NIS2 Mapping:
Suggested SANS Courses to the ECSF

SANS | GIAC CERTIFICATIONS

WORK ROLE	SUMMARY STATEMENT	MISSION	RISK ASSESSMENT	CYBER INCIDENTS	CRITICAL INFRASTRUCTURE	REPORTING
Chief Information Security Officer (CISO)	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.	Oversees and assures compliance with cybersecurity- and data-related legal, regulatory frameworks and policies in line with the organisation's strategy and legal requirements. Contributes to the organisation's data protection related actions. Provides legal advice in the development of the organisation's cybersecurity governance processes.	**LDR512:** Security Leadership Essentials for Managers **LDR514:** Security Strategic Planning, Policy, and Leadership **LDR521:** Security Culture for Leaders	**LDR551:** Building and Leading Security Operations Centers **LDR553:** Cyber Incident Management **SEC402:** Cybersecurity Writing: Hack the Reader	**ICS410:** ICS/SCADA Security Essentials **ICS418:** ICS Security Essentials for Managers **SEC402:** Cybersecurity Writing: Hack the Reader	**LDR419:** Performing a Cybersecurity Risk Assessment **LDR514:** Security Strategic Planning, Policy, and Leadership **SEC566:** Implementing and Auditing CIS Controls
Cyber Incident Responder	Monitor the organisation's cybersecurity state, manage incidents during cyber-attacks and assure the continued operations of ICT systems.	Analyses, evaluates and mitigates the impact of cybersecurity incidents. Monitors and assesses systems' cybersecurity state. According to the organisation's Incident Response Plan, restores systems' and processes' functionalities to an operational state.	**FOR508:** Advanced Incident Response, Threat Hunting, and Digital Forensics **FOR572:** Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response	**FOR508:** Advanced Incident Response, Threat Hunting, and Digital Forensics **FOR572:** Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response	**FOR578:** Cyber Threat Intelligence **ICS515:** ICS Visibility, Detection, and Response	**FOR508:** Advanced Incident Response, Threat Hunting, and Digital Forensics **SEC450:** Blue Team Fundamentals: Security Operations and Analysis
Cyber Legal, Policy, and Compliance Officer	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.	Oversees and assures compliance with cybersecurity- and data-related legal, regulatory frameworks and policies in line with the organisation's strategy and legal requirements. Contributes to the organisation's data protection related actions. Provides legal advice in the development of the organisation's cybersecurity governance processes.	**LDR512:** Security Leadership Essentials for Managers **LDR514:** Security Strategic Planning, Policy, and Leadership	**LDR512:** Security Leadership Essentials for Managers **LDR553:** Cyber Incident Management	**ICS410:** ICS/SCADA Security Essentials **ICS418:** ICS Security Essentials for Managers	**LDR514:** Security Strategic Planning, Policy, and Leadership **SEC566:** Implementing and Auditing CIS Controls
Cyber Threat Intelligence Specialist	Collect, process, analyse data and information to produce actionable intelligence reports and disseminate them to target stakeholders.	Manages cyber threat intelligence life cycle including cyber threat information collection, analysis and production of actionable intelligence and dissemination to security stakeholders and the CTI community, at a tactical, operational and strategic level. Identifies and monitors the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors and their trends, track threat actors' activities and observe how non-cyber events can influence cyber-related actions.	**FOR578:** Cyber Threat Intelligence **SEC497:** Practical Open-Source Intelligence (OSINT)	**FOR578:** Cyber Threat Intelligence **FOR589:** Cybercrime Intelligence	**FOR578:** Cyber Threat Intelligence **ICS515:** ICS Visibility, Detection, and Response	**FOR578:** Cyber Threat Intelligence **FOR589:** Cybercrime Intelligence
Cybersecurity Architect	Plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls.	Designs solutions based on security-by-design and privacy-by-design principles. Creates and continuously improves architectural models and develops appropriate architectural documentation and specifications. Coordinate secure development, integration and maintenance of cybersecurity components in line with standards and other related requirements.	**LDR512:** Security Leadership Essentials for Managers **SEC549:** Enterprise Cloud Security Architecture	**SEC530:** Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise **SEC566:** Implementing and Auditing CIS Controls	**FOR578:** Cyber Threat Intelligence **ICS515:** ICS Visibility, Detection, and Response	**FOR578:** Cyber Threat Intelligence **FOR589:** Cybercrime Intelligence
Cybersecurity Auditor	Perform cybersecurity audits on the organisation's ecosystem.	Conducts independent reviews to assess the effectiveness of processes and controls and the overall compliance with the organisation's legal and regulatory frameworks policies. Evaluates, tests and verifies cybersecurity-related products (systems, hardware, software and services), functions and policies ensuring, compliance with guidelines, standards and regulations.	**AUD507:** Auditing & Monitoring Networks, Perimeters and Systems **SEC566:** Implementing and Auditing CIS Controls	**AUD507:** Auditing & Monitoring Networks, Perimeters and Systems **SEC566:** Implementing and Auditing CIS Controls	**AUD507:** Auditing & Monitoring Networks, Perimeters and Systems **ICS410:** ICS/SCADA Security Essentials	**AUD507:** Auditing & Monitoring Networks, Perimeters and Systems **SEC566:** Implementing and Auditing CIS Controls
