

CYBERSEC 2025
臺灣資安大會

4/15 - 4/17
臺北南港展覽二館

Open
Source Security
Forum

OPEN SOURCE SECURITY FORUM

Wazuh 打造 XDR 資安防護機制經驗分享

鄭郁霖 Jason Cheng

節省工具箱有限公司

技術總監

TEAM
CYBERSECURITY



鄭郁霖

JASON CHENG

節省工具箱有限公司 / 創辦人兼技術總監

中華民國軟體自由協會 / 常務理事

耀達電腦、晟鑫科技、五倍紅寶石、豐康科技 / 技術顧問

資展國際、崑山科大推廣教育 / 講師

2020, 2022 InfoSec Taiwan 台灣國際資安大會 / 講者

2020 COSCUP 開源人年會 / 講者

2019 OpenInfra Days Taiwan / 講者

2019, 2024, 2025 CyberSec Taiwan 台灣資安大會 / 講者

2018, 2019 國際資訊安全組織台灣高峰會 / 講者

CEH, ISO 27001 LA

做資安
XDR
很重要

知道為啥不買？

旁邊加注音表示這是基本啊！

錢能解決的問題都不是問題



問題是沒有錢

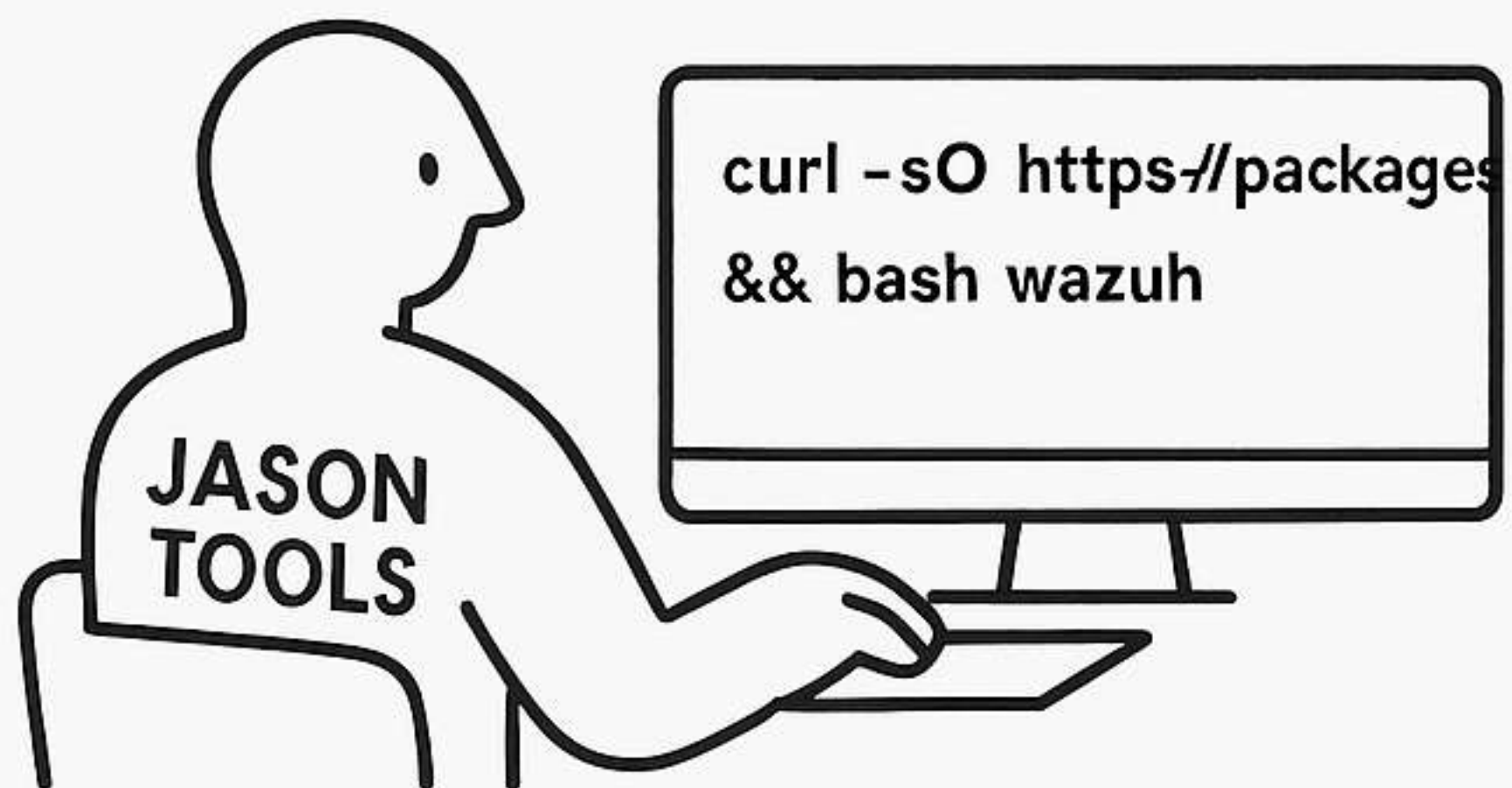


難嗎？不難！

四步上線

簡單到爆

1 EASY INSTALL



2 LOGIN WEBUI



3 DEPLOY AGENT



4 OPEN DASHBOARD

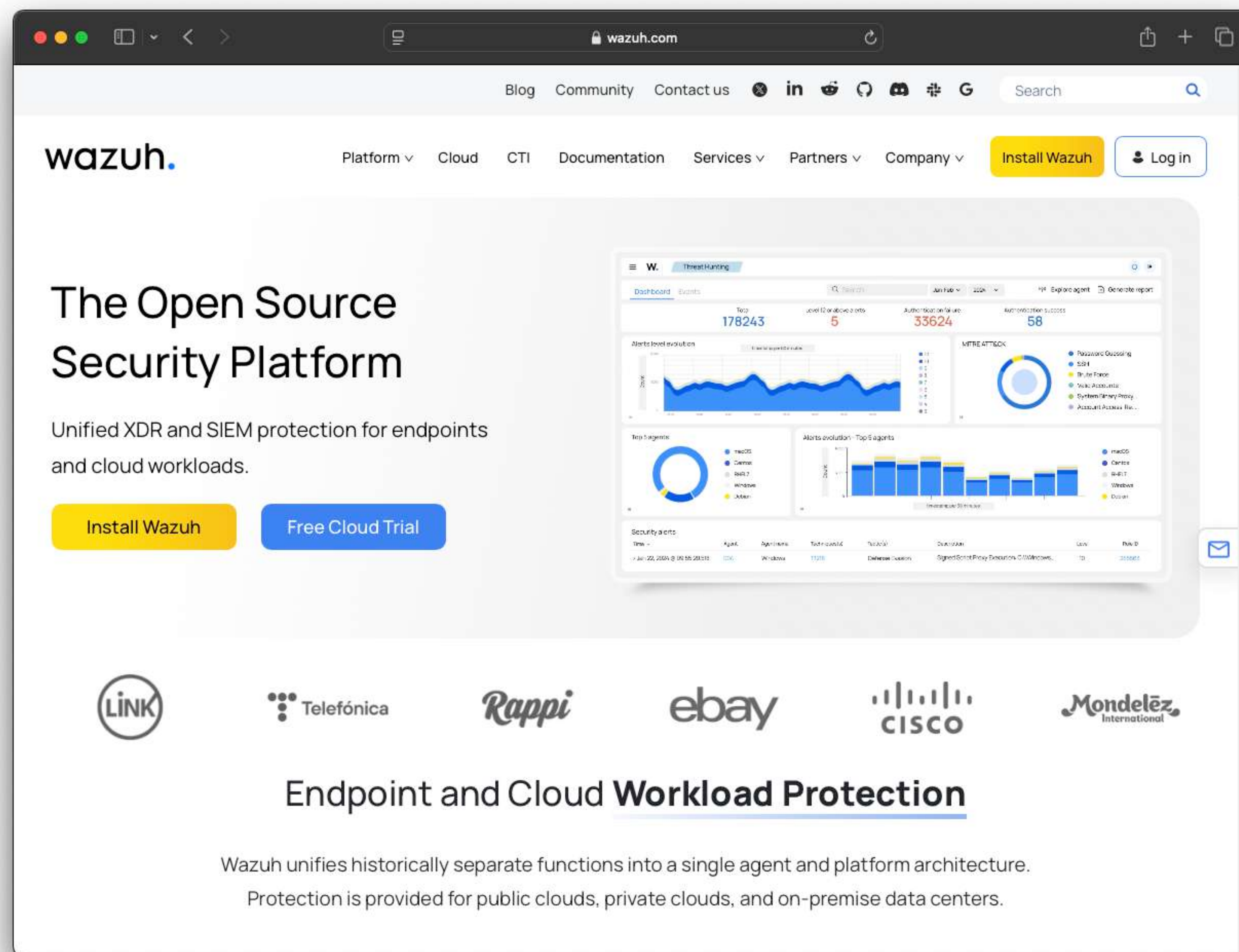


OK!!

功能概觀

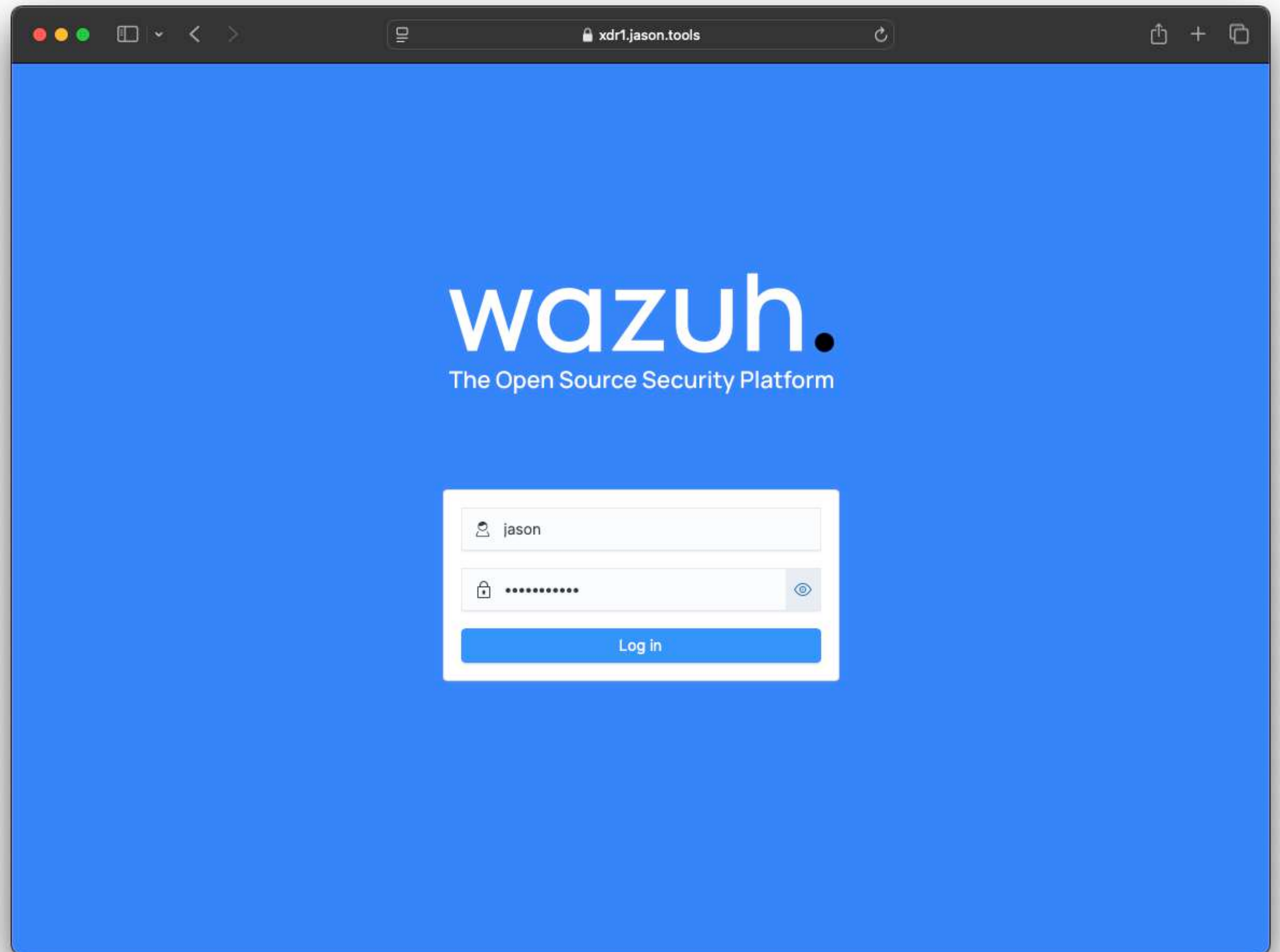
Wazuh

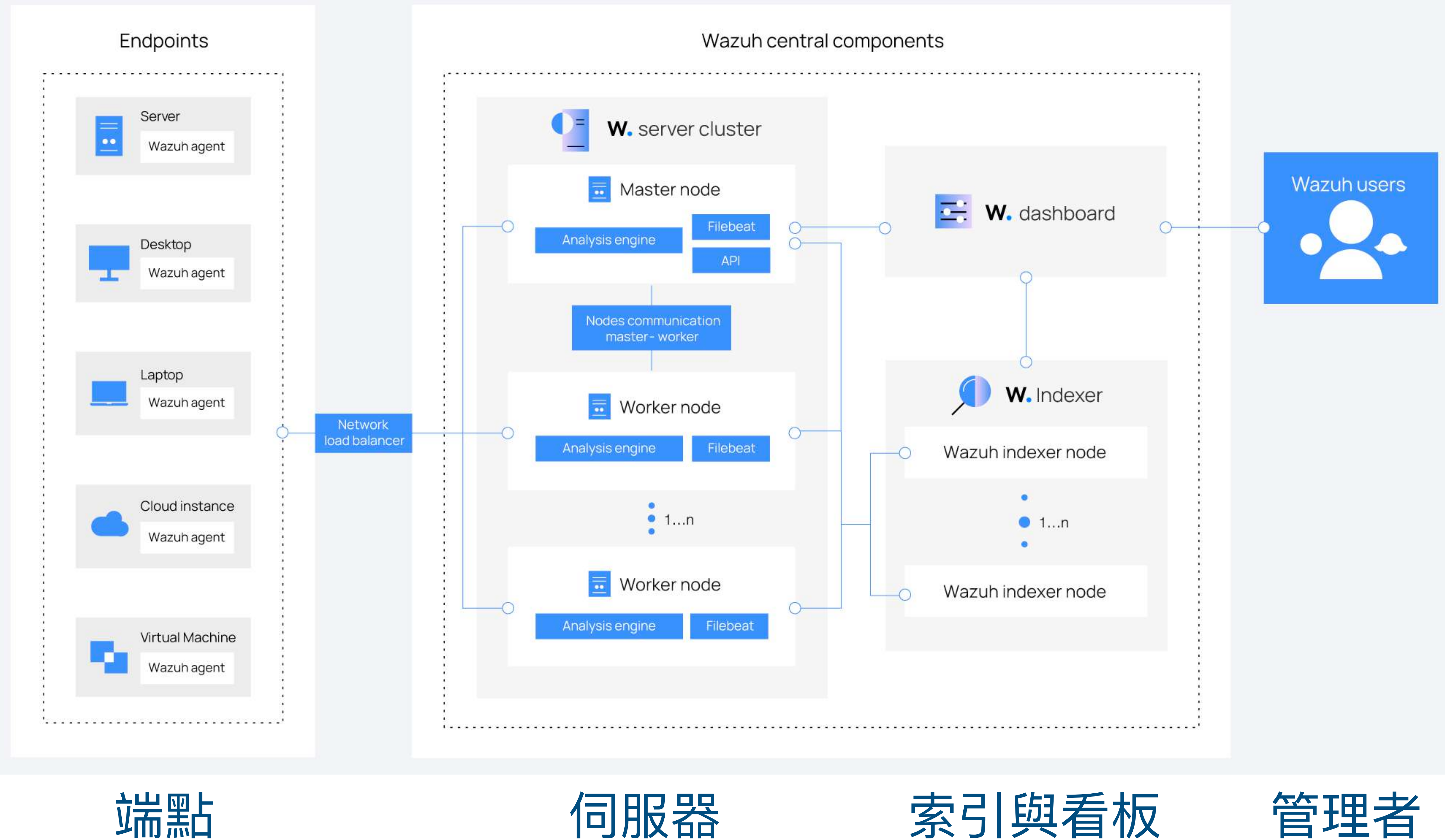
- 商業公司
- 美國
- 開源軟體
- 商業服務



系統特點

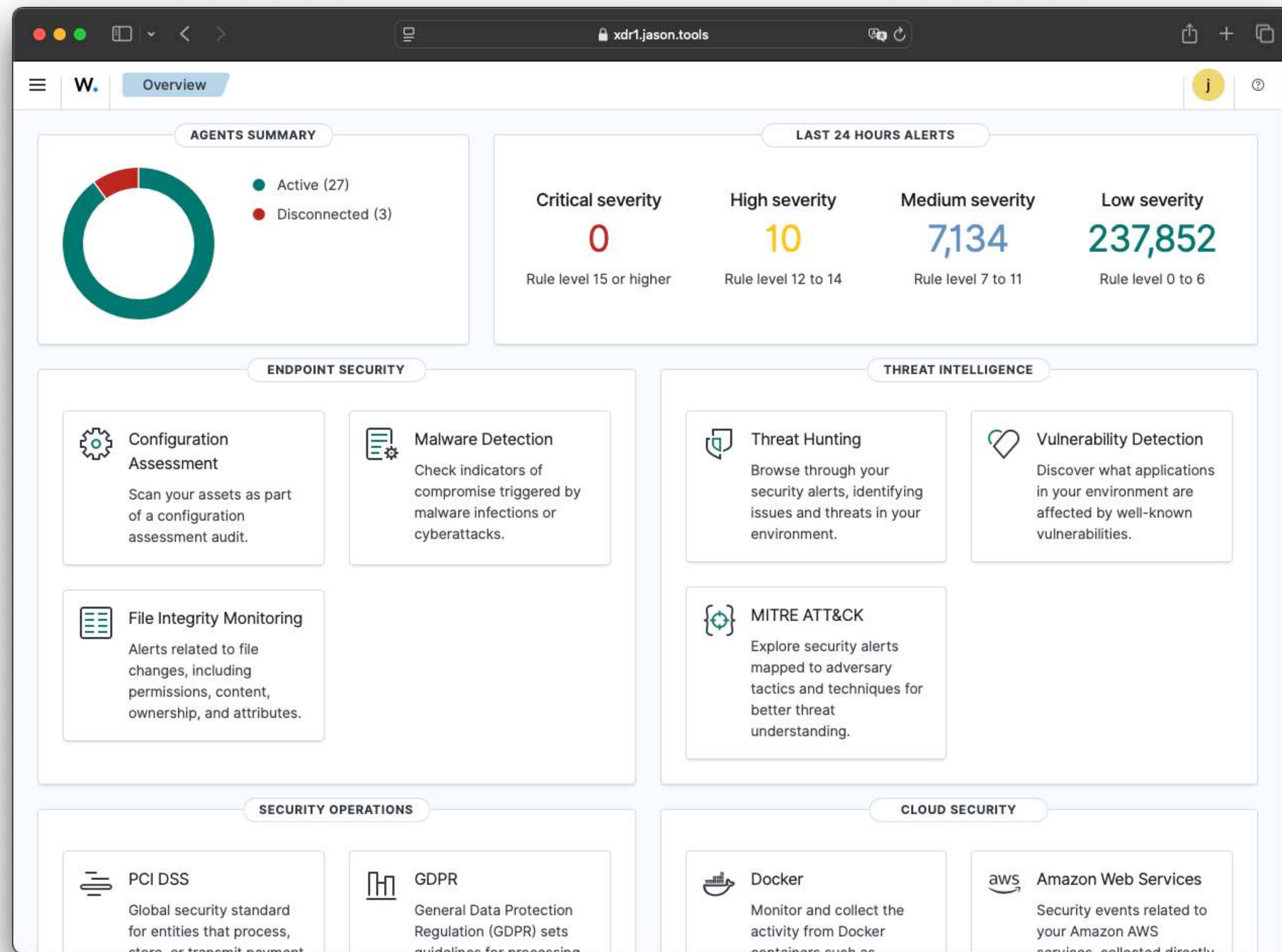
- 功能豐富
- 網頁管理
- 叢集架構
- 開放源碼
- 跨平台





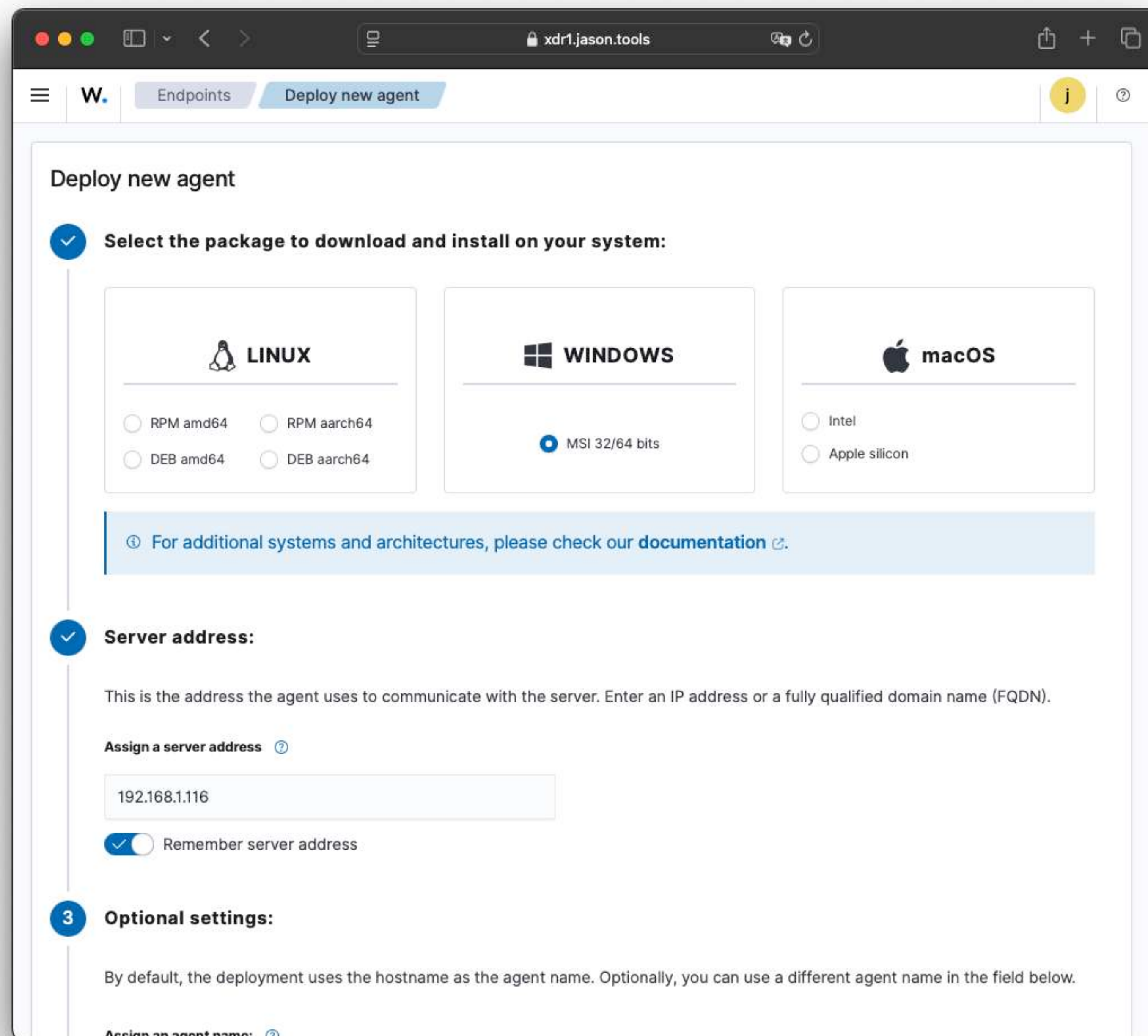
主要功能

- 記錄分析
- 入侵檢測
- 漏洞檢測
- 檔案監控
- 設置評估
- 情資整合



端點

- Linux
- Windows (XP~11/2025)
- macOS (Sierra~)
- Solaris (10~11)
- AIX
- HP-UX
- FreeBSD (OPNsense)



The screenshot shows a web browser window with the URL `xdr1.jason.tools`. The page has a navigation bar with a hamburger menu, a 'W.' logo, and tabs for 'Endpoints' and 'Deploy new agent'. The 'Deploy new agent' tab is active. The main content area is titled 'Deploy new agent' and contains three steps:

- 1 Select the package to download and install on your system:**
 - LINUX:** Includes radio buttons for RPM amd64, RPM aarch64, DEB amd64, and DEB aarch64.
 - WINDOWS:** Includes a radio button for MSI 32/64 bits.
 - macOS:** Includes radio buttons for Intel and Apple silicon.
 - A blue banner below the OS boxes states: "For additional systems and architectures, please check our [documentation](#)."
- 2 Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address ?

