IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

Global Response Centre (GRC) & CIRT Lite

Regional Cyber security Forum 2009, Hyderabad, India
23rd to 25th September 2009

IMPACT – Service offerings

- Global Response Centre
- 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 for a country or region
- 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

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

Information sources for NEWS

Symantec

SANS

Secunia

Kaspersky

Arbor Networks

SOPHOS

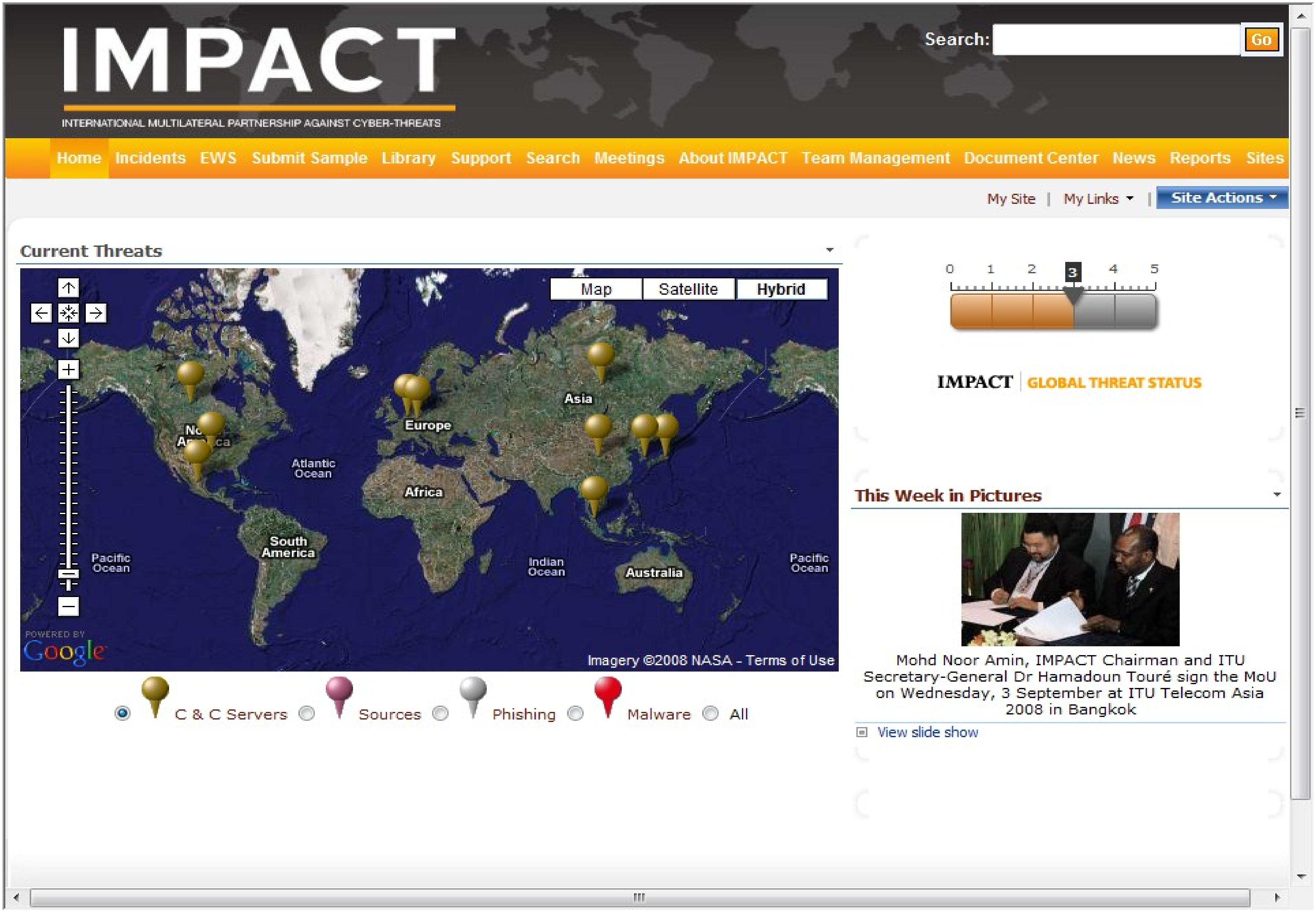
SRI-MTC

F-Secure

Trend Micro

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

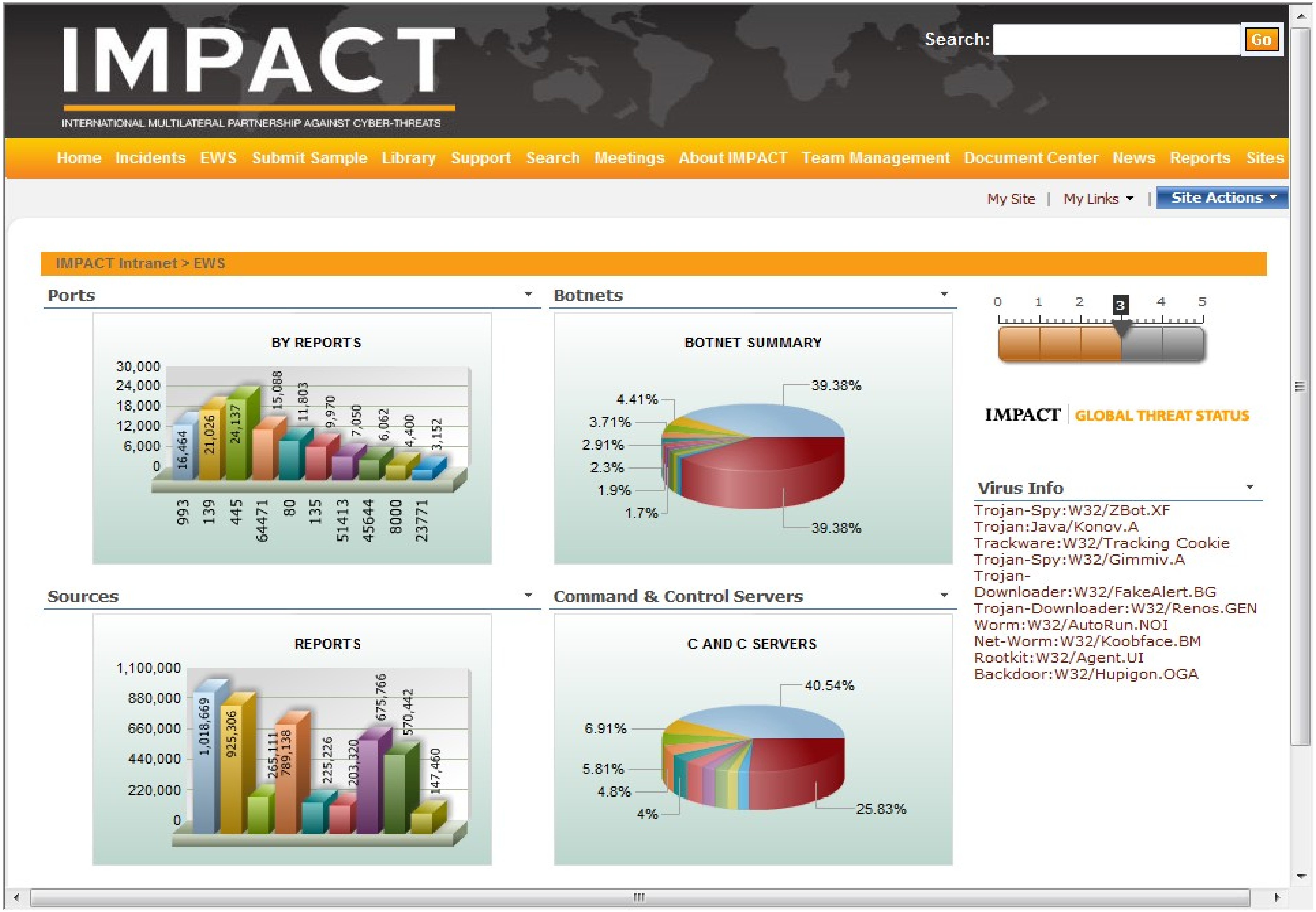


Current Threats

● C & C Servers ○ Sources ○ Phishing ○ Malware ○ All

This Week in Pictures

Mohd Noor Amin, IMPACT Chairman and ITU Secretary-General Dr Hamadoun Touré sign the MoU on Wednesday, 3 September at ITU Telecom Asia 2008 in Bangkok



