Global Information Assurance Certification Paper

Managed Training for the Systems Access Security Analyst

GSEC Version 1.4b, Option 1

Michelle Desnoyers
September 30, 2002

Managed Training for the Systems Access Security Analyst

Abstract

An integral component of a organization's information security team is the person or, depending on the user base and environment size, group of personnel dedicated to handling the daily activities surrounding the setup, modification, and disabling of user system access. The profile of this specific security analyst is that of a generalist who is expected to possess a cross-section of knowledge pertaining to the organizational structure, multiple operating platforms, current and evolving security standards and policies, specialized requirements, and new technologies. While a benefit, strong technical skills and certifications are not necessarily a pre-requisite for entering the field as a mature and keen individual can be provided with customized on-the-job training and excel as a security analyst. The important consideration, however, is to establish a consistent and on-going internal training focus that ensures the same training delivery to all systems access security analysts.

System Access Controls

- **Definition and Principles**

The "Handbook of Information Security Management 1999" establishes that the intent of access control systems is to protect an organization's critical and sensitive information assets from unauthorized disclosure, modification, or destruction.[1] The systems and methodologies falling under the domain of access controls are characterized as either physical, technical, or administrative and operate to attain the three main security principles of assuring confidentiality, integrity, and availability.

User management falls within the administrative controls realm where the information security team has to strike a balance in ensuring adherence to established security policies and procedures while providing accurate and effective user system access privileges. In his article titled "User access chaos needs life cycle management", Chris King also defines user management as having a life cycle with the three phases of provisioning, maintenance, and termination as they relate to systems, applications, and database access.[2]

- **Current Methodologies**

Where an organization has not yet defined and implemented role-based access controls, the processes involved in managing a user's system access encompass the activities of confirming the user requirements, obtaining appropriate resource authorizations, and defining the user's privileges which are all done manually or with a limited amount of automation.

---

[1] Krause, p.1.
[2] King.

Additionally, centralized electronic mail and enterprise file management requires that information security manage all client requests related to corporate email distribution lists, public folders, special email addressing, and network directories.

All of these activities translate into an enormous cross-analysis burden on the security analysts who must assimilate existing policies and procedures with organizational specific requirements and application access idiosyncrasies to fulfill the requirements of a client request. Also from the same article, King accurately assesses that user management is traditionally chaotic in most organizations "…with requests coming from various channels (paper forms, phone calls, e-mails, help desk requests, etc.), and moving through various de facto fulfillment procedures."[3]

- **Evolving Trends and Challenges**

Advancements toward minimizing or eliminating the manual components of managing user access privileges include the implementation of role-based policy and tools which automate the request, authorization, and set-up process through, for example, web-enabled mechanisms. Not only does this release the security analyst from the tedium of repetitive administrative tasks, it mitigates the risk of security exposures related to errors and inaccurate or inconsistent application of access controls and expedites the processing of client requests.

The challenge of transitioning to the fully automated identity management system with delegated administration, provisioning, and user life cycle management is tremendous. It can involve identifying all of the infrastructure architecture components, defining the roles and policies which will manage the system, and educating all of the organization's personnel. This is not a solution that can be accomplished easily or in a short period of time, however, it should be diligently pursued as a means to eliminate the manual security administrative function and its associated issues.

- **Information Security Training Constraints**

Given that the client requirements within an organization seldom remain static, the information security team operates under a heavy, and generally ad hoc, workload which leaves little or no time to receive or provide training. For completing requests, the personnel are subject to both the terms of service agreements or turnaround commitments, as well as shifting work queue volumes due to staffing shortfalls caused by sick and vacation time, leaves, or budget constraints.

Another factor acting as an impediment to a systems access security analyst obtaining both initial and on-going training is the lack of relevant courses or programs geared toward the required skills and competencies for the position.

[3] King.

Local specialized programs are generally non-existent, while vendor and information security certifications (e.g., GIAC) have a focus which is either too narrow, broad, or technical.

The Training Program

Considering that appropriate external training is typically unavailable, and as outlined in the introduction, the solution for an organization's information security team is to establish an on-going and consistent internal training focus that ensures the same training delivery to all systems access security analysts.

