

Sandblast Mobile 整合 MobileIron

客戶需求:

客戶希望能夠透過 Sandblast Mobile 整合 MobileIron 之後,能夠強化手持裝置或手機的 APT 攻擊防禦,並且利用 MDM 功能達到進一步防堵受感染或觸發資安事件的裝置擴大影響。

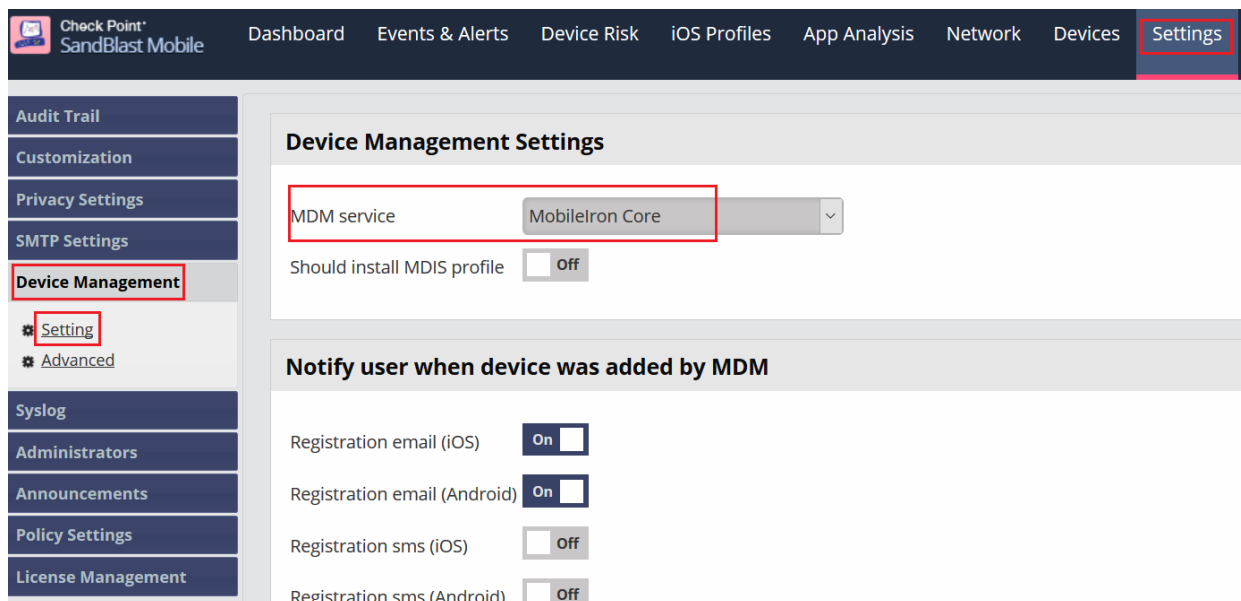
另外本文不討論 MobileIron 設定(雖然客戶的 MobileIron Policy 我也有調整)。

客戶環境:

- Sandblast Mobile 500U(用戶陸續上線中)
- MobileIron 一套

設定:

最重要的,要拿到 MobileIron 設定,MobileIron 分成 Core 和 Sentry 兩部份,Sentry 和終端裝置有關,主要設定在 Core 上面,拿到設定後就可以在 SBM 的 Portal→Settings→Device Management→Setting 把設定填入,如下圖:



The screenshot shows the Check Point SandBlast Mobile Settings page. The top navigation bar includes Dashboard, Events & Alerts, Device Risk, iOS Profiles, App Analysis, Network, Devices, and Settings. The left sidebar lists various settings categories, with Device Management selected. Under Device Management, the Setting option is highlighted. The main content area displays the Device Management Settings, where the MDM service is set to MobileIron Core. Below this, there is a checkbox for 'Should install MDIS profile' which is currently off. The section 'Notify user when device was added by MDM' contains four toggle switches: Registration email (iOS) is On, Registration email (Android) is On, Registration sms (iOS) is Off, and Registration sms (Android) is Off.

準備好你的 MobileIron 設定,填好它,請注意 MobileIron 需要公開憑證,如果您的環境沒有,SBM Portal 就會錯誤,下圖的客戶是正式環境所以沒有問題:

MOBILEIRON CONFIGURATION

General Settings

Server:

Username:

Password:

Label(s):

Mitigation label:

Device status attribute: Off

Device risk attribute: Off

Device TF attribute: Off

Import Personally Identifiable Information (PII)

Device owner name: On

Device phone number: On

Device owner email: On

SSL server Certificate

Advanced options: Off

Buttons: Verify, Cancel, Save

這張圖裡有幾個欄位要注意,必填的有:

Server:客戶的 MobileIron Core 對外的 FQDN

Username/Password:不用我說了吧

Label(s):SBM 和 MobileIron 建立連線之後,會同步 MobileIron 裝置到 SBM Portal 裡的資料庫,至於要同步哪些裝置,看得就是這個 Label 名稱,不要填錯。

