



Qsec GlobalTM

Ixia ThreatARMOR 汰換規劃指南

從情資阻斷、Firewall

聯防、日誌稽核到分階段導入，建立可維運的主動防禦架構。

適用對象：CIO、IT 經理、資安主管、SOC 團隊、網路團隊，以及正在評估 Threat Intelligence Gateway / 情資防禦牆汰換的專案負責人。

QSEC Global | Threat Intelligence Driven Defense

Executive Brief

01. ThreatARMOR

汰換規劃核心：情資阻斷與聯防架構

Ixia ThreatARMOR 的定位是 Threat Intelligence

Gateway，主要價值在於網路前段阻擋惡意、被劫持或不可信來源的連線，並減少 Firewall、SIEM 與 SOC 的警報負載。因此，汰換計畫不能只盤點 TAP、Packet Broker 或流量匯集，也必須盤點情資來源、阻斷政策、Rap Sheet 證據、日誌輸出與 Firewall 聯防流程。

核心定位：ThreatARMOR 汰換應以「情資驅動防禦」為主軸，目標是維持或提升惡意連線阻斷、告警降噪、稽核證據與既有安全設備協同能力。

建議優先釐清的四個問題：

- 目前 ThreatARMOR 採 Inline Blocking、Mirror / Monitor，或混合模式部署？
- 阻斷來源是否包含 IP、Domain、FQDN、URL、GeoIP 或不可信國家 / 地區？
- Firewall、SIEM、SOC、NDR 是否仰賴 ThreatARMOR 的阻斷日誌或事件證據？
- 企業想維持同等能力，還是進一步導入在地化威脅情資、API 串接與集中維運？

Assessment Checklist

02. ThreatARMOR 現況盤點清單

Assessment 的目的，是把 ThreatARMOR 現行承擔的安全控制面完整拆解，避免汰換後只完成設備替換，卻遺漏阻斷、告警、稽核或聯防能力。

盤點面向	應確認事項	汰換產出
部署位置	Internet Edge、Firewall 前 / 後、Core、Data Center、分支據點	部署拓模與流量路徑
運作模式	Inline Blocking、Mirror / Monitor、Bypass、HA 或單機部署	切換與 Rollback 計畫
情資政策	IP、Domain、FQDN、URL、GeoIP、不可信國家 / 地區、白名單	政策遷移清單
日誌與稽核	Blocked Connections、System Events、Rap Sheet、SIEM Forwarding	日誌欄位與保存需求
聯防設備	Firewall、IPS、WAF、SOC、NDR、SIEM、Threat Intel 平台	整合與驗證矩陣

QSEC 建議：先盤點阻斷政策與日誌依賴，再選擇替代架構。若只看吞吐量與連接埠，容易低估 ThreatARMOR 在 SOC 降噪與事件追蹤中的角色。

Capability Mapping

03. 替代能力對照表

ThreatARMOR 汰換需要將既有能力映射到新架構，包含情資更新、阻斷效能、證據呈現、Firewall 卸載與日誌整合。

ThreatARMOR 能力	汰換時應保留 / 強化	QSEC 規劃方向
大規模惡意 IP 阻斷	維持高效能阻斷，避免 Firewall 承擔大量名單比對	以情資防禦牆 / Inline 阻斷架構分攤 Firewall 負載
ATI / GeoIP 情資更新	確認更新頻率、來源可信度與本地情資補強	導入國際與在地化威脅情資萃取流程
Rap Sheet 證據	保留事件說明、阻斷原因與稽核可讀性	建立 SOC 可讀事件欄位與報表格式
On-box / Off-box Logging	維持 SIEM、Syslog、事件保存與查詢需求	規劃 SIEM 欄位對應與告警降噪規則
Firewall Complement	降低 Firewall 無效流量與警報負載	以 Firewall 前 / 後架構完成分層防禦

Target Architecture

04. 建議目標架構

ThreatARMOR 替代架構通常不應直接塞回原位置後結案，而應重新檢視 Firewall 前、Firewall 後、Mirror Mode 與 Inline Blocking 的角色分工。

架構模式	適用情境	設計重點
Firewall 前 Inline	希望在惡意連線進入 Firewall 前先阻斷	Bypass、HA、Rollback、維運窗口需明確
Firewall 後 Mirror / Monitor	先觀察內部橫向攻擊、C2、惡意連線與告警品質	適合 PoC、漸進式導入與威脅狩獵
前後聯防	需要同時降低外部攻擊面與監控內部威脅	SOC 需建立事件關聯與責任分工
分流設備整合	既有架構含 TAP / Packet Broker / SPAN	確認分流策略、封包完整性與工具輸出

建議能力範圍：Inline Blocking、Mirror Mode、Bypass、Threat Intelligence、GeoIP、IP / Domain / FQDN / URL、Syslog / SIEM、API Integration、Firewall 聯防、SOC 事件追蹤。

PoC Scope

05. PoC 驗證重點

PoC 應以 ThreatARMOR

既有安全任務為驗證核心，而不是只做連通測試。建議使用實際日誌樣本、Firewall 告警、SIEM 事件與測試流量來驗證替代架構。

- 阻斷驗證：惡意 IP、Domain、FQDN、URL、GeoIP 或不可信國家 / 地區政策是否有效。
- 效能驗證：Inline 模式下是否維持低延遲與線速處理，且不影響關鍵服務。
- 日誌驗證：Blocked Connections、系統事件與阻斷原因是否能送到 SIEM。
- 告警降噪：Firewall / SIEM 告警量是否下降，SOC 是否能更快聚焦重要事件。
- 備援驗證：Bypass、HA、故障切換與 Rollback 是否符合營運要求。

驗證項目	通過標準
阻斷品質	測試樣本可被正確阻斷，且白名單 / 例外政策可控。
日誌可用性	SIEM 可接收必要欄位，SOC 可理解事件原因。
Firewall 卸載	無效或高風險連線在前段被處理，Firewall 負載與告警下降。
營運安全	切換、故障、回復流程都可被演練與紀錄。

Execution Roadmap

06. ThreatARMOR Migration 五大步驟

階段	工作內容	建議產出
1. ThreatARMOR Assessment	盤點部署位置、模式、政策、日誌、SIEM 與 Firewall 依賴。	現況盤點報告、政策清單
2. Replacement Architecture	設計 Inline / Mirror、Bypass、HA、日誌與情資來源。	目標架構圖、切換計畫
3. PoC Validation	驗證阻斷、效能、日誌、告警降噪與 Rollback。	PoC 報告、風險修正清單
4. Phased Migration	依場域或流量類型分階段切換，保留原架構回復路徑。	切換紀錄、驗收清單
5. SOC Optimization	調整 SIEM 規則、報表、告警門檻與維運手冊。	最佳化建議、維運交接

分階段切換是 ThreatARMOR 汰換的關鍵。建議先用 Mirror / Monitor 或低風險線路驗證，再切入 Inline Blocking。

Suggested Timeline

07. 專案時程範本

週次	主要工作	QSEC 協助重點
Week 1-2	ThreatARMOR 現況盤點與日誌依賴確認	訪談、拓樸、政策與事件欄位盤點
Week 3-4	替代架構設計與 PoC 場景確認	Inline / Mirror、Bypass、SIEM、Firewall 聯防規劃
Week 5-8	PoC 驗證與政策調整	阻斷測試、日誌測試、告警降噪比較
Week 9-12	正式導入第一階段	切換支援、Rollback、驗收與文件化
Week 13+	SOC 最佳化與維運交接	SIEM 規則、報表、維運手冊與技術支援

若企業已有 ThreatARMOR 政策清單、Rap Sheet 報表、Syslog 欄位與 Firewall 告警基準，PoC 與切換時間可明顯縮短。

Risk Control

08. 風險控管與驗收標準

ThreatARMOR 汰換風險通常來自三個面向：阻斷政策變更、Inline 網路風險、以及 SOC / SIEM 事件脈絡中斷。

- 政策風險：白名單、例外規則與 GeolIP 政策需先盤點並版本化。
- Inline 風險：Bypass、HA、故障切換、延遲與封包遺失需納入 PoC。
- 日誌風險：SIEM 欄位、事件名稱、嚴重度與報表需先對應。
- 營運風險：切換窗口、回復條件、責任人與驗收標準需明確。
- 安全風險：汰換期間不可造成高風險連線未被監控或阻斷。

驗收標準：新架構需維持惡意連線阻斷、降低 Firewall / SIEM 無效負載、保留 SOC 可讀事件證據，並符合企業既有變更管理流程。

Planning Worksheet

09. 需求訪談表

問題	填寫欄位
目前 ThreatARMOR 部署在哪些位置？Firewall 前、後或分支？	
目前採 Inline Blocking、Mirror / Monitor 或混合模式？	
目前阻斷政策包含哪些類型？IP、Domain、FQDN、URL、GeoIP？	
是否使用 Rap Sheet、Dashboard 或日誌作為稽核證據？	
Blocked Connections 是否送至 SIEM / SOC 平台？	
Firewall / SIEM 告警量是否有基準資料可比較？	
是否需要 Bypass、HA、分階段切換或維運窗口限制？	

建議在第一次 Assessment 前完成此表，並準備現有拓樸圖、ThreatARMOR 報表、Firewall 告警摘要與 SIEM 欄位樣本。

Common Questions

10. FAQ

ThreatARMOR 汰換是否一定要停機？

不一定。可先以 Mirror / Monitor 驗證，再依維運窗口逐步切換 Inline Blocking。

可以直接用 Firewall 取代 ThreatARMOR 嗎？

需謹慎評估。ThreatARMOR 的價值在於大規模情資阻斷與 Firewall 卸載，直接把名單與政策交給 Firewall 可能造成效能與維運負擔。

PoC 應該驗哪些內容？

至少應驗證阻斷政策、日誌輸出、SIEM 欄位、Firewall 告警降噪、Bypass / HA 與 Rollback。

Assessment 需要多久？

通常 1 至 2 週可完成初步盤點，若有多場域、多 SIEM 或複雜白名單，需保留更多時間。

QSEC 如何協助 ThreatARMOR Migration？

QSEC 可協助現況盤點、替代架構設計、PoC、分階段導入、SOC 最佳化與在地技術支援。

下一步：預約免費 ThreatARMOR Assessment，讓 QSEC Global 協助盤點您的既有部署、政策依賴與可行的汰換路徑。

聯絡方式：hello@qsec.global

QSEC Global | Threat Intelligence | Firewall Offload | SOC Integration | Migration Service