CyberSecurity Training and Capacity Building:
A Starting Point for Collaboration and Partnerships

from the most trusted name in information security

2009 ITU Regional Cybersecurity Forum for Asia-Pacific
23-25 September 2009
Hyderabad, India

Presenter:
Suresh Mustapha
Managing Director, APAC
The SANS Institute
smustapha@sans.org
About SANS

- The SANS (SysAdmin, Audit, Network, Security) Institute
  - Established in 1989
  - Cooperative research and education organization.
  - Programs now reach more than 400,000 security professionals around the world.
  - Leader in Information Security Training
    - 65,000+ alumni
    - 25,000+ certifications (GIAC)
  - At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.
Need for dedicated training and capacity building

“The cyber threat to the United States affects all aspects of society, business, and government, **but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon**, particularly within the Federal Government. [Using an] airplane analogy, we have a shortage of ‘pilots’ (and ‘ground crews’ to support them) for cyberspace.” (Center for Strategic and International Studies, Report of the Commission on Cybersecurity for the 44th Presidency, December 2008)

“The provisioning of **adequate cyber forces** to execute our assigned missions remains our greatest need.” (Gen. Kevin P. Chilton, Commander, U.S. Strategic Command, March 17, 2009, in testimony before the House Armed Services Committee)

“I cannot get the technical security people I need.” (Gen. Charles Croome, Commander, Joint Task Force - Global Network Operations, in response to a question from a CSIS Commissioner asking what is the most critical problem he faces in meeting the growing cyber challenge. May 28, 2008)

“There are **about 1,000 security people in the US** who have the specialized security skills to operate effectively in cyberspace. **We need 10,000 to 30,000.**” (Jim Gosler, Sandia Fellow, NSA Visiting Scientist, and the founding Director of the CIA’s Clandestine Information Technology Office, October 3, 2008.)
Finding the talent

The US Cyber Challenge
A new national talent search and development program: “Ten by Ten”
10,000 cyber analysts/engineers with advanced technical skills by 2010
Examples of what can be done to find talent

For high school students

- **CyberPatriot**, The High School Cyber Defense Competition conducted by the Air Force Association: a competition in computer system and network defense - where the competitors attempt to analyze the security state of the competition network and then must secure the systems while maintaining services and responding to attacks by a hostile Red Team.

For top high school students and for college and graduate students

- **The DC3 Digital Forensics Challenge** conducted by the DoD Cyber Crime Center (DC3): a competition in digital forensics where contestants attempt to uncover evidence on digital media, just like you see on all of the crime scene investigative shows on TV. Whether it is an intrusion by a nation state or a child pornography investigation, digital forensics is the key to answering the who, what, where, when, why, and how questions.

- **The Network Attack Competition conducted by the SANS Institute**: a competition in network vulnerability discovery and exploitation. This program will include substantial ethical and legal instruction. An essential tenet of the emerging US national strategy for cyber security is that offense must inform defense.

For the high school and college students in Singapore

- **The Secure Coding Competition** sponsored by the Infocom Development Authority will help identify and stream Singapore’s next generation of coding talent while conveying the elements and importance of secure coding.
Talent capacity development

Step 1: Baseline training and integration

Step 2: Select the best and most experienced for advanced training

Step 3: Provide specialized training for these elite “Cyber Guardians”

Step 4: Provide career progression for these guardians
Step 1: Baseline training and integration

- Bring up the baseline training for all individuals
- Focus training on ‘job-based, hands-on technical skills’
- Recognize that this new battlefield must include many ‘soft targets’ such as financial system, utilities, and water

Example from US Military
Step 2: Select the best and most experienced for advanced training

- Require a minimum of 5 years of experience in information security
- Outstanding performance reviews from commanders
- Recommendations from commanders and peers
- Require candidates to take the GSEC or CISSP exam and their score is another criteria to evaluate them

Example from US Military
Step 3: Provide specialized training for these elite “Cyber Guardians”

- **Establish a defense** - plan and implement the core areas of a defense: assess, prevent, detect and analyze risk
- **Manage the Perimeter** - understand, set-up, and manage the core components of an organization’s perimeter
- **Threat Identification** - identify attack vectors and how to defend against those threats
- **Vulnerability Analysis** - identify common exposure points that are often overlooked and effective ways to address vulnerabilities
- **Intrusion Analysis** - Implement effective intrusion analysis detective measures through the deployment of IDS/IPS, signatures, anomaly detection, behavior and clipping levels.
- **Defense in depth** - integrate detective measures to better support existing security components throughout the enterprise
- **Incident Response** - plan and implement an effective incident response capability for the organization

Example from US Military
Deploy Cyber Guardians as Teams

Team Leader

**Red Team**
- Windows attacker
- Linux / Unix Attacker
- Network Equipment / embedded Device Attacker
- Web Application Penetration tester
- Rapid Artifact Recovery Forensics Specialist

**Blue Team**
- Hacker Techniques and approaches
- Perimeter Protection and firewall
- Intrusion Analyst
- Incident handling
- Defending Windows
- Defending Linux / Unix
- Computer Forensics Analysis

Example from US Military

from the most trusted name in information security
Overview - Cyber Guardian ‘Q’ Course

- **1 Prerequisite course / certification**
  - SEC401 / GSEC or CISSP
- **3 Baseline courses**
  - SEC503: Intrusion Detection In-Depth
  - SEC560: Network Pen Testing & Ethical Hacking
  - SEC508: Computer Forensics, Investigation, and Response
- **Select an area of focus (Red or Blue)**
  - Select 2 of 6 specialties

Example from US Military

from the most trusted name in information security
‘Base-line’ Skills must be identified first

Cyber Guardian ‘Base-line’ Skills:
• Counter-Intelligence
• Offensive Forensics
• Offensive Data Exfiltration
• Reverse Engineering
• Network / System Evasion
• Malware Analysis
• Risk Mitigation
• Mission Planning
• Detailed Recon
• Exploiting targets
• Post-exploitation activities
• Threat Analysis

Big Question: What ‘Base-line’ CyberSecurity skills do we need to develop in the Asia-Pacific Region?
Skills need to be mapped to appropriate training
Step 4: Provide career progression for these guardians

- Develop career paths that allow for the promotion and retention of enlisted and officers
- Keep IA professionals in the IA field
- Joint partnerships with industry
- Develop a corps of ‘Cyber Minutemen’ who can be given a ‘field commission’ in the event of war

Example from US Military

from the most trusted name in information security
The 20 Coolest Jobs in Information Security

1. Information Security Crime Investigator/Forensics Expert
2. System, Network, and/or Web Penetration Tester
3. Forensic Analyst
4. Incident Responder
5. Security Architect
6. Malware Analyst
7. Network Security Engineer
8. Security Analyst
9. Computer Crime Investigator
10. CISO/ISO or Director of Security
11. Application Penetration Tester
12. Security Operations Center Analyst
13. Prosecutor Specializing in Information Security Crime
14. Technical Director and Deputy CISO
15. Intrusion Analyst
16. Vulnerability Researcher/Exploit Developer
17. Security Auditor
18. Security-savvy Software Developer
20. Disaster Recovery/Business Continuity Analyst/Manager

How to Order:
If you wish to order a copy of the brochure, please click here.
Get a free copy by attending a live SANS training event.

Know a better job?
Write us at cooljobs@sans.org
1. Job description
2. Why it’s cool
3. How it makes a difference
4. How to be successful
Where do we go from here?

Need to Answer the Big Question: What ‘Base-line” CyberSecurity skills and capacity do we need to develop in the Asia-Pacific Region?
CyberSecurity Training and Capacity Building: A Starting Point for Collaboration and Partnerships

from the most trusted name in information security

2009 ITU Regional Cybersecurity Forum for Asia-Pacific
23-25 September 2009
Hyderabad, India

Presenter:
Suresh Mustapha
Managing Director, APAC
The SANS Institute
smustapha@sans.org