مكتب تنمية الاتصالات (BDT)

جنيف، 15 فبراير 2011

المرجع : BDT/POL/CYB/Circular-002

جهة الاتصال : سهيل مارين — الدول الأعضاء

الهاتف : +41 22 730 6057

الفاكس : +41 22 730 5484

البريد الإلكتروني : cybersecurity@itu.int

الموضوع : الاتحاد الدولي للاتصالات – إمباكت – نشر قدرات الأمن السيبراني

حضرات السادة والسيدات،

تحية طيبة وبعد،

أكتب إليكم بصفتي المدير الجديد لمكتب تنمية الاتصالات في الاتحاد الدولي للاتصالات لأبلغ إدارتكم أن مكتب تنمية الاتصالات سوف يواصل دعم الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب السيبراني (إمباكت) وأنه ملتزم بالاستمرار في مساعدة الدول الأعضاء في مجال بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.

وكما تعلمون، كان الاتحاد الدولي للاتصالات والشراكة الدولية متعددة الأطراف لمكافحة الإرهاب السيبراني (إمباكت) قد أبرما مذكرة تفاهم في عام 2008 لكي يصبح المقر العالمي لهيئة إمباكت المجهز بأحدث الوسائل في سيبرجايا بماليزيا المقر الفعلي والذراع التشغيلي لبرنامج الأمن السيبراني العالمي للاتحاد الدولي للاتصالات.

وكان لعلاقات التآزر الوثيقة بين الركائز الخمسة لبرنامج الأمن السيبراني والخدمات التي تقدمها شراكة إمباكت أن جعلت هذه الشراكة بين إمباكت والاتحاد الدولي للاتصالات خطوة حاسمة في الكفاح العالمي ضد التهديدات السيبرانية وسوء استعمال تكنولوجيا المعلومات والاتصالات وفي الوقت نفسه مساعدة الدول الأعضاء في بناء قدراتها للأمن السيبراني.

وباعتباري مدير مكتب تنمية الاتصالات فإني ألتزم بمواصلة العمل على أساس النجاحات السابقة وتنفيذ المبادرات والمشاريع الجديدة استجابة لقرارات المؤتمر العالمي لتنمية الاتصالات لعام 2010 ومؤتمر المندوبين المفوضين لعام 2010.

وقد اكتسب الاتحاد الدولي للاتصالات، من خلال قطاعاته وخاصة قطاع تنمية الاتصالات، خبرة يُعتدّ بها في تسهيل وضع استراتيجيات وطنية للأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات، ويمكن للاتحاد أن يستعين بشبكة واسعة من الهيئات الرائدة في مجال الأمن السيبراني.

ولكي يمكن القيام على وجه صحيح بمعالجة الأعمدة الخمسة لبرنامج الأمن السيبراني العالمي، وكذلك متابعة أعمال الاتحاد في مساعدة البلدان على تطوير قدراتها في مجال الأمن السيبراني، يعمل الاتحاد وإمباكت على توفير الخبرة الفنية التي تسمح للدول الأعضاء باكتشاف التهديدات السيبرانية وتحليلها والرد عليها.

وقد تم تعيين مركز الاستجابة العالمي (GRC) باعتباره منصة عالمية لنظام الإنذار المبكر ومركز الموارد الرئيسي للمجتمع العالمي من أجل التصدي للتهديدات السيبرانية، مع توفير خدمات الاستجابة للطوارئ وآليات تقاسم المعارف في بيئة تبعث على الثقة .

ويتمثل جانب لا يتجزأ من الخدمات المتص ة بمركز الاستجابة العالمي في قيام الاتحاد وإمباكت بتوفير منصة التطبيق التعاوني الآمن إلكترونياً للخبراء (ESCAPE) للدول الأعضا . وهذه المنصة هي أداة تسمح لخبراء الأمن السيبراني من مختلف البلدان بتجميع مواردهم وتقاسم خبراتهم والتعاون عن بعد في بيئة مأمو . وتمكن منصة ESCAPE مركز الاستجابة العالمي من أن يعمل كمحطة وحيدة لمركز التنسيق والاستجابة للبلدان في أوقات الأزمة ويجعل ذلك من الممكن التوصل بسرعة إلى تعيين الموارد المتاحة وتقاسمها وكذلك إدا ة الحوادث وأدوات الاستجاب . وفي الوقت الحاضر يشترك حوالي سبعين دولة عضواً في شراكة الاتحا – إمباكت ويستفيدون من مركز الاستجابة العالمي بدون مقابل .

