



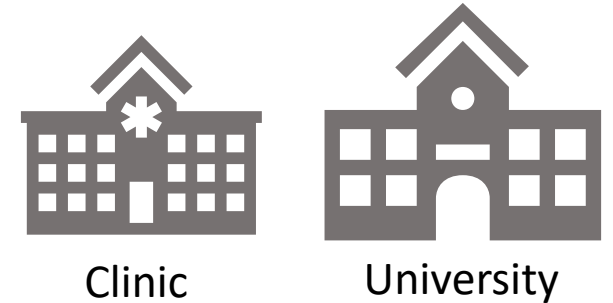
A three-stage machine learning cybersecurity solution for public entities

Dr. Stanisław Saganowski
stanislaw.saganowski@pwr.edu.pl

Wroclaw Centre for Networking and Supercomputing,
Wrocław University of Science and Technology,
Wrocław, Poland

Problem

- Value at risk globally from cyberattacks:
US\$5.2 trillion (2019-2023) [1]



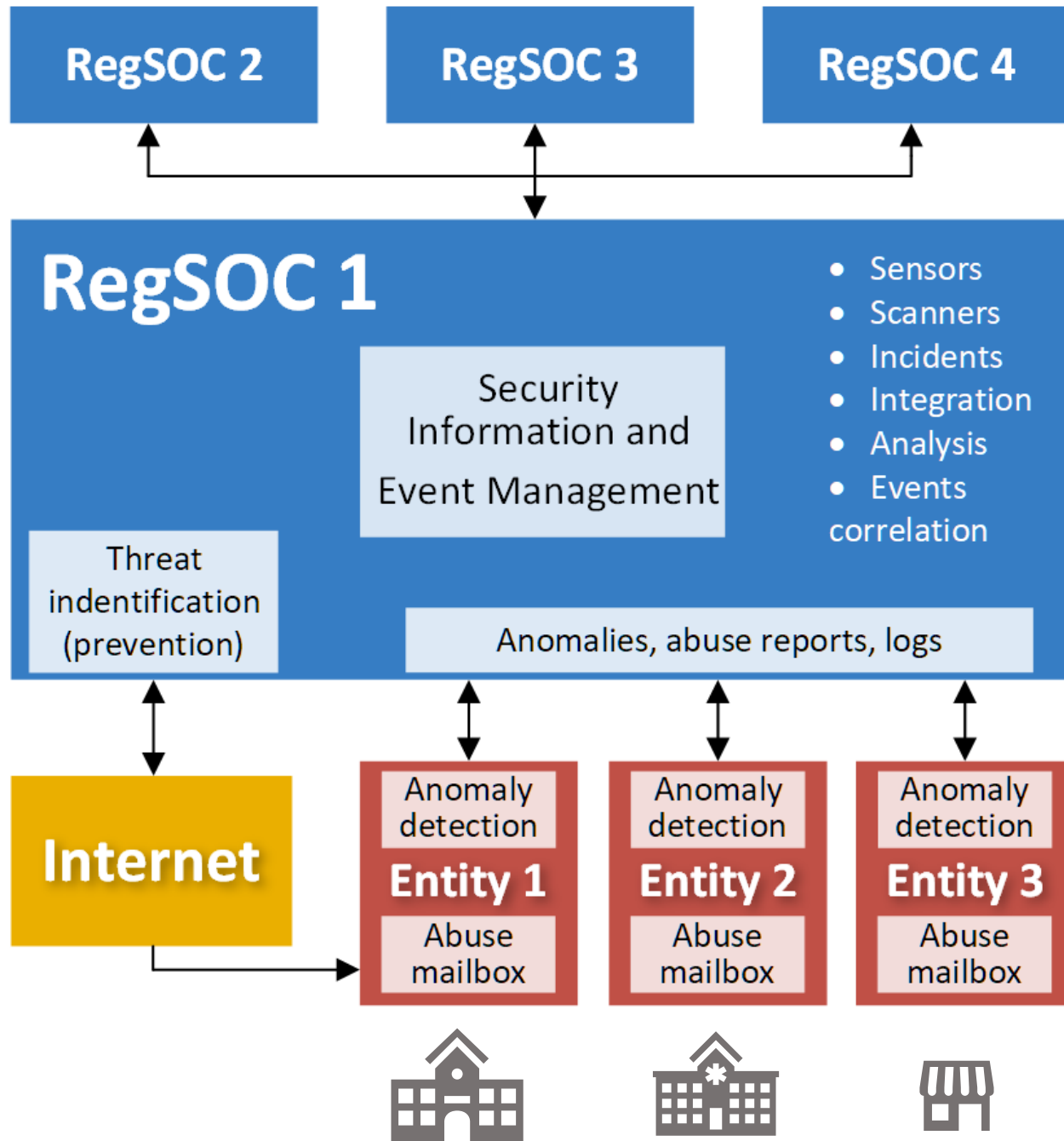
- Small entities can't afford own Security Operation Centers
- Security outsourced to service providers
- Custom infrastructure, physical installation and contact

