# 10 อันดับใบรับรองด้าน Cybersecurity ที่น่าสนใจ

*Sumedt Jitpukdebodin*
*Ammarit Thongthua*
*Secure D Center Co., Ltd.*


# Background and Experience

We operate across the ASEAN region with offices established in Kuala Lumpur, Malaysia and Bangkok, Thailand. We are independent and committed to your long-term goals by bringing a fresh, independent perspective, high passion to do an outstanding job and delivering cost-effective, innovation and high value services using global methodology and framework with our best cyber expertise certified by well-known cyber security certifications.

We trust you will recognize our pragmatic 'hands on' style in the way we have structured our team, our approach and our deliverables. Our approach is based on the simple notion that the success of this project is measured by the results obtained and not just successful completion.

# Cybersecurity Professional Services

## Professional Services

Our cyber security professionals have extensive experience in Incident Response, Threat Hunting, Digital Forensic and Investigation, and understand the technical and real-world scenario of cyber attack

# Cybersecurity Professional Services

## Security Assessment and Penetration Testing

**This service included Red Teaming, Penetration Testing, and Vulnerability Assessment. Our methodology is developed based on various of penetration testing framework and standard including NIST, Cyber Kill Chain, CBEST/CREST STAR and OWASP for our methodology.**

- ❑ *Vulnerability Assessment (VA)*
- ❑ *Infrastructure and Network Penetration Testing*
- ❑ *Web and Web Application Penetration Testing*
- ❑ *Mobile Application Penetration Testing*
- ❑ *Kiosk , ATM , VTM Penetration Testing*
- ❑ *Red Teaming Operation*

# Cybersecurity Professional Services

## Cyber Incident Response and Defensive Service

**Our cyber security professionals have extensive experience in Incident Response, Threat Hunting, Digital Forensic and Investigation, and understand the technical and real-world scenario of cyber attack**

- ❑ *Cybersecurity Incident Response (IR)*
- ❑ *SOC Improvement Consultant*
- ❑ *Digital Forensic and Incident Case Investigation (DF)*
- ❑ *Compromised Assessment (CA)*
- ❑ *Threat Hunting*
- ❑ *Cybersecurity Incident Exercise / Tabletop Exercise (TTX)*
- ❑ *Threat Intelligence (TI)*

# Cybersecurity Professional Services

## Compliance and Audit

**Our cyber security professionals specialize in IT Security consulting including SSDLC, PCI DSS, ISO27001 and other Compliances / Regulations with comprehensive experience in implementation of related processes in term of technical and business**

- *ISO27001 Implementation Consulting*
- *IT and IT Security Compliance Consulting*
- *Internal IT Audit (IA)*
- *NDID MQA Assessment*
- *IT Security Awareness Training*
- *Phishing Drill Testing*

# Cybersecurity Training Platform

## SECPlayground – Cybersecurity Training Platform


**SECPlayground is a cyber security training platform. We offer approachable and accessible hands-on exercise and content by domain experts**

- ❑ *Cybersecurity Knowledge*
- ❑ *Network Security and Web Application Security*
- ❑ *Forensic (Network Analysis ,Disk Analysis ,Log Analysis ,Memory Analysis*
- ❑ *Privilege Escalation*
- ❑ *New Public CVEs*
- ❑ *Secure Software Development (SSDLC) and Secure Source Coding*
- ❑ *Mobile Security*
- ❑ *SOC Analyst and Incident Response*

# Cybersecurity Challenges

- The National Cyber Security
- Authority (NCSA) - THNCA Cyber Academy

- The National Cyber Security Authority (NCSA)
- - Capture the Flag (CTF)

- ICT Mahidol
- - STDiO CTF Competition 2020

- Royal Thai Armed Forces -
- Cybersecurity Contest 2020

- Technology Crime Suppression Division
- - Cybersecurity Conference 2019



# Whoami

## Ammarit Thongthua – CEO @ Secure-D Center

**Background**

• Ammarit has over 18 years of hands-on experience in information systems security and penetration testing. He is proficient in the areas of penetration test, security assessment, information security management, and IT security solution and implementation.

• He conducted penetration test, security source code review, and performed information security operation for large TELCO and large E-commence company. He had implemented various kinds of security system and solution i.e. Intrusion Prevention Detection, Advance Persistence Threat detection, Anomaly Detection, Antivirus, VPN, Security Information and Event Management (SIEM), Vulnerability Management, and Data Loss Prevention. He also has experience in PCI-DSS, ISO27001 standard implementation.

