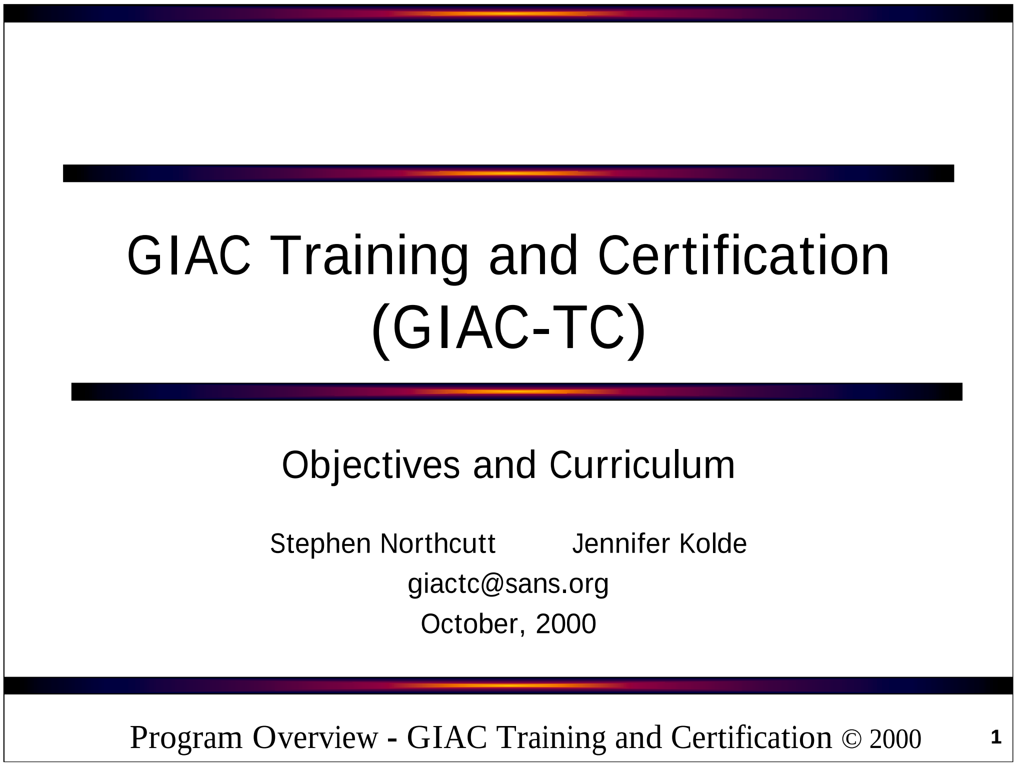


GIAC Training and Certification (GIAC-TC)

Objectives and Curriculum

Stephen Northcutt Jennifer Kolde
giactc@sans.org

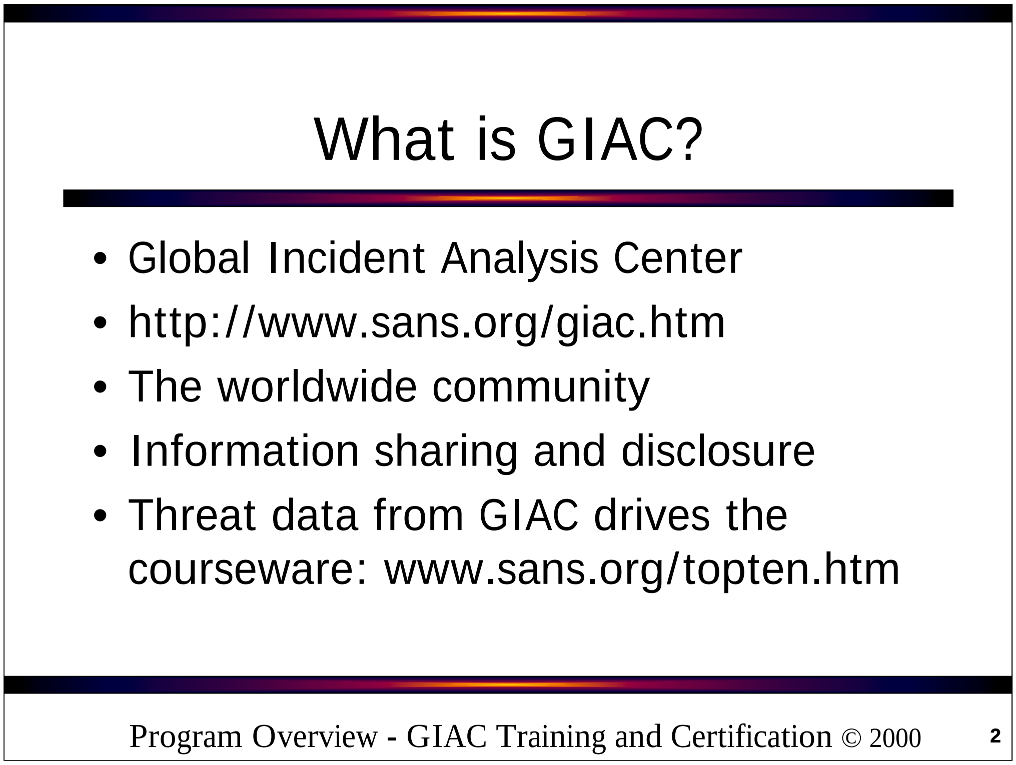
October, 2000

Hello, my name is Stephen Northcutt and I am the director of SANS' Global Incident Analysis Center (GIAC). For the past year, a large number – in fact over 200 – system, network, and security administrators from large and small organizations have helped to create GIAC Training and Certification (GIAC-TC).

The training is built and we are already turning out combat-ready security practitioners, but we haven't written the marketing pitches yet. I never realized that marketing was important, but it turns out that if you field a product and it is exciting and people want it, then they have lots of questions! That is the reason I am writing this infomercial, to explain:

- what GIAC training is;
- what it costs;
- where to get it.

If you have a few minutes to think about your career, sit back, relax and let's talk about GIAC-TC.



What is GIAC?

- Global Incident Analysis Center
- http://www.sans.org/giac.htm
- The worldwide community
- Information sharing and disclosure
- Threat data from GIAC drives the courseware: www.sans.org/topten.htm

Program Overview - GIAC Training and Certification © 2000 2

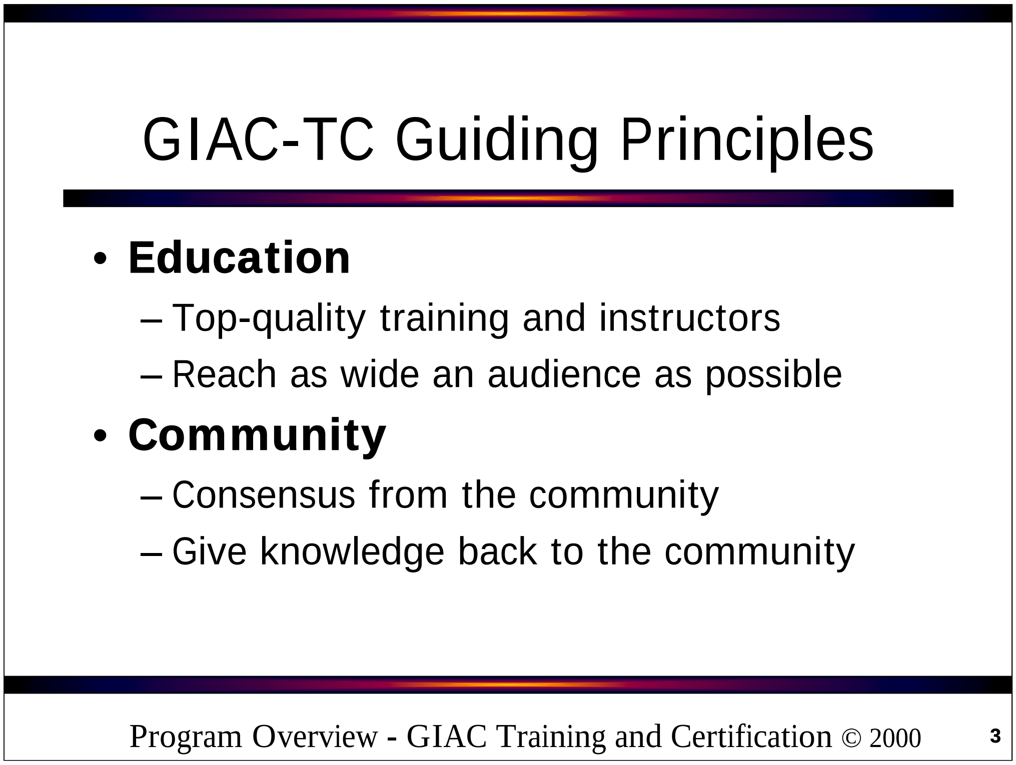
GIAC started in late 1999 as a task force to help monitor computer activity during the Y2K rollover. Since then, it has continued to act as a public clearinghouse for network detects and suspicious activity. To quote from the GIAC Mission Statement:

