Interested in learning more about security?

SANS Institute InfoSec Reading Room

A Survival Guide for Security Professionals

According to Northcutt, "System, Network, and Security administrators all over the world are starting to feel the effects of burnout"(1). This survival guide aims to assist security professionals to balance the responsibilities and requirements of their role to avoid stress and burnout. Security professionals are having to undertake ever-broader responsibilities in an increasingly demanding environment. To minimize the risk of burnout, security professionals must understand the latest technical, legal, and business tre...

Conrad Morgan
GSEC Online
Practical: Version 1.3(Amended December 12, 2001)
Resubmission

A Survival Guide for Security Professionals

Abstract
According to Northcutt, "System, Network, and Security administrators all over the world are starting to feel the effects of burnout"(1). This survival guide aims to assist security professionals to balance the responsibilities and requirements of their role to avoid stress and burnout. Security professionals are having to undertake ever-broader responsibilities in an increasingly demanding environment. To minimise the risk of burnout, security professionals must understand the latest technical, legal, and business trends and their implications, and they need to understand stress and how it can be managed. Ultimately, achieving success and fulfilment in the profession depends upon meeting minimum standards, setting goals for yourself and attaining certification, leveraging the benefits of the security community, and adhering to a code of professional ethics.

Cyber crime trends
The environment that shapes cyber crime motivations is increasingly hostile and unsettled. Global politics has been shaken by the events of September 11 and the US economy has slowed creating instability in the business world. These events and others are changing the motivations behind cyber crimes. Initially, hacking involved individuals whose only motivation was to explore internet technology and extend our knowledge about it. Now, organized groups are turning to the web for either financial or political gain. Organized crime and terrorist adaptation to the internet can tell us much about the future motivations of cyber crime. These groups are able to exploit the transnational nature of the internet; they operate with minimal risk and greater anonymity, with the potential for greater rewards (2). Traditional crimes like money laundering become easy and legitimate when goods are sold through online auctions for less or more than they are worth. John Horgan suggests that 'cyber terrorists' use the internet to organize complex resources on a global basis, using beliefs in politics, religion, or ethnicity to motivate cyber attacks (3).

Identifying potential attackers has become more complex as security professionals need to consider wider sympathies amongst internet users. Groups like the "Dispatchers" have targeted Middle Eastern organizations in response to the September 11 attacks on the US. "Iron Guard" who are aligned

with Hezbollah, and are sympathetic to Al Qaeda, identified the North American companies as being responsible for the US government's action. Increasingly, security professionals must also look inside. The threat is no longer some unknown outsider but a colleague, a professional, a person who has the organization's trust. As Rapalaus has suggested, the insider has knowledge, opportunity, and strong motivation and represents the most significant increase amongst cyber attacks (4). Motivations determine actions and if security professionals understand why an attacker would chose a target they have a better appreciation for the possible threats a systems is exposed to.

Developments in Cyber Law

Developments in cyber law are changing the way security professionals work. Incompatibilities between international definitions of legal codes have undermined the delivery of e-commerce. Geist argues Nations are endeavoring to impose legislation that will homogenize cyber crime laws to guarantee that law enforcement can reach cyber criminals and provide stable conditions for the success of e-commerce (5). In particular security professional must be aware of the redefining of liability. Companies and employees will become increasingly liable for their services and actions. Schneier has suggested the cost of damage caused by virus or DDOS attacks, launched from unsuspecting sites, will become the responsibility of the site not the hacker (6).

To address this emerging risk, insurers and brokers like American International Group, Chubb and Marsh are offering cyber protection policies. For example, Marsh writes endorsements for technology that covers business interruption and if a Web-hosting company crashes. They also have network-security liability which covers a policyholder if the company's Web site accidentally transmits a virus to a third party or if hackers break into a site and steal confidential information, such as credit-card numbers (7). The implications for security professionals are that employment and service contracts will be re-worded as organizations seek to transfer the risk. It will be important to understand employee or contractor obligations, and to ensure that they are clearly identifiable and appropriate.

Security professionals must understand legislation that relates to privacy and civil liberties. Companies might want to know more about their clients and law enforcement might want access to systems to collect evidence. The security professional can be caught between companies exploiting new technologies at the expense of consumer privacy, or between law enforcement agencies that employ tools like CARNIVORE to

gain an advantage in the fight against cyber crime. The Carnivore device acts like many sniffers, it listens in to network traffic and records information, however what distinguishes Carnivore is the ability to differentiate between traffic that is relevant to an investigation and ignore other traffic(8).

There are many scenarios that make demands of the security professional and that places them in danger of breaking the law. Security professionals must acquaint themselves with their rights and obligations by law. For example, to ensure that evidence they gather would be considered acceptable and that it has been collected legally. Security professionals need to know they did not commit a breach of privacy, for example, when auditing web access logs. Ultimately a security professional should appreciate the implications of national and international cyber laws so that they can fully assess the risks to themselves and the organization.

Technology trends

Security professionals should aim to have an awareness of the different technological trends. The difficulty is that the range and content of information is changing at a rate faster than anyone can keep up with. Many hacking tools are produced collaboratively and are used widely due to quick and easy access. If security professionals are to compete with hackers the defense against cyber crime will be predicated upon the security community's ability to share and access information that is accurate and timely. The source of the information must be reputable and trustworthy for it to be of real value. If the information is incorrect or out of date then it is a waste of time and an added risk for the security professional. There are many websites about security, both commercial and non-commercial, what is important is the level of security community support. CERT advisories provide up to date technical reports on new vulnerabilities and computer incidents. CERT study internet security vulnerabilities, handle computer security incidents, publish security alerts, research long-term changes in networked systems, and develop information and training to help improve security. The CERT coordination center, www.cert.org, is based at Carnegie Mellon University and is a center recognized for its excellence in internet security research. The SANS updates provide both technical and broader industry news that affects security professionals. These are regular, well researched, and major vulnerabilities are followed by the release of tools like the SNMP scan, which automatically scanned and identified SNMP vulnerabilities on the network. Further information is available from www.sans.org.

It is easy to become overwhelmed and distracted by the volumes of information. The ability to filter the relevant pieces of information and know when and how to apply them appropriately will be essential.

Certification

SANS certification ensures that the security professional has the prerequisite knowledge for managing security. For individuals, certification provides personal esteem. Certified professionals are recognised by their peers as having achieved a level of professionalism. Certification also provides the best mechanism for ensuring that the commercial perception of security professionals is of exceptional quality and value. SANS security certifications are based upon the consensus of 100 leading security professionals and therefore the curriculum is based upon the knowledge of experienced practitioners. Extra value is perceived because SANs requires a full demonstration of the mastery of the subject with strong academic requirements to ensure authenticity and originality (9).

Certification removes much of the risks of employing and it helps employers gauge value and remuneration. Foote indicates "Workers holding security certifications averaged 8.3% of base salary for skills bonus pay they received in 3Q 2001, up from 7% in the first quarter .. [they] anticipate more accelerated growth in security certification pay over the next two years..."(10). Employers know they are getting a minimum standard of skills and knowledge. Often this translates into savings, as certified professionals will make fewer mistakes resulting in better continuity of service. Certification demonstrates the security professional has enough knowledge to contribute meaningfully on a business level.

Minimum Standards

Minimum standards are a useful tool for avoiding burnout. Minimum standards provide step-by-step instructions for securing systems and are the result of consensus among the security community. Minimum standards reduce the risk of inadvertent oversight and increase the degree of accuracy in scoring systems because security professionals can cross check their work against a list and the same variables are applied consistently.

