Centro de
Investigación en
Computación

SANS

Resumen

Reseña

Course

Ciberseguridad

Instructor

Acosta Bermejo Raúl

Lecture notes

2024-B
Enero del 2025
Última actualizacioón

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. SANS
3. Catálogos

Introducción

Conceptos básicos

.

Introducción

Definiciones

Networking Academy

Historia

1. La primera empresa que empezó con las capacitaciones y certificaciones en sus productos fue CISCO y tuvo mucho éxito.
   1. Creo el CISCO Network Academy, en 1997,
   2. Genero muchos materiales de calidad y prestigio.
   3. https://www.netacad.com/
2. Pronto otras empresas le copiaron.
   i. Rec Hat
   https://www.redhat.com/en/services/training/red-hat-academy
   ii. Hack de Box (Cyber)
   https://www.hackthebox.com/
   iii. Udemy, etc.

SysAdmin Audit, Networking and Security Institute

Definiciones

SANS

SANS

Introducción

Generalidades

- Entrenamientos
  - Capacita y luego certifica.
- Certificaciones
  - GIAC (*Global Information Assurance Certification*)

    Es una empresa que Certifica

    Sus certificaciones son caras pero las mejores.

    https://www.giac.org/
  - En México hay escuelas parners.
  - Otras empresas certificadoras:

    ISACA (*Information Systems Audit and Control Association*)

    https://www.isaca.org/

SANS

Introducción

Referencias

- Fuentes oficiales
  - https://www.sans.org/
  - Todas las Certificaciones
    - https://www.sans.org/cyber-security-certifications
  - Especiales
    - https://www.giac.org/certifications/reverse-engineering-malware-grem/