**Professional and Industry Experience:**

• Published CVE security ( CVE-2020-14558, CVE-2020-14564, CVE-2020-9672, CVE-2020-9673,CVE-2020-5962, CVE-2020-3961, CVE-2019-8256, CVE-2019-9490, CVE-2019-7000, CVE-2018-1067, CVE-2016-5331) in many enterprise softwares and products

• Managed IT security projects including penetration test project and IT security solution implementation project for large medium & large banks and telecommunication.

• Performed black-box and grey-box Mobile Application Penetration tests and security source code review for large telecommunication, medium & large banks and large E-Commerce company on e.g. Electronic Payment, Online Service system.

• Performed security assessment on legacy application and system for the largest telecommunication in Thailand.

• Performed penetration test on Electronic Data Capture (EDC) machine, Automated Teller Machine (ATM), and Kiosk for large bank and telecommunication.

• Conducted the training for technical staff on Secured Software Development Life Cycle course (SSDLC) for large telecommunication and E-Commerce company.

• Conducted research on new technology and tool to improve IT security and Defense in Depth: Security Information Management system, Vulnerability Management, Computer Forensics, Spam mail filtering, etc.

• Conducted the training and knowledge sharing for OWASP and 2600 Thailand IT security community.

**Certification:**

- CISSP, CISM, GXPN, OSCP, C|EHv6, CompTIA Security+, CCNA, CCNP

# Whoami

## Sumedt Jitpukdebodin – CPO @ Secure-D Center

### Background

- Sumedt has over 14 years of hands-on experience in information systems security and penetration testing. He is proficient in the areas of penetration test, Incident handling and response, digital forensic and investigation.
- He conducted penetration test, security source code review, security consultant and performed information security operation for many enterprise company in Thailand. He had implemented various kinds of security system and solution i.e. Intrusion Prevention Detection, Advanced Persistent Threat detection, Anomaly Detection, Antivirus, Security Information and Event Management (SIEM), Vulnerability Management.
- He wrote a Thai security book name's "Network Security and Penetration Testing"

