CIMCOR

解決方案簡介

了解如何使用CIS基準強化系統

安全設定

CIS基準CIS Benchmarks™是確保設定安全的最佳實踐指南。他們是基於共識的各國政府、企業、行業與學術界公認的最佳做法與標準作為眾多設備與平台的推薦設定。

當組織安裝新的作業系統或應用程式時，預設情況下沒有任何東西是安全的，並且一切都已開啟。這包括打開的端口、正在運行的應用程式服務等。CIS Benchmarks™可幫助您以強化的方式設定新的作業系統或應用程式。CIS Benchmarks™已整合到CimTrak的法規遵循模組中，CimTrak在其中提供詳細的警報、報告與控制以：

»評估設定的目前狀態。
»提供必要的步驟，並根據建議的CIS基準糾正任何設定錯誤或安全漏洞。
»當預期的正確的狀態"出現意外、不必要或未經授權的異動時發出警報。
»防止特定的檔案和/或設定異動。
»允許基於異常的規則與獨特的環境和安全條件保持一致。
»如果基準遭到破壞，則進行修護並返轉roll-back到以前的已知與受信任狀態。

無論您是在內部on-premise還是在雲端cloud進行操作，都可以保持CIS Benchmark™的法規遵循。
所有這些都以可客製化、以易於閱讀的圖形界面表示來簡化實現目標的工作。

產品特點

易於使用

CIS基準CIS Benchmarks™與CimTrak完全結合在一起，具有基準庫，可以立即使用與選擇。

增加安全性

利用CIS基準CIS Benchmarks™ 測試與加強工作有助於緩解由於系統設定錯誤而引起的許多常見威脅。

減少並消除存取點

刪除不必要的檔案、軟體與應用程式可以減少惡意行為者可以利用的存取點數量。

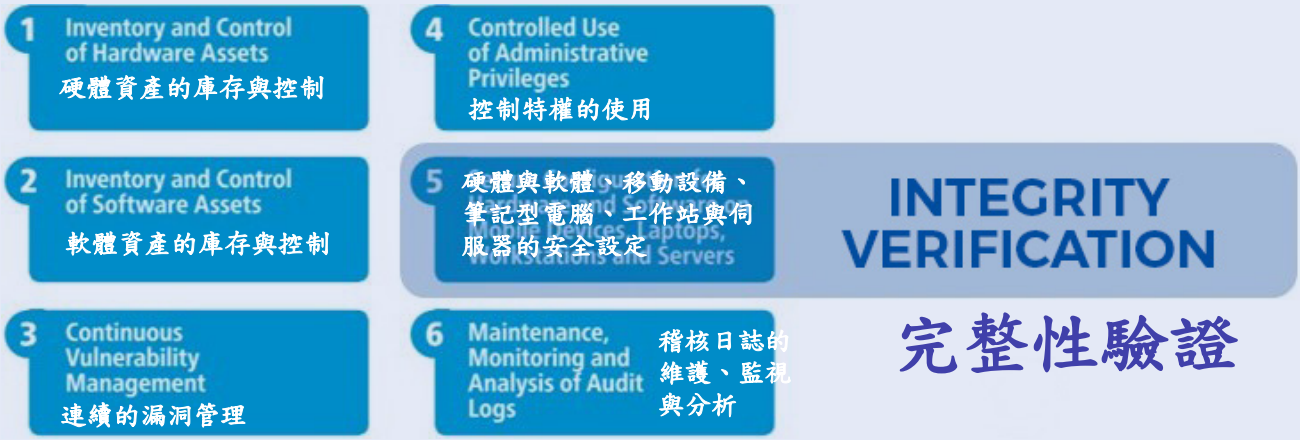
提高效能

如果系統不會承受不必要的服務或無法在有限的記憶體與空間下執行，那麼系統將更高效地工作。

如果遵循CIS Top 20控制規定的最佳實踐，則CimTrak專門提供必要的控制來管理設定與異動管理過程，以防止攻擊者利用漏洞服務與設定。

這就是Cimcor所謂的完整性驗證與保證對於CIS“基本控制”的形成與構建至關重要，特別是在CIS控制5中進行了定義。

基本CIS控制™



“基於我們在國防部、情報界與政府其他部門的廣泛測試，對我來說很清楚–安全設定管理是任何成功的程式安全管理的基本，必不可少的要素。”