非必要欄位:

Mitigation Label:當 SBM 發現裝置觸發資安事件時,會幫裝置貼標籤,這個客戶是用 infected,可自定,這個設定一開始非必要,但如果需要 MDM 做到感染裝置自動隔離或其它動作時,就需要這個標籤。

上述設定填完之後 SBM 會每十分鐘和 MobileIron 同步一次,把裝置撈到 Device 清單裡,如下圖:

ID	Name	Email	Device Num	Device type	OS version	Device details	Client version	Last seen	Status
46337	張	e	+8	IOS Device	10.2.1	iPhone / iPhone 5S	2.72.2.3891	2 hr	Active
46296	杜	h	No number	Android	8.0.0	HTC / HTC_M10h	2.72.4-RELEASE-b3196/3196	7 hr	Active
46294	黃	hi	No number	Android	7.0	HUAWEI / EVA-L09	2.72.4-RELEASE-b3196/3196	4 d	Active
46283	蓋	w	+8	IOS Device	10.3.1	iPhone / iPhone 5S	2.71.0.3799	4 d	Active
41949	j 施	ni	+88	IOS Device	Unknown	unknown / unknown			User Notified
41681	MDMTEST5	MDMTEST	No number	IOS Device	Unknown	unknown / unknown			User Notified
2675	MDMTEST5	MDMTEST5	No number	IOS Device	Unknown	unknown / unknown			User Notified

因為已經和 MDM 產品整合,所以圖中某些功能都會反灰不能使用,如 Add new device,基本上看到這個,代表初始工作已經完成,可以針對要納管的裝置做啟動(Activation)了。

SBM 除非觸發資安事件,否則不會告訴管理員某某用戶安裝了什麼 APP,所以是保有隱私的:

The screenshot shows the 'App Analysis' section of the Check Point SandBlast Mobile console. The top navigation bar includes 'Dashboard', 'Events & Alerts', 'Device Risk', 'iOS Profiles', 'App Analysis', 'Network', 'Devices', and 'Settings'. The user 'nevillekuo@sysage.com.tw' is logged in. The main interface is divided into a left sidebar with a list of 1119 applications and a main content area for the selected app, '魔獸好戰友' (World of Warcraft Companion) by Blizzard Entertainment, Inc.

Application Details:

- Risk:** None
- Install base:** 1
- Policy:** Default
- Threat summary:** (None) This application was identified as legitimate. Location Access: This app might track device location. Tracking location can continue also after the app is closed.
- Description:** Requires an Internet connection and iPhone 4S, iPod touch 5th Generation, iPad 4th Generation or newer. The new World of Warcraft: Legion Companion app for iOS lets you make the most of your time in-game, wherever you may be. Use the app as mission control for you and your followers and easily track the progression of your Class Order Hall. TRACK WORLD QUESTS: View your active world quests and emissary bounties from directly within the app! You can check out the rewards and figure out which quests to do once you're in-game. MISSION CONTROL: See which missions are available to you in your Class Order Hall and get them started, all while you're on the go. You can complete your missions and collect your rewards, as well as manage your followers, upgrade their gear, and recruit troops for future missions.
- Platform:** iOS
- Version:** 1.3.50

Package Information:

Package info	Binary meta data
Name: 魔獸好戰友	File size: 149091426
Package Name: com.blizzard.wowcompanion	MD5: af811ddf24a997496410d6752a9e5776
Application ID: 640ba7c6160191232df8fee11a13528e14c9613eccadcf33db235a38f3c1b8d	SHA1: c1ab3621314fa29b1f1220d84d5afa05586be7d5
	SHA256: 581e02e42ab3120bb335abc6932e7874c66d8673381

下圖則是實際觸發事件的用戶裝置:

The screenshot shows the 'Device Risk' section of the Check Point SandBlast Mobile console. The top navigation bar includes 'Dashboard', 'Events & Alerts', 'Device Risk', 'iOS Profiles', 'App Analysis', 'Network', 'Devices', and 'Settings'. The user 'nevillekuo@sysage.com' is logged in. The main interface is divided into a left sidebar with a list of 1 of 1 devices and a main content area for the selected device.

Device Details:

- Risk level:** High & Medium
- Device type:** All
- Device name:** 黃
- Device ID:** (Redacted)
- Device status:** All
- OS:** 7.0
- Agent version:** 2.72.4-RELEASE-b3196/...
- Device:** HUAWEI / EVA-L09
- ID:** 46294

Event Details:

Severity	Time	Status	User action	Policy	Event
Warning	4 days ago	Installed	No action	Default	Suspicious Property Detected

最後,因為 SBM 畢竟也是雲端產品,隨時都有可能改版,所以介面有可能會變或新增,這也是要注意的地方。