“The Global Incident Analysis Center (GIAC) is an information sharing forum open to every country and community on the planet. GIAC will provide rapid and full disclosure of attack patterns and analysis, including draft analysis to give the network and systems defender the information they need to do the job.”

Thanks to hundreds of alert system and security administrators worldwide who contribute and share information, GIAC is able to collate detects from numerous sources to provide information and analysis of current attacks and attack patterns. This information, combined with additional research and white papers, makes GIAC a key resource for security information.

We try to be the best – in fact, we really **are** the best at finding and quickly analyzing and reporting new attacks, and by far – but being the best is not enough, not even close. This is perhaps the bombshell moment of this infomercial: intrusion detection, incident handling, malicious code – these are all in their infancy. Anti-virus software can detect tens of thousands of signatures; intrusion detection can detect mere hundreds of signatures. This difference is significant! There are no fully-developed tools available to do the job – it must be done by **people.**

This is where you come in. You have a part to play. GIAC cannot reach its potential without you. **The only way we are going to make a difference is to harness the collective intelligence of the community.**



GIAC-TC Guiding Principles

- **Education**
  - Top-quality training and instructors
  - Reach as wide an audience as possible
- **Community**
  - Consensus from the community
  - Give knowledge back to the community

Program Overview - GIAC Training and Certification © 2000 3

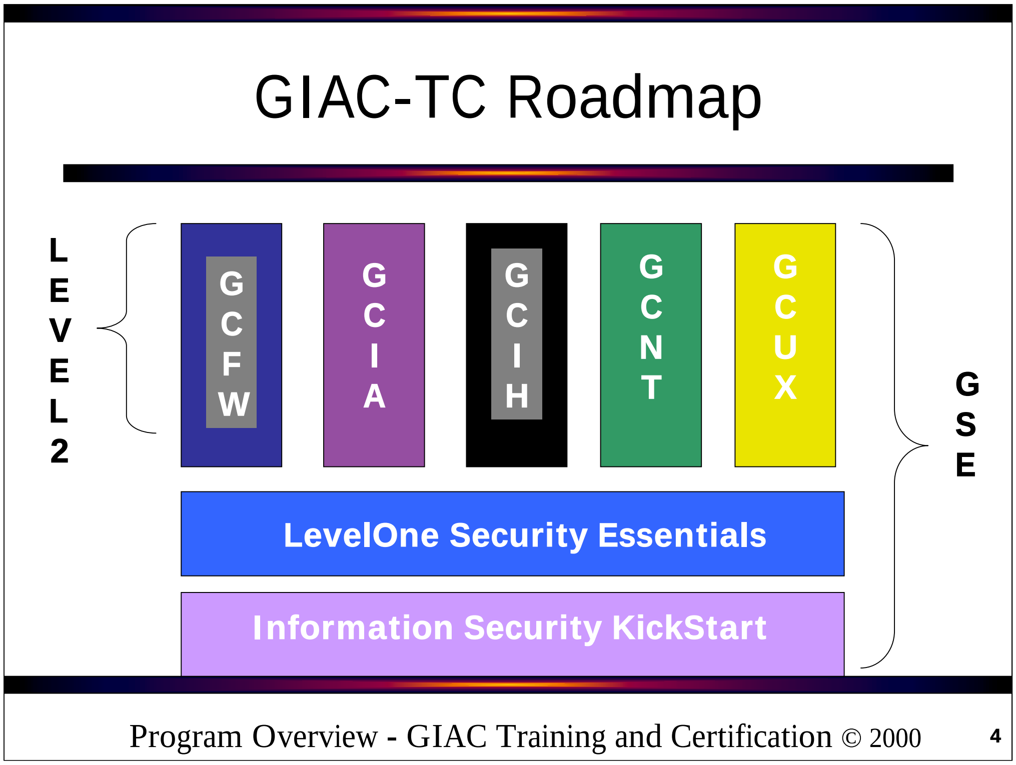
Education and **Community** are the guiding principles of SANS, of GIAC, and of GIAC-TC.

SANS' goal for a number of years has been to provide the best technical training, delivered by the best instructors. In this, we have a proven track record. Many of the core SANS courses now form the basis of the GIAC-TC program.

In the past, our efforts have focused on "live" classroom training at conferences. While this provides an excellent educational forum, it limits us in both time (how often we can offer courses) and space (seating limitations). In addition to ongoing classroom training, we are now expanding our program to offer the GIAC-TC courses over the Internet via the World Wide Web. This will allow students to take SANS GIAC training any time, from anywhere in the world.

In addition, GIAC-TC has a very strong **community focus.** One of GIAC-TC's primary goals is to continually **advance the defensive state of practice of information security.** We do this not only through education, but also by sharing our research with others so that they too can continue to learn.

- Community consensus drives our curriculum and shapes the future direction of the program.
- Public disclosure on our web site – through GIAC, through consensus documents, through the research of GIAC graduates – provides free public information and education.



GIAC-TC Roadmap

LEVEL 2

GCFW

GCIA

GCIH

GCNT

GCUX

GSE

LevelOne Security Essentials

Information Security KickStart

Program Overview - GIAC Training and Certification © 2000 4

You may go as far as you like in the GIAC program. All GIAC courses require both “book learning” and hands-on practice.

The ‘foundation’ course is Information Security KickStart.

LevelOne Security Essentials builds on the basic knowledge established in KickStart and introduces more technical concepts and practices that are essential to understanding LevelTwo material.

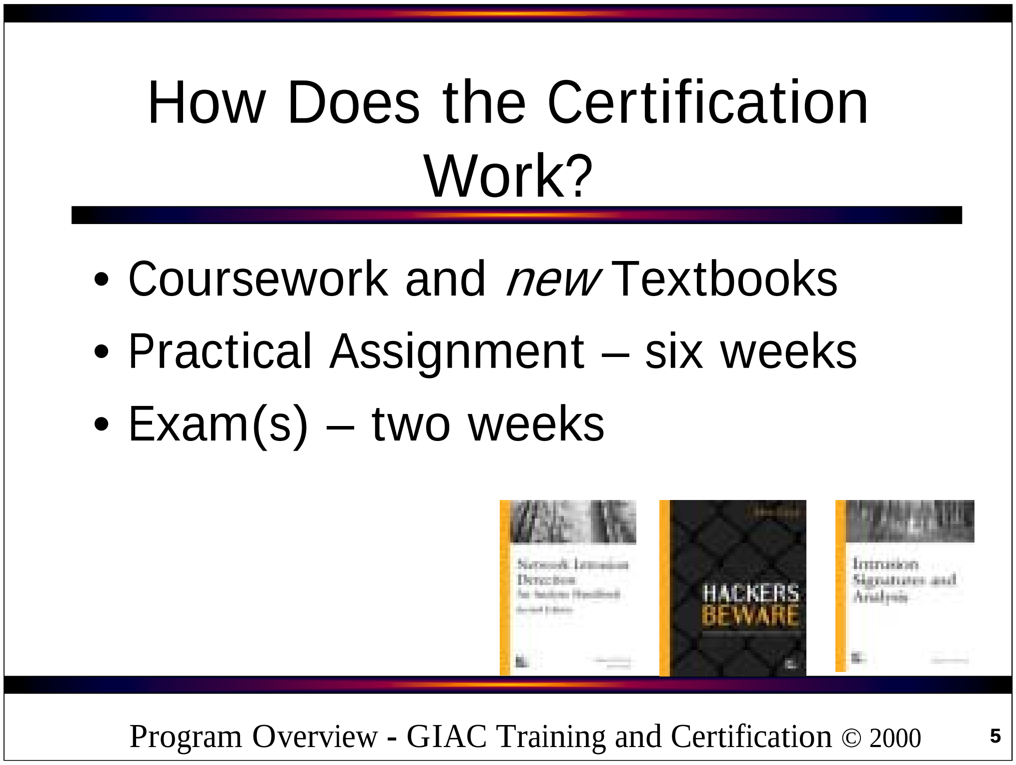
The LevelTwo Subject Area Modules provide in-depth technical training focused on specific security tasks. There are currently five LevelTwo modules:

