alabus

smarter process management

Certified System swiss TS ISO 9001 · ISO 27001

Certified according to
ISO 9001 and 27001

Software made
in Switzerland

Agenda

- **alabus** introduction
- Show of Hands: Who uses ntop?
- Why **alabus** uses ntopng
- Live Flow Monitoring with ntop
- Challenges in Network Security Monitoring
- Our Goals with **alabus** analyzer
- Process Overview: **alabus analyzer**
- Example Day: 24 Hours of Alerts
- Final outcome **alabus analyzer** + **ntopng**
- Q&A

alabus introduction

- Provider of standard solution for the insurance market
- Founded 1998, headquartered in Zürich
- Certified according to ISO 9001 and 27001
- Member of the ASSEPRO Group

swiss made
software

swiss safety center
ISO 9001
ISO/IEC 27001
certified system

Highlights

- **SaaS / on** cloud-based software solution on own servers
- **End – to – End** execution of a process from start to finish
  Modular System
- **State-of-the-art Technology** the best available solution
- **Low operating costs**

Show of Hands: Who uses ntop?

- Who is currently using ntop?
- Do you regularly work with ntop’s alert data?
- If yes, how many hours per week do you spend on it?

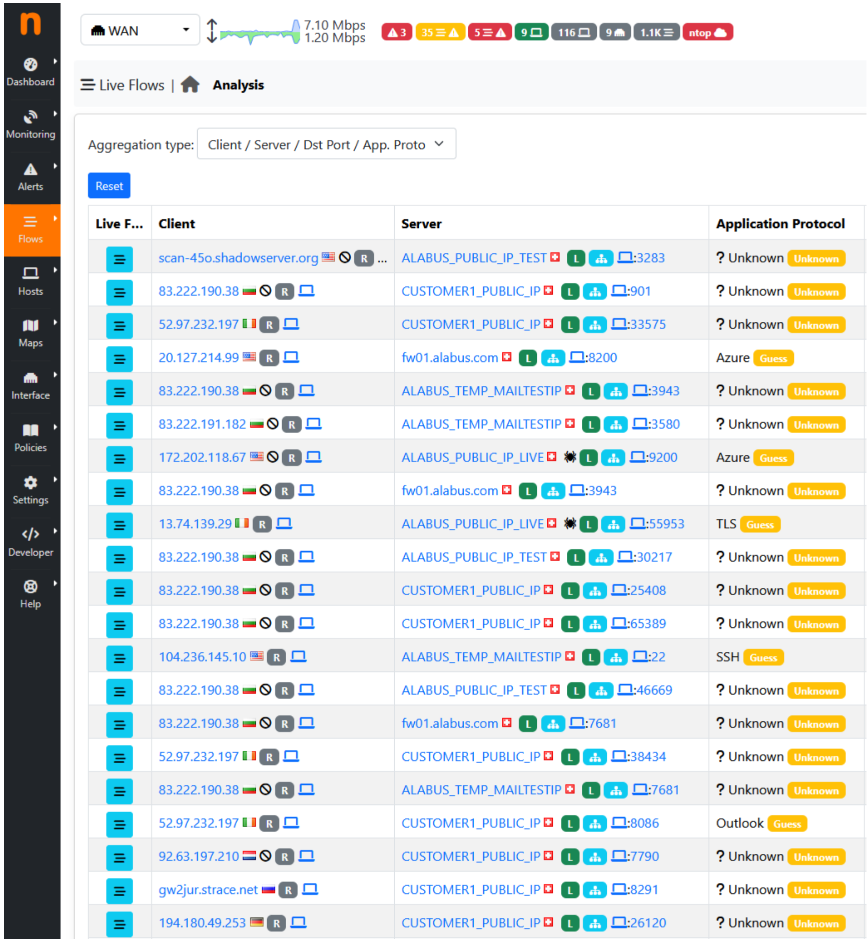
  a) 5 -10 hours b) 20-30 hours

Why alabus uses ntopng

- We need network security that meets the requirements of ISO27001
- Bad experiences with commercial network layer security solutions
  - ➢ Significant costs for a SME company
  - ➢ High staff costs (still too many false-positives)
  - ➢ No complete solutions (no “one stop solution” available)
- “The **alabus** way”:
  - ➢ OpenSource
  - ➢ Customize it with our rules
  - ➢ As a result, you know how it works

