Global Information Assurance Certification Paper

Security Interviewing

The Techniques and the Application

GSEC Practical Assignment, Version 1.4c - Option 1

Todd Skilton
5 November 2004

Contents

Abstract

This paper discusses the usefulness of personal security at its purist form, by presenting techniques involved with carrying out security interviews. The first section of the paper presents the theoretical techniques of security interviewing including the stages of an interview and how to prepare the questions for the interview.

The second section of the paper provides advice on how to implement security interviewing with an operational sense to carry out security vetting on an employee about to join an organisation. The aim of this process is to increase the faith an organisation can have with its employees by alerting organisations at an early stage to any potential security issues an employee or future employee may introduce into the organisation.

Security Interviewing

Introduction

When businesses are asked what elements they have in place to secure there IT infrastructure the most common replies are firewalls, IDS and possibly physical security controls, however the security of the user is rarely mentioned. As security professionals we are well aware of the principles of security in depth and berth, and cover off on a multitude of potential attack vectors.

In the 2003 Computer Security Institute and the FBI Computer Crime survey, 80 per cent of respondents reported insiders to be the most prevalent threat to networks (Howarth, 2004). While this has reduced in the 2004 survey (it is now closer to 50%), what actions are organisations taking to reduce this security threat?

One of the best ways is to consider personnel at their purest form, throwing away technology and focusing purely on the user, or potential user, through the use of security interviews to alert organisations to any potential security issues an employee or future employee may introduce into the organisation.

Interrogation?

When this topic is introduced, eyes often light up and security staff rush to start sharpening the bamboo sticks for the upcoming interrogations. Security interviewing is not interrogation or tactical questioning. These acts are performed by trained police and military personnel on subjects to extract information, often without the consent of the person involved (Wordiq.com, 2004).

The most important difference between a security interview and interrogation, is the subject involved does not have the ability to terminate the interview at their will, whereas personnel who are receiving a security interview can terminate and leave at any time they like.

The aim of a security interview is to extract as much information as possible about a subject. If the interview becomes an interrogation subjects can view the situation as becoming a 'battle of wits', which the subject does not want to loose. This is not conducive to obtaining the information that we need to accurately assess the security threat an individual presents to our organisation (Department of the Army, 1995).

Why Do Security Interviews?

Interviewing is a critical skill for security personnel, and once the skill has been developed to a high standard, interviews become an essential tool during the security vetting process and security investigations. Security vetting is important to confirm subjects details and social and past history as this may give indicators to future behaviours that could jeopardise an organisations security (McGregor, 2003).

People often alter their resumes when applying for positions to make themselves appear more suitable for a role. However the scale and gravity of this 'glossing up' can be staggering. The EMA Reporter of March/April 2001 reported that a survey of 7,000 executive resumes revealed that 23 percent of executives misrepresent accomplishments, including number of years on the job, academic qualifications, and jobs held (Reid, unknown).

If security incidents are occurring in the work place it is important to determine the cause of these, and in the highly competitive modern environment it is important to know staff are genuinely motivated to working for good of the organisation, or if are staff operating with some ulterior motive or hidden agenda (The Integrity Centre, 2004).

Stages of an Interview

There are six basic stages to the interview process (McGregor, 2003):

1. Planning and preparation
2. Administration
3. Lead In
4. Main Body
5. End
6. Post interview administration

1. Planning and Preparation

It is extremely important that all planning and preparation is done in advance of an interview, rather than trying to carry out the preparations as the interview is about to start. The age-old adage of Proper Prior Planning Prevents Poor Performance never rings true in this case. It is critical to never interview without a plan, as the interviewer will not appear competent, and most of the value of the interview will be lost (McGregor, 2003).

Before commencing the interview, consider what the reason and aim of the interview, ensure that all parties know what is expected of them, and the outcomes that are planned for from the interview. Close liaison between all parties is important as the Human Resources (HR) department may already have some issues they would like further explored from a security point of view. Security interviewing should be conducted to support key organisational activities (McGregor, 2003).

It is important to gain some understanding of the previous involvement and possible knowledge of the subject, regarding previous contact with the organisation, especially if they have been interviewed on previous occasions. Security interviews often have great success due to the slight uneasiness a subject feels due to the 'newness' of the whole affair, if a person has been interviewed before or knows what to expect, this effect will not be so pronounced (McGregor, 2003).

