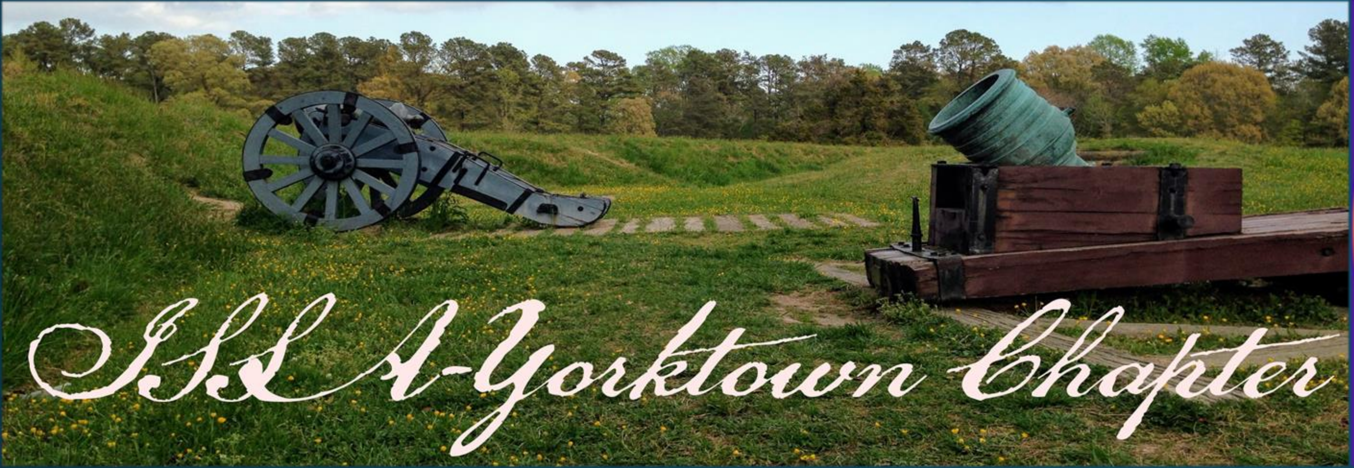


ISTI²

INFORMATION SECURITY TRAINING INSTITUTE, INC.

InfoSec Certifications

Why get them?

Robert W. (Bob) Hodges
Information Security Manager/ISO
BBA, CISSP, GCIH, GSEC Gold, GSLC Gold

Colonial Williamsburg®
THAT THE FUTURE MAY LEARN FROM THE PAST

Top 5 Certifications for 2017

- CISSP: Certified Information Systems Security Professional
- CISM: Certified Information Security Manager
- CompTIA Security+
- GCIH:SANS GIAC Certified Incident Handler/ CEH
- GSEC: SANS GIAC Security Essentials

Top 5 Certifications for 2017

Certification	SimplyHired	Indeed	LinkedIn Jobs	TechCareers	Total
CISSP	10,526	11,617	7,632	15,212	**44,987**
CISM	3,286	3,585	2,337	10,629	**19,837**
Security+	3,038	3,396	1,275	1,431	**9,140**
GCIH/CEH	1,977	2,184	1,427	257	**5,845**
GSEC	1,317	1,477	954	128	**3,876**

