Cyber Security Domains

Major Domains in Cyber Security

Security Governance and Management

- Governance, Risk, and Compliance (GRC)
- Identity and Access Management (IAM)
- Cyber Security Audits
- Security Awareness and Training
- Supply Chain Security
- Disaster Recovery and Business Continuity
- Physical Security

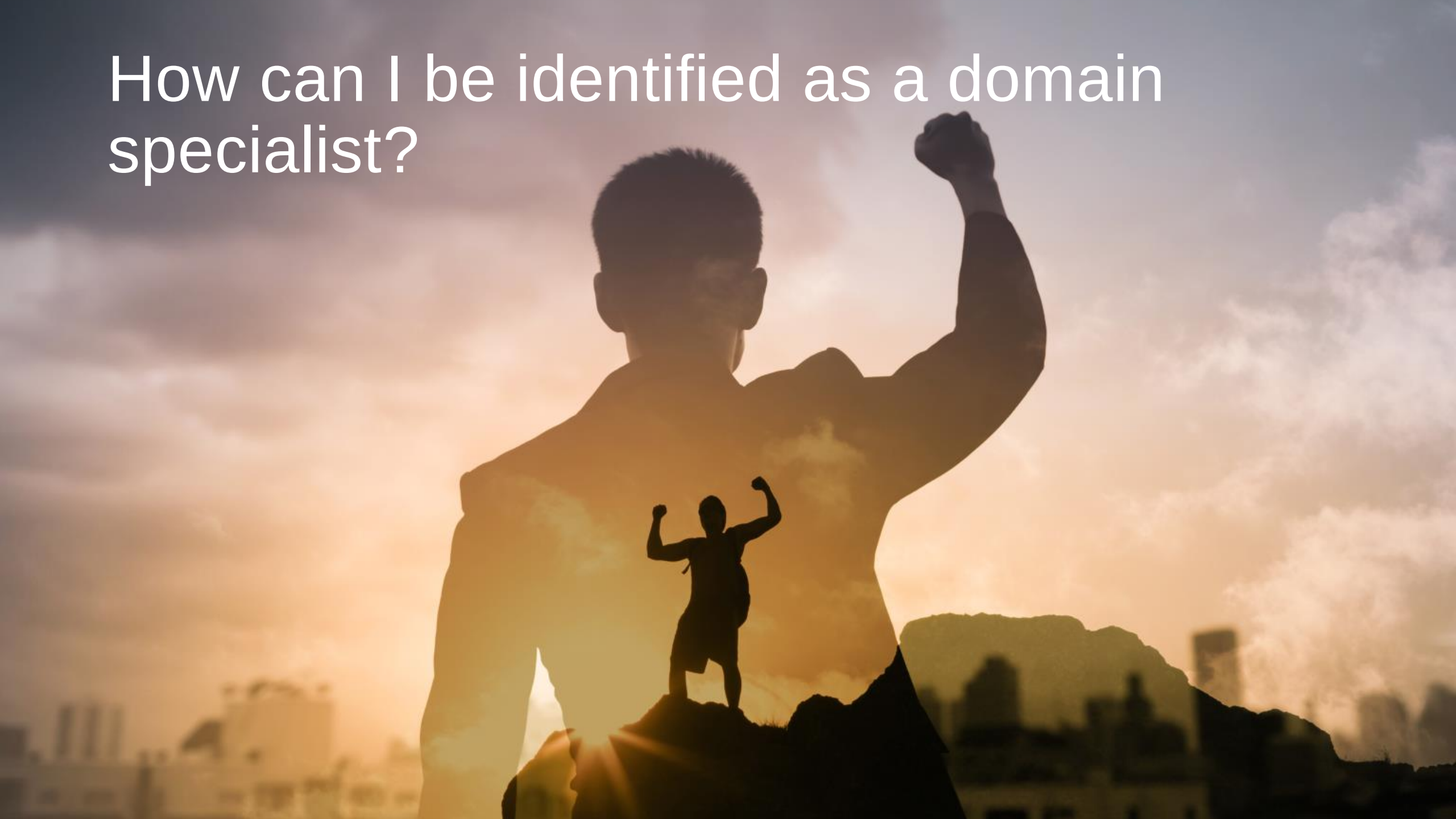
Technology / Platform Focus

- Network Security
- Application Security
- System Security
- Data Security
- Endpoint Security
- Cryptography
- Internet of Things (IoT) Security
- AI/ML Security
- Cloud Security
- Quantum Security
- Blockchain Security

Security Operations

- SIEM (Security information and event management)
- SOAR (Security Orchestration, Automation, and Response)
- Cyber Threat Intelligence
- Incident Response
- Vulnerability Management
- Penetration Testing
- Ethical hacking
- Digital Forensics
- Malware analysis

How can I be identified as a domain specialist?