Catálogos

Listas

AI 2025

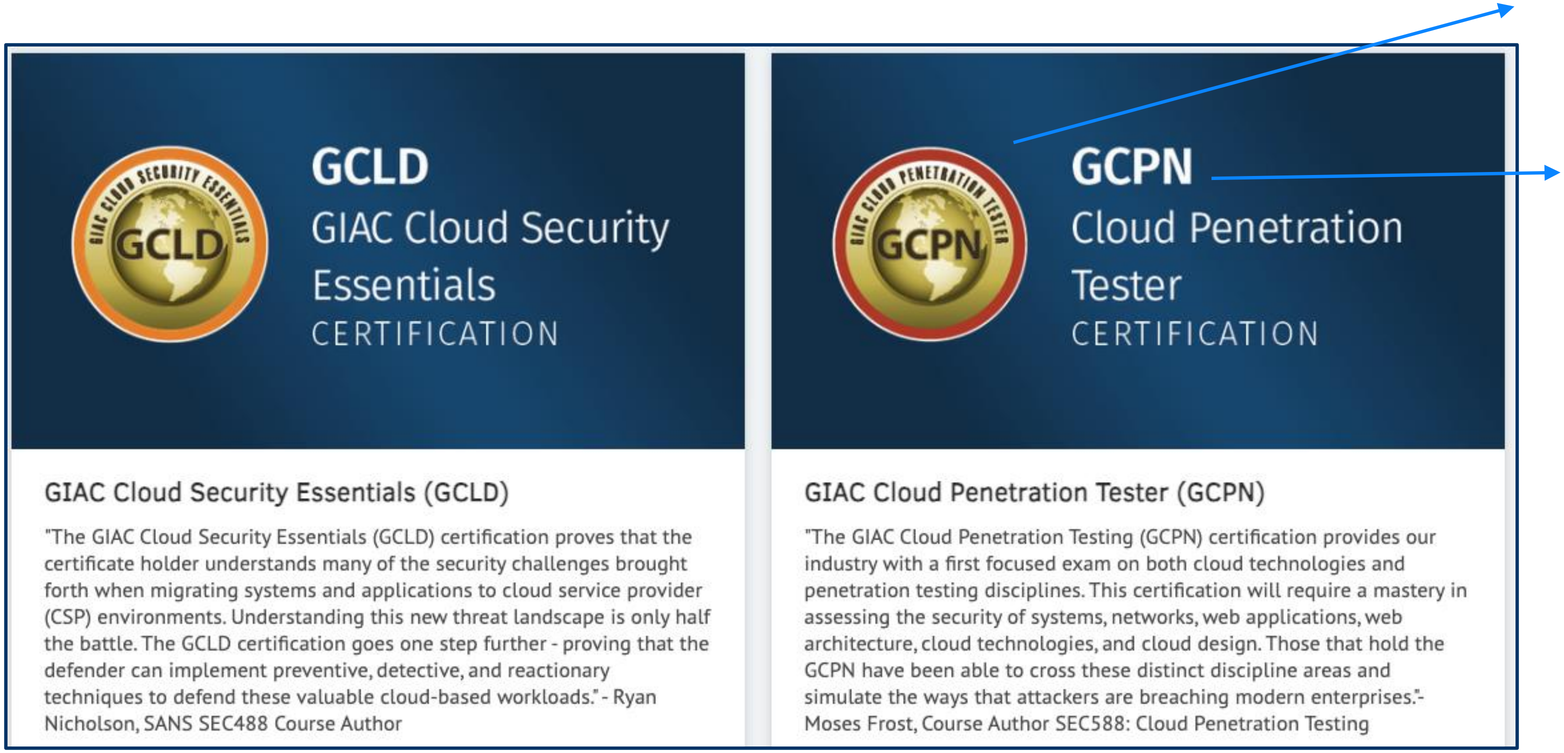
GIAC Catalogos

Total aprox. 61

Blue Team		Red Team	
Cloud Security	8	Offensive Operations	12
Cyber Defense	15	Digital Forensics & Incident Response	14
Industrial Control Systems	3	Security Management	9

Logo

Clave


GCLD
GIAC Cloud Security Essentials
CERTIFICATION
GIAC Cloud Security Essentials
GCLD
GCPN
Cloud Penetration Tester
CERTIFICATION
GIAC Cloud Penetration Tester
GCPN

GIAC Cloud Security Essentials (GCLD)

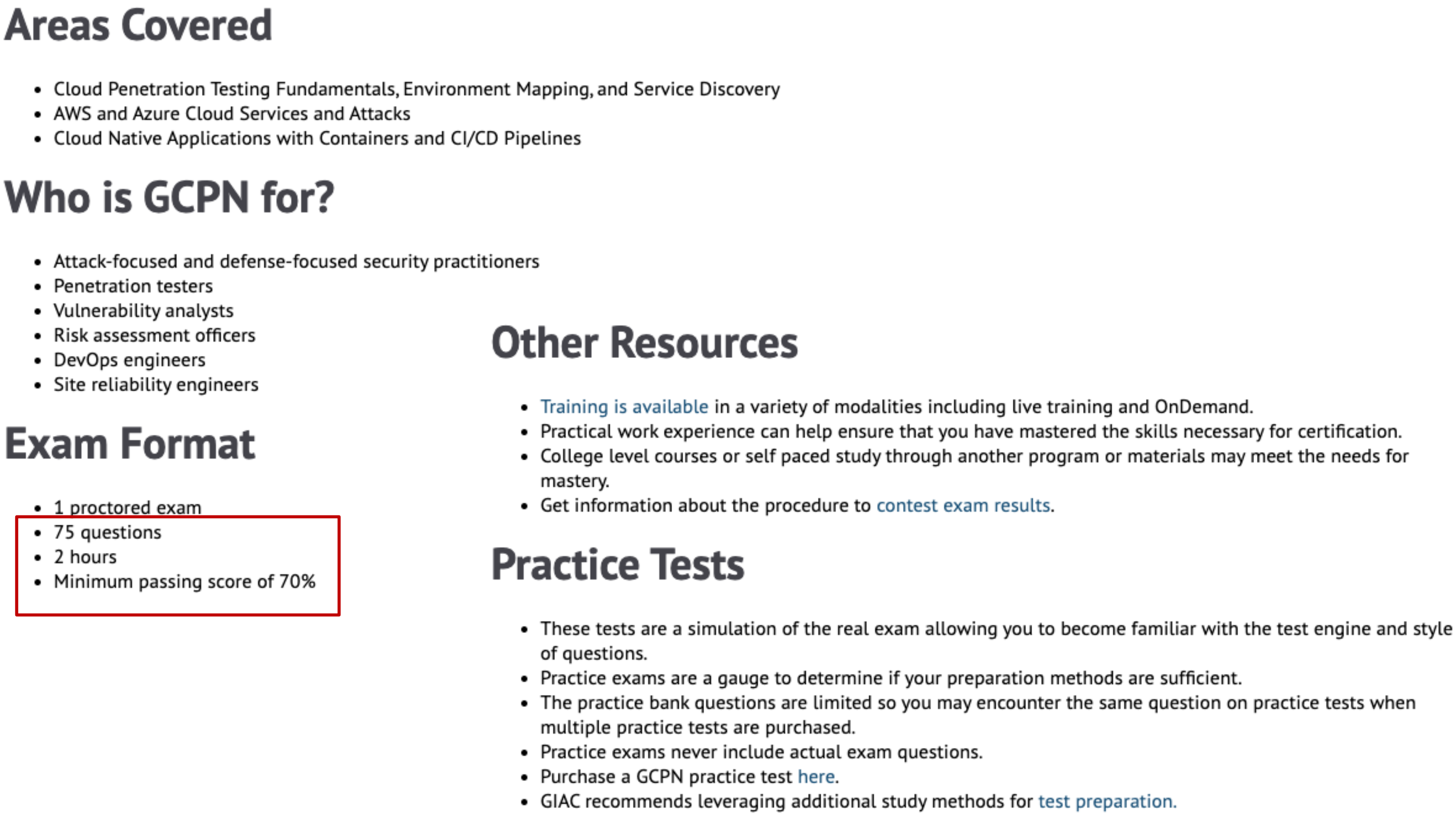
"The GIAC Cloud Security Essentials (GCLD) certification proves that the certificate holder understands many of the security challenges brought forth when migrating systems and applications to cloud service provider (CSP) environments. Understanding this new threat landscape is only half the battle. The GCLD certification goes one step further - proving that the defender can implement preventive, detective, and reactionary techniques to defend these valuable cloud-based workloads." - Ryan Nicholson, SANS SEC488 Course Author

