Global Response Centre (GRC) & CIRT Lite
Regional Cyber security Forum 2009, Santo Domingo, Dominican Republic 23rd to 25th November 2009
IMPACT – Service offerings

- Global Response Centre (GRC)
- CIRT Lite
IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

IMPACT - “GLOBAL RESPONSE CENTRE”
Need for GRC

- Access to the right information at the right time
  - Too many sources of information
  - Information is duplicated across various information sources
  - Very few security incident feeds are customised

- No effective collaboration channels
  - Any single country is vulnerable against a well co-ordinated international cyber attack
  - There is a significant pool of untapped expertise within the security industry and the academia
What does the GRC offer?

- **Syndicate** information from various trusted sources to enable effective remediation of security incidents
- **Automate** the process of collecting, monitoring, selecting, retrieving, tagging, cataloging, visualising and disseminating data on security incidents
- **Collaborate** with member Governments’ agencies, members of academia, members of the security industry and trusted experts to provide resolution to security incidents
- **Operate** a 24x7 Response Centre
Global Response Centre - Components

• The GRC’s ‘Network Early Warning System’ (NEWS) seeks to assist member countries in the early identification of cyber-threats and to provide guidance on the necessary remedial measures.

• Current partners for the GRC include Symantec Corporation, Kaspersky Labs, F-Secure, Trend Micro, Microsoft, SANS Institute among others.
Global Response Centre - Components

- The GRC's ‘Electronically Secure Collaborative Application Platform for Experts’ (ESCAPE). ESCAPE is a unique framework that enables authorised cyber experts across different countries to pool resources and remotely collaborate with each other in a secure and trusted environment.

- ESCAPE enables the GRC to act as a ‘one-stop’ coordination centre for countries in times during emergencies, allowing for swift identification and sharing of available resources across borders.
## GRC Features Definition

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early Warning System</td>
<td>Real-time Information mashup from various sources</td>
</tr>
<tr>
<td>Expertise Finder</td>
<td>Facilitates Expert Knowledge Exchange Network and Real-time communication</td>
</tr>
<tr>
<td>IMPACT Community</td>
<td>Social Networking Facility for IMPACT members</td>
</tr>
<tr>
<td>Remediation Facility</td>
<td>Research and Development Lab</td>
</tr>
<tr>
<td>Malware Threat Analyzer</td>
<td>Malware Submission Facility - Automated Threat Analysis System</td>
</tr>
<tr>
<td>Trend Libraries</td>
<td>Trend Archive</td>
</tr>
<tr>
<td>Global Visualization of Threats</td>
<td>Global Security Health Check. Global Threat Map</td>
</tr>
<tr>
<td>Visualization of Threats by Countries</td>
<td>Threats by Countries</td>
</tr>
<tr>
<td>Incident &amp; Case Management</td>
<td>Case Management and Incident Escalation (Cross-CERT compliant)</td>
</tr>
<tr>
<td>Trend Monitoring &amp; Analysis</td>
<td>Trend Dynamic Data Analysis and Assessment</td>
</tr>
<tr>
<td>Knowledgebase</td>
<td>Libraries of Security Documents and Information</td>
</tr>
<tr>
<td>Reporting</td>
<td>Executive and Technical Report Generation Facility</td>
</tr>
<tr>
<td>IMPACT Honeynet</td>
<td>IMPACT Integrated Honeynet Framework</td>
</tr>
<tr>
<td>Video Broadcasting</td>
<td>Video broadcasting of emergency news from IMPACT</td>
</tr>
<tr>
<td>Threat Route Plotter</td>
<td>Security Threat Trails</td>
</tr>
<tr>
<td>Resolution Finder</td>
<td>Map Resolution to Security Threats</td>
</tr>
<tr>
<td>Remote GRC Integration</td>
<td>Country based GRC integration with IMPACT</td>
</tr>
</tbody>
</table>
Information sources for NEWS

Symantec, SANS, Secunia, Arbor Networks, SOPHOS

F-Secure, Trend Micro

SRI-MTC

Threat Database, Vulnerability Database, Malware Database, Port Database, Pattern Database

Botnets, Command & Control Servers, Sources, Targets, Ports, Viruses, Malwares, Vulnerabilities, Spywares, Phishing, Threat Map, Global Threatcon, Incident Mapping
IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

IMPACT - “CIRT LITE”
Basic setup framework

A framework is necessary for outlining the implementation plan – as guiding principles, so that the basic infrastructure and services are put in place in order to operationalise the national CIRT.

Below are the components proposed for the national CIRT

- *Technical Solution*
- *Organisation structure and manpower planning*
- *Policies/procedures*
- *Training for CIRT staff*
IMPACT – CIRT setup stages

- Awareness
  - Detailed checklists
  - Material for conducting internal awareness checks

- Mobilisation
  - Identification of manpower
  - Preparation of hardware and software

- Capacity Building
  - Training session for resources
  - Installation and configuration of CIRT solutions

- Operations
  - Integration to IMPACT’s GRC
  - Enhancement of CIRT offering
Technical components of CIRT Lite

- Incident Management
- Advisories
- Mailing List
- Public Portal

Optional:
- IMPACT Local Honeypot Deployment
IMPACT’s CIRT-Lite – Architecture
Technical components

Incident Management

- Internal ticket handling and tracking for CIRTs
- Role based workflows for ticket handling
- Processing of vulnerability and incident information
- Incident tracking

Advisories

- Authoring and publishing system for advisories
- Databases for vulnerability information and artifacts
Technical components

• **Mailing list solution for:**
  - Technical Cyber Security Alerts
  - Cyber Security Bulletins
  - Cyber Security Alerts
  - Cyber Security Tips
  - Current Activity

• **Public Portal**
  - Content Management System to manage the CIRT’s web presence

• **IMPACT ESCAPE and NEWS integration to CIRT-Lite**

• **Optional:**
  - IMPACT local HoneyNet deployment
Incident and Advisory management

Overview of recent advisories

[ Advisory Overview ]

Advisory-Statistics

- 3 Draft Advisories
- 0 Published Advisories
- 3 All Advisories - Tickets of the Year
- 3 All Advisories - Tickets

[ unlocked Advisory-Tickets ]

Results: 1-1 - Total hits: 1 - Site: 1

<table>
<thead>
<tr>
<th>Ticket#</th>
<th>Advisory Number</th>
<th>Title</th>
<th>Queue</th>
<th>Priority</th>
<th>State</th>
<th>Created</th>
<th>Ticket</th>
<th>Advisory</th>
</tr>
</thead>
<tbody>
<tr>
<td>20060032810000055</td>
<td>AA-A-0000</td>
<td>Execution of arbitrary code th[.]</td>
<td>Advisory</td>
<td>3 normal</td>
<td>open</td>
<td>03/28/2006 12:08:49</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

[ locked Advisory-Tickets ]

Results: 1-2 - Total hits: 2 - Site: 1

<table>
<thead>
<tr>
<th>Ticket#</th>
<th>Advisory Number</th>
<th>Title</th>
<th>Queue</th>
<th>Priority</th>
<th>State</th>
<th>Created</th>
<th>Ticket</th>
<th>Advisory</th>
</tr>
</thead>
<tbody>
<tr>
<td>20060032810000025</td>
<td>AA-A-0000</td>
<td>Internet Explorer vulnerability[.]</td>
<td>Advisory</td>
<td>3 normal</td>
<td>open</td>
<td>03/28/2006 12:05:39</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
### Incident and Advisory Management

#### Incident view

**Specification**
- **Incident of:** 2008003281000017
- **Title:** Botnet DDoS attack against 85.1.03.16.65
- **Provisional Classification:** Denial-of-service
- **Complexity:** 3 normal
- **Effort:** 2 low
- **Impact:** Denial-of-Service of the attacked system
- **Defence Activity:**
  - **started:** Yes
  - **successful:** Yes
- **Incident reported:** 03/28/2008 11:38:19 GMT-01:00 Berlin Summertime

**Contact Addresses**
- **Reporter:** Salutation: Mr.
  - **Firstname:** Vincent
  - **Lastname:** Viclin
  - **Username:** vincent
- **Victim:** Salutation: Mr.
  - **Firstname:** Vincent
  - **Lastname:** Viclin
  - **Username:** vincent

**Details**
- **State:** open
- **Priority:** 4 high
- **Queue:** Incident
- **Locked:** unlock
- **Created:** 03/28/2006 11:38:50
- **Created by:** Part Bob (bob)
- **Changed:** 03/28/2006 11:45:58
- **Changed by:** Part Bob (bob)
- **Link (Normal):**
- **Link (Parent):**
- **Link (Child):**
Incident and Advisory Management

- The IDMEF - Intrusion Detection Message Exchange Format console

<table>
<thead>
<tr>
<th>MessageID</th>
<th>Type</th>
<th>AnalyzerID</th>
<th>Classification</th>
<th>Created</th>
<th>Imported</th>
</tr>
</thead>
</table>
CIRT-Lite - Mailing List

- Mailing List Portal

**Welcome to the Country-CERT Mailing List Subscription System**

- **Technical Cyber Security Alerts**
  - Subscribe Here
  - Written for system administrators and experienced users, technical alerts provide timely information about current security issues, vulnerabilities, and exploits.

- **Cyber Security Bulletins**
  - Subscribe Here
  - Bulletins summarize information that has been published about new security issues and vulnerabilities for the week prior. They are published weekly and are written primarily for system administrators and other technical users.

- **Cyber Security Alerts**
  - Subscribe Here
  - Written for home, corporate, and new users, these alerts are published in conjunction with technical alerts when there are security issues that affect the general public.

- **Current Activity Updates**
  - Subscribe Here
  - Provide up-to-date information about high-impact types of security activity affecting the community at large. Current activity is updated on an as-needed basis which ranges from several times a week, to several times a day. Subscribers can expect to receive one update per entry as they are published to the Country-CERT website.
CIRT-Lite - Mailing List
CIRT-Lite – Public Portal examples

HELPFUL RESOURCES

Designed to assist the average computer user, GCSC and the Calgary Police Service have created a number of tools to help prevent new cyber crime cases from occurring. Check out the categories below to learn how to protect yourself and your family.

Identify Theft
- Protect your identity. Arm yourself with knowledge.

Phishing
- Criminals often go “phishing” for personal information.

Safe Surfing
- Surf the Internet safely.

Networking
- Communicate safely on social networking sites.

Email & instant Messaging
- Dealing safely: Do & Don’t.

Chain Letters
- Unravel the chain.

Cyber Bullying
- Stop Cyber Bullying.

FURTHER RESOURCES

APWG
Bad Spy Patrol
Babblingbrook
Calgary Crime Stoppers
Canadian Bankers Association
ChatDanger
Cyberbullying.ca
CyberTips.ca
Federal Trade Commission
Fraud.org
Government of Alberta Get Web Wise
Hate, Don’t Buy In
Internet 101
Internet Crime Complaint Center
Kids’ Internet Safety Alliance (KISA)
Media Awareness Network
National Center for Missing and Exploited Children
Netmartz
Organisation Structure

*Public Relations/Legal

- Optionally expertise and budgets permitting the CIRT can also look at additional resource for Public Relations/Legal
Policies and Procedures

Policies are governing principles adopted by CIRTs. In Phase 1, IMPACT will help put the following policies in place:

- Authority & Role of the CIRT
- Information Categorisation
- Incident Report & Handling
CIRT - Capacity building

• Training will include:

- Managing a CIRT
- Incident reporting guidelines
- Response methods
- Incident response tools
- Incident prevention methods
- Other information necessary to protect, detect, report & respond to computer security incidents
Implementation Phases

An integrated plan for the national CIRT setup is divided in 3 phases:

- **Phase 1: (CIRT Lite) Basic infrastructure and services to include:**
  - Reactive services: Incident response & handling, alerts & warnings
  - Proactive services: Announcements

- **Phase 2: Enhanced services to include:**
  - Reactive services: Vulnerability analysis and handling
  - Proactive services: Technology watch
  - Security quality management: Training and awareness

- **Phase 3: Advanced CIRT services**
  - Proactive services: Security audits & assessments
  - Reactive service: Forensics analysis
  - Security quality management services: Risk Analysis, Security Consulting
Implementation Phases (Cont…)

- Establish contact with National CIRTs
- Information gathering (gap analysis)
- Trainings to CIRT personnel
- CIRT Lite hardware & software deployment
- Post-deployment support

Phase 3 → Phase 2
Solution delivery

• Three (3) people/representative selected by each member’s country will attend a regional workshop for five days

• During the Workshop – representatives will be provided with necessary technical knowledge and hardware required in implementing CIRT at their own country

• Representatives will then set up the CIRT in their country

• IMPACT will assist member’s country in configuring hardware and customising the process while setting up the CIRT
E-mail: contactus@impact-alliance.org