Table of Contents

Introduction ............................................................................................................................................................................................ 3
How It Works ........................................................................................................................................................................................... 4
Admissions Requirements ................................................................................................................................................................ 5
Curriculum Design ............................................................................................................................................................................... 5
Course Overview and Electives ................................................................................................................................................. 6-10
Cohort Profiles .............................................................................................................................................................................. 11-32
  Assim A......................................................................................................................................................................... 11-12
  James B......................................................................................................................................................................... 13-16
  Detnarong C............................................................................................................................................................... 17-19
  Edward D...................................................................................................................................................................... 20-22
  Tyrone M...................................................................................................................................................................... 23-25
  David M........................................................................................................................................................................ 26-27
  Raymond N................................................................................................................................................................. 28-32
Introduction

The VetSuccess program provides transitioning U.S. military veterans with advanced technical training, certifications, and connections to high-paying jobs in cybersecurity.

According to the U.S. Department of Labor, about 1.5 million members of our armed services will leave the military over the next 5 years. As they return home and transition to civilian life, SANS seeks to honor their service with a program to help veterans build critical skills, find great jobs, and build rewarding careers. SANS is pleased to introduce VetSuccess, a program that provides returning veterans with a simple, direct path to rewarding careers in cybersecurity.

VetSuccess works by connecting veterans with cybersecurity training and employers.

1. SANS Training:
   SANS is the most trusted and by far the largest source for information security training and certification in the world. For VetSuccess we’ve put together an accelerated program of intensive, immersion training for those veterans with interest and aptitude in cybersecurity. In just 2 to 4 months, graduating veterans master the practical knowledge and develop the elite skills needed to fill mission-critical jobs.

2. Top Employers in Cybersecurity:
   SANS is privileged to work with the leading organizations in the cybersecurity industry. These organizations understand the urgent demand for qualified cyber talent and the need to find, develop, and support that talent for the long term.

3. America’s Veterans:
   Veterans are uniquely suited for cybersecurity jobs. Their training, discipline, and integrity provide an essential foundation for developing the skills and knowledge cybersecurity demands.

VetSuccess is a partnership that brings results because:

- **SANS** provides the best cybersecurity training available.
- **EMPLOYERS** provide the premier workplaces for cyber professionals.
- **VETERANS** provide the talent to complete the intense training and the commitment to succeed in a world-class workplace.
How It Works

SANS recruits and screens applicants. CyberTalent Assessments help identify veterans with a strong foundation of aptitude and skills. SANS identifies transitioning veterans with skills and interest in cybersecurity careers. SANS pre-screens for skill set and aptitude and administer SANS CyberTalent Assessments to ensure program readiness.

Veterans complete the Immersion Academy, a series of SANS training courses that provide deep, technical knowledge and a pathway to GIAC certifications to ensure mastery. Veterans choose one of two course options:

**Two Course Option:**

SEC401 Security Essentials (GSEC certification) and SECS04 Hacker Techniques (GCIH certification)

![GSEC](image1.png) ![GCIH](image2.png)

**Three Course Option:**

Same as 2 course option plus an elective course from the following;

- SEC501 Advanced Security Essentials (GCED certification)
- SEC503 Intrusion Detection In-depth (GCIA certification)
- SEC542 Web App Pen Testing and Ethical Hacking (GWAPT certification)
- FOR408 Windows Forensics Analysis (GCFE certification)

Designed for completion in 3-4 months. GIAC certifications required to ensure content mastery.
Admissions Requirements

Veterans applying to the VetSuccess Academy need to meet the following requirements:

- Hold a bachelor’s degree and have at least one year of professional work experience in information technology, information security, or audit, or
- Hold an associate’s degree and have at least 3 years of professional work experience in these fields.
- Score at or above the 70th percentile of the CTE aptitude and skills assessment exam.
- Submit an application form, a current resume, and delivery of official undergraduate transcripts.
- Participate in an admissions interview.
- Agree to program requirements and restrictions described in the Academy/Participant Memorandum of Understanding.

Curriculum Design

Duration:

Designed to be completed in 3-4 months.

Courses, Labs and Certifications Delivery:

Will be taken either live at a SANS event or online from home or work as determined by SANS. Online labs will supplement courses and provide additional hands-on training.

Course/Certification Waivers:

Certain waivers may be available for previous SANS Institute classes or GIAC experiences.
Course Overview

SEC 401: Security Essentials Bootcamp Style
Certification: GSEC

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment. This course prepares students for the GSEC certification that meets the requirements of the DoD 8570IAT Level 2.

SEC 504: Hacker Techniques, Exploits & Incident Handling
Certification: GCIH

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose doesn’t!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

By helping you understand attackers’ tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the “oldie-but-goodie” attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning for, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.
Elective Courses

**SEC 501: Advanced Security Essentials**  
Certification: GCED

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials - Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that “prevention is ideal, but detection is a must.” However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

Of course, despite an organization's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

**SEC 503: Intrusion Detection In-Depth**  
Certification: GCIA

SEC503 delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material. In addition, most exercises include an “extra credit” stumper question intended to challenge even the most advanced student.

Continued...
Industry expert Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the name implies, Packetrix contains many of the tricks of the trade to perform packet and traffic analysis. It is supplemented with demonstration “pcaps,” which are files that contain network traffic. This allows students to follow along on their laptops with the class material and demonstrations. The pcaps also provide a good library of network traffic to use when reviewing the material, especially for certification.

