The 20 Coolest Jobs in Information Security

...and How They Make a Difference

Including the

TOP GUN JOBS

To order this brochure,
go to www.sans.org/
20coolestcareers

SANS

The 20 Coolest Careers

Introduction

The US is losing the cyber race
– and falling behind at an accelerating pace.
Almost every week, adversary nations use their advanced
cyber skills to burrow deeply into the information systems that control
our government; our online resources such as banking and email; our electric,
water and telecommunications systems; other critical infrastructure such as hospitals
and transportation; and the US companies that do business around the world.

A major cause of our stumbling is that we face an extreme shortage of people with specialized technical security skills – vulnerability analysis, intrusion detection, digital forensics, reverse engineering, protocol analysis, penetration testing, secure network engineering, and computer network attack, to name but a few. Without tens of thousands of people with these specialized skills, we are "blind and dumb" – unable to see most attacks, unable to engineer our systems to block most attacks, unable to identify all of what has been stolen, unable to find the systems that have been infected, unable to eradicate the infections, and, on the offensive side, unable to dominate in cyber space.

The good news is that many young people are considering careers in cyber security and with the right training, they will help fill the gap. Those drawn to the field are motivated by a variety of reasons. Some are looking for a challenge, others want a job that makes a difference, and still others want to solve computer crime, or better yet, help avoid it.

One thing is clear: as the cyber race goes on, the top technical jobs in information security are increasing in importance. SANS recently conducted a global survey to find out what these top jobs are and to rate the best careers in cyber security. The results suggest that the variety of work on the front lines of cyber space is greater than many might suspect, and that over half of the top jobs are the place where the "top guns" in security are often found or seasoned.

"Top guns" are the best and brightest technical security experts – the people who can take apart an exploit and see how it works, find flaws in communications protocols, see an attack as it is forming on the wire, identify the faintest evidence of malicious code and root out the infection, find evidence of criminal activity even when it is carefully hidden, plan and execute an attack that bypasses conventional and even sophisticated defenses, design a network that can block known attack vectors, and more. Without these "top guns" no nation or industry can hope to have effective protection. Their jobs are found in the areas of most critical need for any nation or industry that takes security seriously.

The 20 career descriptions in this booklet are designed to help those interested in entering the field to select the career path that best matches their abilities, their interests, and their objectives. According to the IT specialists who participated in the SANS survey, all 20 careers are interesting and make a substantial difference in protecting organizations' information, networks, applications and systems. The brochure includes a description of the career, advice on how to be successful from the people who have the jobs now, and a list of SANS courses that can help.

Do you know a better job? Write us at ***Cooljobs@sans.org.***

TOP GUN JOB **#1** TOP GUN JOB

InfoSec Crime Investigator/Forensics Expert

"The thrill of the hunt! You never encounter the same crime twice!"

Job Description

This expert analyzes how intruders breached the infrastructure in order to identify additional systems/networks that have been compromised. Investigating traces left by complex attacks requires a forensic expert who is not only proficient in the latest forensic, response, and reverse engineering skills, but is astute in the latest exploit methodologies.

SANS Courses Recommended

- SEC408: Computer Forensic and E-discovery Essentials
- SEC508: Computer Forensics, Investigation & Response (GCFA)
- SEC558: Network Forensics
- SEC610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
- ***SANS Forensics Summit***

Why It's Cool

- "In the private world, the security guy just cleans up the mess to try and keep the ship afloat, but when criminals strike, the crime investigator gets to see that the bad guys go to jail. Want to see the face of your enemy... behind bars? It's a thrill like no other – being pitted against the mind of the criminal and having to reconstruct his lawless path."

How It Makes a Difference

- "You are what stands between your organization and the hackers/malware out there."
- "This is a core job that provides nuts and bolts technical security controls for any enterprise. When things go wrong, this is the person that we all need to ask for help."

How to Be Successful

Having mastered intrusion prevention/detection, computer forensics, hacker exploit techniques, and some reverse engineering of malware, this forensics expert thinks there is always more to learn and actively seeks out new learning opportunities daily.

Attend training, conferences, and summits that focus on methodologies described below.

Listen to the latest podcasts discussing recent events. Use your blog reader to pull articles automatically found on Websites that focus on discussing the latest trends.

Stay abreast of the latest attack methodologies.

How are attackers breaking into networks? Keep up to date on the latest attacker, pen testing, and red-team methodologies. Learn how to track an attacker across multiple system and technologies.

Stay ahead of the curve on the latest forensic and incident response methodologies.

In addition to traditional forensic methodologies, you need to master live data analysis and collection. Learn how to examine volatile data and collect it effectively. Learn how to identify personal identifiable information and payment card information quickly.

Get familiar with techniques that enable you to quickly analyze malware found on your network.

A skilled investigator can examine malware and network signatures to create malware indicators on the network in order to discover additional systems that may have been breached.

-Rob Lee, Forensic/Incident Response Faculty, SANS
Principal Consultant, Mandiant INC.

TOP GUN JOB **#2** TOP GUN JOB

System, Network, and/or Web Penetration Tester*

"You can be a hacker, but do it legally and get paid a lot of money!"

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

- "There is nothing like finding the magic back door that everyone says isn't there!"
- "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. Eventually, you become the 'go-to' person."

** Common starting point for people who become Top Guns. Sophisticated pen testers are considered Top Guns.*

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.

SANS Courses Recommended

- SEC408: Computer Forensic and E-discovery Essentials
- SEC508: Computer Forensics, Investigation & Response (GCFA)
- SEC610: Reverse-Engineering Malware – Malware Analysis Tools and Techniques (GREM)
- *SANS Forensics Summit*

Why It's Cool

- "Knowledge is power. Sophisticated skill set that very few security staff possess. You are called out for the serious breaches. And if you are good, you will no doubt be a millionaire some day."

How It Makes a Difference

- "Now we're getting to the top of the heap. This job requires the analyst to "go deep" into a system, find out what went wrong and what's still wrong, and trace it out to the perpetrators as well as to recommend fixes. This requires a high level of skill and knowledge, and some intricate reasoning and analysis."

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 techniques.

Become expert in knowing how to search networked file and email servers to respond to civil litigation e-Discovery requests. Visit Websites such as forensics.sans.org, a site on which new Websites, blogs, Webcasts, and information are routinely updated. Network with law enforcement via your local Infraguard chapter and at forensic conferences.

Become a master system administrator. You should understand where log files, user files, and how computer operating systems work.

Keep an investigator's mindset. This analyst can piece together what happened on a computer system, and is always thinking about how the evidence could be challenged by opposing council.

A master forensic analyst is an excellent presenter. You must be able to present technical data in an understandable way to management, law enforcement, or a jury. Practice presenting forensic or information security topics, at conferences when possible, and both in writing and public speaking. When you uncover evidence, immediately think about how the evidence would best be presented and how it could be cross-examined.

-Rob Lee, Forensic/Incident Response Faculty,
SANS Principal Consultant, Mandiant INC.

#4
Incident Responder

"Like the secret agent of tech geekdom."

How to Be Successful

You should be familiar with techniques where you can quickly analyze malware found on your network using reverse engineering, network analysis, and digital forensics. A skilled investigator can examine malware and network signatures to create malware indicators that are deployed within an organization's network and systems in order to discover additional systems that may have been breached.

Know your network.

Train on collecting network data from firewalls, IDS/IPS systems, servers, and proxy devices on your network in order to correlate network data. Spend some time getting to know and analyze the network's layout. Identify and assess your critical assets.

Know your systems.

Practice collecting live data from systems including processes, open ports, log files, and network connections. Identify systems that contain sensitive data such as payment card information or personal identifiable information.

Know your team.

Prepare your team and your organization for an eventual incident. "Red-team" your organization with a scripted incident to gauge the response of technical and management teams. Ensure that your team is equipped with techniques and tools needed to respond to multiple systems simultaneously.

Know your enemy.

You should assess your threats. Why would an attacker breach your network or system? Analyze what the attackers might seek to gain by obtaining access to your infrastructure. Predict where an attacker might go.

-Rob Lee, Forensic/Incident Response Faculty,
SANS Principal Consultant, Mandiant INC.

Job Description

When the security of a system or a network has been compromised, the incident responder is the first-line defense during the breach. The responder not only has to be technically astute, he/she must be able to handle stress under fire while navigating people, processes, and technology to help respond and mitigate a security incident.

SANS Courses Recommended

- SEC408: Computer Forensic and E-discovery Essentials
- SEC504: Hacker Techniques, Exploits & Incident Handling (GCIH)
- SEC508: Computer Forensics, Investigation & Response (GCFA)
- SEC558: Network Forensics
- SEC610: REM – Malware Analysis Tools and Techniques (GREM)
- ***SANS Forensics Summit***

Why It's Cool

- "This may be the top of the 'top gun' jobs because it lets you move into a cooler, analytical environment where you can go deep with your knowledge."

How It Makes a Difference

- "These guys can stare down certain death... er, in the form of a complete system failure. They trump the operations guys and keep the system from being put back on the network and make sure everyone is coordinated. They're the coolest cucumbers in the garden cause while everyone else is running around shouting "the system's dead" they have the sense to rationally figure out why."

TOP GUN JOB **#5** TOP GUN JOB

Security Architect

"This job has real reach into the industry and into the future. Here is where you make a real difference."

Job Description

This expert understands business needs as well as technology and environmental conditions (e.g., law and regulations), and can translate them into a security design that allows the organization to efficiently carry out its activities while minimizing risk.

SANS Courses Recommended

- SEC501: Advanced Security Essentials – Enterprise Defender (GCED)

Why It's Cool

- "You get to design the solution, and not just for the perimeter."
- "You get to work with all the tech experts as a team, to plan the technology directions."
- "You get to research and play with new 'toys' all the time."

How It Makes a Difference

- "This is the individual who makes or breaks actual systems, protocols, and applications. Here one makes business bloom or wither. Significant power, great responsibility, like a navigator of a ship."
- "You run the show -- security is in your hands. Can you design a system and operational support mechanism that can stand the attack of the Bad Guys on the most dangerous network out there, the Internet? Prepare to step up to the challenge and use every bit of experience and knowledge you have accumulated because it will be tested, and not by only friendly fire."

How to Be Successful

Understand the business in terms of what is really critical for its survival and success – the exposure, threats, associated risks and the environment (applicable standards, compliance, good practices, legal requirements, etc.), generic or industry-specific.

The core task is to design the optimum combination of security measures, made up of protection, detection and response processes and technologies. Stay up-to-date with the current security strategies and technologies, and with the different products on the market, commercial or open source.