وبالإضافة إلى ذلك تتمتع الدول الأعضاء التي تنضم إلى تحالف الاتحاد إمباكت بإمكانية تقديم طلبات للحصول على تدريب والبعثات التعليمية التي تقدمها إمباكت وشركاؤها مثل معهد إدارة النظم والمراجعة والشبكات والأمن (SANS) ومجلس الجماعة الأوروبية واتحاد نظم الإنترنت (ISC) .

وبالإضافة إلى ذلك، تقوم الحاجة إلى إنشاء هياكل تنظيمية مخصصة على الصعيد الوطني من أجل إدارة الهجمات السيبراني . ومن هذا المنظور، قام تحالف الاتحاد وإمباكت بصياغة استراتيجية لتنفيذ أفرقة استجابة وطنية للحوادث الحاسوبية (CIRT) لتكون بمثابة نقطة اتصال موثوقة للتنسيق المركزي بشأن الأمن السيبراني، وتتيح أنظمة المراقبة والتحذير وخدمات الاستجابة للحوادث . وسيتم إدماج الحل المقترح في مركز الاستجابة العالمي ويجري بالفعل تقديمه إلى البلدان وسيكون متوافقاً مع أفضل الممارسات الدولي .

وقد استكمل تحالف الاتحاد إمباكت بالفعل تقييمات لصالح 21 بلداً ويخطط مواصلة هذا الجهد مع التحرك قدماً لتسهيل التنفيذ الفعلي لأفرقة الاستجابة الوطنية للحوادث الحاسوبية مع تقديم الخبرات المطلوبة للتوصية بأفضل العتاد والبرمجيات الملائمة والمساعدة على صياغة العمليات اللازمة وبناء القدرات البشري .

وتقدم ملحقات هذه الرسالة نظرة عامة عن الخدمات التي يقدمها تحالف الاتحاد وإمباكت وكذلك الوثائق اللازمة للانضمام إلى هذا التحالف توجد عينة لخطابات الرد والملامح القطرية التي يتعين استكمالها). ويمكن الاطلاع على معلومات إضافية عن إمباكت في الموقع :

- http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html

وإذا لم يكن بلدكم قد انضم فعلاً إلى تحالف الاتحاد وإمباكت (ITU-IMPACT) وكان يرغب في المشاركة في الأنشطة المذكورة أعلاه، فيرجى الرد على هذا الخطاب مع إبراز المجال المحدد والخدمات المحددة التي تهتمون بها لصالح بلدكم .

وأرحب بكم في التحالف و تطلع إلى مدخلاتكم القيمة بشأن طريقة تحسين مساعدة الاتحاد للدول الأعضا .

وتفضلوا بقبول فائق التقدير والاحترا .

الأصل عليه توقيع

براهيما سانو
المديـــر

الملحقات :
- المذكرات التقني :
  - مركز الاستجابة العالمي
  - مركز إمباكت للتدريب وتنمية المهارات
- عينة رسالة الرد
- استمارة الملامح القطرية

نسخة إلى :
- رؤساء المكاتب الإقليمية في الاتحاد الدولي للاتصالات

Technical Note

I

GLOBAL RESPONSE CENTRE (GRC)

INTRODUCTION

GRC, as one of the key divisions of IMPACT, has evolved as the centralised threat coordination and analysis centre in collaboration with its research and operational partners. Through its extensive partnership with leading vendors from cybersecurity, academic research networks and governments, GRC provides the global community (especially the government sector) with visualisation of emerging threats, near real-time aggregated threat information and a collaboration platform for helping governments to mitigate threats through effective collaboration.