TONY SAGER, CIS
高級副總裁兼首席傳播者

CIS SecureSuite® Membership　CIS CyberMarket®

此外CimTrak利用相容SCAP 1.2（安全自動化協定Security Automation Protocol）的掃描引擎來監視設定元素，批准的異常與警報並報告未經授權的異動。這也有助於組織成為FedRAMP相容。

如今，有超過150個CIS基準CIS Benchmarks™。目前CimTrak中包含70多個相關基準，並且我們的列表會不斷進行修改、更新與定期增加新的基準。大多數CIS基準包括多個設定描述檔案configuration profile。這些設定檔案描述並定義了指派給各種基準建議的設定。

»1級設定檔案被認為是最基本的要求basic requirement，對操作與性能的影響最小。目的是在考慮對整體業務需求與功能的影響的同時，最大限度地減少攻擊面。
»2級設定檔案是CIS所謂的防禦和深度“defense and depth”，其目的是在安全對於組織整體業務生計與可持續性至關重要的時刻以及最大程度實現安全態勢。

對應與法規遵循

Cimcor使用CIS Benchmarks™對應消除了各種法規遵循要求的麻煩與困惑，從而簡化了評估、維護、報告和糾正設定錯誤的設備的工作。

Show: All / None

Mapping Name	Pass/Fail	Total Tests	Pass Tests	Fail Tests	Waived Tests	Percentage
CIS Controls	Fail	0	665	460	0	59.11%

CIS Controls						
1 - Inventory and Control of Hardware Assets						
1.1 - Utilize an Active Discovery Tool						
1.2 - Use a Passive Asset Discovery Tool						
1.3 - Use DHCP Logging to Update Asset Inventory						
1.4 - Maintain Detailed Asset Inventory						
1.5 - Maintain Asset Inventory Information						
▶ 1.6 - Address Unauthorized Assets	Pass: 0	Fail: 1	Skip: 0	Waived: 0	Total: 1	Pass: 0.00%
1.7 - Deploy Port Level Access Control						
1.8 - Utilize Client Certificates to Authenticate Hardware Assets						
2 - Inventory and Control of Software Assets						
2.1 - Maintain Inventory of Authorized Software						
2.2 - Ensure Software is Supported by Vendor						
2.3 - Utilize Software Inventory Tools						
2.4 - Track Software Inventory Information						
2.5 - Integrate Software and Hardware Asset Inventories						
2.6 - Address unapproved software						
2.7 - Utilize Application Whitelisting						
2.8 - Implement Application Whitelisting of Libraries						
2.9 - Implomont Application Whitelisting of Scripts						
2.10 - Physically or Logically Segregate High Risk Applications						
▶ 3 - Continuous Vulnerability Management	Pass: 1	Fail: 0	Skip: 0	Waived: 0	Total: 1	Pass: 100.00%
3.1 - Run Automated Vulnerability Scanning Tools						
3.2 - Perform Authenticated Vulnerability Scanning						
3.3 - Protect Dedicated Assessment Accounts						
▶ 3.4 - Deploy Automated Operating System Patch Management Tools	Pass: 11	Fail: 0	Skip: 0	Waived: 0	Total: 11	Pass: 100.00%
3.5 - Deploy Automated Software Patch Management Tools						
3.6 - Compare Back-to-back Vulnerability Scans						
3.7 - Utilize a Risk-rating Process						
4 - Controlled Use of Administrative Privileges						
4.1 - Maintain Inventory of Administrative Accounts						
4.2 - Change Default Passwords						
▶ 4.3 - Ensure the Use of Dedicated Administrative Accounts	Pass: 2	Fail: 0	Skip: 0	Waived: 0	Total: 2	Pass: 100.00%