### Professional and Industry Experience:

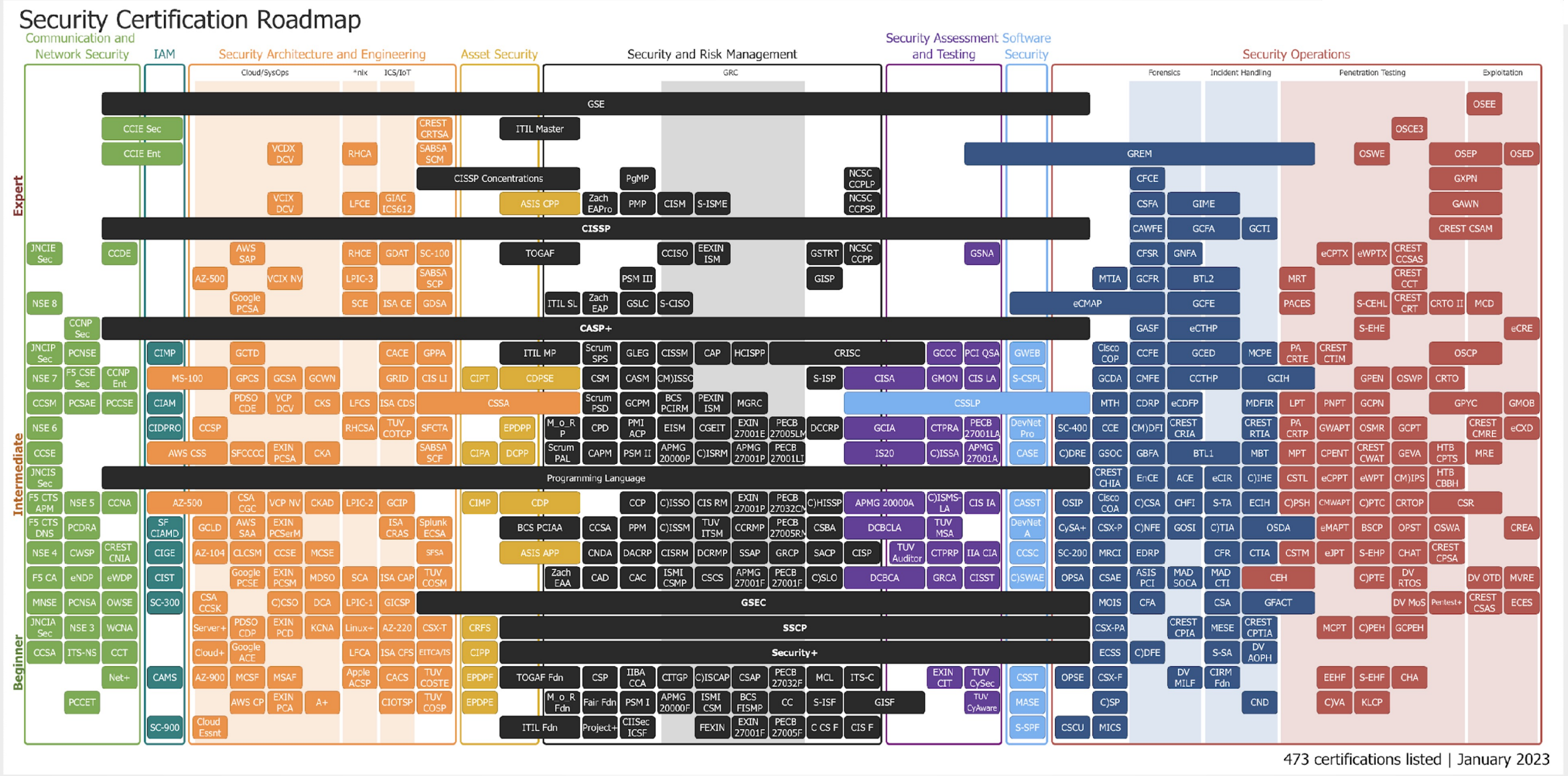
- Published CVE security vulnerabilities (CVE-2019-6832) on Schneider Electric homeLYnk product
- Managed IT security projects including penetration test project and IT security solution implementation project for large medium & large banks and telecommunication.
- Performed black-box and grey-box penetration test, mobile application penetration tests and security source code review for enterprise companies in SEA country.
- Performed incident response, digital forensic, log analysis and malware analysis for medium and large companies.
- Conducted the practical ethical hacking subject for master degree student in lecturer position at Mahidol university.
- Researched on new blue team and red team technique: malware analysis, digital forensic, APT activity, security solution, evading antivirus, obfuscate payload, bypassing security perimeter, etc.
- Developed training platform for educate security operator.
- Cybersecurity challenge (CTF) creator in many security events in Thailand.
- Implemented, customized, and configured on security device e.g. IPS, IDS, Web Application Firewall and SIEM.
- Created curriculum and conducted security training courses in network, web application security, log management, incident response, for large companies.
- Conducted the training and knowledge sharing for OWASP and 2600 Thailand IT security community.

### Certification:

- CC, GPEN, OSCP, CPTE, CompTIA Pentest+, CompTIA CySA+, CompTIA Security+, eCPPT, eWPT

# Cybersecurity Certification

# Overall Cybersecurity




https://pauljerimy.com/security-certification-roadmap/

# 10 Cybersecurity Certifications

| Certification | Price | Type of Certification | Level |
|---|---|---|---|
| CompTIA Security+ | $392 | Fundamental | Beginner |
| CompTIA CASP+ | $494 | Management | Intermediate |
| CompTIA Pentest+ | $392 | Offensive | Beginner |
| (ISC)² Certified Information System Security Professional (CISSP) | $749 | Management | Advanced |
| ISACA Certified Information Security Manager (CISM) | $760 | Management | Advanced |
| ISACA Certified Information Systems Auditor (CISA) | $760 | Management | Advanced |
| Offensive Security Certified Professional (OSCP) | $1599 | Offensive | Intermediate |
| Offensive Security Web Expert (OSWE) | $1599 | Offensive | Intermediate |
| eLearnSecurity Junior Penetration Tester (eJPT) | $200 | Offensive | Beginner |
| GIAC Reverse Engineering Malware (GREM) | $949 | Defensive | Intermediate |