Cyber Security Certifications

- Industry-recognized certifications in Cyber Security are meant to validate skills and knowledge.
- Industry-recognized certifications in the field of cyber security are awarded by various authorities and organizations that set standards, develop curricula, and assess the knowledge and skills of professionals.

Certification bodies (CBs)

- **$(ISC)^2$ (International Information System Security Certification Consortium, Inc.):** Dedicated to providing cyber security education, training, and certification programs for professionals worldwide. Founded in 1989 and is headquartered in the United States.
- **CompTIA (Computing Technology Industry Association):** A trade association that focuses on advancing the IT industry and providing education, certification, and advocacy for IT professionals and businesses globally, offers a wide range of certifications. Founded in 1982.

Certification bodies (CBs)

- **ISACA (formerly the Information Systems Audit and Control Association):** It is a global organization that focuses on IT governance, risk management, and cyber security education, certification, and professional development opportunities. Founded in 1969 and is headquartered in the United States.
- **GIAC (Global Information Assurance Certification):** is a leading provider of cyber security certifications and training programs. Established by the SANS Institute. GIAC certifications are highly regarded in the cyber security industry and are recognized for their practical, hands-on approach to assessing candidates' knowledge and skills.

Certification bodies (CBs)

- **CIS (Center for Internet Security):** It is a nonprofit organization dedicated to improving cyber security readiness and response for both the public and private sectors. Established in 2000. CIS offers the CIS Controls Certification, which validates an individual's expertise in implementing and maintaining the CIS Controls, a set of best practices for cyber security defense

Certification bodies (CBs)

- **EC-Council (International Council of E-Commerce Consultants):** It is a global cyber security certification body and provider of cyber security training programs. Founded in 2001, EC-Council is known for its emphasis on ethical hacking, penetration testing, and information security education.
- **Offensive Security:** Founded in 2007, is headquartered in New York City, United States Offensive Security is known for its hands-on and practical approach to cyber security education, particularly in the field of offensive security, which focuses on ethical hacking, penetration testing, and exploit development.

Governance, Risk, and Compliance (GRC)

- GRC focuses on establishing and maintaining effective cyber security governance, risk management, and compliance programs within organizations.
- This domain includes **risk assessments**, **policy development**, **regulatory compliance**, **security audits**, and **security awareness training**

Governance, Risk, and Compliance (GRC)

- Knowledge base involves familiarity with frameworks, and standards such as ISO 27001, NIST Cyber Security Framework, GDPR, HIPAA, PCI DSS, and industry-specific regulations etc

Governance, Risk, and Compliance (GRC)

- Certifications popular in Industry :
  - **Certified Information Systems Auditor (CISA)**
  - Certified in Risk and Information Systems Control (CRISC)
  - **Certified Information Security Manager (CISM)**
  - Certified Regulatory Compliance Manager (CRCM)
  - Certified in Governance of Enterprise IT (CGEIT)
  - Certified Information Privacy Professional (CIPP)
  - Certified Compliance and Ethics Professional (CCEP)
  - **Certified Information Systems Security Professional (CISSP)**

Network Security

- Network security focuses on protecting the integrity, confidentiality, and availability of data and resources within computer networks. **This domain forms basis for the careers in operational Security as well as management of security**
- This domain includes **measures such as firewalls, intrusion detection/prevention systems, secure network architecture design, virtual private networks (VPNs), and network** segmentation.

Network Security

- Network security engineers:
  - Design and implement secure network architectures
  - **Configure** firewalls, VPNs, and intrusion detection systems
  - Conduct network **vulnerability assessments** and penetration testing
  - **Monitor network traffic** and analyze logs

Network Security

- Network security analysts:
  - Monitor network security event logs
  - Analyze and respond to security incidents
  - Perform network security audits and compliance checks
  - Implement network access control and segmentation

Network Security

Certifications popular and in-demand in market are:

- CompTIA Security+
- **Cisco Certified Network Associate (CCNA) Security**
- **Cisco Certified Internetwork Expert Security (CCIE Security)**
- **Certified Network Defender (CND)**
- Check Point Certified Security Administrator (CCSA)
- **Certified Ethical Hacker (CEH)**

Data Security

- Data security, involves protecting sensitive information from unauthorized access, disclosure, alteration, or destruction.
- This domain encompasses **encryption, access controls, data loss prevention (DLP), secure storage**, data classification, and secure data handling practices**.**

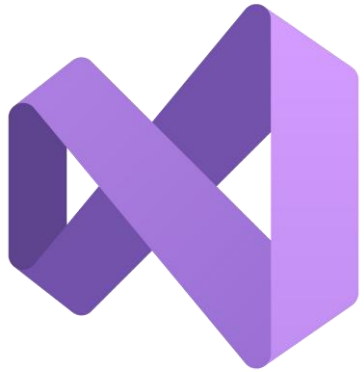
Data Security

Certifications popular in Industry are :

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- **Certified Data Privacy Solutions Engineer (CDPSE)**
- Certified Information Privacy Professional (CIPP)

Application Security

- Application security focuses on securing software applications and systems from security vulnerabilities and threats.
- This domain includes **secure coding practices, web application firewalls (WAFs), penetration testing,** code reviews, vulnerability assessments, and secure software development lifecycles (SDLC).



