The Saudi Cybersecurity Workforce Framework Mapping to SANS | GIAC

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

SANS | GIAC CERTIFICATIONS

WORK ROLE	JOB TITLES	SUMMARY	MISSION	COURSE | CPEs	GIAC CERTIFICATION	SANS.EDU PROGRAM
CYBERSECURITY ARCHITECTURE, RESEARCH, AND DEVELOPMENT						
Cybersecurity Architecture (CA)	• **Cybersecurity Architect** | CARD-CA-001 • **Secure Cloud Specialist** | CARD-CA-002	Conducts cybersecurity design, architecture, research and development activities	Designs and oversees the development and implementation of cybersecurity systems and/or the cybersecurity components of IT systems and networks	**SEC530:** Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise™ | 36 CPEs **SEC549:** Cloud Security Architecture™ | 30 CPEs	**GDSA** GIAC Defensible Security Architecture **GCAD** GIAC Cloud Security Architecture and Design	Cloud Certificate Program
Cybersecurity Research & Development (CRD)	• **Systems Security Development Specialist** | CARD-CRD-001 • **Cybersecurity Developer** | CARD-CRD-002 • **Secure Software Assessor** | CARD-CRD-003 • **Cybersecurity Researcher** | CARD-CRD-004 • **Cybersecurity Data Science Specialist** | CARD-CRD-005 • **Cybersecurity Artificial Intelligence Specialist** | CARD-CRD-006	Conducts cybersecurity design, architecture, research and development activities	Conducts cybersecurity research and development	**SEC522:** Application Security: Securing Web Applications, APIs, and Microservices™ | 36 CPEs **SEC530:** Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise™ | 36 CPEs **SEC566:** Implementing and Auditing CIS Controls™ | 30 CPEs **SEC595:** Applied Data Science and AI/Machine Learning for Cybersecurity Professionals™ | 36 CPEs	**GWEB** GIAC Certified Web Application Defender **GDSA** GIAC Defensible Security Architecture **GCCC** GIAC Critical Controls Certification **GMLE** GIAC Machine Learning Engineer	Cybersecurity Engineering (Core) Certificate Program
LEADERSHIP AND WORKFORCE DEVELOPMENT						
Leadership (L)	• **Chief Information Security Officer/Director** | LWD-L-001 • **Cybersecurity Manager** | LWD-L-002 • **Cybersecurity Advisor** | LWD-L-003	Leads cybersecurity teams and work Develops cybersecurity human capital	Supervises, manages, and leads cybersecurity teams and work	**LDR512:** Security Leadership Essentials for Managers™ | 30 CPEs **LDR514:** Security Strategic Planning, Policy, and Leadership™ | 30 CPEs **LDR520:** Emerging Trends for Cyber Leaders: AI and Cloud™ | 30 CPEs **LDR521:** Security Culture for Leaders™ | 30 CPEs **LDR551:** Building and Leading Security Operations Centers™ | 30 CPEs	**GSLC** GIAC Security Leadership **GSTRT** GIAC Strategic Planning, Policy & Leadership **GSOM** GIAC Security Operations Manager	Cybersecurity Leadership Certificate Program
Leadership (L)	• **Cybersecurity Human Capital Manager** | LWD-WD-001 • **Cybersecurity Instructional Curriculum Developer** | LWD-WD-002 • **Cybersecurity Instructor** | LWD-WD-003	Leads cybersecurity teams and work Develops cybersecurity human capital	Applies knowledge and skills of cybersecurity, human resources development and teaching methodologies to develop, manage, retain and improve the skills of the cybersecurity workforce	**LDR514:** Security Strategic Planning, Policy, and Leadership™ | 30 CPEs **SEC275:** Foundations: Computers, Technology, and Security™ | 30 CPEs **SEC401:** Security Essentials – Network, Endpoint, and Cloud™ | 46 CPEs **SEC403:** Secrets to Successful Cybersecurity Presentation™ | 6 CPEs	**GSTRT** GIAC Strategic Planning, Policy & Leadership **GFACT** GIAC Foundational Cybersecurity Technologies **GSEC** GIAC Security Essentials	Cybersecurity Leadership Certificate Program