*** Disclaimer: The list of certification was gathering from Reddit user only

# Top 10 Cybersecurity Certifications with ChatGPT

| Certification | Price | Type of Certification | Level |
|---|---|---|---|
| Certified Information Systems Security Professional (CISSP) | $749 | Management | Advanced |
| Certified Information Systems Auditor (CISA) | $760 | Management | Advanced |
| Certified Ethical Hacker (CEH) | $1199 | Fundamental | Beginner |
| GIAC Certified Incident Handler (GCIH) | $949 | Fundamental | Beginner |
| CompTIA Security+ | $392 | Fundamental | Beginner |
| Certified in the Governance of Enterprise IT (CGEIT) | $575 | Management | Advanced |
| Certified Information Security Manager (CISM) | $760 | Management | Advanced |
| Systems Security Certified Practitioner (SSCP) | $249 | Fundamental | Beginner |
| Certified in the Risk and Information Systems Control (CRISC) | $575 | Management | Advanced |
| Certified Information Systems Security Professional (CISSP) - ISSEP | $599 | Management | Advanced |



*** ChatGPT training data was not more than 2021

# Top 10 Technical Cybersecurity Certification with ChatGPT

| Certification | Price | Type of Certification | Level |
|---|---|---|---|
| Certified Information Systems Security Professional (CISSP) | $749 | Management | Advanced |
| Certified Ethical Hacker (CEH) | $760 | Management | Advanced |
| GIAC Certified Incident Handler (GCIH) | $949 | Fundamental | Beginner |
| CompTIA Security+ | $392 | Fundamental | Beginner |
| Offensive Security Certified Professional (OSCP) | $1599 | Offensive | Intermediate |
| Certified Penetration Testing Engineer (CPTE) | $550 | Offensive | Beginner |
| Certified Information Systems Auditor (CISA) | $575 | Management | Advanced |
| Certified in the Governance of Enterprise IT (CGEIT) | $575 | Management | Advanced |
| Certified Information Security Manager (CISM) | $760 | Management | Advanced |
| EC-Council Certified Security Analyst (ECSA) | $999 | Fundamental | Beginner |



*** ChatGPT training data was not more than 2021

# Fundamental Cybersecurity Certification

## Fundamental Cybersecurity Certification

- CompTIA Security+
- (ISC)² Certified in Cybersecurity (CC)
- (ISC)² Systems Security Certified Practitioner (SSCP)
- GIAC Security Essentials (GSEC)

