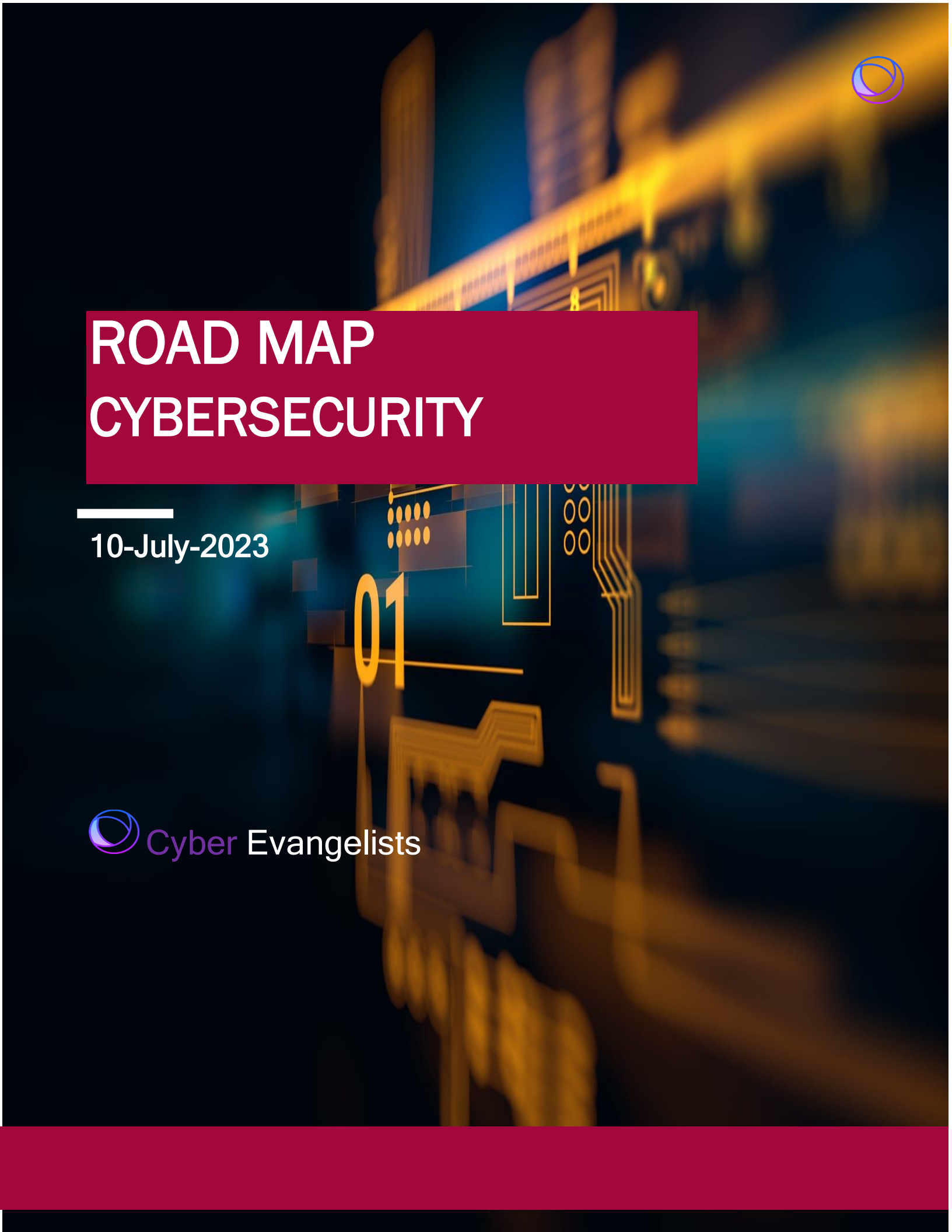


ROAD MAP CYBERSECURITY

10-July-2023

Cyber Evangelists

Table of Contents

Journey to Cybersecurity

Why is Cybersecurity?

Cybersecurity is a Layer of Information security that protects computer systems, networks, and digital information from unauthorized access, attacks, and damage, ensuring data confidentiality, integrity, and availability in the face of evolving cyber threats.

