



獵捕並停止無檔案式的隱匿攻擊

Symantec Endpoint Security

March 18, 2021; 11 am PT



本中文化由保安資訊提供

<https://www.savetime.com.tw>

Vikram Thakur

技術總監

賽門鐵克端點安全(SES)



在 SES Complete 上的新功能：Threat Hunter

引進機器學習和專家分析的組合力量，來幫助識別潛在的違規行為



專業知識 —— 追查針對性攻擊活動

經驗豐富的SoC威脅獵人利用豐富的雲端遙測和機器學習分析來搜尋並發現高真實度事件



資料 —— 獲得完整的全球情報

透過直觀瀏覽（經由 API）賽門鐵克的全球安全數據，以增強您自己的能力來發現和識別攻擊



洞察 —— 策略性的威脅資訊

精細的報告查出惡意行為者使用的趨勢和策略，使用歷史經驗和全球知識來使預測可能的漏洞利用途徑

第一時間就能警示通報：不管是明目張膽地公開犯罪還是鬼鬼祟祟的匿跡隱形

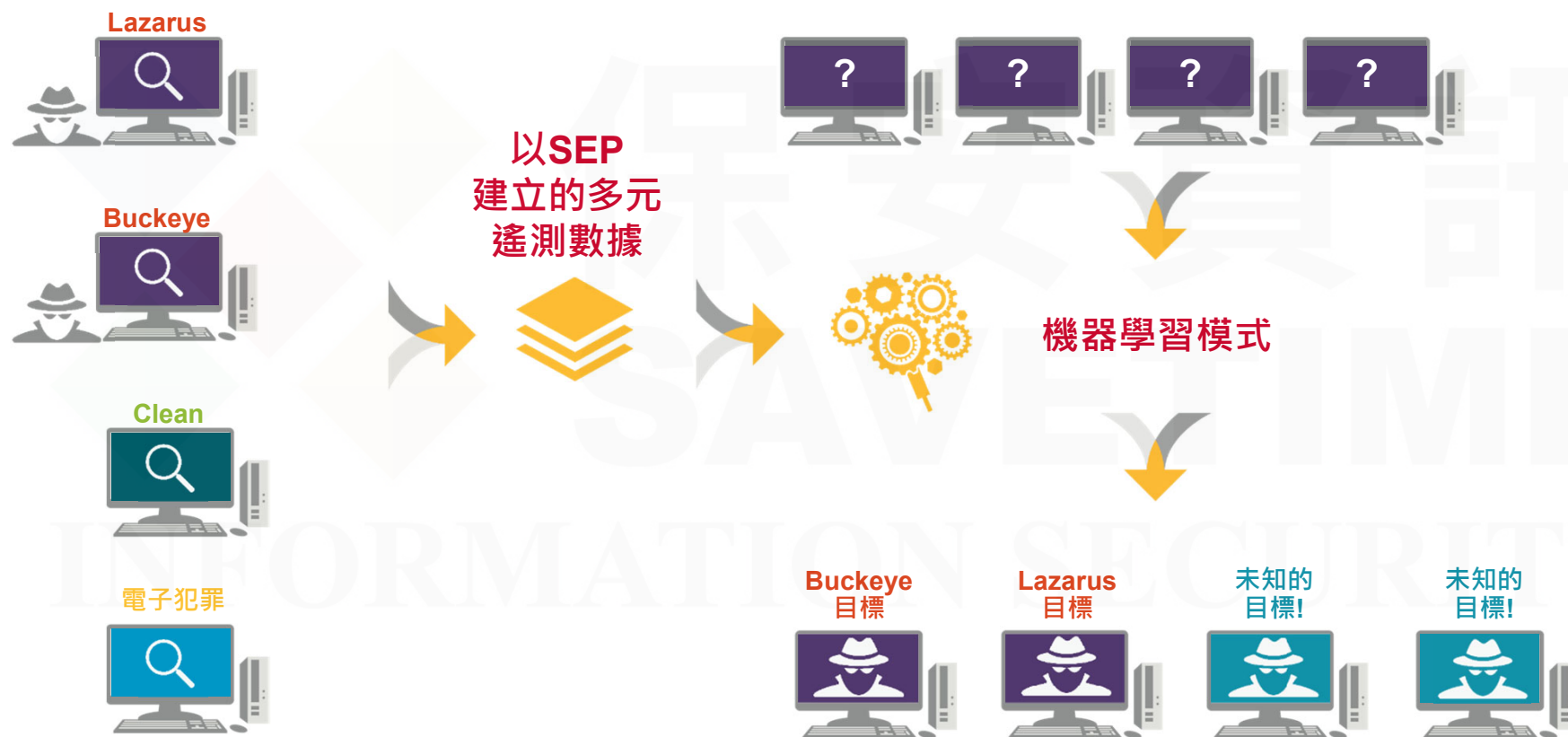


保安資訊
SAVETIME
INFORMATION SECURITY

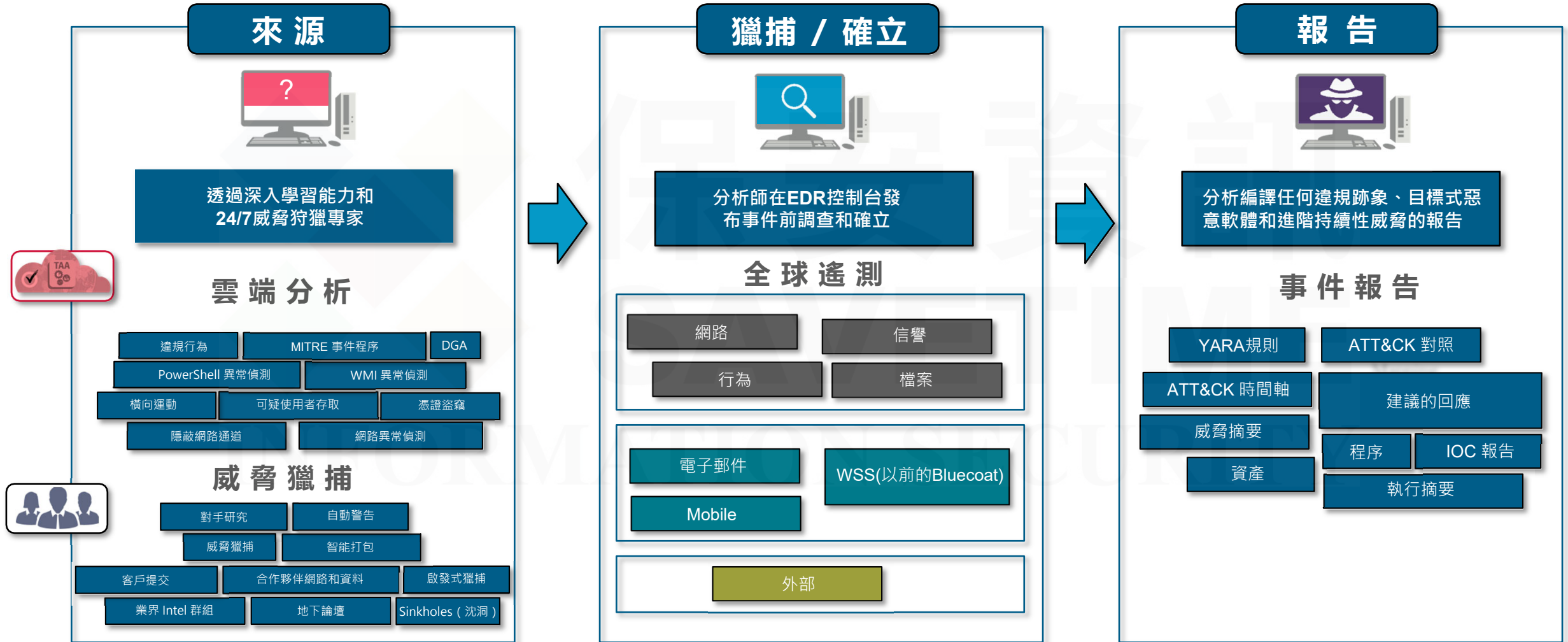