The interviewer should be given all available information on the subject, including resumes and details of background checks performed by HR, and if it's a security investigation, material relating to the state of investigation and any evidence held. If no background checks have yet been performed, the interviewer may choose to do any necessary background checks themselves to gain a greater understanding of the individual (Department of the Army, 1995).

If possible there should be an attempt to match the personalities of the interviewer and the subject as this can assist to obtaining further information during the interview (Department of the Army, 1995).

It is important to consider any legal issues that maybe involved, whether it be national legalisation covering human rights, or internal company policy promoting equal employment opportunities, ensure that the planned lines of questioning comply. Interviewers must ensure that they don't leave themselves or the organisation open to potential legal action or embarrassment in the future (McGregor, 2003).

The interviewer should dress appropriately and maintain a professional image by being punctual. It is critical that the planning that was done during the first stage if the interview process is used and that the interviewer doesn't go off track and tries to bluff their way through the interview (Department of the Army, 1995).

2. Administration

Administrative considerations play a significant role in a successful interview, as poor administration can undermine the effectiveness and professionalism of the interview (McGregor, 2003).

The location of the interview should be chosen carefully. The room or area must be available and not used for other purposes. The room should be private, without the chance of being overheard, and without noise from surrounding offices (McGregor, 2003).

The interviewer must ensure the room chosen for the interview is free from distractions and interruptions. Indicators should be placed on the door to ensure that the interview will not be interrupted. The interviewer should switch off their cell phone and disconnect any phones in the room. The interviewer needs to decide if a desk will be used, and if it is should be cleared. Try and organise the room so that objects such as pictures, clocks or windows are not in the line of sight of the subject. If possible try and have a clock behind the subject so that the interviewer can monitor the time without being seen to look at his or her own watch (McGregor, 2003).

If the person is coming from outside the organisation, reception and security staff must be advised that they will be coming to the organisation so that they are met appropriately (Department of the Army, 1995).

It is strongly advised to consider using technical support and aids to record the interview, and if possible, video it. It provides protection against any future legal challenges, and provides a useful tool to analyse the effectiveness of the interview. It is important to ensure that the equipment is available and functioning correctly (McGregor, 2003).

3. Lead In

The opening period of an interview defines how the interview will progress. The interviewer should introduce themselves and possibly show photographic identification or provide a business card, ensuring that they are courteous but not insincere (Department of the Army, 1995).

The next step is to confirm the identity of the subject, ensuring it is actually the person you are meant to speak to. If required, obtain verification of this using photographic identification (Department of the Army, 1995).

Ensure that the subject knows the reason for the interview to avoid any confusion as to why they are being interviewed. Check how much time the subject has available, or state how long it is anticipated the interview will last. It is important that the interviewer sticks to these time limits. It is polite seek permission before making notes or recording or videoing the interview, normally the subject will agree to this, however you will need to make notes anyway (McGregor, 2003).

Advise the applicants that knowingly supplying false information, or failing to disclose material information, may result in the withdrawal of an offer of employment or may be grounds for dismissal at a later date. Some organisations get subjects to sign a statement acknowledging this (Crown, 2004).

4. Main Body

Finally, with the all the planning and formalities out of the way, it is time for the actual work, and gathering of information to begin. In order to gain the maximum benefit from the interview it is necessary to establish a rapport with the subject to try and relax them as much as possible (McGregor, 2003).

The subject will probably be under an amount of stress already, reducing the likelihood of increasing the tension will help the interview process. Possible points of discussion include the journey to the interview, or maybe a hobby that you have noted from their resume (McGregor, 2003).

The interviewer should be trained so that senior personnel do not intimidate them. If they remain polite and professional, usually the person will respect the interviewer for their specialist skills (Department of the Army, 1995).

Once you have built rapport, the information gathering begins. Try and give the subject a starting point if possible and then let them tell their story in their own

words. The interviewer must remain in control of the interview and should not let the subject ramble or move on to irrelevant subjects (McGregor, 2003).

Interruption of the information flow should be avoided. The interviewer should note any ambiguities and further questions, thereby allowing them to return to these issues later. Once the subject has finished, go back to these points and discuss them aiming to exhaust the subject on information on a particular subject, before turning to another issue. Examples of issues that an interviewer may which to discuss are covered later in this document (McGregor, 2003).

If the subject says something that contradicts something that they have already said, or if they say something that may be interpreted in different ways, get them to reconfirm the facts. A useful method of achieving this is to get the subject to retell parts of their story, but starting from the end point or middle of the story working backwards to the start (McGregor, 2003).

It is important to keep recapping what the subject has said, getting them to further expand the story and fill in blanks or areas with less information. Once the interviewer is happy with the information that has been provided, it is a good idea to go over the story chronologically to ensure it is correct and that the subject has volunteered all the information that they possibly can (McGregor, 2003).

5. End

The interviewer chooses to close the interview when they feel they have all the information they need, not when the subject feels they have said enough (Department of the Army, 1995).

The interview should be brought to a logical conclusion and the subject should be thanked for their time and if appropriate, for the information the subject has provided. This will be of value in the case where you need to talk to them again in the future. Confirm future availability, and the means to contact them in case you have any further questions. The interviewer's contact details should also be passed to the subject in case they think of other information that may be relevant (McGregor, 2003).

Reassure the subject that the information they have given will be disseminated to only those with a valid need to know, and if relevant, ask the subject not to speak to anyone else about the interview (Department of the Army, 1995).

6. Post Interview Administration

Once the interview has been completed the interviewer must evaluate the information received, and to whether it fulfilled the requirements and expectations of the interview. If not they must consider why, and how their performance as an interviewer affected the interview. Can they further develop their skills or modify questioning techniques to make the process more effective in the future? (McGregor, 2003).

A detailed report of the interview must be written up, with appropriate summaries that can be disseminated to appropriate personnel with a need to know (Department of the Army, 1995).

Stress Interviewing

During a stress interview the interviewer deliberately creates a charged, threatening atmosphere. An interviewer can create this situation by contradicting or arguing with the subject or rapidly changing interview topics without warning to annoy and confuse the subject. It is designed to create tension in the candidate, and indicate to the interviewer how the subject may function under that specific kind of stress (UC Regents, 2004).

This type of technique is excellent when recruiting personnel for specific roles, for example Human Intelligence Operatives, however the interviewer must be specifically trained on how to interpret candidate responses (McGregor, 2003).

It is not recommended to use stress in an interview, as irrelevant behaviours and responses can be generated. It will destroy interviewer subject rapport and can create an enemy or at least destroy the positive attitude of a subject (McGregor, 2003).

Preparing Questions

When developing questions, always keep in mind that they must be security related. The following are six main categories of questions that are commonly used by interviewers. Different types of questions may be combined to obtain a certain response (Pittsberg State University, 1998).

1. Closed-ended questions

These questions can be useful when an interviewer wants to know specific information or wishes to further determine the knowledge the subject has on a particular issue. Example: "could you name the five specific personnel who were involved in . . .?" (Pittsberg State University, 1998).

2. Probing questions

These questions are useful to enable the interviewer to obtain further contextual information surrounding an issue, getting further to the heart of the matter. Example: "Why?" "What caused that to happen?" (Pittsberg State University, 1998).

3. Hypothetical questions

Hypothetical situations based on specific security-related areas, designed to see how the subject might handle themselves if put into that situation. It should be noted that this is what they hope they would do, often not what they actually would do, or have done in the past. Example: "What would you do if . . .?; "How would you handle . . .?" (Pittsberg State University, 1998).

4. Loaded questions
These questions force a subject to choose between two undesirable alternatives. These should be avoided during security interviews as it may be construed that the interviewer is putting words into the subjects mouth. It can used to recall a real-life situation where two opposite approaches could be used, then present the situation as a question starting with, "What would be your approach to a situation where . . .?" (Pittsberg State University, 1998).

5. Leading questions
Leading questions should not be used in security interviews, these questions arise when the interviewer sets up the question so that the applicant provides the desired response. When leading questions are asked, the interviewer cannot hope to learn anything about the subject and what really happened. “Our investigations so far have resulted in X appearing to have stolen the equipment. Did X steal the equipment or was it you?” (Pittsberg State University, 1998).

6. Open-ended questions
These are the most effective questions, yield the greatest amount of information, and allow the subject latitude in responding. These questions present little information to the subject, meaning they are not able to predict what sort of answer the interviewer is looking for. Example: "What did you do when you found the money missing?" (Pittsberg State University, 1998).

