US VALOR

INTRODUCTION

US VALOR (US Veterans Advancing Through Learning, Opportunities and Resources), is a California 501(c)(3) nonprofit corporation with a **Department of Labor Registered Apprenticeship Program (RAP)** within the Cybersecurity employment space for the training of transitioning military and veterans to prepare them for meaningful, gainful, and long term employment within emerging local, national and global marketplaces. **US VALOR** exists to help veteran's transition seamlessly from the structure and organization of military life into the civilian workforce by providing valuable technical training in cybersecurity, along with essential soft skills, to prepare them for demanding job opportunities that await.

US VALOR helps veterans establish a new sense of purpose, direction, and community through a shared sense of passion and mission.

US VALOR was born out of actual need, as most transitioning veterans are not readily assimilated into the workforce due to lack of opportunity and having related hands-on experience necessary to find a good job. **US VALOR** is focused on helping fellow veteran's find meaning and reward in their life after their personal sacrifices to this country.

Populations Served

US VALOR is passionate about serving our transitioning military members and veterans in the civilian world. Our focus is on military members that are within 6-months of transitioning out of active duty from the US military, and veterans that just left active duty (within one-year of getting out). **US VALOR** will equally engage all **CAP** program participants without preference of gender, sexual preference, race, color or creed. All transitioning military members and veterans have an equal opportunity to apply and succeed within the proposed program. The veteran community is largely a sister and brotherhood of comrades.

As presented in Military.com (https://www.military.com/hiring-veterans/resources/5-reasons-why-employers-are-not-hiring-vets.html, 2020), even though military veterans are trained and instilled with a strong work ethic and dedication to program/mission accomplishment, many still find that it is difficult and complicated to transfer their skills into a fulfilling careers in the civilian workforce. Per that article, the Center for a New American Security conducted interviews with 87 individuals from 69 companies to understand why veteran-employer gaps exist. Among the issues identified through the interviews, one of the most important one was skills mismatch.

US VALOR

Our goal through the **US VALOR CAP** is to change the story of how difficult transitioning can be primarily by having a program designed and ready for them; not just to train them in technical and business knowledge, skills, and abilities but also to train them in the soft and life skills they will need to become valued employees. We help them learn to become civilians again.

US VALOR's CAP will clearly benefit the veteran's community through a comprehensive design that targets veteran's needs while also helping meet the demand for qualified candidates in the Cybersecurity industry.

Upon completion of the full **US VALOR Cybersecurity Apprenticeship Program**, a candidate will have completed and earned the following certifications:

1. **SANS** – GIAC Security Essentials (GSEC)
2. **ISC²** - Systems Security Certified Practitioner (SSCP)
3. **CompTIA** - Cybersecurity Analyst (CySA+)
4. **CompTIA** - Cloud+
5. **EC-Council** - Certified Network Defender (CCND)
6. **ISACA** - Certified Information Systems Auditor (CISA)
7. **CyberSec** - First Responder® (CFR)
8. **SANS** – GIAC Certified Incident Handler (GCIH)
9. **Fortinet** – Network Security Expert 4 & Network Security Expert 5
10. **Prerequisite Certifications:** CompTIA A+ or Net+, and Sec+

Project Design

a. <u>Apprenticeship Partnership Design</u>

The overall conceptual design of the apprenticeship program has at its' core a highly respected and recognizable progressive series of professional cybersecurity certifications. While there are many technology certifying agencies in existence, our apprenticeship program focuses on our candidates earning highly coveted designations, which are known and respected worldwide, in a very structured and tractable process. Completion of our apprenticeship program will enable and equip the candidates with qualifications for career level employment within a high tech, growing workplace. The **US VALOR** Cybersecurity certification program has been developed based on the NICE Cybersecurity Workforce Framework, in conjunction with the DOD 8140/8570 framework. The DoD has four roles, with increasing requirements, of:

- IAT = Information Assurance Technician
- IAM = Information Assurance Management
- IASAE = Information Assurance Systems Architect & Engineer
- CSSP = Cyber Security Services Provider

US VALOR

The **US VALOR CAP** prepares the apprentices to leave the program with the necessary qualifications (Knowledge, Skills and Abilities) to participate in varying workforce categories/roles. The targeted certifications, acquired via the **US VALOR CAP**, are highlighted in blue in the following job role table (https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/), which provides a list of DoD approved IA baseline certifications aligned to the IAT and CSSP categories and levels of the IA Workforce. Personnel performing IA functions must obtain one of the certifications required for their position, category/specialty and level to fulfill the IA baseline certification requirement. The **US VALOR CAP** strategically places the participating apprentices to have a wide range of work role options upon completion of the program. In addition, **US VALOR** constantly engages with and makes every attempt to negotiate with the certifying agencies to provide reduced or no exam fees for program participants as goodwill contribution in honor of those people who have served and made personal sacrifice for this country.