GIAC Cloud Penetration Tester (GCPN)

"The GIAC Cloud Penetration Testing (GCPN) certification provides our industry with a first focused exam on both cloud technologies and penetration testing disciplines. This certification will require a mastery in assessing the security of systems, networks, web applications, web architecture, cloud technologies, and cloud design. Those that hold the GCPN have been able to cross these distinct discipline areas and simulate the ways that attackers are breaching modern enterprises."- Moses Frost, Course Author SEC588: Cloud Penetration Testing

GIAC Certificaciones

Ejemplo



Areas Covered

- Cloud Penetration Testing Fundamentals, Environment Mapping, and Service Discovery
- AWS and Azure Cloud Services and Attacks
- Cloud Native Applications with Containers and CI/CD Pipelines

Who is GCPN for?

- Attack-focused and defense-focused security practitioners
- Penetration testers
- Vulnerability analysts
- Risk assessment officers
- DevOps engineers
- Site reliability engineers

Exam Format

- 1 proctored exam
- 75 questions
- 2 hours
- Minimum passing score of 70%

Other Resources

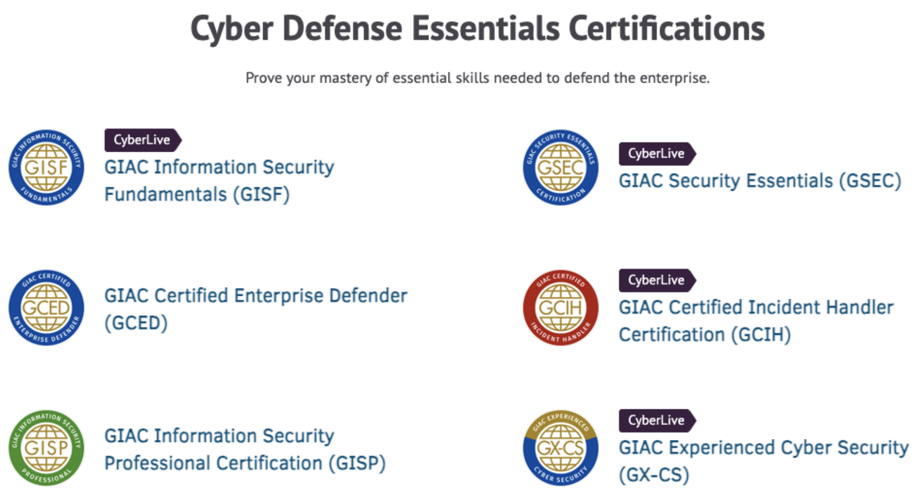
- Training is available in a variety of modalities including live training and OnDemand.
- Practical work experience can help ensure that you have mastered the skills necessary for certification.
- College level courses or self paced study through another program or materials may meet the needs for mastery.
- Get information about the procedure to contest exam results.

Practice Tests

- These tests are a simulation of the real exam allowing you to become familiar with the test engine and style of questions.
- Practice exams are a gauge to determine if your preparation methods are sufficient.
- The practice bank questions are limited so you may encounter the same question on practice tests when multiple practice tests are purchased.
- Practice exams never include actual exam questions.
- Purchase a GCPN practice test here.
- GIAC recommends leveraging additional study methods for test preparation.

