RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Anti-Abuse Training

Setting up an abuse desk

Webinar

RIPE NCC Learning & Development

This session is being recorded

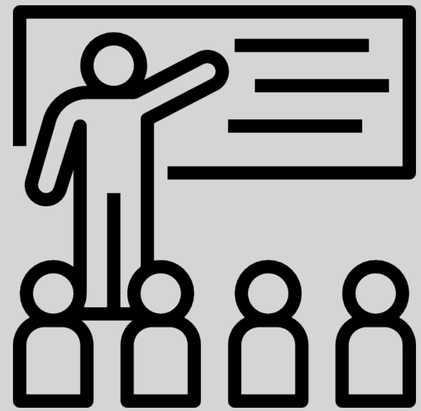
Take the poll!

Do you already have an **Abuse Desk** in your organisation?

1 min.

Agenda

- What is abuse?
- What should I do about it?
- What is an Abuse Desk?
- Setting up an Abuse Desk
- Some help with abuse handling
- And now what?



What is abuse?

Ethics and the Internet

RFC 1087: Ethics and the Internet

- Published way back in **January 1989**
- **Unethical** and **unacceptable** activities are those that:
  - Seek to gain unauthorised access
  - Disrupt the intended use
  - Waste resources (people, capacity, equipment)
  - Destroy the integrity of computer-based information
  - Compromise the users of the Internet
- What do we think **today** about these definitions?

Let’s Talk About Abuse

- It is **difficult to define abuse** because it depends on…
  - National legislation
  - Cultural background
  - Your personal point of view, e.g. experience, expertise and opinion

- What are the **main** characteristics of ABUSE?

Well-Known Types of Abuse

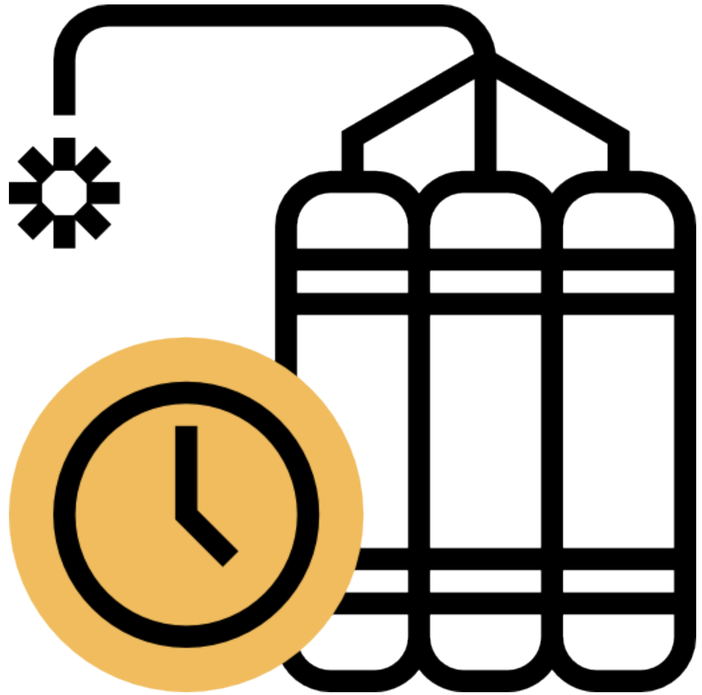
- **Abuse** you might encounter includes:
  - Spam
  - General fraud
  - DDoS attacks
  - Malware
  - Phishing
  - Abuse of an open service (email, DNS, etc.)
  - Copyright/trademark infringements
  - CSAM (Child Sexual Abuse Material)*

Take the poll!

If you have ever been the **recipient** of abuse, what **type of abuse** was it?

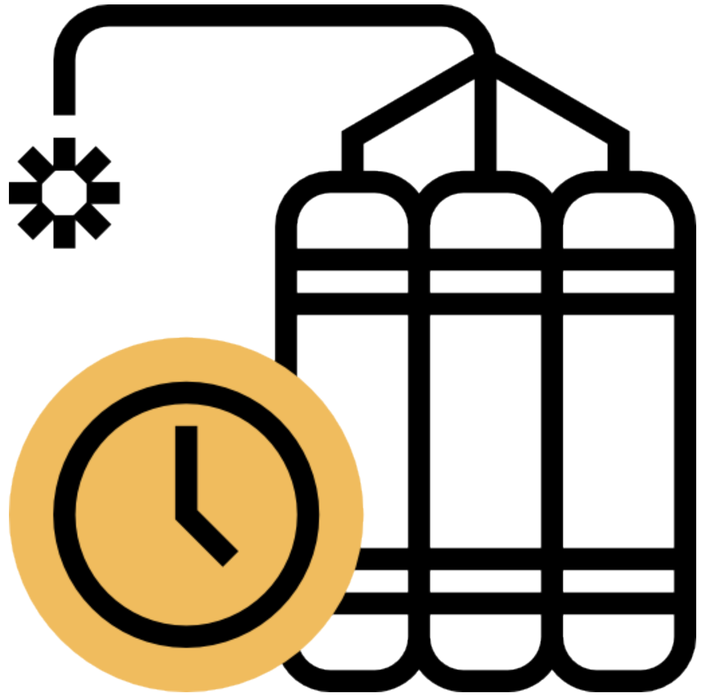
1 min.