# Fundamental Cybersecurity Certification

## Security+ opens the door to your cybersecurity career!

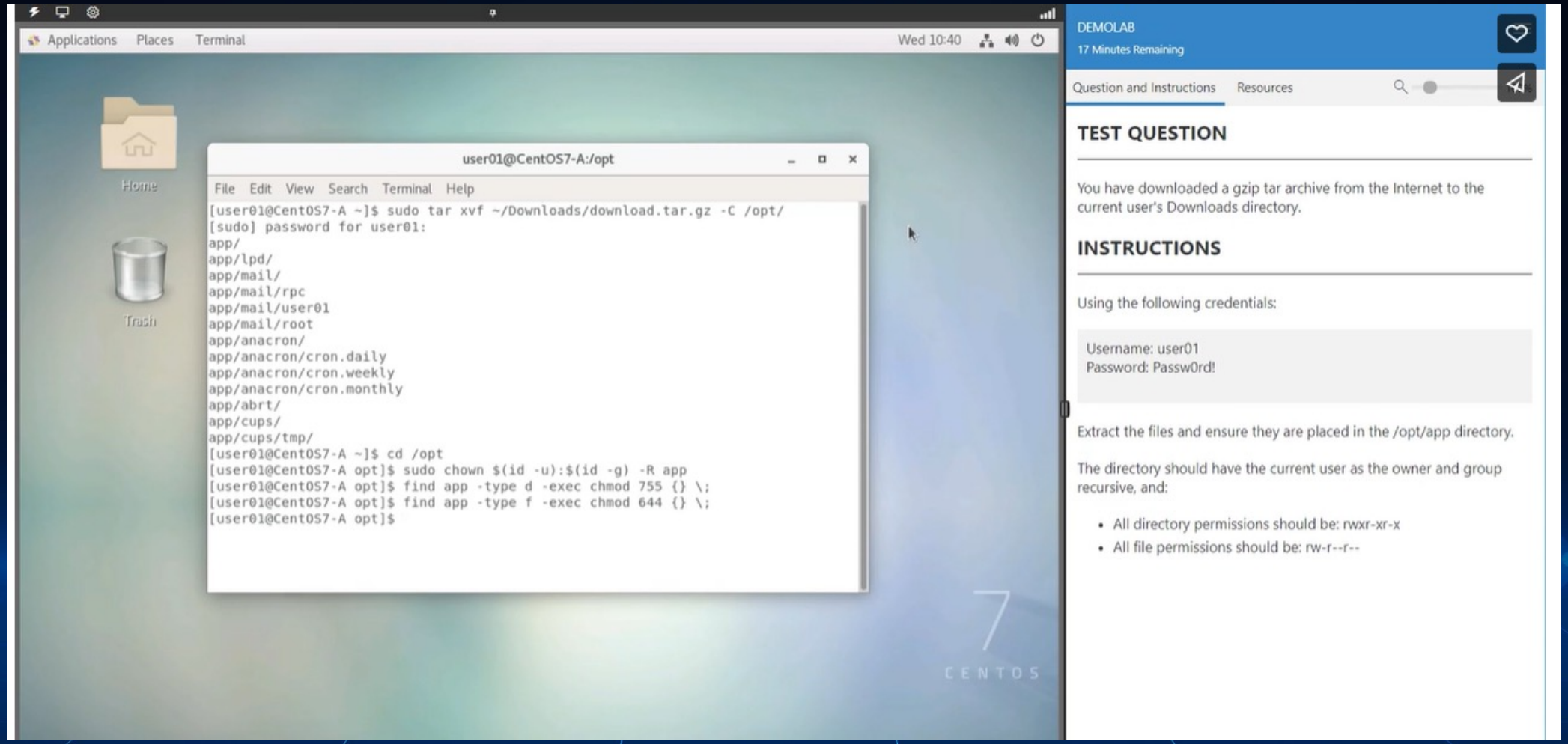

### EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented:

| DOMAIN | PERCENTAGE OF EXAMINATION |
|---|---|
| 1.0 Threats, Attacks and Vulnerabilities | 21% |
| 2.0 Technologies and Tools | 22% |
| 3.0 Architecture and Design | 15% |
| 4.0 Identity and Access Management | 16% |
| 5.0 Risk Management | 14% |
| 6.0 Cryptography and PKI | 12% |
| **Total** | **100%** |

# Fundamental Cybersecurity Certification

## Example of Security + performance-based exam question



# Fundamental Cybersecurity Certification

## (ISC)² Opens Global Enrollment for One Million Certified in Cybersecurity

AUGUST

31 / 2022

*(ISC)² pledges to expand and diversify the cybersecurity workforce by providing free (ISC)² Certified in Cybersecurity℠ education and exams to one million people worldwide*

**Alexandria, Va., August 31, 2022** – (ISC)² – the world's largest nonprofit association of certified cybersecurity professionals – today announced that the (ISC)² One Million Certified in Cybersecurity initiative is now accepting participants. To qualify, individuals must enroll as an (ISC)² Candidate, for free, which entitles them to a wide array of exclusive programs and services to assist individuals starting a cybersecurity career, including free education and exams for the association's new entry-level cybersecurity certification (ISC)² Certified in Cybersecurity℠.

# Fundamental Cybersecurity Certification

There are five domains covered on the exam.

- Security Principles
- Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts
- Access Controls Concepts
- Network Security
- Security Operations

# Fundamental Cybersecurity Certification

## SSCP – The Premier Security Administrator Certification

### Who Earns the SSCP?

The SSCP is ideal for IT administrators, managers, directors and network security professionals responsible for the hands-on operational security of their organization's critical assets, including those in the following positions:

- Network Security Engineer
- Systems Administrator
- Security Analyst
- Systems Engineer
- Security Consultant/Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator

# Fundamental Cybersecurity Certification

## Areas Covered

- Defense in depth, access control and password management
- Cryptography: basic concepts, algorithms and deployment, and application
- Cloud: AWS fundamentals, Microsoft cloud
- Defensible network architecture, networking and protocols, and network security
- Incident handling and response, data loss prevention, mobile device security, vulnerability scanning and penetration testing
- Linux: Fundamentals, hardening and securing
- SIEM, critical controls, and exploit mitigation
- Web communication security, virtualization and cloud security, and endpoint security
- Windows: access controls, automation, auditing, forensics, security infrastructure, and services


