Red Hat

透過自動化提升安全性

Red Hat 客戶
成功案例系列

目錄

前言

自動化帶動安全性升級

在步調快速的環境中整合 IT 安全性團隊與解決方案，是所有組織都必須解決的難題。儘管每一種安全性做法有所差異，但仍有一套策略可以學習和調整，以抵禦惡意活動或無心之過的影響，確實保護您的重要資料、應用程式、IT 系統、網路與裝置。

為協助推廣這套策略，本電子書收錄 5 個 Red Hat® Ansible® Automation Platform 客戶的成功案例。這些組織運用自動化功能整合並擴充安全性解決方案，以協調和統一的方式調查並因應組織中的各種威脅。

自動化如何提升安全性？

大部分組織的安全性團隊知道該採取哪些行動，但是以手動設定系統和應用程式 (特別是如果有數以千計的系統與應用程式) 的方式防範攻擊者時，必需投入過多的時間和技能資源。

自動化功能可以填補這類技能和資源缺口，並且根據內部和外部安全性準則來強化安全性標準，成果就是大幅降低反應時間和減少弱點。

> ***當組織充分部署安全性 AI 與自動化功能，比起未部署安全性 AI 與自動化功能的組織，可以更迅速地偵測並控制資料外洩。***
>
> IBM，Cost of a Data Breach Report 2022 (2022 年資料外洩成本報告)，2022 年 7 月。

Ansible Automation Platform 可協助團隊將安全性解決方案自動化並整合，同時運用精選的模組、角色和劇本，以協調且統一的方式調查並因應企業中的各種威脅。

統一的安全性做法涵蓋哪些層面？

安全性解決方案必須不斷升級，才能搶先一步防範安全性威脅。需要考量的關鍵層面包括：

強化調查

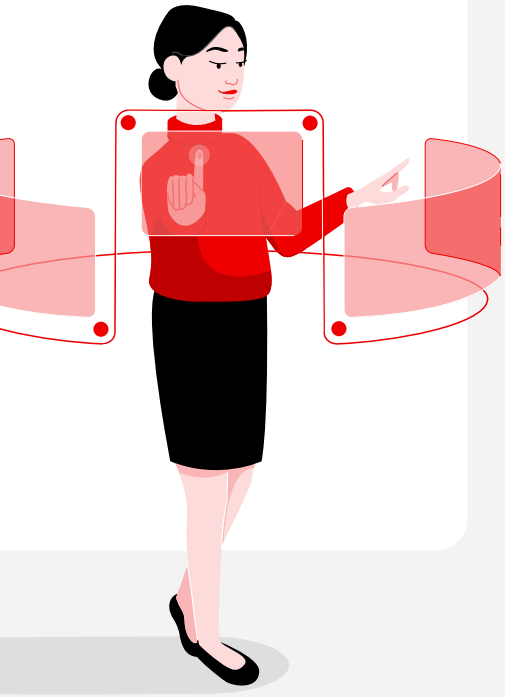
收集來自防火牆、入侵偵測系統 (IDS) 與其他安全性系統的記錄， 即可利用程式設計方法，隨需強化歸類經由安全性資訊和事件管理系統 (SIEM) 執行的活動。

找出威脅

自動調整記錄層級，並建立新的 IDS 規則與新的防火牆原則，以便在更短時間內偵測更多威脅。

回應事件

修復可加速自動化的動作，例如封鎖 IP 位址或網域、允許不具威脅性的流量，或者隔離可疑的工作負載以供深入調查。



為何選擇 Ansible 的安全性自動化功能？

安全性是每一個人的責任，Ansible 是功能強大且無需代理程式的工具，採用人類可讀的語言來提供自動化功能，因此從 IT 營運、開發、網路工程師到安全性團隊在內，整個組織都能使用自動化功能。如此一來，組織就可以運用自動化功能達成更多目標，包括：

- 提升生產力。Ansible 採用人類可讀的簡單語言，就算缺少編寫程式碼或管理的專業技能，也能確保以正確順序執行工作。
- 管理所有 IT 基礎架構。獲得收集和稽核資訊的能力，並隨時掌握設定管理與工作流程調度。
- 提升效率與安全性。無需代理程式的架構讓您可以更迅速地部署解決方案，不必擔心代理程式的弱點遭到利用或需要更新。

以下的成功案例會詳細說明安全性自動化的強大功能與擴充性，以及像 Ansible Automation Platform 這樣的統一自動化平台如何協助組織強化安全性態勢。