Effects of Abuse



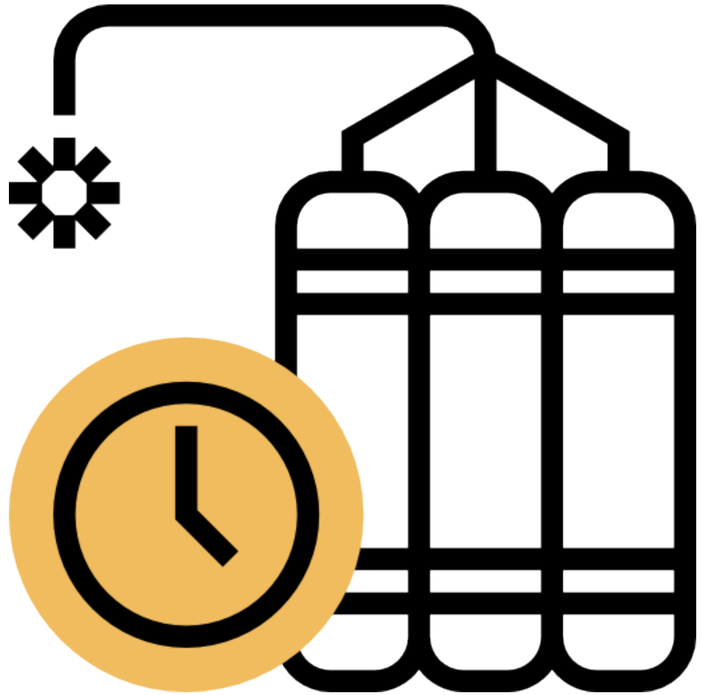
Effects of Abuse

- Abuse causes **damage** and **downtime** for networks



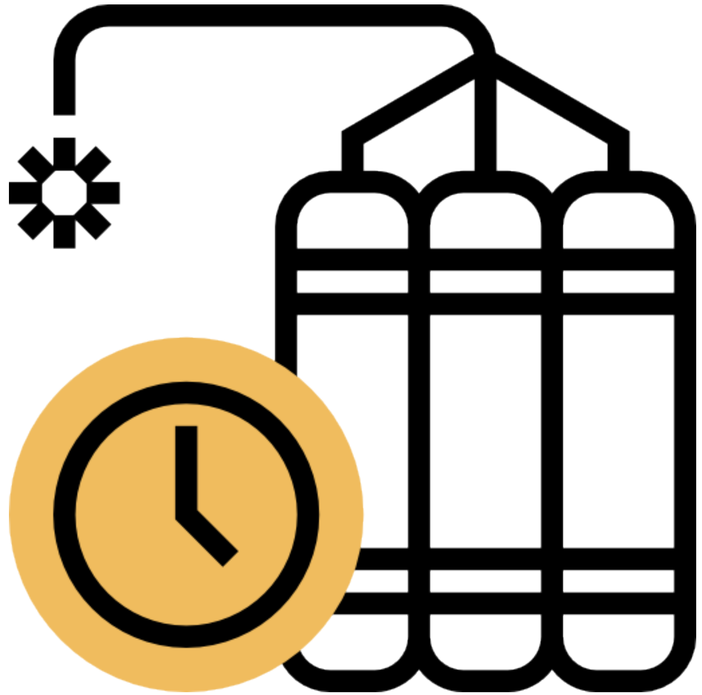
Effects of Abuse

- Abuse causes **damage** and **downtime** for networks
- Businesses **lose** business



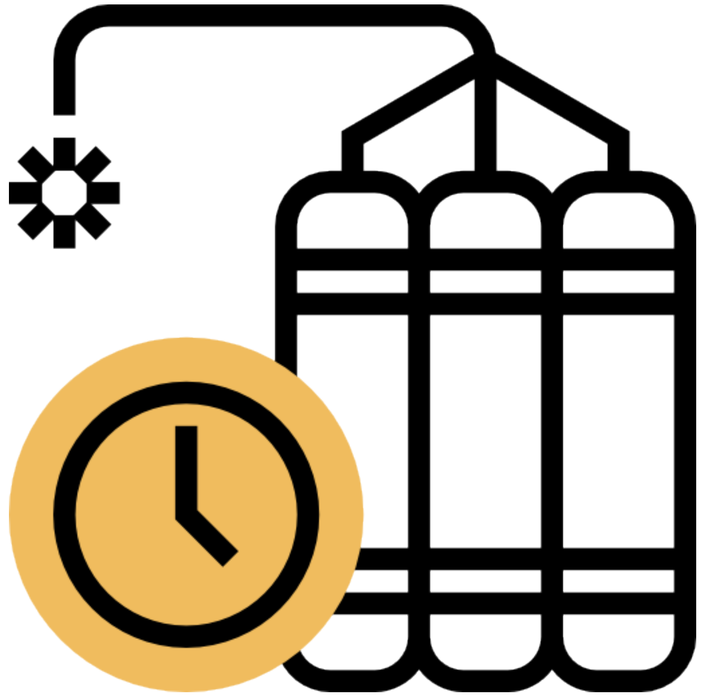
Effects of Abuse

- Abuse causes **damage** and **downtime** for networks
- Businesses **lose** business
- People **suffer** the consequences



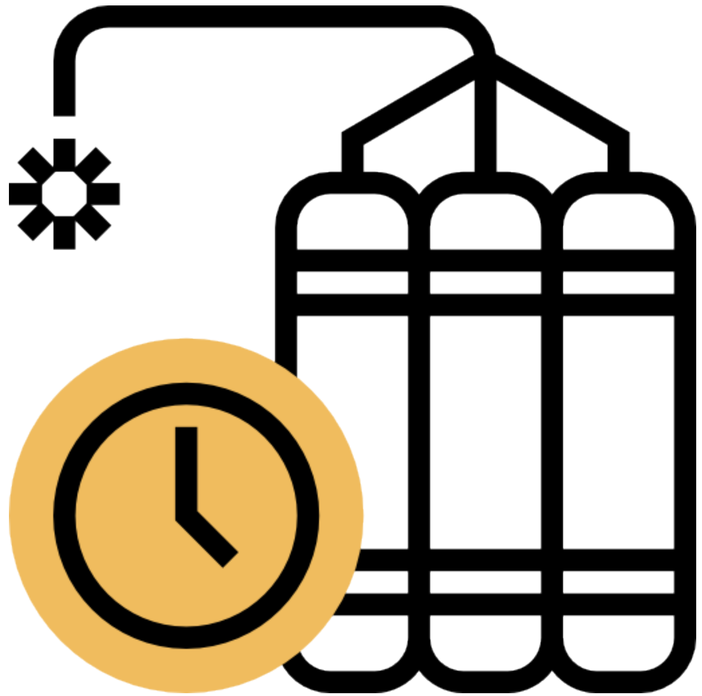
Effects of Abuse

- Abuse causes **damage** and **downtime** for networks
- Businesses **lose** business
- People **suffer** the consequences
- Trust in your network is **eroded**



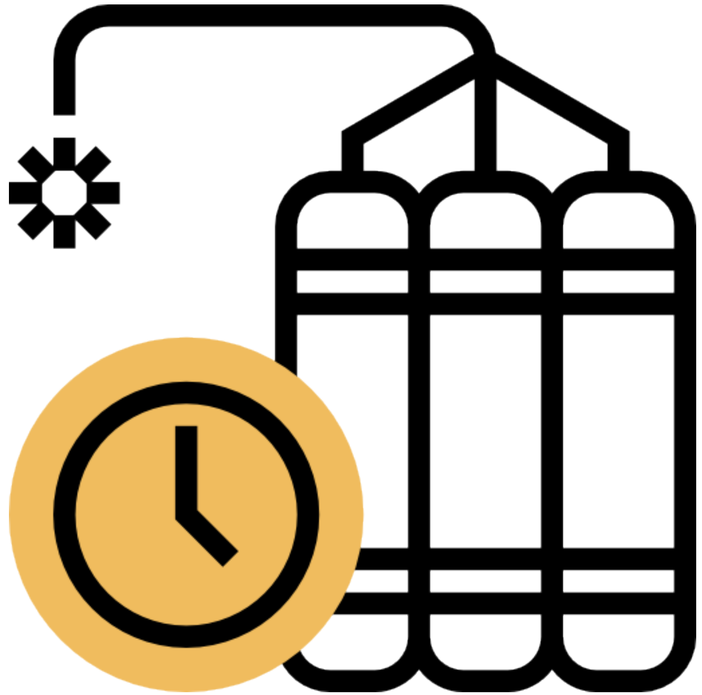
Effects of Abuse

- Abuse causes **damage** and **downtime** for networks
- Businesses **lose** business
- People **suffer** the consequences
- Trust in your network is **eroded**
- Your internal costs **increase**



Effects of Abuse

- Abuse causes **damage** and **downtime** for networks
- Businesses **lose** business
- People **suffer** the consequences
- Trust in your network is **eroded**
- Your internal costs **increase**
- Legal **risks**

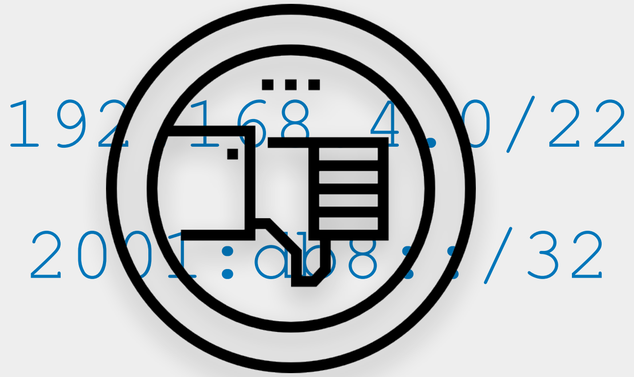


Your IP Reputation

- Helps **evaluate** the quality of an IP address
  - Can be an individual IP or a whole prefix

- A **negative reputation** will likely decrease the traffic you can send and receive

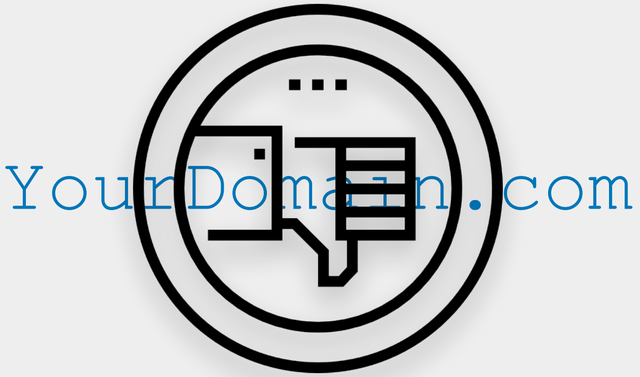
- **Monitoring changes** to your reputation helps to detect abuse



Your Domain Reputation

- Works on a **scoring system**
  - Determined by factors like spam, complaint rates, bounce rates, etc
  - Every network has their own way of calculating the score

- Providers use it to **make decisions** about whether your emails should make it to the inbox or not



Blocklists

- Databases of “**known bad**” or “**suspicious**” IPs or domains
- They help to **prevent** or **block** harmful IPs or domains from accessing networks
- **Public** and **private** blocklists

What should I do about it?

Expectations and Obligations

Take the poll!

Who do you think has **expectations** about abuse being taken care of?

1 min.

The Abuse Victim Expects…

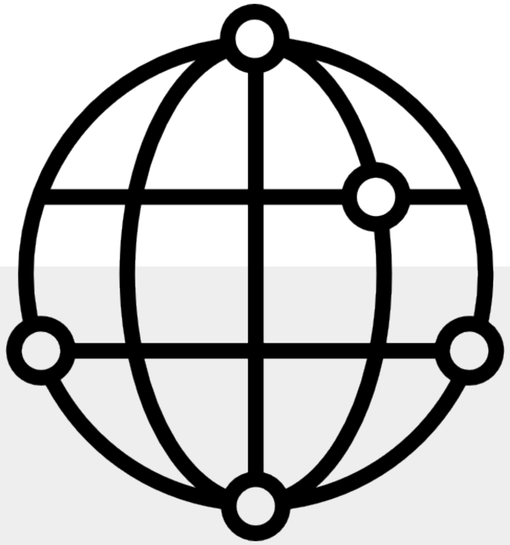
- Victims want the abuse to **stop** immediately, obviously
- They expect to be **heard/listened** to and acknowledged
- Network operators should be **ethical** and **responsible**

Your Local Authorities Expect…

- Network operators and users to follow the local **laws** and **regulations**
- **Obstacles** to abuse and cybercrime
- A **safer** information society

The Internet Community Expects…

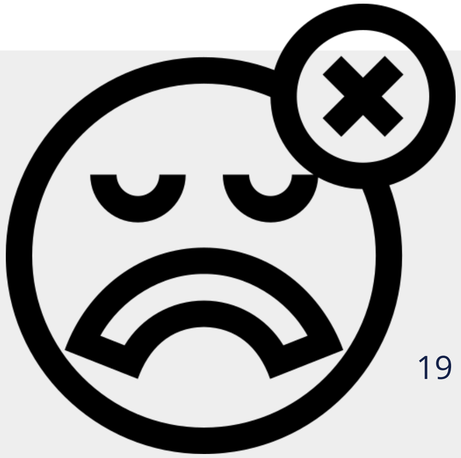
- The abuse from **your network** is causing damage:
  - Network operations degraded or disrupted
  - Financial losses or costs
- You take care of the **vulnerabilities** and **exploits**
- You **deal** with the abusive users
- You be **ethical** towards other networks
- … and **your customers**!



Why Handling Abuse is Important

- **Cybercrime** is on the rise
  - Cybercriminals use your network as part of their infrastructure

- **Consequences** of **not handling** abuse reports
  - Loss of trust in your network
  - Reduced network visibility due to filtering
  - Serious legal problems in certain cases



Why Handling Abuse is Important

- **Benefits** when you **do handle** abuse complaints
  - More stable network operations (uptime)
  - Better visibility of your network on the Internet
  - Reduce operational costs
  - Improved business due to a good reputation

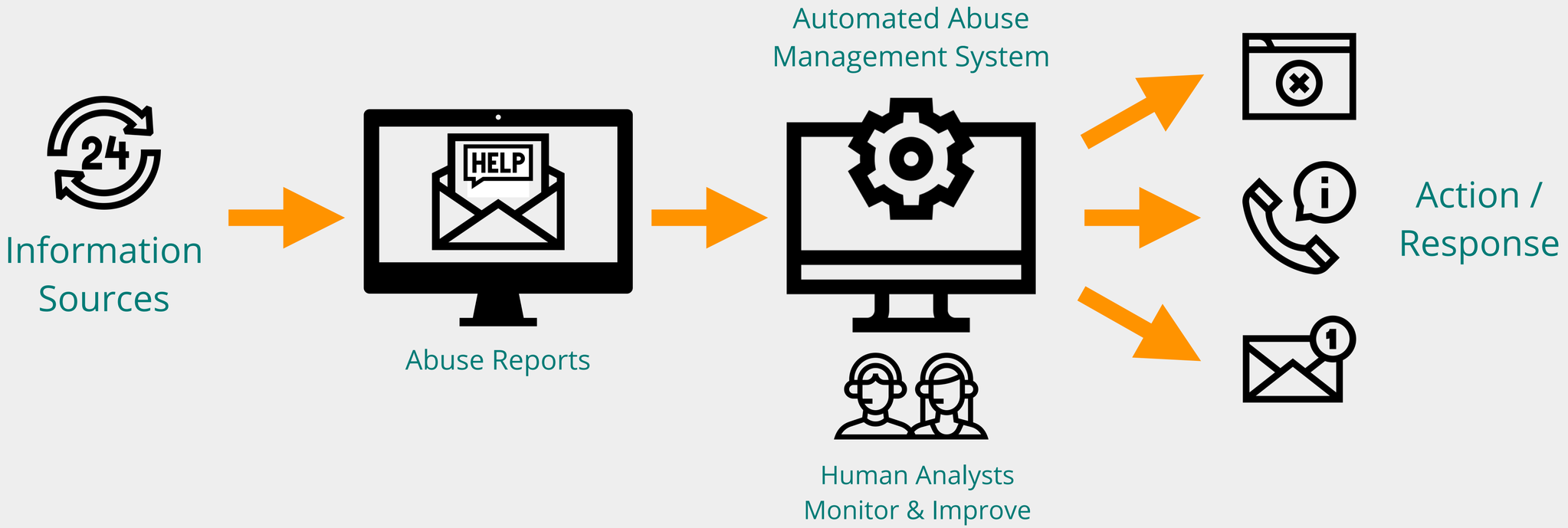
- **Clean, efficient** network = **Happy users** that don't leave!

What is an Abuse Desk?

Listen to complaints

What is an Abuse Desk?

- Usually part of the **Security Operations** function
- Ensures that complaints about IPs or domains are taken care of

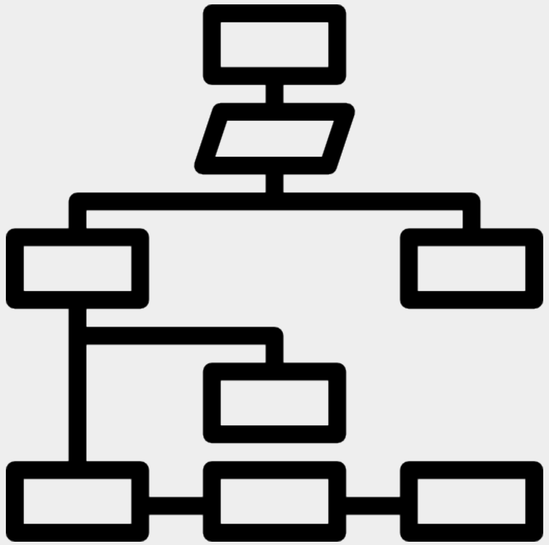


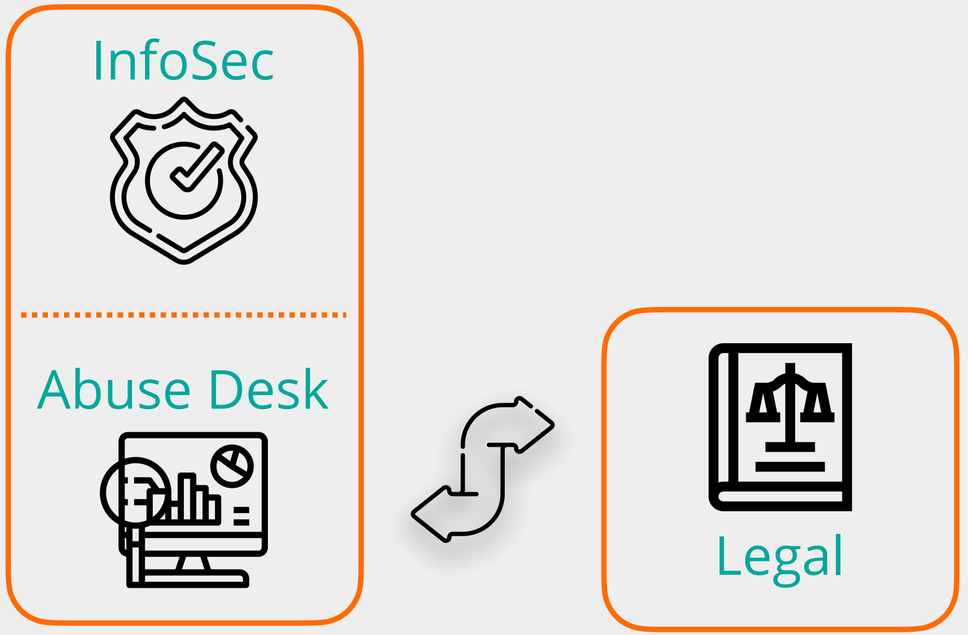
What does an Abuse Desk do?

- **Receives** and **catalogs** the abuse reports
- **Prioritises** the reports that require urgent action
- **Takes action** depending on the issue:
  - Mitigates the impact of the abuse
  - Educates on how to avoid these problems
  - Shuts off customer from the Internet, if it’s the only solution
  - Contacts LEAs if required by law

Where is the Abuse Desk found?

- ***Looks*** like a Help Desk
- But is mostly located under **Information Security**
- Has a lot of contact with the Legal dept.





Take the poll!

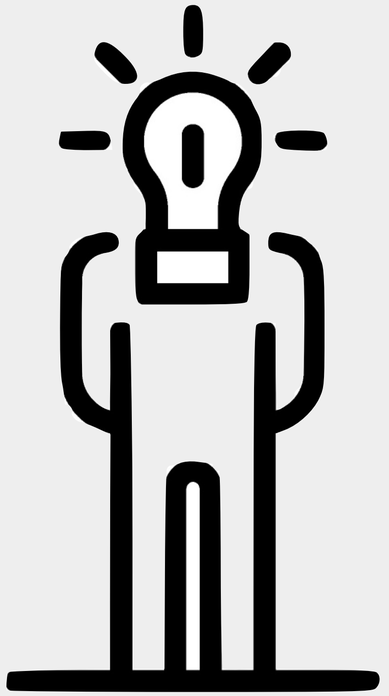
You need to have **highly skilled people** running the abuse desk.

TRUE or FALSE?

1 min.

Useful Skills You Should Have

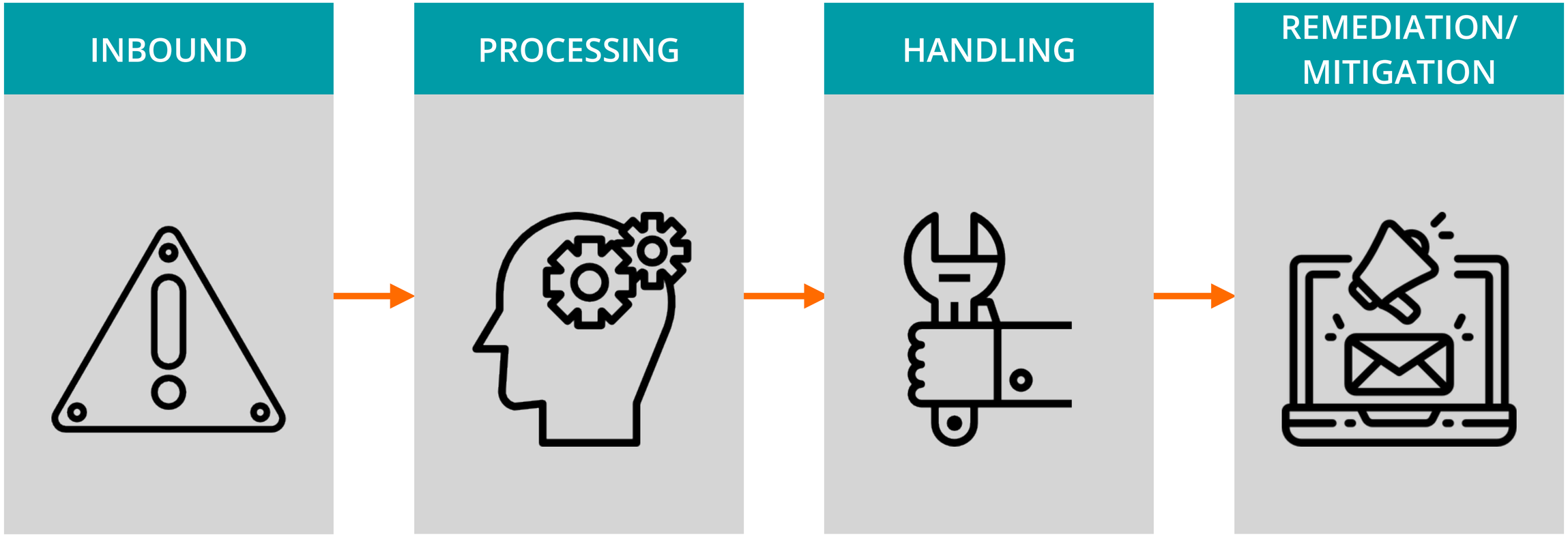
- The abuse desk doesn’t require a network engineer
- But it will **benefit** from skills such as:
  - IP addressing (IPv4 and IPv6 subnetting)
  - Basic understanding of the technologies used in the network
  - Reading log files
  - IP packet analysis
  - Among others…
- **Soft skills** are really important!



