

「WannaCry」強調勒索軟體的威脅： 思科 ISE 涵蓋流程的每個步驟



資產可視性與
法規遵循



快速威脅
控管服務



軟體定義
分段

為了避免您略過來自 WannaCry 勒索軟體的大量攻擊，思科 TALOS 的研究人員會在本部落格中涵蓋相關內容，助您深入了解攻擊，確保安全無虞。WannaCry 影響了全世界成千上萬地點的電腦。惡意軟體會透過蠕蟲的形式散佈，在網路上掃描並感染其他有資安漏洞的設備。他們有什麼要求？惡意軟體會指使感染的使用者在六小時內支付與 \$300 美元等值的比特幣，否則贖金將會提高。

擁有思科 ISE 的客戶可享有完善保護，抵抗這類攻擊。事實上，ISE 可透過許多方式保護您，防止、停止甚至減緩勒索軟體的威脅。

專用思科 ISE 勒索軟體

如要深入瞭解勒索軟體
專用思科 ISE 相關功
能，請前往：
cisco.com/go/ise。

資產可視性 法規遵循

查看網路上有哪些裝置的功能不可忽視，因為您無法保護看不到的裝置。這代表不只看到使用者和裝置的詳細資料，也包含特定裝置的作業系統、防毒軟體、應用程式、硬體、防火牆涵蓋範圍等項目的實際狀態。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main menu includes 'Authentication', 'Authorization', 'Profiling', 'Posture', and 'Client Provisioning'. The 'Policy Elements' dropdown is expanded to show 'Dictionaries', 'Conditions', and 'Results'. The 'Conditions' section is active, displaying a list of 'File Conditions'. The table below shows the details of these conditions:

Name	Description
MS17-010	
<input type="checkbox"/> pc_Vista64_KB4012598_MS17-010	Cisco Predefined Check: Microsoft Security Bulletin M...
<input type="checkbox"/> pc_Vista_KB4012598_MS17-010	Cisco Predefined Check: Microsoft Security Bulletin M...
<input type="checkbox"/> pc_W10_64_KB4019474_MS17-05-03_Ms17-010	Cisco Predefined Check: Microsoft Security Bulletin M...
<input type="checkbox"/> pc_W10_KB4019474_MS17-05-03_Ms17-010	Cisco Predefined Check: Microsoft Security Bulletin M...
<input type="checkbox"/> pc_W81_KB4019215_MS17-05-03_Ms17-010	Cisco Predefined Check: Microsoft Security Bulletin M...
<input type="checkbox"/> pc_W81_64_KB4019215_MS17-05-03_Ms17-010	Cisco Predefined Check: Microsoft Security Bulletin M...
<input type="checkbox"/> pc_W8_KB4012598_MS17-010	Cisco Predefined Check: Microsoft Security Bulletin M...
<input type="checkbox"/> pc_W8_64_KB4012598_MS17-010	Cisco Predefined Check: Microsoft Security Bulletin M...
<input type="checkbox"/> pc_W7_64_KB4019264_MS17-05-03_Ms17-010	Cisco Predefined Check: Microsoft Security Bulletin M...
<input type="checkbox"/> pc_W7_KB4019264_MS17-05-03_Ms17-010	Cisco Predefined Check: Microsoft Security Bulletin M...

以 Wannacry 而言，思科 ISE 可根據套用的修補程式，判斷使用者是否會遭到攻擊。遵守適當的修補程式法規遵循政策，可根據可視性強制執行相關原則。

您甚至可以特別撰寫狀態原則，找出初始檔案位置「C:\Windows\mssecsvc.exe」，然後立即將該裝置從網路上隔離。

快速威脅 遏止服務：

ISE 從其他思科資安產品和第三方解決方案取得威脅和弱點的情報，控管端點的存取權限層級。思科 AMP 和 CTA 可透過 STIX 格式提供端點威脅分級，ISE 可根據其行為控制端點，防止進一步遭到網路存取感染。與弱點評量供應商（例如 Qualys、Rapid7 和 Tenable）整合可掃描端點的弱點，並找出 WannaCry 是否可以使用永恆之藍漏洞程式。找到後，ISE 會自動收到警示，使用「高」CVSS 分數顯示端點的弱點狀態並封鎖裝置。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area is titled 'Endpoints' and shows details for a specific endpoint with MAC address 00:50:B6:70:5B:5B. The endpoint profile is 'Windows7-Workstation' and its current IP address is 10.40.132.131. The 'Vulnerabilities' tab is active, displaying a vulnerability alert with the following details:

- Title: Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010) and Shadow Brokers
- CVSS score: 9.3
- CVEIDS: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148
- Reported by: Qualys
- Reported at: Mon May 08 14:42:11 PDT 2017

Below the vulnerability alert, there is an 'Authorization Policy' section with a dropdown menu set to 'First Matched Rule Applies'. Underneath, there is a table of exceptions:

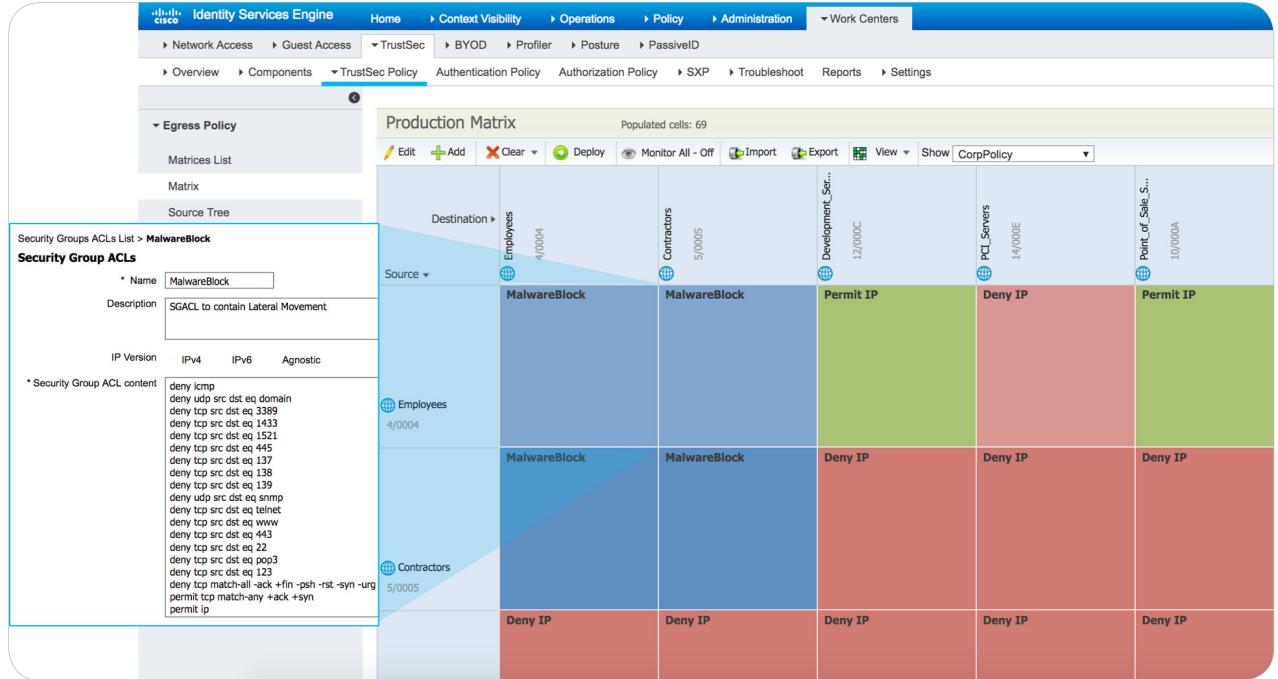
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Vulnerable Assets Policy	if (Threat:Qualys-CVSS_Base_Score GREATER 5 OR Threat:Rapid7 Nexpose-CVSS_Base_Score GREATER 5 OR Threat:Tenable Security Center-CVSS_Base_Score GREATER 5)	then Quarantined_Systems AND RemediationAccess

ISE 也可以收到相關警示，隔離遭入侵的裝置。無論 ISE 是與思科 Firepower 或 Stealthwatch 或任一思科技術夥伴整合，您都可以立即自動回應並控制威脅。例如，Stealthwatch 會依據攻擊的階段觸發 [WannaCry 的安全性事件](#)：Addr_Scan on port

445/tcp、High SMB Peers、Worm Activity、Worm Propagation 和 Connection to Tor。一旦確認為惡意攻擊，只要按一下按鈕即可向 ISE 回報，將攻擊來源裝置從網路隔離。

軟體已定義 區段：

入侵的可能性極高。無論面對零日攻擊 (Day Zero Attack) 或是像「Wanna Cry」這類攻擊已知弱點的漏洞程式，可擴充、可調整的網路區段都可以有效降低 (或一次性阻止) 勒索軟體在系統間散佈。思科 TrustSec 改變了啟用軟體定義區段的遊戲規則，強制執行快速靈活的群組政策。這讓限制任何大小網路的橫向運動變得可行，甚至可將相同類別的使用者/裝置建立微區段。[瞭解詳情](#)。



DEFCON 原則集可大幅加強您的事件回應手冊中，應對系統攻擊的預先定義回應方式。變更 DEFCON 狀態不會變更個別使用者和裝置授權，或是手動實作原則變更，而是會變更定義使用者、裝置與系統如何交流的 TrustSec 原則，基本上會關閉「網路吊橋」，保護您的重要資料並維持基礎服務。例如，您可以將 DEFCON 4 定義為移除所有網路中的訪客，將 DEFCON 3 定義為移除所有網路中的自攜裝置使用者，將 DEFCON 2 定義為限制點對點的流量，並

將 DEFCON 1 定義為嚴格限制您「皇冠珠寶」的存取權。

如您所見，透過思科 ISE 處理勒索軟體攻擊的方式有許多種。對於現今威脅的規模與複雜度，目前仍沒有一勞永逸的解藥。因此思科提供有效的安全性解決方案組合，不僅簡單易用、開放存取，且全面自動化。

如要深入瞭解勒索軟體專用思科 ISE 相關功能，請前往：cisco.com/go/ise。