8570.1/ 8140.1

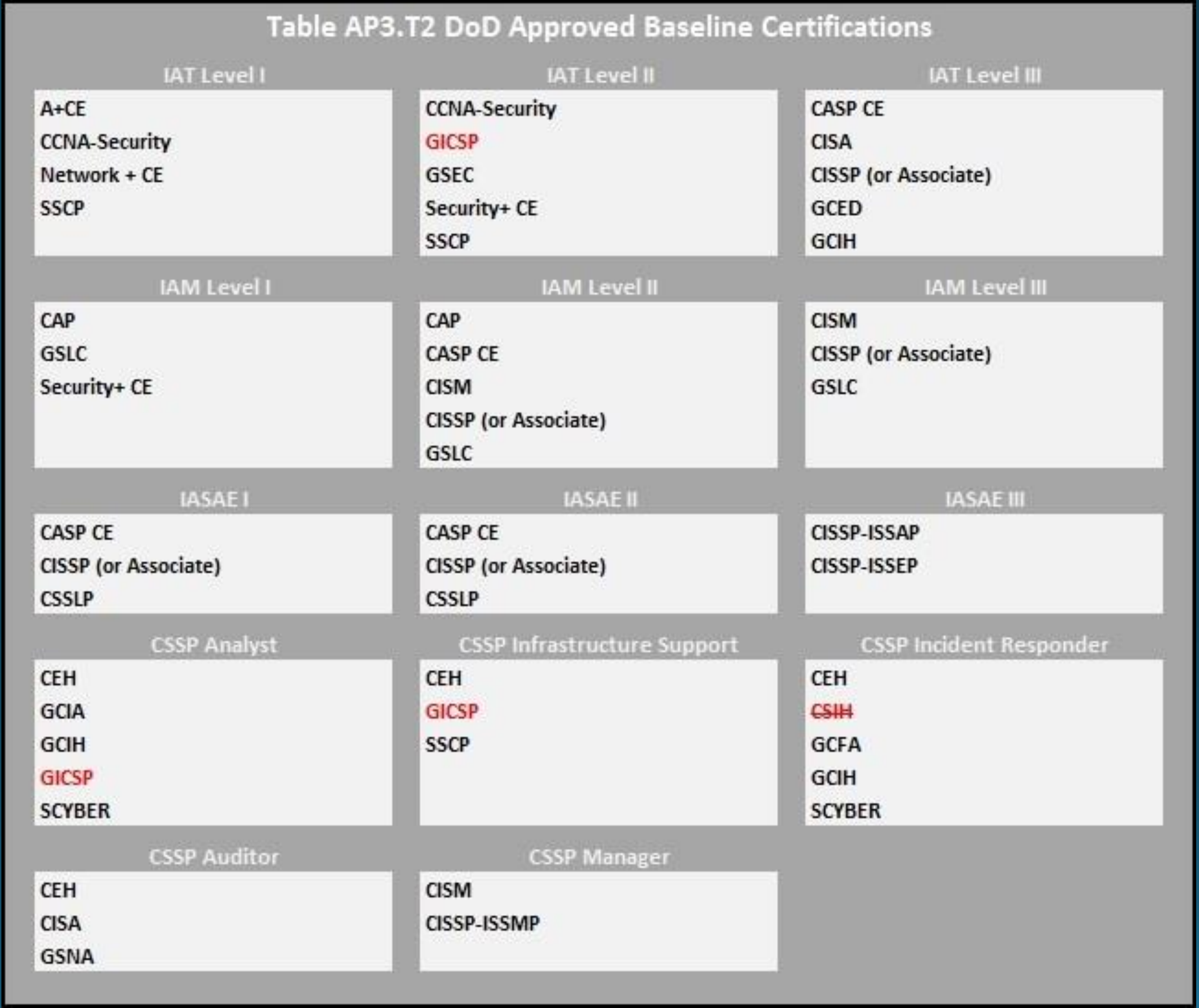


Table AP3.T2 DoD Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+CE	CCNA-Security	CASP CE
CCNA-Security	GICSP	CISA
Network + CE	GSEC	CISSP (or Associate)
SSCP	Security+ CE	GCED
	SSCP	GCIH

IAM Level I	IAM Level II	IAM Level III
CAP	CAP	CISM
GSLC	CASP CE	CISSP (or Associate)
Security+ CE	CISM	GSLC
	CISSP (or Associate)	
	GSLC	

IASAE I	IASAE II	IASAE III
CASP CE	CASP CE	CISSP-ISSAP
CISSP (or Associate)	CISSP (or Associate)	CISSP-ISSEP
CSSLP	CSSLP	

CSSP Analyst	CSSP Infrastructure Support	CSSP Incident Responder
CEH	CEH	CEH
GCIA	GICSP	~~CSIH~~
GCIH	SSCP	GCFA
GICSP		GCIH
SCYBER		SCYBER

