

"The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeros, little bits of data... There's a war out there... and it's not about who's got the most bullets. It's about who controls the information."

Federation of American Scientists – Intelligence Resource Program

# **Computer Emergency Response Team**

# **CERT**

## **Creation and Management**

# **INSTRUCTORS**

# Jean Robert



CEO Groupe Iservices

Partner

- ✓ Certified Ethical Hacker (CEH)
- ✓ Certified Information System Security (CISSP)
- ✓ Certified Forensic Investigation
- ✓ Certified Security Analyst

Specialist in

- ✓ Penetration Testing
- ✓ Information System Risk Assessment



# Mohammed Ibrahim



- ✓ Research Fellow, Melbourne University
- ✓ Senior Advisor – MIPT, Somalia
- ✓ .so ccTLD Manager



# Jacques Houngbo



- ✓ Certified Ethical Hacker,
- ✓ CEHEC Council Certified Security Analyst, ECSA
- ✓ Senior IT Consultant at Strategic Consulting Group



# Marcus K. G. Adomey



- ✓ Network Systems Administrator,  
University of Ghana, Legon
- ✓ Lecturer at Central University  
College, Ghana
- ✓ Member of ghCERT Creation  
Advisory Committee
- ✓ Editor in Chief AfriCERT  
Technical teaching Material



**In collaboration with JPCERT/CC**



# Suguru Yamaguchi

JPCERT **CC**®

- ✓ Board of Trustees at JPNIC / Japan Network Information Center
- ✓ Professor at Nara Institute of Science and Technology
- ✓ Board member at JPCERT/CC
- ✓ AAF Coordination Committee Member



# Koichiro Komiyama

JPCERT **CC**®

- ✓ Known as Sparky
- ✓ Software vender 4yrs ->  
JPCERT/CC -5yrs
- ✓ Watch and Warning Group ->  
Global Coordination Division

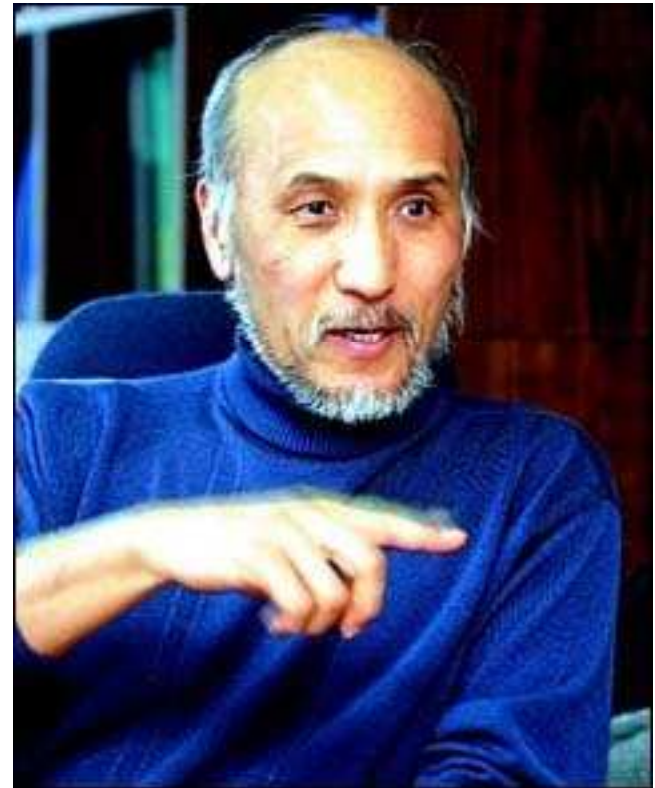


**WITH**

# Prof. Kilnam Chon



- ✓ Professor Emeritus
- ✓ Co-Chair, Africa Asia Forum on Network Research & Engineering



# Participants' Self Introduction

- **Names**
- **Country**
- **Organization**
- **What does your work involve**
- **What do you expect from this workshop?**
- **Do you have any specific issue/concern to create security team in your organization?**
- **What ever you want to share with us.**

## **Our mission is ...**

- ✓ To give you big picture of “Information Security” and “Information Security Technologies”
- ✓ To provide technical information which are required for CSIRT engineers.
- ✓ To help you understand how to start up a CSIRT of your own.

## **Our ultimate goal is ...**

- ✓ In the near future, you should creates a CSIRT in your country.

| DATE  | START | END   | TITLE  | INSTRUCTOR            |
|-------|-------|-------|--|-----------------------|
| Day 1 |       |       |  |                       |
|       | 08.45 | 09.45 | Introduction - Overview of Global Information Security | Marcus Adomey         |
|       |       |       | break  |                       |
|       | 10.00 | 12.30 | Setup and Role of CSIRT                                | Jean-Robert Hountomey |
|       |       |       | Lunch  |                       |
|       | 13.30 | 15.30 | CSIRT Services   | Jacques Hougbo        |
|       |       |       | break  |                       |
|       | 15.45 | 17.00 | Building Trust Networks                                | Mohamed Ibrahim       |
|       |       |       | Diner  |                       |

| DATE  | START | END   | TITLE   | INSTRUCTOR    |
|-------|-------|-------|---|---------------|
| Day 2 |       |       |   |               |
|       | 08:45 | 09:30 | Introduction "CSIRT philosophy and culture"       | Marcus Adomey |
|       | 09:30 | 09:45 | CSIRT operations and technology                   | Marcus Adomey |
|       | 09:45 | 10:00 | break   |               |
|       | 10:00 | 12:30 | Technical overview of Information Security        | Marcus Adomey |
|       | 12:30 | 13:30 | Lunch   |               |
|       | 13:30 | 17:30 | Technical overview of Information Security (cont) | Marcus Adomey |



| DATE  | START | END   | TITLE  | INSTRUCTOR                      |
|-------|-------|-------|--|---------------------------------|
| Day 3 |       |       | 2010/11/21   |                                 |
|       | 09:00 | 10:00 | Incident handling - Preparation                        | Jacques Hougbo                  |
|       | 10:00 | 11:00 | Practice - Making incident detection and analysis easy | Jean Robert /<br>Jacques Hougbo |
|       | 11:30 | 12:30 | Incident handling – Detection and analysis             | Jacques Hougbo                  |
|       | 12:30 | 13:00 | Practice – Profile networks and systems                | Jean Robert /<br>Jacques Hougbo |
|       | 14:00 | 15:00 | Practice – Log analysis, network traffic analysis      | Jean Robert /<br>Jacques Hougbo |
|       | 15:00 | 15:45 | Incident handling - Containment, eradication, recovery | Jacques Hougbo                  |
|       | 16:00 | 17:00 | Incident handling - Post incident activities           | Jacques Hougbo                  |

| DATE  | STAR<br>T | END   | TITLE   | INSTRUCTOR               |                 |
|-------|-----------|-------|---|--------------------------|-----------------|
| Day 4 |           |       | 2010/11/22  |                          |                 |
|       | 09:00     | 09:15 | Understanding cultures behind technology          | Mohamed Ibrahim          |                 |
|       | 09:15     | 10:15 | Information Gathering and Analysis                | Jean Robert              |                 |
|       | 10:15     | 10:30 | Break   |                          |                 |
|       | 10:30     | 12:30 | Publishing Technical Documents                    | Mohamed Ibrahim          |                 |
|       | 12:30     | 13:30 | Lunch   |                          |                 |
|       | 13:30     | 14:30 | Advanced training materials(Web)                  | Mohamed Ibrahim          |                 |
|       | 14:30     | 15:30 | Advanced training materials<br>(Malware Analysis) | Basic                    | Mohamed Ibrahim |
|       |           |       |   | Environment              | Mohamed Ibrahim |
|       |           |       |   | Runtime<br>Analysis      | Marcus Adomey   |
|       |           |       |   | Static Analysis<br>Basic | Marcus Adomey   |
|       |           |       |   | Static Analysis<br>Tools | Marcus Adomey   |
|       | 15:30     | 15:45 | break   |                          |                 |
|       | 15:45     | 17:45 | Introduction for Incident Handling Drill          | JPCERT                   |                 |

**There will be evening sessions for  
movies and discussion  
From 8.00pm – 9.30pm**

**THANK YOU!!!**