GIAC Catalogos

Lista

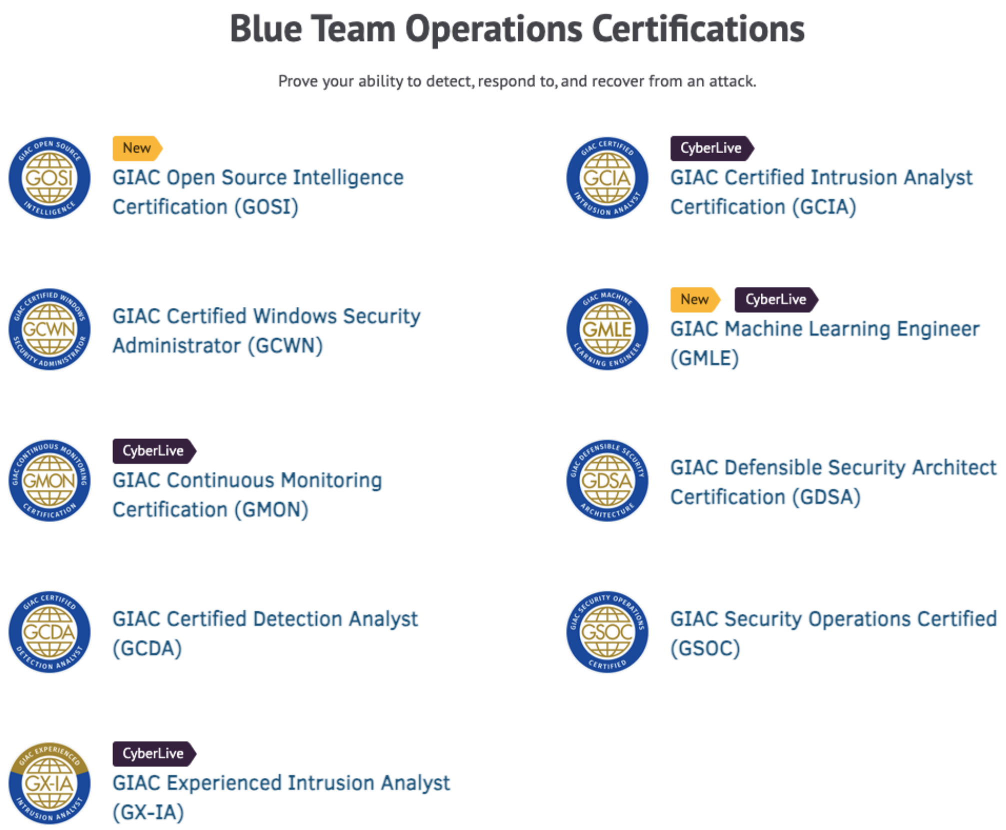


Cyber Defense Essentials Certifications

Prove your mastery of essential skills needed to defend the enterprise.

- CyberLive — GIAC Information Security Fundamentals (GISF)
- CyberLive — GIAC Security Essentials (GSEC)
- GIAC Certified Enterprise Defender (GCED)
- CyberLive — GIAC Certified Incident Handler Certification (GCIH)
- GIAC Information Security Professional Certification (GISP)
- CyberLive — GIAC Experienced Cyber Security (GX-CS)

Blue Team



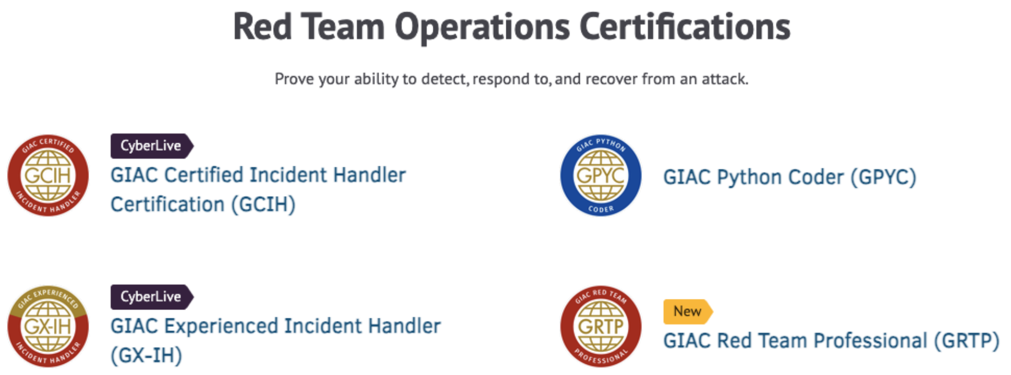
Blue Team Operations Certifications

Prove your ability to detect, respond to, and recover from an attack.

- New — GIAC Open Source Intelligence Certification (GOSI)
- CyberLive — GIAC Certified Intrusion Analyst Certification (GCIA)
- GIAC Certified Windows Security Administrator (GCWN)
- New CyberLive — GIAC Machine Learning Engineer (GMLE)
- CyberLive — GIAC Continuous Monitoring Certification (GMON)
- GIAC Defensible Security Architect Certification (GDSA)
- GIAC Certified Detection Analyst (GCDA)
- GIAC Security Operations Certified (GSOC)
- CyberLive — GIAC Experienced Intrusion Analyst (GX-IA)

GIAC Catalogos

Lista



Red Team Operations Certifications

Prove your ability to detect, respond to, and recover from an attack.

