WHITE PAPER

Corelight

Open Network Detection & Response

以 Zeek 為核心的開放式網路偵測與回應平台

讓 SOC 看見網路上真正發生的事，
不再被黑箱工具的誤報淹沒

Zeek 原創團隊打造 · Black Hat NOC 官方供應商 · Gartner NDR 領導者

SaaSPodium 拓維雲智資安顧問團隊
Authorized Distributor of Corelight
版本 1.0 | 2026 年 4 月

目錄

執行摘要

現代企業網路邊界已經模糊。Zero Trust、混合辦公、多雲架構、加密流量比例超過 95%、東西向流量爆炸、IoT/OT 裝置難以管理——這些變化讓傳統以 Perimeter Firewall 為核心的安全架構失效。端點偵測(EDR)雖然重要,但無法覆蓋未安裝 Agent 的裝置(印表機、IoT、Legacy 系統、雲端工作負載),也無法看見橫向攻擊的全貌。

Network Detection & Response(NDR)因此成為現代 SOC 的必備能力。但 NDR 市場魚龍混雜——多數 NDR 產品宣稱「AI 偵測」,但 SOC 分析師收到的告警只是一個黑箱結果:「偵測到可疑行為」,**卻看不到可驗證的證據**。當 IR 團隊需要進行事件調查、威脅獵捕(Threat Hunting)、法遵舉證時,這些「AI 偵測器」無法提供完整的網路活動記錄。

Corelight 採取完全不同的路線: 以業界唯一信賴的開源網路監控引擎 **Zeek**(前身為 Bro,由 Lawrence Berkeley National Lab 的 Vern Paxson 等人開發)為核心,產出經過解析、結構化、關聯的「網路活動證據(Network Evidence)」,讓 SOC 不僅能偵測威脅,更能在事後完整重建攻擊鏈。

Corelight 的核心優勢:

- **Evidence-First 哲學** — 不是黑箱告警,是可驗證、可查詢、可追溯的網路證據
- **Zeek + Suricata 雙引擎** — 結合業界最成熟的開源協議分析器與入侵偵測引擎
- **加密流量偵測(ETA)** — 不需解密即可識別加密流量中的惡意行為
- **與 SIEM / XDR 深度整合** — CrowdStrike NG-SIEM、Microsoft Sentinel、Splunk、Google SecOps、Elastic 原生整合
- **Smart PCAP 精準封包擷取** — 只在有意義時保留完整封包,節省儲存同時保留證據
- **Black Hat USA NOC 官方供應商** — 全球最嚴苛的網路環境中實戰驗證多年

> *「Darktrace 告訴我們『有異常』,但 Corelight 告訴我們『誰在什麼時間、透過什麼協議、連到哪裡、做了什麼』。這就是可處置告警與不可處置告警的差別。」— 某全球金融集團 SOC 主管*

一、NDR 為什麼成為 SOC 必備能力

1.1 EDR 與 SIEM 的天然盲區

現代 SOC 通常已投資 EDR(端點偵測)與 SIEM(日誌管理)。但這兩類工具留下了明顯盲區:

EDR 的限制:

- 只能保護已安裝 Agent 的端點,無法覆蓋:印表機、IP Camera、IoT 裝置、BMS 系統、OT/ICS 設備
- 無法看見雲端工作負載的東西向流量(Container-to-Container、Pod-to-Pod)
- 攻擊者可使用「無檔案攻擊」繞過 EDR 監控
- 攻擊者的橫向移動(Lateral Movement)在 EDR 中只能看到端點視角的碎片

SIEM 的限制:

- 依賴日誌來源,若裝置未送日誌,SIEM 無從偵測
- 日誌格式不一、欄位不完整,難以跨來源關聯
- 攻擊者可清除或篡改日誌以掩蓋行蹤
- 日誌無法重建完整的網路會話(Session)內容

NDR 填補的盲區:

NDR 透過被動式網路流量監控(Tap、SPAN、雲端 VPC Flow),不需要任何 Agent,不依賴日誌送出,直接從網路這個「無法撒謊」的層面觀察所有流量。這提供了以下關鍵能力:

- 看見所有連網裝置的行為,包括那些無法安裝 Agent 的
- 觀察完整的連線會話(誰連到誰、多久、傳輸多少資料)
- 偵測橫向移動、C2 通訊、資料外流、異常協議
- 為事件調查提供不可篡改的「網路真相」

1.2 SOC Visibility Triad(SOC 可視性三元素)

Gartner 提出的「SOC Visibility Triad」已成為業界共識:現代 SOC 必須同時具備三個視角才能有效防禦:

視角	工具類別	涵蓋範圍
端點	**EDR / XDR**	端點行為、檔案活動、Process 啟動、已安裝 Agent 的裝置
日誌	**SIEM / SDPP**	應用程式日誌、雲端 Audit Log、身份驗證、合規追蹤
網路	**NDR**	**所有裝置的網路行為、協議分析、橫向移動、加密流量異常、IoT/OT 覆蓋**