1. Ninth Annual Cost of Cybercrime Study, March 6th 2019, <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>

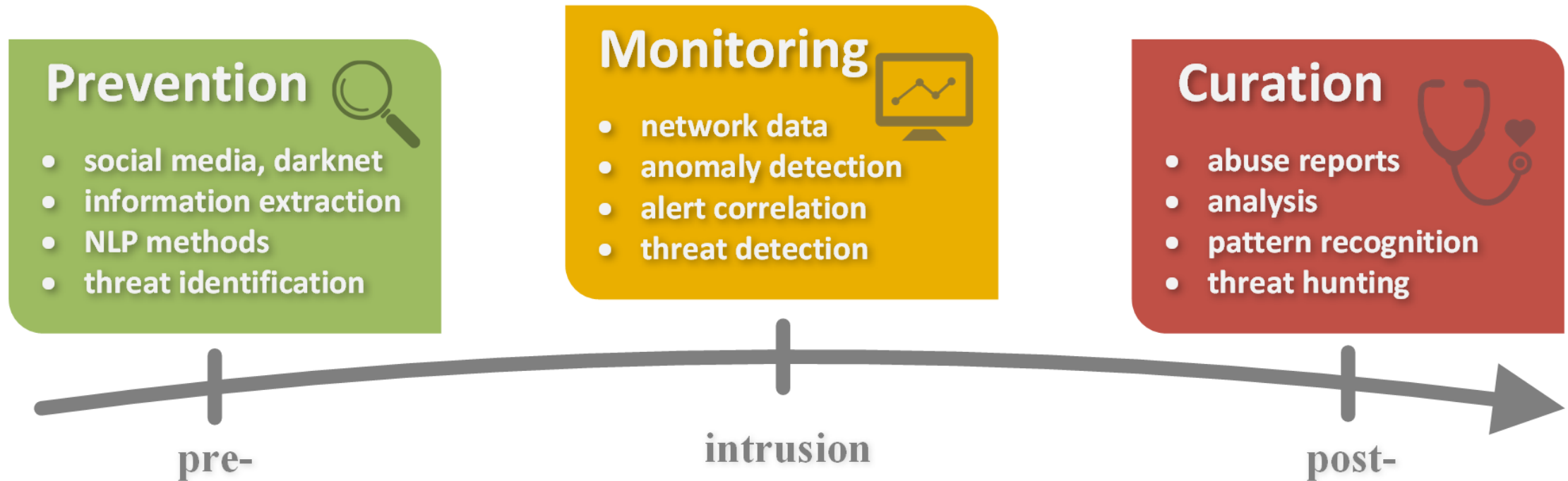
RegSOC initiative

- RegSOC: Regional Center for Cybersecurity
 - Financed by the Polish Ministry of Digital Affairs
 - Targets small entities
 - Operates locally, learns globally
 - **Open-source**
-
- Deadline: March 2021



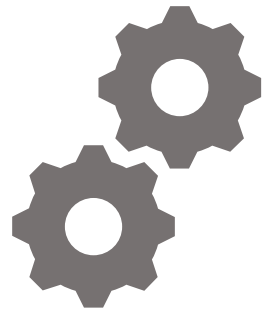


A three-stage security solution



Stage 1: Prevention

- Threat identification
- Social media, news portals, Darknet
- Natural Language Processing
- Software-, system-, device-related security issues (vulnerability, exploit, patch), new malware or hacking methods



Examples: Twitter

THN The Hacker News @TheHackersNews Follow

Important→ Someone hacked the official site of #PHP PEAR and replaced package manager (go-pear.phar) with a "tainted version"

[thehackernews.com/2019/01/php-pe ...](https://thehackernews.com/2019/01/php-pe...)

If you have downloaded/updated #pearPHP package manager from its official site in past 6 months, consider yourself compromised.



1:49 AM - 23 Jan 2019

271 Retweets 204 Likes

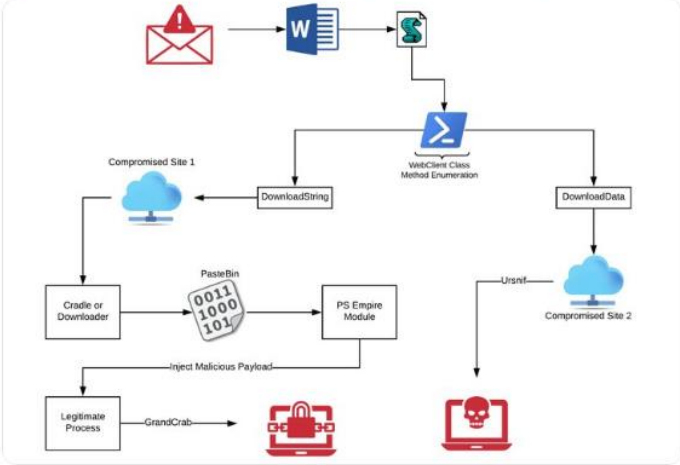
6 271 204

THN The Hacker News @TheHackersNews Follow

New malware campaigns spotted in the wild, using malicious Microsoft Office docs to infect PCs with GandCrab #ransomware and Ursnif info-stealer #malware

[thehackernews.com/2019/01/micros ...](https://thehackernews.com/2019/01/micros...)

