**在ENS中使用專家規則來防止惡意利用**

專家規則是基於文本的自定義規則，可以在ENS Threat Prevention 10.5.3+中的“利用阻止”策略中創建。與可以在訪問保護策略中創建的自定義規則相比，專家規則提供了更多參數，並提供了更大的靈活性。它還允許系統管理以非常精細的級別控制/監視端點系統。專家規則不依賴於用戶模式掛鉤。因此，它們對系統性能的影響很小。創建此博客是作為基本指南，向我們的客戶展示如何創建他們以及可以幫助阻止哪些威脅。結論中可以找到更多詳細信息。

**專家規則如何運作**

以下各節說明如何通過EPO和ENS添加專家規則。

**從EPO添加專家規則**

1.選擇**系統樹| 子組（例如：ens\_10.6.0）| 分配的政策| 產品（端點安全威脅防護）| 漏洞利用防護（我的默認設置）**



2.導航到**簽名**，然後單擊**添加專家規則**。



3.在“ **規則”**部分中，填寫字段。

一種。選擇規則的嚴重性和操作。嚴重性僅提供信息；它沒有對規則操作的選擇。

b。選擇要創建的規則類型。該**規則內容**字段填入模板選定類型。

C。更改模板代碼以指定規則的行為。



選擇新的類類型時，“規則內容”字段中的代碼將替換為相應的模板代碼。Endpoint Security從20000開始自動分配ID號。EndpointSecurity *不會限制您可以創建的專家規則的數量。*

4.保存規則，然後保存設置。

5.將策略強制應用於客戶端系統。

6.在客戶端系統上驗證新的專家規則。

**直接在端點上添加專家規則：**

如果我們需要從EPO添加專家規則，它將被推送到整個EPO“​​ WORKGROUP”的所有端點。在某些情況下，可能需要在非EPO（非企業環境中，通過獨立設置安裝ENS）的一/兩個系統或ENS系統中應用專家規則；在這種情況下，必須將專家規則直接添加到端點。可以使用McAfee Endpoint Security UI在Endpoint系統上直接編寫和應用專家規則。步驟如下：

1.打開McAfee Endpoint Security。轉到**設置**。



2.轉到**威脅預防| 顯示高級。**



3.向下滾動到“專家規則”部分，然後單擊“ **添加專家規則”。**



4.專家規則編譯器應彈出，最終用戶可以在其中直接編寫和編譯專家規則，並在編譯後將規則強制應用到系統。



如果專家規則中沒有語法錯誤，則可以通過單擊“強制”按鈕將其應用到系統中。如果存在語法錯誤，則可以在日誌文件％ProgramData％\ McAfee \ Endpoint Security \ Logs \ ExploitPrevention\_Debug.log中找到詳細信息

**測試規則**

創建新規則時，應首先在“報告”模式下對其進行測試，以便可以觀察到檢測結果。在獲得對規則足夠的信心後，可以將其轉到“阻止”模式。

**專家規則示例：**

**基本規則：**

以下規則將檢測cmd.exe的實例，該實例在c：\ temp下創建任何文件。*請注意，cmd.exe可以由任何用戶和系統的任何部分運行。*

規則 {

流程{

包括OBJECT\_NAME {-v“ cmd.exe”}

}

目標{

匹配FILE {

包括OBJECT\_NAME {-v“ c：\\ temp \\ \*\*”}

包括-訪問“創建”