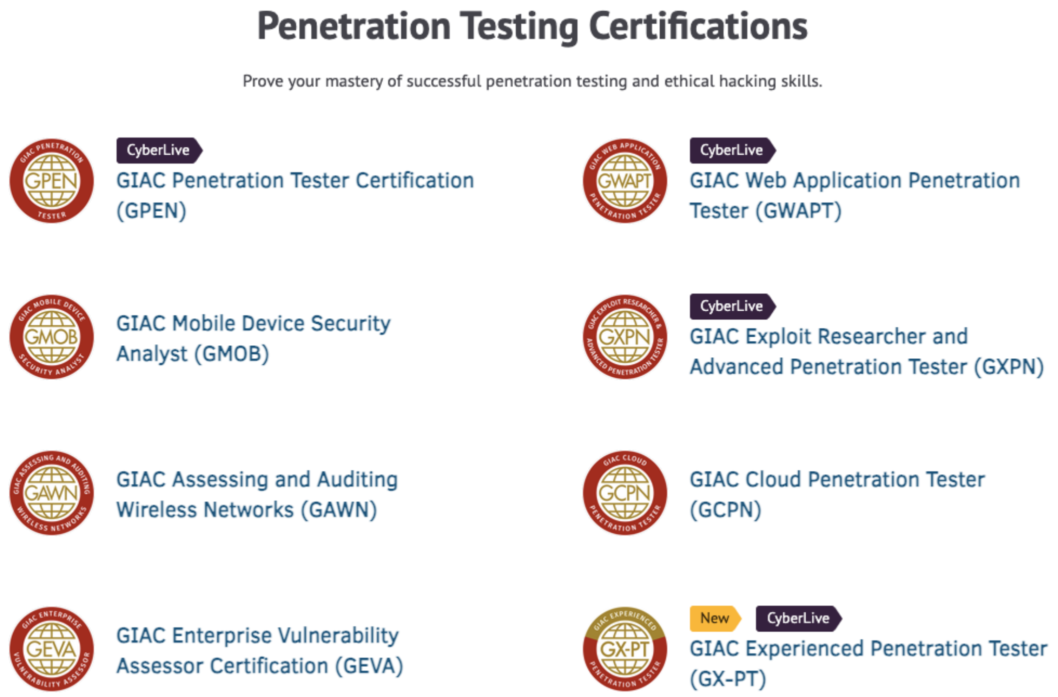
CyberLive
GIAC Certified Incident Handler Certification (GCIH)

GIAC Python Coder (GPYC)

CyberLive
GIAC Experienced Incident Handler (GX-IH)

New
GIAC Red Team Professional (GRTP)

Red Team



Penetration Testing Certifications

Prove your mastery of successful penetration testing and ethical hacking skills.

CyberLive
GIAC Penetration Tester Certification (GPEN)

CyberLive
GIAC Web Application Penetration Tester (GWAPT)

GIAC Mobile Device Security Analyst (GMOB)

CyberLive
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

GIAC Assessing and Auditing Wireless Networks (GAWN)

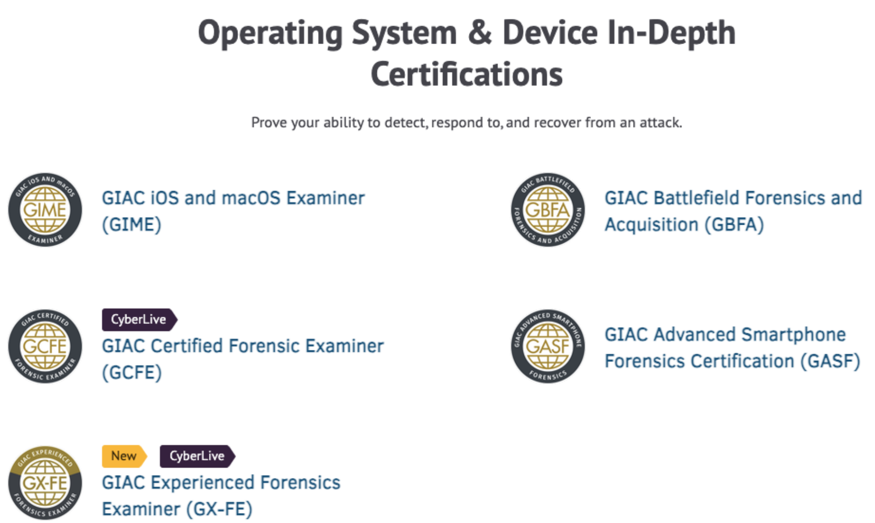
GIAC Cloud Penetration Tester (GCPN)

