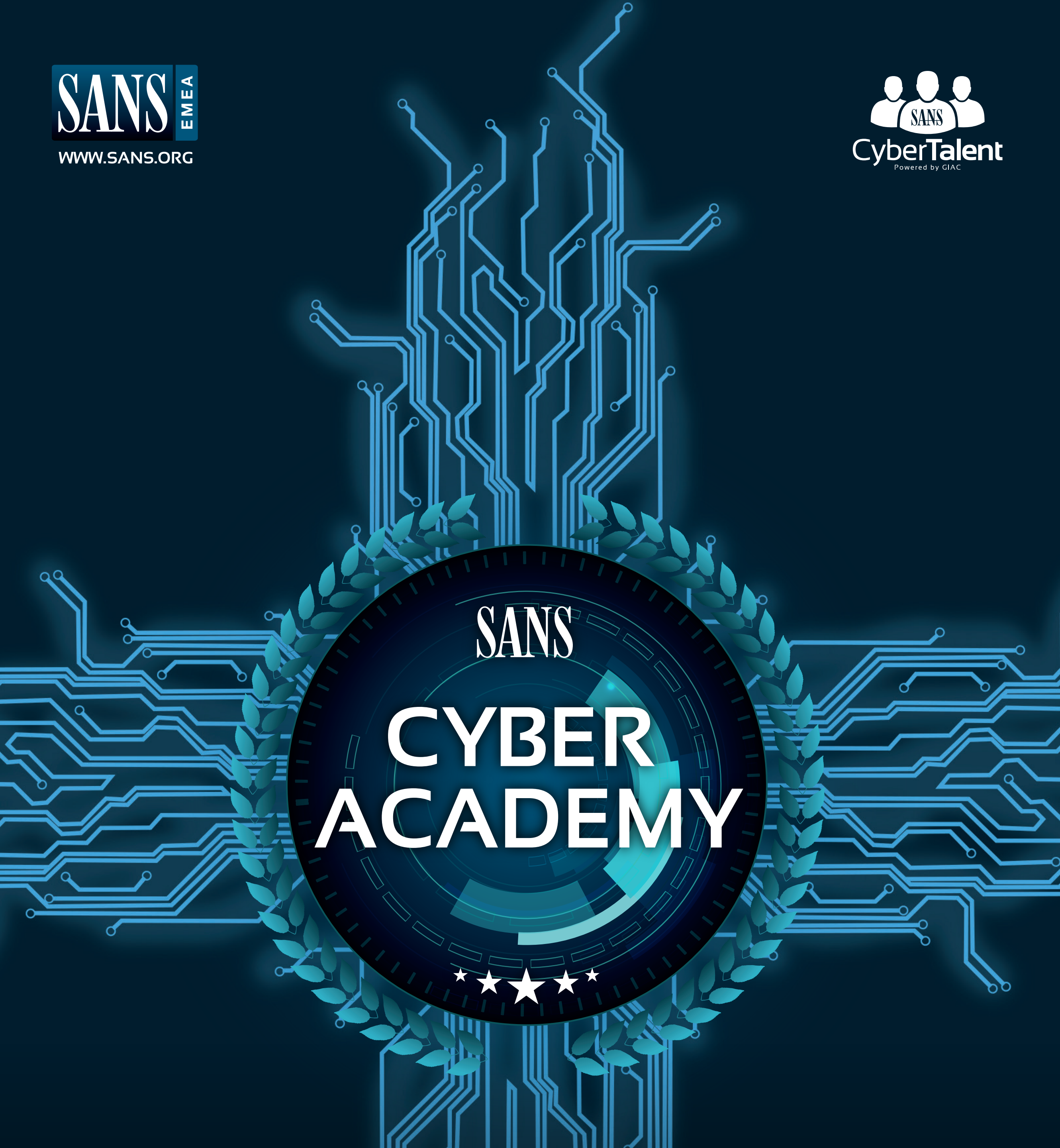
SANS EMEA
WWW.SANS.ORG

SANS CyberTalent
Powered by GIAC



SANS CYBER ACADEMY

SELECTION // ASSESSMENT // TRAINING EXAMINATION //GRADUATION

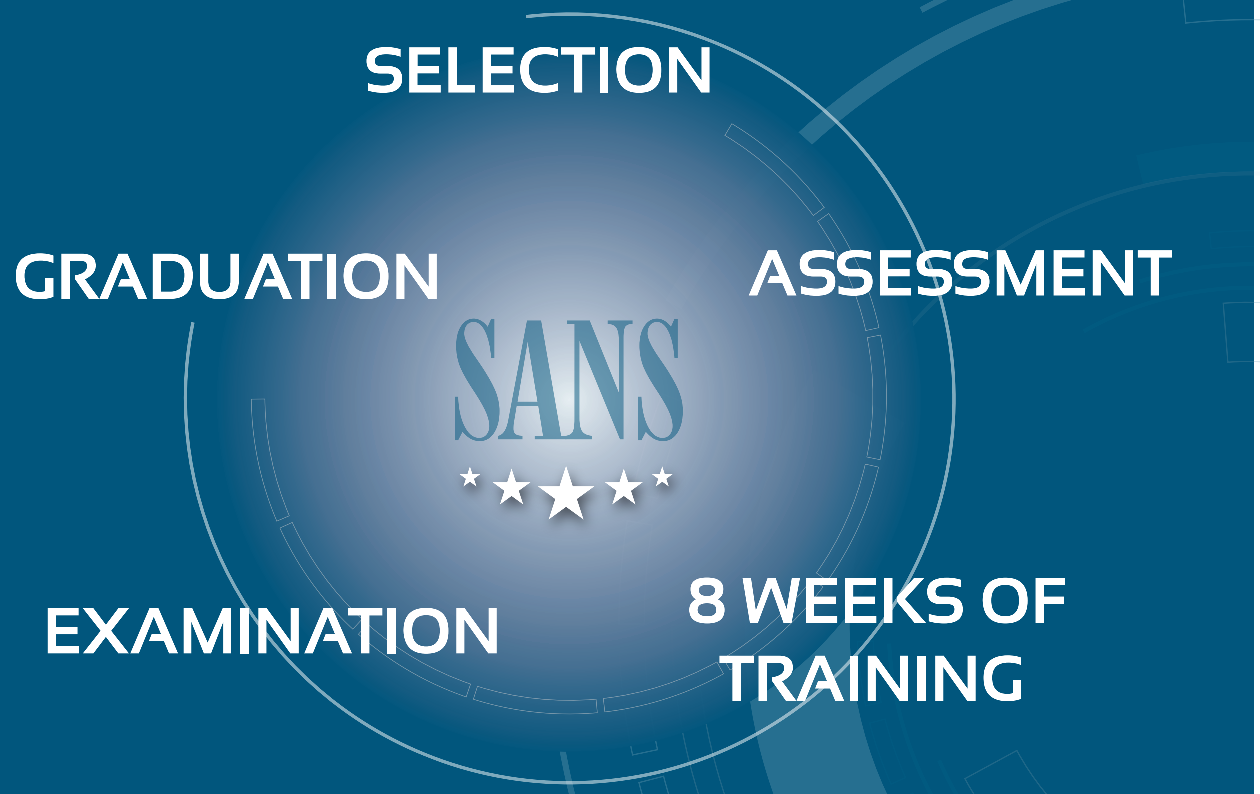
Security, Forensics, Pen Testing, Audit, Secure Development, Management, Incident Handling, Intrusion Analysis

HM Government
SANS is a Cyber Security Supplier to Government

GIAC SECURITY ESSENTIALS GSEC

GIAC CERTIFIED INCIDENT HANDLER GCIH

GIAC CERTIFIED FORENSIC EXAMINER GCFE



SANS Cyber Academy is an intensive training programme designed to give carefully selected students the tools, in-depth cyber security knowledge and certifications they require to be immediately deployable and effective within an enterprise.

The syllabus is taught by the world's leading specialists in the field of information security, condensing the very best courses currently available on the market into eight weeks.

As the most trusted information security provider in the world, SANS is dedicated to addressing the current shortage in cyber security skills and its Academy is a significant step towards this.

Why SANS Cyber Academy?

We know that the lack of cyber security skills is hardly going to be news to you. The fact that there is a solution to tackle it, however, may be.

The 2013 National Audit Office Landscape Review on the UK cyber security strategy identified that it could take up to twenty years to bridge the gap in skills. The current pipeline of graduates and practitioners is insufficient to meet growing demand and the challenge of developing people and expertise is far from insignificant.

The issue will not disappear until we collectively change our approach. You have told us that enterprise businesses and government organisations struggle to find, recruit and retain cyber security talent, and we listened. SANS Cyber Academy is our response; the first meaningful endeavour within the market to resolve critical skills shortage.

SANS Institute is the most trusted information security training provider in the world. Our Cyber Academy effectively condenses the highest quality training programmes currently available into an eight week period, without compromising quality.

We recognise that there is no replacement for time spent in the role, however the Cyber Academy programme allows organisations to rapidly train new recruits or hire fully-trained Academy scholarship graduates, thereby saving time and money.

The current pipeline of graduates and practitioners is insufficient to meet growing demand and the challenge of developing people and expertise is far from insignificant.

What SANS Cyber Academy Delivers

In order to maintain up to date, relevant skills, even the highest calibre of cyber security professionals requires ongoing skills based training.

Training time for a developing cyber security professional translates to typically 18 to 24 months before they can be regarded as truly operational to the standards required.

And there lies our challenge. Truly credible, practically applied training takes time and should include access to the highest quality programmes available globally, taught by the best instructors in the world. The Academy condenses the quality of content that SANS is renowned for into an eight week period, revolutionising the way we all work and how we recruit, retain and develop our security skills on a local and global scale.

Here are just some of the key benefits:

There is no compromise on quality

Only the very best candidates are recruited by SANS and presented to the industry. If you elect to send your own candidates, they will be subject to the same rigorous assessments. The training programme is a commercial model that typically fits within standard recruiting processes, fees and training budgets, but with a difference: a guaranteed return on investment.

Recruitment is no longer an unpredictable process

The Academy removes the uncertainty and significant cost of traditional recruitment processes. It also mitigates the risk of companies paying disproportionate salaries for often mediocre talent resourced via recruitment agencies lacking industry knowledge.

You stand a better chance of retaining your talented people

The programme develops and encourages employee loyalty due to the substantial investment in the student's future career, enabling employers to build a reliable cyber security team. Such investments in employees tend to encourage loyalty and commitment to a long term, productive career.

Scholarship arrangements are also available that could result in a greater likelihood of employee retention, as a substantial investment has been made and the employee is subject to a drawdown risk.

18 months of education in 8 weeks

The intensive programme gives students more hands-on keyboard time than is offered anywhere else and exposes them to realistic simulations of the past decade's most significant cyber security issues.

They undertake NetWars challenges that give real world experience and allow student scoring and ranking over the course of the programme. This enables them to develop and improve their skills, always with informative, accurate reports and progress indicators, which are shared with the employer.

The nature of the Academy programme allows the employer to recruit and deploy more cyber security professionals at the base level with development paths to more specialist skill sets, resulting in significant cost savings.

The SANS Promise

SANS Institute's world-class training content and instructors guarantee that students receive current best practice and have been trained by the world's top practitioners in the field of cyber security. They will be able to apply our information security training the day they get back to the office.

Selection

Finding the Best Candidates

We understand that one size doesn't fit all when it comes to the recruitment, training and development of the right people. With that in mind, we have developed three options for graduate enrolment into SANS Cyber Academy.

1. Company Sponsorship

A company may directly sponsor and put forward their best candidates, perhaps from their own graduate recruitment programme or existing talent pool. The company should apply directly to SANS Institute Cyber Academy for consideration and acceptance.

When a candidate is sponsored by their employer, we recommend that they agree to specific contractual commitments to aid retention within the sponsoring organisation.

2. SANS Scholarship

SANS are able to source, assess and train the best candidates from top universities across the UK and Europe and from other sources such as The UK Cyber Security Challenge and NetWars competitions.

After training and graduation, the graduates will be made available to organisations where they will be able to apply their skills from the first day of their employment.

3. SANS UK Vets for Success

SANS will actively work with the UK Armed Forces and associated charities to source, assess and train the very best candidates who are veterans of conflict or retiring from the services.

It has been shown that candidates recruited from the Armed Forces have very high success rates and can thrive when placed in the correct security roles.

Assessment

The Key to Success

SANS boast many years of expertise in developing and teaching the greatest technical breadth and depth of security knowledge and therefore hold significant tenure in relation to developing students and upcoming cyber security talent.

In addition to our industry leading training, we have developed a number of capabilities that assist with human capital and recruitment processes that many enterprises and substantial organisations rely upon.

There is a three stage assessment process at the beginning of the Cyber Academy programme, ensuring that candidates with the greatest potential are recruited and a high conversion rate to qualified security professionals is achieved. These are the Aptitude Assessment, Skills Assessment and Instructor Interview.

CyberTalent Aptitude Assessment

This assessment uses psychometric testing principles based on a profile of raw traits, which correlate and determine the candidates that are successful in information security roles.

Indicators include (amongst many others) attention to detail, logical extrapolation, parsing capabilities and demonstration of an ability to learn technical principles and quickly apply them to solve problems.

CyberTalent Skills Assessment

This assessment draws from the millions of GIAC questions and answers available to SANS, combined with substantial psychometric data from successful and unsuccessful candidates who have taken our examinations.

It is an effective test of knowledge, identifying those with existing expertise in certain areas versus those that require specific development. It is a very powerful early indicator, which enables ranking and streamlining of the candidate base or implementation of steps to help students develop and be successful.

CyberTalent Interview

All potential candidates will be interviewed by one of the Cyber Academy instructors. SANS instructors are industry leading experts and have extensive classroom experience, as well as real world experience of working in the cyber security profession. They are in an ideal position to identify talent and recognise challenges before investment in training and development begins.

At each stage of this process SANS will engage with employers and partner organisations to identify the students most likely to succeed, those that should proceed with the programme or alternatively to propose remediation to help borderline students be successful. This stage also provides an opportunity to identify the potential top performers and nurture them to be technical influencers and leaders within the programme.

8 Week Training Programme

There is a wide and ever-increasing range of cyber security disciplines but they can be broadly classified as Defensive, Forensic, Offensive, Development and Managerial.

At the fundamental level however, cyber security professionals have a common set of skills. Whilst traditionally practitioners have been explicitly focused on defence or offence, it is increasingly recognised by governments and industry that blended skills and an understanding of all disciplines leads to far better cyber security execution.

SANS Cyber Academy is designed to rapidly accelerate the development of these core skills and also provide paths for specialist development of more senior information security professionals. Cyber Academy students are able to contribute to the workplace immediately upon deployment and the core programme spans the critical areas that are key to the success of security professionals in any organisation today.

Training

SANS Cyber Academy ran in 2015 and saw thirty new Cyber Academy graduates enter the employment market after scoring in the top 10% of all GIAC examinations globally. Following this success, SANS Cyber Academy will take place again in 2016. The intensive eight week training programme consists of classes and labs five days per week, running from 9am to 5pm daily, as well as NetWars challenges and evening events.

The following core learning areas are covered:

1. Technology Fundamentals

Students will review the core components of modern computers, smartphones and networks to ensure that they have the fundamental knowledge for skilled development. A surprising number of security professionals lack these fundamental skills, which hinders their ability to grasp more advanced topics.

2. Security Essentials

Students will learn how the various security functions tie together to thwart attackers. This module is based on the most popular SANS course, SEC 401. Students will initially learn the basic, but fundamental, traits of a successful security professional.

3. Enterprise Infrastructure

Students will learn about enterprise infrastructure challenges, such as mobile device management and remote working. They will learn how hackers exploit these scenarios and how to secure against such attacks.

4. OS Security - Building and Securing Linux and Windows Environment

Students will learn how to build the infrastructure used in modern enterprises including web servers, DNS, file servers and authentication services. These infrastructures will be thoroughly analysed both from a defensive and offensive perspective.

5. Virtualisation and Cloud Infrastructure Security

Virtualisation and Cloud services have become a default in most environments and will play a fundamental role in the future development of our technology. The students will learn about the security challenges, risks and mitigations surrounding them.

6. Compliance Audit and Risk

IT security plays a significant role in driving the compliance and risk management of any organisation. Students will learn how these procedures work in an enterprise, what is required to make the procedures sustainable and what they can do to contribute.

7. Incident Response

Incidents and attacks are a matter of 'when' and not 'if'. The students will learn how incident response can fail by analysing previous significant failures. They will learn the incident response process and how they can contribute to successful suppression of attack.

8. Basic Forensic Principles

Students will learn how to collect evidence and identify and track those who have perpetrated attacks, identifying the events that transpired to allow the attack to occur. They will learn to be alert to specific indicators, with the view to preventing future attacks.

9. Penetration Testing and Ethical Hacking

Students will be introduced to the framework for enterprise testing as well as common tools and techniques. They will build a foundation which informs their other security work or provides a path to further specialist studies. Any security professional must know how attackers think and what tools or methods they will use against an organisation.

- **The most intense, hands-on training curriculum**
- **Unparalleled amount of practical time**
- **Realistic enterprise environments, running the latest technologies**
- **Incident simulations**
- **NetWars challenges**
- **Study real and recent data**
- **Breaches and hacks**

Programme Schedule*

	Monday	Tuesday	Wednesday	Thursday	Friday
Week 1		Welcome & Hackathon	401.4 Secure Communications	401.5 Windows Security	401.6 Unix/Linux Security
Week 2	Practice Exam Day	GSEC Proctored Exam	504.1 Incident Handling	InfoSec Social Skills	Challenge Day
Week 3	504.2 Hacker Techniques: Recon & Scanning	504.3 Hacker Techniques: Exploitation	504.4 Hacker Techniques: Passwords & WebApps	504.5 Hacker Techniques: Covering Tracks	504.6 Capture the Flag Exercise
Week 4	Study Day	Challenge Day	NetWars	Practice Exam Day	GCIH Proctored Exam
Week 5	408.1 Windows Digital Forensics & Advanced Data Triage	408.2 Windows Registry Forensics & Analysis	408.3 USB Devices, Shell Items & Key Word Searching	408.4 Email, Key Additional Artefacts and Event Logs	408.5 Web Browser Forensics
Week 6	408.6 Windows Forensic Challenge	580.1 Pentesting with Metasploit	580.2 Pentesting with Metasploit	Study Day	Challenge Day
Week 7	Project Day	Project Day	433.1 Planning a Security Awareness Programme	Careers Fair	IR Team Exercise & Hack the Drone
Week 8	Network Build, Hack & Defend		Practice Exam Day	GCFE Proctored Exam	Graduation

* **Schedule content is subject to change**

In addition to SANS' most in demand courses, the Cyber Academy programme includes a wealth of hands-on and team work challenges. Below is a brief summary of some of the activities.

Challenge Days
Students work in teams to solve a variety of challenges spanning defensive, forensic and offensive disciplines. Challenges range from easy to extreme difficulty, requiring significant research and prototyping to form solutions. These challenges are fun but also provide students with an environment where they must think, overcome frustrating road blocks and work together to go beyond their existing knowledge.

Network Build, Hack & Defend
Students work in groups to build a secure network. Common services such as DNS, DHCP, Mail, LDAP, Wireless and logging services are configured to provide security professionals with a solid foundation in the challenges of delivering a functional yet secure environment.

IR Team Exercise & Hack the Drone
Students combine their course knowledge to date in order to demonstrate security product testing skills. They analyse a black box device, reverse engineer how to access it and use programming/scripting skills to hijack a drone and fly it. This fun game also teaches the ramifications of poor security decisions or bad coding.

Examination and Certification

What it means to you and your graduate

Graduates of the SANS Cyber Academy programme will have obtained a number of certifications that demonstrate their practical capabilities and knowledge. These are based on examinations proctored at the Cyber Academy and align with our ANSI certified assessment body, GIAC. Graduates will complete three major certifications: GSEC, GCIH and GCFE.

GSEC (GIAC Security Essentials Certification):

Passing this examination demonstrates that students understand defensive technologies, security policy and the major security issues enterprises face.

Perhaps more critically it demonstrates that students have mastered security concepts and language, which helps drive a consistent understanding of security across a team within the enterprise. This is the most popular SANS certification and a highly valued certification to achieve.

GCFE (GIAC Forensic Examiner Certification):

The GCFE certifies that students have the knowledge, skills and ability to conduct typical incident investigations including e-Discovery, forensic analysis and reporting, evidence acquisition, browser forensics and tracing user and application activities on Windows systems.

GCIH (GIAC Certified Incident Handler Certification):

This requires students to have a solid understanding of incident response processes and strategy enabling them to react effectively in the event of a potential or confirmed attack.

This assessment also tests the students' understanding of attacker techniques from malicious code to how they enumerate and target network resources. This is invaluable in any organisation as individuals with these skills are able to play a key supporting role in identifying attackers and their likely approaches and can react correctly in the event of crisis.

Additionally, graduates will achieve the SANS Cyber Academy Practitioner Certification. This new award is for those that complete the extensive practical exercises included in the programme. The certification comes in two grades: silver and gold.

Graduation

Previous bootcamp style programmes have shown that a balance of defensive, offensive and forensic scenarios creates the best opportunity for development of every candidate.

Successful graduates of the Cyber Academy programme would be suitable for a junior role in a security advisory team, incident response or an SOC analyst role. They may often have broader knowledge and expertise than existing security specialists, however still need time to formalise their understanding of the enterprise and to develop deeper technical understanding through experience.

We conduct continuous assessment and report back on the progress of the students' development and learning, which is included in our recommendations on role alignment and areas of strength and weakness. This report, combined with aptitude results and incremental assessments, will be an extremely helpful asset in placing the individual at work. Employers are also offered the chance to discuss the results with SANS to maximise their success in the workplace.

Below is a list of recommended roles appropriate for a SANS Cyber Academy graduate. These will create opportunities for further specialist study and we will work with you to provide the most appropriate learning path and areas of specialism for your graduate.

Graduate Roles

- Junior SOC Analyst: Identifying potential incidents and applying first level triage in the security operations centre.
- Junior Security Advisor: The breadth of knowledge acquired through the programme makes the graduate ideal for work identifying potential risks to the business and initial strategies to mitigate them.
- Junior Penetration Tester: Further study is required to excel in this area, however through the programme many graduates will develop ample skill for internal red team roles and research.
- Behavioural Malware Analyst: First level triage to identify if code is good or bad, not more advanced reversing capabilities.
- Incident Responder Team Member: Reacting to raised alarms and identifying containment and response strategy for an attack.

Next Steps

To receive further information email **cyberacademy@sans.org** or to discuss Cyber Academy with a SANS director contact Stephen Jones via **sjones@sans.org** or Matt Anderson via **manderson@sans.org**

Phone:

0203 384 3470

Address:

SANS EMEA
PO Box 124
Swansea
SA3 9BB
UK

Web:

www.sans.org/ukcyberacademy
www.sans.org/emea

SANS EMEA
WWW.SANS.ORG