Cyber Learning Solutions
2014 Extended Course Catalog

Raytheon Cyber Solutions Inc. (RCSI)
cyber-training@list.app.ray.com
www.raytheon.com
CONTENTS

The Raytheon Difference ................................................................. 3
Executive Courses ........................................................................... 4
Manager Courses ........................................................................... 4
Practitioner Courses ....................................................................... 5
Exercise and Capstone Courses ....................................................... 8
Cyber Background™ Series Courses ............................................... 8
Course Development ................................................................. 9

© 2014, Raytheon Company. All rights reserved. Federal copyright law prohibits the reproduction, distribution, public performance, or public display of copyrighted materials without the express and written permission of the copyright owner. The course materials and descriptions in this catalog are provided solely for the purpose of evaluating Raytheon’s products and services for purchase by government agencies, private companies and individuals. All other uses are prohibited.
THE RAYTHEON DIFFERENCE

A full spectrum of solutions

Raytheon’s Cyber Operations Training curriculum stems from unmatched expertise, the kind that can only come from one of the largest training and technology organizations in the world. Raytheon delivers proven training programs and best practices across the entire cyber operations spectrum, and integrates cyber operations training into hybrid mission planning to optimize operational effects. We partner with an extensive network of industry experts to translate deep technical knowledge about the latest threats, exploitation techniques, malware and advance defensive strategies into relevant, up-to-date training. Cyber Operations Training’s customizable offerings include executive-level training, frontline mission management training, specific training for cyber practitioners, and broad-based training for the overall workforce. We address the full spectrum of topics related to cyber operations including trusted sourcing/supply chain management, software development, engineering and information assurance. Our learning environments include classroom, web-based/distance learning and mobile training teams for continuing education.

Performance that’s proven

Raytheon’s Cyber Operations Training programs are utilized within our own global workforce in order to manage computer network operations and defenses, as well as to enhance the skills and situational awareness of our personnel across multiple disciplines within the company.

Benefits — and a commitment — that endure

Raytheon is committed to building partnerships that are centered around continuous learning, so we remain engaged with customers even after formal training is complete. This ensures our customers are continually updated on new threats, vulnerabilities and best practices. We offer access to our most innovative and secure virtual platform to provide simple to complex simultaneous learning and a mechanism for up-to-date training and solutions to real time problem sets.

The global training leader

Raytheon Company is one of the world’s largest training organizations and is responsible for some of the industry’s most complex multi-year training programs. Our proven processes focus on customer requirements to address our customers’ most difficult challenges.

Customer success is our mission — and that mission never rests.
### EXECUTIVE COURSES

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C100-2014-01</td>
<td>Cyberexecutive™ (1 Day)</td>
</tr>
<tr>
<td>C107-2012-01</td>
<td>Cyberexecutive™ (3 Hour)</td>
</tr>
</tbody>
</table>

A one-day abridgement of our cyberexecutive™ curriculum, this course will focus on selected issues of interest to executive audiences while focusing on specific industry/organization needs. Instructional teams will work with the customer to determine the depth and range of topics.

**Course Format/Availability**

Instructor Led; 1 Day (On Site)

### MANAGER COURSES

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C200-2014-01</td>
<td>Cybermanager™ Course (2 Day)</td>
</tr>
</tbody>
</table>

The cyberexecutive™ course provides leaders and decision makers with a detailed introduction to current issues facing industry and government in the field of cyber security and the tools to make smart decisions about an organization’s vulnerabilities, risks and response posture to the most pressing and sophisticated cyber attacks.

**Who benefits from this course?**

Executives/senior managers, senior technical staff, technical and non-technical teams requiring an in-depth introduction to cyber security.

**What Students Will Learn**

Issues relating to the cyber landscape, hacker tools and techniques, human and social cyber, current events, planning and integrating cyber security into an organization.

**Course Outline**

1. The Cyber Landscape
2. Finding Vulnerabilities
3. Getting on Networks
4. Achieving Network Effects
5. Human Cyber Techniques
6. Advanced Persistent Threats
7. Social Network Security
8. Hactivism
9. Technology Outsourcing
10. Law, Ethics and Privacy

**Course Format/Availability**

Instructor Led; 2 Days (On Site)
C300-2014-01 CyberPractitioner Course (5 Day)

The cyber manager’s course is a week-long introduction to offensive and defensive cyber security with an emphasis on the technical fundamentals required to effectively manage cyber security professionals and operations. This course is tailored for practitioners and technically savvy managers.

Who benefits from this course?