GOVERNANCE, RISK, COMPLIANCE, AND LAWS						
Governance, Risk, and Compliance (GRC)	• **Cybersecurity Risk Officer** | GRCL-GRC-001 • **Cybersecurity Compliance Officer** | GRCL-GRC-002 • **Cybersecurity Policy Officer** | GRCL-GRC-003 • **Security Controls Assessor** | GRCL-GRC-004 • **Cybersecurity Auditor** | GRCL-GRC-005	Develops organizational cybersecurity policies Governs cybersecurity structures and processes, manages cyber risks and assures compliance with the organization's cybersecurity, risk management and related legal requirements	Governs cybersecurity structures and processes Manages cyber risks and assures IT systems against the organization's cybersecurity and risk management requirements Develops and updates the organization's cybersecurity policies	**LDR419:** Performing a Cybersecurity Risk Assessment™ | 12 CPEs **LDR514:** Security Strategic Planning, Policy, and Leadership™ | 30 CPEs **LDR519:** Cybersecurity Risk Management and Compliance™ | 30 CPEs	**GSTRT** GIAC Strategic Planning, Policy & Leadership	Cybersecurity Leadership Certificate Program
Laws and Data Protection (LDP)	• **Cybersecurity Legal Specialist** | GRCL-LDP-001 • **Privacy/Data Protection Officer** | GRCL-LDP-002	Develops organizational cybersecurity policies Governs cybersecurity structures and processes, manages cyber risks and assures compliance with the organization's cybersecurity, risk management and related legal requirements	Ensures the organization complies with cybersecurity and data protection laws and regulations	**SEC566:** Implementing and Auditing CIS Controls™ | 30 CPEs	**GCCC** GIAC Critical Controls Certification	Cybersecurity Leadership Certificate Program
INDUSTRIAL CONTROL SYSTEMS AND OPERATIONAL TECHNOLOGIES (ICS/OT)						
Industrial Control Systems and Operational Technologies (ICS/OT)	• **ICS/OT Cybersecurity Architect** | ICSOT-ICSOT-001 • **ICS/OT Cybersecurity Infrastructure Specialist** | ICSOT-ICSOT-002 • **ICS/OT Cybersecurity Defense Analyst** | ICSOT-ICSOT-003 • **ICS/OT Cybersecurity Risk Officer** | ICSOT-ICSOT-004 • **ICS/OT Cybersecurity Incident Responder** | ICSOT-ICSOT-005	Conducts cybersecurity tasks for Industrial Control Systems and Operational Technologies (ICS/OT)	Performs work related to cybersecurity governance, risk management and compliance; design and development; operations and administration; protection and defense for OT systems such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems	**ICS410:** ICS/SCADA Security Essentials™ | 36 CPEs **ICS418:** ICS Security Essentials for Leaders™ | 12 CPEs **ICS456:** Essentials for NERC Critical Infrastructure Protection™ | 31 CPEs **ICS515:** ICS Visibility, Detection, and Response™ | 36 CPEs **ICS612:** ICS Cybersecurity In-Depth™ | 30 CPEs **ICS613:** ICS/OT Penetration Testing & Assessments™ | 30 CPEs	**GICSP** GIAC Global Industrial Cyber Security Professional **GCIP** GIAC Critical Infrastructure Protection **GRID** GIAC Response and Industrial Defense	Industrial Control Systems Security