Setting up an Abuse Desk

How to get started

The Abuse Handling Process

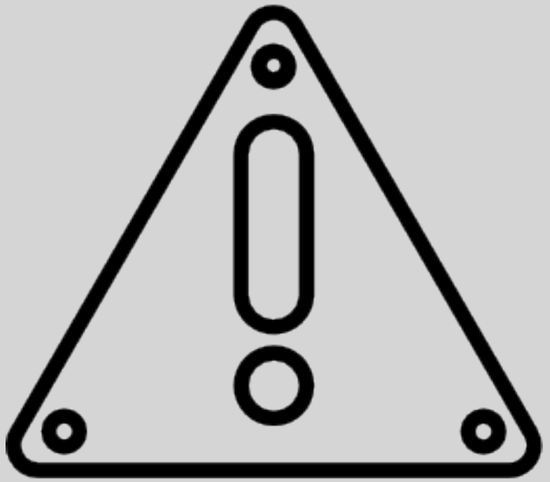


SPEED is the most important factor!

Inbound

- Inbound data can come from several sources:
  - **abuse@** mailbox
  - Internal sources
  - Threat intelligence
  - Other external sources

- Is the data in the abuse report **complete**?



The Abuse Mailbox

- **RIPE-705** - “**Abuse Contact Management in the RIPE Database**” defines the abuse contact for RIPE region IPs and ASNs
- Mandatory on all **aut-num** objects and directly allocated **inet(6)num** objects
- “abuse-mailbox:” contains email address where abuse reports should be sent
- The abuse-mailbox address is validated every year

Search results

This is the RIPE Database search service. The objects are in RPSL format. The RIPE Database is subject to Terms and Conditions.

Responsible organisation: Reseaux IP Europeens Network Coordination Centre (RIPE NCC)
Abuse contact info: abuse@ripe.net

```
inetnum:        193.0.24.0 - 193.0.30.255
netname:        RIPENCC-MEETING-PUBLIC
descr:          Reseaux IP Europeens Network Coordination Centre (RIPE NCC)
```

Standardised Abuse Reports

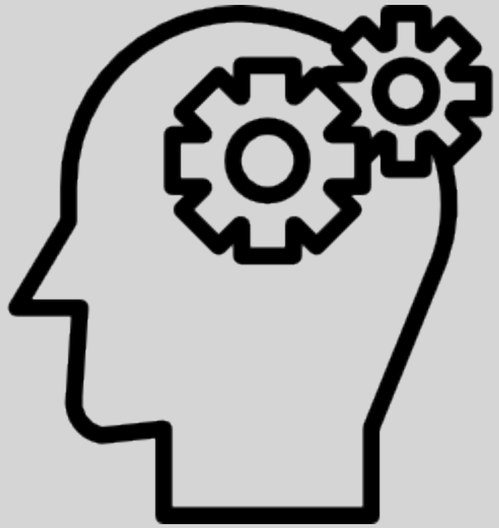
- Allows **automation** of abuse reports
- Makes abuse handling **easier**
- **XARF** is a popular standard
  - Simple, extensible, and structured, and, therefore, easily automated

https://github.com/abusix/xarf


```
{
      "Version": "2",
      "ReporterInfo": {
        "ReporterOrg": "ExampleOrg",
        "ReporterOrgDomain": "example.com",
        "ReporterOrgEmail": "reports@example.com",
        "ReporterContactEmail": "contact@example.com",
        "ReporterContactName": "Mr. Example",
        "ReporterContactPhone": "+ 01 000 1234567"
      },
      "Disclosure": true,
      "Report": {
        "ReportClass": "Activity",
        "ReportType": "Spam",
        "ReportSubType": "Trap",
        "Date": "2018-02-05T14:17:10Z",
        "SourceIp": "192.0.2.55",
        "SourcePort": 54321,
        "DestinationIp": "198.51.100.33",
        "DestinationPort": 25,
        "SmtpMailFromAddress": "spam@example.com",
        "SmtpRcptToAddress": "victim@example.com",
        "Samples": [
          {
            "ContentType": "message/rfc822",
            "Base64Encoded": true,
            "Description": "The spam mail",
            "Payload": "bWFpbA=="
          }
        ]
      }
    }
```

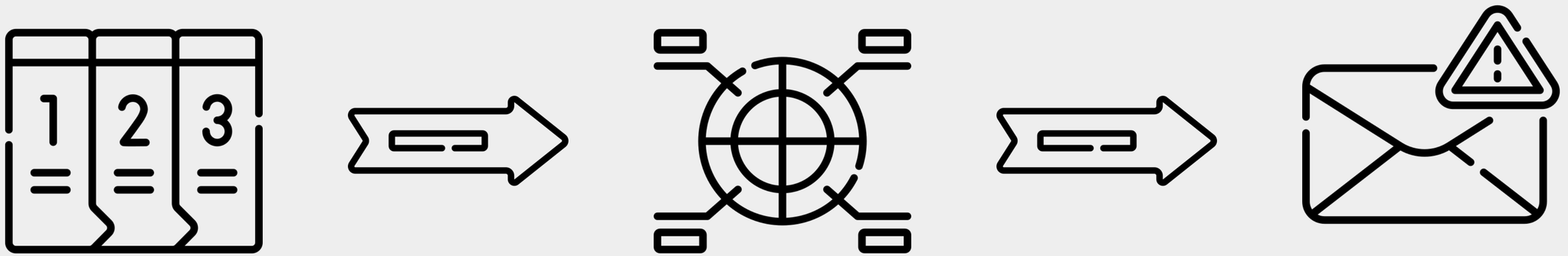
Processing

- **Link** the events from a resource to its end user
- **Aggregate** the events and identify the end users
- Aggregation provides a **view** of what you need to handle
- Move as much “manual handling” into “**automatic processing**”