Threat Hunter--威脅獵手



Threat Hunter--威脅獵手 | 雲端分析

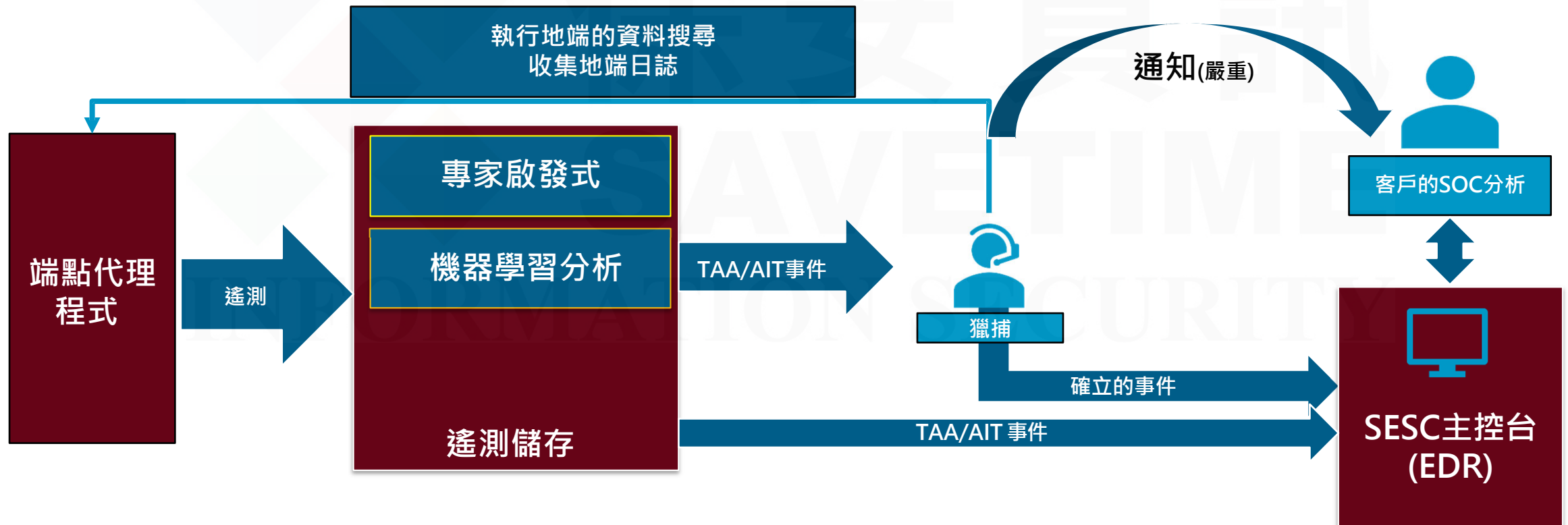


Threat Hunter--威脅獵手 | 機器和人類一起狩獵



Threat Hunter--威脅獵手 | 高水準的流程

1. 專家啟發式生成新事件，並在SESC中確立現有的目標式攻擊分析
2. 關鍵攻擊挖掘與情報(CADI)分析通知客戶關鍵OOB事件
3. 一個在內部網路中活動的惡意程式被定義為一個**關鍵事件**