三個視角互補,缺一不可。少了 NDR,企業等於在網路層完全無監控,這是當代攻擊者最愛的盲區。

1.3 法規與監管要求推動 NDR 普及

近年多個主要法規與監管框架明確要求網路可視性:

- NIST Cybersecurity Framework 2.0 強調 Detect 與 Respond 必須具備網路層能力
- MITRE ATT&CK 框架將 Lateral Movement、Command & Control 列為關鍵戰術,需網路監控
- 歐盟 NIS2 指令要求關鍵基礎設施具備網路行為監控能力
- 金融監理(如台灣金管會、美國 NYDFS)要求具備東西向流量監控
- 零信任架構(Zero Trust)的核心原則之一就是「持續驗證網路行為」

二、Corelight 的獨特定位與 Zeek 血統

2.1 Zeek 的 30 年傳承

Zeek(前身為 Bro)誕生於 1995 年,由 Lawrence Berkeley National Lab 的 Vern Paxson 博士開發。設計初衷是讓網路科學家能以程式化的方式描述網路行為,而非僅依賴預設規則。經過 30 年的發展,Zeek 已成為:

- 全球頂尖大學、國家實驗室、超級電腦中心的標準網路監控工具
- 美國國防部、能源部、NASA 等政府機構的指定產品
- 全球最大金融機構、科技公司、電信業者的網路安全基石
- CNCF、Linux Foundation 等開源社群的重要專案

Corelight 由 Zeek 的三位核心創造者共同創立:

- **Vern Paxson** — Zeek 原創者、UC Berkeley 教授、網路安全領域最受尊敬的學者之一
- **Robin Sommer** — Zeek 核心貢獻者,10+ 年 LBNL 資深研究員
- **Seth Hall** — Zeek Project Leader、OSU/OARnet 背景,深度參與多個國家級網路監控專案

後期團隊更加入知名資安專家:

- **Richard Bejtlich** — Network Security Monitoring(NSM)領域的奠基者、多本經典資安著作的作者,於 Corelight 擔任 Principal Security Strategist

2.2 為什麼 Zeek 血統重要

網路協議分析是極度困難的工程挑戰。要正確解析各種協議(HTTP、TLS、DNS、SMB、RDP、Kerberos、SQL、DNP3 等工業協議)、在高流量下維持準確性、處理協議變形與對抗逃避技術——這需要十年以上的累積。

Zeek 累積了 30 年的協議解析能力,支援 70+ 種協議的深度分析,包括:

- 常見應用協議:HTTP、HTTPS、DNS、SMTP、FTP、SSH、Telnet
- 認證協議:Kerberos、NTLM、RADIUS、LDAP
- 檔案傳輸:SMB、NFS、FTP、AFP
- 遠端控制:RDP、VNC、SSH
- 資料庫協議:MySQL、MongoDB、Redis、PostgreSQL(部分)
- 工業控制:DNP3、Modbus、S7comm、IEC 104
- VPN 與通道:IPsec、GRE、GTP、WireGuard
- 加密流量:TLS 1.2/1.3 元資料分析(JA3、JA4 指紋)

任何一家聲稱「我們也做網路協議分析」的 NDR 廠商,實際上都無法追上 Zeek 的深度與穩定性。這是 Corelight 最難以複製的優勢。

2.3 Corelight 的商業定位

Corelight 不是「又一家 NDR 新創」。其商業發展歷程反映了企業級市場的認可:

- 2013 年 Broala 成立(Corelight 前身),由 Zeek 核心團隊創辦
- 2017 年正式更名 Corelight,推出商業化 Zeek 產品

- 2019 年 Black Hat NOC 正式採用 Corelight 作為網路監控基礎
- 2022 年獲 Insight Partners、Accel 等領投 USD 75M E 輪融資
- 2023 年進入 Gartner NDR Market Guide 代表廠商
- 2024 年與 CrowdStrike、Microsoft、Mandiant 建立深度整合合作
- 2025 年持續擴展雲端 NDR 能力(AWS、Azure、GCP 原生整合)

三、平台架構與核心能力

3.1 Corelight Open NDR Platform

Corelight Open NDR Platform 由三大產品組件組成:

產品	定位	核心能力
Sensors	**網路感測器**	Zeek + Suricata 雙引擎,支援實體 Appliance、VM、Container、Cloud(AWS VPC Traffic Mirror、Azure vTAP、GCP Packet Mirror)。
Investigator	**調查與分析平台**	SaaS 平台,提供 AI 告警、威脅獵捕、攻擊鏈視覺化、證據查詢、MITRE ATT&CK 對應。
Smart PCAP	**智慧封包擷取**	基於告警觸發的精準 PCAP 擷取,同時保留證據並控制儲存成本。

3.2 部署模式與覆蓋範圍

地端部署(On-Premises)

支援多款 Appliance 規格,涵蓋從分支機構(Gbps 級)到核心資料中心(100Gbps+)的各種流量規模。採用被動式監控,透過 SPAN Port、Network Tap 或 Packet Broker 收取鏡像流量。

虛擬化部署(Virtual)

