Wazuh & ntopng – perfect match

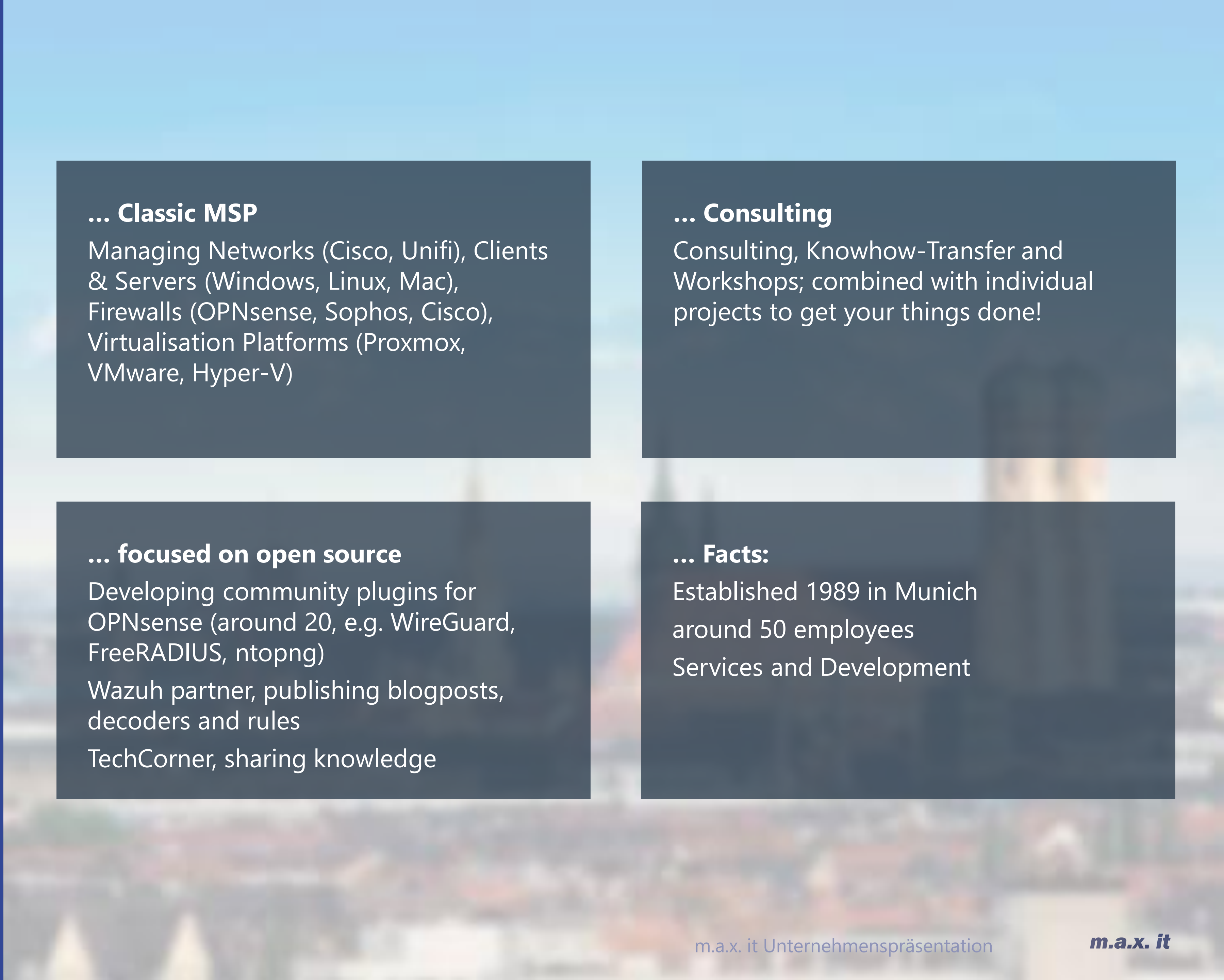
07.05.2025

Author: Michael Münz

Contact: michael.muenz@max-it.de

m.a.x. it

about us…



… Classic MSP

Managing Networks (Cisco, Unifi), Clients & Servers (Windows, Linux, Mac), Firewalls (OPNsense, Sophos, Cisco), Virtualisation Platforms (Proxmox, VMware, Hyper-V)

… Consulting

Consulting, Knowhow-Transfer and Workshops; combined with individual projects to get your things done!

… focused on open source

Developing community plugins for OPNsense (around 20, e.g. WireGuard, FreeRADIUS, ntopng)

Wazuh partner, publishing blogposts, decoders and rules

TechCorner, sharing knowledge

… Facts:

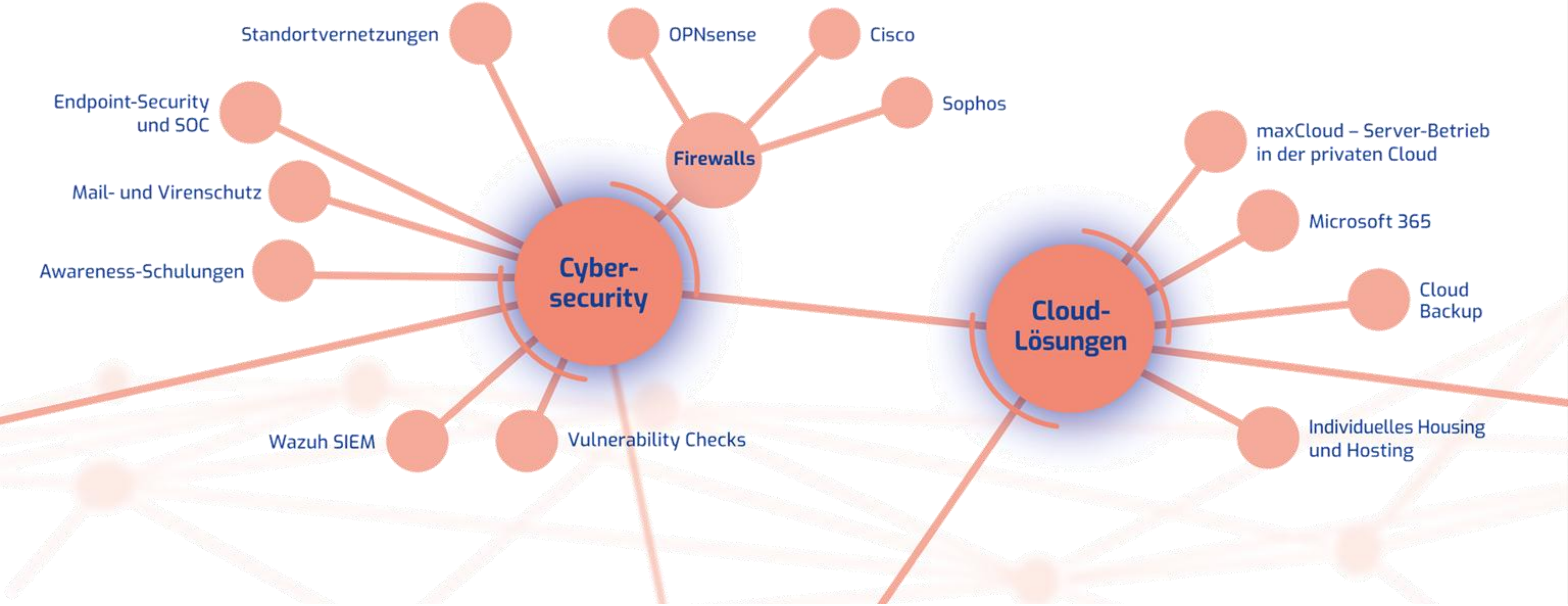
Established 1989 in Munich

around 50 employees

Services and Development

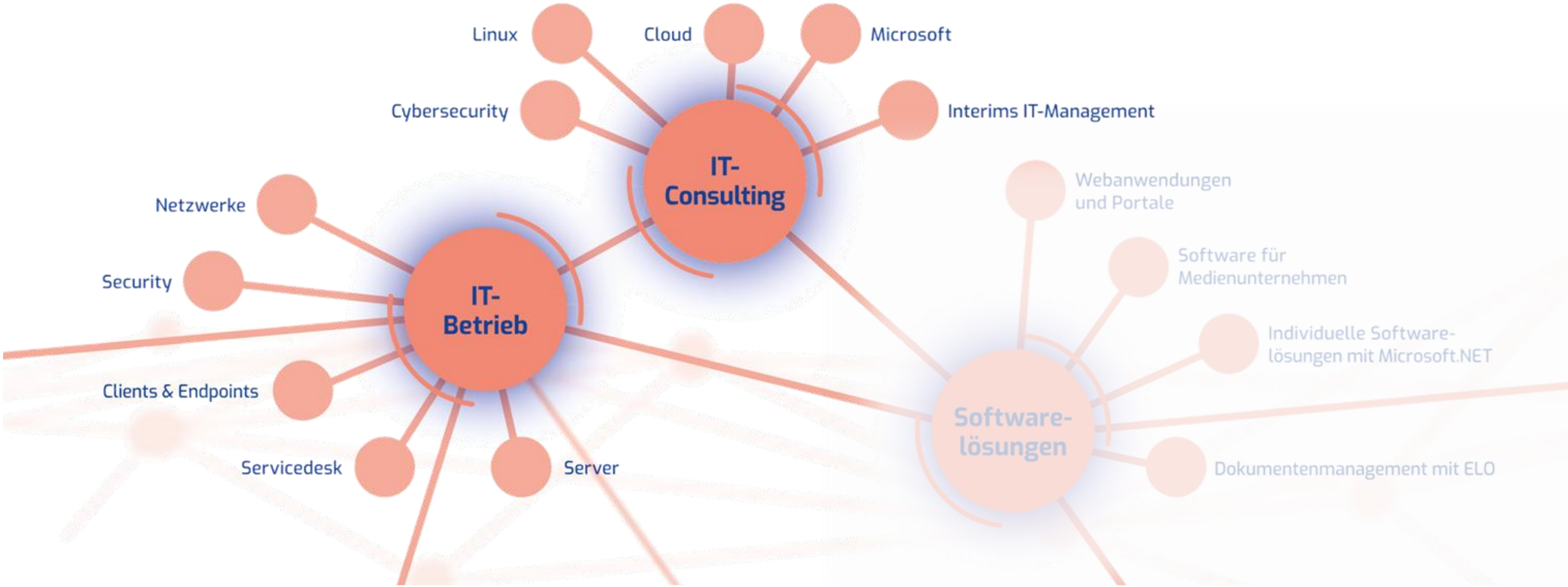
m.a.x.imum IT-Services

Infrastructure and Cybersecurity



m.a.x.imum IT-Services

Infrastructure and Cybersecurity



Wazuh

Main Features

- Centralized Log Management
  - Collect logs (agent and Syslog) from multiple servers and applications to monitor system activity and identify anomalies.
  - Generate audit trails for forensic analysis after a security incident.
- Intrusion Detection System (IDS)
  - Detect brute force attacks by monitoring unusual login attempts across systems.
  - Identify unauthorized access to sensitive files or directories in real-time.
  - Trigger alerts for suspicious network traffic patterns, such as port scanning.

Wazuh

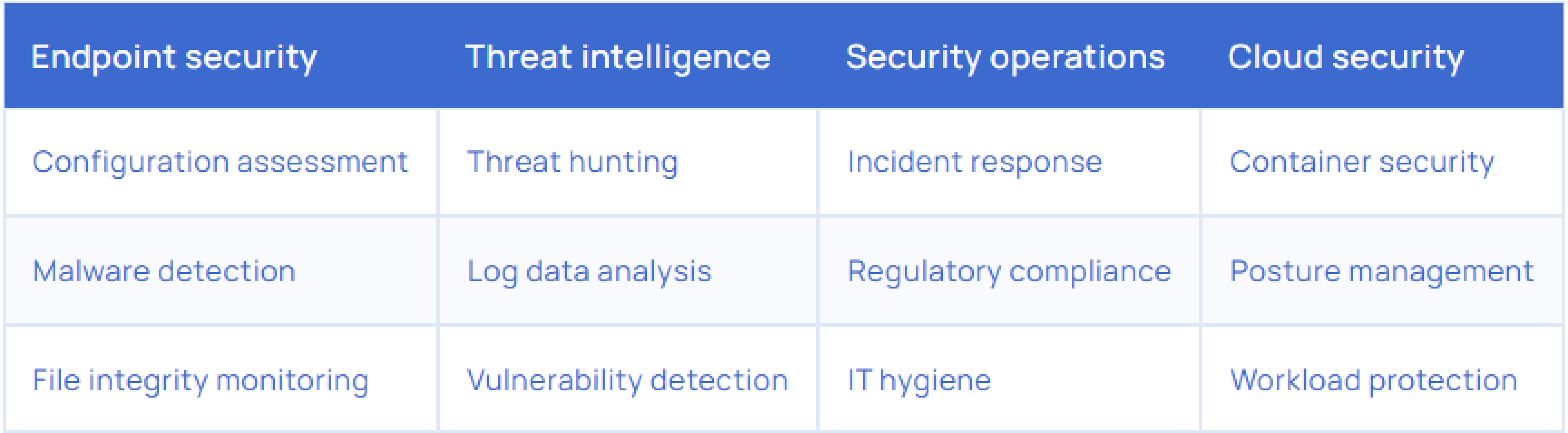
Main Features

- Vulnerability Detection
  - Scan endpoints for unpatched software vulnerabilities and generate remediation reports.
  - Ensure software compliance by detecting outdated packages or libraries.
- Compliance Management
  - Monitor system settings to ensure compliance with standards like GDPR, HIPAA, or PCI DSS.
  - Detect deviations from security baselines and enforce compliance policies.
- File Integrity Monitoring
  - Monitor critical system files for unauthorized modifications in real-time.
  - Detect tampering in web directories, preventing website defacement attacks.

Wazuh

Why Wazuh?

- Free Security Platform offering SIEM capabilities

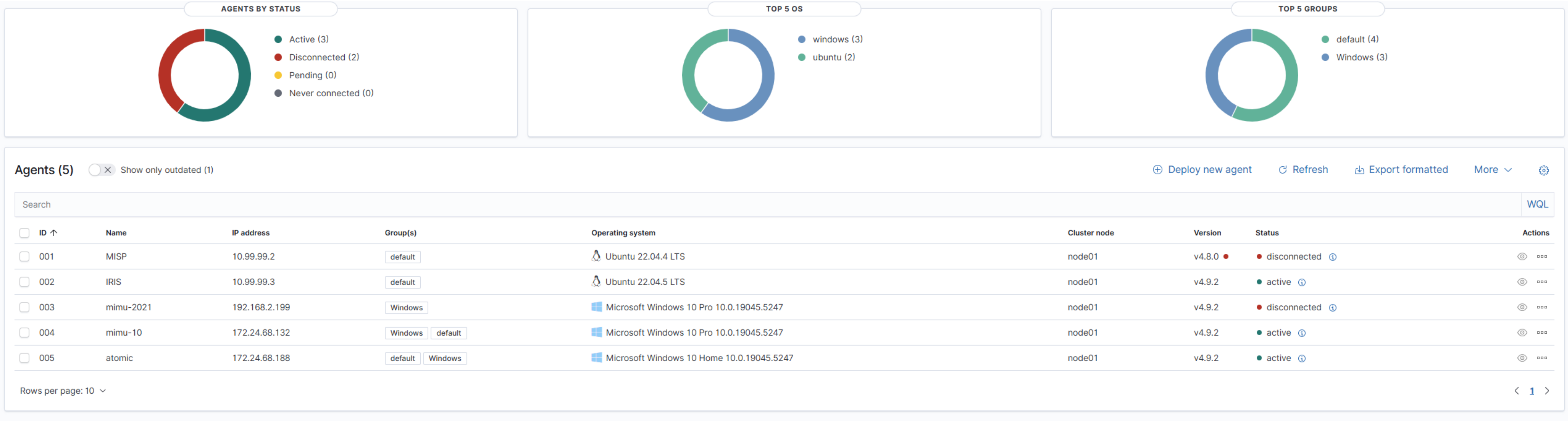


Endpoint security	Threat intelligence	Security operations	Cloud security
Configuration assessment	Threat hunting	Incident response	Container security
Malware detection	Log data analysis	Regulatory compliance	Posture management
File integrity monitoring	Vulnerability detection	IT hygiene	Workload protection

Wazuh

Agents overview

- Agent-based Log-collection (Windows, Linux, Mac, BSD), also supporting Syslog for agent-less systems like Switches, Appliances etc.

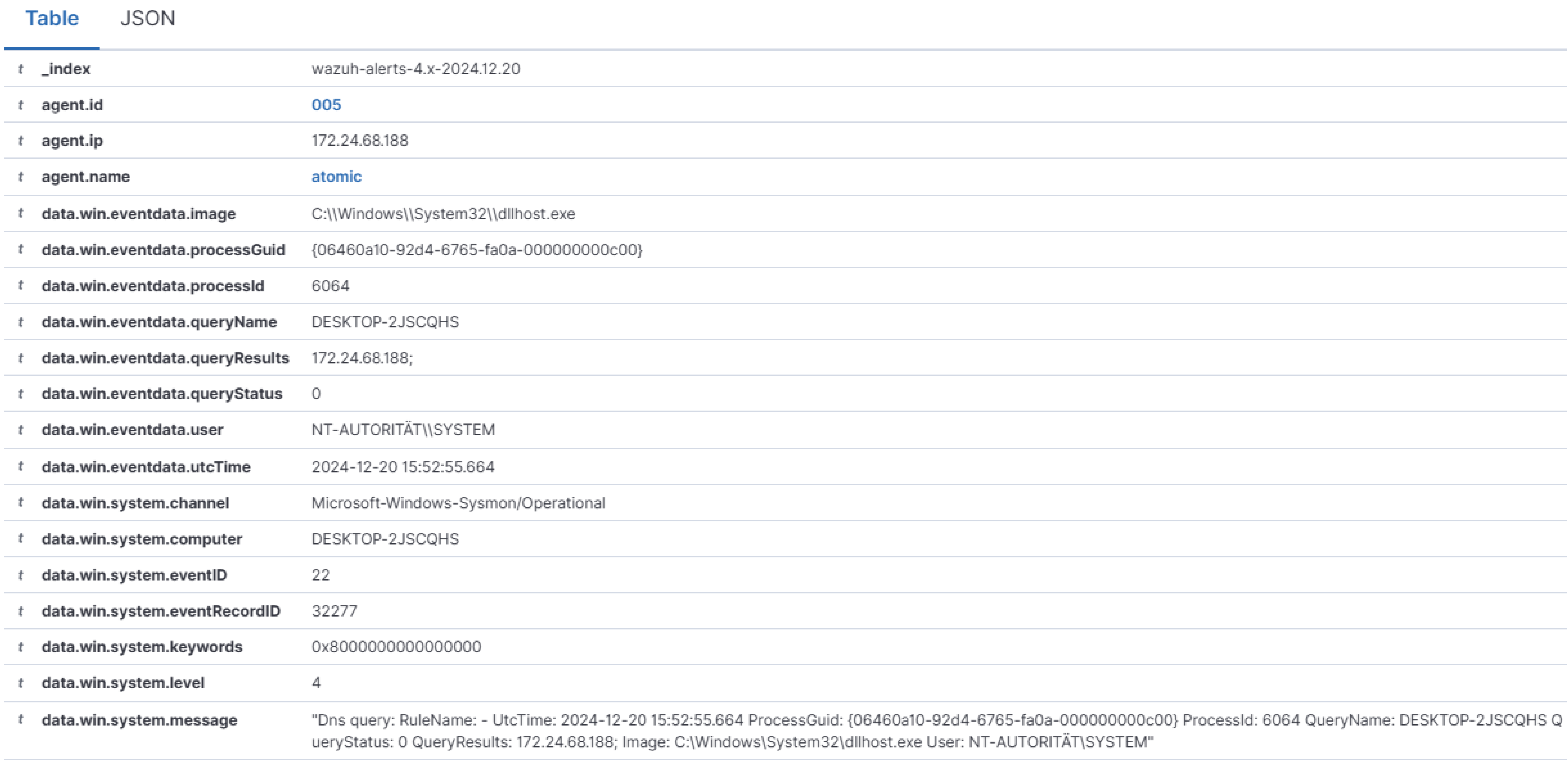


ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	MISP	10.99.99.2	default	Ubuntu 22.04.4 LTS	node01	v4.8.0 ●	● disconnected	
002	IRIS	10.99.99.3	default	Ubuntu 22.04.5 LTS	node01	v4.9.2	● active	
003	mimu-2021	192.168.2.199	Windows	Microsoft Windows 10 Pro 10.0.19045.5247	node01	v4.9.2	● disconnected	
004	mimu-10	172.24.68.132	Windows default	Microsoft Windows 10 Pro 10.0.19045.5247	node01	v4.9.2	● active	
005	atomic	172.24.68.188	default Windows	Microsoft Windows 10 Home 10.0.19045.5247	node01	v4.9.2	● active	

Wazuh

Threat hunting

- Search logs, filter by decoded fields, create visualisations like top X attackers

