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

SANS

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.**

SANS

from the most trusted name in information security

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)*

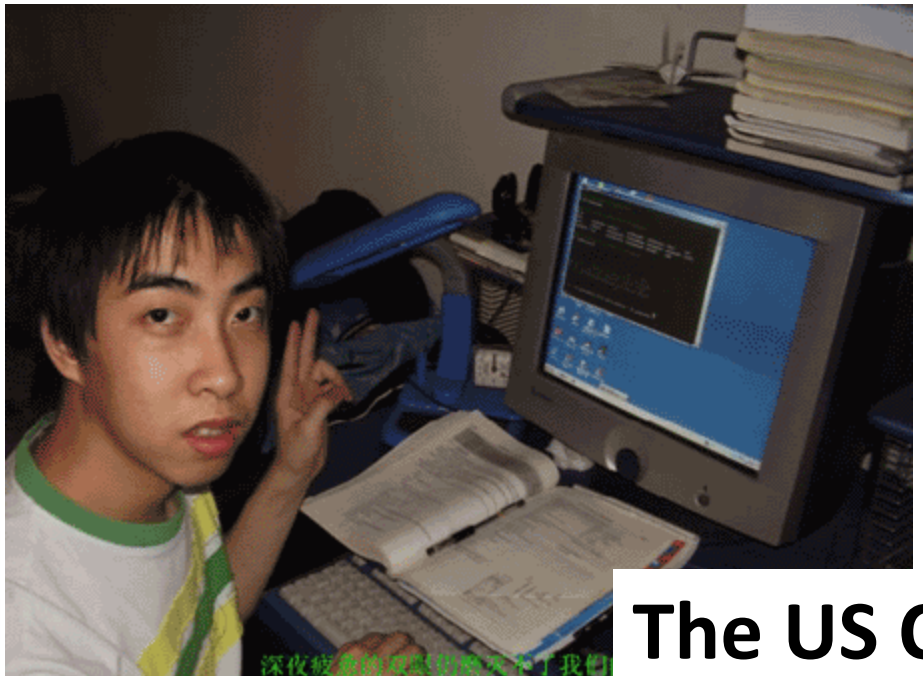
*"The provisioning of **adequate cyber forces** to execute our assigned missions remains **our greatest need**." (Gen. Kevin P. Chilton, Commander, U.S. Strategic Command, March 17, 2009, in testimony before the House Armed Services Committee)*

***"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.)*

SANS

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

SANS

from the most trusted name in information security

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 organizations 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 through out 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

Example from US Military

Blue Team

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

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

‘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?

SANS TRAINING AND YOUR CAREER ROADMAP

SECURITY CURRICULA

Incident Handling Curriculum

- SEC501 Advanced Security Essentials – Enterprise Defender GCED
- SEC504 Hacker Techniques, Exploits and Incident Handling GCIH
- SEC508 Computer Forensics, Investigation, and Response GCFA

Additional Incident Handling Courses

- SEC517: Cutting-Edge Hacking Techniques STAR
- SEC550: Advanced Information Recon STAR

Penetration Testing Curriculum

- SEC540 VoIP Security
- SEC542 Web App Pen Testing and Ethical Hacking GWAPT
- SEC560 Network Pen Testing and Ethical Hacking GPEN
- SEC617 Wireless Ethical Hacking, Pen Testing, and Defenses GAWN
- SEC709 Developing Exploits for Penetration Testers and Security Researchers

Additional Penetration Testing Courses

- DEV538: Web Application Pen Testing
- SEC553: Metasploit for Pen Testers STAR
- SEC559: Wireless Security Exposed
- SEC561: Network Penetration Testing

Beginners

- SEC301 Intro to Information Security GISF
- SEC401 SANS Security Essentials Bootcamp Style GSEC

SEC301 NOTE: *If you have experience in the field, please consider our more advanced course – SEC401.*

Network and Application Security Curriculum

- SEC501 Advanced Security Essentials – Enterprise Defender GCED

Additional Network and Application Security Courses

- SEC334: SANS Training for the CompTIA Security+ Certification
- SEC440: 20 Critical Security Controls
- SEC535: Network Security Projects Using Hacked Wireless Routers
- SEC556: Comprehensive Packet Analysis STAR

Intrusion Analysis Curriculum

- SEC501 Advanced Security Essentials – Enterprise Defender GCED
- SEC502 Perimeter Protection In-Depth GCFW
- SEC503 Intrusion Detection In-Depth GCIA

Additional Intrusion Analysis Courses

- SEC352: Protecting Your Personal Privacy on the Internet
- SEC557: Virtualization Security and Operations

System Administration Curriculum

- SEC501 Advanced Security Essentials – Enterprise Defender GCED
- SEC505 Securing Windows GCWN
- SEC506 Securing Unix/Linux GCUX

Additional System Administration Courses

- SEC351: Computer and Network Security Awareness STAR
- SEC434: Log Management In-Depth
- SEC441: Windows Forensics
- SEC509: Securing Oracle GSOC
- SEC531: Windows Command-Line Kung Fu STAR
- SEC546: IPv6 Essentials
- SEC564: Security Architecture for Sys Admins