1

EMORY UNIVERSITY

美國埃默里大學 (Emory University) 運用 Red Hat Ansible Automation Platform 降低 sudo 威脅

> ***沒有人認為我們有辦法每 30 天就修補 Linux 伺服器，但使用 Red Hat Ansible Automation Platform 之後，我們不僅達成這項目標，這也成了不可或缺的工作。***
>
> 埃默里大學資訊科技辦公室系統工程主管 Steve Siegelman

埃默里大學位於喬治亞州亞特蘭大，在亞特蘭大都會區的校園內有超過 15,000 名學生。埃默里大學與全球各地的機構都建立學術研究合作關係，同時也是喬治亞州規模最大的醫療系統，自然會成為網路攻擊的目標。攻擊者會企圖透過埃默里大學的數位足跡利用和取得機密資訊。

一旦經由弱點找到進入點，攻擊者便能暗中在整個網路四處移動，並在奪取智慧財產後不著痕跡地逃離。 該校的資訊科技辦公室 (OIT) 負責維護學生、員工、教師、研究人員和其他相關人士所使用的系統，以確保網路和資料不會遭到未授權存取，以及面臨可能的安全性資料外洩事件。這就是為何在 2021 年 1 月出現了相關警報。當時 Red Hat 團隊向 OIT 發佈警示，指出埃默里大學的 Red Hat Enterprise Linux® 系統中的弱點已影響到作業系統的 sudo 公用程式。

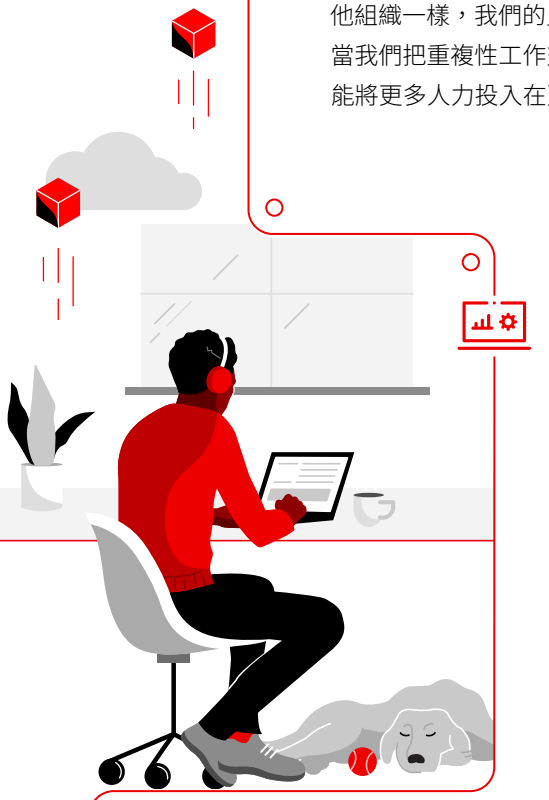
Ansible 自動化功能可加速修復安全性風險

修補更新只需要數小時而非數週

OIT 利用 Red Hat Enterprise Linux 管理超過 500 個伺服器，深知如果必須以手動方式安裝修補程式，未來一定會遇到難題，進而危及大學的基礎架構。而解決方案就是使用 Ansible Playbooks，將修補程式自動套用至各個伺服器。原本需要兩週才能完成所有伺服器的修復工作，現在總共只需四個小時。

釋出重要資源並集中投入更具價值的專案

最初，埃默里大學只在財務系統上部署 Ansible Automation Platform，後來學生和人力資源系統也採用此平台。「和許多其他組織一樣，我們的員工人數沒有增加，卻必需完成更多工作。當我們把重複性工作交給 Ansible Automation Platform 後，就能將更多人力投入在更重要的專案上。」Siegelman 表示。



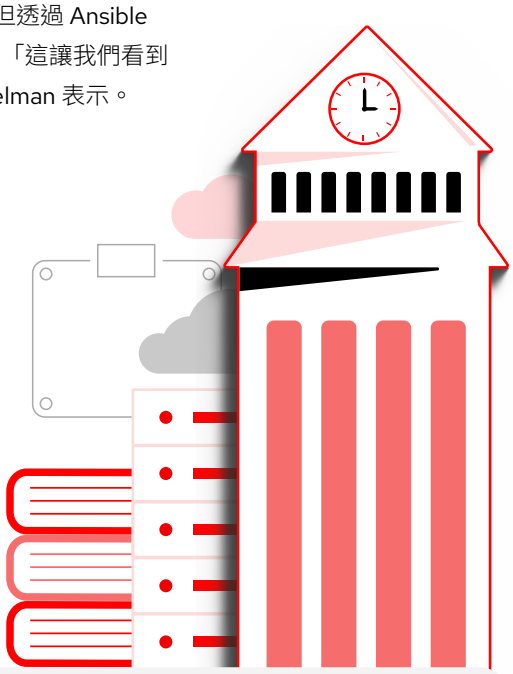
IT 員工可以專注於應對 COVID-19 帶來的挑戰

2020 年 3 月，Ansible Automation Platform 再次證明其具有彈性的優勢。當時埃默里大學被迫關閉校園，並要求學生和工作人員在家上課及工作。這是所有學校和組織都面臨的相同難題。

