MARCRAFT
an ETG Brand

CYBER SECURITY

AMERICA NEEDS TRAINED PROFESSIONALS!

Demand for Cyber Security employees is expected to rise to **6 million globally** by 2019, with a projected **shortfall of 1.5 million**, says Michael Brown, CEO at Symantec, the world's largest security software vendor.

ESSENTIAL & ADVANCED LEVELS

NOT JUST SIMULATION

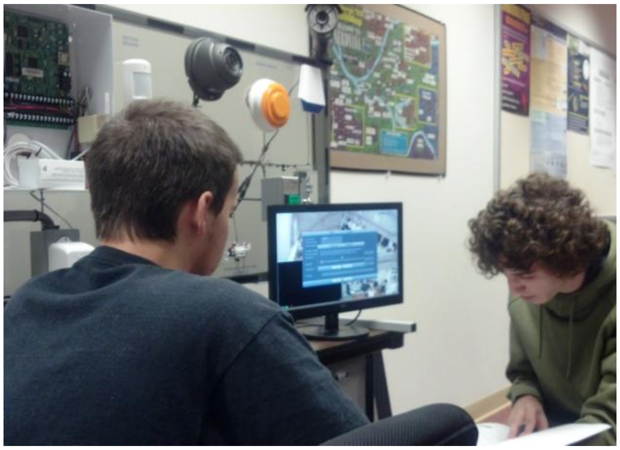
IoT Devices
Card Readers
Wireless Sniffers
Smart Meter
Motion Detector
Video Cameras
Bluetooth Sniffers
PLC and SCADA
Biometric Devices
Virtualization Systems

Cyber Security is an all-encompassing domain of Information Technology – it comprises the entire set of security-related technologies and issues

THE GOVERNMENT NIST FRAMEWORK

The new **MARCRAFT *CYBER SECURITY ESSENTIALS*** course, based on the **National Institute of Standards and Technology,** encompasses **180-240** hours of both theory and extensive **hands-on equipment** and software labs.

- Physical Asset Security Systems & Devices
- Local Host, Local Network & Internet Security
- Enterprise Network Security
- Industrial Control System (ICS) Network Security
- Medical/IoT Network Security
- Ethical Hacking Roles and Tools

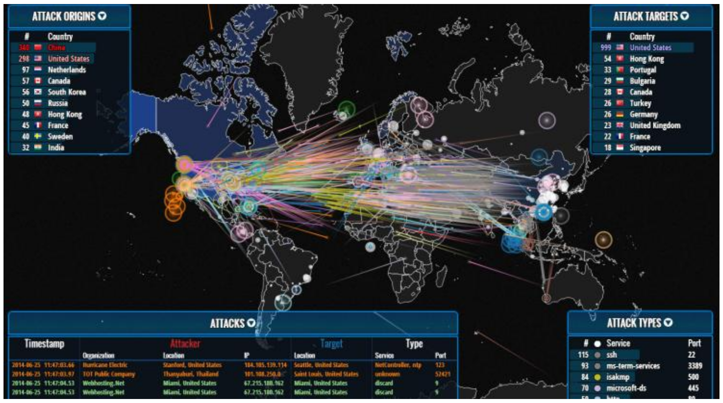


Be sure to call 800-441-6006 or e-mail us at info@marcraft.com for a FREE EVALUATION copy of the Student Text and Lab Guides

MARCRAFT
an ETG Brand

CYBER SECURITY

Identify, Protect, Detect, Respond, Recover



ATTACK ORIGINS

#	Country
340	China
298	United States
97	Netherlands
57	Canada
56	South Korea
50	Russia
48	Hong Kong
45	France
40	Sweden
32	India

ATTACK TARGETS

#	Country
999	United States
54	Hong Kong
33	Portugal
29	Bulgaria
28	Canada
26	Turkey
26	Germany
23	United Kingdom
22	France
18	Singapore

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-25 11:47:03.66	Hurricane Electric	Stanford, United States	184.105.139.114	Seattle, United States	NetController, ntp	123
2014-06-25 11:47:03.97	TOT Public Company	Thanyaburi, Thailand	101.108.250.0	Saint Louis, United States	unknown	52421
2014-06-25 11:47:04.53	Webhosting.Net	Miami, United States	67.215.180.162	Miami, United States	discard	9
2014-06-25 11:47:04.53	Webhosting.Net	Miami, United States	67.215.180.162	Miami, United States	discard	9

ATTACK TYPES

#	Service	Port
115	ssh	22
93	ms-term-services	3389
84	isakmp	500
70	microsoft-ds	445

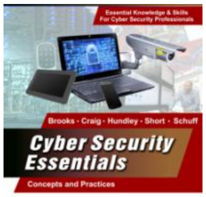
Cyber Security skills are in high demand, as threats continue to plaque enterprises around the world.

