iSecurity
The Hub of Security Innovations

Find & Fix breaches faster

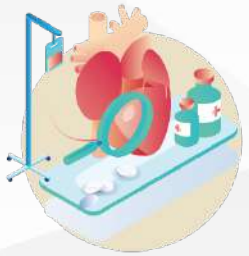
資安人手不足，您的資安維運中心有跟上數位轉型的腳步嗎?

數位資安 Philis Tseng

iSecurity數位資安CyberResillence

強化企業資安體質
為未知威脅做好準備

1 Stop More Attacks
超前部署，拒敵於境外



2&3 Find & Fix breaches faster
次世代資安維運中心

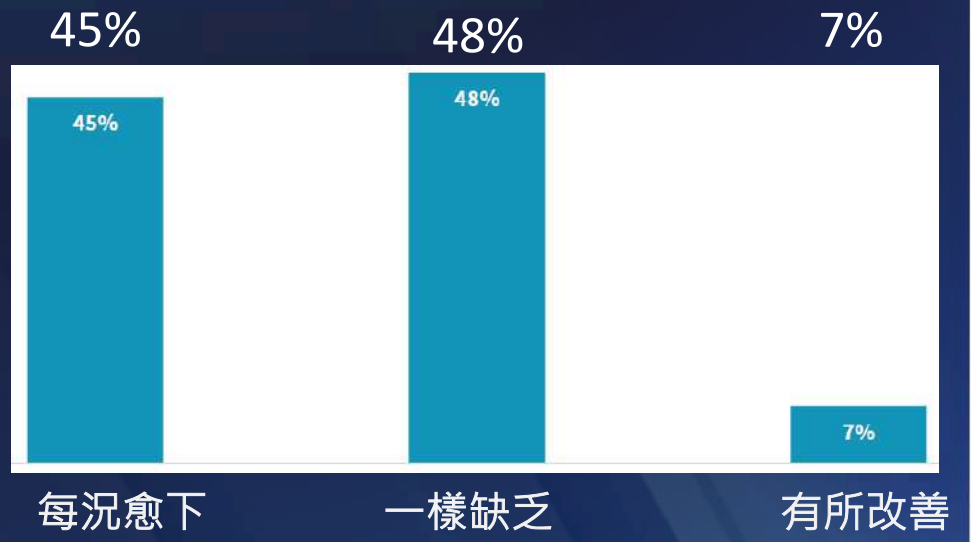
4 Reduce breach impact
阻絕擴散降低損害

iSecurity
The Hub of Security Innovations

- Enterprise Strategy Group is an integrated IT research, analyst, strategy, and validation firm that offers market intelligence, analysis, and consulting services.

- Information Systems Security Association (ISSA) is a not-for-profit, international professional organization of information security professionals and practitioners.

資安人力短缺造成組織業務影響



The data base on Cooperative Research Project by ESG and ISSA
The Life and Times of Cybersecurity Professionals 2020

ESG & ISSA 研究報告

After 10 Years, Why Has Nothing Changed?

過了十年，為何沒有任何改變?