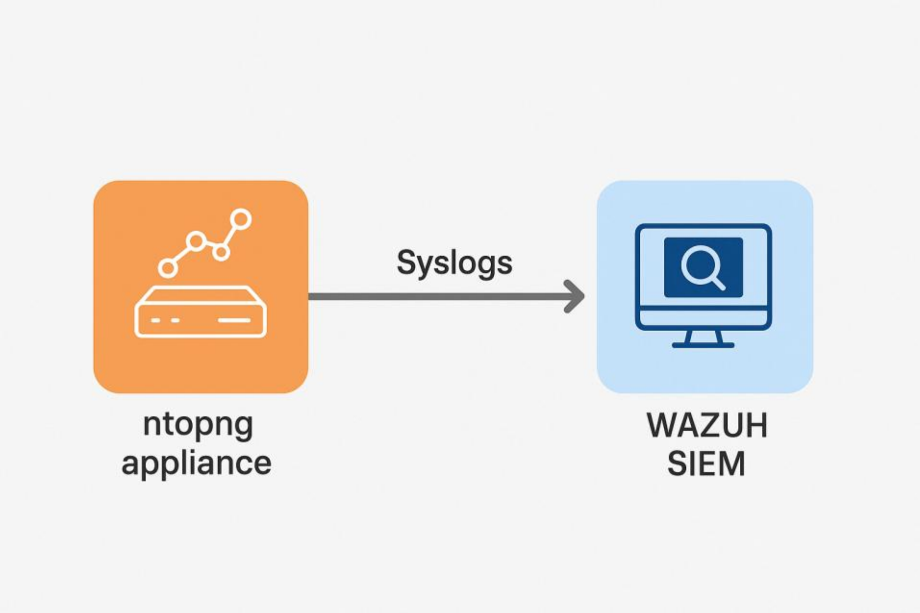


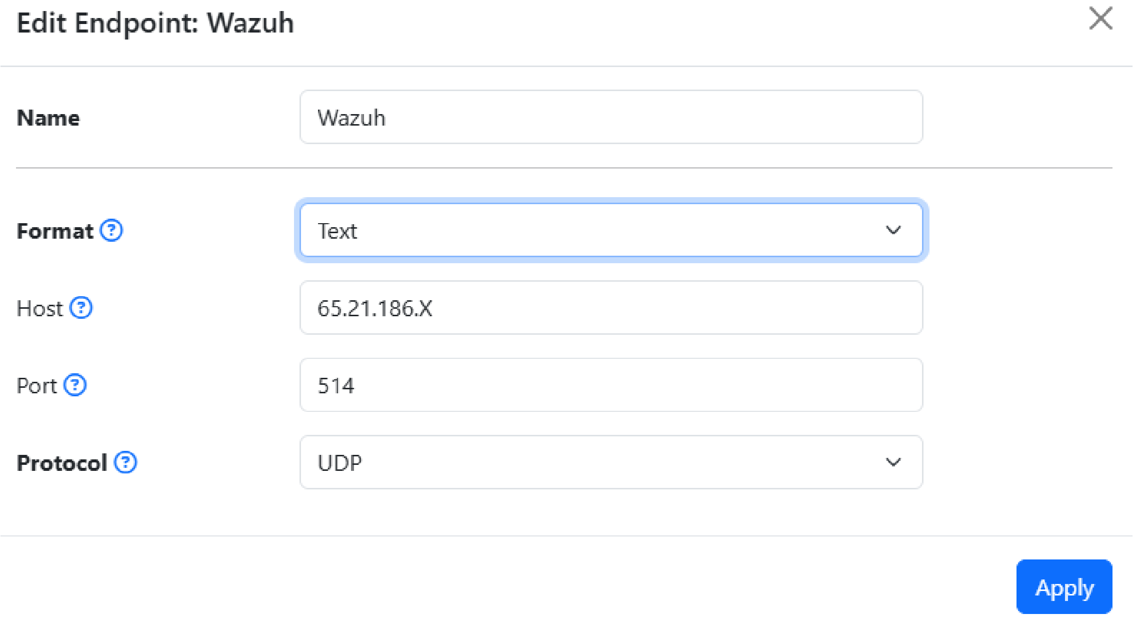
_index	wazuh-alerts-4.x-2024.12.20
agent.id	005
agent.ip	172.24.68.188
agent.name	atomic
data.win.eventdata.image	C:\\Windows\\System32\\dllhost.exe
data.win.eventdata.processGuid	{06460a10-92d4-6765-fa0a-000000000c00}
data.win.eventdata.processId	6064
data.win.eventdata.queryName	DESKTOP-2JSCQHS
data.win.eventdata.queryResults	172.24.68.188;
data.win.eventdata.queryStatus	0
data.win.eventdata.user	NT-AUTORITÄT\\SYSTEM
data.win.eventdata.utcTime	2024-12-20 15:52:55.664
data.win.system.channel	Microsoft-Windows-Sysmon/Operational
data.win.system.computer	DESKTOP-2JSCQHS
data.win.system.eventID	22
data.win.system.eventRecordID	32277
data.win.system.keywords	0x8000000000000000
data.win.system.level	4
data.win.system.message	"Dns query: RuleName: - UtcTime: 2024-12-20 15:52:55.664 ProcessGuid: {06460a10-92d4-6765-fa0a-000000000c00} ProcessId: 6064 QueryName: DESKTOP-2JSCQHS QueryStatus: 0 QueryResults: 172.24.68.188; Image: C:\Windows\System32\dllhost.exe User: NT-AUTORITÄT\SYSTEM"

ntopng

Connecting Wazuh

- Send Syslog events to Wazuh via System -> Notifictions -> Endpoint:





Edit Endpoint: Wazuh

Name	Wazuh
Format	Text
Host	65.21.186.X
Port	514
Protocol	UDP

ntopng

Connecting Wazuh

- Formats available in community edition are Text, Text(5424) and Raw JSON
  - We developed decoders and rules only for Text as Raw JSON is too raw for extracting fields
- Formats in pro edition are ECS and check_mk in addition
  - We also developed decoders and rules for ECS which uses JSON without escaping
- In System -> Notifications -> Recipients you need to define alert levels to send and link to Syslog endpoint
- That‘s all for ntopng!