SEC503 is most appropriate for students who are or will become intrusion detection/prevention or security analysts, although others may benefit from the course as well. Students range all the way from seasoned analysts to novices with some TCP/IP background, but to keep pace with the class students are expected to have at least a basic working knowledge of TCP/IP (seewww.sans.org//media/security-training/tcpip quiz.php). Please note that the Packetrix VMware used in class is a Linux distribution, so we strongly recommend that you spend some time getting familiar with a Linux environment that uses the command line for entry, along with learning some of the core Unix commands, before coming to class.

Preserving the security of your site in today’s threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and often vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in SEC503: Intrusion Detection In-Depth is to acquaint you with the core knowledge, tools, and techniques to defend your networks. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

SEC 560: Network Penetration Testing and Ethical Hacking
Certification: GPEN

As a cybersecurity professional, you have a unique responsibility to find and understand your organization’s vulnerabilities and to work diligently to mitigate them before the bad guys pounce. Are you ready? SEC560, the flagship SANS course for penetration testing, fully arms you to address this duty head-on.

The Must-Have Course for Every Well-Rounded Security Professional

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world’s best penetration testers to help you do your job safely, efficiently...and masterfully.

Learn the Best Ways to Test Your Own Systems Before the Bad Guys Attack

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test - and on the last day of the course you’ll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario.

Continued...
You’ll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you’ve mastered in this course.

**Equipping Security Organizations with Comprehensive Penetration Testing and Ethical Hacking Know-How**

You will learn how to perform detailed reconnaissance, studying a target’s infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won’t just cover run-of-the-mill options and configurations, we’ll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you’ll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You’ll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

**SEC 542: Web App Penetration Testing and Ethical Hacking**

Certification: GWAPT

Web applications play a vital role in every modern organization. But, if your organization does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no “patch Tuesday” for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws through exploitation.
FOR 408: Windows Forensics Analysis
Certification: GCFE

Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. Understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7, Windows 8/8.1, Windows 10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out - attendees learn to analyze everything from legacy Windows XP systems to just discovered Windows 8.1 artifacts.
Assim A.

**Rank:** Staff Sergeant

**Security Clearance:** Active TS/SCI clearance.

**Professional Summary:**
Transitioning US Veteran with 6 years of experience in cyber systems, cryptographic equipment and communications security. Three years of experience in intrusion detection systems and 2 years of management. Current Computer Science Major at Regis University and within one year of graduation.

**Geographic Preference:**
- Columbus, Ohio
- San Antonio, Texas

**Certifications:**
- GCIH – GIAC Certified Incident Handler: November 2016
- GWAPT – GIAC Web Application Penetration Tester: December 2016

**Education:**
- A.A.S., Electronic Systems Technology, Community College of the Air Force, Montgomery, AL: May 2015 -- 4.0 GPA
- B.S., Computer Science, Regis University, Denver, CO: Projected 2017-- 3.8 GPA

**Technical Skills:**
- Cryptographic equipment and communications security
- C++, Java, Ruby, SQL, Prolog programming languages
- HTML, CSS
- Networking

**Employment History:**

**USAF**

May 2016 to Present
Lackland AFB, TX

**Test Engineer**
- Performs vulnerability assessments, signal analysis, and emissions security testing on DoD communication and information systems.
- Maintains equipment worth $9.5M and testing laboratories worth $20M.
Assim A. continued

May 2013 to May 2016
Buchel AB, Germany

Communications Maintenance Tech
- Repaired and maintained $30M Intrusion Detection System including networking and telephone switching equipment.
- Maintained and configured Nuclear Command and Control communications equipment.
- Maintained base-wide radio and telephone systems.
- Performed multiple system upgrades including software and hardware overhauls.

Feb 2012 to May 2013
Ft Bragg, NC

Ground Radio Technician
- Deployed, maintained and operating mobile radio systems including Harris PRC 117 and PRC 113 radios.
- Maintained communications security through use of Cryptographic devices.
- Configured mobile data systems via MILSTAR links.
James B.

**Rank:** Retired  
**Security Clearance:** N/A

**Professional Summary:**  
Experienced Information Security Analyst with diverse industry experience in education, private contracting and government. Professional expertise includes systems applications, project management and information protection analysis.

**Geographic Preference:**  
- Indianapolis, IN  
- Remote

**Certifications:**  
- GCIH – GIAC Certified Incident Handler: November 2016  
- GPEN – GIAC Penetration Tester: December 2016  
- Information Assurance Security Officer: June 2009  
- OSCP (To be completed in February 2017)

**Education:**  
- Southern New Hampshire University- General Studies (To be completed Spring 2017) Online/ Bachelor of Science  
- Lean Six Sigma Green Belt : January 2009  
- Risk Communication: March 2007  
- Physical Security: March 2007  
- Certified Ethical Hacker: December 2012  
- Security+: November 2012  
- SEC 504: Hacker Techniques, Exploits & Incident Handling: November 2016  
- SEC 560: Network Penetration testing and Ethical hacking: December 2016

Continued...
James B. continued

Technical Skills:

