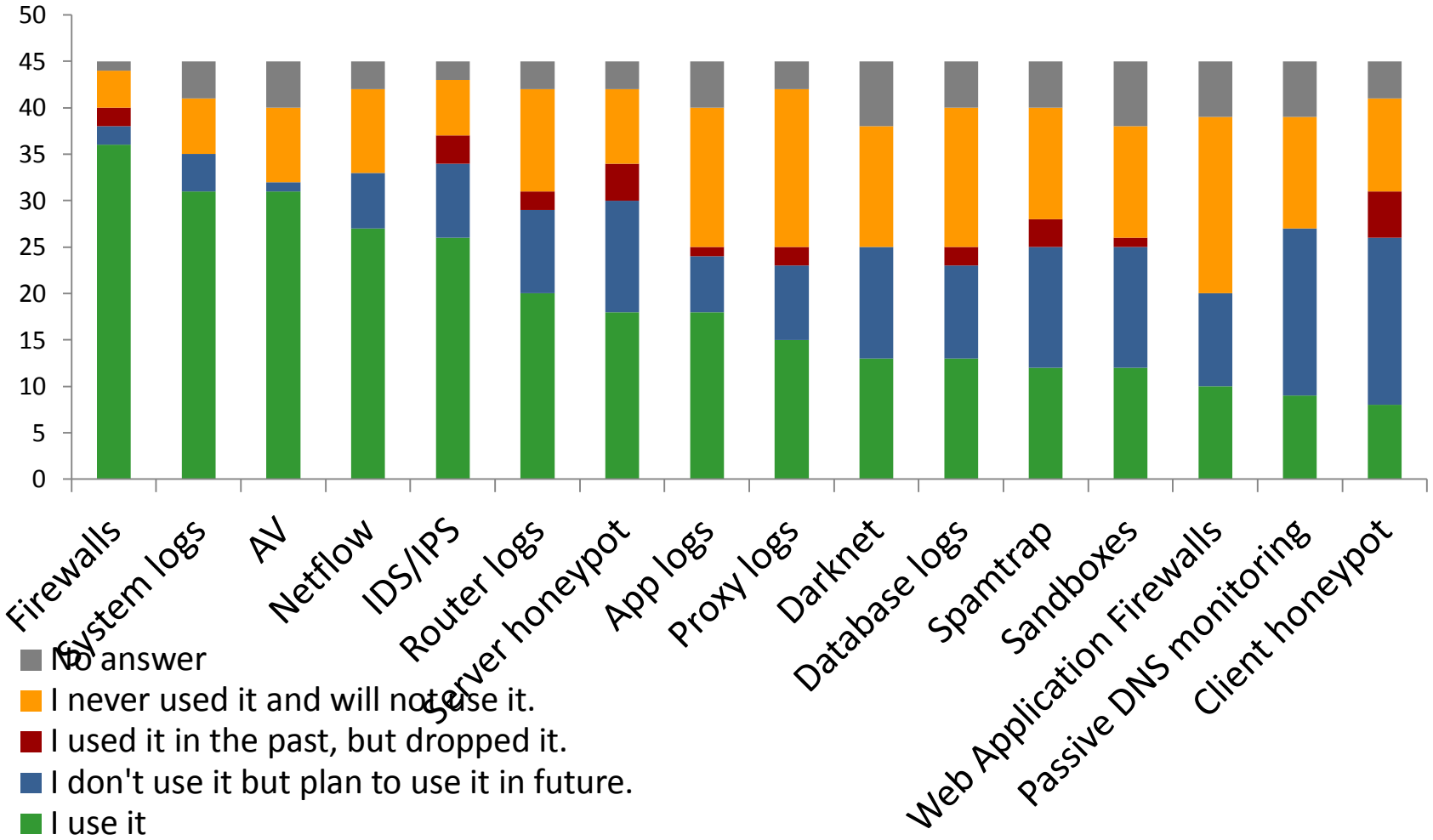
External sources of information

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



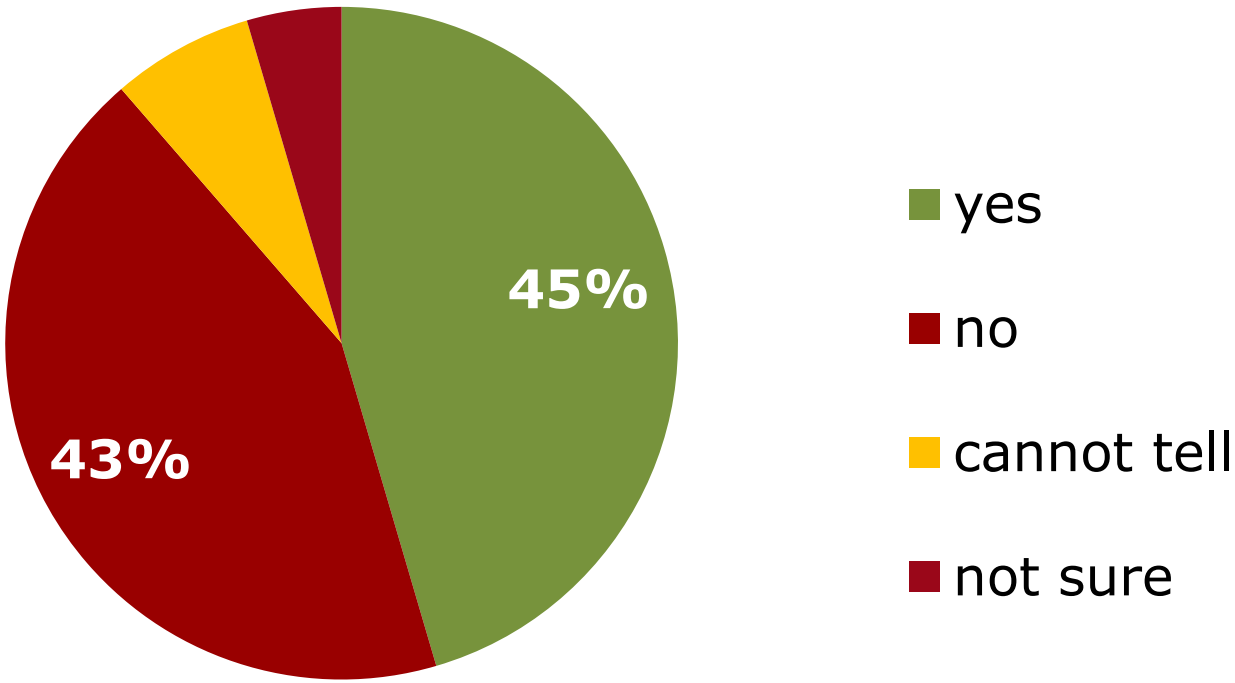