法規遵循工作包括：

PCI DSS
NIST 800-53
NIST 800-171
GDPR
DISA STIGS
SOX SARBANES OXLEY 404
HIPAA
ISO 27K
還有更多

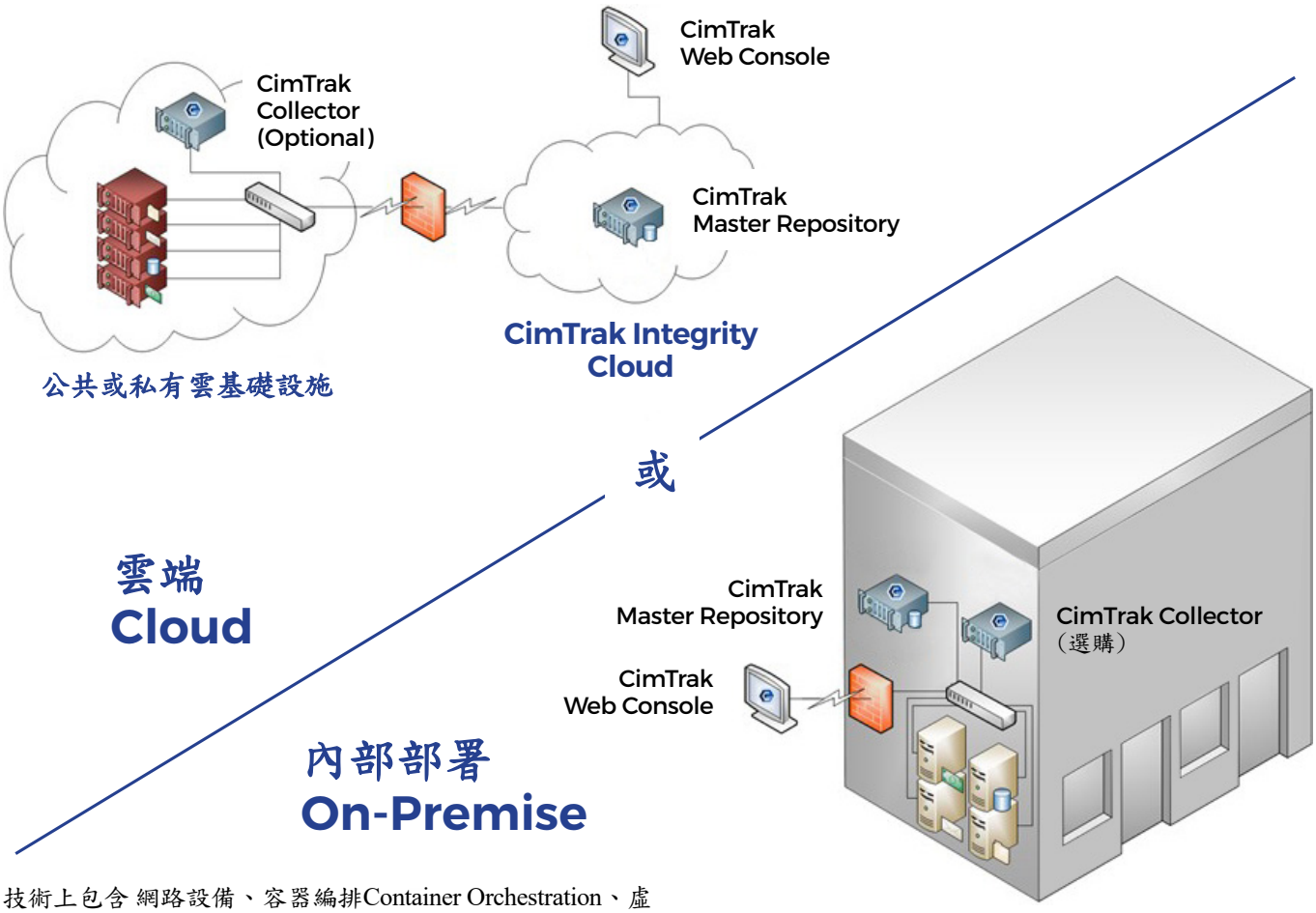
CimTrak中整合的基準包括：

AMAZON LINUX
APPLE OS
CENTOS LINUX CISCO
DEBIAN LINUX
FEDORA FAMILY
LINUX GOOGLE
CHROME IBM AIX
MIT KERBEROS
MICROSOFT IIS
MICROSOFT OFFICE
MICROSOFT SQL SERVER
MICROSOFT WEB BROWSER
MICROSOFT WINDOWS DESKTOP
MICROSOFT WINDOWS SERVER
MONGODB
MOZILLA FIREFOX
NGINX
ORACLE DATABASE
ORACLE LINUX
ORACLE MYSQL
ORACLE SOLARIS
POSTGRESQL
RED HAT ENTERPRISE
LINUX SUSE LINUX
UBUNTU LINUX
VMWARE
AND MANY MORE