OIT 需要快速部署資料中心伺服器，才能處理重要員工進出校園的各項記錄。特定員工需要填寫已匯入系統的問卷。如果是手動在伺服器上設定，可能要費時數天，但透過 Ansible Automation Platform，數分鐘就能設定完成。「這讓我們看到自動化在後端可以發揮什麼樣的功能。」Siegelman 表示。

運用自動化推動校園之外的安全性創新

在埃默里大學的未來發展計畫中，自動化需求是一大關鍵，尤其是要將系統轉移至雲端時。「我們有一些舊版系統是新舊建置混雜，同時我們也在 AWS 平台投入了大量心力。」Siegelman 表示。「在同時使用多種不同系統的情況下， Ansible Automation Platform 讓我們可以建立標準化的可重複流程。不論平台是在雲端還是內部部署，一切都看起來井然有序。」



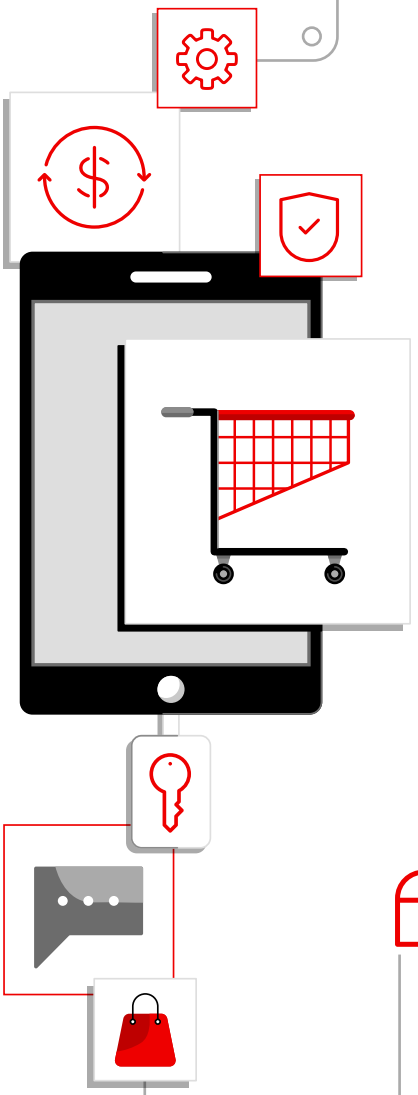
下載
埃默里大學成功案例

2

零售商 Schwarz Group 運用 Red Hat Ansible Automation Platform 將 IT 自動化

來自德國的 Schwarz Group 是全球第四大零售公司，在 33 個國家營運超過 12,500 間店點。Schwarz 致力於快速提升國際能見度，而為了達到這項目標，公司必須維持一致的店面管理做法，同時兼顧適應地方需求的彈性，以及快速展店的敏捷性 (尤其是在新市場)，此外還需要降低風險。

為了以一致的方式管理店面，同時兼顧適應地方需求的彈性，Schwarz 集團從現有的 Puppet 管理移轉到 Red Hat Ansible Automation Platform。建立一致的營運基礎後，Schwarz 便可以運用自助服務功能迅速部署創新的數位服務，並維持競爭力，同時保有穩固的安全性態勢。



一致性是確保全球數千家零數店面安全性的關鍵

Schwarz IT 有超過 3,500 名工程師，需要支援超過 1,000 個 SAP 系統和 28PB 的資料中心託管儲存空間。每間 Schwarz 店面都需要操作 Storeserver。這是由公司在當地的 IT 團隊安裝的集中式營運系統，可控制店面的多種功能，包括結帳機台系統、閉路監視器 (CCTV) 以及回收與獎勵計畫。

為改善使用者管理與授權，Schwarz IT 希望能引進受控且有效率的自助服務功能，來加快部署流程。為了達到這項目標，Schwarz IT 選擇實作 Ansible Automation Platform。

> ***社群版的流程複雜又耗時，無法滿足我們的需求。自動化是我們企業營運中的一大要素，而企業級支援就是我們選擇採用 Red Hat 解決方案的主要原因。***
>
> Schwarz IT 核心基礎架構服務部門 Storeserver 主管 Felix Kuehner。