ESG

ISSA
Information Systems Security Association International

iSecurity
The Hub of Security Innovations

資安維運中心的挑戰

資安人力短缺

缺乏具備足夠經驗的資安從業人員,影響組織能有效改進資安運作效率與處理機制

不斷演變的新型威脅

日新月異的攻擊手法不斷地出現,複雜程度也同步升高,增加偵測抵擋的難度

資安事件分級分類

在人力資源有限的情況下,資安事件卻是無限的增加,如何有效地分辨事件分級分類,避免誤報以及資源的浪費

需要中央化的資安中心

組織需要一個有效率的中央化運作機制來評估資安的風險與威脅防護情形

過慢的響應時間

平均花費197天的時間發現嚴重的資安事件以及69天的時間進行Incident response,根據事件處理調查統計資料

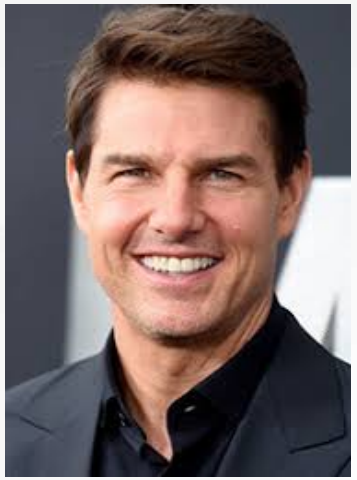
被動式的安全防護機制

現今大部分的組織仍是採取被動式的防禦機制,缺乏積極主動的威脅評估與改善進度

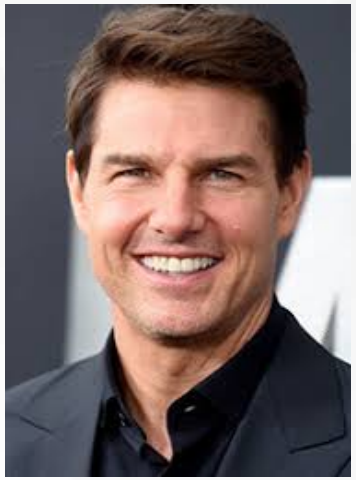
iSecurity
The Hub of Security Innovations

資安團隊人力配置

SECURITY ANALYST
資安分析師
負責使用資安工具分析事件與流程來提供資安的防護機制。 涵蓋多階層L1、L2 、 L3的角色。



SECURITY ENGINEER
資安工程師
協助資安工具的測試與導入,監控安全系統與網路運作,執行漏洞修補、安全防護系統等相關作業



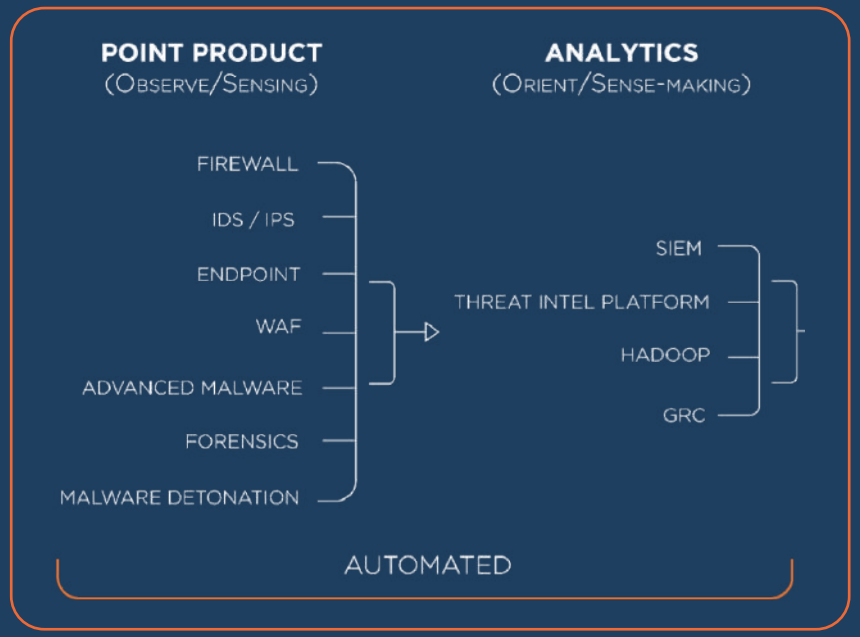
SECURITY ARCHITECT
資安架構師
資安解決方案的整體評估、架構規劃、分析制定流程與前期導入的內部教育前導資深人員

CISO/CIO
資安長
建立資安團隊短中長期發展規劃,制定資安策略、衡量準則、服務提供、人員管理等管理規劃

iSecurity
The Hub of Security Innovations

現今的資安維運中心工作流程

前端資安監測　　後端分析工具



前端資安監測：負責監控各式系統與網路的資安設備,將可疑事件Alert送到後端分析工具SIEM等進行整合.

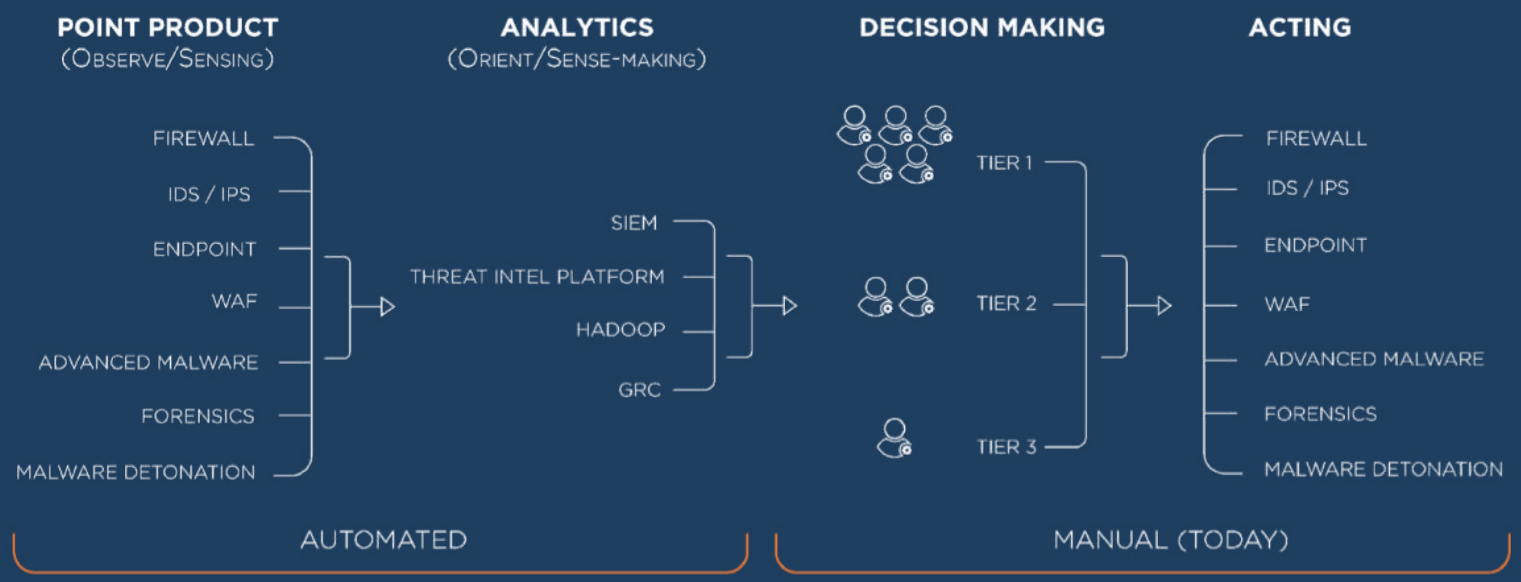
後端分析工具：將前端各式Alert等資訊進行關聯分析判斷.篩選Incident進行後續調查作業

以上皆為自動化Automated資安維運中心工作流程

iSecurity
The Hub of Security Innovations

現今的資安維運中心工作流程

前端資安監測　後端分析工具　事件決策過程　響應事件



是否該Escalate事件?　是否該進行Action調查?

是否該去協調響應Orchestration此事件的對應措施?

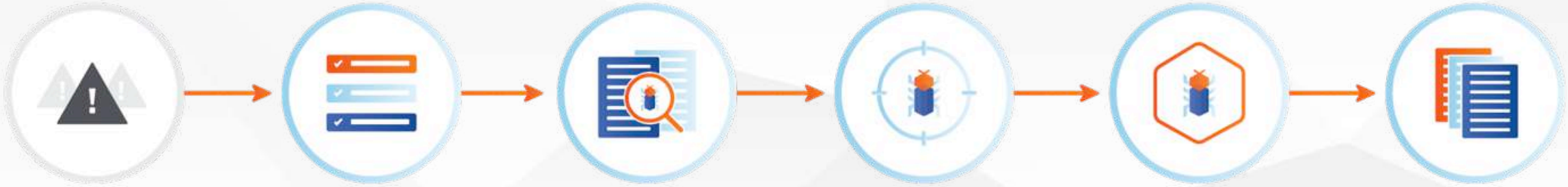
此階段完全需依賴資安人員的經驗判斷,大幅消耗資安團隊的資源,並且難以面對不斷產生的新資安事件進行對應動作,導致響應事件的時間持續的增長中

資安團隊需要進一步的自動化響應平台

缺乏Incident自動化篩選機制，排除False Positives等資源消耗!

需要協同聯合多重資安解決方案，降低Incident事件響應的時間!

建立統一的標準作業化流程，確保完整執行每一次事件的調查程序!



