GCC THREATS AND COUNTERMEASURES

Harshul Joshi
SVP, Cyber Advisory Services

DECEMBER 2017

DARKMATTER

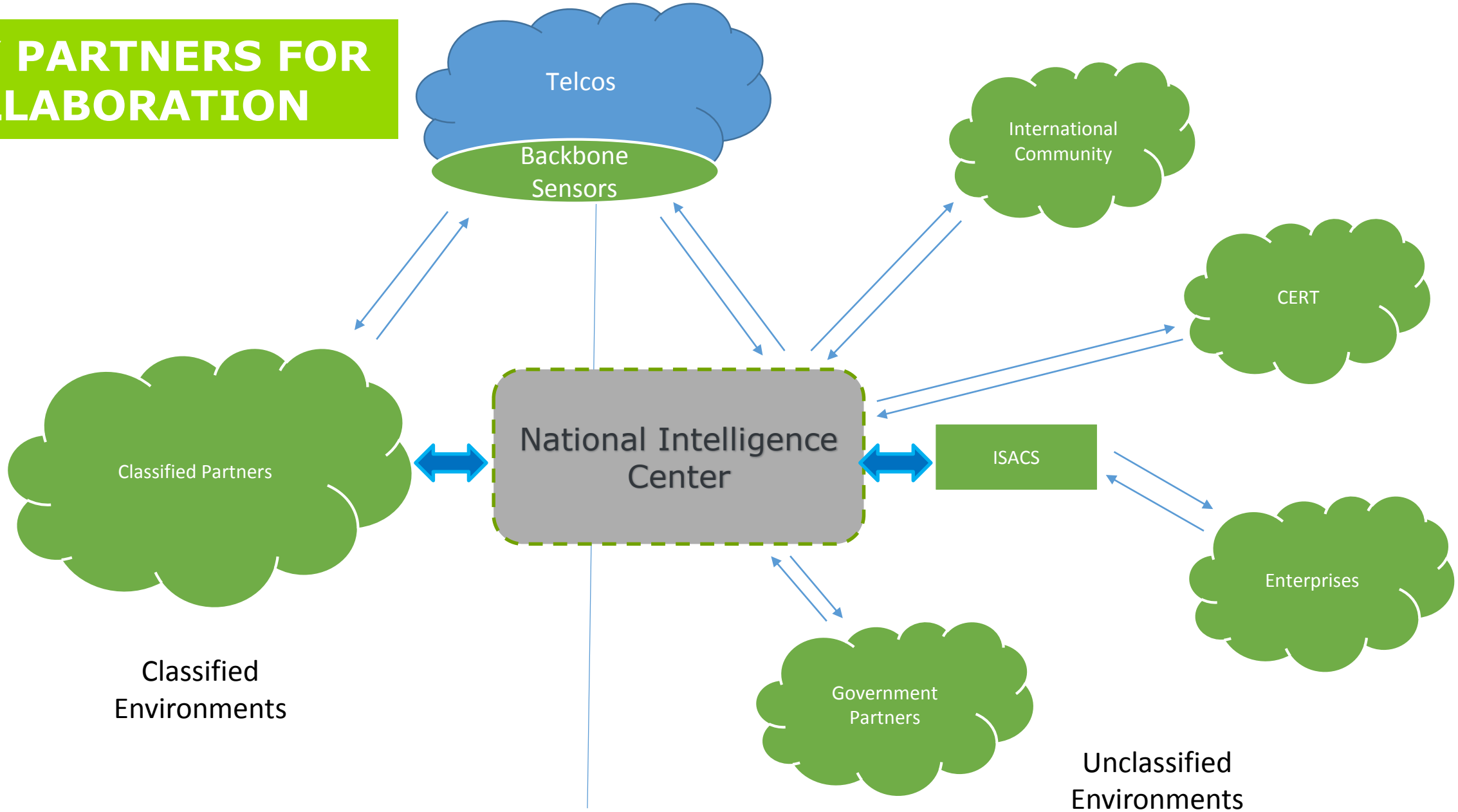
HIGH-LEVEL THREAT LANDSCAPE - UAE

- Numerous incidents associated with use or re-use of nation-state level cyber weapons
  - Alleged NSA exploits used against SWIFT and EastNets described by The Shadow Brokers
- Numerous ransomware and destructive malware incidents across the GCC
  - Some building upon leaks of CIA Vault 7 or other cyber weapons
- Attacks on oil and gas sector – e.g., we observed in the KSA and UAE
  - Greenbug espionage group who placed remote access Trojans designed to exfiltrate data
  - MuddyWaters malware using Power Shell exploits to establish a foothold, command and control and data exfiltration
- And much more

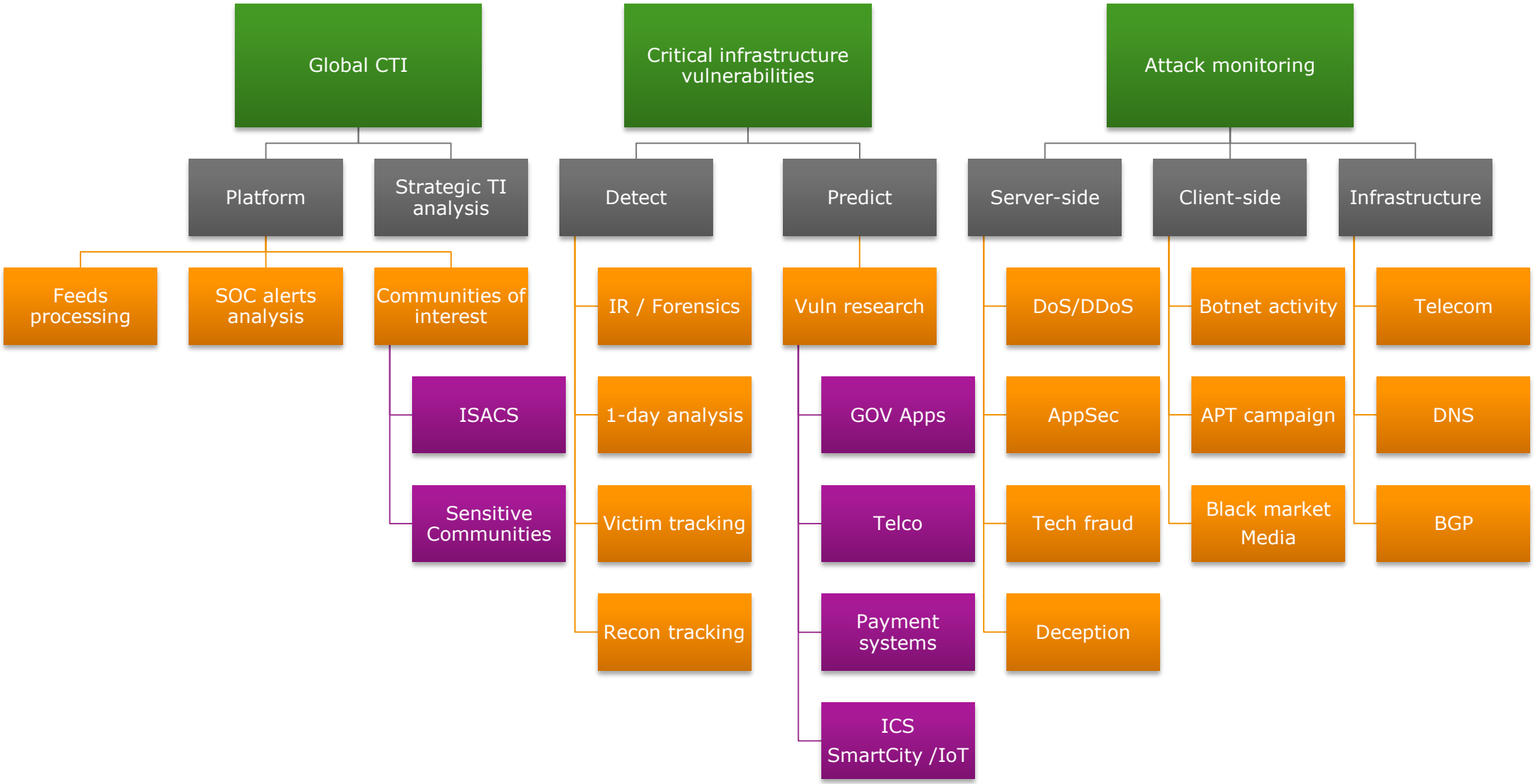
STATE OF COLLABORATION AND INTEL TODAY

- OSINT advisories and news articles about threats and vulnerabilities reach security teams in an un-timely manner in many cases
- Frameworks for sharing de-classified and private threat information across government, academia, sectors or even intra-sector are nascent at this time
- Indicators of compromise (IOCs) and / or tactics, techniques and procedures (TTPs) may or may not accompany alerts
  - If they do accompany alerts, they may or not be actionable in context (are they pertinent to my company?) or format (e.g., XLS, or STIX, etc.?)
  - If they are actionable, the security team may not know what to do with them or may not have the right process or technology in place
- Real collaboration requires human coordination and leadership -- the actual care and feeding, and other work beyond the creation of a platform or the intent to collaborate

KEY PARTNERS FOR COLLABORATION



EXAMPLE ECOSYSTEM TO BUILD COUNTERMEASURES



DESIRED OUTCOMES

- Goals: Region-specific TI collection and analysis:
  - Living threat and vulnerability landscape
  - Actionable information for electronic dissemination aligned with sector / access-level
  - Classified IOCs -> Unclassified
  - Resilience monitoring for cyber infrastructure
  - Early warning system for sector-level / national-level attacks

CONCLUSIONS

- UAE and GCC will face increasing cyber security threats in 2018 and beyond
- While cyber intelligence collaboration and countermeasures are relatively immature, some sectors, notably government and financial services, are moving in the right direction
- Real solutions transcend platform and threat feed implementations, and must include:
  - Public policy support (e.g., national policy, central bank)
  - Creation of threat intelligence centers and ISACS
  - Public / private partnerships
  - Subject matter expertise
- Dark Matter is helping to make this a reality – we'd be happy to tell you more