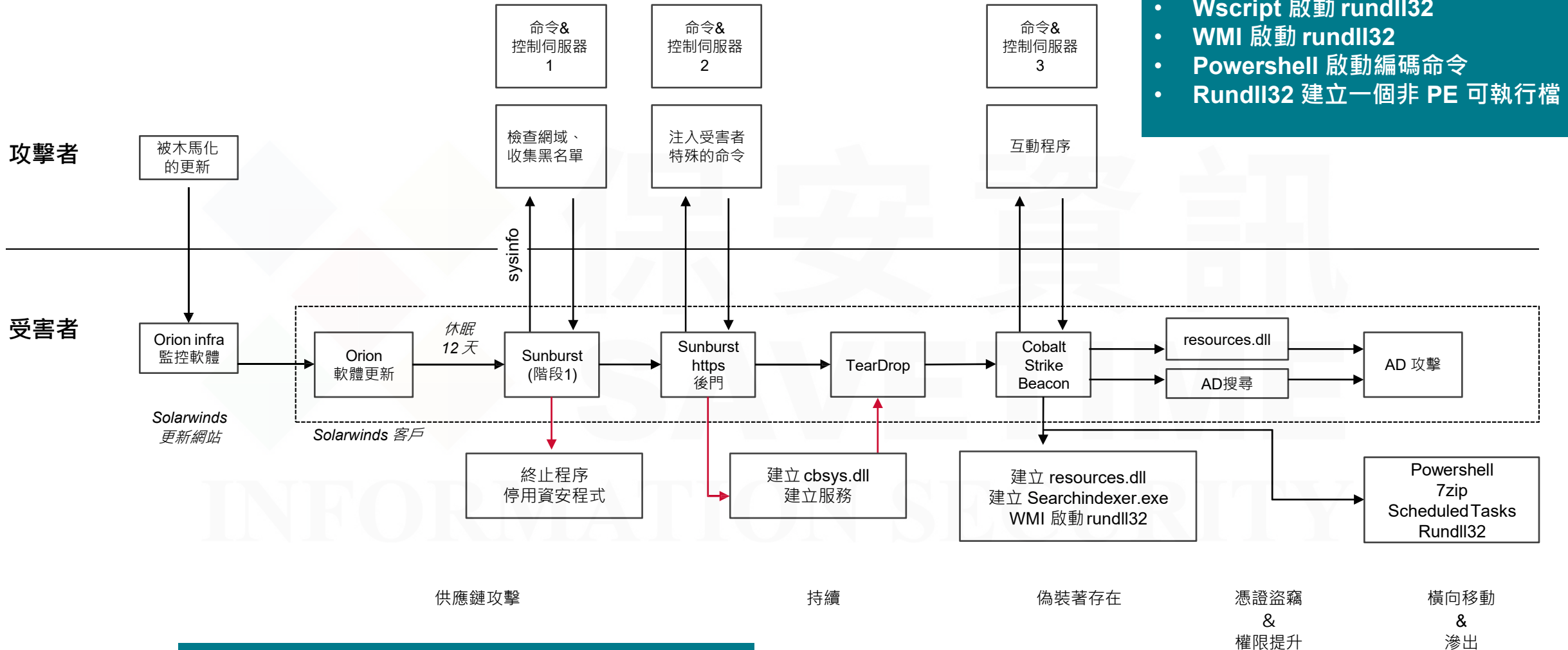




Threat Hunter--威脅獵手範例



Sunburst 攻擊鏈



EDR 事件規則：

- 嘗試透過 Wscript 執行 rundll32
- 嘗試透過 WMIPRVSE 執行 rundll32

Threat Hunter--威脅獵手 | Symantec的AI+安全專家協助的SOC

The screenshot displays the Symantec Endpoint Protection console interface. On the left is a navigation sidebar with various icons. The main area shows a list of incidents under the 'Incidents' tab. A modal window is open for incident 100310, providing detailed information.

ID	DESCRIPTION	LAST SEEN
100310	Threat Hunter Analysts Identified a backdoored SolarWin...	De
100295	Sandbox detection: 1929.exe	De
100305	Memory Exploit Attack: Data Execution Protection - Execu...	De
100306	Memory Exploit Attack: Return-Oriented-Programming - ...	De
100294	Suspicious PowerShell detected: suspicious encoded com...	De
100293	Suspicious PowerShell detected: suspicious encoded com...	De
100292	Suspected ransomware activity.	De
100291	Sandbox detection: Kz8AuFrBb.exe	De
100290	Sandbox detection: qlFhpp5QD.exe	De
100289	Suspected ransomware activity.	De
100288	Sandbox detection: zZupB2a7H.exe	De
100287	Sandbox detection: HXZNMZty1.exe	De
100286	Sandbox detection: a1SuYIZIX.exe	De
100285	Suspicious PowerShell detected: suspicious encoded com...	No

Incident 100310 Details:

- ID:** 100310
- DESCRIPTION:** Threat Hunter Analysts identified a backdoored SolarWinds Orion updater in your environment
- SEVERITY:** High
- AFFECTED ENDPOINTS:** 1
- EVENT COUNT:** 24
- STATUS:** Open
- DETECTION TYPE:** Cloud Analytics
- CONCLUSION:** Analyst Reviewed
- FIRST SEEN:** Dec 3, 2020 04:42:30 PM
- LAST SEEN:** Dec 7, 2020 10:53:05 PM
- LAST UPDATED:** Dec 18, 2020 05:26:44 PM

Conclusion: Yes SUSPECTED BREACH

IOCs:

```
sha256 019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
sha256 ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
sha256 d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600
sha256 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
sha256 dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
sha256 eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed
sha256 c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
sha256 ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
domain websitetheme[.]com
domain databasenalora[.]com
```



保安資訊

SAVETIME

INFORMATION SECURITY

威脅情資 API





偵測



獵捕

保安資訊
SAVE THE
INFORMATION SECURITY

威脅情資 API | 獵捕的挑戰



- Age / TTL
- 儀表
- 誤判 (FPs)
- 資源



- 確立 / 前後關聯
 - 曾見過?
 - 何種縱向關係?
 - 什麼地理位置?
 - 相關樣本?
 - SIEM軸點上的訊息?
 - 程序鍊?