CSSP Auditor	CSSP Manager
CEH	CISM
CISA	CISSP-ISSMP
GSNA	

2017

8570.1/ 8140.1

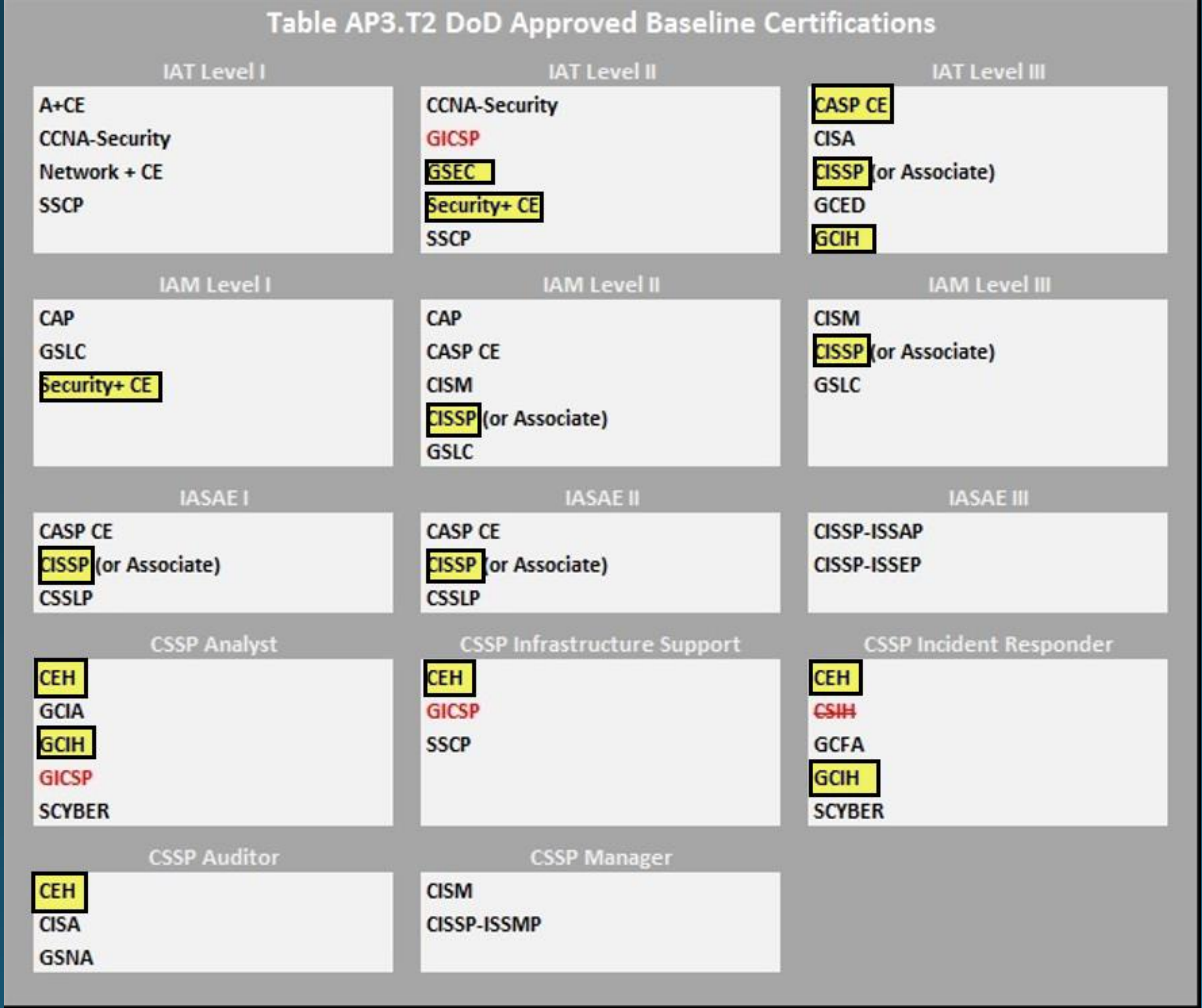


Table AP3.T2 DoD Approved Baseline Certifications

IAT Level I

- A+CE
- CCNA-Security
- Network + CE
- SSCP

IAT Level II

- CCNA-Security
- GICSP
- GSEC
- Security+ CE
- SSCP

IAT Level III

- CASP CE
- CISA
- CISSP (or Associate)
- GCED
- GCIH

IAM Level I

- CAP
- GSLC
- Security+ CE

IAM Level II

- CAP
- CASP CE
- CISM
- CISSP (or Associate)
- GSLC

IAM Level III

- CISM
- CISSP (or Associate)
- GSLC

IASAE I

- CASP CE
- CISSP (or Associate)
- CSSLP

IASAE II

- CASP CE
- CISSP (or Associate)
- CSSLP

IASAE III

- CISSP-ISSAP
- CISSP-ISSEP

CSSP Analyst

- CEH
- GCIA
- GCIH
- GICSP
- SCYBER

CSSP Infrastructure Support

- CEH
- GICSP
- SSCP

CSSP Incident Responder

- CEH
- ~~CSIH~~
- GCFA
- GCIH
- SCYBER

CSSP Auditor

- CEH
- CISA
- GSNA

CSSP Manager

- CISM
- CISSP-ISSMP

2017

CISSP versus CASP

CISSP Exam	CASP Exam
Per (ISC)^2, the CISSP cert claims to measure: *"knowledge and understanding of new threats, technologies, regulations, standards, and practices"*	Per CompTIA, the CASP cert claims to measure: *"technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments"* and *"competency in enterprise security; risk management; incident response; research and analysis; integration of computing, communications and business disciplines; and technical integration of enterprise components"*

CISSP versus CASP

CISSP Exam	CASP Exam
Per (ISC)^2, who the CISSP cert is for (by role): •Security Consultant •Security Manager •IT Director/Manager •Security Auditor •Security Architect •Security Analyst •Security Systems Engineer •Chief Information Security Officer •Director of Security •Network Architect •$599.00 •6 Hours •250 Questions	Per CompTIA, who the CASP cert is for (by role): •Cybersecurity / IS Professional •Information Security Analyst •Security Architect •IT Specialist INFOSEC •IT Specialist, Cybersecurity •$426.00 •2 ¾ Hours •90 Questions

CISSP versus CASP

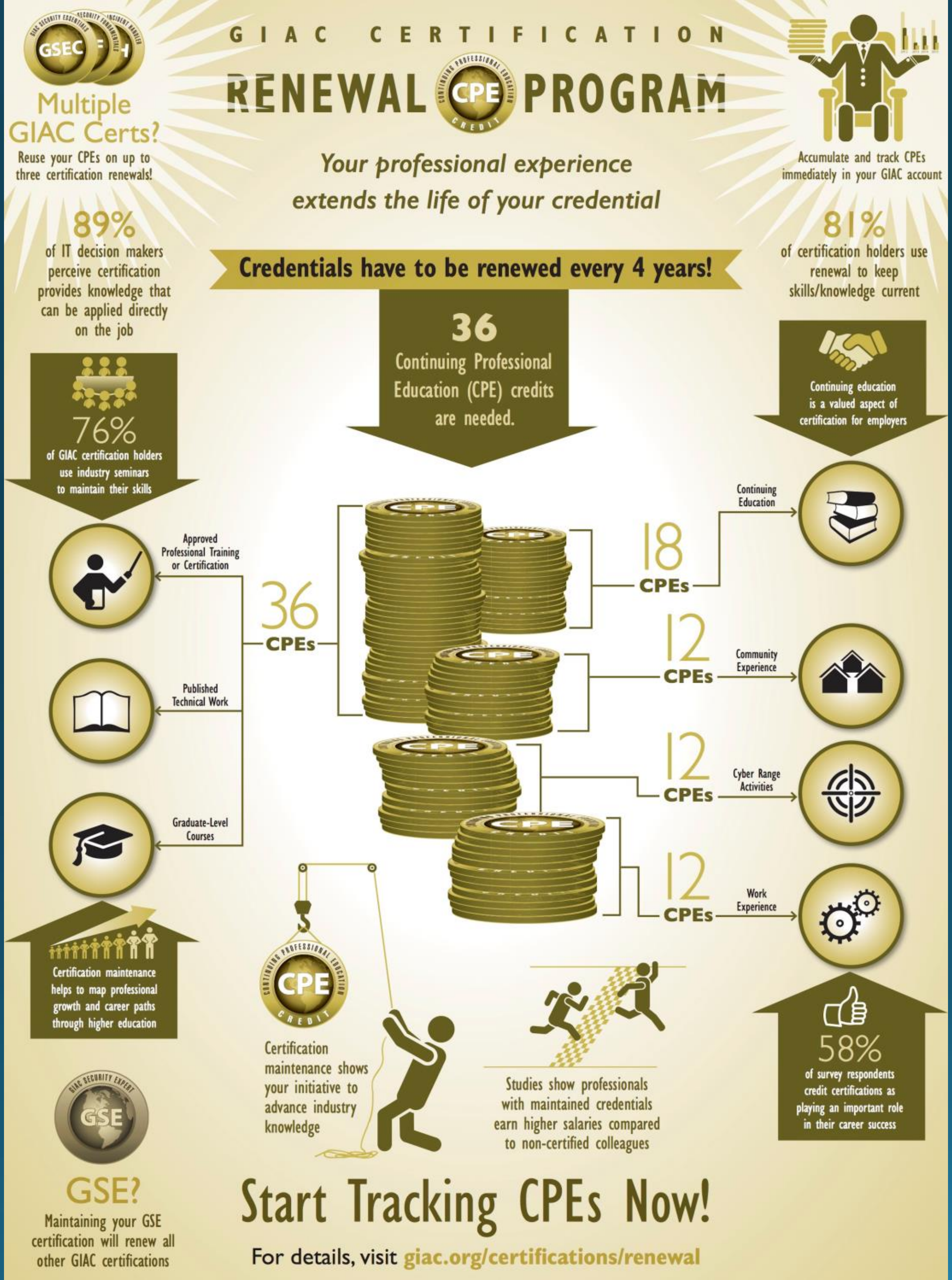
CISSP Certification	CASP Certification
$85.00 per year 120 CPEs per 3-year cycle.	$49.00 per year 75 CEUs per 3-year cycle.