Direct leaders and supervisors of IT security/cyber security/cyber operations requiring a detailed technical introduction to the domain in a one week format.

What Students Will Learn

Tools and techniques employed by hackers and defenders in the current cyber security landscape, as well as emerging issues related to managing cyber projects.

Course Outline

1. Fundamentals of Cyber
2. Terms, Tasks and Targets
3. Using an Exploit
4. Examining Network Traffic
5. Format, System and Web Vulnerabilities
6. Network and Application Security Tools
7. Reverse Engineering
8. Human Cyber Techniques
9. Law, Ethics and Privacy

The course includes hands-on exercises culminating in a three hour “Hacker Jeopardy” challenge exercise.

Course Format/Availability

Instructor Led; 5 Days (On Site)

C300-2012-01 Cyberprofessional™ Course

Our signature course for technical practitioners, the cyberprofessional™ course teaches the tools and techniques used by attackers and defenders in all critical aspects of the cyber domain. The course builds on fundamentals in reverse engineering, attack techniques, and human dimensions of cybersecurity to design sophisticated attack and defense scenarios. The course culminates in a three-day capstone exercise that simulates a diversity of real-world cyber attacks.

Who benefits from this course?

IT security professionals seeking to hone their cyber attack and defense skills, operational cyber practitioners working in a national security context, software engineers looking to understand cybersecurity in order to develop advanced defenses

Course Outline

1. Week One: Fundamentals
   a. What is Cyber?
   b. Vulnerabilities
   c. Security Tools and Techniques
   d. Reverse Engineering
   e. Human Cyber Techniques
2. Week Two: Applications
   a. Gaining Access
   b. Collection and Effects
   c. Communication and Stealth
   d. Counter Adversary CNO
   e. Forensics
3. Week Three: Advanced Topics and Exercises
   a. Social Cyber
What Students Will Learn

Hands-on techniques for attacking and defending a computer network against cyber attacks ranging from sophisticated malware to Hactivist and social engineering vulnerabilities.

b. Mobile and Wireless Security
c. Capstone

The course includes a three day hands-on capstone experience that presents students with twenty technical challenges from all aspects of cyber. A realistic narrative based on a defense, industrial or government scenario keeps students engaged; a capture-the-flag style contest keeps them challenged to learn and have fun!

Course Format/Availability

Instructor Led; 15 Days (On Site)
<table>
<thead>
<tr>
<th>Week</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Applications: Gaining Access</td>
<td>Applications: Collection and Effects</td>
<td>Applications: Communication and Stealth</td>
<td>Applications: Counter Adversary CNO</td>
<td>Applications: Forensics</td>
</tr>
<tr>
<td></td>
<td>800 Characterizing Targets</td>
<td>Surveying a Computer</td>
<td>Covert Communication and Command Control</td>
<td>Adversary Techniques: Spear Phishing</td>
<td>Incident Handling</td>
</tr>
<tr>
<td></td>
<td>900 Exercise: ID a Cyber Target</td>
<td>Collecting Target Data</td>
<td>Adversary Techniques: Host Data Forensics</td>
<td>Host Data Forensics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1000 Using COTS Access Tools</td>
<td>Steganography</td>
<td>Exercise: Identify Source</td>
<td>Exercise: Counter Effects</td>
<td>Network Data Forensics</td>
</tr>
<tr>
<td></td>
<td>1100 Metasploit Exploits</td>
<td>Hands-on: Steganography</td>
<td>Exercise: Counter Effects</td>
<td>ANTIFORENSICS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1200</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1300 Writing a Custom Exploit</td>
<td>Network Effects</td>
<td>Rootkits</td>
<td>Adversary Techniques II: Intellectual Property Theft</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1400 Shellcoding</td>
<td>Denial of Service</td>
<td>Hands-on: Rootkits</td>
<td>Attack Forensics: Hands On</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1500 Elevating Privilege</td>
<td>Advanced CNO Effects</td>
<td>Persistence Techniques</td>
<td>Exercise: Tag and Track Data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1600 Privsec Tools</td>
<td>Exercise: Mission Effects</td>
<td>Hands-on: Persistence</td>
<td>Exercise: Redirection</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Advanced Topics: Social Cyber</td>
<td>Advanced Topics: Mobile and Wireless</td>
<td>Capstone</td>
<td>Capstone</td>
<td>Capstone</td>
</tr>
<tr>
<td></td>
<td>800 Web 2.0 and Social Media</td>
<td>Intro to Mobile and Wireless</td>
<td>Capstone Introduction</td>
<td>Capstone Exercise</td>
<td>Capstone Exercise</td>
</tr>
<tr>
<td></td>
<td>900 Information Gathering</td>
<td>802.11 Vulnerabilities</td>
<td>Capstone Exercise: Block One</td>
<td>Capstone Exercise: Block Three</td>
<td>Capstone Exercise: Block Five</td>
</tr>
<tr>
<td></td>
<td>1000 Privacy and Anonymity</td>
<td>Wireless Survey</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1100</td>
<td>Key Cracking and Attacks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1200</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1300 Social Identities</td>
<td>Mobile Handset Vulnerabilities</td>
<td>Capstone Exercise: Block Two</td>
<td>Capstone Exercise: Block Four</td>
<td>Capstone Wrapup Discussions</td>
</tr>
<tr>
<td></td>
<td>1400 Data Analysis Techniques</td>
<td>Hands-on: Mobile Handset</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1500 Connective Data</td>
<td>Rogue Network Attacks</td>
<td></td>
<td></td>
<td>Course Evaluations</td>
</tr>
<tr>
<td></td>
<td>1600</td>
<td>Hands-on: Open BTS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EXERCISE AND CAPSTONE COURSES

Prerequisite for this course is the 3 week CyberProfessional course.

C400-2014-01 Cyber Capstone Course

This fast-paced, five day exercise course tests students’ ability to solve realistic problems in the cyber domain while competing in teams to earn points and have fun. Twenty technical challenges ranging from vulnerability discovery to insider threat detection, forensics and social network analysis are combined with a fully-developed narrative that allows students to play the role of an IT professional, cyber warrior or critical decision maker. Gameplay can be scaled between easy, medium and hard challenges within the same learning objectives.

Who benefits from this course?

Students who have completed introductory and advanced cyber training who want an exercise course to fully integrate their learning, and teams desiring a practical exercise to assess and develop their cyber skills.

What Students Will Learn

How to apply practical learning in a range of cyber topics to a realistic, fast-paced set of technical challenges.

Technical Challenges Include:

- Vulnerability Discovery
- Reverse Engineering
- Incident Forensics
- Insider Threat
- Malware
- Social Network Analysis
- Crisis Response

Course Format/Availability

Instructor Led; Exercise; 5 Days (On Site); This course will be finalized upon customer request.

CYBER BACKGROUND™ SERIES COURSES

About Cyber Background™ Series Courses

The national need for cyber skills cannot be met fully by professionals with the prerequisite knowledge and experience to proceed directly to advanced learning. Unfortunately, many entry-level certificate programs jump directly to technical application without teaching the foundational knowledge needed to succeed in the cyber domain. The Cyber Background™ Series provides an alternate path to this foundational knowledge for students without formal education in computer science, network security or a related discipline. These five-day, instructor-led courses follow a traditional lecture, text and exercise format.
<table>
<thead>
<tr>
<th>Code</th>
<th>Course Name</th>
<th>Format/Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>C600-2014-01</td>
<td>Assembly Programming</td>
<td>Instructor Led; 5 Day (On Site)</td>
</tr>
<tr>
<td>C600-2014-02</td>
<td>Binary Exploitation</td>
<td>Instructor Led; 5 Day (On Site)</td>
</tr>
<tr>
<td>C600-2014-03</td>
<td>Phoenix</td>
<td>Instructor Led; 5 Day (On Site)</td>
</tr>
<tr>
<td>C600-2014-04</td>
<td>Reverse Engineering</td>
<td>Instructor Led; 5 Day (On Site)</td>
</tr>
</tbody>
</table>

**COURSE DEVELOPMENT**

**Instructional Design and Development Services from Raytheon**

Raytheon is the world’s leading developer and provider of full service, integrated training solutions for government agencies and the largest commercial organizations. We have successfully managed some of the most complex training outsourcing programs in the world. We deliver a comprehensive menu of training solutions and services based on proven training expertise and processes that help our customers achieve measurable operational advantages, improved readiness and enhanced performance, while optimizing efficiencies and reducing costs.

While each engagement is unique, our promise remains the same: to improve organizational performance and personnel effectiveness – efficiently, cost-effectively and exponentially. Our proven value comes from our approach. Because every organization – and every training challenge – is different, we partner with customers to
deliver solutions specifically tailored to their needs. This highly customized approach is unique to Raytheon and allows us to deliver significant, measurable and targeted results while making the most of an organization’s training budget – driving down costs per training event and improving training efficiency.