Gather all the reports

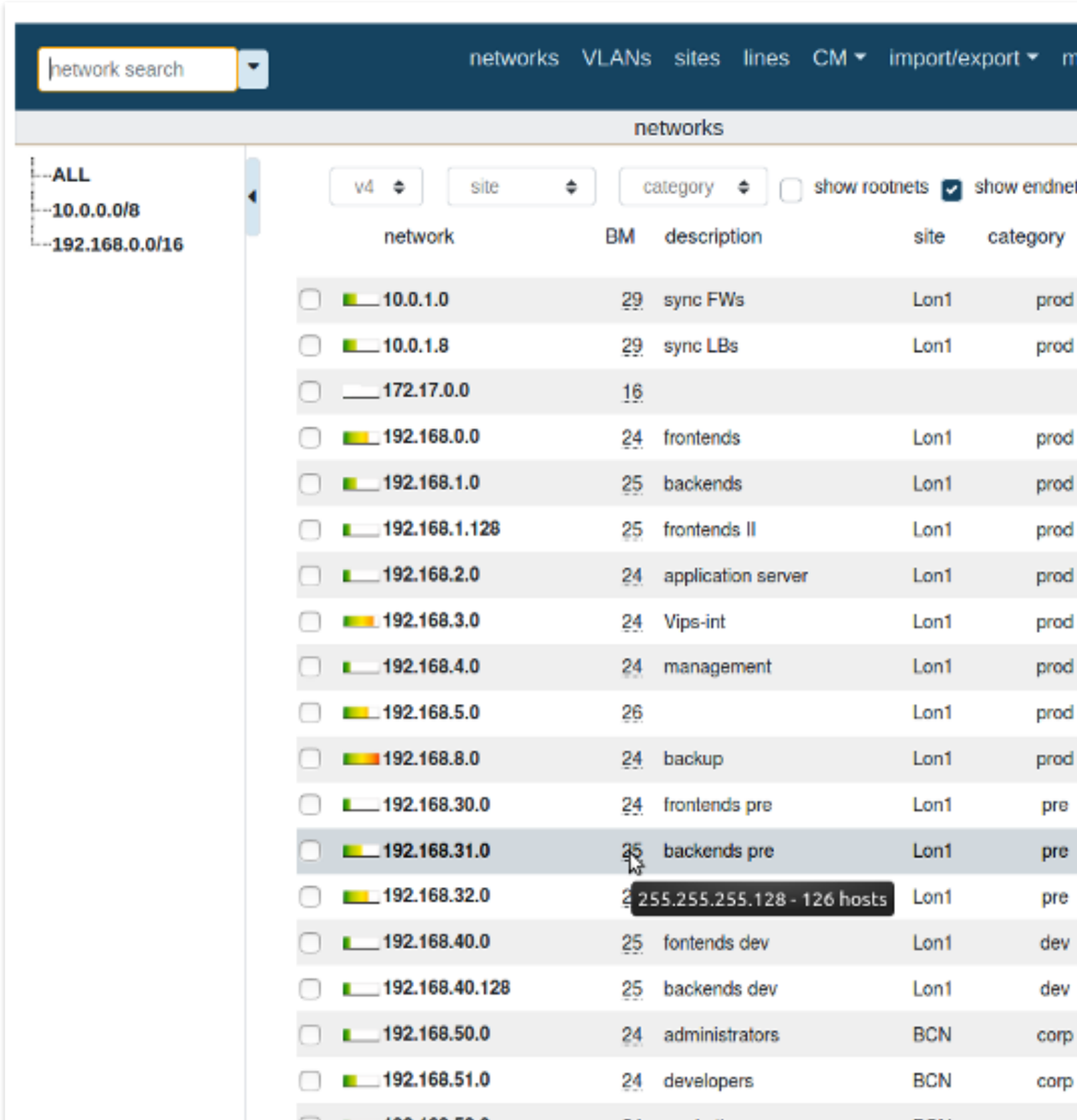
- An **Abuse Management** tool helps
  - Catalog and classify incidents
  - Correlate abuse reports with open cases
  - Send notifications about incidents



Link resources to end users

- You want to be able to **contact** the end user to solve the problem

- An **IPAM tool** helps to resolve domains and IP addresses to customers

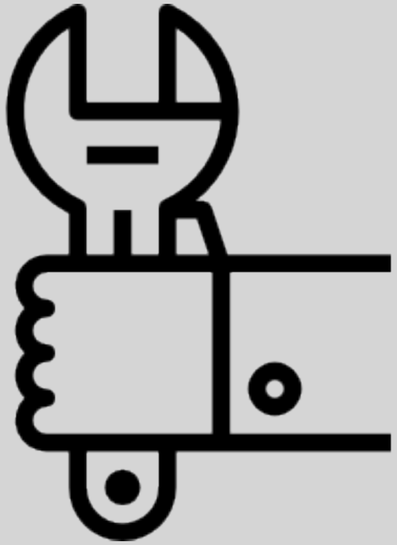


Source: http://www.gestioip.net/imagenes/ip_address_management_new.png

Handling

- **Prioritising** which event should be handled
  - Quantity: 25000 spam reports > 1000 spam reports
  - Type of event: **spam** vs **phishing** vs **DDoS attack**

- You prioritise based on **your situation**
  - Some issue types are more urgent for you
  - Some sources are of more importance for you



How urgent is it?

- Set **priorities** and **processes** for the different issue types

Issue Type	Urgency Indicator	Process to follow
Spam	Lots of reports; not too many consequences	**A**
Phishing	Consequences for the end users	**B**
Malware	Few indicators visible to ISP; requires external data	**C**
Copyright	Has consequences for the end user	**D**
Botnets	Not visible until attack happens	**E**
CSAM	High priority; has severe legal implications	**F**

Exceptions

- Some incidents **cannot** be automated
- There will always be **special** cases where manual intervention is required
- The long term goal is to automate as much as possible

Remediation / Mitigation

- How to **solve** the issue will depend on:
  - What is the root cause of the issue?
  - What is your environment like?

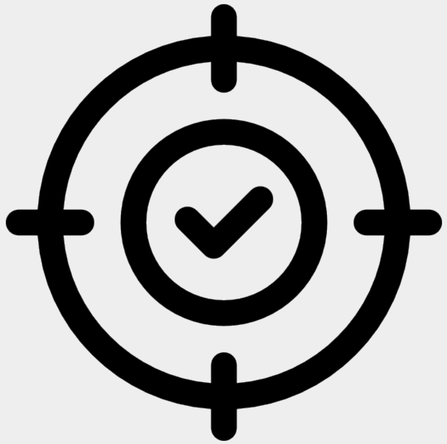
- Which **actions** can you take to **solve** the issue without completely shutting down the end user?

How to Measure the Success?

- **Start** with a first measurement:
  - How many abuse reports were received when the abuse desk started?

- **Keep** daily / weekly / monthly statistics
  - Issues reported / End users contacted / Issues resolved

- **Compare** the statistics over time
  - Do you see a growth or reduction in amount of issues reported?



Take the poll!

What are the **four steps** in the abuse handling process?

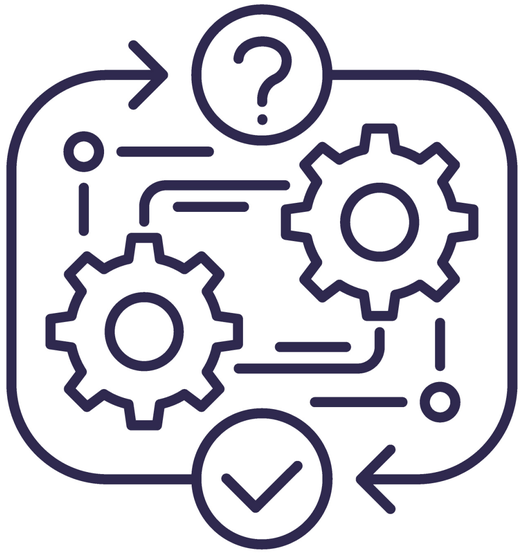
1 min.

