



ICS/SCADA
CYBER SECURITY

Exam
Blueprint

EC-Council

ICS/SCADA Cyber Security

Exam Blueprint

Sr. No.	Domain	Topics	Domain %
1	Introduction to ICS/SCADA Network Defense	Typical Security Model	16
		ICS/SCADA Overview	
		Risk	
		Security Policy	
		ICS/SCADA Attacks	
		Attacks Surface	
		Protocols and Siemens	
		Modbus and BACnet	
		Challenges with ICS/SCADA Risk	
		Asset Identification and System Characterization	
		Vulnerability Identification and Threat Modelling	
		SCADA Framework	
		IT and ICS Comparison	
		Standards	
2	TCP/IP 101	Encapsulation and De-encapsulation	14
		TCP/IP	
		IPv4, UDP, TCP Header	
		Threat Containment	
		Network Protocols	
		ICS/SCADA Protocols	
3	Introduction to Hacking	Motives, Goals, and Objectives of Information Security Attacks	16
		Hacking and Ethical Hacking	
		Mindset of the Attacker	
		Types of Testing	
		Hacking Methodology	
		Footprinting	
		Scanning	

		Enumeration	
		Vulnerability Research	
		Exploration	
		Common ICS Architectures	
		Modems and Wardialing	
		Penetration Testing	
		ICS/SCADA Testing	
4	Vulnerability Management	Defining “Vulnerability”	13
		Vulnerability Scanners	
		Vulnerability Assessment	
		Malware Ecosystem	
		Vulnerability Management	
		Asset Identification and Conpot	
		ICS/SCADA Scanning	
		Metasploit and ICS/SCADA	
		Metasploit and Modbus	
		Metasploit and Bacnet	
		Vulnerability Severity	
		Common Vulnerability Scoring System (CVSS)	
5	Standards and Regulation for Cybersecurity	Standards and Regulations	6
		ISO 27001	
		CFATS	
		IEC 62443	
		NIST SP 800-82	
		Defense in Depth Strategy	
		Industry Best Practices for ICS	
		ICS/SCADA Regulations Workshop	
6	Securing the ICS/SCADA Network	Physical Security	16
		Securing the ICS Protocols	
		IPsec	
		IPsec Modes	
		IPsec Rules	
		Firewall Scripting	

		Isolating a Server	
		ICS Vulnerability Assessment and Risk Management	
		ICS Testing	
7	Bridging the Air Gap	ICS/SCADA Connections	6
		Next Generation Firewall	
		ICS Monitoring	
		Log Aggregation	
		Zone Monitoring	
		SIEM	
		Information Management	
		Reports and Alerts	
		Incident Investigation and Response	
		Log Storage and Retention	
8	Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)	Why Intrusion Detection?	13
		Intrusion Detection 101	
		IDS Features	
		Topology Concerns	
		Under Attack	
		Intrusion Prevention	
		Types of IPS	
		Intrusion Analysis	
		Signs of Compromise	
		Log Analysis	
		Malware	
		APT Defined	
		MITRE ATT&CK Matrix	
		Event Correlation	
ICS Malware			