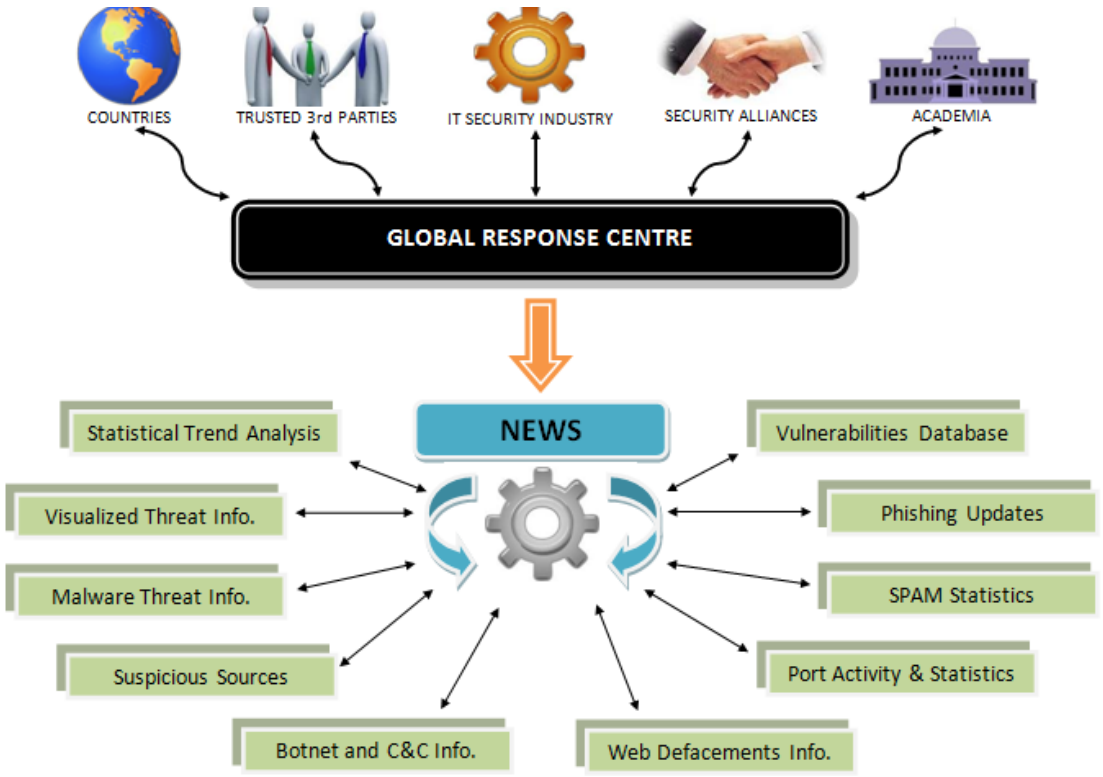
The GRC consists of the two main components offered to the ITU-IMPACT alliance members:

Network Early Warning System (NEWS) and 1

Electronically Secure Collaborative Application Platform for Experts (ESCAPE). 2

NEWS (Network Early Warning System)

GRC, through its alliances with partners like Microsoft, Symantec, Kaspersky, Trend Micro, ISC^2, SANS, F-Secure and many more, provides a well developed threat analysis, diagnosis and prioritisation scheme via NEWS. NEWS fuses data from multiple trusted sources and this aggregated data is then made available to key focal points in partner countries. This process provides the ability to rapidly distribute actionable information back to key national agencies, law enforcement agencies and trusted cybersecurity experts who can identify cyber threats at their inception and take necessary measures to prevent them.

