



Cybersecurity For LMR Systems

Alvin Singh

Motorola Solutions

Agenda

- Why Cybersecurity for LMR Systems
- Attack Surface
 - Ransomware
 - Other Identified Risks
 - How Threat actors target Radio systems
- State and Federal Government Cyber Requirements
- What can be done
 - Customers
 - Vendors

Why Cybersecurity is Important for LMR

- No longer 'walled gardens' or air gapped environments
- Cyber attacks such as data breach and ransomware are a direct threat to LMR systems

142%

increase in number of ransomware groups attacking US public safety agencies in 2023*

29%

Of Threat actors leveraged legitimate credentials to access Public Safety networks

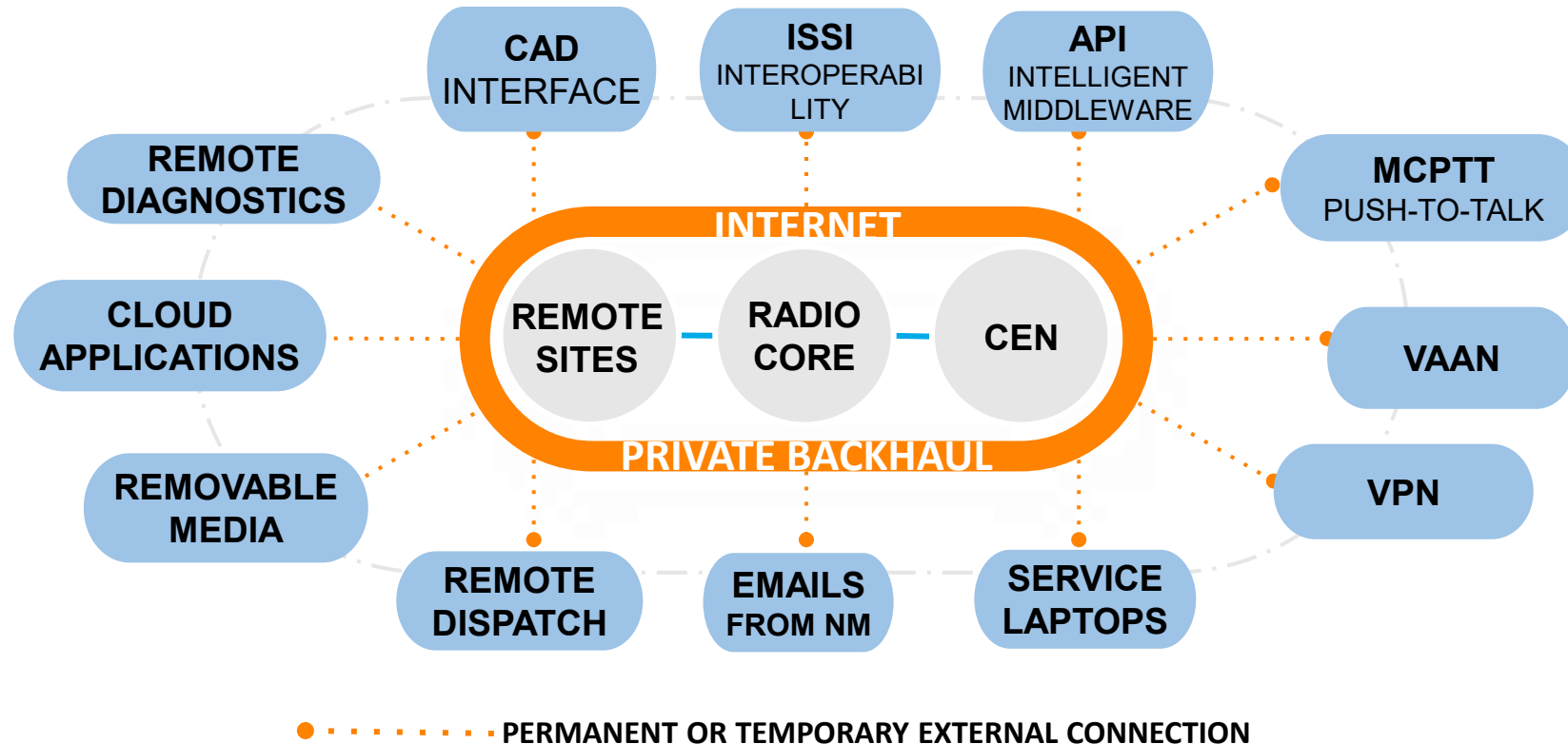
63%

increase in ransomware attacks on US public safety organizations during 2023*

**PSTA 2024 reports*

LMR IS NOT A “CLOSED NETWORK”

LMR NETWORKS HAVE VULNERABILITIES SIMILAR TO THOSE FOUND IN IT NETWORKS

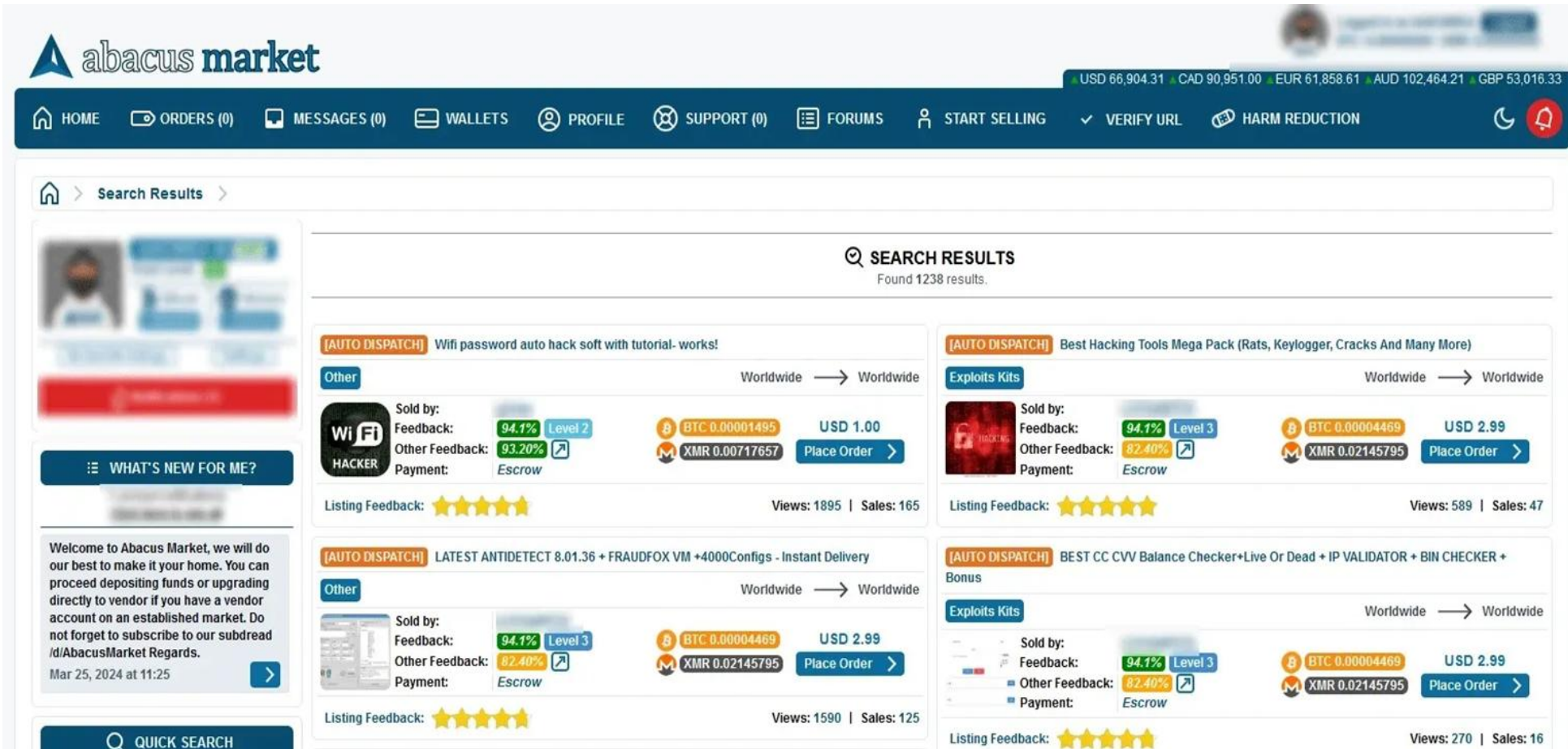


CISA-IDENTIFIED CYBER AND PHYSICAL RISKS WITHIN LMR

- Interception or Eavesdropping
- Poor Cyber Hygiene
- Denial of Service
- Malicious applications, malware & Data Exfiltration
- Spear Phishing & social engineering

Marketplaces

Organized cyber extortion



The screenshot displays the Abacus Market website interface. At the top, there's a navigation bar with links for HOME, ORDERS (0), MESSAGES (0), WALLETS, PROFILE, SUPPORT (0), FORUMS, START SELLING, VERIFY URL, and HARM REDUCTION. A currency converter bar shows rates for USD, CAD, EUR, AUD, and GBP. The main content area is titled "SEARCH RESULTS" and shows "Found 1238 results." Below this, there are four product listings, each with a title, category, seller information, feedback, and a "Place Order" button.

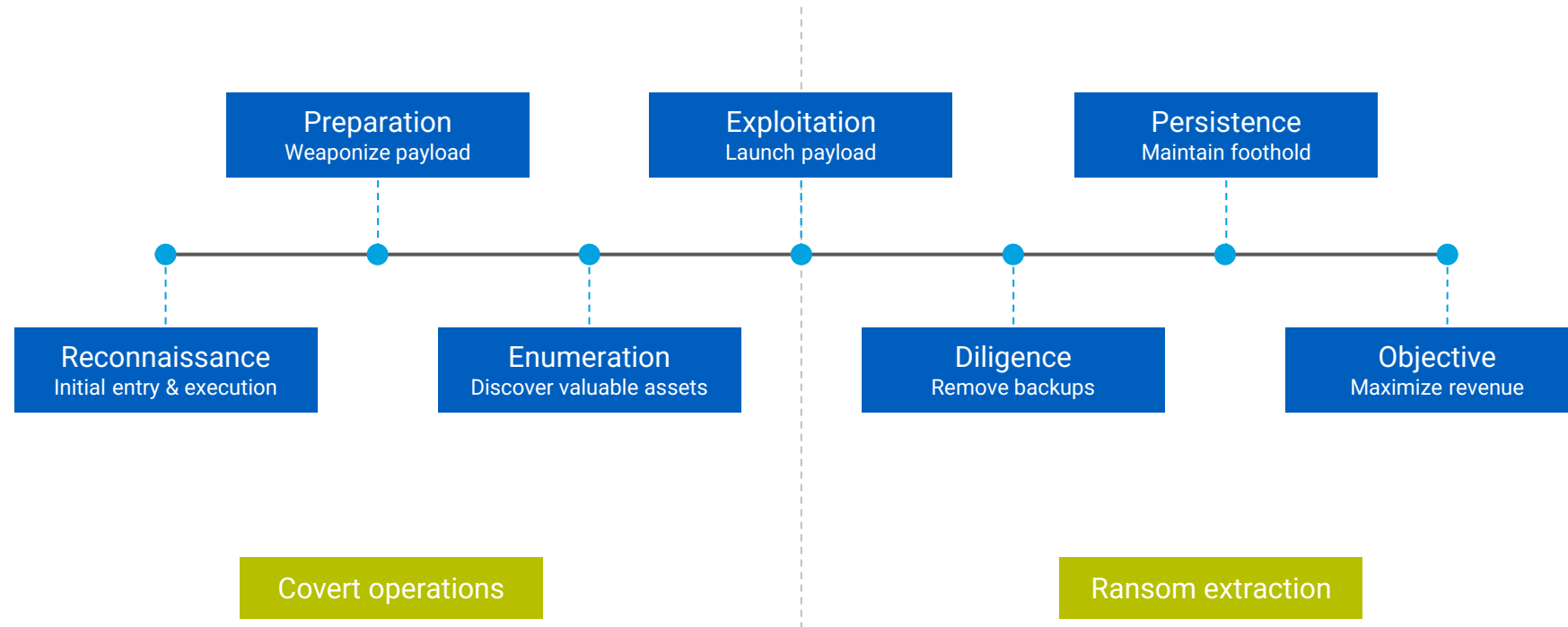
Product Listings:

- [AUTO DISPATCH] Wifi password auto hack soft with tutorial- works!**
 - Category: Other
 - Sold by: [Profile]
 - Feedback: 94.1% Level 2
 - Other Feedback: 93.20%
 - Payment: Escrow
 - Price: USD 1.00
 - Cryptocurrency: BTC 0.00001495, XMR 0.00717657
 - Listing Feedback: ★★★★★
 - Views: 1895 | Sales: 165
- [AUTO DISPATCH] Best Hacking Tools Mega Pack (Rats, Keylogger, Cracks And Many More)**
 - Category: Exploits Kits
 - Sold by: [Profile]
 - Feedback: 94.1% Level 3
 - Other Feedback: 82.40%
 - Payment: Escrow
 - Price: USD 2.99
 - Cryptocurrency: BTC 0.00004469, XMR 0.02145795
 - Listing Feedback: ★★★★★
 - Views: 589 | Sales: 47
- [AUTO DISPATCH] LATEST ANTIDETECT 8.01.36 + FRAUDFOX VM +4000Configs - Instant Delivery**
 - Category: Other
 - Sold by: [Profile]
 - Feedback: 94.1% Level 3
 - Other Feedback: 82.40%
 - Payment: Escrow
 - Price: USD 2.99
 - Cryptocurrency: BTC 0.00004469, XMR 0.02145795
 - Listing Feedback: ★★★★★
 - Views: 1590 | Sales: 125
- [AUTO DISPATCH] BEST CC CVV Balance Checker+Live Or Dead + IP VALIDATOR + BIN CHECKER + Bonus**
 - Category: Exploits Kits
 - Sold by: [Profile]
 - Feedback: 94.1% Level 3
 - Other Feedback: 82.40%
 - Payment: Escrow
 - Price: USD 2.99
 - Cryptocurrency: BTC 0.00004469, XMR 0.02145795
 - Listing Feedback: ★★★★★
 - Views: 270 | Sales: 16

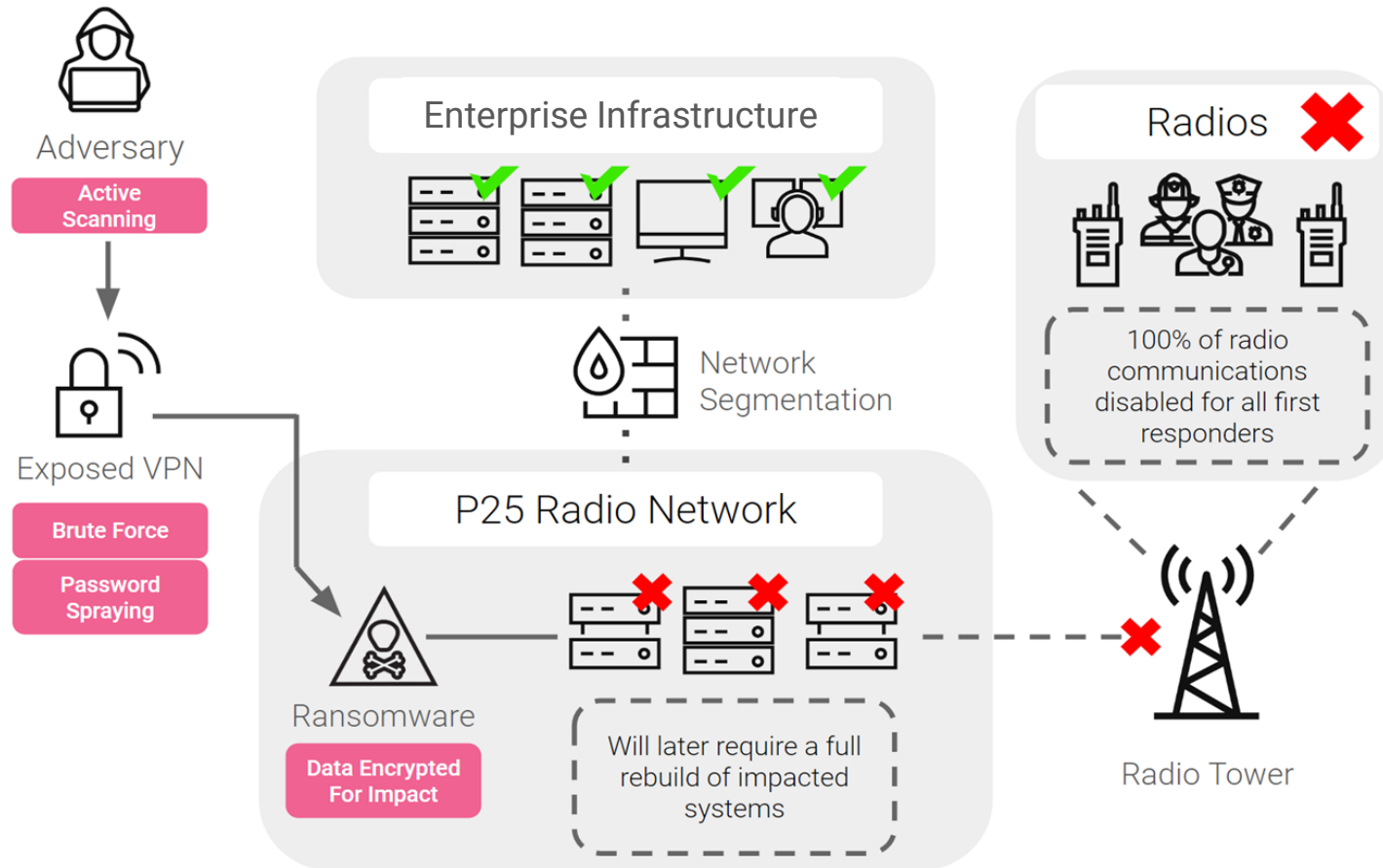
On the left side of the page, there's a sidebar with a "WHAT'S NEW FOR ME?" section and a "QUICK SEARCH" bar.

Attack Elements

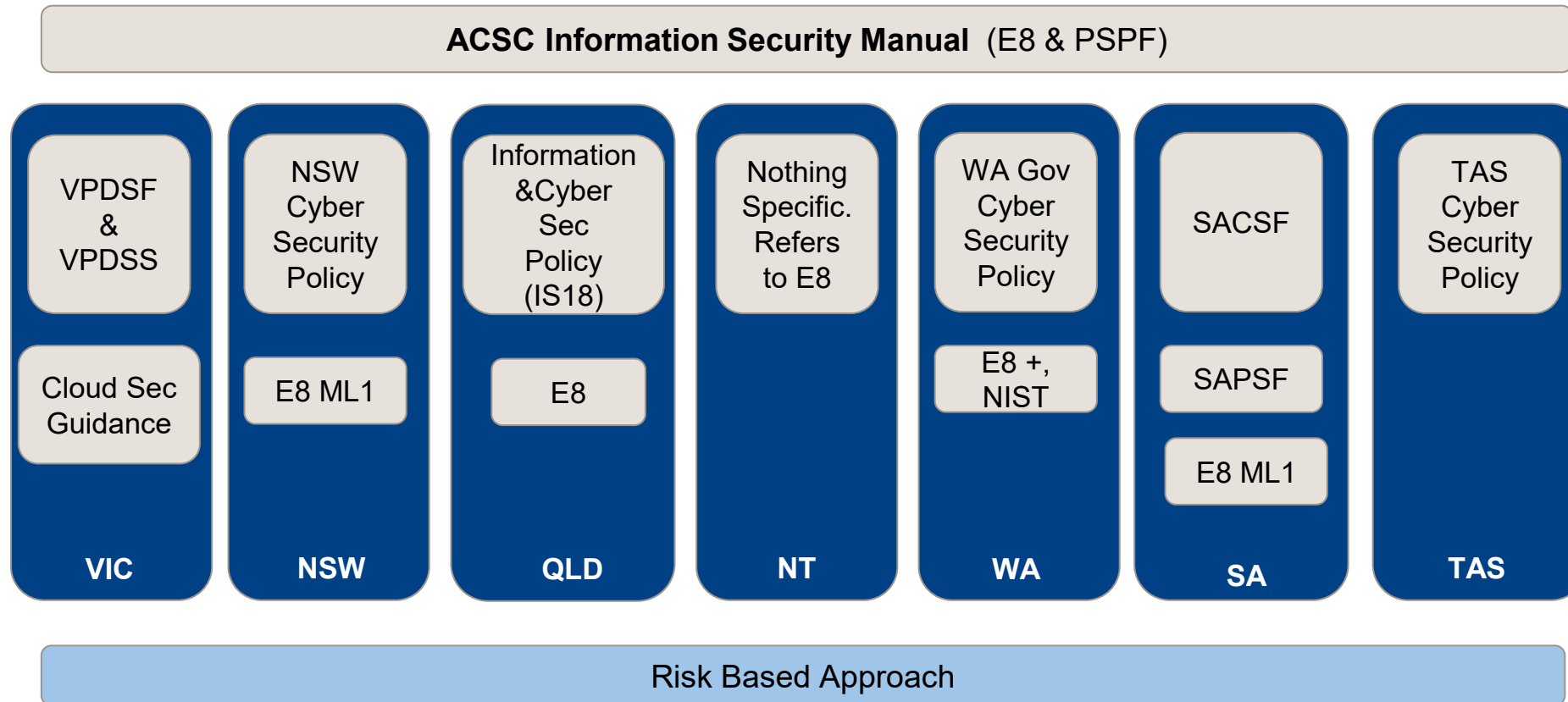
Fundamental parts of every ransomware attack



Radio System Attack Diagram



State Government Cyber Frameworks & Requirements



What should we do to protect LMR systems in Australia



- Governance – People, Process & Technology
- Refer to ACSC guidelines - Essential 8, ACSC ISM
- Implement the required controls
- Managing Risks
- Continuous Improvement.

Motorola Solutions Cybersecurity Services

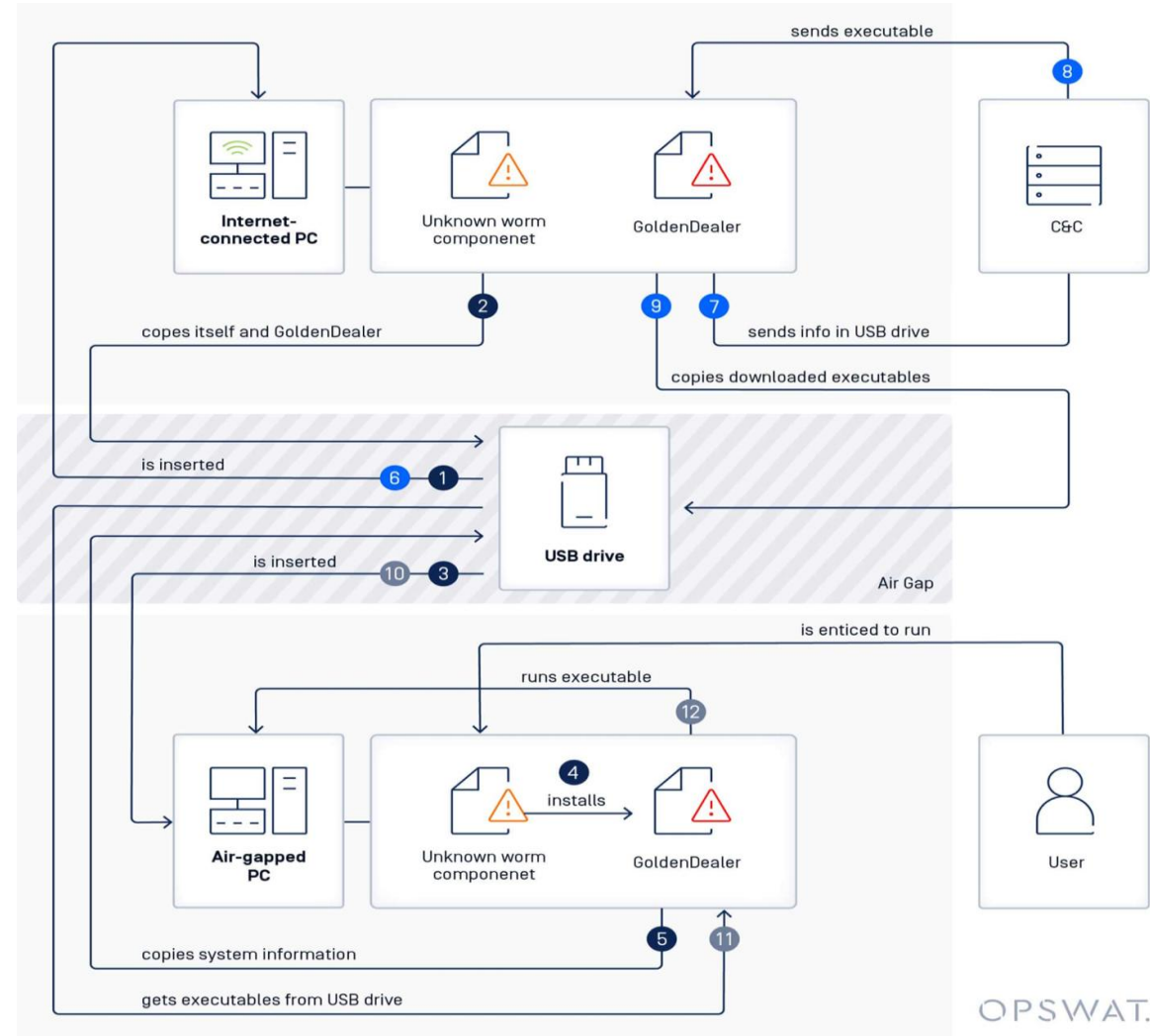
Defence In Depth Approach



Thank You

Breaching Air Gapped Networks

- Campaign by APT group GoldenJackal
Targeting Government organizations in Europe in 2024



How threat actors target LMR Systems

INITIAL ACCESS	EXECUTION	DISCOVERY	LATERAL MOVEMENT	DATA COLLECTION	ATTACK IMPACT
External Remote Services (RDP, VPN, SMB)	Windows Management Instrumentation	Network Share Discovery	SMB/Windows Admin Shares	Data From Local System	Data Encrypted for Impact
Trusted Relationship	Malicious File	Domain Account Discovery	Remote Desktop Protocol	Data From Network Shared Drive	Data Extort/Publish
Spearphishing Attachment	Malicious Link	File and Directory Discovery	Lateral Tool Transfer	Email Collection	Telephony Denial of Service
Spearphishing Link	Windows Command Shell	System Network Connections Discovery	Exploitation of Remote Services	Audio Capture	Broadcast Denial of Service
Exploit Public-Facing Application	PowerShell	Domain Groups Discovery	Replication Through Removable Media	Data From Removable Media	Network Denial of Service
Inherent Access (Insider Threat)	Native API	System Information Discovery			Data Destruction
Valid Accounts	Service Execution	Security Software Discovery			Inhibit System Recovery
Hardware or Key Theft		System Service Discovery			System Shutdown/Reboot
Hardware Addition		Network Service Scanning			Service Stop
Replication Through Removable Media					Disk Structure Wipe