Application Security

- Application security developers:
  - Design and develop secure software applications
  - Implement secure coding practices and secure development lifecycle
  - Conduct application security testing and code reviews
  - Integrate application security with system and network security

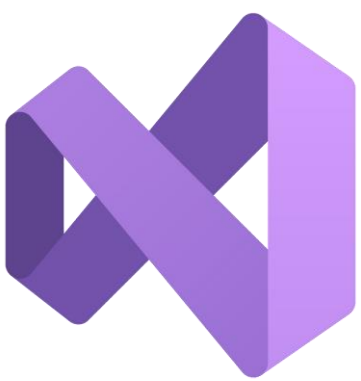
Application Security

- Application security testers:
  - Conduct application security testing and vulnerability assessments
  - Identify and report application security vulnerabilities
  - Develop and execute application security test plans
  - Collaborate with developers to remediate security issues

Application Security

Certifications popular in Industry are as follows:

- Certified Secure Software Lifecycle Professional (CSSLP)
- GIAC Secure Software Programmer (GSSP)
- **Certified Application Security Engineer (CASE)**
- Checkmarx Certified Secure Software Developer (CCSSD)
- Certified Ethical Hacker (CEH)



System Security

Protecting computer systems, including hardware, software, and firmware, from unauthorized access, use, disclosure, disruption, modification, or destruction

System Security

System security administrators:

- Install, configure, and patch operating systems and software
- Manage user accounts, permissions, and access control
- Configure and monitor system security settings
- Perform system backups and disaster recovery

System Security

System security engineers:

- Design and implement secure system architectures
- Conduct system vulnerability assessments and penetration testing
- Develop and implement system security policies and procedures
- Integrate system security with network security

System Security

Certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Systems Professional (CISSP-ISSAP)

End-Point Security

- Endpoint security focuses on securing individual devices, **such as desktops, laptops, mobile devices,** and servers, from cyber security threats.
- It includes antivirus/antimalware software, host-based intrusion detection/prevention systems (HIDS/HIPS), endpoint detection and response (EDR) and device encryption

End-Point Security

Certifications popular in Industry are as follows:

- Certified Endpoint Protection Professional (CEPP)
- Certified Endpoint Security Administrator (CESA)
- Certified McAfee Security Specialist (CMSS)
- CompTIA Cyber security Analyst (CySA+)

Cloud Security

- Cloud security involves protecting data, applications, and infrastructure deployed in cloud environments from cyber security threats.

Cloud Security

- This includes understanding cloud service models (Infrastructure as a Service, (Platform as a Service, Software as a Service) / (IaaS, PaaS, SaaS), cloud deployment models (public, private, hybrid), cloud security architecture, identity and access management (IAM), encryption, network security, and compliance frameworks.

Cloud Security

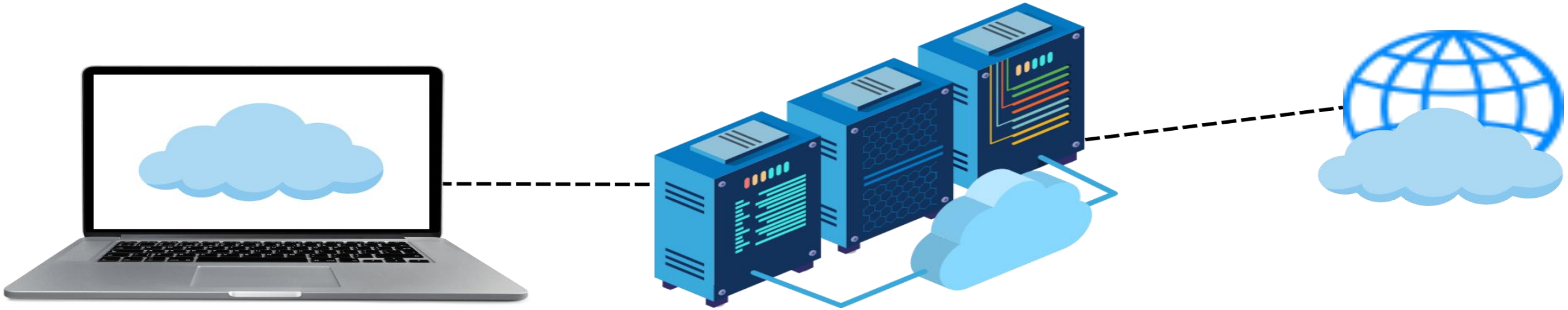
- **Cloud Platform Certifications** from leading cloud service providers are as follows:
  - Amazon Web Services (AWS): AWS Certified Security
  - Microsoft Azure: Microsoft Certified: Azure Security Engineer Associate
  - Google Cloud Platform (GCP): Professional Cloud Security Engineer

