abusix

Datasheet

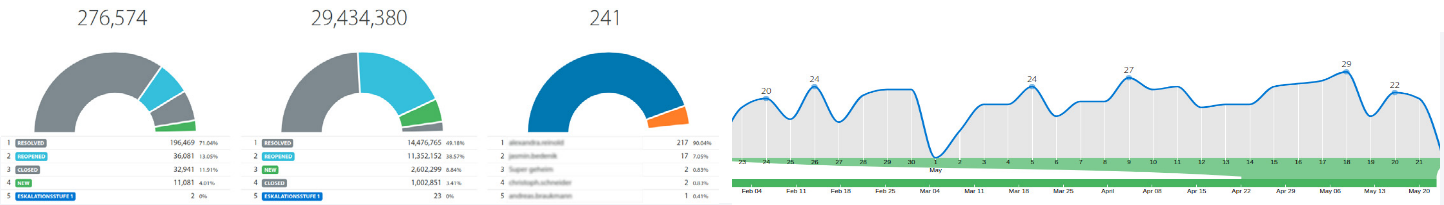
Abusix's AbuseHQ

Security and Abuse Orchestration, Automation, and Response

Abusix's AbuseHQ™ is the industry's first full-featured, security and abuse orchestration, automation and response platform for service providers. The service orchestrates 3rd party reports of abuse and data from service provider edge systems, thereby simplifying the identification of abuse and nefarious use of service provider's networks in real time, actioning problems with automated configurable workflows, and provides the ongoing critical visibility that access and hosting providers need to measure responses and assure that their networks, the internet, and their customers remain safe.

A BETTER APPROACH TO NETWORK PROVIDER SECURITY

Easily gain real-time visibility to subscriber network security and abuse issues



276,574

1	RESOLVED	196,469	71.04%
2	REOPENED	36,081	13.05%
3	CLOSED	32,941	11.91%
4	NEW	11,081	4.01%
5	ESKALATIONSSTUFE 1	2	0%

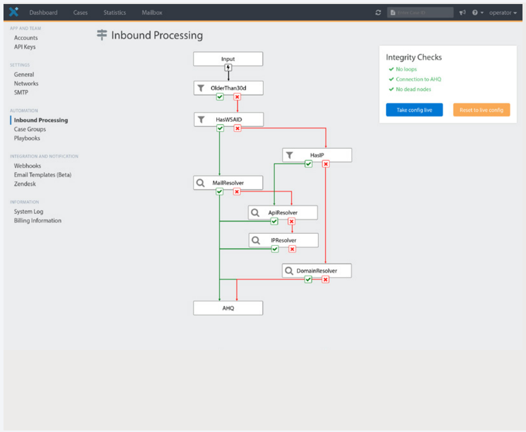
29,434,380

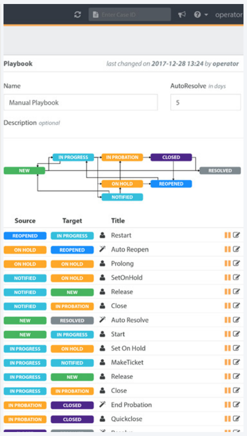
1	RESOLVED	14,476,765	49.18%
2	REOPENED	11,352,152	38.57%
3	NEW	2,602,299	8.84%
4	CLOSED	1,002,851	3.41%
5	ESKALATIONSSTUFE 1	23	0%

241

1	[redacted]	217	90.04%
2	[redacted]	17	7.05%
3	[redacted]	2	0.83%
4	[redacted]	2	0.83%
5	[redacted]	1	0.41%

Resolve 99% of subscriber security & abuse incidents automatically





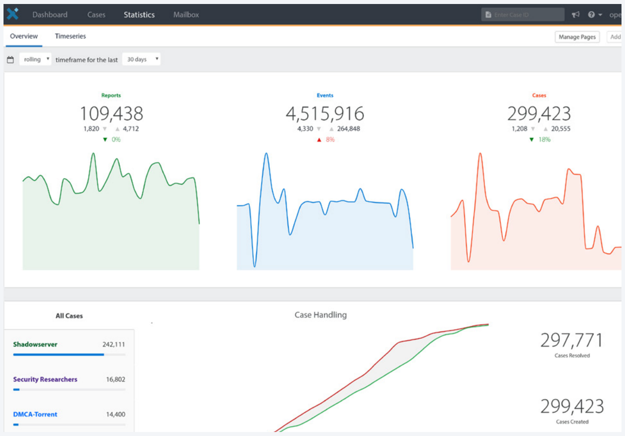
last changed on 2017-12-28 13:24 by operator

Name: Manual Playbook

AutoResolve in days: 5

Source	Target	Title
REOPENED	IN PROGRESS	Restart
ON HOLD	REOPENED	Auto Reopen
ON HOLD	ON HOLD	Prolong
NOTIFIED	ON HOLD	SetOnHold
NOTIFIED	NEW	Release
NOTIFIED	IN PROBATION	Close
NEW	RESOLVED	Auto Resolve
NEW	IN PROGRESS	Start
IN PROGRESS	ON HOLD	Set On Hold
IN PROGRESS	NOTIFIED	MakeTicket
IN PROGRESS	NEW	Release
IN PROGRESS	IN PROBATION	Close
IN PROBATION	CLOSED	End Probation
IN PROBATION	CLOSED	Quickclose

Protect your network, your business reputation & your customers



All Cases

Shadowserver	242,111
Security Researchers	16,802
DMCA-Torrent	14,400

297,771 Cases Resolved

299,423 Cases Created

Abusix's AbuseHQ™ is the industry's first security and abuse orchestration platform that identifies and neutralizes the abuse and nefarious use of service provider networks in real time. It provides the necessary visibility that access and hosting providers need to protect their network and keep their customers safe.

ORCHESTRATION

Just as an orchestra brings together a group of instrumentalists to create a symphony, AbuseHQ™ allows you to easily orchestrate different data and technology elements you need to make informed decisions and take necessary actions for abuse and security events.

Data Integrations

- AbuseHQ™ supports both templated email and API integrations with other informational systems.
- Data enrichment services that integrate with AbuseHQ™ include whois, blacklist, phishing service or malware reporting services and countless others..

Infrastructure Integration

- AbuseHQ™ API integrations are used to resolve subscriber information and also use data elements in decision making like subscriber subscription date, class of service, etc; making workflows smarter and improving automation decisioning.

Service Integrations

- Webhook or API integrations with upstream systems like ticketing, CRM, MTAs, provisioning, wall gardens, billing, customer web portals and others are easy to configure.
- AbuseHQ™ templating integrates with your SMTP mail platform.
- AbuseHQ™ integrates into upstream systems like RT, Salesforce, Zendesk, jira to name a few, helping orchestrate the bridge between you, your support organization and subscribers.

AUTOMATION

AbuseHQ™ fully automates security and abuse workflows, increases subscriber alert speed, raises productivity and dramatically improves network security while lowering support costs, thus making your network unattractive for bad actors and their bots.

Event Normalization

- AbuseHQ™ automatically parses inbound abuse reports from over 500+ formats received from over 7,000 reporting sources, including arf, acns, iodef, Shadowserver, etc. forever freeing you from parser maintenance.
- Abusix Real-time Threat Intelligence allows you to see a real-time view of botnet activity within your network, to prevent being blacklisted.
- OSINT, edge security alerting in the form of any web, log, stream or email source may be injected via the AbuseHQ™ API, providing you a single pane of 'subscriber security glass'
- Automatically identify the reported endpoint regardless of whether the report is an IP, domain or URL report, eliminating the need to look up subscriber information manually.

Event Clustering

- Automatically connect related subscriber events together in a case, regardless if the endpoint is static, dynamic or a shared resource like MTAs, web hosting or other services,
- Data is automatically enriched by tagging network ranges, subscriber service level, abuse type, vulnerability, malware, and more.
- Automation ensures that events are clustered within a defined time horizon allowing you to deal only with what's current vs old mails that were recently complained about.
- Clustering occurs on three tiers; by (1) subscriber, (2) subcategory of license, resource or subaccount, and (3) abuse type case.

Playbook Rules and Triggers

- Playbook groups allow you to automate case prioritization with drag and drop so you always focus on what your organization cares about most.
- Playbooks easily mold to your existing policies and rules for enforcement.
- Customizable automated rule processing allows you to handle subscriber abuse events individually or as cases.
- Escalations for reinforcement subscriber performance requirements with each new email in a sequence are easy to create.
- Sharing of abuse report and case information with your subscribers is simple with our integrated report sharing feature.
- Workflows can easily escalate cases to internal security teams and/or legal stakeholders by email, text, slack or other systems that notify or get approvals when case threat levels are escalated.
- Make security and risk assessments earlier lowering overall network operations and support costs.
- Playbooks allow you to naturally and continually make incremental process improvements to your automated, semi-automated and manual workflow processes, reducing organizational costs and dramatically decreasing legal risk.

RESPONSE

AbuseHQ™ allows you to help users in a uniform consistent manner, enforce your acceptable use policies (AUP), thus keeping your network clean & robust for your users and increasing their satisfaction, all while lowering your organizational risk, ensuring safe harbor protection and maximizing your shareholders profit by ensuring your network services are used as you intend.

- Greatly simplify network operator security operations by providing a single pane of glass for all subscriber security and abuse related issues, while assuring a safer more secure network by lowering MTTR (mean time to respond).
- Reduce subscriber security and vulnerability issues, network abuse, thereby improving the reputation of your network and reducing blacklistings.
- Act on fraud, copyright and phish notifications in real time and catch repeat offenders; thereby dramatically reducing legal risk.
- Improve subscriber response to compromised machine notifications, customer care and quality of service; thus increasing subscriber satisfaction and retention.

REPORTING

With AbuseHQ™ you can report on priorities determined by business context metrics such as risk management and efficiency. This allows abuse and security teams to prioritize abuse and security operations activities, response to events & threats and automate most mundane activities through playbooks.

- See your inbound mail and case queue in a standardized view separating reports from spam.
- Prioritization of the cases by any of the 100+ preconfigured sub-filters making viewing and reporting on cases super simple.
- Easily see subscriber case histogram and all the underlying data to make better decisions.
- Understand overall network abuse trending by abuse types, abuse reporter, malware, infections flows and status easily to track trends and make strategic subscriber campaign decisions.

SYSTEM REQUIREMENTS

- A web browser
- A forwarding abuse@ address

ABOUT ABUSIX

Based in the United States with operations in Germany, Canada, Argentina and Brazil. Abusix has long been considered one of the world's leading authorities on tracking and solving network threats. Abusix Raw Intelligence provides an unparallel view of threats. The Abusix Mail Intelligence service, our blacklist processes and curates our Threat Intelligence and other threat research. By using AbuseHQ to automate orchestration of threat and abuse intelligence, automate event attribution, case creation and actioning of policy at specific event and source thresholds, our customers are able to detect and resolve abuse and security issues faster and more than before, while gaining the necessary visibility to protect their network and keep their customers safe.

Contact us to learn more about **AbuseHQ**

sales@abusix.com | +1 (855) 522-8749 | www.abusix.com

Disclaimer: This datasheet is for informational purposes only. Abusix makes no warranties, express or implied, in this summary. Companies, names, and/or data used in screens and sample output are fictitious unless otherwise noted.