Cyber Defence Technical Information Sharing in a Multinational Environment

Ms. Manisha Parmar, Senior Scientist
Cyber Security Service Line
What is Smart Defence?

‘It is a renewed culture of cooperation that encourages Allies to cooperate in developing, acquiring and maintaining military capabilities to undertake the Alliance’s essential core tasks agreed in the new NATO strategic concept.’

‘That means pooling and sharing capabilities, setting priorities and coordinating efforts better.’
What is the MN CD2?

• A smart defence project, the Multi-National Cyber Defence Capability Development:
  – consists of 4 nations (Canada, Romania, the Netherlands and Norway) with participation from Finland
  – is pursuing several Work Packages (WPs) related to the growth of Cyber Defence capabilities
  – is supported by the NATO Communication and Information Agency or NCI Agency
MN CD2 Values

• Nations want to improve their cyber defences capabilities by working together
• Nations want to leverage their investment by exploiting common funded activities and capabilities to the fullest
Cyber Defence Technical Information Sharing

• Subset of MN CD2 nations: CAN, ROU, NLD & FIN
• Developed “CIICS”; the Cyber Information and Incident Coordination System
• Now, working together to establish the NATO CIICS Federation; community for sharing cyber defence technical information in trusted environment
What is CIICS?

• Pronounced “kicks” – it is a web based application used for CD information sharing and incident management, both within organizations and across organizational boundaries – Or within nations and across national boundaries

• CIICS is comprised of two major subsystems:
  – Ticket Management Subsystem (TMS)
  – Information Sharing Subsystem (ISS)

• CIICS implements STIX for structured sharing of data
Why We Didn’t Choose an Existing Tool

Not possible to find an existing tool which met a multinational requirement set, with sometimes conflicting requirements.

No tool (at the time) supported information sharing across organizational boundaries.

Nations desired end product to be freely distributable to any national agencies without license limitations.

Led to CIICS which is highly configurable and supports customized work flow support.
What is the NATO CIICS Federation?

- Newly created federation, originated by the three CIICS sponsoring nations: Canada, Romania and the Netherlands
  - NCI Agency presently acting as software custodian on behalf of the federation
- Trusted community to share CD information and, as desired, data on past or present incidents
- Federation is governed by the CIICS Support Board (CSB) with representation from MN CD2 participating nations and the NCI Agency
NATO CIICS Federation Architecture

- CIICS is a hybrid architecture with centralized (offline) governance and direct peer to peer sharing.
CIICS Sharing Models

• Ticket Management Subsystem allows for either local only or joint sharing; governed by Role Based Access Control (RBAC)
  – TMS data considered sensitive, thus, finer access controls in place to access data
  – Default is local tickets unless explicitly shared via Joint Coordination Ticket

• Information Sharing Subsystem:
  – Wiki style (unstructured) repository
    • Communities of Interest for users either local or federation wide; based on public, protected or private communities
  – Reference library (structured, based on STIX)
    • Fully visible and accessible to all users in federation
Primary Objectives of the NATO CIICS Federation

• Primary objective: to promulgate timely, generic CD technical information to assist national and military Computer Emergency Response Teams (CERTs) to:
  – identify new and/or zero day threats in a timely manner;
  and
  – Identify relationships between what may first appear as isolated events

• Enable responders to jointly coordinate response to attacks targeted against multiple nations
Derived Objectives of the NATO CIICS Federation

- Knowledge base growth to aid in incident mitigation by quickly reviewing historical incidents with similar characteristics
- Enable responders to solicit other experts for inputs and/or suggestions
- Enable analysts to identify trends and facilitate post attack analysis
Sponsoring nations will be online by February 2016.

NATO CIICS Federation fully deployed: this was the easy part!

Additional nations on board when license agreement for CIICS usage is signed.

Then what? … how do you encourage collaboration from users who traditionally work in a “need to know” environment?

New users will attempt to consume before contribute.
• In the unclassified environment:
  – Overcoming user fear of accidentally sharing sensitive or classified information within the unclassified domain
    • As a result, users will withhold information unless absolutely certain of sensitivity
  – Preventing users from over sharing; focus on quality over quantity and encourage sharing of valuable data, not just stuff you find on the Internet
Information Sharing Challenges (2)

- In a multinational environment:
  - National Memorandums of Understanding (MOUs) do not cover information sharing at a technical level for Cyber Defence, nor do bilateral agreements or treaties for cooperation
  - Users do not know one another, collaboration must occur based on inherent trust
    - Not easy to plan face to face meetings due to large distances and high turn over of military staff make the establishment of personal relationships difficult
  - Users must agree on a common language (English); understanding of terms/definitions is not consistent
Review Using DOTMLPF-I

- **Doctrine**: customizable workflow for national incident workflows, national policy for inter-national CD sharing
- **Organization**: inherited by CERT team structure
- **Training**: documentation and training provided to nations in a “train the trainer” fashion, if requested, for CIICS deployment and features
- **Material**: hardware & operating system requirements to operate CIICS outlined
- **Leadership & Education**: CERT leadership guidance on incident management and CD information sharing; agency recommendations on guidelines
- **Personnel**: availability of CERT staff national responsibility
- **Facilities**: physical resources and location a national responsibility
- **Integration**: developed in the tool itself
Assumption Look-back

All aspects of the DOTMLPF-I had been addressed with the exception of multinational CD information sharing policies

Discovered that national policies for information sharing in multinational environments is non-existent or immature

Major Gap Identified!
Guidelines and procedures for information sharing in a multinational environment must be developed!

• This was further shown as a NATO-wide limitation via Cyber Coalition 2015 exercises

• Organizations require self-assessment to ensure they possess the capabilities to effectively participate in community; this can be done using recommendations provided by NCI Agency.
Fallout

- Despite a well designed and created product, the primary objectives of the NATO CIICS Federation would not be fully met without the necessary CD information sharing guidelines and procedures
- CIICS development concluded successfully (on time, on budget) but...

A tool is only the enabler; how the tool is used dictates whether it is truly successful and user accepted!
Remediation

• Identify legal requirements to enable information exchange between nations and implement appropriate paperwork, as necessary (multilateral agreements, MOUs, etc.)

• **Document** Terms of Use (TOU) for unclassified information sharing
  – Nations responsible to transform TOU into policy!

• Train **Leaders** to implement policy and leverage technical features to support it

• Consider classified information sharing environment and advantages / disadvantages
Legal Requirements for Information Sharing

• We already have a CIICS License Agreement governing use of the tool
• Need to decide if Non Disclosure Agreements (NDAs) or Memorandums of Understanding (MOUs) are required
• Require CIICS Terms of Use for agreement by all participants!
• Developing the CIICS Terms of Use (TOU) for Unclassified Information Sharing
  – Include guidelines for how to become an active information contributor by identifying national roles/responsibilities, as well as recommendations for national guidelines
    • E.g. focus on the intrusion attempt, not whether it was successful or not, zero out low order bits in the IP to hide network subnet
Classified Information Sharing Group

• Establishing an information sharing group in the classified environment requires much more planning and strategy

• Unique set of advantages and disadvantages;
  – longer to establish due to security checks and accreditation for tools with potentially smaller subset of users
  – may result in higher quality threat intelligence (non repudiation) that is actionable faster
Expected Outcomes

• With a TOU released, nations should have a better understanding of **what** needs to be shared, **when** it should be shared and with **who**

• Still cannot force users to share; leap of faith that a culture shift will occur with proper guidance and leadership
Who Can Join the Federation?

- Membership is open to NATO Nations and Partner Nations, as well as other nations on a case by case basis, at the discretion of the CSB.
- Commercial / industry partners can also join the federation with CSB approval.
- A nation does not need to join the MN CD2 in order to join the federation.
Questions

For more information, or to provide comments or feedback, contact:

Ms. Manisha Parmar
Senior Scientist,
Cyber Security Service Line
NATO Communication and Information Agency

manisha.parmar@ncia.nato.int