Forensics Curriculum

- SEC408 Computer Forensic and E-discovery Essentials
- SEC508 Computer Forensics, Investigation, and Response GCFA
- SEC558 Network Forensics
- SEC563 Mobile Device Forensics
- SEC606 Drive and Data Recovery Forensics
- SEC610 REM: Malware Analysis Tools & Techniques GREM

Additional Forensics Courses

- SEC526: Advanced Filesystem Recovery & Memory Forensics STAR

APPLICATION SECURITY CURRICULA

Web App Security Curriculum

- DEV319 Intro to Web Application Security STAR
- DEV422 Defending Web Applications Security Essentials

DEV319 NOTE: *If you have experience in the field, please consider our more advanced course – DEV422.*

Web App Pen Testing Curriculum

- SEC542 Web App Pen Testing and Ethical Hacking GWAPT

Additional Web App Pen Testing Courses

- SEC538: Web App Pen Testing

Secure Coding Curriculum

- DEV541 Java/JEE – Secure Coding GSSP-JAVA
- DEV544 .NET – Secure Coding GSSP-.NET
- DEV545 PHP – Secure Coding
- DEV548 C – Secure Coding GSSP-C

Additional Secure Coding Courses

- DEV304: Software Security Awareness
- DEV320: Introduction to the Microsoft Security Development Lifecycle
- DEV534: Secure Code Review for Java Web Apps
- DEV536: Secure Coding for PCI Compliance
- AUD428: Java Quality Assurance, Security Testing and Auditing

AUDIT CURRICULUM

- SEC301 Intro to Information Security GISF
- SEC401 SANS Security Essentials Bootcamp Style GSEC
- AUD410 IT Security Audit & Control Essentials
- AUD507 Auditing Networks, Perimeters & Systems GSNA

Additional Audit Courses

- AUD423: Training for the ISACA® CISA® Cert Exam
- AUD428: Java Quality Assurance, Security Testing & Auditing
- AUD429: IT Security Audit Essentials Bootcamp
- AUD439: Auditing OCTAVE
- SEC440: 20 Critical Security Controls
- AUD521: PCI/DSS 1.2: Becoming and Staying Compliant STAR

LEGAL CURRICULUM

- SEC301 Intro to Information Security GISF
- SEC401 SANS Security Essentials Bootcamp Style GSEC
- LEG523 Legal Issues in Information Technology and Information Security GLEG

Additional Legi…

- LEG412: C…
- LEG413…
- LEG416: S…
- LEG417: Legal… Technology…
- LEG425: Applying Law to … Dangers

MANAGEMENT CURRICULUM

- SEC301 Intro to Information Security GISF
- SEC401 SANS Security Essentials Bootcamp Style GSEC
- MGT512 SANS Security Leadership Essentials For Managers with Knowledge Compression™
- MGT414 SANS® +S™ Training Program for the CISSP® Certification Exam GISP
- MGT525 Project Management and Effective Communications for Security Professionals and Managers GCPM