192.168.1.116

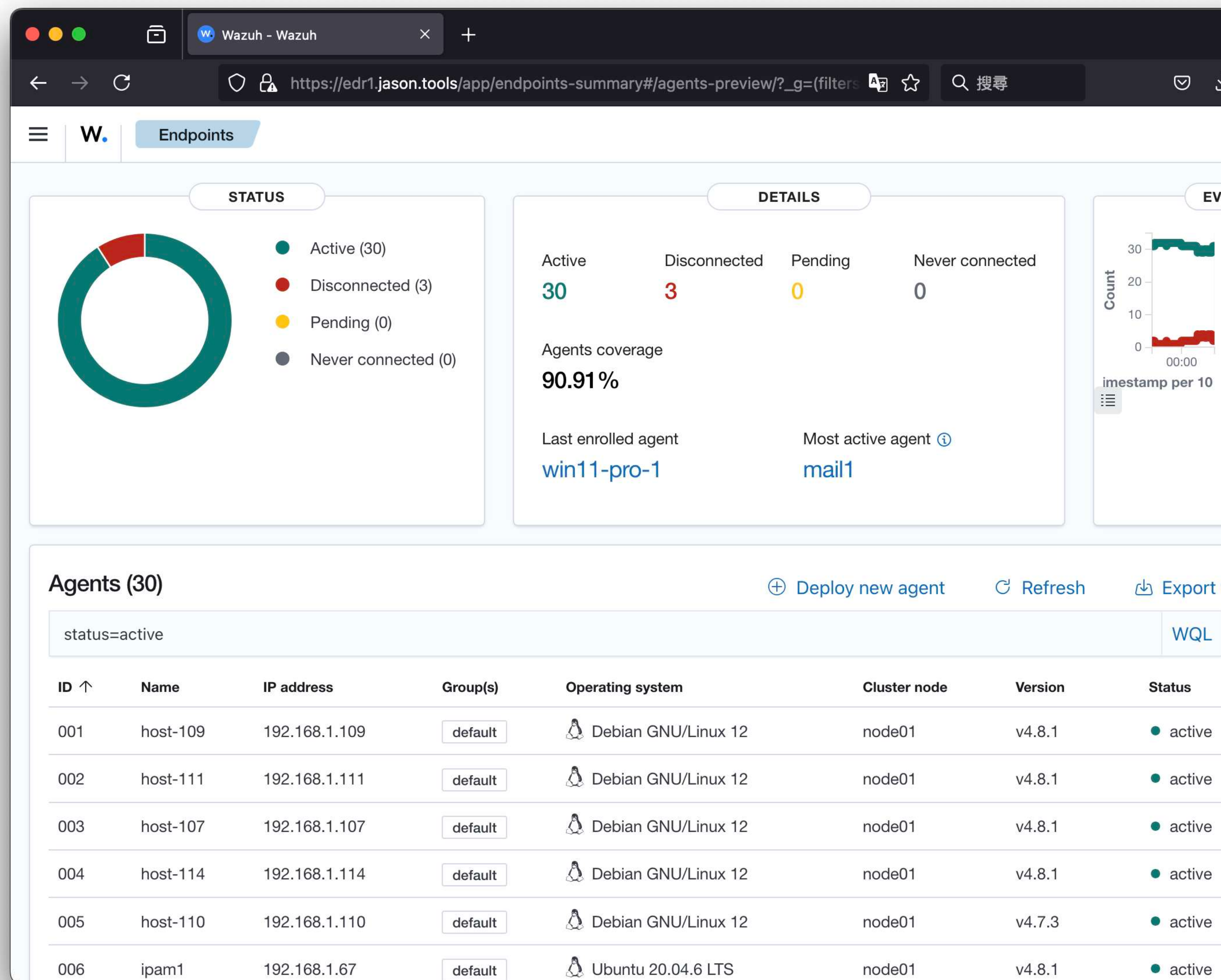
☒ Remember server address
- 3 Optional settings:**

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: ?

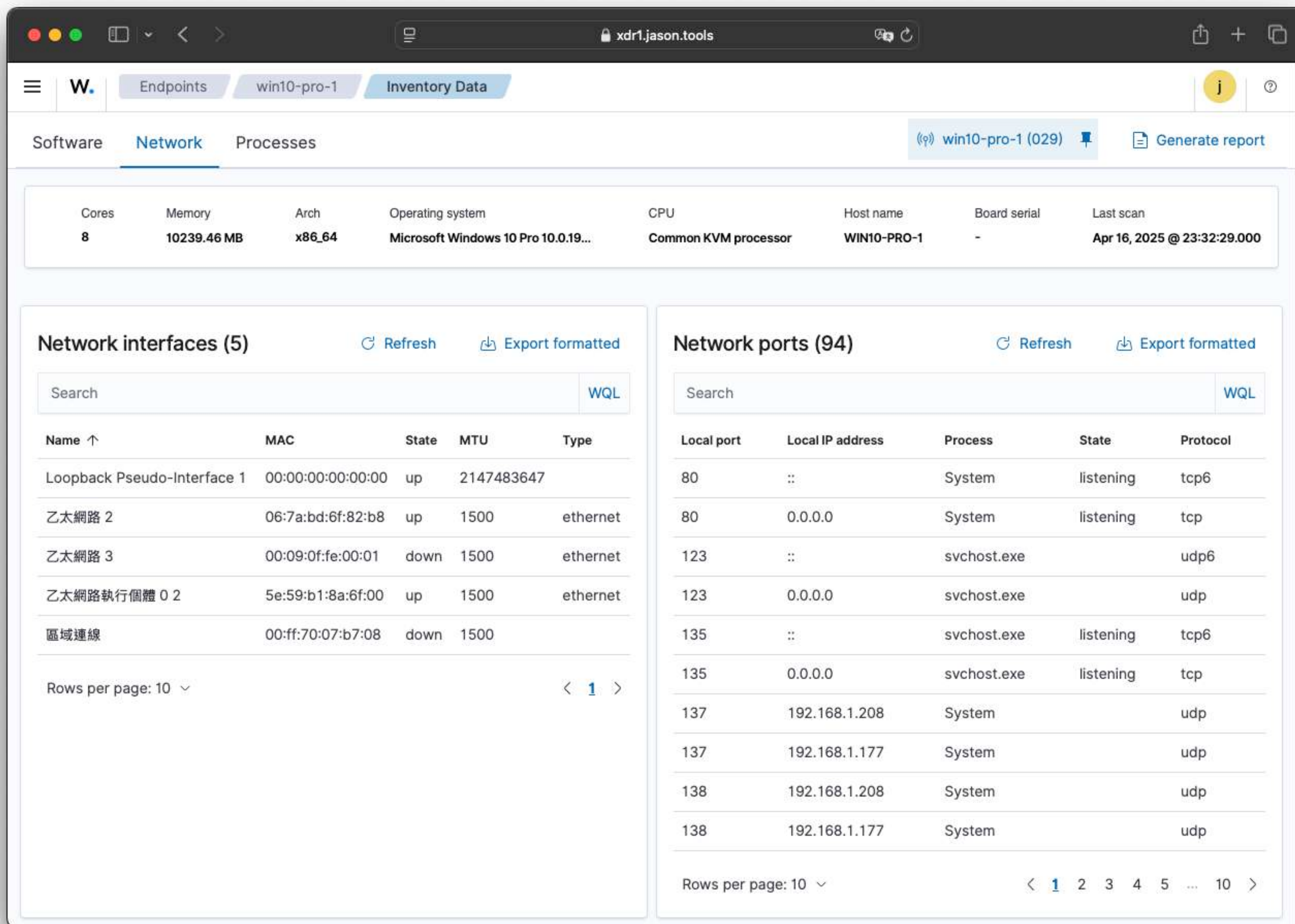
端點管理

- 連線狀況
- 端點名稱
- 端點位址
- 作業系統
- 程式版本
- 最後連線時間



端點資產

- 網路介面
- 網路連接埠
- 網路設定
- 系統更新
- 安裝軟體
- 處理程序



The screenshot displays the 'Inventory Data' section for endpoint 'win10-pro-1'. It includes a summary bar with system details and two main panels: 'Network interfaces (5)' and 'Network ports (94)'. Both panels have search bars, 'Refresh' and 'Export formatted' buttons, and a 'WQL' link. The network interfaces table lists various interfaces with their MAC addresses, states, and MTUs. The network ports table lists open ports with their local IP addresses, processes, states, and protocols.

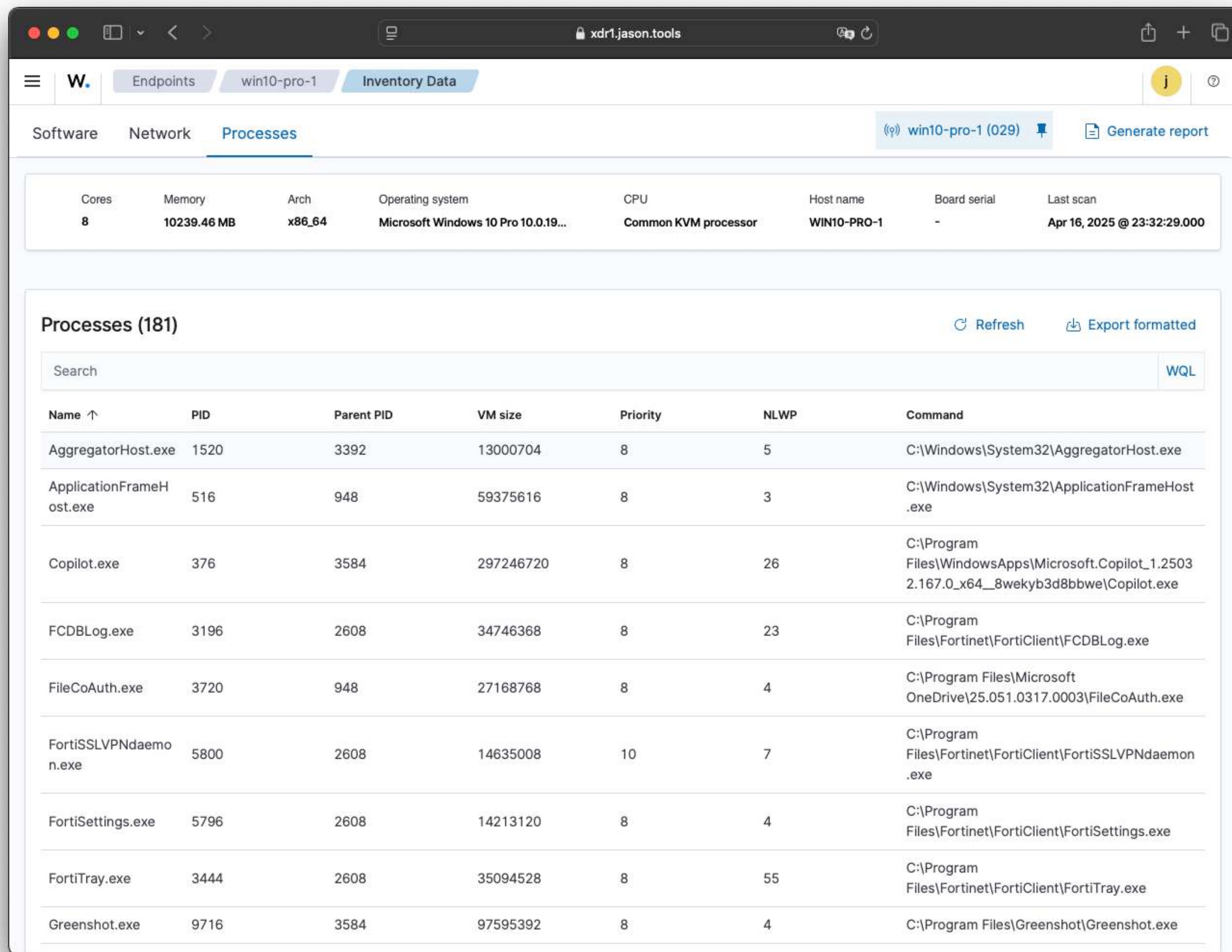
Cores	Memory	Arch	Operating system	CPU	Host name	Board serial	Last scan
8	10239.46 MB	x86_64	Microsoft Windows 10 Pro 10.0.19...	Common KVM processor	WIN10-PRO-1	-	Apr 16, 2025 @ 23:32:29.000

Name ↑	MAC	State	MTU	Type
Loopback Pseudo-Interface 1	00:00:00:00:00:00	up	2147483647	
乙太網路 2	06:7a:bd:6f:82:b8	up	1500	ethernet
乙太網路 3	00:09:0f:fe:00:01	down	1500	ethernet
乙太網路執行個體 0 2	5e:59:b1:8a:6f:00	up	1500	ethernet
區域連線	00:ff:70:07:b7:08	down	1500	

Local port	Local IP address	Process	State	Protocol
80	::	System	listening	tcp6
80	0.0.0.0	System	listening	tcp
123	::	svchost.exe		udp6
123	0.0.0.0	svchost.exe		udp
135	::	svchost.exe	listening	tcp6
135	0.0.0.0	svchost.exe	listening	tcp
137	192.168.1.208	System		udp
137	192.168.1.177	System		udp
138	192.168.1.208	System		udp
138	192.168.1.177	System		udp

端點資產

- 網路介面
- 網路連接埠
- 網路設定
- 系統更新
- 安裝軟體
- 處理程序



Endpoints win10-pro-1 Inventory Data

win10-pro-1 (029) Generate report

Cores	Memory	Arch	Operating system	CPU	Host name	Board serial	Last scan
8	10239.46 MB	x86_64	Microsoft Windows 10 Pro 10.0.19...	Common KVM processor	WIN10-PRO-1	-	Apr 16, 2025 @ 23:32:29.000

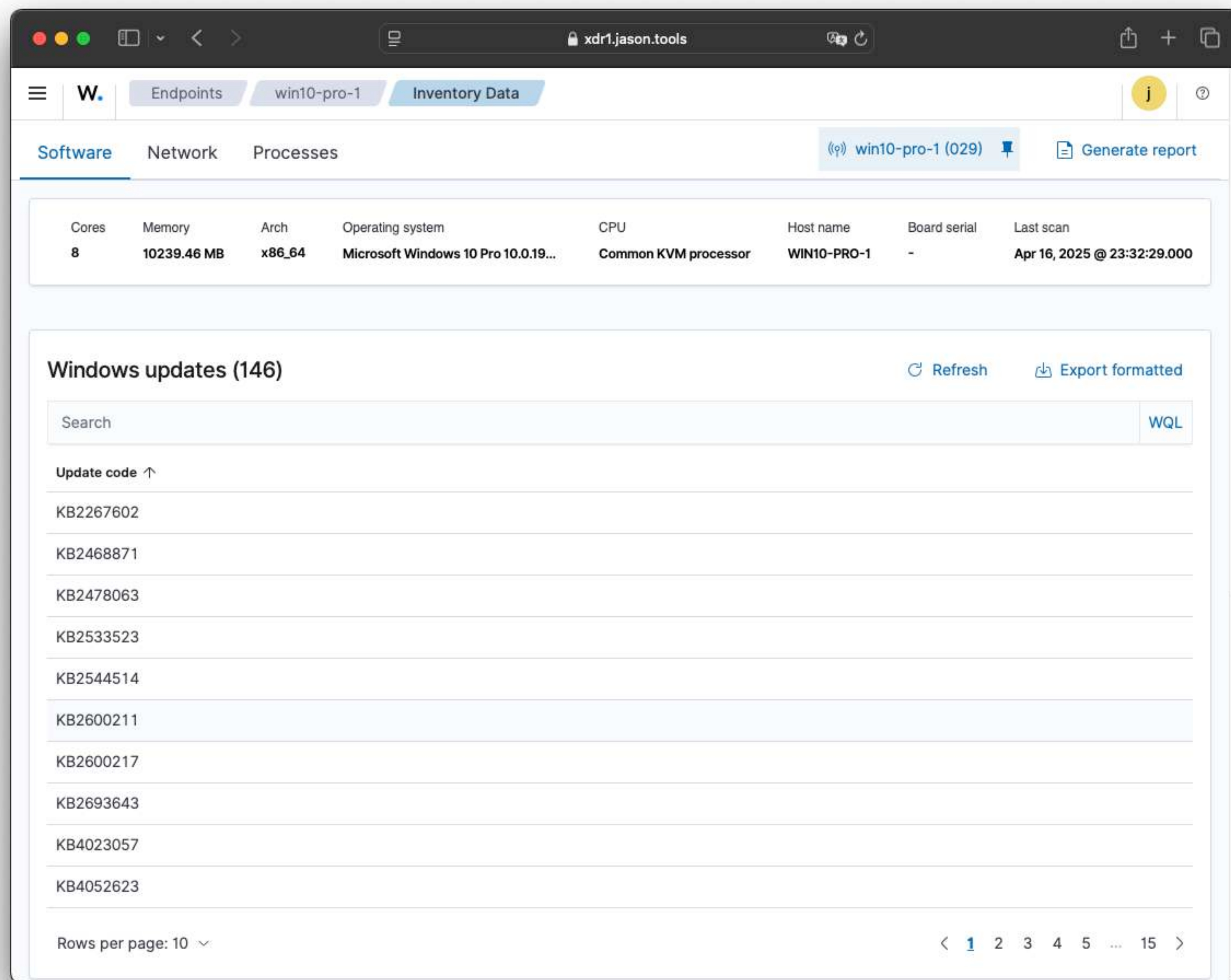
Processes (181) Refresh Export formatted

Search WQL

Name ↑	PID	Parent PID	VM size	Priority	NLWP	Command
AggregatorHost.exe	1520	3392	13000704	8	5	C:\Windows\System32\AggregatorHost.exe
ApplicationFrameHost.exe	516	948	59375616	8	3	C:\Windows\System32\ApplicationFrameHost.exe
Copilot.exe	376	3584	297246720	8	26	C:\Program Files\WindowsApps\Microsoft.Copilot_1.2503.2.167.0_x64__8wekyb3d8bbwe\Copilot.exe
FCDBLog.exe	3196	2608	34746368	8	23	C:\Program Files\Fortinet\FortiClient\FCDBLog.exe
FileCoAuth.exe	3720	948	27168768	8	4	C:\Program Files\Microsoft OneDrive\25.051.0317.0003\FileCoAuth.exe
FortiSSLVPNdaemon.exe	5800	2608	14635008	10	7	C:\Program Files\Fortinet\FortiClient\FortiSSLVPNdaemon.exe
FortiSettings.exe	5796	2608	14213120	8	4	C:\Program Files\Fortinet\FortiClient\FortiSettings.exe
FortiTray.exe	3444	2608	35094528	8	55	C:\Program Files\Fortinet\FortiClient\FortiTray.exe
Greenshot.exe	9716	3584	97595392	8	4	C:\Program Files\Greenshot\Greenshot.exe