GIAC CERTIFICATIONS

## Exam Format

- 1 proctored exam
- 106-180 questions
- Time limit of 4-5 hours
- Minimum passing score of 73%

# Fundamental Cybersecurity Certification

| | CompTIA Security+ | (ISC)2 Systems Security Certified Practitioner (SSCP) | EC-Council Certified Ethical Hacker (CEH) | GIAC Security Essentials (GSEC) |
|---|---|---|---|---|
| Performance Based Questions | ✓ | | | |
| Experience Level | Entry-level cybersecurity | Entry-level security | Entry-level penetration testing | Entry-level cybersecurity |
| Exam Focus | Core cybersecurity skills required by security and network administrators | Basic concepts of computing and security | Penetration Testing | Basic understanding of information security beyond simple concepts |
| Vendor Neutral | Yes | Yes | Yes | Yes |

# Offensive Security Certification

## Offensive Security Certification

- GIAC Penetration Tester (GPEN)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- GIAC Certified Web Application Defender (GWEB)
- Offensive Security Certified Professional (OSCP)
- Offensive Security Web Assessor (OSWA)
- Offensive Security Web Expert (OSWE)
- CompTIA Pentest+
- ECCOUNCIL – Certified Ethical Hacker (C|EH)
- Certified Red Team Professional (CRTP)
- eLearnSecurity Mobile Application Penetration Tester (eMAPT)
- GIAC Mobile Device Security Analyst (GMOB)

# Offensive Security Certification

- Module 01: Introduction to Ethical Hacking +
- Module 02: Foot Printing and Reconnaissance +
- Module 03: Scanning Networks +
- Module 04: Enumeration +
- Module 05: Vulnerability Analysis +
- Module 06: System Hacking +
- Module 07: Malware Threats +
- Module 08: Sniffing +
- Module 09: Social Engineering +
- Module 10: Denial-of-Service +
- Module 11: Session Hijacking +
- Module 12: Evading IDS, Firewalls, and Honeypots +
- Module 13: Hacking Web Servers +
- Module 14: Hacking Web Applications +
- Module 15: SQL Injection +
- Module 16: Hacking Wireless Networks +
- Module 17: Hacking Mobile Platforms +
- Module 18: IoT and OT Hacking +
- Module 19: Cloud Computing +
- Module 20: Cryptography +

EC-Council
Hackers are here. Where are you?

C|EH™
Certified Ethical Hacker

### C|EH Knowledge Exam

- 125 multiple-choice questions
- 4 hours
- ANSI 17024 accredited

### C|EH Practical Exam

- 6 hours practical exam
- 20 scenario based questions
- Prove your skills and abilities

# Offensive Security Certification

## PEN-200

### PENETRATION TESTING WITH KALI LINUX

PEN-200 (PWK) is our foundational penetration testing course. Students learn the latest tools and techniques, and practice them in a virtual lab that includes recently retired OSCP exam machines. Earn your Offensive Security Certified Professional (OSCP) certification.

Starting at
$1599

Register for PEN-200

Level: ●●○○

# Offensive Security Certification

## Exam Structure

**60 points**

3 independent targets

- 2-step targets (low and high privileges)
- Buffer Overflow may (or may not) be included as a low-privilege attack vector
- 20 points per machine
  - **10** points for low-privilege
  - **10** points for privilege escalation

**40 points**

2 clients
1 domain controller

- Active Directory set
- Points are awarded only for the full exploit chain of the domain
- No partial points will be awarded

# Defensive Security Certification

## Defensive Security Certification

- CompTIA CySA+
- ECCOUNCIL – Computer Hacking Forensic Investigator (CHFI)
- eLearnSecurity Certified Digital Forensics Professional (eCDFP)
- GIAC Reverse Engineering Malware (GREM)
- GIAC Security Operations Certified (GSOC)
- Blue Team Level 1 (BTL1)
- Blue Team Level 2 (BTL2)
- Offensive Security Defence Analyst (OSDA) certification

# Defensive Security Certification

CompTIA Cybersecurity Analyst (CySA+) is an IT workforce certification


## EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented. The CompTIA CySA+ exam is based on these objectives.

| DOMAIN | PERCENTAGE OF EXAMINATION |
|---|---|
| 1.0 Threat Management | 27% |
| 2.0 Vulnerability Management | 26% |
| 3.0 Cyber Incident Response | 23% |
| 4.0 Security Architecture and Tool Sets | 24% |
| **Total** | **100%** |

# Defensive Security Certification

- Domain 1 - Security Fundamentals +
- Domain 2 - Phishing Analysis +
- Domain 3 - Threat Intelligence +
- Domain 4 - Digital Forensics +
- Domain 5 - SIEM +
- Domain 6 - Incident Response +

- Categorizing Phishing Emails
- Manual Artifact Extraction
- Attachment Analysis
- Phishing Response Capstone
- NEW – Threat Intelligence Platform: MISP
- NEW – OpenCTI and MISP
- Identifying File Systems
- Metadata and File Carving
- Hashing and Integrity
- NEW – Data Acquisition
- Windows Investigation 1
- Windows Investigation 2
- Volatility For Memory Analysis
- Autopsy For Disk Analysis
- Windows Event Log Analysis
- Splunk Investigation 1
- Splunk Investigation 2
- Splunk Investigation 3
- Splunk Investigation 4
- Wireshark Network Investigations (x3)
- DeepBlueCLI For Event Log Analysis
- CMD and PowerShell For Incident Response
- NEW – Suricata and Snort Analysis

# Defensive Security Certification

## EC-Council Certified Incident Handler (ECIH)


### Course Outline

Module 01: Introduction to Incident Handling and Response

Module 02: Incident Handling and Response Process

Module 03: Forensic Readiness and First Response

Module 04: Handling and Responding to Malware Incidents

Module 05: Handling and Responding to Email Security Incidents

Module 06: Handling and Responding to Network Security Incidents

Module 07: Handling and Responding to Web Application Security Incidents

Module 08: Handling and Responding to Cloud Security Incidents

Module 09: Handling and Responding to Insider Threats

# Cybersecurity Management Certification

## Cybersecurity Management & Audit Certification

- (ISC)² Certified Information System Security Professional (CISSP)
- ISACA - Certified Information Security Manager (CISM)
- ISACA - Certified Information Systems Auditor (CISA)
- CompTIA Advanced Security Practioner+ (CASP+)
- ITIL Managing Professional (ITIL MP)

# Cybersecurity Management Certification

| Domains | Average Weight |
|---|---|
| 1. Security and Risk Management | 15% |
| 2. Asset Security | 10% |
| 3. Security Architecture and Engineering | 13% |
| 4. Communication and Network Security | 13% |
| 5. Identity and Access Management (IAM) | 13% |
| 6. Security Assessment and Testing | 12% |
| 7. Security Operations | 13% |
| 8. Software Development Security | 11% |
| Total | 100% |

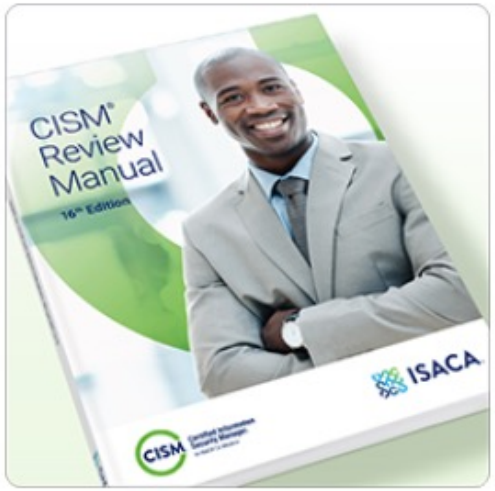
| | |
|---|---|
| **Length of exam** | 4 hours |
| **Number of items** | 125 - 175 |
| **Item format** | Multiple choice and advanced innovative items |
| **Passing grade** | 700 out of 1000 points |