Cloud Security

- **Cloud Platform Certifications** from leading cloud service providers are as follows:
  - CompTIA: CompTIA Cloud+
  - Certified Cloud Security Professional (CCSP)
  - Certificate of Cloud Security Knowledge (CCSK)
  - Certified Cloud Security Specialist (CCSS)
  - Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) certifications

Security Operations

- SecOps involves the day-to-day monitoring, detection, analysis, and response to cyber security threats and incidents.
- This domain includes security information and event management (SIEM), security orchestration, automation, and response (SOAR), threat hunting, incident response, and security analytics.



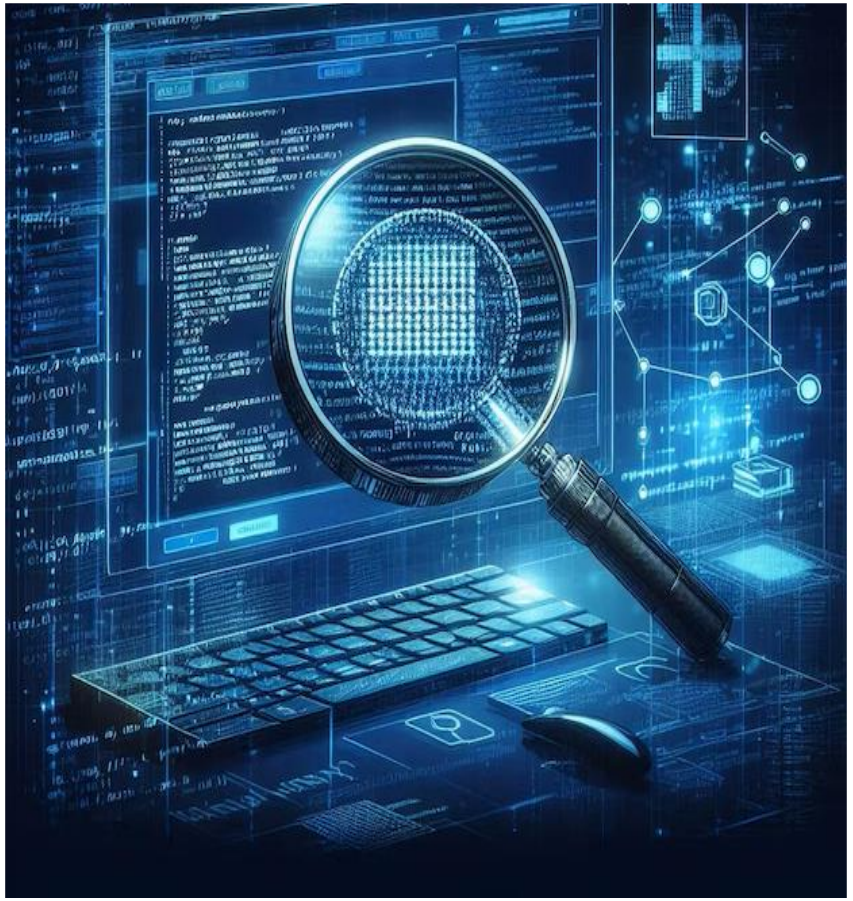
Security Operations

Certifications popular in Industry are as follows:

- IBM Certified Analyst – (SIEM)
- Certified SOC Analyst (CSA+)
- EC-Council Certified Incident Handler (ECIH)
- GIAC Certified Incident Handler (GCIH)
- Certified Ethical Hacker (CEH)

Digital Forensics

- Develop technical skills in digital forensics tools, techniques, and methodologies.
- This includes understanding disk imaging, file system analysis, memory forensics, network forensics, mobile device forensics, malware analysis, and forensic data acquisition.



Digital Forensics

- Certifications popular in Industry are as follows:
  - Certified Forensic Computer Examiner (CFCE)
  - Certified Computer Examiner (CCE)
  - Certified Forensic Analyst (GCFA)
  - Certified Hacking Forensic Investigator (CHFI)
  - GIAC Certified Forensic Examiner (GCFE)
  - GIAC Network Forensic Analyst (GNFA)