在為期兩天的工作坊中， Schwarz IT 的團隊與 Red Hat 技術專家一同合作檢視架構，並為新的自動化解決方案建立最佳做法。

現在該集團每天執行超過 5,000 項 Ansible Automation Platform 工作，來管理店面伺服器。

依職位授予系統存取權來改善風險管理

採用 Ansible Automation Platform 之後，Schwarz IT 就可以透過適用的自助服務功能授權應用程式和開發作業，更有效掌握控制系統存取權的平衡。依職位授予存取權，意味著應用程式團隊能以一般使用者的身分將部署作業自動化，不需要根存取權，就能存取重要的核心業務系統。Kuehner 表示：「這項功能不僅能提供高度的一致性，還能促使個人主動參與全新和現有的專案。」

採用 Ansible Automation Platform 獲得初步成果之後，Schwarz IT 規劃要繼續發掘更多方法，以協助 The Schwarz Group 實現一致卻又能快速反應的店面營運模式。

我們很重視與 Red Hat 的合作關係，也希望能持續運用 Ansible 來找出讓公司更進步、更有效率的新做法。

Schwarz IT 核心基礎架構服務部門 Storeserver 主管
Felix Kuehner

下載
Schwarz 成功案例

Agile Defense 運用 Red Hat Ansible Automation Platform 提升安全合規性

3

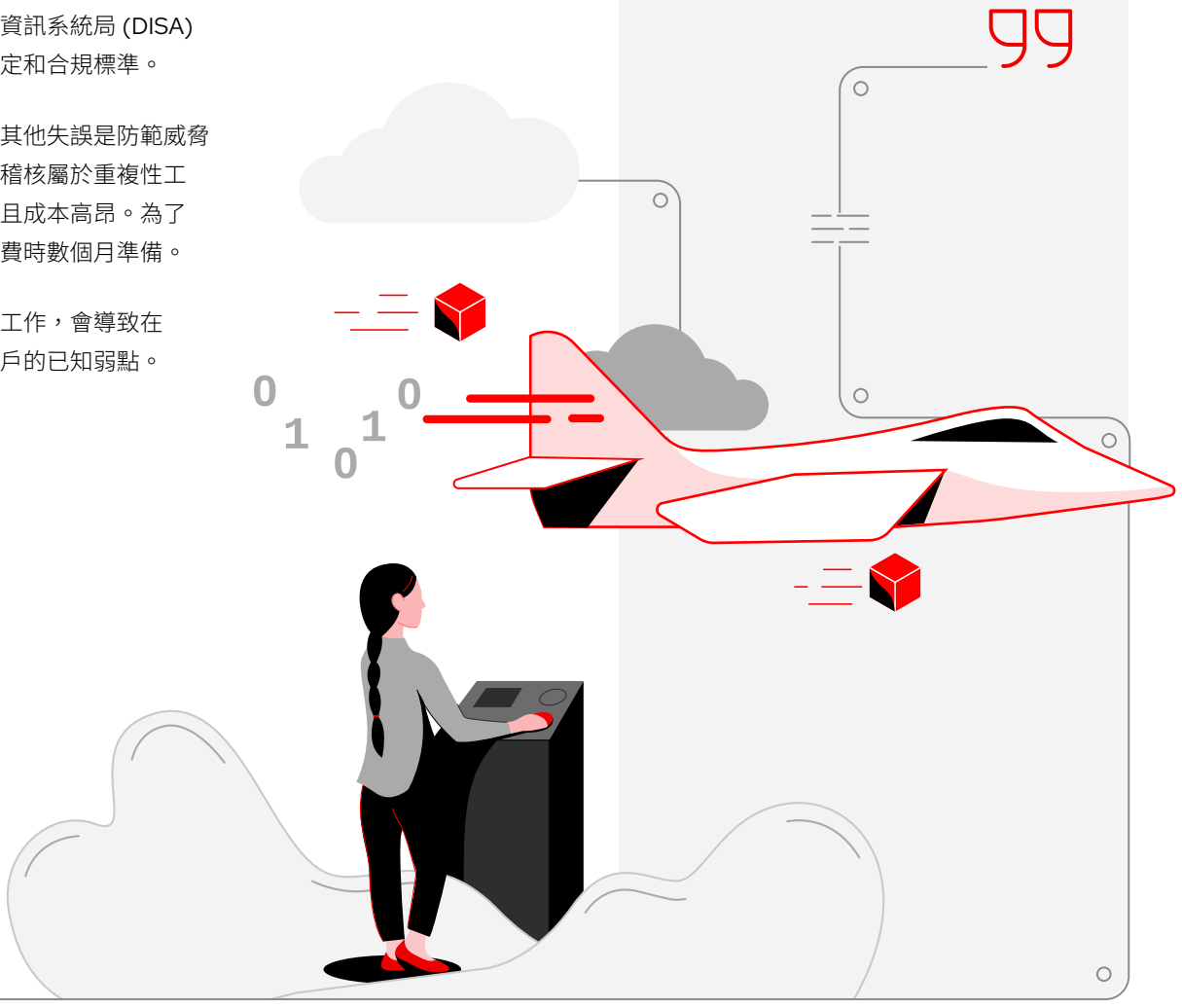
Agile Defense 是位於維吉尼亞州雷斯頓的知名資訊科技服務公司，由於有許多客戶是美國政府機關，包括一些美國行政部門以及隸屬於美國國防部的分支機關，因此 IT 安全性就成了公司的首要之務。