#powershell #hacking #cybersecurity #infosec



3:35 AM - 25 Jan 2019


237 Retweets 215 Likes

Carbon Black, Inc. and Cisco Talos Intelligence Group

1 237 215

Examples: Darknet

[SELL] Medical Fullz Databases - 67.000 Records Thread Modes



thedarkoverlord •
Junior Member
Progress: 33%

Posts: 15
Threads: 4
Reputation: 0
Level: 2 [👤👤👤]
Total Points: 4
Rank 4 / 40
91% to upload Level
Activity 4 / 4
3% to upload your Rank
Experience 62
38% to upload Experience

09-19-2018, 08:21 PM # 1

You know who we are. We're **thedarkoverlord**. We hack only the best targets. Today, we're bringing you something delicious and special.

Up for grabs today are several medical practises that we've hacked and stolen their databases. The databases contain **PII and PHI**. This is **SSN/DOB** and much more.

The prices are undisclosed and negotiable. If you want to buy copies of the databases that no one else will have then the price will be higher. We will use the escrow service if desired and the escrow team will confirm our products.

For your own privacy, please PM us and use PGP. You'll find our key on our profile.

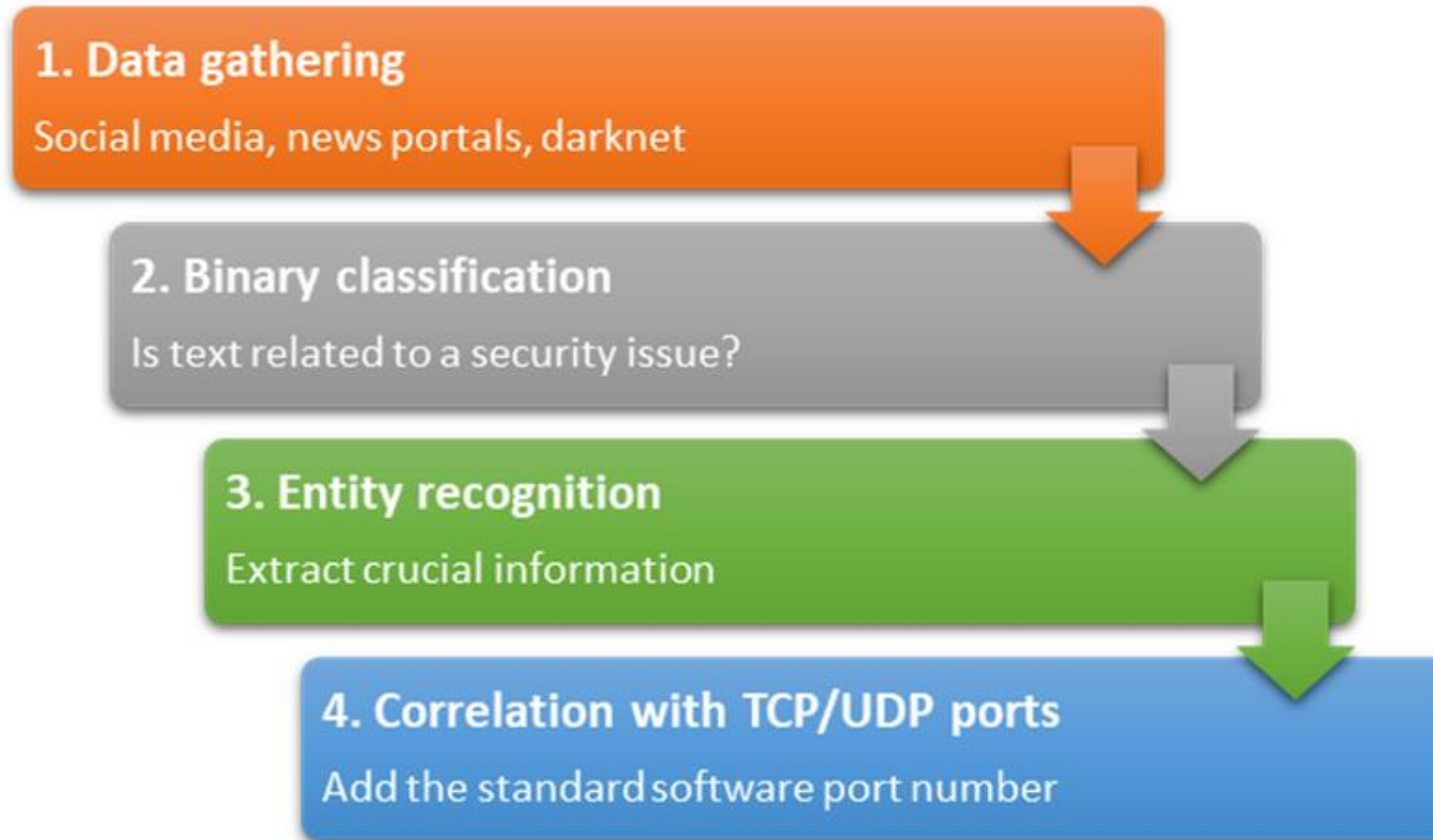
1. New York Dentistry - 3.000 Records

Tables

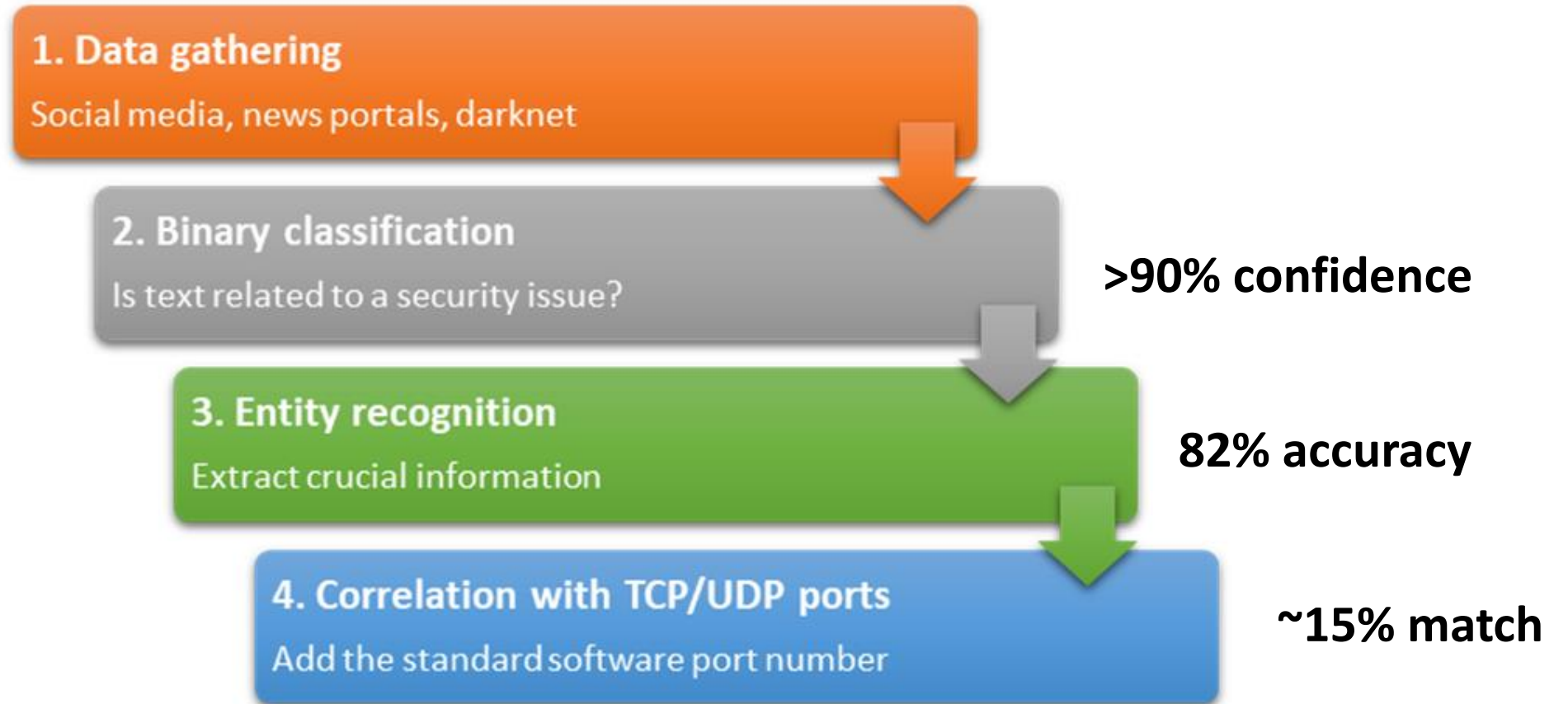
Code:

```