Wazuh

Install ntop additions

- Easiest way to install decoders and rules:
    - SSH into your Wazuh instance and download decoders and rules
        - wget https://raw.githubusercontent.com/mimugmail/wazuh-ntop/refs/heads/main/rules/ntopng_ecs_rules.xml -o /var/ossec/etc/rules/ntopng_ecs_rules.xml

        OR

        - wget https://raw.githubusercontent.com/mimugmail/wazuh-ntop/refs/heads/main/rules/ntopng_text_rules.xml -o /var/ossec/etc/rules/ntopng_text_rules.xml
        - wget https://raw.githubusercontent.com/mimugmail/wazuh-ntop/refs/heads/main/decoders/ntopng_json_decoder.xml -o /var/ossec/etc/decoders/ntopng_json_decoder.xml

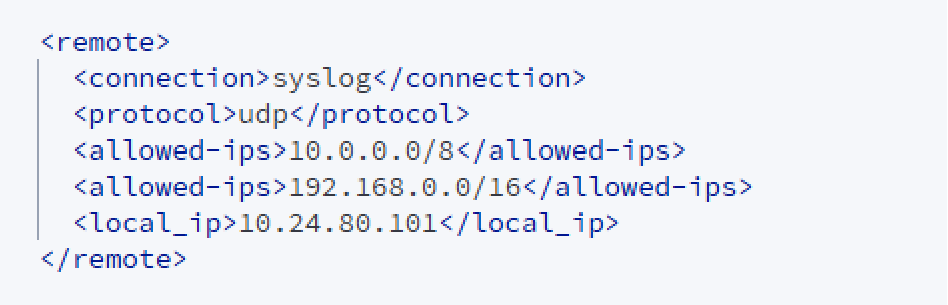
        OR

        - wget https://raw.githubusercontent.com/mimugmail/wazuh-ntop/refs/heads/main/decoders/ntopng_text_decoder.xml -o /var/ossec/etc/decoders/ntopng_text_decoder.xml
    - /var/ossec/bin/wazuh-control restart

Wazuh

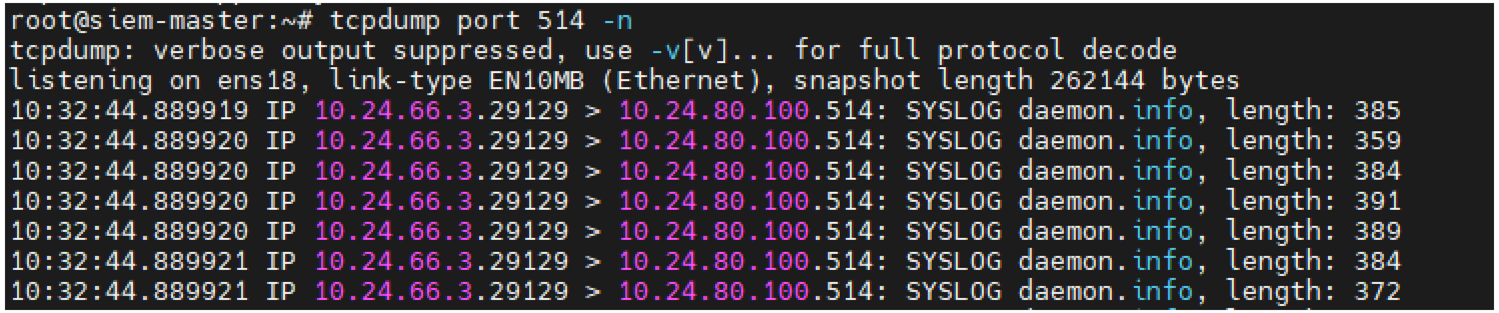
Syslog

- Enable native Syslog (https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/syslog.html)



```
<remote>
  <connection>syslog</connection>
  <protocol>udp</protocol>
  <allowed-ips>10.0.0.0/8</allowed-ips>
  <allowed-ips>192.168.0.0/16</allowed-ips>
  <local_ip>10.24.80.101</local_ip>
</remote>
```

- Check via console for arriving packets:

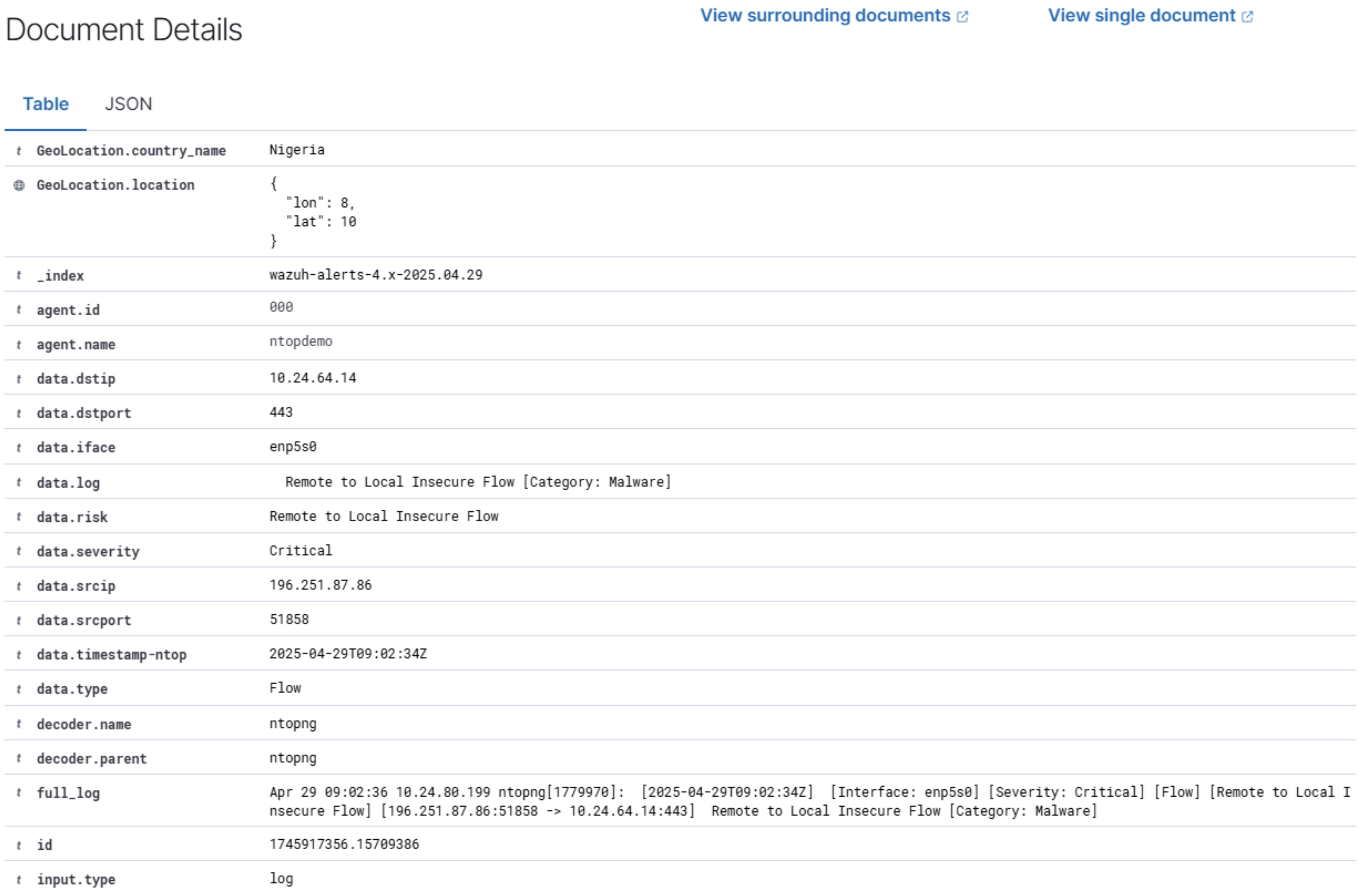


```
root@siem-master:~# tcpdump port 514 -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens18, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:32:44.889919 IP 10.24.66.3.29129 > 10.24.80.100.514: SYSLOG daemon.info, length: 385
10:32:44.889920 IP 10.24.66.3.29129 > 10.24.80.100.514: SYSLOG daemon.info, length: 359
10:32:44.889920 IP 10.24.66.3.29129 > 10.24.80.100.514: SYSLOG daemon.info, length: 384
10:32:44.889920 IP 10.24.66.3.29129 > 10.24.80.100.514: SYSLOG daemon.info, length: 391
10:32:44.889920 IP 10.24.66.3.29129 > 10.24.80.100.514: SYSLOG daemon.info, length: 389
10:32:44.889921 IP 10.24.66.3.29129 > 10.24.80.100.514: SYSLOG daemon.info, length: 384
10:32:44.889921 IP 10.24.66.3.29129 > 10.24.80.100.514: SYSLOG daemon.info, length: 372
```

Wazuh

Sample alerts

- Detect alerts …
- Geo Location included
- Further debug in ntopng



Document Details

View surrounding documents ↗ View single document ↗

Table JSON

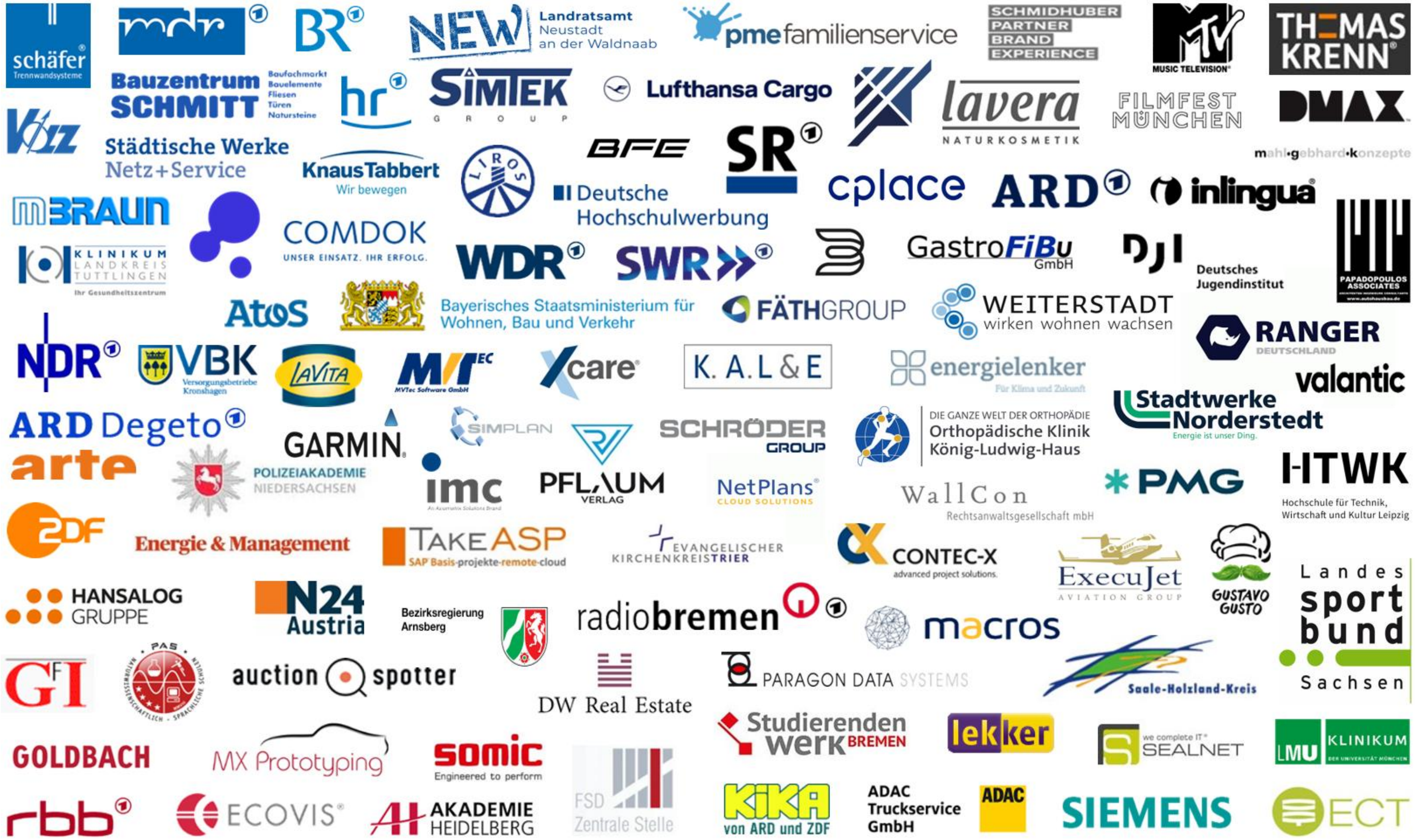
t	GeoLocation.country_name	Nigeria
⊕	GeoLocation.location	{ "lon": 8, "lat": 10 }
t	_index	wazuh-alerts-4.x-2025.04.29
t	agent.id	000
t	agent.name	ntopdemo
t	data.dstip	10.24.64.14
t	data.dstport	443
t	data.iface	enp5s0
t	data.log	Remote to Local Insecure Flow [Category: Malware]
t	data.risk	Remote to Local Insecure Flow
t	data.severity	Critical
t	data.srcip	196.251.87.86
t	data.srcport	51858
t	data.timestamp-ntop	2025-04-29T09:02:34Z
t	data.type	Flow
t	decoder.name	ntopng
t	decoder.parent	ntopng
t	full_log	Apr 29 09:02:36 10.24.80.199 ntopng[1779970]: [2025-04-29T09:02:34Z] [Interface: enp5s0] [Severity: Critical] [Flow] [Remote to Local Insecure Flow] [196.251.87.86:51858 -> 10.24.64.14:443] Remote to Local Insecure Flow [Category: Malware]
t	id	1745917356.15709386
t	input.type	log

Wazuh

What‘s next?

- Please fork and contribute PRs back to make rules and decoders better!
- Add more rules for undecoded logs
- Extract more information from text log to build nice graphs!

Our customers …


schäfer Trennwandsysteme
mdr
BR
NEW
Landratsamt Neustadt an der Waldnaab
pme familienservice
SCHMIDHUBER PARTNER BRAND EXPERIENCE
MTV MUSIC TELEVISION
THOMAS KRENN
Bauzentrum SCHMITT Baufachmarkt Bauelemente Fliesen Türen Natursteine
hr
SIMTEK GROUP
Lufthansa Cargo
lavera NATURKOSMETIK
FILMFEST MÜNCHEN
DMAX
VDZ
Städtische Werke Netz+Service
KnausTabbert Wir bewegen
LIROS
BFE
SR
mahl·gebhard·konzepte
Deutsche Hochschulwerbung
cplace
ARD
inlingua
mBRAUN
COMDOK UNSER EINSATZ. IHR ERFOLG.
WDR
SWR
GastroFiBu GmbH
DJI Deutsches Jugendinstitut
PAPADOPOULOS ASSOCIATES
KLINIKUM LANDKREIS TUTTLINGEN Ihr Gesundheitszentrum
Atos
Bayerisches Staatsministerium für Wohnen, Bau und Verkehr
FÄTHGROUP
WEITERSTADT wirken wohnen wachsen
RANGER DEUTSCHLAND
NDR
VBK Versorgungsbetriebe Kronshagen
LaVita
MVTEC MVTec Software GmbH
Xcare
K.A.L&E
energielenker Für Klima und Zukunft
valantic
ARD Degeto
Stadtwerke Norderstedt Energie ist unser Ding.
arte
GARMIN.
SIMPLAN
SCHRÖDER GROUP
DIE GANZE WELT DER ORTHOPÄDIE Orthopädische Klinik König-Ludwig-Haus
POLIZEIAKADEMIE NIEDERSACHSEN
imc
PFLAUM VERLAG
NetPlans CLOUD SOLUTIONS
WallCon Rechtsanwaltsgesellschaft mbH
PMG
HTWK Hochschule für Technik, Wirtschaft und Kultur Leipzig
ZDF
Energie & Management
TAKEASP SAP Basis-projekte-remote-cloud
EVANGELISCHER KIRCHENKREIS TRIER
CONTEC-X advanced project solutions.
ExecuJet AVIATION GROUP
GUSTAVO GUSTO
Landessportbund Sachsen
HANSALOG GRUPPE
N24 Austria
Bezirksregierung Arnsberg
radiobremen
macros
GFI
PAS
auction spotter
DW Real Estate
PARAGON DATA SYSTEMS
Saale-Holzland-Kreis
GOLDBACH
MX Prototyping
somic Engineered to perform
FSD Zentrale Stelle
Studierendenwerk BREMEN
lekker
we complete IT SEALNET
LMU KLINIKUM DER UNIVERSITÄT MÜNCHEN
rbb
ECOVIS
AH AKADEMIE HEIDELBERG
KiKA von ARD und ZDF
ADAC Truckservice GmbH
ADAC
SIEMENS
ECT