DETECTION

偵測與威脅發現

- Alert 進入SIEM 或 其他來源
- 開始建立Alert分析流程作業

TRIAGE

事件分級分類

- 分級分類機制啟動
- 資安分析師介入流程

INVESTIGATION

調查分析階段

- 事件升級至調查流程階段
- 收集端點與網路相關資訊分析

HUNTING

威脅獵捕

- 進行威脅獵捕作業探詢尚未發現的可疑影響範圍

CONTAINMENT

圍堵隔離

- 依據調查進度執行對應的圍堵機制
- 協調相關人員執行端點管控行為Action

REMEDIATION

修補作業

- 進行修復工程作業
- 檢視整體事件分析回報
- 關閉事件

SOAR資安協調自動化響應平台

Security orchestration, automation and response

Alerts from SIEM

SIEM告警自動化整合

Data整合

Enrich豐富化情資

Investigation 事件調查與升級

Orchestration

Reporting 事件報告

Data Ingestion	Data Enrichment Correlation Link Analysis	Incident Response Tier Escalation	Orchestration Notification Workflow Execution	Reporting

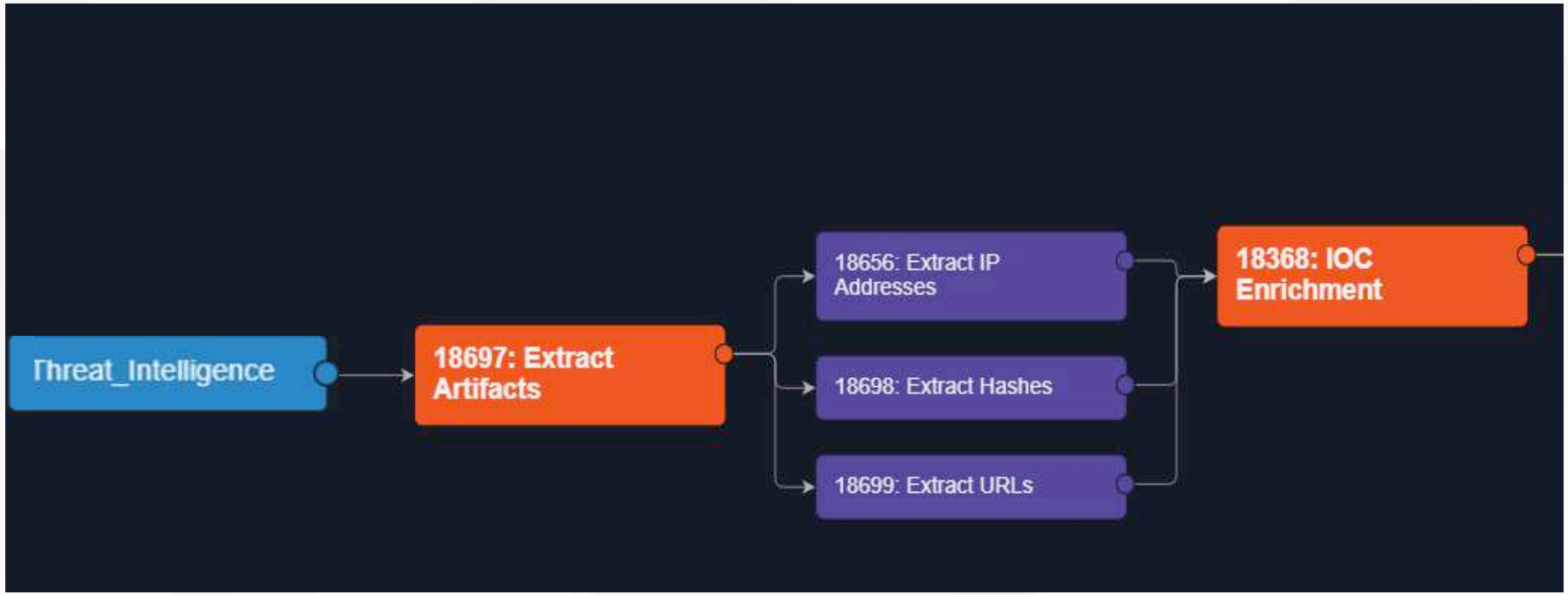
SOAR Use Case實際應用情境 - Threat intelligence威脅情資自動化調查

調查案例 ：

組織內部端點持續連線至可疑的外部網站，需要進一步分析事件的嚴重性
Intranet endpoint connect to malicious websites continually. Further investigation requiremented.

整合資訊	整合情境
Source來源	IOC (Hash, IP, URL/Domain)
Enrichment豐富化情資	IPSM (IP, network site, antivirus version) Threat intelligence (e.g. Virustotal, IBM X Force, …)
Response響應機制	Incident correlation report/dashboard Endpoint Product(e.g. add in black list) Mail

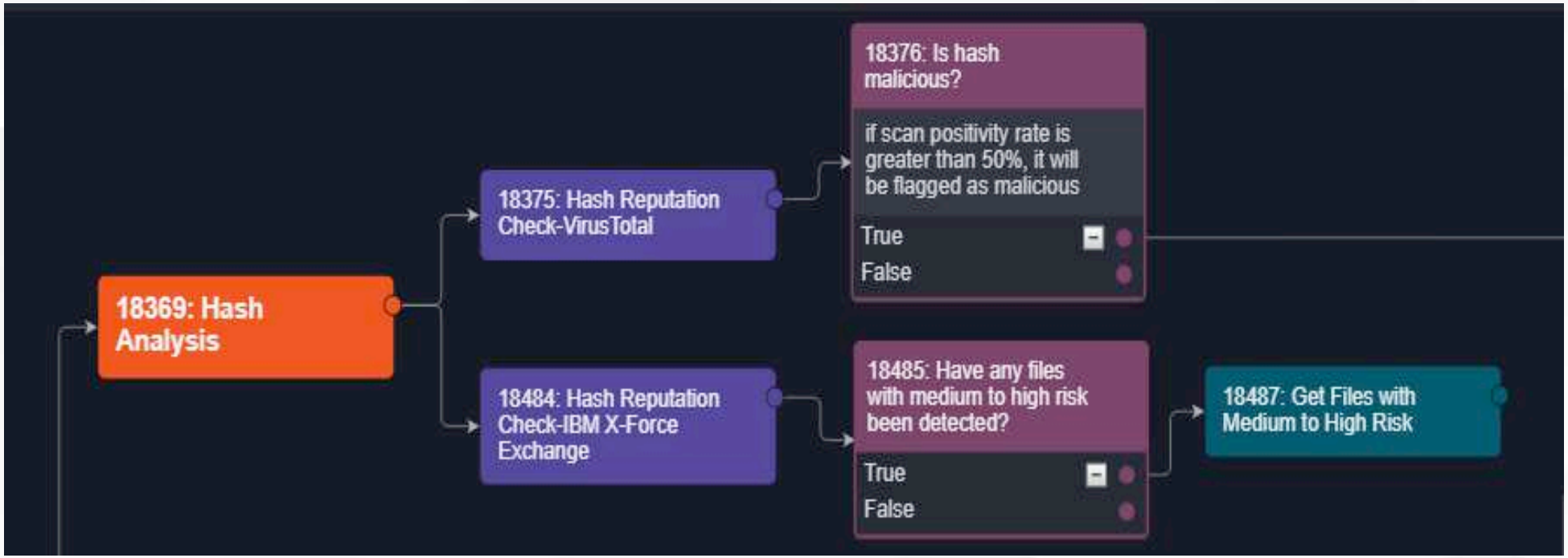
SOAR Use Case實際應用情境 - Threat intelligence威脅情資自動化調查