管理與架構

CimTrak的CIS Benchmark™法規遵循模組Compliance Module是CimTrak Integrity Suite的加購功能，旨在簡化您的CIS Benchmark需求。它的儀表板與報告功能非常直覺，可以單一檢視查看測試結果與法規遵循評分。此視圖提供了通用的CIS法規遵循要求，並作為一個單獨的測試與修護說明進行了說明，以幫助您的組織完全實現CIS法規遵循，並確保保持這種狀態。法規遵循模組可以在本地或雲端中執行。

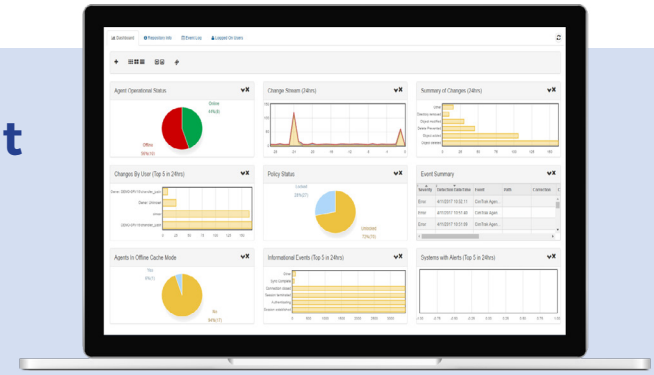
CimTrak可在內部部署On-Premise或在雲端Cloud使用



**當技術上包含 網路設備、容器編排Container Orchestration、虛擬化管理程序Hypervisors與法規遵循時必須有CimTrak Collector。

Test CimTrak in your environment today with a Free Trial

»TRY CIMTRAK NOW



支援平台

CimTrak for Servers, Critical Workstations & POS Systems
WINDOWS: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise
WINDOWS SERVER: 2003, 2008, 2012, 2016, 2019
LINUX: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle
SUN SOLARIS: x86, SPARC Red Hat, SUSE, Ubuntu, others
MAC: Intel, Power PC
HP-UX: Itanium, PA-RISC
AIX

監控的Windows參數
FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES: compressed, hidden, offline, read-only, archive, reparse point
Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

監控的Unix參數
FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

支援的網路設備 CimTrak For Network Devices
Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Netgear, NetScreen, Palo Alto, Others

支援的資料庫 CimTrak For Databases
Oracle, IBM DB2, Microsoft SQL Server
MySQL PARAMETERS MONITORED, Default rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored procedures, Table definitions, Triggers, User defined data types, Users, Views

支援的虛擬化管理程序Hypervisors
Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

支援的雲端平台
Google Cloud, Amazon AWS, Microsoft Azure

支援的容器編排 Container & Orchestration 整合
Docker, Docker Enterprise, Kubernetes, Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS)

支援的票務Ticketing 整合
CA ServiceDesk, Atlassian Jira, ServiceNow, BMC Remedy

支援的 SEIM 整合
IBM QRadar, McAfee Event Security Manager, Splunk, LogRhythm, Microfocus Arcsight, and others

CIMCOR

Cimcor開發了創新的下一代檔案完整性監控File Integrity Monitoring軟體。CimTrak Integrity Suite即時監控與保護各種實體、網路、和虛擬IT資產，同時提供有關所有異動的詳細舉證資訊。使用CimTrak保護基礎設施可幫助您遵循法規並保持這種狀態。

詳細 Cimcor 公司 Cimtrak 產品資訊請聯繫
台灣地區代理商 商丞科技 02-29148001