☆ 5 minutes into the pilot, ntop flagged a VLAN config issue that the commercial tool had completely missed

Live Flow Monitoring with ntop



☰ Live Flows | Analysis

Aggregation type: Client / Server / Dst Port / App. Proto

Reset

Live F...	Client	Server	Application Protocol
☰	scan-45o.shadowserver.org R ...	ALABUS_PUBLIC_IP_TEST L :3283	? Unknown Unknown
☰	83.222.190.38 R	CUSTOMER1_PUBLIC_IP L :901	? Unknown Unknown
☰	52.97.232.197 R	CUSTOMER1_PUBLIC_IP L :33575	? Unknown Unknown
☰	20.127.214.99 R	fw01.alabus.com L :8200	Azure Guess
☰	83.222.190.38 R	ALABUS_TEMP_MAILTESTIP L :3943	? Unknown Unknown
☰	83.222.191.182 R	ALABUS_TEMP_MAILTESTIP L :3580	? Unknown Unknown
☰	172.202.118.67 R	ALABUS_PUBLIC_IP_LIVE L :9200	Azure Guess
☰	83.222.190.38 R	fw01.alabus.com L :3943	? Unknown Unknown
☰	13.74.139.29 R	ALABUS_PUBLIC_IP_LIVE L :55953	TLS Guess
☰	83.222.190.38 R	ALABUS_PUBLIC_IP_TEST L :30217	? Unknown Unknown
☰	83.222.190.38 R	CUSTOMER1_PUBLIC_IP L :25408	? Unknown Unknown
☰	83.222.190.38 R	CUSTOMER1_PUBLIC_IP L :65389	? Unknown Unknown
☰	104.236.145.10 R	ALABUS_TEMP_MAILTESTIP L :22	SSH Guess
☰	83.222.190.38 R	ALABUS_PUBLIC_IP_TEST L :46669	? Unknown Unknown
☰	83.222.190.38 R	fw01.alabus.com L :7681	? Unknown Unknown
☰	52.97.232.197 R	CUSTOMER1_PUBLIC_IP L :38434	? Unknown Unknown
☰	83.222.190.38 R	ALABUS_TEMP_MAILTESTIP L :7681	? Unknown Unknown
☰	52.97.232.197 R	CUSTOMER1_PUBLIC_IP L :8086	Outlook Guess
☰	92.63.197.210 R	CUSTOMER1_PUBLIC_IP L :7790	? Unknown Unknown
☰	gw2jur.strace.net R	CUSTOMER1_PUBLIC_IP L :8291	? Unknown Unknown
☰	194.180.49.253 R	CUSTOMER1_PUBLIC_IP L :26120	? Unknown Unknown

Every second, there are hundreds of scans, attacks and connection attempts

Challenges in Network Security Monitoring

- Large volumes of network data and many alerts

→ Correct there are to many alerts?