Be sure to encompass all security aspects in the organization, including all types of assets: physical security, network security (Firewalls, WAF, IDS, UTM, etc.), host & device security (Windows, UNIX, IOS, etc.), application security (C, PHP, Java, ASP, etc.), data security (databases, storage, etc.) and user security (authentication, awareness, etc.).

Make sure you know what the current security threats are, how they are exploited, and what the most effective strategies are to stop them. Training in hacking techniques will enable you to understand the security assessment reports that will contribute to the security architecture redesign of existing IT infrastructures, which is the majority of the cases.

In sum, the Security Architect must be able to design the appropriate operations processes to ensure that the security level achieved in the initial design is maintained over time. Understanding the different tasks that a typical Security Operations Center carries out can be the best way to learn how to design those processes.

-Jess Garcia, Security Analyst, One eSecurity

#6

Malware Analyst

"Only go here if you have been called. You know who you are."

How to Be Successful

Three suggestions for becoming a good malware analyst:

Recognize your strengths and weaknesses.

A skilled malware analyst possesses expertise from programming as well as system and network administration. Most individuals are stronger in one of these areas than the other so start with the tasks that build upon your strengths, and develop a plan for expanding your expertise in weaker areas to ensure a well-balanced skill-set.

Stay abreast of the threat landscape.

Research and understand new threats by reading blogs, books, and papers that discuss malware characteristics and analysis techniques. Attend conferences where you can brainstorm with and learn from other malware analysts.

Contribute to the malware research community.

Share your insights, findings and suggestions with other analysts via mailing lists, blogs, web forums, conferences, and other venues. You will not only contribute to the community's joint skill set, but also interact with peers who can share their perspectives and help you become the analyst you want to be.

-Lenny Zeltser (www.zeltser.com)

Job Description

A malware analyst examines malicious software to understand the nature of the threat. This usually involves reverse-engineering the compiled executable to figure out how the program interacts with its environment. The analyst may be asked to document the specimen's attack capabilities, understand its propagation characteristics, and define signatures for detecting its presence.

SANS Courses Recommended

- SEC610: Reverse-Engineering Malware – Malware Analysis Tools and Techniques (GREM)
- SEC709: Developing Exploits for Pen Testers & Security Researchers
- ***SANS Pen Testing Summit***

Why It's Cool

- "It's a very exclusive club. You can't go to a class and suddenly do this job. This is the 'bad boy/girl' character archetype. This person could be a successful criminal, but chooses to be one of the 'good guys' instead."

How It Makes a Difference

- "Take your skills into a place and figure out everything that can go wrong, and tell them about it, and make sure they listen. The suits and movers and shakers will be strongly motivated to say there's nothing wrong, and you have to spoil their pipe dream. Maybe they have holes, and maybe there's already some bad code in the middle of the thing. You have to tell them – and prove it! Could be pretty cool, because now you're a mover and shaker too."

#7
Network Security Engineer*

"If there's one indispensable person, it's the network person. This is where the action is."

Job Description

Responsible for designing, implementing and managing a network so that proper security is built into the overall infrastructure. This expert not only understands routers and switches, but has a detailed knowledge of firewalls, IDS, IPS, VPN and other critical security components. Understanding both network principles and security allows the network security engineer to build a robust network that provides proper functionality and the correct level of security.

SANS Courses Recommended

- SEC401: SANS Security Essentials Bootcamp Style (GSEC)
- SEC501: Advanced Security Essentials – Enterprise Defender (GCED)
- SEC502: Perimeter Protection In-Depth (GCFW)

Why It's Cool

- "This cyber-warrior is on the front line and has to have nerves of steel and high intellect. It's cool because either you have the DNA for it or you don't. It's a very exclusive club."

How to Be Successful

Communication

You can have all of the knowledge in the world and the best process and technology but if you cannot communicate and speak the language of the people you are talking with, you will be ineffective. If you send out emails or speak up in meetings and everyone just smiles as if you hadn't said anything, you are talking, but not communicating. If you work in security, the most important part of communication is to be able to effectively translate between business goals and technical risks. If you cannot explain to management why something is important they will not fund it.

-Dr. Eric Cole, Security Consultant and SANS Fellow

How It Makes a Difference

- "Rubber-meets-the-road job where security skills meet business needs. Screw up, and your company is owned."
- "Oftentimes you are the one called in to explain why something happened and how you're going to prevent it from happening again. If you're a thrill seeker, then this really is the job for you."
- "You get to help discover and set policy and then ultimately you get to fix the problem."
- "Management ALWAYS needs their network up and operational."
- "You have to know so much, and yet, that's what makes you so valuable to everyone. If you like being the center of attention and being asked to come up with a solution, then you'll like this job."

** Common starting point for people who become Top Guns*

#8
Security Analyst

“High-level protection. You’re setting the practices that keep companies out of the news.“

How to Be Successful

You are the go-to person for not only explaining threats and vulnerabilities, but for coming up with techniques to mitigate flaws. Critical for success is your ability to communicate with diverse audiences, from high-level management to technical engineers, using written and oral formats.

A technical aptitude is a necessary part of the individual filling this role. With no limit to the number of technical specifications that can introduce flaws, you have to be able to quickly study and understand the protocols, specifications and technology that pose a threat to the organization.