LName, FName, MI, MIPrefName, Gender, Status, FamPos, BirthDate, FirstVisit, WPhone, WExt, SS, MedAlerts, Salutation, Title, Other ID, Street, Street2, City, State, Zip, HPhone, Guar_LName, Guar_FName, Aging_0, Aging_30, Aging_60, Aging_90, Billing_Type, Balance, LastPayDate, LastPayAmt, PP_Total, PP_Balance, PP_Payment, PP_Payment_Date, Prov_Name, Prov_Title, Emp_Name, Emp_Add1, Emp_Street2, Emp_Add2, Emp_Phone, PIns_Name, PIns_RemBenf, SIns_Name, SIns_RemBenf, RefTo_Name, RefTo_Add1, RefTo_Street2, RefTo_Add2, RefTo_Phone, RefTo_Date, RefTo_FName, RefTo_MI, RefTo_Salutation, RefBy_Name, RefBy_Add1, RefBy_Street2, RefBy_Add2, RefBy_Phone, RefBy_FName, RefBy_MI, RefBy_Salutation, LastVisit, LastRef, RefBy_Title, RefTo_Title, RefBy_Email, RefTo_Email, Appt_Date, Appt_Time, Appt_Reason, Appt_Name, Appt_Provider, Appt_Phone, Appt_Add1, Appt_Street2, Appt_Add2, CC_DueDate, CC_TypeName, CC_TypeDesc, CC_PriorWorkDate, CC_StatusType, CC_StatusDesc, CC_ApptDate, CC_ApptTime, CC_ApptReason, CC_ApptProv, EMailAddress, DriversLicense, Fax, Pager, OtherPhone, Fee_Sched, LastMissedApptDate, CC_Note, PIns_GroupName, PIns_Address, PIns_Address2, PIns_CitySTZip, PIns_Phone, PIns_PhoneExt, PIns_Contact, SIns_GroupName, SIns_Address, SIns_Address2, SIns_CitySTZip, SIns_Phone, SIns_PhoneExt, SIns_Contact, PMTP_Date, PMTP_FinCharge, PMTP_LateCharge, PMTP_Interval, PMTP_Balance, P
```