Skills need to be mapped to appropriate training

GIAC

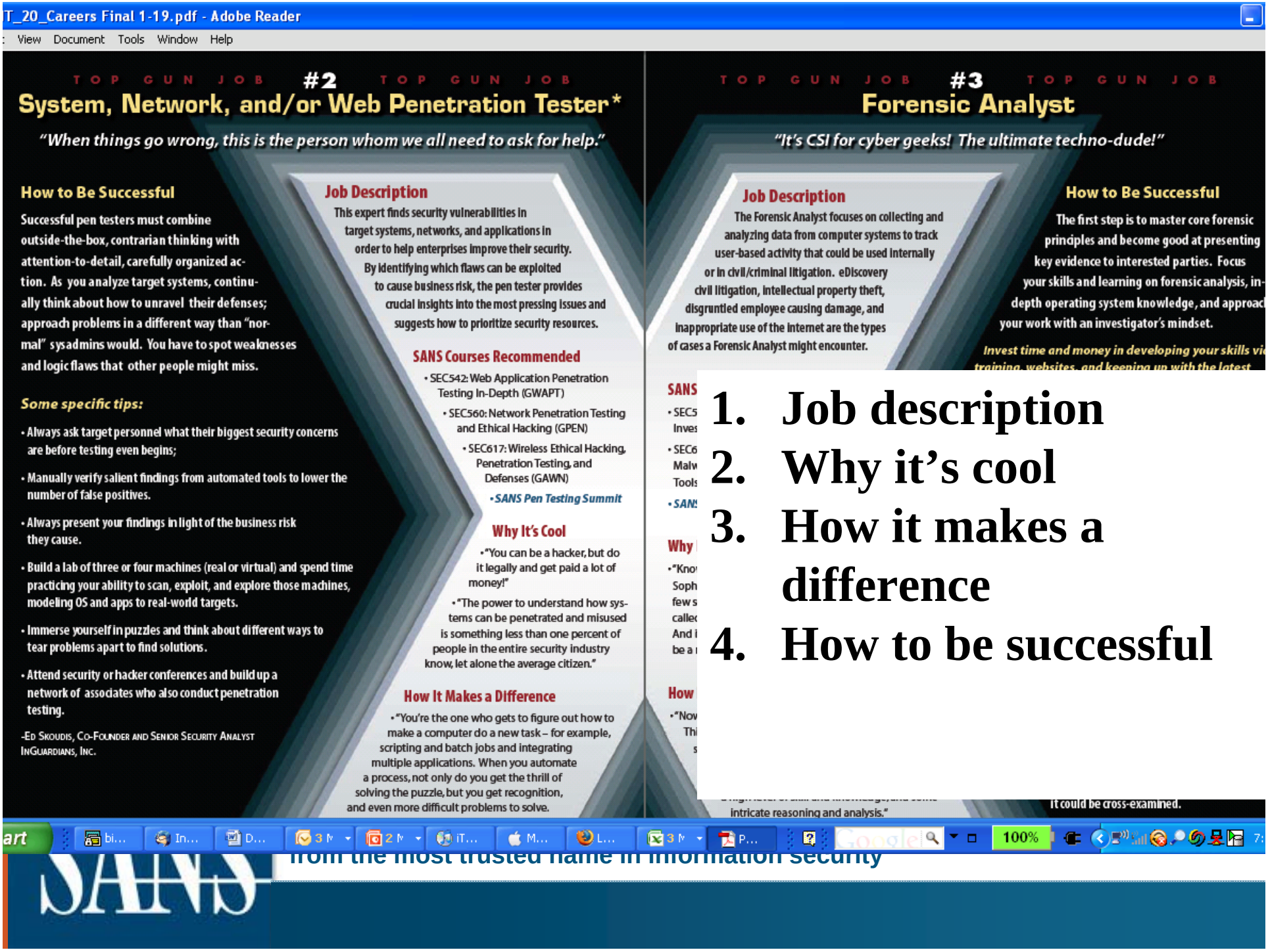
Click here to learn more about GIAC Certifications.

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

20 Coolest Jobs in INFOSEC


T_20_Careers Final 1-19.pdf - Adobe Reader
View Document Tools Window Help
TOP GUN JOB #2 TOP GUN JOB
System, Network, and/or Web Penetration Tester*
"When things go wrong, this is the person whom we all need to ask for help."
How to Be Successful
Successful pen testers must combine outside-the-box, contrarian thinking with attention-to-detail, carefully organized action. As you analyze target systems, continually think about how to unravel their defenses; approach problems in a different way than "normal" sysadmins would. You have to spot weaknesses and logic flaws that other people might miss.
Some specific tips:
• Always ask target personnel what their biggest security concerns are before testing even begins;
• Manually verify salient findings from automated tools to lower the number of false positives.
• Always present your findings in light of the business risk they cause.
• Build a lab of three or four machines (real or virtual) and spend time practicing your ability to scan, exploit, and explore those machines, modeling OS and apps to real-world targets.
• Immerse yourself in puzzles and think about different ways to tear problems apart to find solutions.
• Attend security or hacker conferences and build up a network of associates who also conduct penetration testing.
-Ed Skoudis, Co-Founder and Senior Security Analyst InGuardians, Inc.
Job Description
This expert finds security vulnerabilities in target systems, networks, and applications in order to help enterprises improve their security. By identifying which flaws can be exploited to cause business risk, the pen tester provides crucial insights into the most pressing issues and suggests how to prioritize security resources.
SANS Courses Recommended
• SEC542: Web Application Penetration Testing In-Depth (GWAPT)
• SEC560: Network Penetration Testing and Ethical Hacking (GPEN)
• SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)
• SANS Pen Testing Summit
Why It's Cool
• "You can be a hacker, but do it legally and get paid a lot of money!"
• "The power to understand how systems can be penetrated and misused is something less than one percent of people in the entire security industry know, let alone the average citizen."
How It Makes a Difference
• "You're the one who gets to figure out how to make a computer do a new task – for example, scripting and batch jobs and integrating multiple applications. When you automate a process, not only do you get the thrill of solving the puzzle, but you get recognition, and even more difficult problems to solve.
TOP GUN JOB #3 TOP GUN JOB
Forensic Analyst
"It's CSI for cyber geeks! The ultimate techno-dude!"
Job Description
The Forensic Analyst focuses on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation. eDiscovery civil litigation, intellectual property theft, disgruntled employee causing damage, and inappropriate use of the Internet are the types of cases a Forensic Analyst might encounter.
How to Be Successful
The first step is to master core forensic principles and become good at presenting key evidence to interested parties. Focus your skills and learning on forensic analysis, in-depth operating system knowledge, and approach your work with an investigator's mindset.
Invest time and money in developing your skills via training, websites, and keeping up with the latest
1. Job description
2. Why it's cool
3. How it makes a difference
4. How to be successful
intricate reasoning and analysis."
it could be cross-examined.
100%
SANS
from the most trusted name in information security

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

SANS

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