Section 3.5 in NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program refers to the concept of "setting the bar" for determining the complexity of the training material to be developed with levels of beginning, intermediate, and advanced.[4] In the case of the person entering the discipline of user management, the material should be designed at a 'beginning' level and would serve as an introductory guide to security concepts and objectives and carry forward into the organizational layout, operating systems and environments, and security administration tools.

- **Introduction to Security Objectives**

Even if there isn't any prior formal exposure to the concepts of information security, the security analyst candidate should be able to demonstrate an inherent common sense toward the protection of information. At this point, an apparent security orientation supersedes the priority of technical skills or certifications. Mike Hays, director of education services for the Americas at Symantec Corporation, also concurs in his interview with SC Magazine with his statement "By identifying individuals with both the aptitude for and interest in security, organizations can invest in getting them knowledge and skills they need."[5]

It is important to introduce the new security analyst to the principles of information security and how they relate to the security framework established for the organization. For definition within this document, the security framework is essentially a defined set of standards for the purpose of protecting the organization's technology environment and corporate information assets and should be one of the first documents the new analyst reads when joining the team. These standards are applicable to the management, information technology, data owner, and user community and outline specific expectations on roles, responsibilities, and acceptable conduct.

The next item on the training agenda should be a high-level explanation of information security's policies and procedures. This can include a lesson on

[4] NIST, p. 20.
[5] Armstrong, p.30.

authentication concepts, security awareness topics, the do's and don'ts for a security analyst, and a preliminary look at the tools and templates used in the client request workflow.

- **Understanding the Organization**

An overview of the company or group of companies that comprise the organization, along with its general business objectives, should be presented to the trainee prior to introducing all of the operating systems and applications and their associated access controls. This allows for a better comprehension of how the systems and data are used by the clients and why information security is applied particularly when the analyst needs to reference and interpret resource authorizer records.

Organizational information is best provided in a visual format such as an organization chart which can usually be obtained from human resources. These charts are particularly valuable as an on-going reference when obtaining appropriate access authorizations and they should include both a department description and supervisory names and titles, be accessible to all analysts from either a network folder or intranet location, and be updated regularly.

Following this, it is also useful to demonstrate how access controls can be used to define levels of access to an application or data based on, for example, departmental and positional requirements. This can be done by examining the access privileges for two users from the same department who perform different jobs and comparing those permissions which are common for both and those which are different, possibly due to a segregation of duties.

- **Operating Systems and Environments**

Not all of the operating systems and environments will necessarily be a part of the beginning level curriculum, however, an ideal training program will still outline their existence, usage, and applicable access controls. The trainee will be able to use this information in the present terms of understanding the references when analyzing a client request and in the future terms of charting training progression.

The training emphasis for this section will be on familiarizing the analyst with the environment in which the most time will be spent on user management. As an example, depending on the organization, this could be Windows NT/2000 or Unix. Again, it is not a cast-in-stone requirement that the trainee possess advanced technical skills or a certification prior to entering this position. John Hunt, principal for the security and privacy practice at PricewaterhouseCoopers, reiterates this sentiment when asked how important infosecurity experience is as opposed to specific infosecurity certifications by Illena Armstrong of SC Magazine with his response:

> While certifications are good to obtain and provide focus and diligence, they have never been a significant factor in this industry.

> Professionals need to be focused on where the business is going – get into their environment and recognize it. This can only truly be achieved by on-the-job experience. Experience/hands-on is key versus just certifications in an area.[6]

Before advancing to the toolset training, and particularly if the trainee is an external hire and new to the organization, it is a good idea to allow the novice analyst an opportunity to become familiar with the organization's environment by navigating through the available email system, network drives, and applications. The trainee's ability and comfort in maneuvering throughout the environment is essential for continuation of the training. Actually performing the keystrokes, actions, and tasks enhances the learner's ability to pick up and retain the skills being taught. In the context of a discussion on e-learning, Tony O'Driscoll, an e-business strategy consultant with IBM, commented that the best way to apply knowledge when learning is to be paired with someone who can show how it works in the real world.[7]

- **Tools for Security Administration**

Once it has been impressed upon the trainee how much power a security administrator wields, along with the professional and ethical obligations that accompany it, the program advances to the use of the tools for access controls and user management. The focus of the lessons is to gain proficiency with the various tools to perform inquiries, analyze requests, and apply appropriate modifications or updates for fulfillment of requests.

During the training program, it is unlikely that the trainer is able to dedicate full days due to regular workload commitments. A balanced approach would be to schedule no more than 75% of the day for training, enabling the trainer to return to other responsibilities while the trainee then has an opportunity to review what has been learned during the course of the day. Depending on the pace of the training and barring any disruptions, introduction to the tools for security administration could already occur on day two. It is not unrealistic to be able to provide sufficient training in one or more of these tools to allow the new analyst to attempt processing a couple of 'easy' requests as homework exercises during the latter part of the day. This method of blending instruction with actual tasks is effective for applying practical knowledge, instilling confidence and self-initiative, and cumulative learning as requests become more complex and diverse.

Training Tools

Neither in-house nor external development of customized training tools for systems access security analysts is a viable option in the face of information technology's fast-paced changes and tight training and development budgets.

[6] Armstrong, p.26.
[7] Nagel.

As an example, while web-based delivery would be desirable for many aspects of the training program, it wouldn't be cost or time-effective to set up a system which would place a strain on security personnel resources for both its development and frequent content maintenance. Instead, more traditional methods for providing and managing training such as checklists are employed in this program.

- **Checklists**

Standardized checklists broken down by subject area are an effective tool for consistent training delivery as they provide both an 'at-a-glance' measurement of the training progress and assurance that no topics or key points are overlooked.

Both the trainer and trainee can maintain paper copies of the checklists for a visual confirmation of what has been completed, what is left to cover, and what may need to be revisited.

- **Process and Procedures**

The training plan has to include step-by-step instruction on the process and procedures to be used for the core tasks performed in the user management function. The associated documented procedures should be in a location that is easily referenced.

- **Documentation**

If an analyst is expected to reference procedures while learning and to ensure consistency of applying access controls, it is imperative that a central source of information or 'handbook' be established and maintained. While limited personnel resources can hinder the development of the handbook, an effort should at least be made to store all reference and procedural material in a central repository on a secured network drive. Ideally, and if possible, the handbook should be set up as a web-based resource on an intranet and have a search engine functionality.

- **Dedicated Trainer and Coaching**

Trainees benefit from consistent training delivery when only one or two senior analysts are designated to this task. Each new or developing analyst can be assured that the dissemination of information and practical training aligns with that of every other systems access security analyst within the workgroup. The trainee is also able to develop a rapport with the facilitator which fosters a coaching relationship and encourages continuing learning and development.

Another advantage of consistent training is team-building which is further asserted by Lincoln Bittner in his article "Corporate Culture: Training, Part II". He states "If your training is consistent with each employee, then they will be able to go to each other for reinforcement. The ability to go to a coworker for reinforcement is the cornerstone of any great team, and will build self-confidence and trust into the organization."[8]

Managing the Training

The new security analyst is typically ready to enter the systems access work queue in the second week of training delivery. This does not mean that the training is complete however. Training continues to be a work-in-progress as the learner seeks affirmation of correct analysis and process and encounters more complex situations. It is easy at this point to abandon scheduled learning sessions and, thus, it is now especially important to ensure a structured mechanism is in place to promote continuous and planned training.

- **Training Record and Personal Development Portfolio**

An approach to consider for managing an individual's training is to incorporate the maintenance of an information security training record or database with the set up of a personal development portfolio for each analyst.

Initially, the database will consist of the high-level or core competencies defined for every functional position within the information security workgroup. It will also chart an individual's progress in achieving each competency. Its maintenance will be the responsibility of the supervisor or trainer and include input from the trainee to ensure it is current and accurate.

The personal development portfolio, on the other hand, shifts more responsibility onto the analyst for self-directed learning and development. On its website, TNA, a UK training consultancy company, defines the concept of this portfolio as an organized and goal-driven vehicle designed to enhance competence in the workplace.[9] The site further outlines the portfolio as a method to focus on skills and behavior development by:

- analyzing development needs and developing learning plans
- implementing a learning strategy
- recording work and learning experiences and opportunities
- assessing the value and transferability of skills, experiences, and achievements[10]

- **Needs Assessment**

Both the concepts of self-directed learning and a personal development portfolio require establishing the training needs and the activities to achieve them. Using the training database and the portfolio as a guide, a checkpoint should be planned within a few weeks of the initial training delivery for a progress evaluation. This is an opportunity for both the trainer and trainee to assess the effectiveness of the training to date, any gaps, and the next sequence of learning

[8] Bittner.
[9] TNA.
[10] TNA.

activities.

A particular advantage of self-directed training is that it empowers the learner in "initiating the learning, making the decisions about what training and development experiences will occur, and how."[11] While availability and budget limitations may restrict pursuing some external learning opportunities, learners are still given the responsibility for managing their development and remaining aligned with the progress of other team members.

- **Skill Development and Education Opportunities**

The nature of system access request processing will continuously promote skill development for a security analyst. If a request requires an infrequently encountered or unfamiliar skill, the analyst has an opportunity for reinforcement or new learning. The analyst can also proactively identify the desire to acquire a relevant skill and ask that it be added to the training plan. This development does not have to be strictly security-related and can also include any in-house offerings such as soft skills or project management courses.

As already mentioned, there are fewer education opportunities as a result of unavailability and budgeting constraints. This should not discourage the learner, however, from investigating any possible options providing a good business case can be presented.

- **Quality Assurance and Compliance**

A safeguard function within an information security group is to perform a compliance review on all completed requests to ensure accuracy and adherence to established policies and procedures. Aside from being a quality assurance tool, this function also serves to identify any training deficiencies that may exist. The deficiency item can either be followed up on a case-by-case basis or added to the analyst's training plan.

- **Awareness Communications**

Information security is a dynamic environment which demands continual interaction between its team members to ensure everyone remains apprised of all changes which affect them. These changes can include current issues, organizational changes, and new procedures, tools, and technologies.

With the sharing of appropriate information, everyone can be assured of operating at the same level of understanding and adapting their processes accordingly. Several effective means of communicating necessary information are group discussions, email messages with 'awareness' in the title, and team meetings.

- **Ongoing Mentorship**

[11] McNamara.

Trainers can continue to act in a coaching or mentor capacity without the formal establishment of a mentoring program. The developing security analyst should be comfortable with approaching the trainer or senior analyst for any reason; whether it is to solicit assistance, insight, guidance, or an opinion.

Conclusion

For many organizations, managing systems access continues to be a manual administrative function requiring dedicated information security analysts who possess a vast cross-section of knowledge and perform a broad range of activities. With a number of factors limiting training options, effective development of the security analyst is best managed by a defined internal training program that encourages consistent on-the-job training delivery. If the program is applied properly and with commitment, information security can achieve a solid team with a strong competence in securing the organization's user management environment.

List of References

Armstrong, Illena. “Shaping up for Infosec Training.” SC Magazine July 2002: 24-30.

Bittner, Lincoln. “Corporate Culture: Training, Part II”. 1 February 2002.
URL: http://www.suite101.com/article.cfm/7801/88267

King, Chris. “User access chaos need life cycle management”. 18 September 2002.
URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2880429-1,00.html

Krause, Micki and Hal Tipton. Handbook of Security Management 1999. Boca Raton: Auerbach, 1999. 1.

McNamara, Carter. “Strong Value of Self-Directed Learning in the Workplace: How Supervisors and Learners Gain Leaps in Learning”.
URL: http://www.mapnp.org/library/trng_dev/methods/slf_drct.htm

Nagel, Becky. CertCities.com News (Show Report: Online Learning Conference and Expo 2002). 25 September 2002.
URL: http://certcities.com

National Institute of Standards and Technology (NIST). “Building an Information Technology Security Awareness and Training Program”. NIST Special Publication 800-50. Draft: 2002 July.

TNA.
URL: http://www.trainingneedsanalysis.co.uk/tna_pdp.htm

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: May 30th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event