

NCIRC (NATO Computer Incident Response Capability)

11th TF-CSIRT Meeting – 15 Jan 2004, Madrid

Suleyman Anil

Head, NCIRC Coordination Centre (CC)

NATO Office of Security, NATO HQ, 1110 Brussels

s.anil@hq.nato.int +32 2 707 4939

Outline

- Concept
- Constituency
- Services
- Infrastructure
- Status

NCIRC Concept - Development

- “CONOPS” – 18 months
- NATO-specific functions and responsibilities
- Concept Approval by highest IT Authority in NATO (Jan 02)
- Funding Allocation by Political Decision (end 02)
- Momentum of Sep 11

NCIRC Concept - Definition

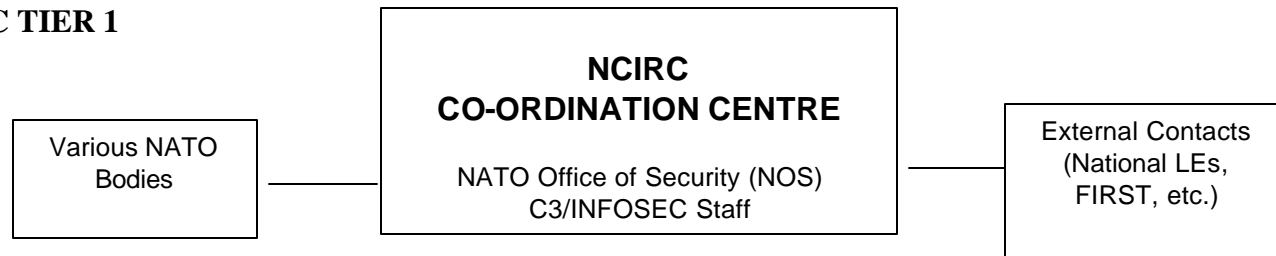
- Technical and Legislative support services to respond to computer security incidents within NATO
- Centralized Services for:
 - Preventive Measures (bulletins, software updates, VA Teams, etc.)
 - Responsive Measures (Incident & IDS Support and Response)
 - Legislative Support (Forensic, Investigations, Policy Updates)

NCIRC Concept - Requirement

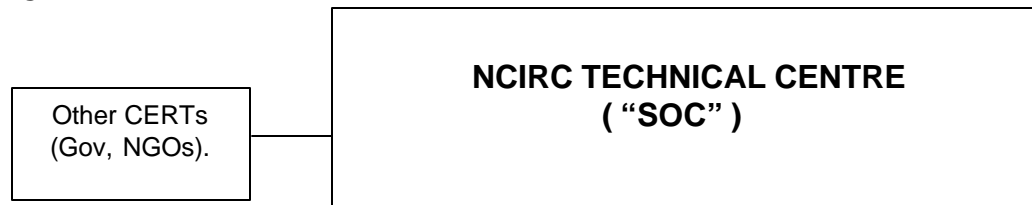
- NATO-wide response coordination during an incident
- Central knowledge base to support local Sys Admins
- Centralized on-line and on-site services
- Centralized forensic and LE support arrangements
- Optimization of resources
- Contacts with external CERTs/CSIRTs

NCIRC Concept – Functional View

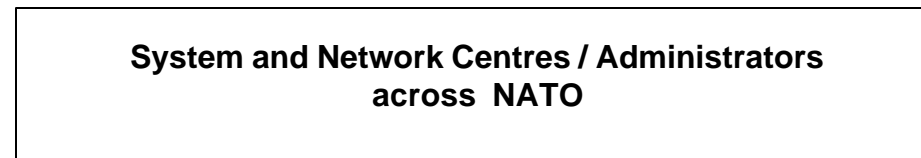
NCIRC TIER 1



NCIRC TIER 2



NCIRC TIER 3



Constituency

- Closed Networks
- Open Networks (Internet enabled)
- Total of about 25.000 workstations (locally managed)
- Gateways to National Networks
- Central CMBs/CCBs
- Common baselines and standards (reasonably)
- Centralized Network Management (backbone routers & circuits)
- Central HelpDesks
- Central Inspection Authority

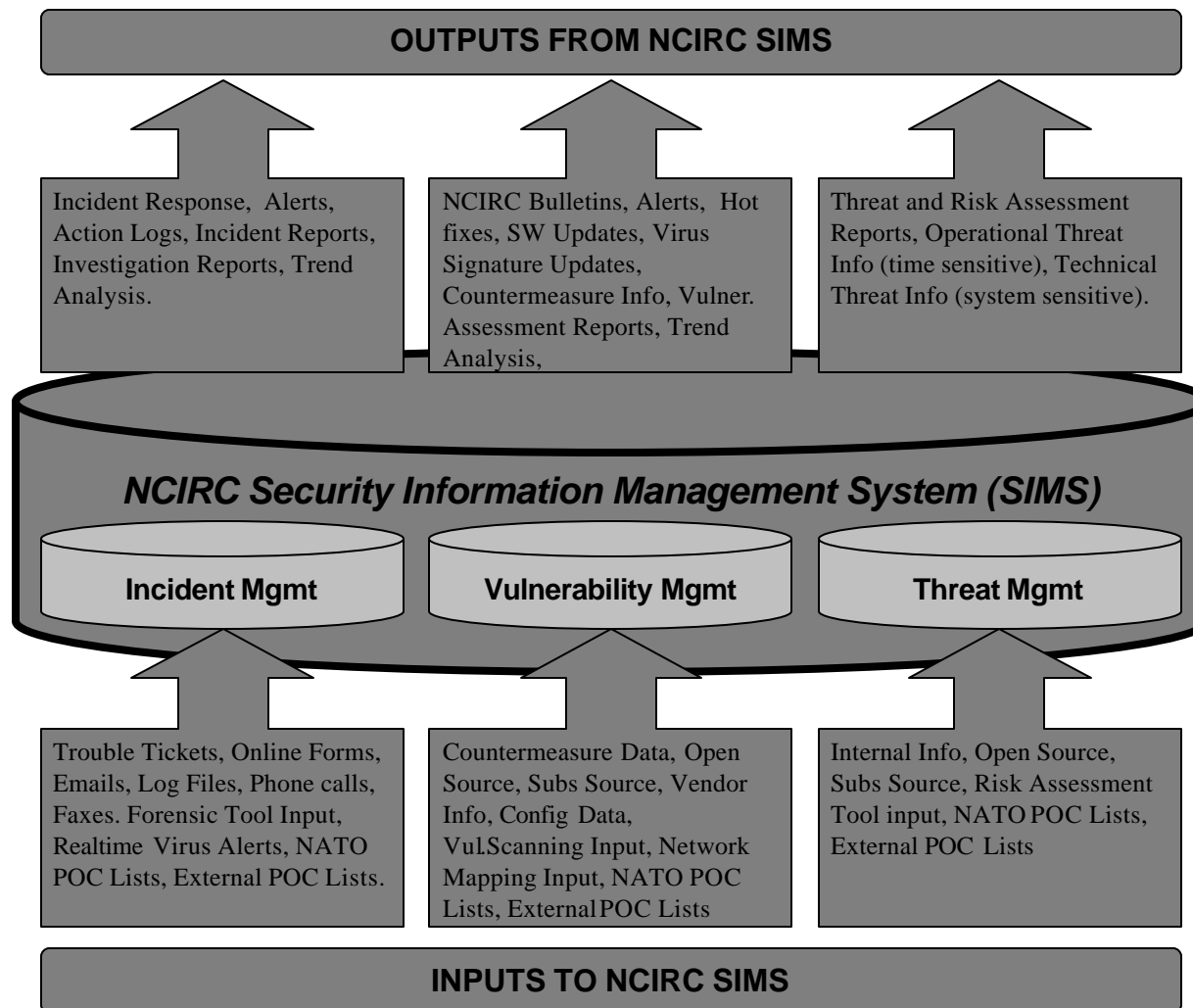
NCIRC Services

- Incident Handling
- Vulnerability and Threat Information
- Vulnerability Assessment (online / on site)
- Consultancy Services (Scientific and Forensic)
- Online Data Collection and Monitoring (IDS, Antivirus, Firewalls)
- Online Support (auto updates, downloads, SOPs)
- Off-line incident analysis and security testing

Infrastructure

- New “SOC”
- Two Dedicated LANs to support Closed & Open Networks
- Security Information Management System (SIMS)
- WEB Portals
- Enterprise Software Licenses
- Offline/mobile Equipment
- Consultancy Services
- Subscribed Services
- Additional Manpower

Infrastructure - SIMS



Status

- Existing capability - limitations
- New Contract award before end Jan 04
- Completion by 2nd Q 2004

Questions ?