避免網路罪犯以未授權的方式存取公司系統與基礎架構，是公司當前最切身相關的目標。許多資料外洩事件都是因為設定錯誤而發生。對於美國國防部 (DoD) 和聯邦機構而言，防範威脅的做法是遵守國防資訊系統局 (DISA) 嚴格的資訊、安全性、設定和合規標準。

定期稽核檢查設定錯誤和其他失誤是防範威脅的一其中一部份，但這類稽核屬於重複性工作、需要投入大量資源而且成本高昂。為了執行稽核，各機構可能要費時數個月準備。

以被動反應手動執行這項工作，會導致在每次檢查之間都會暴露客戶的已知弱點。

> ***我們的客戶會在檢查前逐漸停止生產工作，同時準備好所有的文件。***
>
> Agile Defense 解決方案工程師
> Shawn Draper



運用自動化功能減緩稽核的衝擊

對於許多 Agile Defense 的政府客戶而言，設定錯誤和稽核是常見的痛點。作為自詡透過資訊科技創新的知名 IT 服務公司，Agile Defense 與 Red Hat 合作，打造安全技術實作指引 (STIG) 設定、回報與修復工具。STIG 自動化解決方案可執行臨時的系統稽核工作，也可選擇性修復設定錯誤，並回報裝置的目前狀態。STIG 自動化解決方案也稱為 Agile Defense 的合規即服務 (CPaaS)，採用具彈性和可擴充自動化功能的 Red Hat Ansible Automation Platform。

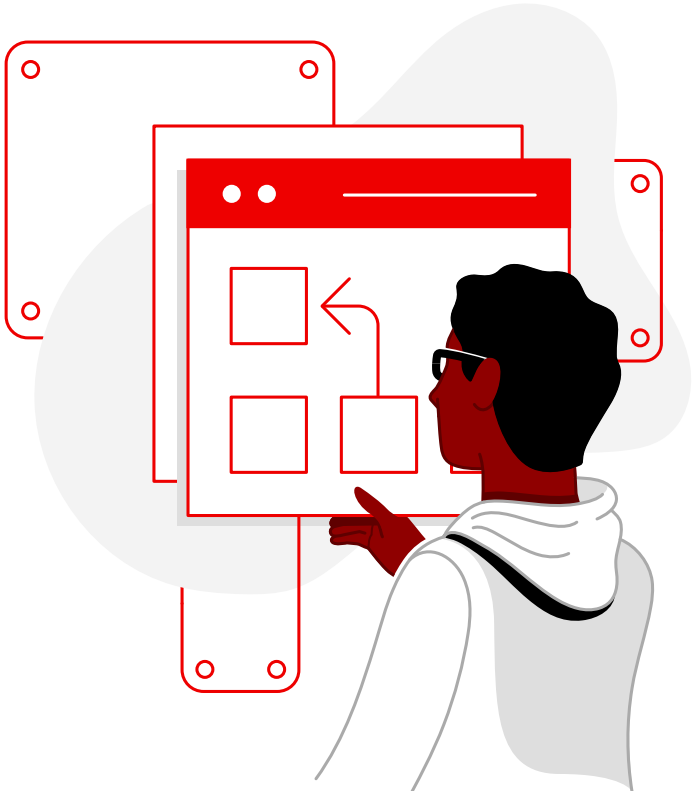
此外，Red Hat 也與 DISA 合作打造適用於 Red Hat Enterprise Linux 的 STIG，深知為每一種裝置、作業系統和軟體版本建立標準的重要性。

> ***我們選擇用 Red Hat Ansible Automation Platform 解決問題，因為這個平台可以和任何對象通訊。***
>
> Agile Defense 解決方案工程師 Shawn Draper

