



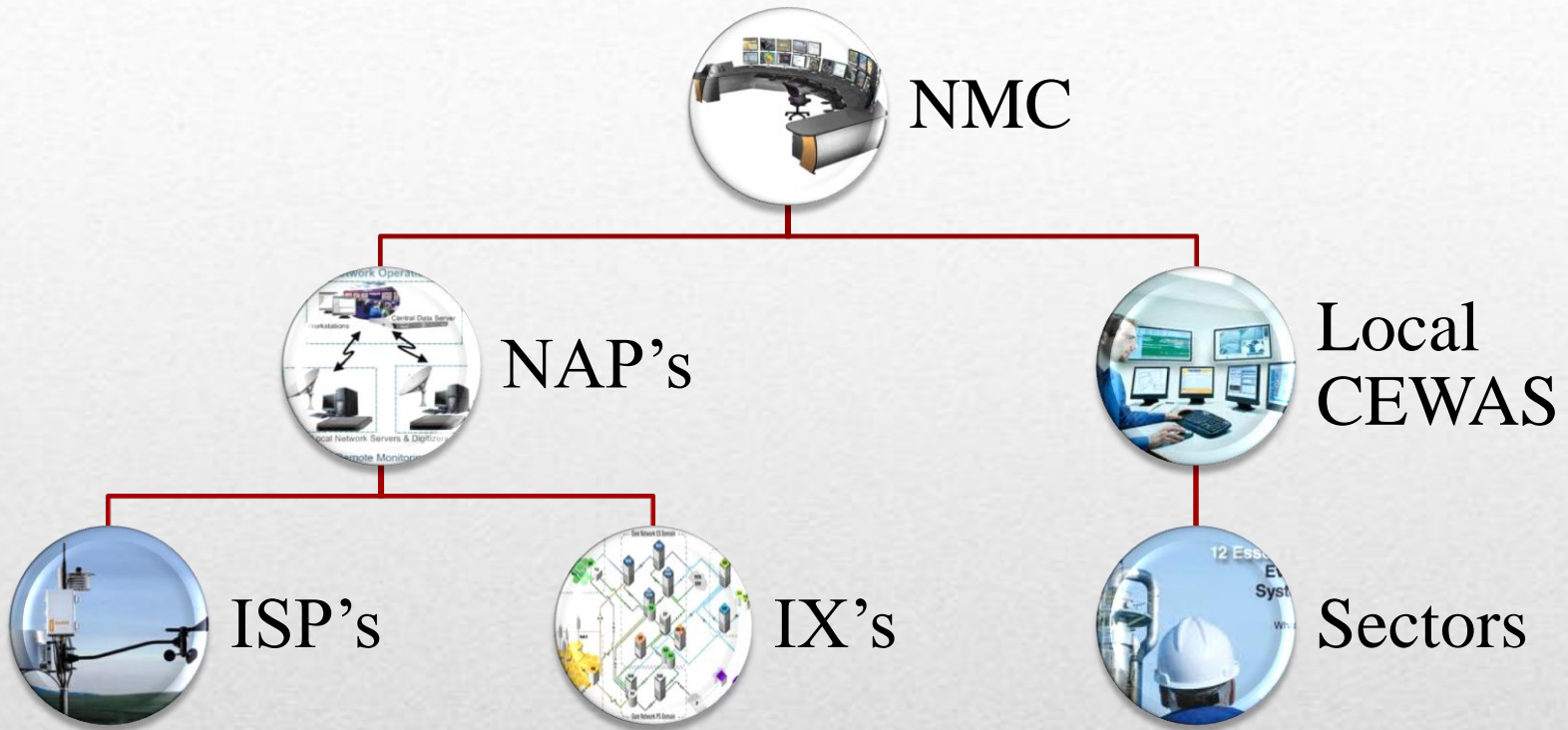
Id-SIRTII

CEWAS

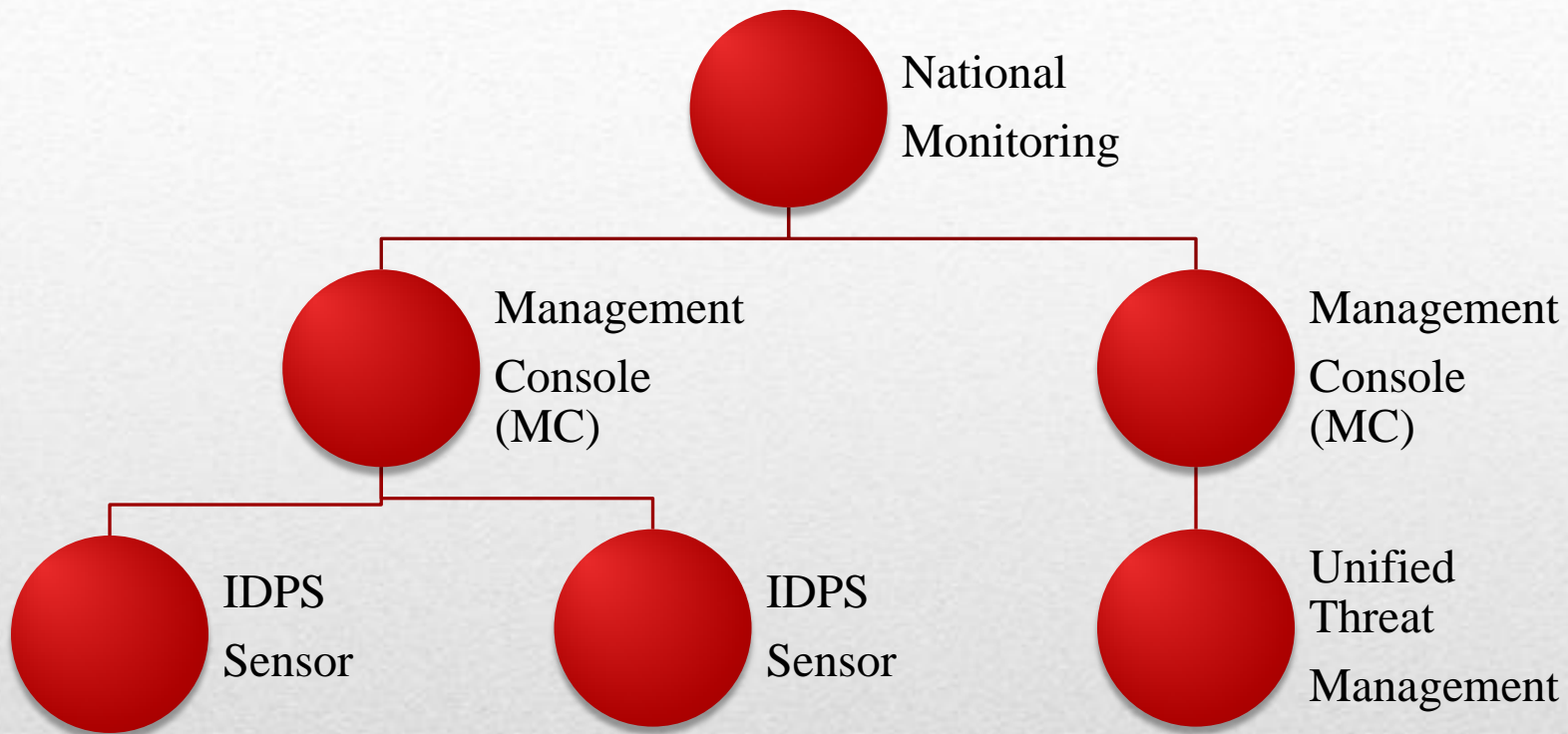
Cyber Early Warning System

- Part of National Cyber Defense Initiatives Strategy
- Priority to monitor National Critical Infrastructure
- National Monitoring and Crisis Coordination Center
- Incident Report, Analysis and Mitigation Center
- Cyber Emergency Response Team (CERT) including Mitigation, Recovery/BCP SOP and Management
- International Collaboration Protocol and Focal Point
- National Early Warning and Detection Infrastructure
- Promoting awareness and information sharing

CEWAS Organization



CEWAS Architecture



CEWAS Topology



Type of Attacks

- Caused by natural disaster - *not detected*
- Caused by social unrest (riot, war) - *not detected*
- Caused by IT system vulnerability- **DETECTED** (*DOS, spoof, sniff, flood, malware, SQL injection, XSS etc.*)
- Caused by human weakness/social engineering- *several (phishing/malicious sites, malicious code, SPAM)*
- Caused by lack of policy, procedures/standard, regulation and compliance- *not detected (part of IT security audit)*

Event Detection

- More than 60 million people connected
- Number 2 on Facebook number 3 on Twitter
- 35 million daily access to local online media
- 50 Gbit/s local traffic 60 Gbit/s international
- 2 million active internet/mobile banking users
- New generation (40 million students in 2014)
- Personalized services with multiplay application
- More private and sophisticated technology

Challenge: Growth

- 2 of 3 computer sold are notebooks/netbook/tablet
- Blackberry, smartphone, proxy application issues
- More than 180 million cellulars personal numbers
- More than 80 million cellular data users (pre paid)
- Average unlimited internet access now below US\$10
- 99% district was serve at least by GPRS access
- More than 40% Node-B networks (3G) penetration
- Incoming 4G (LTE) networks (early bid in 2012)

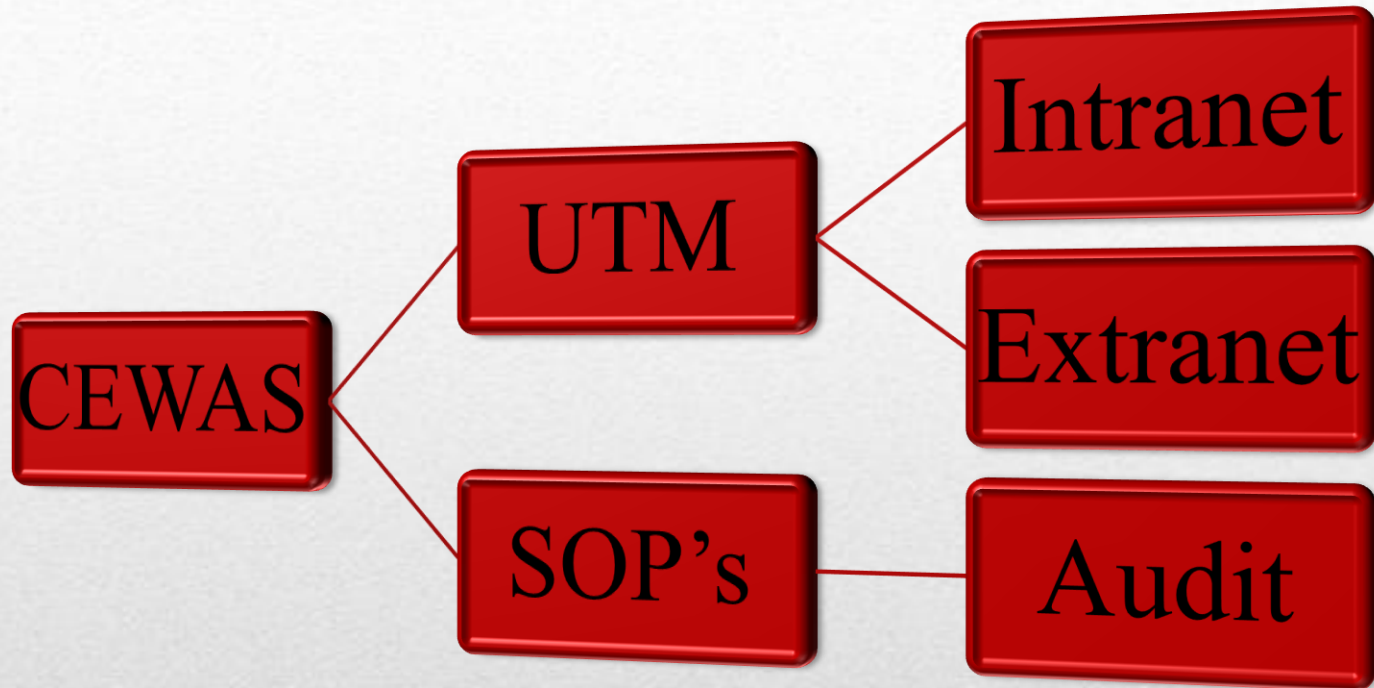
Challenge: Mobile

- Sophistication/targetted attack
- Personal information stealing
- Account hijacking & fraud crime
- Lack of awareness, user behaviour
- Mostly caused by data over exposure
- Social engineering techniques
- Phising & malicious code as tools
- Human, the weakest security link

Undetected Threat

- Trojans and backdoor
- Unsecure programming
- Counterfeit equipment
- Data/information misuse
- Level of access policy breach
- Physical security perimeter breach
- Inappropriate disposal procedures

Insider Attacks



In House CEWAS

- Professional certified human resources
- Skill improvement (training, drill)
- Continuous research and development
- Updated data and base of knowledge
- Log management and correlation analysis
- Periodic security assesment and audit (CIA)

Real STRENGHT

- Ravindo Tower 17th Floor
- Kebon Sirih Raya, Kav. 75
- Central Jakarta, 10340
- Phone +62 21 3192 5551 ; Fax +62 21 3193 5556
- office@idsirtii.or.id ; www.idsirtii.or.id

Thank You
