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

TEAM CYBERSECURITY

**鄭郁霖 Jason Cheng**

節省工具箱有限公司

技術總監

節省工具箱
JASON TOOLS

# 簡介

## 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

節省工具箱
JASON TOOLS

起因

做ㄗㄨㄛˋ資ㄗ安ㄢ

XDR

很ㄏㄣˇ重ㄓㄨㄥˋ要ㄧㄠˋ

知道為啥不買？

旁邊加注音表示這是基本啊！

節省工具箱
JASON TOOLS

結果

# 錢能解決的問題都不是問題

# 😭 問題是沒有錢 😭

節省工具箱
JASON TOOLS

# 難嗎？不難！

節省工具箱
JASON TOOLS

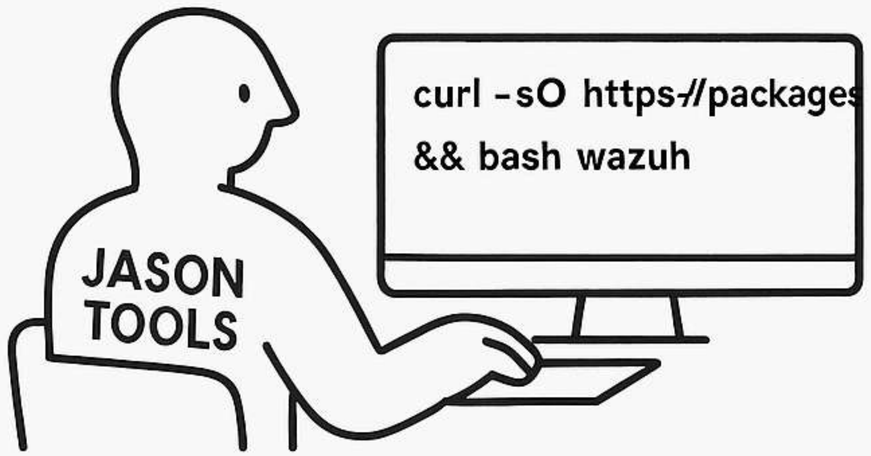
# 四步上線

簡單到爆

節省工具箱
JASON TOOLS

# 四步上線

## 1 EASY INSTALL




## 2 LOGIN WEBUI


## 3 DEPLOY AGENT


## 4 OPEN DASHBOARD


OK!!