Ansible Playbooks 的安全性優勢

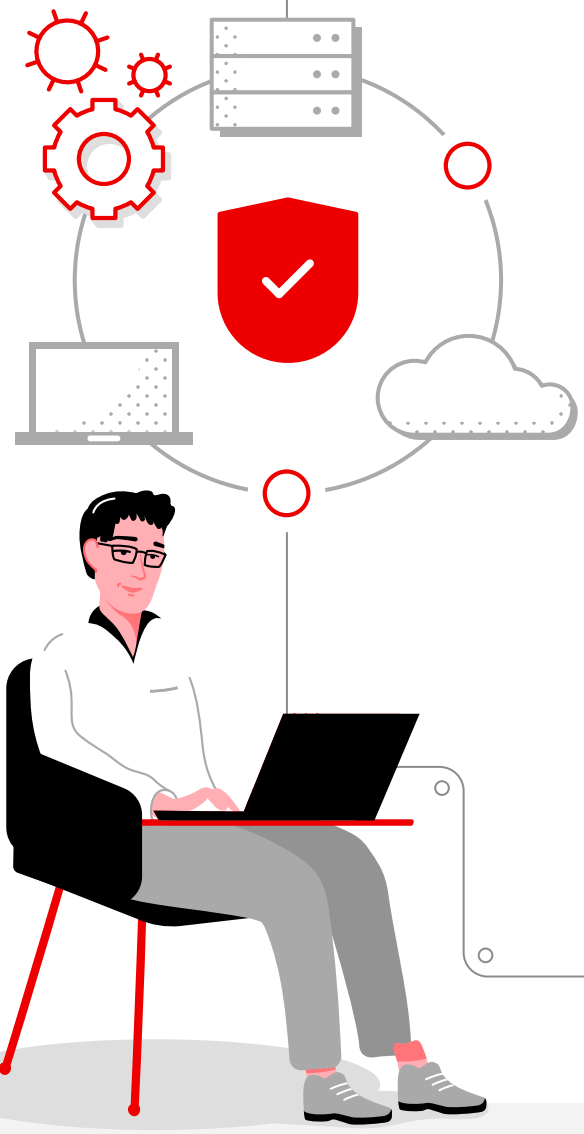
CPaaS 運用 Red Hat Ansible Automation Platform 的設定管理自動化功能，來稽核暴露在外的弱點。「Red Hat Ansible Automation Platform 可以連結裝置，並執行在 Ansible Playbook 中指定的命令。」Draper 表示。

CPaaS 自動辨識設定錯誤後，也可以依循自訂 Ansible Playbook 中的命令來自動修復錯誤。Agile Defense 已經建立多種劇本，分別用於測試不同類型的裝置。其中包括適用於 Red Hat 平台、Windows 裝置、VMware Hypervisor、Cisco 路由器與交換器，以及防火牆的劇本。



客戶用於稽核的時間減少

CPaaS 可以自動產出所有必要的文件，協助處理所有的文書作業。更特別的是，CPaaS 會利用 Ansible Automation Platform 編寫 XML 檢查檔案 (可在 DISA 的 STIG Viewer 中檢視)，來檢查網路上的所有裝置和已辨識的弱點，供稽核人員檢視。這類成品可以顯示目前狀態資訊，並指出特定的安全性設定已完成實作。Ansible Automation Platform 也讓客戶可以延伸 CPaaS 的功能，來管理工作流程與程式庫、安排稽核時間，以及引進角色存取控制。CPaaS 也可以確保裝置之間的一致性。



> ***自動化的一大優勢，就是每一次都能達到相同的效果。***
>
> Shawn Draper

面對網路威脅，主動監控由 CPaaS 提供的機構安全性態勢是做足準備的重要一環。過去，這種監控方式需要投入大量資源，而且必須在端點裝置上另外安裝軟體。使用 Ansible Automation Platform 掃描暴露在外的弱點之後，Agile Defense 的 CPaaS 為美國政府客戶省下 98% 的稽核時間。

下載
Agile Defense 成功案例

4

Cepsa 利用 Red Hat Ansible Automation Platform 提升效率

國際能源與化學公司 Cepsa 的目標是達成全球減碳。2022 年，該公司制定策略，要成為永續運輸、生質燃料和綠氫的領導者，將業務重心放在西班牙與葡萄牙，並以能源轉型作為重要基準。

Cepsa 必須在提高效率和確保合規的同時，降低成本、風險和停機時間，才能成功。為了達到這項目標，公司開始將流程自動化，以節省工時、改善服務反應時間，並提升 IT 安全性。Cepsa 與 Red Hat 諮詢服務合作，採用 Red Hat Ansible Automation Platform，在自動化主管的帶領下，讓自動化成為創新策略的核心支柱。最後，Cepsa 的生產力提升 35%，反應次數也增加 10–15%。

