SANS Courses Roadmap

Douranacademy.com

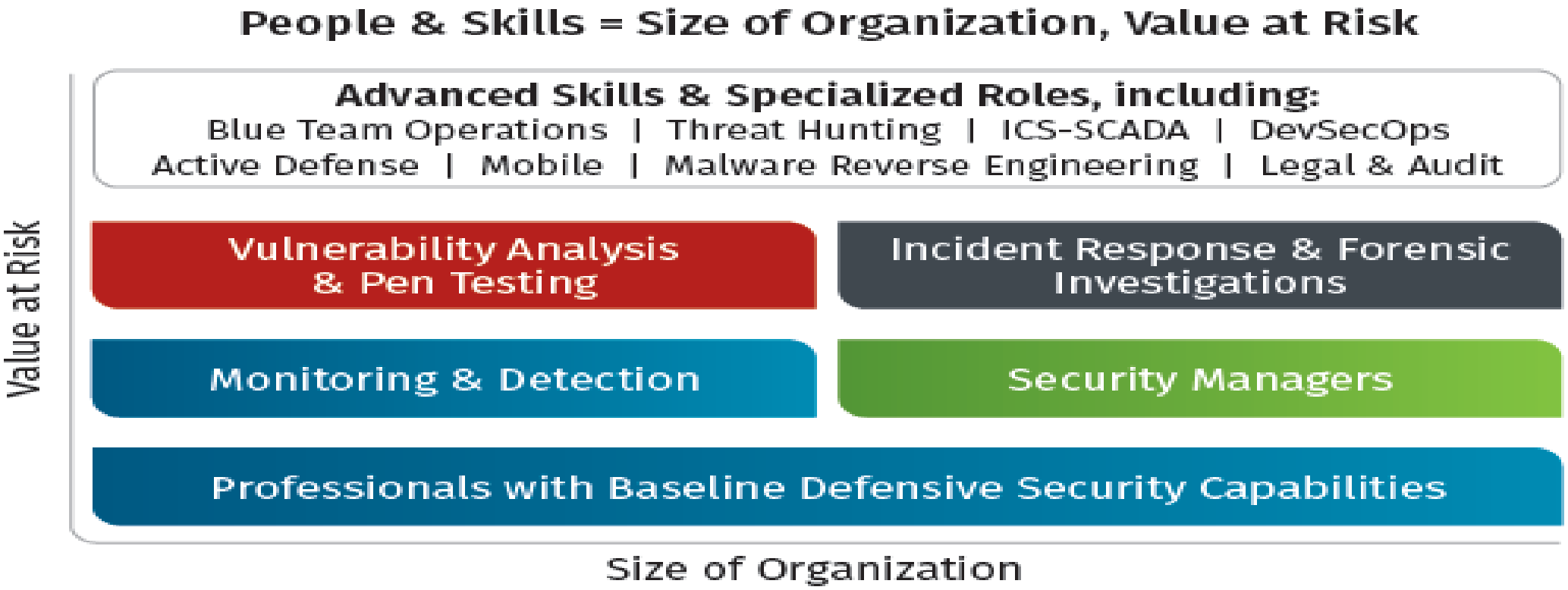
t.me/douranAC

Instagram@douranacademy

Tel:43585 264 , 266

Mobile: 09383207884

Based on our global research, SANS has identified effective strategies for building an information security group



SANS Training Format

Live Classroom Instruction

Training Events

Our live events feature SANS instructors teaching multiple courses at a single location. You'll get:

- Focused, immersive learning without distractions
- Direct access to SANS Certified Instructors
- Opportunities to network with and learn from other cybersecurity professionals
- The chance to attend SANS@Night events, NetWars, vendor presentations, industry receptions, and many other activities

Our live events in North America serve thousands of students annually in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Smaller, regional events are scheduled in most major metropolitan areas throughout the year.

Summits

SANS Summits take place over one or two days, and focus on a single topic of particular interest to the community. We curate our presentations and speakers to ensure that participants get the most relevant and applicable information.

Before or after each Summit we offer SANS courses that are closely aligned with the topic, so you can enhance your Summit experience with in-depth training while you're there.

Community SANS Courses

Our Community events offer SANS courses, coursewares, and labs taught by up-and-coming instructors in more local, regional areas.

With smaller classes, you get more direct interaction with your instructor, and the regional location means an easier, less expensive commute.

Private Classes

A SANS Certified Instructor can train your staff privately at your location, incorporating insights, experiences, and questions specific to your business objectives.

Private training allows your team to freely discuss sensitive issues, and spend more time focusing on the topics most relevant to your organization.

Online Training

SANS Online Training features top course authors and instructors teaching our most popular courses, delivered via four flexible online platforms:

- **OnDemand:** Learn anytime, anywhere with our custom OnDemand platform
- **vLive:** Attend virtual evening sessions with SANS instructors
- **Simulcast:** Livestream a daytime SANS course from a live event
- **SelfStudy:** Self-paced learning with books and MP3s

Our online training platforms include either four or six months of access to your course, as well as support from a team of SANS subject-matter experts. Access to all course labs and the ability to revisit content without limits ensures that you can master the content at your own pace.

Because you can rewind, revisit, and reinforce the course material, retention is easier and your learning outcome will be the same as if you attended live SANS training. Try out the OnDemand platform by viewing a course preview at sans.org/demo.

DOURAN GROUP

SANS Flagship Programs and Free Resources

GIAC CERTIFICATIONS

GIAC Certifications

SANS courses are the ideal preparation for a GIAC Certification, the highest standard in cybersecurity certification. More than 30 GIAC Certifications allow you to demonstrate your unique expertise in specialized areas of cybersecurity. No other certification program in the world comes close to GIAC in validating real-world knowledge and skill, due largely to the extensive exam preparation process and team of expert contributors.

giac.org

SANS Technology Institute

Graduate and Undergraduate Programs in Cybersecurity

The SANS Technology Institute offers a leadership-focused master's degree program and job-specific graduate certificate programs for working InfoSec professionals and an undergraduate certificate program for college students and mid-career professionals seeking to launch a career in cybersecurity. Corporate tuition reimbursement or VA education benefits often apply.

sans.edu

CyberTalent

SANS CyberTalent

SANS CyberTalent provides innovative workforce development and talent management solutions for the cybersecurity industry. Our web-based assessment tools and Immersion Academies help organizations build, retain, and motivate a high-performance cybersecurity team as well as grow the cybersecurity workforce.

sans.org/cybertalent

SANS SECURITY AWARENESS

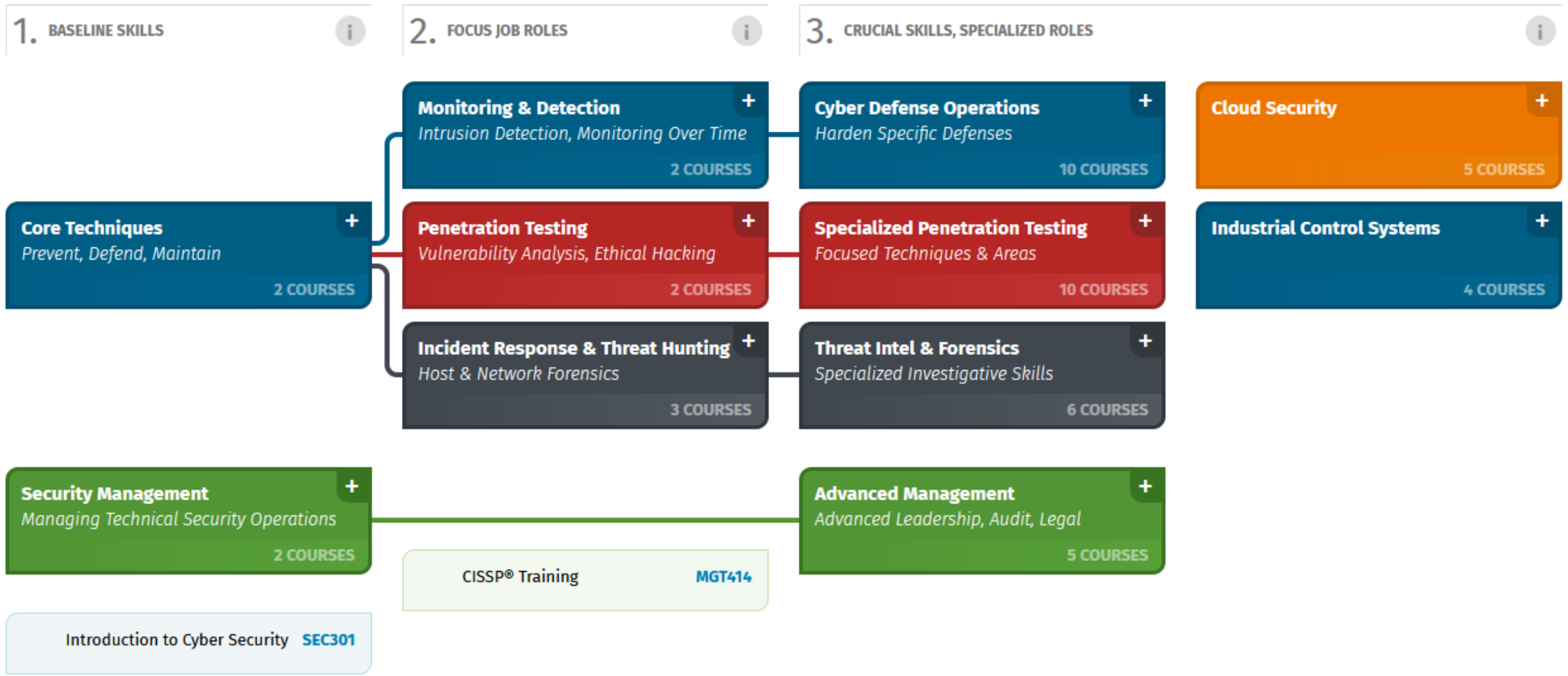
SANS Security Awareness

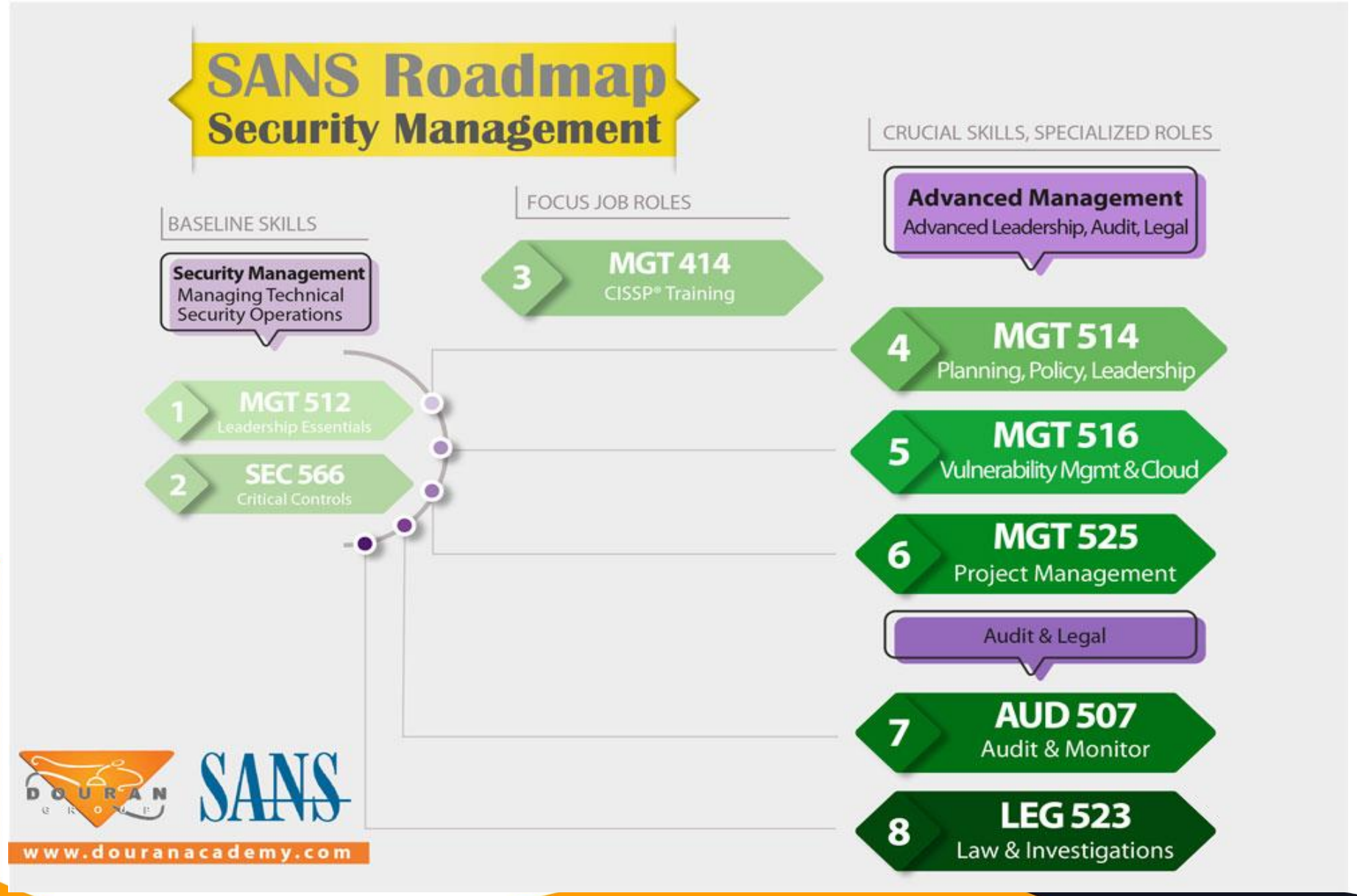
SANS Security Awareness offers a robust suite of computer-based security awareness training modules, support materials, and online phishing training that is engaging and effective. You can host our training on any learning management system, in many languages, to create a secure culture within your organization.

sans.org/awareness

DOURAN GROUP

Cyber Security Skills Roadmap




SANS Roadmap
Security Management
BASELINE SKILLS
Security Management
Managing Technical
Security Operations
1 MGT 512
Leadership Essentials
2 SEC 566
Critical Controls
FOCUS JOB ROLES
3 MGT 414
CISSP® Training
CRUCIAL SKILLS, SPECIALIZED ROLES
Advanced Management
Advanced Leadership, Audit, Legal
4 MGT 514
Planning, Policy, Leadership
5 MGT 516
Vulnerability Mgmt & Cloud
6 MGT 525
Project Management
Audit & Legal
7 AUD 507
Audit & Monitor
8 LEG 523
Law & Investigations
DOURAN
GROUP
SANS
www.douranacademy.com

MGT 512, Security Leadership Essentials for Managers

You Will Be Able To

- Become an effective information security Manager
- Get up to speed quickly on information security issues and terminology
- Establish a minimum standard of security knowledge, skills, and abilities
- Speak the same language as technical security professionals

This course prepares you to:

- Make sense of different cybersecurity frameworks
- Understand and analyze risk
- Manage technical personnel
- Build a vulnerability management program
- Strategically leverage a SIEM
- Change behavior and build a security-aware culture
- Effectively manage security projects

• SECTION 1: Building Your Program

- **Topics:** Security Frameworks; Understanding Risk; Security Policy; Program Structure.

SECTION 1: Building Your Program

Topics: Security Frameworks; Understanding Risk; Security Policy; Program Structure.