The Saudi Cybersecurity Workforce Framework Mapping to SANS | GIAC

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

SANS | GIAC CERTIFICATIONS

WORK ROLE	JOB TITLES	SUMMARY	MISSION	COURSE | CPEs	GIAC CERTIFICATION	SANS.EDU PROGRAM
PROTECTION AND DEFENSE						
Defense (D)	• **Cybersecurity Defense Analyst** | PD-D-001 • **Cybersecurity Infrastructure Specialist** | PD-D-002 • **Cybersecurity Specialist** | PD-D-003	Identifies, analyzes, monitors, mitigates, and manages threats and vulnerabilities to IT systems and networks Uses defensive measures and multi-source information to report events and respond to incidents	Uses monitoring and analysis tools to identify and analyze events and to detect incidents	**SEC450:** SOC Analyst Training – Applied Skills for Cyber Defense Operations™ | 36 CPEs **SEC501:** Advanced Security Essentials – Enterprise Defender™ | 38 CPEs **SEC503:** Network Monitoring and Threat Detection In-Depth™ | 46 CPEs **SEC504:** Hacker Tools, Techniques, and Incident Handling™ | 38 CPEs **SEC511:** Cybersecurity Engineering: Advanced Threat Detection & Monitoring™ | 46 CPEs **SEC522:** Application Security: Securing Web Applications, APIs, and Microservices™ | 36 CPEs **SEC530:** Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise™ | 36 CPEs	**GSOC** GIAC Security Operations Certified **GCED** GIAC Certified Enterprise Defender **GCIA** GIAC Certified Intrusion Analyst **GCIH** GIAC Certified Incident Handler **GMON** GIAC Continuous Monitoring Certification **GWEB** GIAC Certified Web Application Defender **GDSA** GIAC Defensible Security Architecture	Cloud Certificate Program
Protection (P)	• **Cryptography Specialist** | PD-P-001 • **Identity and Access Management Specialist** | PD-P-002 • **Systems and Security Analyst** | PD-P-003	Identifies, analyzes, monitors, mitigates, and manages threats and vulnerabilities to IT systems and networks Uses defensive measures and multi-source information to report events and respond to incidents	Uses cybersecurity tools to protect information, systems and networks from cyber threats	**SEC450:** SOC Analyst Training – Applied Skills for Cyber Defense Operations™ | 36 CPEs **SEC497:** Practical Open-Source Intelligence (OSINT)™ | 36 CPEs **SEC501:** Advanced Security Essentials – Enterprise Defender™ | 38 CPEs **SEC503:** Network Monitoring and Threat Detection In-Depth™ | 46 CPEs **SEC504:** Hacker Tools, Techniques, and Incident Handling™ | 38 CPEs **SEC511:** Cybersecurity Engineering: Advanced Threat Detection & Monitoring™ | 46 CPEs **SEC522:** Application Security: Securing Web Applications, APIs, and Microservices™ | 36 CPEs **SEC587:** Advanced Open-Source Intelligence (OSINT) Gathering and Analysis™ | 36 CPEs	**GSOC** GIAC Security Operations Certified **GOSI** GIAC Open Source Intelligence **GCED** GIAC Certified Enterprise Defender **GCIA** GIAC Certified Intrusion Analyst **GCIH** GIAC Certified Incident Handler **GMON** GIAC Continuous Monitoring Certification **GWEB** GIAC Certified Web Application Defender **GSOA** GIAC Strategic OSINT Analyst	Cybersecurity Engineering (Core) Certificate Program