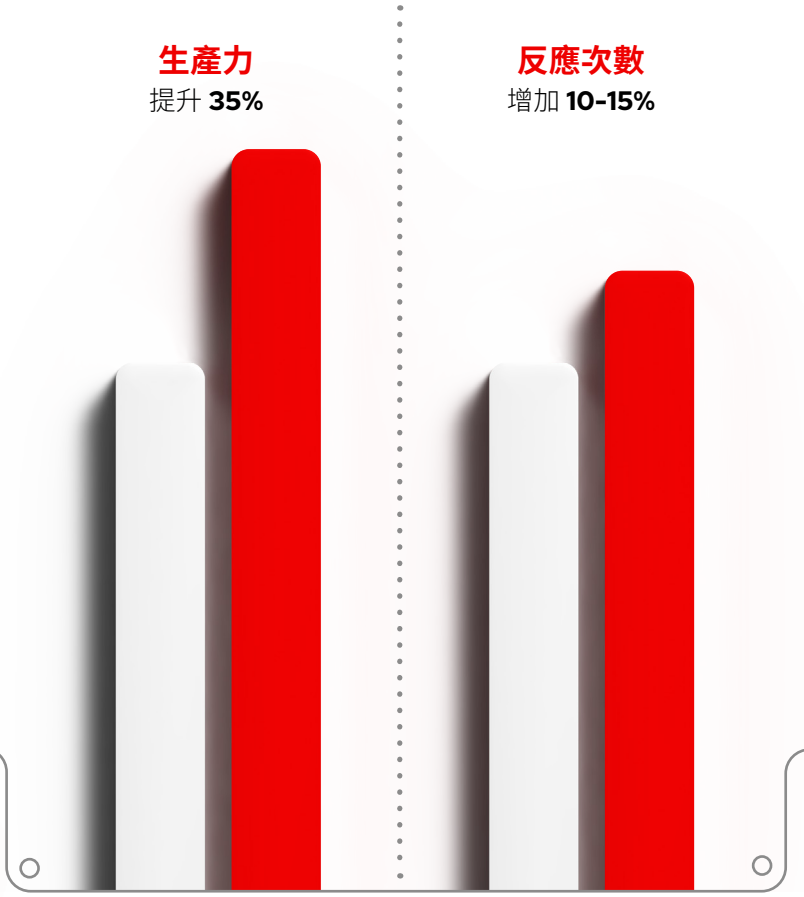
強化存取控制以改善 IT 安全性

Cepsa 初期的自動化專案宣告成功，並且與 Red Hat 長期合作之後，公司決定將 Ansible 延伸應用至整個企業。Ansible Automation Platform 為 Cepsa 提供受支援的基礎，可大規模建置和操作自動化服務，以及可編製的協作型受信任執行環境。不僅效率因此提升，還能將安全性至關重要的複雜 IT 環境標準化。

Ansible 的劇本語法易於理解，讓 Cepsa 可以為內部系統的任何環節定義安全性參數，不論是設定防火牆規則、鎖定使用者和群組，或者套用自訂安全性原則都沒有問題。標準化流程也有助於 Cepsa 減少內部系統額外安全性管理權限的數量，進而降低風險。現在，Cepsa 依照職位和部門將使用者分組，以確保授予適當的權限層級，並避免過度存取。

最後，Cepsa 的生產力提升 35%，反應次數也增加 10–15%。

現在技術人員不需要登入資料就可以存取 Ansible Automation Platform，並且重新啟動服務，讓他們可以確保流程會以程式碼預先定義的相同方式執行。



自動化技術是正面文化轉變的助力，可以促進團隊之間的協同合作。Red Hat 和我們合作，落實最佳做法，整個組織都因為他們的專業知識而獲益良多。

Cepsa 開發與營運部門
自動化經理 Francisco José Martín

透過專業自動化指引轉型為以安全性為重的文化

Red Hat Consulting 協助 Cepsa 實行所需的變革，讓全新自動化技術和方法能發揮出最大價值。Red Hat 專家從旁協助 Cepsa 團隊，讓該公司瞭解敏捷工作方法以及透過持續整合和持續交付 (CI/CD) 方法持續改善品質的重要性。

下載
Cepsa 成功案例

5

SIEMENS

Siemens 運用 Red Hat Ansible Automation Platform 提升通訊安全性

Siemens 是歐洲最大的工程公司，總部位於德國慕尼黑。作為跨國科技集團，Siemens 將發展重點放在電動化，從發電、傳輸和配電，到智慧電網解決方案，以及高效率電力應用方式。