CISSP versus CASP

- CASP exam is easier than the CISSP exam.
- CISSP Annual potential salary increase: $16,273

GSEC versus Security+

GSEC Certification	Security+ Certification
• 4 year cycle • 36 CPE's –or- • Retest • ~300-$700	• 3 year cycle • 50 CEU's • For life • $147 - $225



GIAC CERTIFICATION RENEWAL CPE PROGRAM

Your professional experience extends the life of your credential

Credentials have to be renewed every 4 years!

36 Continuing Professional Education (CPE) credits are needed.

Multiple GIAC Certs?

Reuse your CPEs on up to three certification renewals!

Accumulate and track CPEs immediately in your GIAC account

89% of IT decision makers perceive certification provides knowledge that can be applied directly on the job

81% of certification holders use renewal to keep skills/knowledge current

76% of GIAC certification holders use industry seminars to maintain their skills

Continuing education is a valued aspect of certification for employers

36 CPEs

- Approved Professional Training or Certification
- Published Technical Work
- Graduate-Level Courses

18 CPEs — Continuing Education

12 CPEs — Community Experience

12 CPEs — Cyber Range Activities

12 CPEs — Work Experience

Certification maintenance helps to map professional growth and career paths through higher education

Certification maintenance shows your initiative to advance industry knowledge

Studies show professionals with maintained credentials earn higher salaries compared to non-certified colleagues

58% of survey respondents credit certifications as playing an important role in their career success

GSE?

Maintaining your GSE certification will renew all other GIAC certifications

Start Tracking CPEs Now!

For details, visit giac.org/certifications/renewal

GSEC versus Security+

- Security+ class roughly contains roughly 30-40% of the material in the SANS Security Essentials Bootcamp.

- Security+ exam is easier versus the GSEC exam.
- Annual potential salary increase: $7,320

CISM: Certified Information Security Manager

- 200 Question Exam
- 4 Hours
- 5 Years Experience
- 3 Years Security Management Experience.
- $475
- If you have a CISSP, this certification won’t really be of any extra help getting you *the* job.

GCIH:GIAV Certified Incident Handler

- 175 Questions exam
- Open-book
- $200-800
- Hardcore
- Somewhat like the CEH, Certified Ethical Hacker
- Annual potential salary increase: $15,300

GCIH:GIAV Certified Incident Handler

- Backdoors and Trojan Horses
- Buffer Overflows
- Covering Tracks: Networks
- Covering Tracks: Systems
- Denial of Service Attacks
- Exploiting Systems using Netcat
- Format String Attacks
- Incident Handling Overview and Preparation
- Incident Handling Phase 2 Identification
- Incident Handling Phase 3 Containment
- IP Address Spoofing
- Network Sniffing
- Password Attacks
- Reconnaissance
- Rootkits
- Scanning: Host Discovery
- Scanning: Network and Application Vulnerability Scanning and Tools
- Scanning: Network Devices
- Scanning: Service Discovery
- Session Hijacking, Tools and Defenses
- Types of Incidents
- Virtual Machine Attacks
- Web Application Attacks
- Worms, Bots, and Bot-Nets

BUT WAIT
THERE'S MORE
memegenerator.net

What Can You Do to achieve your optimal potential, get paid more, and achieve greater job satisfaction?

- There are many steps you can take.
  - Respected security certifications remain valuable.
  - Defend against burnout.
  - Be responsible for making your job more compelling, thrilling and satisfying.
  - If you want to advance, or have the ability to shape your job more to your liking, build your leadership skills.
  - Join a professional organization, and get involved by volunteering in them, such as OWASP, ISSA, ISACA, IEEE, HackFormers, InfraGard, HIMSS.
  - Attend security cons and actively network
  - RSA Conference, DEFCON, Black Hat, BSides, ShmooCon, DerbyCon, LASCON
  - Give talks
  - Volunteer, feed your passion.

KEEP
CALM
AND
ASK
QUESTIONS
www.keep-calm.net

Citations

- http://www.tomsitpro.com/articles/information-security-certifications,2-205.html
- https://www.itdojo.com/casp-vs-cissp-lets-explore/
- https://www.alienvault.com/blogs/security-essentials/are-security-certifications-worth-your-time