GIAC Enterprise Vulnerability Assessor Certification (GEVA)

New CyberLive
GIAC Experienced Penetration Tester (GX-PT)

GIAC Catalogos

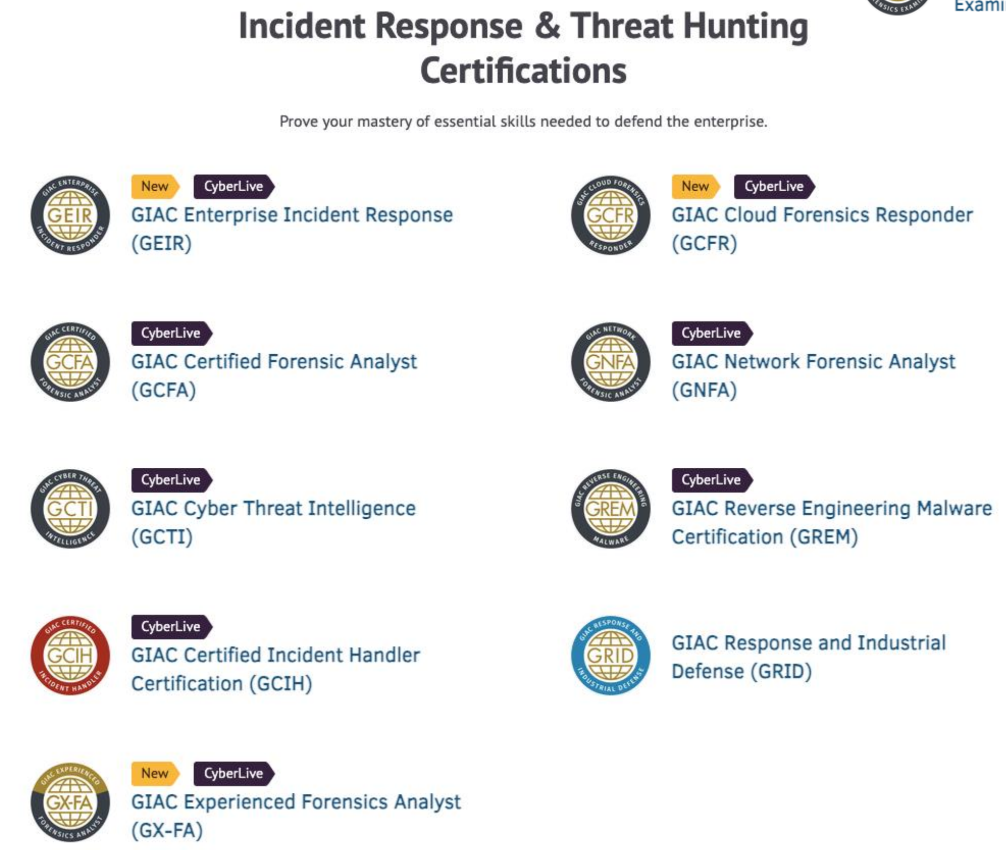
Lista



Operating System & Device In-Depth Certifications

Prove your ability to detect, respond to, and recover from an attack.

- GIAC iOS and macOS Examiner (GIME)
- GIAC Battlefield Forensics and Acquisition (GBFA)
- CyberLive GIAC Certified Forensic Examiner (GCFE)
- GIAC Advanced Smartphone Forensics Certification (GASF)
- New CyberLive GIAC Experienced Forensics Examiner (GX-FE)



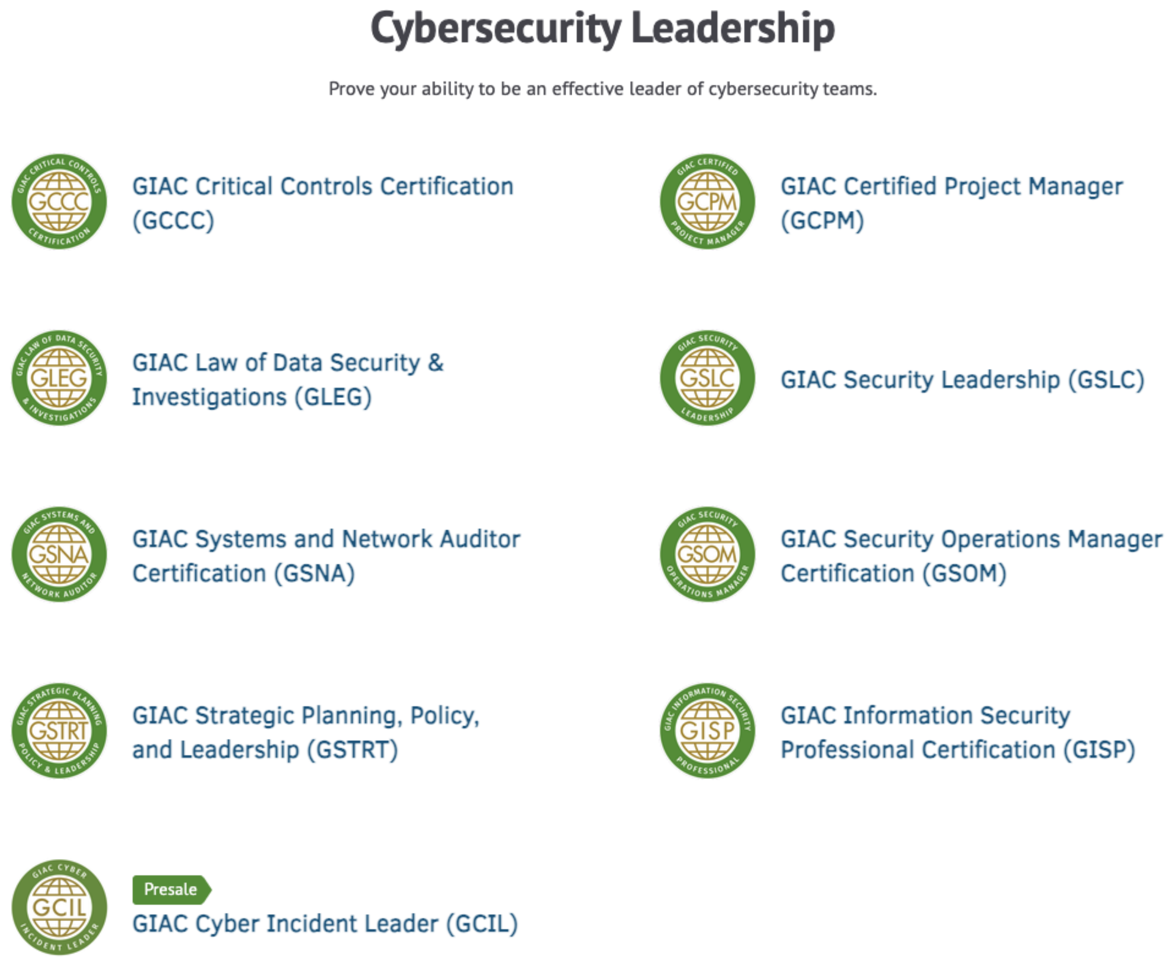
Incident Response & Threat Hunting Certifications

Prove your mastery of essential skills needed to defend the enterprise.

- New CyberLive GIAC Enterprise Incident Response (GEIR)
- New CyberLive GIAC Cloud Forensics Responder (GCFR)
- CyberLive GIAC Certified Forensic Analyst (GCFA)
- CyberLive GIAC Network Forensic Analyst (GNFA)
- CyberLive GIAC Cyber Threat Intelligence (GCTI)
- CyberLive GIAC Reverse Engineering Malware Certification (GREM)
- CyberLive GIAC Certified Incident Handler Certification (GCIH)
- GIAC Response and Industrial Defense (GRID)
- New CyberLive GIAC Experienced Forensics Analyst (GX-FA)

GIAC Catalogos

Lista



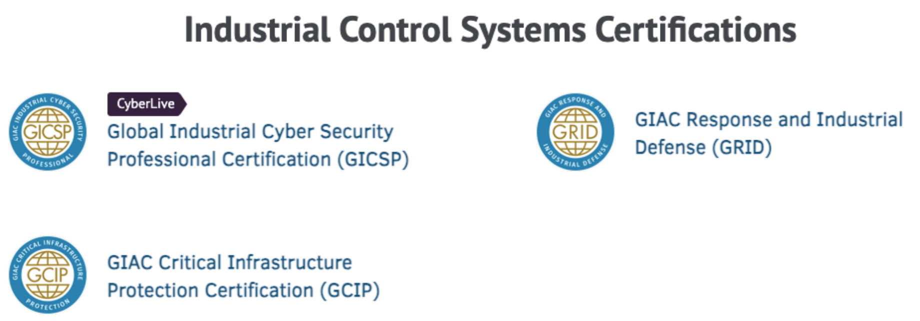
Cybersecurity Leadership

Prove your ability to be an effective leader of cybersecurity teams.