威脅情資 API | 優點

透過 API 直接訪問 Symantec 的全球智慧型網路



即時威脅確立

- 在入侵指標(IOC)上透過快速搜尋加速根源脈絡調查
- 透過搜尋相關的入侵指標(IOC)來確定攻擊範圍
- 與威脅情資平台整合



威脅情資 API | SHA256 搜尋

- 包括檔案雜湊值、網域或 IP 位址的任何資訊：
 - 信譽
 - 威脅名稱
 - 盛行率 (散佈)
 - Age
 - 產業
 - 地理位置
 - 程序處理歷程
 - 相關指標
 - 其他檔案
 - URLs

```
{
  "insight": {
    "targetOrgs": {
      "topCountries": [
        "us",
        "tw",
        "es",
        "de",
        "mx"
      ],
      "topIndustries": [
        "government",
        "information technology",
        "professional services"
      ]
    },
    "firstSeen": "2020-09-11",
    "reputation": "BAD",
    "prevalence": "Thousands",
    "fileSha256":
      "af730c7947f9aa7bf0d6e2940b7b41774c69bacaa41cf2e5d65f
      e11aca0c732a",
    "lastSeen": "2020-09-11"
  }
}
```

威脅情資 API | 即時搜尋的優點 vs 動態訊息

- API

- 在本地端觀察到的活動提供全球的背景資料
- 使用 API 即時搜尋
- 提供其他指標去找到額外的證據
- 不用下載和儲存

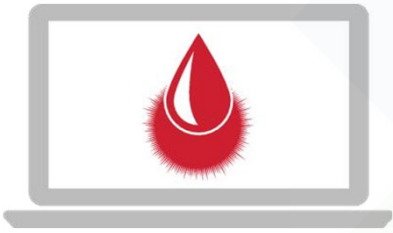
- 動態訊息

- 需要下載過程並將與觀察到的入侵指標 (IOC) 動態訊息的資料匹配
- 價值難以量化
- 指標沒有顯示與其他指標相關
- 通常與威脅情資相關

```
"processChain": {  
  "fileSha256": "2be981b3686ee5e725583f5936f5f0a0992723cad784457f91d9d1d5a15a0852",  
  "chain": [  
    {  
      "parent": {  
        "fileSha256": "75bb70a262337ceaaa3d4e91282b1e5a0691cb027f1b304cf2fa63a042139c22",  
        "processName": "ksdlllauncher.exe",  
        "parent": {  
          "fileSha256": "77fd3f04b6d3c4c0c6b05363b1cc95edc0c0539e1eacff2ceae87b9f2783f8f1",  
          "processName": "userinit.exe",  
          "parent": {  
            "fileSha256": "b5170d0e86b93d83c67636fe2c1207139cfcbc9114bbfd74d127cddcbd8fa114",  
            "processName": "winlogon.exe"  
          }  
        }  
      }  
    },  
    {  
      "child": {  
        "fileSha256": "0000000000000000000000000000000000000000000000000000000000000000",  
        "processName": "dummy.exe"  
      }  
    }  
  ],  
}
```

威脅情資 API | 實際確立案例 #1

攻擊 SolarWinds 的 Teardrop 後門



```
{
  "file": "b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07",
  "reputation": "BAD",
  "prevalence": "LessThanFive",
  "firstSeen": "2020-06-08",
  "lastSeen": "2021-02-09",
  "targetOrgs": {
    "topCountries": [
      "us",
      "pl"
    ]
  }
}
```

```
{
  "file": "b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07",
  "state": [
    {
      "technology": "AntiVirus",
      "firstDefsetVersion": "20210129.003",
      "threatName": "backdoor.teardrop"
    }
  ]
}
```