The existence of standards enables security professionals to prove levels of due care and reassure suppliers or clients that necessary measures have been taken to protect their interests. The co-operation between CIS and SANS best illustrates this process of consensus. Between them they have drawn upon examples of outstanding security standards from

organisations such as NSA and made procedures and checklists for securing Windows 2000, Cisco IOS configurations, firewalls and web applications (11).

Security professionals should be aware the process of consensus and its results are open to interpretation. Some environments and systems do not warrant the levels of effort required by these documents. Burdensome checklists might discourage their use and are no good unless enforced. Ultimately minimum standards provide expectations and guidance only, the certified professional is qualified to interpret and apply them in each environment and add value by determining what is best. Incorporating minimum standards into the daily routine will remove large degrees of uncertainty and simplify many of the complex tasks but it won't replace the knowledge provided by certification.

Information Assurance

E-commerce advantage is dependent upon the ability to ensure confidentiality, integrity, and availability. If a business is unable to maintain confidentiality, if it reveals the information that separates it from its competitors, then it loses its commercial advantage. Often what drives value in the new economy is not the product itself but the information and resources surrounding it, marketing plans, research, and sales strategies.

Trust in information is essential, if it is not reliable and the integrity not guaranteed then it has little commercial value. Imagine if Wall Street brokers could not trust the figures before them: how would they decide when to buy or sell? If the service or product is not available then businesses are unable to trade. Security professionals must learn to recognize the information assets that drive value in an organization and assist managers to understand their value and the risks.

Risk management

Security professionals should understand risk. This can be a difficult issue, since risk is relative and individuals perceive risk differently in the same context. What a security professional identifies as a risk and an opportunity to prevent major costs, a manager might dismiss as one expense among many others. The difference in these perceptions is based on the level of knowledge and understanding of internet security. Helping managers to understand requires calculating the level of risk.

Relating Vulnerabilities to Threats

The level of risk is related to the exposure of a vulnerability to a threat. Vulnerabilities are areas of

weakness, but on there own and undisturbed they do not increase the risk. Identifying vulnerabilities in operating systems and applications involves different audit processes. Networks for example, can be audited using programs like Nessusd which provides automated tests against known vulnerabilities on web servers, ftp servers, Cisco routers, windows operating systems and much more. Nessus is comprised of client server architecture. The client interface is available on Windows or Linux and the server runs on Unix machines only. Further information can be found at www.nessus.org. This enables security professionals to assess a large range of vulnerabilities across services and platforms in a short period of time.

However, no single application identifies all of the vulnerabilities, some are more common than others and should be identified as low hanging fruit and eliminated. When a threat is applied against vulnerability the level of risk increases. Threats can be identified by their vector or method of attack. The vector for many mobile code attacks is via email, or the method for delivering DDOS attacks is via network connections.

Once vulnerability and the threat have been identified it is possible to establish the cost of mitigating the risk (12). Some solutions are simple and only require patching, others require structural changes like adding equipment. These costs are best presented against the potential cost of damage. This means calculating what would be the cost of having staff and resources idle while the database is down, or the potential cost over the next year if the server went down an average number of times. Quantifying the possible risks allows managers to understand the commercial implications. With this appreciation they are better positioned to decide weather to accept, mitigate, or transfer the risk to insurers.

Creating Defense in Depth

Knowing the strengths and weaknesses of an organization helps security professionals to choose appropriate tools and strategies for defense. Brian Kenny defines defense in depth as a "..strategy[that]combines the capabilities of people, operations, and security technologies to establish multiple layers of protection … the objective is to implement defenses at multiple locations so that critical enclave resources are protected and can continue to operate in the event that one or more defenses are circumvented"(13). Security professionals create defense in depth by employing security policies, change and configuration management procedures, network security devices and anti virus software.

Policy as a level of defense
Security policies provide the primary level of defense. They communicate the expectations an organization has of its employees and suppliers. If the expectations are not clear then ambiguity can lead to mistakes. Not everyone is intent upon hacking or industrial espionage, however many people simply do not understand the implications of their actions.

Policies provide authority in the event something intentional occurs. Without management sanction there is no security. If security professionals do not have support then they will not be able to enforce or sanction individuals for subverting the requirements. Nor will security professionals be able to justify their actions in emergencies.

Policies and accompanying procedures must identify the property and processes of an organization and then prioritize their value and ongoing administration. Information assets like internal databases, internet resources, software packages, or workstations each perform a function for a business the absence of which would be a cost to the company. By identifying the requirements of the company and reducing the risks security professionals are lowering the expense side of the ledger and improving the business bottom line.

Change and Configuration Management
Security professionals can use change and configuration management to add another layer of defense. Establishing baseline configurations and performing regular comparisons of critical system variables allows the security professional to know the state of the systems at a given time. This increases the ability to manage an incident and limit the damage to the client. Change management ensures the continuity of service by structuring the change process and maintaining a normal state.

By placing limits around when and who can authorise changes security professionals improve service. Often simple rules (such as not installing service packs until a certain time has past) give an organisation the benefit of experience without the cost. Security professionals must undertake preliminary research into the changes, what is planned, what are the expected results, if it goes wrong how will you back out? Do you have checks for after the install, are all the dependent services functioning?

Security professionals need to employ change management because it reduces human error and increases the ability to know the system. By maintaining a record of changes and configurations security professionals are adding context and depth to the management of security.

Network level defense

Security professionals can gain substantial knowledge and control at the network layer. Sun Tzu suggests knowing the terrain is vital to a successful defense strategy (14). Perimeter firewalls can filter the noise coming in from the internet, thus restricting the volume and types of traffic, allowing attention to focus on permitted traffic.

A centralised stateful inspection firewall looks further into packets by considering tcp, ip and application layer information. This ensures those packets that do not comply with either expected tcp/ip behaviour or company rule bases are dropped and logged. No system will catch everything so it is wise to employ a network based intrusion detection system like snort. Snort is capable of performing real-time traffic analysis and packet logging. Snort can perform protocol analysis, content searching, matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more(15). Snort can apply further scrutiny to tcp/ip behaviour if it is employed with a mysql database. This makes it easier to correlate information across greater periods of time with more intense scrutiny. Snort is available on both unix and windows based hosts. More information can be found at www.snort.org.

Security professionals can gain granular control over communication between network resources by applying ingress or egress filtering. Ingress filtering applies rules to traffic originating from an external network and egress applies rules to traffic originating from the internal network. The ability to identify which internet protocol addresses are valid and coming from the correct source is critical for defense. For example, address spoofing involves altering the source ip address to appear as though it originated from the internal network. Egress filtering prevents routers from being tricked into forwarding malicious packets to their targets.

Egress filtering enables security professionals to provide a further layer of intrusion detection where they can detect and manage internally initiated connections that are not permitted.

Application layer

Anti virus software both on the mail server and the workstation desktop extends security to the application level. The software packages available provide thousands of signatures for known viruses and are easily managed through central management stations. Signature downloads can be scheduled for any frequency required which means organisations are able to maintain up to date signature files for the latest

viruses. Companies like Symantec, www.symantec.com, provide the ability search for a virus, source a fix, and have general documents about anti virus management.

Security professionals should understand defense strategies, employ as many barriers as is possible, and learn as much about the behaviour of the network and services so that they have the advantage of knowing the terrain.

Managing Stress

How security professionals manage stress is critical to how much they enjoy the job and the profession. The event driven nature of security work makes it acutely stressful, and security professionals are unlikely to receive any sympathy as they fight their way through the incident procedures.

Stress has costs at individual, organisational, and societal levels. Stress is likely to affect decision-making, it can cause mood swings, and it can alienate people from their colleagues. Organizational stress can be caused by poor job descriptions, lack of communications, or poor working conditions. All result in low quality of service, high staff turn over, a bad reputation and dissatisfied workers. Ultimately, security professionals risk losing confidence and allowing complacency to creep in.