Threat identification: approach



Threat identification: results

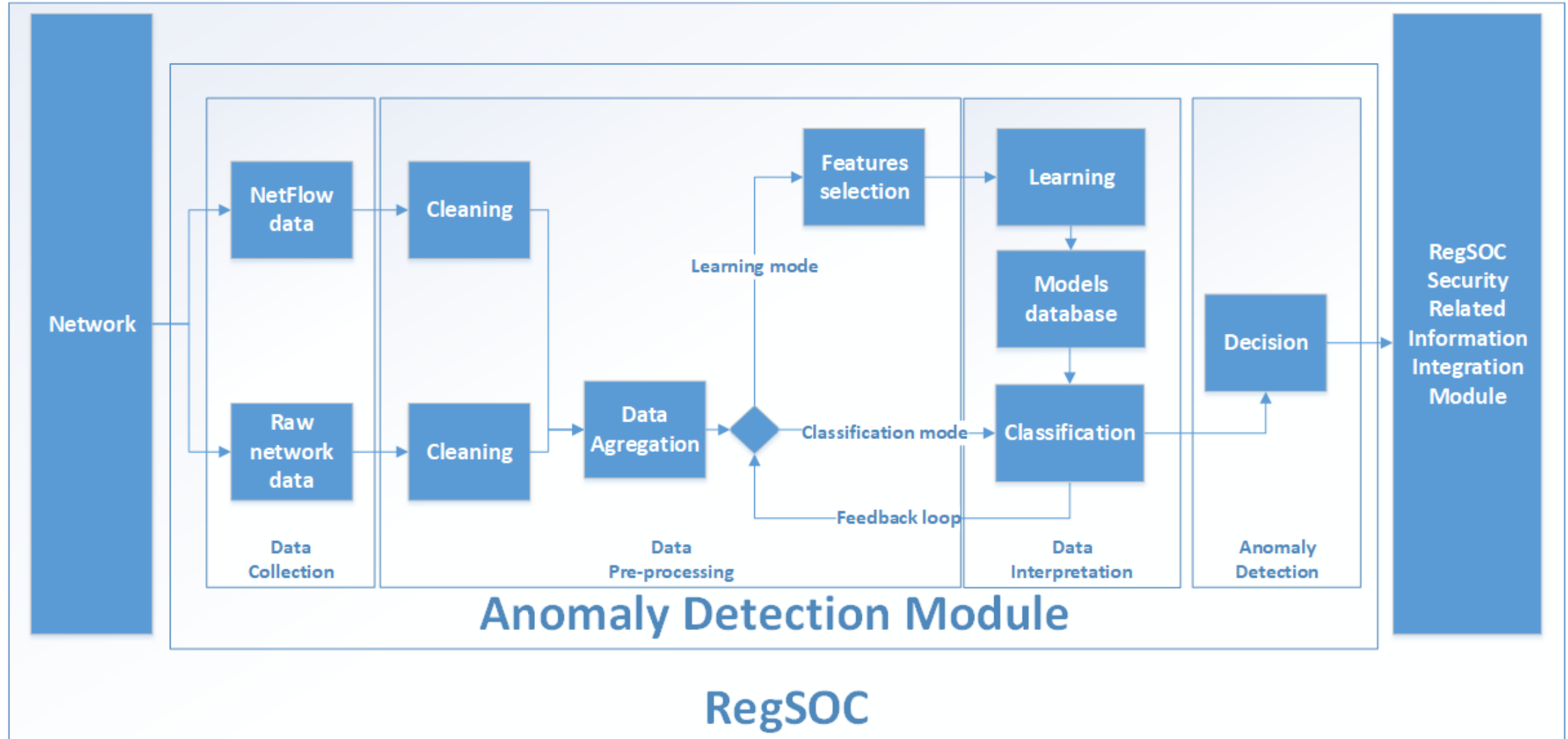


Stage 2: Monitoring

- Anomaly detection
- Up to 10 Gbps, real-time analysis
- Anonymization (GDPR)
- Deep neural network
- Modes: (1) learning; (2) classification
- Validation sets: 99% accuracy



Anomaly detection



Monitoring: other components

- Campaign identification
- Spam analysis
- Honey-net
- Nessus scanner
- Physical sensors: Intrusion Detection System, Intrusion Prevention System, honey-pots, ...