節省工具箱
JASON TOOLS

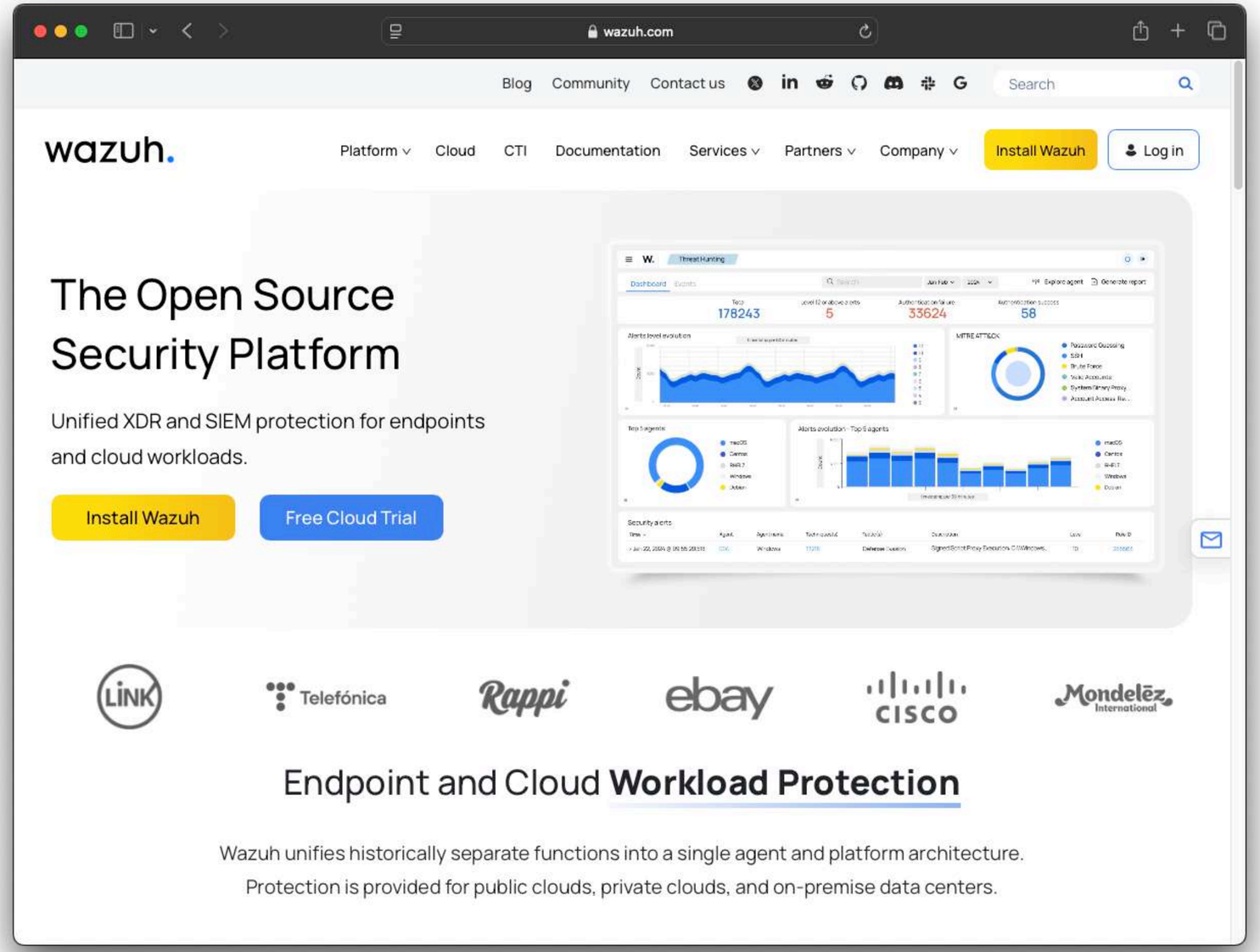
# 功能概觀

節省工具箱
JASON TOOLS

原廠

# Wazuh

- 商業公司
- 美國
- 開源軟體
- 商業服務

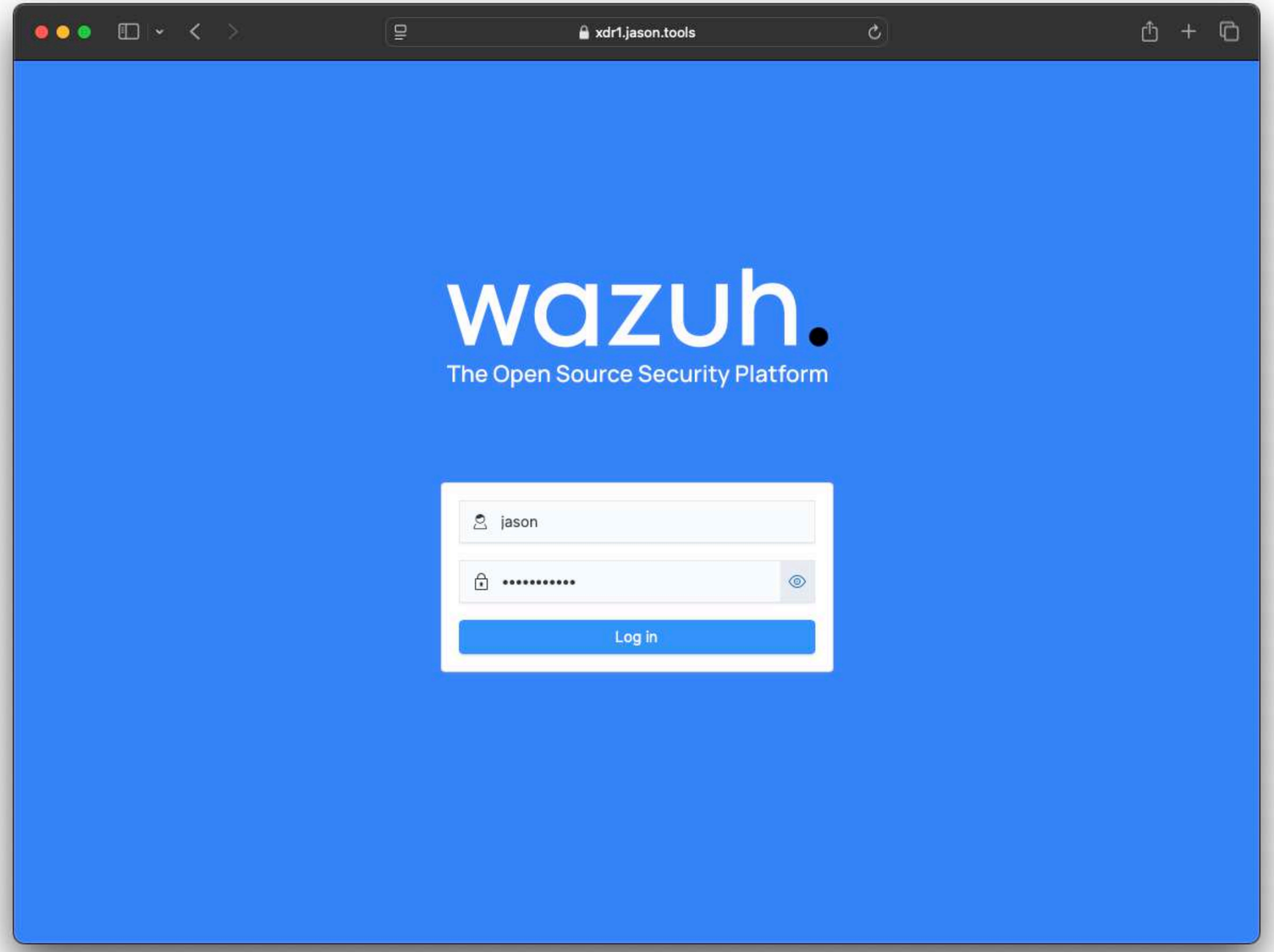


節省工具箱
JASON TOOLS

功能概觀

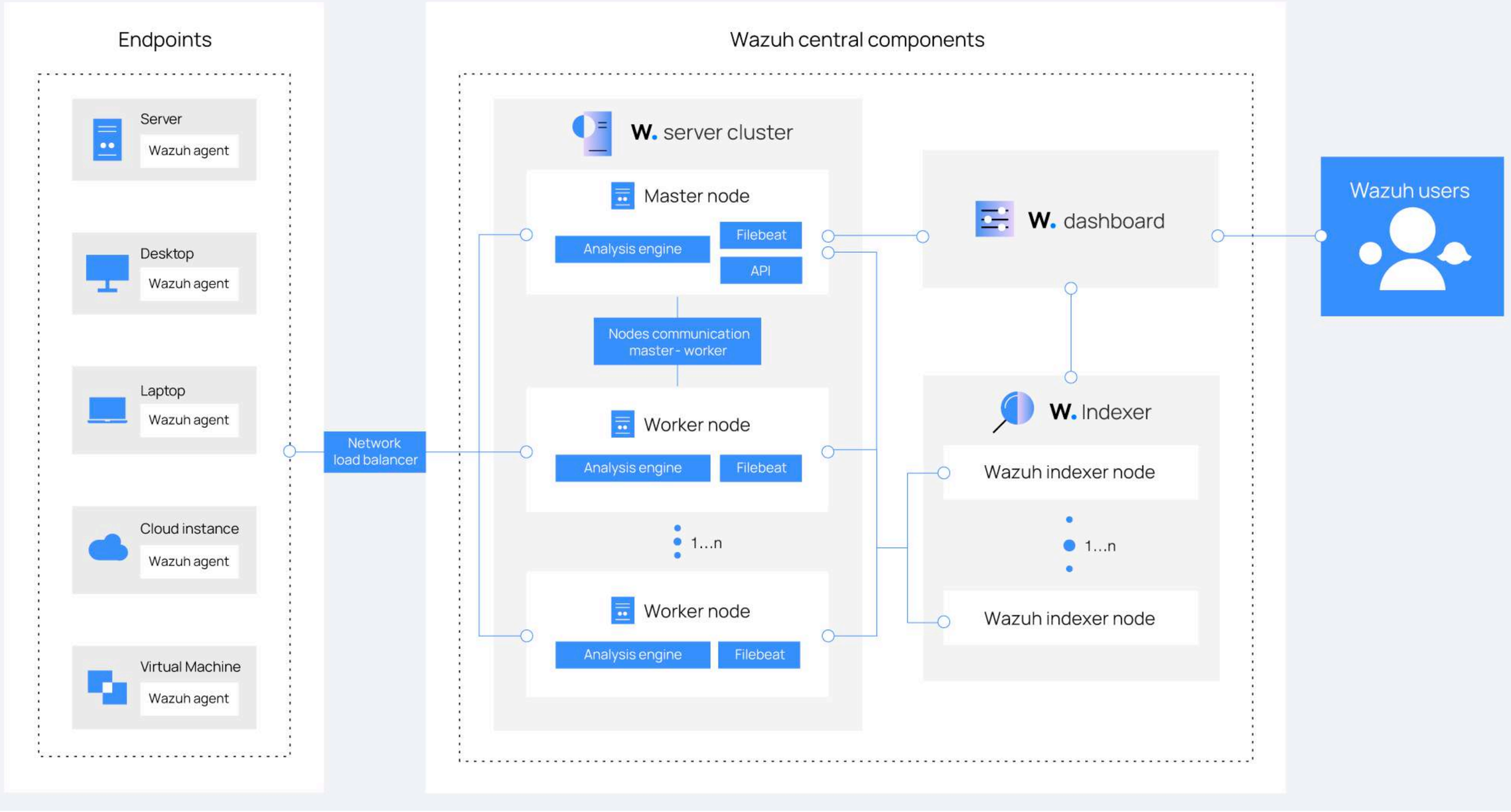
# 系統特點

- 功能豐富
- 網頁管理
- 叢集架構
- 開放源碼
- 跨平台



節省工具箱
JASON TOOLS

# 架構




端點　伺服器　索引與看板　管理者

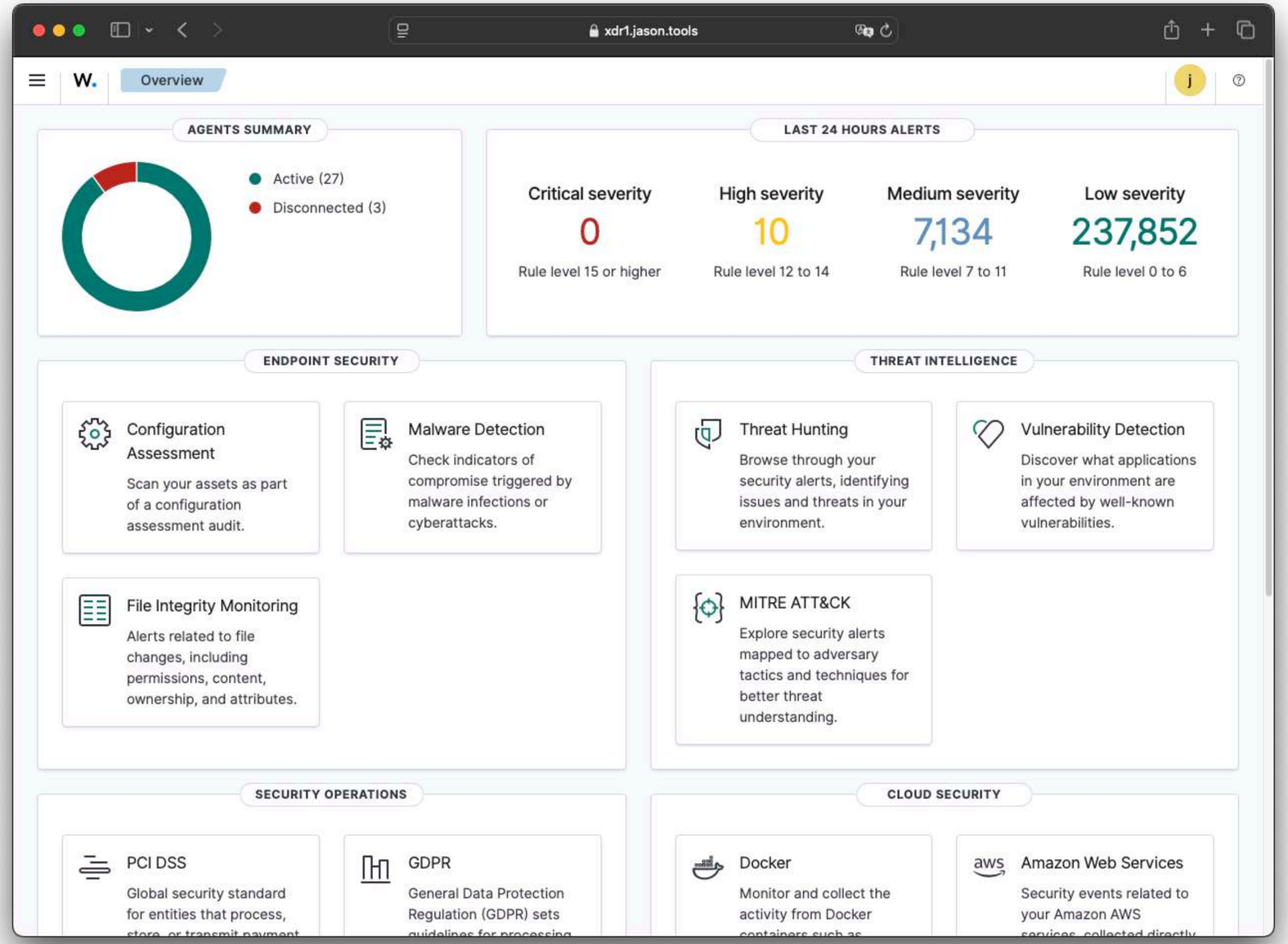
資料來源 https://wazuh.com/platform/

節省工具箱
JASON TOOLS

功能概觀

# 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

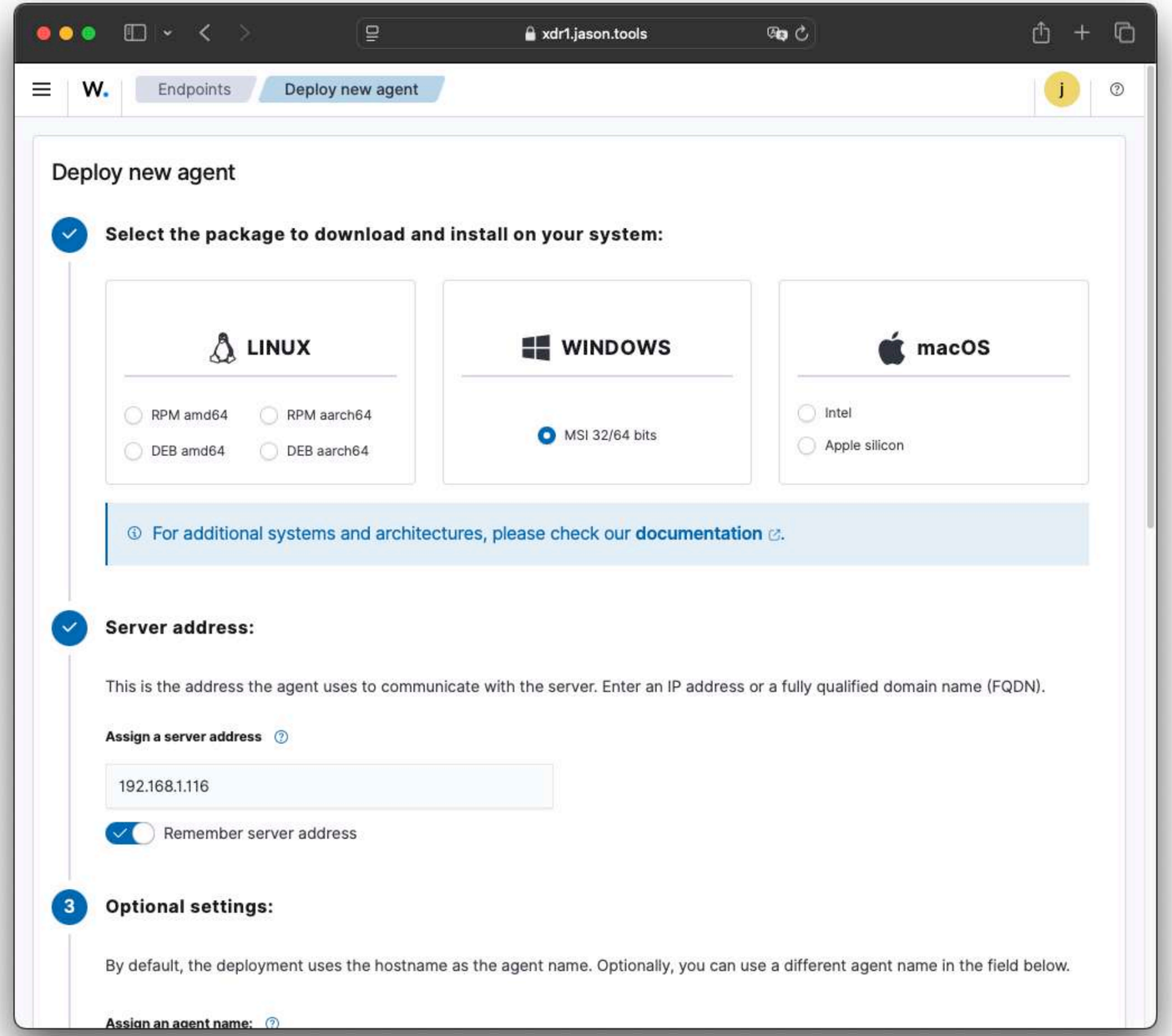


節省工具箱
JASON TOOLS

功能概觀

# 端點

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

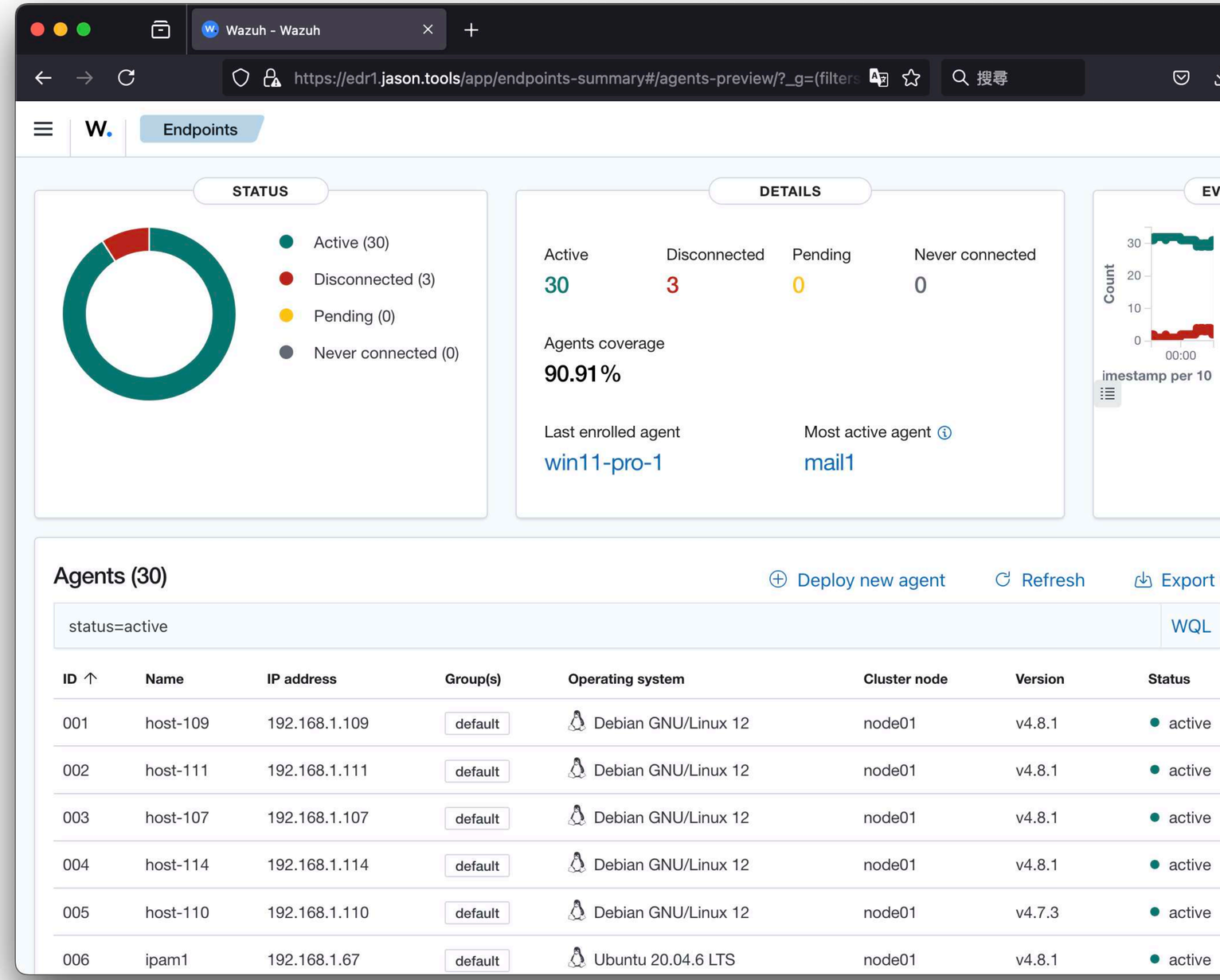


節省工具箱
JASON TOOLS

功能概觀

# 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

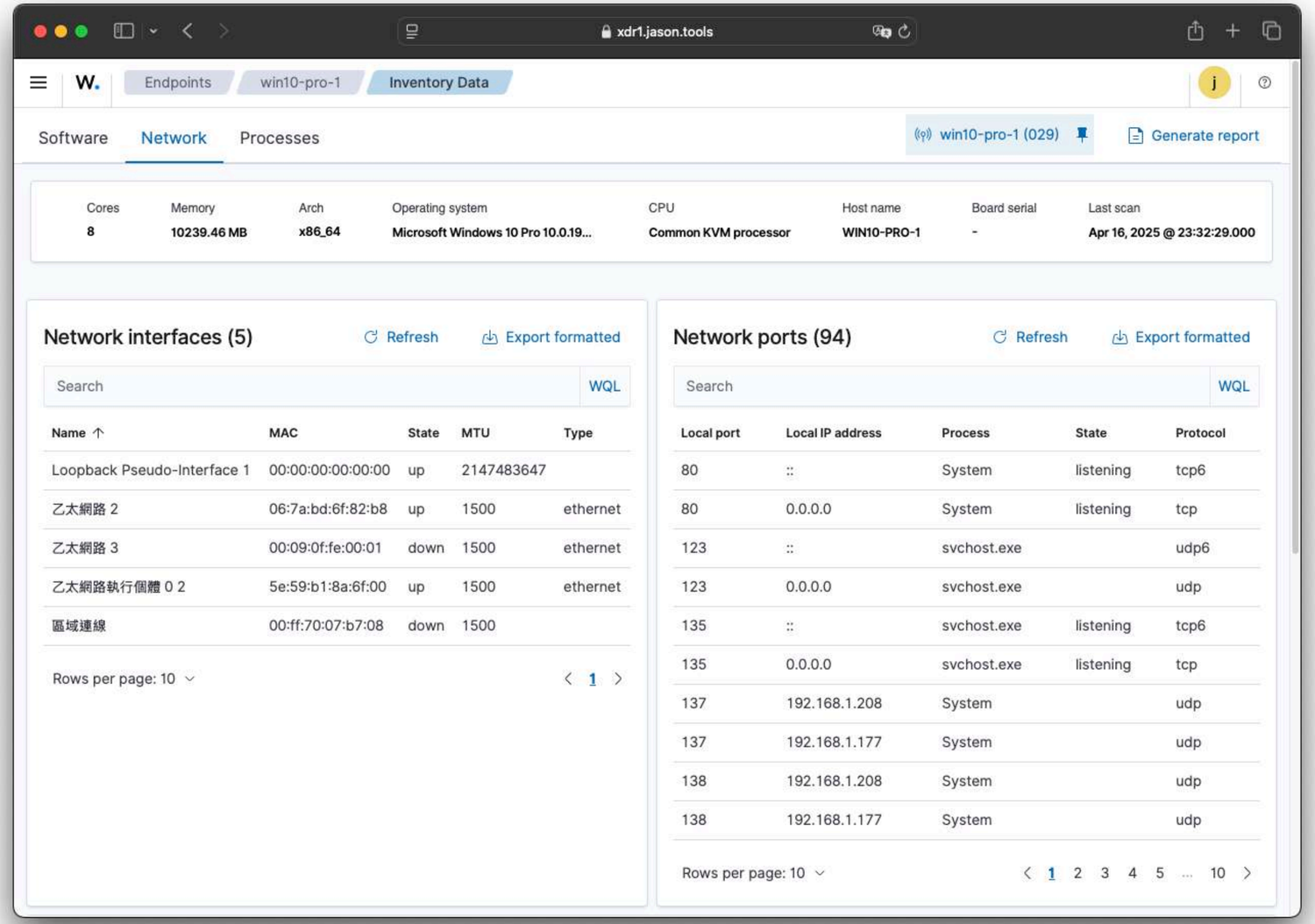


節省工具箱
JASON TOOLS

功能概觀

# 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

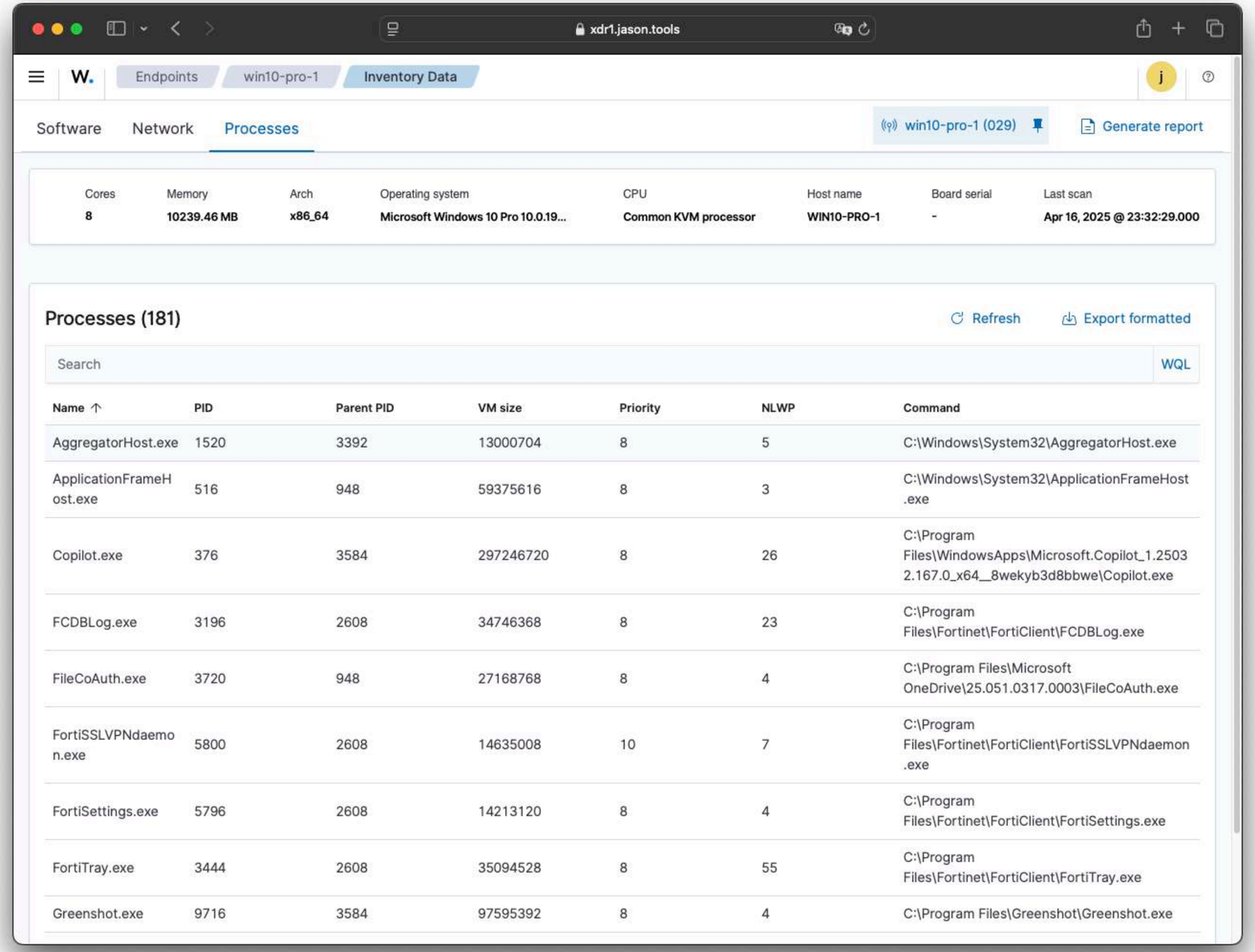


節省工具箱
JASON TOOLS

功能概觀

# 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

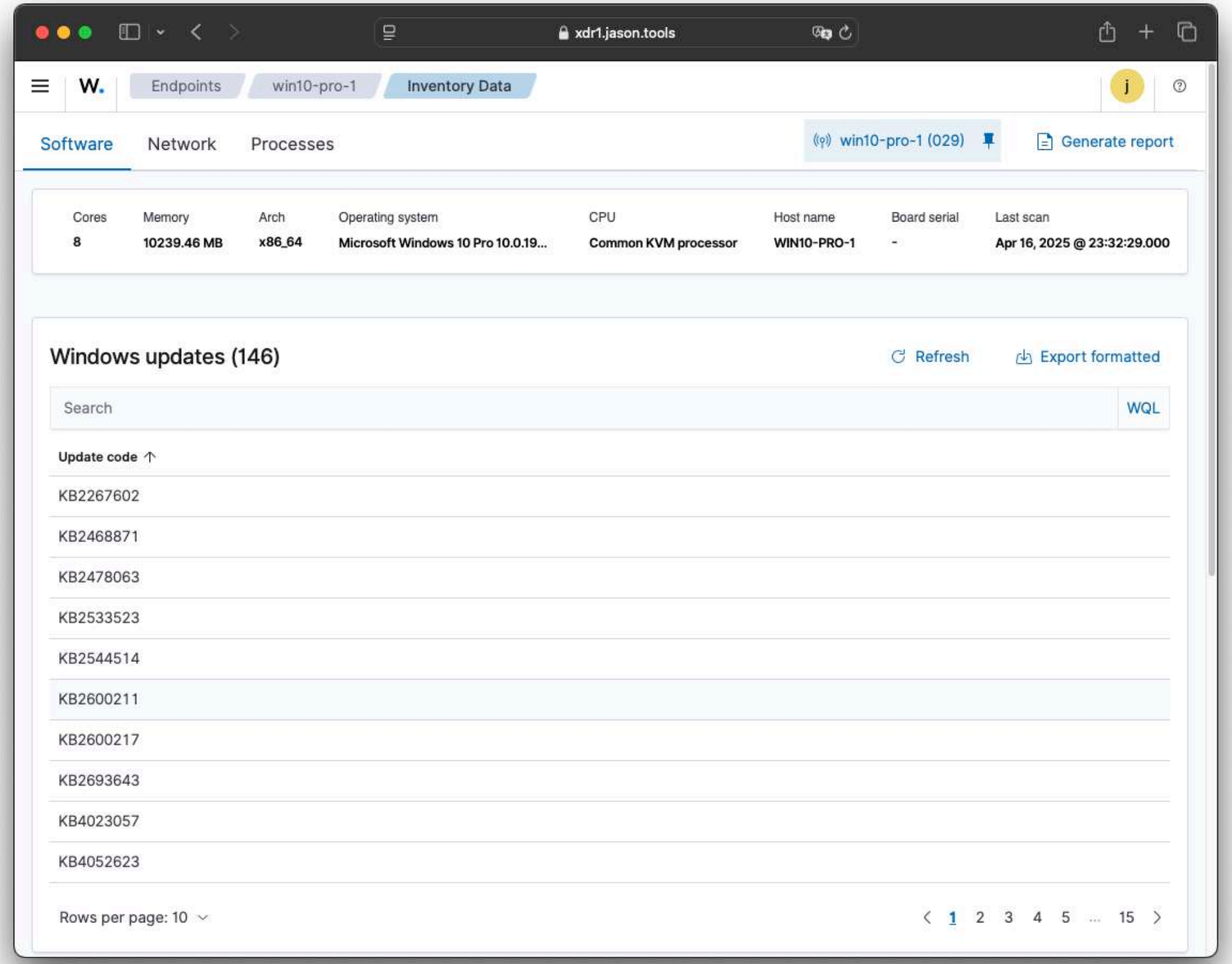


節省工具箱
JASON TOOLS

功能概觀

# 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

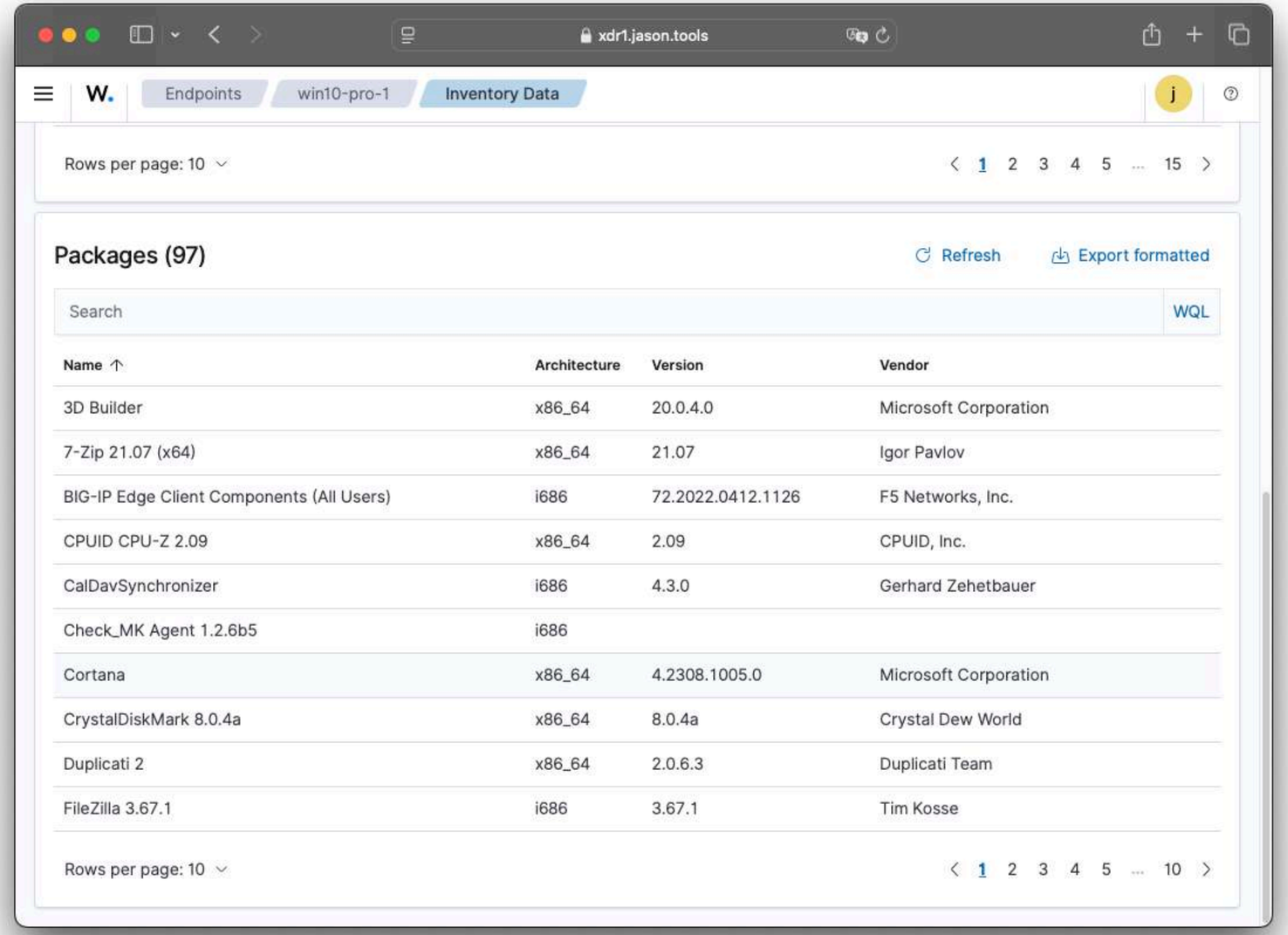


節省工具箱
JASON TOOLS

功能概觀

# 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

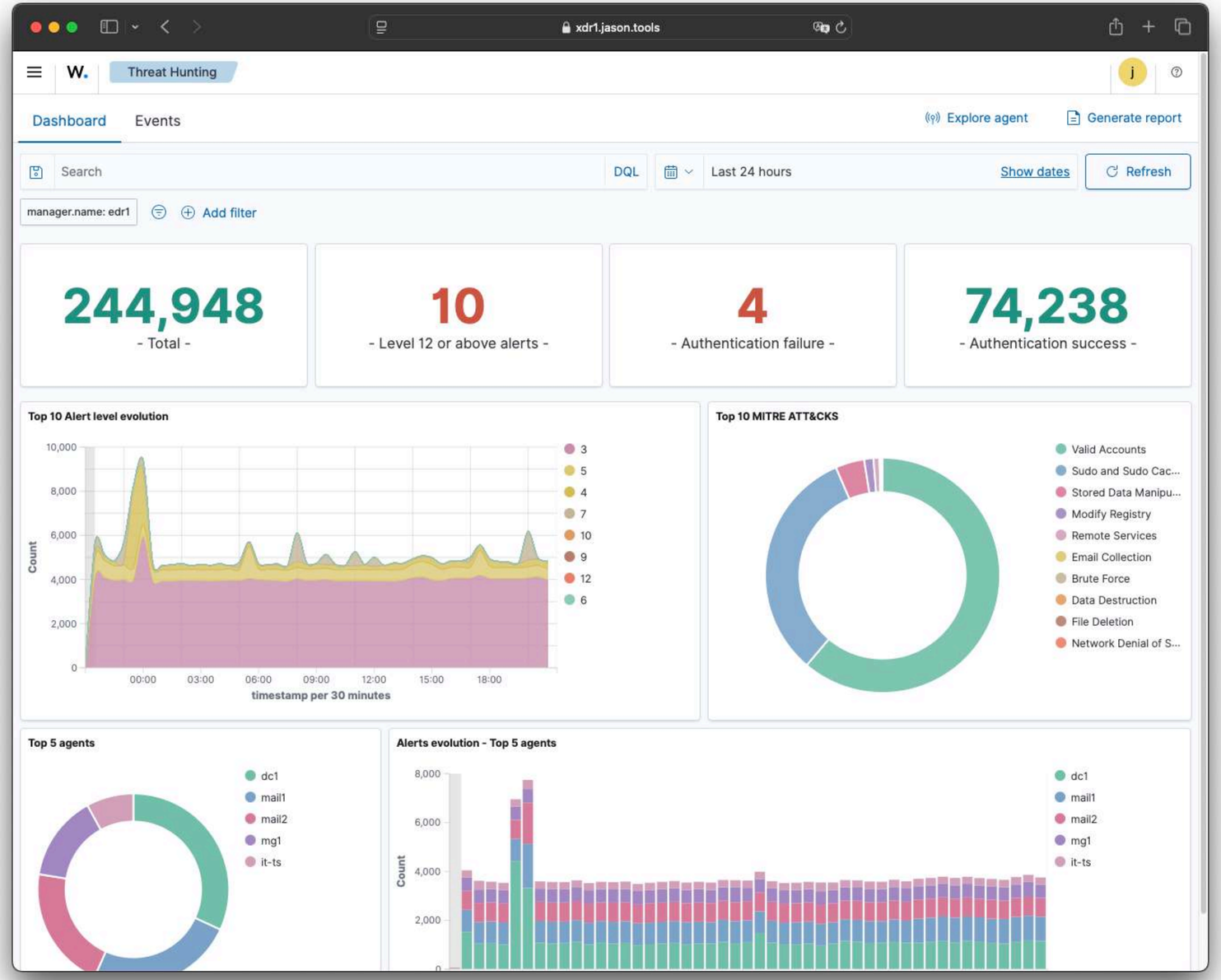


節省工具箱
JASON TOOLS

功能概觀

# 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

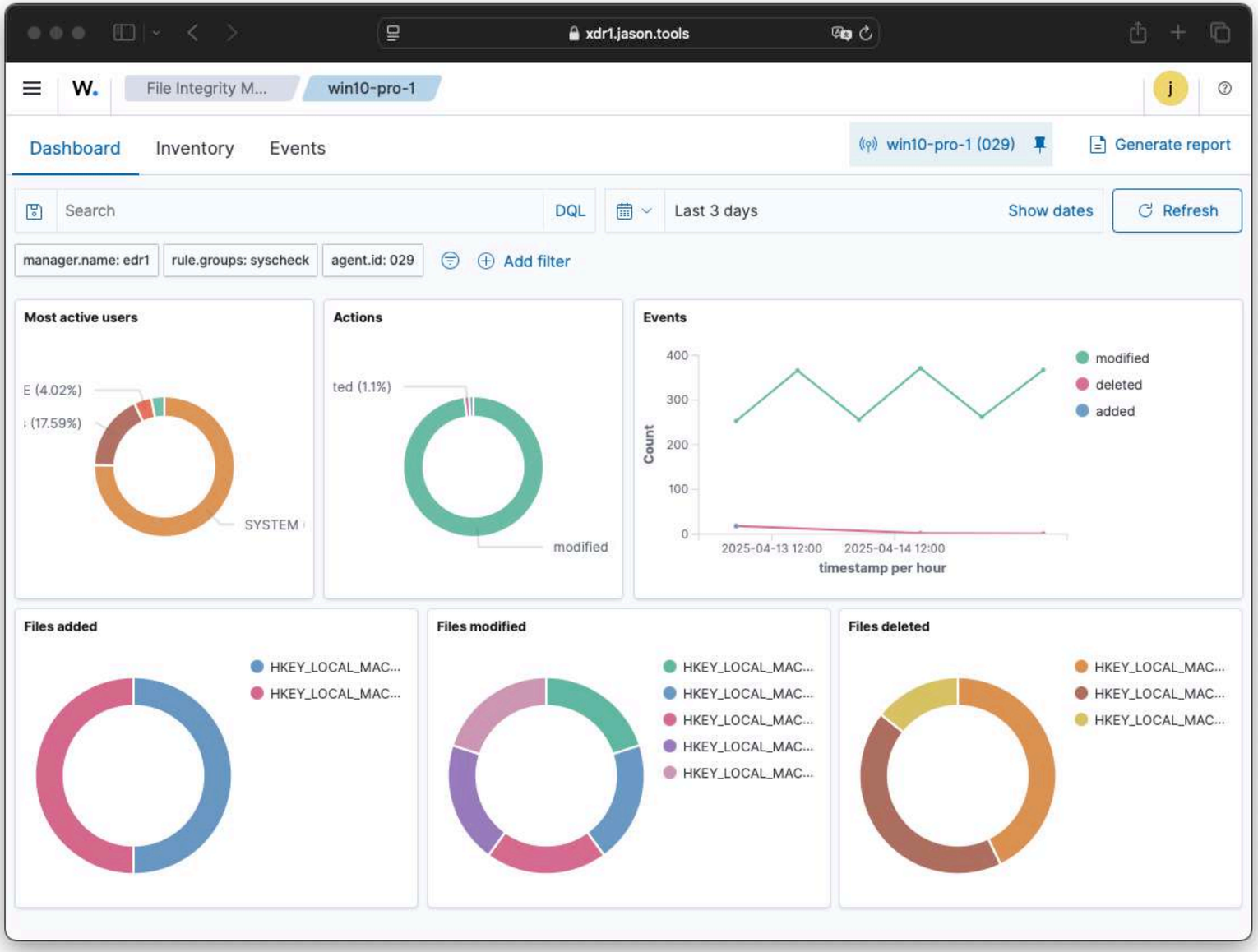


節省工具箱
JASON TOOLS

功能概觀

# 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

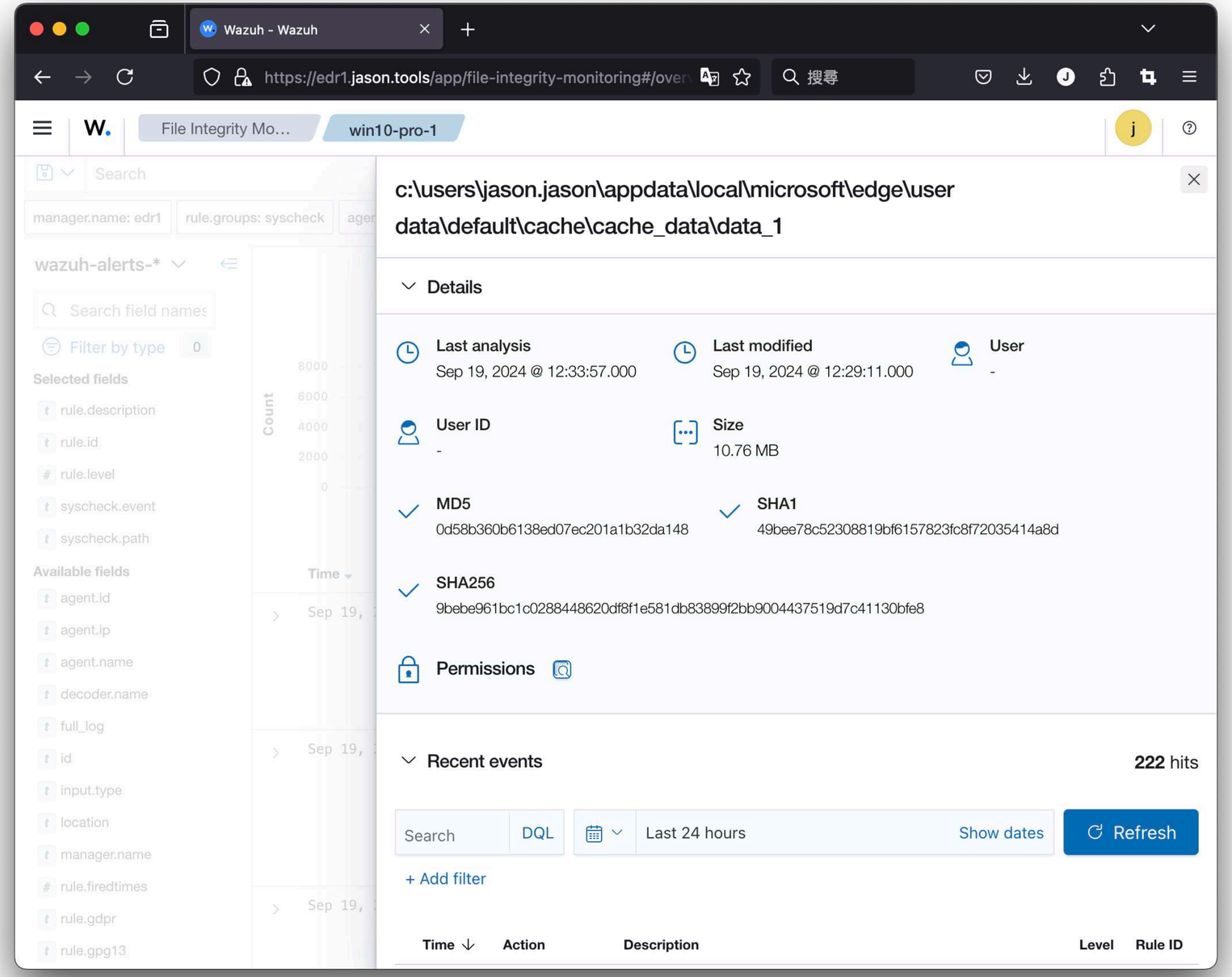


節省工具箱
JASON TOOLS

功能概觀

# 完整性

- 詳細事件
- 端點名稱
- 檢查路徑
- 發生動作
- 規則說明

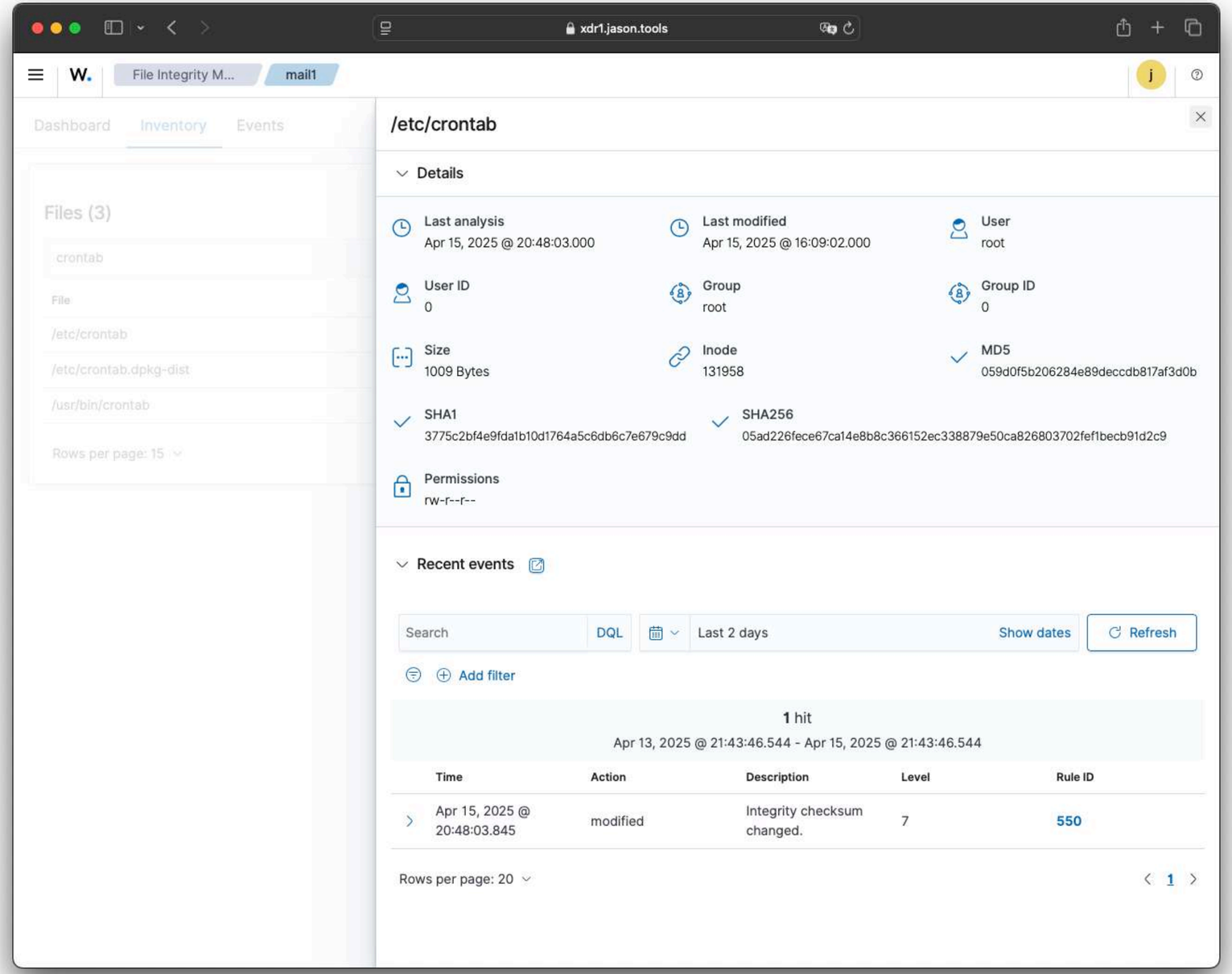


節省工具箱
JASON TOOLS

功能概觀

# 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

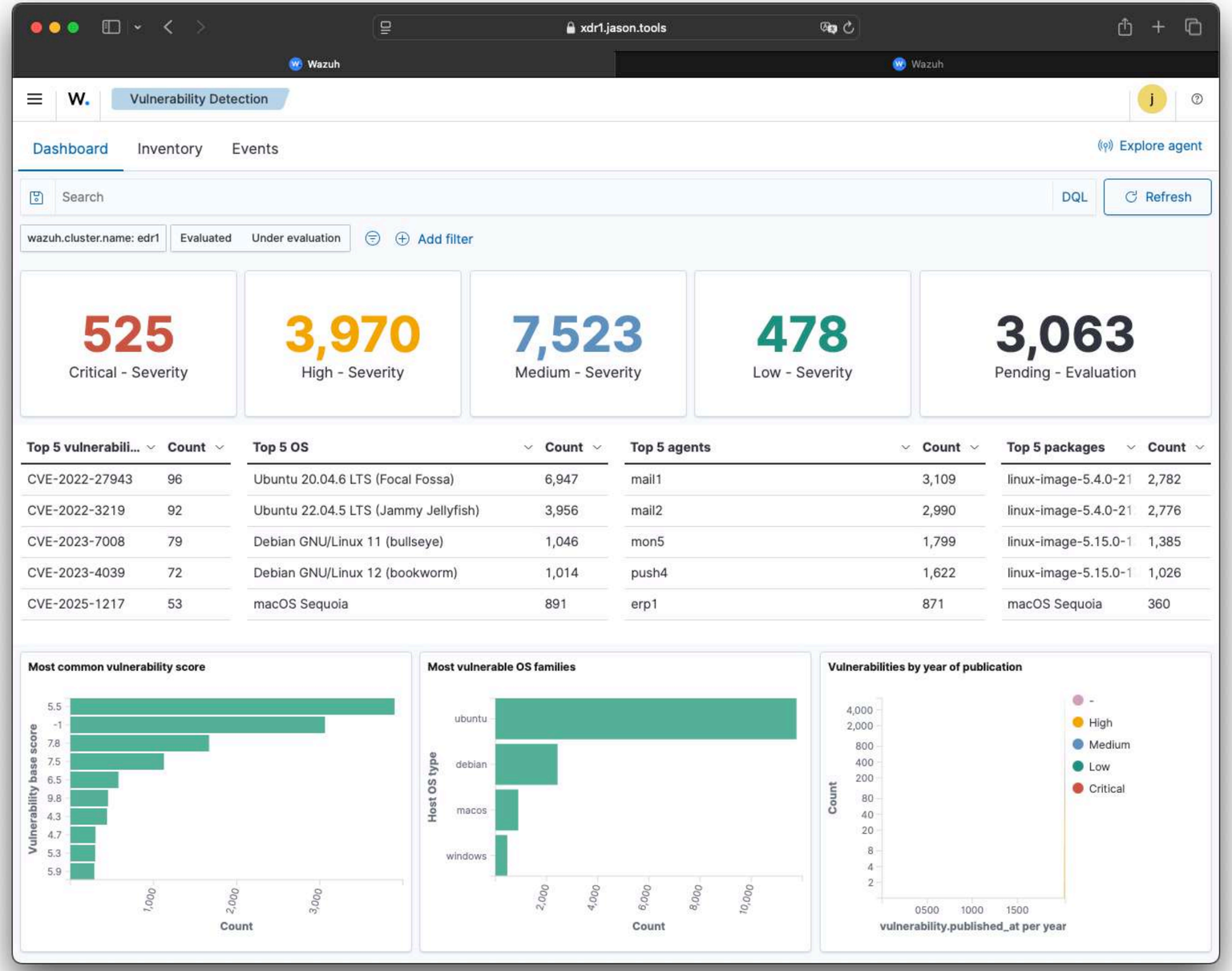


節省工具箱
JASON TOOLS

功能概觀

# 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



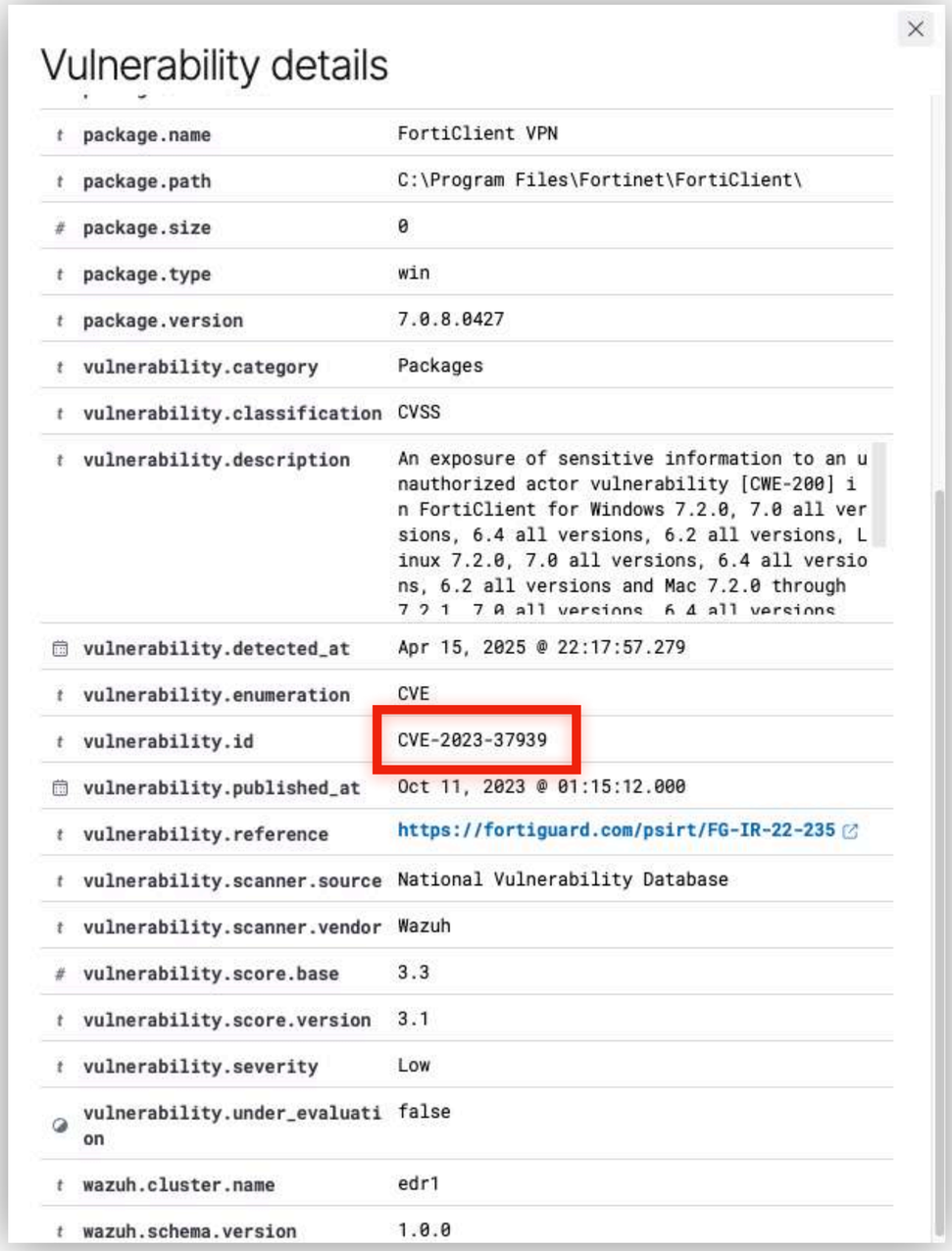
節省工具箱
JASON TOOLS

功能概觀

# 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!!!



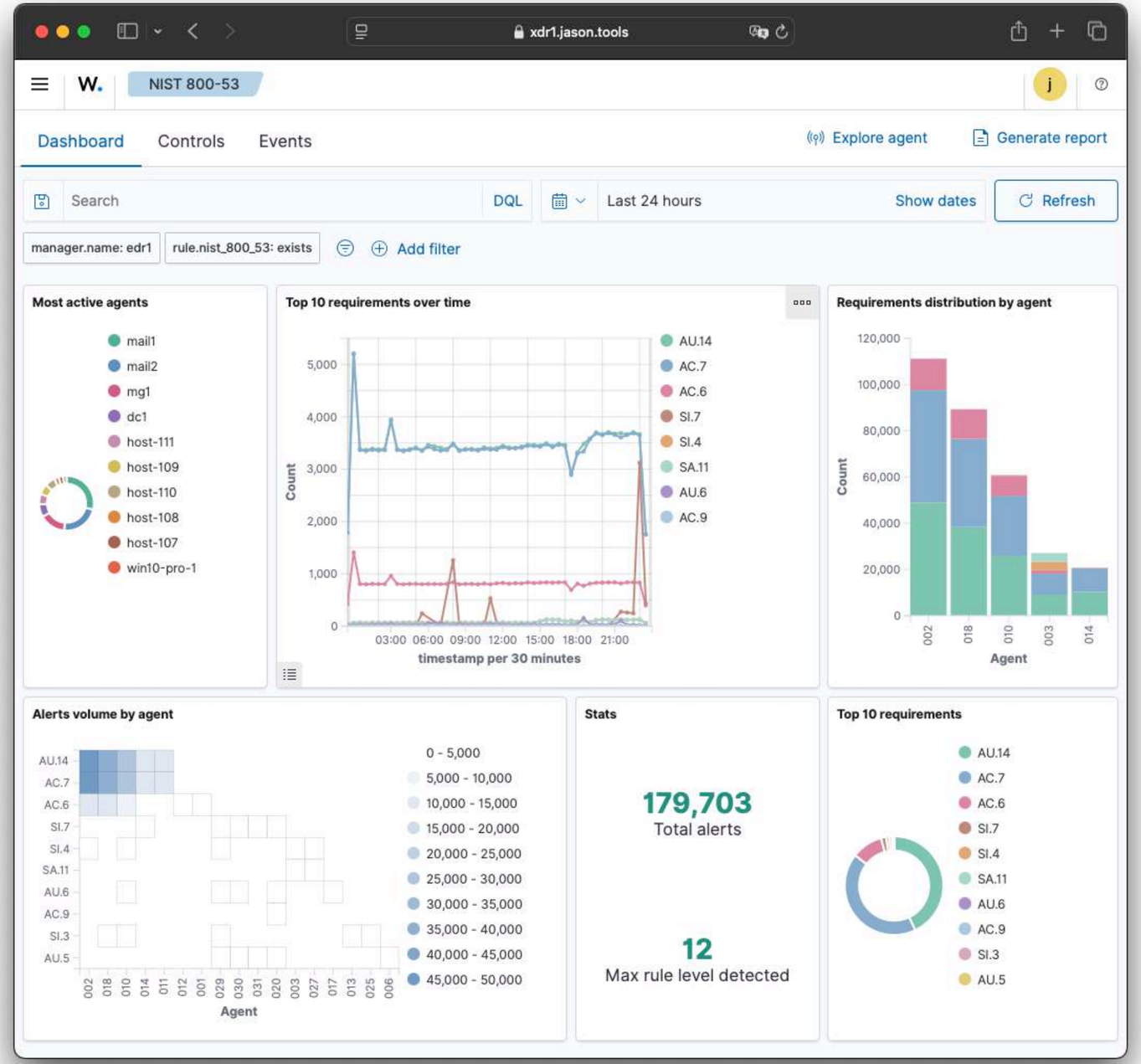
節省工具箱
JASON TOOLS

功能概觀