As a security analyst, you will have a greater understanding of technology and security threats than most of your peers. With this information comes the responsibility to share your knowledge to help increase your co-workers’ security skill set, significantly improving the overall security of the organization. From a technical perspective, your analysis and research keep you at the cutting-edge of security and information systems, a widely respected position in any company.

-Josh Wright, Senior Security Analyst,
InGuardians, Inc.

Job Description

Responsible for research and analysis of security threats that may affect a company’s assets, products or technical specifications. This analyst will dig into technical protocols and specifications for a greater understanding of security threats than most of his/her peers, identifying strategies to defend against attacks through intimate knowledge of the threats.

SANS Courses Recommended

- SEC501: Advanced Security Essentials – Enterprise Defender (GCED)
- SEC503: Intrusion Detection In-Depth (GCIA)
- SEC560: Network Penetration Testing and Ethical Hacking (GPEN)
- ***SANS Pen Testing Summit***

Why It’s Cool

- “It is the only clear path to the real top gun of security: chief information security officer.”
- “You get to write the policies and standards that the entire organization must abide by, or else. This job gives you visibility within the organization. You get to work with senior management. Often you manage the monitoring and compliance to policy of the organization.”

How It Makes a Difference

- “If you want to make a difference but don’t necessarily want all the managerial BS, this is the job for you.”
- “Creating policy that becomes the backbone of the entire organization; teaching both end users and management about security and security solutions; consulting on latest company projects to build in security from the start; evaluating the latest technology to provide training and consulting solutions.”

#9
Computer Crime Investigator

"Brain and badge? That is the coolest."

Job Description

Computer crime investigators include both 'sworn' law enforcement officers and 'un-sworn' employees of departments who are dedicated information security investigators. Both are entrusted with the preservation, acquisition, storage, detailed analysis, and clear reporting of digital evidence from many sources: from audio to data bases, e-mail to financial data, pictures and beyond – almost every contemporary crime has some digital evidence.

SANS Courses Recommended

- LEG523: Legal Issues in Information Technology and Information Security (GLEG)
- SEC408: Computer Forensic and E-discovery Essentials
- SEC427: Browser Forensics
- SEC504 Hacker Techniques, Exploits & Incident Handling (GCIH)
- SEC508: Computer Forensics, Investigation & Response (GCFA)
- SEC560: Network Penetration Testing and Ethical Hacking (GPEN)
- SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)
- ***SANS Pen Testing Summit***
- ***SANS Forensics Summit***

Why It's Cool

- "Ability to catch the bad guys...the end result is a rush."
- "This is where the geeks among us can really show up the jocks."

How to Be Successful

While there is no path to becoming an Information Crime Investigator, acquiring the following skills will improve your chances. Certify in computer or digital forensics. Learn about network security fundamentals – more and more evidence is being gathered in networked environments. Know your local, state, or regional law enforcement requirements for technical support staff. Join groups like InfraGard and HTCIA to learn about the field and emerging investigative challenges. Check local and online college and university courses in Criminal Justice that focus on digital investigations. Attend conferences on digital investigations and a rapidly emerging parallel field, eDiscovery for lawyers. Read the results of the current legal cases. Speak with as many people as possible in law enforcement, especially those directly involved in digital investigations.

-Bob Hillery, Co-founder & Senior Security Analyst, InGuardians, Inc

How It Makes a Difference

- "The final step in catching the Bad Guys is yours to do."
- "The coolest job ever when you're working for the federal intelligence community. Your job is to deter, detect, and neutralize or exploit threats to national security by people who would use computer technology as the means or object of espionage, sabotage, or terrorism. You must possess all of the skills of the preceding job titles because you will often work alone or undercover. You are called upon when the stakes are high and failure is not an option."

#10
CISO/ISO or Director of Security

"Seems like I can get a lot done with little to no push back"

How to Be Successful

Organizations succeed by taking risks, and they frequently fail because they then don't manage the risk-taking very well. The risks are business risks, and the security team needs to see business constituencies as "customers". The "this is how it's always worked" idea must be discarded. Data-driven decisions, devolving perimeter, any-device thinking, collaboration technologies, virtualization, and mobile data are diametrically opposed to prior thinking. Today's solutions are tomorrow's threat, and global and geopolitical landscape shifts are tightly coupled to intellectual and informational threats.

Experience is often the training ground, and diverse thought along with scenario planning is the requirement for a good outcome. Focus on the business goals: Never forget that this is the basis for security thinking.

How It Makes a Difference

- "You have the creative direction to influence and directly contribute to the overall security of an organization. You are the senior security player, the only one whom the CEO will trust."
- "This position usually reports at a very high level, and gets to see and influence the big picture. You work with physical security, IT, the businesses, even the FBI and other law enforcement agencies."
- "You are da Boss. You can pick and choose who does what, what gets done, and motivate and then share the credit with your people. You make a real impact on a daily basis."

Job Description

Today's Chief Information Security Officers are no longer defined the way they used to be. While still technologists, today's CISO/ISO's must have business acumen, communication skills, and process-oriented thinking. They need to connect legal, regulatory, and local organizational requirements with risk taking, financial constraints and technological adoption.

SANS Courses Recommended

- MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam (GISP)
- MGT504: Hacking For Managers (GCIM)
- MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™ (GSLC)
- MGT525: Project Management and Effective Communications for Security Professionals and Managers (GCPM)

Why It's Cool

- "Authority always wins."
- "These people get to decide where to build the "watch towers", how many rangers are stationed in the park, where fires can be safely built, and the rules of engagement."

TOP GUN JOB **#11** TOP GUN JOB

Application Penetration Tester

"You're an 'ethical hacker'. It takes equal parts technical ability and creativity."

Job Description

This expert contributes an integral piece to the company's software development life cycle. He/she does everything from developing code to reverse-engineering binaries to examining network traffic.

SANS Courses Recommended

- DEV422: Web Application Security Essentials
- SEC542: Web App Penetration Testing and Ethical Hacking (GWAPT)
- SEC560: Network Penetration Testing and Ethical Hacking (GPEN)
- ***SANS Penetration Testing & Ethical Hacking Summit***

Why It's Cool

- "Combines applying different thought processes to system analysis with exploration tools, and a sort of dangerous level of knowledge."

How It Makes a Difference

- "We desperately need more of these experts – this has been such a black hole for so long."
- "The application pen tester must think like an attacker to make the application perform the goal they are trying to accomplish. It takes equal parts technical ability and creativity to become a top notch application pen tester."
- "This job is out on the leading edge, and where most of the action and vulnerabilities are. This job requires a very full skill set."
- "This job rocks because it is always easier to break someone's stuff than it is to secure it."

How to Be Successful

As applications are designed and developed, the application pen-tester needs to adjust testing and evaluation to the stage the application is in, and then evaluates the application and its security posture by examining all of its parts and processes. This will involve the application, its code base and its surrounding environment.

To be the best of the best, you need to understand the languages used to develop the applications, the strengths and weaknesses inherent in the chosen language, the interactions the language provides with the environment, and the development tools used and how they generate the applications. And one more thing – since a large number of applications moving into environments are brought in from a vendor, the application pen-tester needs to understand the purchasing process, and be able to review contracts.

-Kevin Johnson, InGuardians, Inc.

TOP GUN JOB **#12** TOP GUN JOB

Security Operations Center Analyst

"This person is part human guard dog of the network and part cyber-detective."

How to Be Successful

One of the best assets for success is curiosity – a healthy sense of paranoia that makes you continually wonder whether the bad guys are outsmarting you. You need a zest for investigating the unknown, a strong sense of pride and a relentless commitment to defend your network with a 'not-on-my-watch, not-on-my- network' attitude.

You're almost guaranteed job security since writing secure code hasn't always been a priority. Legacy code is rife with vulnerabilities and development of new protocols and applications appears prone to repeating past mistakes. But this also means that you need to be willing to learn and stay apprised of new methods for exploiting and prevention.

Finally, it helps if you are not daunted by a job that requires you to multi-task and prioritize. If you work in a larger group, you have to function well as a team member. The demands are great, but there is no better reward than knowing you've successfully defended your network by outsmarting and thwarting the efforts of the hackers.

-Vern Stark, Principal Network Security Engineer, The Johns Hopkins University Applied Physics Laboratory and Judy Novak, Senior Research Engineer, BAE Systems

Job Description

This analyst is entrusted with configuration, customization, and examination of output from security tools and software installed on the network. The job requires an understanding of network traffic in general, insight into site-specific traffic and protocols, and an awareness of Internet threats.

SANS Courses Recommended

- SEC502: Perimeter Protection In-Depth (GCFW)
- SEC503: Intrusion Detection In-Depth (GCIA)
- SEC504: Hacker Techniques, Exploits and Incident Handling (GCIH)
- SEC560: Network Penetration Testing and Ethical Hacking (GPEN)
- *SANS Pen Testing Summit*

Why It's Cool

- "Fire rangers...if they don't catch the initial blaze, there goes the forest. These are the guys who see the trees in a forest of information."
- "This cyber-warrior is on the front line and has to have nerves of steel and high intellect."

How It Makes a Difference

- "You're at the heart of the IT operation and have a good handle on all that is occurring on your network."
- " These are the people that really keep the organization secure. Sometimes all they get are little bits of information, but when collected from multiple sources, they see the big picture concerning possible attacks or breaches, and the overall security posture of the organization."

#13
Prosecutor Specializing in InfoSec Crime

*"The 'Bad Guys' are smarter, harder to catch.
The folks that can actually get convictions have to be smarter still."*

Job Description

Government attorney who guides law enforcement investigations into computer crimes and represents the State in lawsuits against defendants accused of technology crime.

SANS Courses Recommended

- LEG523: Legal Issues in Information Technology and Information Security (GLEG)
- SEC401: SANS Security Essentials Bootcamp Style (GSEC)

Why It's Cool

- "Information Security Crime is high dollar compared to Armed Robbery."
- "Very Cool, courtroom presence empowered to send the bad guys off to prison!"

How It Makes a Difference

- "Attorneys are talking heads...but anyone who can consistently get convictions for information crime or claim a case that sets a precedent is a god among men! All hail the successful Prosecutor Specializing in Information Security Crime!"

How to Be Successful

This expert attorney must be broadly conversant in the field of information technology. He needs a curious mind, and is constantly seeking to keep abreast of the latest developments in digital equipment and the applications that society adopts. A successful computer crime prosecutor will need a nimble intellect, a strong background in computer forensics, and the ability to understand new ideas and practices as changes in law and technology challenge old assumptions.

To be effective as a prosecutor, an attorney needs personal integrity, as well as a sense of duty to uphold justice, recognizing both society's need for protection and the value of individual civil rights.

The best prosecutors have a talent for working in teams of diverse professionals, including accountants, forensics specialists, police officers, other attorneys and security experts. At the same time, the prosecutor will be comfortable as a scholar of law, demonstrating skills for research, analysis and balanced judgment. He or she will also be able to distill complex information into a simple and articulate explanation of law, facts, technology – talented with both written word and spoken language.

-Benjamin Wright, Attorney,
(benjaminwright.us)

TOP GUN JOB **#14** TOP GUN JOB

Technical Director and Deputy CISO

"Top technical dog. Managing and directing the analysts and engineers that make info security happen."

How to Be Successful

Security changes rapidly so you have to stay current in order to leverage technology wisely. The best security technical directors also focus on the technology that is already in place. Most organizations find out they have suffered a breach of security from outside notification, and if your security budget is 5% of IT, that just does not wash. All of the tools can work, but it requires focus and training to make them work, just plugging them in is not enough.

You will be responsible for understanding the trends in security. Attend the larger trade shows, RSA, Interop and SANS 2009, and invest time in speaking with the vendors. Collect business cards, maintain the dialog with vendors, listen to webcasts by the security vendors. Keep asking questions.

Learn about the business logic at your organization -- you are there to help protect its valuable intellectual property. Be part of the eDiscovery team, or stay on top of what they are learning. Know where your valuable intellectual assets are, what the information flows are, and make sure the technology is deployed to protect the information. Attend business meetings. Have lunch with internal audit once at least one a month, and maintain a dialog about process and control.

-Stephen Northcutt, President,
The SANS Technology Institute
(www.sans.edu)

Job Description

This expert has to be a strong support for the CISO, you have to succeed at the famous People-Process-and-Technology triangle. You have the enviable role of technology focus, but never forget people and process.

SANS Courses Recommended

- MGT404: Fundamentals of Information Security Policy
- MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam (GISP)
- MGT504: Hacking For Managers (GCIM)
- MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™ (GSLC)
- MGT525: Project Management and Effective Communications for Security Professionals and Managers (GCPM)

Why It's Cool

- "The guy that actually "does the work" that makes the security office run smoothly. Making decisions and making things happen. That's coolness."

How It Makes a Difference

- "For the technologist in any company, this job is nearly the top of the technology ladder from a hands-on perspective. With a high level of strategic thinking and the additional enabling of direct involvement in solution design and deployment, this person holds or has access to virtually every key to the technology infrastructure when it comes to contribution and ability to influence."

#15
Intrusion Analyst

"You are the gate keeper – as the intruders are trying to find ways into your network, it is up to you to close the doors."

Job Description

This analyst is responsible for monitoring traffic, blocking unwanted traffic from and to the Internet, and dealing with attackers. Firewalls and IPS technology are the starting point for hardening the network against possible intrusion attempts. Knowledge in firewall policies and functionality is crucial in network security.

SANS Courses Recommended

- SEC401: SANS Security Essentials Bootcamp Style (GSEC)
- SEC502: Perimeter Protection In-Depth (GCFW)
- SEC503: Intrusion Detection In-Depth (GCIA)

Why It's Cool

- "Almost nobody in the general populus knows what this stuff is, but they know it's critical and can only be done by skilled, motivated, specialists. It's cool because either you have the DNA for it or you don't. It's a very exclusive club."

How It Makes a Difference

- "Nothing is better than a good IPS, nothing is worse than a bad IPS. This is such a critical point in the network that managing it effectively is one of the more important tasks in the company."
- "Not only are you protecting the perimeter, but you are also watching traffic on the inside for threats in real time. You are on the edge, doing what it takes to make the company safe."

How to Be Successful

A successful Intrusion Analyst likes to answer puzzles, solve riddles, and analyze mysteries. You need to have strong technical and analytical skills. An Intrusion Analyst will often work alongside HR and Legal conducting investigations and performing analysis. It is vital to have deep business insight in order to comprehend the impact of an incident on an organization.

Logs, logs, logs. If you were to pick one place to learn about your network, systems, and applications it would have to be logs. Start small and look through logs for 30 minutes a week. Document your operational wins. One day it may be that you silenced chatty printer UPNP announcements, improving network performance. On another bright log filled day, you might catch an intruder stealing company documents right off the network file server. Logs to start with: Syslog, Microsoft Event logs, Web server, File Server, and application server logs, Firewall, IPS, IDS, and Netflow.

Always keep in mind the importance of your task. Many investigations may lead to civil or criminal proceedings, furthering the impact your analysis will have. Keep up to date with the latest trends by participating in Dshield, reading the Internet Storm Center, Shadow Server, Securityfocus, and the Honeynet Project. There are thousands more options to choose from, but these sites consistently deliver new content and are on the pulse of the Internet.

-Mike Poor, Co-Founder and Senior Security Analyst, InGuardians, Inc

TOP GUN JOB **#16** TOP GUN JOB

Vulnerability Researcher/Exploit Developer

"Wow factor – I can't believe (s)he actually does that. Talk about thinking outside of the box!"

How to Be Successful

First, you need the patience to step through the initiation process. All of the vulnerability scanning tools, penetration testing tools and Proof-of-Concept (PoC) exploit code publicly available are great to leverage, but you must become one of the developers of these tools. Start by researching vulnerabilities on platforms that provide little protection against exploitation. Once you understand how, what and why your efforts are successful, you can move on to a newer platform.

The goal of any programmer is not to introduce vulnerabilities that can be exploited. It is your job to poke and prod at every possible location where execution may be affected. Commonly known as fuzzing, this process helps you to identify potential locations within a program that may be vulnerable to an unexpected exception, Denial-of-Service (DoS) or possible code execution. It also requires you to disassemble the program, reverse engineer it and analyze its behavior when running in a debugger.

Some tips on getting started:

Pick a language such as C and get familiar with functions, forking & threading, pointers and overall program behavior; pick a platform such as Linux or Windows to start. Analyzing both simultaneously can be counterproductive; start walking a simple program such as "Hello World" through a debugger and disassembly; become familiar with debuggers such as GDB, OllyDbg and ImmunitySec. Take an older exploit that has been publicly disclosed, get it to work properly and understand why and how it works. Try not to get frustrated. Everyone in this field has been there and many researchers will help you get to the next step.

-Stephen Sims, Certified SANS Instructor

Job Description

This expert is responsible for making the absolute declaration that an application or the OS the organization is using or considering, is safe or unsafe. (S)he identifies weaknesses in both public and home-grown applications, and develops Proof of Concept (PoC) code to validate the findings.

SANS Courses Recommended

- SEC503: Intrusion Detection In-Depth (GCIA)
- SEC542: Web App Penetration Testing and Ethical Hacking (GWAPT)
- SEC560: Network Penetration Testing and Ethical Hacking (GPEN)
- SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)
- SEC709: Developing Exploits for Pen Testers & Security Researchers
- ***SANS Pen Testing Summit***

Why It's Cool

- "You are providing proactive approaches to security, finding out how much damage and what type has been done in order to keep systems secure and up and running. To prevent damage is a cool job."

How It Makes a Difference

- "This work has input into the system design process as well as the review and analysis of an existing system. Since you have to be on top of all the current threats, you have a pretty wide-ranging role and are kind of on your own."

#17 Security Auditor

"This should be listed as a top gun job. With the Wall Street fiasco, auditors are going to be very sought after."

Job Description

Management depends on this expert to measure and report on risk to the organization by measuring compliance with policies, procedures and standards. These experts are among the few in the organization, who are actually asked for their honest opinion on what could be improved or done better to make the organization more efficient and profitable through risk management.

SANS Courses Recommended

- AUD410: IT Security Audit and Control Essentials (GSAE)
- AUD507: Auditing Networks, Perimeters, and Systems (GSNA)
- SEC401: SANS Security Essentials Bootcamp Style (GSEC)

Why It's Cool

- "How cool is it to have people fear your report. CIOs tremble, Finance VPs shake. This job can offers an opportunity for travel, high pay, and the opportunity to help a lot of organizations or divisions."

How It Makes a Difference

- "You get to find the holes and recommend patches to get the company safe."
- "You have a helicopter view of a company and interact with all levels."

How to Be Successful

Above all else, a Security Auditor needs to be an effective communicator. This means that we must be able to express ourselves clearly and in an interesting way to both management and to the technical staff in the organization.

The second most important trait is twofold: first, a significant level of technical competence so that we can effectively evaluate controls, recommend controls and determine whether those in place are actually working to meet the security and audit objectives. The second part is a level of modesty – we have to be able to admit to ourselves and others that we need to rely on technical staff to really understand how the technical controls function, and to leverage these individuals to expand our own knowledge base, rather than pretending to know everything.

Perhaps the third most important quality for a successful Security Auditor is sincere interest and diligence. We must not settle for easy answers. We must be willing to dig for the truth regardless of the effort involved and have the determination to develop partnerships within the business that will allow the entire organization to work together to achieve higher levels of excellence and, as a result, lower levels of risk.

-David Hoelzer, Director of Research, Enclave Forensics, (dhoelzer@enclaveforensics.com)

#18
Security-savvy Software Developer*

"Kool, because this is VERY rare."

How to Be Successful

The role of security-savvy software developer is challenging and rewarding from multiple perspectives. To be successful, you must understand a multitude of attack vectors used to exploit software to avoid the introduction of flaws. This experience is also needed to leverage the same attack tools and techniques an adversary might use to exploit your software, identifying flaws to be addressed before product shipment.

In a development role, your position will be vital to the company's success, including your ability to communicate the techniques used for secure software development to your peers. This can be challenging, since few enjoy having their work criticized and flaws identified, but is a necessary component of an overall secure software strategy. This role is critical to not only the success of the company, but also to all the customers who implement your software. Secure software development has a direct and undeniable impact on the ability of an organization to protect their systems and information assets, and you play a key role in that success.

-Joshua Wright,
Senior Security Analyst, InGuardians, Inc.

Job Description

The security-savvy software developer leads all developers in the creation of secure software, implementing secure programming techniques that are free from logical design and technical implementation flaws. This expert is ultimately responsible for ensuring customer software is free from vulnerabilities that can be exploited by an attacker.

SANS Courses Recommended

- DEV422: Web Application Security Essentials
- DEV541: Secure coding in Java/JEE: Developing Defensible Apps (GSSP-JAVA)
- DEV544: Secure Coding in .NET: Developing Defensible Apps (GSSP-.NET)
- DEV545: Secure Coding in PHP: Developing Defensible Apps

Why It's Cool

- "You get to make something that actually runs and does something (and won't break under pressure)."
- "These guys are the senior developers by virtue of their programming prowess."