DoD 8570.01Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+ CE CCNA-Security CND Network+ CE SSCP	CCNA Security CySA+ GICSP GSEC Security+ CE CND SSCP	CASP+ CE CCNP Security CISA CISSP (or Associate) GCED GCIH
CSSP Analyst	**CSSP Infrastructure Support**	**CSSP Incident Responder**
CEH CFR CCNA Cyber Ops CCNA-Security CySA+ GCIA GCIH GICSP Cloud+ SCYBER	CEH CySA+ GICSP SSCP CHFI CFR Cloud+ CND	CEH CFR CCNA Cyber Ops CCNA-Security CHFI CySA+ GCFA GCIH SCYBER
CSSP Auditor	**CSSP Manager**	
CEH CySA+ CISA GSNA CFR	CISM CISSP-ISSMP CCISO	

US VALOR

The 18-month, step-by-step **US VALOR CAP** path, to be followed by each candidate, is outlined below:

Phase	**Step 1: Pre-requisites/Preparation**
Timing	Must be completed prior to application decision by committee. May be completed after submitting initial application.
Tasks	Candidates complete application and interviews with our **US VALOR** team
Tasks Outputs	**US VALOR** conducts candidates background checks
	Completion of **CompTIA Net+ (or A+)** and **CompTIA Sec+** certifications, through FedVTE, which provides free online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, and US military veterans.
Certifications:	**CompTIA Net+** - covers the configuration, management, and troubleshooting of common wired and wireless network devices. Also included are emerging technologies such as unified communications, mobile, cloud, and virtualization technologies. Specific areas of focus include critical security concepts to helping networking professionals work with security practitioners, key cloud computing best practices and typical service models, coverage of newer hardware and virtualization techniques and concepts to give individuals the combination of skills to keep the network resilient (source Comptia.org). Training hours: 60 hours
	CompTIA Sec+ - The exam will certify that you have the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations. This powerful credential will help take your IT career to the next level (source Comptia.org). Training hours: 45 hours
Phase	**Step 2: Pre-Apprenticeship Training**
Timing	The pre-apprenticeship program will be completed during the final six months of active duty service or shortly after exit from the military. The duration of this phase is expected to last 6 months normally, following transition from the military.

Tasks	Candidates will undergo cybersecurity training as well soft skills training, and utilize cybersecurity training content developed and conducted by DoD, Manufacturing Extension Partnership/Procurement Technical Assistance Center (MEP/PTAC), Propel San Diego, and California Supply Chain Analysis & Diversification Effort (CASCADE) personnel.
Tasks Outputs	Completion of **SANS GSEC (GIAC Security Essentials)**, **ISC2 SSCP (Systems Security Certified Practitioner)** and **CompTIA CySA+ (Cybersecurity Analyst)** certifications, with **US VALOR** paying for the registrations/certification fees.
Certifications:	**GSEC** – The SANS **GIAC Security Essentials (GSEC)** certification validates a practitioner's knowledge of information security beyond simple terminology and concepts. GSEC certification holders are demonstrating that they are qualified for hands-on IT systems roles with respect to security tasks. (source giac.org) Training Hours: 60 Hours, Skill level: Beginner
	SSCP – The ISC2 **Systems Security Certified Practitioner (SSCP)** is a global IT security certification. The SSCP recognizes your hands-on, technical abilities and practical experience. It shows you have the skills to implement, monitor and administer IT infrastructure using information security policies and procedures — ensuring the confidentiality, integrity and availability of data. (source isc2.org). Training Hours: 12 Hours, Skill level: Basic
	CySA+ - The CompTIA **Cybersecurity Analyst (CySA+)** certification verifies that successful candidates have the knowledge and skills required to leverage intelligence and threat detection techniques, analyze and interpret data, identify and address vulnerabilities, suggest preventative measures, and effectively respond to and recover from incidents. (source Comptia.org). Training Hours: 12.5 Hours, Skill level: Intermediate
Phase	**Step 3: Formal Apprenticeship Training**
Timing	The duration of this phase is 12 months and is the final phase in the CAP. Upon completion of the apprenticeship program, each employer partner will have first choice of any apprentice that worked for them.
Tasks	Four 3-month long work rotations will be conducted, supported by our employer partners. This process has a "No risk guarantee"; if the apprentices need more training, they can participate in another rotation.
Tasks Outputs	Employer partner pays wages to apprenticeship as W2 employee during apprenticeship rotation. Apprentice works 40 hours per week, for a total of 50 weeks = 2,000 hours.
Outputs Phase	Completion of **GIAC Security Essentials (GSEC), CompTIA Cloud+, EC-Council Computer Hacking Forensic Investigator, ISACA -**