Stage 3: Curation

- Abuse reports - abuse@domain.com
- Contain: IP address, date, type of activity, logs
- Activity: port scanning, login attacks, spam emitting, etc.
- Ignored by admins (unstructured, not standardized)
- Wrocław Academic Computer Network: 15k IPs, 3 years, 7k reports
- Regex + pattern recognition + heuristics



Dear Sir/Madam,

We have detected abuse from the IP address (156. [redacted]), which according to a whois lookup is on your network. We would appreciate if you would investigate and take action as appropriate. Any feedback is welcome but not mandatory.

Log lines are given below, but please ask if you require any further information.

(If you are not the correct person to contact about this please accept our apologies - your e-mail address was extracted from the whois record by an automated process. This mail was generated by Fail2Ban.)

IP of the attacker: 156. [redacted]

You can contact us by using: [redacted]

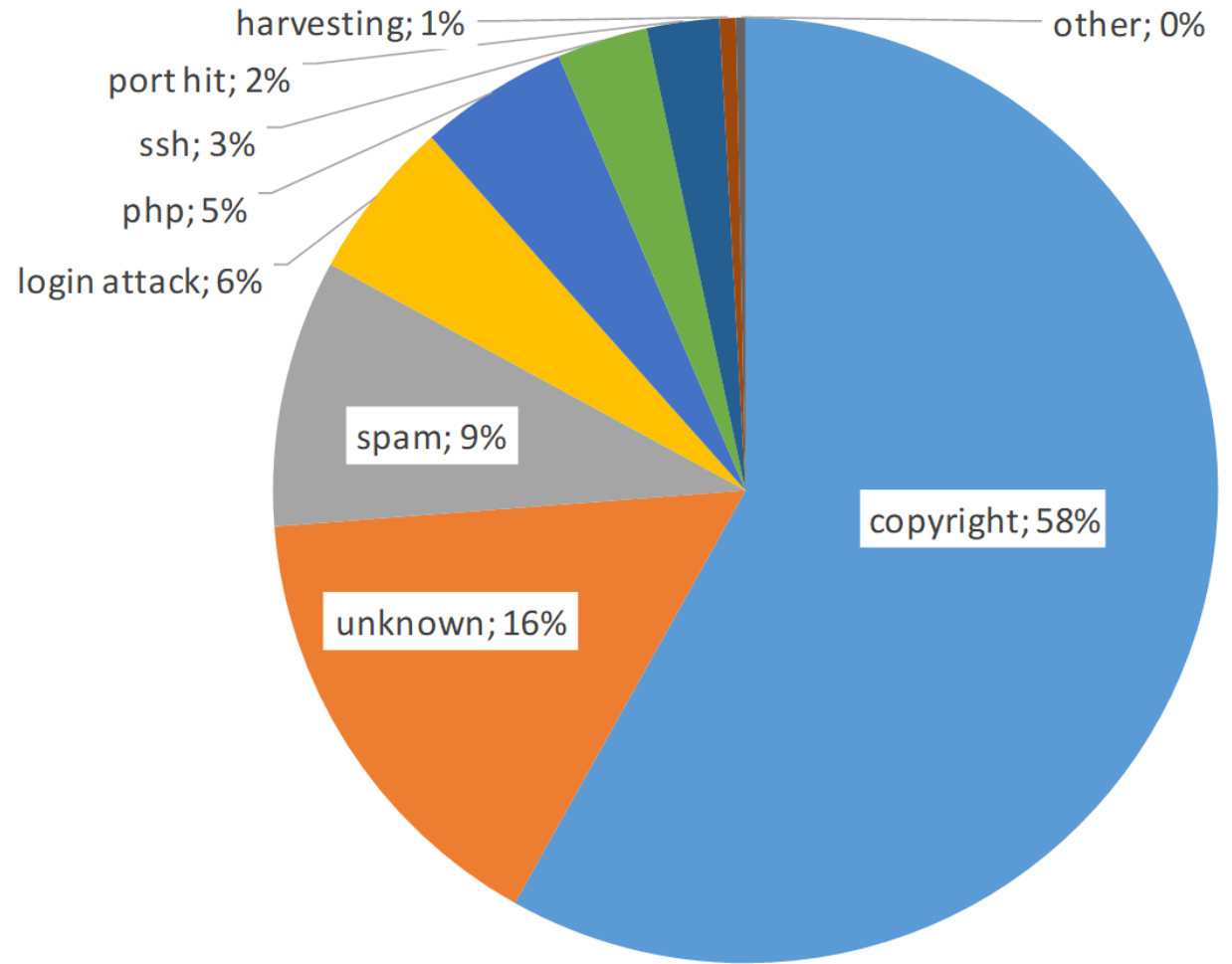
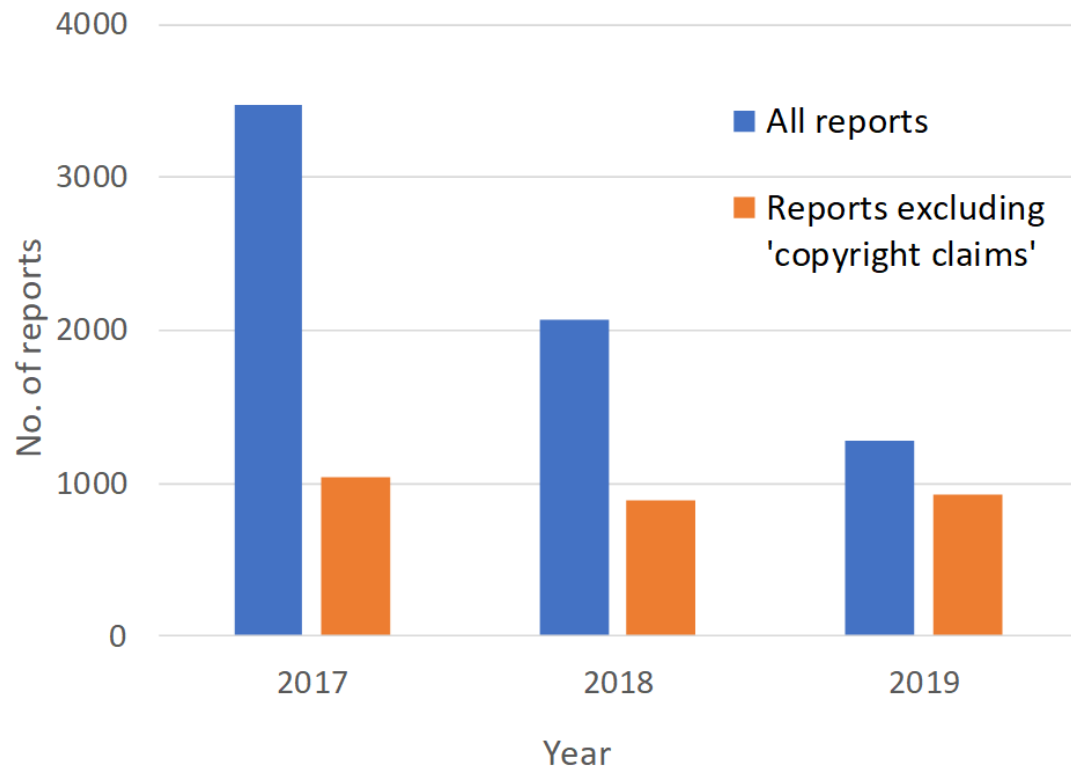
Addresses to send to:
abuse@wask.wroc.pl