Balancing demands and time management are crucial for stress management. Work in the industry is deadline-driven and crisis driven, and people want their problem resolved first. Unfortunately security priorities do not always fit other peoples and they might not appreciate the demands upon the security professional's time. Being able to identify and organize the tasks through out the day will make it easier to deal with unexpected events.

Heller insists, "Be realistic about what you can achieve in one day" (16). Take time to make a list of all the tasks required and assign them priorities, by looking at the list others can see how much security professionals have on and reassess their urgency. Is the task important? Is the job urgent, or is the project to be done at some stage?

Get a feel for any patterns in the day or working week. Are their peaks and troughs? Around this structure the day so that some of the "to do" tasks are completed, ensure that urgent ones are done, and make sure time is available to work on the important projects. If security professionals know more about their workload the easier it is to say no when a request is not possible. Enjoyment and satisfaction comes from doing interesting work as well as completing urgent tasks.

Project Management

Project management provides many techniques for reducing stress and ensuring quality. Projects differ from tasks in that they usually extend over a longer period of time, involve more people, and have more complex deliverables. Security projects are no different. Security professionals have clients, both internal and external, they have expectations both in terms of cost and service, their preconceptions will be different and their goals might be also. Security professionals also have colleagues; their motivation and levels of enthusiasm will be different at different times. Their skill levels will also vary in quality and relevance to the project too. Get a feel for each of these variables at the out set and plan for how they might impact upon the result.

Crucial to the success of a project is the goal. It must be understood and shared by everyone from clients to team members. If no one understands what they are striving for then the project will inevitably run into problems. Make sure everyone has the same understanding and expectations. Document them and get sign off from management for future reference. Make a list of all the jobs and the milestones. Assign a person who is responsible for a jobs completion and gauge their progress based on the agreed milestones. Make sure there is enough flexibility in the list to respond to unexpected events. Establish a fall back option in case all does not go to plan. As progress is made through the jobs always stop to reassess wether the project is on track.

It is essential to manage expectations. Whether it's the boss or the client give them realistic expectations, anything else is destined to fail. O'Connell uses the first law of project management as a guide. If anyone of these changes: functionality, delivery date, effort, cost then all the others will change correspondingly (17) If compromise is inevitable know what to sacrifice. Develop several options and aim for the best. A common strategy is to build room into the project proposal, for example add 10% to the cost, that way if required there is room for adjustment. To ensure that the client approves of the work use incremental delivery, stage the introduction of policies and procedures, get feed back as the project progresses. Security professionals can never plan too much, security is in the details, and professionals should attempt to plan for every eventuation before undertaking a project. Good planning will avoid a lot of stress and burnout.

Professional Ethics

Ultimately security professionals must make decisions and take responsibility for their actions. In a commercial environment, often measured by key performance indicators, the pressure to

deliver is high. The temptation is to sacrifice professional principles, quality, and liability to deliver on time.

Developing a set of professional ethics will help security professionals' focus on the important issues. While SANS is currently establishing their code of ethics the ISC2 organisation provides an ethics framework that outlines its expectations of CISSP certified professionals. The four codes of ethics direct security professionals to protect society, act honourably and legally, provide diligent and competent service, and advance and protect the profession (18).

Security professionals are responsible for insuring the safety of infrastructure and the people who depend upon it, this responsibility should not be taken lightly. Instability in infrastructure impacts on people's lives. Security professionals should endeavour to inspire public confidence in information systems and security.

Honesty is an essential ethic. The ability to be direct and fair about issues, even if it is unpopular, earns respect amongst peers in the long run. Clients also appreciate being kept up to date regardless if it is good or bad news. Ethics also provide a measure for performance and association. If a certified professional falls short of the standards and brings the profession into disrepute then removal of certification disassociates the individual from the community.

An ethical framework enables security professional to make confident decisions in the face of adversity, ethics provide reassurance when the options are not obvious, and set a level of professional expectations to aspire to.