SECTION 3: Protecting and Patching Systems

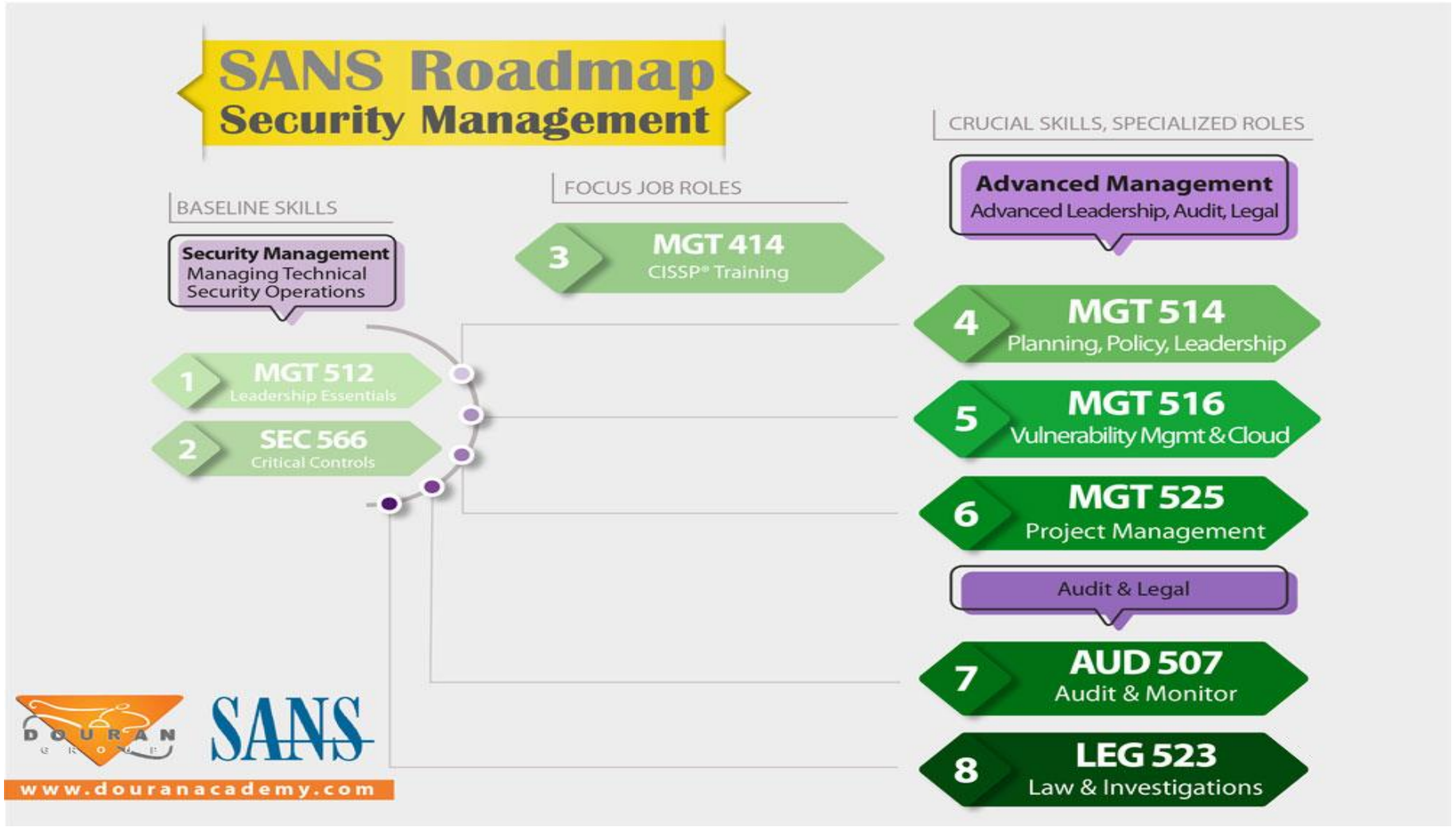
Topics: Host Security; Application Security; Physical Security; Vulnerability Management

SECTION 4: Leading Modern Security Initiatives

Topics: Security Awareness; Maturity Model; Project Management; Projects, Programs; Portfolios Management Process; Cloud Security; Amazon Web Services; Modern Security Architecture: Zero Trust Model; User, Device, and Application Authentication and Access; Management Methods; Managing Technical People

SECTION 5: Detecting and Responding to Attacks

Topics: Logging and Monitoring; Security Operations Center; Incident Response; Contingency Planning; War Game


SANS Roadmap
Security Management
BASELINE SKILLS
Security Management
Managing Technical
Security Operations
1 MGT 512
Leadership Essentials
2 SEC 566
Critical Controls
FOCUS JOB ROLES
3 MGT 414
CISSP® Training
CRUCIAL SKILLS, SPECIALIZED ROLES
Advanced Management
Advanced Leadership, Audit, Legal
4 MGT 514
Planning, Policy, Leadership
5 MGT 516
Vulnerability Mgmt & Cloud
6 MGT 525
Project Management
Audit & Legal
7 AUD 507
Audit & Monitor
8 LEG 523
Law & Investigations
DOURAN
SANS
www.douranacademy.com

SEC 566, Implementing and Auditing the Critical Security Controls – In-Depth

You Will Be Able To

- Apply a security frame work based on actual threats that is measurable, scalable, reliable
- Understand the importance of each control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilize tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of controls
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002
- Audit each of the Critical Security Controls, with specific, proven templates, checklists

DOURAN GROUP

SECTION 1: Introduction and Overview of the 20 Critical Controls

Topics: #1: Inventory of Authorized and Unauthorized Devices; #2: Inventory of Authorized and Unauthorized Software.

SECTION 2: Critical Controls 3, 4, 5, and 6

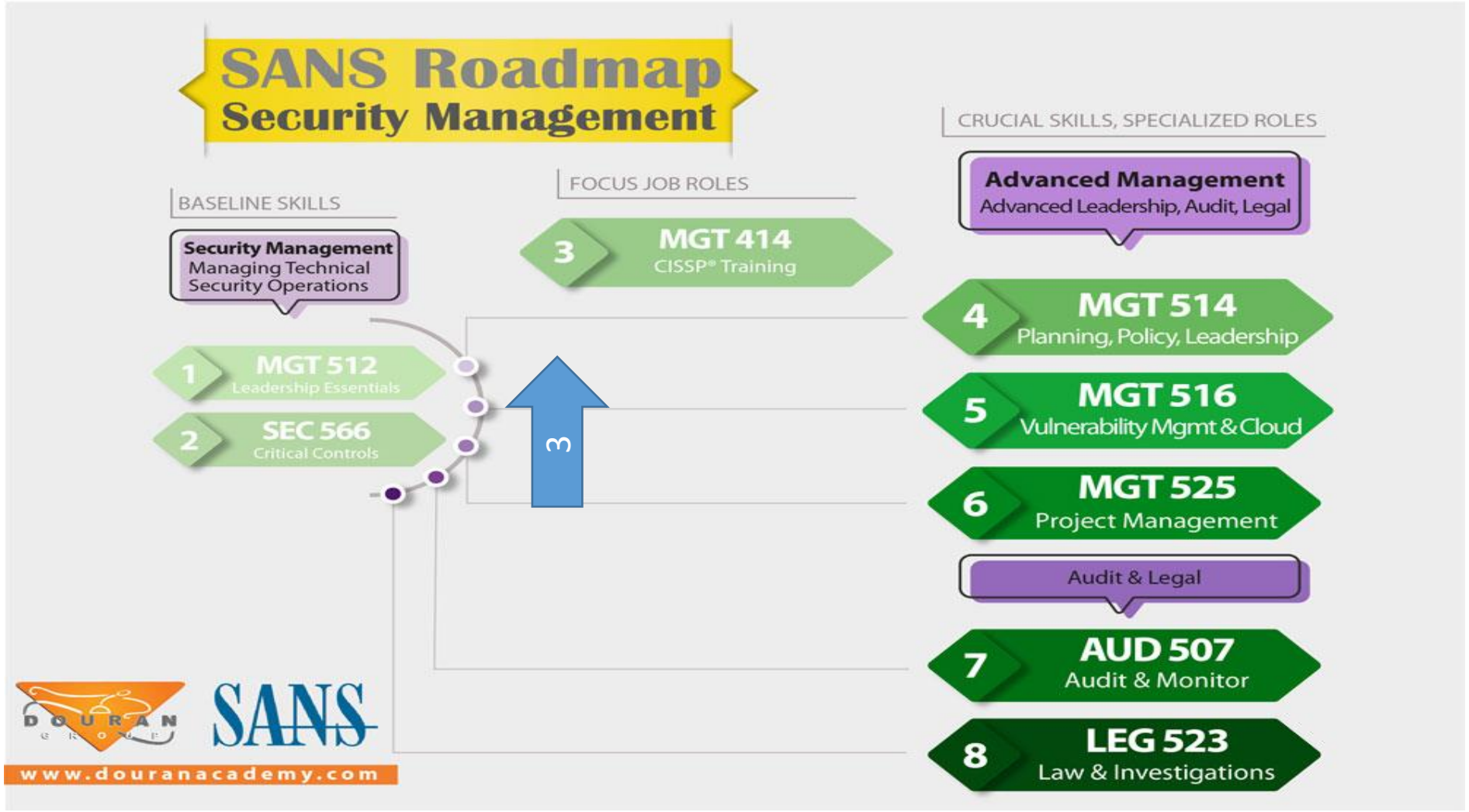
Topics: #3: Secure Configuration s for Hardware and Software on Laptops, Workstations, and Servers; #4: Continuous Vulnerability Assessment; #5: Controlled Use of Administrative Privileges; #6: Maintenance, Monitoring, and Analysis of Audit Logs

SECTION 3: Critical Controls 7, 8, 9, 10, and 11

Topics: #7: Email and Web Browser Protections; #8: Malware Defenses; #9: Limitation and Control of Network Ports, Protocols, and Services; #10: Data Recovery Capability #11: Secure Configurations for Network Devices

SECTION 4: Critical Controls 12, 13, 14, and 15

Topics: #12: Boundary Defense; #13: Data Protection; #14: Controlled Access Based on the Need to Know; #15: Wireless Device Control


SANS Roadmap
Security Management
BASELINE SKILLS
Security Management
Managing Technical Security Operations
FOCUS JOB ROLES
3 MGT 414
CISSP® Training
CRUCIAL SKILLS, SPECIALIZED ROLES
Advanced Management
Advanced Leadership, Audit, Legal
4 MGT 514
Planning, Policy, Leadership
5 MGT 516
Vulnerability Mgmt & Cloud
6 MGT 525
Project Management
Audit & Legal
7 AUD 507
Audit & Monitor
8 LEG 523
Law & Investigations
1 MGT 512
Leadership Essentials
2 SEC 566
Critical Controls
3
DOURAN GROUP
SANS
www.douranacademy.com

SEC 566, Implementing and Auditing the Critical Security Controls – In-Depth

You Will Be Able To

- Apply a security frame work based on actual threats that is measurable, scalable, reliable
- Understand the importance of each control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilize tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of controls
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002
- Audit each of the Critical Security Controls, with specific, proven templates, checklists

DOURAN GROUP

SECTION 1: Introduction and Overview of the 20 Critical Controls

Topics: #1: Inventory of Authorized and Unauthorized Devices; #2: Inventory of Authorized and Unauthorized Software.

SECTION 2: Critical Controls 3, 4, 5, and 6

Topics: #3: Secure Configuration s for Hardware and Software on Laptops, Workstations, and Servers; #4: Continuous Vulnerability Assessment; #5: Controlled Use of Administrative Privileges; #6: Maintenance, Monitoring, and Analysis of Audit Logs

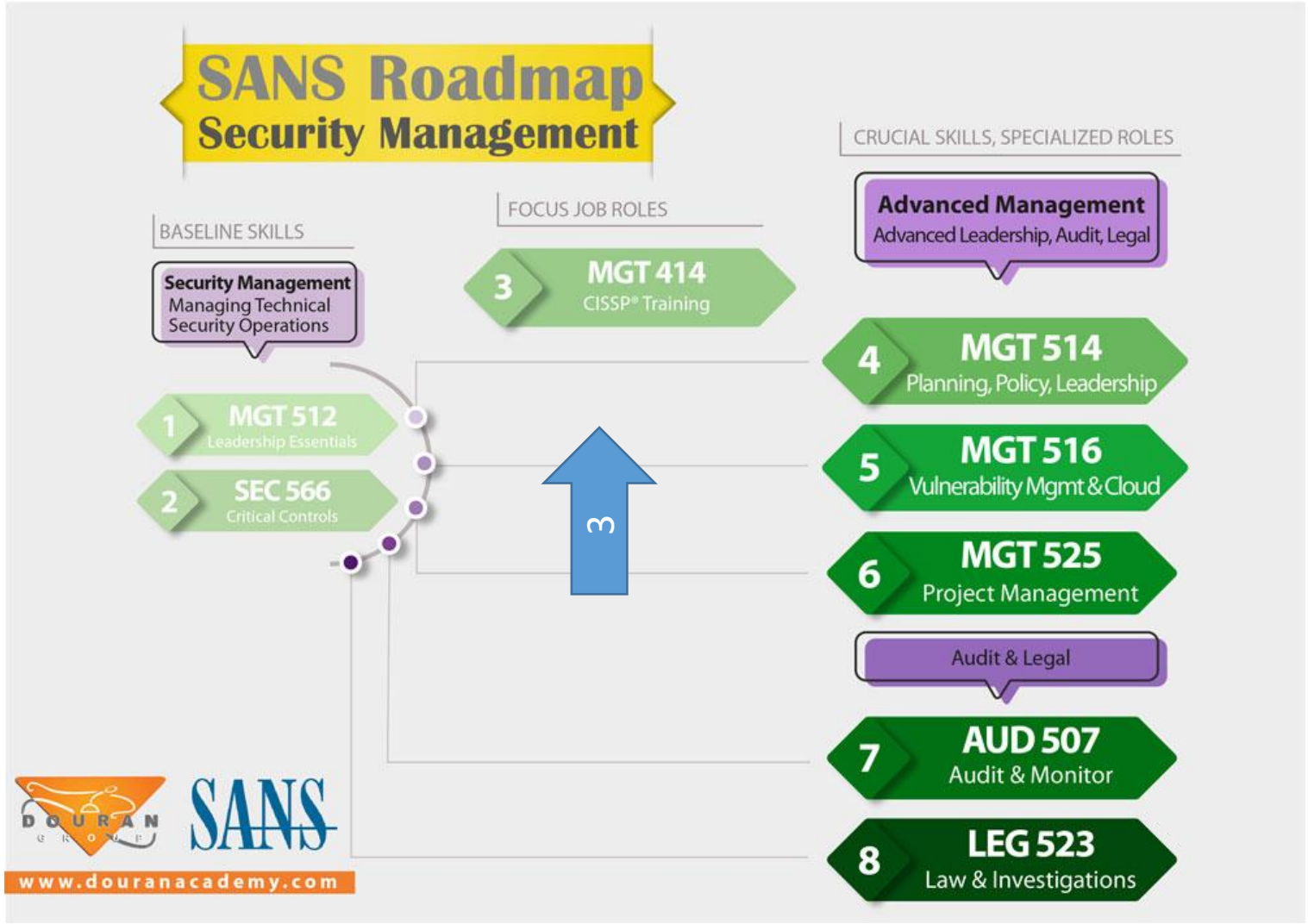
SECTION 3: Critical Controls 7, 8, 9, 10, and 11

Topics: #7: Email and Web Browser Protections; #8: Malware Defenses; #9: Limitation and Control of Network Ports, Protocols, and Services; #10: Data Recovery Capability #11: Secure Configurations for Network Devices

SECTION 4: Critical Controls 12, 13, 14, and 15

Topics: #12: Boundary Defense; #13: Data Protection; #14: Controlled Access Based on the Need to Know; #15: Wireless Device Control

DOURAN GROUP


SANS Roadmap
Security Management
BASELINE SKILLS
Security Management
Managing Technical
Security Operations
1 MGT 512
Leadership Essentials
2 SEC 566
Critical Controls
FOCUS JOB ROLES
3 MGT 414
CISSP® Training
3
CRUCIAL SKILLS, SPECIALIZED ROLES
Advanced Management
Advanced Leadership, Audit, Legal
4 MGT 514
Planning, Policy, Leadership
5 MGT 516
Vulnerability Mgmt & Cloud
6 MGT 525
Project Management
Audit & Legal
7 AUD 507
Audit & Monitor
8 LEG 523
Law & Investigations
DOURAN
GROUP
SANS
www.douranacademy.com

MGT 414, SANS Training Program for CISSP® Certification

You Will Be Able To

- Understand the eight domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

This course prepares you to:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

SECTION 1: Introduction; Security and Risk Management

Topics: Overview of CISSP® Certification; Introductory Material; Overview of the Eight Domains; Domain 1: Security and Risk Management

SECTION 2: Asset Security and Security Engineering – Part 1

Topics: Domain 2: Asset Security; Domain 3: Security Engineering (Part 1)

SECTION 3: Security Engineering – Part 2; Communication and Network Security

Topics: Domain 3: Security Engineering (Part 2); Domain 4: Communication and Network Security

SECTION 4: Identity and Access Management

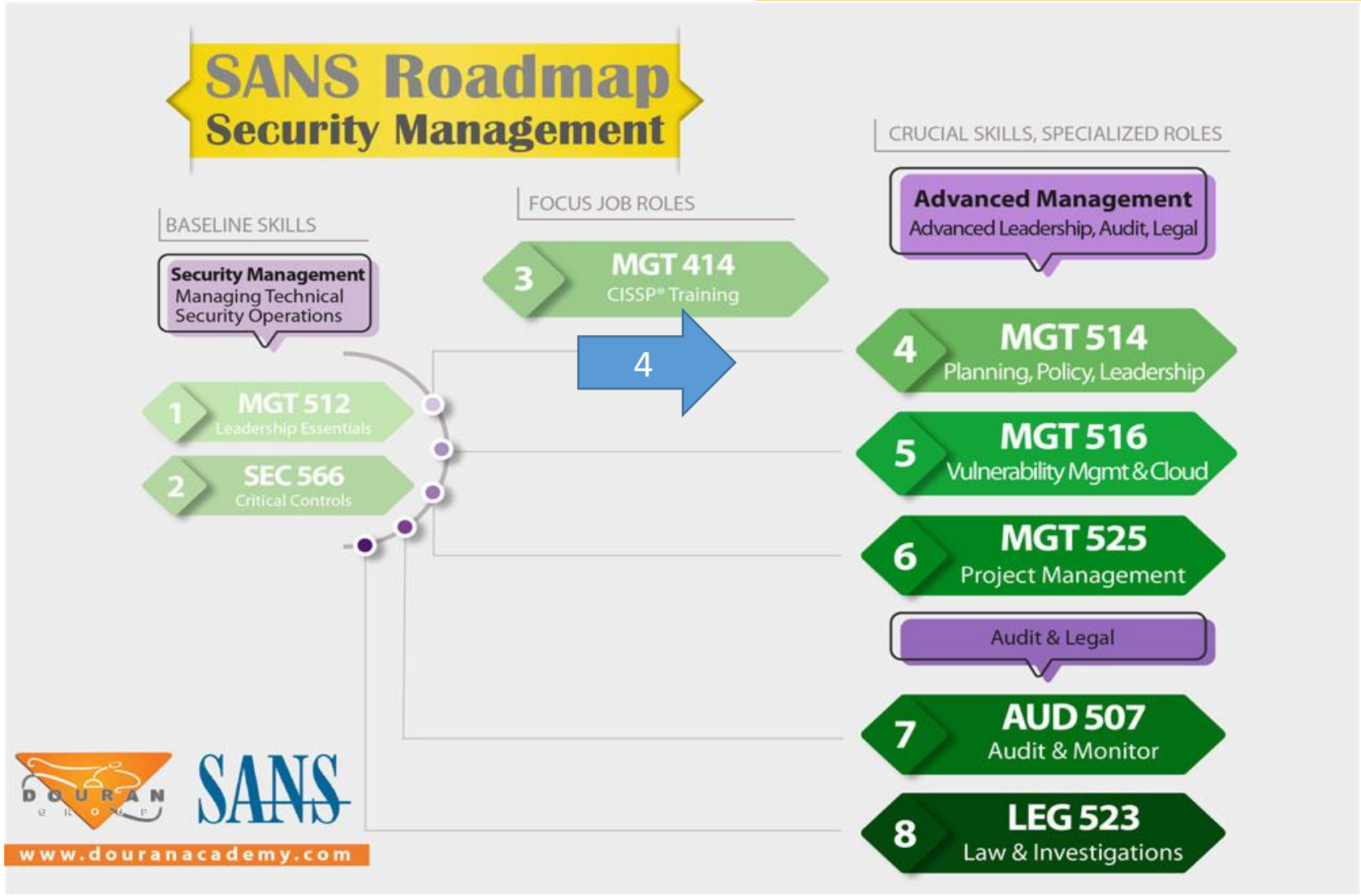
Topics: Domain 5: Identity and Access Management