}

}

}

**它針對特定的惡意行為的規則：**

可以創建以下規則來幫助阻止由各種惡意軟件家族和攻擊技術執行的特定惡意活動。

**阻止遠程過程注入的專家規則[MITRE技術過程注入**[**T1055**](https://attack.mitre.org/techniques/T1055/)**]：**

規則 {

流程{

包括OBJECT\_NAME {-v“ \*\*”}

排除OBJECT\_NAME {-v“ SYSTEM”}

排除OBJECT\_NAME {-v“％windir％\\ System32 \\ WBEM \\ WMIPRVSE.EXE”}

排除OBJECT\_NAME {-v“％windir％\\ System32 \\ CSRSS.EXE”}

排除OBJECT\_NAME {-v“％windir％\\ System32 \\ WERFAULT.EXE”}

排除OBJECT\_NAME {-v“％windir％\\ System32 \\ SERVICES.EXE”}

排除OBJECT\_NAME {-v“ \* \\ GOOGLE \\ CHROME \\ APPLICATION \\ CHROME.EXE”}

}

目標{

匹配THREAD {

包括OBJECT\_NAME {-v“ \*\*”}

排除OBJECT\_NAME {-v“ \*\* \\ MEMCOMPRESSION”}

排除OBJECT\_NAME {-v“％windir％\\ System32 \\ WERFAULT.EXE”}

包括-access“寫”

}

}

}

**通過訪問lsass.exe內存來防止powershell.exe和powershell\_ise.exe進程轉儲憑據的專家規則[MITER**[**TECHNOLOGY**](https://attack.mitre.org/techniques/T1003/)**Credential Dumping**[**T1003**](https://attack.mitre.org/techniques/T1003/)**]：**

規則 {

流程{

包括OBJECT\_NAME {-v“ powershell.exe”}

包括OBJECT\_NAME {-v“ powershell\_ise.exe”}

排除VTP\_PRIVILEGES類型的BITMASK {-v 0x8}

}

目標{

匹配過程{

包括OBJECT\_NAME {-v“ lsass.exe”}

包括-nt\_access“！0x10”

排除-nt\_access“！0x400”

}

}

}

**專家規則，可防止使用“ SchTasks.exe”實用程序[MITRE技術預定任務**[**T1053**](https://attack.mitre.org/techniques/T1053/)**] 創建可疑任務（PowerShell腳本或批處理文件）：**

規則 {

流程{

包括OBJECT\_NAME {-v“ SchTasks.exe”}

包括PROCESS\_CMD\_LINE {-v“ \* / Create \*”}

}

目標{

匹配過程{

包括PROCESS\_CMD\_LINE {-v“ \*\*。bat \*\*”}

}

匹配過程{

包括PROCESS\_CMD\_LINE {-v“ \*\*。ps1 \*\*”}

}

}

}

**防止啟動條目創建的專家規則[MITER Technique Persistence**[**T1060**](https://attack.mitre.org/techniques/T1060/)**]：**

攻擊者可以使用多種技術來通過系統重新啟動來保持持久性。最受歡迎的技術之一是在“ **啟動”**文件夾中創建條目。以下專家規則將阻止任何進程在“啟動”文件夾中創建文件。最近，互聯網目睹了對已存在十年的WinRAR漏洞（CVE-2018-20251）的全面利用，可以通過將文件拖放到啟動目錄中來加以利用。以下專家規則也將阻止此類嘗試。

規則 {

流程{

包括OBJECT\_NAME {-v \*\*}

}

目標{

匹配FILE {

包括OBJECT\_NAME {-v“ \*\* \\ AppData \\ Roaming \\ Microsoft \\ Windows \\開始菜單\\ Programs \\ Startup \\ \*\*”}

包括-訪問“創建寫”

}

}

}

**在Adobe Reader中阻止JavaScript執行的專家規則：**

利用客戶端軟件漏洞來在網絡中獲得初步立足並不新鮮[MITRE技術[T1203](https://attack.mitre.org/techniques/T1203/) ]。Adobe Reader是一個非常受歡迎的目標，因為與其他任何瀏覽器一樣，它也支持JavaScript，這使得利用變得更加容易。可以在任何網絡中部署以下專家規則，以防止Adobe Reader執行任何類型的JavaScript。

規則 {

流程{

包括OBJECT\_NAME {-v“ AcroRd32.exe”}

}

目標{

匹配第{

包括OBJECT\_NAME {-v“ EScript.api”}

}

}

}

下表顯示了以上四個專家規則在Miter Att＆ck矩陣中的排列方式。

