ANOMALI®

管理威脅情資
教戰手冊

助您評估、選擇、管理以及最佳化威脅情資平台
(Threat Intelligence Platform:TIP) 的指南

索引

第 1 章：前言

威脅情資平台是什麼？

資安威脅者(Threat Actors)的攻擊手法不斷進化與進步。威脅組織試圖利用威脅情資來瞭解這些攻擊的背景資訊，這些都是攻擊者及其策略、技術和程序 (TTP) 的可採取行動之資訊。威脅情資平台 (TIP) 是一套全面整合威脅情資分析流程、並將耗時的風險偵測作業自動化的解決方案，能大幅減少資安事件對應所需的時間，讓分析師能夠在整合的環境中調查、並迅速回應不同的資安威脅，並且與和企業內部的不同功能的資安團隊進行合作。

運用威脅情資來幫助資安事件偵測和預警

Ponemon Institute 近期針對 IT 專業人員進行調查，詢問受訪者如何利用威脅情資，進行資安事件分析的相關資訊。

- **85%** 的 Ponemon 調查受訪者表示，**威脅情資**對於建立精實的企業資安架構至關重要，但只有 **41%** 的受訪者表示**自己的單位能夠有效地偵測並對應來自外部的資安威脅**。
- 不到**半數或 48%** 的 Ponemon 受訪者擁有**專屬的威脅情資平台**。
- 僅有 **33%** 的 Ponemon 受訪者表示他們**有足夠的預算可進行威脅偵測**。

資料來源：威脅情資的價值：北美與英國公司的年度研究，Ponemon Institute，2019 年

第 1 章：前言

威脅情資平台與其他安全解決方案有何不同：

- ***根據我們彙總來自於不同的資訊對象的結果***：大多數的安全解決方案僅著重於其環境內部的資訊。而成熟的威脅情資平台，會主動消化並建立外部情資，和內部事件資料的關聯，提供資安人員對於已知、以及潛在的威脅更全面的洞見。
- ***對資料進行彙整 (curation)、標準化(normalization)、追記細節 (enrichment)，以及風險評分(risk scoring)***：透過人工方式建立來自個別入侵指標 (Indicators)的威脅情資報告和概況，是一項繁重且耗時的程序。威脅情資平台能將以上程序的絕大部分自動化，幫助分析師大幅減少花在彙整和清理資料的時間，而將更多的資源專注於提供高精確度的資安判斷，以實現主動式防禦的目標。
- ***與現有的安全系統整合***：許多資安廠商試圖取代其他系統。而威脅情資平台 (TIP) 則是與您現有的解決方案直接整合，提高整體資安安全解決方案的綜效。
- ***分析與共享威脅情資***：威脅情資毫的價值，隨著與其他專業資安團隊的分享而倍增。透過情資平台來安全地共享威脅情資，能幫助企業建立更完整、更可靠的聯防預警，以便快速回應任何潛在的威脅風險。

威脅攻擊者會重複利用眾多的滲透手段 (TTP)，鎖定背景類似和企業組織、以及和基礎設作為攻擊目標。您對惡意攻擊者相關資訊與背景資訊瞭解愈多，安全團隊就能愈快、且愈有效地阻絕這些惡意攻擊可能造成的傷害。

第 1 章：前言

威脅資料來源一覽

威脅情資平台的設計理念，是善用各種不同的內容和格式威脅情資來源，並且將其去蕪存菁。資安團隊會根據所處企業的資安目標和相關的風險，佐以不同類別的威脅情資，以來判斷並進行主動防禦。

典型的資料來源包括：

- ***第三方獨立研究的情資內容***：資安廠商所銷售的威脅情資，一般著重於國家支援的網軍或的專門的攻擊組織、以及深網與暗網的動向。這類摘要通常包含更全面、而且難以取得的獨家資訊。
- ***開源的威脅情資(Open Source Feeds)***：開源的威脅情資是來自個別資安研究人員或單位、以及資安廠商公開發表並共享的免費資訊。內容包含阻絕名單(Block list) 等的訊息。
- ***威脅共享群組 (Threat Sharing Group)***：例如資訊分享分析中心 (ISAC) 等威脅共享群組，會和通過審查的成員分享產業相關的威脅資料。
- ***開放原始碼分析平台***：MISP 是開放原始碼的惡意軟體資訊共享平台。雖然 MISP 欠缺完整的威脅情資平台功能，但對於僅需要蒐集、分享、並建立 IOC 關聯資料庫的人員而言，可以視為一項入門的的選擇。
- ***社群知識庫***：MITRE ATTACK™ 架構
  是現今非常受歡迎的網路安全框架 (Framework) 之一。這是一套開放給所以資安人員的知識庫，內容提供根據實際觀察所得的攻擊者策略與手法匯整而成。此架構也可被運用於私人企業、政府及網路安全產品與服務社群中，並發展成特定威脅模型與方法的基礎。

Anomali 幫助改善並分析所蒐集到的情資，並提昇我們的使用者對於威脅風險的了解。從而讓使用者能更準確地辨識組織內外部潛伏的威脅，並增加資安應對的時效性。

IT 專業人員 | 航太與國防

第 2 章：威脅情資平台能因應哪些挑戰？

將威脅資料自動化，以利更快速的洞見分析

網路安全攻擊的數量與複雜度與日俱增。各組織需要確切瞭解所面對的威脅為何，才能主動解決威脅，並判斷如何更有效地因應事件。

分析師會檢查各種安全解決方案的警示，通常來自安全資訊與事件管理 (SIEM) 系統，以找出攻擊的證據。然而由於 SIEM 的設計是為了處理和儲存組織的所有資料，因此產生的許多警示並不是真正的威脅。通常這些誤判並不代表真正的惡意攻擊事件，但卻會浪費寶貴的資源來調查警示。

更由於員工人數本就有限，這些誤判可能會對資安團隊帶來極大的負荷。威脅情資可協助分析師篩選這些警示，並將所收錄的威脅情資與內部威脅標記建立關聯，藉此驗證這些警示。

威脅情資本身可能帶來許多挑戰。IOC 的數目可能高達數百萬，而辨識相關內容的所需要的過程也相當耗費人力。威脅情資平台的設計，能自動援尋出所輸入資料的相關性，以便更快速地洞悉真正的網路威脅。

目前在職場上約有 350,000 個網路安全相關的職缺，
且預計在 2021 年以前，全球將會有近 350 萬個網路安全工作的職缺

資料來源：Cyber Security Ventures

第 3 章：威脅情資平台應具備哪些功能？

威脅情資的常見使用者

威脅情資平台的設計，是為了讓分析師減少花費在手動管理資訊上的時間。原始資料會轉換成完整的情報，簡單易懂、容易分享，而且最重要的是，這些資料都能作為行動的依據。透過情報蒐集、自動分析，以及與現有的資安產品整合，企業組織就能夠瞭解與自身相關的威脅風險。威脅情資平台的最常見使用者包括：

- 威脅情資分析師 (Threat Intelligence Analysts)
- 資安監控中心 (SOC) 的資安分析師
- 網路威脅獵捕師 (Cyber Threat Hunters)
- 事件應變 (IR) 分析師 (Incident Response Analysts)
- 資安長 (CISO)

第 3 章：威脅情資平台應具備哪些功能？

資料彙總和整理

威脅情資平台會自動從多個來源蒐集威脅資料、資訊和情報。資安分析師應具有可設定自訂資料匯入的彈性，同時能快速擷取來自廠商或信任之第三方的資訊。接著，此情報資料庫將會導入調查和其他安全工具。

威脅情資平台(TIP)所蒐集到的資料，可能包含許多重複、以及不再具有惡意，或者是風險已降低到不足以採取行動的威脅情資。威脅情資平台(TIP) 具備機器學習演算法，可根據與網路威脅相關的眾多因素，為資訊進行分類、並衡量個別的 IOC的風險性。收錄的指標會以容易閱讀的格式呈現，並提供風險分數和相關情報。

我們根據關聯式標記(tags)和IOC 類型來擷取、加強並整合資訊的能力，大幅提昇了我們的SOC 在應用威脅情資上的效率。再加上透過自動化整合後進行的分層處理，我們的整體效能更是大幅躍進

SOC 主管| 能源與公用事業

第 3 章：威脅情資平台應具備哪些功能？

調查

威脅情資分析師負責調查威脅，並建立新的威脅情資來為資安策略提供指引。這類分析通常需要數十種工具和無數小時來完成。

威脅情資平台(TIP)能讓分析師透過自動化、可擴充的工作流程來進行調查，並與不同的團隊協同合作。分析師可管理已知的 IOC 和樞紐(Pivot)以調查未知的威脅。在同一項調查中，分析師可將指標與情報建立關聯，建立相關觀察與威脅簡報，並辨識出威脅攻擊者及其 TTP。

第 3 章：威脅情資平台應具備哪些功能？

自動化

威脅情資平台(TIP)的設計是要充分利用機器和人類雙方的優勢。自動化可減少人為錯誤，避免分析師出現「警示疲勞」，並讓資安團隊有足夠的時間和資訊，對網路威脅做出進階的判斷。

牽涉到大量資料的耗費人力與重複之程序已完全自動化。這包括移除重複的資料、將不同格式合併為易於閱讀的資訊、並以額外的資料來強化指標(IOC)內容，然後再與現有的資安解決方案整合。

Anomali 可讓我們處理從多個情報資源產生的大量資料，並識別與我們組織相關的威脅。現在我們能更快速地匯入威脅資料、為風險建立相關性，並將真正有需要的指標匯出到我們的 SIEM 中，以進行主動式的資安威脅管理與應對。

情報分析師| FinServ

第 3 章：威脅情資平台應具備哪些功能？

整合

威脅情資平台(TIP) 是在資訊與您現有安全解決方案之間的中間人，且不需要手動設定連線。這些指標會傳送到防火牆、以及入侵偵測系統(IDS/IPS)進行主動封鎖、並建立 SIEM 和端點解決方案中的資訊關聯，以排定警示的優先順序，並傳送到協調平台以改善工作流程。

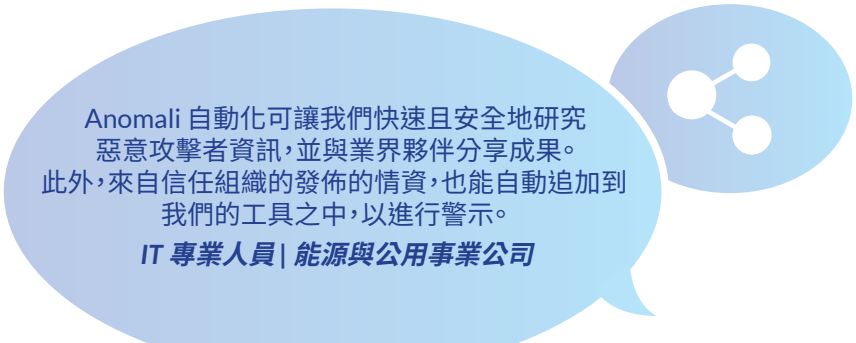
這些整合的彈性能快速改善資安團隊辨識、以及抵禦威脅的能力。無論組織的資安架構是全雲端式(cloud-based)、還是內部部署(on-premises)、或者兩者兼具的任何組合，都能完整地對應。

第 3 章：威脅情資平台應具備哪些功能？

協同合作與共享

組織更能預測攻擊者策略、辨識惡意行為，並利用詳細且情境化的威脅情資來封鎖攻擊。資安團隊可與其他團隊合作，以建立情報並透過分享來保護社群，進而提升其防禦能力。

TIP 有助於合作調查，並能即時雙向共享情報。如資訊分享分析中心 (ISAC) 的共用群組，通常會利用威脅情資平台讓相似產業類別的公司密切合作，協助組織從廣泛資源與專業知識中獲益。



雖然 59% 的受訪者表示其組織會與他人分享威脅情資，但 56% 的受訪者表示他人可能會濫用資料，因此他們不願意分享威脅情資。

資料來源：威脅情資的價值：北美與英國公司的年度研究，Ponemon Institute，2019 年

第 4 章：如何將威脅情資管理融入資訊安全的生命週期

建立強而有力的資安防禦是一種週而復始的過程。然而，嘗試改善資訊安全的生命週期中的所有程序，例如規劃、監控、偵測、分析、應變、補救和意見回饋，可能會讓您疲於奔命。威脅情資可透過提供背景資訊來支援各個階段，以協助引導這些行動，使其更快速且更具目標性。

規劃

資安團隊必須為所有可能性做好規劃。他們會根據自家生產的產品或服務、在處的地理位置、政治立場等等，來評估組織最可能面臨的威脅風險為何。威脅情資使這些團隊能夠證明或找出推翻其理論的證據。分析師可更清楚掌握哪些威脅與其相關，以及這些威脅攻擊者的攻擊手法。除了分析這些資料、資訊和情報之外，TIP 還可讓分析師了解哪些工具最能有效預防與應對特定的網路攻擊，並加以利用。

監控與偵測

偵測並監控惡意行為的方法有數種，但結合使用威脅情資是主動防範這些威脅的唯一之道。引進經過驗証的外部的情資，來確認威脅攻擊者的背景資料及手法(TTP)，讓資安分析師不再需要自行先累積大量的研究，來判斷哪些項目屬於或不屬於惡意行為。組織可將威脅情資與現有資安系統的資料建立關聯，快速辨視出這些惡意指標是否存在。任何被識別為可疑的事件，都會自動傳送給整合系統進行監控。如此一來，現在的資安產品和人員，就能在威脅進入網路***之前***先行封鎖攔截。

第 4 章：威脅管理如何融入資訊安全的生命週期

調查與分析

一旦發現惡意侵入的跡象，分析師便會進行調查，以判定其組織所受到的影響。威脅情資平台(TIP)提供完整的工作流程，讓分析師能檢查證據、並連結不同片段的資訊。分析師從個別的 IOC、進而查詢 WHOis 資訊、PassiveDNS 等，以找出先前未知的威脅。

應變與補救

在事件發生時，威脅情資平台(TIP) 可協助分析師識別模式和相關的威脅攻擊者，以便更快速地告知補救和應變作業。例如，TIP 可會匯報不同的攻擊者常用的特定工具或策略，以幫助資安分析師進行更精準的事件調查。

Anomali 幫助我們將指標擷取作業自動化，因此分析師有更多時間可利用 Anomali 提供的資料來快速調查、並了解資安事件的來龍去脈。

情報分析師 | FinServ

第 4 章：威脅管理如何融入資訊安全的生命週期

意見回饋

意見回饋階段對於改善您目前的安全性至關重要。威脅情資平台對於評估需改進之處非常實用，因為它們介於工具與資訊之間。

需考量的關鍵領域包括：

- ***監控階段***，以判斷哪些情資來源對辨識及封鎖威脅最有幫助。
- ***偵測和分析階段***，以記錄得出結論所花費的時間。
- ***應變與補救階段***，以判定是否已擁有正確資訊，以及應變所需時間。例如，若惡意攻擊者成功感染系統，TIP 使用者可以查看該威脅的相關資訊是否已存在於資料庫中，若不存在，則是否有其他來源包含該資訊。

第 5 章：Anomali®

使用 Anomali 管理威脅情資

Anomali 利用威脅資料、資訊和情報來制定有效的網路安全決策。本平台能自動化偵測、排定優先順序，並分析出哪些是對於您組織最威脅性的風險。Anomali 採用機器學習、自動化處理、以及龐大的合作夥伴生態系統，讓分析師充分運用威脅情資來徹底地洞悉與因應網路攻擊。

以下三個元件是 Anomali 平台的一部分。

- **ThreatStream®** 是為分析師打造的威脅情資平台，可建立威脅情資並調查安全事件。透過機器學習來蒐集、釐清脈絡、並將複雜的大量指標進行風險評等，以排定警示的優先順序，並為安全策略提供指引。
- **Anomali Match™** 是一套針對企業環境進行高速、自動化的資安事件檢測而打造的威脅偵測引擎。Anomali Match 可將十二個月的元數據(metadata)，與主動式威脅情資建立關聯，以向您揭露任何未被發覺的潛伏威脅。
- **Anomali Lens™** 讓威脅與資安分析師能夠更快速且更精確地做出決策。Anomali Lens 可從任何行動裝置或瀏覽器頁面立即存取策略性(strategic)和戰術(tactical)情報。所有層級的分析師都能獲得即時分數和背景資訊，加速決策過程。主管人員也可以輕鬆得知對於該威脅情資，本身的對應狀況，以隨時掌握企業的最新威脅。

Anomali 優勢

- 辨識對於貴組織的目標式威脅
- 自動化威脅偵測與分析
- 洞悉威脅攻擊者和行為，藉此強化應變能力
- 減少攻擊的影響，節省時間與資源
- 允許內外部 CTI 群組之間進行協同作業

Anomali 隨時提供我們最新網路威脅情資及所有必要資訊，使我們的安全作業更上一層樓。我們因而能夠更有效地保護組織，預防不斷出現的威脅。

IT 經理 | 電腦服務公司

第 6 章：個案研究

科羅拉多威脅情資分享 (CTIS) 個案研究

2017 年，科羅拉多州與 Anomali 合作組成科羅拉多威脅情資分享網路 (CTIS)，連結州、郡、市政府與部落政府，讓資安團隊能共享、分析，並更有效地因應威脅。

挑戰

科羅拉多州難以建立安全的入口網站，讓當地社區分享重要的網路安全資訊。先前透過電子郵件分享資訊的方式既不安全、也缺乏主動合作機制，而且無法因應緊急狀況。在缺乏流暢、安全的威脅情資共享環境之下，導致各個州部門失去能防範並抑制網路攻擊的重要資訊。

解決方案

科羅拉多州與 Anomali 合作，提供一套全方位的威脅共享與分析平台，讓州政府所有部門，都能在一個單一、中央控管的環境來共享機密資訊。此入口網站為地方政府提供更高的資訊掌握度，並透過經完整審查的使用者之間所建立可信社群 (Trusted Circle)來即時分享潛在威脅的相關資料。

主要優勢

- 所有地方、部落、郡及各州部門均可透過科羅拉多州存取流暢安全的威脅共享功能。
- 能透過與其它各州的 ISAC進行協同合作並分享情報。
- 強而有力的威脅調查工具群組，讓安全分析師能迅速評估並瞭解攻事件。

「我們在科羅拉多州開發 CTIS，是為了因應推動更廣泛分享網路威脅的關鍵需求。」科羅拉多州資訊長 Trevor Timmons 表示。「我們發現州內各政府層級，現在都能快速運用情資，且不同部門和各郡都有積極的合作關係。我們強烈鼓勵各州實施網路威脅情資共享計畫，以強化其資安防禦。」

取得白皮書 »

第 6 章：個案研究

聯邦系統整合(Federal System Integrator) 個案研究

聯邦系統整合(FSI) 是提供資訊系統、工程設計與分析解決方案的科技廠商，備受美國情報體系、美國國防部、與其他聯邦機構的肯定。FSI 擁有超過 40 年的經驗，能夠設計、開發及提供具高度影響力的關鍵任務服務與解決方案，協助客戶克服最複雜的難題。

挑戰

身為處理客戶機密情報、以及情資單位的系統整合方案的開發商，FSI 的智慧財產 (IP) 包含重要的高價值資訊。此 IP 對美國政府而言極為重要，必須持續受到保護並確保其安全。

解決方案

因此 FSI運用 ThreatStream自動化網路威脅情資平台為其解決方案。ThreatStream™ 平台能將可據以行動的情報、與現有的資安基礎設施加以整合，來對攻擊者進行反制。

主要優勢

- 整合及彙整多個威脅情資來源，同時排除冗餘項目
- 提供交叉驗證分析
- 快速運用高可信度的情報

「使用 ThreatStream 讓我們能更有效率地進行防禦，不論是最簡單的網路攻擊，或是每天嘗試入侵公司資產的縝密攻擊行為。」Federal Systems Integrator CISO。

閱讀完整的個案研究 »

第 6 章：個案研究

阿聯銀行協會 (ISAC) 個案研究

阿聯銀行協會 (ISAC) 是一個代表在阿拉伯聯合大公國 (UAE) 營運的 50 名成員銀行之非營利組織，也是 UAE 銀行業的領導級產業協會。

挑戰

網路攻擊的頻率和複雜度不斷攀升，對組織和整個產業帶來重大挑戰，這些組織必須保護資料和系統，避免遭受強大的攻擊。由於網路威脅攻擊者與群組共享他們的工具、技術和程序 (TTP) 來攻擊和滲透組織，因此保護企業網路和關鍵基礎設施的人員必須使用相同方法，以受信任、安全且有效的方式與同儕協同合作。

解決方案

2017 年 9 月推出的 UBF Tasharuk 計畫，採用 Anomali 的旗艦產品 ThreatStream。 阿聯銀行協會會員使用此平台在各區域金融機構之間分享相關、及時且可據以行動的情報。Anomali 對資訊分享分析中心 (ISAC) 所承諾的加值元件，是稱為「Anomali：威脅分析中心 (A-TAC)」的情報研究團隊。

主要優勢

- 強化對 UAE 銀行業網路威脅的情境意識
- 由業者組成的集中式經審查社群，著重於集體安全目標
- 改善整體產業對網路攻擊的資安態勢和恢復能力

「透過推出 Tasharuk，我們就能讓參與銀行的反網路犯罪工作更加精簡，並讓他們瞭解潛在的惡意威脅，以強化他們的防禦系統。」HE Abdul Aziz Al Ghurair，阿聯銀行協會主席。

查看部落格 »

第 7 章：結論

網路罪犯、國家級攻擊者和駭客，無時無刻都在嘗試找出目標的組織弱點帝進行滲透。瞭解自身弱點、預先防範威脅、並對事件迅速進行補救，對您的組織而言極為重要。

然而，雖然您可能已從內部安全系統和外部威脅摘要蒐集大量資料，但是手動輸入這些資料會耗去您大量的資源，更何況還必須花費額外的人力來處理大量的誤判和漏判。調查所有此類事件會因為網路安全人才短缺，而快速癱瘓已是緊繃狀態的資安團隊。

TIP 將整合及分析內外部威脅資料、資訊與情報的程序自動化，提供可作為行動依據的威脅情資、加速並簡化整個資訊安全的生命週期。不論是辨識相關的 IOC 並準備因應、監控、偵測及分析威脅、回應事件，或是想改善安全作業，TIP 皆能提供所需的背景資訊，以更快速且有效地預防及解決威脅。

Anomali 幫我們減少了80% 的誤判率，成效相當於多了兩名全職的資安人員。

IT 總監 | 醫療保健

讓 Anomali 協助您達成威脅情資和管理目標。

進一步瞭解

ANOMALI 每週威脅摘要

免費 STIX/TAXII：STAXX

申請試用版

ANOMALI®

網站：www.anomali.com

聯絡我們：**+1 844-4-THREATS** (847328)
+44 8000 148096 (國際免付費電話)

Anomali® 提供情報導向的網路安全解決方案。組織仰賴 Anomali 平台來利用威脅資料、資訊與情報做出有效的網路安全決策、降低風險並強化防禦能力。Anomali 利用機器學習最佳化威脅情資、以此支援資安團隊辨視出潛伏的威脅。Anomali 平台可讓組織在信任的社群之間協同合作並分享威脅資訊，是全球 ISAC 和跨國企業最廣為採用的平台。如需更多資訊，請造訪 www.anomali.com，並追蹤我們的 Twitter @Anomali。

808 Winslow Street, Redwood City, CA 94063