Cybersecurity Educator	Improves cybersecurity knowledge, skills and competencies of humans.	Designs, develops and conducts awareness, training and educational programmes in cybersecurity and data protection-related topics. Uses appropriate teaching and training methods, techniques and instruments to communicate and enhance the cybersecurity culture, capabilities, knowledge and skills of human resources. Promotes the importance of cybersecurity and consolidates it into the organisation.	**LDR433:** Managing Human Risk **SEC402:** Cybersecurity Writing: Hack the Reader	**SEC402:** Cybersecurity Writing: Hack the Reader **SEC403:** Secrets to Successful Cybersecurity Presentation	**ICS410:** ICS/SCADA Security Essentials **ICS418:** ICS Security Essentials for Managers	**LDR514:** Security Strategic Planning, Policy, and Leadership **SEC566:** Implementing and Auditing CIS Controls
Cybersecurity Implementor	Develop, deploy and operate cybersecurity solutions (systems, assets, software, controls and services) on infrastructures and products.	Provides cybersecurity-related technical development, integration, testing, implementation, operation, maintenance, monitoring and support of cybersecurity solutions. Ensures adherence to specifications and conformance requirements, assures sound performance and resolves technical issues required in the organisation's cybersecurity-related solutions (systems, assets, software, controls and services), infrastructures and products.	**SEC568:** Combating Supply Chain Attacks with Product Security Testing **SEC501:** Advanced Security Essentials – Enterprise Defender	**LDR551:** Leading and Building Security Operations Centers **LDR553:** Cyber Incident Management	**ICS410:** ICS/SCADA Security Essentials **ICS418:** ICS Security Essentials for Managers	**SEC401:** Security Essentials: Network, Endpoint and Cloud **SEC566:** Implementing and Auditing CIS Controls
Cybersecurity Researcher	Research the cybersecurity domain and incorporate results in cybersecurity solutions.	Conducts fundamental/basic and applied research and facilitates innovation in the cybersecurity domain through cooperation with other stakeholders. Analyses trends and scientific findings in cybersecurity.	**SEC402:** Cybersecurity Writing: Hack the Reader **SEC403:** Secrets to Successful Cybersecurity Presentation	**FOR508:** Advanced Incident Response, Threat Hunting, and Digital Forensics **SEC501:** Advanced Security Essentials – Enterprise Defender	**ICS410:** ICS/SCADA Security Essentials **ICS418:** ICS Security Essentials for Managers	**LDR419:** Performing a Cybersecurity Risk Assessment **SEC566:** Implementing and Auditing CIS Controls
Cybersecurity Risk Manager	Manage the organisation's cybersecurity-related risks aligned to the organisation's strategy. Develop, maintain and communicate the risk management processes and reports.	Continuously manages (identifies, analyses, assesses, estimates, mitigates) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Establishes a risk management strategy for the organisation and ensures that risks remain at an acceptable level for the organisation by selecting mitigation actions and controls.	**LDR419:** Performing a Cybersecurity Risk Assessment **LDR514:** Security Strategic Planning, Policy, and Leadership	**LDR419:** Performing a Cybersecurity Risk Assessment **LDR553:** Cyber Incident Management	**ICS410:** ICS/SCADA Security Essentials **ICS418:** ICS Security Essentials for Managers	**LDR419:** Performing a Cybersecurity Risk Assessment **SEC566:** Implementing and Auditing CIS Controls
Digital Forensics Investigator	Ensure the cybercriminal investigation reveals all digital evidence to prove the malicious activity.	Connects artefacts to natural persons, captures, recovers, identifies and preserves data, including manifestations, inputs, outputs and processes of digital systems under investigation. Provides analysis, reconstruction and interpretation of the digital evidence based on a qualitative opinion. Presents an unbiased qualitative view without interpreting the resultant findings.	**FOR500:** Windows Forensic Analysis **FOR585:** Smartphone Forensic Analysis In-Depth	**FOR498:** Digital Acquisition and Rapid Triage **FOR500:** Windows Forensic Analysis	**FOR578:** Cyber Threat Intelligence **ICS515:** ICS Visibility, Detection, and Response	**FOR498:** Digital Acquisition and Rapid Triage **FOR500:** Windows Forensic Analysis
Penetration Tester	Assess the effectiveness of security controls, reveals and utilise cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors.	Plans, designs, implements and executes penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures. Identifies vulnerabilities or failures on technical and organisational controls that affect the confidentiality, integrity and availability of ICT products (e.g. systems, hardware, software and services).	**SEC504:** Hacker Tools, Techniques, and Incident Handling **SEC560:** Enterprise Penetration Testing	**SEC560:** Enterprise Penetration Testing **SEC660:** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	**ICS612:** ICS Cybersecurity In-Depth **ICS613:** ICS Penetration Testing and Assessments	**ICS515:** ICS Visibility, Detection, and Response **SEC560:** Enterprise Penetration Testing