SECTION 5: Security Assessment and Testing; Security Operations

Topics: Domain 6: Security Assessment; Domain 7: Security Operations

SECTION 6: Software Development Security

Topics: Domain 8: Software Development Security


SANS Roadmap
Security Management
BASELINE SKILLS
Security Management
Managing Technical
Security Operations
1 MGT 512
Leadership Essentials
2 SEC 566
Critical Controls
FOCUS JOB ROLES
3 MGT 414
CISSP® Training
4
CRUCIAL SKILLS, SPECIALIZED ROLES
Advanced Management
Advanced Leadership, Audit, Legal
4 MGT 514
Planning, Policy, Leadership
5 MGT 516
Vulnerability Mgmt & Cloud
6 MGT 525
Project Management
Audit & Legal
7 AUD 507
Audit & Monitor
8 LEG 523
Law & Investigations
DOURAN
GROUP
SANS
www.douranacademy.com

MGT 516, Managing Security Vulnerabilities: Enterprise and Cloud

You Will Be Able To

- Create, implement, or improve your vulnerability management program
- Establish a secure and defensible enterprise and cloud computing environment
- Build an accurate and useful inventory of IT assets in the enterprise and cloud
- Identify existing vulnerabilities and understand the severity level of each
- Prioritize vulnerabilities for treatment
- Effectively report and communicate vulnerability data within your organization
- Engage treatment teams and make vulnerability management

This course prepares you to:

- Prepare: Define, build, and continuously improve the program
- Identify: Identify vulnerabilities present in our operating environments
- Analyze: Analyze and prioritize identified vulnerabilities and other program metrics
- Communicate: Present the findings from analysis appropriately and efficiently for each
- stakeholder group

SECTION 1: Overview and Identify

Topics: Course Introduction and Overview; Cloud Overview; Cloud Design and Architecture; Asset Management; Finding Vulnerabilities

SECTION 2: Identify and Analyze

Topics: Finding Vulnerabilities; Analyzing Vulnerabilities; Introduction to Solution Grouping

SECTION 3: Communicate and Treat

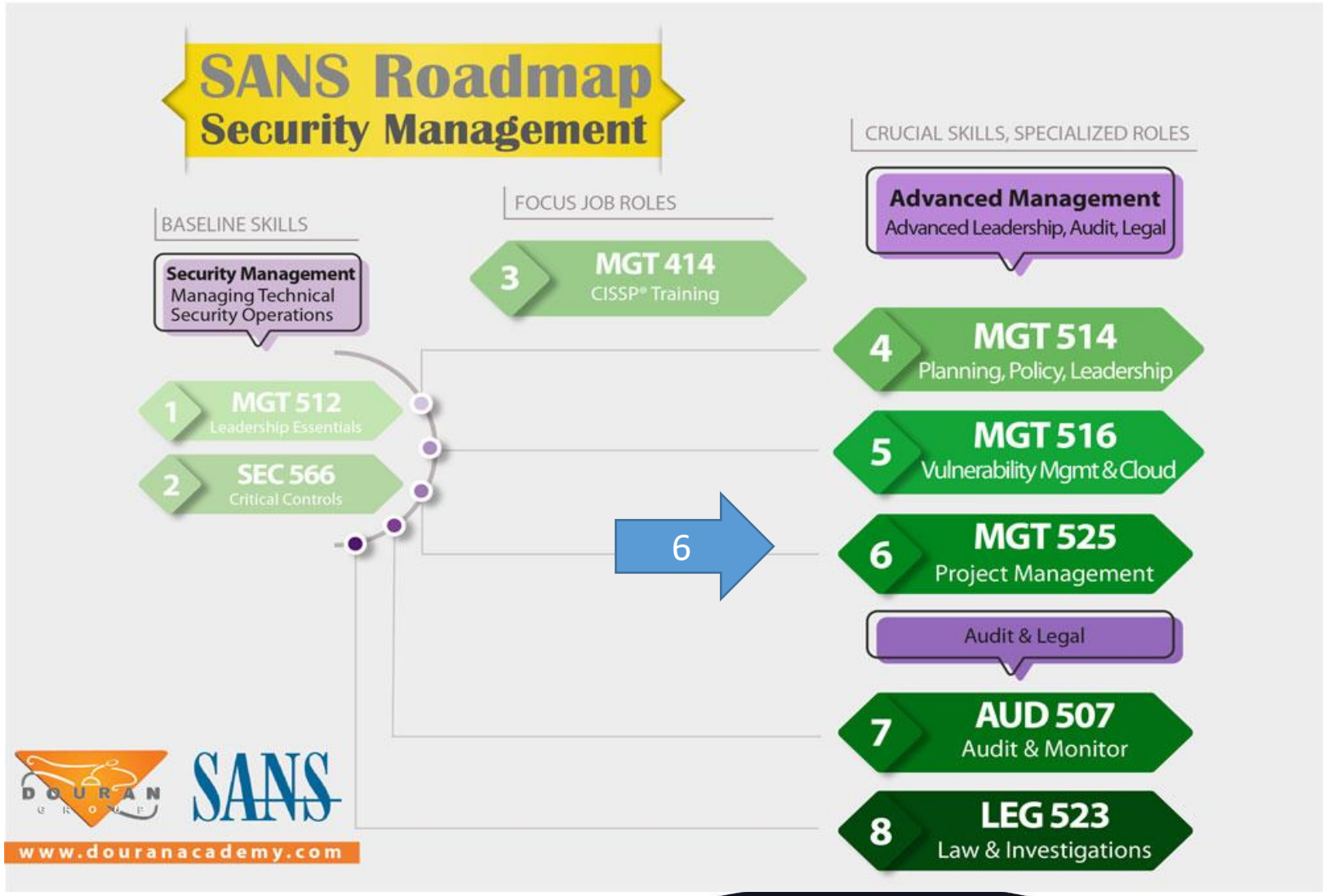
Topics: Communication; Treatment

SECTION 4: Treatment, Buy-in, and Program

Topics: Treatment; Buy-in; Program

SECTION 5: Managing Vulnerabilities: Capstone Lab Exercise

Topics: Section 5 begins with a review of a scenario that triggers the group capstone exercise. The section is broken up into various sections and scenarios that stem from the main case study, which enables students to delve into various aspects of the PIACT model. A review of findings and conclusions will follow each section of the exercise, allowing each team to present its findings to the other teams and to engage in class discussions on the topics covered.


SANS Roadmap
Security Management
BASELINE SKILLS
Security Management
Managing Technical
Security Operations
FOCUS JOB ROLES
3 MGT 414
CISSP® Training
CRUCIAL SKILLS, SPECIALIZED ROLES
Advanced Management
Advanced Leadership, Audit, Legal
1 MGT 512
Leadership Essentials
2 SEC 566
Critical Controls
4 MGT 514
Planning, Policy, Leadership
5 MGT 516
Vulnerability Mgmt & Cloud
6
6 MGT 525
Project Management
Audit & Legal
7 AUD 507
Audit & Monitor
8 LEG 523
Law & Investigations
DOURAN
GROUP
SANS
www.douranacademy.com

MGT 525, IT Project Management, Effective Communication, and PMP® Exam Prep

You Will Be Able To

- Recognize the top failure mechanisms related to IT and InfoSec projects, so that your projects can avoid common pitfalls
- Create a project charter that defines the project sponsor and stakeholder involvement
- Document project requirements and create a requirements traceability (life cycle)
- Clearly define the scope of a project in terms of cost, schedule and technical deliverables
- Create a work breakdown structure defining work packages, project deliverables and acceptance criteria
- Develop a detailed project schedule, including critical path tasks and milestones
- Develop a detailed project budget, including cost baselines and tracking mechanisms

This course prepares you to:

- This course is offered by the SANS Institute as a PMI® Registered Education Provider (R.E.P.)
- R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP)® and other professional credentials. PMP® is a registered trademark of Project Management Institute, Inc.

DOURAN GROUP

MGT 514, Security Strategic Planning, Policy, and Leadership

You Will Be Able To

- Develop security strategic plans that incorporate business and organizational drivers
- Develop and assess information security policy
- Use management and leadership techniques to motivate and inspire your teams

This course prepares you to:

- Develop Strategic Plans
- Create Effective Information Security Policy
- Develop Management and Leadership Skills

SECTION 1: Strategic Planning Foundations

Topics: Vision and Mission Statements; Stakeholder Management; PEST Analysis; Porter's Five Forces; Threat Actors; Asset Analysis; Threat Analysis

SECTION 2: Strategic Roadmap Development

Topics: Historical Analysis; Values and Culture; SWOT Analysis; Vision and Innovation; Security Framework; Gap Analysis; Roadmap Development; Business Case Development; Metrics and Dashboards; Marketing and Executive Communications

SECTION 3: Security Policy Development and Assessment

Topics: Purpose of Policy; Policy Gap Analysis; Policy Development; Policy Review; Awareness and Training

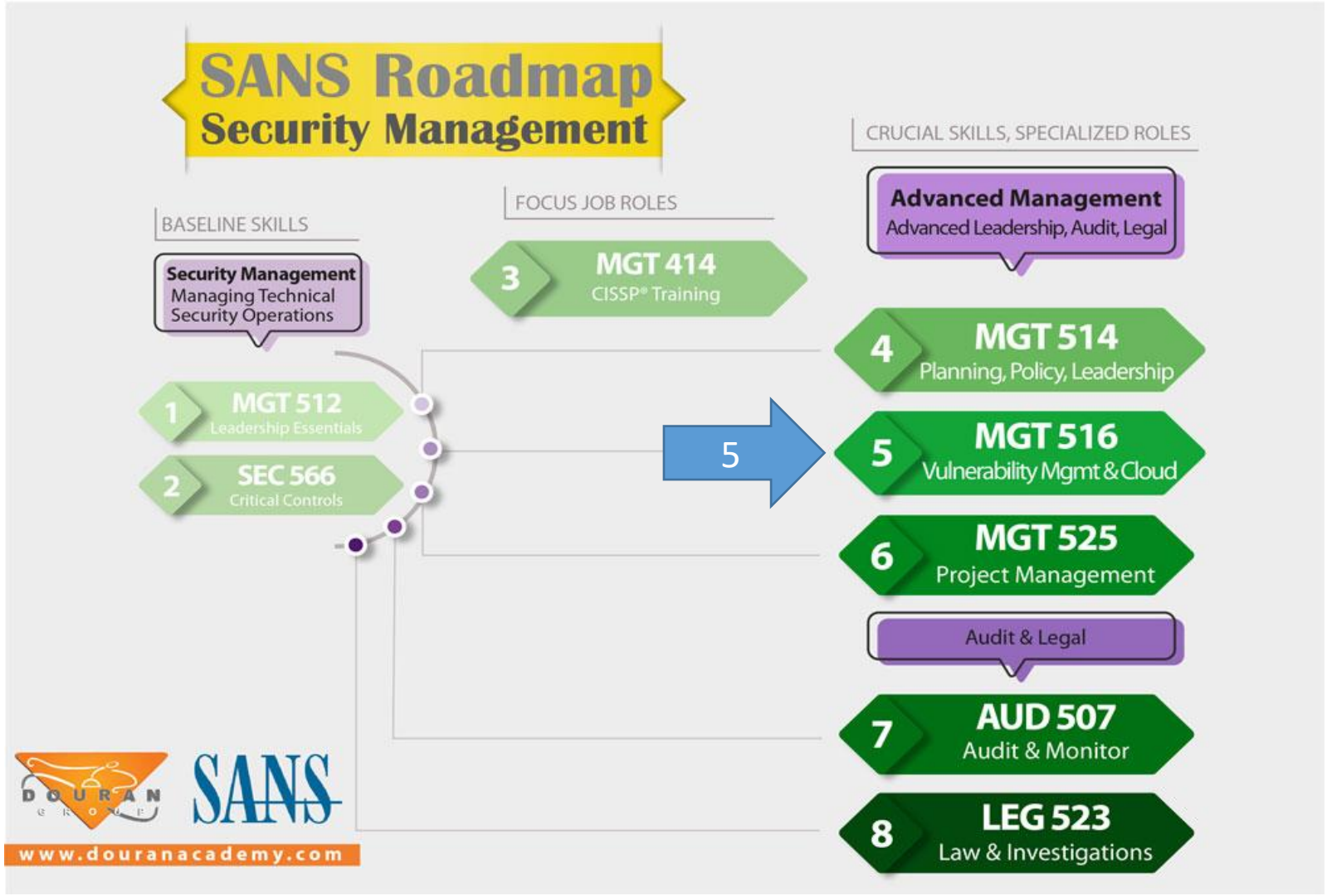
SECTION 4: Leadership and Management Competencies

Topics: Leadership Building Blocks; Creating and Developing Teams; Coaching and Mentoring; Customer Service Focus; Conflict Resolution; Effective Communication; Leading Through Change; Relationship Building; Motivation and Self-Direction; Teamwork; Leadership Development

SECTION 5: Strategic Planning Workshop

Topics: Creating a Security Plan for the CEO; Understanding Business Priorities; Enabling Business Innovation; Working with BYOD; Effective Communication; Stakeholder Management

DOURAN GROUP


SANS Roadmap
Security Management
BASELINE SKILLS
Security Management
Managing Technical
Security Operations
1 MGT 512
Leadership Essentials
2 SEC 566
Critical Controls
FOCUS JOB ROLES
3 MGT 414
CISSP® Training
5
CRUCIAL SKILLS, SPECIALIZED ROLES
Advanced Management
Advanced Leadership, Audit, Legal
4 MGT 514
Planning, Policy, Leadership
5 MGT 516
Vulnerability Mgmt & Cloud
6 MGT 525
Project Management
Audit & Legal
7 AUD 507
Audit & Monitor
8 LEG 523
Law & Investigations
DOURAN
SANS
www.douranacademy.com

SECTION 1: Project Management Structure and Framework

Topics: Definition of Terms and Process Concepts; Group Processes; Project Life Cycle; Types of Organizations; PDCA Cycle

SECTION 2: Project Charter and Scope Managements

Topics: Formally Initiating Projects; Project Charters; Project Scope Development; Work Breakdown Structures; Scope Verification and Control

SECTION 3: Schedule and Cost Management

Topics: Process Flow; Task Lead and Lag Dependencies; Resource Breakdown Structures; Task Duration Estimating; Critical Path Scheduling; Cost Estimating Tools; Cost vs. Quality; Cost Baselining; Earned Value