- Active Directory
- Project Management
- VMware Thin App
- VMware ESXi
- Citrix XenApp/XenDesktop
- Citrix XenServer
- System Center Configuration Manager
- System Center Operations Manager
- OpenVas
- Aircrack
- Nessus
- Wireshark
- Powershell
- WMIC
- Netcat
- Mandiant Redline
- Windows Server 2008/2012
- Microsoft Azure
- Firewall
- BurpSuite
- Fiddler
- Metasploit
- NMAP
- ZAP
- Social Engineer Toolkit (SET)
- Rainbow Crack
- John the Ripper
- Cewl
- HPING3
- MS SysInternals
- C programming
- Python programming (2.7, 3.4)
- BASH
- Zabbix
- HTML
- Javascript
- Sharepoint

Employment History:

Browsium
04/2015-06/2016
Redmond, WA (Remote)

System Engineer
Was instrumental in assisting of the creation and implementation of Service and Support Standard Operating Procedures
- Was able to troubleshoot and resolve web application issues escalated from customer support with a 100% success rate item
- Instrumental in Internet Explorer Migration for AT&T and DirecTV
- Served as operating system expert, providing technical support for entire organization and clients
- Prepared and presented technical proposals for clients

Indiana Army National Guard
01/2009-05/2015
Muncie, Indiana

Operation and Infosec Assistant
- Trained and instructed 30 subordinates and supported units on multiple automation systems.
- Effective decision-maker in high-pressure environments.
- Coordinated the fielding of all computing and software for new equipment.
- Set up, tested and configured networks, desktops, laptops and printers
- Oversaw the daily performance of computer systems
- Developed organizational change management strategies.

Continued...
James B. continued

Blackboard Inc
09/2014-04/2015
Indianapolis, Indiana (Remote)

Implementation Consultant and Technical Architect (Contractor)
- Worked with Project Managers for 100% customer satisfaction
- Worked with 10 clients (Government and Higher Education) to integrate their Student Information Systems with Blackboard Learn include account and course provisioning
- Completed Systems Implementations for higher education and government clients and monitored cloud environment for Blackboard Consulting
- Defined client responsibilities and monitored status of tasks.
- Assisted in Implementation of Zabbix servers for clients
- Assisted in teaching Server Administration Course for Blackboard Learn (Dec 2015)

Stefanini
01/2014-09/2014
Indianapolis, Indiana

Technical Team Lead (Contractor)
- Prepared and presented technical proposals for clients.
- Streamlined acquisition of reporting requirements and specifications to disseminate across multiple business lines and IT support teams.
- Developed and managed project plans while providing status updates to management.
- Provided System Administration to Global Team and priority travel sites (7 locations)
- Managed team of 3-7 technical professionals.
- Defined project deliverables and monitored status of tasks.
- Provided Tier 3/System Engineer support to company personnel (1500 personnel)

Indiana University
06/2012-12/2013
Indianapolis, Indiana

IT Support Developer
- Prepared technical architecture proposals for enhancements and integration of existing third party software systems.
- Provided Data Migration and Integration solutions for IT department, directorate, and Indiana University.
- Provided senior technical support to both in-house staff and user departments for all network applications.
- Developed and managed project plans while providing status updates to management.
- Designed, documented and executed maintenance procedures, including system upgrades, patch management and system backups.

Continued...
James B. continued

• Served as operating system expert, providing technical support for entire organization.
• Developed IT strategic vision and drove key departmental objectives.
• Troubleshot and resolved application and hardware issues with a 100% success rate.
• Provided Tier1-3 IT support to company personnel. (1500 tickets closed in 2013)
• Troubleshot and resolved web applications (Citrix, SIS, GotoMeeting) issues escalated from customer support and other departments with a 100% success rate

US Army
01/2008-01/2009
Mosul, Iraq

Assistant Operation Sergeant
• Tasked with monitoring the safety, security, health and well being of installation of 65 personnel.
• Worked with higher headquarters: prepared and executed weekly and daily briefings.
• Responsible for over two and a half million dollars in combat equipment and information systems.
• Monitored equipment usage reports.
• Maintained computer life cycle, tasked with ensuring Internet Service Providers (ISP) lines were compliant with DOD and Civilian network.
• Troubleshot deploying soldiers computer issues for network connectivity, yet not limited to MS Office, Skype,
• Windows XP and Vista.
• Maintained directorate MS SharePoint sites (3), File-servers (5), and (2) Databases.
• Tasked with field of knowledge of tactical combat service support via intelligence briefs; Briefed command/platoon elements on up to date enemy movement and activity.
• Focused on creation of Excel Database with trip ticket capabilities

US Army
01/2004-01/2007
Camp Atterbury, Indiana

Battle Captain, Joint Operations Center
• Implemented from inception, an Emergency Management Office and Incident Control Center.
• Tasked with oversight for the safety, health and welfare of up to 12,000 personnel.
• Administered the Red Cross notification process, which tracked illness, injury and mortality of the service member’s families.
• Tracked all adverse weather activity and launched contingency plans to deal with those events.
• Monitored all incidents involving Homeland Security, soldier illness and injury during training operations, as well as utility outages.
• Disseminated safety and operational updates for military operational equipment and issued suspense dates for scheduled implementation.
• Conducted enforcement of suspense dates.
• Updated a database, which tracked all activity within the Emergency Management Office.
Detnarong C.