Some help with abuse handling

Tools and Services

Automation Helps

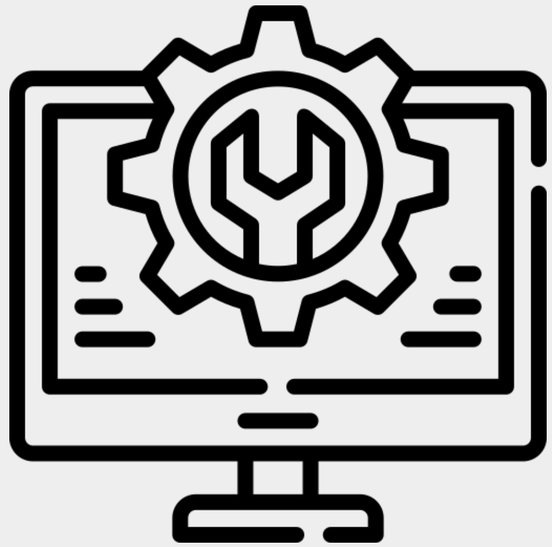
- **Save time** and let the computer do the grunt work!
- **Software** can do the repetitive tasks:
  - Collect the reports
  - Aggregate the cases to identify priorities
  - Cross-reference with other data input
  - Take actions to solve simple issues



IP Address Management Tools

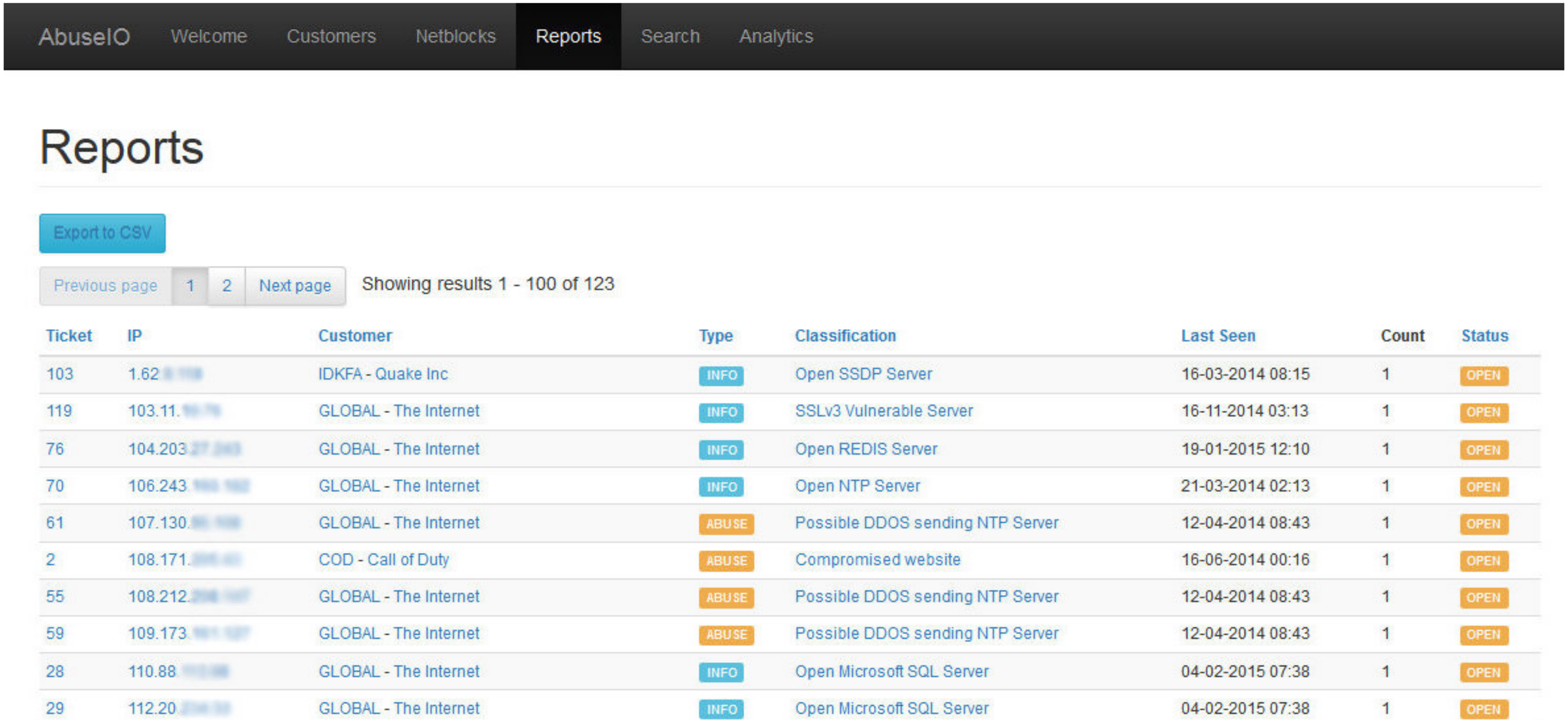
- **Data tracked** by an IPAM system includes information such as IP addresses in use, and the associated devices and users
- **Centralised collection** of this information supports troubleshooting and abuse investigations

- **IPAMs (free)**
  - Netbox
  - GestióIP
  - NIPAP
  - There are more!
- **IPAMs (paid)**
  - There are many available
  - Simply search for “IPAM tool”



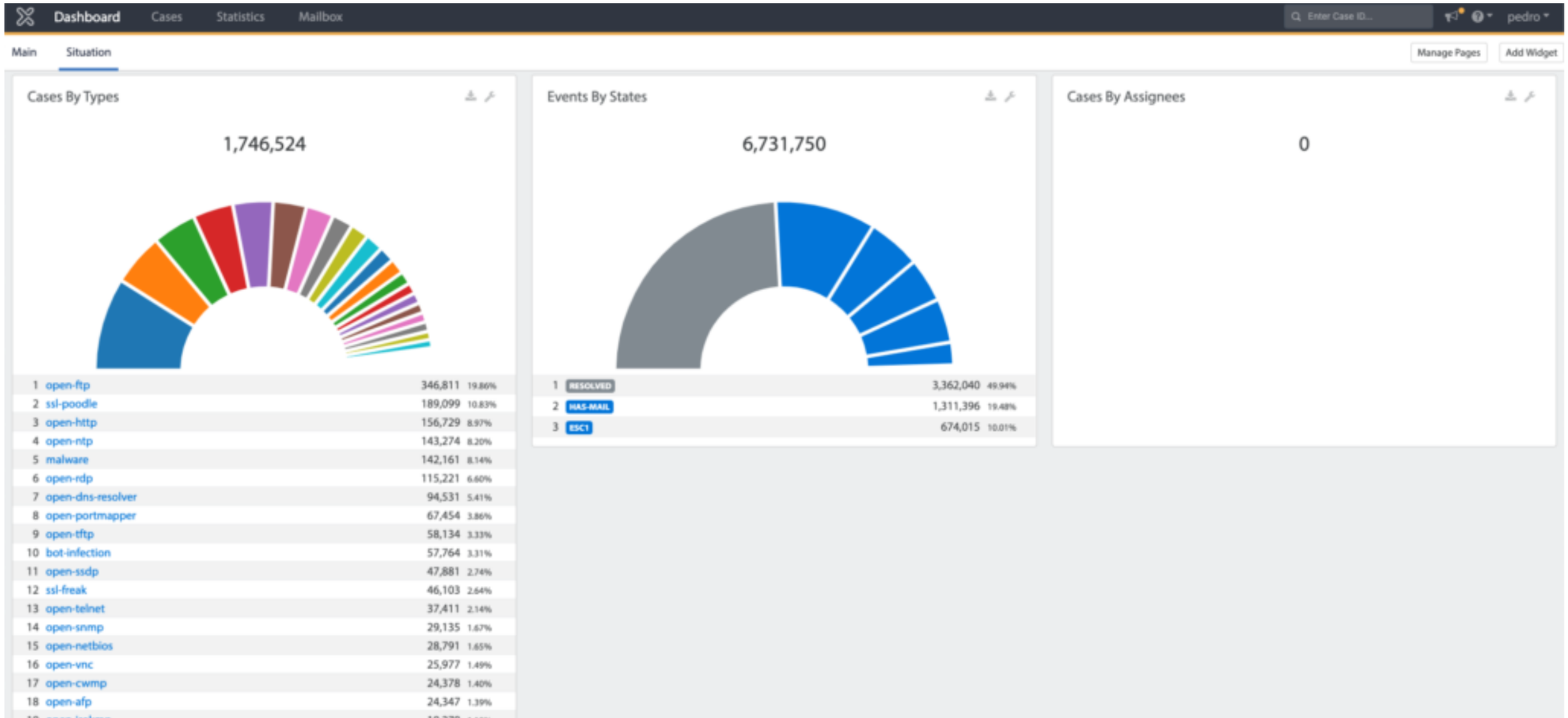
Abuse Management Software

- **AbuseIO (Open Source)**
  https://abuse.io



Abuse Management Software

- **AbuseHQ (SaaS)**
  https://abusix.com/products/abusehq/



Stay Ahead of the Game

- **Read** the BCOPs

  i.e. “Good Practice In Minimising Email Abuse”

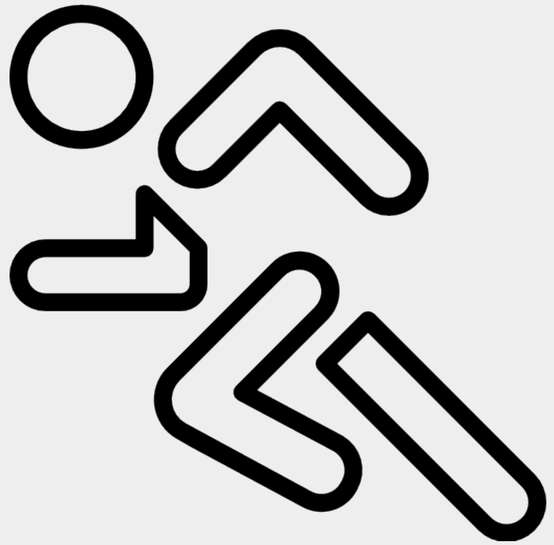
  https://www.ripe.net/publications/docs/ripe-409

- **Connect** with other abuse desks

  The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)

  https://www.m3aawg.org/

- **Keep up to date** with the latest developments



More sources of data

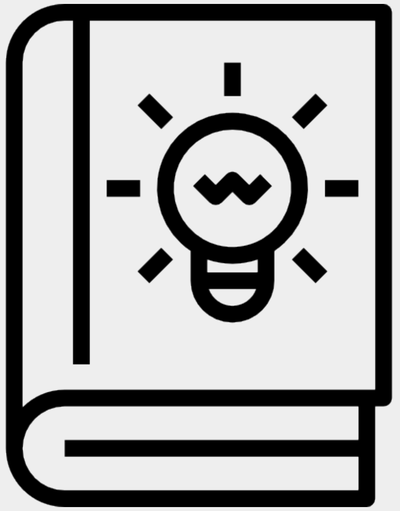
- **AbuseIPDB**
  - https://www.abuseipdb.com

- **Talos IP & Domain Reputation Center**
  - https://talosintelligence.com/reputation_center

- **Shadowserver**
  - https://www.shadowserver.org

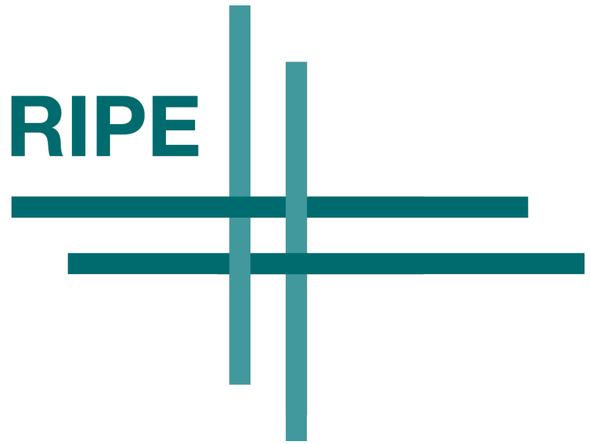
- **Spamcop**
  - https://www.spamcop.net

- ***Know more? Let us know!***



Participate in the Community

- **Sign up** for the Anti-Abuse working group!
- **Discuss** and **share** information
  - On technical and non-technical methods of preventing or reducing network abuse
- **Help** to produce and update a Best Common Practice document
- Get and give **advice** on strategic and operational topics



https://www.ripe.net/participate/ripe/wg/active-wg/anti-abuse

Questions

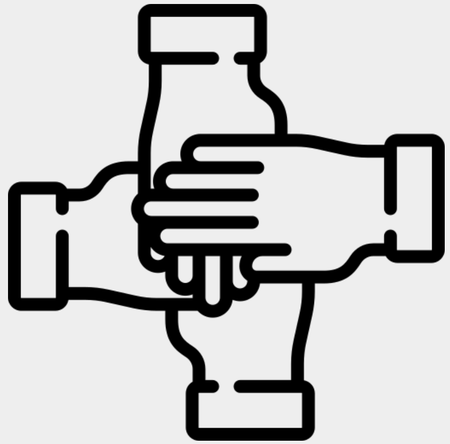
And now, what?

Call to Action

Your Next Steps…

- **Prepare** your inbound data sources
- **Set up** your IPAM and Abuse Management tool
- **Set priorities** for the different possible incidents
- **Create procedures** for handling the different types of incidents
- **Set up** your metrics and statistics

Start handling those abuse reports!



We want your feedback!

What did you think about this session? Take our survey at:

https://www.ripe.net/feedback/anti-abuse

RIPE NCC
Academy

Learn something new today!

academy.ripe.net

RIPE NCC Certified Professionals

https://getcertified.ripe.net/

Ënn

Vége

Son

Lõpp

Kraj

Fine

Fim

Соңы

Endir

დასასრული

Amaia

Sfârşit

Fin

Slut

An Críoch

Finvezh

הסוף

Loppu

النهاية

Einde

پایان

վերջ

Tmiem

Slutt

Конец

Fí

Край

Ende

Кінець

Liðugt

Konec

Край

Beigas

Y Diwedd

Koniec

Finis

Kpaj

Fund

Τέλος

Pabaiga

What’s Next in Network Security

Webinars

Attend another webinar live wherever you are.

- IP Blocklisting Basics (1 hr)
- Anti-Abuse (1.5 hrs)

For more info click the link below

learning.ripe.net

Want to learn more?

Check out other e-learning courses we offer.

For more info click the link below

academy.ripe.net

Up for a challenge?

Look at our range of examinations available for certification.

For more info click the link below

getcertified.ripe.net

Copyright Statement

[...]

The RIPE NCC Materials may be used for **private purposes, for public non-commercial purpose, for research, for educational or demonstration purposes**, or if the materials in question specifically state that use of the material is permissible, and provided the RIPE NCC Materials are not modified and are properly identified as RIPE NCC documents. Unless authorised by the RIPE NCC in writing, any use of the RIPE NCC Materials for advertising or marketing purposes is strictly forbidden and may be prosecuted. The RIPE NCC should be notified of any such activities or suspicions thereof.

[...]

Find the full copyright statement here:
https://www.ripe.net/about-us/legal/copyright-statement