How It Makes a Difference

- "No security architecture or policy can compensate for poorly written, buggy, insecure software. If one pays the necessary attention to security when a product is initially developed, one doesn't need to go back and add security later on."
- "This is where the rubber meets the road. These are the people making a difference where it really matters...in the software that runs the world."

** Often a stepping stone to a Top Gun job.*

TOP GUN JOB #19 TOP GUN JOB

Security Maven in an Application Developer Organization

"Maven? Just about the best position in this list. You're a programmer and a security engineer and a manager all wrapped up in one. Too cool."

Job Description

Development expert and security activist, the main function of this expert is to proactively and continuously improve security within the development lifecycle. An important part of that is persuading your colleagues to exercise best practices and avoid the security pitfalls in software development.

SANS Courses Recommended

- DEV422: Web Application Security Essentials
- DEV541: Secure Coding in Java/JEE: Developing Defensible Apps (GSSP-JAVA)
- DEV544: Secure Coding in .NET: Developing Defensible Apps (GSSP-.NET)
- SEC401: SANS Security Essentials Bootcamp Style (GSEC)
- SEC542: Web App Penetration Testing and Ethical Hacking (GWAPT)

Why It's Cool

- "One of the best jobs of all, you write your own job description, multiply yourself through younger people, and leave operational stuff to others. If you are lucky, then you have no Blackberry either."

How It Makes a Difference

- "Here's where the developers get to strut their stuff. You've spent hours learning about the latest vulnerabilities and how to prevent your applications from being susceptible to them. Now, you get to pass this knowledge on to the rest of your team so they become better developers. You can mentor your co-workers, tackle tough assignments that need security built in, and explain to marketing people why a certain feature is not compatible with security."

How to Be Successful

To be successful, the first requirement is to earn respect from your colleagues. The maven must persuade and impress the others to practice security in development. Respect doesn't come automatically in a development organization – it must be earned over time and through hard work.

Having superior security knowledge is a basic requirement, but even when you have this knowledge, others won't necessarily come to you for advice. For that you need relationship-building and inter-personal skills. You have to make the development crew feel that you are fighting on their side, and that your focus is on security. If your colleagues feel that you are just an enforcer of security policies, you will fail miserably.

Application security changes rapidly. Make sure you stay current with the latest news and trends on attack and defense techniques. Stay on top of the recent features in your development platforms, especially on security features. When others come to you for security advice, you should be well prepared and able to give them the best possible security solutions.

-Jason Lam, Security Analyst, Major Financial Company

#20
Disaster Recovery/Business Continuity Analyst/Manager

"You are on the front line when the bombs are falling."

How to Be Successful

Every time there is a major disaster – the attacks of 9/11, Hurricane Katrina – we find examples of organizations that learned their Continuity of Operations Plans (COOPs) had failures. We rely on Disaster Recovery/Business Continuity analysts and managers to keep this to a minimum.

They have to focus on a number of threats ranging from natural disasters, epidemics, terrorism (not so much an actual terrorist act, although it is an important consideration, but the secondary effects of terrorism, such as impact on air travel, and therefore business), to malware, insider attacks, and espionage.

The best DR/BC analysts and managers have a strong security background because anytime there is a disaster, there is a potential security exposure. Basic skills include facilitating and coordinating Disaster Recovery and Business Continuity Plan activities. This is usually done in conjunction with an organization's Information Technology division, but should also be coordinated with Information Security. Tasks include testing, contract reviews and negotiations, equipment and strategy analysis, and plan creation, analysis and maintenance.

-Stephen Northcutt, President,
The SANS Technology Institute
(www.sans.edu)

Job Description

These experts ensure that strategic, long-term and tactical recovery plans are identified, developed, maintained, and successfully tested for business essential systems. Some DR/BCP Professionals may be involved in reviewing and maintaining DR contracts for mission critical systems for hot, warm and cold sites. They should be very involved in planning, leading and participating in DR testing as well as reviewing and maintaining DR budget, policies, guidelines and strategies.

SANS Courses Recommended

- SEC504: Hacker Techniques, Exploits, and Incident Handling (GCIH)
- SEC508: Computer Forensics, Investigation, and Response (GCFA)
- ***SANS Forensics Summit***

Why It's Cool

- "Being able to deal with an emergency and have a plan in place so that it's not hysteria, but controlled and orderly handling of events to bring people back online – that's cool."

How It Makes a Difference

- "When a disaster strikes, everyone is looking to you for guidance and assurance. You lead the way to victory or out of the situation to bring your company back to where they were before hand."
- "Big responsibility, all kinds of contingency planning. Bad things are going to happen. This person, if any, will help us get through them, or even mitigate them in the first place."

SANS

SANS is the most trusted and by far the largest source for information security training and certification in the world. It also develops, maintains, and makes available, at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system – the Internet Storm Center.

The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. 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 provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited. This training is full of important and immediately useful techniques that you can put to work as soon as you return to your office. Courses were developed through a consensus process involving hundreds of administrators, security managers, and information security professionals, and they address both security fundamentals and awareness as well as the in-depth technical aspects of the most crucial areas of IT security.

www.sans.org

ISBN 1-56496-780-8 $5.00

53000

9 781564 967800

To order this brochure, go to
www.sans.org/20coolestcareers

03/09