從賽門鐵克威脅情資 API 中提取

```
{
  "file": "b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07",
  "related": [
    {
      "iocType": "File",
      "iocValues": [
        "6e4050c6a2d2e5e49606d96dd2922da480f2e0c70082cc7e54449a7dc0d20f8d"
      ],
      "relation": "bySignature"
    },
    {
      "iocType": "Network",
      "iocValues": [
        "infinitysoftwares.com",
        "bigtopweb.com"
      ],
      "relation": "byThreatActor"
    },
    {
      "iocType": "File",
      "iocValues": [
        "56de41fa0a94fa7fff68f02712a698ba2f0a71afcecb217f6519bd5751baf3ed",
        "5c1f6855966ce40d5cbbb2696c077bef0d9f0f692951f226e81e75f337d97090",
        "de3f1f1546a6b4d0aab140da1c6bdf0f51ecb003f0025f9f1c27ba2ddb825f43",
        "1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8fd6d730c",
        "3f58aba2b697ba896607ed6dd7d93349cb82fad4f814f77f3b5b7ce9437607b5",
        "eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a20ed",
        "c5a818d9b95e1c548d6af22b5e8663a2410e6d4ed87df7f9daf7df0ef029872e",
        "240ef5b8392b8c7a5a025c36a7e5b0e03e5bb0d01a28703bb22e6159a4fd10e",
        "be9dbbec6937dfe0a652c0603d4972ba354e83c06b8397d6555fd1847da36725",
        "955609c f0b4ea38b409d523a0f675d8404fee55c458ad079b4031e02433fdbf3",
        "a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d",
        "ffdbdd460420972fd2926a7f460c198523480bc6279dd6cca177230db18748e8",
        "da6005596768540ae5cf407693bd2c138cb6443dce67a0030862bb71d9e18b",
        "2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d",
        "e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d",
        "f2d38a29f6727f4ade62d88d8a68de0d52a0695930b8c92437a2f9e4de92e418",
        "abe22cf0d78836c3ea072daea f4c5eeaf9c29b6feb597741651979fc8fbd2417",
        "0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589",
        "b8a05cc492f70ffa4adcd446b693d5aa2b71dc4fa2bf5022bf60d7b13884f666",
        "92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690",
        "02c5a4770ee759593ec2d2ca54373b63dea5ff94da2e8b4c733f132c00fc7ea1",
        "290951fcc76b497f13dcb756883be3377cd3a4692e51350c92cac157fc87e515",
        "20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfdc21cde692fd9",
        "a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2",
        "db9e63337dacf0c0f1baa06145df5f1007002c63124f99180f520ac11d551420",
        "cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6"
      ],
      "relation": "byThreatActor"
    }
  ]
}
```

IOCs 細節與其他資訊：<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds>

威脅情資 API | 實際確立案例 #2

利用程序處理歷程(譜系)進一步調查

```
{
  "file": "3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71",
  "related": [
    {
      "iocType": "File",
      "iocValues": [
        "90afa15e86a5d6fcbfc39b24beb42b900f2890f2dd4f780b64c621aac9407d8f",
        "8e3d03fbfb110da6da3662a44f8b913db5c8b17baae58fc5d6f1d6d023ff3091",
        "893c54c229b49f2c384fb88fd64af42029948b7d5c3f9ce343b0f2df93d0b8a5"
      ],
      "relation": "bySignature"
    },
    {
      "iocType": "File",
      "iocValues": [
        "e790365725392aa2e75cd72922110925b8db1f8bb5b54207d3e429e52894bbdc",
        "3b5bf2d8fc5ba5f7ddb1cf624fca53ce3a16a40021c1d1455b469fda00144bd1",
        "c5587f286397d8c398f78f738ffd402ccf5487b4415d794e8f3cb430d717c9b4",
        "f6b4d18fa0d3c4958711ac0d476c21a6fdf2897f989a0ad290b43f463dd8b5b0",
        "360ffb7dafc5c3e60055ea589146d075329ad924421025d97c03adca8d162761",
        "9bf76ea21f5fc2c8c43ffa9095936efc61d44495b81f70c5fe77694b694aa",
        "8694c5732d26921eea29589a9fa4182139ef3d9ea6b6d0acca8994b4aa5defe5",
        "09326e764daf190d1a888e6e4786fae471ef93befb03abb405357f6ded5f9abc",
        "13ad43ee6d19dfc9709c3106d796bc3f21791a564e443d042a5aa117f2680649",
        "bf74b5707c2f035da0a348658a60e22c32d0f57340826fc4efcba3b41ea9c8f3",
        "882a3a0f60fb5bb17b06a1d4798a1bfc3cde621fc8242bedd810932fa0e6f10f",
        "c4e98f07170cec69cacdd5cedb8927e48a2a299cb1b8cda87526e768af6174f0",
        "0dc1fbe9f8855738768b02f656651f4936a40631987d626a59ea70c8c0d62f0c",
        "a86d6a6d1f5a0efcd649792a06f3ae9b37158d48493d2eca7f52dcc1cb9b6536"
      ],
      "relation": "byProcessChain"
    }
  ]
}
```



```
{
  "file": "3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71",
  "chain": [
    {
      "parent": {
        "parent": {
          "file": "f6b4d18fa0d3c4958711ac0d476c21a6fdf2897f989a0ad290b43f463dd8b5b0",
          "processName": "winit.exe"
        },
        "file": "d7bc4ed605b52274b45328fd9914fb0e7b90d869a38f0e6f94fb1bf4e9e2b407",
        "processName": "services.exe"
      }
    }
  ]
}
```