WILL YOU BE READY?

FOR THE STUDENT:

Fully Illustrated Text and Lab Guides

* Complete Theory Instruction
* Extensive Technical Instruction
* Integrated Hands-On Labs
* Industry Certification Test Prep
* Online Curriculum Available

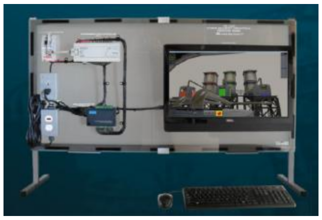


Essential Knowledge & Skills For Cyber Security Professionals

Brooks · Craig · Hundley · Short · Schuff

Cyber Security Essentials

Concepts and Practices



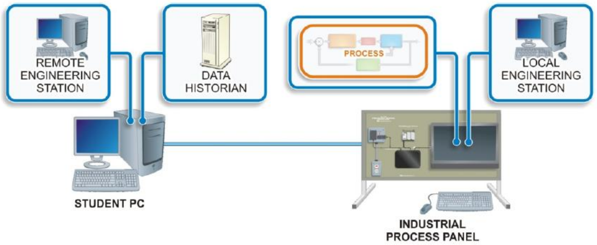
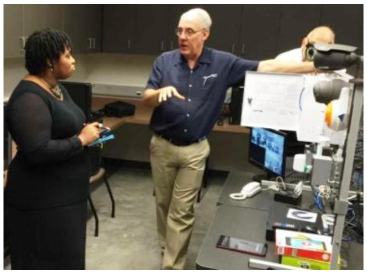


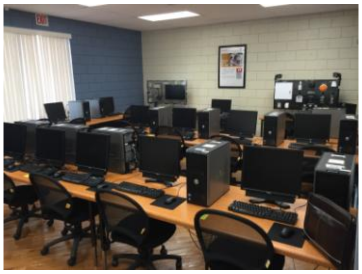
Figure 40-1: Standalone ICS Network

FOR THE INSTRUCTOR:

Fully Illustrated Instructor's Guide with PowerPoint Presentations

*Onsite Classroom Set-up and Training
* Online Classroom Management
* Master Reset Control
* Free 1-800 Tech Support
* Equipped for 24-32 Students





FOR THE EMPLOYER:

Potential IT Employee with:

* Training Based on the NIST Framework
* Well-Rounded Technical Skills
* Significant Hands-On Experience
* Industry Certifications

CSX CYBERSECURITY FUNDAMENTALS CERTIFICATE

CompTIA Security+

GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL GICSP

CISSP

CERTIFIED ETHICAL HACKER

ACCESSDATA CERTIFIED EXAMINER ACE

CYBER SECURITY ESSENTIALS

Chapter 1 ***Infrastructure Security*** - Introduces the concepts and techniques associated with physical infrastructure security devices, systems and techniques used to combat theft, prevent physical damage, maintain system integrity and services, and limit unauthorized disclosure of information. Key information includes physical access control systems, authentication techniques and systems, monitoring and notification systems, surveillance systems, and environmental security activities.

Chapter 2 ***Local Host Security*** - Focuses on tools and techniques used to secure the three perimeters of all local computing devices. Key topics include physical port access hardening, OS hardening, application hardening, and drive, folder and file encryption, local firewall and browser security practices.

Chapter 3 Local Networking Security - Deals with security aspects associated with *local area networks* (*LANs*). *Important topics* examined include network topologies (connection schemes) and standard network connectivity devices, servers, the OSI model*,* network control strategies, networking protocols (rules) such as TCP/IP, IP addressing schemes and the Ethernet standard. It also includes logical access control for network environments - including user and group access controls instituted through the server's network OS, network authentication options, wireless network security considerations, securing network backup media.