Ports

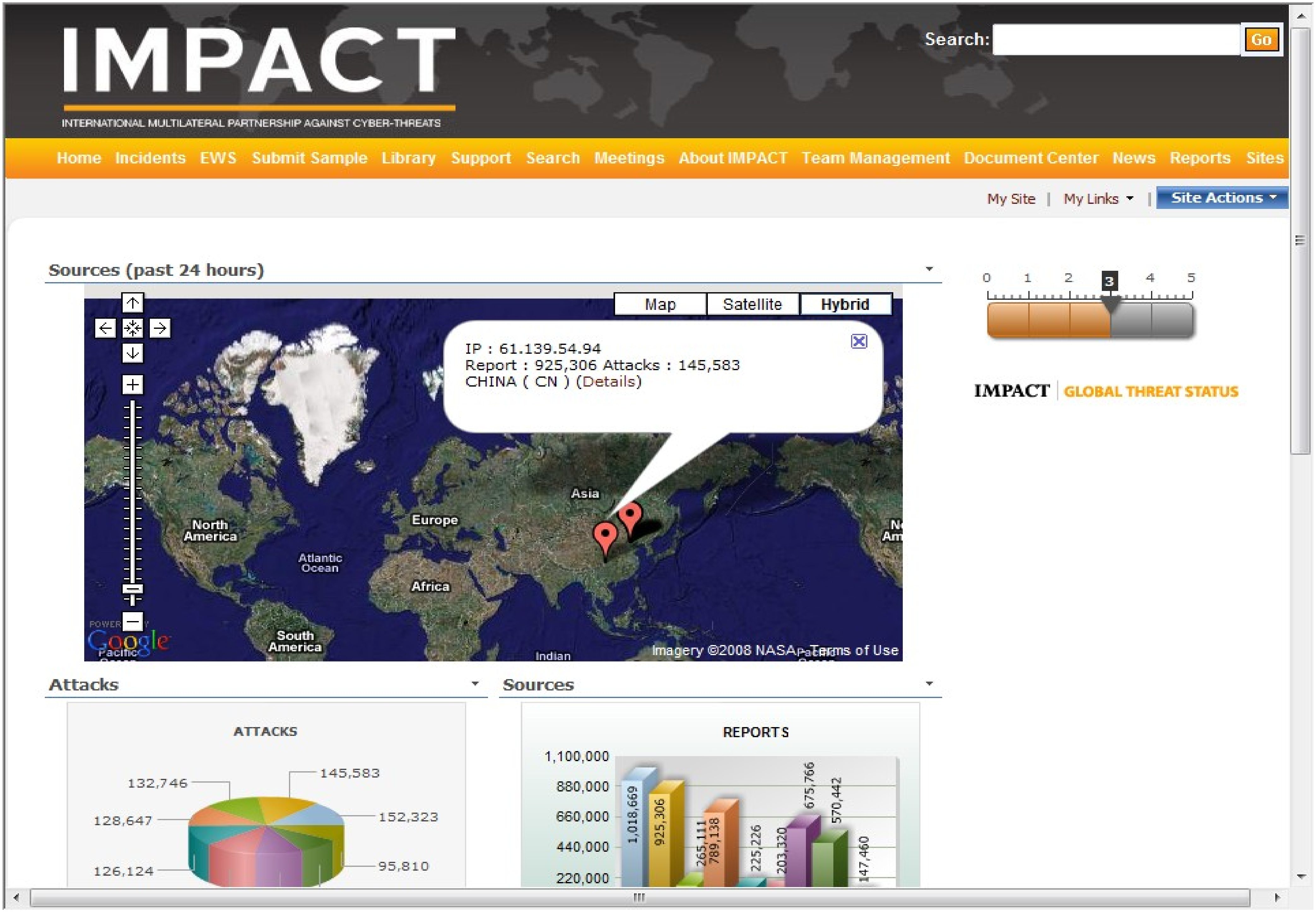
Botnets

Virus Info

Trojan-Spy:W32/ZBot.XF
Trojan:Java/Konov.A
Trackware:W32/Tracking Cookie
Trojan-Spy:W32/Gimmiv.A
Trojan-Downloader:W32/FakeAlert.BG
Trojan-Downloader:W32/Renos.GEN
Worm:W32/AutoRun.NOI
Net-Worm:W32/Koobface.BM
Rootkit:W32/Agent.UI
Backdoor:W32/Hupigon.OGA

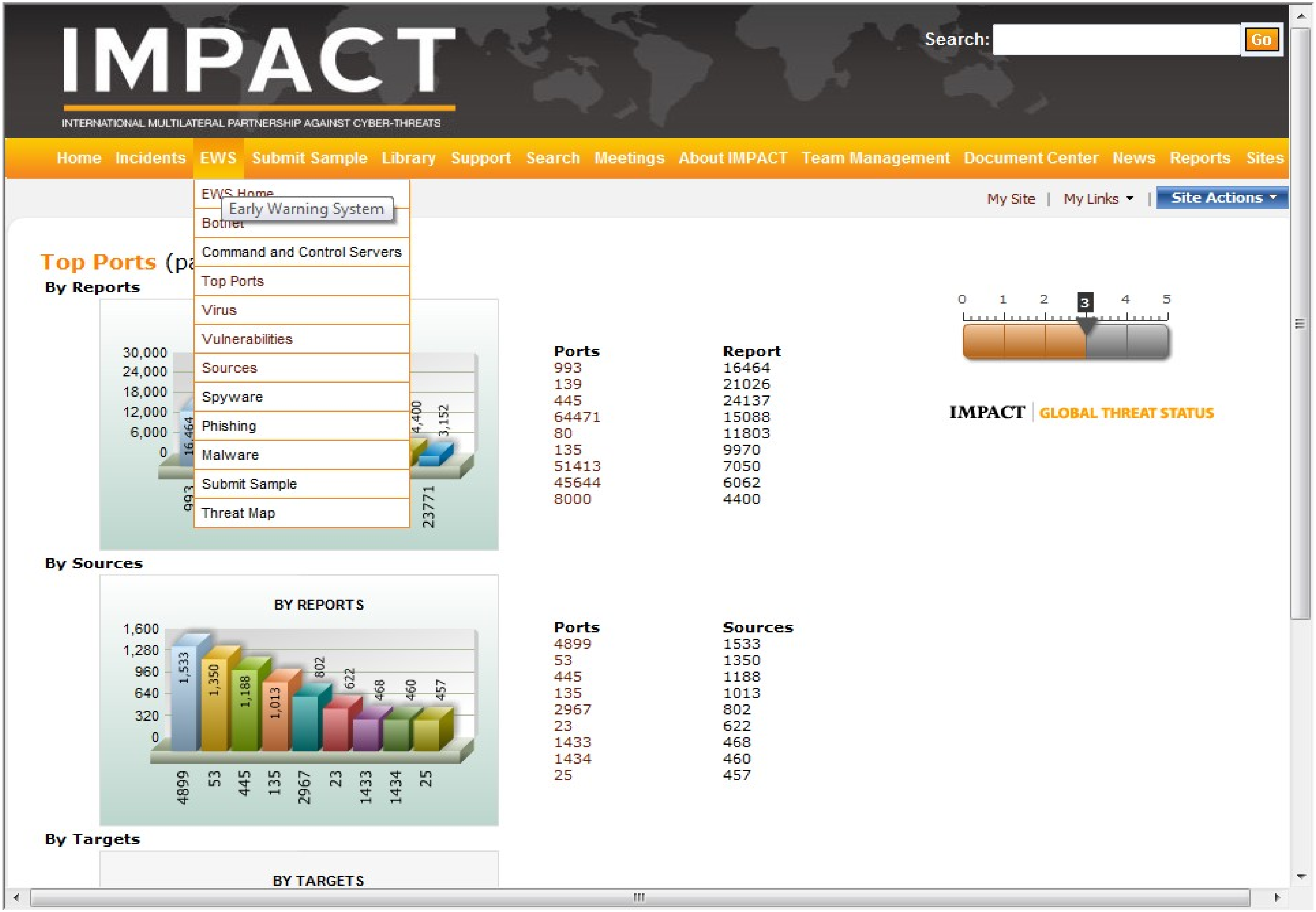
Sources

Command & Control Servers



Sources (past 24 hours)