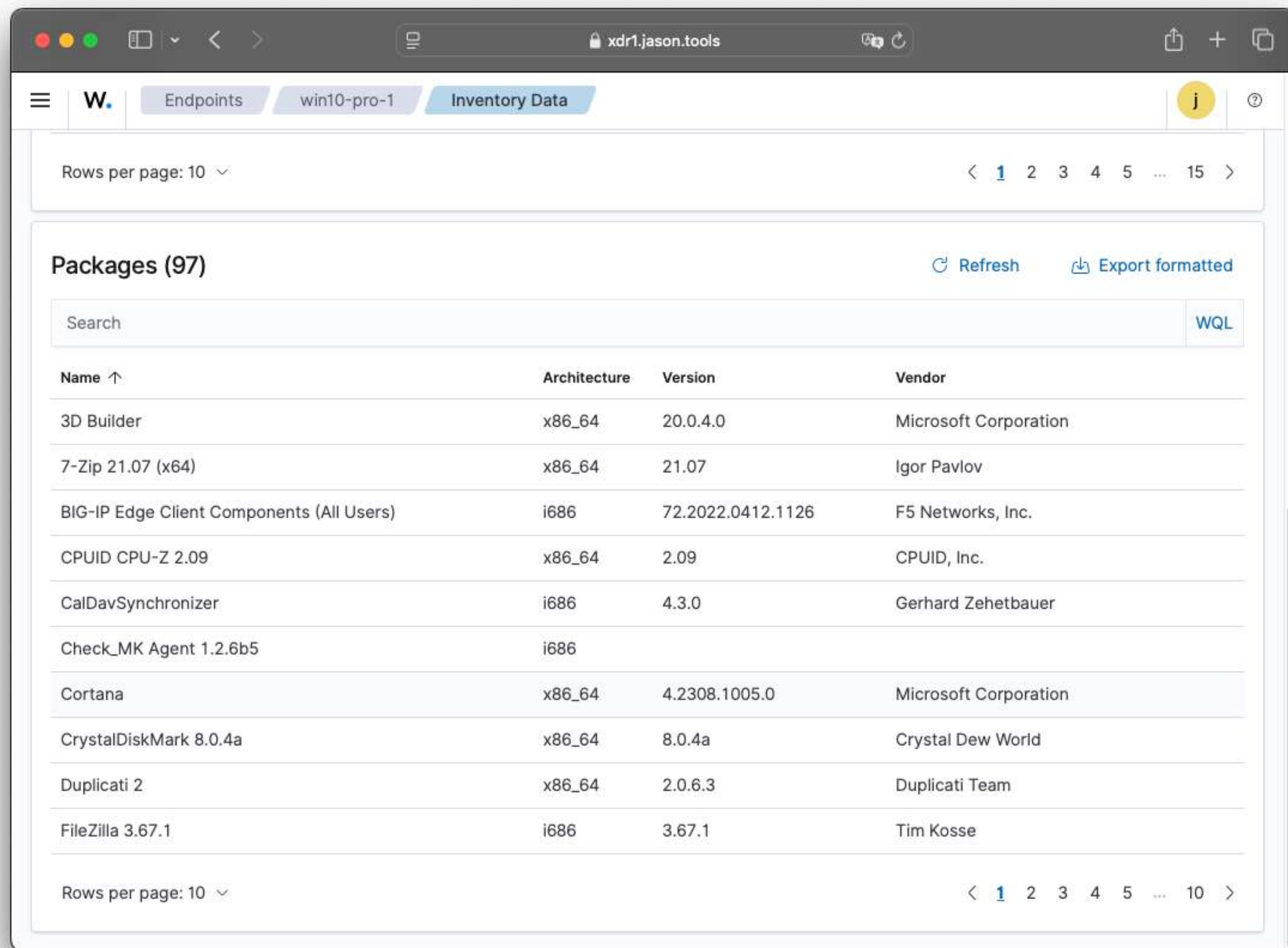
端點資產

- 網路介面
- 網路連接埠
- 網路設定
- 系統更新
- 安裝軟體
- 處理程序



端點資產

- 網路介面
- 網路連接埠
- 網路設定
- 系統更新
- 安裝軟體
- 處理程序



Rows per page: 10 < 1 2 3 4 5 ... 15 >

Packages (97) Refresh Export formatted

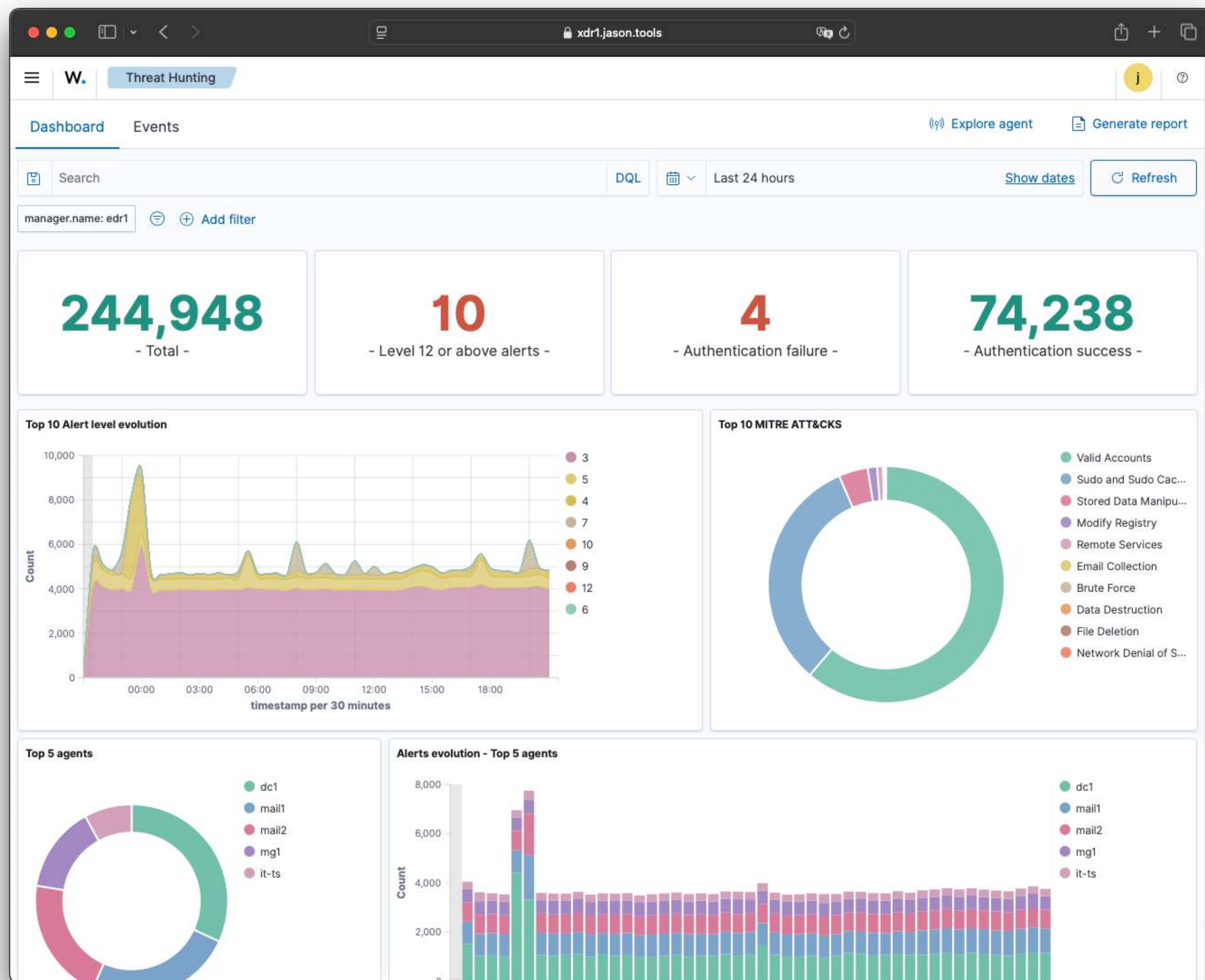
Search WQL

Name ↑	Architecture	Version	Vendor
3D Builder	x86_64	20.0.4.0	Microsoft Corporation
7-Zip 21.07 (x64)	x86_64	21.07	Igor Pavlov
BIG-IP Edge Client Components (All Users)	i686	72.2022.0412.1126	F5 Networks, Inc.
CPUID CPU-Z 2.09	x86_64	2.09	CPUID, Inc.
CalDavSynchronizer	i686	4.3.0	Gerhard Zehetbauer
Check_MK Agent 1.2.6b5	i686		
Cortana	x86_64	4.2308.1005.0	Microsoft Corporation
CrystalDiskMark 8.0.4a	x86_64	8.0.4a	Crystal Dew World
Duplicati 2	x86_64	2.0.6.3	Duplicati Team
FileZilla 3.67.1	i686	3.67.1	Tim Kosse

Rows per page: 10 < 1 2 3 4 5 ... 10 >

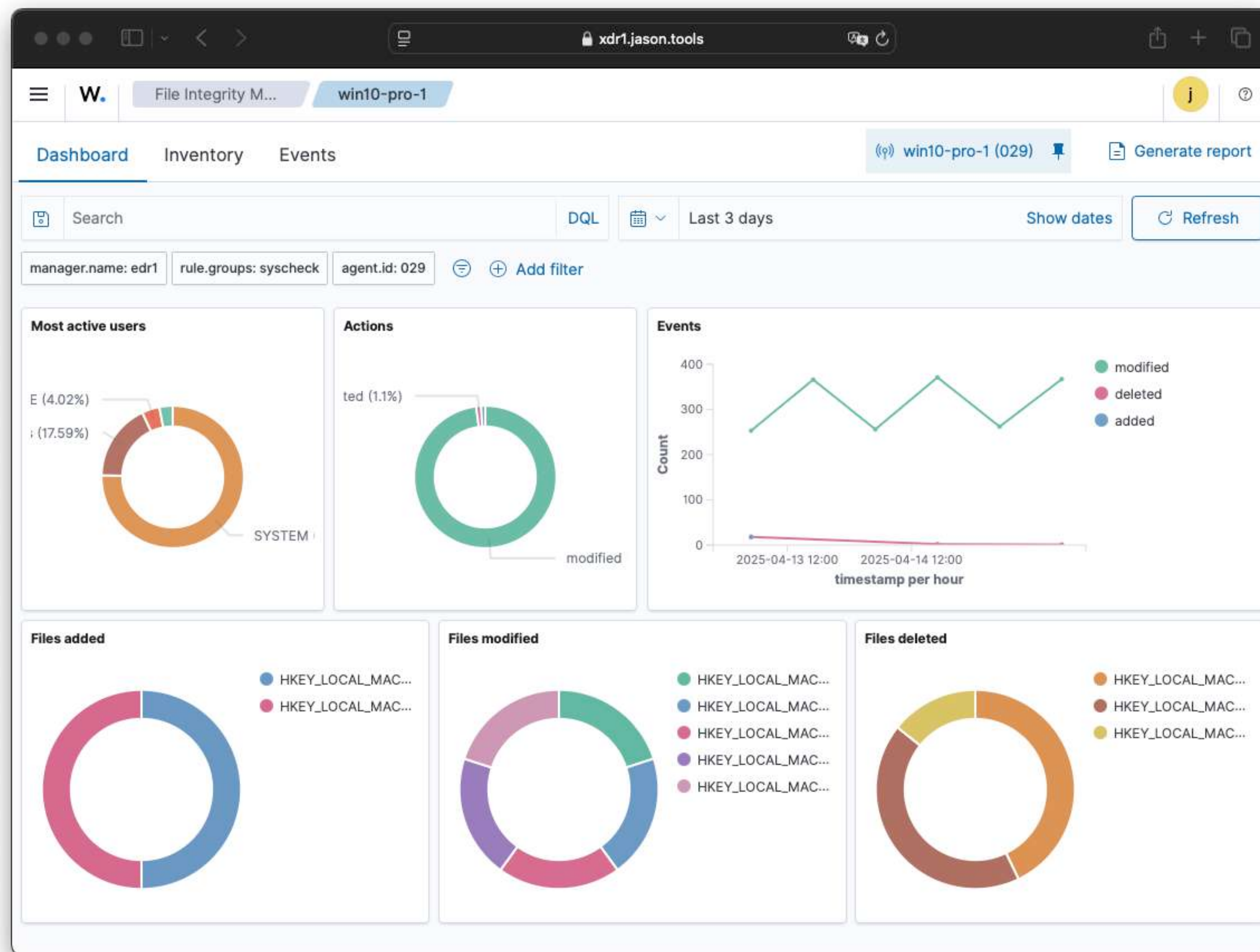
威脅監測

- 事件
- 警報事件
- 認證失敗
- 認證成功
- 端點事件
- MITER ATT&CK



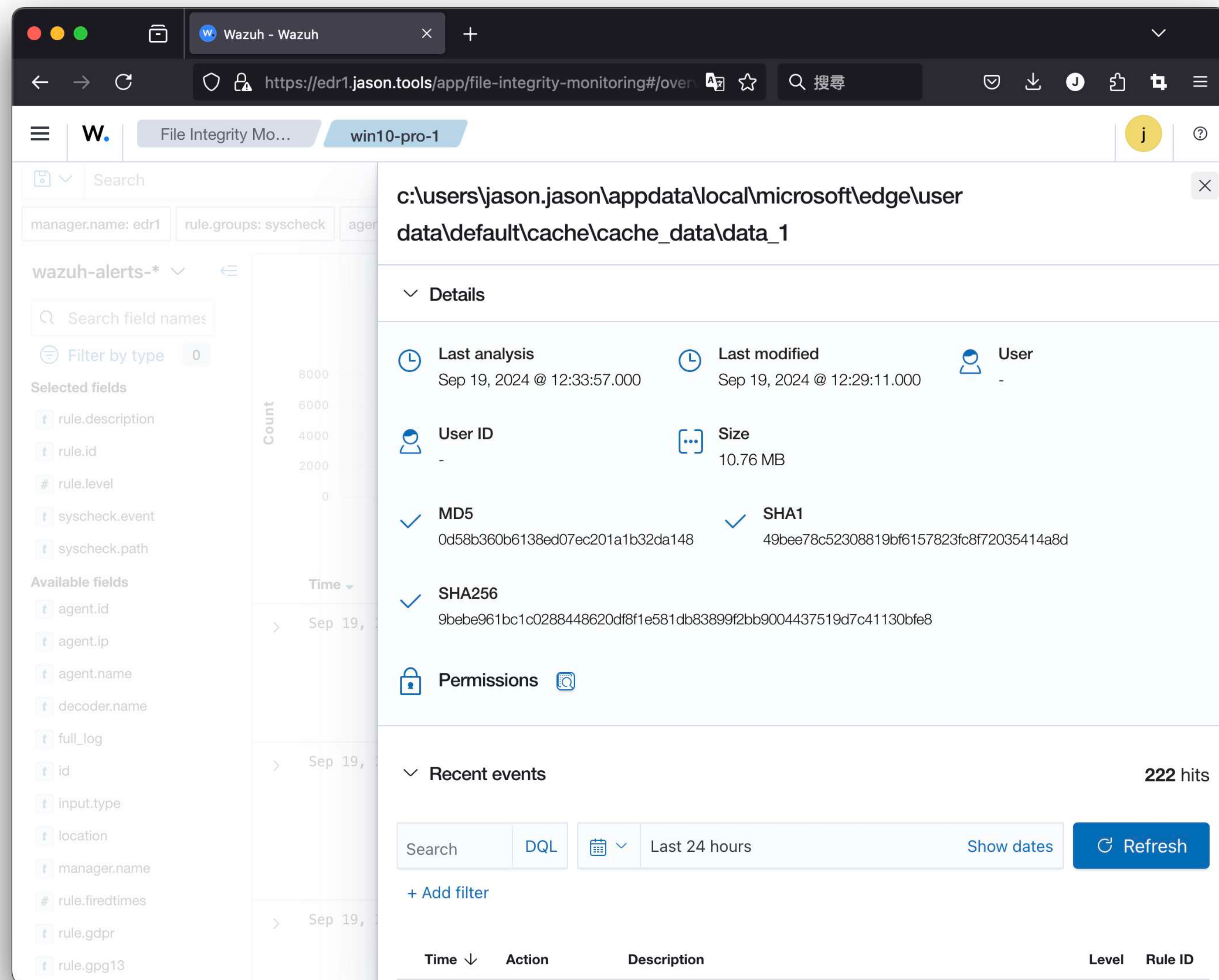
完整性

- 監測檔案
- 系統檔案
- 端點排行
- 動作統計
- 規則分佈
- 帳戶排行



完整性

- 詳細事件
- 端點名稱
- 檢查路徑
- 發生動作
- 規則說明



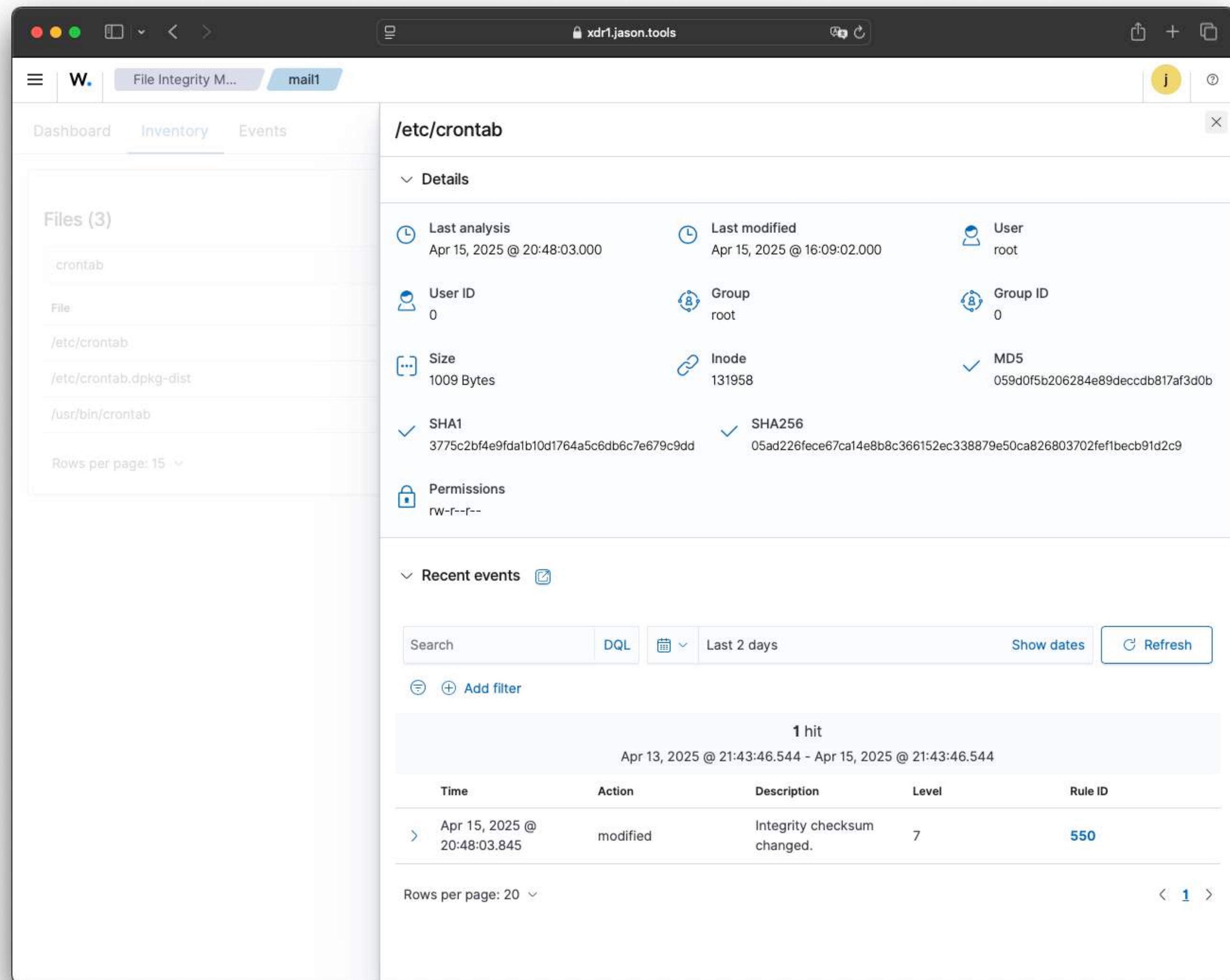
The screenshot displays the Wazuh File Integrity Monitoring (FIM) interface. The main window shows the details of a file integrity check for the path `c:\users\jason.jason\AppData\Local\Microsoft\Edge\UserData\Default\Cache\cache_data\data_1`. The details section includes:

- Last analysis:** Sep 19, 2024 @ 12:33:57.000
- Last modified:** Sep 19, 2024 @ 12:29:11.000
- User:** -
- User ID:** -
- Size:** 10.76 MB
- MD5:** 0d58b360b6138ed07ec201a1b32da148
- SHA1:** 49bee78c52308819bf6157823fc8f72035414a8d
- SHA256:** 9bebe961bc1c0288448620df8f1e581db83899f2bb9004437519d7c41130bfe8
- Permissions:** -

The interface also shows a list of recent events with 222 hits. The search bar is set to "Last 24 hours" and the "Refresh" button is visible.

完整性

- 檔案異動日期
- 使用者 / 群組
- 大小 / 雜湊值
- 機碼異動日期
- 機碼值 / 類型
- 動作 / 雜湊值
- 歷史變動記錄



The screenshot displays the 'File Integrity Monitoring' (FIM) interface for the file `/etc/crontab`. The interface is divided into two main sections: 'Files (3)' on the left and 'Details' on the right.

Files (3):

File
<code>/etc/crontab</code>
<code>/etc/crontab.dpkg-dist</code>
<code>/usr/bin/crontab</code>

Rows per page: 15

Details:

- Last analysis:** Apr 15, 2025 @ 20:48:03.000
- Last modified:** Apr 15, 2025 @ 16:09:02.000
- User:** root
- User ID:** 0
- Group:** root
- Group ID:** 0
- Size:** 1009 Bytes
- Inode:** 131958
- MD5:** 059d0f5b206284e89deccdb817af3d0b
- SHA1:** 3775c2bf4e9fda1b10d1764a5c6db6c7e679c9dd
- SHA256:** 05ad226fece67ca14e8b8c366152ec338879e50ca826803702fef1becb91d2c9
- Permissions:** rw-r--r--

Recent events:

Search [] DQL [] Last 2 days [] Show dates [] Refresh []

+ Add filter

1 hit

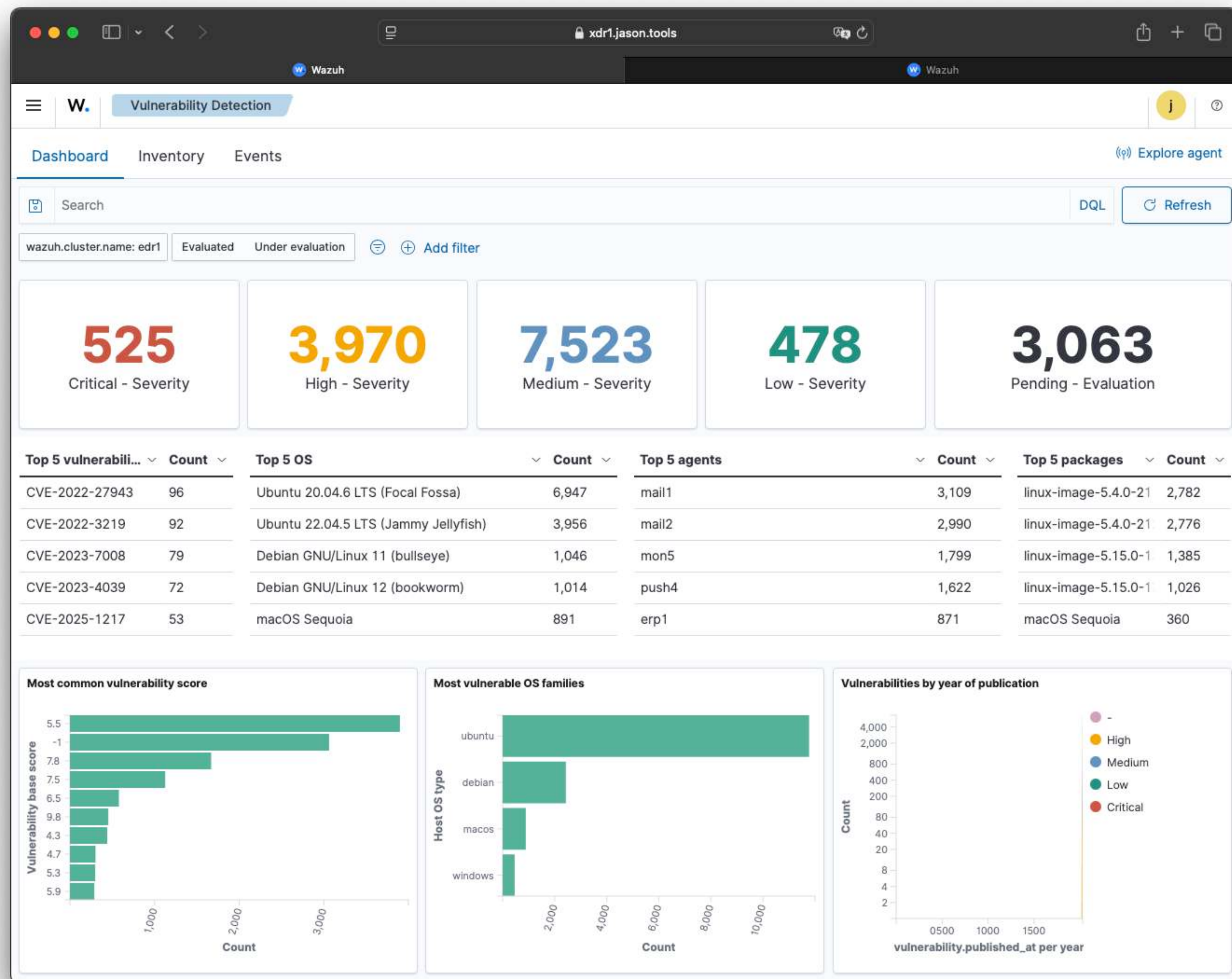
Apr 13, 2025 @ 21:43:46.544 - Apr 15, 2025 @ 21:43:46.544

Time	Action	Description	Level	Rule ID
Apr 15, 2025 @ 20:48:03.845	modified	Integrity checksum changed.	7	550

Rows per page: 20

軟體漏洞

- 軟體名稱
- 軟體版本
- 嚴重性
- CVE 編號
- CVSS 分數
- 檢出日期



軟體漏洞

- 軟體漏洞細節
- CVE 編號
- 發生版本
- 掃描日期
- 更新日期
- 參考資料

剛剛聽說

CVE 委員會沒錢維護了!!!