Survey

Internal tools used



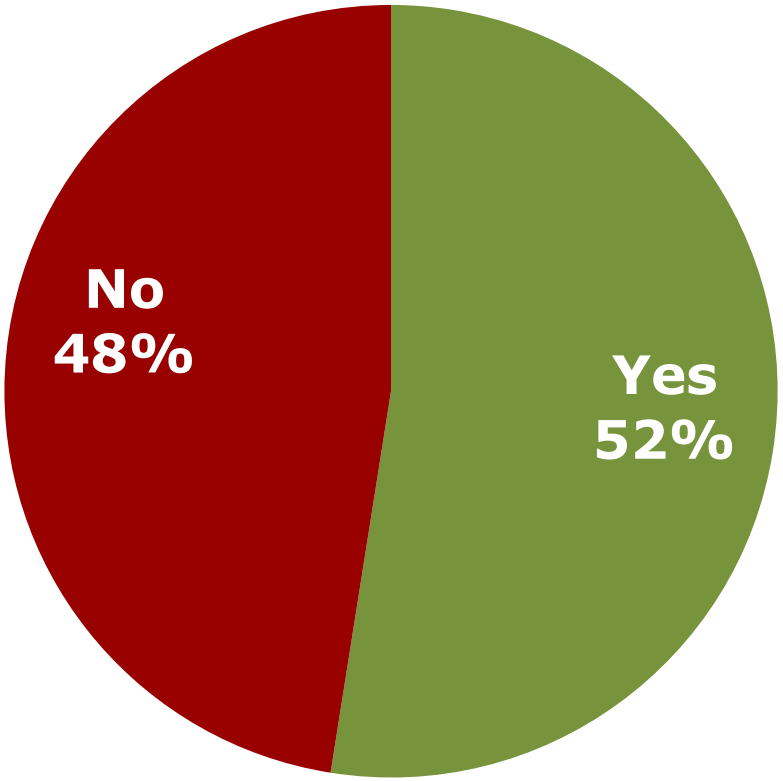
Survey

Do you collect data about other constituencies?



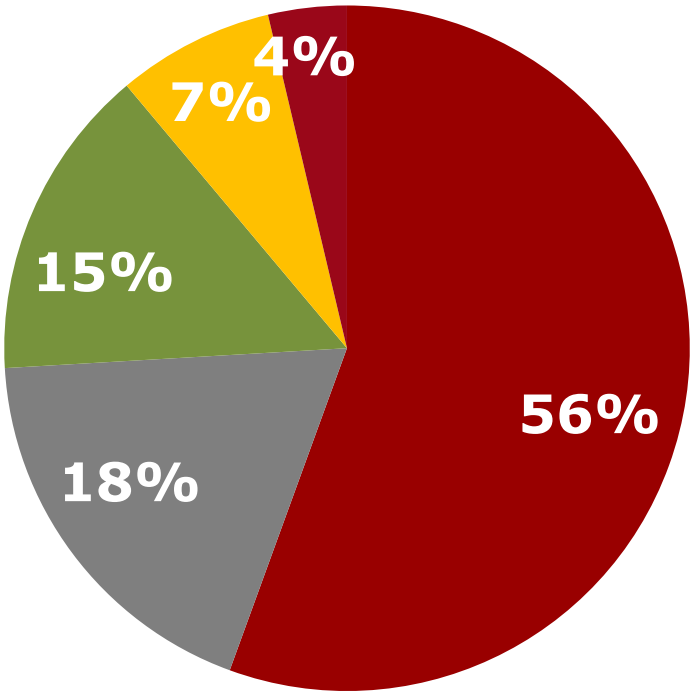
Survey

Do you share this information?



Survey

Under what rules do you share?



- Limited access
- Other
- Anyone (public)
- Commercial
- Public subscription based