提供 VMware、Hyper-V、KVM 版本,可部署於企業虛擬化平台,適合資料中心內的東西向流量監控。

雲端部署(Cloud)

AWS VPC Traffic Mirror、Azure vTAP、GCP Packet Mirroring 原生整合,無需改變雲端架構即可取得完整流量可視性。支援跨帳戶、跨 VPC、跨區域部署。

容器化部署(Kubernetes)

提供 Kubernetes 原生部署選項,可作為 DaemonSet 部署於每個 Node,監控 Pod 之間的東西向流量。

3.3 Zeek 產出的網路證據

Zeek 不只是「偵測異常」,而是將每一筆網路活動結構化為可查詢的證據記錄。主要日誌類型:

- **conn.log** — 所有連線紀錄(來源、目的、埠、協議、封包數、資料量、持續時間)
- **http.log** — HTTP 請求與回應(URL、User-Agent、Referrer、狀態碼、回應大小)
- **ssl.log / x509.log** — TLS 握手元資料、憑證資訊、JA3/JA4 指紋
- **dns.log** — DNS 查詢與回應、可疑域名偵測、DGA 分析
- **files.log** — 網路中傳輸的檔案元資料、MIME 類型、Hash
- **smb.log / kerberos.log / ntlm.log** — 企業內部認證與檔案共享活動

- **notice.log** — Zeek 原生偵測到的異常事件

3.4 Corelight-Exclusive 能力(超越開源 Zeek)

Corelight 不只是提供 Zeek 的商業支援,更大量擴展了 Zeek 的能力:

- **Corelight C2 Collection** — 與 Mandiant 合作的 Command & Control 通訊偵測,涵蓋 100+ 個 APT 家族
- **Corelight ML Detections** — 機器學習偵測(Beaconing、Data Exfiltration、Internal Recon)
- **Encrypted Traffic Collection** — 加密流量偵測的擴充 Package,覆蓋 TLS、SSH、QUIC
- **Entity Analytics** — 以「主機」為單位建立行為基線,自動識別偏離的異常
- **Investigator(SaaS 平台)** — 非開源 Zeek 的使用者只能自行建立查詢工具,Corelight 提供企業級 SaaS 調查平台

四、Evidence-First:Corelight 的差異化哲學

NDR 市場最核心的分水嶺,不是「誰的 AI 模型更好」,而是「遇到事件時,SOC 能不能拿到真相」。Corelight 以 Evidence-First 哲學,根本上區別於以「黑箱 AI 告警」為中心的競品。

4.1 黑箱 AI 告警的致命缺陷

多數 NDR 廠商以「AI 偵測」為行銷主軸,典型告警是這樣的:

> ⚠ *ALERT: Anomalous behavior detected on 10.1.2.3. Confidence: 87%.*

SOC 分析師收到這個告警後,必須問:

- 到底做了什麼異常?
- 是跟誰通訊?
- 用什麼協議?
- 傳輸什麼資料?
- 持續多久?
- 是否已擴散到其他主機?

如果 NDR 工具無法回答這些問題,告警實際上是無法處置的。而多數黑箱 AI 型 NDR 正是如此——他們強調「告警準確率」,但無法提供告警背後的原始證據。

4.2 Corelight 的證據鏈

同一個場景,Corelight 提供的不是「告警」,而是完整的網路證據鏈:

- conn.log:10.1.2.3 於 03:14:22 UTC 連線至 185.234.72.19:443,持續 4 小時 23 分鐘,傳輸 2.4 GB
- ssl.log:使用 TLS 1.3,JA3 指紋 = a0e9f5d64349fb13...,憑證發行者為「Let's Encrypt」,有效期 72 小時(異常短)
- dns.log:主機 10.1.2.3 在過去 24 小時內查詢了 847 個不同域名,其中 89% 為 DGA 特徵
- notice.log:此主機的 Beaconing Pattern 與已知 APT32 C2 通訊特徵匹配
- Smart PCAP:相關連線的完整封包已保留,可供深度分析

這不是「可能有問題」,而是「這裡是證據,請你來判斷」。這個哲學根本性地改變了 SOC 的工作方式:從被告警追著跑,變成以證據為基礎主動追查。

4.3 為什麼這對 SOC 成熟度至關重要

三種常見的 SOC 工作模式,需要的工具能力截然不同:

- **Tier 1 告警處理** — 需要可信賴的告警,但黑箱 AI 告警品質不穩時反而造成疲勞
- **Tier 2 事件調查** — 絕對需要完整證據,黑箱告警完全無法支撐調查
- **Tier 3 威脅獵捕** — 需要可查詢、可關聯的原始資料,只有 Evidence-First 產品能做到

Corelight 的 Evidence-First 哲學,讓一份投資同時服務了三種層級的分析師需求。競品工具則通常只能服務 Tier 1,Tier 2/3 仍需要其他工具補強。

五、競爭格局分析:Corelight vs. ExtraHop vs. Vectra AI vs. Darktrace

NDR 市場的主要競爭者包括 ExtraHop、Vectra AI、Darktrace。每一家都有其歷史背景與市場定位,也各自存在明顯的侷限。本章節提供深度比較分析。