Detection of Deception

One of the easiest ways to reduce the possibility of being deceived is the use of good questioning technique. Deceitful persons find open-ended questions hardest to answer and they prefer closed questions because these contain a context that will allow the subject to provide an appropriate answer (McGregor, 2003).

Interview subjects who want to avoid giving an answer that they suspect will count against them, or when they encounter a question they are unable to answer, are likely to engage in a variety of strategies to hide the truth (McGregor, 2003).

These strategies will generally be signalled by verbal flags that, while suggesting the possibility of deception, cannot be taken at face value. Further questioning or verification checking must be used to validate them (McGregor, 2003).

Note the subjects verbal, vocal and visual clues - often what they are saying is often less important than how they are saying it and their body and eyes may contradict them (McGregor, 2003).

In many cases however, the signals will be perceived as a ‘gut feeling’ that something is amiss. The instinctive reaction on the part of the interviewer is to

then probe the area directly, which inevitably results in terrific frustration as the subject is now alerted to the suspicion and carefully covers her or his tracks. It is hard to catch subjects without cunningly worded questions or logic traps (McGregor, 2003).

When deception is detected it cannot be challenged directly, but must be treated as part of the process (McGregor, 2003).

Ultimately, the most effective tool in the detection of deception are the records kept of the interview, especially if videoing the video, as it is usually not until the interview is over and the tapes are reviewed that the extent and nature of any deception becomes evident. Because deceitful people operate largely in the emotional domain they are very good at leaving the right impression as long as they are there in person. Once the person is not physically present it is much easier to be objective in the analysis of the answers presented (McGregor, 2003).

When a candidate is encountered, who in the opinion of the interviewer is giving false answers, discipline is needed to remain objective and focus on open ended questions and a systematic inspection of the language of the candidate without giving any leads or cues. When a candidate is being untruthful, the observation that the panel is making notes, combined with the knowledge that this written material is also backed up with technology, it can be extremely unsettling, particularly if there have been some direct questions about sensitive issues (McGregor, 2003).

Common Mistakes

Untrained, unconfident or inexperienced interviewers often make a number of common mistakes. It is critical that interviewers train and practice to ensure these do not occur.

- The interviewer looks or behaves in an inappropriate or incompetent manner. If this happens it will usually destroy any credibility they, and the organisation had established and may well turn a potentially useful subject into a hostile one (McGregor, 2003).

- Interviews being conducted without sufficient preparation. Not only will the interviewer be wasting their time and resources and look unprofessional, they will waste the time of the subject due to the unproductiveness of the interview (McGregor, 2003).

- The interviewer makes assumptions. If there is any doubt about what the subject has stated then the interviewer must clarify this with the subject (McGregor, 2003).

- The use of poor questioning technique, including asking leading questions will encourage the subject to give you the answer that they think you want, thereby rendering the interview useless (McGregor, 2003).

- Confusing security interviewing with interrogation. The interviewer takes the demeanour of 'Dirty Harry' and attempts to beat the answers out of the subject. The interviewer must remember that the subject does not have to answer the questions and can terminate the interview at any time (McGregor, 2003).

- Getting into an argument. It is important that the interviewer remains objective. If the interviewer gets into an argument with the subject, they will look ridiculous. It is important that the interviewer never challenges a subjects view, or get drawn into giving their own opinions or say how stupid or wrong the subjects ideas are (McGregor, 2003).

- Making threats. If the interview is not being productive or the subject is not being cooperative, it is important the interviewer never threatens the subject. At best the interviewer will appear to be a bully, or at worst the interviewer might make an enemy, destroy an investigation or have a legal complaint made against them or the organisation (McGregor, 2003).

Conclusion

Security interviewing is a skill that personnel need to be taught and that needs to be practiced, until highly proficient. The greater the proficiency of the interviewer in being able to use good questioning techniques and structured interviews, the greater the success of the interview due to the amount of information obtained from the subject, in the shortest possible timeframe (McGregor, 2003).

The security interview is something that is often overlooked in the modern environment, but it can quickly show signs of breaches of corporate policy, allowing proper investigation to be initiated and the appropriate resultant correction action to be taken (McGregor, 2003).

A well trained security interviewer will be able to assist in this investigation and thoroughly establish the relevant issues and extract the required information. If the interview is used as part of a security vetting before the person is hired into the organisation may prevent the individual from being employed, thereby saving the organisation from the potential financial loss it may have been otherwise exposed to (McGregor, 2003).

Annex A: Security Interviewing - Going Operational

A security interview can be used in a number of ways within an organisation with the prime example that is to be described here is the security vetting process including from the background research, the conduct of the interviews and the recommendation to the organisation about the security suitability of a subject.

Security Vetting

It is well known that governments throughout the world perform security vetting relating to the sensitivity of information that personnel would have access to, checking various records and conducting interviews of referees and the subject before granting a clearance to access nationally sensitive or classified information. Private organisations have information and resources that are sensitive to that organisation and can represent large quantities of time and investment.

This process normally commences after the Human Resources department has confirmed they would like to offer an applicant a position. It is therefore prudent that human resources have made the decision to employ individuals with the understanding that they will be security vetted before the process commences, so it does not have to factor in the suitability of a person for a position.

Security vetting is normally conducted in three stages:

- Paper background check,
- Referee checks,
- Subject interview

The process is conducted in this order as this enables the checking of the information obtained in the stage before. Whether all stages in this process are to be conducted or not depends on the type of position and the sensitivity or access to information personnel in that position are likely to have.

Paper Background Checks

A background check attempts to verify the background history of a subject, and can be as in depth as an organisation chooses, however it normally involves the completion of one or more of the following (The Integrity Centre[2], 2004)

- Verification of a subjects personal details (birth and marriage records),
- Criminal conviction history check,
- Civil litigation history check,
- Driver's license check (classes of licence held),
- Traffic offences history check,
- Personal credit history check,
- Education Verification,
- Employment Verification.

For the majority of this information you will need to obtain the permission of the individual you are vetting in order to have it released to you. Once Human Resources have notified you of the fact they wish to offer this person a role, the appropriate release forms and a security questionnaire are sent to the applicant to be completed and returned.

Upon the release of this information the security personnel need to analyse the information, and decide whether there are any factors that may lead to the individual being considered a security risk. Depending on the organisation, they may choose to terminate the process at that point, consider the applicant in light of the further information that has been presented, and either offer or deny the position to the applicant.

Referee Checking

If further assurance is required the next stage is referee checking.

It is suggested that a photograph of the applicant be taken at the interview. It should be explained to the applicant that this photograph is used for documentation and identity verification purposes.

One of the questions on the security questionnaire sent to an applicant should be for them to nominate both 'business' and 'personal' referees (normally two of each), and sign a waiver consenting to them passing information about the applicant, that may affect their employment.

The referee interviews can be conducted face to face, or by telephone, however it is preferred where possible to conduct the interviews in person, especially as sensitive information maybe conveyed. It is preferred that the referees that the security personnel speak to different referees than which HR spoke to.

The purpose of the referee check is to obtain an independent assessment of the typical behaviours shown by the subject. In conducting referee checks there are two important behaviours to bear in mind. The referees answers may tell you more about the behaviour of the referee than the candidate, and the answers may tell you more about what the referee thinks you are looking for. To avoid obtaining misleading information it is important that you focus on behaviours and refrain from giving clues as to your personal feelings.

Ideally the business referees will be past employers, who must be able and willing to confirm (Department of the Army, 1995):

- The completeness and accuracy of the applicants CV in relation to claims made about the referees organisation,
- Claimed academic and professional qualifications,
- Work performance and ability while employed by them,

- The identity of the person from the photograph taken at the initial applicants interview,
- The character of the applicant.

Typical questions could include (McGregor, 2003):

- On what dates did X start and finish with you?
- How much sick leave or time off did X take?
- What was this mainly due to?
- What was the exact nature of X's work?
- Why did X leave?
- Would you employ X again? In what capacity?

Personal referees should have known the subject for a length period of time – normally a minimum of 5 years, so they are able and willing to confirm (McGregor, 2003):

- When and under what circumstances they met the subject,
- When they last met and under what circumstances,
- Periods of association,
- Types of association, such as friends, co-workers, or both,
- Frequency of contact, for both social and professional association,
- Whether there has been any form of communication between the referee and subject since their last physical contact.

Questions should be structured around (Department of the Army, 1995):

- General reputation
- Family
- Leisure time activities,
- Morals,
- Personal habits,
- Assets the referee is aware of,
- Whether the subject drinks alcohol, or partakes in drugs.

It is always very important to quantity the descriptions given by referees, for example if the referee claims the person is a drunk, the referees definition of the term should be clearly established and specific details obtained (Department of the Army, 1995).

The Subject Interview

It is tempting at this stage to now leap into straight into the final interview, but it is important to analyse all the information available. By this stage the interviewer will have information from the Human Resources department, along with all the material collected during the background check and the referee interviews.

Of particular interest to the interviewer are areas that are still vague, or material that has been uncovered that contradicts that given by the subject on his security

questionnaire or different from the resume given to Human Resources on their original application.

It is important to remember that the interviewee will question the subject on their personal history and background, regardless of whether this information has been already been provided in the resume, from background searches or from the referees.

When the interviewer asks for information, the subject should generally be asked to provide this information in reverse chronological order, in order to make them think backwards, the opposite of the way people generally concoct stories and experience life.

Suspicion is likely to be raised if a subject cannot recall when they have resided, worked, or gone to school. In addition, the candidate will often inadvertently tell you things during this part of the interview that they may otherwise not say. Remember at all times this is a security interview trying to establish the truth about a subject's history (The Integrity Centre[3], 2004).

While all such matters should have already been verified by the background check the subject could be asked to bring along original documentation such as a passport or driving licence with photograph (identity verification), recent utility bill(s) (home address verification), academic or professional qualifications and references from school, college, university and previous employers. Copies can be made at the security interview if required, to enable further checks to be made with the authors that they are genuine (Crown, 2004).

When formulating the questions to ask, remember that any questions must stay within relevant Human Rights legalisation and comply with company policy. Familiarity with the appropriate legalisation for your country will help greatly in this area.

Topics and potential questions that may be presented (Department of the Army, 1995):

- Full Name
- Maiden name (if appropriate)
- Tribe/clan affiliation (if appropriate)
- Date and place of birth
- Address and phone number
- Past addresses
- Marital status
- Profession or trade
- Current employment
- Past employment
- Schools/universities attended – qualifications obtained
- Passport number

- Military service
- Drugs and alcohol / solvents
- Drivers license
- Criminal and traffic convictions
- Partner details

Annex B: Bibliography

Crown. “Managing Staff Securely – The “Insider” Threat” 2004. URL: http://www.mi5.gov.uk/output/Page58.html (30 Oct 2004).

Department of the Army. “Appendix A: Counter-Human Intelligence Techniques and Procedures.” FM34-60 Counterintelligence. 3 Oct. 1995. URL: http://www.fas.org/irp/doddir/army/fm34-60/fm34-60a.htm (30 Oct. 2004).

Howarth, Fran. “FBI publishes computer crime and security stats.” 5 Aug. 2004. URL: http://www.theregister.co.uk/2004/08/05/fbi_security_stats/ (30 Oct. 2004).

McGregor, Keith. Advanced Interviewing Skills for Personnel Selection. Wellington: Gilmour McGregor and Associates Ltd, 2003.

Pittsberg State University. “Policies & Procedures Classified & Unclassified Employees Interviewing Guide (updated 11/30/98)” 30 Nov. 1998. URL: http://www.pittstate.edu/hrs/inter.htm (30 Oct 2004).

Reid, E. John. “Human Resource Training Products and Programs.” unknown. URL: http://www.reid.com/hr.html (30 Oct 2004).

The Integrity Centre, Inc. “Why should we do Security Interviews?” 12 Oct. 2004. URL: http://www.integctr.com/Screening/FAQ106S.asp (30 Oct 2004).

The Integrity Centre[2], Inc. “What is a Background Check?” 12 Oct. 2004. URL: http://www.integctr.com/Screening/FAQ104S.asp (30 Oct 2004).

The Integrity Centre[3], Inc. “The Examiner (tm)” 12 Oct. 2004. URL: http://www.integctr.com/Screening/ TheExaminer.asp (30 Oct 2004).

UC Regents. “Effective Interviewing Guide – Stress Interviewing” 2004. URL: http://www.gsm.ucdavis.edu/careers/guide/interview/stress.htm (30 Oct 2004).

Word IQ.com. “Definition of Interrogation” 26 Sep. 2004. URL: http://www.wordiq.com/definition/Interrogation (30 Oct 2004).

Last Updated: July 22nd, 2017

Upcoming Training

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
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor