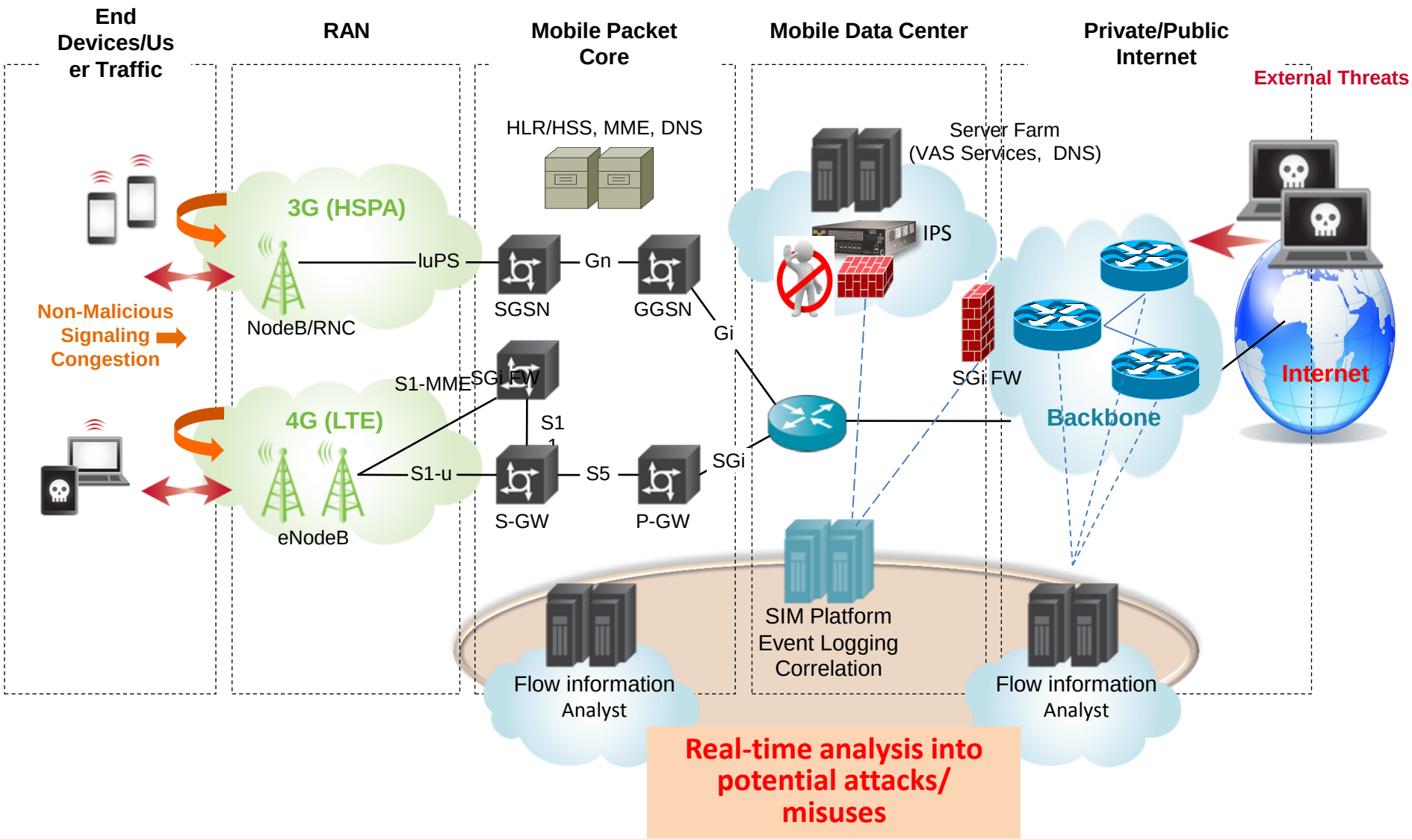
FAR EAS TONE

遠傳

SP 網路攻擊防護機制

報告人 ：林 筱 偉

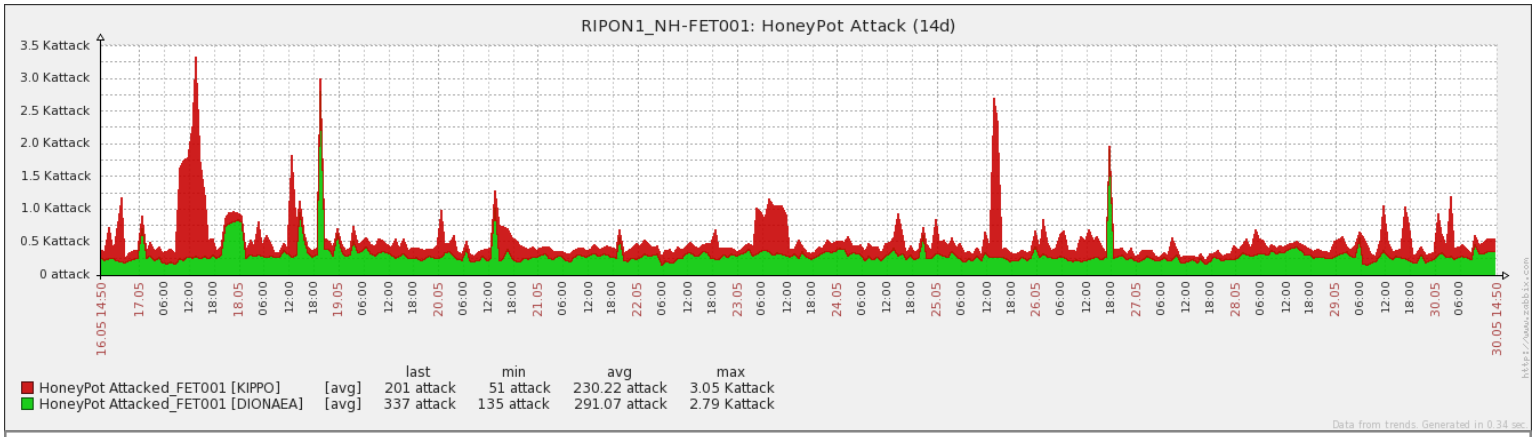
MSP Service Network

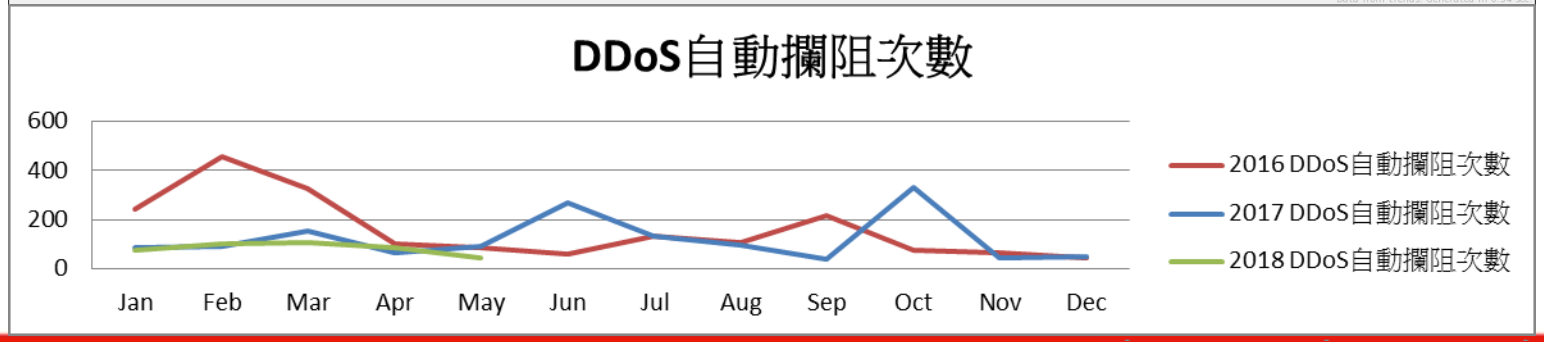


DOS Attacks State

利用HoneyPot 誘捕器收集/觀察外部攻擊來源行為，強化事前預警機制。

Analysis Time Frame	Attack Volume	Automatic Blocking
2017/11 ~ 2018/5	Avg. 26634 / Month	Avg. 120 / Month





網路防護機制的建立

- 常見網路攻擊模式 1. 頻寬耗損, 2. 資源消耗. 3. 應用層漏洞入侵

流量監控	• Honey Pot 預警機制，收集觀察攻擊來源行為 • IPS/ IDS 輔助分析
即時告警分析	• 網路流量工程, Netflow
多層阻斷	• 手動/ 自動執行限制 / 阻斷存取
封包過濾	• 過濾惡意攻擊流量, 維持正常服務

資安攻擊類型與因應

- 常見網路攻擊手法多以大流量或大量小封包連線，讓網路設備/系統無法正常運作造成網路服務影響。
- 經由應用服務系統的安全漏洞入侵服務主機，將造成服務中斷與資料外洩等影響。

	Mitigation Technique	Volume Based Attacks (頻寬消耗型)	Protocol Attacks (資源消耗型)	Application Layer Attacks
量測方式		**bits** per second (BPS)	**Packets** per second (PPS)	**Requests** per second (concurrent connection)
影響類型		saturate the bandwidth of the host/site target	consumes actual server resources	to crash the Application service ex. web server
Blackhole	系統自動通知上游SP業者將特定受害IP 做攔阻)	V	V	
Traffic Mitigation	流量管理	V	V	
Firewall	Service filtering		V	V
IPS	Intrusion pattern protection		V	V

結 語

- 建立 7 x 24 SOC 維運組織 對資安告警事件進行即時處理。
- 持續強化資安技術專業知識，提升資安技術專業人員的能力。
- 因應新衍生的網路攻擊事件，適時更新資安防護系統。
- 結合外部組織，建立資安資訊分享。如 國內外資安領域專業組織、設備系統廠商等。

FAREASTONE 遠傳

敬　請　指　教

Thank You