Vulnerability Assessment (VA)	• **Vulnerability Assessment Specialist** | PD-VA-001 • **Penetration Tester/Red Team Specialist** | PD-VA-002	Identifies, analyzes, monitors, mitigates, and manages threats and vulnerabilities to IT systems and networks Uses defensive measures and multi-source information to report events and respond to incidents	Tests IT systems and networks and assesses their threats and vulnerabilities	**SEC542:** Web App Penetration Testing and Ethical Hacking™ | 36 CPEs **SEC555:** Detection Engineering and SIEM Analytics™ | 30 CPEs **SEC560:** Enterprise Penetration Testing™ | 36 CPEs **SEC573:** Automating Information Security with Python™ | 36 CPEs **SEC588:** Cloud Penetration Testing™ | 36 CPEs **SEC660:** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™ | 46 CPEs **SEC760:** Advanced Exploit Development for Penetration Testers™ | 40 CPEs	**GWAPT** GIAC Web Application Penetration Tester **GCDA** GIAC Certified Detection Analyst **GPEN** GIAC Penetration Tester **GPYC** GIAC Python Coder **GCPN** GIAC Cloud Penetration Tester **GXPN** GIAC Exploit Researcher & Advanced Penetration Tester	Penetration Testing and Ethical Hacking Certificate Program
Incident Response (IR)	• **Cybersecurity Incident Responder** | PD-IR-001 • **Digital Forensics Specialist** | PD-IR-002 • **Cyber Crime Investigator** | PD-IR-003 • **Malware Reverse Engineering Specialist** | PD-IR-004	Identifies, analyzes, monitors, mitigates, and manages threats and vulnerabilities to IT systems and networks Uses defensive measures and multi-source information to report events and respond to incidents	Investigates, analyzes and responds to cyber incidents	**FOR508:** Advanced Incident Response, Threat Hunting, and Digital Forensics™ | 36 CPEs **FOR509:** Enterprise Cloud Forensics and Incident Response™ | 36 CPEs **FOR518:** Mac and iOS Forensic Analysis and Incident Response™ | 36 CPEs **FOR528:** Ransomware and Cyber Extortion™ | 24 CPEs **FOR572:** Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response™ | 36 CPEs **FOR577:** Linux Incident Response and Threat Hunting™ | 36 CPEs **FOR608:** Enterprise-Class Incident Response & Threat Hunting™ | 36 CPEs **FOR610:** Reverse-Engineering Malware: Malware Analysis Tools & Techniques™ | 36 CPEs **FOR710:** Reverse-Engineering Malware: Advanced Code Analysis™ | 36 CPEs **LDR553:** Cyber Incident Management™ | 30 CPEs **SEC504:** Hacker Tools, Techniques, and Incident Handling™ | 38 CPEs	**GCFA** GIAC Certified Forensic Analyst **GCFR** GIAC Cloud Forensics Responder **GIME** GIAC iOS and macOS Examiner **GNFA** GIAC Network Forensic Analyst **GLIR** GIAC Linux Incident Responder **GEIR** GIAC Enterprise Incident Responder **GREM** GIAC Reverse Engineering Malware **GCIL** GIAC Cyber Incident Leader **GCIH** GIAC Certified Incident Handler	Penetration Testing and Ethical Hacking Certificate Program
Threat Management (TM)	• **Threat Intelligence Analyst** | PD-TM-001 • **Threat Hunter** | PD-TM-002	Identifies, analyzes, monitors, mitigates, and manages threats and vulnerabilities to IT systems and networks Uses defensive measures and multi-source information to report events and respond to incidents	Collects and analyzes information about threats Searches for undetected threats and provides actionable insights to support cybersecurity decision making	**FOR508:** Advanced Incident Response, Threat Hunting, and Digital Forensics™ | 36 CPEs **FOR577:** Linux Incident Response and Threat Hunting™ | 36 CPEs **FOR578:** Cyber Threat Intelligence™ | 36 CPEs **FOR589:** Cybercrime Investigations™ | 30 CPEs **FOR608:** Enterprise-Class Incident Response & Threat Hunting™ | 36 CPEs **SEC503:** Network Monitoring and Threat Detection In-Depth™ | 46 CPEs **SEC541:** Cloud Security Threat Detection™ | 30 CPEs **SEC599:** Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses™ | 36 CPEs	**GCFA** GIAC Certified Forensic Analyst **GLIR** GIAC Linux Incident Responder **GCTI** GIAC Cyber Threat Intelligence **GEIR** GIAC Enterprise Incident Responder **GCIA** GIAC Certified Intrusion Analyst **GCTD** GIAC Cloud Threat Detection **GDAT** GIAC Defending Advanced Threats	