===== Excerpt from log for 156. [redacted] =====

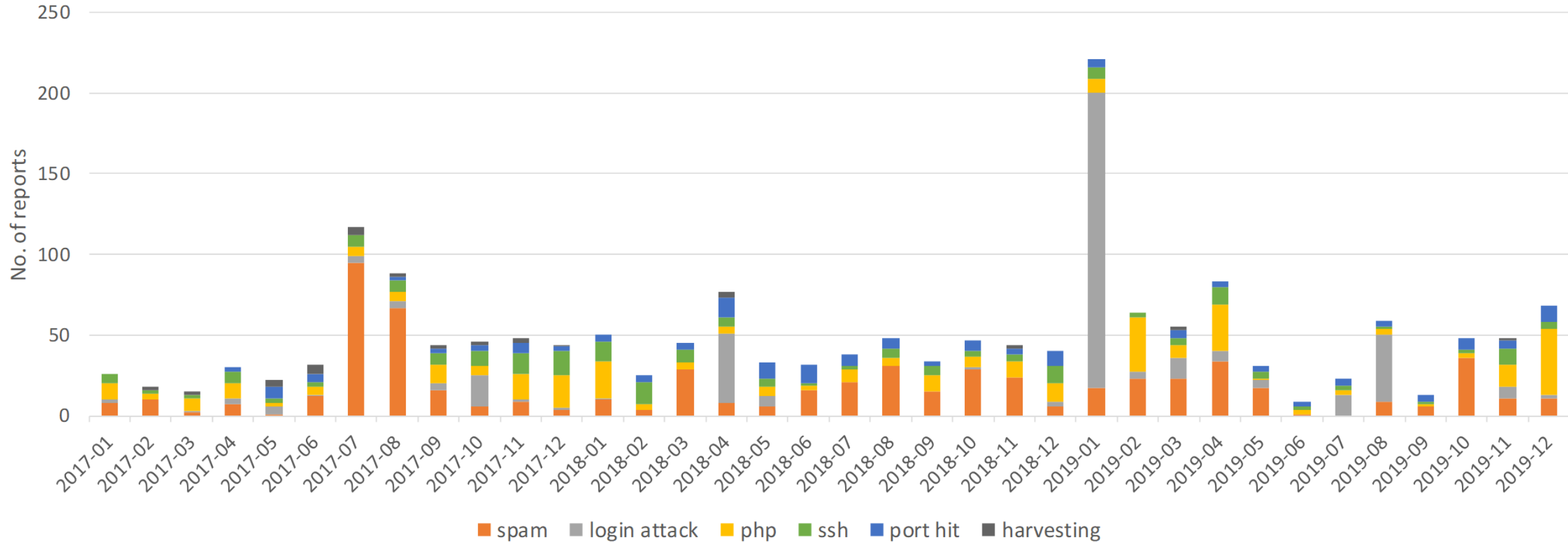
Note: Local timezone is [redacted]

```
Jan [redacted] shared01 sshd[ [redacted] ]: Invalid user [redacted] from 156. [redacted]
Jan [redacted] shared01 sshd[ [redacted] ]: pam_unix(sshd:auth): authentication failure; logname= uid=0
euid=0 tty=ssh ruser= rhost=156. [redacted]
Jan [redacted] shared01 sshd[ [redacted] ]: Failed password for invalid user [redacted] from 156. [redacted] port
35322 ssh2
Jan [redacted] shared01 sshd[ [redacted] ]: Received disconnect from 156. [redacted] port 35322:11:
Normal Shutdown, Thank you for playing [preauth]
Jan [redacted] shared01 sshd[ [redacted] ]: Disconnected from 156. [redacted] port 35322 [preauth]
```

