Cybersecurity Network Administration and Security Training

Course	Deliverables	Outputs	Duration (Weeks)	(AU)/Technical Staff Course (SOC) / Application User Course
Network Administration/Security	● Acquire, install, and configure networking devices – routers and switches using subnetting. ● Knowledge of TCP/IP and OSI models to analyse network activity with tools like Wireshark. ● Use Wireshark to capture network packet data and analyse network activity. ● Understand network security protocols and vulnerabilities. ● Use offensive tools to attack networks and systems and use countermeasures to limit activities. ● Perform all activities across the cyber kill chain. Learn an array of tools and tactics. ● Perform advanced host exploitation and persistence.	Participants will develop core KSAs to perform network administration and security tasks.	10	SOC
System Administration/ Security	● Foundational knowledge of computer security. ● Develop solid skills to install, configure, and secure applications. ● Install Active Directory, Domain Services, and configure both Linux and Windows systems and servers. ● Knowledge of vulnerability and remediation in context of patch and configuration management.	Participants will develop core KSAs on System Architecture, Operating Systems, System Exploits (hardware, operating system, and memory).	10	SOC
Governance, Risk and Compliance (GRC)	● Knowledge of asset management and use within enterprise environment. ● Knowledge policies, procedures, and standards. ● Install and configure network and security devices to implement key functions. ● Analyse functions through the lens of attack and defence capabilities. ● Knowledge and skills to perform incident response activities – Respond and Recover from events.	Participants will learn how to deliver on the Identify, Protect, Detect, Respond, and Recover functions within the enterprise to deliver cyber and information security. Participants will learn the NIST Risk Management Framework core objectives. Case studies on the Gordon Loeb Model will serve as a guide to implementation.	4	AU
Penetration Testing and Forensic Analysis	● Focus on using Kali Linux and penetration testing tools using methodologies such as the cyber kill chain and MITRE ATTCK Framework. ● Knowledge of the Penetration Testing Execution Standard (PTES). ● Perform offensive attacks on individually developed infrastructure from Systems and Networking courses. ● Identify and Monitor attacks using capabilities developed in Network and Systems courses. ● Conduct case study and research on malware and Advanced Persistent Threat groups. ● Conduct Linux, Mobile, and Windows forensic activities	The participant will use techniques performed by malicious threat actors to compromise network and systems. This provides the requisite KSAs of a penetration tester to proactively find network and system vulnerabilities as a core tenant of risk management. A list of 50+ tools will be provided to support this capability.	7	SOC
Threat Analysis, Intelligence, and Modelling	● Knowledge of threat analysis, intelligence, and modelling as a core tenant of organizational risk management. ● The importance of the risk formula Risk = Threat x Vulnerability ● Knowledge of threat actor monetization methods, intelligence gathering and sources, and intelligence analysis ● Operational and situational awareness and planning with intelligence	Participants will learn about the Cyber Kill Chain, Centre of Gravity (COG) Analysis, and CTI Diamond Model. Their application using the Cyber Intelligence Preparation of the Environment (IPE). Case studies on the Fraud Triangle theory will enable critical thinking.	7	AU/SOC
Security Orchestration, Automation, and Response (SOAR)	● Knowledge of heterogeneous log data sources and configurations to define operational logging levels. ● Knowledge of the types of data contained in log files. ● Configure data sources and SPLUNK to capture and analyse log data and automating alert and notifications. ● Knowledge of Incident Response and Crisis Management processes.	Participants will learn core KSAs to engineering solutions that allow analysing the data from various information and technology assets - network devices, workstations, servers, routers, firewalls, and other connected devices. This will be applied to enterprise developed by participants and groups. The free Splunk Fundamentals certificate must be obtained by every participant. The free AWS Cloud Fundamentals certificate must be obtained by every participant.	5	SOC
Cybersecurity Management and Strategy	● Knowledge of Cyber Resilience ● Knowledge Data Protection ● Discuss Privacy vs Security ● Crisis Management ● Analyse Old System for Technology Change ● Systems Change, Innovation, and Thinking	Participants will leave with high criical thinking and ability to affect change using new cybersecurity skills.	5	AU/SOC

Course	Deliverables	Outputs	Duration (Weeks)	(AU)/Technical Staff Course (SOC)	Application User Course
Final Project (Advanced Cybersecurity Capability Placement Framework)	● Demonstrate KSAs acquired from all courses to present an enterprise infrastructure with core cyber systems and controls. ● Recommend best practices to improve security in each implementation. ● Implement security controls and countermeasures. ● Demonstrate constructive and critical thinking to inform cyber decision-making. ● Apply governance, risk, and compliance ● Use professional communications to present and share with cohort	Participant technical and written group projects will be a demonstration of all the KSAs acquired during the training.	3	AU/SOC	