SECTION Communications and Project Resources

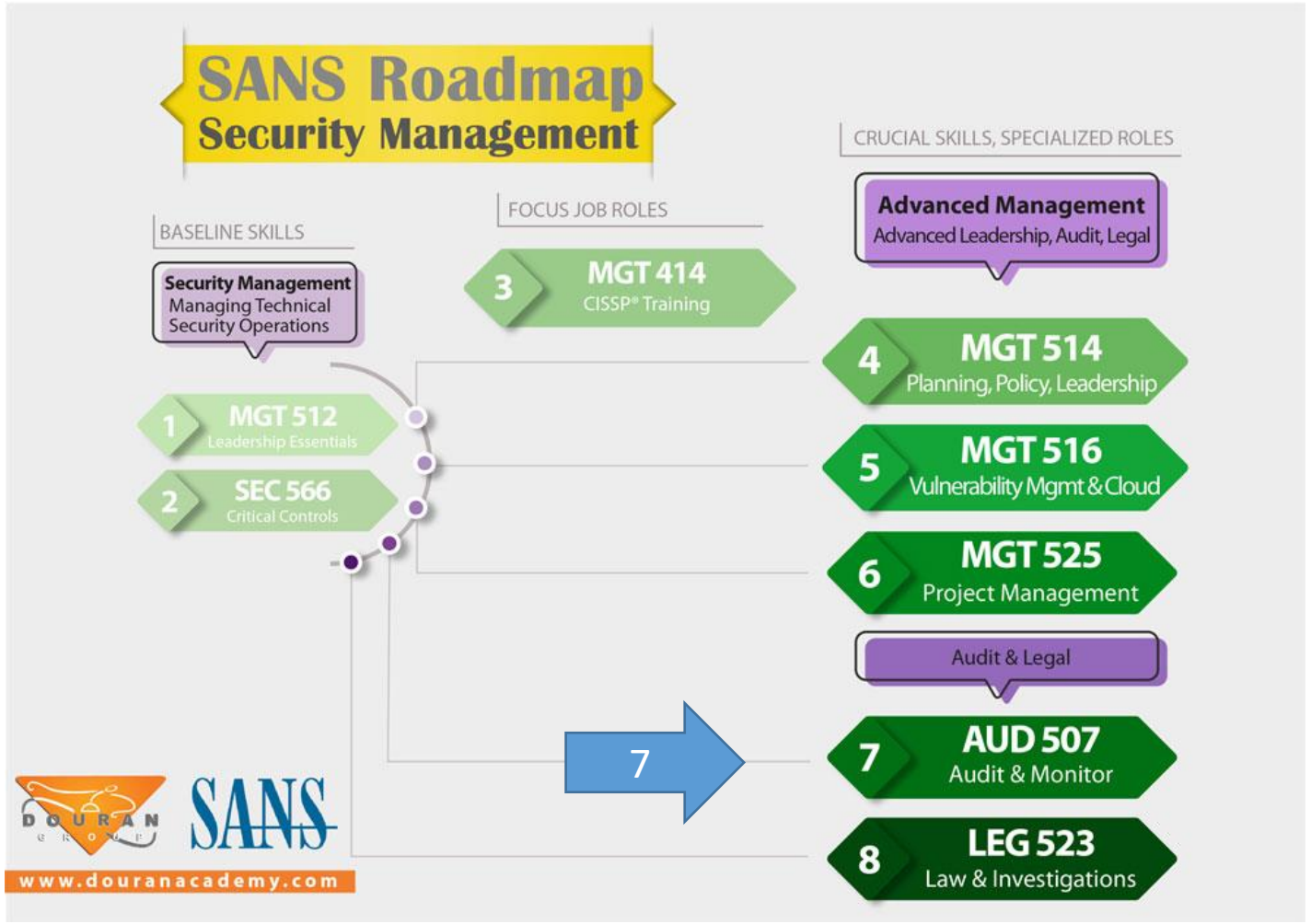
Topics: Acquiring and Developing Your Project Team; Organizational Dependencies and Charts; Roles and Responsibilities; Team Building;

SECTION 5: Quality and Risk Management

Topics: Cost of Quality; Quality Metrics; Continual Process Improvement; Quality Baselines; Quality Control; Change Control; Risk Identification; Risk Assessment

SECTION 6: Procurement, Stakeholder Management, and Project Integration

DOURAN GROUP


SANS Roadmap
Security Management
BASELINE SKILLS
Security Management
Managing Technical
Security Operations
FOCUS JOB ROLES
3
MGT 414
CISSP® Training
CRUCIAL SKILLS, SPECIALIZED ROLES
Advanced Management
Advanced Leadership, Audit, Legal
1
MGT 512
Leadership Essentials
2
SEC 566
Critical Controls
4
MGT 514
Planning, Policy, Leadership
5
MGT 516
Vulnerability Mgmt & Cloud
6
MGT 525
Project Management
Audit & Legal
7
7
AUD 507
Audit & Monitor
8
LEG 523
Law & Investigations
DOURAN
GROUP
SANS
www.douranacademy.com

AUD 507, Auditing & Monitoring Networks, Perimeters, and Systems

You Will Be Able To

- Understand the different types of controls (e.g., technical vs. non-technical)
- Conduct a proper risk assessment of a network to identify vulnerabilities and prioritize them
- Establish a well-secured baseline for computers and networks, constituting a standard against which one can conduct audits
- Perform a network and perimeter audit
- Audit firewalls to validate that rules/settings are working as designed, blocking traffic
- Checking vulnerability assessment tools effectively

This course prepares you to:

You'll be able to provide general checklist that can be customized for your audit practice. Each of these sections includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class

SECTION 1: Effective Audit Management, Risk Assessment, and Virtualization Auditing

Topics: Auditor's Role as it Relates to Policy Creation, Policy Conformance, Assessing Strategies

SECTION 2: Effective Network and Perimeter Auditing/Monitoring

Topics: Capturing and Analyzing Network Traffic; Analyzing and Validating Device Configurations; Testing Public Services; Network Mapping and Continuous Monitoring

SECTION 3: Web Application Auditing

Topics: Understanding HTTP, HTML, and Related Technologies; Related Technologies; The Burp Proxy; OWASP Top 10 List; Web Server Configuration; Secure Development Practices;

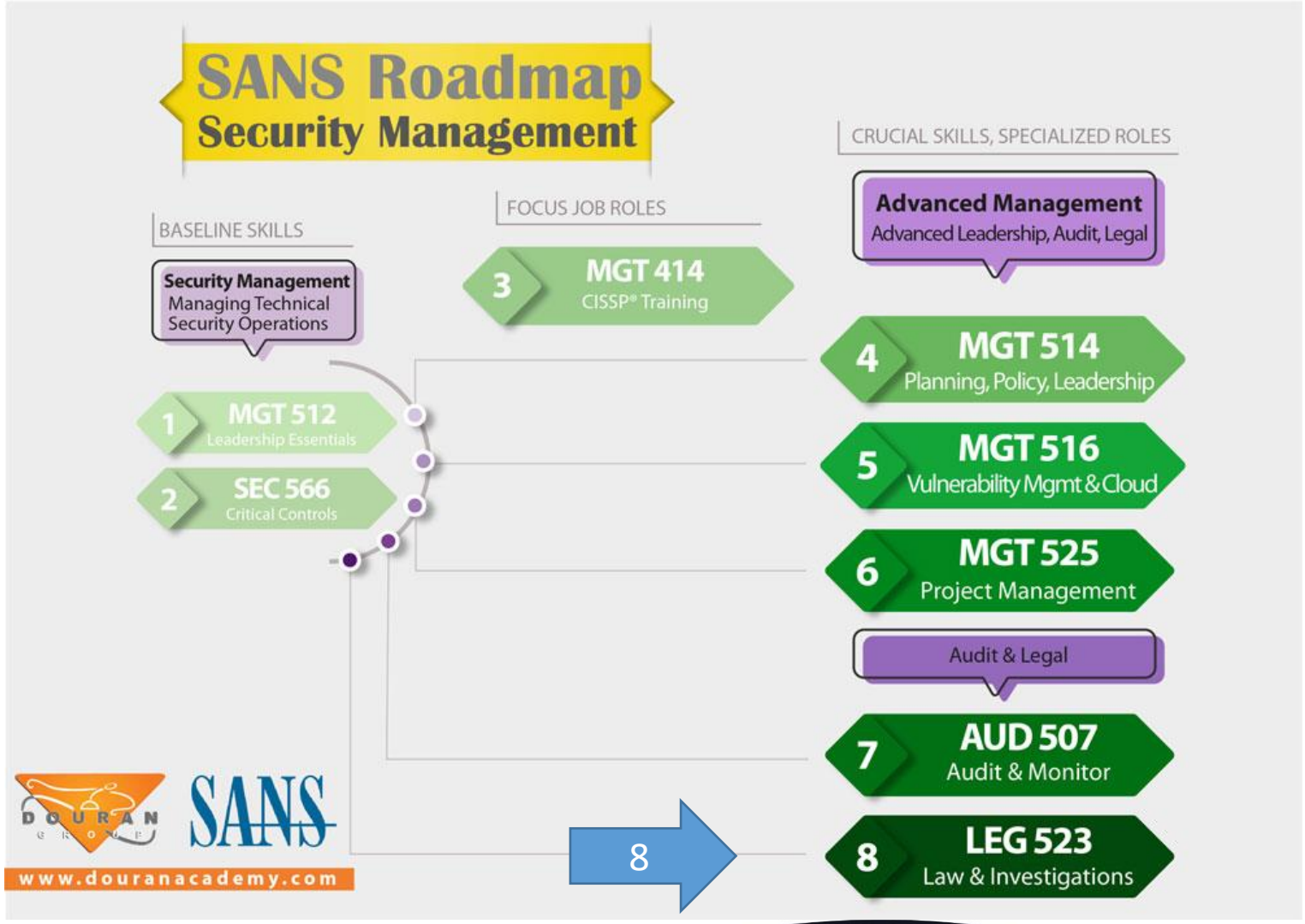
SECTION 4: Advanced Windows Auditing and Monitoring

Topics: Windows Support; PowerShell; Windows Management Instrumentation (WMI); LDAP; Password Management and Auditing; User Right Assignments; Security Settings; File and Share Permissions; Registry Permissions

SECTION 5: Advanced UNIX Auditing and Monitoring

Topics: Linux Basics; Command Line Tools and Scripting; Scripting; System Information; File Permissions; File Integrity; Services; Patching; Users, Groups and Privilege Management

SECTION 6: Audit the Flag Capstone Exercise


SANS Roadmap
Security Management
BASELINE SKILLS
Security Management
Managing Technical
Security Operations
1 MGT 512
Leadership Essentials
2 SEC 566
Critical Controls
FOCUS JOB ROLES
3 MGT 414
CISSP® Training
CRUCIAL SKILLS, SPECIALIZED ROLES
Advanced Management
Advanced Leadership, Audit, Legal
4 MGT 514
Planning, Policy, Leadership
5 MGT 516
Vulnerability Mgmt & Cloud
6 MGT 525
Project Management
Audit & Legal
7 AUD 507
Audit & Monitor
8 LEG 523
Law & Investigations
8
DOURAN GROUP
SANS
www.douranacademy.com

LEG 523, Law of Data Security and Investigations

You Will Be Able To

- Work better with other professionals at your organization who make decisions about the law of data security and investigations
- Exercise better judgment on how to comply with technology regulations
- Evaluate the role and meaning of contracts for technology, services, software and outsourcing
- Help your organization better explain its conduct to the public and to legal authorities
- Anticipate technology law risks before they get out of control
- Implement practical steps to cope with technology law risk

This course prepares you to:

You'll be able to produce your own checklist, or provide you with a general checklist that can be customized for your law practice. Each of these sections includes hands-on exercises

SECTION 1: Fundamentals of Data Security Law and Policy

Topics: introduction to cyber and data protection law, GDPR

SECTION 2: E-Records, E-Discovery, and Business Law

Topics: how dealing with records and evidence, practical understanding of e-discovery and policies on the retention and destruction of data. law of evidence and records management

SECTION 3: Contracting for Data Security and Other Technology

Topics: focus on the essentials of contract law sensitive to the current requirements for security, Compliance with many of the new data security laws requires contracts.;

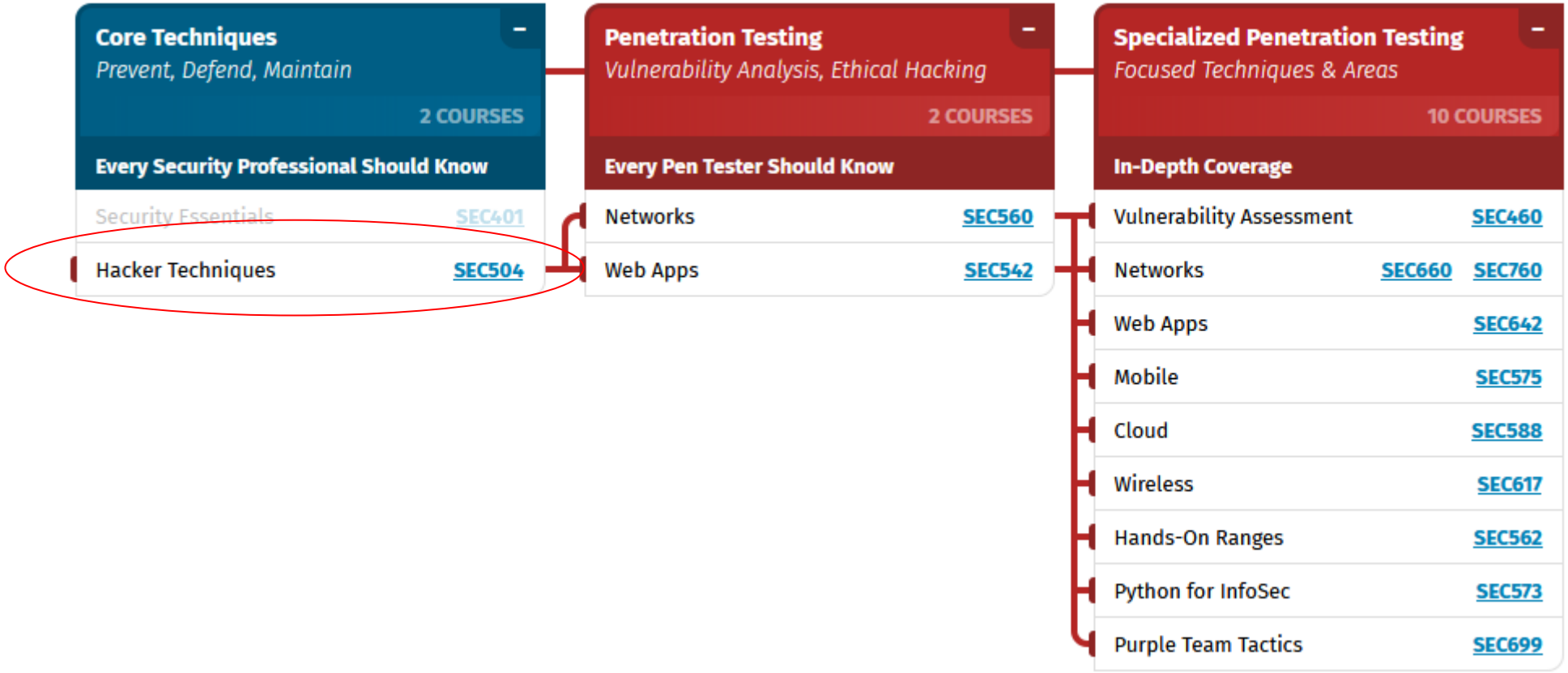
SECTION 4: The Law of Data Compliance, How to Conduct Investigations

Topics: methods to analyze a situation and then act in a way that is ethical, defensible, and reduces risk, methods and justifications for maintaining the confidentiality of an investigation

SECTION 5: Applying Law to Emerging Dangers, Cyber Defense

Topics: Section five is organized around extended case studies in security law: break-ins, investigations, extortion, rootkits, phishing, botnets, espionage, and defamation. The studies lay out the chronology of events and critique what the good guys did right and what they did wrong.

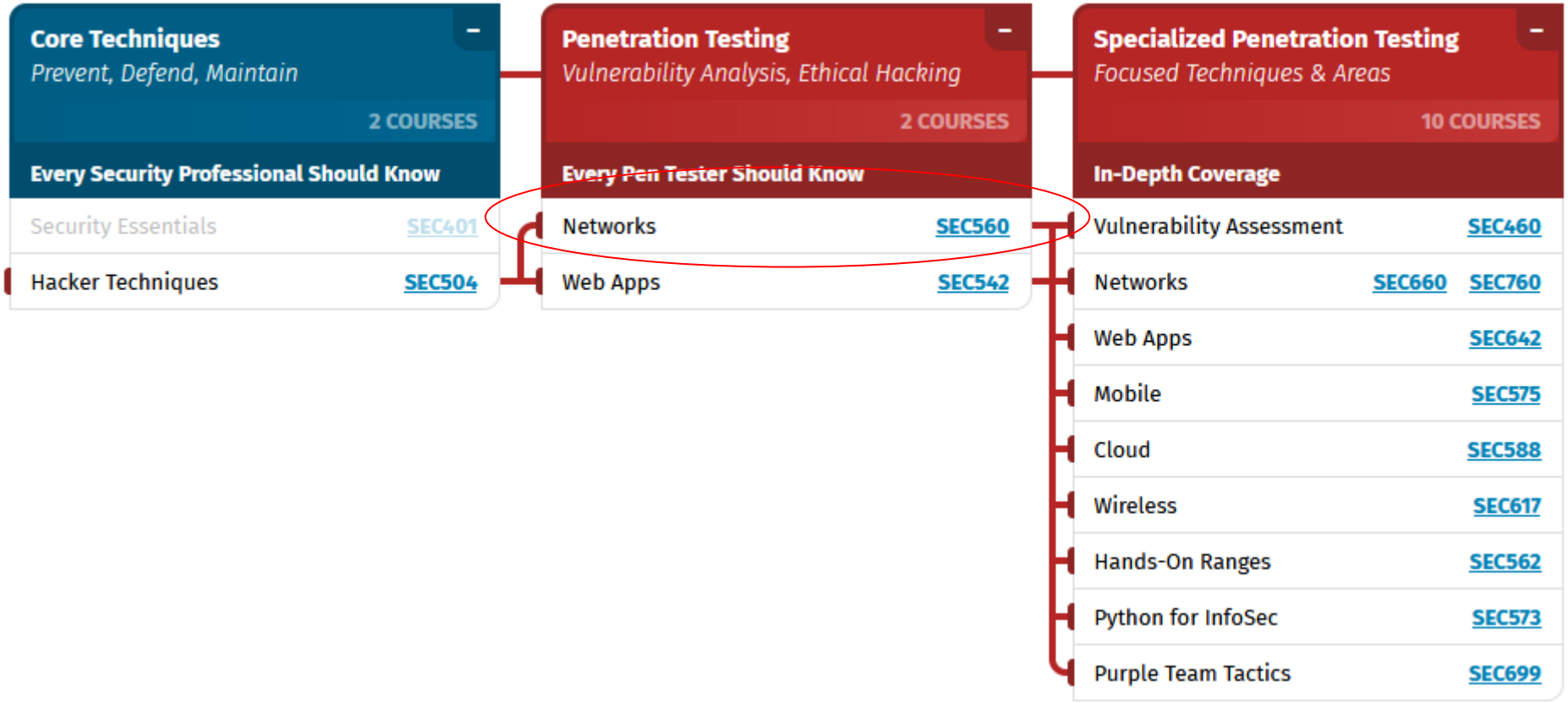
SANS Roadmap Penetration Testing



SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

- SEC504.1: Incident Handling Step-by-Step and Computer Crime Investigation
- SEC504.2: Computer and Network Hacker Exploits - Part 1
- SEC504.3: Computer and Network Hacker Exploits - Part 2
- SEC504.4: Computer and Network Hacker Exploits - Part 3
- SEC504.5: Computer and Network Hacker Exploits - Part 4
- SEC504.6: Hacker Tools Workshop

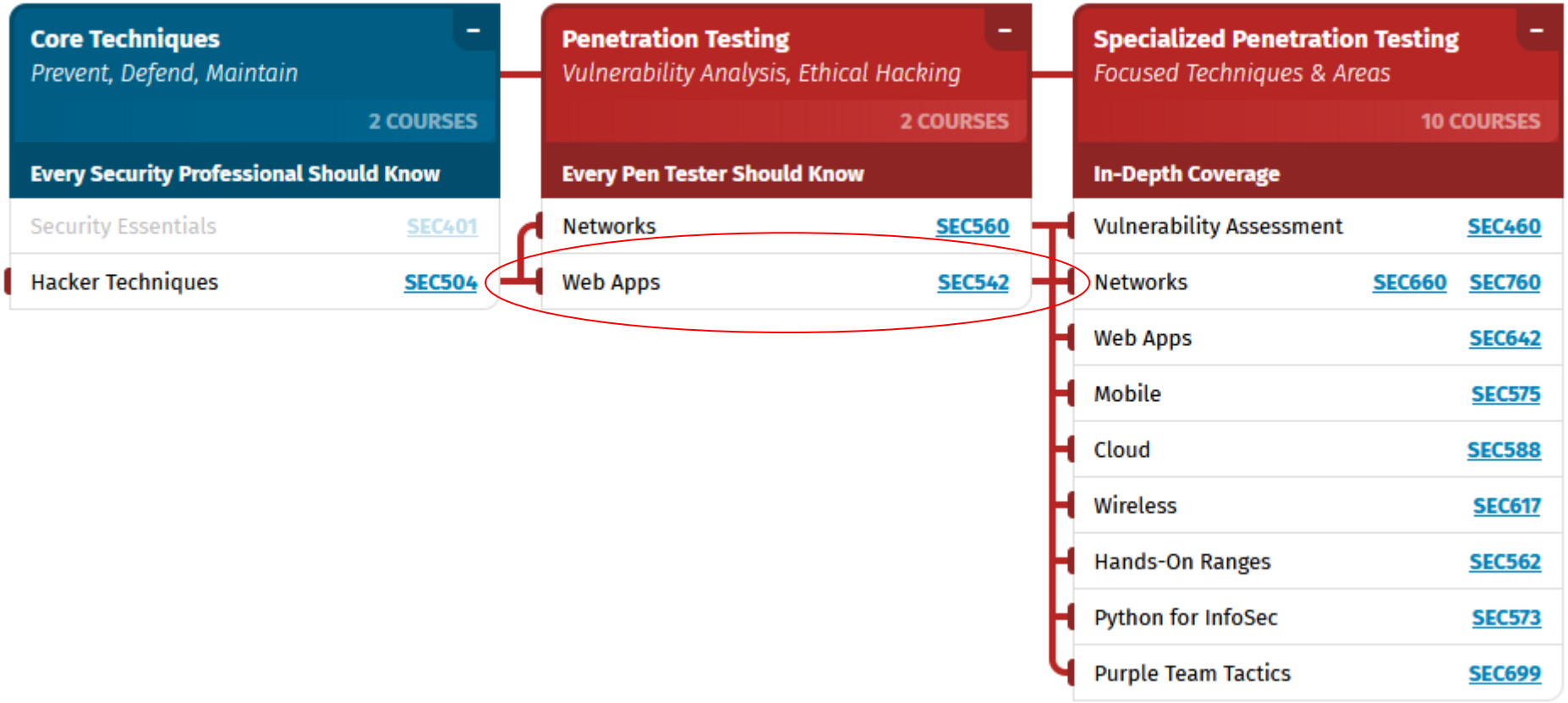
SANS Roadmap Penetration Testing



SEC560: Network Penetration Testing and Ethical Hacking

+ SEC560.1: Comprehensive Pen Test Planning, Scoping, and Recon
+ SEC560.2: In-Depth Scanning
+ SEC560.3: Exploitation
+ SEC560.4: Password Attacks and Merciless Pivoting
+ SEC560.5: Domain Domination and Web App Pen Testing
+ SEC560.6: Penetration Testing Workshop

SANS Roadmap Penetration Testing

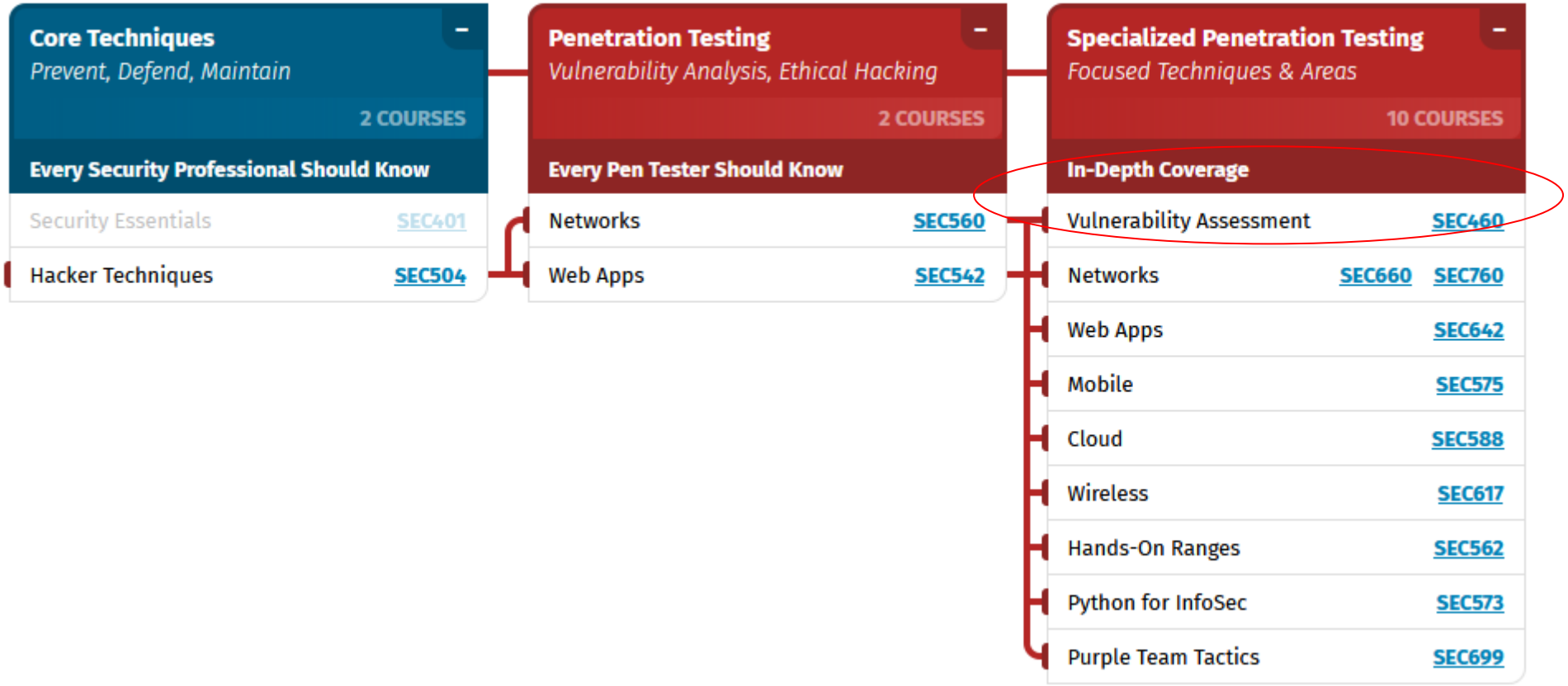


SEC542: Web App Penetration Testing and Ethical Hacking

+ SEC542.1: Introduction and Information Gathering
+ SEC542.2: Configuration, Identity, and Authentication Testing
+ SEC542.3: Injection
+ SEC542.4: XXE and XSS
+ SEC542.5: CSRF, Logic Flaws and Advanced Tools
+ SEC542.6: Capture the Flag

DOURAN GROUP

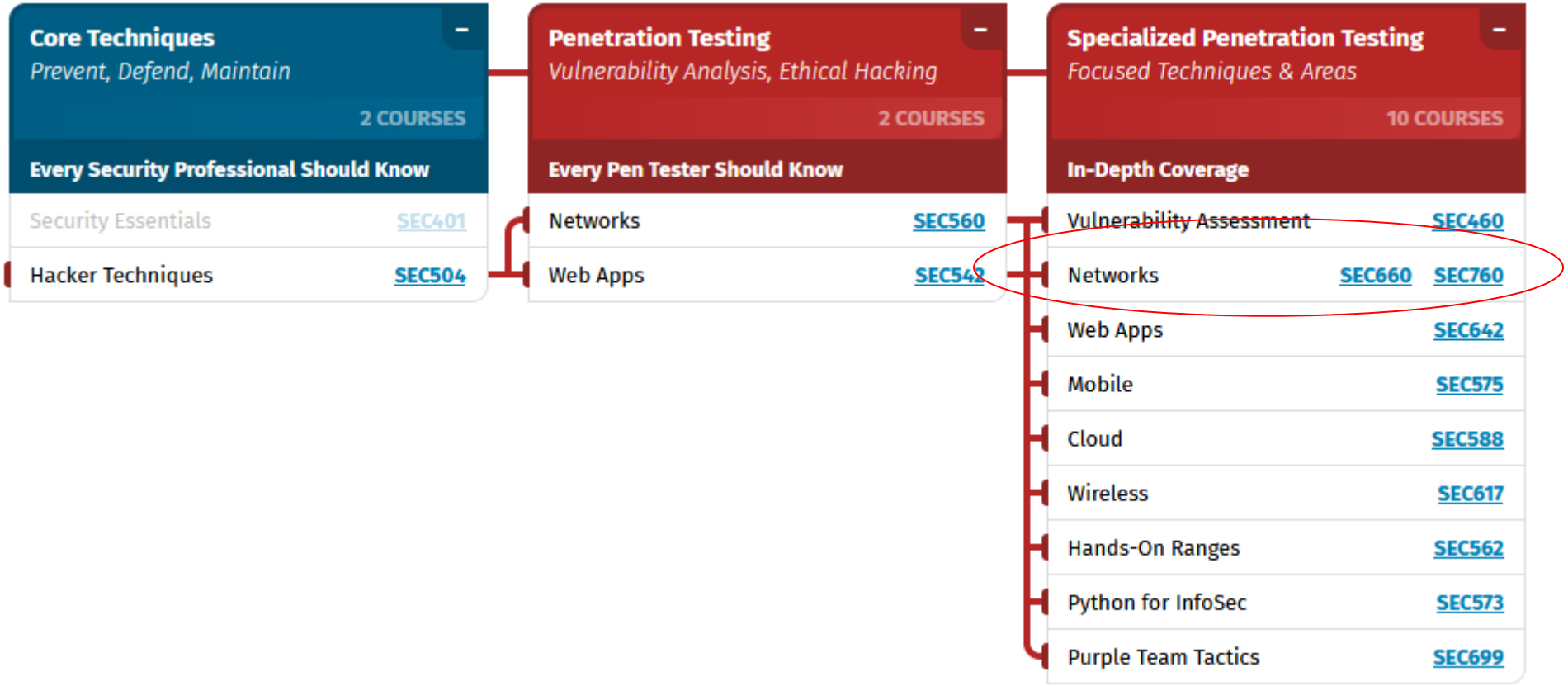
SANS Roadmap Penetration Testing



SEC460: Enterprise Threat and Vulnerability Assessment

+ SEC460.1: Methodology, Planning, and Threat Modeling
+ SEC460.2: Discovery
+ SEC460.3: Enhanced Vulnerability Scanning and Automation
+ SEC460.4: Vulnerability Validation, Triage, and Data Management
+ SEC460.5: Remediation and Reporting
+ SEC460.6: Vulnerability Assessment Foundry Hands-on Challenge

SANS Roadmap Penetration Testing



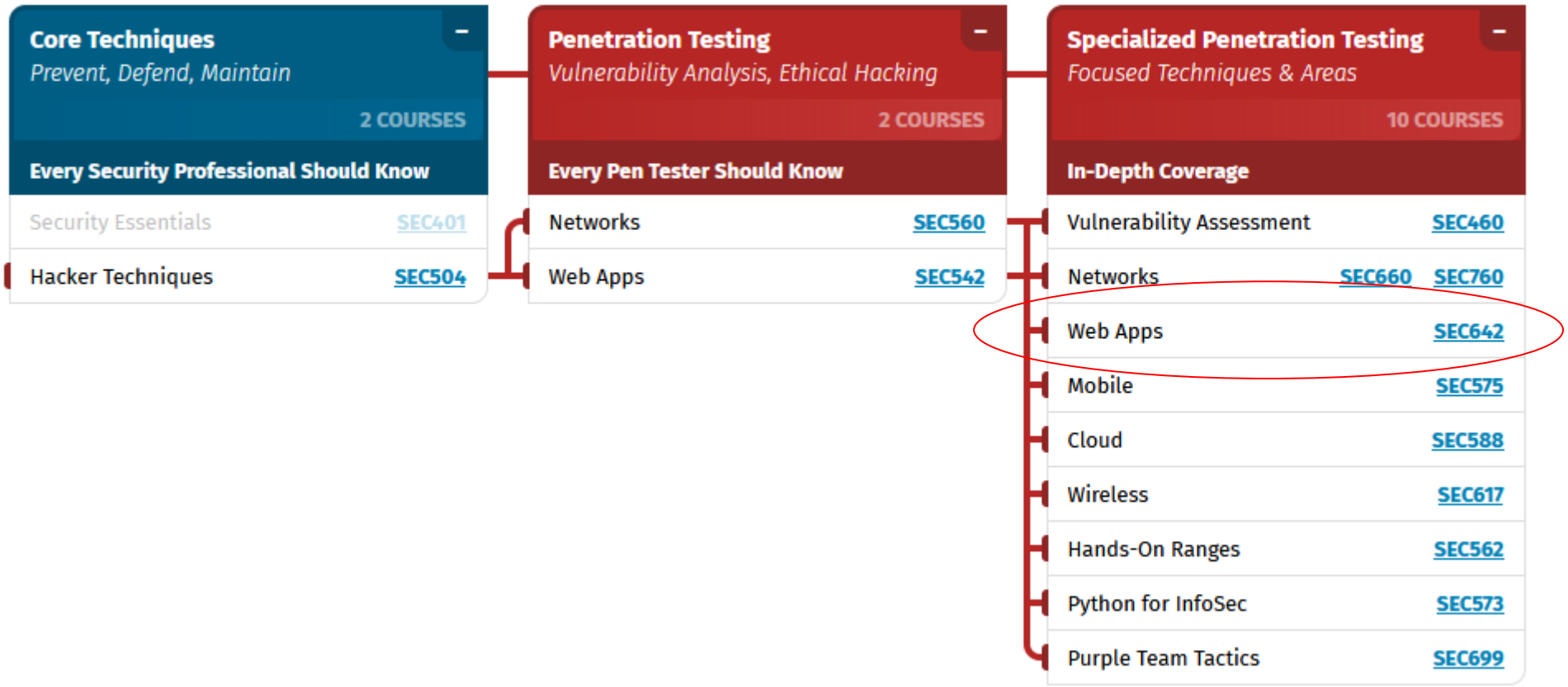
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

+ SEC660.1: Network Attacks for Penetration Testers
+ SEC660.2: Crypto and Post-Exploitation
+ SEC660.3: Python, Scapy, and Fuzzing
+ SEC660.4: Exploiting Linux for Penetration Testers
+ SEC660.5: Exploiting Windows for Penetration Testers
+ SEC660.6: Capture the Flag Challenge

SEC760: Advanced Exploit Development for Penetration Testers

+ SEC760.1: Exploit Mitigations and Reversing with IDA
+ SEC760.2: Advanced Linux Exploitation
+ SEC760.3: Patch Diffing, One-Day Exploits, and Return-Oriented Shellcode
+ SEC760.4: Windows Kernel Debugging and Exploitation
+ SEC760.5: Advanced Windows Exploitation
+ SEC760.6: Capture-the-Flag Challenge

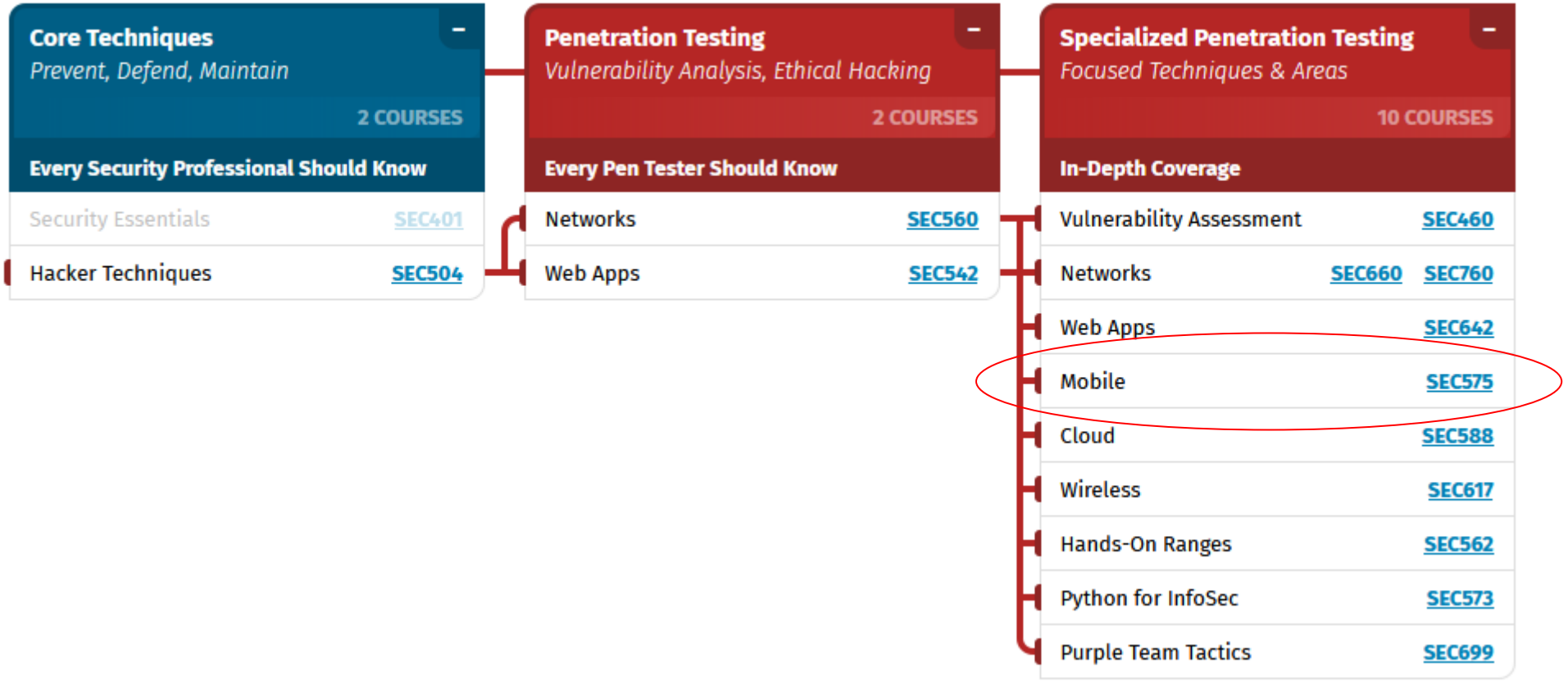
SANS Roadmap Penetration Testing



SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

+ SEC642.1: Advanced Attacks
+ SEC642.2: Web Frameworks
+ SEC642.3: Web Cryptography
+ SEC642.4: Alternative Web Interfaces
+ SEC642.5: Web Application Firewall and Filter Bypass
+ SEC642.6: Capture the Flag

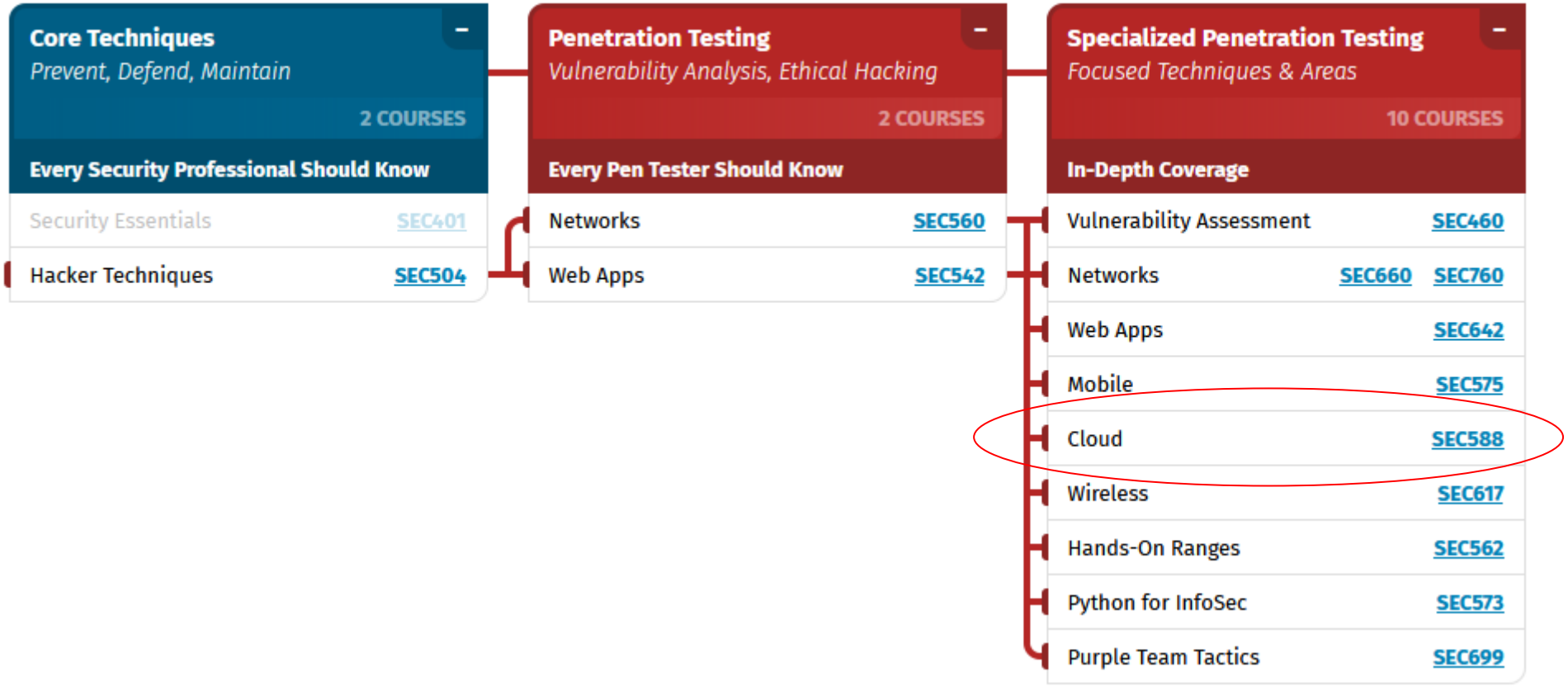
SANS Roadmap Penetration Testing



SEC575: Mobile Device Security and Ethical Hacking

+ SEC575.1: Device Architecture and Application Interaction
+ SEC575.2: The Stolen Device Threat and Mobile Malware
+ SEC575.3: Static Application Analysis
+ SEC575.4: Dynamic Mobile Application Analysis and Manipulation
+ SEC575.5: Mobile Penetration Testing
+ SEC575.6: Hands-on Capture-the-Flag Event

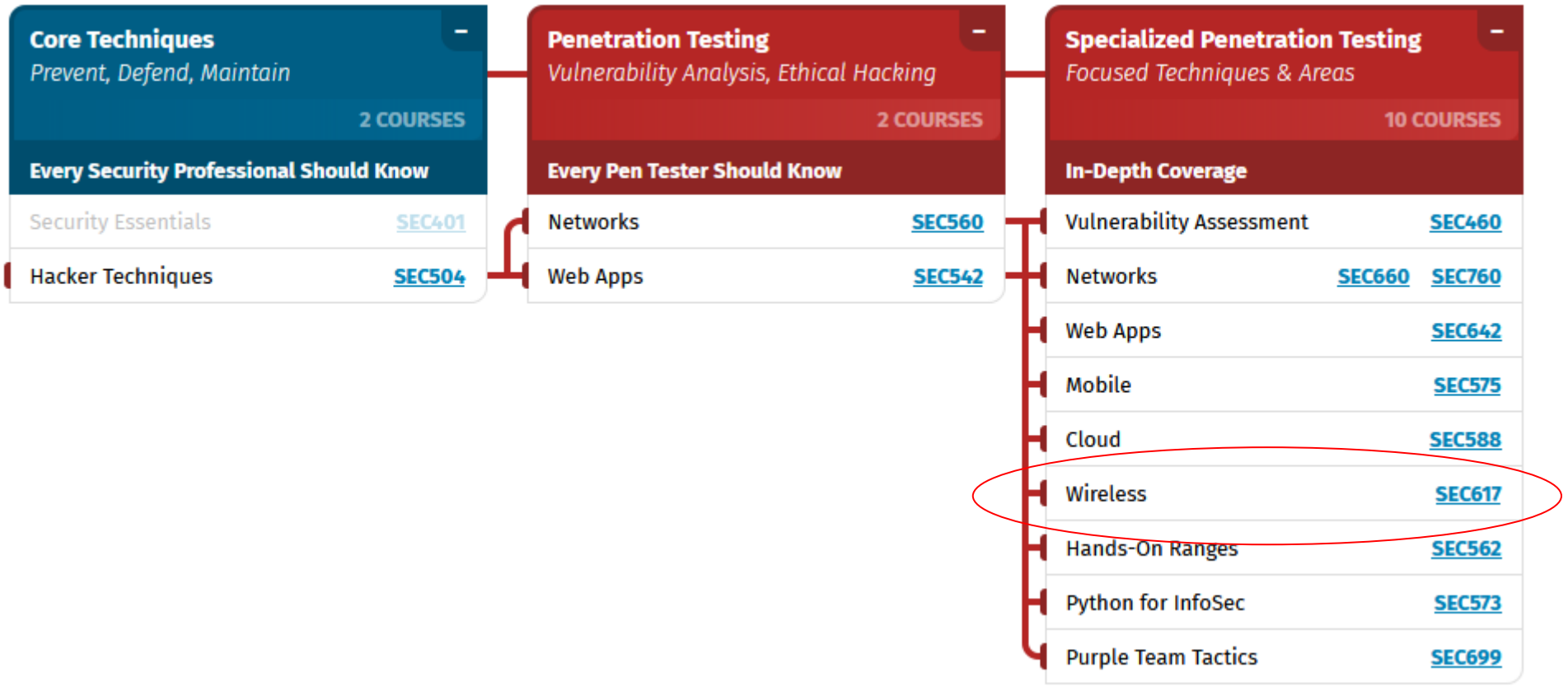
SANS Roadmap Penetration Testing



SEC588: Cloud Penetration Testing

+ SEC588.1: Discovery, Recon, and Architecture at Scale
+ SEC588.2: Mapping, Authentication, and Cloud Services
+ SEC588.3: Azure and Windows Services in the Cloud
+ SEC588.4: Vulnerabilities in Cloud Native Applications
+ SEC588.5: Exploitation and Red Team in the Cloud
+ SEC588.6: Capstone

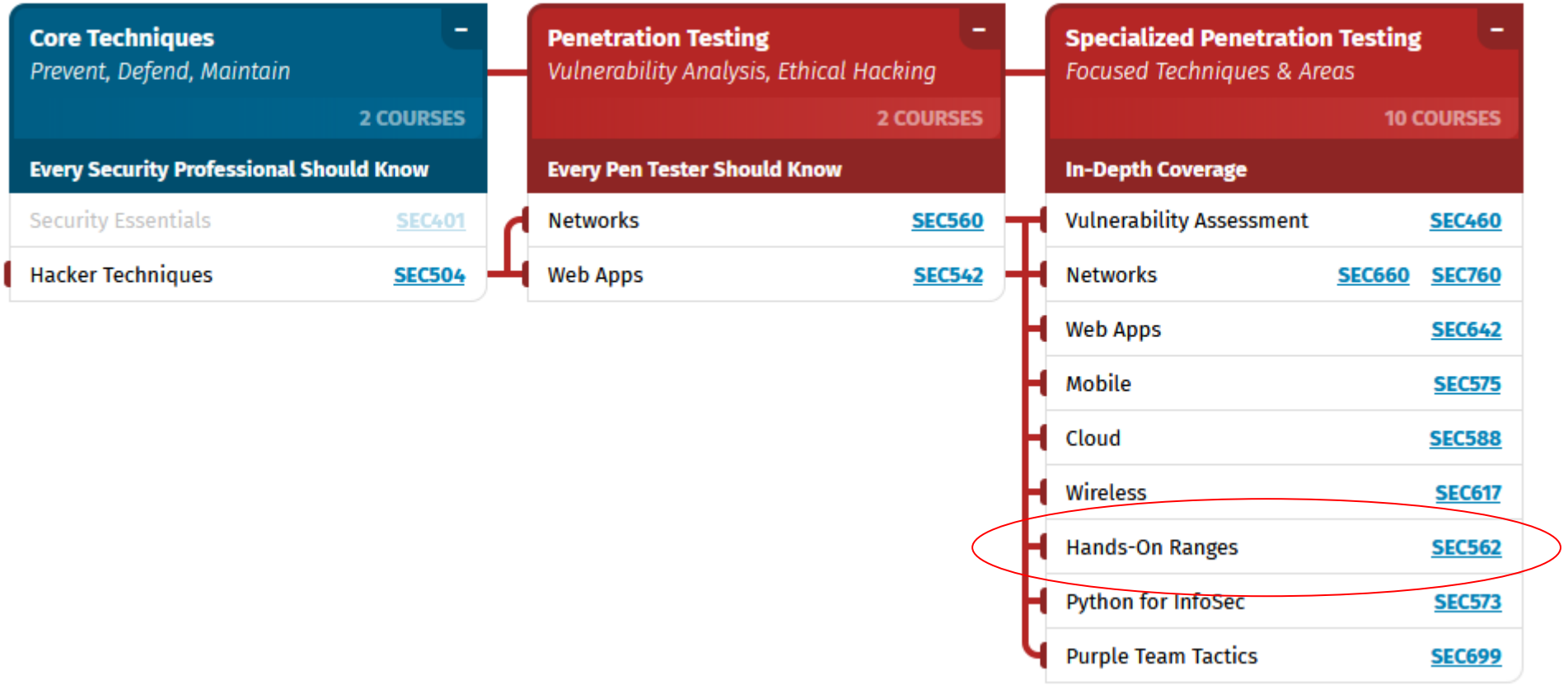
SANS Roadmap Penetration Testing



SEC617: Wireless Penetration Testing and Ethical Hacking

+ SEC617.1: Wi-Fi Data Collection and Analysis
+ SEC617.2: Wi-Fi Attack and Exploitation Techniques
+ SEC617.3: Enterprise Wi-Fi, DECT, and Zigbee Attacks
+ SEC617.4: Bluetooth and Software Defined Radio Attacks
+ SEC617.5: RFID, Smart Cards, and NFC Hacking
+ SEC617.6: Hands-on Capture-the-Flag Event

SANS Roadmap Penetration Testing



SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise

+ SEC562.1: Team Building, Visualizing the Battlespace, Recon, and HMIs

+ SEC562.2: Protocol Manipulation, Data Integrity, and Operator Interface Terminals

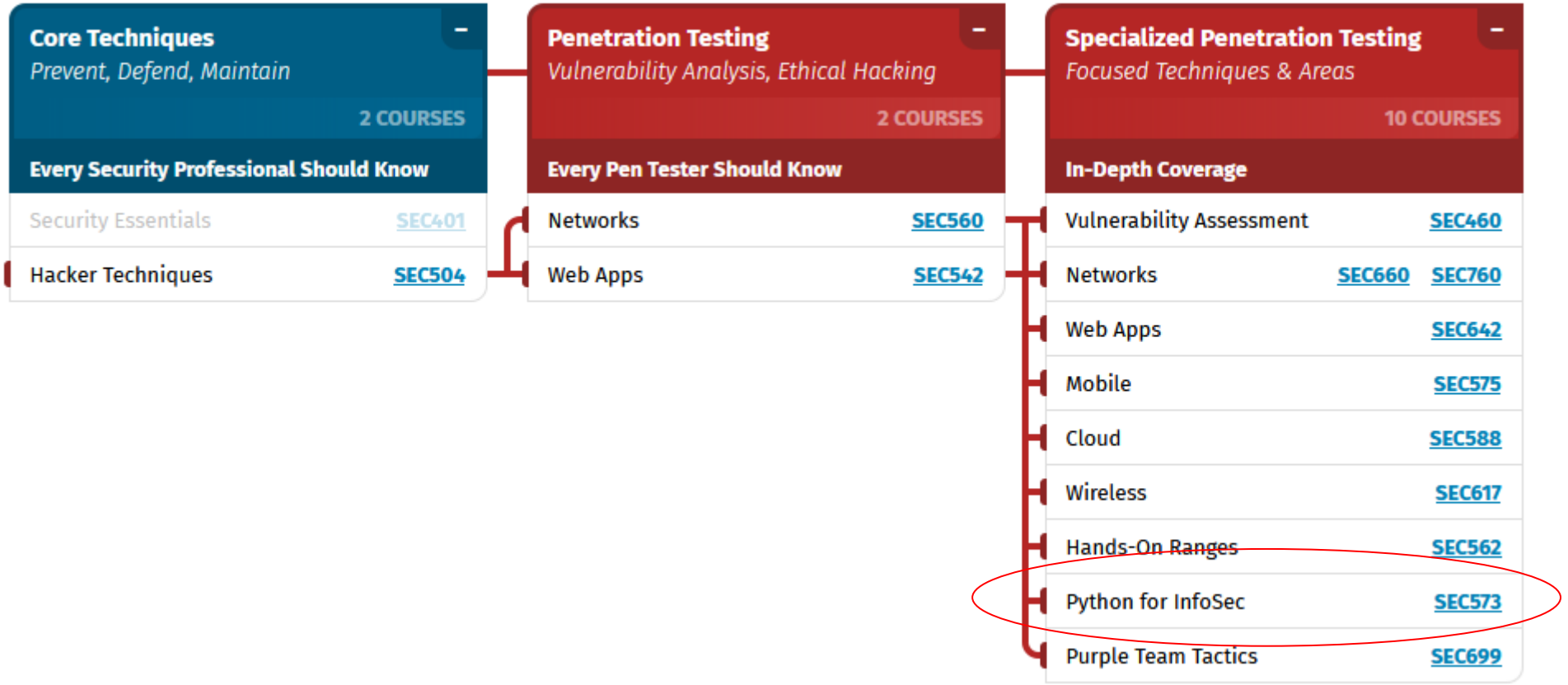
+ SEC562.3: Malware Analysis, Privilege Escalation, Incident Response, Passwords Guessing, and Networking Equipment

+ SEC562.4: Cryptography and ICS Protocols

+ SEC562.5: Power Grid, Weapons Systems, and Network Manipulation

+ SEC562.6: Force-On-Force Attack and Defend

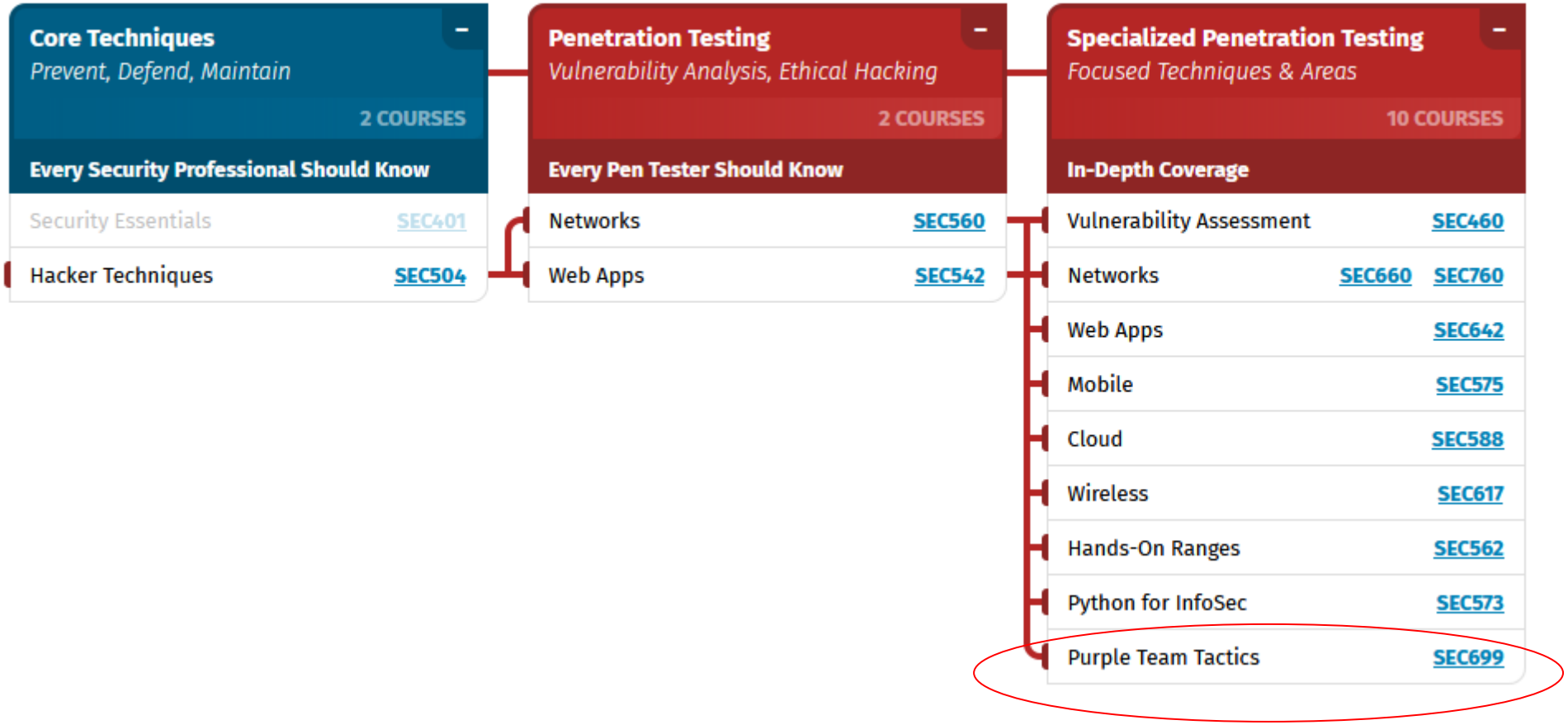
SANS Roadmap Penetration Testing



SEC573: Automating Information Security with Python

+ SEC573.1: Essentials Workshop with pyWars
+ SEC573.2: Essentials Workshop with MORE pyWars
+ SEC573.3: Defensive Python
+ SEC573.4: Forensics Python
+ SEC573.5: Offensive Python
+ SEC573.6: Capture-the-Flag Challenge

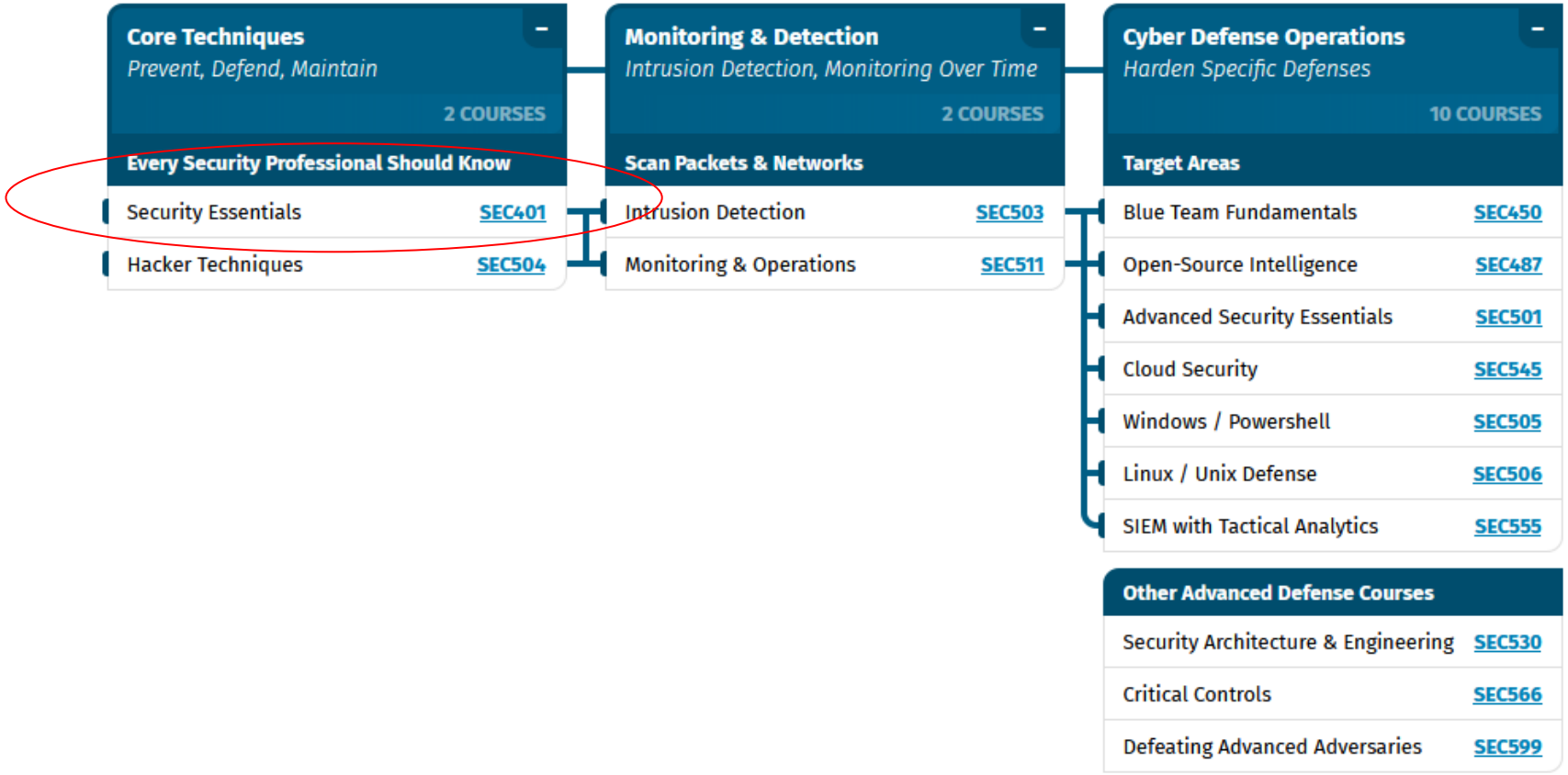
SANS Roadmap Penetration Testing



SEC699: Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection

+ SEC699.1: Adversary Emulation for Breach Prevention & Detection
+ SEC699.2: Advanced Initial Execution Techniques - Threat Actor APT-28
+ SEC699.3: Advanced Active Directory Attacks - Threat Actor APT-34
+ SEC699.4: Stealth Persistence Strategies & Turla
+ SEC699.5: Azure AD Attacks
+ SEC699.6: Adversary Emulation Capstone

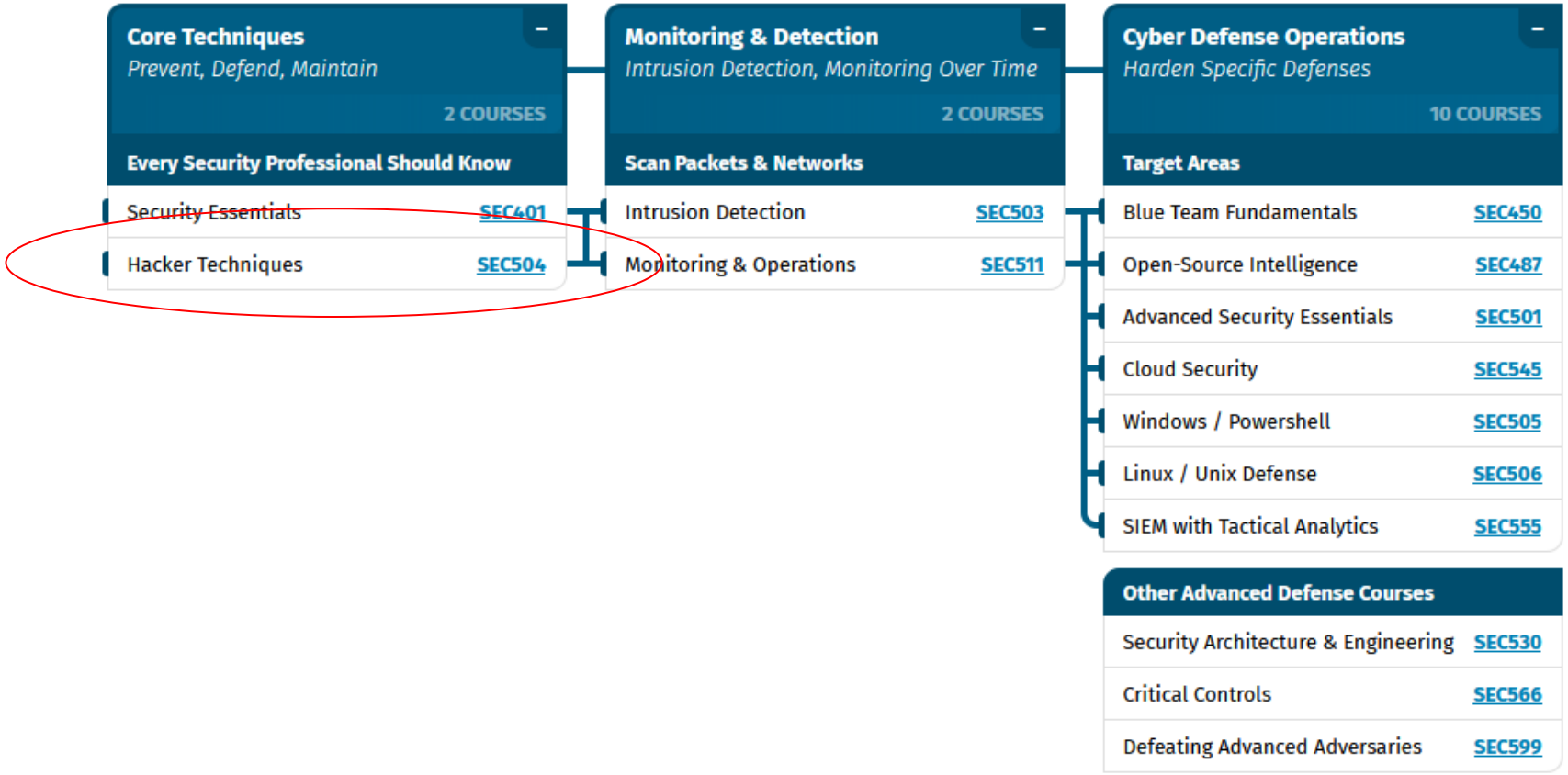
Cyber Defense Operations Roadmap



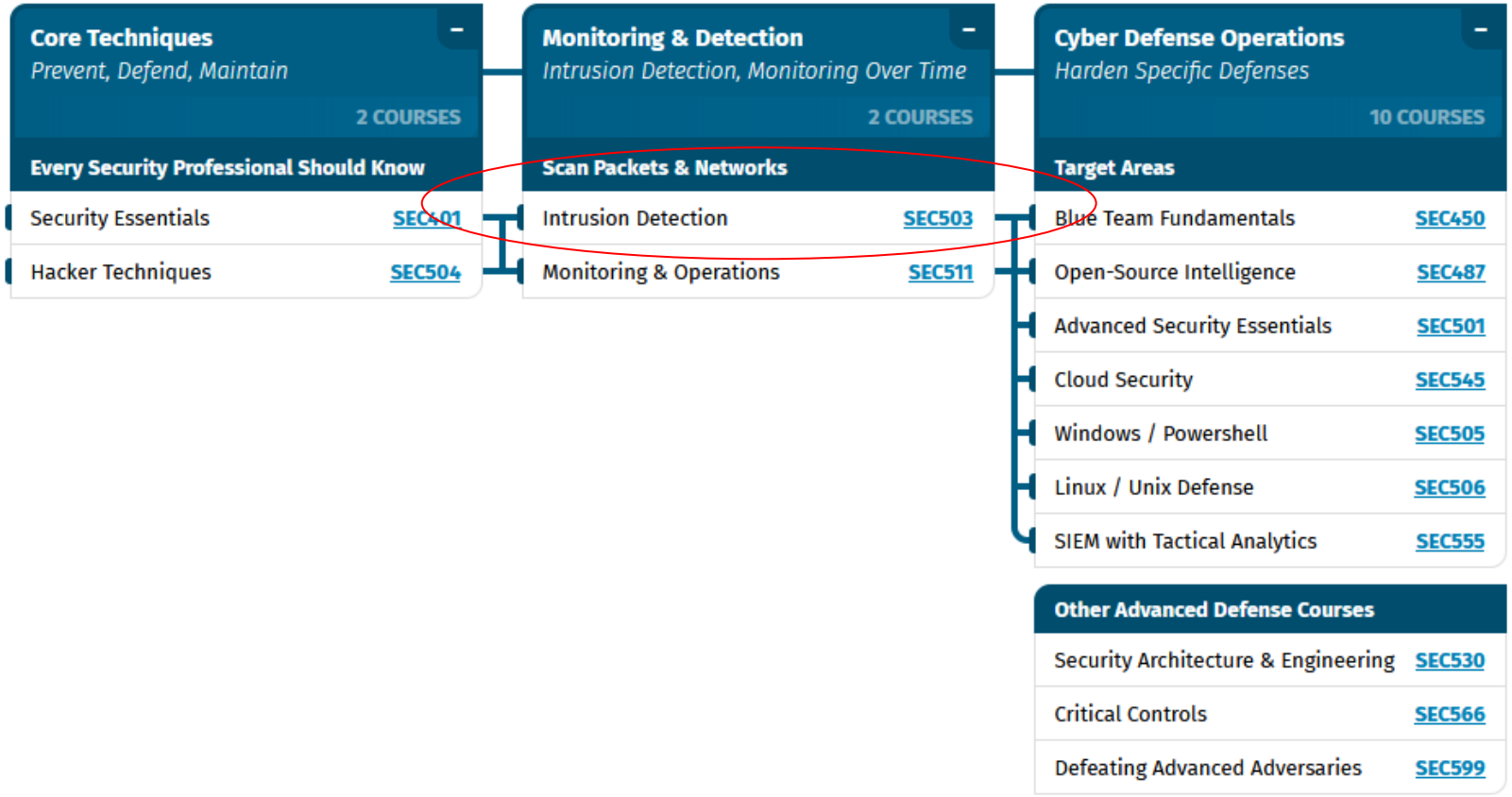
SEC401: Security Essentials Bootcamp Style

+ SEC401.1: Network Security Essentials
+ SEC401.2: Defense-in-Depth and Attacks
+ SEC401.3: Threat Management
+ SEC401.4: Cryptography, Incident Response, and Risk Management
+ SEC401.5: Windows Security
+ SEC401.6: Linux Security