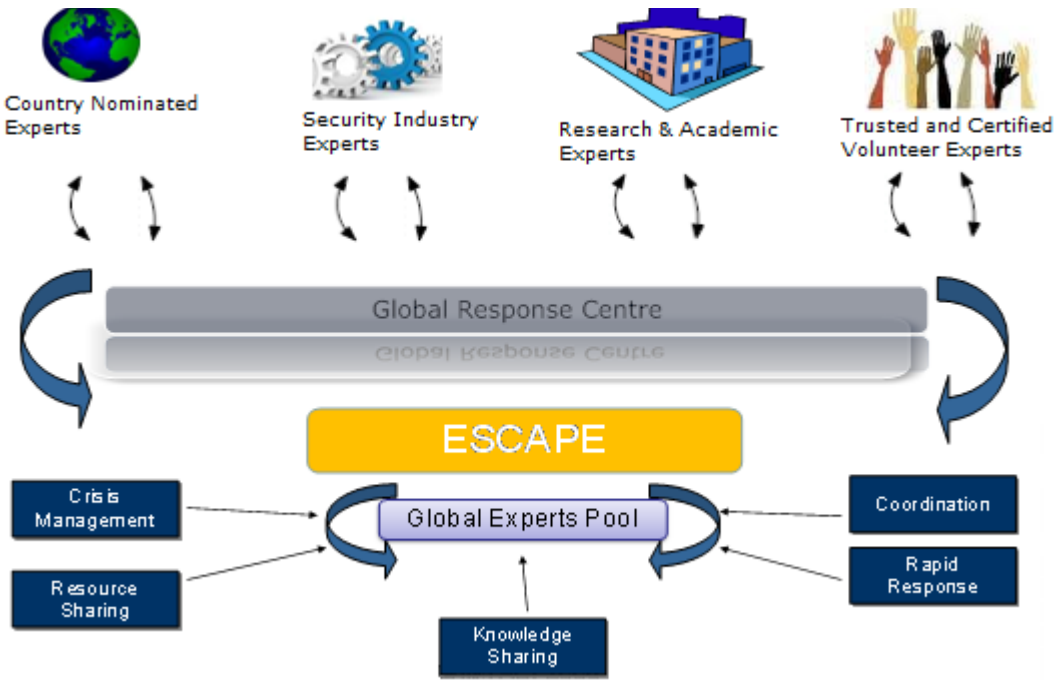


Under this system GRC provides information on different aspects of cybersecurity such as:

- Malware: recent malware discovered by vendors across the globe, the details and remediation steps.
- Suspicious Source IP's: list of suspicious source IP addresses that the community needs to be aware of, their origin and statistical information.
- Botnet: comprehensive information of botnet activities, such as where and how many C&C servers and bots are running. Details of suspicious botnet IP's are also provided.
- Spam Sources: aggregated information on spam source addresses and locations.
- Ports: that represent higher rates of involvement in suspicious activities from the attacker's side or the target end.
- Latest Vulnerabilities: discovered by vendors and other cybersecurity experts that need immediate attention and/or resolution.
- Phishing: detailed analysis and other valuable information on phished sites, domains, contents etc to stop further attacks.
- Web defacements: on the web page defacements that take place on a daily basis in the world.

ESCAPE (Electronically Secure Collaborative Application Platform For Experts)

ESCAPE is a collaboration platform that enables authorised cyber experts across different countries to collaborate with each other remotely, within a secure environment. This includes IT experts, regulators, Computer Incident Response Teams (CIRTs) and others. It consists of modules such as the Knowledge Exchange Network (KEN), Automated Threat Analysis System (ATAS), Incident Management, Blogs, Forums, security advisories etc. By converging resources and expertise from many different countries at any time, ESCAPE enables partner countries and the global community to collectively respond to cyber threats, especially during crisis or outbreaks.



These systems enable the GRC to act as a one-stop coordination and response centre for partner countries during emergencies, enabling swift identification and the sharing of available resources across borders.

Introductory Package

All member countries are provided access to the GRC's introductory package. This entitles them to have access to NEWS and ESCAPE. IMPACT's NEWS provides IMPACT members an up to the minute view of cyber threats around the world. These threats are drawn on data from dozens of public and private security feeds and are presented as a collection of easy to read charts, graphs, maps and tables. NEWS allows the members to seek the sources of attacks emerging round the globe; identify the current cyber threats and cyber security breakouts.