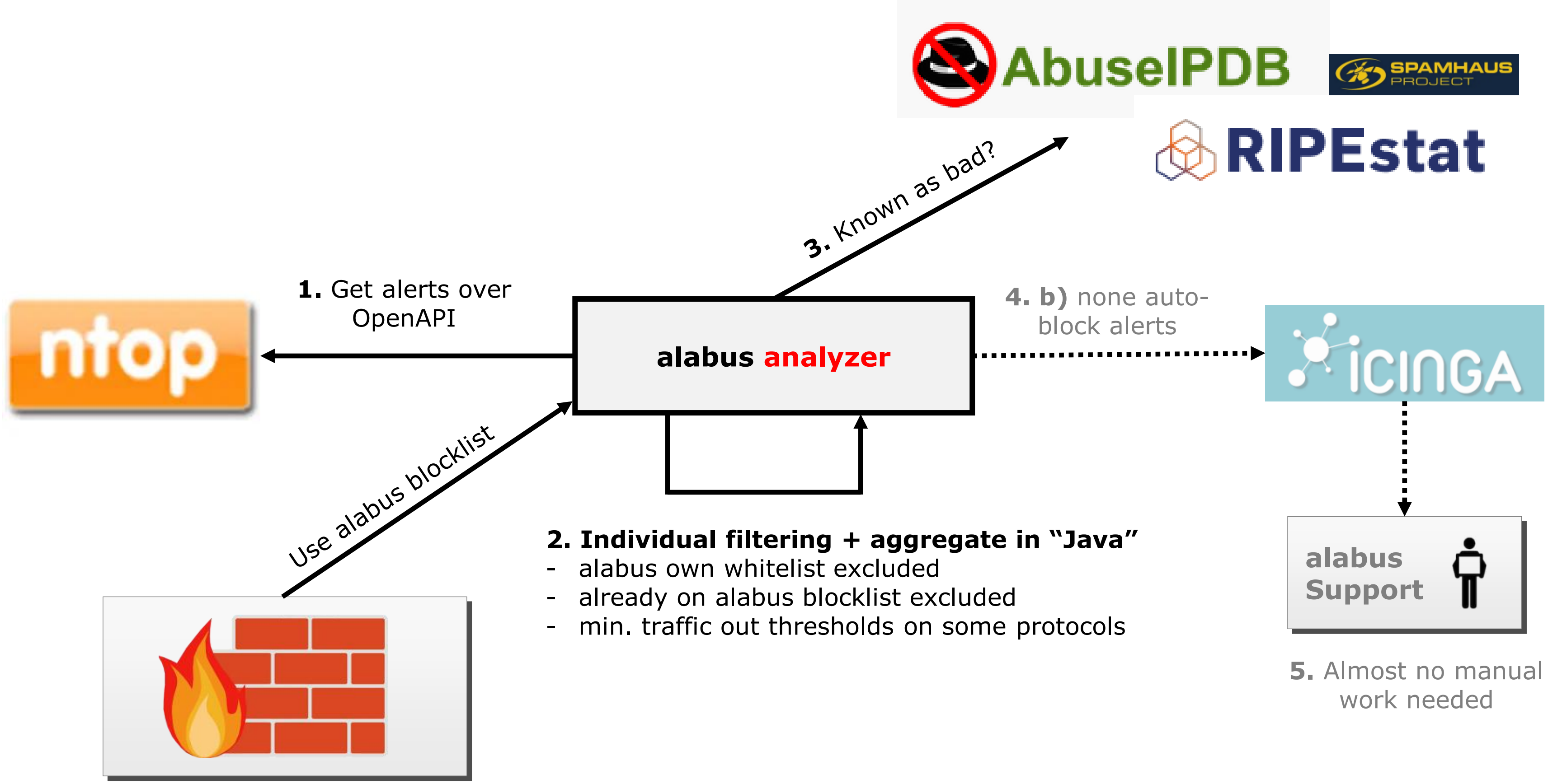
- **Limited human resources to process all alerts in near time**

- Need for an efficient solution for continuous monitoring

Our Goals with alabus analyzer

- **Alert reduction by at least 90%**
- Create a near-time, not supervised active response system
- Reduced network monitoring costs by factors