- Firewalls, Perimeter Protection, and VPNs (GCFW)
- Intrusion Detection in Depth (GCIA)
- Advanced Incident Handling and Hacker Exploits (GCIH)
- Securing Windows (GCNT)
- Securing Unix (GCUX)

Students who:

- complete and maintain certification in all areas; and
- receive either a 90 or above on an exam or an “honors” rating on their practical in at least one LevelTwo certification

are eligible to sit for the GIAC Security Engineer (GSE) certification.



How Does the Certification Work?

- Coursework and *new* Textbooks
- Practical Assignment – six weeks
- Exam(s) – two weeks

Network Intrusion Detection
An Analyst's Handbook
Second Edition
HACKERS BEWARE
Intrusion Signatures and Analysis

Program Overview - GIAC Training and Certification © 2000 5

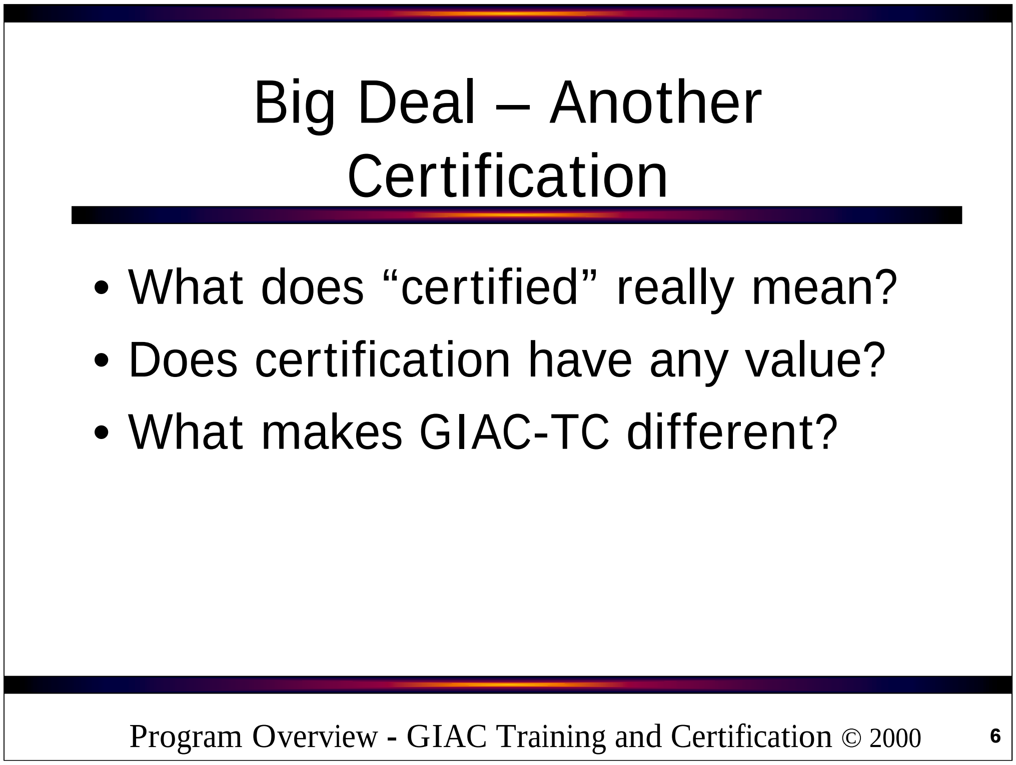
The path to GIAC certification consists of the following:

- **Course work,** presented either in a class or online. Courses are typically three to six days at a conference, or an equivalent number of hours online (i.e., a three day conference course would be roughly equivalent to 18 hours of online training).

- **Practical assignment.** This is a written project that is designed to demonstrate not only that you have learned the material, but that you can successfully take what you have learned and apply it to real-world situations. The practical is due six weeks from the date you begin the certification process.

- **One or more exams** (depending on the specific course). Once your practical has been approved, you are eligible to take the exam(s). Exams are designed to test your mastery of the course material. Exams are multiple choice and must be completed within a given time limit (generally two hours). The exams are administered online and can be taken from any computer with Internet access – you do not have to schedule exams in advance or visit a test center. Exams must be completed no later than two weeks from the practical deadline.

Currently, the GIAC certification is available to students who take SANS GIAC courses at a conference or take them online. Starting in 2001, the certifications will be available to anyone who wishes to take them, independent of SANS GIAC courses.



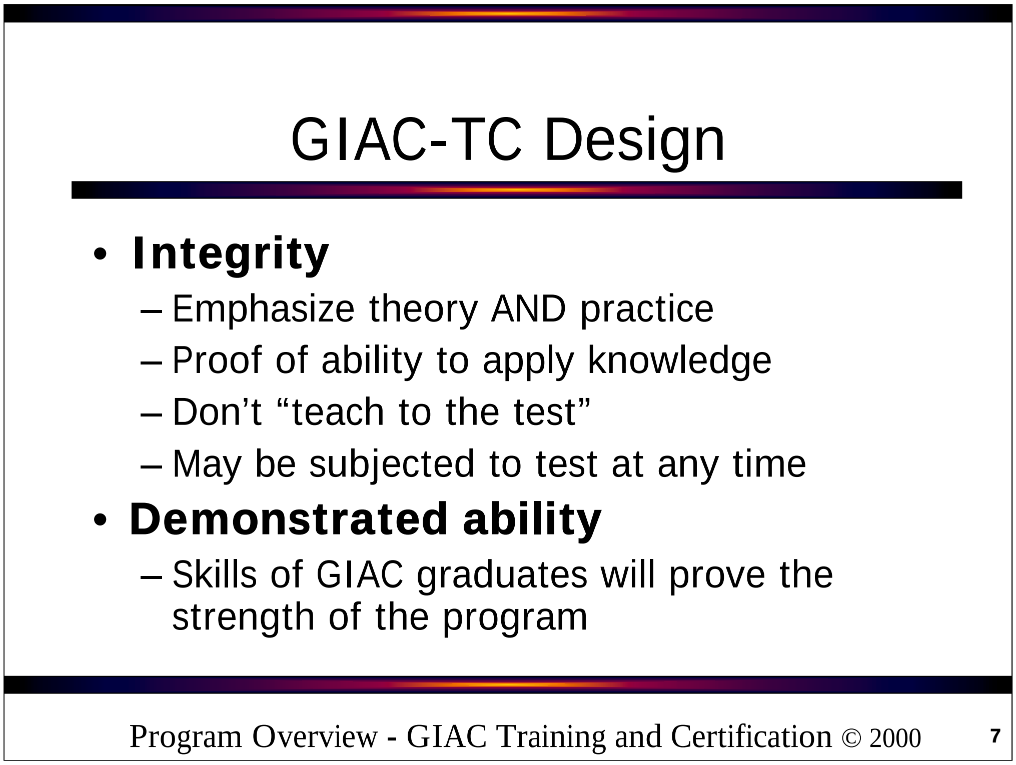
Big Deal – Another Certification

- What does “certified” really mean?
- Does certification have any value?
- What makes GIAC-TC different?