從賽門鐵克威脅情資 API中提取

威脅情資 API | 整合選項

- 包含在 **Symantec Endpoint Security Complete**
 - 不單獨銷售
- 透過 **API**
 - 支援自定工作流程
 - 已可用
- 威脅情資平台
 - 與已存在的 SOC 做 Out-of-box 工作流程支援

Documentation Examples Try Now

API Table of Contents

Name	Path	Value
fileInsight	/v1/threat-intel/insight/file/{file_sha256}	This API returns file insight enrichments for given file sha256.
domainInsight	/v1/threat-intel/insight/network/{network}	This API returns file insight enrichments for given file sha256.

> GET /v1/threat-intel/insight/file/{file_sha256}

> GET /v1/threat-intel/insight/network/{network}

<https://apidocs.securitycloud.symantec.com>





保安資訊
SAVETIME
INFORMATION SECURITY

策略情資



策略情資 | 概述

- 即時簡短的戰略情資特別是與組織、產業別或地區相關
 - 摘要
 - 目標產業
 - 目標地理位置
 - 工具/TTPs (手法、技術與過程)
 - 建議
 - IOCs/Yara 規則
 - 參考
- 正規簡短策略威脅、產業或地理位置概要
 - 透過長期歷史統計攻擊類型群組、威脅資料更新或特定產業、地區的趨勢影響做預測
- 每日威脅資料更新

White Paper



Symantec
A Division of Broadcom

Sophisticated Groups and Cyber Criminals Set Sights on Lucrative Financial Sector

By Threat Hunter Team



Table of Contents

- Introduction
- Ransomware: A High-Cost Threat
 - Case Study: WastedLocker
- APT Groups: Cyber Criminals Not the Only Concern
- Deep Dive: Jointworm - Sophisticated Attack Group Sets its Sights on the Financial Sector
 - Tools, Tactics, and Procedures
 - Case Study: Jointworm Activity Across a Financial Organization in Europe
 - Downloading Additional Tools and Malware
 - Additional Tricks
 - What Does Jointworm Want?
- Malicious Activity: Detections Trend Upwards
 - Geographical Spread: Which Countries Recorded the Most Malware Detections?
 - Network Activity: Further Insight into Cyber Criminals' Endeavors
- Conclusion
- Best Practices
- Appendix (i)
- Appendix (ii)

Introduction

The financial sector (comprised of banks and other financial organizations) has always been a favorite target of cyber criminals, and it's not hard to understand why. The huge amounts of money passing in and out of financial organizations on a daily basis—now in a primarily digital format—make them a prime target for profit-focused cyber criminals.

Symantec, a division of Broadcom has examined the activity targeted at some of our biggest financial customers since the start of 2019 and have found that detections of both malware and ransomware on customer networks are trending upwards.

The monthly detections in both categories have gone up and down since the start of 2020, with ransomware detections dropping sharply in March as the world went into lockdown due to COVID-19. However, the overall trend for detections is still upwards, showing that financial institutions still

感謝您



賽門鐵克解決方案專家--保安資訊
<https://www.savetime.com.tw>

相關參考資訊下載(PDF)--保安資訊整理提供

- ◆ 賽門鐵克全球情資(GIN)資訊圖表
- ◆ 賽門鐵克端點安全解決方案全覽
- ◆ 賽門鐵克郵件安全解決方案全覽
- ◆ 賽門鐵克網頁/雲端安全解決方案全覽
- ◆ 賽門鐵克端點安全在2020 MITER Engenuity ATT & CK® 評比中大放異彩





BROADCOM[®]

connecting everything[®]

INFORMATION SECURITY