	Certified Information Systems Auditor (CISA), GIAC Certified Intrusion Analyst (GCIA), GIAC Certified Incident Handler (GCIH), Fortinet NSE 4 &5 certifications, with **US VALOR** paying for the registrations/certification fees.
Certifications	**Cloud+** – CompTIA **Cloud+** reflects an emphasis on incorporating and managing cloud technologies as part of broader systems operations. It assumes a candidate will weave together solutions that meet specific business needs and work in a variety of different industries. It includes new technologies to support the changing cloud market as more organizations depend on cloud-based technologies to run mission critical systems, now that hybrid and multi-cloud have become the norm. Training Hours: 2 Hours, Skill level: Beginner
	CHFI – EC-Council **Computer Hacking Forensic Investigator (CHFI)** Digital crime is more prevalent than ever, and the attacks are getting highly complex. Security software can't pinpoint it---the eyes and expertise of a trained computer forensics professional is necessary. Our online Computer Hacking and Forensics training course teaches you how to become that professional. Love the idea of digital forensics investigation? That's what computer forensics is all about. You'll learn how to; determine potential online criminal activity at its inception, legally gather evidence, search and investigate wireless attacks. Additional topics include unlocking passwords, the establishment and maintenance of a physical "chain of custody" and recovering lost and deleted data. Training Hours: 17 Hours, Skill level: Intermediate
	CISA – ISACA's **Certified Information Systems Auditor** (CISA) certification, you can do just that. CISA is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems. CISA certification is foundational to a successful IT career. If you are an entry-level to mid-career professional, CISA can showcase your expertise and assert your ability to apply a risk-based approach to planning, executing and reporting on audit engagements. Gain instant credibility in your interactions with internal stakeholders, regulators, external auditors, and customers. Training Hours: 13 hours, Skill level: Intermediate
	Certified Incident Handler (GCIH) – The **GIAC Certified Incident Handler** certification validates a practitioner's ability to detect, respond, and resolve computer security incidents using a wide range of essential security skills. GCIH certification holders have the knowledge needed to manage security incidents by understanding common attack techniques, vectors and tools, as well as defend against and respond to

	such attacks when they occur. Training Hours: 55 Hours, Skill level: Intermediate
	GIAC Certified Intrusion Analyst (GCIA) - The **GIAC Certified Intrusion Analyst** certification validates a practitioner's knowledge of network and host monitoring, traffic analysis, and intrusion detection. GCIA certification holders have the skills needed to configure and monitor intrusion detection systems, and to read, interpret, and analyze network traffic and related log files. Hours: 55 Hours, Skill level: Intermediate
	NSE 4 – Network Security Professional – The Fortinet **Network Security Professional** designation identifies your ability to configure, install, and manage the day-to-day configuration, monitoring, and operation of a FortiGate device to support specific corporate network security policies. The Network Security Professional training is composed of two courses: FortiGate Security and FortiGate Infrastructure. **NSE 5 – Network Security Analyst** – The Fortinet **Network Security Analyst** designation recognizes your ability to implement network security management and analytics using Fortinet security devices. The Network Security Analyst curriculum offers four courses. Fortinet recommends this curriculum for network and security professionals who require the expertise to centrally manage, analyze, and report on Fortinet security devices.