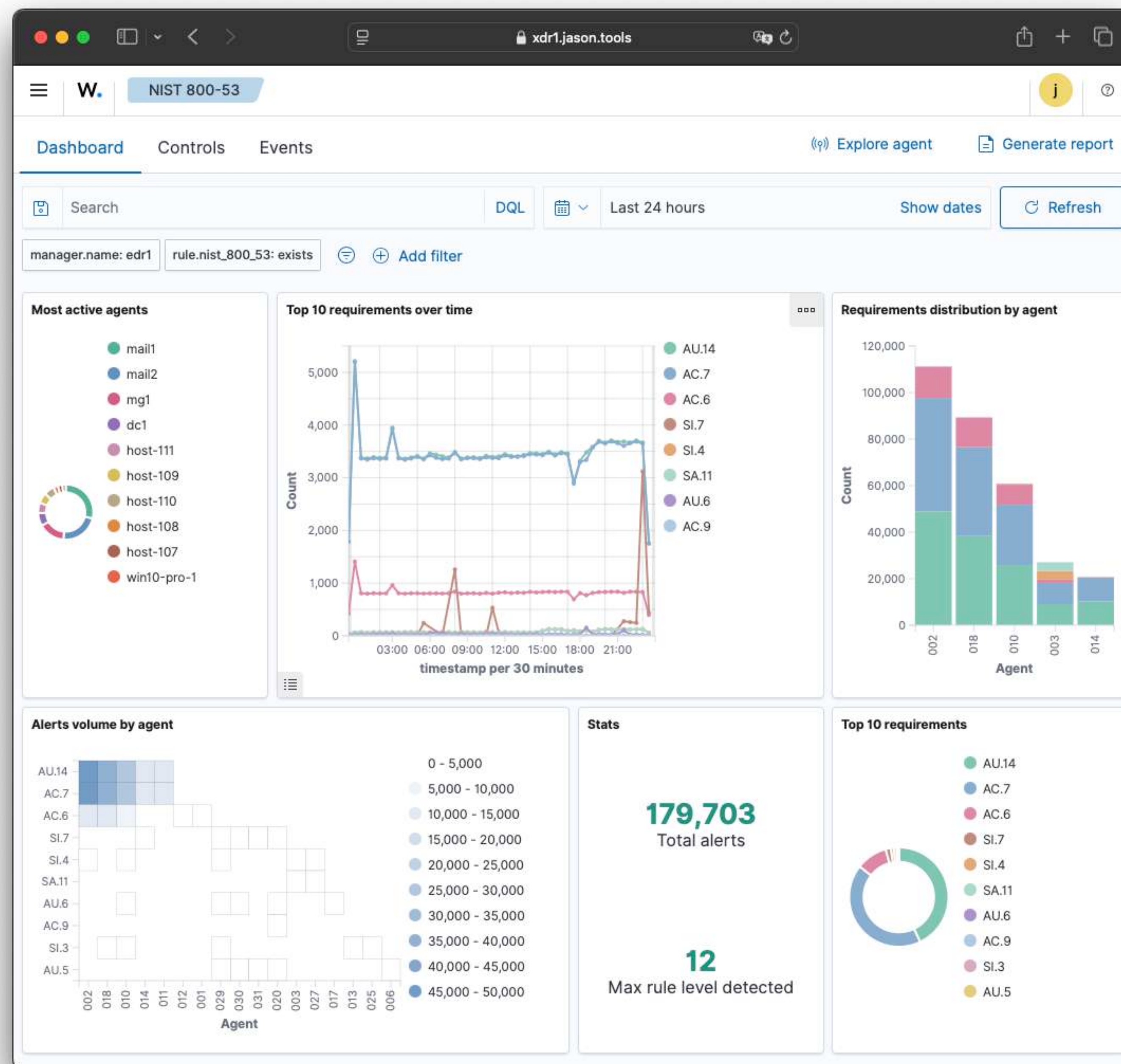
Vulnerability details

t package.name	FortiClient VPN
t package.path	C:\Program Files\Fortinet\FortiClient\
# package.size	0
t package.type	win
t package.version	7.0.8.0427
t vulnerability.category	Packages
t vulnerability.classification	CVSS
t vulnerability.description	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in FortiClient for Windows 7.2.0, 7.0 all versions, 6.4 all versions, 6.2 all versions, Linux 7.2.0, 7.0 all versions, 6.4 all versions, 6.2 all versions and Mac 7.2.0 through 7.2.1 7.0 all versions 6.4 all versions
📅 vulnerability.detected_at	Apr 15, 2025 @ 22:17:57.279
t vulnerability.enumeration	CVE
t vulnerability.id	CVE-2023-37939
📅 vulnerability.published_at	Oct 11, 2023 @ 01:15:12.000
t vulnerability.reference	https://fortiguard.com/psirt/FG-IR-22-235
t vulnerability.scanner.source	National Vulnerability Database
t vulnerability.scanner.vendor	Wazuh
# vulnerability.score.base	3.3
t vulnerability.score.version	3.1
t vulnerability.severity	Low
🕒 vulnerability.under_evaluation	false
t wazuh.cluster.name	edr1
t wazuh.schema.version	1.0.0

合規看板

- PCI DSS
- GDPR
- HIPAA
- NIST 800-53
- TSC

沒關係
我也看不懂
但是看起來很厲害





功能概觀

產製報告

- 看板報告
- 資產報告
- 清單報告
- 其它

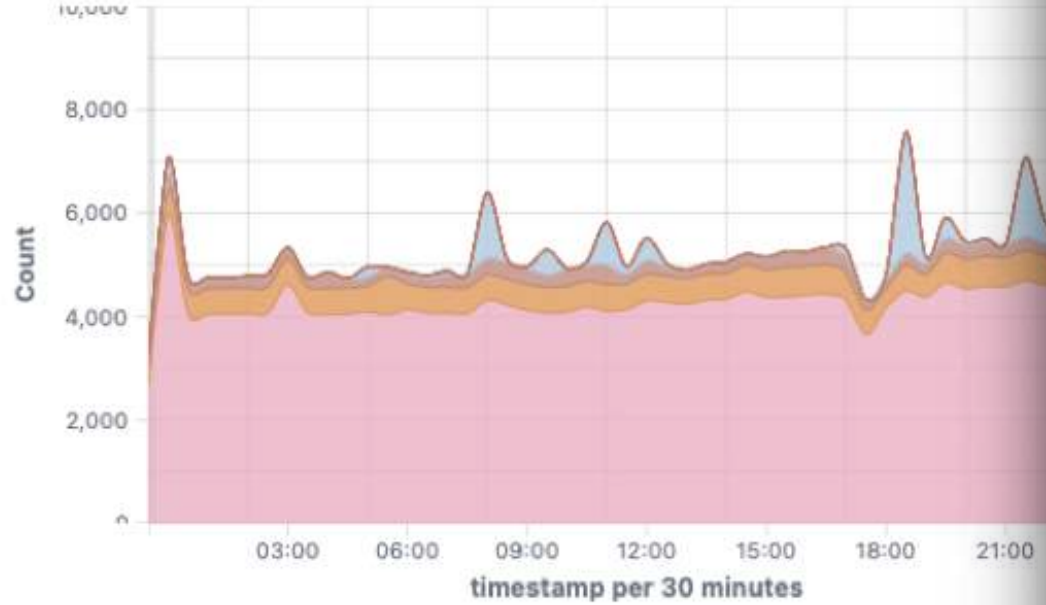
節省工具箱
JASON TOOLS

Threat hunting report

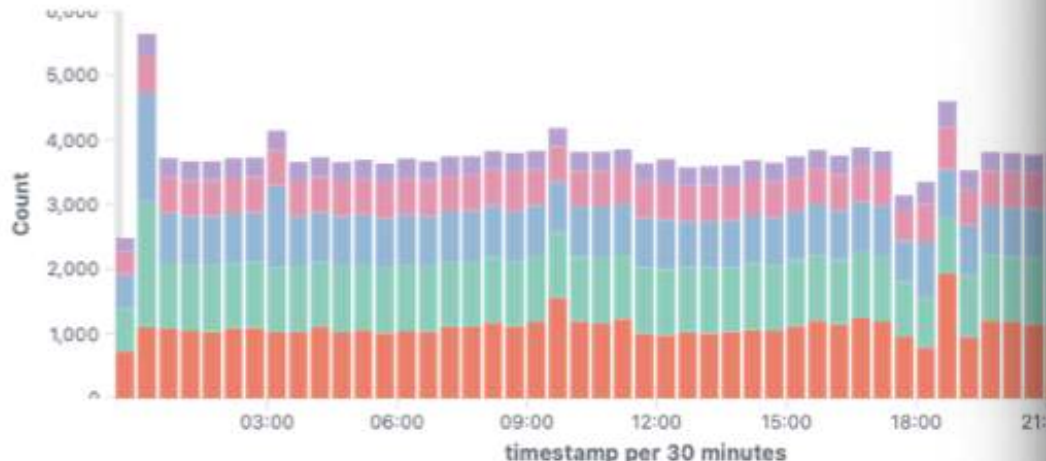
Browse through your security alerts, identifying issues and threats in

◎ 2025-04-15T23:39:50 to 2025-04-16T23:39:50
Q manager.name: edr1

Top 10 Alert level evolution



Alerts evolution - Top 5 agents



Jason Tools Co., Ltd

節省工具箱
JASON TOOLS

service@jason.tools
https://www.jason.tools

Inventory data report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
014	host-111	192.168.1.111	Wazuh v4.11.1	edr1	Debian GNU/Linux 12	Mar 29, 2025 @ 15:11:09.000	Apr 16, 2025 @ 23:40:58.000

Hardware information

- 16 cores
- Intel(R) Xeon(R) D-2141I CPU @ 2.20GHz
- 125.46GB RAM

Operating system information

- Linux
- #1 SMP PREEMPT_DYNAMIC PMX 6.8.12-4 (2024-11-06T15:04Z)
- x86_64
- 6.8.12-4-pve
- Debian GNU/Linux 12 (bookworm)

Packages

Name	Architecture	Version	Vendor	Description
defusedxml		0.7.1		
lm-sensors	amd64	1:3.6.0-7.1	Aurelien Jarno <aurel32@debian.org>	utilities to read temperature/voltage/fan sensors
libglusterd0	amd64	10.3-5	Patrick Matthäi <pmatthaei@debian.org>	GlusterFS glusterd shared library
python3-singledispatch	all	3.4.0.3-4	Debian Python Team <team+python@tracker.debian.org>	single-dispatch generic functions for Python
thin-provisioning-tools	amd64	0.9.0-2	Debian LVM Team <team+lvm@tracker.debian.org>	Tools for handling thinly provisioned device-mapper meta-data
libraqm0	amd64	0.7.0-4.1	ماحمودى <aelmahmoudy@users.sourceforge.net>	Library for complex text layout
kvm-control-daemon	all	1.5-1	Proxmox Support Team <support@proxmox.com>	Kernel Samepage Merging (KSM) Tuning Daemon
libradosstriper1	amd64	18.2.4-pve3	Ceph Maintainers <ceph-maintainers@ceph.io>	RADOS striping interface

Jason Tools Co., Ltd

Page 1 of 46

套件搭配



節省工具箱
JASON TOOLS

套件
搭配

端點防護

- Defender
- ClamAV

Document Details		View surrounding documents	View single document
data.win.eventdata.source ID	4		
data.win.eventdata.source Name	Downloads and attachments		
data.win.eventdata.state	1		
data.win.eventdata.status Code	1		
data.win.eventdata.threat ID	2147814524		
data.win.eventdata.threat Name	Trojan:Script/Wacatac.H!ml		
data.win.eventdata.type ID	8		
data.win.eventdata.type Name	FastPath		
data.win.system.channel	Microsoft-Windows-Windows Defender/Operational		
data.win.system.computer	win10-pro-1.jason.tools		
data.win.system.eventID	1116		
data.win.system.eventRecordID	58595		
data.win.system.keywords	0x8000000000000000		
data.win.system.level	3		
data.win.system.message	"Microsoft Defender Antivirus has detected malware or other potentially unwanted software. For more information please see the following: https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Script/Wacatac.H!ml		
data.win.system.opcode	0		



節省工具箱
JASON TOOLS

套件
搭配



端點防護

- Defender
- ClamAV

Document Details

[View surrounding documents](#)

[View single document](#)

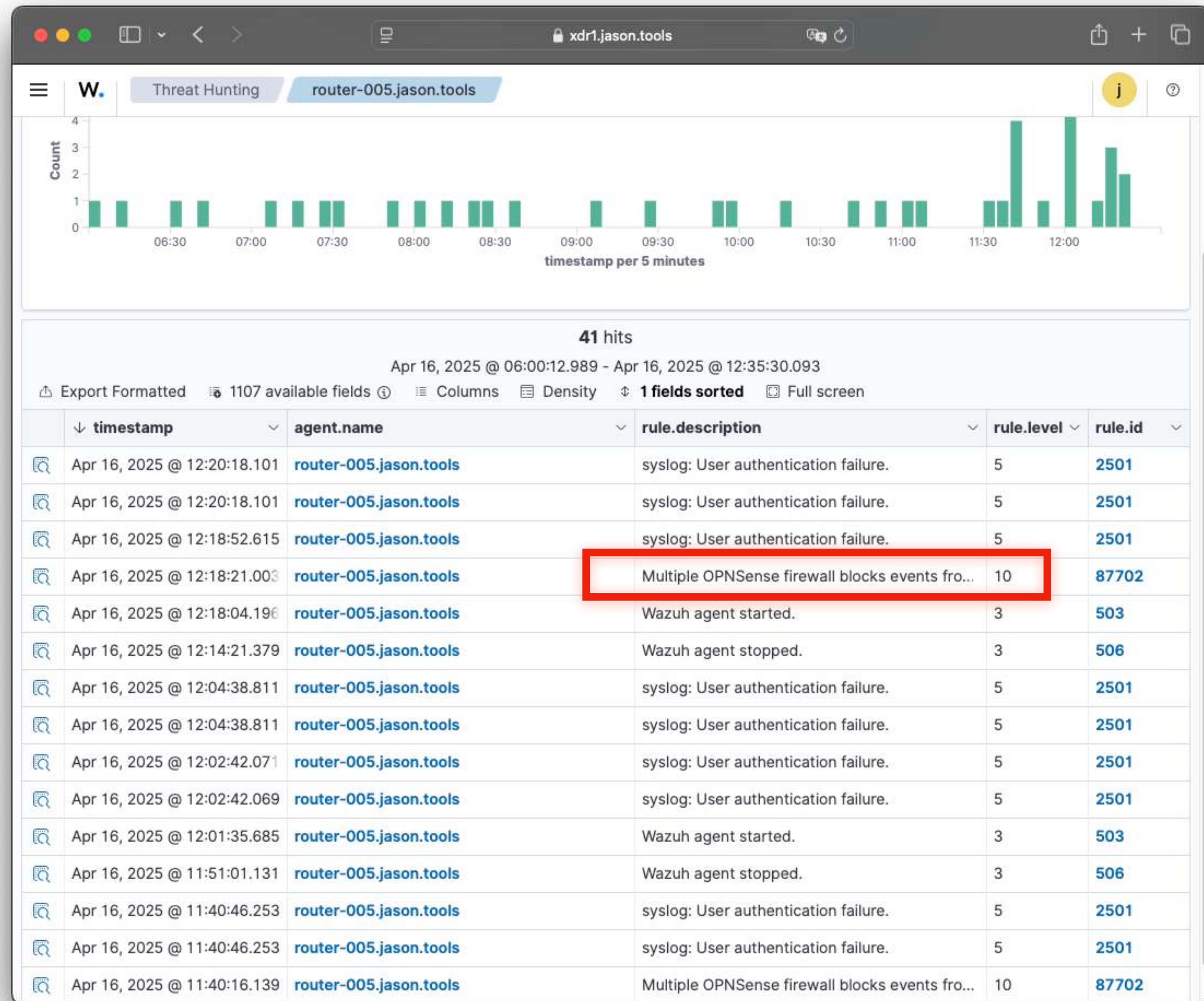
Table

JSON

t _index	wazuh-alerts-4.x-2025.04.16
t agent.id	031
t agent.ip	192.168.1.142
t agent.name	oxidized2
t data.extra_data	Win.Dropper.Upatre-7492034-0
t data.id	2a49e153eb3e6046c73328c2e3c75c3c
t data.url	/opt/xiLqAec6.zip
t decoder.name	clamd
t decoder.parent	clamd
t full_log	Apr 16 04:27:15 oxidized2 clamd[2470820]: /opt/xiLqAec6.zip: Win.Dropper.Upatre-7492034-0(2a49e153eb3e6046c73328c2e3c75c3c:39719) FOUND
t id	1744777635.125619152
t input.type	log
t location	journald
t manager.name	edr1
t predecoder.hostname	oxidized2
t predecoder.program_name	clamd
t predecoder.timestamp	Apr 16 04:27:15
t rule.description	ClamAV: Virus detected

防火牆

● OPNsense



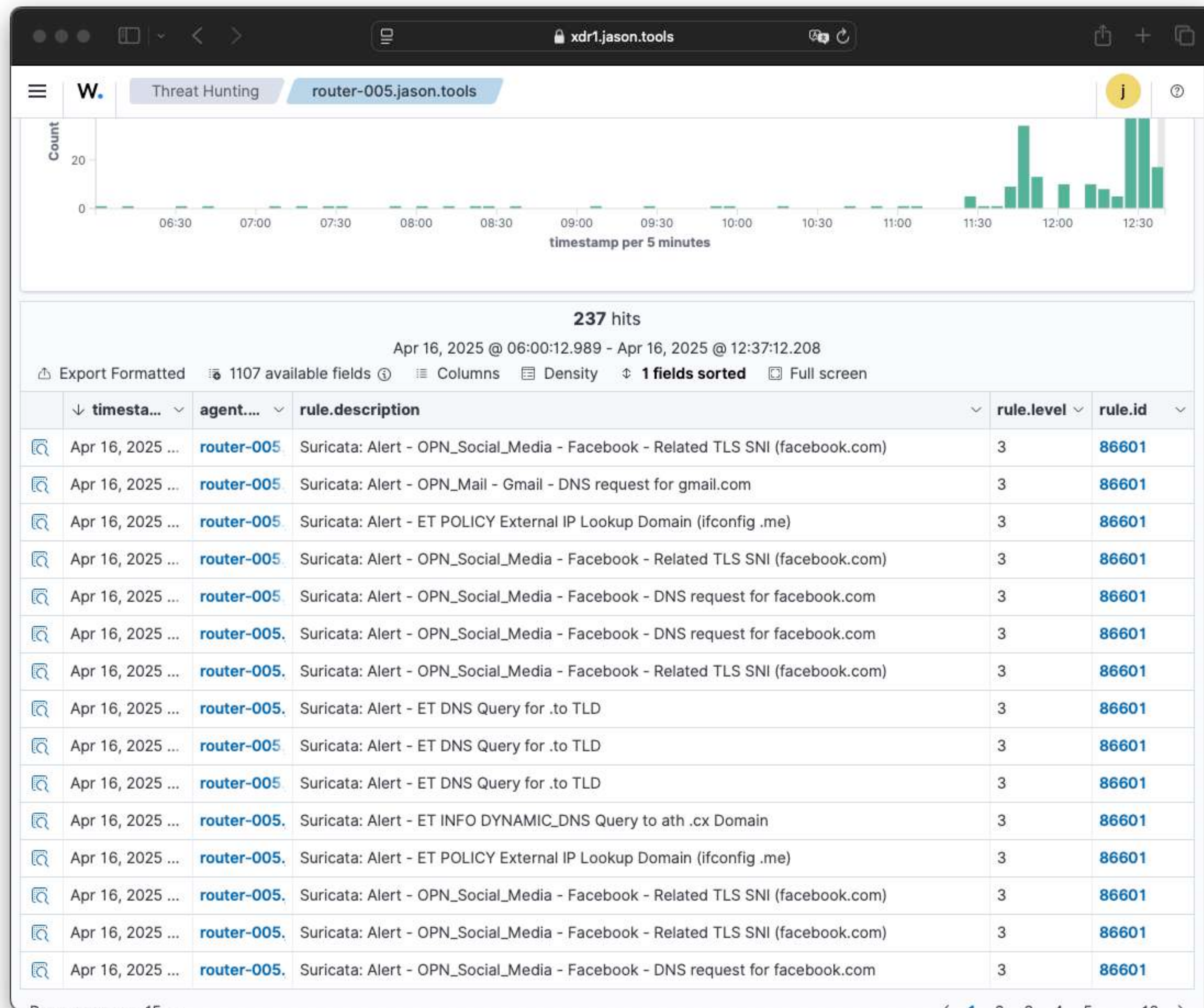
防火牆

● OPNsense

Discover		wazuh-alerts-4.x-2025.04.16#-sxDPZYBo2fM0Ddu09pE		j	?
t	predecoder.timestamp	Apr 16 14:22:55			
t	previous_output	Apr 16 14:22:54 router-005.jason.tools filterlog[29050]: 76,,,badf9fd7b03523686df3cda925091a44,pppoe0,match,block,out,4,0x0,,63,58873,0,none,1,icmp,84,220.132.181.91,142.250.196.195,datalength=64 Apr 16 14:22:53 router-005.jason.tools filterlog[29050]: 76,,,badf9fd7b03523686df3cda925091a44,pppoe0,match,block,out,4,0x0,,63,48376,0,none,1,icmp,84,220.132.181.91,142.250.196.195,datalength=64 Apr 16 14:22:52 router-005.jason.tools filterlog[29050]: 76,,,badf9fd7b03523686df3cda925091a44,pppoe0,match,block,out,4,0x0,,63,44539,0,none,1,icmp,84,220.132.181.91,142.250.196.195,datalength=64 Apr 16 14:22:51 router-005.jason.tools filterlog[29050]: 76,,,badf9fd7b03523686df3cda925091a44,pppoe0,match,block,out,4,0x0,,63,52304,0,none,1,icmp,84,220.132.181.91,142.250.196.195,datalength=64 Apr 16 14:22:50 router-005.jason.tools filterlog[29050]: 76,,,badf9fd7b03523686df3cda925091a44,pppoe0,match,block,out,4,0x0,,63,48211,0,none,1,icmp,44,220.132.181.91,1.1.1.1,datalength=24 Apr 16 14:22:50 router-005.jason.tools filterlog[29050]: 76,,,badf9fd7b03523686df3cda925091a44,pppoe0,match,block,out,4,0x0,,63,14476,0,none,1,icmp,84,220.132.181.91,142.250.196.195,datalength=64 Apr 16 14:22:49 router-005.jason.tools filterlog[29050]: 76,,,badf9fd7b03523686df3cda925091a44,pppoe0,match,block,out,4,0x0,,63,28476,0,none,1,icmp,84,220.132.181.91,142.250.196.195,datalength=64 Apr 16 14:22:48 router-005.jason.tools filterlog[29050]: 76,,,badf9fd7b03523686df3cda925091a44,pppoe0,match,block,out,4,0x0,,63,60030,0,none,1,icmp,84,220.132.181.91,142.250.196.195,datalength=64 Apr 16 14:22:47 router-005.jason.tools filterlog[29050]: 76,,,badf9fd7b03523686df3cda925091a44,pppoe0,match,block,out,4,0x0,,63,46179,0,none,1,icmp,1368,220.132.181.91,17.253.117.201,datalength=1348 Apr 16 14:22:47 router-005.jason.tools filterlog[29050]: 76,,,badf9fd7b03523686df3cda925091a44,pppoe0,match,block,out,4,0x0,,63,56153,0,none,1,icmp,84,220.132.181.91,142.250.196.195,datalength=64 Apr 16 14:22:46 router-005.jason.tools filterlog[29050]: 76,,,badf9fd7b03523686df3cda925091a44,pppoe0,match,block,out,4,0x0,,63,47113,0,none,1,icmp,1368,220.132.181.91,17.253.117.201,datalength=1348			
t	rule.description	Multiple OPNSense firewall blocks events from same source.			
#	rule.firedtimes	1			

IDS/IPS

● Suricata (OPNsense)