5.1 Corelight vs. ExtraHop

ExtraHop 是 NDR 市場的老牌廠商之一,起家於網路效能監控(NPM),後轉型資安領域。2021 年被 Bain Capital 與 Crosspoint Capital 以 USD 9 億收購私有化。其 Reveal(x) 產品在金融、醫療、製造業有相當市占。

ExtraHop 的核心特徵:

- 網路效能監控(NPM)出身,強項在於即時線路分析
- 自建協議解析器,支援 70+ 種協議
- 有線性能(Wire Data)分析能力強
- 商業模式以高階 Appliance 硬體為主

ExtraHop 的痛點:

- **封閉式架構** — 資料格式與協議解析器皆為專有,資料被鎖定在 ExtraHop 平台內,難以導出或整合
- **告警偏向黑箱** — AI 偵測邏輯不透明,無法驗證偵測根據
- **Threat Hunting 能力受限** — 查詢語言與介面為 ExtraHop 專有,難以跨工具關聯
- **授權成本極高** — 以硬體 Appliance 為核心的商業模式,單點授權費常達 USD 100K-300K
- **雲端部署能力較弱** — 傳統上以地端硬體為主,雲端選項相對較新
- **缺乏開源生態** — 獨家協議解析器無法享受社群貢獻,覆蓋廣度落後於 Zeek 社群

Corelight 相對 ExtraHop 的優勢:

- **開放架構** — 基於開源 Zeek,資料為開放格式(JSON),可無痛整合 SIEM、Data Lake、SOAR
- **透明偵測邏輯** — 每個偵測可追溯到具體 Zeek 腳本,SOC 可驗證與客製化
- **強大的 Threat Hunting 能力** — Zeek 日誌直接可用於 Splunk SPL、Sentinel KQL、Elasticsearch DSL 等標準查詢語言
- **授權模式更靈活** — 提供硬體、軟體、雲端多種形式,TCO 通常優於 ExtraHop
- **原生雲端支援更強** — AWS、Azure、GCP 原生整合,多年雲端部署經驗
- **社群生態優勢** — 全球 Zeek 社群持續貢獻新協議解析器與偵測內容

5.2 Corelight vs. Vectra AI

Vectra AI 以「AI-Driven NDR」為主要訴求,在北美市場有一定能見度。2023 年獲 Blackstone 領投 USD 1.5 億融資,商業規模持續擴大。

Vectra AI 的核心特徵:

- 強調 AI 與機器學習偵測為產品核心
- 以「Attack Signal Intelligence」為行銷主軸
- 自有的 Threat Detection Model 涵蓋雲端與地端

- Cognito Platform 為統一介面

Vectra AI 的痛點:

- **協議解析深度不及 Zeek** — AI 強但底層網路解析相對淺,複雜協議(SMB、Kerberos、工業協議)覆蓋有限
- **典型黑箱告警問題** — AI 偵測邏輯不透明,SOC 難以驗證「為什麼這算異常」
- **缺乏豐富原始證據** — 不提供 Zeek 等級的結構化網路日誌,威脅獵捕能力受限
- **PCAP 能力相對弱** — 相比 Corelight Smart PCAP,Vectra 的封包擷取選項較有限
- **告警量大但可處置性未必高** — 客戶普遍回饋 Vectra 告警量偏高,需要大量人工校調

Corelight 相對 Vectra AI 的優勢:

- **深度協議分析** — Zeek 覆蓋 70+ 種協議,遠超過 Vectra 的基礎分析
- **證據驅動的偵測** — 不只告警,更提供完整網路活動記錄,支持完整事件調查
- **Smart PCAP 深度證據** — 關鍵事件的完整封包可供深度分析,支援法遵與 IR
- **更透明的偵測邏輯** — Zeek 腳本可檢視、可客製化、可由 SOC 自主擴展
- **更好的 SIEM / XDR 整合** — 結構化日誌可直接用於 SIEM 規則撰寫,不需封閉 API

5.3 Corelight vs. Darktrace

Darktrace 以「Self-Learning AI」為品牌核心,於 2021 年倫敦證交所上市。其 Enterprise Immune System 產品在全球有廣泛知名度,但近年也受到分析師與前員工對於「AI 真實能力」的質疑。

Darktrace 的核心特徵:

- 以「Self-Learning AI」「Autonomous Response」為行銷主軸
- Enterprise Immune System 涵蓋網路、端點、雲端、郵件等多個領域
- Antigena 自動回應模組
- Cyber AI Analyst 自動調查功能

Darktrace 的痛點:

- **極度黑箱的 AI** — Darktrace 的核心 AI 模型(貝氏網路)偵測邏輯幾乎完全不透明,SOC 無法驗證告警
- **誤報率高** — 業界公認 Darktrace 在複雜企業環境中誤報問題嚴重,需大量人工調整
- **行銷大於實質** — 多位前員工與分析師公開質疑 Darktrace 的 AI 實際效能與行銷敘述不符
- **原始證據能力薄弱** — 無提供 Zeek 等級的網路日誌,威脅獵捕與事件調查高度依賴 Darktrace 本身 UI
- **難以整合第三方工具** — 封閉式資料結構,與 SIEM、SOAR、XDR 整合深度有限
- **Antigena 自動回應的信任問題** — 企業普遍不敢開啟自動回應,因無法驗證 AI 判斷基礎
- **價格昂貴** — 業界公認 Darktrace 為 NDR 市場價格最高之一

Corelight 相對 Darktrace 的優勢:

- **完全透明的偵測** — 每個偵測都有具體的 Zeek 腳本、威脅情報、MITRE ATT&CK 技術對應
- **Evidence-First 哲學** — 提供可查詢、可驗證、可匯出的原始網路證據

- **更可信的偵測能力** — 結合 Zeek、Suricata、Mandiant C2 情報,偵測基礎有實質技術支撐
- **開放整合架構** — 深度整合主流 SIEM / XDR,不將企業鎖定於單一平台
- **TCO 顯著較低** — 典型價格約為 Darktrace 的 50-70%

5.4 四大 NDR 平台綜合比較表

比較面向	Corelight	ExtraHop	Vectra AI	Darktrace
協議解析深度	★★★★★	★★★★	★★★	★★
偵測透明度	★★★★★	★★	★★	★
原始證據 / Threat Hunting	★★★★★	★★★	★★	★★
Smart PCAP	★★★★★	★★★	★★	★★
AI / ML 偵測能力	★★★★	★★★	★★★★★	★★★★
加密流量分析	★★★★★	★★★	★★★	★★★
SIEM 整合深度	★★★★★	★★★	★★★	★★
雲端原生部署	★★★★★	★★★	★★★★	★★★
開源社群生態	★★★★★(Zeek)	無	無	無
工業協議 OT/ICS	★★★★★	★★	★★	★★
典型授權成本	$$$	$$$$	$$$	$$$$$
導入複雜度	中	高	中	中
告警可處置性	★★★★★	★★★	★★★	★★
MITRE ATT&CK 對應	★★★★★	★★★	★★★★	★★★

六、與 CrowdStrike NG-SIEM 的整合優勢

CrowdStrike 是全球市占最高的 EDR 廠商,近年積極擴展為 XDR 與 Next-Gen SIEM 平台(基於 Falcon LogScale)。許多企業希望以 CrowdStrike 作為資安中樞。然而,CrowdStrike 本身不提供 NDR——這正是 Corelight 的關鍵角色。

6.1 Corelight 與 CrowdStrike 的戰略合作

Corelight 是 CrowdStrike 生態系中 NDR 類別的首選合作夥伴:

- Corelight 為 CrowdStrike Marketplace 正式認證夥伴
- 原生整合 Falcon Next-Gen SIEM(LogScale)與 Falcon Insight XDR
- Corelight 網路證據自動豐富 CrowdStrike 端點告警
- 聯合產品 Roadmap 與技術整合研發

6.2 整合後的具體能力

能力一:端點-網路雙視角關聯

當 CrowdStrike Falcon 在某主機偵測到可疑活動(如 Cobalt Strike Beacon),Corelight 可立即提供該主機的完整網路活動:它連到哪些外部 IP、使用什麼 C2 協議、傳輸多少資料、是否有橫向移動。

能力二:填補 EDR 覆蓋盲區

CrowdStrike Falcon 無法安裝在印表機、IoT 裝置、OT 設備、部分 Legacy 系統上。Corelight 透過網路被動監控,為這些無 Agent 設備提供完整的資安可視性。整合後,CrowdStrike 儀表板可直接看到這些裝置的異常行為。

能力三:威脅獵捕的網路維度

CrowdStrike 的 Threat Hunting 強項在於 Endpoint Activity。Corelight 增加了網路維度——威脅獵人可在同一介面內查詢端點 process 活動與網路 session 資料,建立完整攻擊鏈。

能力四:NG-SIEM 資料效率

Corelight 產出的 Zeek 日誌經過高度結構化,進入 Falcon LogScale 後查詢效率極高,且資料量比傳統 SIEM 收納原始封包摘要小 10 倍以上,大幅降低 SIEM 授權費用。

6.3 Corelight + CrowdStrike vs. 其他 NDR + CrowdStrike 的差異

雖然 ExtraHop、Vectra、Darktrace 也能技術上對接 CrowdStrike,但整合深度明顯不及 Corelight:

- **Corelight 結構化日誌直接進入 LogScale,無需額外轉換**——其他 NDR 的資料格式封閉,需要中介層轉換,查詢效能差
- **Corelight 與 CrowdStrike 有正式的聯合產品工程合作**——其他 NDR 是單向 API 整合,深度有限
- **Corelight 為 Falcon 商店的推薦 NDR 選項**——客戶採購時可透過 CrowdStrike 直接加購
- **Corelight 加密流量指紋(JA3/JA4)可直接豐富 CrowdStrike 威脅情報**——其他 NDR 多以告警為單位整合,無法提供指紋級細節

> *「加入 Corelight 後,我們的 CrowdStrike Threat Hunting 從『端點上的 Process』擴展為*

> *『端點 + 網路的完整攻擊鏈』,這是質的變化。」— 某電信業 Threat Hunting 主管*

七、與 Microsoft Defender / Sentinel 的整合優勢

微軟資安生態(Defender for Endpoint、Defender XDR、Sentinel)在全球擁有巨大市占,特別是 M365 深度使用的企業。Corelight 與微軟建立了深度的技術整合,成為微軟生態中 NDR 能力的首選。

7.1 與 Microsoft Sentinel 的原生整合

- Corelight 為 Microsoft Sentinel Content Hub 官方 Solution
- 預建 100+ 個偵測規則與 KQL 查詢,直接可用
- 預建多個 Workbook,呈現網路威脅概覽、加密流量分析、MITRE ATT&CK 對應
- Playbook 自動化整合(Logic Apps)可進行自動回應
- Zeek 日誌透過 Log Analytics Agent 或 Data Collection Rules 高效送入 Sentinel

7.2 與 Microsoft Defender XDR 的整合

- Defender for Endpoint 端點告警可自動關聯 Corelight 網路證據
- Defender for Cloud 偵測到的雲端威脅可透過 Corelight 查看東西向流量細節
- Defender for IoT 偵測 OT 環境,但覆蓋深度受限,Corelight 提供完整 OT 協議分析(DNP3、Modbus、S7comm)
- 統一 Incident View:Defender 告警 + Corelight 網路事件在單一 Timeline 中呈現

7.3 為什麼微軟生態特別需要 Corelight

微軟雖有 Defender for IoT 產品,但在網路監控的深度與廣度上,與 Corelight 相比有明顯差距:

- **Defender for IoT 的限制** — 主要針對 OT 環境與特定協議,IT 網路、雲端流量覆蓋不完整
- **微軟無獨立 NDR 產品** — 這是微軟資安堆疊中公認的缺口,微軟官方也主動推薦客戶搭配專業 NDR
- **Corelight 與微軟的聯合客戶案例** — 許多 Fortune 500 企業採用 Sentinel + Corelight 作為標準架構

7.4 整合架構圖示

典型 Corelight + Microsoft 整合架構:

層級	元件	角色
資料收集	**Corelight Sensors**	收集所有網路流量,產出 Zeek + Suricata 結構化日誌
雲端流量	**AWS VPC Mirror / Azure vTAP**	Corelight 雲端 Sensor 接收並分析雲端流量
端點	**Defender for Endpoint**	端點行為偵測,與 Corelight 網路證據雙向關聯
日誌平台	**Microsoft Sentinel**	統一 SIEM,接收 Corelight + Defender + 其他來

層級	元件	角色
		源
偵測關聯	**Defender XDR + Sentinel Analytics**	Corelight 規則包 + 微軟規則,跨來源關聯
自動回應	**Sentinel Playbooks**	依照告警嚴重度自動執行隔離、封鎖、通知等動作
調查介面	**Microsoft Defender Portal**	統一事件視圖,SOC 無需切換工具

7.5 為何其他 NDR 整合微軟較弱

ExtraHop、Vectra、Darktrace 雖然也聲稱整合微軟,但實際體驗上差距明顯:

- **Corelight 結構化日誌直接符合 Sentinel 資料表架構** — KQL 查詢可直接寫,其他 NDR 需要大量 Parser 工作
- **Corelight Sentinel Solution 經過微軟官方認證** — 預建 Workbook、Playbook、Analytics Rule 開箱即用
- **Corelight 是微軟 Security Alliance 成員** — 聯合銷售、聯合解決方案、聯合客戶支援
- **Defender for IoT 內部團隊與 Corelight 有持續技術交流** — 互補而非競爭,真正的聯合方案

八、加密流量偵測(Encrypted Traffic Analytics)

根據 Google 研究,2025 年網際網路流量中超過 95% 已加密(HTTPS、TLS、QUIC)。企業內部流量的加密比例也快速上升(Kerberos 加密、SMB 簽章、應用程式 TLS)。這帶來一個根本問題:傳統依賴明文檢查的資安工具正在大規模失效。

8.1 加密流量的偵測挑戰

- 無法檢查內容,但可以分析元資料
- SSL 解密(SSL Decryption / TLS Interception)成本高、效能負擔大、隱私法規風險
- TLS 1.3 與 ECH(Encrypted Client Hello)讓傳統 DPI 更困難
- 攻擊者大量使用合法 CA 憑證,憑證信任本身已不足以判斷惡意

8.2 Corelight 的加密流量偵測能力

Corelight 完全不需解密,仍能從加密流量中提取大量可用情報:

- **JA3/JA4 指紋** — TLS Client Hello 參數指紋,可識別特定惡意軟體家族的通訊
- **JA3S/JA4S 指紋** — 伺服器端指紋,可識別 C2 伺服器
- **SNI(Server Name Indication)** — 目標網域名稱,即使流量加密仍可見
- **憑證分析** — 發行者、有效期、自簽憑證、Let's Encrypt 短效憑證異常
- **TLS Metadata** — 版本、密碼套件、ALPN 協議、Session Resumption 模式
- **流量模式分析** — 封包大小分佈、傳輸時間模式、Beaconing 週期性

這些能力讓 Corelight 能在完全不解密的情況下,識別:

- 已知惡意軟體的 C2 通訊(透過 JA3 指紋比對)
- 可疑的加密通道(自簽憑證、短效憑證、非常見 CA)
- 資料外流行為(加密流量的體積與模式異常)
- 使用加密通道的橫向移動

8.3 對比:其他 NDR 加密流量能力的侷限

- ExtraHop:提供有限的 JA3 指紋,但依賴自家資料庫更新
- Vectra:主要依賴行為模式分析,指紋能力相對弱
- Darktrace:以 AI 分析為主,但缺乏透明的指紋級證據
- Corelight:Zeek 社群持續貢獻最新指紋,結合 Mandiant C2 Collection,偵測廣度業界領先

九、Black Hat NOC 的實戰驗證

Black Hat 是全球規模最大、最具影響力的資安會議,每年在 Las Vegas、London、Asia 等地舉辦。其現場網路環境是全球最具挑戰性的實戰測試場——數千位頂尖駭客、資安研究人員、零日漏洞展示、滲透測試工具同台。

9.1 Black Hat NOC 的選擇

自 2019 年起,Black Hat 官方 NOC(Network Operations Center)正式採用 Corelight 作為網路監控核心。Corelight 貢獻了:

- Zeek + Suricata 雙引擎流量分析
- 即時威脅偵測與事件回應
- 會場流量完整證據保存
- 與 Cisco、Palo Alto、NetWitness、Lumen 等其他 NOC 夥伴的資料共享

9.2 為什麼這件事重要

Black Hat NOC 的採用具有三層意義:

- **技術可信度** — 能在全球最複雜、最惡意的網路環境中運作,代表產品可應對企業級挑戰
- **社群認可** — Black Hat NOC 由業界頂尖資安人員組成,他們選擇 Corelight 是基於實際效能而非行銷
- **持續改善** — 每年 Black Hat 都是 Corelight 的實戰演練,新發現與新技術持續回饋至產品

ExtraHop、Vectra、Darktrace 均未取得此等級的社群實戰認證。

> *「在 Black Hat NOC,我們依賴 Corelight 來監控一個基本上所有人都在嘗試入侵或展示攻擊的網路。Corelight 提供了我們需要的那種『看見真相』的能力。」 — Neil Wyler(Grifter),Black Hat NOC Lead*

十、典型應用場景

10.1 替換老舊 IDS / 新增 NDR 能力

某半導體客戶原使用 Cisco Stealthwatch + Snort,但已無法跟上現代威脅與加密流量挑戰。替換為 Corelight 後,偵測範圍擴大 3 倍、誤報降低 70%、Threat Hunting 能力首次建立。

10.2 替換 ExtraHop / 其他封閉式 NDR

某金融客戶使用 ExtraHop Reveal(x) 5 年,但苦於資料被鎖在 ExtraHop 平台、無法有效整合 Splunk。切換至 Corelight 後,Zeek 日誌直接進入 Splunk,威脅獵捕效率提升 5 倍,年度總成本降低 45%。

10.3 CrowdStrike 客戶擴展 NDR 能力

某製造業客戶已導入 CrowdStrike Falcon,但 OT 環境、印表機、IoT 裝置無法安裝 Agent。導入 Corelight 後,完整覆蓋 3,500+ 無 Agent 裝置,並在 Falcon 介面中直接關聯網路證據。

10.4 Microsoft Sentinel 客戶強化網路偵測

某跨國集團全面採用 Microsoft Sentinel,但網路偵測依賴日誌,遇到 IoT、雲端東西向流量完全盲目。整合 Corelight 後,Sentinel 收到結構化網路證據,預建 100+ 個偵測規則立即可用。

10.5 OT / ICS 環境可視性

某電力業客戶需監控 SCADA / ICS 環境,但無法在 PLC、RTU 上安裝任何 Agent。Corelight 支援 DNP3、Modbus、S7comm、IEC 104 等工業協議,被動式監控完整呈現 OT 網路活動。

10.6 雲端東西向流量監控

某 SaaS 公司在 AWS 多區域部署,擔心 Pod-to-Pod、Service-to-Service 流量缺乏可視性。透過 VPC Traffic Mirror + Corelight Cloud Sensor,完整記錄雲端內部流量,偵測 supply chain 攻擊的橫向擴散。

十一、導入流程與最佳實務

SaaSPodium 提供標準化的四階段 Corelight 導入方法論,典型週期 6-10 週:

階段	時程	主要活動
Phase 1 Assess	第 1-2 週	網路架構盤點、SPAN/TAP 部署規劃、Sensor 規格選型、資料流向設計(到 SIEM/XDR)、Use Case 優先排序。
Phase 2 Deploy	第 3-4 週	Sensor 部署(地端/雲端/虛擬)、網路鏡像設定、初始測試、Investigator SaaS 啟用、SIEM 整合連線建立。
Phase 3 Tune	第 5-8 週	偵測規則校調、業務情境客製化、與 CrowdStrike/Sentinel 深度整合、Playbook 建立、團隊培訓。
Phase 4 Operate	第 9 週及之後	正式營運、持續優化、新 Use Case 擴展、季度健檢、威脅獵捕工作坊。

導入最佳實務

- **優先覆蓋關鍵網路節點** — 先部署於資料中心核心、Internet Edge、關鍵業務區段,不求一次全網覆蓋
- **與既有 SIEM/XDR 整合作為第一優先** — 讓 Corelight 資料流入 SOC 日常工作流,確保價值立即可見
- **投資 Threat Hunting 人才** — Corelight 最大價值在於 Tier 2/3 的深度分析能力,需有人才發揮
- **建立 OT/IT 聯合工作小組** — 若覆蓋 OT 環境,需 IT 資安與 OT 維運密切合作

十二、商業價值與 TCO 分析

以下為典型中大型企業(5,000 員工、地端 + 多雲、日均流量 5 Gbps)導入 Corelight 後的商業價值分析:

指標	導入前	導入 Corelight 後
網路可視性覆蓋率	40%(僅端點 + 日誌)	**95%+(含 IoT、OT、雲端東西向)**
平均威脅偵測時間(MTTD)	22 天	**4 小時**
平均事件調查時間	8-12 小時	**1-2 小時(證據即時可查)**
Threat Hunting 能力	有限	**成熟 Tier 3 能力**
加密流量盲區	95% 流量無視野	**透過 JA3/JA4 完整分析**
SIEM 資料費用影響	基準	**減少 30-40%(結構化資料更有效率)**
合規舉證能力	依賴日誌拼湊	**完整網路證據鏈**
典型投資回報	—	**6-12 個月達正向 ROI**
年度 TCO(對比 Darktrace)	假設 USD 900K	**USD 480K-600K(-35%)**

綜合而言,Corelight 不只是新增一個偵測工具,而是根本性改變 SOC 的工作模式與成熟度:

- 從被動告警處理轉為主動證據分析
- 從片段式事件拼湊轉為完整攻擊鏈還原
- 從依賴黑箱 AI 轉為可驗證的網路真相
- 從單一廠商鎖定轉為開放式 SOC 架構

十三、SaaSPodium 的服務承諾

作為 Corelight 在台灣與亞太區的授權代理商,SaaSPodium 提供完整的 Corelight 解決方案服務:

- **免費 Network Visibility Assessment** — 協助企業評估現有網路可視性成熟度、識別盲區、量化威脅偵測缺口。
- **Corelight 授權與硬體諮詢** — 依網路規模、流量特徵、雲端比例、產業需求,提供最適合的 Sensor 組合與授權方案。
- **結構化 POC 服務** — 提供 4 週 POC,以企業實際網路流量驗證 Corelight 偵測與整合效能,對比既有工具。
- **導入顧問服務** — Corelight 認證工程師協助完成 Sensor 部署、SPAN/TAP 規劃、SIEM/XDR 整合、規則客製化。
- **從 ExtraHop / Vectra / Darktrace 遷移服務** — 針對現有使用其他 NDR 的企業,提供並行驗證、規則對照、資料遷移。
- **與 CrowdStrike / Microsoft 聯合部署** — 具備 CrowdStrike Falcon 與 Microsoft Sentinel 的整合經驗,提供一站式部署服務。
- **Threat Hunting 工作坊** — 協助企業培育 Tier 2/3 威脅獵人,充分發揮 Corelight 的深度分析能力。
- **中文技術支援** — 繁體中文技術支援窗口、季度健檢、新功能導入諮詢。
- **Cloud-Native Security Pack 整合方案** — Cycode + Upwind + Cribl + Corelight 完整現代化雲端資安堆疊,提供一站式架構諮詢。

結語

NDR 的戰場正在重新定義。過去十年,業界被「AI 偵測」的行銷主宰,但成熟的 SOC 團隊逐漸認知到:沒有證據的 AI 告警,不是資安,是雜訊。

Corelight 以 Zeek 為核心、以 Evidence-First 為哲學,為現代 SOC 提供的不只是又一個偵測工具,而是:

- 可信賴的網路真相,不再被黑箱告警主導
- 可驗證的偵測邏輯,SOC 可檢視、可客製、可擴展
- 可查詢的完整證據,支援 Tier 1 處置、Tier 2 調查、Tier 3 獵捕
- 可整合的開放架構,與 CrowdStrike、Microsoft、Splunk、Google SecOps 等生態共榮

SaaSPodium 作為 Corelight 授權代理商,擁有完整的售前諮詢、導入實施、長期支援能力,協助企業從 NDR 評估、POC、部署到威脅獵捕成熟,建立現代化的網路偵測與回應架構。

下一步:看見網路上真正發生的事

免費 Network Visibility Assessment | 4 週 POC | NDR 遷移諮詢

SaaSPodium 拓維雲智資安顧問團隊

Authorized Distributor of Cribl, Corelight, Cycode and Upwind | Freshworks Premier Partner | Device42 Distributor