由於業務相當敏感，Siemens 致力於維持在安全性技術方面的領先地位。為了確實保護機密資訊的存取，Siemens 的 295,000 名員工和其商業合作夥伴的 100,000 員工都使用公開金鑰基礎架構 (PKI)，以檢查公開金鑰的憑證與身分。擴大採用這項技術的目的是確保物聯網 (IoT) 通訊的安全。目前公司要維護兩種用於不同應用程式應用情境的 PKI 環境。

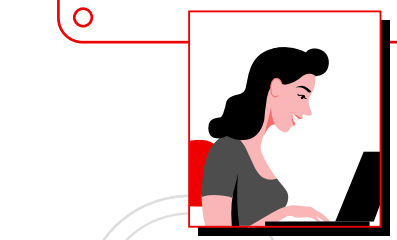
> ***這一點之所以如此重要，是因為 Red Hat Ansible Automation Platform 的基礎架構即程式碼做法不只是引進新工具，而是需要系統管理員徹底改變思維。***
>
> Siemens 公開金鑰基礎架構 (PKI) 主管
> Rufus Buschart

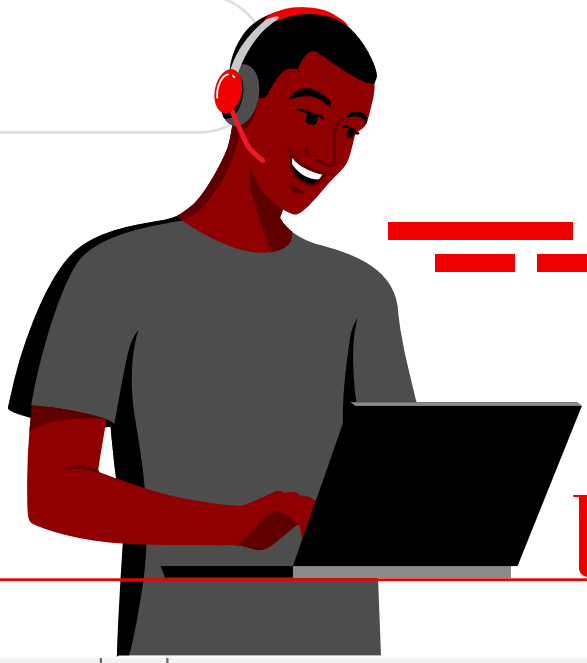
每當我們需要 Red Hat，他們的團隊都不會讓我們失望。我們的願景是與他們合作，開發出自動化的最佳做法平台，將組織效率和創新能力最佳化。

Rufus Buschart

隨著組織內各個服務團隊之間的通訊需求增加，Siemens PKI 團隊面對的設定複雜度也越來越高。為支援這項需求，Siemens 選擇用 Ansible Automation Platform 取代舊版自動化解決方案。

採用 Ansible Automation Platform 之後，現在 Siemens 可以將管理工作自動化、協助提升設定品質，並協助改善公司整體的通訊安全性。此外，Siemens 也受益於 Red Hat 的專業知識，並規劃與 Red Hat 合作深入研究，要將測試流程自動化，以建立持續部署的通用藍圖為目標。





下載
Siemens 成功案例

結論

Ansible Automation Platform 可協助組織管理自動化安全性系統，預先防範惡意攻擊。Ansible 提供數百種模組，可協助安全性團隊將 IT 環境與 IT 流程的所有層面自動化，並整合多個團隊來保護複雜的周邊安全性，同時統一安全性做法和強化安全性態勢。

Ansible Automation 可協助安全性團隊：

串連工作流程與劇本，以重複使用模組。

安全性團隊可以設定一連串共用程式庫、劇本或權限的工作，將調查或修復工作徹底自動化。

支援本機目錄服務與存取設定。

將使用者目錄服務與基礎架構配對之後，安全性團隊可以集中管理工作的存取與執行、將作業子集指派給特定角色，並且與其他群組共同處理工作。

整合並集中管理記錄。

整合第三方外部記錄彙總服務，有助於安全性團隊辨識趨勢、分析基礎架構事件、監控異常情況，以及歸納分散事件的關聯性。

使用 RESTful API 整合外部應用程式。

安全性團隊可以運用 Red Hat Ansible Automation Platform 管理其他企業級應用程式，例如安全性調度與自動化反應 (SOAR) 解決方案。

運用自動化功能
強化安全性態勢。

深入瞭解
Red Hat Ansible Automation Platform。

北美地區
1 888 REDHAT1
www.redhat.com

歐洲、中東與非洲地區
00800 7334 2835
europe@redhat.com

亞太地區
+65 6490 4200
apac@redhat.com

拉丁美洲地區
+54 11 4329 7300
info-latam@redhat.com