The introductory package also provides the member countries the ability to discover and connect with other cyber security professionals throughout the IMPACT network via ESCAPE. By applying enterprise social networking techniques to IMPACT member countries, IMPACT allows members to draw on the wealth of expertise within the IMPACT community. The introductory package provides up to five multiple logins to the ESCAPE and ability to add local cyber security experts to the IMPACT expert community. With this package the member countries can escalate their security problems to the global IMPACT experts, who provide assistance and right solutions. Furthermore, ESCAPE provides periodic security news, reports, and ability to upload a malware for inspection and analysis by the IMPACT experts.

For the introductory package IMPACT dedicates a Computer Security Incident response team member to provide assistance as and when required.

IMPACT – Introductory Package Functionality Offered

Description	***Introductory***
Global Response Centre	
• **Access to the GRC**	**From up to 2 Public IP Addresses**
• **Ability to have access to NEWS data and visualization**	√
• **Maximum number of NEWS/ESCAPE portal accounts**	**5**
• **Ability to invite local experts to the IMPACT expert community**	√
• **Ability to escalate incidents to the IMPACT expert community**	√
• **Ability to upload malware for IMPACT analysis**	√
• **Ability to receive periodic security news**	√
• **Ability to receive periodic security reports (Generic)**	√
• **Ability to subscribe to ESCAPE's content**	√
• **Minimum number of Computer Security Incident Response Team members nominated**	**3**
Training & Skill Development	
• **Training on ESCAPE**	√
• **Training on NEWS**	√

Technical Note

II

IMPACT CENTRE FOR TRAINING AND SKILLS DEVELOPMENT

As a global, non-profit organisation, IMPACT has received generous grants from leading information security training providers. These grants enable IMPACT to offer highly sought-after training courses to qualified security professionals from any one of our partner countries. Through this programme, IMPACT is able to offer various training courses courtesy of the SANS Institute and EC-Council. These organisations are widely acknowledged as the top information security certification bodies in the world and are renowned for providing exceptional high quality courses and certifications that are recognised throughout the information security community.

IMPACT-SANS Joint Programme for Improving Cyber-Security Education (ICE)

Scholarship Programme

IMPACT-SANS has jointly partnered to draw out the ICE program with the objective of creating skilled security personnel in both areas of network and application for governments around the world. This ICE program is fully sponsored by IMPACT-SANS and is open to all partner countries of IMPACT – specifically developing nations that have joined IMPACT's global agenda to address cyber-threats.

SANS security training courses will be awarded to recipients from IMPACT partner countries with the prerequisite background in security. The courses offered are aimed at developing local talents within the partner countries to instructor status, and with the knowledge obtained, the local instructors will be expected to contribute by conducting security seminars, workshops and community programs.

Prospective candidates from IMPACT partner countries are required to fill out an application form, inclusive of a letter of support from their local government representative, before being screened for eligibility. It is hoped that the awareness, training and education program provided through ICE will benefit IMPACT partner countries and at the same time, contribute to enhance cyber-space security for all.

IMPACT-EC-Council Training Scholarship Programme

IMPACT- EC-Council is offering an exclusive scholarship program to assist partner countries of IMPACT to develop more skilled, knowledgeable and certified information security professionals and practitioners. This programme is specifically designed to assist governments, businesses and academia to raise their capability and competency, to combat cyber threats and to remain resilient.

IMPACT-EC-Council provides full scholarship to qualified candidates to attend the following web-based courses:

- Network Security Administrator **(E|NSA)**
- Certified Ethical Hacker **(C|EH)**
- Computer Hacking Forensic Investigator **(C|HFI)**
- Certified Security Analyst **(E|CSA)**
- Licensed Penetration Tester **(L|PT)**
- Certified Disaster Recovery Professional **(E|DRP)**

IMPACT Training and Skills Development Programmes

IMPACT offers a full range of structured and specialised training courses that to partner countries and organisations. These courses are conducted by world class instructors with proven expertise in their particular disciplines. All IMPACT courses are designed, developed and delivered to provide clients with the necessary skills and knowledge required to understand the technologies involved and key security mission they are addressing. Due to the complexity and rapid advancement of technology, it is vital to establish high standards for development of these courses.