# Cybersecurity Management Certification

## Certified Information Security Manager (CISM)

CISM Certified Information Security Manager
An ISACA® Certification

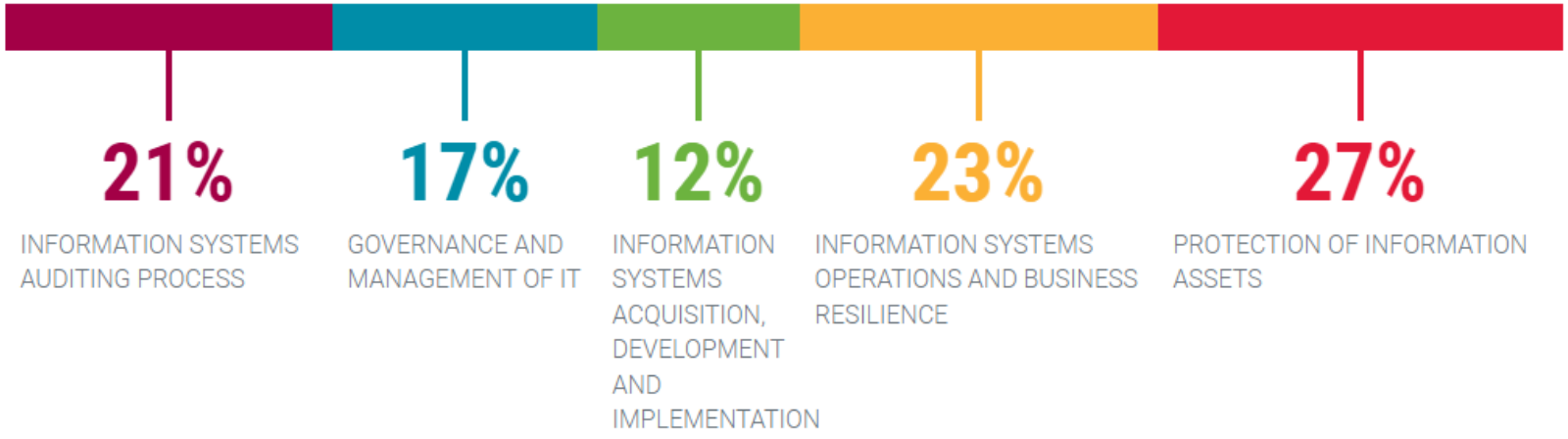
| 17% | 20% | 33% | 30% |
|---|---|---|---|
| INFORMATION SECURITY GOVERNANCE | INFORMATION SECURITY RISK MANAGEMENT | INFORMATION SECURITY PROGRAM | INCIDENT MANAGEMENT |



# Cybersecurity Management Certification

## Certified Information Systems Auditor (CISA)

CISA Certified Information Systems Auditor
An ISACA® Certification




# Certification from Cybersecurity training platform

## Cybersecurity training platform

- SECPlayground
- Hack The Box (HTB)
- TryHackMe
- PentesterLab
- Cyberdefenders
- Rangeforce
- Letsdefend
- Portswigger

# 4 notice about certification

- Certification mean nothing if you cheat it.
- Certification mean nothing when you on the field.
- Certification shall support by company.
- Certification need to maintain.



*** Disclamer: The list of Certification was gathering from Reddit user only

# Reference


- https://www.reddit.com/r/cybersecurity/comments/r9usal/what_certifications_are_most_useful_in_security/
- https://www.reddit.com/r/cybersecurity/comments/x5c0yi/if_you_could_only_obtain_3_Certifications_which/
- https://www.reddit.com/r/cybersecurity/comments/zi6nbe/what_skillsets_experience_or_certifications/
- https://www.reddit.com/r/cybersecurity/comments/zkn00z/certification_recommendations/
- https://www.reddit.com/r/cybersecurity/comments/yg2vil/i_just_passed_my_security_blue_team_level_1/
- https://www.reddit.com/r/cybersecurity/comments/yti6wu/certifications/
- https://www.reddit.com/r/cybersecurity/comments/xxtdi2/are_there_any_nontech_certifications_courses_that/
- https://www.reddit.com/r/cybersecurity/comments/xlsk0a/certifications/
- https://www.reddit.com/r/cybersecurity/comments/wvw33h/blue_team_certifications/
- https://www.reddit.com/r/cybersecurity/comments/vqm516/certifications_on_the_road_to_ciso/
- https://www.reddit.com/r/cybersecurity/comments/wre5m8/cybersecurity_certifications_for_linux/
- https://www.reddit.com/r/cybersecurity/comments/ta1xnt/which_certifications_should_you_go_for/
- https://www.reddit.com/r/cybersecurity/comments/v779tk/certification_and_career/
- https://www.comptia.org/
- https://www.offensive-security.com/
- https://www.isc2.org/
- https://www.isaca.org/
- https://www.eccouncil.org/
- https://www.sans.org/
- https://securityblue.team/


Secure D, your secure daemon