Pre-requisites

- Understanding computer hardware components
- Familiarity with different connection types (Ethernet, Wi-Fi, Bluetooth, NFC, Infrared)
- Troubleshooting common operating system issues
- Knowledge of popular websites and their basic functionality (iCloud, Google Suite)
- Basic understanding of computer networking concepts (IP addressing, subnetting, protocols)

Module 01- OS Path

Course Learning Outcome

After completion of this module, you will

CLO's	Description
1	Understand the different type of OS and their version like Linux (RedHat, Debian), MacOS, windows
2	Able to Installation and Configuration OS
3	Grant permissions and perform crud on files

Content

Proficiency in various operating systems (e.g., Windows, Linux) is necessary for securing and administering computer systems.

1. Installation and Configuration
2. Navigating using GUI and CLI (Administration and troubleshooting).
3. Installing Software and Applications (Manages libraries and dependencies).
4. Performing CRUD on Files (Create, Read, Update, and delete files and directories)
5. Troubleshooting (Resolve issues such as System crashes)
6. Common Commands (commands of Linux, Windows, or MacOS to interact with CLI).

Module 02- Network Phase

Course Learning Outcome

After completion of this module, you will

CLO's	Description
1	Understand of OSI model, Common ports, and protocol
2	Understand network topologies
3	Understand IP terminology and subnetting
4	Able to use common virtualization technologies and tools

Content

Networking knowledge is essential in cybersecurity for analyzing network traffic, identifying vulnerabilities, implementing secure configurations, and safeguarding against network-based threats.

1. OSI Model (Physical, Data Link, Network, Transport, Session, Presentation, Application)
2. Common Protocols (TCP/IP, HTTP, FTP, DNS, SNMP, SSH, SSL/TLS, and RFD)
3. Network Topologies (Star, Ring, Mesh, Bus).
4. IP Terminologies (localhost, loopback, CIDR, Subnet Mask, default gateway)
5. Troubleshooting tools (ns lookup, iptables, port scanner, netstat, ping, arp)
6. Virtualization tools and technologies (VM Ware, virtual Box, Hypervisor, Hostos)
7. Authentication methodologies (Kerberos, LDAP, SSO, Local Auth, RADIUS).

Module 03- Security Phase

Course Learning Outcome

After completion of this module, you will

CLO's	Description
1	Understand different types of attack and their mitigation technique
2	Understand CIA Triad
3	Understand Hacking tools and Frameworks
4	Incident Response and Forensics

Content

Security Skills and Knowledge, cybersecurity professionals can effectively protect systems, networks, and data from a wide range of threats and ensure a robust security posture.

1. Attack Types and Differences (Phishing, Tailgating, DDOS/DOS, Social Engineering, Brute force/Password Spray, Zero Day, reconnaissance)
2. Cryptography (Salting, Hashing, Key Exchange, Obfuscation, PKI)
3. Threat Intelligence (APT, Zero Day).
4. Frameworks and standards (Kill Chain, Diamond Model, ATT&CK, CIS, CSF, NIST, ISO)
5. Incident Response process and tools (Preparation, Identification, Containment, Eradication, Recovery, Lesson Learned, Nmap, autopsy, grep, tail, arp, ipconfig)
6. Security Tools: (SIEM, IDS, IPS).
7. Secure Coding (Prevent XSS, CSRF)

8. Security Protocols (FTP/SFTP, SSL/TLS, IPSEC, DNSSEC, LDAPS, SRTP)
9. Hardening Concepts (MAC-based, NAC-based, Port Blocking, ACLs, Sinkholes, Patching Endpoint Security)
10. Security Tools (Virus Total, Joe Sandbox, any. run, avoid, URLs can, WHOIS)
11. Targeted Audience (Stakeholder, HR, Legal, Compliance, Management)

Module 04- Cloud Phase

Course Learning Outcome

After completion of this module, you will

CLO's	Description
1	Understand concepts of security in the cloud
2	Understand the basic and general flow of deploying in the cloud
3	Understand the difference between cloud and on-premises
4	Understand the concept of infrastructure as code
5	Understand the concept of Serverless
6	Understand the concept of CDN

Content

Cloud Skills and Knowledge, cybersecurity professionals can effectively secure cloud infrastructure, protect data, and ensure compliance in cloud environments.

1. Cloud Services (IaaS, PaaS, and SaaS).
2. Cloud Models (Public, Private, Hybrid)
3. Cloud Environments (AWS, GCP, Azure)
4. Cloud Storage (DropBox, Box, S3, OneDrive, iCloud, Google Drive)

Module 05- Programming (Optional)

Course Learning Outcome

CLOs	Description
1	Understand Basic of Programming Language

Content

1. Python
2. C++/C
3. JavaScript
4. GO
5. Bash
6. PowerShell

Hands-on Experience Platforms (CTFs)

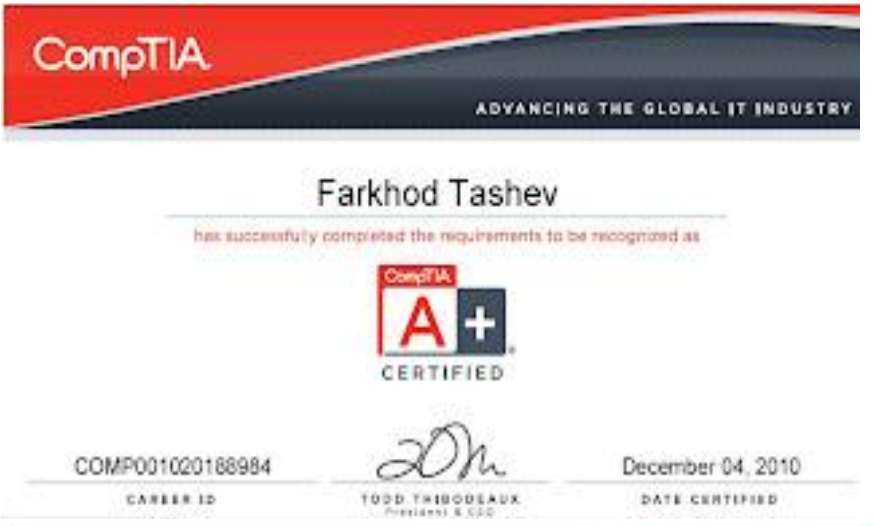
These hands-on experience platforms provide opportunities for individuals to apply their knowledge, develop practical skills, and gain experience in real-world scenarios within the cybersecurity field.

1. Hack The Box: A popular online platform that offers a wide range of vulnerable machines and challenges to practice penetration testing and offensive security skills.
2. TryHackMe: An interactive platform that provides virtual environments and guided learning paths to help users gain practical experience in various cybersecurity domains.
3. VulnHub: A platform that hosts virtual machine images with intentionally vulnerable configurations, allowing users to practice their hacking and security skills in a safe and controlled environment.
4. PicoCTF: An educational platform that offers a series of capture-the-flag challenges suitable for beginners to advanced users, covering a wide range of cybersecurity topics.
5. SANS Holiday Hack Challenge: An annual holiday-themed CTF created by the SANS Institute, featuring a mix of puzzles, challenges, and real-world scenarios to test and enhance cybersecurity skills.

Certifications

Here some Certifications are needed.
Certifications for Beginner in Cybersecurity:

1. CompTIA A+
2. CompTIA Linux+
3. CompTIA Network+
4. Cisco Certified Network Associate (CCNA)
5. CompTIA Security+


CompTIA
ADVANCING THE GLOBAL IT INDUSTRY

Farkhod Tashev

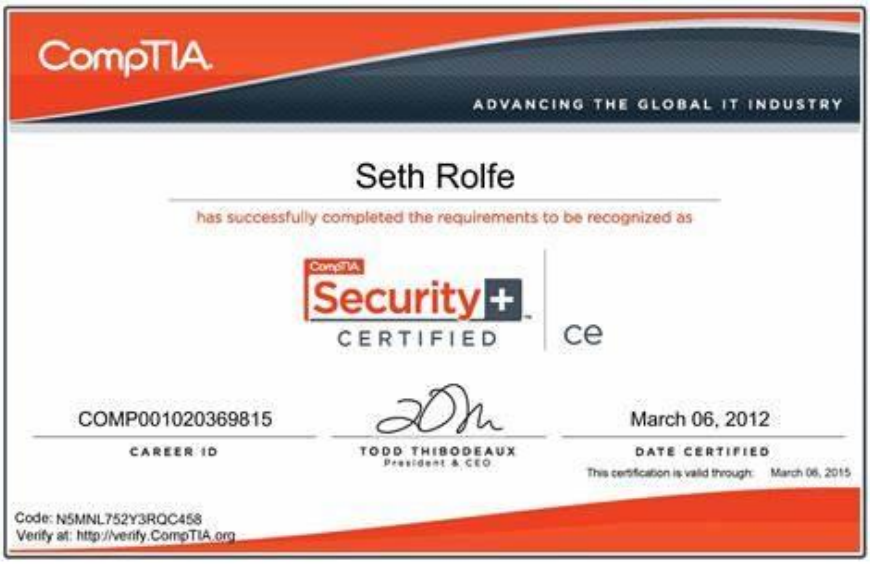
has successfully completed the requirements to be recognized as

CompTIA A+ CERTIFIED

COMP001020188984 — CAREER ID

TODD THIBODEAUX, President & CEO

December 04, 2010 — DATE CERTIFIED


CompTIA
ADVANCING THE GLOBAL IT INDUSTRY

Seth Rolfe

has successfully completed the requirements to be recognized as

CompTIA Security+ CERTIFIED ce

COMP001020369815 — CAREER ID

TODD THIBODEAUX, President & CEO

March 06, 2012 — DATE CERTIFIED

This certification is valid through: March 06, 2015

Code: N5MNL752Y3RQC458
Verify at: http://verify.CompTIA.org


CISCO

Cisco Certifications

Mohammad A. Mannan

HAS SUCCESSFULLY COMPLETED THE CISCO CERTIFICATION REQUIREMENTS AND IS RECOGNIZED AS A

Cisco Certified Network Associate

CISCO CERTIFIED CCNA NETWORK

CERTIFICATION DATE September 22, 2012
VALID THROUGH September 22, 2015
CISCO ID NO. CSCO12224571

Validate this certificate's authenticity at www.cisco.com/go/verifycertificate
Certificate Verification No. 411919741307HLZL

John Chambers
Chairman and CEO
Cisco Systems, Inc.

Certifications for Advanced in Cybersecurity:

1. Certified Information Systems Security Professional (CISSP)
2. Certified Information Systems Auditor (CISA)
3. Certified Information Security Manager (CISM)
4. GIAC Security Essentials (GSEC)
5. GIAC Penetration Tester (GPEN)
6. GIAC Web Application Penetration Tester (GWAPT).
7. Offensive Security Certified Professional (OSCP).
8. CREST Certified Tester (CCT)
9. Certified Ethical Hacker (CEH)


International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Vladimir Buldyzhov

the credential of

Certified Information Systems Security Professional

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

Dr. Kevin Charest - Chairperson

Lori Ross O'Neil - Secretary

CISSP

ANSI ISO/IEC 17024

475694
Certification Number

Jun 1, 2020 - May 31, 2023
Certification Cycle

Certified Since: 2014

(ISC)²

Verify Member is in good standing at:www.isc2.org/verify

Printed On: 6/1/2020


Certification Number
ECC28711706812

C|EH Certified Ethical Hacker

This is to acknowledge that

John Lloyd Lagura

has successfully completed all requirements and criteria for

Certified Ethical Hacker

certification through examination administered by EC-Council

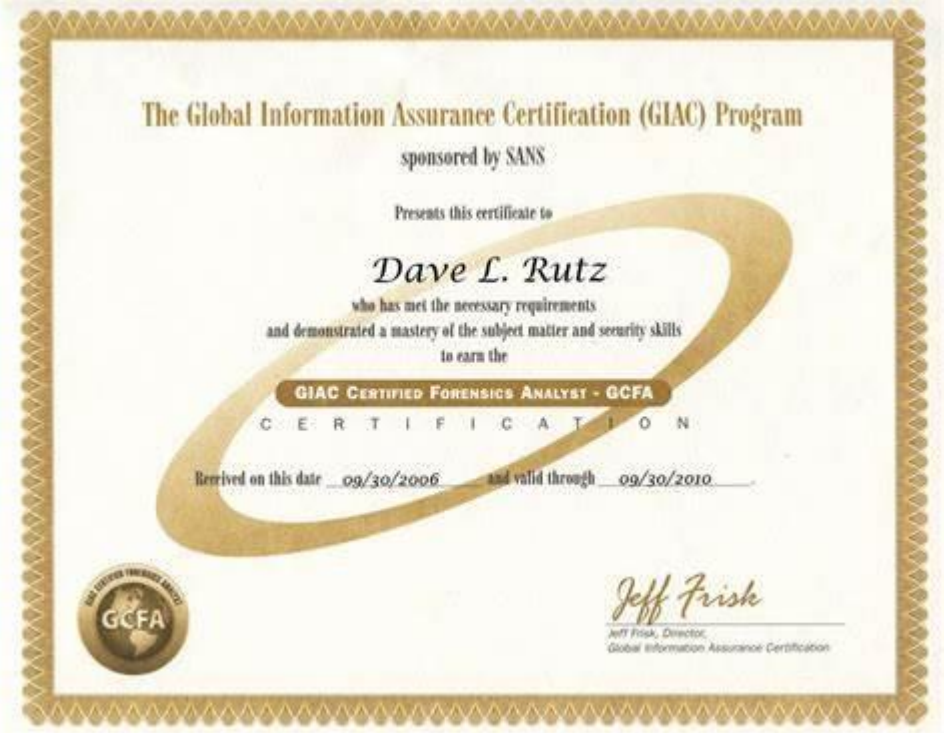
Issue Date: 11 May, 2018

Expiry Date: 10 May, 2021

ANSI

EC-Council

Sanjay Bavisi, President



Further Resources:

1. Website and Blogs:
    - SecurityWeek (www.securityweek.com)
    - Krebs on Security (krebsonsecurity.com)
    - The Hacker News (thehackernews.com)
    - SANS Institute (www.sans.org)
    - OWASP (www.owasp.org)
2. Online Learning Platforms:
    - Cybrary (www.cybrary.it)
    - Udemy (www.udemy.com)
    - Coursera (www.coursera.org)
    - edX (www.edx.org)
    - Pluralsight (www.pluralsight.com)
3. Books:
    - "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto
    - "Hacking: The Art of Exploitation" by Jon Erickson
    - "Network Security Bible" by Eric Cole
    - "CISSP All-in-One Exam Guide" by Shon Harris and Fernando Maymí
    - "The Tangled Web: A Guide to Securing Modern Web Applications" by Michal Zalewski
4. Online Communities and Forums:
    - Reddit: r/netsec, r/AskNetsec, r/HowToHack
    - Stack Exchange: security.stackexchange.com
    - Hack Forums (www.hackforums.net)
5. Professional Organizations and Conferences:

- Information Systems Security Association (ISSA)
- DEF CON (www.defcon.org)
- Black Hat (www.blackhat.com)
- RSA Conference (www.rsaconference.com)

6. Security Tools and Frameworks:
    - Metasploit Framework
    - Wireshark
    - Nmap
    - Burp Suite
    - Open Web Application Security Project (OWASP)

Keynote's

Cybersecurity covers networking, operating systems, and security practices. Knowledge of protocols, network architecture, and secure communication is vital. Operating systems require installation, configuration, troubleshooting, and securing user permissions. Security practices involve network, web, and cloud security, incident response, and using security tools. Certifications like CompTIA Security+ and CEH validate foundational skills. CTF competitions (e.g., Hack The Box, picoCTF) enhance problem-solving abilities. Combining certifications and CTFs develops a comprehensive skill set for staying competitive in cybersecurity.