**Rank:** SPC

**Security Clearance:** Secret

**Professional Summary:**
Degreed professional with 10 years of hands-on experience working on computers and electronic devices. Excellent in troubleshooting all information technology related equipment such as PCs, wireless handheld devices, thin clients, switches, router, printers and other end user devices. Ability to analyze and repair computer problems such as desktop computers, laptops and various components/peri-

**Geographic Preference:**
San Francisco, California, Oakland, California East bay. Emeryville, California, San Diego, California, San Jose, California, San Antonio, Texas or Austin Texas

**Certifications:**
- GCIH – GIAC Certified Incident Handler: November 2016
- GPEN – GIAC Penetration Tester: December 2016
- CompTIA A+: September 2015
- CompTIA Network+: January 2016
- CompTIA Security +: May 2016

**Education:**
- B.S., Technical Management (Systems Development Life Cycle), DeVry University Fremont, CA: 2009
- Military Science: Petroleum Supply Specialist, United State Army Quartermaster School, Fort Lee, VA: 2010
- SEC 504: Hacker Techniques, Exploits & Incident Handling: November 2016
- SEC 560: Network Penetration testing and Ethical hacking: December 2016
Detnarong C. continued

Technical Skills:

Systems:
Win XP, 7, 8, 10, Linux-based OS, Mac OS and Android,

Software:

Employment History:

Freelance IT Service
February 2014 to present

While attending school in perusing to attain my certifications, I serve my community and neighborhood with IT Services. I provided network engineer and administrator services, consulting and building a desktop tower to selecting the best laptop to fits their needs and budgets. Troubleshooting and Diagnosis issue, upgrade and repair damage computer and laptops, from removing virus, malware, adware, and spyware to backing and recovering lost and or corrupted data. Replacing hardware as well as installing new update patch and services to new operating system and software. I also assist in teaching user awareness in keeping their system and network safe and secured. I attended and volunteer with the Wounded Warrior Transition Academy in repairing faulting desktop and laptop hardware components. Repaired and refurbish over 100 systems, installing new operating system and drivers, saving the company over 80 thousand of dollars.

United Army Reserved
December 2013 – April 2017

Petroleum Supply Specialist Part-Time
• My service contract will be ending April 2017

United Stated Army
July 2010 – Dec 2013
LOCATION(S) South Korea 2012-2013, El Paso TX 2013- 2014, San Antonio Texas 2014-Present

Petroleum Supply Specialist/Section Manager
Managed and supervised supplies and personnel; operated and maintained storage, dispensing, and distribution facilities and pipeline systems for petroleum, oils, and lubricants (POL). Received and dispensed bulk and packaged petroleum products; operated forklift trucks, conveyors, and cranes in loading, unloading, moving, and storing petroleum supplies; marked petroleum containers for proper identification; conducted safety inspections and preventative maintenance of storage facilities and handling equipment.
Detnarong C. continued

- Managed a 15-person facility, ensuring proper training and cross training of all personnel.
- Taught 100 personnel in safety and HAZMAT waste handling.
- Established inventory control systems, creating for the first time an online tracking system to ensure 100% inventory availability when needed, with no excess equipment and supplies. Resulted in 100% mission readiness at all times.
- Ensured adequate availability of fuel supply for over 1000 personnel and vehicles.
- Managed setup and evaluated job sites, developed and implemented successful strategic plans.
- Awarded multiple company achievement awards for performance and contribution to the success of the company network integration.
- Achieved the good conduct award for 3 years of exemplary behavior, efficiency, and fidelity while with the company.

Wells Fargo Bank,
August 2008 – July 2010
San Francisco, CA

Treasury Service Associate
Customer service oriented in addressing Commercial Card Expense Reporting. Used Excel and Linux-based Total System Services (TSYS), as well as the Main Frame Hogan System, to configure purchasing cards. Constructed new accounts in addition to setting purchasing card parameters. Assisted cardholders on the phone in reporting lost/stolen cards and increasing/decreasing their purchasing limits. Generated weekly reports on accounts for account managers and for the monthly meeting.

- Managed 20 company vendors, with 99% (target 85%) in resolving issues and 100% (target 90%) in request processing.
- Increased department work productivity 50% by developing a simpler Excel service request form, enabling faster processing; earned a promotion due to the improvement in productivity.
- Earned an award for most number of customer issues resolved via phone; received recommendations from vendor account administer for exceptional service.

Washington Mutual Bank
Oakland CA

Senior Teller
Provided account services to customers by receiving deposits and loan payments; cashed checks; issued savings withdrawals; recorded night and mail deposits; sold cashier’s checks, traveler’s checks, and series E bonds; answered questions in person or on the telephone; referred to other bank services. Recorded transactions and prepared currency transaction report. Cross-sold bank products; informed customers of new services and product promotions; ascertained customers' needs; and directed customers to a branch representative.

- Supervised and trained 10 new tellers.
- Awarded multiple bonuses for of other bank services and increasing business revenue by 20%
- Saved bank thousands of dollars by confiscating counterfeited money and fraudulent checks.
Edward D.

**Rank:** E6/Petty Officer First Class  
**Security Clearance:** Secret

**Professional Summary:**
Results-oriented leader with 11 years of experience incorporating personal development, professional training, operational management, and foundational cybersecurity skills. Highly capable of utilizing critical thinking abilities and training to analyze complex requirements to develop and apply effective solutions.