IP : 61.139.54.94
Report : 925,306 Attacks : 145,583
CHINA (CN) (Details)



Top Ports (pa

By Reports

Ports	Report
993	16464
139	21026
445	24137
64471	15088
80	11803
135	9970
51413	7050
45644	6062
8000	4400

By Sources

Ports	Sources
4899	1533
53	1350
445	1188
135	1013
2967	802
23	622
1433	468
1434	460
25	457

By Targets

IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

IMPACT - "CIRT *LITE*"

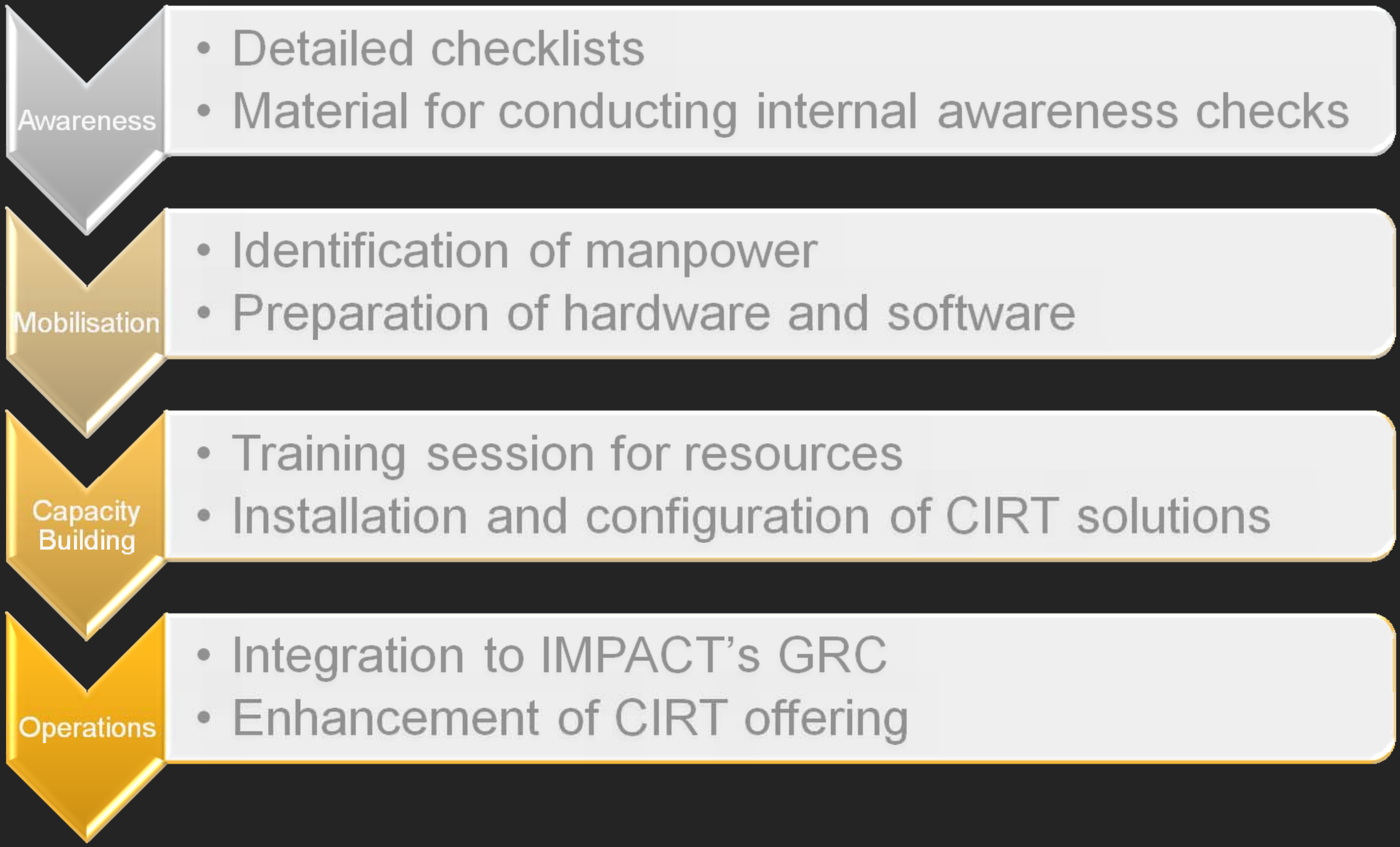
Basic setup framework

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

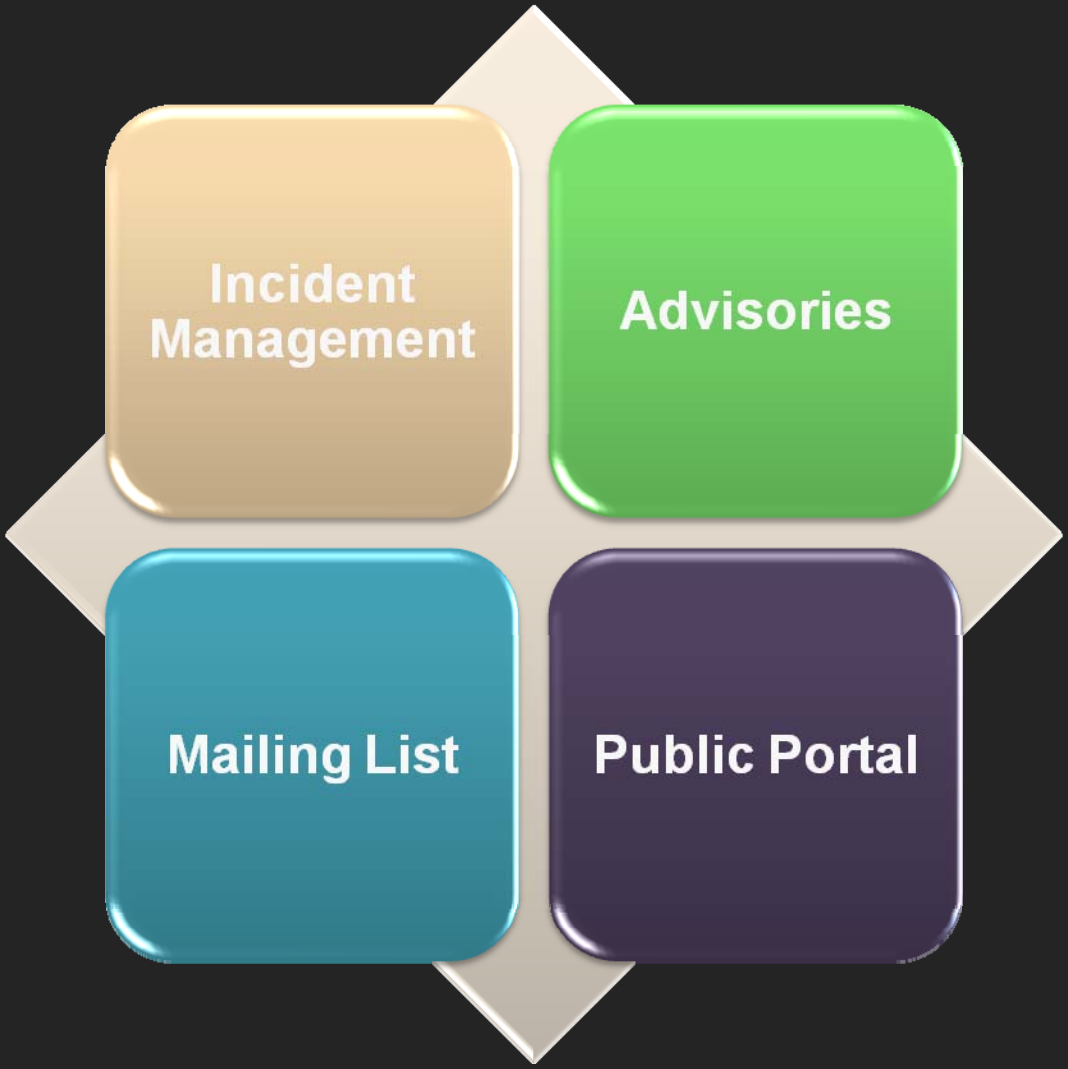