# 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

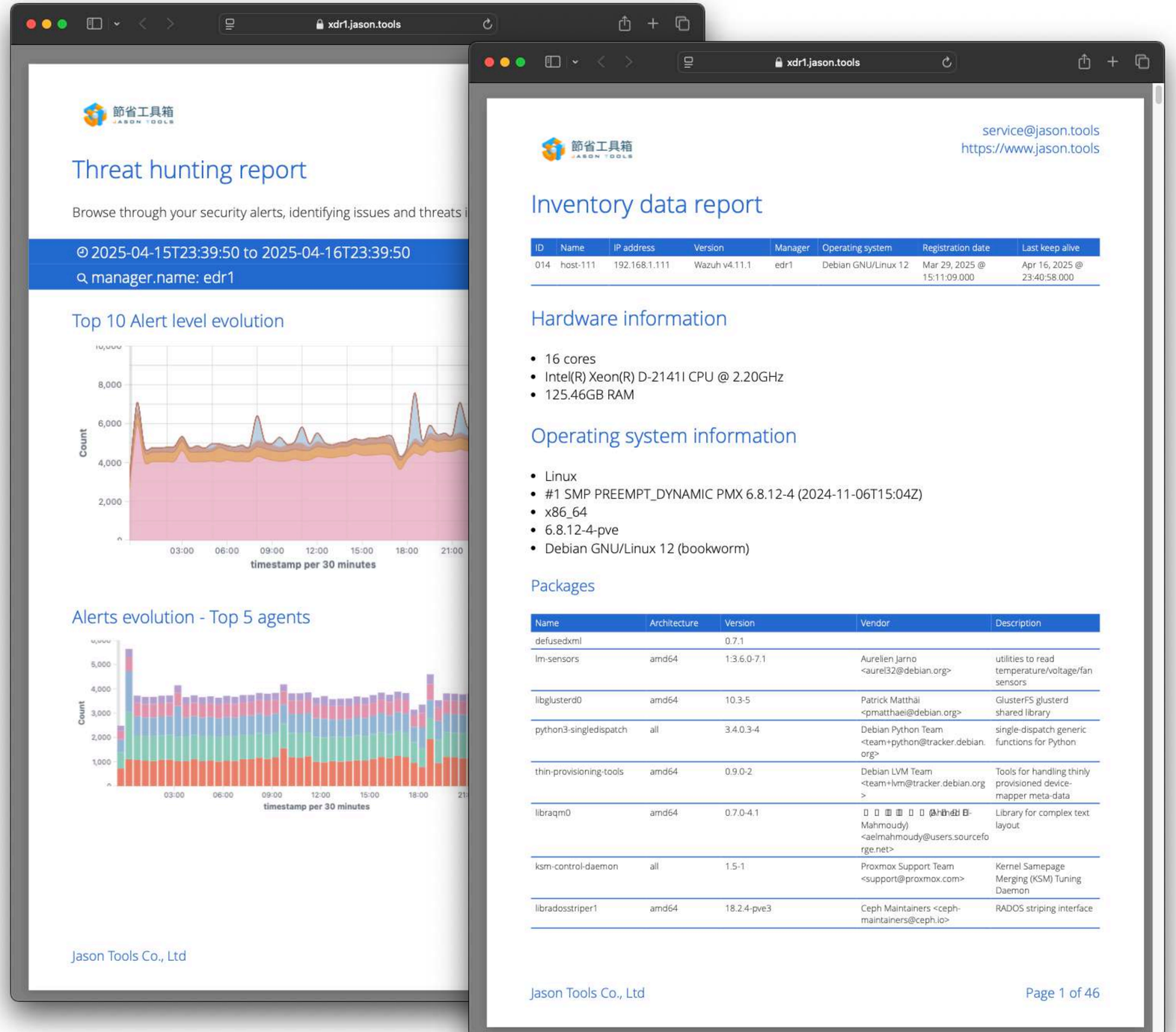


節省工具箱
JASON TOOLS

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

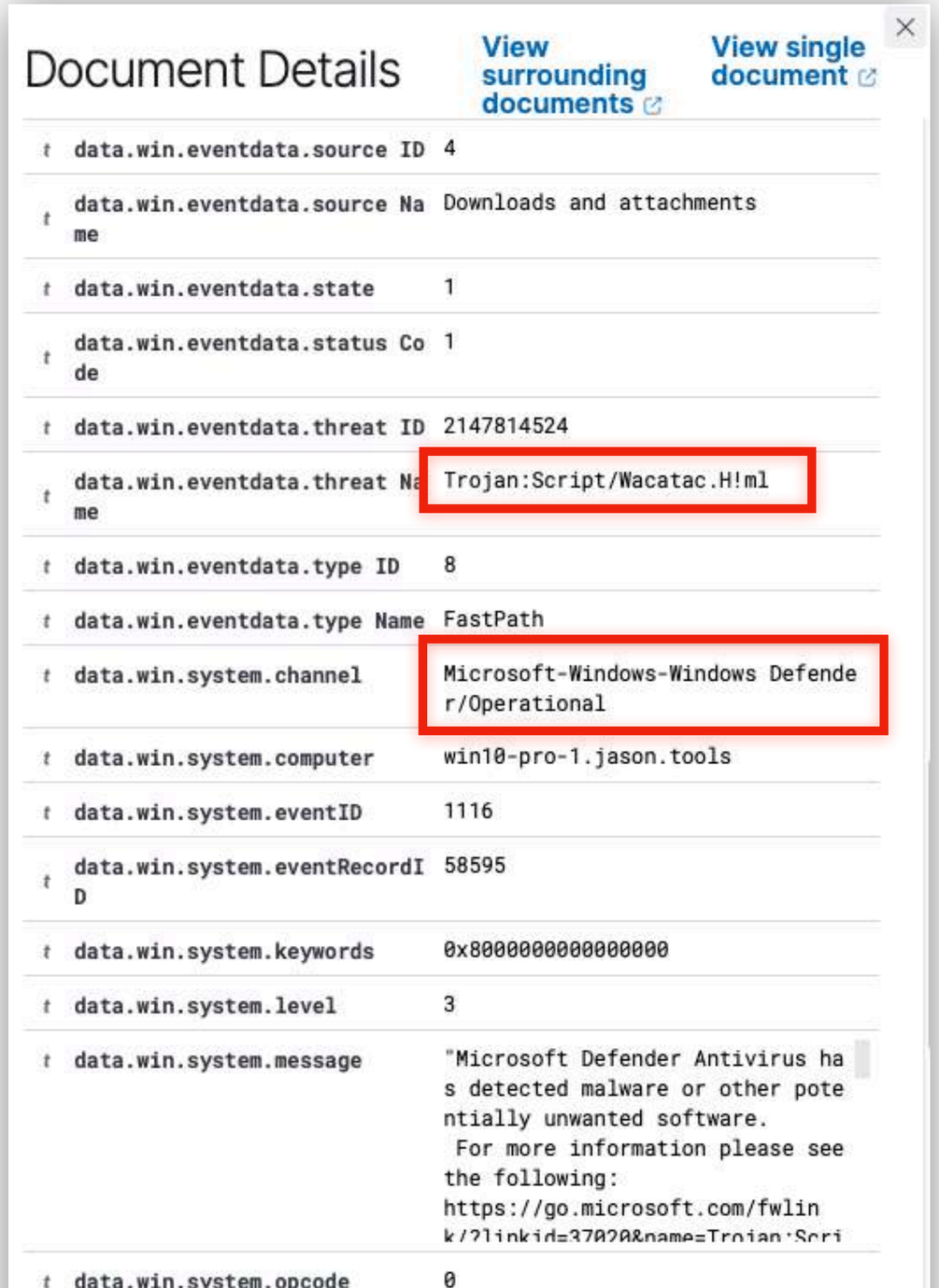
# 套件搭配

節省工具箱
JASON TOOLS

套件搭配

# 端點防護

- Defender
- ClamAV

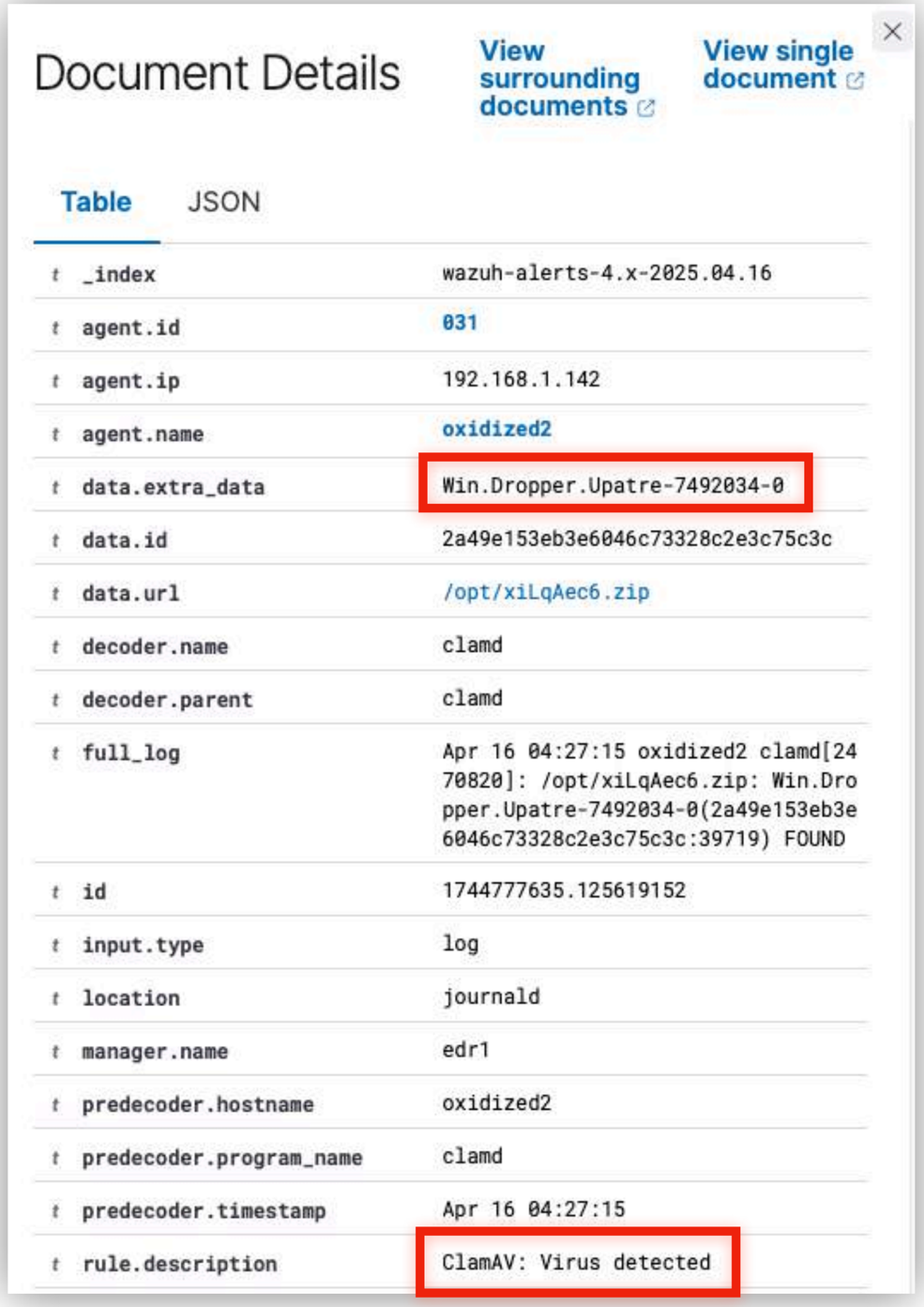


節省工具箱
JASON TOOLS

套件搭配

# 端點防護

- Defender
- ClamAV

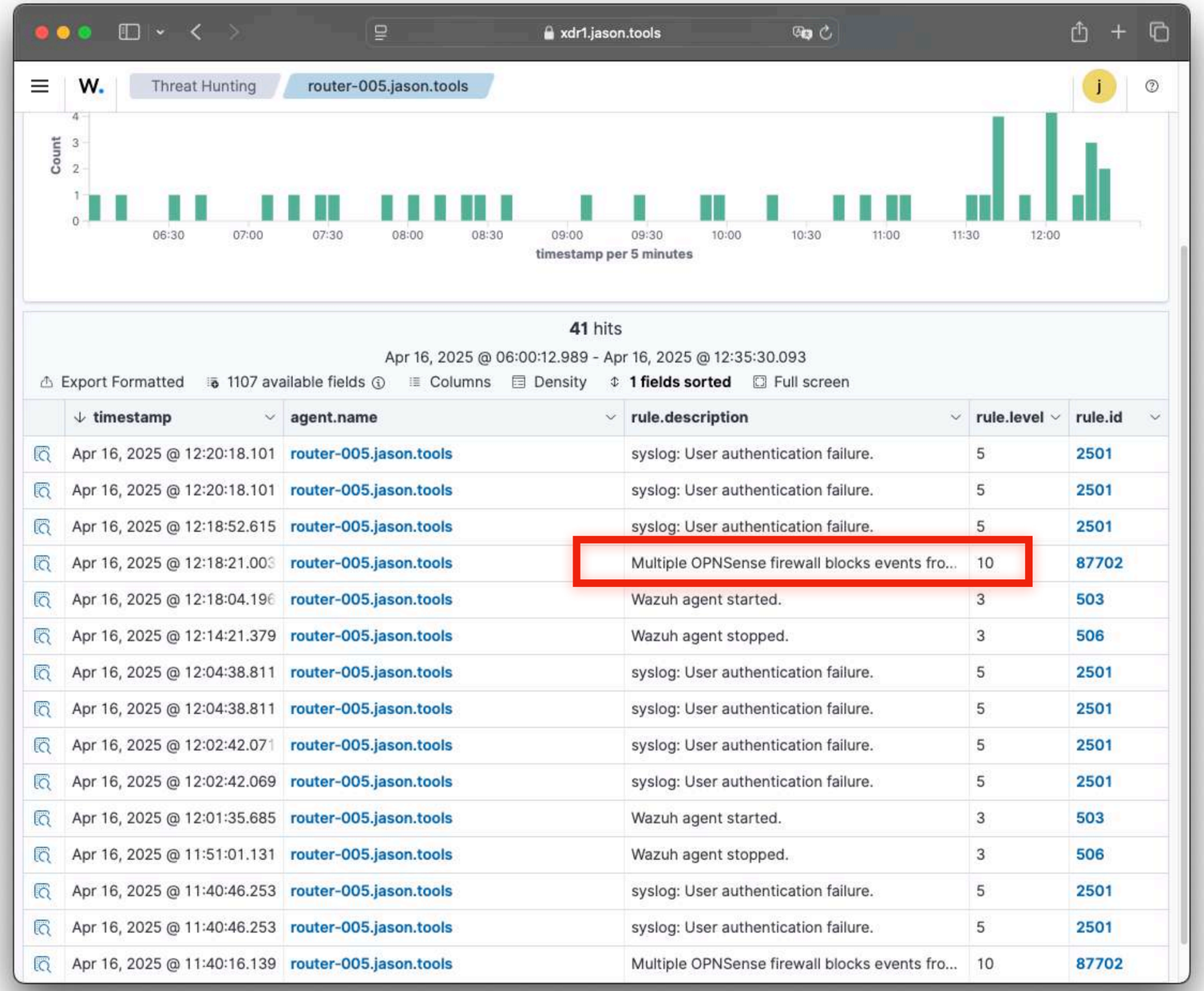


節省工具箱
JASON TOOLS

套件搭配

# 防火牆

- OPNsense



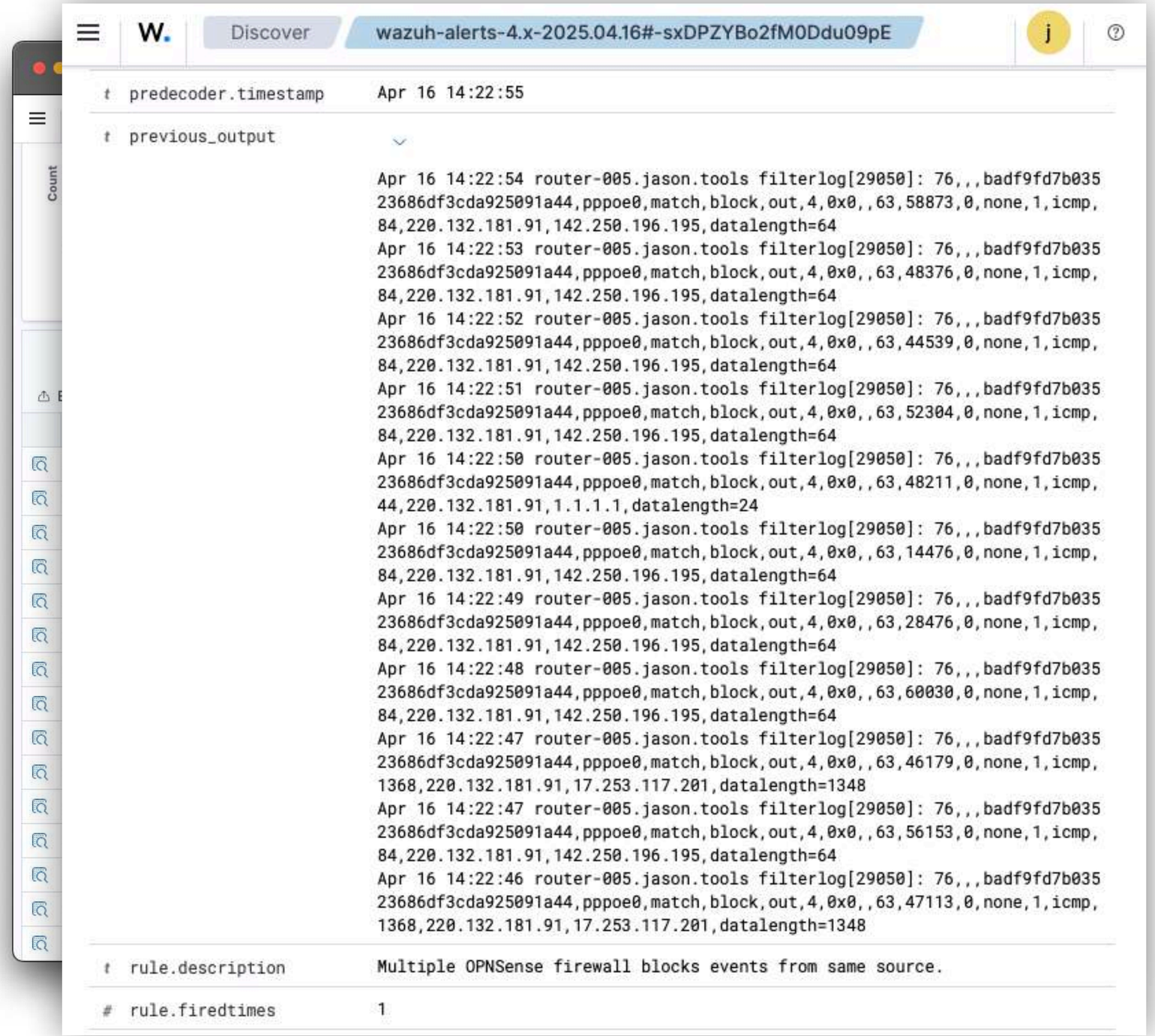

| timestamp | agent.name | rule.description | rule.level | rule.id |
|---|---|---|---|---|
| Apr 16, 2025 @ 12:20:18.101 | router-005.jason.tools | syslog: User authentication failure. | 5 | 2501 |
| Apr 16, 2025 @ 12:20:18.101 | router-005.jason.tools | syslog: User authentication failure. | 5 | 2501 |
| Apr 16, 2025 @ 12:18:52.615 | router-005.jason.tools | syslog: User authentication failure. | 5 | 2501 |
| Apr 16, 2025 @ 12:18:21.003 | router-005.jason.tools | Multiple OPNSense firewall blocks events fro... | 10 | 87702 |
| Apr 16, 2025 @ 12:18:04.196 | router-005.jason.tools | Wazuh agent started. | 3 | 503 |
| Apr 16, 2025 @ 12:14:21.379 | router-005.jason.tools | Wazuh agent stopped. | 3 | 506 |
| Apr 16, 2025 @ 12:04:38.811 | router-005.jason.tools | syslog: User authentication failure. | 5 | 2501 |
| Apr 16, 2025 @ 12:04:38.811 | router-005.jason.tools | syslog: User authentication failure. | 5 | 2501 |
| Apr 16, 2025 @ 12:02:42.071 | router-005.jason.tools | syslog: User authentication failure. | 5 | 2501 |
| Apr 16, 2025 @ 12:02:42.069 | router-005.jason.tools | syslog: User authentication failure. | 5 | 2501 |
| Apr 16, 2025 @ 12:01:35.685 | router-005.jason.tools | Wazuh agent started. | 3 | 503 |
| Apr 16, 2025 @ 11:51:01.131 | router-005.jason.tools | Wazuh agent stopped. | 3 | 506 |
| Apr 16, 2025 @ 11:40:46.253 | router-005.jason.tools | syslog: User authentication failure. | 5 | 2501 |
| Apr 16, 2025 @ 11:40:46.253 | router-005.jason.tools | syslog: User authentication failure. | 5 | 2501 |
| Apr 16, 2025 @ 11:40:16.139 | router-005.jason.tools | Multiple OPNSense firewall blocks events fro... | 10 | 87702 |