We believe in developing courses to enhance the knowledge and skills of IT Security developers and professionals. This would enable businesses and organisations to heighten their capabilities in managing and securing their IT infrastructures, business processes and most importantly, the people themselves. Our challenge is to ensure the knowledge and skills gained from a course are current, relevant and applicable to their job function as a security professional.

The key to success in the field of information security is to begin with a course that gives in-depth foundation in the vital areas of information security, with a view to specialised areas of cybersecurity, relevant to an individual's job function. The **IMPACT SecurityCore**, developed by IMPACT, is a prerequisite that leads to the two specialised areas of cybersecurity - **Technical** and **Management**. The participants are able to escalate their knowledge and skills by attending the specialised courses under these tracks. Other courses offered by this centre include Network Forensics and Investigation, Malware Analysis and Reverse Engineering, Securing ISP Networks & Systems and Network Investigation for Law Enforcement.

Sample Response Letter

Mr. Brahima Sanou
Director
Telecommunication Development Bureau
International Telecommunication Union
Place des Nations
CH-1211Geneva 20
Switzerland

Ref : BDT/POL/CYB Circular-002

Subject: Deployment of Cybersecurity capabilities - IMPACT Global Response Center

Dear Director,

In reference to your letter on the aforementioned subject, we would like to thank you for the opportunity given to <COUNTRY> to be involved in the ITU-IMPACT initiative.

In this regard, we are pleased to confirm our interest in joining the coalition and have the opportunity to receive concrete services and facilities within the framework of the ITU Global Cybersecurity Agenda and support the ITU Development Sector in its efforts toward achieving Cybersecurity.

In consideration for <COUNTRY> being a Partner and obtaining access to the services of the GRC and the facilities of IMPACT, <COUNTRY> is interested in the following areas:

Global Response Center (NEWS,ESCAPE)
Training and skills development
Centre for Security Assurance and Research
Centre for Policy and International Cooperation

Thank you and looking forward for our future fruitful collaboration and cooperation.

Yours sincerely,

_____

Date

_____

Submit by Email | Print Form

IMPACT COUNTRY PROFILE

1. COUNTRY DETAILS:

Country		Currency	
Capital		Timezone	
Country Code (dialling in)		International Prefix (dialling out)	
Mobile Technology		Neighbouring Countries	
International Memberships			

2. COUNTRY CYBERSECURITY FOCAL POINT:

Name					
Address					
City		State		Zip Code	
Website					
Phone		Fax			

Main Contacts:

Name	Position	Telephone	Email

Year Created		Number of Staff	
Reports To			

Responsibilities:

- ☐ ISP Licencing
- ☐ Spectrum Management
- ☐ Certification & Certifying
- ☐ Dispute Resolution
- ☐ Universal Service Provision
- ☐ Rate Regulation & Monitoring
- ☐ Enforcement
- ☐ Cybersecurity Law Maker
- ☐ Quality Monitoring
- ☐ Economic Regulation
- ☐ Technical Regulation
- ☐ Mandatory Standards
- ☐ Information Security
- ☐ Technology Roadmap
- ☐ Others:

3. COMPUTER INCIDENT RESPONSE TEAM INFORMATION (If Present):

Organization					
Address					
City		State		Zip Code	
Website					
Main Contact			Phone		
Email			Fax		

4. COUNTRY'S LAWS & LEGISLATIONS ON CYBERSECURITY:

(Briefly explain the adoption of appropriate legislation against the misuse of information and communication technologies for criminal or other purposes, including activities intended to affect the integrity of national critical infrastrucutres (CNI).)

5. SUBSCRIPTION TO IMPACT SERVICES:

We would be subscribed to the below services:

- ☐ ESCAPE
- ☐ NEWS
- ☐ GRC Mailing List
- ☐ IMPACT News Letter

6. ACCESS INFORMATION:

Public IP Address	
Name	
Telephone	
Email	

7. SIGNATORY:

I, the undersigned, have the power and authority to submit this application on behalf of my organization:

Name		Date	
Title		Signature:	