Collaborative Security: Responsibility, Confidence and Consensus

Trend Micro Inc.

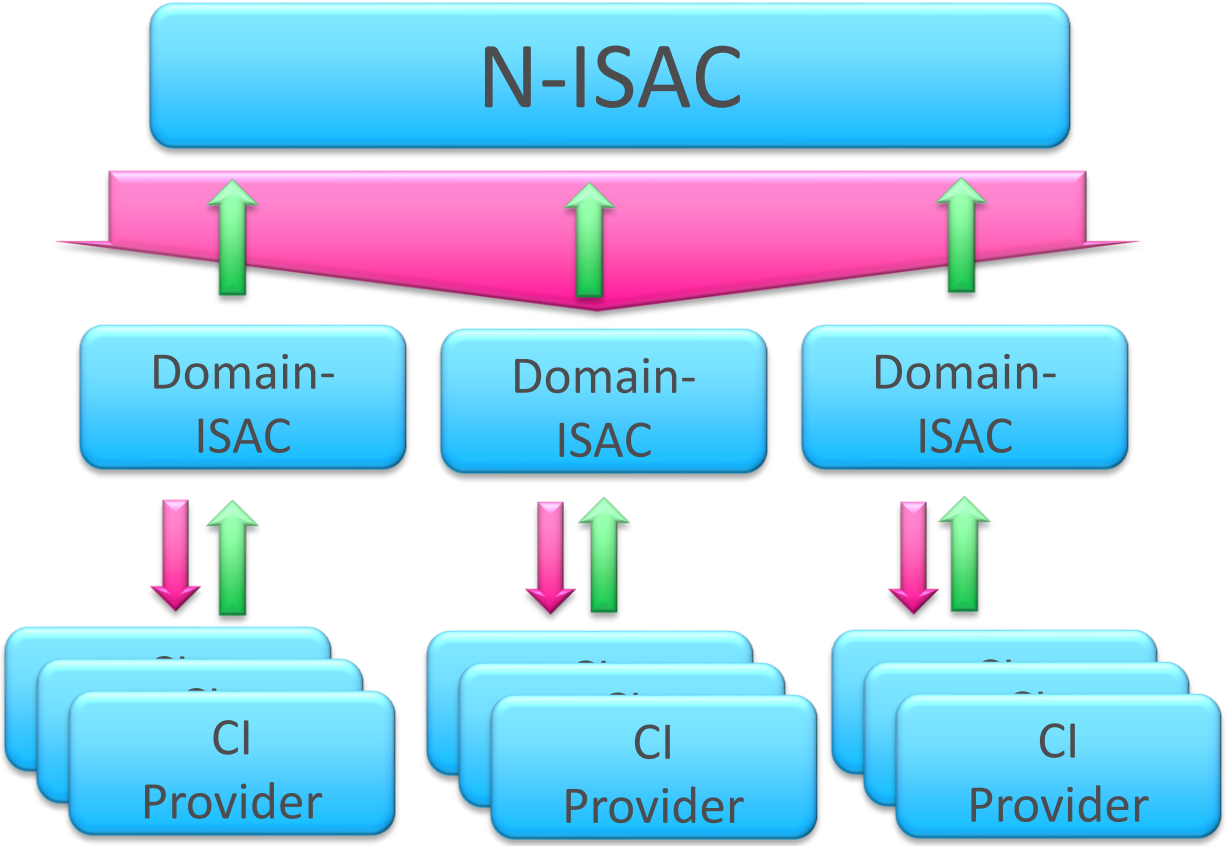


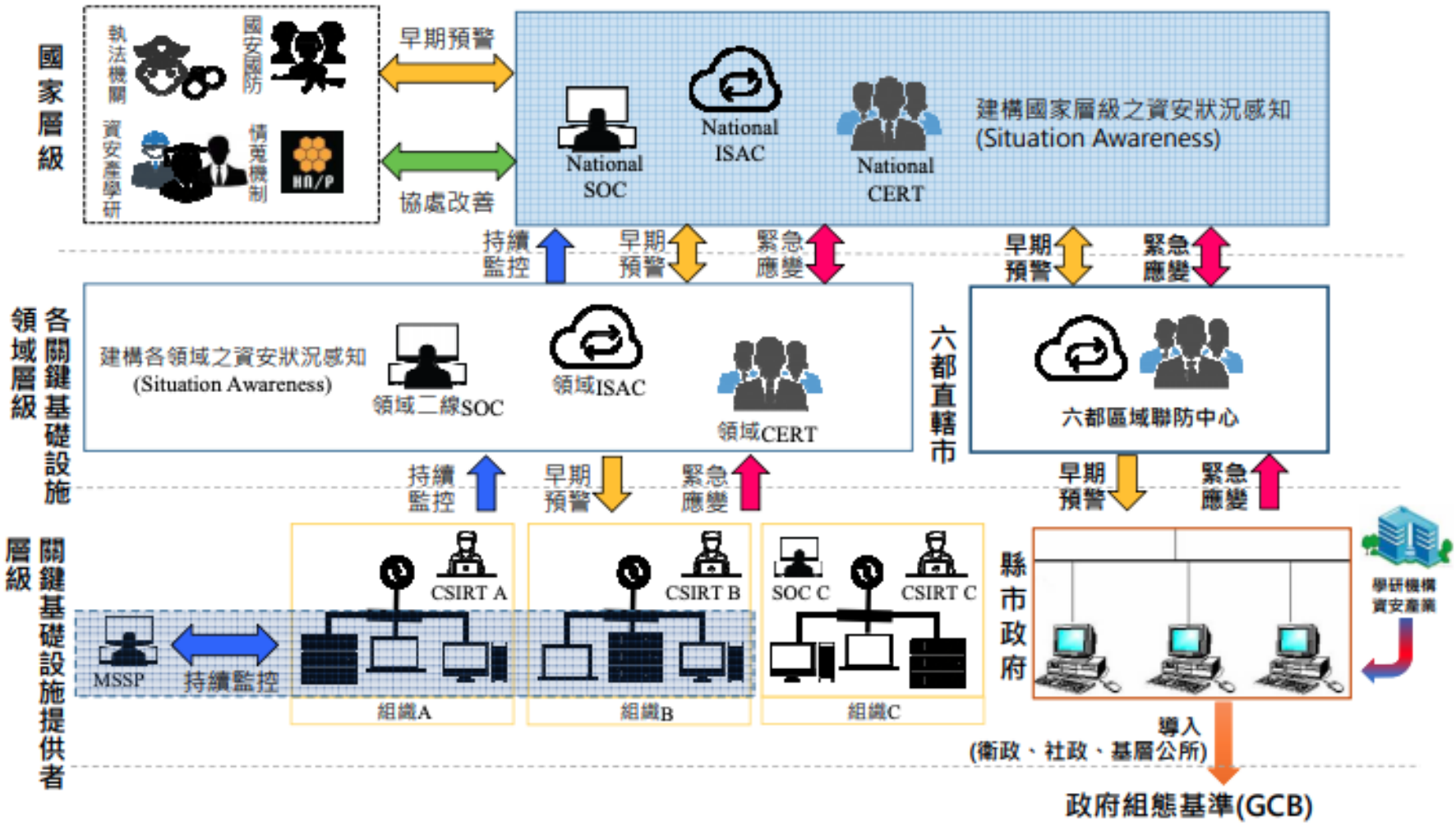
Threat Intelligence is critical for cyber security



TREND MICRO

Take Taiwan Government as an example..




國家層級
執法機關
國安國防
資安產學研
情蒐機制
早期預警
協處改善
National SOC
National ISAC
National CERT
建構國家層級之資安狀況感知
(Situation Awareness)
持續監控
早期預警
緊急應變
早期預警
緊急應變
各關鍵基礎設施領域層級
建構各領域之資安狀況感知
(Situation Awareness)
領域二線SOC
領域ISAC
領域CERT
六都直轄市
六都區域聯防中心
持續監控
早期預警
緊急應變
早期預警
緊急應變
關鍵基礎設施提供者層級
MSSP
持續監控
CSIRT A
CSIRT B
SOC C
CSIRT C
組織A
組織B
組織C
縣市政府
學研機構
資安產業
導入
(衛政、社政、基層公所)
政府組態基準(GCB)

The challenge of information sharing

- Lack of motivation and mutual benefit
  - Regulation enforcement is still the key driver of incident information reporting
  - Punishment is more than help for the victims to report cyber incident information
- The cyber threat is more customized than ever
  - The value of sharing for single malicious object is getting less
  - Understanding whole attack campaign take longer time

TREND MICRO

Suggestion: Areas to improve

- Build up the ability and capacity of incident response, incident investigation even threat research
  - National CERT
  - Domain CERT
  - Commercial sector (company CSIRT or outsourcing)
- Have a mechanism to share threat intelligence without victim information disclosure
- Facilitate the atmosphere of collaboration

TREND MICRO

Right concept and attitude for the authority and the public

Educate,
Educate,
Educate,

Thank You

TREND MICRO