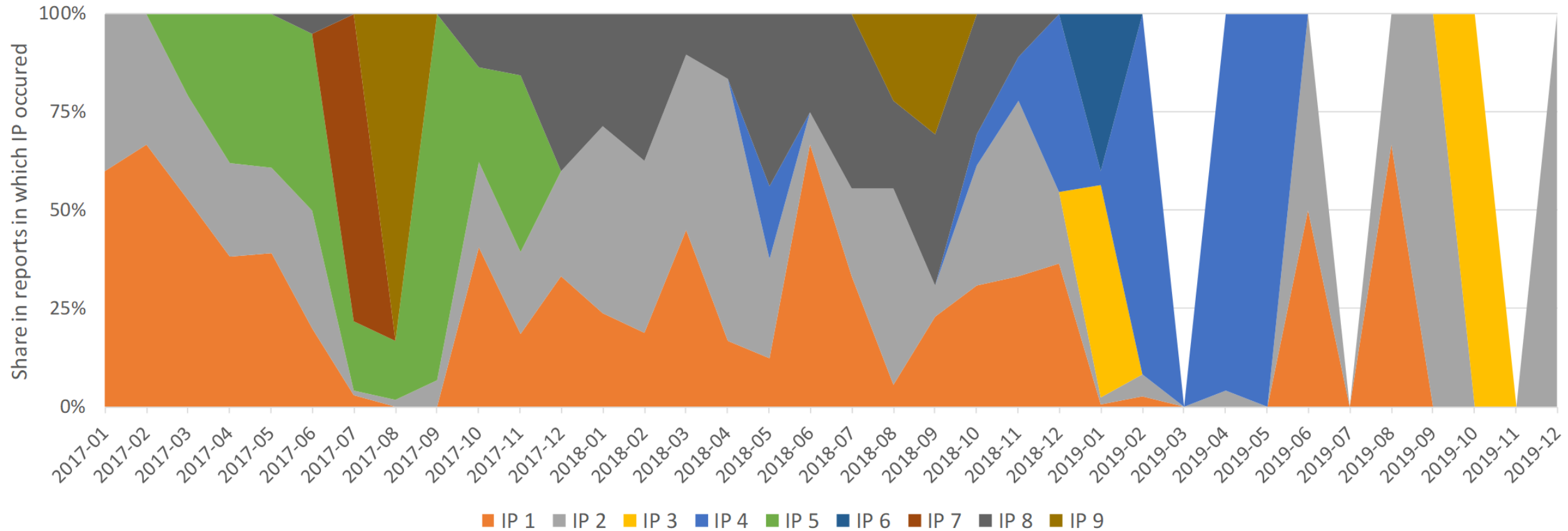
Abuse mails (1)



Abuse mails (2)



Abuse mails (3)



Summary

- RegSOC for small entities
- Threat identification (Internet)
- Real-time threat detection (local network)
- Threat hunting – abuse reports
- Open-sourced in March '21



Thank you!

Questions?

This presentation was created as a part of the Regional Security Operations Center (RegSOC) project (Regionalne Centrum Bezpieczeństwa Cybernetycznego), co-financed by the National Centre for Research and Development as part of the CyberSecIdent - Cybersecurity and e-Identity program.



Dr. Stanisław Saganowski

stanislaw.saganowski@pwr.edu.pl

Wrocław Centre for Networking and Supercomputing,
Wrocław University of Science and Technology,
Wrocław, Poland



Wrocław University
of Science and Technology