- 取出SIEM事件中的 IP, Hash, URL資訊

18656 : 取出事件中之相關 IP
18698 : 取出事件中之相關 Hash
18699 : 取出事件中之相關 URL

SOAR Use Case實際應用情境 - Threat intelligence威脅情資自動化調查



- Hash 情資分析

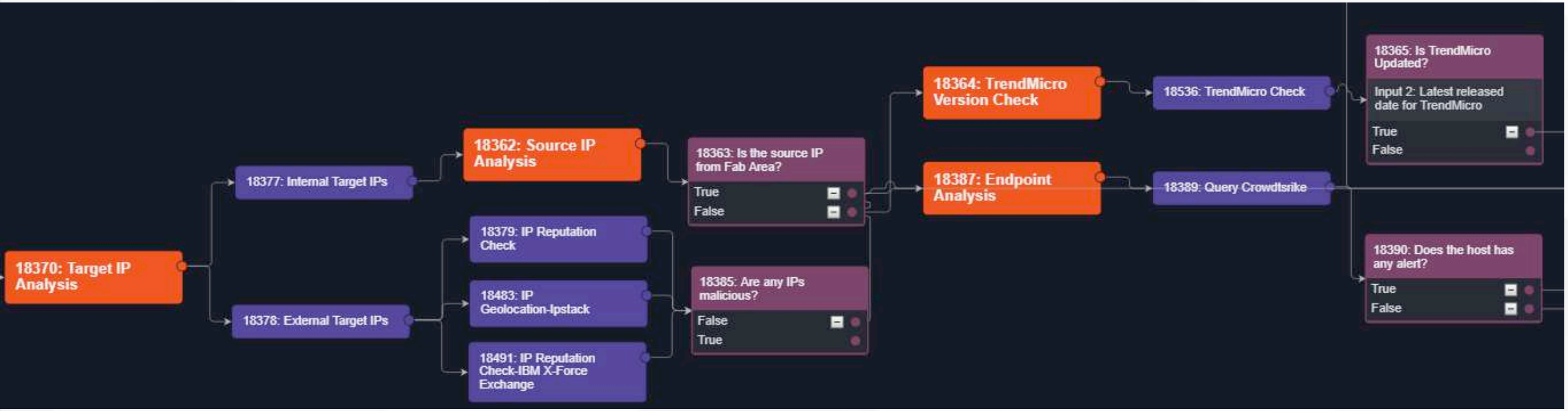
18376 : 確認該 Hash 是否為惡意

- Source : VirusTotal

18376 : 確認該 Hash 是否為惡意

- Source : IBM X-Force

SOAR Use Case實際應用情境 - Threat intelligence威脅情資自動化調查



- IP 情資分析

18363 : 確認該內部 IP 是否來自研發室部門

- Source : IPSM

18365 : 確認該內部 IP Antivirus版本是否更新至最新

18483 : 取得該外部 IP 之 Geolocation

- Source : IPstack

18491 : 取得該外部 IP 情資

- Source : IBM X-Force

- 端點情資分析

18390 : 確認該端點是否有產生 EDR 告警

- Source : EDR Product

iSecurity

SOAR Use Case實際應用情境 - Threat intelligence威脅情資自動化調查

- 取得 URL 情資

18381 : 取得 Whois 情資
- Source : Whois

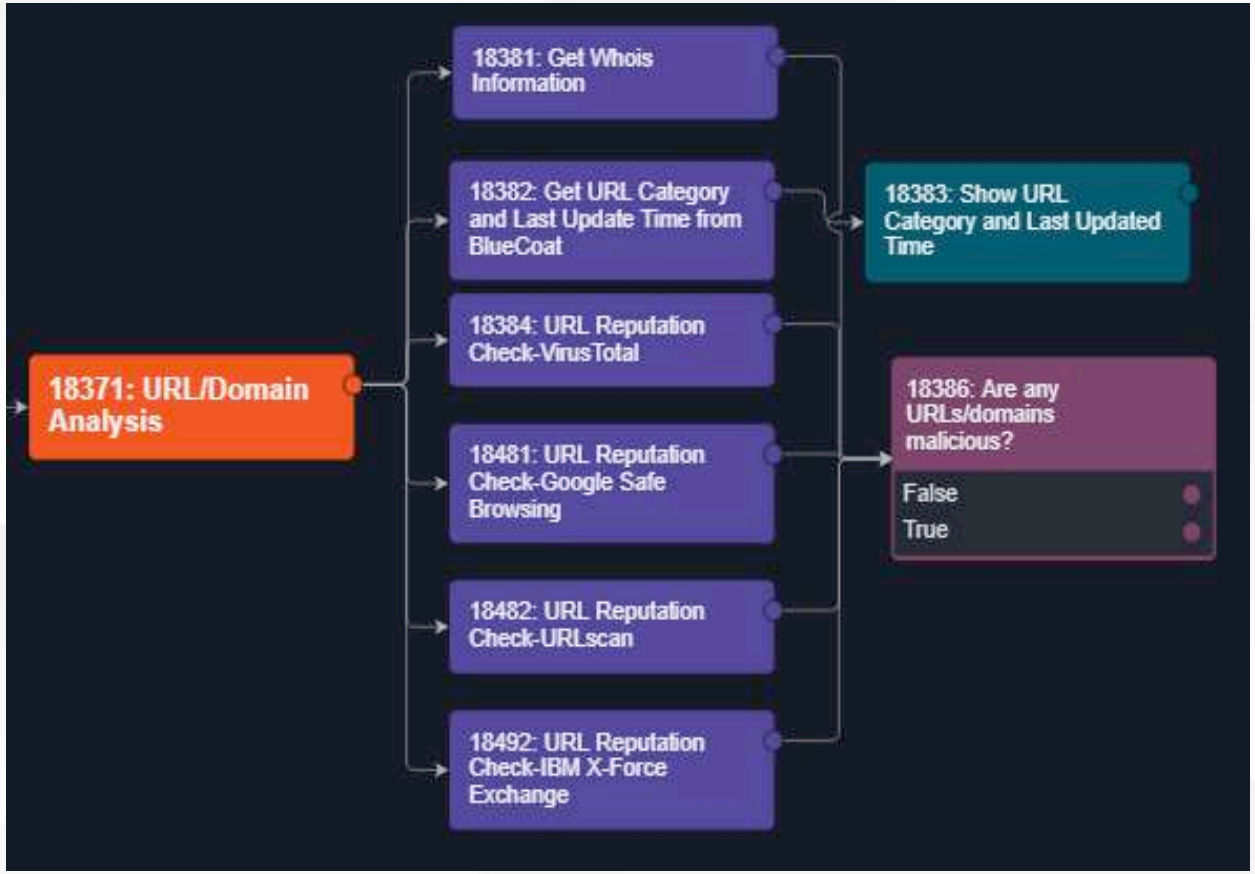
18382 : 取得 URL Category 及 Last Update Time 資訊
- Source : Web Proxy

18384 : 取得 URL Reputation
- Source : VirusTotal

18481: 取得URL Reputation
- Source : Google Safebrowsing

18482 : 取得 URL Reputation
- Source : Check-URLScan

18492 :取得 URL Reputation
- Source : IBM X-Force



SOAR Use Case實際應用情境 - Threat intelligence威脅情資自動化調查

- 取得 User Information

18373 : 取得 User Information

- Source : HR DB / AD

SOAR Use Case實際應用情境 - Threat intelligence威脅情資自動化調查

- Notification and Mitigation

18396 : 阻擋 IP

- Target : Firewall API

18397 : 阻擋 Domain

- Target : Proxy API

18398 : 阻擋 User

- Target : AD

18490 : 隔離檔案

- Target : EDR / Antivirus Product

18532 : 傳送簡訊至管理者

18530 : 傳送 Email 至管理者

- 報表彙整

18400 : 彙整及產出報表

SOAR Savings有效節省人力時間與成本控制

	BEFORE	AFTER
C&C NETWORK EVENTS PER MONTH	200	200
FALSE POSITIVES	164	164
MINUTES TO CLOSE EACH FP	15	3
TRUE POSITIVES	36	36
MINUTES TO CLOSE EACH TP	30	6
HOURS PER WEEK	59	10
TOTAL YEARLY COST	NTD 453,120	NTD 76,800

SAVINGS FROM ONE SOAR WORKFLOW:

NTD 376,320 / YEAR

49 HRS. / WEEK

iSecurity
The Hub of Security Innovations

SOAR自動化協調響應平台五大效益

01 快速自動化響應機制

02 大幅改善SOC作業效率

03 標準化事件處理

04 視覺化流程追蹤

05 節省時間與人力成本

D3 Security SOAR資安協調自動化響應平台

全球注視Global Traction

- Fastest-growing SOAR vendor *(Frost & Sullivan, 2019)*
- 100+ of the Fortune 500
- Growth in MSSP and midmarket solutions

加拿大溫哥華Vancouver

- 100 people strong
- Security expertise throughout
- *Good in the SOC* since ‘02

D3 SOAR資安協調自動化響應平台

D3 SECURITY

CODELESS PLAYBOOKS

無須撰寫Python程式碼即可建立與整合組織應用情境設計

FULL IR LIFECYCLE

延伸完整的IR調查週期橫跨各響應階段

CISSP SUPPORT

具備CISSP認證的資安自動化專家協助支援

ATT&CK INTELLIGENCE

對應ATT&CK framework框架的主動式IR與威脅獵捕機制

THANK YOU

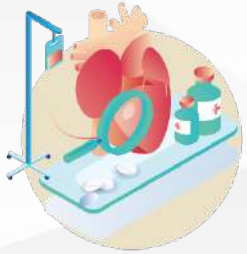
D3 Security
www.d3security.com

iSecurity
www.isecurity.com.tw

展覽編號
B22

強化企業資安體質
為未知威脅做好準備

1 Stop More Attacks
超前部署，拒敵於境外



2&3 Find & Fix breaches faster
次世代資安維運中心

4 Reduce breach impact
阻絕擴散降低損害

iSecurity
The Hub of Security Innovations