Summary

To avoid burnout and stress security professionals need to balance increasing responsibilities and demands upon their time, skills, and knowledge. Instability and hostility in the global environment has forced businesses to demand strategic risk management knowledge from security professionals.

Demands for more skills and knowledge increases the level of stress experienced by security professionals who are unable to meet these expectations because they are working in isolation and without a complete knowledge of security management.

SANS Certification equips the security professional with a framework to deal with managing security. Understanding information assurance theories helps security professionals to focus on key issues. Knowledge of defense strategies, vulnerabilities, and threats means the security professional possesses a better appreciation of the business and technical

risks and therefore is better prepared to meet the demands placed upon them.

SANS certification provides membership to a security community that can share the burden of information management. Minimum standard checklists and vulnerability tools released by the community reduce the complexity and time involved with security administration. This improves the quality of the day-to-day job, giving security professionals time to focus strategic security management issues.

Certification also introduces security professionals to a code of ethics. These are rules that exist over and above the demands of the job. Ethics outline acceptable behaviour that ensures security professionals would not compromise their integrity. This framework reassures the security professional that they are making the right decisions.

Stress management is an area that security professionals need to become more aware of. By its very nature security management is event and crisis driven. Developing tools like time and project management will help reduce the impact of stressful events by ensuring more control over them. If security professionals take the time to learn to recognise and understand stress, how it affects professional and personal lives, they will reduce the impact stress has.

Security professionals have the tools and knowledge available to reduce the demands placed upon them. The framework provided by certification and stress management are the best tools for avoiding stress and burnout.

List of References

1. Northcutt, Stephen. GIAC Certification Update Edition 6. 2001, November 8

2. Williams, Phil. ”Organized Crime and Cyber crime: Synergies, Trends, and Responses“
http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm

3. Horgan, John and Taylor, Max. “The Making of a Terrorist”. Jane's Intelligence Review. 2001
http://www.infowar.com/class_3/01/class3_112801a_j.shtml

4. Rapalus, Patrice. “2001 Computer Crime and Security Survey". Computer Security Institute. 2001
http://www.gocsi.com/prelea/000321.html

5. Geist, Michael. "Cyber law 2002: The Next Generation". http://www.globeandmail.com/servlet/GIS.Servlets.ArticleNews/relatedstories/gam/20020103/TWGEIS3

6. Schneier, Bruce. "Important Trends Shaping Security In 2002" SANS NEWSBITES BONUS ISSUE Volume 4, Bonus Issue. January 7, 2002

7. Best, "Best's Review", January 2002, A.M. Best Company http://www.bestreview.com/2002-01/pc_lossnotes.html

8. FBI "Carnivore" 2002 http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm.

9. SANS "Can Security Certification Make a Difference?" 2002 http://www.giac.org/cert_dif.php

10. Foote, David. "Pay raises and demand for security professionals continue to outpace other IT jobs". 2001 http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci783646,00.html

11. Center for Internet Security. "Benchmarks", 2002 http://www.cisecurity.org/bench.html

12. Northcutt, Stephen & Novak, Judy. "Network Intrusion Detection: Sec Ed" 2000, Indiana, New Riders p391-395

13. Mckenny, Brian. "Defense in Depth" http://www.mitre.org/pubs/edge/february_01/mckenney.htm

14. Samuel B Griffith "Sun Tzu the Art of War" London, 1963, Oxford Press

15. Roesch, Marty. "What is Snort" 2002 http://www.snort.org/about.html

16. Heller, Robert," Essential Managers Manual"1998, New York, Dorling Kindersley p86-100

17. O'Connell, Fergus "Silver Bullet: How to Run Successful Projects" 1996, New York, Prentice Hall London. p.9

18. International Information Security Certifications consortium, "Code of Ethics" 2002, http://www.isc2.org/cgi/content.cgi?category=12

Last Updated: June 25th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London July 2018	OnlineGB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced