abusix

Guardian Ops Fight Automation with Automation

Identify and neutralize the abuse and nefarious use of service provider networks in real time.

ABUSIX IS MAKING THE INTERNET A SAFER PLACE

The traditional security approach at network service providers is still focused on protecting the user from foreign attacks. This approach, however, is not enough since a 100% secure hosting and internet access does not exist. Abusix provides the missing piece in today's network security environment.

Based in Silicon Valley with operations in Karlsruhe, Germany, Abusix has long been considered one of the world's leading authorities on finding, reporting and resolving network service provider threats. Abusix's SaaS service centralizes and correlates all abuse and security events reported to and from sources within access, ISP and hosting provider networks. Using our service to orchestrate and automate the entire abuse & subscriber security lifecycle from event attribution, case creation, to mitigation or resolution, our customers are able respond faster in resolving abuse and security issues in their hosted subscriber networks.

ABUSEHQ: A BETTER APPROACH TO INTERNET SECURITY

Abusix provides the visibility that access and hosting providers need to protect their network and keep their customers safe.

1

LESS MUNDANE, MORE SECURITY

Automate repeat processes using workflows to resolve up to 99% of network abuse incidents without human intervention.

2

SPEED-UP RESPONSE, PROTECT SUBSCRIBERS

Speed up response, make business operations simpler and improve your customer service and loyalty.

3

REDUCE EXPOSURE, REDUCE COST

Reduce subscriber security and vulnerability issues, network abuse and fraud in a network quickly, thereby dramatically decreasing network operator's legal risk and related costs.

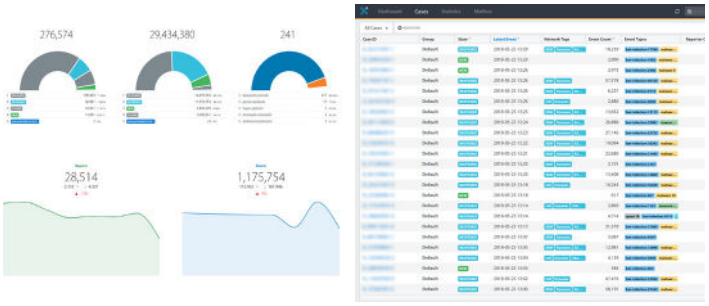
GUARDIAN OPS FOR SECURITY AND ABUSE TEAMS

Abusix's Guardian Ops – the security and abuse orchestration platform - increases network security, lowers reputational and legal risk, and increases subscriber's safety.

ORCHESTRATION

Orchestration integrates different technologies (both security-specific and non-security-specific) to work together to optimize human effort within cyber security and abuse desks. By helping your security and abuse teams understand context, orchestration empowers them to make good abuse handling and security operations decisions.

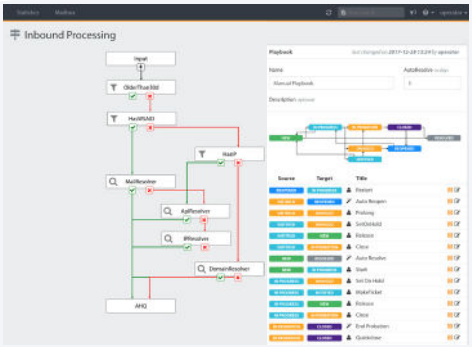
Easily Gain Real-Time Visibility in to Subscriber Network Security and Abuse Issues



AUTOMATION

Automation ensures quick and effective execution of repetitive tasks while assuring uniform application of thresholds and policy without bias or errors. Using automation, machines do the mundane wack-a-mole processing of information and sending routine email notifications AKA "task-oriented human work", while humans focus on more important decision-making for things like escalating issues or troubleshooting.

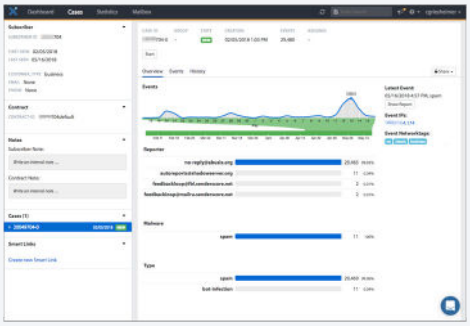
Resolve 99% of Subscriber Security and Abuse Incidents Automatically



RESPONSE

Abuse handling and security operations teams must be consistent in their response to incidents and threats. Using orchestration and automation tools, abuse and security teams can speed up response, make business operations simpler and improve your customer service and loyalty.

Protect Your Network, Your Business Reputation and Your Customers



TRUSTED BY:

telenor StackPath DigitalOcean windstream SYNACOR

INTEGRATES WITH TOOLS YOU RELY ON

AND MANY MORE...

CASE-STUDY: A SERVICE PROVIDER WITH ZERO OPEN ABUSE CASES

83%

Faster RESPONSE TIME

92%

Reduction in ANALYSTS WORKLOAD

99%

Events RESOLVED AUTOMATICALLY

telenor

"Guardian Ops has reduced the amount of malicious traffic leaving our network. Now our abuse specialists can focus on the highest priority and most complex network security issues, while leaving the vast quantity of cases to Guardian Ops."

VEGAR ASMUL, Security Analyst, Telenor