paloalto NETWORKS

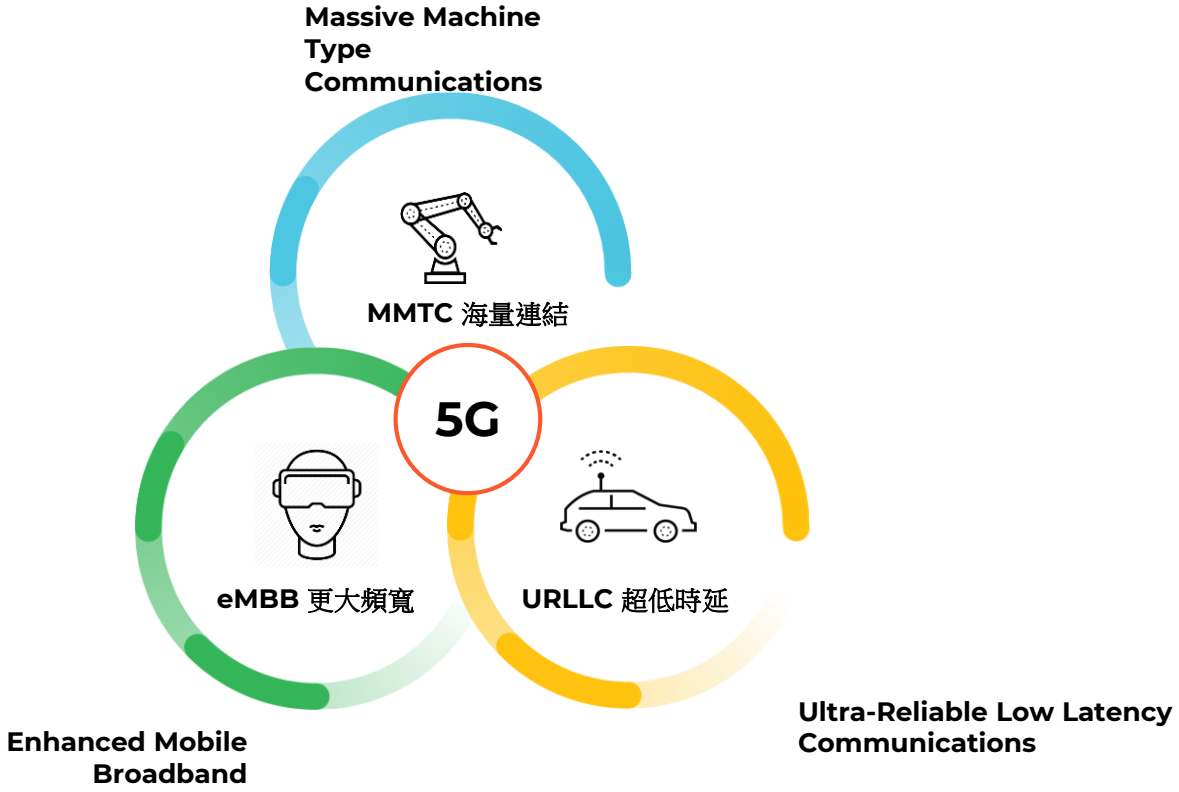
WE'VE GOT NEXT
我們掌握未來

新世代校園與物聯網路的可視安全
5G 新場域的挑戰

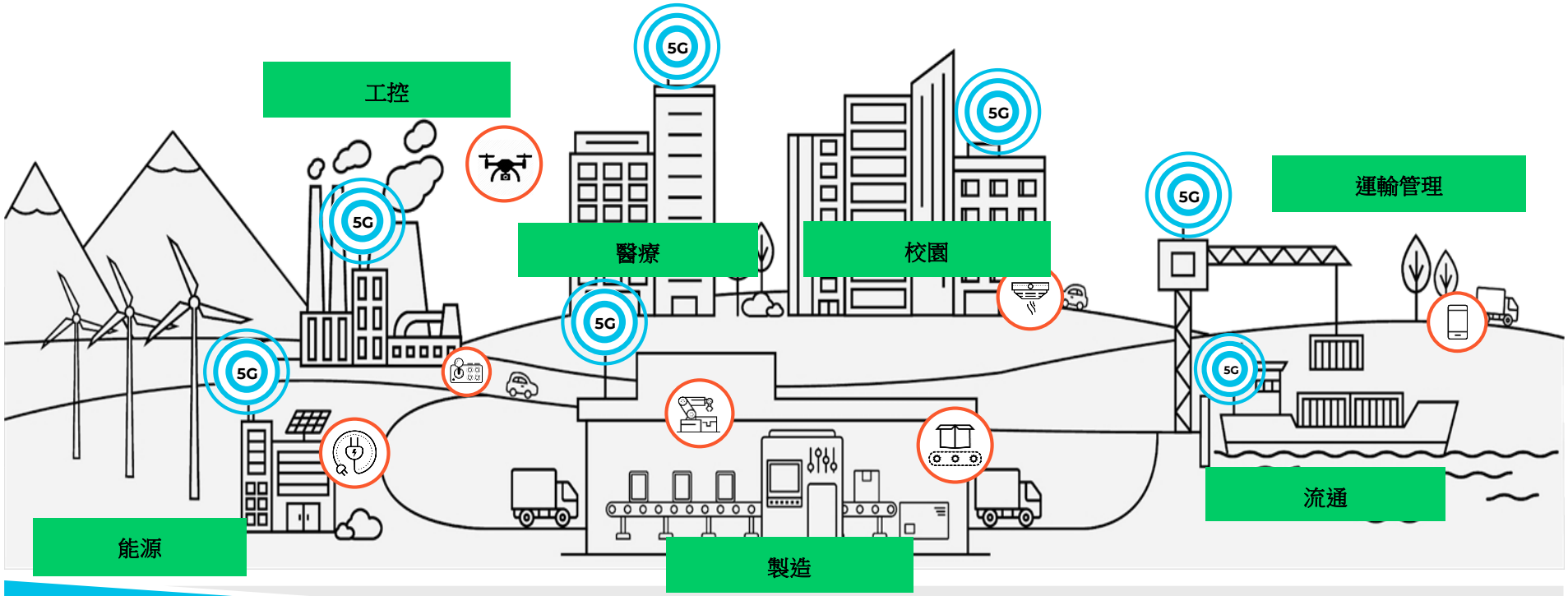
美商帕洛爾托網路有限公司
技術顧問
王信強

全球趨勢

5G 將重塑應用場景


Massive Machine Type Communications
MMTC 海量連結
5G
eMBB 更大頻寬
URLLC 超低時延
Enhanced Mobile Broadband
Ultra-Reliable Low Latency Communications

主要商務應用產業－垂直場域



企業私網

公眾服務

5G 推動數位轉型

中小學數位學習精進方案

智能製造

工業4.0

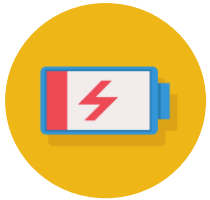

保護關鍵資產
• 有效的安全情報
（用户/設備ID/威脅關聯）
• 對M2M / IoT行為模式的可視性
保護關鍵服務
• 未修補的舊版操作系統中安全地連接5G物聯網
• 識別並阻斷已知/未知惡意威脅
• 信令和數據平面漏洞防護
數據安全
• 避免專有信息，知識產權資產和商業的數據泄露
• 數據隱私與合規

智慧工程

營造、礦場現代化

物聯網 / 產業垂直整合應用常見攻擊手法

服務干擾或阻斷攻擊
（惡意競爭、勒索等常見營利目的）



裝置耗能攻擊
（常見於空窗期逐行特定目的）

物聯網場域安全

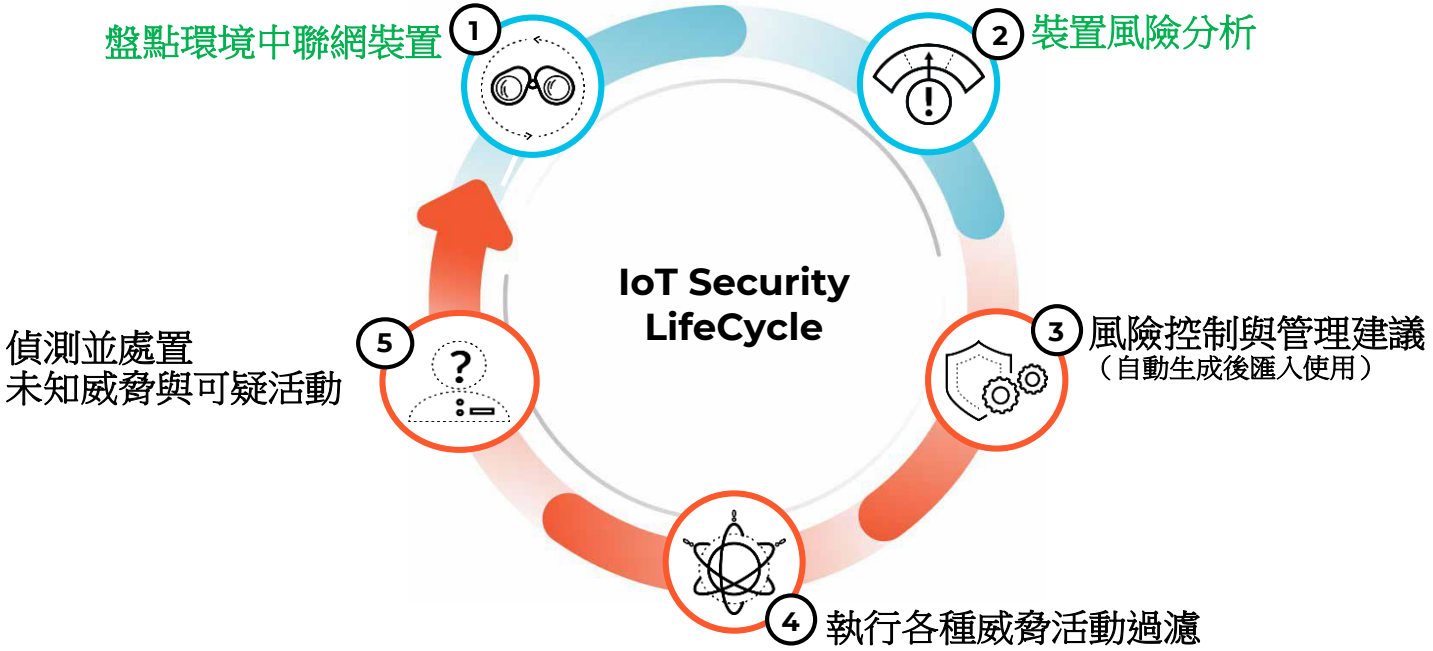
NIST 網路安全框架

IoT 物聯網安全提供可映射到 NIST 網絡安全框架的信息

Cybersecurity Framework Version 1.1

識別	防護	檢測	回應	修復
• IoT asset discovery & inventory • IoT risk exposure and security posture assessment	• Context-aware network segmentation to reduce attack surface • Zero-trust Policy for IoT • ACLs to only permit trusted behaviors	• Behavioral baselining and anomaly detection for IoT • IoT Vulnerabilities	• Real-time IoT enforcement using network security controls • Quarantine deviant IoT asset • Integration with XSOAR, NAC and ticketing systems	• Recommendations on available patches for CVEs, OS/Firmware

物聯網安全最佳實踐


1 盤點環境中聯網裝置
2 裝置風險分析
3 風險控制與管理建議
（自動生成後匯入使用）
4 執行各種威脅活動過濾
5 偵測並處置
未知威脅與可疑活動
IoT Security
LifeCycle

呼應：威脅建模 IoT Security Machine Learning: Personality & Context

App-ID: Enhanced application logs

Firewall traffic logs

DNS Traffic

Threat Logs

LOG DATA

Patented 3-Tier Model

- MAC address
- IP address
- DNS response
- Threat ID
- HTTP/2
- App Header
- App payloads
- ...
- ...

Tier 1 = Device Type
Generic Device Category

Tier 2 = Vendor & Model
Manufacturer Information

Tier 3 = Device Instance
Unique Personality & Context

Customer 1 Customer 2 Customer ...

Machine learning
+
Crowdsourced data
+
App-ID/Deep Packet Inspection (DPI)

Device & Threat Detection

- Device Identity (50+ attr)
- Behavioural Baseline
- Behavioral Anomalies
- Risk Assessment
- Threat Detection

Automated Zero Trust based Policy Recommendations

呼應：漏洞檢測 Comprehensive Risk Framework and Assessment

Threats

Exploits | Malware

- Abnormal connections between IoTs
- Malicious files on devices
- Connections to risky website
- Abnormal traffic between devices
- Personal device connecting to a large no. of devices
- .....

Vulnerability

CVES

- Default passwords
- End of Life OS/Apps/Devices
- Obsolete protocols
- Cloud/network connections
- CVE tracking
- .....

Context

Static | Dynamic

- Misconfiguration
- Unusual software
- Patch-level
- Apps-Name/version
- Internal/ external connection type and frequency
- Unexpected amount of data transmission
- Device behavior anomalies
- Manufacturer specifications
- .....

Leverages ML, Crowdsourced Telemetry, Unit 42 Threat Research

Palo Alto Networks Unit 42 IoT Threat Report Findings

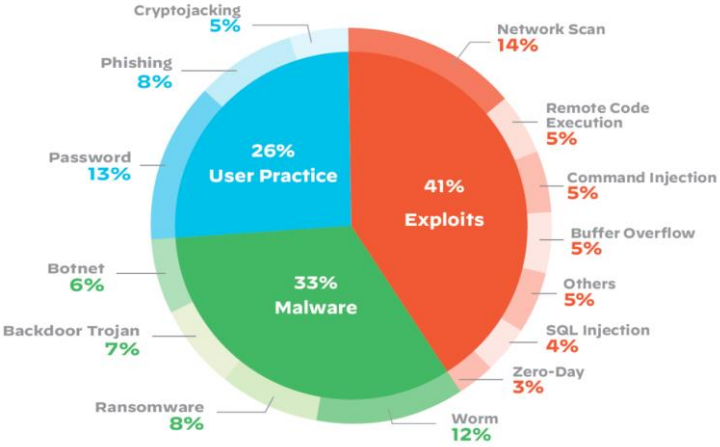
Why are IoT the Ideal Entry Point ?

- Zero to Minimum Built-In Security
- Browser Interface Vulnerabilities
- Outdated Operating Systems
- Failure to Adhere to Security Best Practices

Most High Risk Devices?

- Medical Imaging Systems — 51%
- Patient Monitoring Systems — 26%
- Security Cameras — 33%
- Printers — 24%
- Medical Device Gateways — 9%
- Consumer Electronics — 7%
- Energy Management Devices — 6%
- IP Phones — 5%