套件搭配



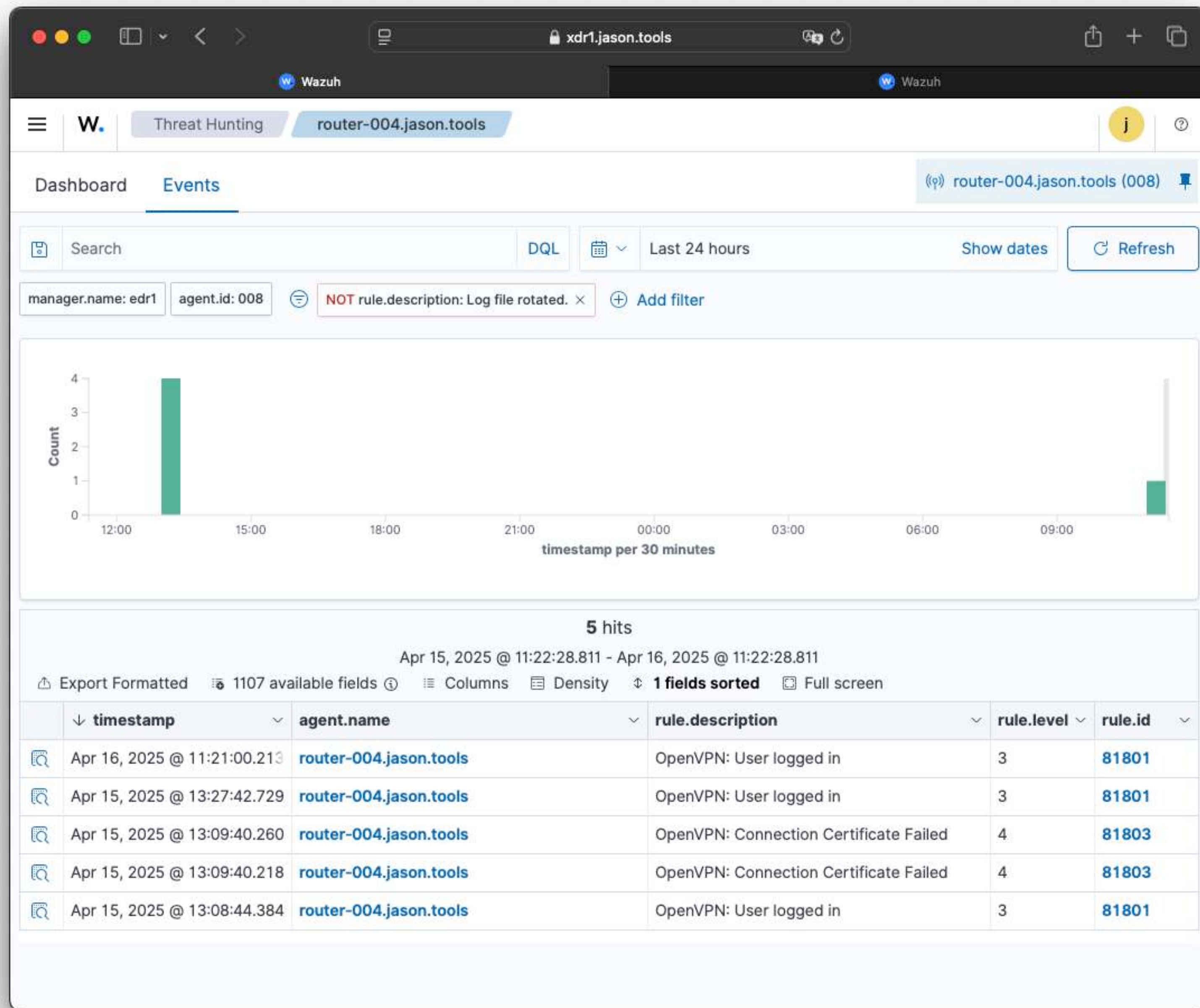
IDS/IPS

● Suricata
(OPNsense)

data.alert.action	allowed
data.alert.category	Potentially Bad Traffic
data.alert.gid	1
data.alert.metadata.attack_target	Client_and_Server
data.alert.metadata.confidence	High
data.alert.metadata.created_at	2022_11_21
data.alert.metadata.deployment	Perimeter
data.alert.metadata.mitre_tactic_id	TA0011
data.alert.metadata.mitre_tactic_name	Command_And_Control
data.alert.metadata.mitre_technique_id	T1568
data.alert.metadata.mitre_technique_name	Dynamic_Resolution
data.alert.metadata.performance_impact	Low
data.alert.metadata.signature_severity	Informational
data.alert.metadata.updated_at	2024_12_01
data.alert.rev	2
data.alert.severity	2
data.alert.signature	ET INFO DYNAMIC_DNS Query to ath .cx Domain
data.alert.signature_id	2039814
data.app_proto	dns
data.dest_ip	8.8.8.8
data.dest_port	53
data.direction	to_server
# data.dns.query.id	62,761
# data.dns.query.opcode	0
data.dns.query.rname	ilan-ns1.ath.cx
data.dns.query.rtype	A

VPN 連線

● OpenVPN
(OPNsense)



VPN 連線

● OpenVPN (OPNsense)

t	GeoLocation.country_name	Taiwan
🌐	GeoLocation.location	{ "lon": 121, "lat": 23.5 }
t	_index	wazuh-alerts-4.x-2025.04.16
t	agent.id	008
t	agent.ip	192.168.1.13
t	agent.name	router-004.jason.tools
t	data.srcip	42.79.195.155
t	data.srcport	51087
t	data.srcuser	jason
t	decoder.name	openvpn
t	decoder.parent	openvpn
t	full_log	Apr 16 11:20:59 router-004.jason.tools openvpn_server1[87062]: 42.79.195.155:51087 [jason] Peer Connection Initiated with [AF_INET]42.79.195.155:51087
t	id	1744773660.112056101
t	input.type	log
t	location	/var/ossec/logs/opnsense_syslog.



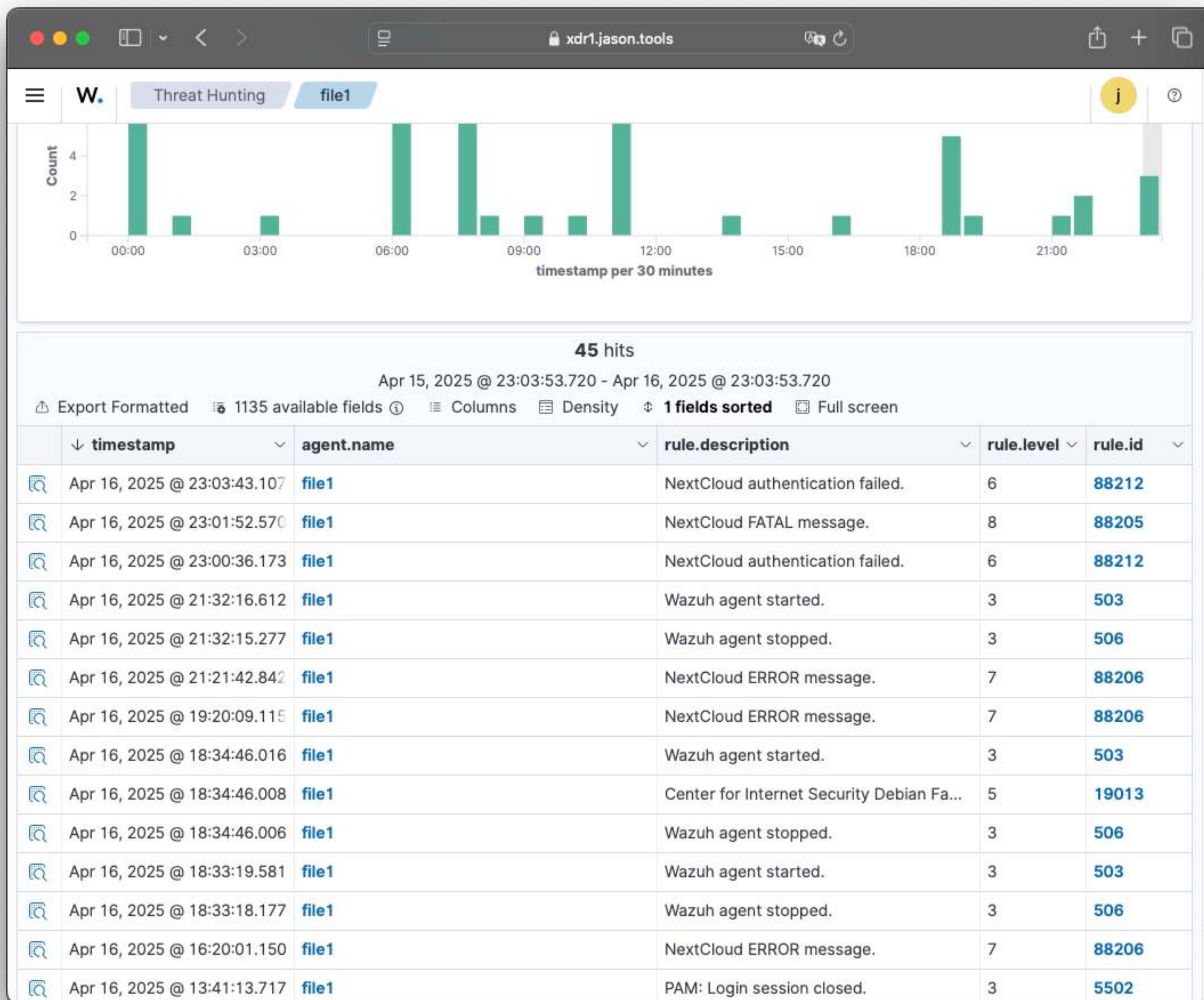
節省工具箱
JASON TOOLS

套件
搭配



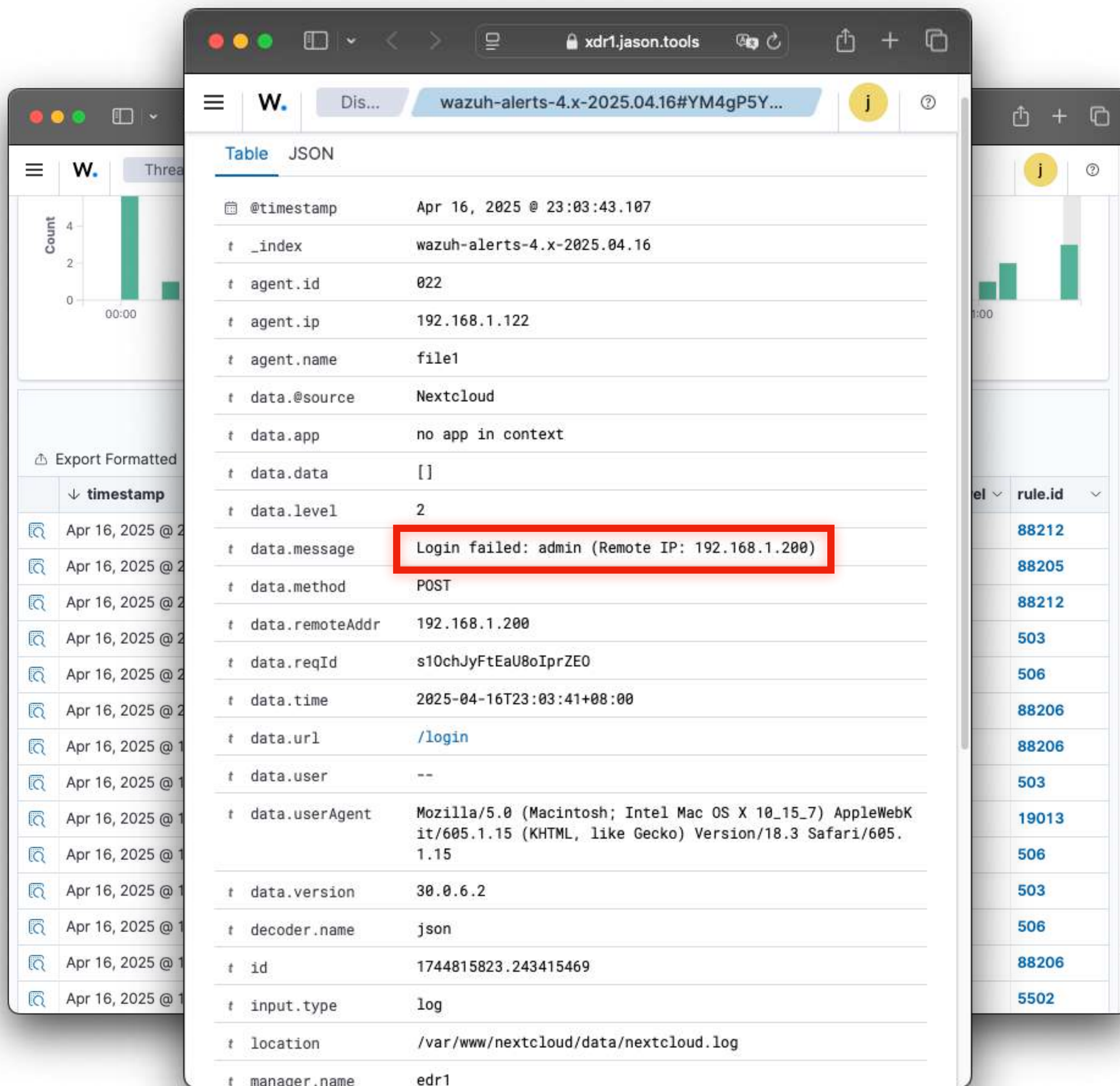
網路硬碟

● Nextcloud



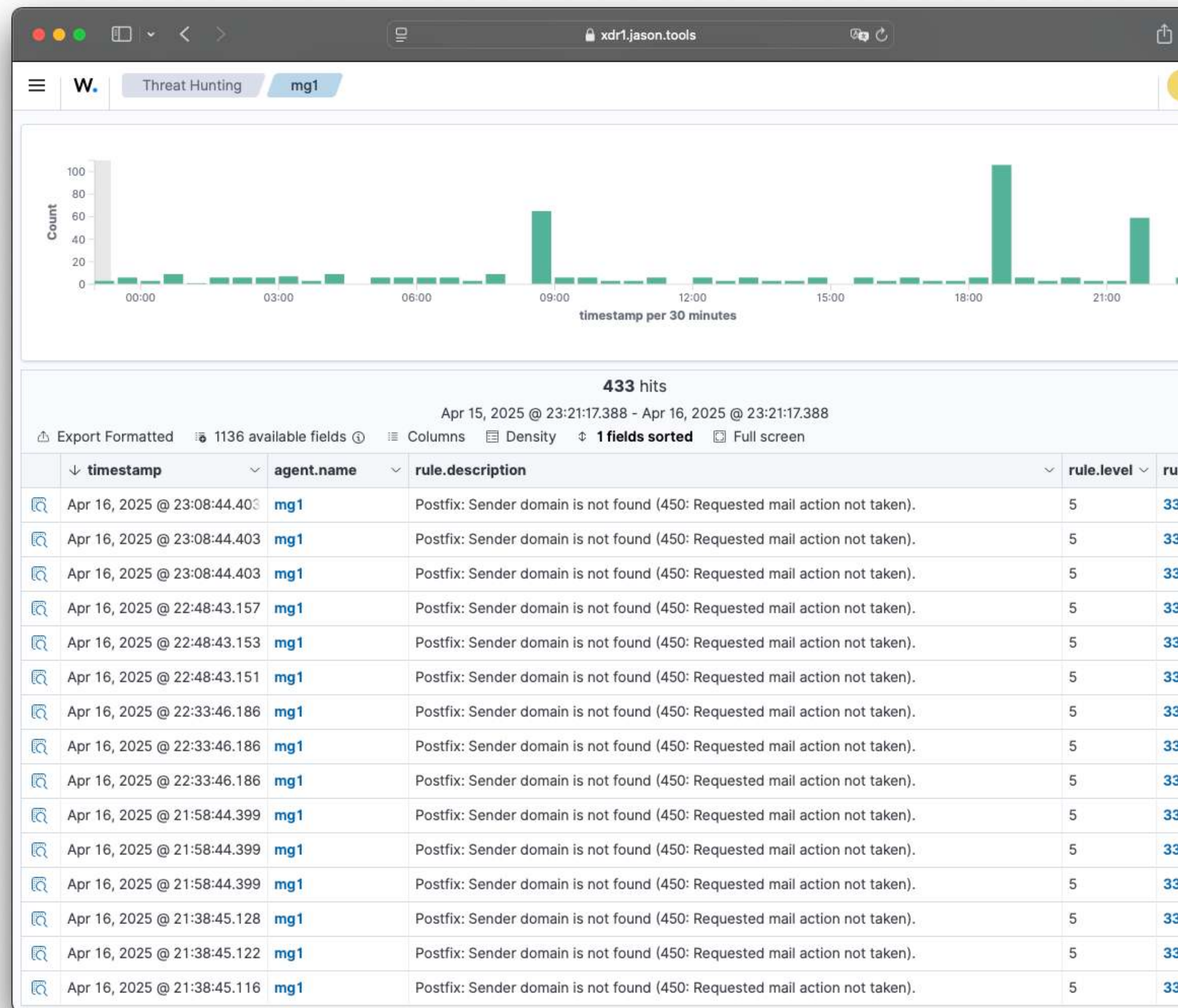
網路硬碟

● Nextcloud



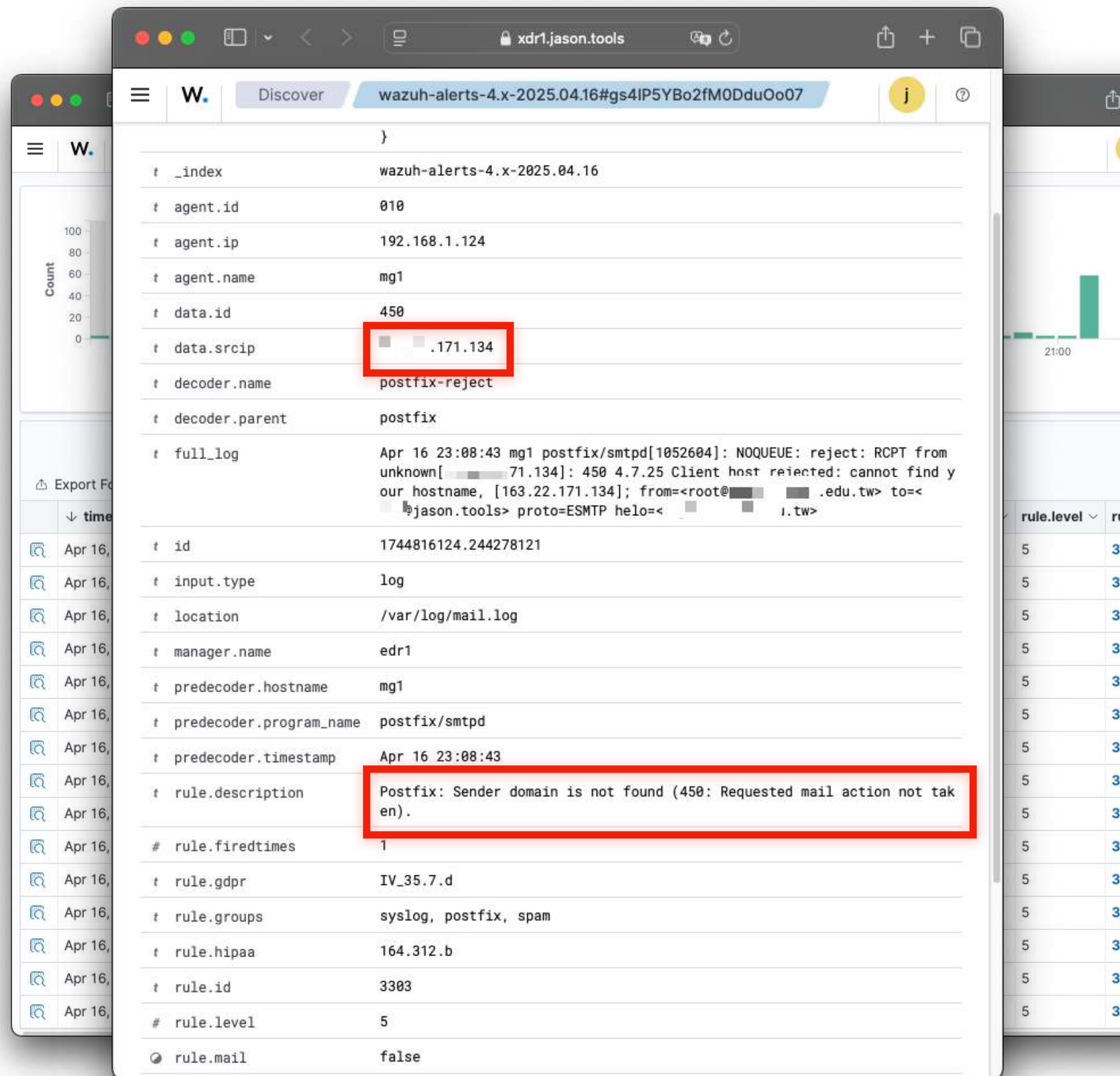
郵件主機

- Proxmox MG
- Zimbra
- Postfix



郵件主機

- Proxmox MG
- Zimbra
- Postfix

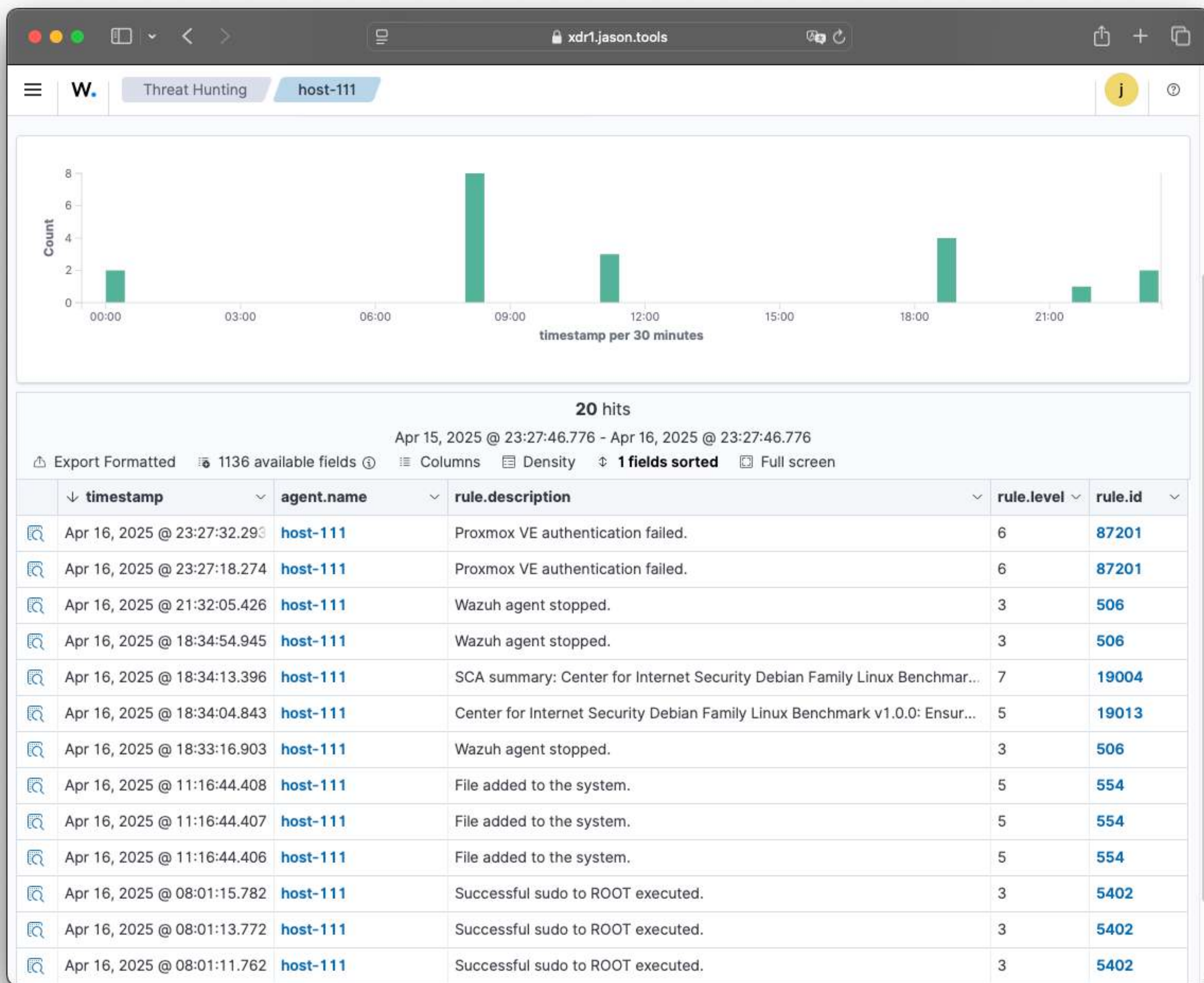


The screenshot displays the Wazuh alerts interface in a web browser. The URL bar shows 'xdr1.jason.tools'. The interface includes a sidebar with a 'Discover' tab and a main content area showing a list of alerts. The selected alert is for a mail rejection event.

Field	Value
_index	wazuh-alerts-4.x-2025.04.16
agent.id	010
agent.ip	192.168.1.124
agent.name	mg1
data.id	450
data.srcip	[REDACTED].171.134
decoder.name	postfix-reject
decoder.parent	postfix
full_log	Apr 16 23:08:43 mg1 postfix/smtpd[1052604]: NOQUEUE: reject: RCPT from unknown[REDACTED]71.134]: 450 4.7.25 Client host rejected: cannot find your hostname, [163.22.171.134]; from=<root@[REDACTED].edu.tw> to=<[REDACTED]@jason.tools> proto=ESMTP helo=<[REDACTED].tw>
id	1744816124.244278121
input.type	log
location	/var/log/mail.log
manager.name	edr1
predecoder.hostname	mg1
predecoder.program_name	postfix/smtpd
predecoder.timestamp	Apr 16 23:08:43
rule.description	Postfix: Sender domain is not found (450: Requested mail action not taken).
# rule.firedtimes	1
rule.gdpr	IV_35.7.d
rule.groups	syslog, postfix, spam
rule.hipaa	164.312.b
rule.id	3303
# rule.level	5
rule.mail	false

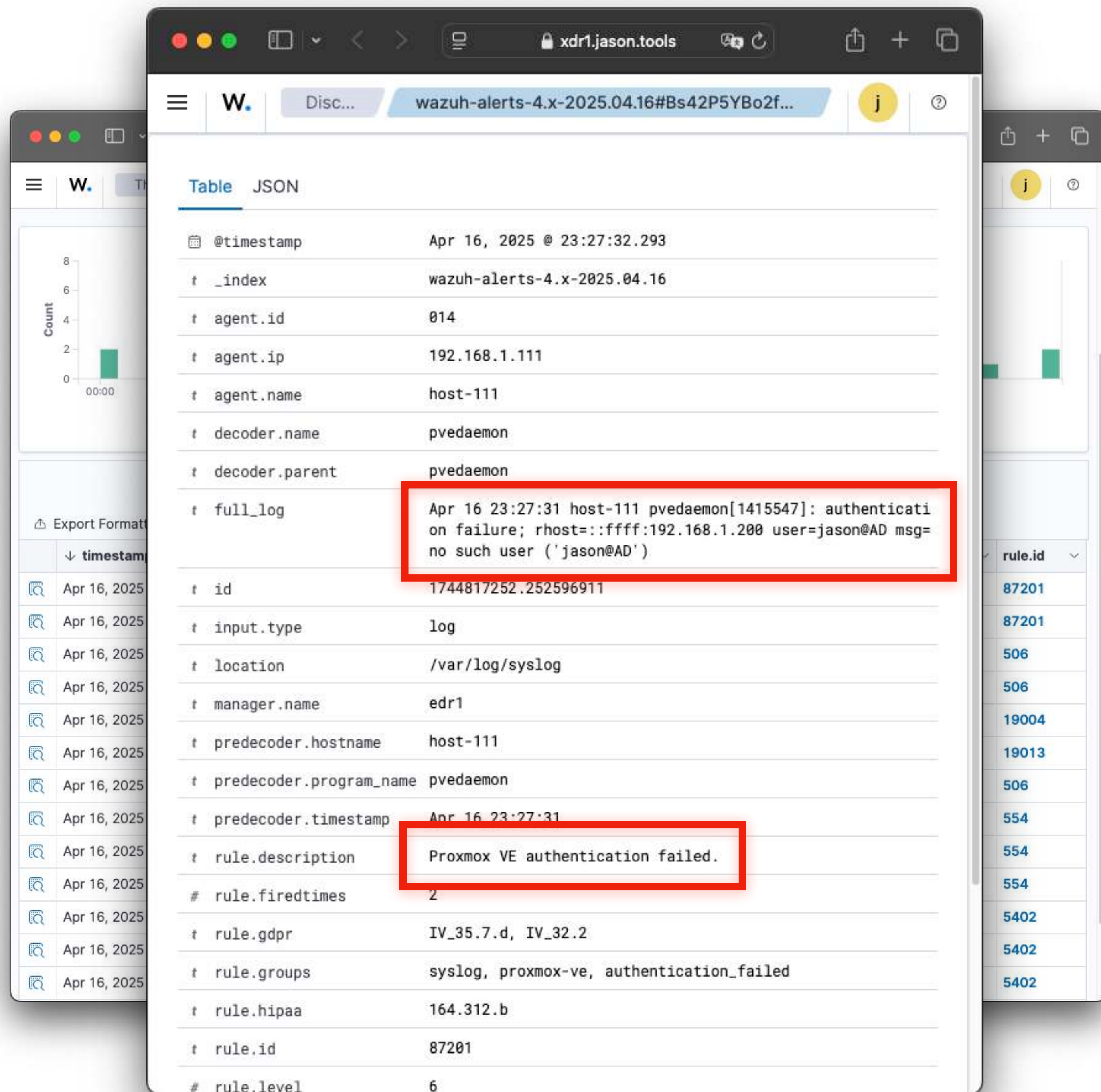
虛擬化

Proxmox VE



虛擬化

● Proxmox VE

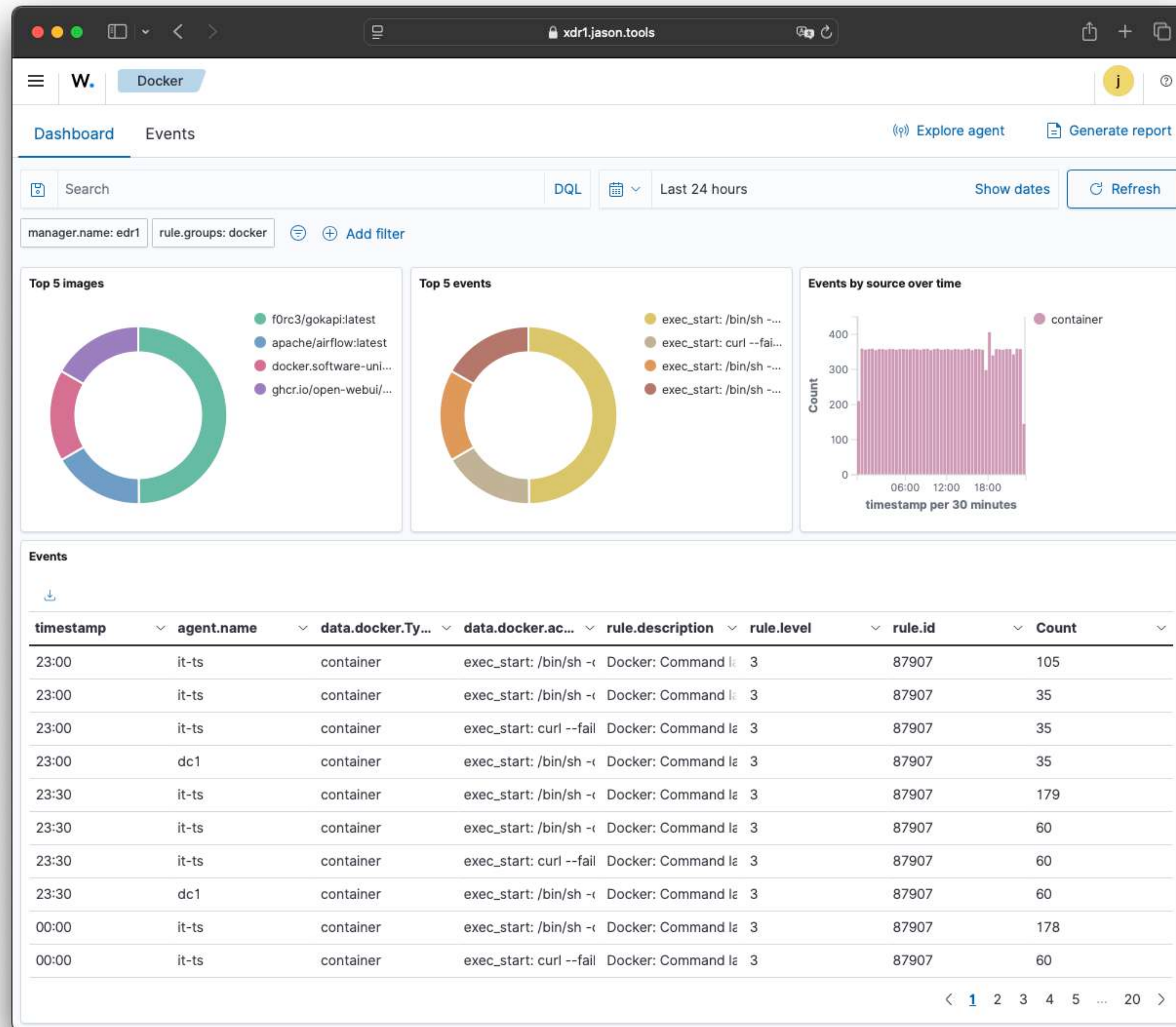




套件搭配

容器

Docker





套件搭配



容器

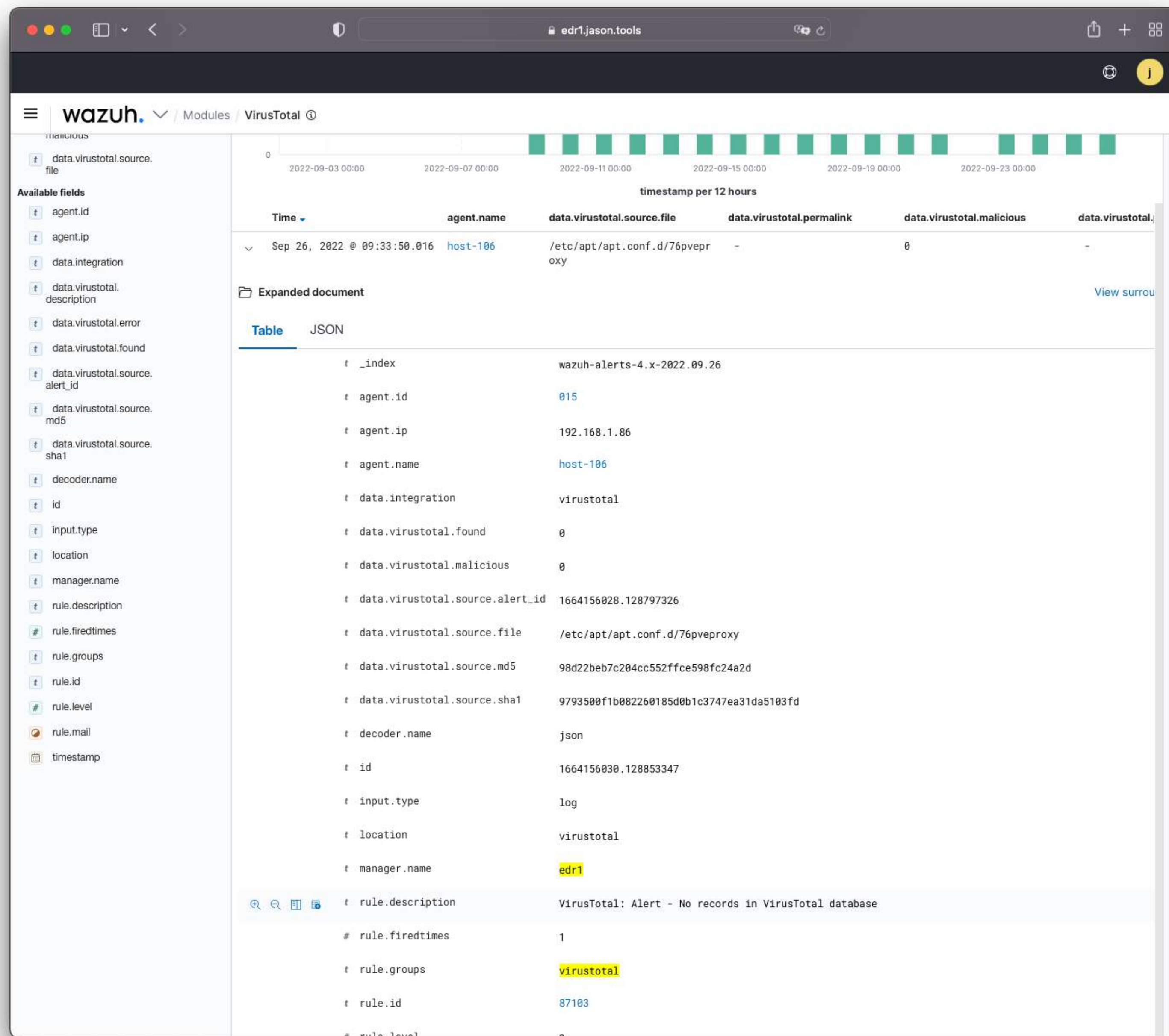
Docker

@timestamp	Apr 16, 2025 @ 23:12:25.594
_index	wazuh-alerts-4.x-2025.04.16
agent.id	025
agent.ip	192.168.1.89
agent.name	it-ts
data.docker.Action	exec_start: /bin/sh -c curl --silent --fail http://localhost: \${PORT:-8080}/health jq -ne 'input.status == true' exit 1
data.docker.Actor.Attributes.execID	c159eb235a9aebcaed136a2f56106a6ab9fcbd75db4d367c6b049aa180bc6f98
data.docker.Actor.Attributes.image	ghcr.io/open-webui/open-webui:latest
data.docker.Actor.Attributes.name	open-webui
data.docker.Actor.Attributes.org.opencontainers.image.created	2025-01-23T21:48:04.047Z
data.docker.Actor.Attributes.org.opencontainers.image.description	User-friendly AI Interface (Supports Ollama, OpenAI API, ...)
data.docker.Actor.Attributes.org.opencontainers.image.licenses	BSD-3-Clause
data.docker.Actor.Attributes.org.opencontainers.image.revision	b72150c881955721a63ae7f4ea1b9ea293816fc1
data.docker.Actor.Attributes.org.opencontainers.image.source	https://github.com/open-webui/open-webui
data.docker.Actor.Attributes.org.opencontainers.image.title	open-webui
data.docker.Actor.Attributes.org.opencontainers.image.url	https://github.com/open-webui/open-webui
data.docker.Actor.Attributes.org.opencontainers.image.version	main
data.docker.Actor.ID	ec0f0af75ed15b83872c76d4a95e4f6f3d9df406df0a795e4a03237575aaabc7
data.docker.Type	container
data.docker.from	ghcr.io/open-webui/open-webui:latest
data.docker.id	ec0f0af75ed15b83872c76d4a95e4f6f3d9df406df0a795e4a03237575aaabc7
data.docker.scope	local
data.docker.status	exec_start: /bin/sh -c curl --silent --fail http://localhost: \${PORT:-8080}/health jq -ne 'input.status == true' exit 1
data.docker.time	1744816345

惡意檔案比對

- VirusTotal
- 比對雜湊值

問題是沒錢買
VirusTotal API
啊啊啊啊



The screenshot displays the Wazuh VirusTotal module interface. On the left, a sidebar lists available fields for filtering and sorting. The main area shows a table of alerts with columns for Time, agent.name, data.virustotal.source.file, data.virustotal.permalink, data.virustotal.malicious, and data.virustotal. Below the table, an 'Expanded document' section shows the full JSON alert details.

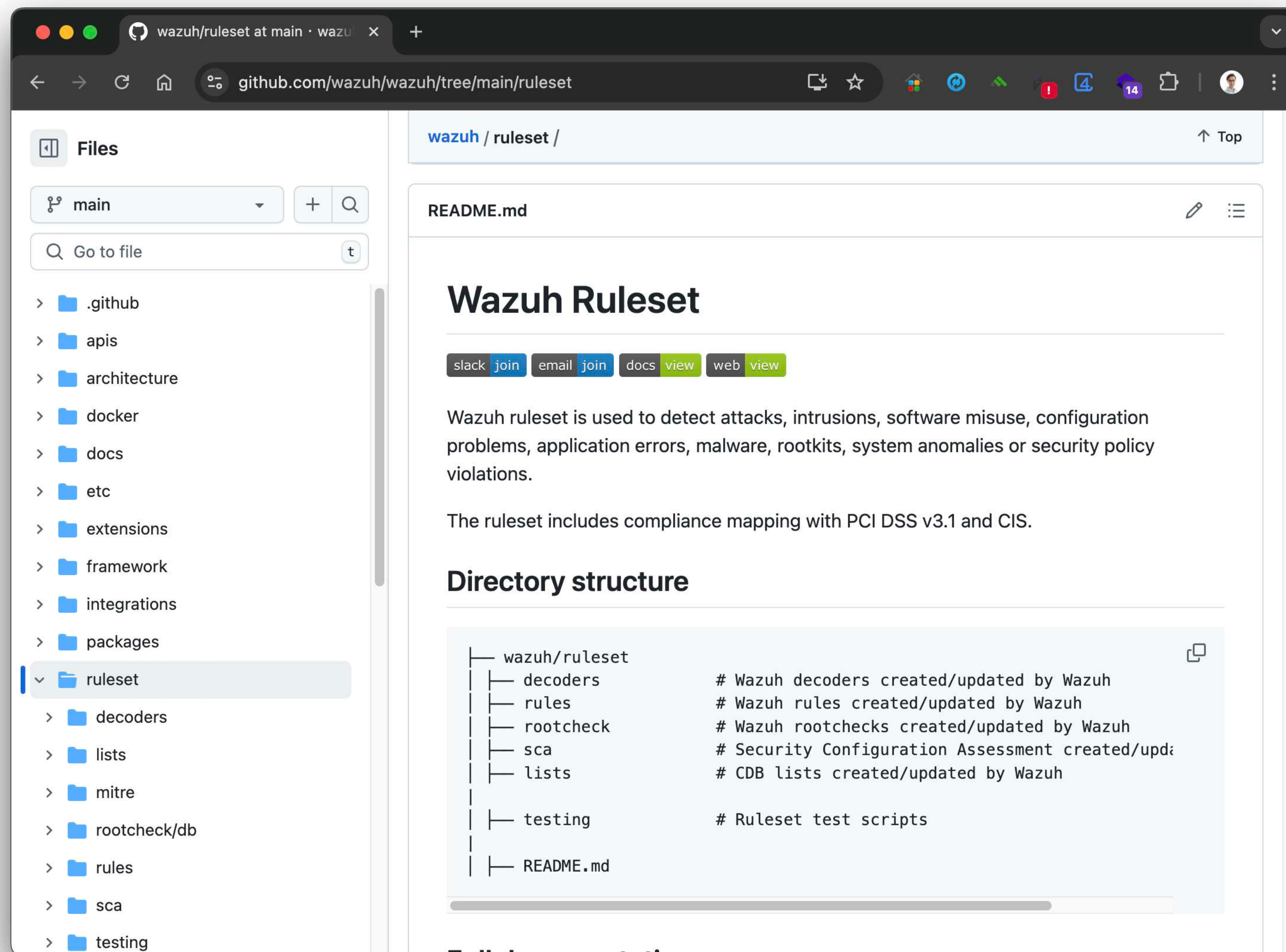
Time	agent.name	data.virustotal.source.file	data.virustotal.permalink	data.virustotal.malicious	data.virustotal.
Sep 26, 2022 @ 09:33:50.016	host-106	/etc/apt/apt.conf.d/76pveproxy	-	0	-

Expanded document

Field	Value
_index	wazuh-alerts-4.x-2022.09.26
agent.id	015
agent.ip	192.168.1.86
agent.name	host-106
data.integration	virustotal
data.virustotal.found	0
data.virustotal.malicious	0
data.virustotal.source.alert_id	1664156028.128797326
data.virustotal.source.file	/etc/apt/apt.conf.d/76pveproxy
data.virustotal.source.md5	98d22beb7c204cc552ffce598fc24a2d
data.virustotal.source.sha1	9793500f1b082260185d0b1c3747ea31da5103fd
decoder.name	json
id	1664156030.128853347
input.type	log
location	virustotal
manager.name	edr1
rule.description	VirusTotal: Alert - No records in VirusTotal database
rule.firedtimes	1
rule.groups	virustotal
rule.id	87103
rule.level	2

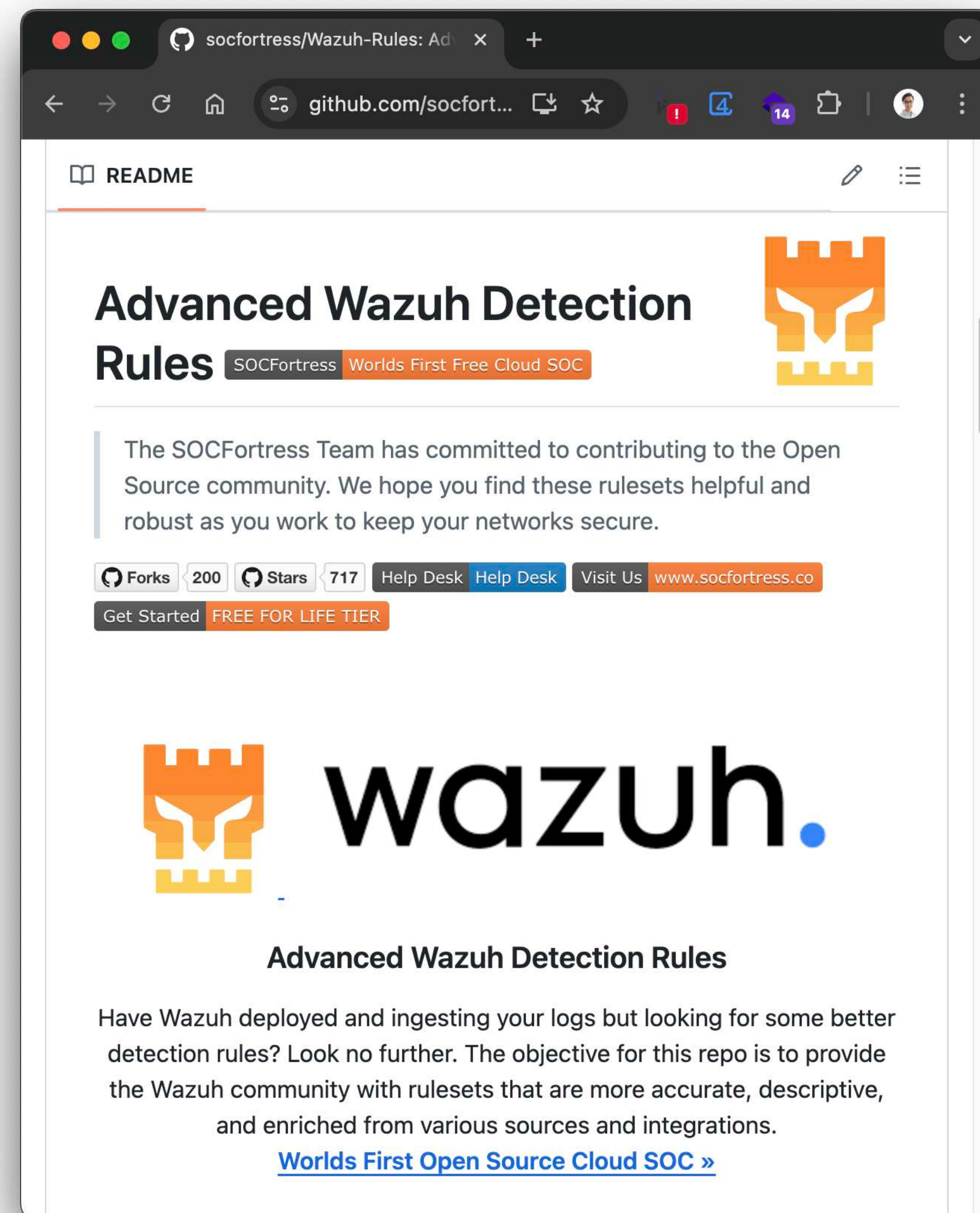
更多規則

- 內建規則
- 自動更新
- 手動啟用



更多進階規則

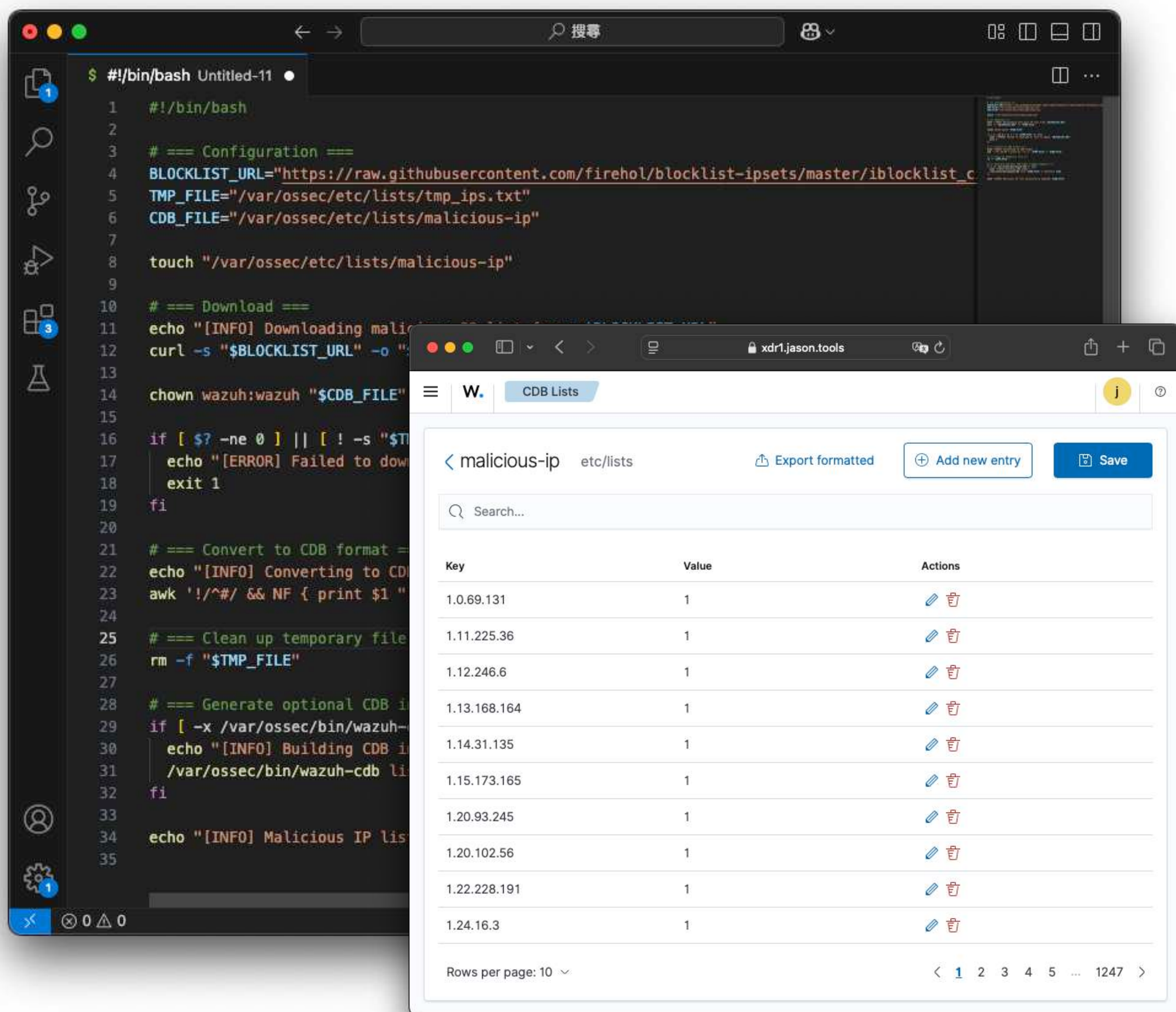
- Sysmon
- Sophos
- Suricata
- Falco
- Modsecurity
- F-Secure
- Snyc
- Sigcheck
- Crowdstrike
- Alienvault
- AbuseIPDB
- Auditd
- Maltrail
- Open Audit
- OPNsense
- Trend Micro
- Powershell
- Office365
- Osquery
- Yara