節省工具箱
JASON TOOLS

套件搭配

# 防火牆

- OPNsense

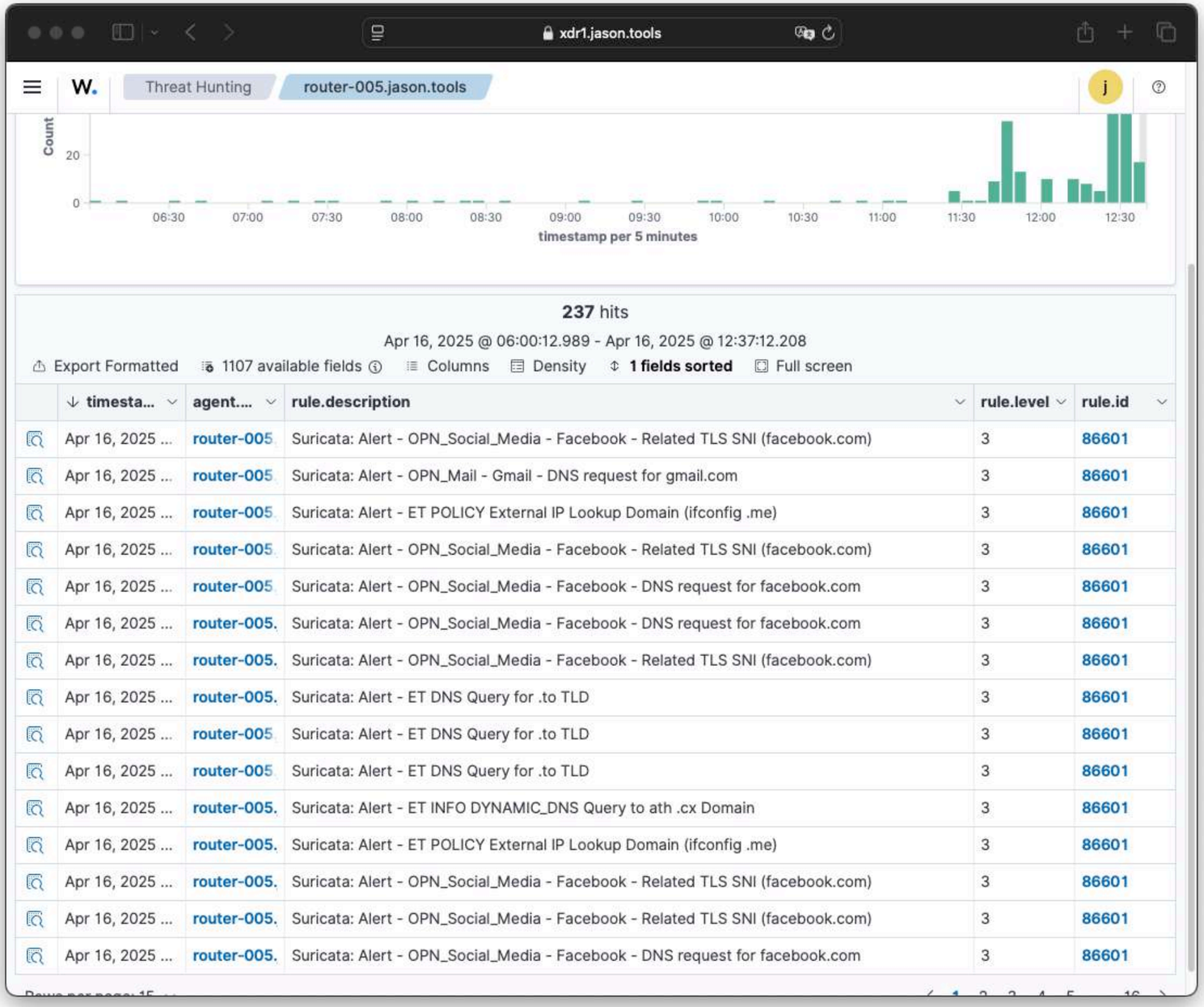


節省工具箱
JASON TOOLS

套件搭配

# IDS/IPS

- Suricata
  (OPNsense)



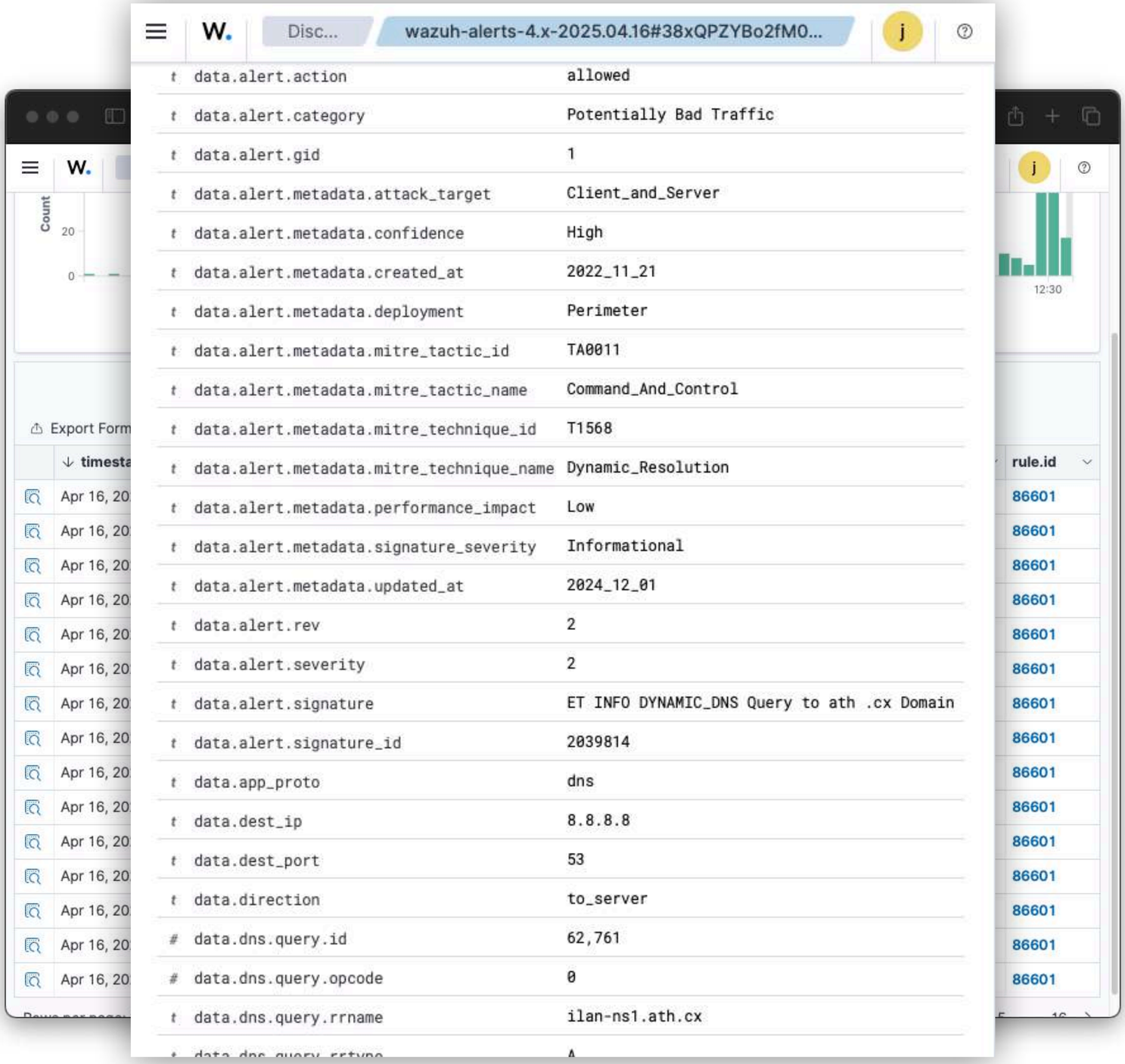

| | timesta... | agent.... | rule.description | rule.level | rule.id |
|---|---|---|---|---|---|
| | Apr 16, 2025 ... | router-005 | Suricata: Alert - OPN_Social_Media - Facebook - Related TLS SNI (facebook.com) | 3 | 86601 |
| | Apr 16, 2025 ... | router-005 | Suricata: Alert - OPN_Mail - Gmail - DNS request for gmail.com | 3 | 86601 |
| | Apr 16, 2025 ... | router-005 | Suricata: Alert - ET POLICY External IP Lookup Domain (ifconfig .me) | 3 | 86601 |
| | Apr 16, 2025 ... | router-005 | Suricata: Alert - OPN_Social_Media - Facebook - Related TLS SNI (facebook.com) | 3 | 86601 |
| | Apr 16, 2025 ... | router-005 | Suricata: Alert - OPN_Social_Media - Facebook - DNS request for facebook.com | 3 | 86601 |
| | Apr 16, 2025 ... | router-005. | Suricata: Alert - OPN_Social_Media - Facebook - DNS request for facebook.com | 3 | 86601 |
| | Apr 16, 2025 ... | router-005. | Suricata: Alert - OPN_Social_Media - Facebook - Related TLS SNI (facebook.com) | 3 | 86601 |
| | Apr 16, 2025 ... | router-005. | Suricata: Alert - ET DNS Query for .to TLD | 3 | 86601 |
| | Apr 16, 2025 ... | router-005 | Suricata: Alert - ET DNS Query for .to TLD | 3 | 86601 |
| | Apr 16, 2025 ... | router-005 | Suricata: Alert - ET DNS Query for .to TLD | 3 | 86601 |
| | Apr 16, 2025 ... | router-005. | Suricata: Alert - ET INFO DYNAMIC_DNS Query to ath .cx Domain | 3 | 86601 |
| | Apr 16, 2025 ... | router-005. | Suricata: Alert - ET POLICY External IP Lookup Domain (ifconfig .me) | 3 | 86601 |
| | Apr 16, 2025 ... | router-005. | Suricata: Alert - OPN_Social_Media - Facebook - Related TLS SNI (facebook.com) | 3 | 86601 |
| | Apr 16, 2025 ... | router-005. | Suricata: Alert - OPN_Social_Media - Facebook - Related TLS SNI (facebook.com) | 3 | 86601 |
| | Apr 16, 2025 ... | router-005. | Suricata: Alert - OPN_Social_Media - Facebook - DNS request for facebook.com | 3 | 86601 |

節省工具箱
JASON TOOLS

套件搭配

# IDS/IPS

- Suricata
  (OPNsense)

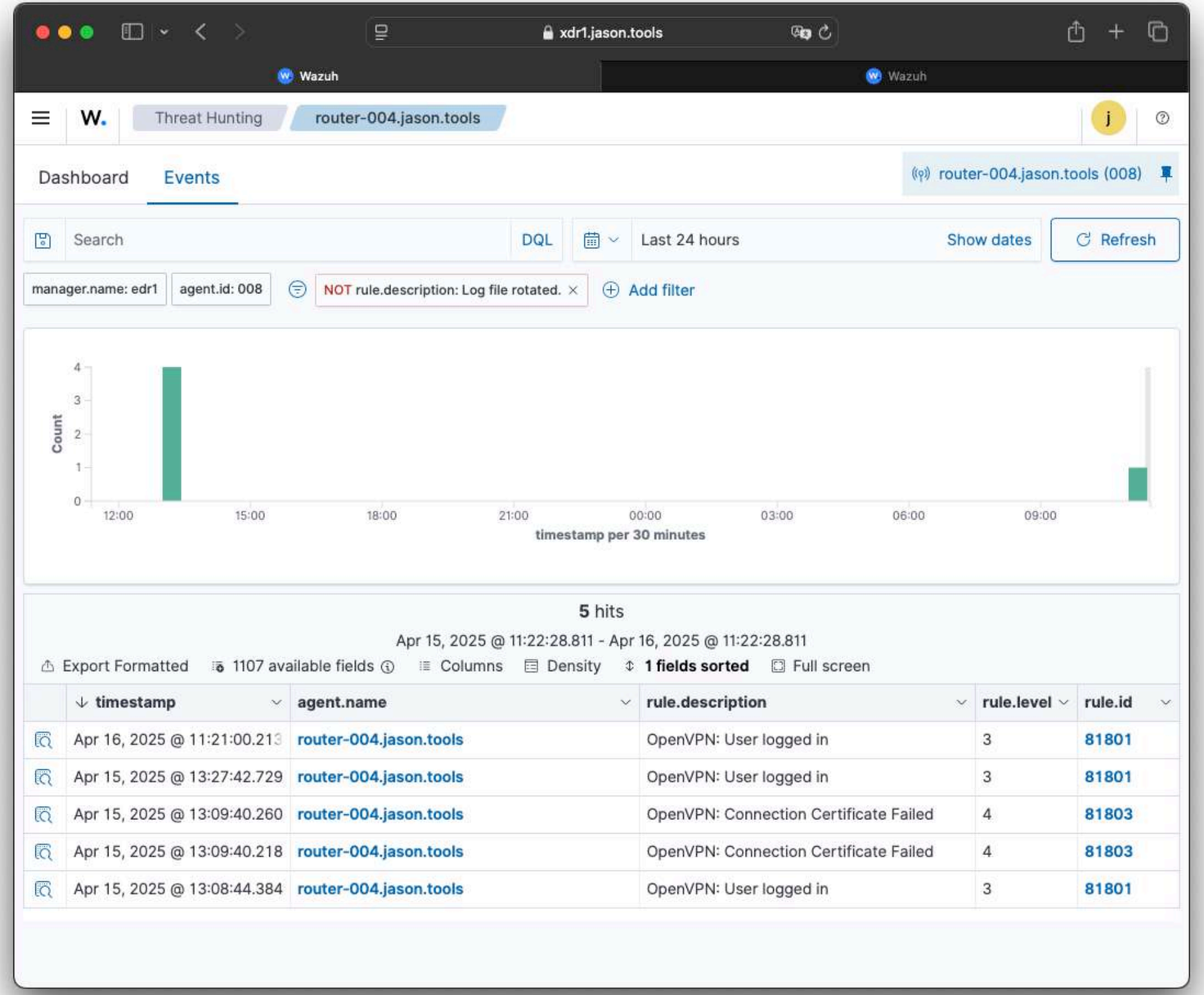


節省工具箱
JASON TOOLS

套件搭配

# VPN 連線

- OpenVPN
  (OPNsense)



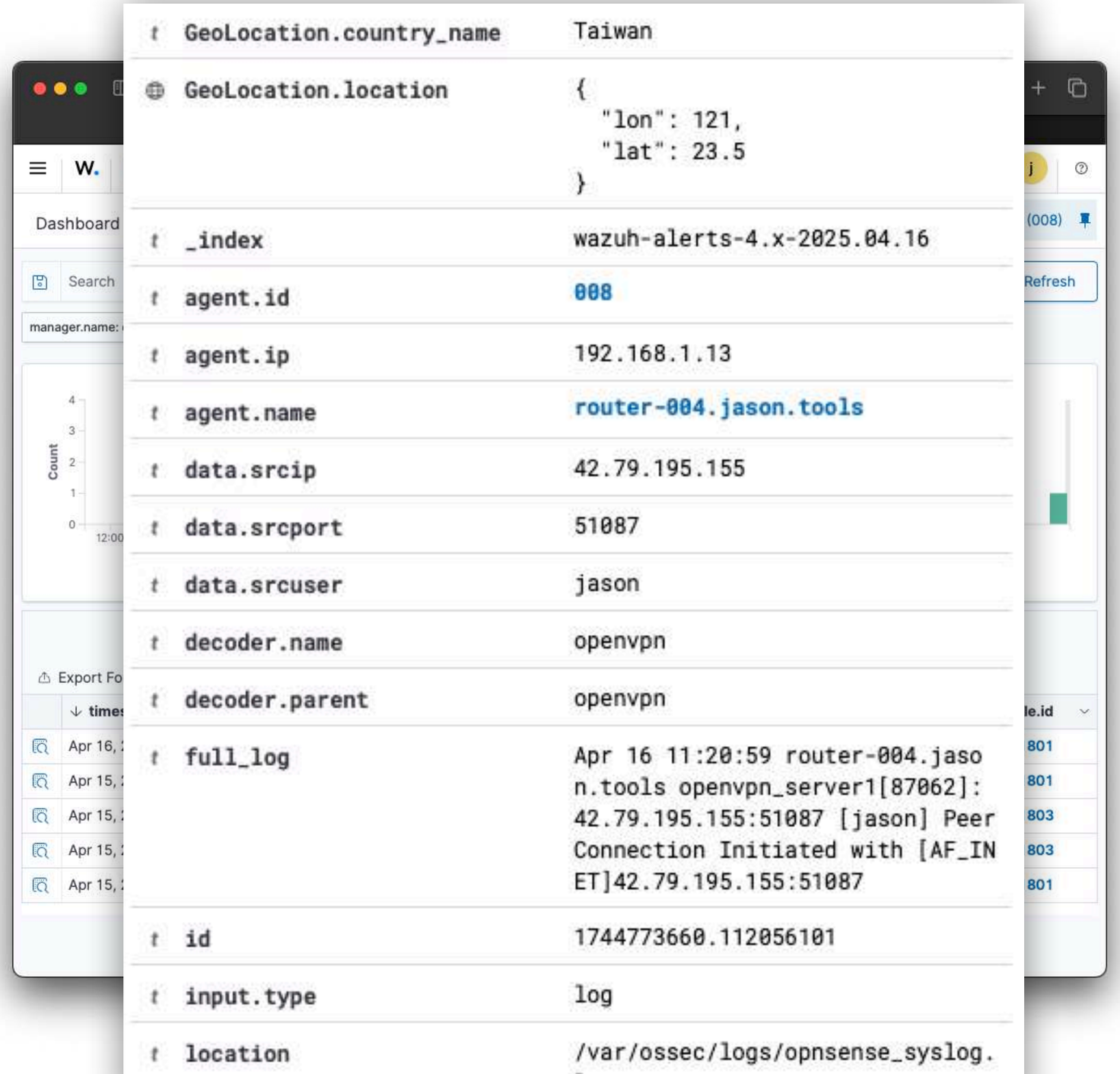

| timestamp | agent.name | rule.description | rule.level | rule.id |
|---|---|---|---|---|
| Apr 16, 2025 @ 11:21:00.213 | router-004.jason.tools | OpenVPN: User logged in | 3 | 81801 |
| Apr 15, 2025 @ 13:27:42.729 | router-004.jason.tools | OpenVPN: User logged in | 3 | 81801 |
| Apr 15, 2025 @ 13:09:40.260 | router-004.jason.tools | OpenVPN: Connection Certificate Failed | 4 | 81803 |
| Apr 15, 2025 @ 13:09:40.218 | router-004.jason.tools | OpenVPN: Connection Certificate Failed | 4 | 81803 |
| Apr 15, 2025 @ 13:08:44.384 | router-004.jason.tools | OpenVPN: User logged in | 3 | 81801 |

節省工具箱
JASON TOOLS

套件搭配

# VPN 連線

- OpenVPN
  (OPNsense)

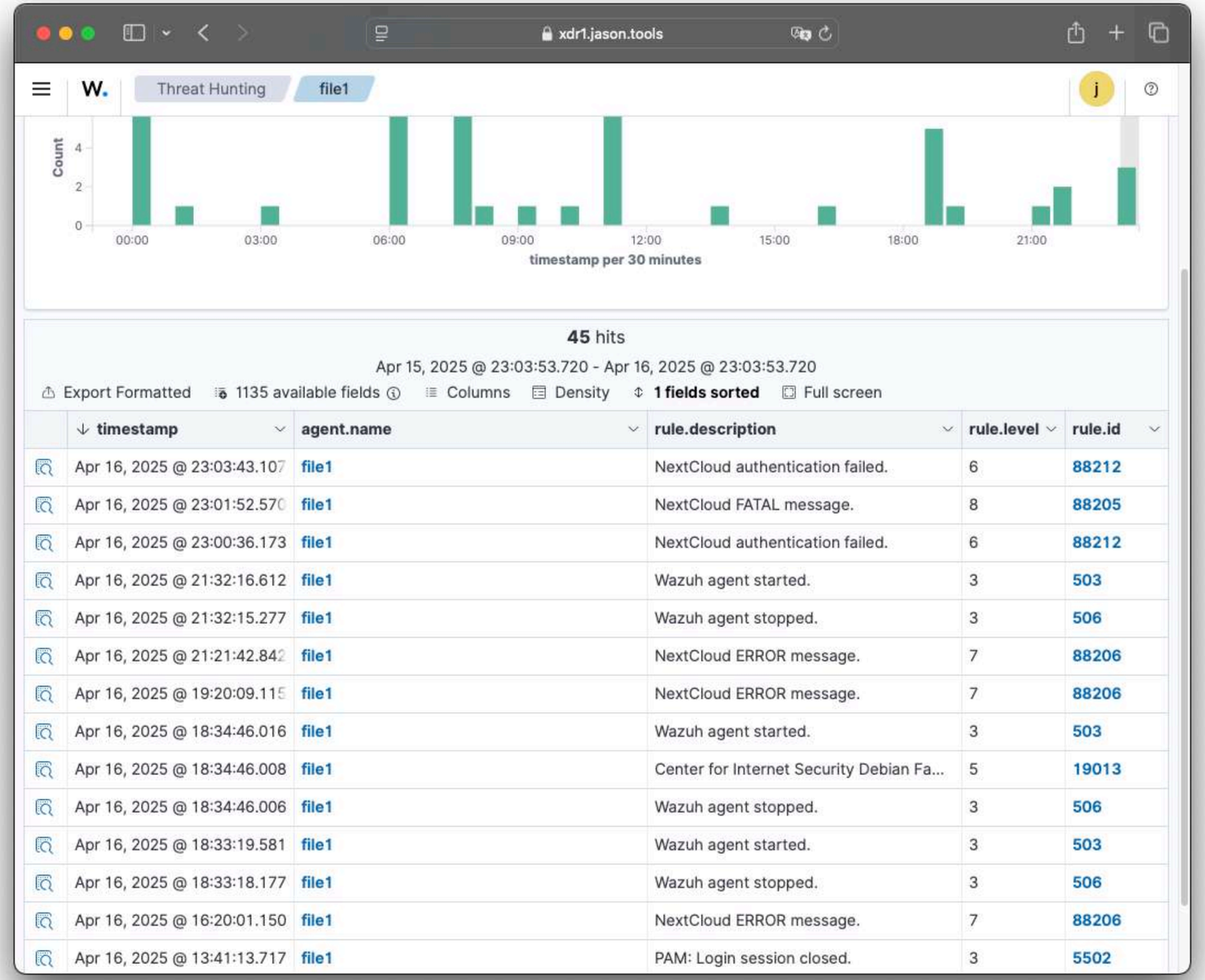


節省工具箱
JASON TOOLS

套件搭配

# 網路硬碟

- Nextcloud



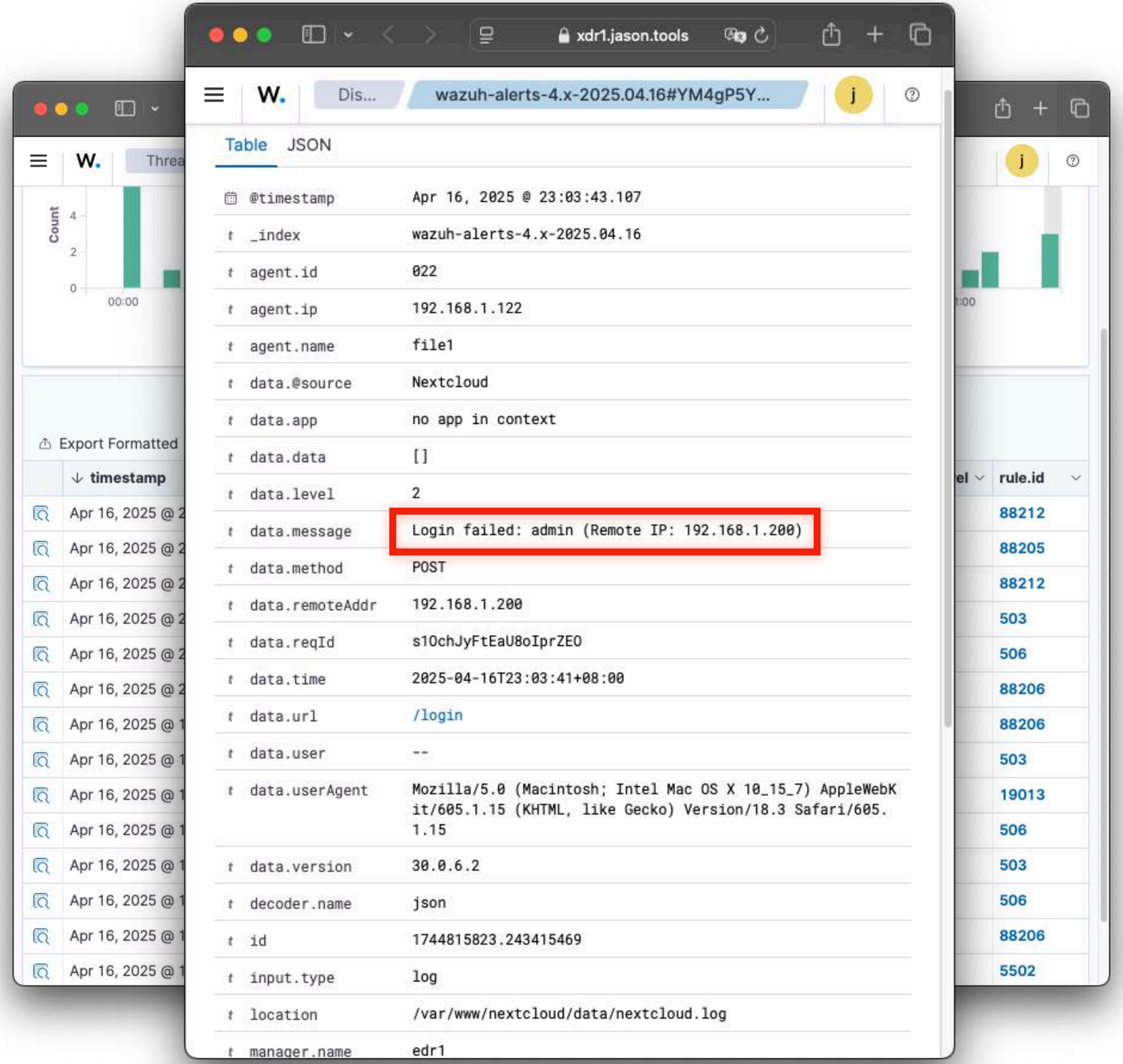

| timestamp | agent.name | rule.description | rule.level | rule.id |
|---|---|---|---|---|
| Apr 16, 2025 @ 23:03:43.107 | file1 | NextCloud authentication failed. | 6 | 88212 |
| Apr 16, 2025 @ 23:01:52.570 | file1 | NextCloud FATAL message. | 8 | 88205 |
| Apr 16, 2025 @ 23:00:36.173 | file1 | NextCloud authentication failed. | 6 | 88212 |
| Apr 16, 2025 @ 21:32:16.612 | file1 | Wazuh agent started. | 3 | 503 |
| Apr 16, 2025 @ 21:32:15.277 | file1 | Wazuh agent stopped. | 3 | 506 |
| Apr 16, 2025 @ 21:21:42.842 | file1 | NextCloud ERROR message. | 7 | 88206 |
| Apr 16, 2025 @ 19:20:09.115 | file1 | NextCloud ERROR message. | 7 | 88206 |
| Apr 16, 2025 @ 18:34:46.016 | file1 | Wazuh agent started. | 3 | 503 |
| Apr 16, 2025 @ 18:34:46.008 | file1 | Center for Internet Security Debian Fa... | 5 | 19013 |
| Apr 16, 2025 @ 18:34:46.006 | file1 | Wazuh agent stopped. | 3 | 506 |
| Apr 16, 2025 @ 18:33:19.581 | file1 | Wazuh agent started. | 3 | 503 |
| Apr 16, 2025 @ 18:33:18.177 | file1 | Wazuh agent stopped. | 3 | 506 |
| Apr 16, 2025 @ 16:20:01.150 | file1 | NextCloud ERROR message. | 7 | 88206 |
| Apr 16, 2025 @ 13:41:13.717 | file1 | PAM: Login session closed. | 3 | 5502 |

節省工具箱
JASON TOOLS

套件搭配

# 網路硬碟

- Nextcloud

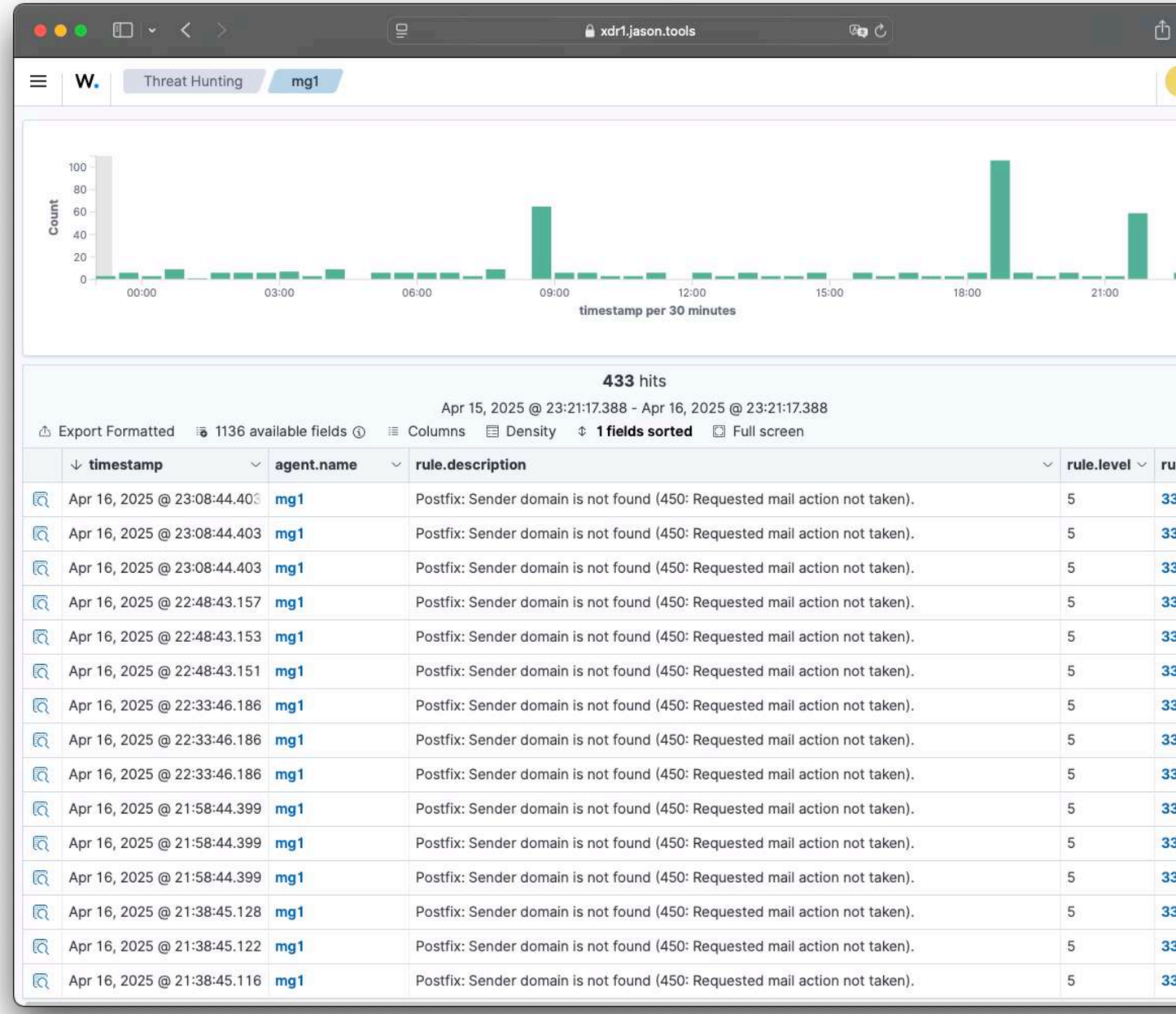


節省工具箱
JASON TOOLS

套件搭配

# 郵件主機

- Proxmox MG
- Zimbra
- Postfix

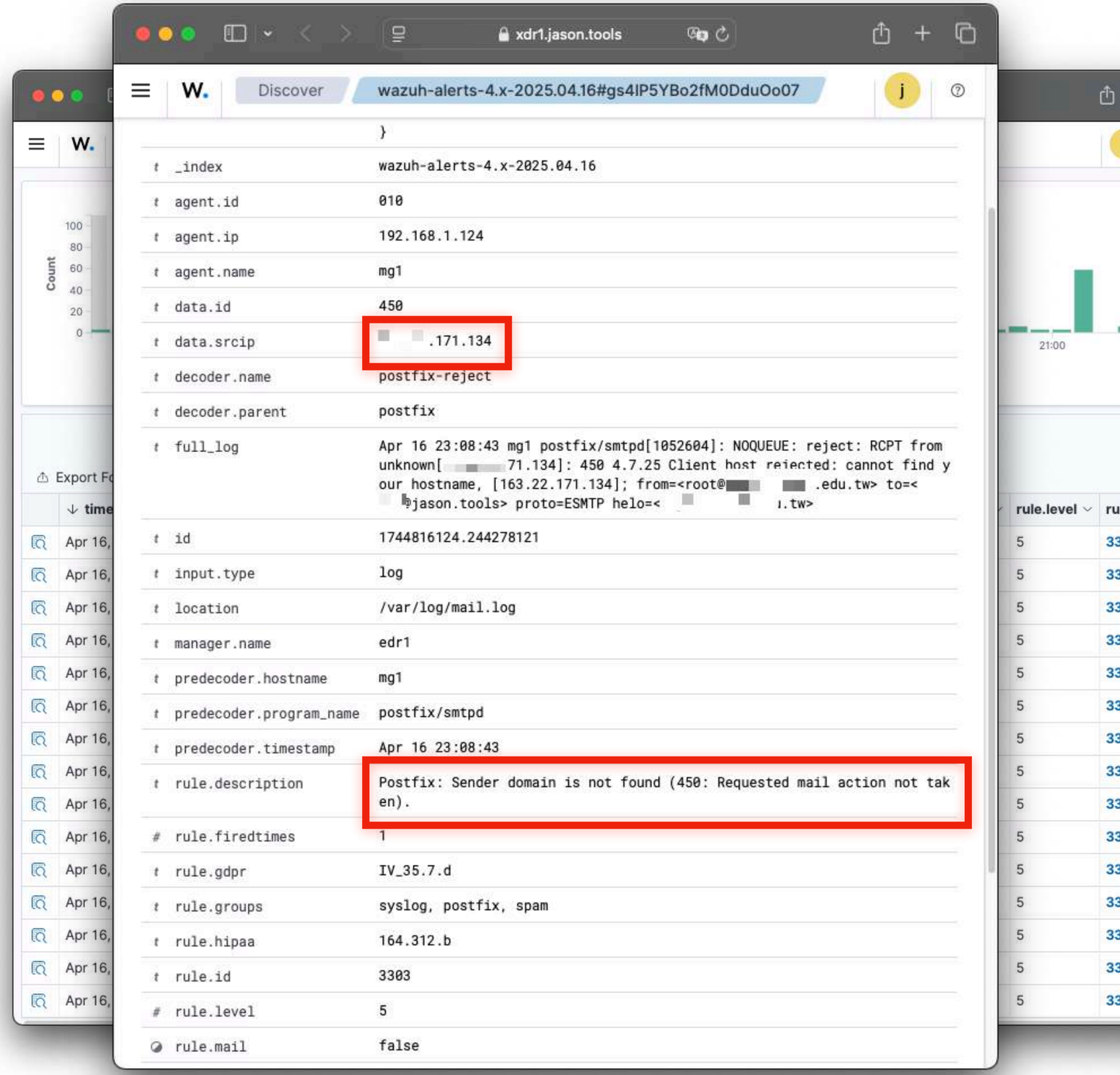


節省工具箱
JASON TOOLS

套件搭配

# 郵件主機

- Proxmox MG
- Zimbra
- Postfix

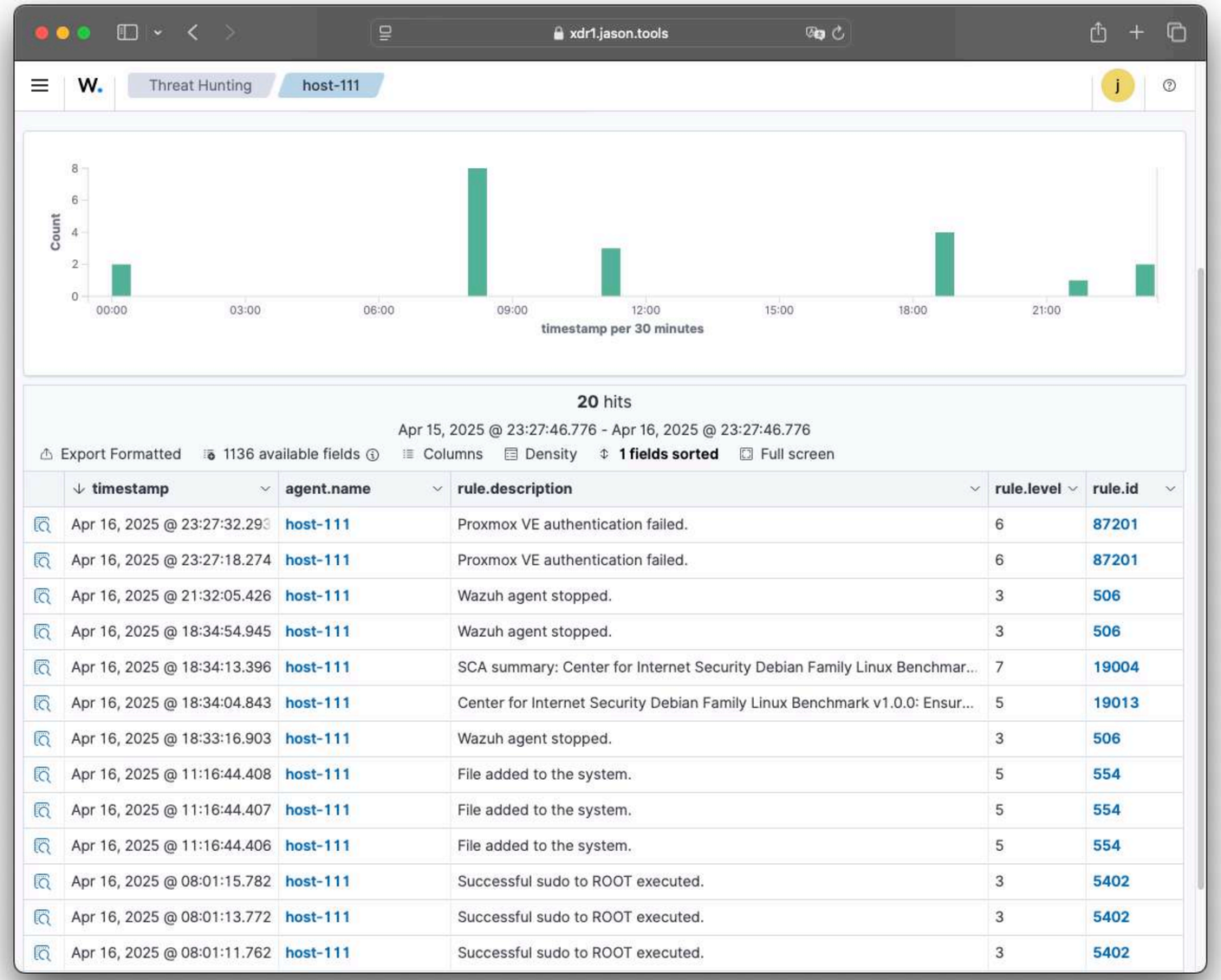


節省工具箱
JASON TOOLS

套件搭配

# 虛擬化

- Proxmox VE



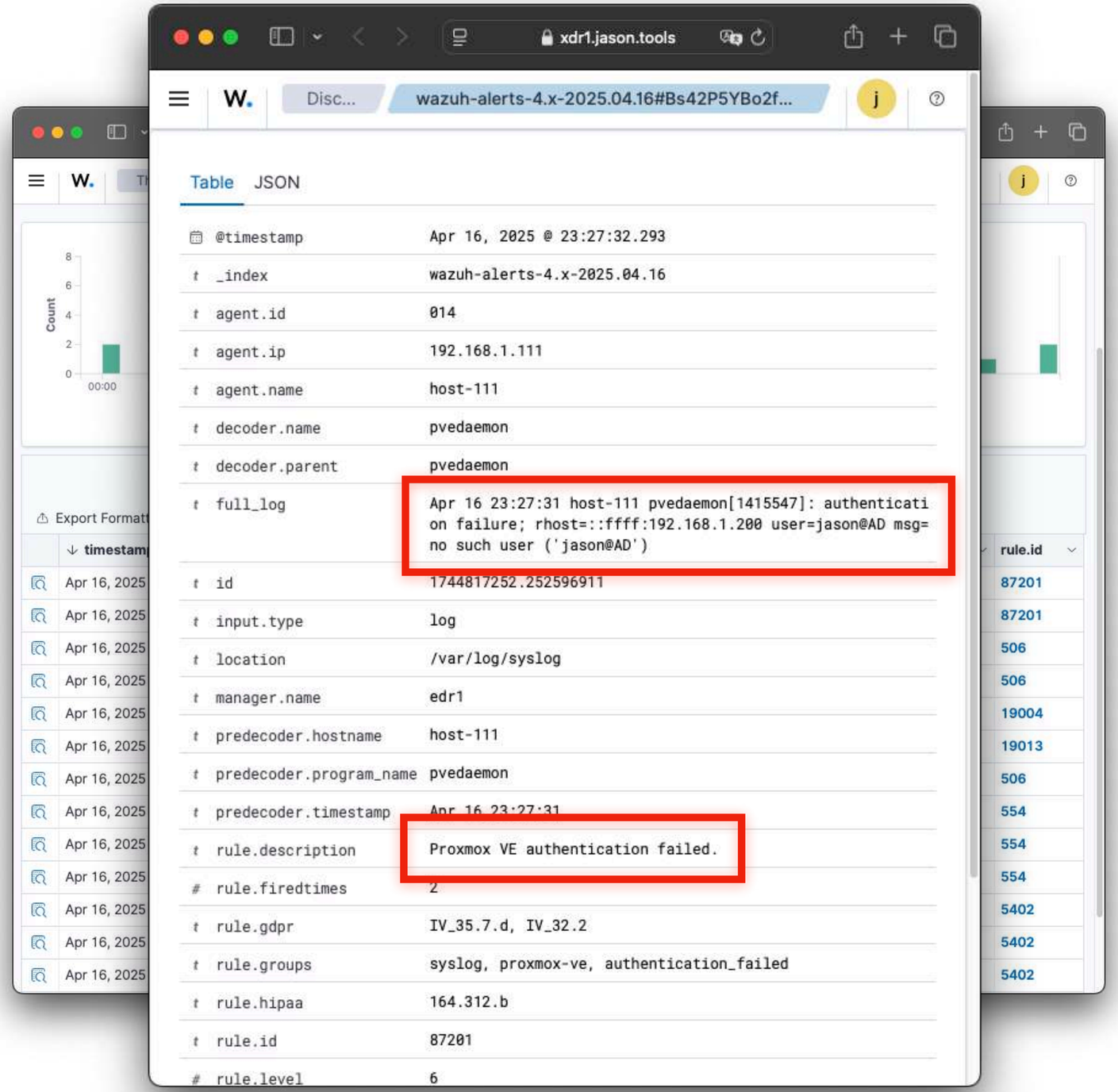

| timestamp | agent.name | rule.description | rule.level | rule.id |
|---|---|---|---|---|
| Apr 16, 2025 @ 23:27:32.293 | host-111 | Proxmox VE authentication failed. | 6 | 87201 |
| Apr 16, 2025 @ 23:27:18.274 | host-111 | Proxmox VE authentication failed. | 6 | 87201 |
| Apr 16, 2025 @ 21:32:05.426 | host-111 | Wazuh agent stopped. | 3 | 506 |
| Apr 16, 2025 @ 18:34:54.945 | host-111 | Wazuh agent stopped. | 3 | 506 |
| Apr 16, 2025 @ 18:34:13.396 | host-111 | SCA summary: Center for Internet Security Debian Family Linux Benchmar... | 7 | 19004 |
| Apr 16, 2025 @ 18:34:04.843 | host-111 | Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensur... | 5 | 19013 |
| Apr 16, 2025 @ 18:33:16.903 | host-111 | Wazuh agent stopped. | 3 | 506 |
| Apr 16, 2025 @ 11:16:44.408 | host-111 | File added to the system. | 5 | 554 |
| Apr 16, 2025 @ 11:16:44.407 | host-111 | File added to the system. | 5 | 554 |
| Apr 16, 2025 @ 11:16:44.406 | host-111 | File added to the system. | 5 | 554 |
| Apr 16, 2025 @ 08:01:15.782 | host-111 | Successful sudo to ROOT executed. | 3 | 5402 |
| Apr 16, 2025 @ 08:01:13.772 | host-111 | Successful sudo to ROOT executed. | 3 | 5402 |
| Apr 16, 2025 @ 08:01:11.762 | host-111 | Successful sudo to ROOT executed. | 3 | 5402 |

節省工具箱
JASON TOOLS

套件搭配

# 虛擬化

- Proxmox VE

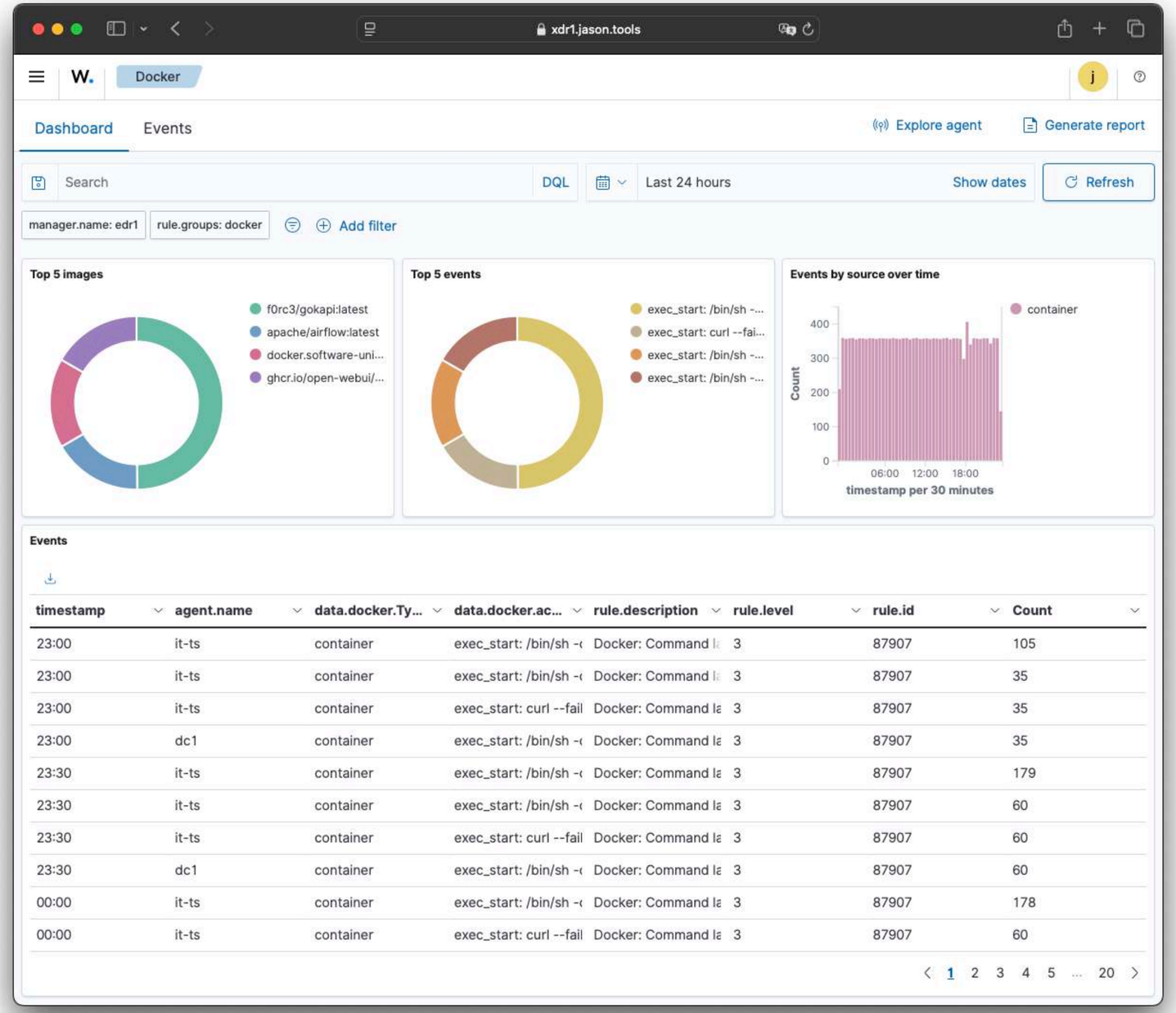


節省工具箱
JASON TOOLS

套件搭配

# 容器

- Docker

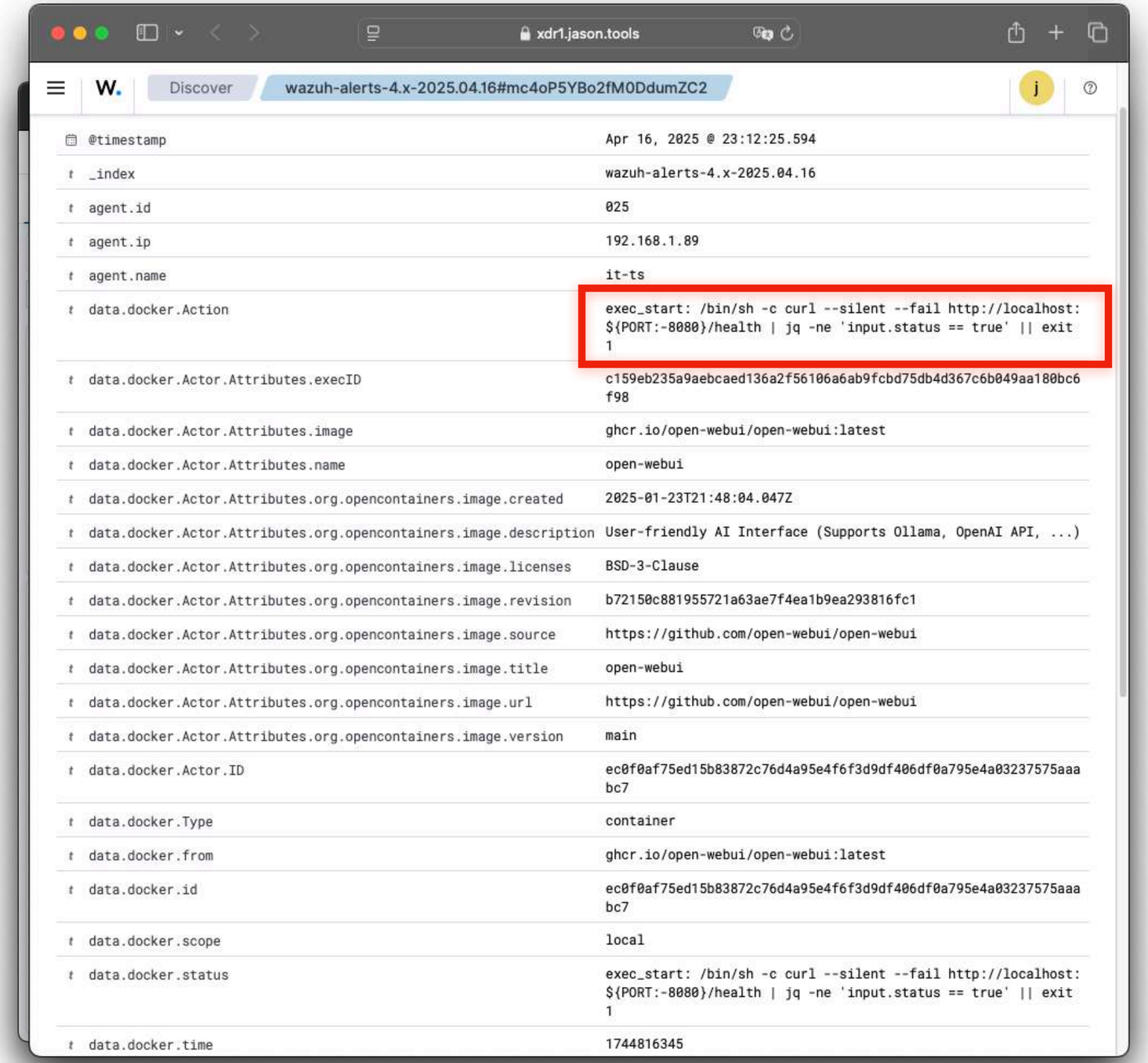


節省工具箱
JASON TOOLS

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 |

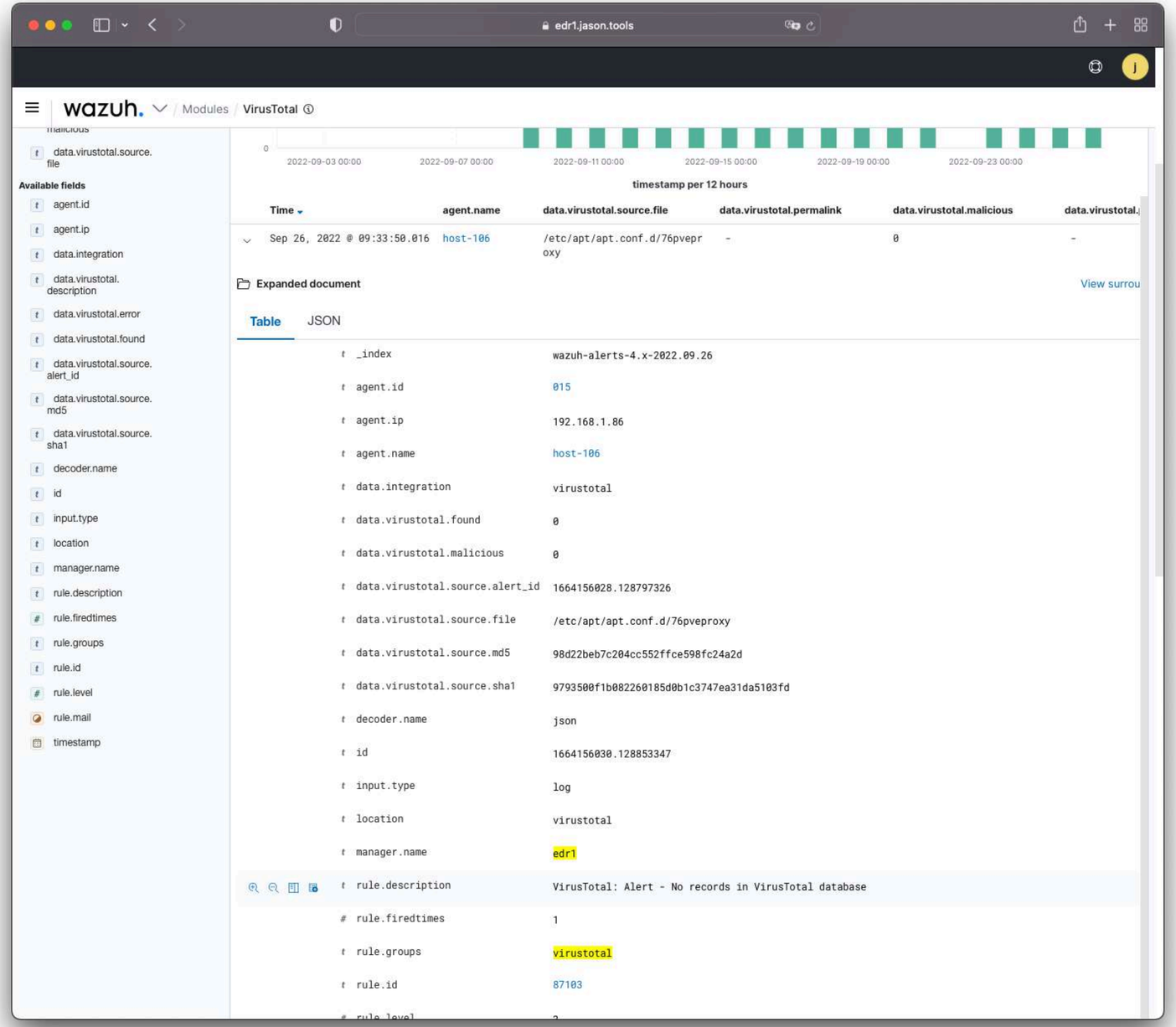
節省工具箱
JASON TOOLS

套件搭配

# 惡意檔案比對

- VirusTotal
- 比對雜湊值

問題是沒錢買
VirusTotal API
啊啊啊啊

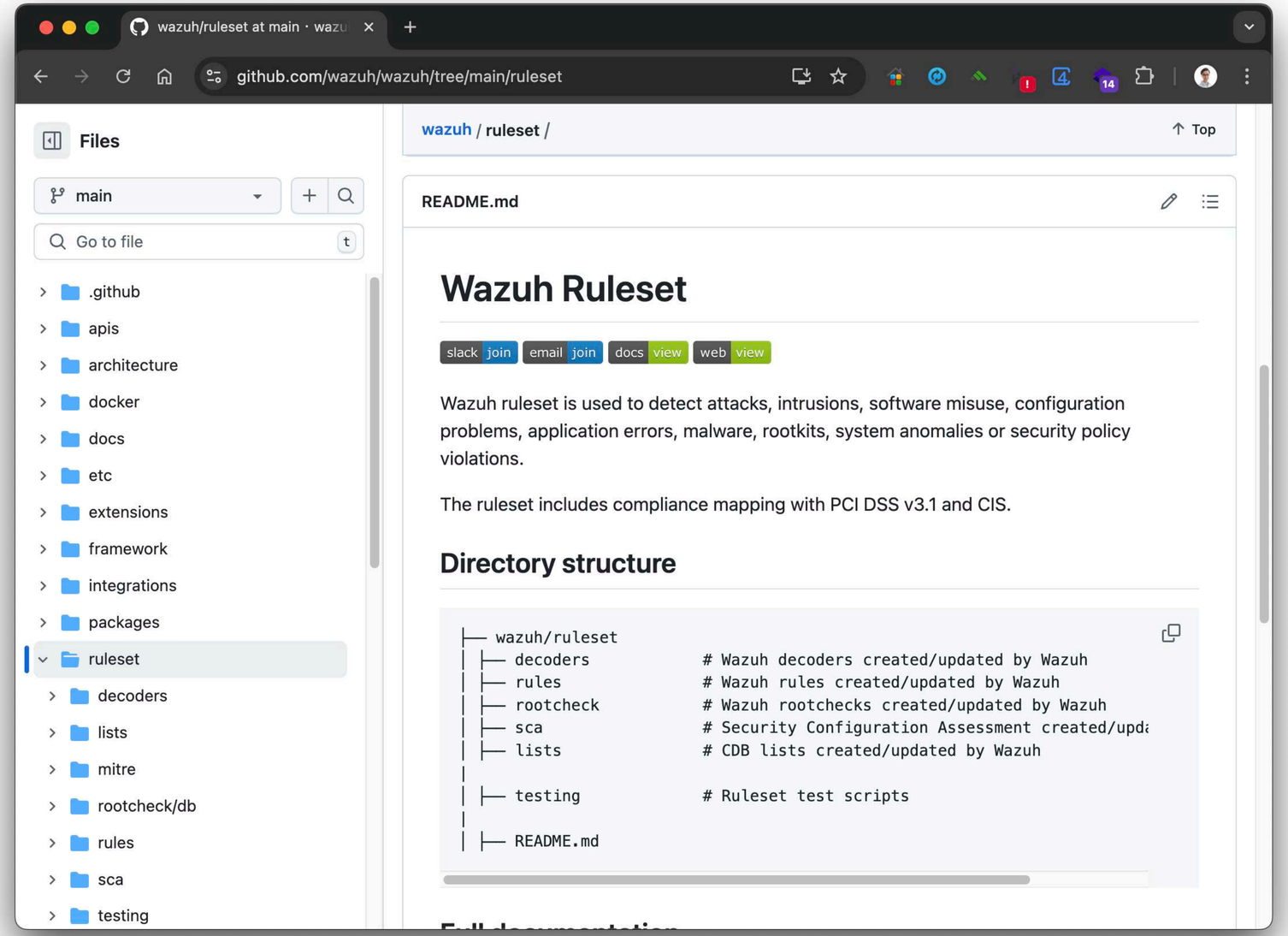


節省工具箱
JASON TOOLS

套件搭配

# 更多規則

- 內建規則
- 自動更新
- 手動啟用

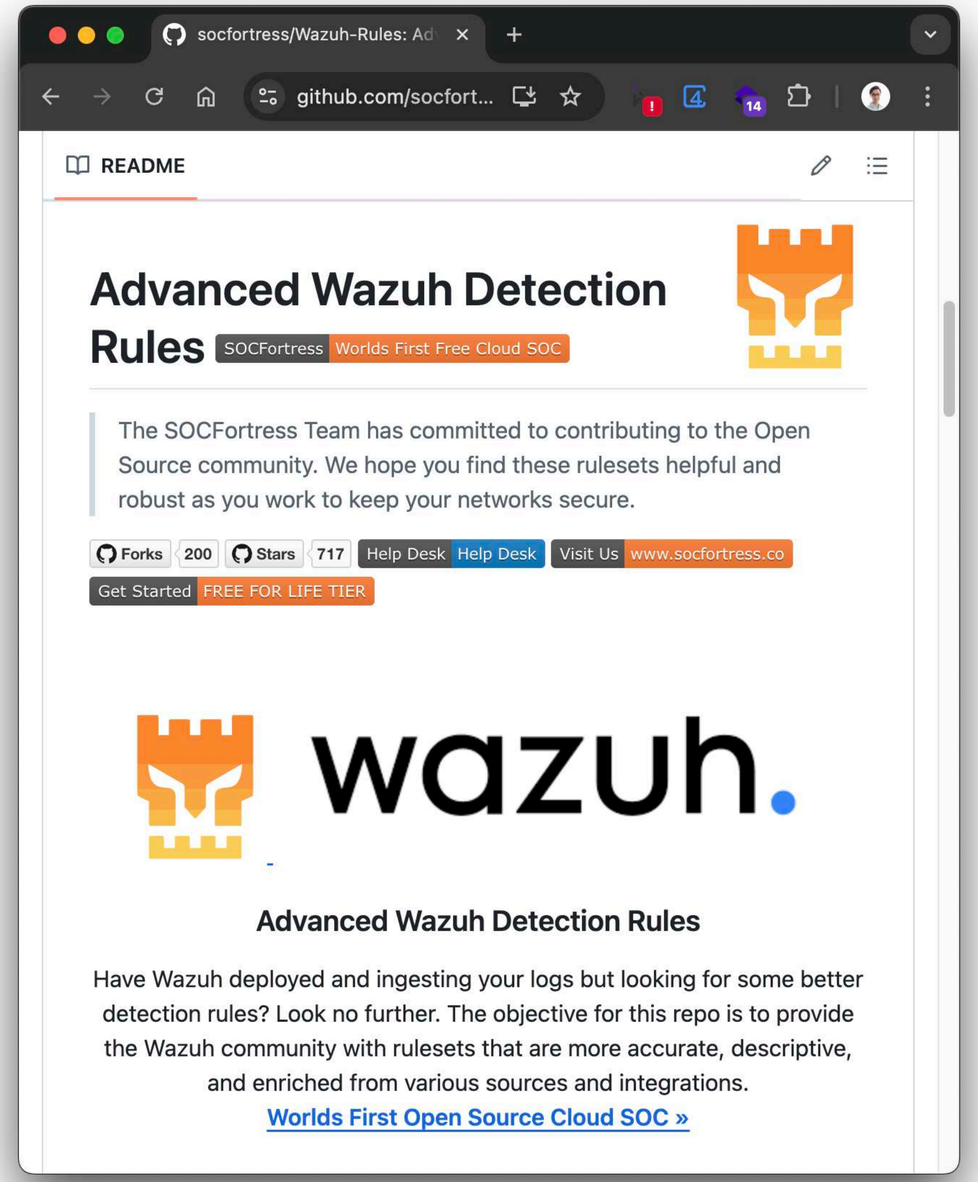


節省工具箱
JASON TOOLS

套件搭配

# 更多進階規則

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




https://github.com/socfortress/Wazuh-Rules

節省工具箱
JASON TOOLS

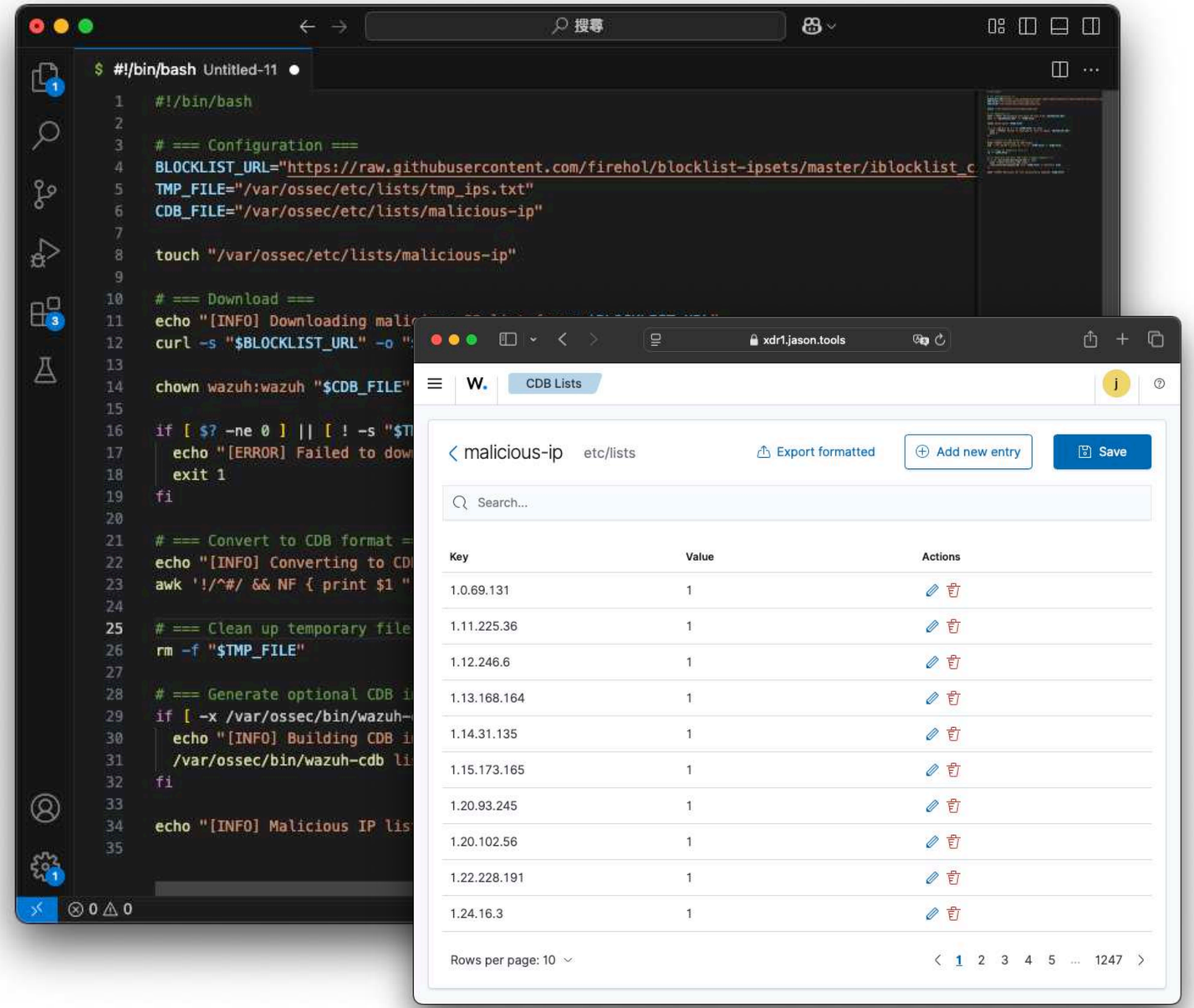
# 阻斷回應

節省工具箱
JASON TOOLS

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



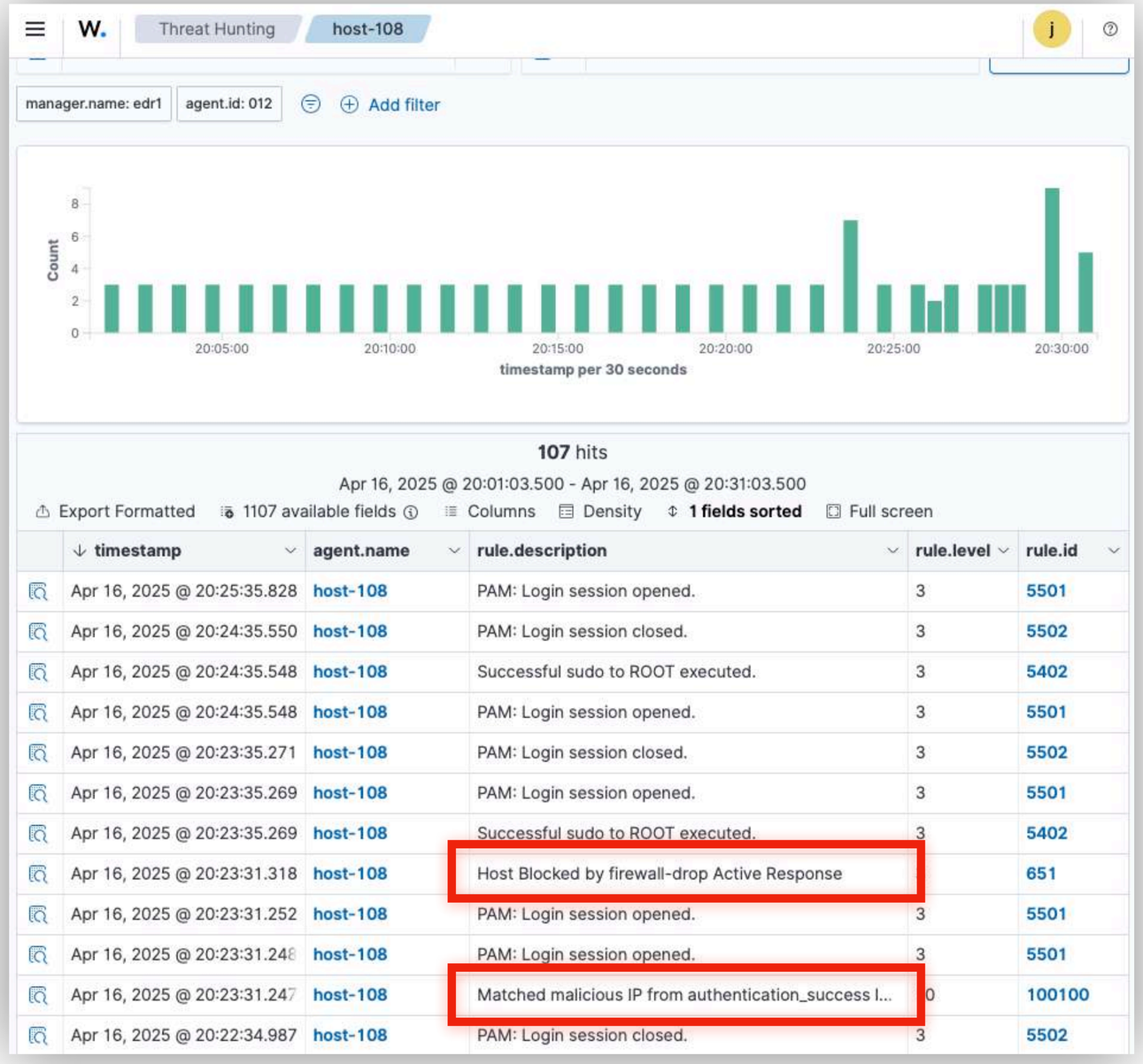

https://github.com/jasoncheng7115/it-scripts/blob/master/wazuh/update-malicious-ip.sh

節省工具箱
JASON TOOLS

阻斷回應

# 阻斷惡意 IP

- 自動偵測阻斷
- Linux
  (firewall-drop)
- Windows
  (netsh)
- OPNsense
  (pfctl)



節省工具箱
JASON TOOLS

# 阻斷回應

偵測到連入 IP 位於惡意清單

| | | |
|---|---|---|
| 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 |
| ◕ | rule.mail | false |

端點立刻封鎖 IP

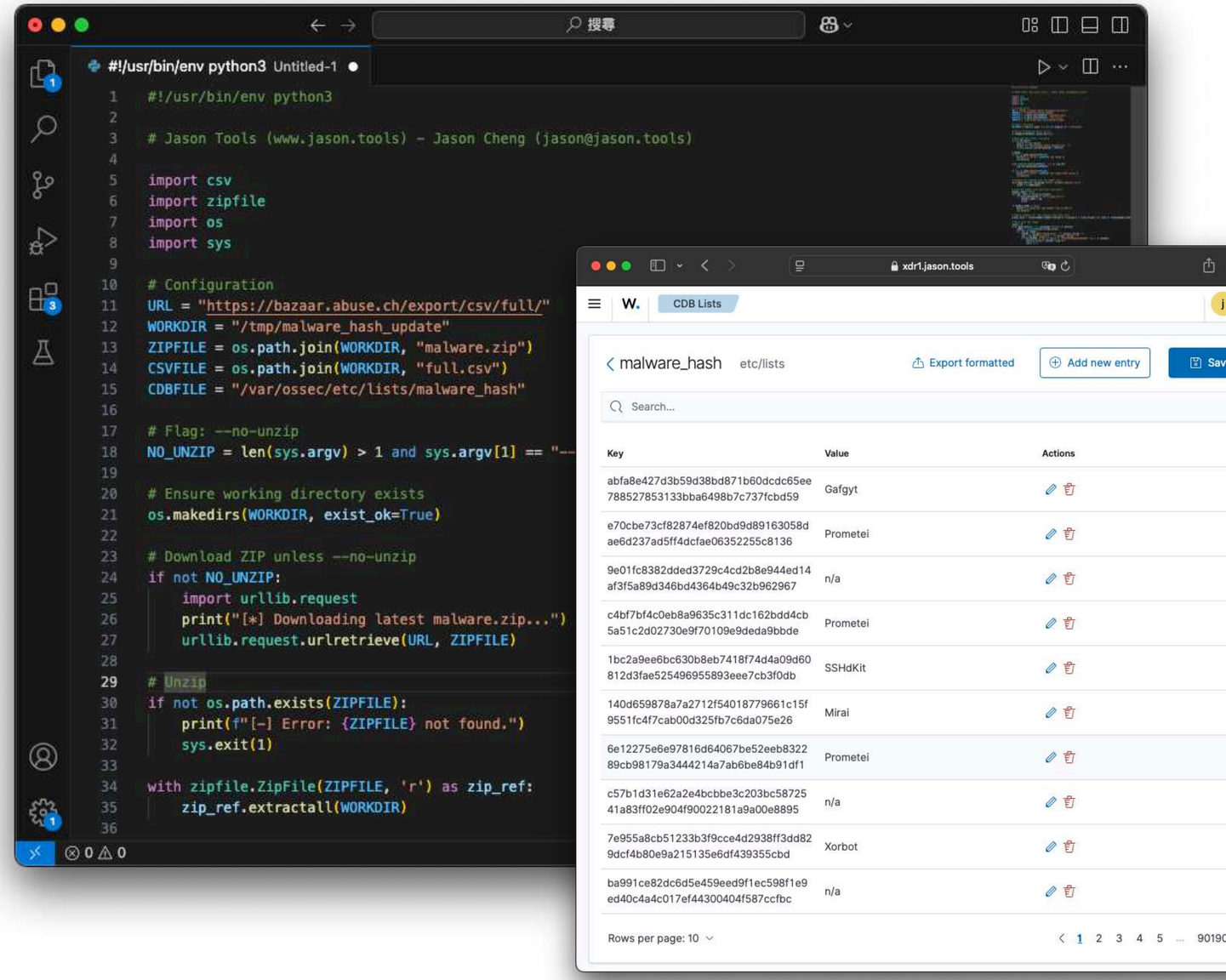
| | | |
|---|---|---|
| ? | data.parameters.alert.rule.description | Matched malicious IP from authentication_success logs |
| ? | data.parameters.alert.rule.firedtimes | 1 |
| ? | data.parameters.alert.rule.groups | malicious-ip |
| ? | data.parameters.alert.rule.id | 100100 |
| ? | data.parameters.alert.rule.level | 10 |
| ? | data.parameters.alert.rule.mail | false |
| ? | 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 |
| 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 |

節省工具箱
JASON TOOLS

阻斷回應

# 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



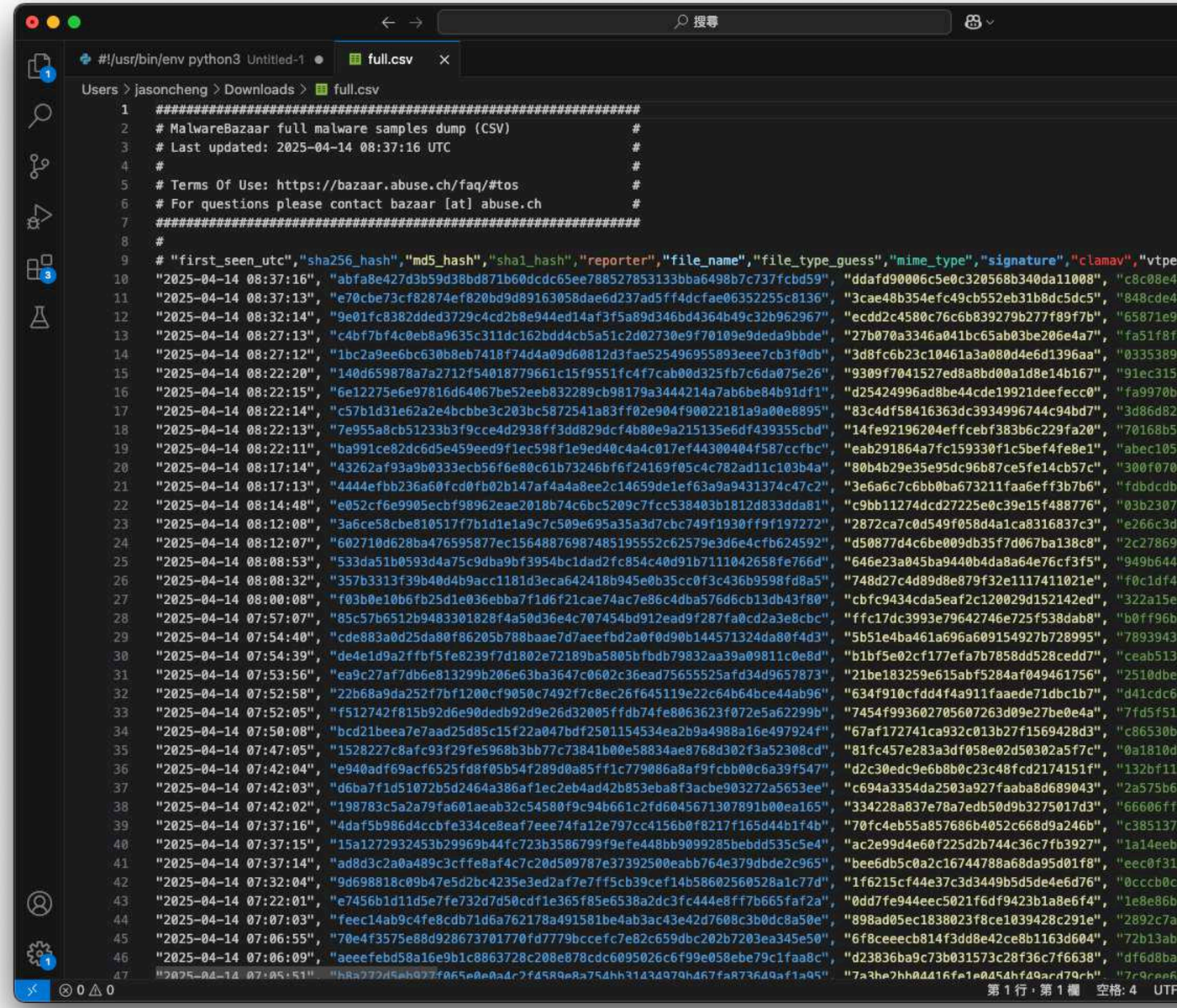

https://github.com/jasoncheng7115/it-scripts/blob/master/wazuh/update-malware-hash-list.py

節省工具箱
JASON TOOLS

阻斷回應

# 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



節省工具箱
JASON TOOLS

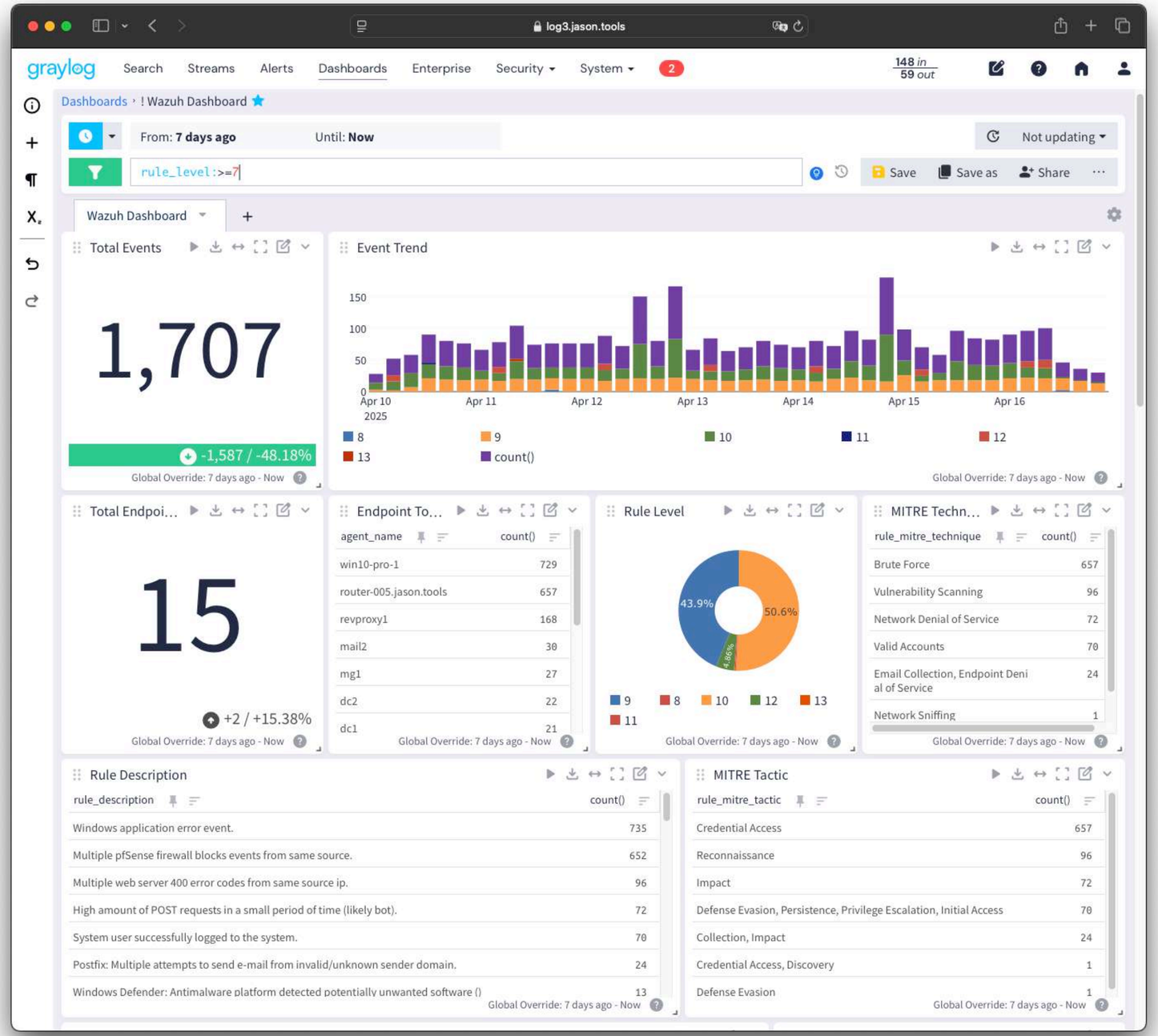
# Graylog 搭配使用

節省工具箱
JASON TOOLS

搭配 Graylog

# 整合看板

- 轉送記錄
- 欄位拆解
- 看板製作

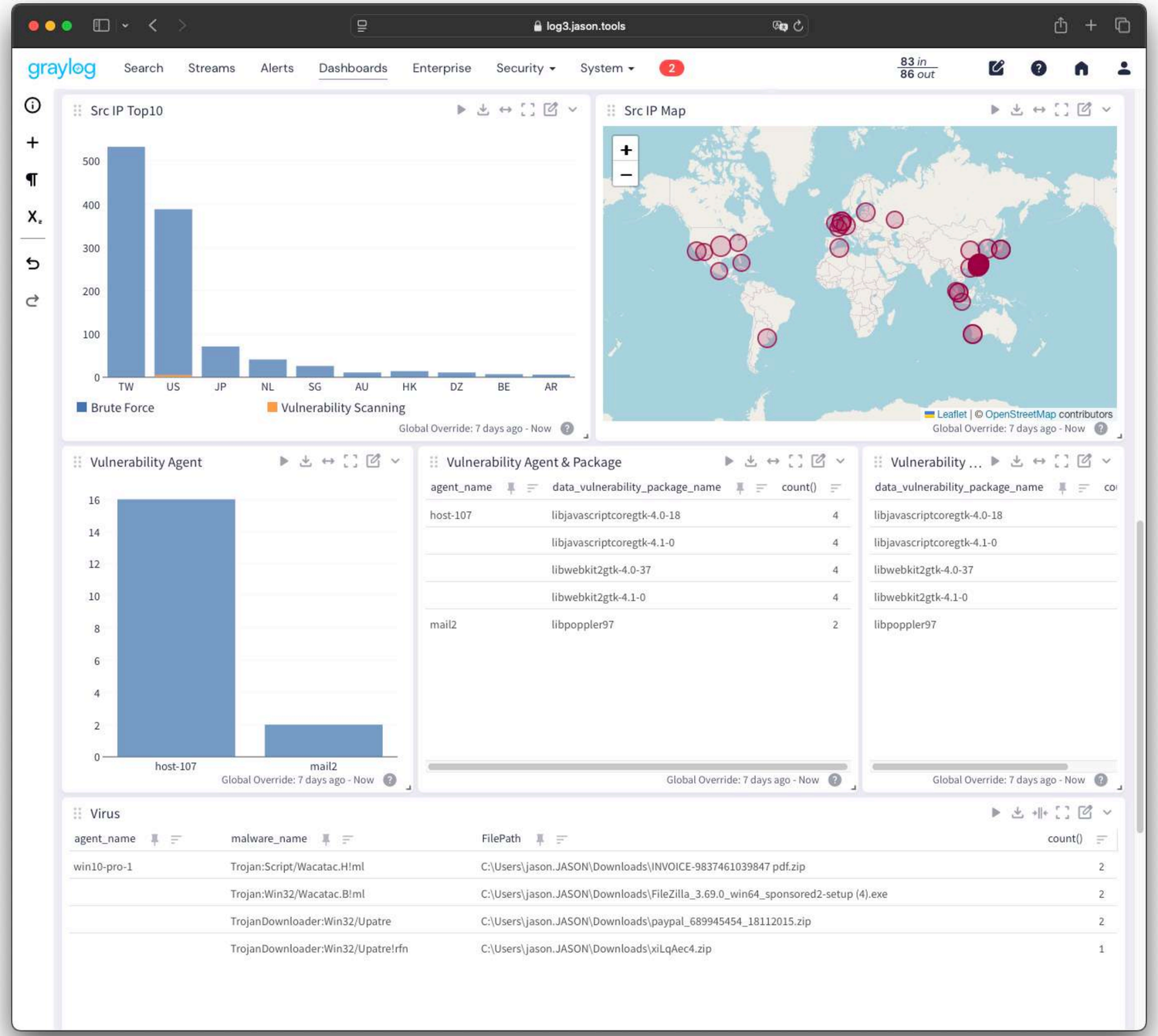


節省工具箱
JASON TOOLS

搭配 Graylog

# 整合看板

- 來源國家
- 軟體漏洞
- 惡意檔案

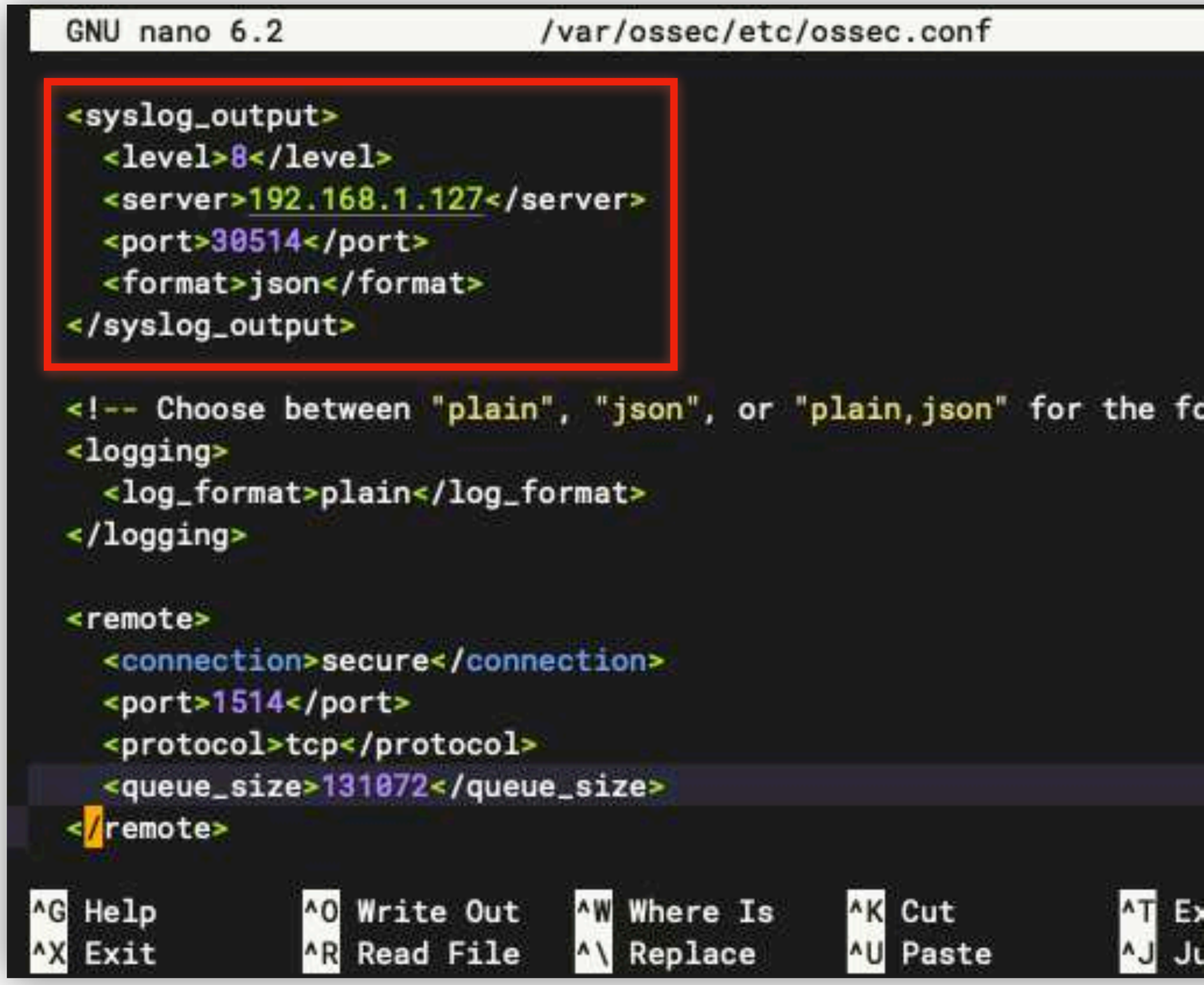


節省工具箱
JASON TOOLS

搭配 Graylog

# 轉送記錄

- 修改設定
- 轉送位址
- 指定等級
- 選定格式

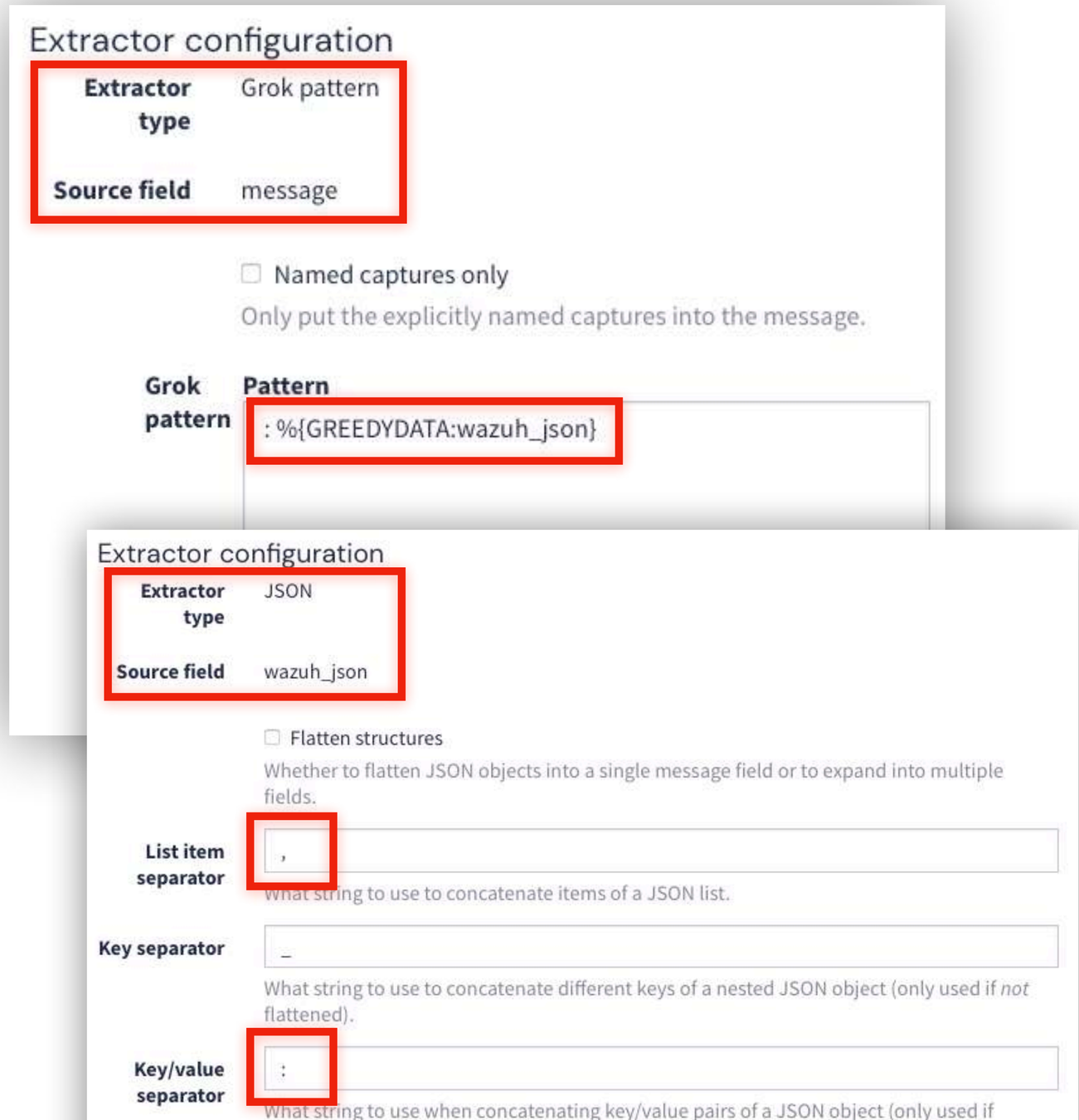


節省工具箱
JASON TOOLS

搭配 Graylog

# 轉送記錄

- 抽出 JSON 字串
- 拆解 JSON 欄位



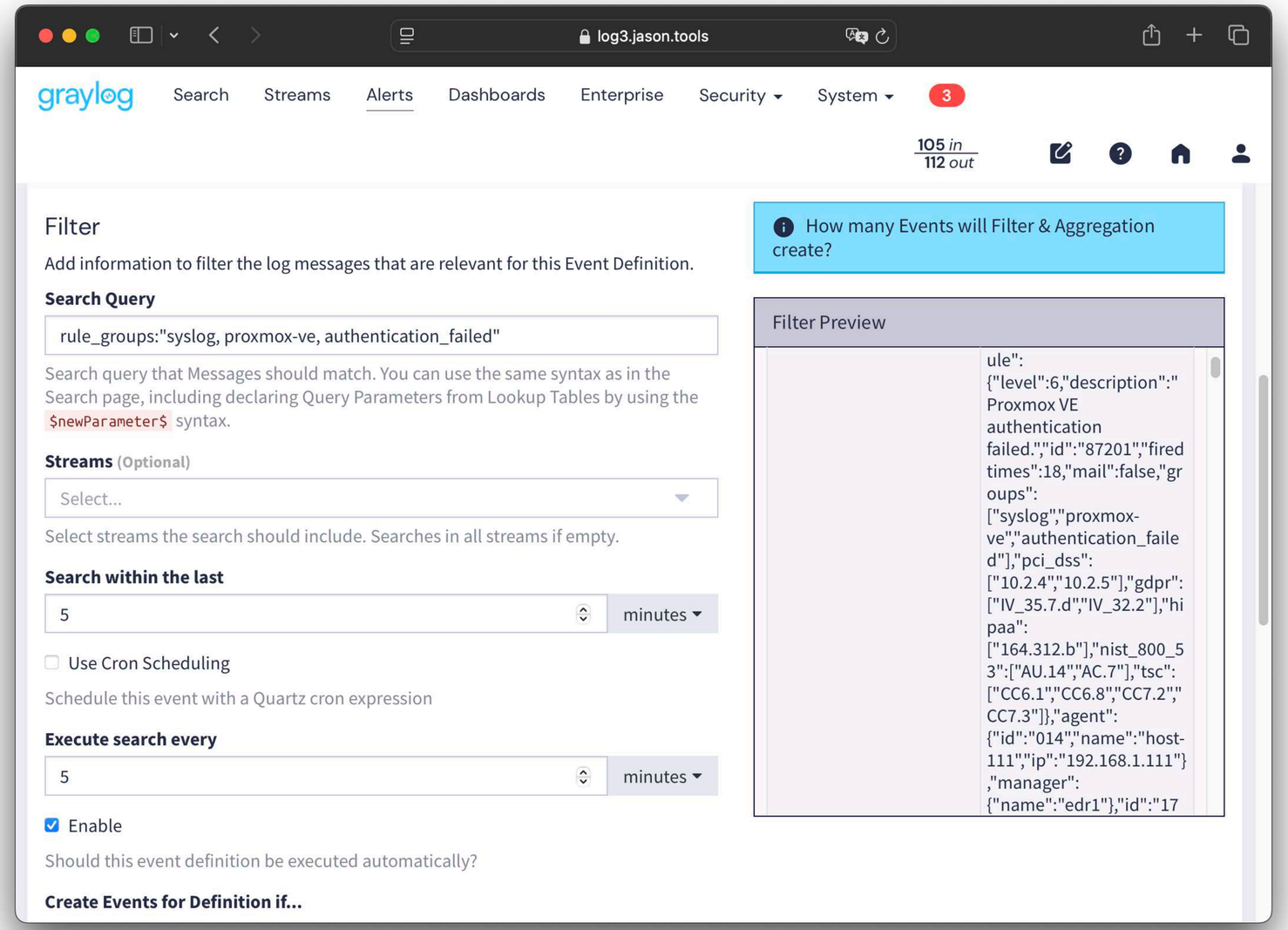
節省工具箱
JASON TOOLS

搭配 Graylog

# 警報發送

- 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

節省工具箱
JASON TOOLS

功能

# 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

節省工具箱
JASON TOOLS

功能

# 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

節省工具箱
JASON TOOLS

# 未來計劃

節省工具箱
JASON TOOLS

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

節省工具箱
JASON TOOLS

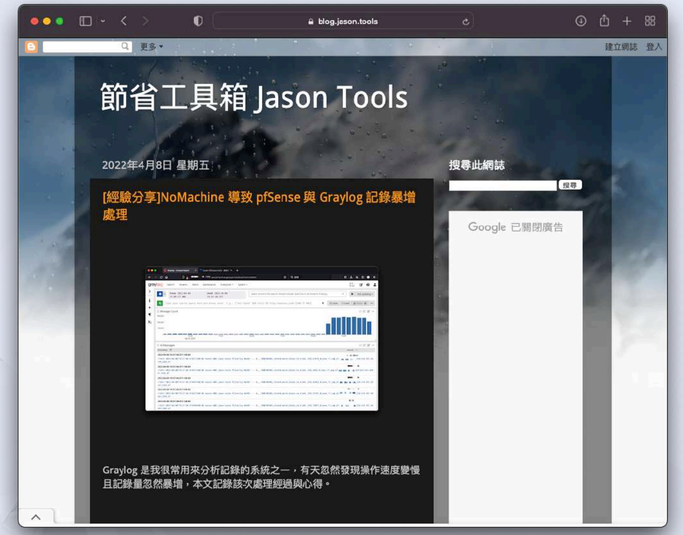
# 參考資料

節省工具箱
JASON TOOLS

# 連結


## 節省工具箱公司

**www.jason.tools**




## 節省工具箱網誌

**blog.jason.tools**

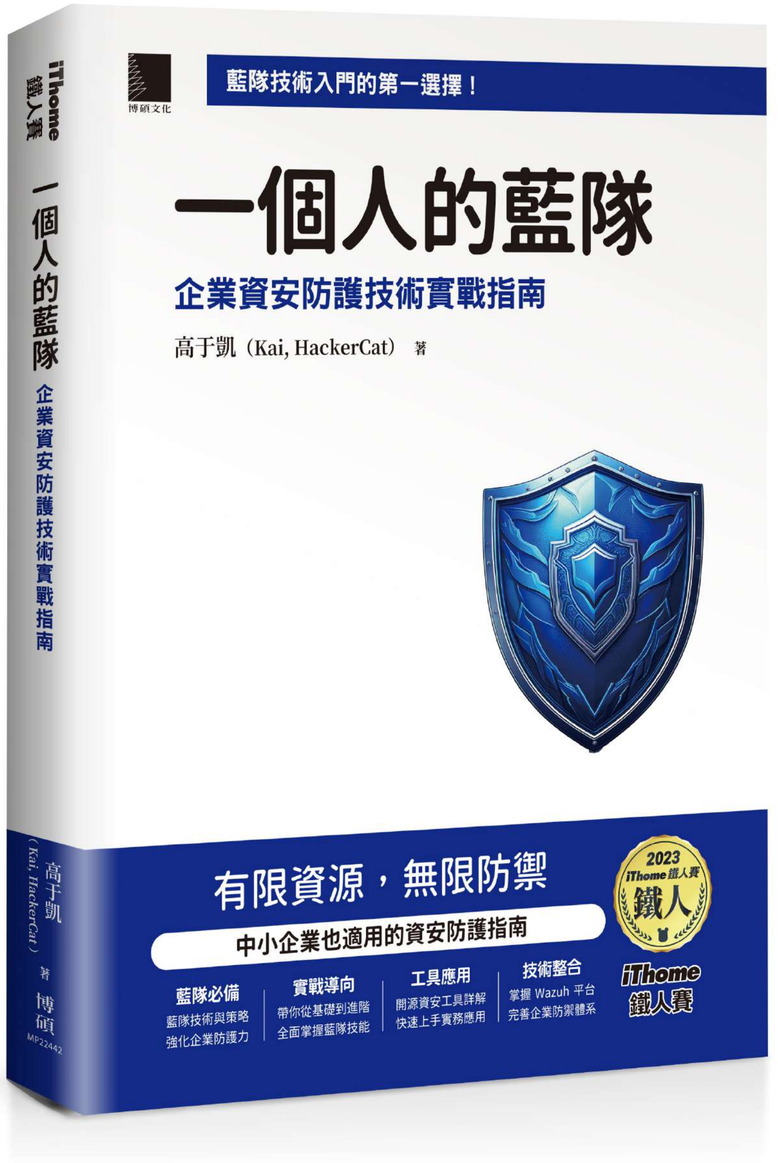
節省工具箱
JASON TOOLS

好書推薦

# 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

節省工具箱
JASON TOOLS

結束

# 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