

資安攻擊防禦模組

網路攻擊愈趨複雜，DDoS攻擊、APT攻擊、網路入侵、惡意程式、跨網站指令碼（Cross-Site Scripting）等攻擊勒索軟體無所不在，需一有效方案可有效防護，並統一管理，並提供多樣統計報表以掌握資安防護全局。

APT攻擊防禦模組

導入新世代資安管理平台暨端點勒索軟體防護，防護APT攻擊、網路入侵、惡意程式、勒索軟體、殭屍網路等複雜網路攻擊，並建立統一管理介面，多樣統計報表，大幅提升機關資安防護能力。

The screenshot displays a security incident response dashboard with the following sections:

- Header:** Incident ID: 645ee214-c8f1-442c-92a7-94...; Triggered By: Check Point SandBlast Agent Anti-Bot; Trigger Time: 2018/2/3 1:42:50.
- Entry Point:** tonic.exe created [bot.exe]
- Remediation (14 files):** A table listing files with their reputation and full paths.

REPUTATION	FILE NAME	FULL PATH	STATUS
🔴	tonic.exe	c:\program files (x86)\v2_studios\tonic\tonic.exe	🗑️
🔴	bot.exe	c:\program files (x86)\v2_studios\tonic\received files\bot.exe	🗑️
🟢	schtasks.exe	c:\windows\syswow64\schtasks.exe	🔍
🟢	schtasks.exe	c:\windows\syswow64\schtasks.exe	🔍
🟢	schtasks.exe	c:\windows\syswow64\schtasks.exe	🔍
🟢	powershell.exe	c:\windows\syswow64\windowspowershell\v1.0\powershell...	🔍
- Business Impact (11 events):** A table listing damaged files and their full paths.

DAMAGE	FILE NAME	FULL PATH
🔴	people.gif	c:\program files (x86)\v2_studios\tonic\images\people.gif
🔴	unknownimage.gif	c:\program files (x86)\v2_studios\tonic\images\unknownimage.gif
🔴	sp_santa.gif	c:\program files (x86)\v2_studios\tonic\images\sp_santa.gif
🔴	sp_principal_victoria.gif	c:\program files (x86)\v2_studios\tonic\images\sp_principal_victoria.gif
🔴	offline.wav	c:\program files (x86)\v2_studios\tonic\sounds\offline.wav
🔴	online.wav	c:\program files (x86)\v2_studios\tonic\sounds\online.wav
- Suspicious Activity (8 categories):** A list of event categories with severity indicators.
 - Script Execution (1 event)
 - System Security Policy Change (3 events)
 - Dropped File Deletion (1 event)
 - Persistence (6 events)
 - Dangerous Execution (5 events)
 - Dropped Executable (5 events)
- Incident Details (10 processes):** A process flow diagram showing the execution path of the malware.

特色

- 大幅提升資安防護能力
- 有效控制應用程式資安防護能力
- 避免勒索軟體攻擊
- 提供統計資訊，作為評估依據
- 完整報表，以利日後政策

DDoS防禦模組

建置DDoS防護系統，可防護府內各式對外服務遭受阻斷式服務攻擊，例如：網站、DNS服務等，除外對內之外也可偵測內對外阻斷服務攻擊，常見於府內電腦中毒感染病毒成為殭屍網路一員。



WAF網站防禦模組

網頁應用程式可說是由外而內的攻擊管道之一，欲防範諸如SQL資料隱碼 (SQL Injection)、跨網站指令碼 (Cross-Site Scripting) 等攻擊行為，大多會在網頁伺服器的前方建置WAF (Web Application Firewall，網頁應用程式防火牆) 來抵擋。如今面對駭客組織化、商業化後，促使攻擊手法隨時都在進步，WAF更必須與時俱進，因應攻擊手法的變化，來進行辨識與攔阻。

本模組除管理端外，使用端必須再購買使用授權

經銷商蓋章



華麗得股份有限公司
Hualeader Co., Ltd.
TEL : 02-89235035
service@hualeader.com