阻斷回應

阻斷惡意 IP

- 參考開源清單
- 自動下載更新
- 更新CDB清單
- 自訂比對規則



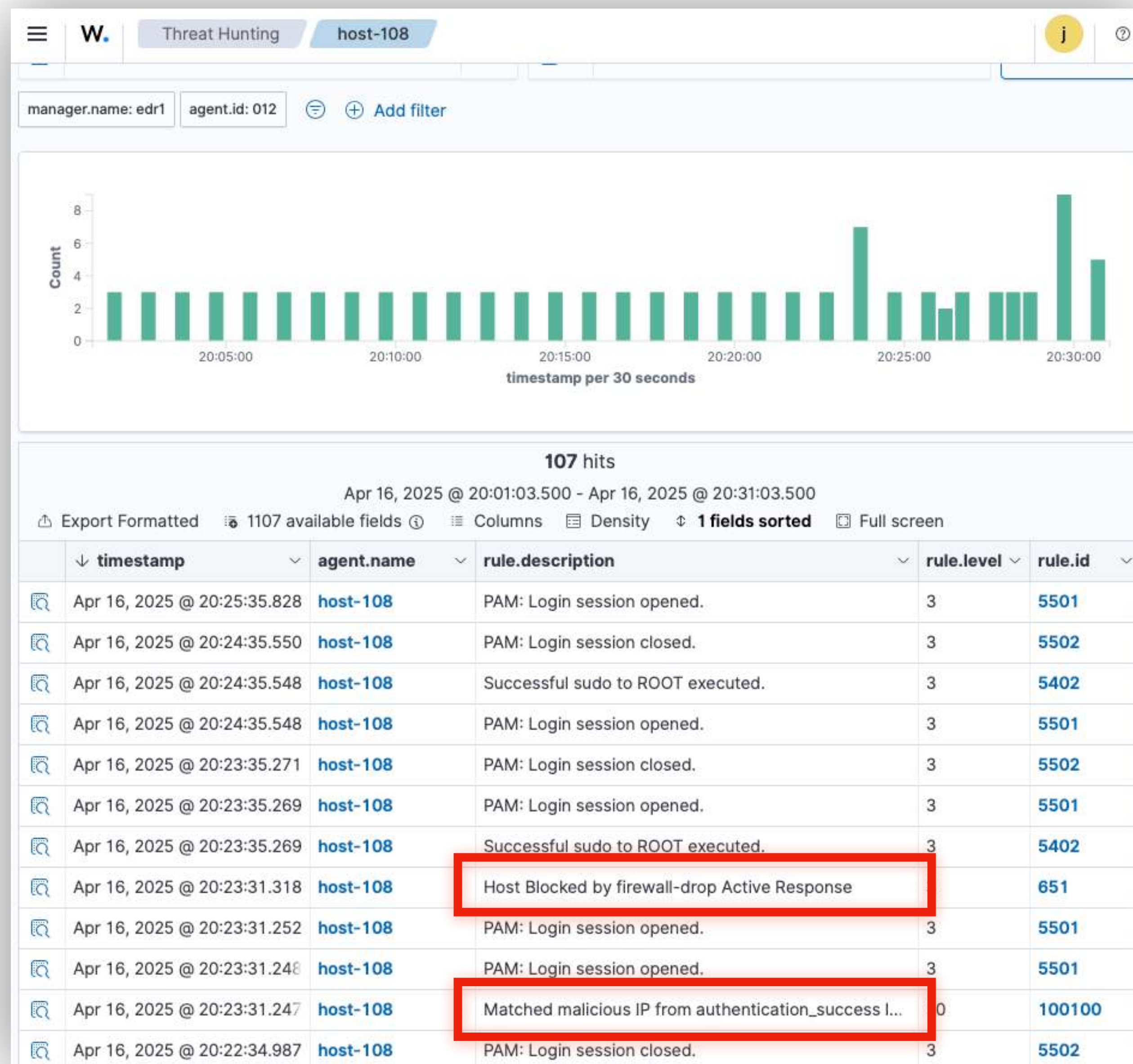
阻斷惡意 IP

● 自動偵測阻斷

● Linux
(firewall-drop)

● Windows
(netsh)

● OPNsense
(pfctl)





阻
斷
回
應

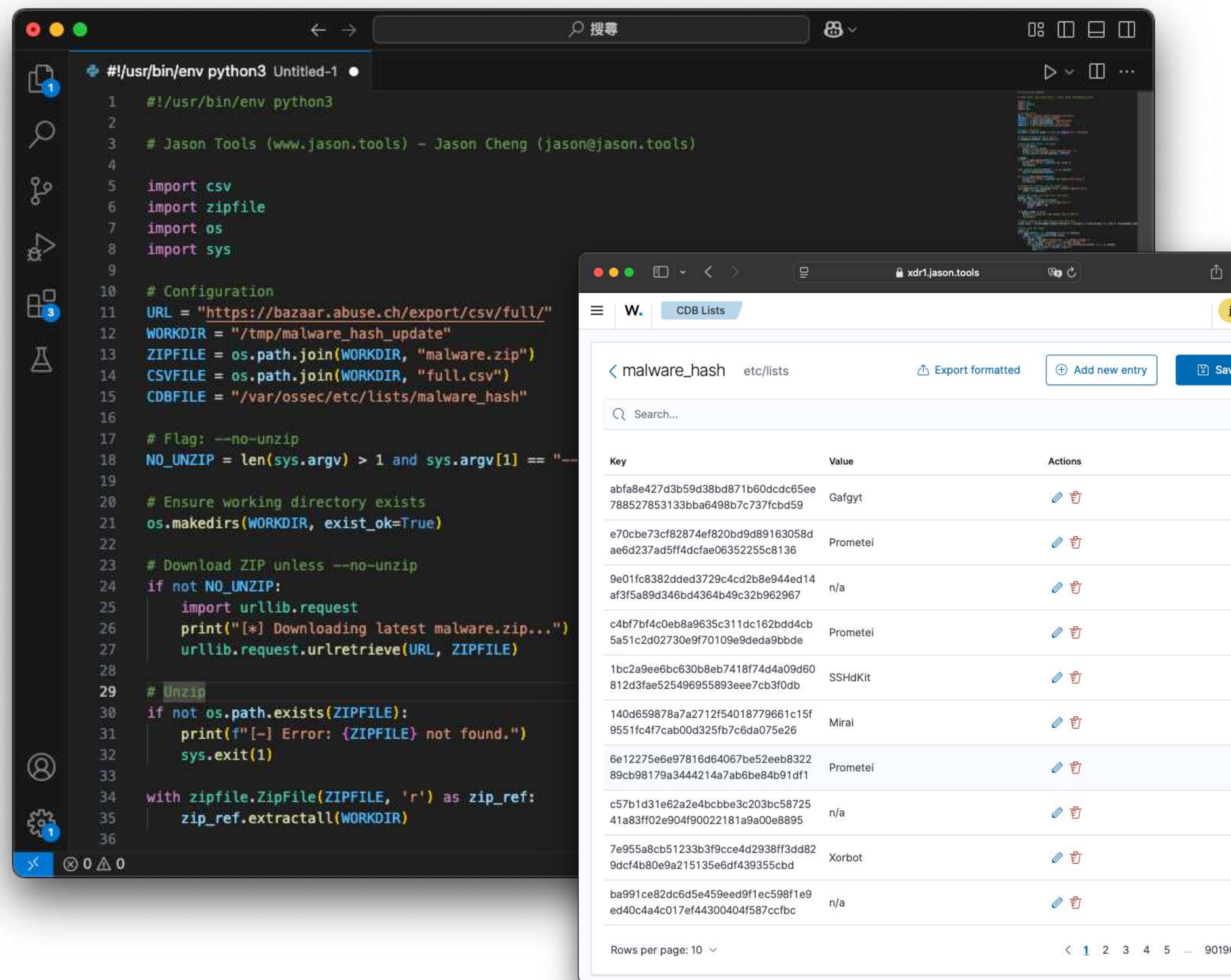
W.	Discover	wazuh-alerts-4.x-2025.04.16#_c2N...
t	_index	wazuh-alerts-4.x-2025.04.16
t	agent.name	host-108
t	data.dstuser	root
t	data.srcip	192.168.1.142
t	data.srcport	53340
t	decoder.name	sshd
t	decoder.parent	sshd
t	full_log	Apr 16 20:23:29 host-108 sshd[3489902]: Accepted password for root from 192.168.1.142 port 53340 ssh2
t	id	1744806211.212189871
t	input.type	log
t	location	/var/log/auth.log
t	manager.name	edr1
t	predecoder.hostname	host-108
t	predecoder.program_name	sshd
t	predecoder.timestamp	Apr 16 20:23:29
t	rule.description	Matched malicious IP from authentication_success logs
#	rule.firedtimes	1
t	rule.groups	malicious-ip
t	rule.id	100100
#	rule.level	10
t	rule.mail	false

W.	Discover	wazuh-alerts-4.x-2025.04.16#AM6NPpYBo2fM0Ddu9gAb
t	data.parameters.alert.manager.name	edr1
t	data.parameters.alert.pre	
t	data.parameters.alert.pre	
t	data.parameters.alert.pre	
t	data.parameters.alert.rule.description	Matched malicious IP from authentication_success logs
t	data.parameters.alert.rule.firedtimes	1
t	data.parameters.alert.rule.groups	malicious-ip
t	data.parameters.alert.rule.id	100100
t	data.parameters.alert.rule.level	10
t	data.parameters.alert.rule.mail	false
t	data.parameters.alert.timestamp	2025-04-16T20:23:31.247+0800
t	data.parameters.extra_args	
t	data.parameters.program	active-response/bin/firewall-drop
t	data.srcip	192.168.1.142
t	data.version	1
t	decoder.name	ar_log_json
t	decoder.parent	ar_log_json
t	full_log	>
		2025/04/16 20:23:31 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"},"command":"add","parameters":{"extra_args":[],"alert":{"timestamp":"2025-04-16T20:23:31.247+0800","rule":{"level":10,"description":"Matched malicious IP from authentication_success logs","id":"100100","firedtimes":1,"mail":false,"groups":["malicious-ip"]} "agent":{"
t	id	1744806211.212191096
t	input.type	log
t	location	/var/ossec/logs/active-responses.log
t	manager.name	edr1
t	rule.description	Host Blocked by firewall-drop Active Response
#	rule.firedtimes	1
t	rule.gdpr	IV_35.7.d
t	rule.gpg13	4.13
t	rule.groups	ossec, active_response
t	rule.id	651

端點立刻封鎖 IP

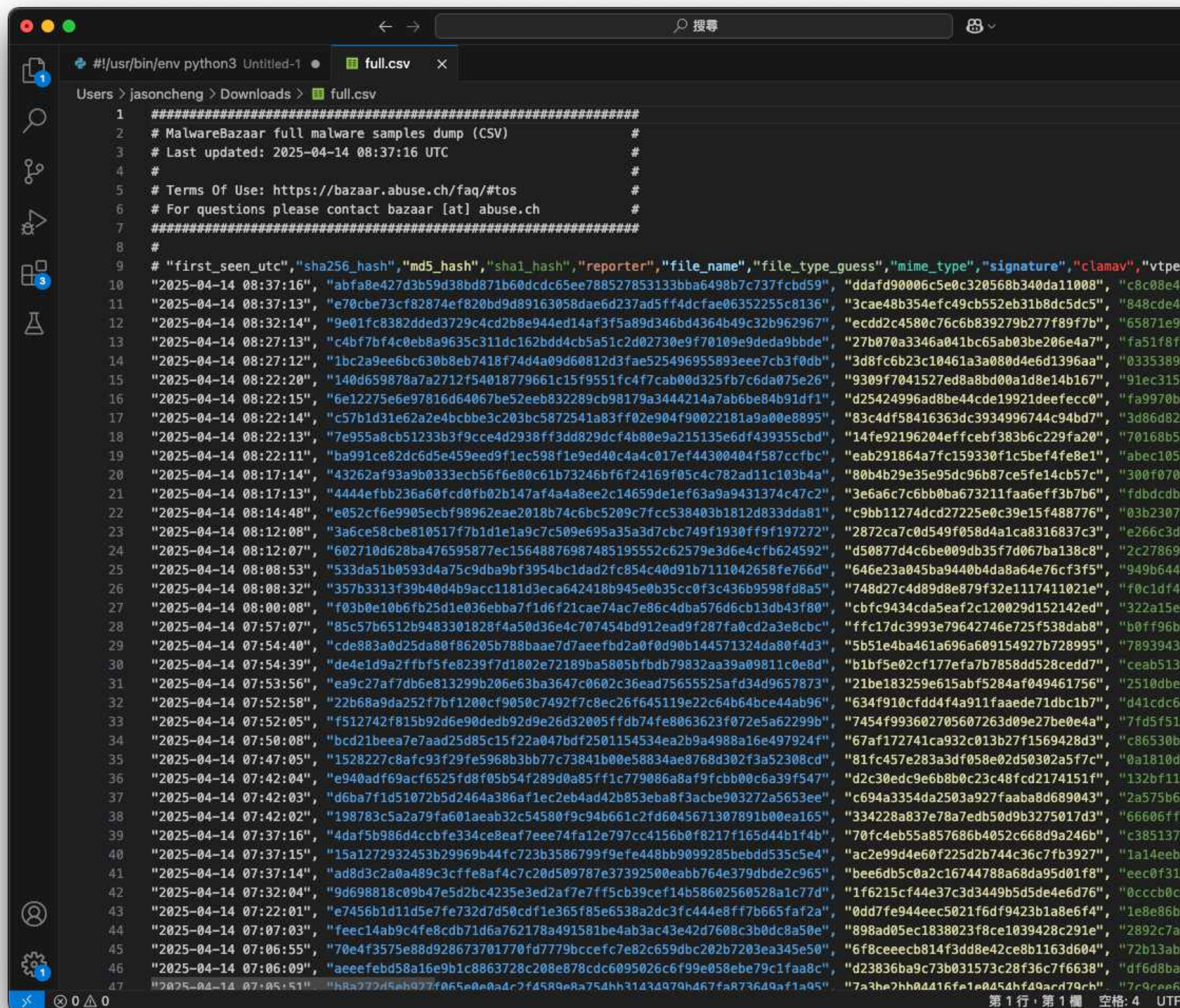
阻斷惡意檔案

- 參考開源清單
- 自動下載更新
- 更新CDB清單
- 自訂比對規則



阻斷惡意檔案

- bazaar.abuse.ch
- 每 24 小時更新一次
- 資料數 901892 筆
- sha256/md5
- reporter/signature



```
#!/usr/bin/env python3 Untitled-1 • full.csv x
Users > jasoncheng > Downloads > full.csv
1 #####
2 # MalwareBazaar full malware samples dump (CSV) #
3 # Last updated: 2025-04-14 08:37:16 UTC #
4 # #
5 # Terms Of Use: https://bazaar.abuse.ch/faq/#tos #
6 # For questions please contact bazaar [at] abuse.ch #
7 #####
8 #
9 # "first_seen_utc", "sha256_hash", "md5_hash", "sha1_hash", "reporter", "file_name", "file_type_guess", "mime_type", "signature", "clamav", "vtrpe
10 "2025-04-14 08:37:16", "abfa8e427d3b59d38bd871b60dc65ee788527853133bba6498b7c737fcbdb59", "ddafd90006c5e0c320568b340da11008", "c8c08e4
11 "2025-04-14 08:37:13", "e70cbe73cf82874ef820bd9d89163058dae6d237ad5ff4dcfae06352255c8136", "3cae48b354efc49cb552eb31b8dc5dc5", "848cde4
12 "2025-04-14 08:32:14", "9e01fc8382dded3729c4cd2b8e944ed14af3f5a89d346bd4364b49c32b962967", "ecdd2c4580c76c6b839279b277f89f7b", "65871e9
13 "2025-04-14 08:27:13", "c4bf7bf4c0eb8a9635c311dc162bdd4cb5a51c2d02730e9f70109e9deda9bbde", "27b070a3346a041bc65ab03be206e4a7", "fa51f8f
14 "2025-04-14 08:27:12", "1bc2a9ee6bc630b8eb7418f74d4a09d60812d3fae525496955893eee7cb3f0db", "3d8fc6b23c10461a3a080d4e6d1396aa", "0335389
15 "2025-04-14 08:22:20", "140d659878a7a2712f54018779661c15f9551fc4f7cab00d325fb7c6da075e26", "9309f7041527ed8a8bd00a1d8e14b167", "91ec315
16 "2025-04-14 08:22:15", "6e12275e6e97816d64067be52eeb832289cb98179a344421a7ab6be84b91df1", "d25424996ad8be44cde19921deefec0", "fa9970b
17 "2025-04-14 08:22:14", "c57b1d31e62a2e4cbcbbe3c203bc5872541a83ff02e904f90022181a9a00e8895", "83c4df58416363dc3934996744c94bd7", "3d86d82
18 "2025-04-14 08:22:13", "7e955a8cb51233b3f9cce4d2938ff3dd829dcf4b80e9a215135e6df439355cbd", "14fe92196204effcebf383b6c229fa20", "70168b5
19 "2025-04-14 08:22:11", "ba991ce82dc6d5e459eed9f1ec598f1e9ed40c4a4017ef44300404f587ccfbc", "eab291864a7fc159330f1c5bef4fe8e1", "abec105
20 "2025-04-14 08:17:14", "43262af93a9b0333ecb56f6e80c61b73246bf6f24169f05c4c782ad11c103b4a", "80b4b29e35e95dc96b87ce5fe14cb57c", "300f070
21 "2025-04-14 08:17:13", "4444efbb236a60fcd0fb02b147af4a4a8ee2c14659de1ef63a9a9431374c47c2", "3e6a6c7c6bb0ba673211faaeff3b7b6", "fdbdcdb
22 "2025-04-14 08:14:48", "e052cf6e9905ecbf98962eae2018b74c6bc5209c7fcc538403b1812d833dda81", "c9bb11274cd27225e0c39e15f488776", "03b2307
23 "2025-04-14 08:12:08", "3a6ce58cbe810517f7b1d1e1a9c7c509e695a35a3d7cbc749f1930ff9f197272", "2872ca7c0d549f058d4a1ca8316837c3", "e266c3d
24 "2025-04-14 08:12:07", "602710d628ba476595877ec15648876987485195552c62579e3d6e4cfb624592", "d50877d4c6be009db35f7d067ba138c8", "2c27869
25 "2025-04-14 08:08:53", "533da51b0593d4a75c9dba9bf3954bc1dad2fc854c40d91b711042658fe766d", "646e23a045ba9440b4da8a64e76cf3f5", "949b644
26 "2025-04-14 08:08:32", "357b3313f39b40d4b9acc1181d3eca642418b945e0b35cc0f3c436b9598fd8a5", "748d27c4d89d8e879f32e1117411021e", "f0c1df4
27 "2025-04-14 08:00:08", "f03b0e10b6fb25d1e036ebba7f1d6f21cae74ac7e86c4dba576d6cb13db43f80", "cbfc9434cda5eaf2c120029d152142ed", "322a15e
28 "2025-04-14 07:57:07", "85c57b6512b9483301828f4a50d36e4c707454bd912ead9f287fa0cd2a3e8cbc", "ffc17dc3993e79642746e725f538dab8", "b0ff96b
29 "2025-04-14 07:54:40", "cde883a0d25da80f86205b788baae7d7aefb2a0f0d90b144571324da80f4d3", "5b51e4ba461a696a609154927b728995", "7893943
30 "2025-04-14 07:54:39", "de4e1d9a2ffbf5fe8239f7d1802e72189ba5805bfbdb79832aa39a09811c0e8d", "b1bf5e02cf177efa7b7858dd528cedd7", "ceab513
31 "2025-04-14 07:53:56", "ea9c27af7db6e813299b206e63ba3647c0602c36ead75655525afd34d9657873", "21be183259e615abf5284af049461756", "2510dbe
32 "2025-04-14 07:52:58", "22b68a9da252f7bf1200cf9050c7492f7c8ec26f645119e22c64b64bce44ab96", "634f910cfdd4f4a911faae71dbcb1b7", "d41cdc6
33 "2025-04-14 07:52:05", "f512742f815b92d6e90dedb92d9e26d32005ffdb74fe8063623f072e5a62299b", "7454f993602705607263d09e27be0e4a", "7fd5f51
34 "2025-04-14 07:50:08", "bcd21beea7e7aad25d85c15f22a047bdf2501154534ea2b9a4988a16e497924f", "67af172741ca932c013b27f1569428d3", "c86530b
35 "2025-04-14 07:47:05", "1528227c8afc93f29fe5968b3bb77c73841b00e58834ae768d302f3a52308cd", "81fc457e283a3df058e02d50302a5f7c", "0a1810d
36 "2025-04-14 07:42:04", "e940ad69ac6525fd8f05b54f289d0a85ff1c779086a8af9fcb00c6a39f547", "d2c30edc9e6b8b0c23c48fcd2174151f", "132bf11
37 "2025-04-14 07:42:03", "d6ba7f1d51072b5d2464a386af1ec2eb4ad42b853eba8f3acbe903272a5653ee", "c694a3354da2503a927faaba8d689043", "2a575b6
38 "2025-04-14 07:42:02", "198783c5a2a79fa601aeab32c54580f9c94b661c2fd6045671307891b00ea165", "334228a837e78a7edb50d9b3275017d3", "66606ff
39 "2025-04-14 07:37:16", "4daf5b986d4ccbf334ce8eaf7eee74fa12e797cc4156b0f8217f165d44b1f4b", "70fc4eb55a857686b4052c668d9a246b", "c385137
40 "2025-04-14 07:37:15", "15a1272932453b29969b44fc723b3586799f9efe448bb9099285bebdd535c5e4", "ac2e99d4e60f225d2b744c36c7fb3927", "1a14eeb
41 "2025-04-14 07:37:14", "ad8d3c2a0a489c3cffe8af4c7c20d509787e3739250eabb764e379dbde2c965", "bee6db5c0a2c16744788a68da95d01f8", "eec0f31
42 "2025-04-14 07:32:04", "9d698818c09b47e5d2bc4235e3ed2af7e7ff5cb39cef14b58602560528a1c77d", "1f6215cf44e37c3d3449b5d5de4e6d76", "0cccb0c
43 "2025-04-14 07:22:01", "e7456b1d11d5e7fe732d7d50cdf1e365f85e6538a2dc3fc444e8ff7b665faf2a", "0dd7fe944eec5021f6df9423b1a8e6f4", "1e8e86b
44 "2025-04-14 07:07:03", "feec14ab9c4fe8cdb71d6a762178a491581be4ab3ac43e42d7608c3b0dc8a50e", "898ad05ec1838023f8ce1039428c291e", "2892c7a
45 "2025-04-14 07:06:55", "70e4f3575e88d928673701770fd7779bccefc7e82c659dbc202b7203ea345e50", "6f8ceeeeb814f3dd8e42ce8b1163d604", "72b13ab
46 "2025-04-14 07:06:09", "aeefebd58a16e9b1c8863728c208e878cdc6095026c6f99e058ebe79c1faa8c", "d23836ba9c73b031573c28f36c7f6638", "df6d8ba
47 "2025-04-14 07:05:51", "h8a772d5ab927f0665e0e0a4dc2f4589e8a754hb31434979b467fa873640a1a95", "7a3be2bb04416fe1e0454bf49acd79cb", "7c9ce66
```