Threats

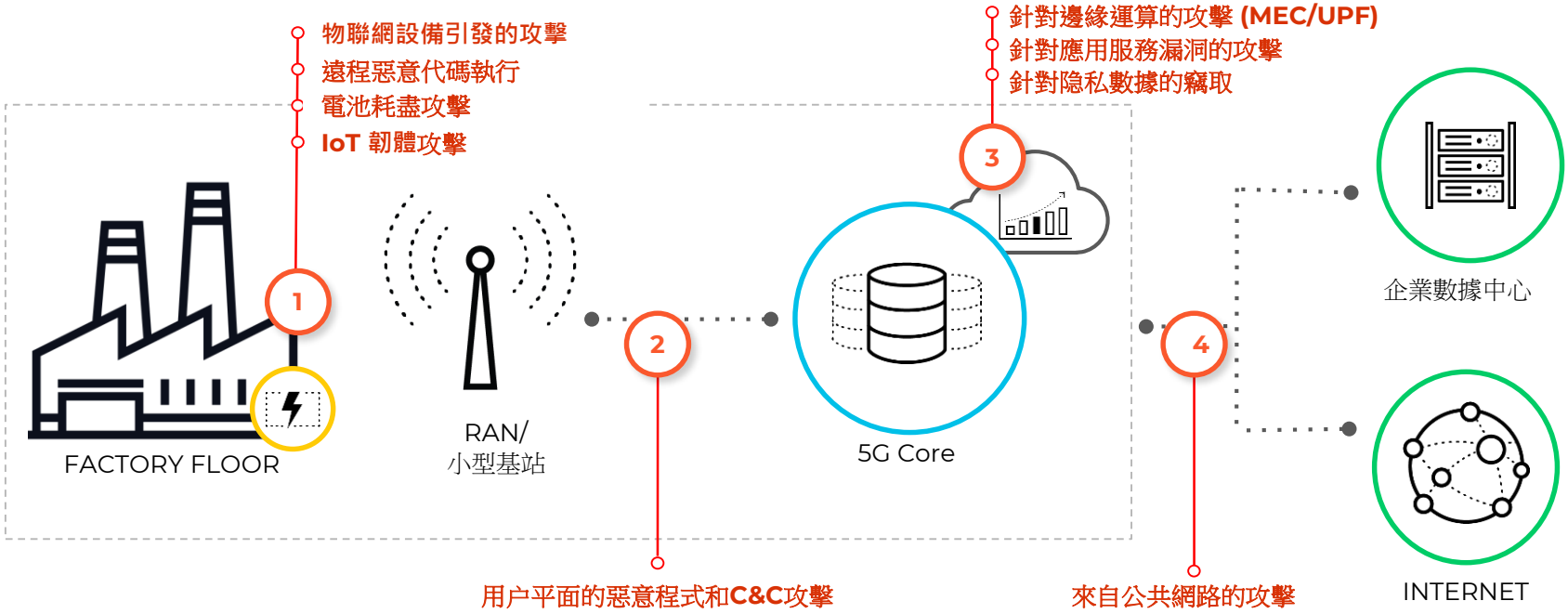


平台整合

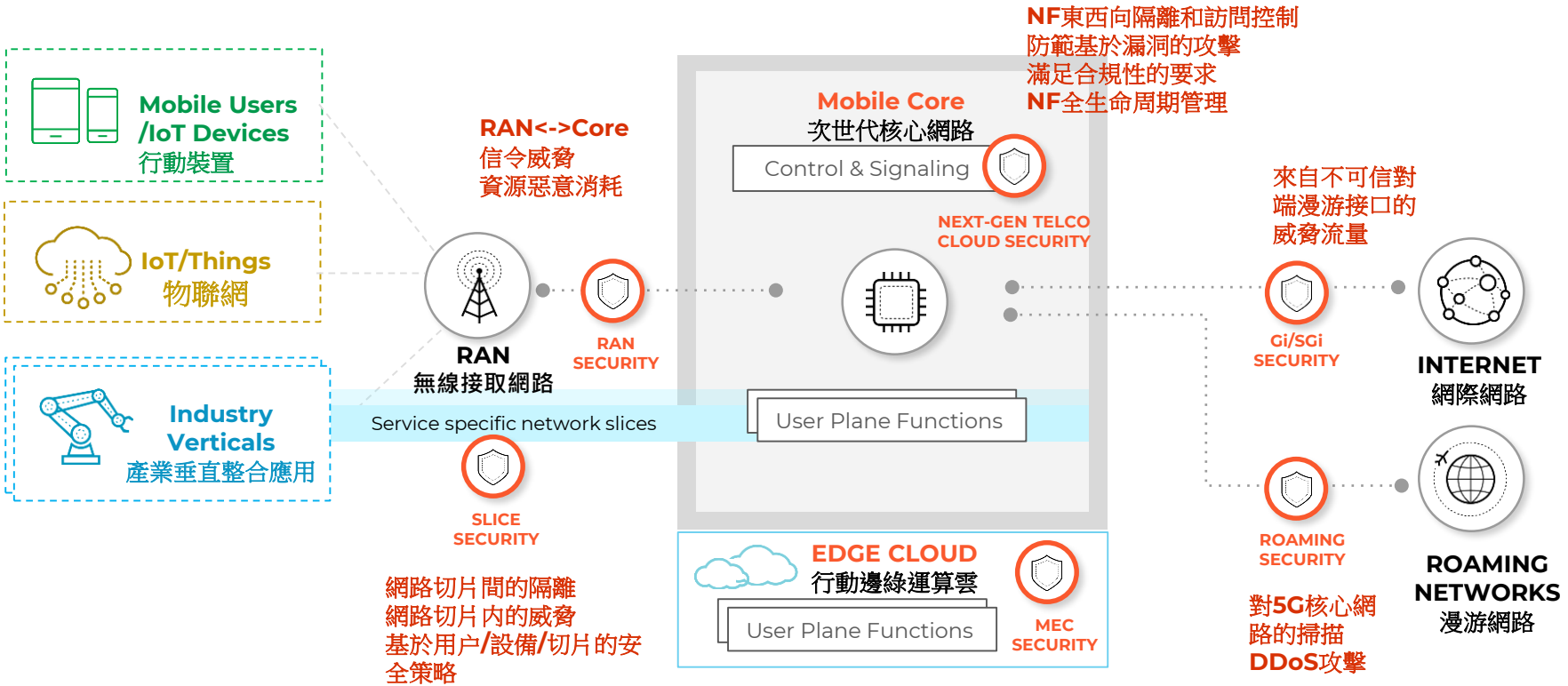
SIEM Solutions	LogRhythm	splunk>	Cortex XDR
		IBM QRadar	ArcSight
Vulnerability Management	Qualys.	RAPID7	tenable
NAC Solution	FORESCOUT	cisco	aruba a Hewlett Packard Enterprise company
Asset Management	servicenow	nuvolo	AIMS

邊緣運算安全

私有場域安全


物聯網設備引發的攻擊
遠程惡意代碼執行
電池耗盡攻擊
IoT 韌體攻擊
針對邊緣運算的攻擊 (MEC/UPF)
針對應用服務漏洞的攻擊
針對隱私數據的竊取
1
2
3
4
FACTORY FLOOR
RAN/
小型基站
5G Core
企業數據中心
INTERNET
用户平面的惡意程式和C&C攻擊
來自公共網路的攻擊

邊緣運算核網


Mobile Users
/IoT Devices
行動裝置
IoT/Things
物聯網
Industry
Verticals
產業垂直整合應用
RAN<->Core
信令威脅
資源惡意消耗
RAN
無線接取網路
RAN
SECURITY
Service specific network slices
SLICE
SECURITY
網路切片間的隔離
網路切片內的威脅
基於用戶/設備/切片的安全策略
Mobile Core
次世代核心網路
Control & Signaling
NEXT-GEN TELCO
CLOUD SECURITY
User Plane Functions
NF東西向隔離和訪問控制
防範基於漏洞的攻擊
滿足合規性的要求
NF全生命周期管理
EDGE CLOUD
行動邊緣運算雲
User Plane Functions
MEC
SECURITY
來自不可信對
端漫游接口的
威脅流量
Gi/SGi
SECURITY
INTERNET
網際網路
ROAMING
SECURITY
ROAMING
NETWORKS
漫游網路
對5G核心網
路的掃描
DDoS攻擊

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

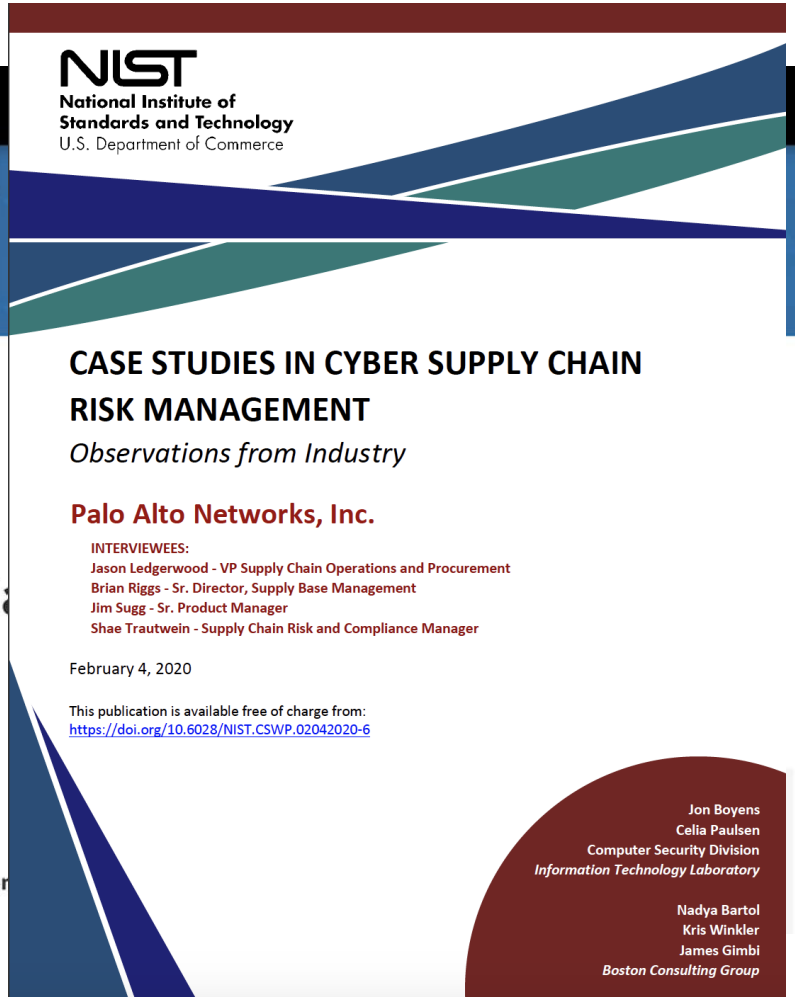
White Paper

Case Studies in Cyber Supply Chain Risk M
Inc.

Date Published: February 2020

Author(s)

Jon Boyens (NIST), Celia Paulsen (NIST), Nadya Bartol (Boston Consulting Group), Kris Winkler (Bostor Group), James Gimbi (Boston Consulting Group)



GSMA 5G/4G GTP-U 安全指南 FS.37

- 由**Palo Alto Networks**領導的與全球多家電信商合作的成果
- 這些指南涵蓋了GTP-U用户面存在的安全風險和相對應的解決方案
- 移動服務電信商需要為特定應用提供安全的5G網路切片服務
- 5G中安全控制的缺乏可能會影響移動電信商與其服務的垂直行業之間的合作成效
- 5G行業應用的規模化部署更加需要有自動化的檢測和預防機制

GENERATE NEW REVENUE STREAMS WITH 5G ENTERPRISE CYBERSECURITY AND SASE

Running
Monday, 28 June: 10:30 - 11:30 CEST

Location
My MWC Online, Hall Virtual

Share
Share

paloalto NETWORKS AT&T dish

5G is here. Are you prepared to drive the transformation?

謝謝您的聆聽