

# Abuse Desk Training



# Our Panel

## Presenters:

- **Matthew Stith**  
Anti-abuse Specialist, Rackspace  
Vice-Chair Board of Directors @m3aawg  
Chair Hosting Committee @m3aawg
- **Tobias Knecht**  
CEO, Abusix, Inc.  
Chair Anti-Abuse Working Group @ RIPE  
Chair Anti-Abuse Desk SiG @ m3aawg

# AGENDA

- AUP
- Making the case for a dedicated abuse desk
- Building process
- Getting started with abuse handling

# Acceptable Use Policy

- Protects both the company and customers from abuse of services
  - Set clear standards for proper system use
  - Use language that is meant to deter potential customers who could negatively impact your business

## Acceptable Use Policy (AUP)

- Make sure that what is being published in your terms is enforceable
- Policies that are specific to your network
- A global AUP that is bound to all products. Multiple policies tend to cause confusion and contradictory information.
- Do not allow customer modification to the policy in contract negotiation\*

## AUP: Suggestions and Tips

- You do not have to reinvent the wheel
  - It is ok to reference and use parts of other companies policies
- Make everything clear to the potential customer and in some cases mention specifics
- Length of document
  - Doesn't need to explain everything and some pieces can be generalized (ie. do not send unsolicited mail)

## AUP Example

Let's look at some acceptable use policies

Let's build an acceptable use policy

## AUP: Review

- Conduct a yearly review of your policy or when a change to local, state, government laws occurs
  - Will ensure that you are following best practices and keeping information up to date
  - Remove or modify outdated information
  - New issues that are network specific may require updates
- Sometimes changes need to happen outside of the yearly review



## Making the case for dedicated abuse resources

- Collect relevant data to support the case (Data is King!)
  - Number of complaints received
  - Issues caused by compromise, fraud, phishing, malware
  - Customer impact from abuse
  - Support, Operations, Engineering impact without a dedicated team
  - Focus on the most urgent issue to your network

## Making the case

- Industry growth
  - Developing contacts within the anti-abuse community
    - Faster remediation of issues
    - Visibility into problems occurring on other networks
  - Training opportunities
    - Certifications
    - How to trainings (like what we are doing now!)
  - Positive reputation solidification

## Making the case

- Setting proper expectations with customers
  - Singular message from the company
- Preventing Churn (Not a cost center)
- Providing training and support to sales, operations, and support staff
  - Red flags
  - Proper routing of issues
  - Key knowledge of policies

## Developing processes

- Giving guidelines for enforcement of Acceptable Use Policy
- Process should be assigned to tasks that are repeated constantly, require escalation, or represent critical issues

## Developing Process: Building a Process

- Focus on simplicity
- Should be easily repeatable (prefabricated responses are your friend)
- Have clear direction for the customer and support to take
- Set deadlines for remediation
- Stay away from threatening language in communication but be firm (with exceptions)
- Do not divulge a process to customer

## Developing processes

- Dangers of lack of process
  - Legal issues
  - Customer impact due to abuse
    - Blacklisting
    - Retaliation
    - Downtime
  - Ineffective communication with customers, other employees, and external parties on abuse related issues
    - Misinformation
    - Unrealistic expectation
  - Inability to enforce the Acceptable Use Policy

## Developing Process: Building Exercise

- Type
- Urgency
- Expected customer response time frame
- Expected resolution time frame
- Result of non-compliance
- Closing
  - A note on mitigation/remediation

## Process Example: Type

Spam

“Spamvertising”

Phishing (Inbound/Outbound)

Hacked or defaced pages

Child sexual abuse material

Malicious Signups

Copyright/Trademark

DDOS/Outbound malicious traffic

Rogue DNS

.....and the list goes on and on



# Process Example: Urgency

Complaint Priorities for System Abuse	Priority Level
<ul style="list-style-type: none"><li>• Child exploitation<sup>14</sup></li><li>• Offensive or harmful content</li><li>• Data theft from the corporation</li></ul>	<b>Critical</b> P0
<ul style="list-style-type: none"><li>• Botnet C&amp;C</li><li>• DDoS</li><li>• Data theft on network</li><li>• Data theft from network</li></ul>	<b>High</b> P1
<ul style="list-style-type: none"><li>• Malware drops</li><li>• Phish data drops</li><li>• Phish hosting</li><li>• Dictionary/bruteforce attacks</li><li>• Data theft as client</li></ul>	<b>Medium</b> P2
<ul style="list-style-type: none"><li>• Spam</li><li>• Control panel</li><li>• SSH forwarding</li><li>• Spamvertising on network</li><li>• Spamvertising support network, hacking/cracking</li><li>• Remote file injection</li></ul>	<b>Low</b> P3
<ul style="list-style-type: none"><li>• Web defacement</li><li>• Exploitable services</li><li>• Port scanning</li><li>• Comment spamming</li></ul>	<b>Very Low</b> P4
<ul style="list-style-type: none"><li>• Copyrights and trademark issues.</li></ul>	*

## Process Example: The customer

- How long should you give a customer to respond?
  - What is an acceptable response?
- How long should you give the customer to resolve?
- Do you route the customer to another part of the organization?
- Suspend at notification

## Process Example: Non-compliance

- Check any special exceptions and also the type of customer
- No response no resolution
  - Mitigation
  - Suspension
  - Termination

## Process Example: Closing

- Customer confirms resolution
  - Ticket update\*
  - Phone call
  - Chat
- Company confirms resolution
- Issue has been tabled and has long resolution (mitigation)

# Remediation vs Mitigation

- Remediation
  - Completed resolution of the issue
- Mitigation
  - Temporary resolution of the issue

# Agenda

- State of Anti-Abuse
- X-ARF
- Abuse Reporting BCP
- Abuse Handling Automation BCP
- Abuse Handling – A Perfect World

# State of Anti-Abuse

- State of Anti-Abuse
- X-ARF
- Abuse Reporting BCP
- Abuse Handling Automation BCP
- Abuse Handling – A Perfect World

# X-ARF

- State of Anti-Abuse
- X-ARF
- Abuse Reporting BCP
- Abuse Handling Automation BCP
- Abuse Handling – A Perfect World



# Abuse Reporting BCP

- State of Anti-Abuse
- X-ARF
- Abuse Reporting BCP
- Abuse Handling Automation BCP
- Abuse Handling – A Perfect World

# Abuse Handling Automation BCP

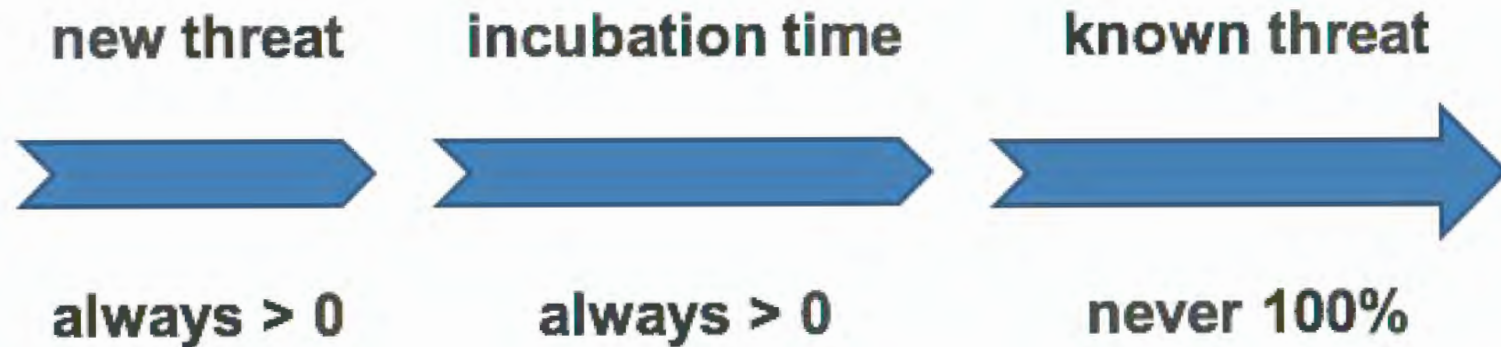
- State of Anti-Abuse
- X-ARF
- Abuse Reporting BCP
- Abuse Handling Automation BCP
- Abuse Handling – A Perfect World

# Abuse Handling

## *A Perfect World*

**inbound – protect your users  
from the internet**

**outbound – protect the internet  
from your user**



industry is focusing on detecting new threats  
and make them known.

This is where **abuse handling** starts

# number #1 priority: speed

The **faster** you react and **mitigate/remediate** the **less** interesting you'll be for the **bad guys**.

# number #2 priority: **sustainability**

The **better** you mitigate  
the **less follow ups** you have to handle.

number #3 priority:  
**completeness**

The **cleaner** your environment is,  
the **less trouble** is coming your way.