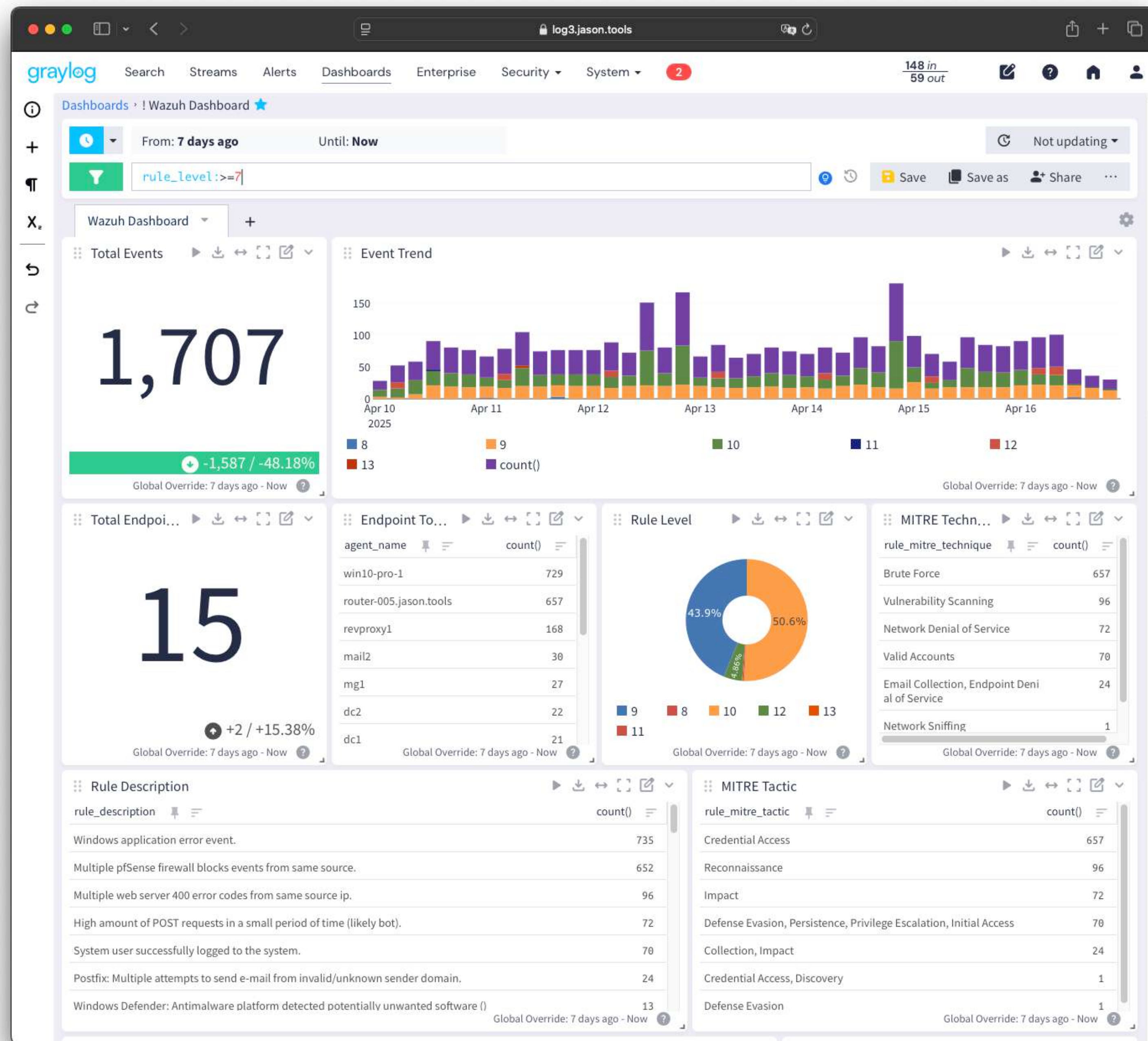
節省工具箱
JASON TOOLS

Graylog 搭配使用



整合看板

- 轉送記錄
- 欄位拆解
- 看板製作

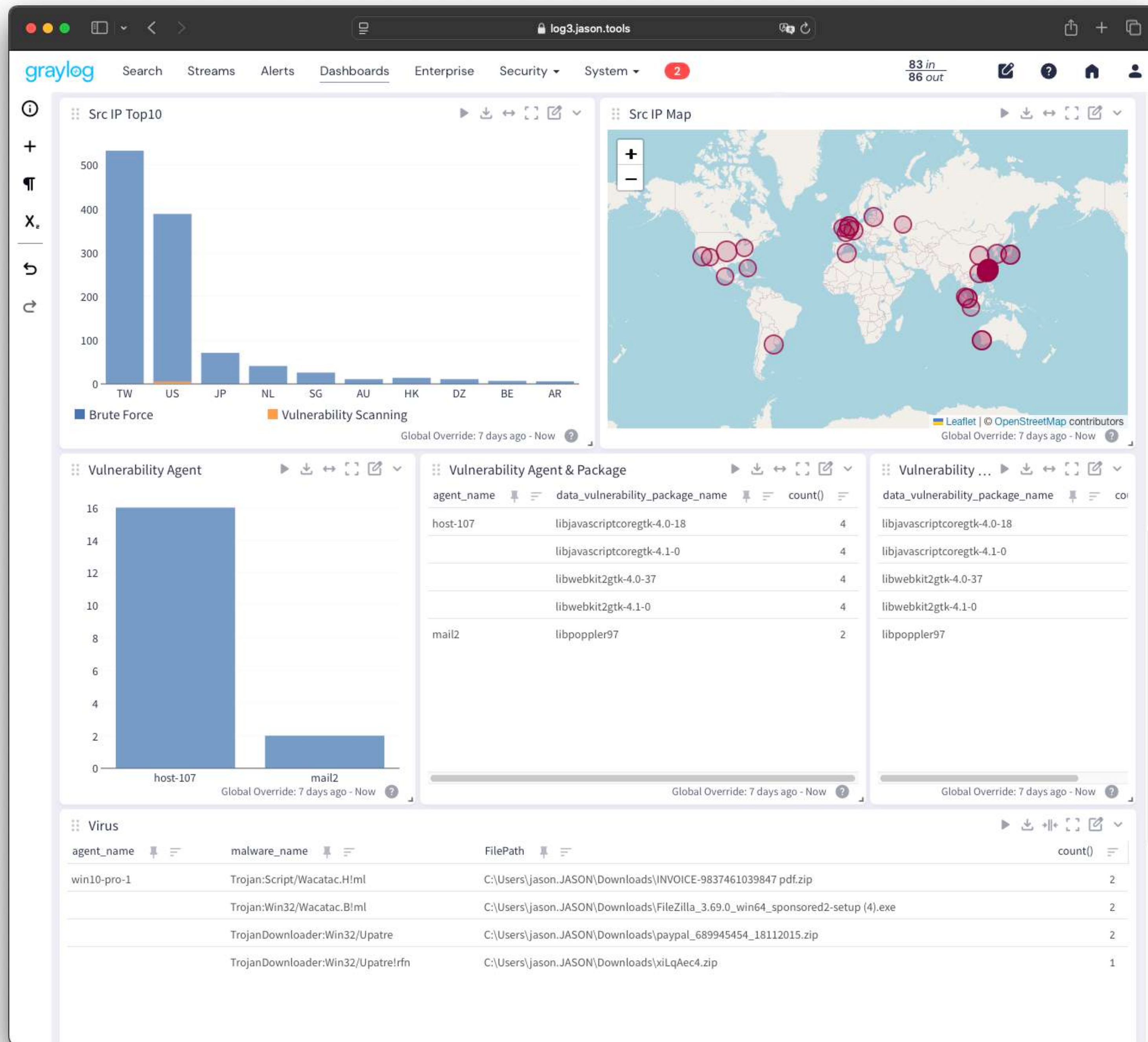




搭配 Graylog

整合看板

- 來源國家
- 軟體漏洞
- 惡意檔案





- 修改設定
- 轉送位址
- 指定等級
- 選定格式

```
GNU nano 6.2 /var/ossec/etc/ossec.conf

<syslog_output>
  <level>8</level>
  <server>192.168.1.127</server>
  <port>30514</port>
  <format>json</format>
</syslog_output>

<!-- Choose between "plain", "json", or "plain,json" for the fo
<logging>
  <log_format>plain</log_format>
</logging>

<remote>
  <connection>secure</connection>
  <port>1514</port>
  <protocol>tcp</protocol>
  <queue_size>131072</queue_size>
</remote>

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Ex
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Ju
```



- 抽出 JSON 字串
- 拆解 JSON 欄位

Extractor configuration

Extractor type	JSON
Source field	wazuh_json

☐ Flatten structures
Whether to flatten JSON objects into a single message field or to expand into multiple fields.

List item separator
What string to use to concatenate items of a JSON list.

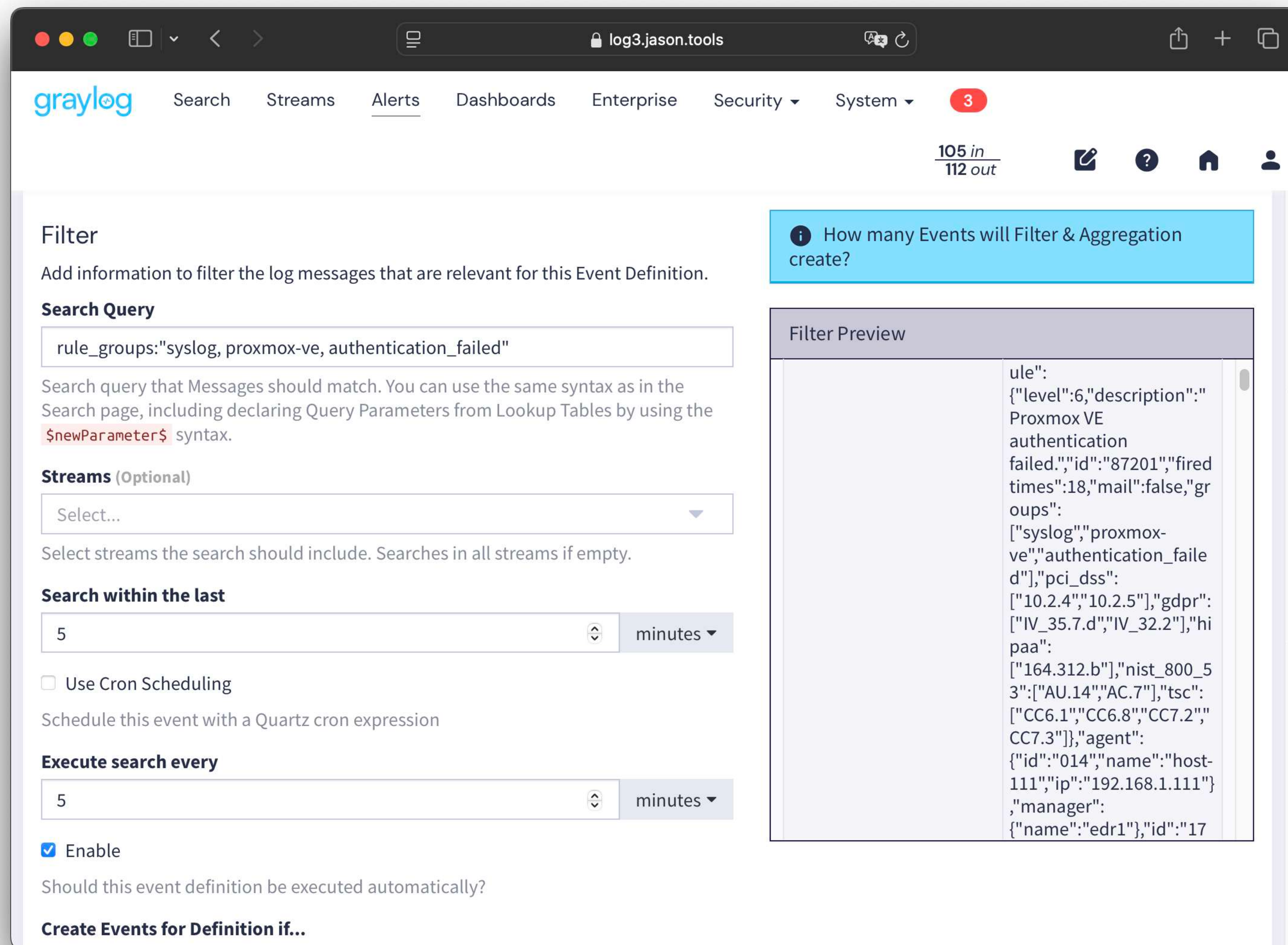
Key separator
What string to use to concatenate different keys of a nested JSON object (only used if *not* flattened).

Key/value separator
What string to use when concatenating key/value pairs of a JSON object (only used if



- 設定條件
- 限制閥值
- 發送訊息
- 搭配系統

LibreNMS+Telegram





節省工具箱
JASON TOOLS

Agent 資料來源



監測來源 Agent:

- 目前執行程序
- 資源使用狀況
- 執行程序建立或終止
- 目前登入使用者
- 登入登出事件
- 使用者權限變更
- 提權記錄
- 帳號建立或異動刪除
- 目前監聽連接埠
- 網路連線狀況表
- 已安裝軟體套件
- 已啟動系統服務
- 系統排程作業

監測來源 Agent:

- 檔案完整性監控
- 重要系統檔案異動
- 檔案權限變更
- 惡意軟體偵測
- 防火牆記錄
- DNS 查詢
- 處理器使用率
- 記憶體使用率
- 磁碟使用率
- 系統負載

未來計劃

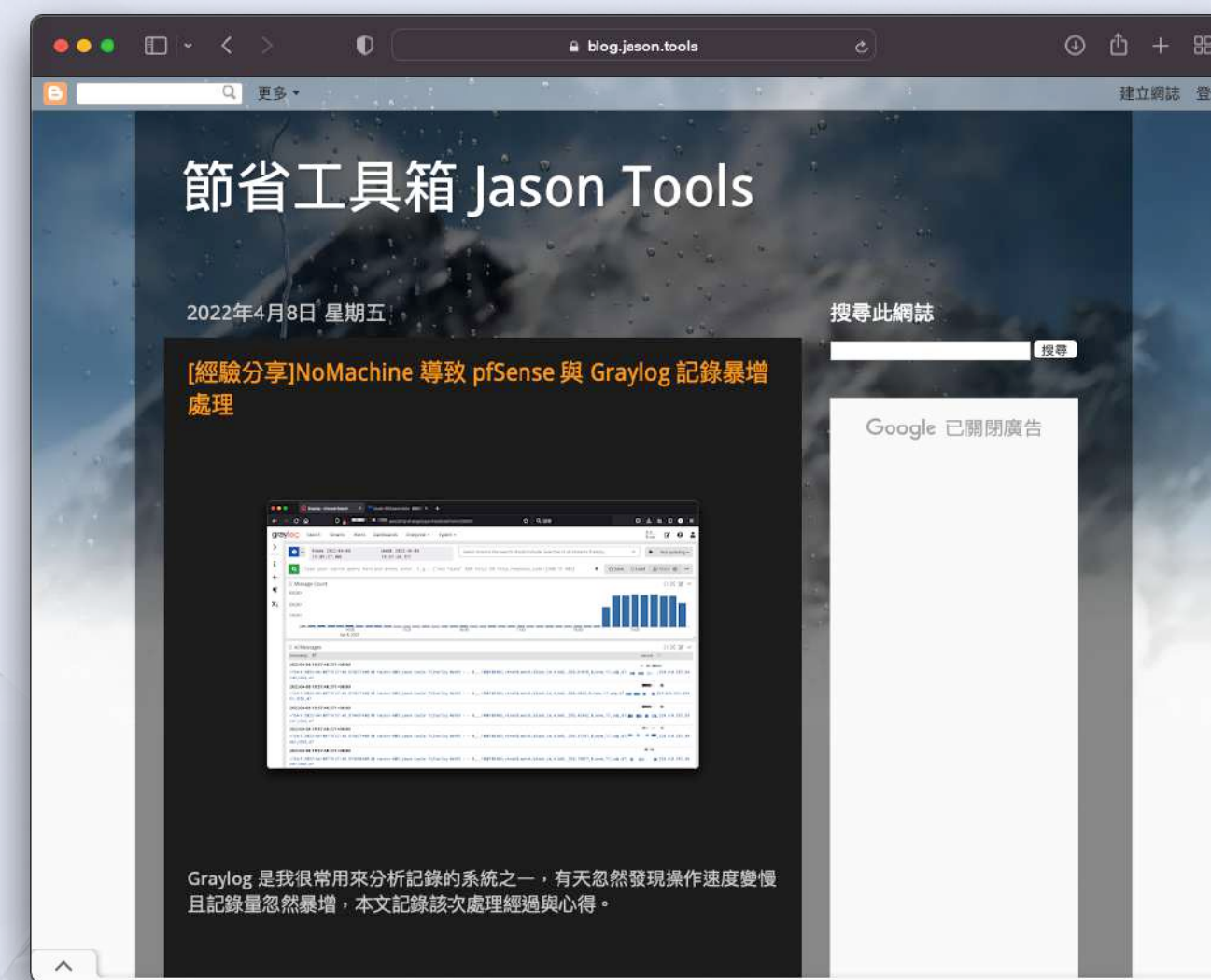
強化監測

- 整合自建 MISP 判斷威脅
<https://github.com/juaromu/wazuh-misp>
- 整合 Sigma Rules 增強識別能力
<https://github.com/theflakes/StoW>
- 整合自建 AI 判讀行為與軌跡，並自動畫時序圖
唉，前天做到一半 AI 主機的 CPU 跟 GPU 操到燒掉，沒成果可以放.....嗚嗚

參考資料



節省工具箱公司
www.jason.tools

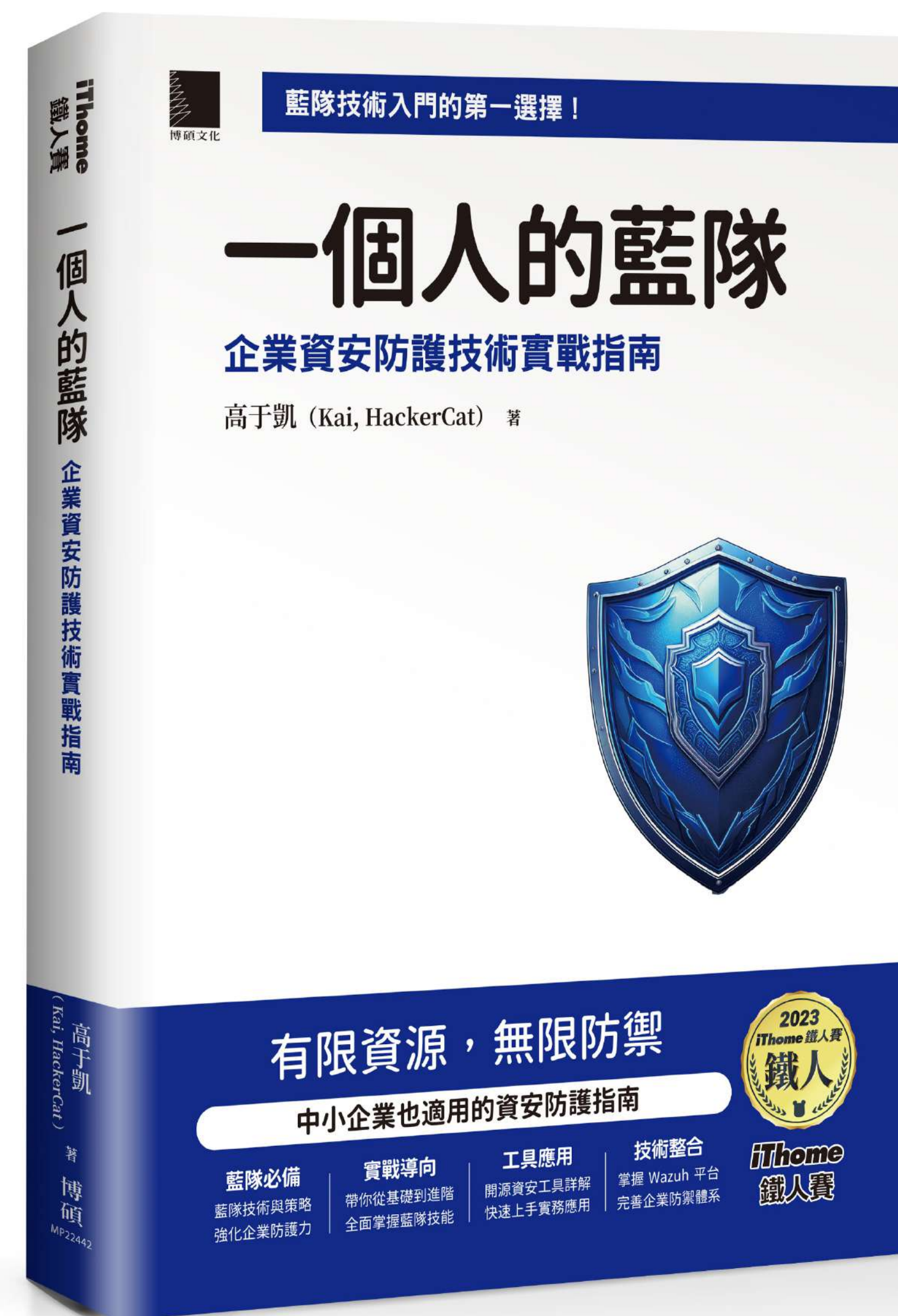


節省工具箱網誌
blog.jason.tools

強力推薦

- HackerCat 著作
- Wazuh 使用指南
- Jason 推薦序 😎

看看這標題，多麼 ~~淒涼~~ 紮實....



這本不是我寫的不要誤會

謝謝您。

節省工具箱有限公司

企業應用開源軟體方案導入專家