Process Overview alabus analyzer



1. Get alerts over OpenAPI

alabus analyzer

3. Known as bad?

Use alabus blocklist

4. b) none auto-block alerts

2. Individual filtering + aggregate in “Java”

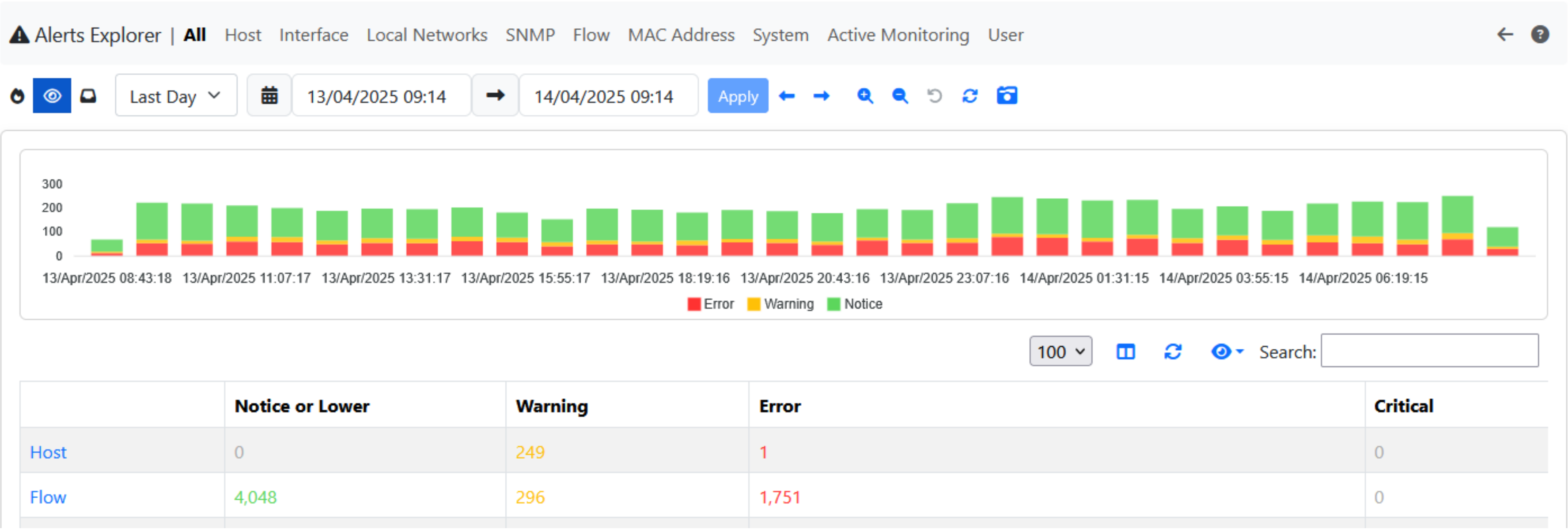
- alabus own whitelist excluded
- already on alabus blocklist excluded
- min. traffic out thresholds on some protocols

alabus Support

5. Almost no manual work needed

4. a) automatic alabus blocklist entry based on external data (AbuseIPDB + DNS blocklists)

Example day: alerts in 24h

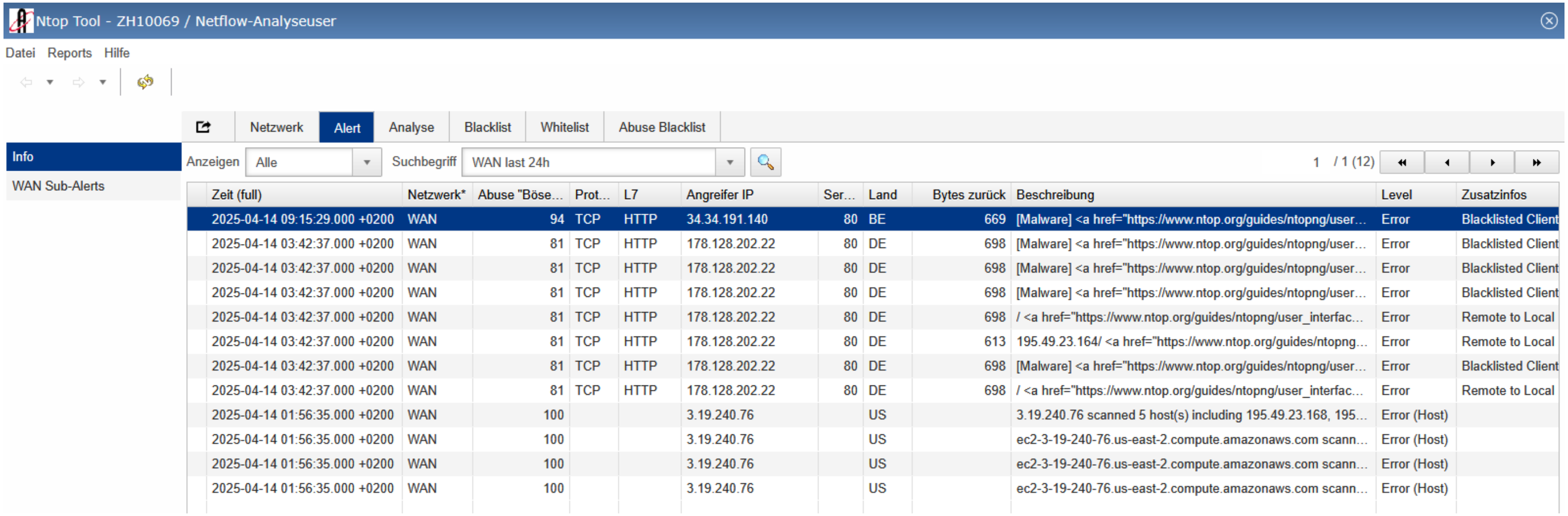


	Notice or Lower	Warning	Error	Critical
Host	0	249	1	0
Flow	4,048	296	1,751	0

2’297 host and flow alerts above level note which need human attention

-> **Very difficult to handle**

Example day: same alerts shown in alabus analyzer



Anzeigen: Alle

Suchbegriff: WAN last 24h

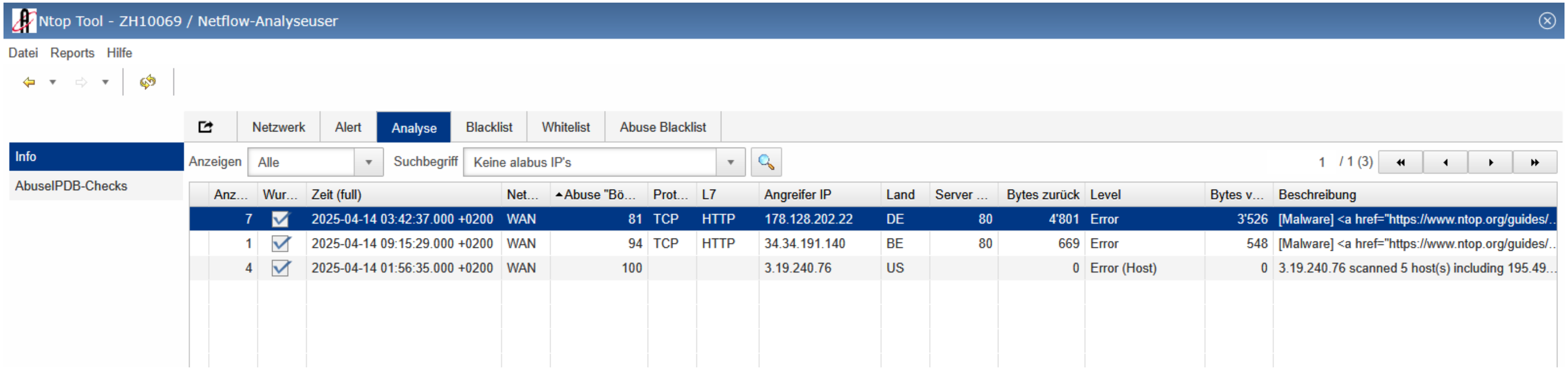
1 / 1 (12)

Zeit (full)	Netzwerk*	Abuse "Böse...	Prot...	L7	Angreifer IP	Ser...	Land	Bytes zurück	Beschreibung	Level	Zusatzinfos
2025-04-14 09:15:29.000 +0200	WAN	94	TCP	HTTP	34.34.191.140	80	BE	669	[Malware] <a href="https://www.ntop.org/guides/ntopng/user...	Error	Blacklisted Client
2025-04-14 03:42:37.000 +0200	WAN	81	TCP	HTTP	178.128.202.22	80	DE	698	[Malware] <a href="https://www.ntop.org/guides/ntopng/user...	Error	Blacklisted Client
2025-04-14 03:42:37.000 +0200	WAN	81	TCP	HTTP	178.128.202.22	80	DE	698	[Malware] <a href="https://www.ntop.org/guides/ntopng/user...	Error	Blacklisted Client
2025-04-14 03:42:37.000 +0200	WAN	81	TCP	HTTP	178.128.202.22	80	DE	698	[Malware] <a href="https://www.ntop.org/guides/ntopng/user...	Error	Blacklisted Client
2025-04-14 03:42:37.000 +0200	WAN	81	TCP	HTTP	178.128.202.22	80	DE	698	/ <a href="https://www.ntop.org/guides/ntopng/user_interfac...	Error	Remote to Local
2025-04-14 03:42:37.000 +0200	WAN	81	TCP	HTTP	178.128.202.22	80	DE	613	195.49.23.164/ <a href="https://www.ntop.org/guides/ntopng...	Error	Remote to Local
2025-04-14 03:42:37.000 +0200	WAN	81	TCP	HTTP	178.128.202.22	80	DE	698	[Malware] <a href="https://www.ntop.org/guides/ntopng/user...	Error	Blacklisted Client
2025-04-14 03:42:37.000 +0200	WAN	81	TCP	HTTP	178.128.202.22	80	DE	698	/ <a href="https://www.ntop.org/guides/ntopng/user_interfac...	Error	Remote to Local
2025-04-14 01:56:35.000 +0200	WAN	100			3.19.240.76		US		3.19.240.76 scanned 5 host(s) including 195.49.23.168, 195...	Error (Host)	
2025-04-14 01:56:35.000 +0200	WAN	100			3.19.240.76		US		ec2-3-19-240-76.us-east-2.compute.amazonaws.com scann...	Error (Host)	
2025-04-14 01:56:35.000 +0200	WAN	100			3.19.240.76		US		ec2-3-19-240-76.us-east-2.compute.amazonaws.com scann...	Error (Host)	
2025-04-14 01:56:35.000 +0200	WAN	100			3.19.240.76		US		ec2-3-19-240-76.us-east-2.compute.amazonaws.com scann...	Error (Host)	

Same list with **alabus** rules and filtered

-> Only **12** host and flow alerts needs attention

Example day: 24h semi-automated handling of alerts



Anzeigen: Alle | Suchbegriff: Keine alabus IP's | 1 / 1 (3)

Anz...	Wur...	Zeit (full)	Net...	Abuse "Bö...	Prot...	L7	Angreifer IP	Land	Server ...	Bytes zurück	Level	Bytes v...	Beschreibung
7	☑	2025-04-14 03:42:37.000 +0200	WAN	81	TCP	HTTP	178.128.202.22	DE	80	4'801	Error	3'526	[Malware] <a href="https://www.ntop.org/guides/...
1	☑	2025-04-14 09:15:29.000 +0200	WAN	94	TCP	HTTP	34.34.191.140	BE	80	669	Error	548	[Malware] <a href="https://www.ntop.org/guides/...
4	☑	2025-04-14 01:56:35.000 +0200	WAN	100			3.19.240.76	US		0	Error (Host)	0	3.19.240.76 scanned 5 host(s) including 195.49...

After analyze: only 3 alerts with high abuse IPDB level/confidence left

-> **Automatically** added to the blocklist

-> and automatically used by the firewalls

-> all our firewalls download this blocklist

-> No additional manual work is needed in this case

Final outcome alabus analyzer + ntopng

- Optimized network monitoring system for SME’s
- Up to **99.8%** reduction of alerts for human attention
- 24/7 near-time active response
- Increase network transparency and traceability
- Significant cost reduction in network monitoring
- Last but not least -> **you know what happens in your network**

Are you interested? Speak to us.

Thank you

alabus

smarter process management

Adrian Ruoss
adrian.ruoss@alabus.com

Aleksandra Haak
aleksandra.haak@alabus.com

alabus ag
Birchstrasse 189
CH-8050 Zürich

Phone: +41 44 315 18 90
Web: www.alabus.com

Certified according to
ISO 9001 and 27001

Software made
in Switzerland