On the Job Learning/Training (OJL/OJT): This training will be coordinated, tracked, and sometimes provided by our staff. We have several training partners we will be working with, including Cybrary for Cybersecurity certification training and FedVTE for Cybersecurity certification training (free for veterans). Our staff will coordinate with the California State Apprenticeship Agency, the California Department of Apprenticeship Services, and the DOL Office of Apprenticeships to make sure we are meeting, following, and reporting on the RAP standards and results.

Related Technical Instruction (RTI): This instruction will be managed by our staff and provided by the previously mentioned training partners. The primary technical instruction for our apprenticeship program is for Cybersecurity certifications. This will be provided by our training partners, and will be at no cost to the apprentices, including the tuition, and the costs of the certification tests. The training will be provided virtually via online programs.

Enrollment Strategy and Assessment Process: US VALOR will utilize the local military branch bases and their Transition Assistance Program (TAP) staff, as well as their Transition Readiness Program (TRP) staff to help us find potential candidates for the apprenticeship program. We will be working with the commanders of each applicant's unit

to ensure we receive the appropriate approval from the commander before formally accepting a candidate. When a candidate is located, they will first complete our application. After review, they will be contacted for a phone or in-person interview with **US VALOR** staff. When this is complete, eligible candidates will then go through an assessment program, through CyberKnights, which is a designed to assess a person's capabilities and capture their certifications, proficiencies, history, and additional assessments. All of this, combined with the candidate meeting all pre-requisites, will be used to make a final determination an applicant's acceptance.

Partner Engagement for ensuring access and ability to participate, Assistance Technology: US VALOR will focus on transitioning military and young veterans; as such our most important partner engagement will be with the local bases and their staff. Within the San Diego and Las Angeles Counties, there are many Marine Corps, Navy, Army and Air Force installations. Having good relationships with these bases is paramount to our being able to have access to a strong pool of potential applications. It is unlikely that any assistance technology will be required for any candidate, however, if a candidate does have any disability that requires an accommodation to allow them to participate, we will support their needs.

Supportive Services: US VALOR will provide several services to each apprentice including:

- Initial Career Assessment
- Training scheduling and coordination
- Certification exam registration and scheduling
- Training technology support
- Soft skills and employment skills training
- DoD training workshops

These services will provide the support needed for each apprentice to complete the **CAP**.

The **US VALOR CAP** brings together cutting-edge education providers, highly in demand cybersecurity certifications, a structured program based on the **US VALOR** concept of a "Pathway" that leads the candidates through the learning and certification process, a foundation based on the national standard bearer for frameworks, and the support of an ecosystem all focused on helping young transitioning military and veterans become well trained, well equipped, successful members of the national cybersecurity workforce.

The structure of the training program is specifically designed to provide the candidates with a full range of training in all areas of cybersecurity. Many of these certificates are stackable, for example, the CompTIA Network+, Security+, and CySA+ follow the recommended pathway for a Cybersecurity Analyst. In addition, the candidates are receiving certifications from five of the top six cybersecurity certification providers. This gives them a balance and credibility through having these various certifications.

US VALOR

The structure of our pre-apprenticeship program is designed to provide the transitioning military candidates and young veterans with a combination of technical training, workforce skill development, and soft skill development all structured to prepare them to join the apprenticeship program well prepared to have every chance to succeed. We know that one of the greatest challenges the military have when returning to or joining the civilian workforce is in their communication skills. They have spoken a different language while in the military. Learning to not use jargon and acronyms they have learned and internalized for many years in the military can be challenging. **US VALOR** will help them learn about professional communication, and what to expect in the workforce. We will also train them in skills like negotiation, networking, and time management.

In the later portion of our pre-apprenticeship program, we will begin an OJT program that will connect the candidates with our employer partners. They will spend time shadowing their cybersecurity staff, exposing them to their work, culture, and day-to-day activities. This will not only connect them with their future apprenticeship program employer partners, it will also prepare them for what to expect once they begin their apprenticeship. This is especially helpful for youth, as it is likely they have not worked in a professional civilian business environment before. Our RTI program, which will occur during both the pre-apprenticeship program and the apprenticeship program, will also adequately prepare them to thrive in the professional workforce.

Under the **US VALOR CAP** pre-apprenticeship program, as our candidates will be taking their training through cybersecurity education providers that are focused on training and preparing students for taking the proctored certification exams; the result is that their transition from student to apprentice will be an easier transition than a traditional community college student to apprentice.

US VALOR will work with our partners to align their training programs to California state educational programs and to their workforce programs. We will be working directly with the California Department of Apprenticeship Standards. We will be working with the Employment Training Panel, and other stakeholders in the San Diego and LA counties, to increase opportunities for young transitioning military. Finding gainful employment is often challenging due to the misunderstanding of many civilian managers.

We will work with the local secondary education programs on behalf of our apprentices, to champion their continuing education after graduating from the apprenticeship program, in order to drive the ongoing development of our apprenticeship graduates as they choose to pursue higher educational degrees.

The **US VALOR CAP** will also benefit by cost-shared institutional leadership from Kelly Kendall and Chuck Buresh. Kelly Kendall, President and Executive Director of **US VALOR**, has over 20 years in sales, marketing, and IT experience. He served as a Marine (Infantry) and is a disabled Veteran. His background is in B2B sales, B2C sales, sales management, and marketing within the IT and financial services industries. He is an entrepreneur, with a passion for startups. He has an MBA from Colorado Christian University and a Bachelor of Science in Business Management from The University of Phoenix. Chuck Buresh, Chairman of the Board for **US VALOR**, has over 25 years of experience providing technical and administrative leadership during corporate IT modernization initiatives for several of the top Fortune 100 corporations. Mr. Buresh holds an MBA degree from The University of California at Los Angeles, and a Bachelor of Science from Michigan State University. He holds a number of professional certifications, including PMP, CISA, CISM and CISSP.

With the support of the Department of Labor Office of Apprenticeships, the State of CA Department of Apprenticeship Services, SynED and their CASCADE grant and KNC Strategic Services as our primary employer partner, we have no doubt this program continue well into the future. There is no one part of our **CAP** design that cannot be replaced with a suitable alternative. We will maintain the necessary staff within **US VALOR** and unless we decide to increase the number of students in each monthly cohort, we will not need to grow our staff. If at any time we do need help, we will be able to draw volunteers from the community, our partners, and other organizations.

The US VALOR Team of Partners

The **US VALOR** direct program pay staff will be comprised of a Program Manager (PM), Program Coordinator (PC), and Administrator (exact names TBD) which will oversee the day-to-day operations of the **CAP** over the four-year lifetime, with particular emphasis on support and monitoring of the program apprentices. These staff members will be identified/hired upon award of the program. The PM will be at a full-time level over the life of the program, the PC will be at 50% level over the life of the program, and the Administrator will be at 25% over the life of the program. The **US VALOR** staff will be located in the southern California region and travel throughout the San Diego and Los Angeles counties as needed to engage with and manage the partners and the apprentices throughout the life of the program.

US VALOR is a California 501(c)(3) nonprofit corporation seeking funding to establish a government accredited Registered Apprenticeship Program (RAP) within the Cybersecurity employment space for the training of transitioning military and veterans to prepare them for meaningful, gainful, and long term employment within emerging local, national and global marketplaces. **US VALOR** exists to help veteran's transition seamlessly from the structure and organization of military life into the civilian workforce by providing valuable technical training in cybersecurity, along with essential soft skills, to prepare them for demanding job opportunities that await.

KNC Strategic Services, located in Oceanside CA, has a mission to provide Cybersecurity Professional Services to government agencies, defense contractors, and utility providers, while focusing on training and hiring veterans, and giving back to the American Military and Veteran community. KNC was founded by a team of principal management whose diverse and respectable career backgrounds span the U.S. Military and Wall Street. Two of the founders are Service-Disabled Veterans of the United States Marine Corps.

SynED is a non-profit organization that acts as a catalyst to help others improve their lives through education and knowledge and skill acquisition, giving them rich career opportunities.

- SynED seeks to facilitate collaboration and communication to find common ground in an increasingly complex and diverse educational ecosystem.
- Their network of professionals provides services to leverage existing resources and initiatives. SynED identifies the people, processes and technology needed to achieve your goals and maximize your returns. Their experts offer the industry-specific knowledge and experience to craft effective strategies and solutions that will drive performance, lower costs and generate value in higher education.
- SynED identifies emerging best practices for effective articulation between employers, jobseekers and education providers. We identify issues, processes and technologies based on evidence and identify goals and objectives that meet the needs of stakeholders. SynED translates research projects into processes that reflect best practices.
- SynED manages the Cyber-Guild Community project, a California activity (https://cyber-guild.org/). Cyber-Guild is the leading integrated community engagement program of synED focused on raising cybersecurity awareness and learning across the United States of America, and globally at all levels.