Capacity Building

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

Operations

- Integration to IMPACT’s GRC
- Enhancement of CIRT offering

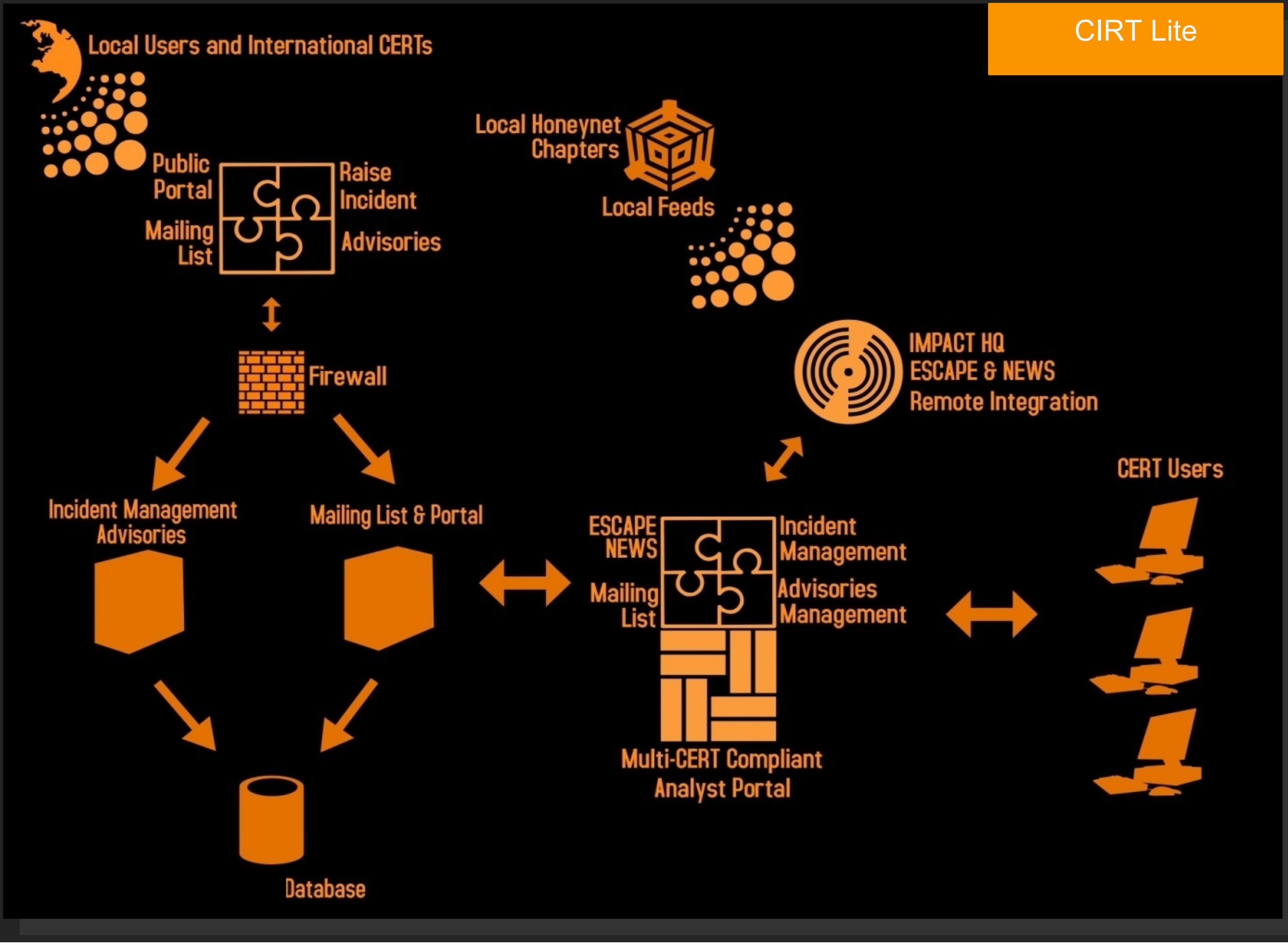
Technical components of CIRT Lite



<u>Optional</u>:

- 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

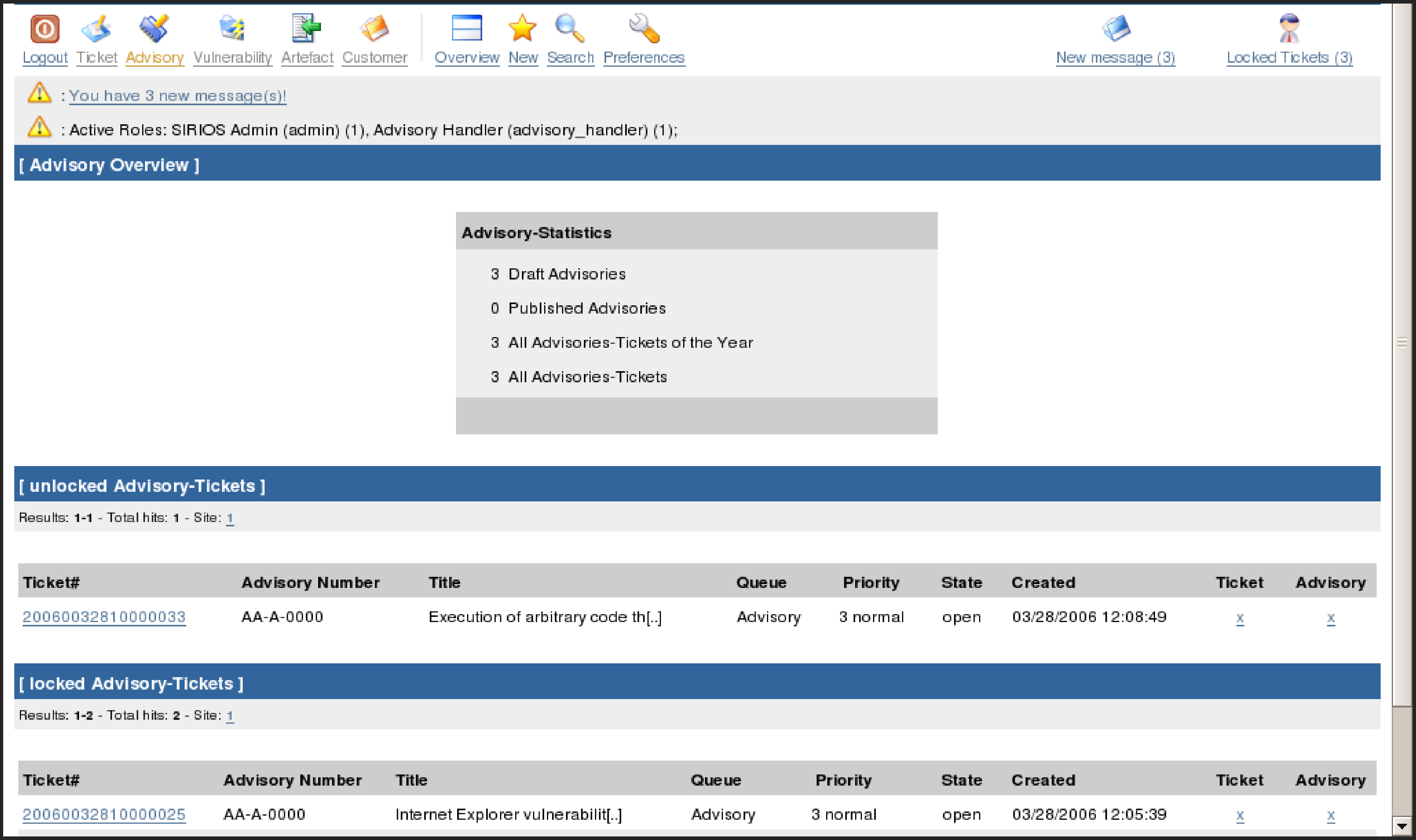
- Authoring and publishing system for advisories
- Databases for vulnerability information and artifacts

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



⚠ : You have 3 new message(s)!

⚠ : Active Roles: SIRIOS Admin (admin) (1), Advisory Handler (advisory_handler) (1);

[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

Ticket#	Advisory Number	Title	Queue	Priority	State	Created	Ticket	Advisory
20060032810000033	AA-A-0000	Execution of arbitrary code th[..]	Advisory	3 normal	open	03/28/2006 12:08:49	x	x

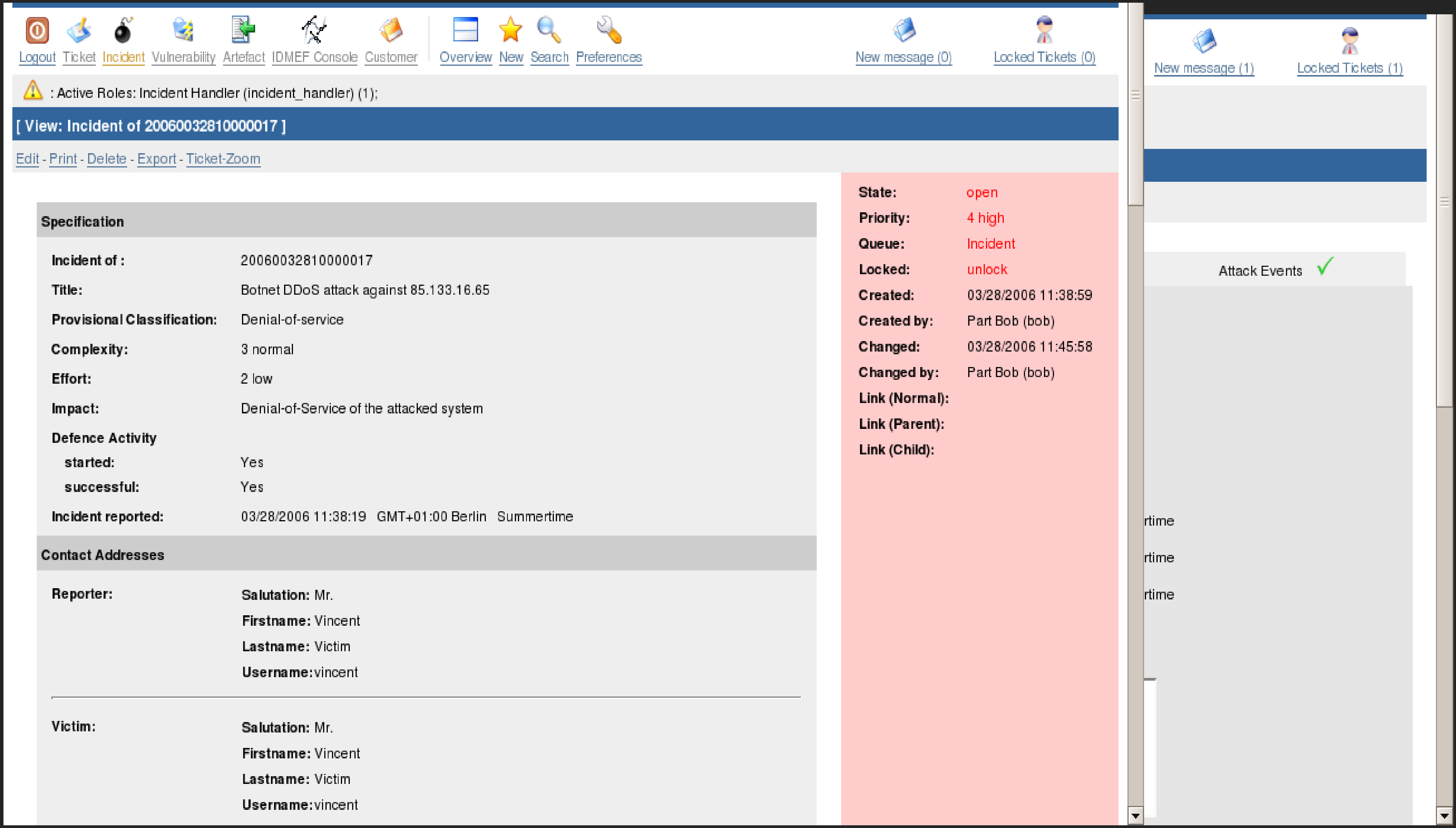
[locked Advisory-Tickets]

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

Ticket#	Advisory Number	Title	Queue	Priority	State	Created	Ticket	Advisory
20060032810000025	AA-A-0000	Internet Explorer vulnerabilit[..]	Advisory	3 normal	open	03/28/2006 12:05:39	x	x

Incident and Advisory Management

Incident view



⚠ : Active Roles: Incident Handler (incident_handler) (1);

[View: Incident of 20060032810000017]

Edit - Print - Delete - Export - Ticket-Zoom

Specification

Incident of : 20060032810000017

Title: Botnet DDoS attack against 85.133.16.65

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: 03/28/2006 11:38:19 GMT+01:00 Berlin Summertime

Contact Addresses

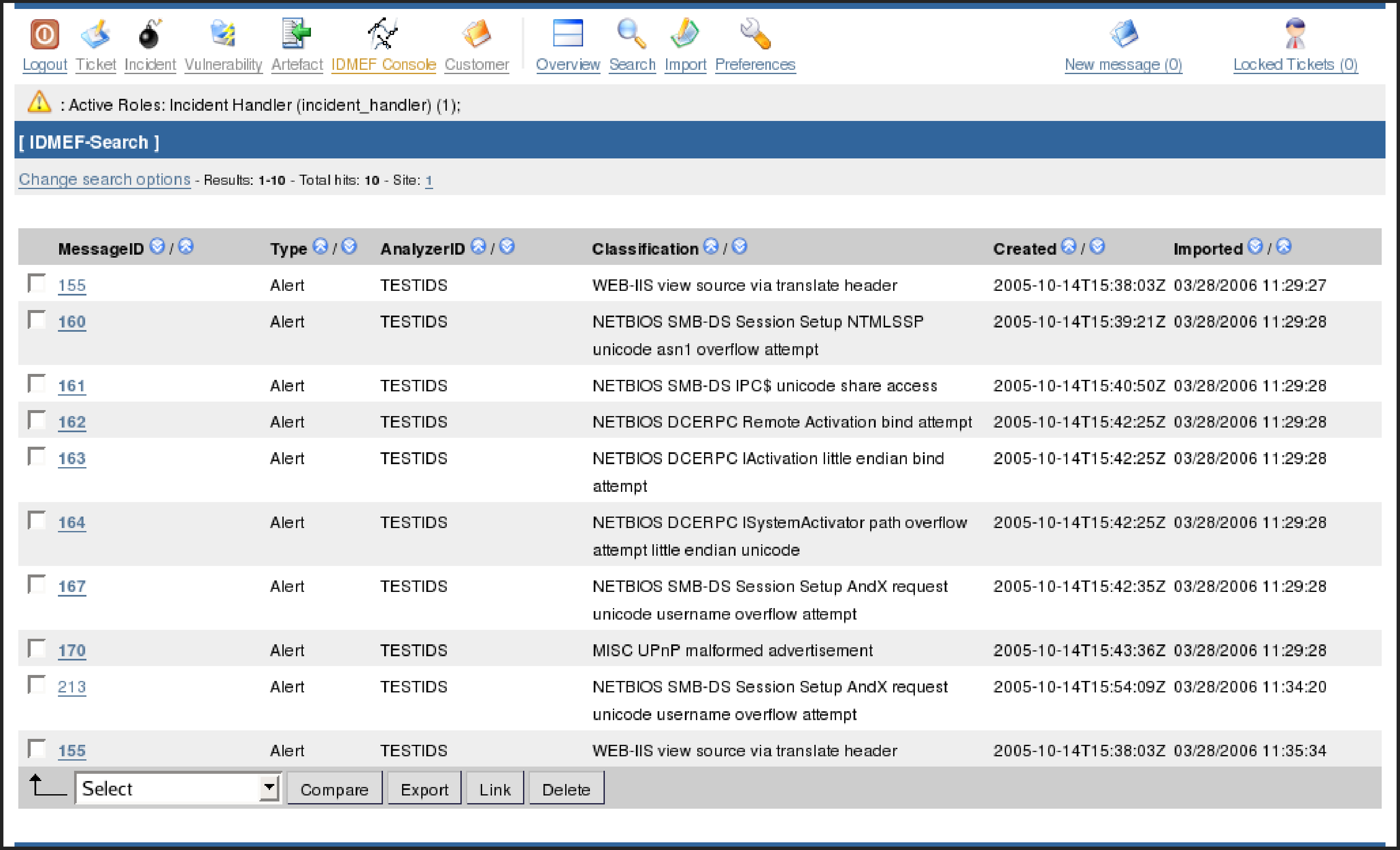
Reporter:
Salutation: Mr.
Firstname: Vincent
Lastname: Victim
Username:vincent

Victim:
Salutation: Mr.
Firstname: Vincent
Lastname: Victim
Username:vincent

State: open
Priority: 4 high
Queue: Incident
Locked: unlock
Created: 03/28/2006 11:38:59
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



: Active Roles: Incident Handler (incident_handler) (1);

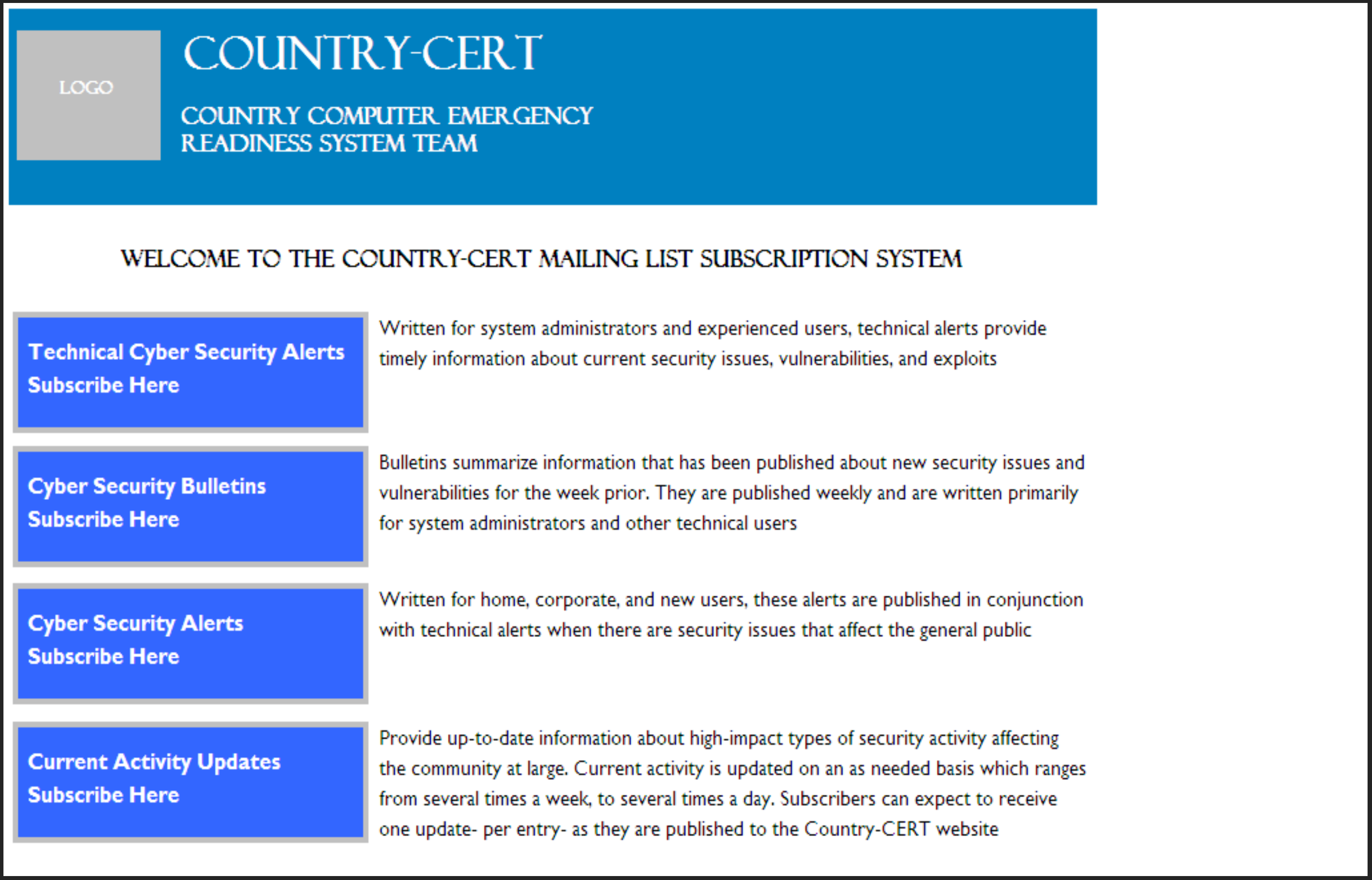
[IDMEF-Search]

Change search options - Results: **1-10** - Total hits: **10** - Site: 1

	MessageID	Type	AnalyzerID	Classification	Created	Imported
□	155	Alert	TESTIDS	WEB-IIS view source via translate header	2005-10-14T15:38:03Z	03/28/2006 11:29:27
□	160	Alert	TESTIDS	NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt	2005-10-14T15:39:21Z	03/28/2006 11:29:28
□	161	Alert	TESTIDS	NETBIOS SMB-DS IPC$ unicode share access	2005-10-14T15:40:50Z	03/28/2006 11:29:28
□	162	Alert	TESTIDS	NETBIOS DCERPC Remote Activation bind attempt	2005-10-14T15:42:25Z	03/28/2006 11:29:28
□	163	Alert	TESTIDS	NETBIOS DCERPC IActivation little endian bind attempt	2005-10-14T15:42:25Z	03/28/2006 11:29:28
□	164	Alert	TESTIDS	NETBIOS DCERPC ISystemActivator path overflow attempt little endian unicode	2005-10-14T15:42:25Z	03/28/2006 11:29:28
□	167	Alert	TESTIDS	NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt	2005-10-14T15:42:35Z	03/28/2006 11:29:28
□	170	Alert	TESTIDS	MISC UPnP malformed advertisement	2005-10-14T15:43:36Z	03/28/2006 11:29:28
□	213	Alert	TESTIDS	NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt	2005-10-14T15:54:09Z	03/28/2006 11:34:20
□	155	Alert	TESTIDS	WEB-IIS view source via translate header	2005-10-14T15:38:03Z	03/28/2006 11:35:34

CIRT-Lite - Mailing List

- Mailing List Portal



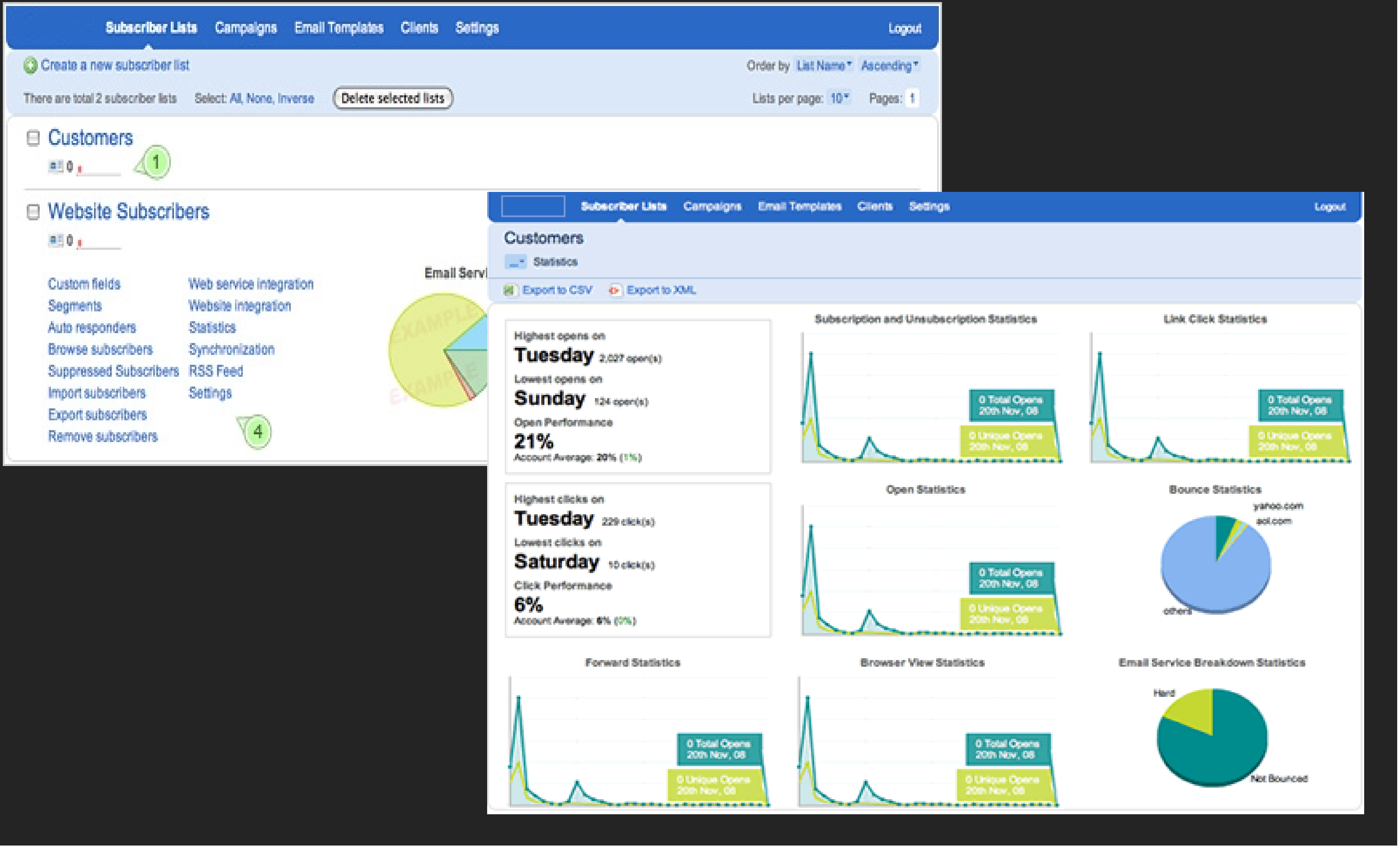
COUNTRY-CERT

COUNTRY COMPUTER EMERGENCY READINESS SYSTEM TEAM

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



There are total 2 subscriber lists   Select: All, None, Inverse

□ Customers
0

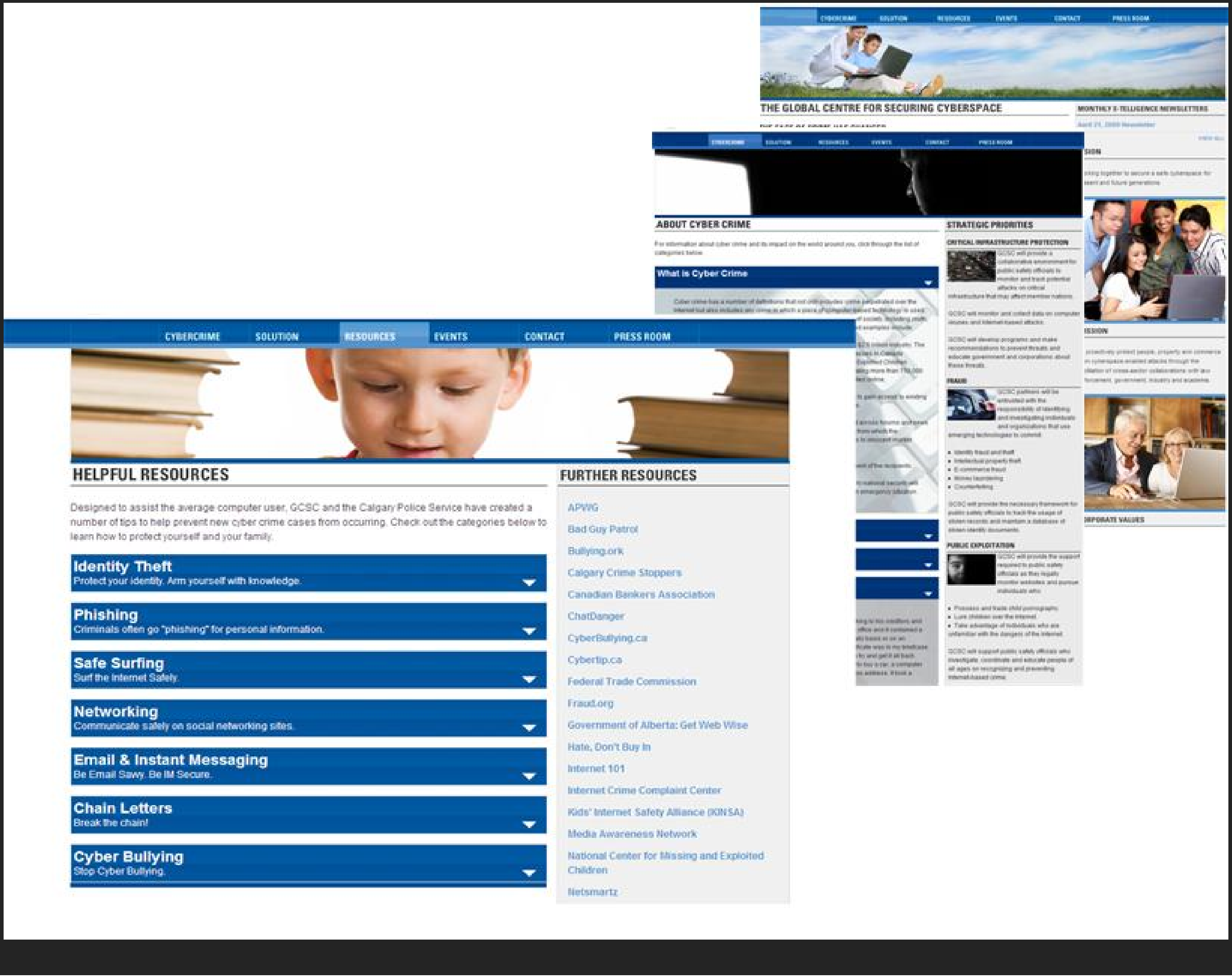
□ Website Subscribers
0

Customers

Highest opens on
Tuesday 2,027 open(s)
Lowest opens on
Sunday 124 open(s)
Open Performance
21%
Account Average: 20% (1%)

Highest clicks on
Tuesday 229 click(s)
Lowest clicks on
Saturday 10 click(s)
Click Performance
6%
Account Average: 6% (0%)

CIRT-Lite – Public Portal examples



THE GLOBAL CENTRE FOR SECURING CYBERSPACE

MONTHLY E-TELLIGENCE NEWSLETTERS

April 21, 2009 Newsletter

ABOUT CYBER CRIME

For information about cyber crime and its impact on the world around you, click through the list of categories below.

What is Cyber Crime

STRATEGIC PRIORITIES

CRITICAL INFRASTRUCTURE PROTECTION

GCSC will provide a collaborative environment for public safety officials to monitor and track potential attacks on critical infrastructure that may affect member nations.

GCSC will monitor and collect data on computer viruses and Internet-based attacks.

GCSC will develop programs and make recommendations to prevent threats and educate government and corporations about these threats.

FRAUD

GCSC partners will be entrusted with the responsibility of identifying and investigating individuals and organizations that use emerging technologies to commit:

- Identity fraud and theft
- Intellectual property theft
- E-commerce fraud
- Money laundering
- Counterfeiting

GCSC will provide the necessary framework for public safety officials to track the usage of stolen records and maintain a database of stolen identity documents.

PUBLIC EXPLOITATION

GCSC will provide the support required to public safety officials as they legally monitor websites and pursue individuals who:

- Process and trade child pornography
- Lure children over the Internet
- Take advantage of individuals who are unfamiliar with the dangers of the Internet

GCSC will support public safety officials who investigate, coordinate and educate people of all ages on recognizing and preventing Internet-based crime.

ISION

working together to secure a safe cyberspace for present and future generations.

ISSION

proactively protect people, property and commerce in cyberspace enabled attacks through the facilitation of cross-sector collaborations with law enforcement, government, industry and academia.

ORPORATE VALUES

HELPFUL RESOURCES

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

Identity 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
Be Email Savvy. Be IM Secure.

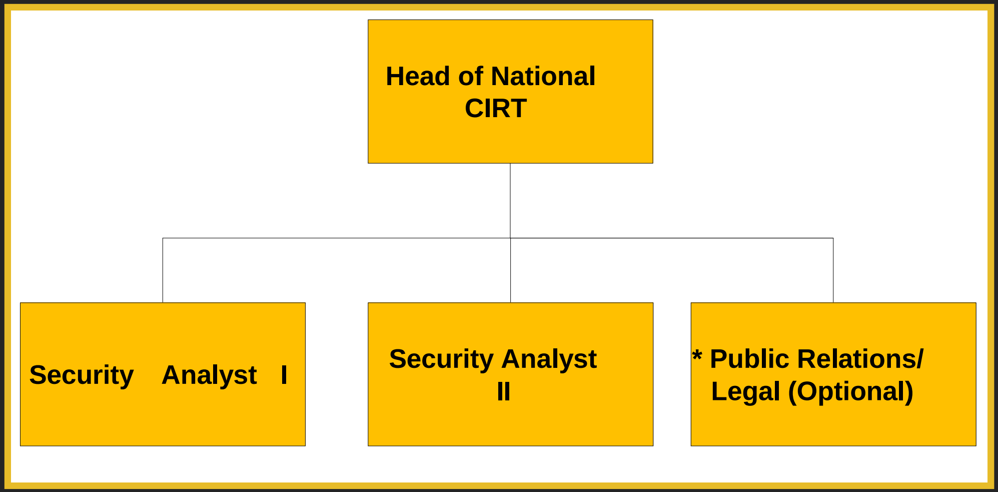
Chain Letters
Break the chain!

Cyber Bullying
Stop Cyber Bullying.

FURTHER RESOURCES

- APWG
- Bad Guy Patrol
- Bullying.ork
- Calgary Crime Stoppers
- Canadian Bankers Association
- ChatDanger
- CyberBullying.ca
- Cybertip.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 (KINSA)
- Media Awareness Network
- National Center for Missing and Exploited Children
- Netsmartz

Organisation Structure



Head of National CIRT

Security Analyst I

Security Analyst II

* Public Relations/ Legal (Optional)

***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 Categorization
- Incident Report & Handling

CIRT STAFF TRAINING

- Training will include:

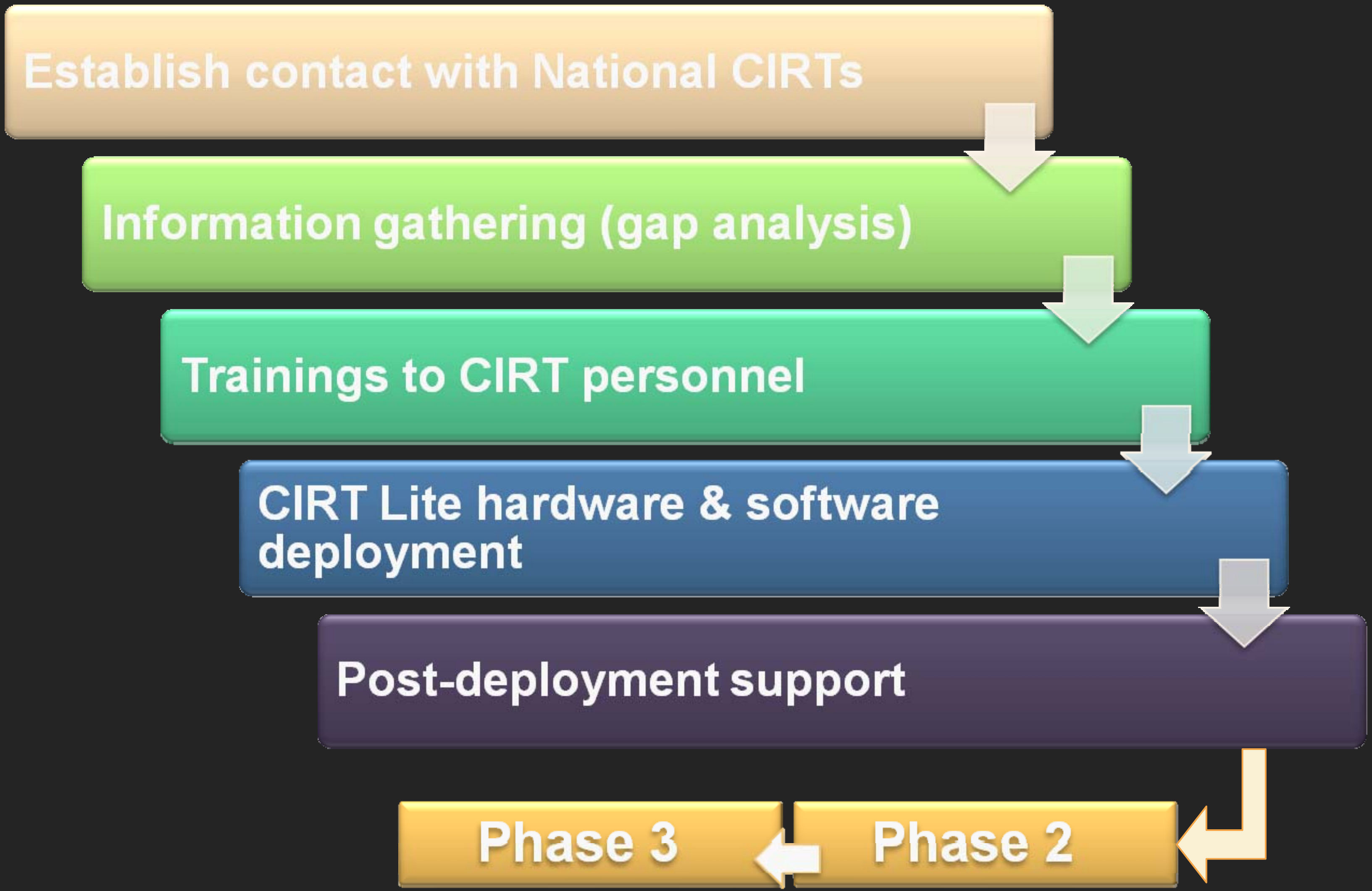
- Managing a CIRT
- Incident reporting guidelines
- Response methods
- Incident response tools
- Incident prevention methods
- Other information necessary to protect, detect, report & respond to computer security incidents

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 2

Phase 3

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

IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

E-mail : anuj.singh@impact-alliance.org