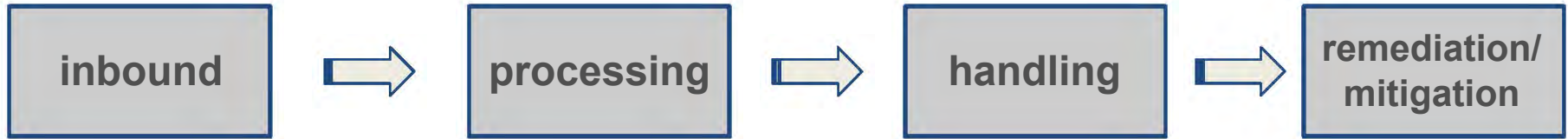


**that all sounds good  
so how do I start?**

# First a few **lessons** learned

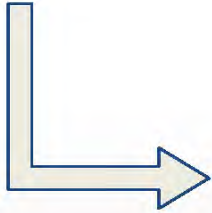
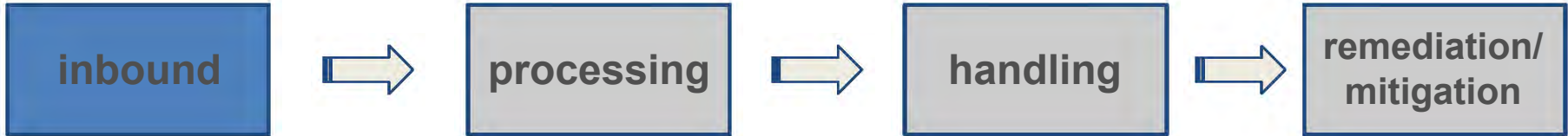
1. Be **pragmatic!** It's not a Science Project.
2. Data is **King!**
3. Good **tooling** creates actionable **knowledge**
4. Know your **Challenge!**
5. Implement and **live the process!**
6. Automate! **Automate!** Automate!
7. **Iterate!** Grow based on your growing information and knowledge.
8. Pull **other departments** into your process (fraud/billing/vetting/ ...)
9. Look over the **fence** on what the **industry** does.
10. **Provide information** and data to other Abuse Desks.

# How does a process look like?



**It's not just about reactive vs. proactive.  
It's about SPEED!**

# Variations of Inbound Data

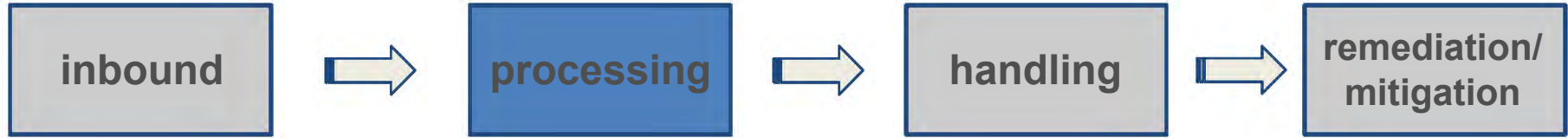


1. **abuse@ Mailbox**
2. **Internal Sources**
3. **Threat Intelligence**
4. **Other external Sources**
5. **...**

# Security Issues Indicators

<b>Spam:</b>	largest by volume but not by value
<b>Copyright:</b>	instance of well defined unit cost
<b>Phishing:</b>	low volume, high value implications to users
<b>Malware:</b>	few indicators visible to ISP, need ext. data
<b>Botnets:</b>	silent until attack, next ext. Data
<b>Vulnerabilities:</b>	low but increasing volume, proactive
<b>Child Exploitation:</b>	very low volume, but high priority
<b>Offensive Content:</b>	very low volume, but high priority (Weapons, Drugs, ...)
...	...
...	we see around 40 - 45 additional report types

# Making sense of all the information



Customer/Subscriber allocation leads to aggregation.

Aggregation gives you a complete view on what you need to handle.

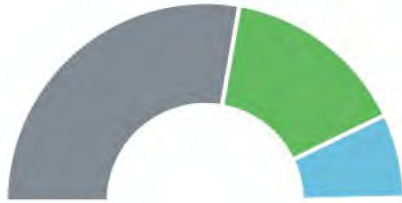
You want to move as much “manual handling” into “automated processing”

# Why customer allocation is important

Cases By States



779,803



Events By States



22,254,892



Cases By States



74 917



1	CLOSED	36 774	49,09%
2	REOPENED	25 911	34,59%
3	NEW	12 231	16,33%
4	IN PROGRESS	1	0%

Events By States

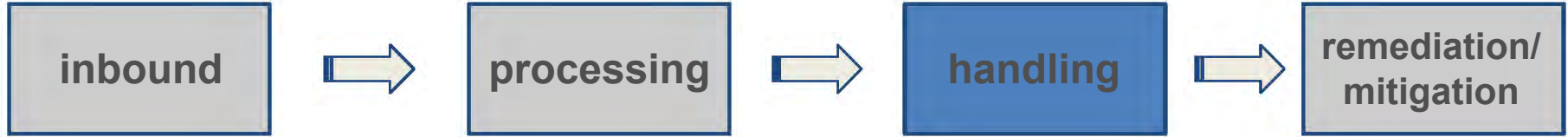


10 166 322



1	REOPENED	4 184 681	41,16%
2	NEW	3 231 576	31,79%
3	CLOSED	2 750 061	27,05%
4	IN PROGRESS	4	0%

# prioritizing and decision making



## Prioritize:








- Amount of Events: 30,000 spamreports vs 5,000 spamreports
- Event Types: phishing vs. spam vs. copyright ...
- ...

You prioritize, based on ***your*** environment.

You will always have manual reviews to do. But you will minimize them.

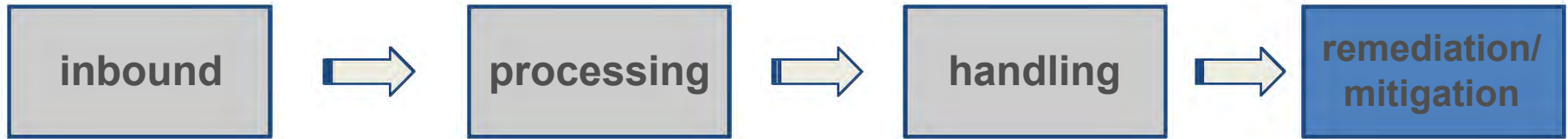


# divide and conquer

	<b>Phishing</b> <i>56 unresolved Cases</i>	≡
	<b>Spam</b> <i>1,913 unresolved Cases</i>	≡
	<b>Malware</b> <i>62 unresolved Cases</i>	≡
	<b>Spamhaus</b> <i>0 unresolved Cases</i>	≡
	<b>DMCA</b> <i>552 unresolved Cases</i>	≡
	<b>Spamvertized Sites</b> <i>2 unresolved Cases</i>	≡
	<b>Default Group</b> <i>Catches all unmatched Events</i>	

lower < Priority > higher

# how to finally solve the issue



## Root causes:

1. **Compromised Account/Customer/Server**
2. **Fraud - Criminal Activity**
3. **User Behavior**
4. **Vulnerability - Advanced**

## Environment:

- **Business or Private Customer**
- **What product is the customer on?**
- **T&C, Policies that are in place.**
- ...

# flexibility improves the process

**Playbook** *last changed on 2017-05-22 19:57 by superuser*

Name AutoResolve *in days*

Description *optional*

```
graph LR; NEW[NEW] --> IN_PROGRESS[IN PROGRESS]; IN_PROGRESS --> ON_HOLD[ON HOLD]; ON_HOLD --> REOPENED[REOPENED]; REOPENED --> RESOLVED[RESOLVED]; IN_PROGRESS --> RESOLVED;
```

Source	Target	Title	
REOPENED	RESOLVED	Resolved	✎
REOPENED	IN PROGRESS	Restart	✎
ON HOLD	REOPENED	Auto Reopen	✎
ON HOLD	IN PROGRESS	Resume	✎
NEW	IN PROGRESS	Start	✎
IN PROGRESS	RESOLVED	Resolve	✎
IN PROGRESS	ON HOLD	Set On Hold	✎

[+ Add Transition](#)

# What **tooling** is out there?

**Ticket systems can work, but are  
not designed for abuse work.**

**abuse.io**

**very small volumes**

**integration/development/maintenance needed**

**no automation at all**

**offline customer allocation**

**open-source**

# Abacus

Small to mid size volumes

integration/development/**maintenance needed**

**small** pieces of **automation**

customer allocation

priced per seat

# AbuseHQ

small to huge volumes

**advanced parsing** (~3000 formats)

**no maintenance** or development needed

little integration, depending on **level of automation**

can be **fully automated** with case groups and **playbooks**

priced on features



# Thank you

- <http://m3aawg.org>
  - <https://www.m3aawg.org/published-documents>
  - [https://www.spamhaus.org/isp/aup\\_builder/](https://www.spamhaus.org/isp/aup_builder/)
  - <https://www.m3aawg.org/m3aawg-lacnic-partnership>
- 
- [matthew.stith@rackspace.com](mailto:matthew.stith@rackspace.com)
  - [tk@abusix.com](mailto:tk@abusix.com)
  - [dennis.dayman@returnpath.com](mailto:dennis.dayman@returnpath.com)