Proficio

Proficio is an award-winning managed security services provider (MSSP), delivering 24/7 security monitoring and managed detection and response (MDR) services to organizations around the world. Since Proficio was founded ten years ago, we have grown significantly. Today we help enterprises across multiple industries by providing the highest level of cybersecurity protection at an affordable cost. Proficio's team of security experts works around-the-clock from our Security Operations Centers (SOCS) in San Diego, Singapore, and Barcelona monitoring security events and hunting for targeted attacks. We use a combination of propriety tools and industry-leading security technologies to detect threats and contain attacks before they can cause damage.

US VALOR

Training Fees and Expenses

Cybrary will provide the following core CAP tenants and services that will be directly used by the apprentices. All fees will be covered and provided by US VALOR.

Item	Description	Cost/Unit
Training Memberships	12-month training membership per apprentice	$599

Cybrary is a cybersecurity and IT workforce development platform. Its ecosystem of people, companies, content, and technologies converge to create an ever-growing catalog of online courses and experiential tools that provide IT and cybersecurity learning opportunities to anyone, anywhere, anytime. Cybrary has received industry recognition since its 2015 founding, often being named as an innovator and pioneer in cyber and IT development. Since January 2015, Cybrary has grown its user base to over 2 million and has 96% of Fortune 1000 companies learning on their platform. Cybrary will provide training memberships to our apprentices. They will be able to utilize these memberships to complete all of the required training time for each Cybersecurity certification needed.

US VALOR will cover all certification testing fees. They will be paid directly to the certification organizations. They will be used solely for the apprentices. The breakdown of fees for the varying certifications that will be offered throughout the CAP project are shown below:

Cybersecurity Pre-apprenticeship Pathway

- **1st three months**
  - **ISC2 - Systems Security Certified Practitioner (SSCP)**
    - https://www.isc2.org/Certifications/SSCP
    - Free training online VIA FedVTE (fedvte.usalearning.gov) for veterans
    - Annual membership and renewal fee: $65.00
    - Exam fee: $250.00
    - **Total: $315**

  - **SANS GIAC Security Essentials (GSEC)**
    - https://www.giac.org/certification/security-essentials-gsec
    - Online Live Instructor Led Training Course Fee and Exam Fee: $3,909.50 (60 hours)
    - Includes a 50% in-kind donation from SANS
    - **Total: $3,909.50**

- **2nd three months**
  - **CompTIA - Cybersecurity Analyst (CySA+)**
    - https://www.comptia.org/certifications/cybersecurity-analyst
    - Free training online VIA FedVTE (fedvte.usalearning.gov) for veterans

- Annual membership and renewal fee: $25.00
- Exam fee: $349.00
- **Total: $375**

Formal Apprenticeship Program

- **1st three months**
  - **CompTIA Cloud+** • https://www.comptia.org/certifications/cloud
  - Annual membership and renewal fee: $25
  - Exam fee: $329
  - **Total: $354**

- **2nd three months**
  - **EC-Council Computer Hacking Forensic Investigator**
  - https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/
  - Annual membership and renewal fee: $100
  - Exam fee: $550
  - **Total: $650**

- **3rd three months**
  - **ISACA - Certified Information Systems Auditor (CISA)**
  - https://www.isaca.org/
  - Annual membership and renewal fee: $135.00
  - Exam fee: $575.00
  - **Total: $710**

  - **SANS GIAC Certified Intrusion Analyst** • https://www.giac.org/certification/certified-intrusion-analyst-gcia
  - •Online Live Instructor Led Training Course Fee and Exam Fee: $3,909.50 (60 hours)
  - **Total: $3,909.50 ($65.15/hour)**

- **4th three months**
  - **CyberSec First Responder® (CFR)**
  - https://logicaloperations.com/certifications/1/CyberSec-First-Responder
  - Exam fee: $250
  - **Total: $250**

  - **Fortinet NSE 4/5**
  - https://training.fortinet.com/local/staticpage/view.php?page=certifications
  - **One exam voucher free per candidate**
  - **Second exam voucher: $400**
  - **Total: $400**