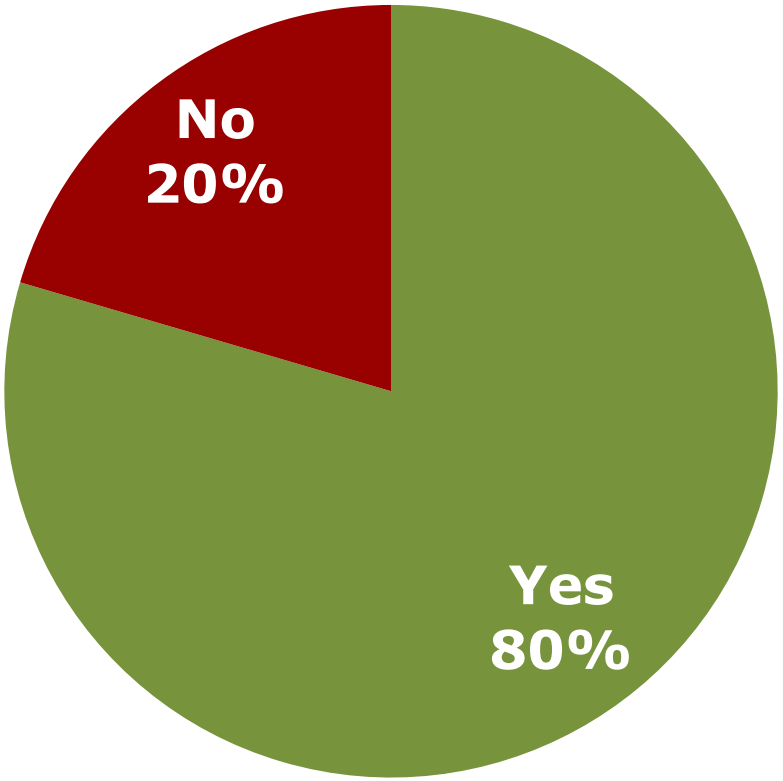
Survey

CERTs that collect info about others and share

23,4%

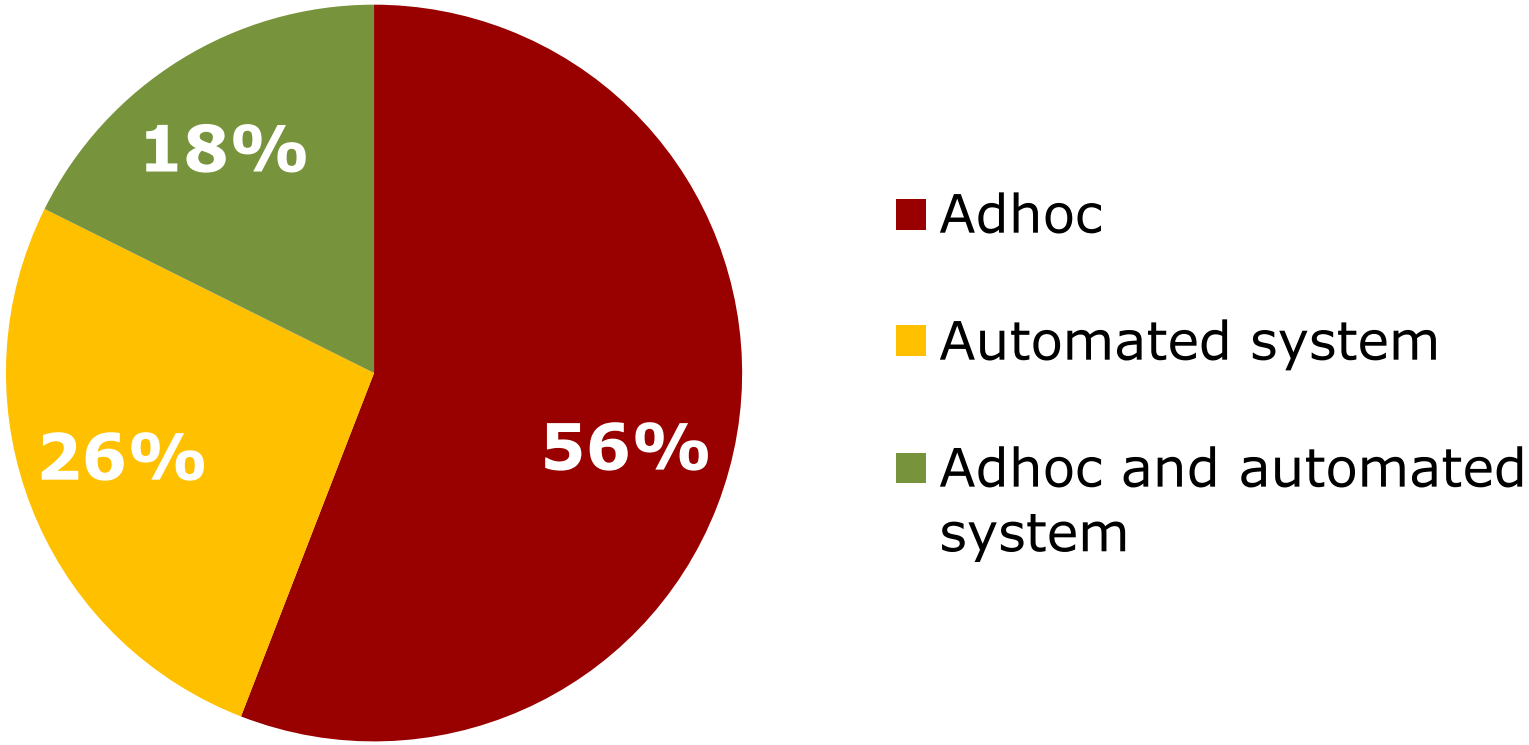
Survey

Do you correlate?



Survey

how do you correlate information from multiple sources



Survey

CERTs that automate the correlation process in any way

35,2%

Analysis

- Evaluation criteria:
  - Timeliness
  - Accuracy
  - Ease of use
  - Coverage
  - Resources required
  - Scalability (for internal tools)
  - Extensibility (for internal tools)

- **Significant degree of subjectiveness present** (expert judgment, survey responses, workgroup expert opinions)

Summary of external sources

Service	Timeliness	Accuracy of results	Ease of use	Coverage	Resources required
DNS-BH Malware Domain Blocklist	Fair	Good	Excellent	Excellent	Excellent
MalwareURL	Good	Good	Excellent	Excellent	Excellent
DSHIELD	Excellent	Fair	Good	Excellent	Excellent
Google Safe Browsing Alerts	Good	Fair	Good	Excellent	Good
HoneySpider Network (as a service)	Excellent	Fair	Good	Fair	Excellent
AusCERT	Good	Good	Good	Good	Excellent
Cert.br data feed	Good	Good	Fair	Good	Good
FIRE	Good	Good	Fair	Good	Good
Team Cymru - TC Console	Excellent	Good	Good	Excellent	Excellent
EXPOSURE	Good	Good	Excellent	Good	Excellent
AmaDa	Excellent	Good	Excellent	Fair	Excellent
Malware Domain List	Excellent	Good	Excellent	Good	Excellent
Zeus/SpyEye Tracker	Good	Excellent	Excellent	Fair/Good	Excellent
The Spamhaus Project Datafeed	Excellent	Good	Good	Excellent	Good
Shadowserver Foundation	Good	Good	Excellent	Good/Excellent	Excellent
SGNET	Good	Excellent	Good	Fair	Good
ARAKIS	Good	Good	Excellent	Good	Excellent
Malc0de database	Excellent	Good	Excellent	N/A	Excellent
ParetoLogic URL Clearing House	Excellent	Good	Good	N/A	Good
SpamCop	Excellent	Good	Good	Excellent	Good
Arbor ATLAS	Good	Good	Excellent	Excellent	Excellent
CBL (Composite Blocking List)	Excellent	Excellent	Fair/Good	Excellent	Good
Cert.br Spampots	Excellent	N/A	Good	Fair	Fair
Team Cymru's CAP	Good	Excellent	Excellent	Excellent	Good
Project Honeypot	Good	Good	Excellent	Excellent	Good/Excellent
Malware Threat Center	Good	Fair	Excellent	Fair	Good
Smart Network Data Services	Good	Good	Excellent	Excellent	Good
Malware Patrol	Excellent	N/A	Excellent	N/A	Excellent
Zone-H	Excellent	Excellent	Good	Good	Fair/Excellent
Cisco IronPort SenderBase	Excellent	Good/Excellent	Excellent	Excellent	Good

Top 5 recommended external sources

- Shadowserver foundation
  (http://www.shadowserver.org)
- Zeus/SpyEye Tracker
  (https://spyeyetracker.abuse.ch, https://zeustracker.abuse.ch)
- Google Safe Browsing Alerts
  (http://safebrowsingalerts.googlelabs.com)
- Malware Domain List
  (http://www.malwaredomainlist.com/)
- Team Cymru's CSIRT Assistance Program
  (http://www.team-cymru.org/Services/CAP/)

Summary of internal tools

Category	Timeliness	Accuracy of results	Ease of use	Coverage	Resources required	Scalability	Extensibility
Client honeypot	Excellent	Fair-Excellent	Fair/ Good	Fair/ Good	Good	Excellent	Fair
Server honeypot	Excellent	Good	Good	Good	Good	Good	Good
Firewalls	Excellent	Fair	Good	Fair/ Good	Good	Excellent	Fair- Excellent
IDS/IPS	Excellent	Good	Good	Fair- Excellent	Fair/ Good	Good	Fair- Excellent
Netflow	Excellent	Good	Fair	Fair/Good	Fair	Good/ Excellent	Good
Sandboxes	Excellent	Fair/ Good	Fair	N/A	Fair	Fai- Excellent	Fair- Excellent
Darknet	Excellent	Good	Fair	Fair- Excellent	Fair	Good	Fair
Passive DNS monitoring	Excellent	Good/ Excellent	Good	Fair/ Good	Good	Good/ Excellent	Fair
Spamtrap	Excellent	Fair/ Good	Fair	Fair	Good	Good	Good
Web Application Firewalls	Excellent	Good/ Excellent	Fair	Fair	Fair	Good	Good
App logs	-	-	-	-	-	-	-
Antivirus	Excellent	Good	Good	Fair- Excellent	Good	Good	N/A

Recommended tools

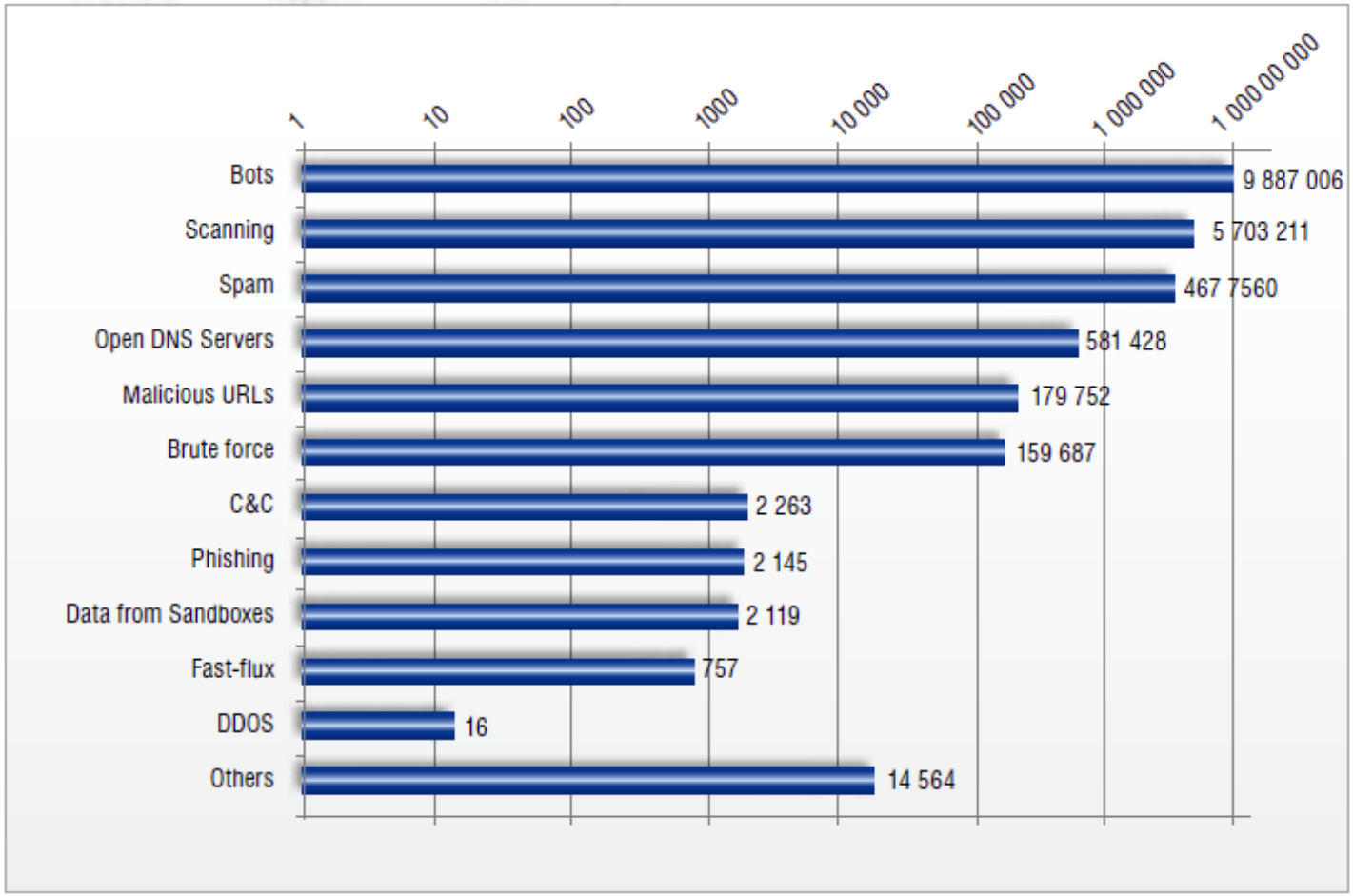
Tools divided in 3 groups

- Standard
  - Often by design part of network and available for use by CERTs
  - Examples: routers, firewalls, antivirus systems, IDS/IPS systems, netflow and various kinds of logs
- Advanced
  - Beyond the standard networking tools. Additional resources may be required
  - Examples: darknets, server honeypots, spamtraps and networks of sensors
- Upcoming
  - Even more resources and skills needed.
  - Examples: client honeypots, sandboxes, passive DNS analysis techniques

Study impact

What changed for CERT Polska?

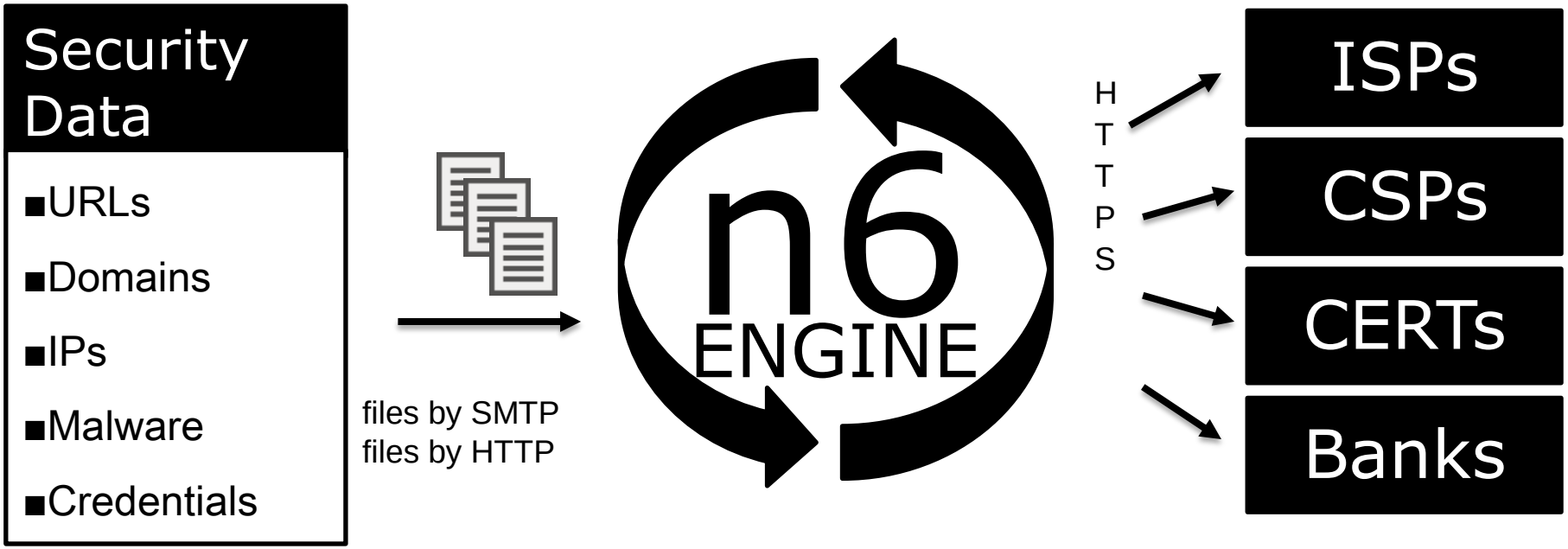
Incidents for Poland: 2011



Tools for correlation & sharing

- Abuse Helper (http://www.abusehelper.be/)
- Megatron (contact SITIC/CERT.se)
- Collective Intelligence Framework (http://code.google.com/p/collective-intelligence-framework/)
- n6 by CERT Polska (currently in beta)

n6 PLATFORM


Security Data
URLs
Domains
IPs
Malware
Credentials
files by SMTP
files by HTTP
n6
ENGINE
HTTPS
ISPs
CSPs
CERTs
Banks

n6 What we share

Aggregated sources:

- our systems (ARAKIS, HSN, internal tools ...)
- external organizations - major data providers covered in this report & closed ones

Types of data

malicious URLs	scanning	brute force
malicious artifacts	C&C servers	fast flux
infected hosts (bots)	DDoS	phishing

Some open questions …

- Why are CERTs not interested in obtaining free information about problems in their constituency?
- Why are CERTs not interested in sharing data?
- Why do CERTs not deploy tools for automated sharing of incidents?

Recommendations for improvements

Data providers

- Identification and vetting of data consumers
  - Establish contacts with relevant communities
  - Do screening of data recipients
  - Easy process of registration
- Data format and distribution
  - Adapt existing standards and methods whenever possible
  - Provide complementary data usable for correlation (eg, timestamps, incident type)
  - Provide data timely
  - Provide description on how the data is obtained
- Data quality enrichment
  - Filter, correlate, verify to reduce false positives
  - Provide feedback mechanisms
  - Implement and explain principles of data aging and removal
  - Assign confidence levels to data
  - Keep aggregated data to analyse trends and patterns, enrich data with statistical information

Recommendations for improvements

Data consumers

- Acquire access to datasets
  - Review and consider usage of sources, tools recommended here
  - Develelop own monitoring capabilities
  - Establish relationships with relevant communities (eg, FIRST, TF-CSIRT)
  - Consider what data can be shared with others
- Integrate external data feeds with incident handling systems
  - Try to be flexible and prepared to handle different formats
  - Store data in a way which would help to provide correlation, analysis, visualisation
  - Correlate, verify with data from internal monitoring systems
- Verify quality of data feeds
  - Correlate, filter, enrich data; group related incident reports
  - Give feedback to data providers
- When possible improve internal monitoring capabilities possibly becoming data provider
  - More you are ready to give – more you can expect to get back

Recommendations for improvements

EU and national level

- Facilite wider usage of underused technologies
- Encourage the adoption of common standards for the exchange of incident information
- Integrate wide scale statistical incident data
  - perform long term analysis and correlation
  - produce reports, research materials, advisories and predictions
- How to improve reporting of data leaks to victims?
- How to reach the balance between privacy protection and security provision needs ?

CONTACT DETAILS

European Network and Information Security Agency (ENISA)
Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece

cert-relations@enisa.europa.eu

CERT Polska/NASK

ul. Wąwozowa 18, 02-796

Warsaw, Poland

n6@cert.pl

REPORT:
http://www.enisa.europa.eu/activities/cert/support/proactive-detection