Chapter 4 Cyber Security – Dealing with security issues posed by Wide Area Networks (WANs) such as the Internet and protection of the organization from external threats. The *key elements* of this chapter cover authentication protocols, data cryptography, and data encryption techniques. It also examines Virtual Private Networks (VPNs) and firewalls, System Auditing and Event Logging as tools, along with different types of Intrusion Detection Systems (IDS).

Chapter 5 Enterprise Network Security - Focuses on traditional *Information Technology* security typically found in domain-based enterprise\business network environments. *Key topic areas* covered includes traditional business network configuration and variations, including intranets, extranets. It also discusses common protective network structures including security zones, tunnels, DMZs and Honey Pots. It also covers application security considerations, including software design, database security, and application security. It also covers server and network virtualization activities, cloud security concerns, as well as organizational risk assessment/ analysis, implementing corporate policies, business contingencies and disaster recovery planning.

Chapter 6 Industrial Cyber Security Systems – Encompasses computing and intelligent control systems associated with *automated processes*, *Industrial Control Systems* (*ICS*), utility-related *smart grid* systems, smart meters, and *Supervisory Control and Data Acquisition* (*SCADA*) systems. It also introduces non-IT network devices such as Programmable Logic Controllers (PLCs), Remote Telemetry Units (RTUs) and Intelligent Electronic Devices (IEDs), as well as cloud computing and Internet of Things (IoT) concepts to the industrial network environment.

Chapter 7 ***Medical/IoT Network Security*** – Highlights the increased liability issues and governmental regulations attached to medical record handling. It examines computing and network devices and practices specific to medical record handling security. The proliferation of medical Internet of things devices and the vulnerabilities of these devices along with techniques and practices used to secure them are covered.

Chapter 8 Introduction to Ethical Hacking – Examines the history of "hacking", hacker types (Black/White/Gray), actors (Script kiddies, Cyber Terrorist, Cyber Hacktivists, Cyber Criminals, nation-state sponsored hackers), and important hacking examples. The chapter focuses on penetration testing (pentesting) - Legalities, pentest teams, attack strategies (Lockheed-Martin Kill Chain), and test reporting. Different types of cyber attacks (sniffing, Man in the Middle, attacks, Cache poisoning, social engineering methods, etc) are conducted.

According to ISACA "The majority of enterprises said practical, **hands-on experience** was the most important qualification in a security candidate"

MARCRAFT
an ETG Brand

CYBER SECURITY ADVANCED

CISSP *Certified Information Systems Security Professional*

Advanced Enterprise:

Security and Risk Management
Asset Security
Security Engineering
Communications and Network Security
Identity and Access Management
Security Assessment and Testing
Security Operations
Software Development Security

Advanced Internet of Things (IoT):

Design, build, program, troubleshoot and secure IoT devices. Create IoT devices to perform specific tasks including - temperature measurements, proximity detection, remote monitoring, remote access control, and automated lighting control . Secure IoT devices and systems to avoid potentially damaging or dangerous exploitable vulnerabilities associated with these devices.

GICSP *Global Industrial Cyber Security Professional*

Industrial Security Systems:

Access Management
Change Management
Cyber Security Essentials for ICS
Disaster Recovery
ICS Architecture
ICS Modules and Elements Hardening
ICS Security
Incident Management
Basic Process Control Systems
Safety and Protection Systems
Physical Security

CEH *Certified Ethical Hacker*

Hacking, Cracking, Internet Jacking:

Penetrate into Network Systems
Scan, Test, Hack and Secure Networks
Use Perimeter Defenses to Scan and Attack
Intrusion Detection, Buffer Overflows, DDoS
Learn Threats to Cloud Computing
Pen Testing
Mobile Phone Hacks
Virus, Trojan, Backdoors, Social Engineering
Information Security Controls and Laws

New!

DIGITAL FORENSICS

Based on NIST, students learn industry hands-on practices for the recovery and investigation of material found in digital devices.

Introduction to Digital Devices
Investigative Procedures
Hardware 101
Operating Systems/File Systems
Passwords and Trouble Zones
Tools of the Trade

Evidence
Retrieving Data
Mobile Device Forensics
Network Forensics
Online World and Email
Preparing to Testify

Be sure to call 800-441-6006 or e-mail us at info@marcraft.com for a FREE EVALUATION copy of the Student Text and Lab Guides