**Geographic Preference:**
San Antonio, TX

**Certifications:**
- GSEC – GIAC Security Essentials Certification
- GCIH – GIAC Certified Incident Handler
- CompTIA A+

**Education:**
- M.S., Cybersecurity (active) 12 semester hours completed - University of Dallas, Dallas, TX.: December 2017
- B.S., Information Systems Security, American Military University, Charles Town, WV: May 2012

**Technical Skills:**
- Nmap port scanner  
- Network mapping  
- Netcat: File transfer, backdoors, and relays  
- Metasploit  
- Exploitation using built in OS commands  
- Privilege escalation  
- Advanced pivoting techniques  
- Setup of virtual lab environment  
- Windows/Linux tutorial  
- TCP dump analysis  
- Password cracking  
- Host-based discovery with Dumpsec  
- Hashing to preserve digital evidence  
- Analyzing networks with hping and nmap  
- Event correlation with Splunk  
- Use of steganography tools  
- Securing a Windows system with MBSA and SCA
Edward D. continued

Employment History:
United States Navy
February 2006 - Present

Naval Air Station Lemoore/Strike Fighter Squadron 94
Lemoore, CA
November 2013 - PRESENT

• Supervised 14 personnel in the processing, expediting and material receipt of aviation components. Maintained an inventory of 676 support equipment items valued at over $11 million with 100% inventory accuracy.
• Transferred and received 17 aircraft with zero discrepancies resulting in a full mission capable squadron. Work center efforts contributed to 438 combat flights with the utilization of 105,302 pounds of ordnance in support of Operation Inherent Resolve.
• Committed to the personal and professional development of junior personnel; leadership lead to two candidates selected for Sailor of the Quarter and eight selected for rank promotion.
• Facilitated alcohol and drug abuse for managers/supervisors ensuring personnel under supervisors’ purview will be proactive in reducing alcohol and drug incidents.

Center for Information Dominance Monterey
Monterey, CA
June 2010 - October 2013

• Selected as 2011 Sailor of the Quarter
• Led and qualified 25 mail clerks in sorting and distributing over 100,000 pounds of mail and parcels to 750 assigned personnel.
• Authored a report which identified shortfalls and solutions to improve the efficiency of mail operations which resulted in saving 30 man hours a month.
• Created mail database utilizing Microsoft Access which effectively streamlined mail sorting and distribution.
• Organized four community relation events that directly enhanced the organization’s relationship with the local community. Single-handedly coordinated the volunteer efforts for the AT&T Pro-Am Golf Tournament for two consecutive years.
• Created Microsoft Access database that tracked and managed volunteer hours completed by organization personnel.
• Upgraded RAM for 50 computers which provide prerequisite training for students attending Defense Language Institute.
• Instructed over 100 hours to 300 personnel of bystander intervention which ensured personnel serve as strong leaders in reducing domestic and sexual violence.

Continued...
Edward D. continued

NAS Whidbey Island/Electronic Attack Squadron 130
Oak Harbor, WA
February 2006 - June 2010

- Supervised six junior personnel in providing customer service and material support to 175 aircraft mechanics maintaining five aircraft. Work center efforts contributed to over 250 combat flights in support of Operation Iraqi Freedom.
- Managed a $6.8 million budget; closed out two fiscal years with zero discrepancies while accurately obligating 99.8% of all awarded grants towards organization's operational commitments.
- Proactively located contractor and purchased mandatory shipboard equipment in accordance with Federal Acquisition Regulation procedures totaling over $37K.
- Procured 100% of deployment assets for organization in preparation for combat deployment.
- Achieved 99% quality assurance audit with no repeat discrepancies ensuring work center processes and procedures are in accordance with governing rules and regulations.

Awards and Achievements

- Navy and Marine Corps Achievement Medal (x2)
- Military Outstanding Volunteer Medal
- U.S. Army Certificate of Achievement for Volunteer Service
- Global War on Terrorism Expeditionary Medal
- Global War on Terrorism Service Medal
- 2011 Sailor of the Year, Candidate
- Letters of Commendation (x3)
Tyrone M.

**Rank:** Petty Officer 1st Class (PO1)

**Security Clearance:** Current TS/SCI w/ Full Scope Poly

**Professional Summary:**
GIAC Security Essentials (GSEC) and GIAC Certified Incident Handler (GCIH) certified professional with demonstrated knowledge and technical skills in a variety of security tasks. Proven ability to identify and effectively evaluate network and system vulnerabilities, then using industry best practices to configure systems to be more secure. Capable of troubleshooting complex problems in a variety of information systems independently, using a Google-first approach, capturing lessons learned to continuously drive process improvement. Excellent ability to work with cross-functional teams to drive projects to completion. Tech enthusiast that strives to learn how new technology can help businesses become more efficient at tackling tough problems.

**Geographic Preference:**
San Antonio, TX Area - not able to relocate at this time

**Certifications:**
- GCIH – GIAC Certified Incident Handler: November 2016
- GPEN – GIAC Penetration Tester: December 2016

**Education:**
- BA Economics/Minor Math, St. Mary’s University, San Antonio, TX: December 2014
- AA Chinese Language and Culture, Defense Language Institute, Monterey, CA: February 2012
- SEC 504: Hacker Techniques, Exploits & Incident Handling: November 2016
- SEC 560: Network Penetration testing and Ethical hacking: December 2016

**Technical Skills:**
- Access Control
- Incident Response
- Incident Handling
- Vulnerability Management
- Configuration Management
- Information Security
- System Troubleshooting
- Vulnerability Assessment
- Disaster Recovery
- Network Security
- Windows Security
- Linux Security
- Wireless Security
- Malware Detection
- Web App Security
- Security Policy
**Tyrone M. continued**

**Lab Setup:**
- Home-built virtual lab used to practice using different network security suites to scan, identify, and mitigate various OS and application vulnerabilities
- Running up to 5 VMs at a time to include: Ubuntu, Windows 10, Windows Server 2016, Kali Linux, Metasploitable, and Security Onion to hone network security monitoring (NSM) technical proficiency
- Using a variety of tools to conduct lab testing: Windows and Linux cmd line tools, InSSIDer, nmap, nessus, netcat, metasploit, Cain, John the Ripper, Bro, tcpdump, and Wireshark

**Employment History:**

**US Navy Reserve, Cyber Language Analyst:**
San Antonio, TX, 2012 - Present
Conducted specialized Chinese language analysis using digital network intelligence techniques to produce adversarial threat assessments and serialized reports. Operated sophisticated tools and computer systems to uncover the means, motives, and methods adversaries used to attack our network infrastructure.

**USAA, Business & Insurance Specialist:**
San Antonio, TX, April 2015 - October 2016
As a customer service and sale representative (insurance policy service - auto, home, and valuable personal policy) for USAA, provided member on-boarding, servicing and/or facilitation of product sales in a call center.
- Identified over 40 member life-events daily and provided relevant service solutions to deepen customer relationships and improve members financial security, while exceeding team expectations
- Stayed up-to-date on current compliance policies and processes to maintain an adherence rate of 97%, greatly reducing downtime and exceeding member satisfaction

**LG-Tek, Access Control Specialist:**
San Antonio, TX, August 2012 - April 2015
Guarded access control points and provided continuous monitoring for over 3,000 personnel daily, using customer site approved policies and procedures to prevent or detect leakages of classified material and to prevent unauthorized contraband from being introduced into the classified environment.

**United States Navy, Language Analyst:**
Honolulu, HI, 2002 - 2012
- Completed multiple deployments in support of OPERATION IRAQI FREEDOM and OPERATION ENDURING FREEDOM, accumulating over 2200 career flight-hours onboard Navy P3C ISR aircraft.
- As a Collection Supervisor, supervised the daily intelligence collection efforts of a 6-member joint service team
- Performed in-depth analysis; manipulated computerized data-bases; produced finished summary reports and other support by integrating multi-source intelligence

Continued...
Tyrone M. continued

- Provided quality control on numerous time-sensitive tactical intelligence reports utilized by fleet and national intelligence agencies to provide threat warning, indications and warning and short/long-term intelligence and trend analysis
- Analyzed target telecommunications infrastructure
- Conducted Information Operations using foreign language skills and advanced computer systems; collected, analyzed and exploited foreign language communications signals-of-interest to identify, locate, and analyze worldwide threats
- Liaised with NSA HQ, NSA field sites, other intelligence agencies, and fleet forces on intelligence items of interest
- Managed reporting on critical system events; mitigated issues through hourly status reports and minimized impact on tasking
- Provided tailored information operations, threat warning, and reach-back support to meet mission requirements of Pacific Fleet Naval Component Commanders.
- Supplied critical threat-warning data to warfighting and intelligence platforms deployed world-wide, supporting Pacific Command Area of Responsibility objectives.
- Fused collected technical data with resourced analysis and successfully predicted potential adversarial actions based on target experience, pre-set activity indicators, and historical norms, which directly contributed to awareness and allocation of cryptologic resources
- Transcribed, filtered, and analyzed routine foreign intelligence intercepted communications; operated SIGINT equipment and accessed databases
- Led 31 personnel on 9 direct support combat operations; decreased days deployed for the organization by 10%
- Part of a team of subject matter experts that helped plan and cowrite the first Tactics, Techniques, and Procedures (TTP) manual for airborne intelligence operations. This provided our community with a single source to meet our technical training needs
- Taught over 400 hours of indoctrination training for new employees. This helped the organization maintain an 88% proficiency score on all qualification evaluations
- Frequently briefed senior officers on various topics related to information operations and proper operating procedures
- Named Navy Information Operations Detachment K-Bay’s employee of the year (2012) for “exceptional professionalism and commitment to team objectives”
David M.

**Rank:** Staff Sergeant

**Security Clearance:** Secret (Out of Scope); I am in the process of getting a TS SCI but that might not be completed until mid 2017.

**Professional Summary:**
Seeking a challenging position as a Cybersecurity professional where I can maximize my skills and leverage past experiences. Offering a 10 year proven record of managing multiple large and medium enterprise IT projects, troubleshooting complex problems on several systems, overcoming obstacles and integrating teams that exceeded organizational objectives.

**Geographic Preference:**
1. San Antonio, Texas
2. Austin, Texas
3. Albuquerque, New Mexico

**Certifications:**
- GCIH – GIAC Certified Incident Handler: November 2016
- GPEN – GIAC Penetration Tester: December 2016
- Pursuing: PMI Project Management Professional: January 2016

**Education:**
- B.S., Information Systems Management, Minor in History, University of Maryland, Online: Summer 2017, Completed 113 hours, Deans list 2013 & 2014
- A.A.S., Electronic Systems Technology, Community College of the Air Force, Correspondence: 2010, 4.0 GPA
- SEC 504: Hacker Techniques, Exploits & Incident Handling: November 2016
- SEC 560: Network Penetration testing and Ethical hacking: December 2016

**Technical Skills:**
- Wireshark
- Issue Resolution
- Linux Security
- Vulnerability Assessment
- Nmap
- Nessus
- Metasploit
- Information Assurance
- Incident Handling
- Malware Detection
- Configuration Management
David M. continued

Employment History:

31st Communications Squadron, United States Air Force
August 2013 – October 2016
Aviano Air Base, Italy

IT Project Manager:
• Oversaw project planning and implementation; defined scope, goals and deliverables to successfully upgrade $4.3M Presidential and executive communications system
• Coordinated base’s $10M digital radar install; execution reduced maintenance costs 80% and increased reliability
• Modernized base alert system; handled project initiation, planning, implementation, control and closure of $200K contract

J-63, Africa Command
February – July 2014
Djibouti, Djibouti Africa

Assistant Non-Commissioned-Officer-In-Charge:
• Evaluated new architecture acquisitions, 3 concurrent system upgrades, 6 team deployments and 3 site closures over East Africa
• Synergistic manager; drove inter-organizational teams to complete standard 3-month emergency task in 29 days
• Evaluated new architecture acquisitions, 3 concurrent system upgrades, 6 deployments and 3 site closures over East Africa

603rd Air Control Squadron, United States Air Force
October 2010 – July 2013
Aviano Air Base, Italy

Radio Frequency Transmission Systems Journeyman:
• Implemented lessons learned decreasing local outages 50%; ensured compliance with project deliverables that maintained pilot-aircraft link despite constant primary network outages
• Managed $11M equipment account; reallocated two legacy antennas & eight IT assets; poised squadron for closure
• Excelled as crew chief, field deployment exercises; developed and executed training plan that certified 15 trainees on 40 GMT tasks
Raymond N.

**Rank:** Chief Warrant Officer 3  
**Security Clearance:** TS/SCI

**Professional Summary:**
I am a transitioning Army Warrant Officer with experience in program management and project management while working in very diverse roles to improve national security, cyber security, facility technical and physical security, counterintelligence operations and investigations.

**Geographic Preference:**
San Antonio, Texas

**Certifications:**
- GCIH – GIAC Certified Incident Handler: November 2016
- GPEN – GIAC Penetration Tester: December 2016
- CompTia's Sec+ce (maintained since 2009)
- CompTia A+ce (maintained since 2009)
- CompTia Net+ce (maintained since 2009)
- Technical Surveillance Countermeasures Certification
- Master Technical Special Agent Certification

**Education:**
College:
- A.A.S. in Intelligence Operations, Cochise College, Bisbee Arizona, 2004
- Computer Network Systems Administration studies (Central Texas College: 50cr hours, no degree achieved)
- Cyber Security degree program (ECPI University: 33cr hours, no degree achieved)
- GCIH – GIAC Certified Incident Handler: December 2016
- GPEN – GIAC Penetration Tester: January 2017
- Security+ (CompTIA)
- Network+ (CompTIA)
- A+ (CompTIA)
- Hack and Defend Course (TechNow)
- Silent Runner Basic and Advanced Course (AccessData)
- Introduction to Networks, Computers and Hardware (Defense Cyber Investigations Training Academy)
Raymond N. continued

- Fluke WLAN WIFI Analyzer & Spectrum XT Course (FlukeNetworks)
- Advanced Silent Runner Fundamentals Course (AccessData)
- Intermediate Component Detection Course (NSA)
- Network Traffic Analysis for TSCM Course (NSA)
- TSCM Computer Fundamentals Course (NSA)
- TSCM Fundamentals Course (NSA)
- Advanced Counter-surreptitious Entry Course (U.S. Army)
- Investigative Locksmith Course (U.S. Army)
- Advanced Alarms and Physical Security (Fox Valley Homeland Security Center/Technical College)
- Tactical and Automotive Locksmith Course (Lockmasters Security Institute)
- National Intelligence Familiarization Course (U.S. Army)
- Contingency Operations Course (U.S. Army)
- Counterintelligence Force Protection Source Operations Course (U.S. Army)
- Intelligence in Combatting Terrorism Course (U.S. Army)
- Reid Basic and Advanced Interview and Interrogation Course (Reid and Associates)
- Laboratory for Scientific Interrogation (U.S. Army)
- Counterintelligence/Human Intelligence Operations Management Course (U.S. Army)
- Occupational Skills Instructor Training Course (U.S. Army)
- Action Officer Course (U.S. Army)
- Warrant Officer Management Course (U.S. Army)
- Noncommissioned Officer Management Course (U.S. Army)

Technical Skills:

- Experience setting up routers, hubs, computers, printers and scanners in a LAN and WLAN configuration
- Experience with switches in a port mirroring configuration to conduct LAN and VLAN network traffic analysis investigations.
- Familiarization with the use of Wireshark, Metasploit, Cain and Abel, John the Ripper, Snort, NetStumbler, TCPDump, NMAP, Netstat, Enum, FGDump, and other tools relevant to identifying vulnerabilities to network architecture and security policies.
- In-Depth experience in computer investigations/inspections for physical and logical vulnerabilities to systems configurations that would allow for insider threats as well as externally gained access manipulation.
- Proficient in the use of Microsoft Office Products
- Program Management
- Project Management
- Team Building
- Critical Thinking
- Risk Management
- Information Research and Analysis
- Networking and Negotiations

Continued...
Raymond N. continued

Employment History:

**U.S. Army**

June 2014 - Present
San Antonio, Texas

**Transitioning Regional Program Manager:**

Regional program manager for the U.S. Southern Command area of operations in support of U.S. Special Operations Command-South, U.S. Army South, Joint Task Force-GTMO, Joint Task Force-Bravo and the Joint Interagency Task-Force-South. Responsible for management, coordination, supervision and conduct of technical surveillance countermeasures investigations and operations, senior official security support, facility technical and physical security threat vulnerability assessments, training and development of assigned technical counterintelligence special agents, and frequent briefings to senior leaders on all investigations and operations. Additionally served as an advisor to supported organizations for technical/physical security concerns and counterintelligence investigations/operations requirements. Hands-on cyber experience include network traffic analysis using the Fluke Optiview Network Analyzer and Fluke Optiview XG Network Analyzer in-line with network switches, as well as physical inspection of the computer systems. Physical inspections of the computer systems include log analysis for violations of automation policies, as well as security settings and physical make-up of the computer systems do not allow for insider threat compromise of the systems.

- Nominated for the 2014 Department of Defense Team of Year
- Submitted for a Legion of Merit for exceptional service to the U.S. Southern Command and Secretary of Defense

**U.S. Army**

June 2008 – June 2014 (6 years 1 month)
Hawaii

**Regional Operations Officer:**

Regional operations officer for the U.S Pacific Command area of operations in support of U.S. Special Operations Command Pacific, U.S. Army South, and U.S. Pacific Command. Responsible for management, coordination, supervision and conduct of technical surveillance countermeasures investigations and operations, senior official security support, facility technical and physical security threat vulnerability assessments, training and development of assigned technical counterintelligence special agents, and frequent briefings to senior leaders on all investigations and operations. Additionally served as an advisor to supported organizations for technical/physical security concerns and counterintelligence investigations/operations requirements. Hands-on cyber experience include network traffic analysis using the Fluke Optiview Network Analyzer and Fluke Optiview XG Network Analyzer in-line with network switches, as well as physical inspection of the computer systems. Physical inspections of the computer systems include log analysis for violations of automation policies, as well as security settings and physical make-up of the computer systems do not allow for insider threat compromise of the systems.

- Recognized as the 2013 Department of Defense Team of the Year
- Received the Meritorious Service Medal for significant contributions to all assets within the region
- Received the Army Commendation Medal for direct support to the U.S. Special Operations Command Pacific

Continued...
Raymond N. continued

U.S. Army
January 2007 – January 2008 (1 year 1 month)
Maryland

**Senior Technical Counterintelligence Special Agent:**
Responsible for detection and neutralization of clandestine surveillance systems targeting the U.S. Army, DoD activities, and national level agencies, as well as conduct force protection operations and technical surveillance countermeasures investigations, educate senior officials on critical technical and physical security programs, and provide recommendations to improve security procedures. Hands-on cyber experience include network traffic analysis using the Fluke Optiview Network Analyzer in-line with network switches, as well as physical inspection of the computer systems. Physical inspections of the computer systems include log analysis for violations of automation policies, as well as security settings and physical make-up of the computer systems do not allow for insider threat compromise of the systems.

- Received the Army Commendation Medal for exceptional service to supported assets within the Continental United States

U.S. Army
January 2006 – January 2007 (1 year 1 month)
Iraq

**Counterintelligence Special Agent and Advisor:**
- Received the Military Intelligence Corps Association’s coveted Knowlton Award for Intelligence Excellence
- Received the Joint Commendation Medal and Global War on Terrorism Service Medal for exceptional service during Operation Iraqi Freedom

U.S. Army
December 2002 – June 2004 (1 year 7 months)
Arizona

**Instructor/Writer (Counterintelligence/Human Intelligence Course):**
- Received the Army Commendation Medal for significant accomplishments toward training development

U.S. Army
June 2001 – December 2002 (1 year 7 months)
Puerto Rico

**Counterintelligence Special Agent**
- Selected as the U.S. Army South Soldier of the Year, and represented the theater/regional command as one of only 12 competitors at the U.S. Army’s very first Soldier of the Year competition. Received the Army Commendation Medal and recognized by the Chief of Staff of the Army General Eric Shinseki for significant accomplishment
- Received the Army Commendation Medal for significant contributions to the unit and support assets.
- Received the Meritorious Volunteer Service Medal for significant support to the Red Cross and victims of the 9/11/2001 terrorist attacks

Continued...
Raymond N. continued

U.S. Army
May 1998 – June 2001 (3 years 2 months)
Fort Drum, NY

Counterintelligence Special Agent
- Assisted with the first successful installation and employment of CHATS within a deployed envi-
  ronment in Bosnia-Herzegovina.
- Received two Army Achievement Medals during assignment with 10th Mountain Division for
  significant contributions to supported assets and assigned unit