Program Overview - GIAC Training and Certification © 2000 6

There is a lot of debate over the “value” of certification. Some argue that certification is important because it demonstrates a certain measurable level of skill. Others argue that passing a test is fairly meaningless, and that only experience is the true measure of ability. (You may have heard of the term “paper” certification – a derogatory term used to describe someone who has passed a test and earned a certification, but is unable to apply that knowledge in a practical sense in “real world” situations.)

We believe that, while certification is not the **only** measure of ability, it **does** have both meaning and value – if properly designed and administered.



GIAC-TC Design

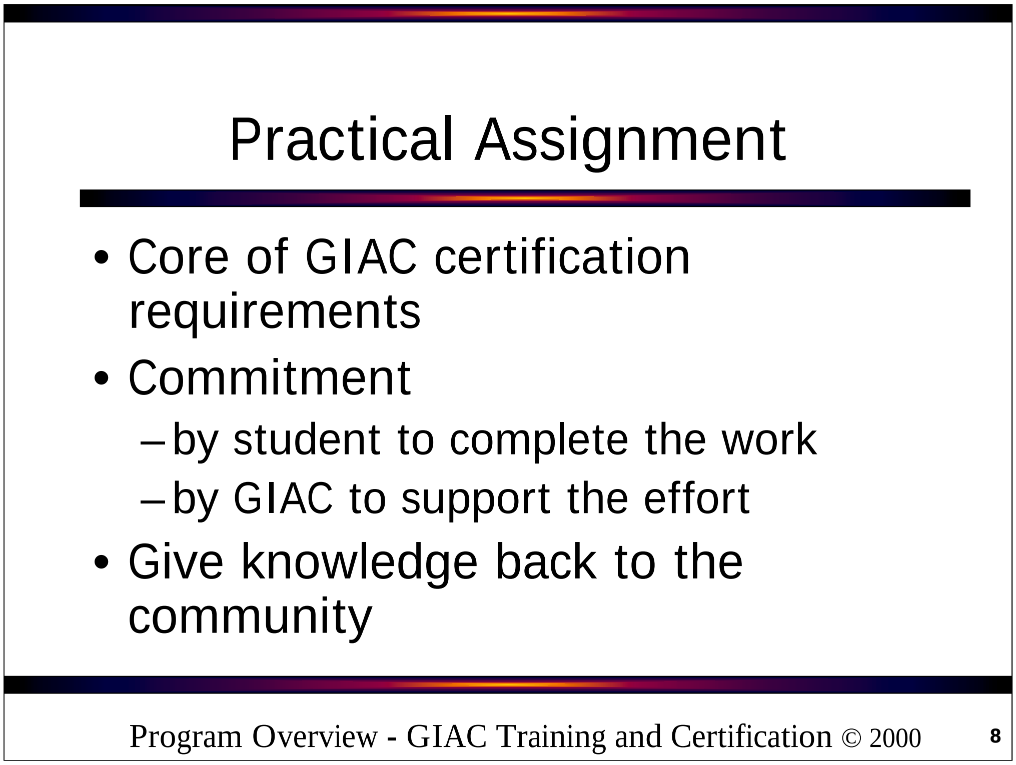
- **Integrity**
  - Emphasize theory AND practice
  - Proof of ability to apply knowledge
  - Don’t “teach to the test”
  - May be subjected to test at any time
- **Demonstrated ability**
  - Skills of GIAC graduates will prove the strength of the program

Program Overview - GIAC Training and Certification © 2000 7

A properly designed certification program should be able to establish a standard of excellence – an expectation that someone who holds the certification possesses a minimum level of knowledge and skill. The “proof” of this assertion comes from two elements.

The first is the design of the certification itself. A major criticism of certification programs is that they reward students who are good at ‘book learning’, but prove nothing about someone’s ability to put knowledge into practice. The GIAC program strongly emphasizes the **practical** aspects of information security – not just what it is and how it works, but **how to apply it.**

The second element is the demonstrated ability of the program’s graduates to do the job that the certification claims they can do. Over time we are confident that **you,** as GIAC certified professionals, will prove the integrity of your own certification through your own accomplishments. It’s your certification; it’s your investment. You have just as much stake in the program as we do!



Practical Assignment

- Core of GIAC certification requirements
- Commitment
  - by student to complete the work
  - by GIAC to support the effort
- Give knowledge back to the community

Program Overview - GIAC Training and Certification © 2000 8

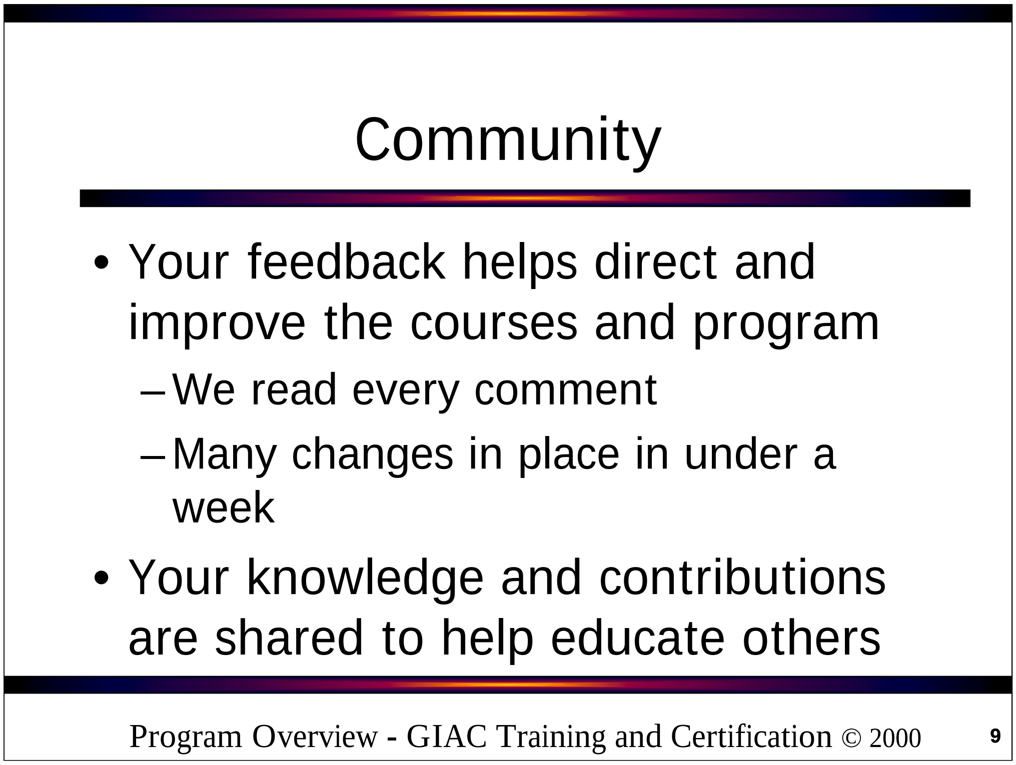
Not only does GIAC-TC emphasize the practical application of security knowledge, we also require students to **prove** that they can apply their knowledge before they can be GIAC certified.

The core of the GIAC certification is the practical assignment. This is a paper or research project designed to demonstrate the student's ability to put knowledge into practice. GIAC is unique among security certifications in having such a requirement. It is one of the key elements that sets us apart from the rest.

The practical assignment represents an important commitment. First, by you as a student to complete the work. A GIAC certification isn't as "easy" as absorbing material and passing a test. It requires effort on your part to learn the material, do the work, and come up with a final result that demonstrates your skill. This is your chance to shine – all passing practicals are posted on the GIAC-TC web site, so your work will be associated with your name.

It's also a commitment by us to you as students and to the certification itself. Why doesn't anybody else have a practical requirement for certification? Because it's much easier to use a computer to grade electronically-administered exams. GIAC practicals are individually processed and graded – no small effort. We do it because we feel it's critical to the certification – and in most cases, we do it in 72 hours or less.

Finally, the practicals are one more way that GIAC – and you – are able to give back to the community. Our database of practicals is growing and getting a lot of notice. These documents help to further share information and educate people around the world.



Community

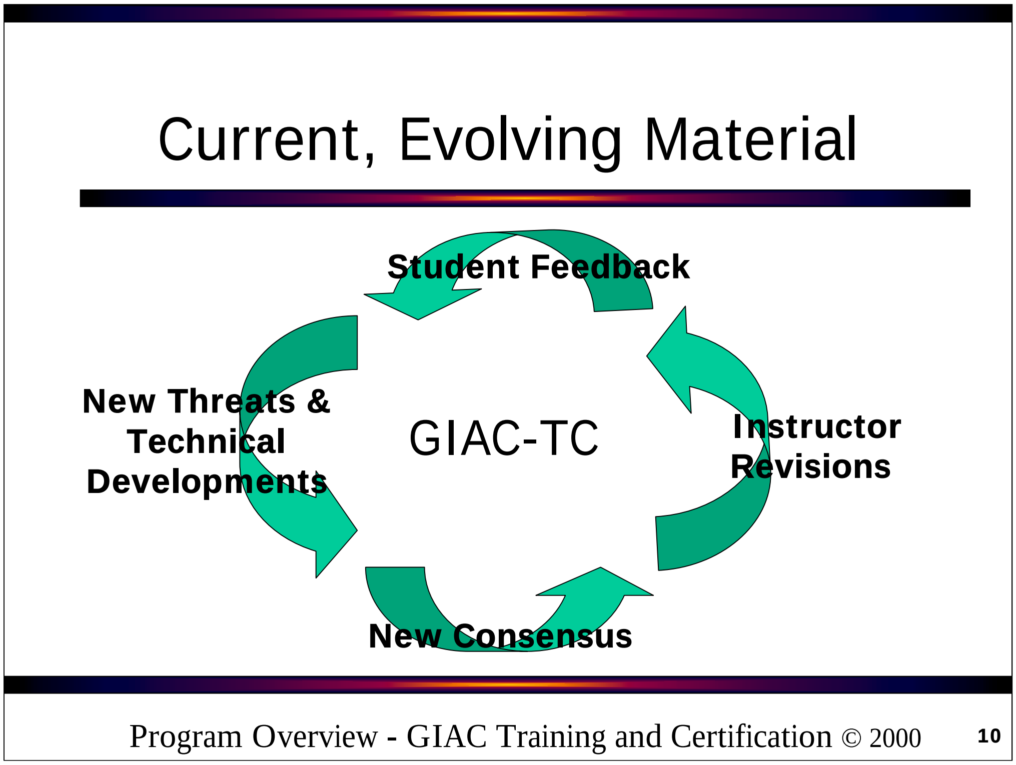
- Your feedback helps direct and improve the courses and program
  - We read every comment
  - Many changes in place in under a week
- Your knowledge and contributions are shared to help educate others

Program Overview - GIAC Training and Certification © 2000 9

Another important aspect of the GIAC-TC program is that (as we've said before!) it is very much a community program. GIAC is not some monolithic entity dictating a specific program. If you've worked with SANS before, you should be familiar with the ever-present evaluation form! We constantly ask you for comments, feedback, suggestions for improvement.

This isn't just going through the motions – we take your comments very seriously, read them all, and take your suggestions into account for future improvements. If we're not meeting your needs, we're not doing our jobs. You actually have input into what we teach and how we teach it – this is not something you can say about most other programs.

We also realize the value of shared knowledge. Not everyone can afford training classes. By sharing knowledge, publishing practicals and other information, we make valuable information available to everyone.



Current, Evolving Material

GIAC-TC

Student Feedback

Instructor Revisions

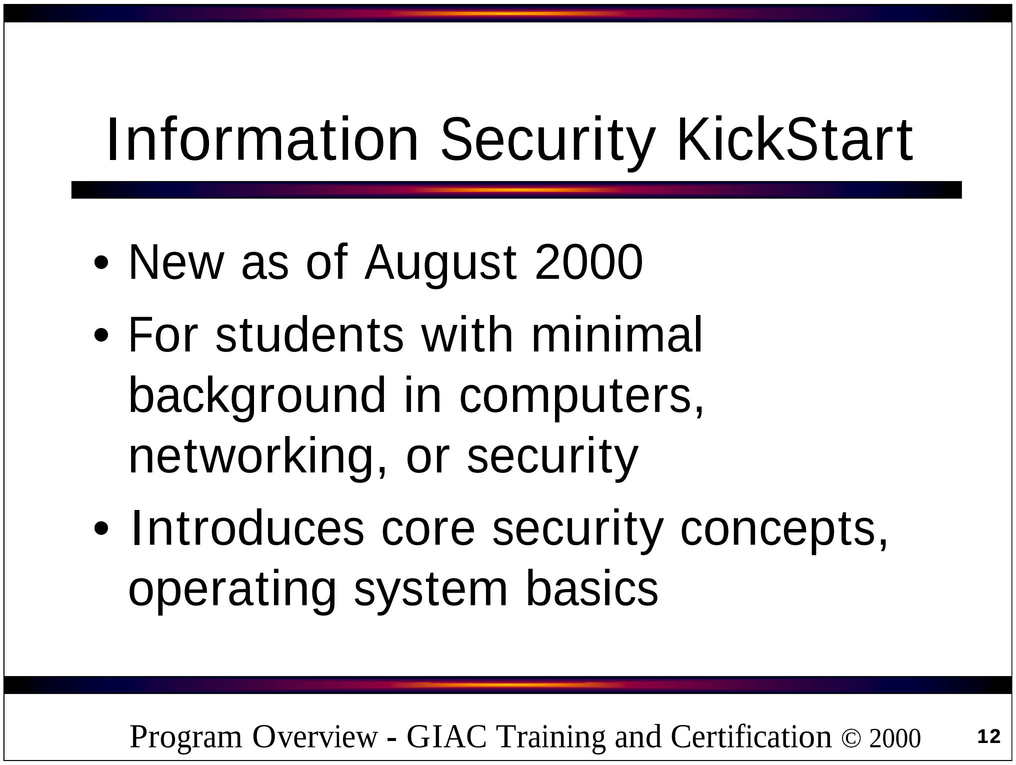
New Consensus

New Threats & Technical Developments

Program Overview - GIAC Training and Certification © 2000 10

Another difference between GIAC-TC and other programs is that GIAC is constantly evolving. GIAC courses are not static – and therefore they don’t become dated. Information security (like technology in general) is a rapidly changing field. GIAC courses are revised on an ongoing basis – generally, every few months. Student feedback and new technical developments lead to new consensus on best practice, which are incorporated into GIAC material through instructor revisions…and the cycle begins again. Courses are revised, exams updated to reflect new material, new practical assignments developed to build on earlier research. GIAC continues to raise the bar, setting new standards for excellence.

GIAC-TC Courses

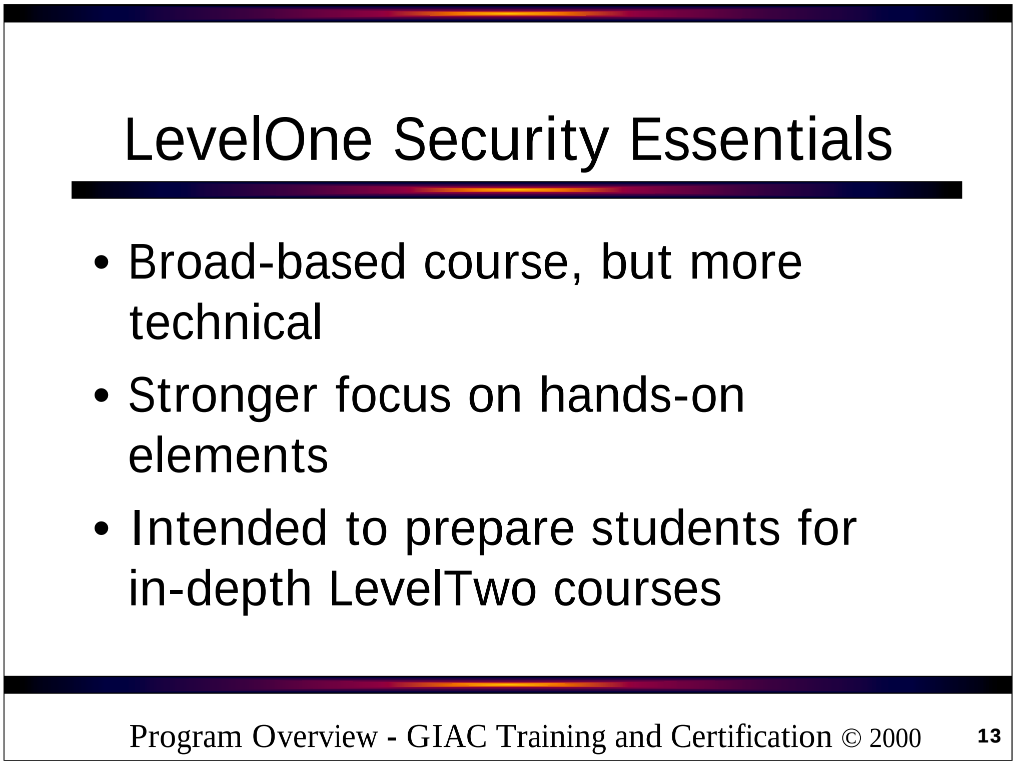


Information Security KickStart

- New as of August 2000
- For students with minimal background in computers, networking, or security
- Introduces core security concepts, operating system basics

Information Security KickStart is targeted at students who have little or no background in computers, networking, or security. It is a basic course that provides a broad overview of security topics, including networking and communications, authentication and access control, and security standards. It also includes an overview of operating system basics for both Windows and Unix/Linux, an introduction to security and risk management, and an overview of intrusion detection and the elements of a secure network architecture.

Students who successfully complete the KickStart program will receive a certificate indicating that they have met the program requirements.



LevelOne Security Essentials

- Broad-based course, but more technical
- Stronger focus on hands-on elements
- Intended to prepare students for in-depth LevelTwo courses

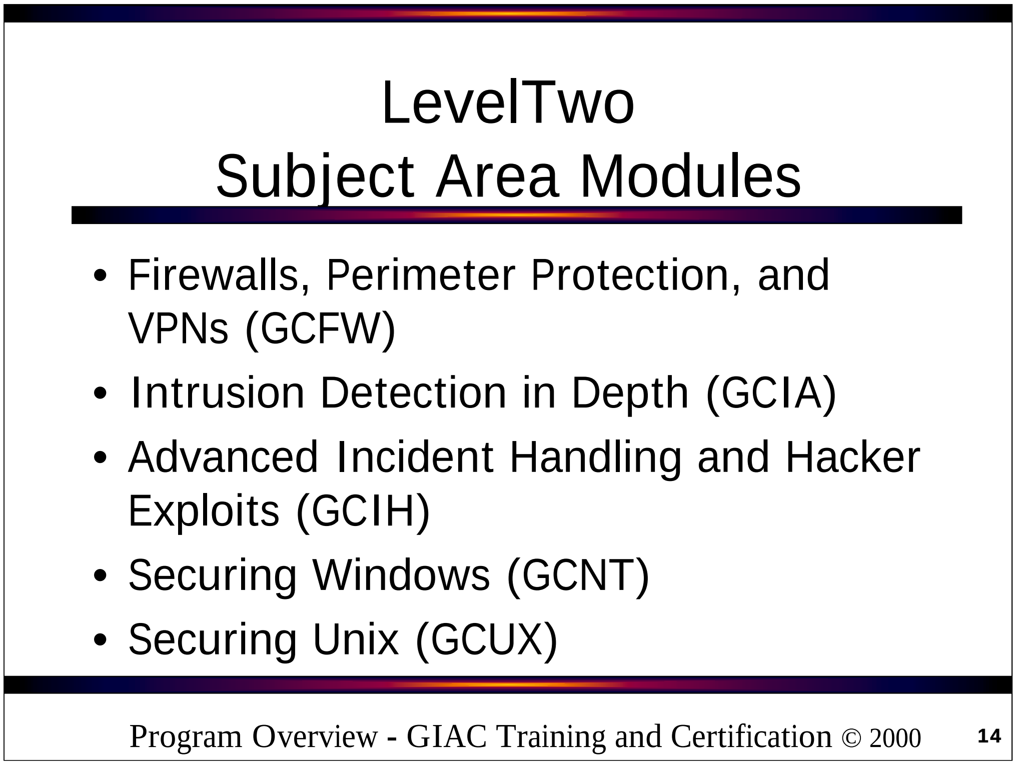
Program Overview - GIAC Training and Certification © 2000 13

The LevelOne Security Essentials course is also a broad-based course, but begins to focus on some of the more technical elements of both the theory and practice of information security. LevelOne is targeted at students who already have some familiarity with networking, operating systems, and security concepts.

LevelOne covers topics such as the TCP/IP protocol; networking; current network threats; security policy; malicious software; and cryptography. It also covers more detailed technical topics for both Windows and Unix/Linux, such as backups, auditing, password management, and secure system configuration.

Students who successfully complete the Security Essentials requirements will earn the GIAC Security Essentials Certification (GSEC).

Security Essentials is the GIAC core foundational course, and consists of the essential concepts that any person in a security-related position should know. LevelOne also provides the base of knowledge that will prepare students for the in-depth technical material offered in the LevelTwo Subject Area Modules.



LevelTwo Subject Area Modules

- Firewalls, Perimeter Protection, and VPNs (GCFW)
- Intrusion Detection in Depth (GCIA)
- Advanced Incident Handling and Hacker Exploits (GCIH)
- Securing Windows (GCNT)
- Securing Unix (GCUX)

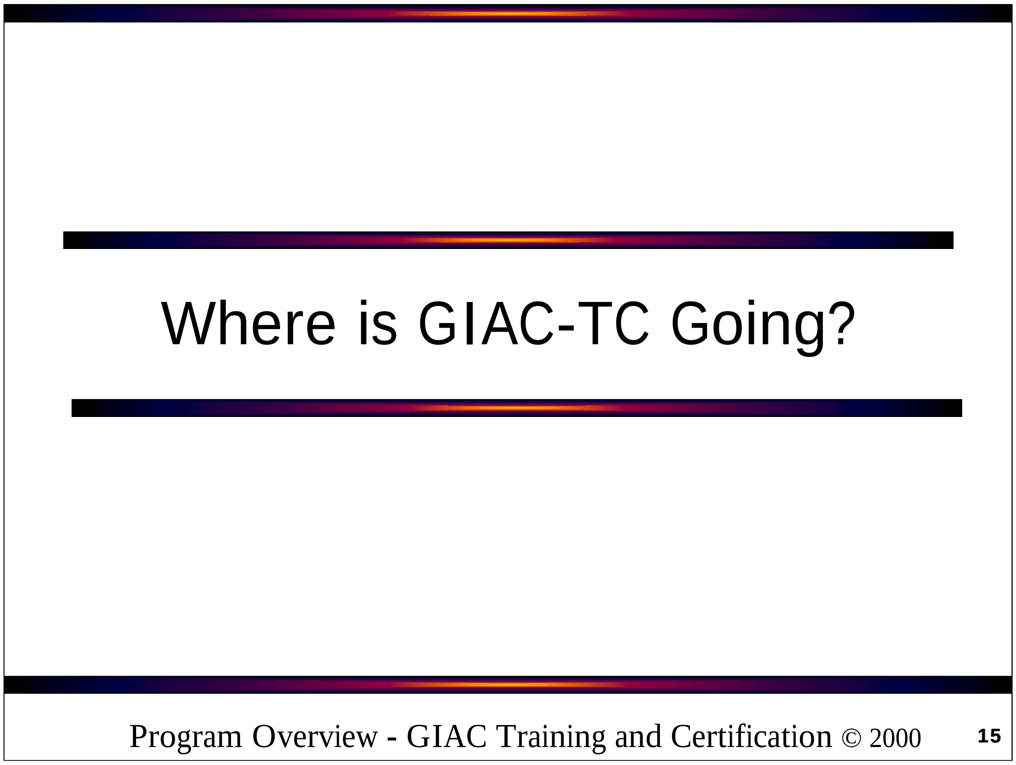
Program Overview - GIAC Training and Certification © 2000 14

LevelTwo subject area modules provide in-depth technical training in specific areas of information security. Students taking LevelTwo courses are expected to have a working knowledge of the course subject matter.

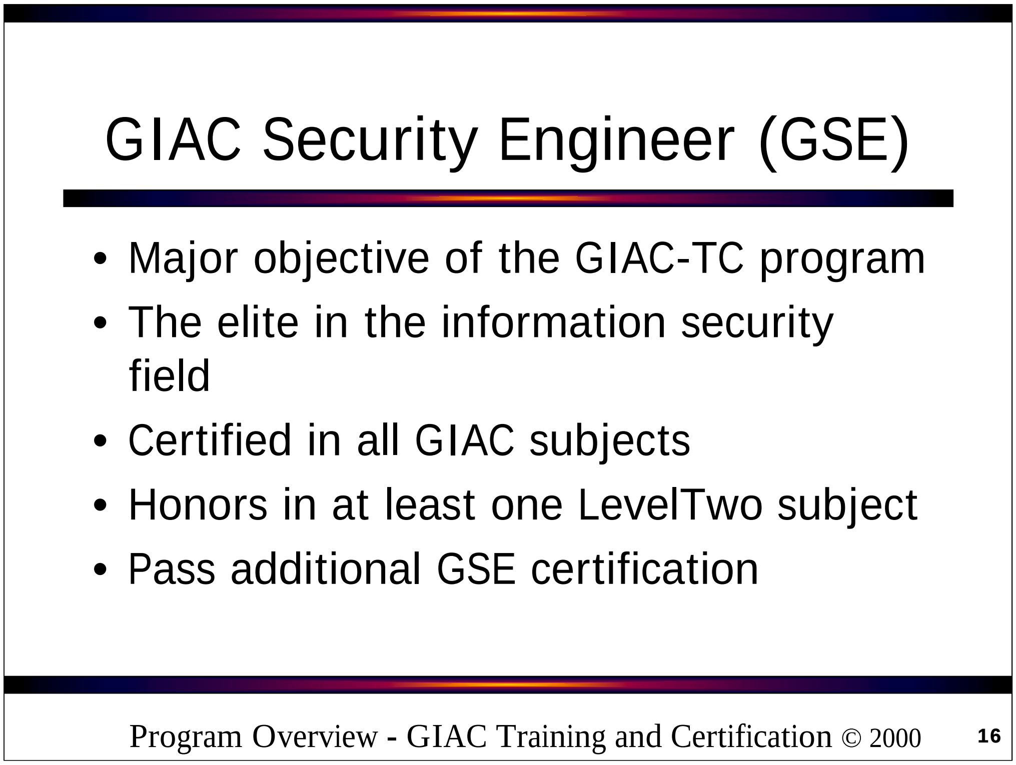
Successful completion of LevelTwo courses leads to the following certifications:

- Firewalls, Perimeter Protection, and VPNs: GIAC Certified Firewall Analyst (GCFW)
- Intrusion Detection in Depth: GIAC Certified Intrusion Analyst (GCIA)
- Advanced Incident Handling and Hacker Exploits: GIAC Certified Incident Handler (GCIH)
- Securing Windows: GIAC Certified Windows Security Administrator (GCNT)
- Securing Unix: GIAC Certified Unix Security Administrator (GCUX)

Students who receive certification in a Subject Area Module have demonstrated that they possess the core skills required of an individual responsible for a particular area of information security.



Where is GIAC-TC Going?



GIAC Security Engineer (GSE)

- Major objective of the GIAC-TC program
- The elite in the information security field
- Certified in all GIAC subjects
- Honors in at least one LevelTwo subject
- Pass additional GSE certification

Program Overview - GIAC Training and Certification © 2000 16

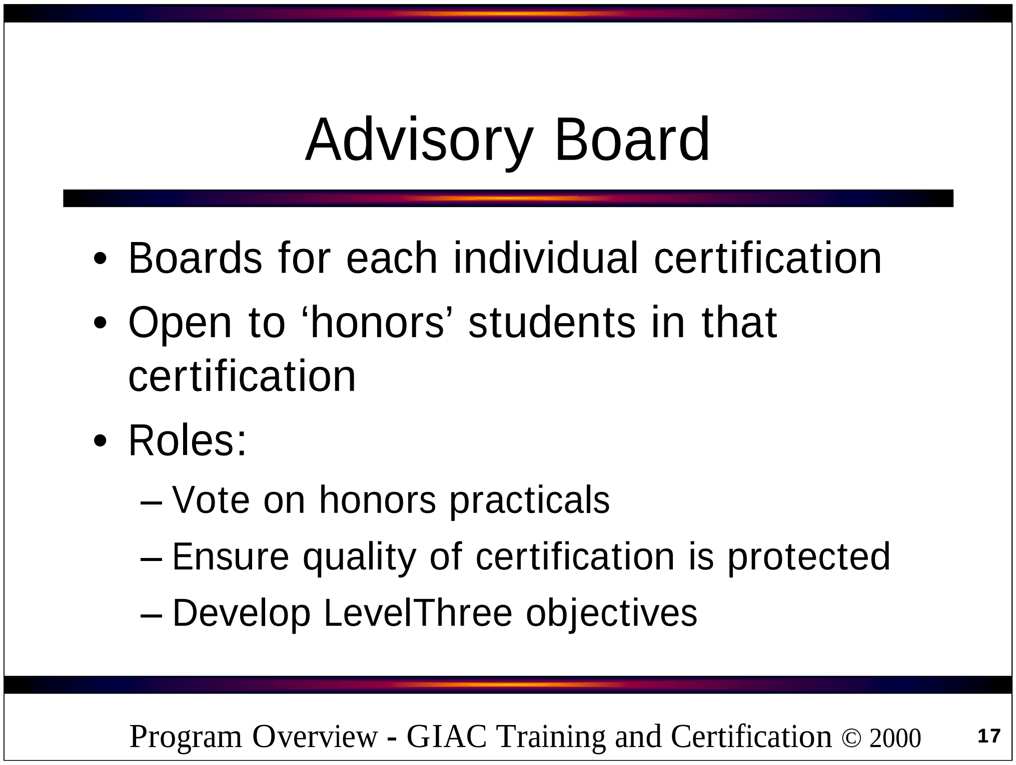
So, what are we working towards with the GIAC-TC program? GIAC-TC wants to provide:

- practical security training for all levels of experience, from beginner to advanced;
- in-depth training in specific essential security topics (Subject Area Modules).

These two criteria allow us to provide training at all levels, and to meet a variety of needs: from individuals who want broad, basic security training, to people looking for detailed training in a specific area, to those who want a roadmap to pursue an in-depth technical education in all areas of information security. It is this last group of people, however – those that want to understand and be proficient in all areas of information security – in which we take a particular interest.

Knowledge in a particular area – intrusion detection or Windows security – is both important and valuable. Individuals who earn **any** of the GIAC certifications have worked hard, demonstrated essential technical skill, and should rightfully take pride in their accomplishment.

But individuals who make the effort to not only learn, but to *master* all of the essential elements of information security belong to a very special group. These individuals will be the elite of information security – the top practitioners in the field. Students who receive and maintain all of the GIAC certifications, and receive “honors” in at least one LevelTwo certification, will be eligible to sit for the GIAC Security Engineer (GSE) certification. The GSE will be available in 2001.



Advisory Board

- Boards for each individual certification
- Open to ‘honors’ students in that certification
- Roles:
  - Vote on honors practicals
  - Ensure quality of certification is protected
  - Develop LevelThree objectives

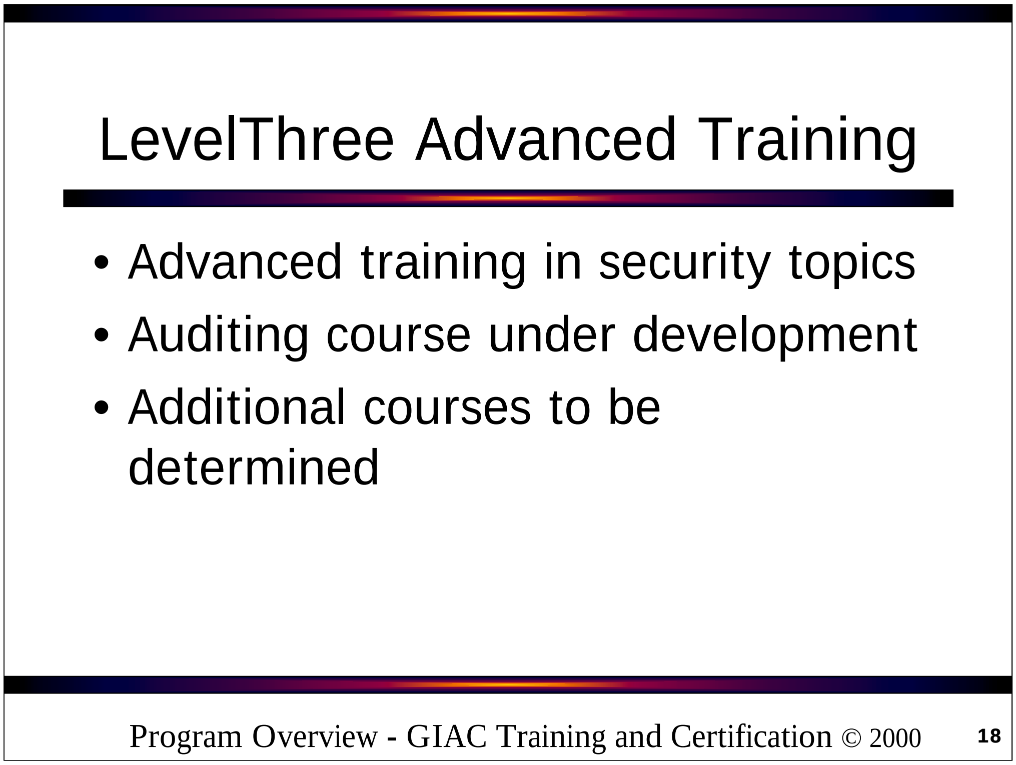
Program Overview - GIAC Training and Certification © 2000 17

GIAC has been building the ranks of certified individuals throughout the past year. Now that we have laid the foundation, we are asking certified students who are willing to assist to give back to the community – and the GIAC-TC program – by helping to guide and shape the certification for the future.

This is **your** certification. You have a stake in what it means and in the effort you invest to achieve it. GIAC is about both education and community, and **all** GIAC students and certified professionals are encouraged to provide comments and suggestions – your feedback is used to continually revise and improve the program.

In addition, “honors” students are invited to participate in the Advisory Board for their certification. Participation is voluntary, and means that you will be able to contribute to key program elements, such as:

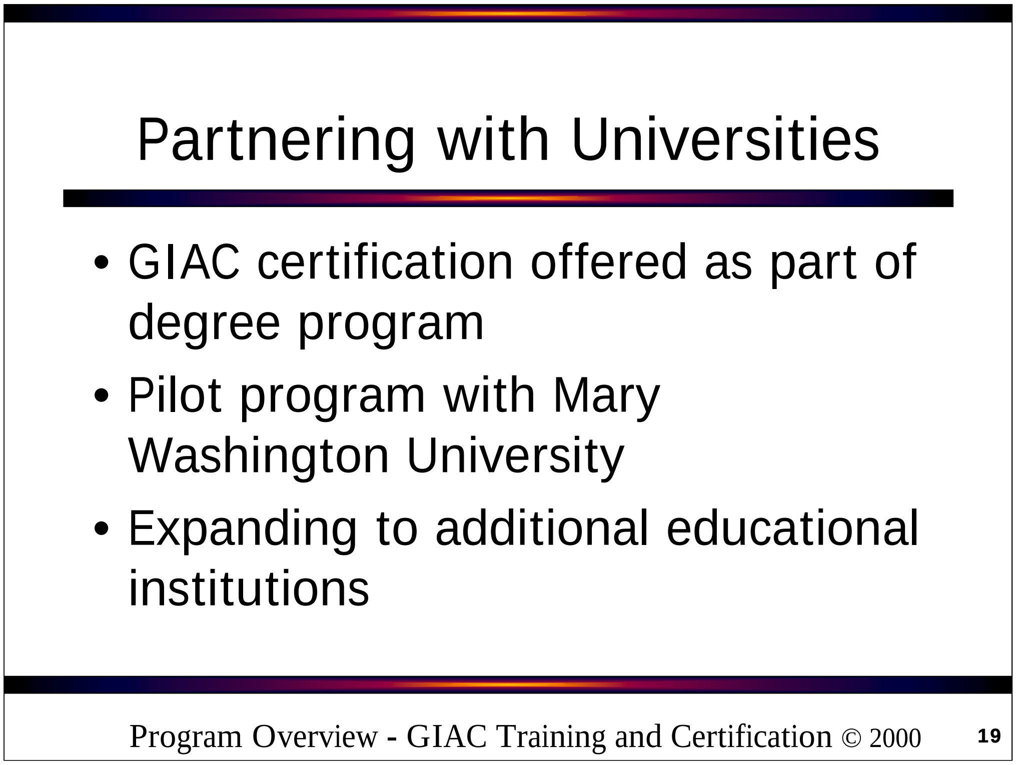
- voting on “honors” awards for student practicals;
- providing additional guidance to shape the certification and protect its integrity and value;
- help to define objectives for advanced LevelThree training.



LevelThree Advanced Training

- Advanced training in security topics
- Auditing course under development
- Additional courses to be determined

GIAC security training does not stop with LevelTwo. An advanced LevelThree curriculum is currently under development, with an advanced Auditing course scheduled to be one of the first offerings.



Partnering with Universities

- GIAC certification offered as part of degree program
- Pilot program with Mary Washington University
- Expanding to additional educational institutions

Program Overview - GIAC Training and Certification © 2000 19

GIAC-TC is currently partnering with Mary Washington University in Virginia to offer GIAC certification to university students enrolled in degree programs. At Mary Washington, GIAC training is available to approved students enrolled in the MBA degree program. Students are able to take GIAC courses online, receive GIAC certification, and earn credit towards their degree.

We are in the process of expanding these partnerships to include other academic institutions.

Wherever We Take It!

Thank You!

Program Overview - GIAC Training and Certification © 2000 20

GIAC-TC is **your** certification. If you are willing to get involved, you have the chance to tell us how you would like it to grow and develop!