- GIAC Critical Controls Certification (GCCC)
- GIAC Certified Project Manager (GCPM)
- GIAC Law of Data Security & Investigations (GLEG)
- GIAC Security Leadership (GSLC)
- GIAC Systems and Network Auditor Certification (GSNA)
- GIAC Security Operations Manager Certification (GSOM)
- GIAC Strategic Planning, Policy, and Leadership (GSTRT)
- GIAC Information Security Professional Certification (GISP)
- Presale GIAC Cyber Incident Leader (GCIL)

GIAC Catalogos

Lista

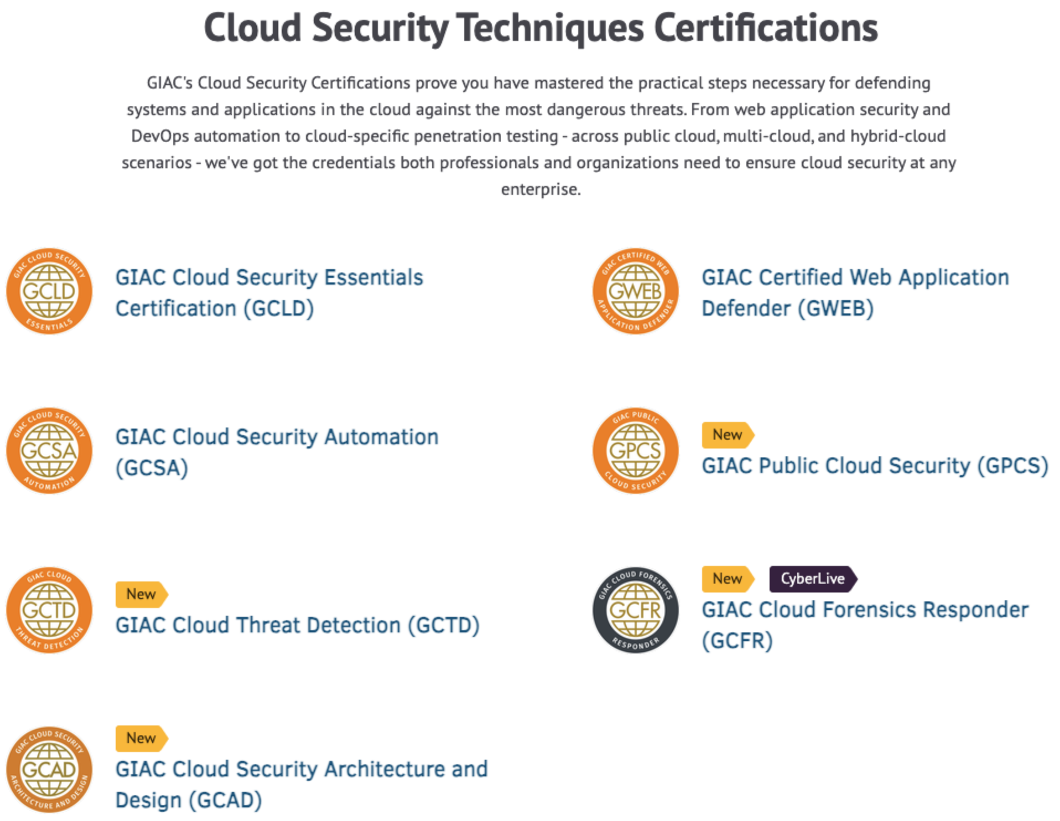


Industrial Control Systems Certifications

CyberLive
Global Industrial Cyber Security Professional Certification (GICSP)

GIAC Response and Industrial Defense (GRID)

GIAC Critical Infrastructure Protection Certification (GCIP)



Cloud Security Techniques Certifications

GIAC's Cloud Security Certifications prove you have mastered the practical steps necessary for defending systems and applications in the cloud against the most dangerous threats. From web application security and DevOps automation to cloud-specific penetration testing - across public cloud, multi-cloud, and hybrid-cloud scenarios - we've got the credentials both professionals and organizations need to ensure cloud security at any enterprise.

GIAC Cloud Security Essentials Certification (GCLD)

GIAC Certified Web Application Defender (GWEB)

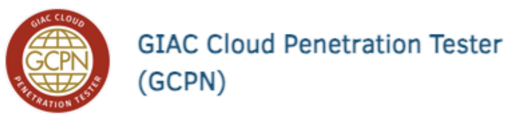
GIAC Cloud Security Automation (GCSA)

New
GIAC Public Cloud Security (GPCS)

New
GIAC Cloud Threat Detection (GCTD)

New CyberLive
GIAC Cloud Forensics Responder (GCFR)

New
GIAC Cloud Security Architecture and Design (GCAD)



GIAC Cloud Penetration Tester (GCPN)

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652