OCSF 發布公告：開放式網路安全架構框架

2022 年 10 月 20 日發布｜專家觀點

亞當·布羅姆維奇
（Adam Bromwich）
Broadcom Inc. Symantec Endpoint Security部門副總裁兼總經理

Symantec Enterprise 引領未來

多年來，客戶一直要求業界提出一種使數據更具互通性並使工具之間更容易通信的方法。現在，我們終於做到了。

OCSF 的發布

在 2022 年的 BlackHat 大會上，幾家領先的技術公司聯合發布一個新的開放數據標準，用於共享網路安全訊息，稱為開放式網路安全架構框架 (OCSF)。OCSF 本質上為客戶提供一種從不同安全工具共享數據的共通方式，這是一個很大的突破。OCSF 專案是由 Splunk 和 AWS 合作發起，並在 Symantec (現為 Broadcom 軟體的一部分) 開發的 ICD 架構基礎上進行發展。

OCSF 的採用

到目前為止，企業的安全運營中心 (SOC) 必須投入大量的努力來使各種工具協同工作，這本應是更好地尋找威脅的寶貴時間。一般來說，SOC 使用約 45 種不同的安全工具，這持續導致了管理上的困難，因為這些工具以不同的方式存儲其遙測數據。

當 SOC 首次發展起來時，所有大型安全軟體供應商都宣稱自己的平台是解決方案。然而，這種“單一供應商”的解決方案並不奏效。企業繼續依賴多家供應商，結果是產生多種不相容的安全遙測數據集。大型企業最終不得不投資於自行整合其所有安全工具，以便具有任何數據的查詢功能。在大多數大型公司中，我看到 SOC 雇用一支完整的工程師團隊，他們的工作就是轉換數據和更新程式以處理新類型的數據。

> “ OCSF 專案是由 Splunk 和 AWS 合作發起的，並在 Symantec (現為 Broadcom 軟體的一部分) 開發的 ICD 架構基礎上進行發展。

這不僅僅是必須進行大量整合工作的負擔。準確性是另一個重大問題。由於各種產品使用不同的方式存儲各自的數據，對企業而言，在轉換過程中會存在更高的錯誤和風險。

這種整合和轉換工作會很快的讓人厭倦--尤其是企業添加或升級其安全基礎設施時。不意外，在近年來，SOC 變得更加直言不諱和要求更多，告訴供應商他們希望產品更容易整合，而不是作為城堡般的獨立存在。

OCSF 的驅動力

OCSF 透過提供一種通用的方式來儲存遙測數據以消除麻煩，這使得工具的整合變得更加容易。資訊可以從一個工具傳遞到另一個工具。這種架構是一致的，數據可以無縫地流入 SOC 所依賴的資料湖和分析工具中。

這個專案對我來說特別重要，因為 OCSF 的起源可以追溯到 Symantec 企業的一項倡議，就是讓我們的所有產品都能夠相互關聯數據。這個倡議很快揭示出關鍵的挑戰。這看起來可能很簡單，但要讓多個產品以相同的方式存儲數據並處理機器、檔案和事件並不容易。在 Symantec 內部的這一標準化努力演變為我們的整合網路防禦 (ICD) 平台。時至今日，同樣的架構和方法現在成為開源專案的基礎，這個成果就是 OCSF。

OCSF 的未來

OCSF 是由安全工程師們設計。它旨在為每天參與網路安全工作並面臨日益複雜環境的人們提供便利。我們需要更多供應商採用 OCSF 格式，使其成為通用標準。往往，標準提案都會對特定公司有利。但在這裡不是這種情況。採用 OCSF 對任何人都沒有專利優勢。作為一個行業，我們通過為客戶做正確的事情而共同受益。支持一個共同的標準是一個明智之舉。

關於作者

亞當・布羅姆維奇 (Adam Bromwich)

Broadcom Inc. Symantec Endpoint Security 部門副總裁兼總經理

Adam 領導著一個由工程師和分析師組成的全球團隊，他們開發改變遊戲規則的安全技術、攻擊情報和安全內容來保護 Symantec Enterprise 客戶。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/announcement-ocsf-open-cybersecurity-schema-framework

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。