Cyber Defense Operations Roadmap



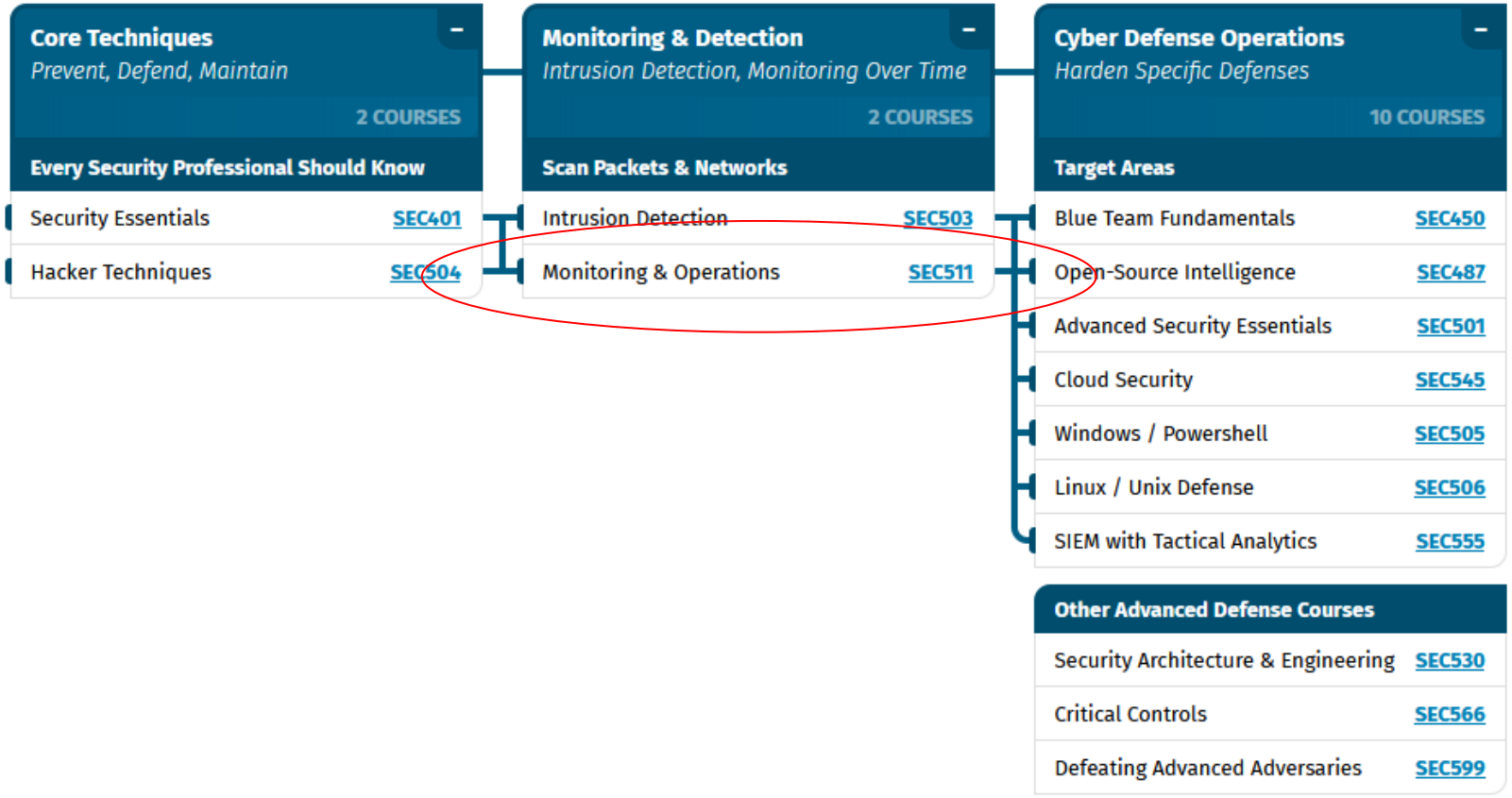
Cyber Defense Operations Roadmap



SEC503: Intrusion Detection In-Depth

+ SEC503.1: Fundamentals of Traffic Analysis: Part I
+ SEC503.2: Fundamentals of Traffic Analysis: Part II
+ SEC503.3: Signature Based Detection
+ SEC503.4: Anomalies and Behaviors
+ SEC503.5: Modern and Future Monitoring: Forensics, Analytics, and Machine Learning
+ SEC503.6: IDS Capstone Challenge

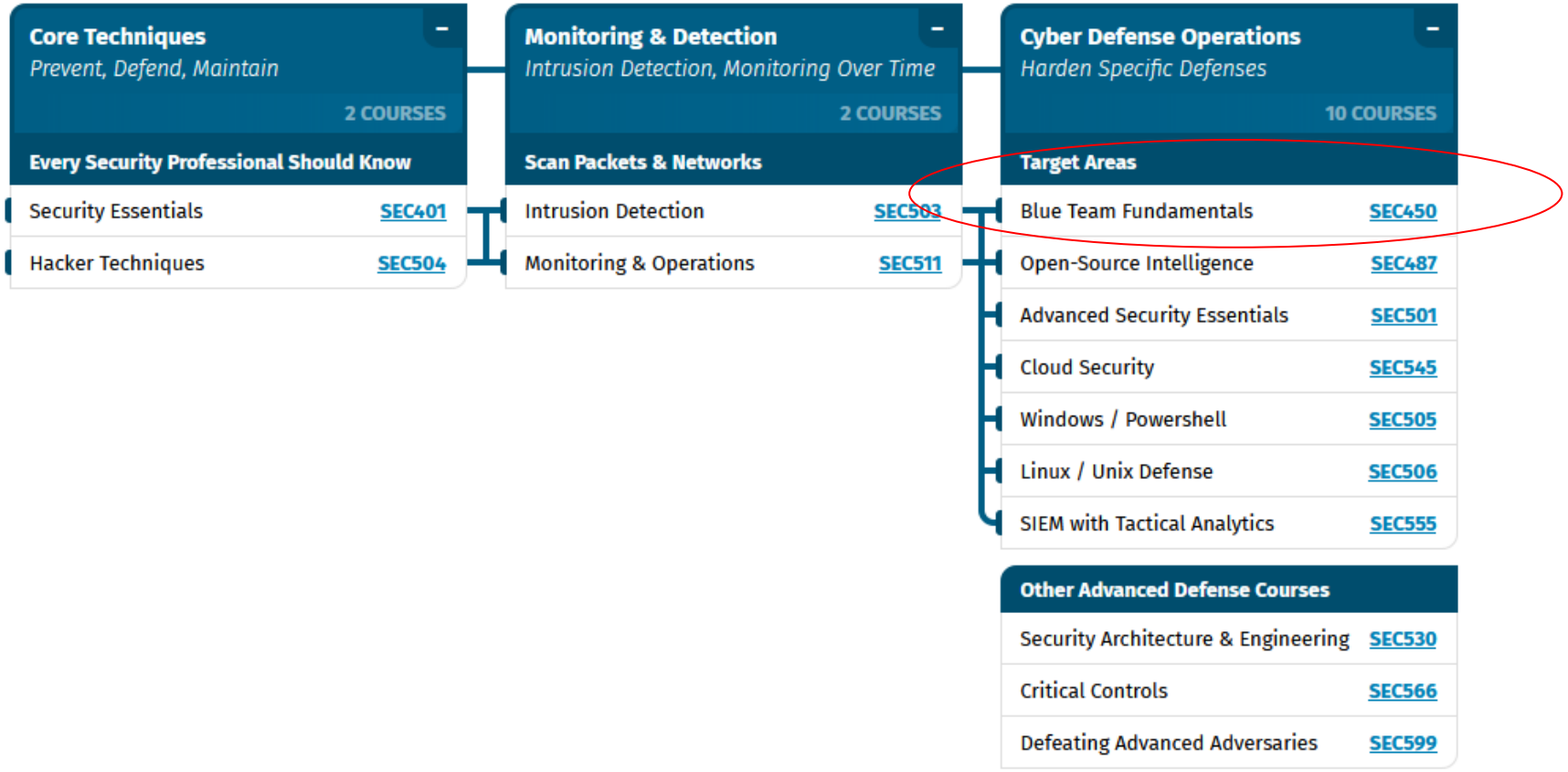
Cyber Defense Operations Roadmap



SEC511: Continuous Monitoring and Security Operations

+ SEC511.1: Current State Assessment, Security Operations Centers, and Security Architecture
+ SEC511.2: Network Security Architecture
+ SEC511.3: Network Security Monitoring
+ SEC511.4: Endpoint Security Architecture
+ SEC511.5: Automation and Continuous Security Monitoring
+ SEC511.6: Capstone: Design, Detect, Defend

Cyber Defense Operations Roadmap



SEC450: Blue Team Fundamentals: Security Operations and Analysis

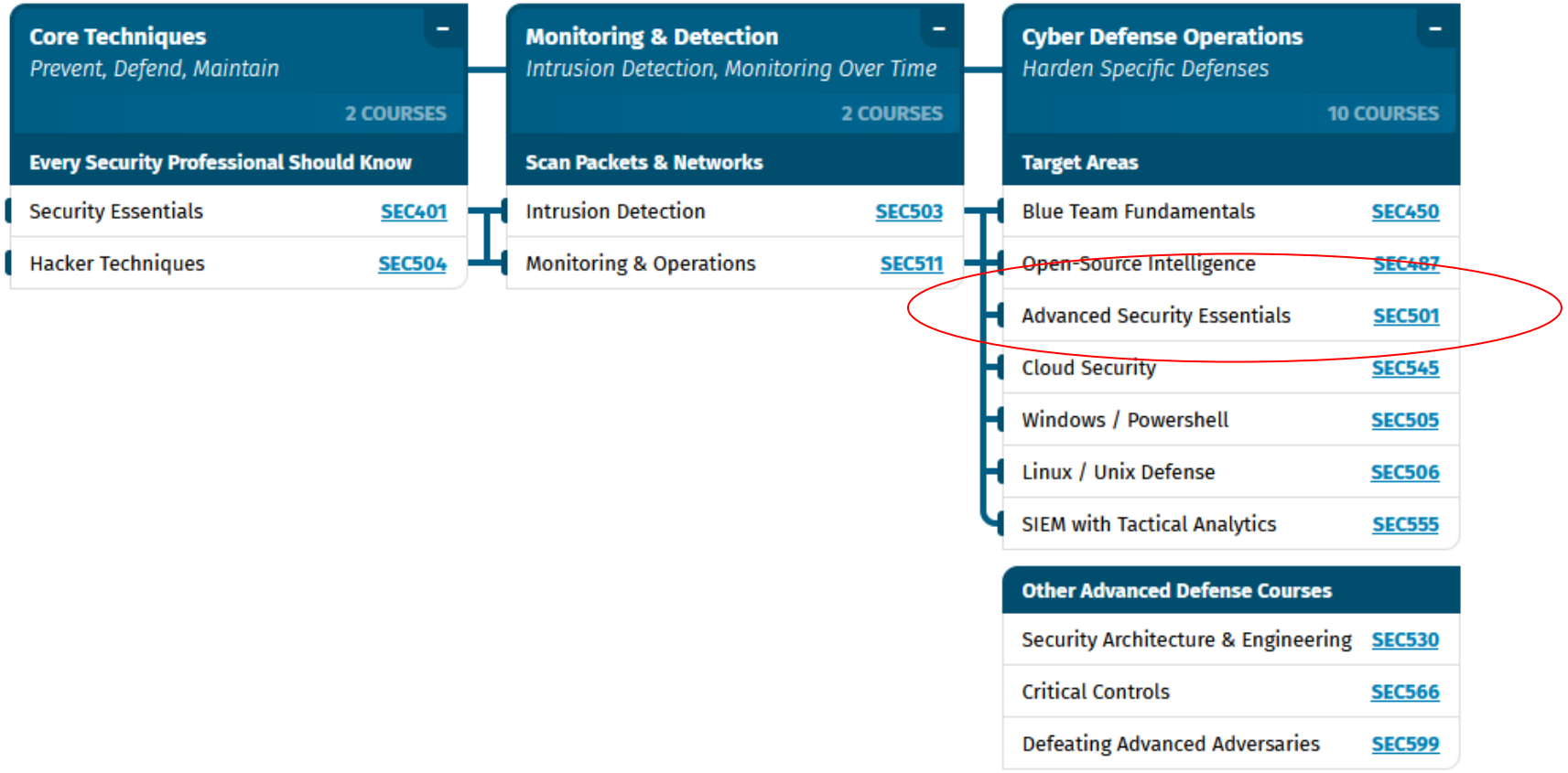
+ SEC450.1: Blue Team Tools and Operations
+ SEC450.2: Understanding Your Network
+ SEC450.3: Understanding Endpoints, Logs, and Files
+ SEC450.4: Triage and Analysis
+ SEC450.5: Continuous Improvement, Analytics, and Automation
+ SEC450.6: Capstone: Defend the Flag

Cyber Defense Operations Roadmap

SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis

+ SEC487.1: Foundations of OSINT
+ SEC487.2: Gathering, Searching, and Analyzing OSINT
+ SEC487.3: Social Media, Geolocation, and Imagery
+ SEC487.4: Networks, Government, and Business
+ SEC487.5: The Dark Web, Breach Data, and International Issues
+ SEC487.6: Capstone: Capture (and Present) the Flag

Cyber Defense Operations Roadmap



SEC501: Advanced Security Essentials - Enterprise Defender

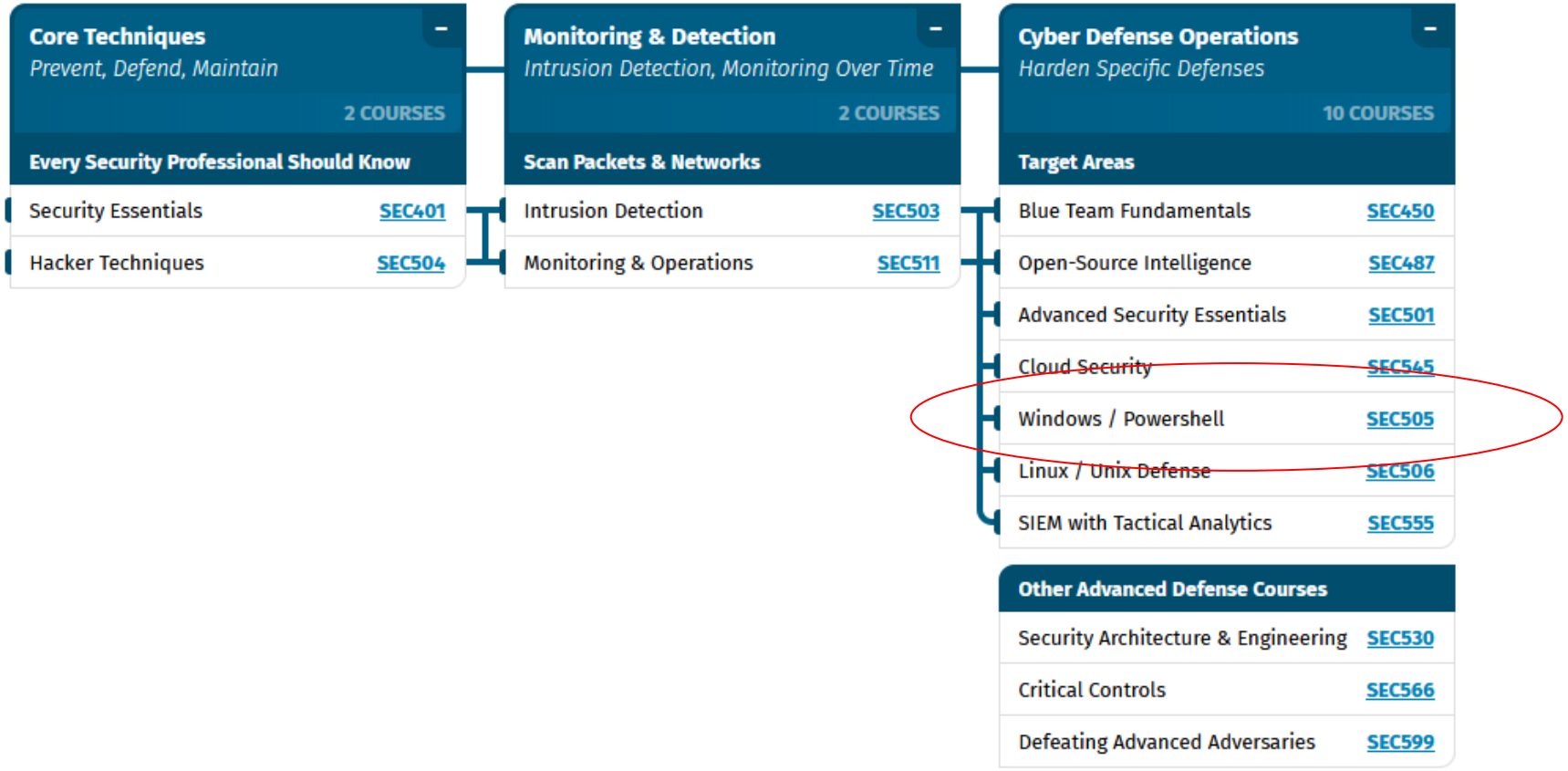
+ SEC501.1: Defensible Network Architecture
+ SEC501.2: Penetration Testing
+ SEC501.3: Security Operations Foundations
+ SEC501.4: Digital Forensics and Incident Response
+ SEC501.5: Malware Analysis
+ SEC501.6: Enterprise Defender Capstone

Cyber Defense Operations Roadmap

SEC545: Cloud Security Architecture and Operations

+ SEC545.1: Cloud Security Foundations
+ SEC545.2: Core Security Controls for Cloud Computing
+ SEC545.3: Cloud Security Architecture and Design
+ SEC545.4: Cloud Security - Offense and Defense
+ SEC545.5: Cloud Security Automation and Orchestration

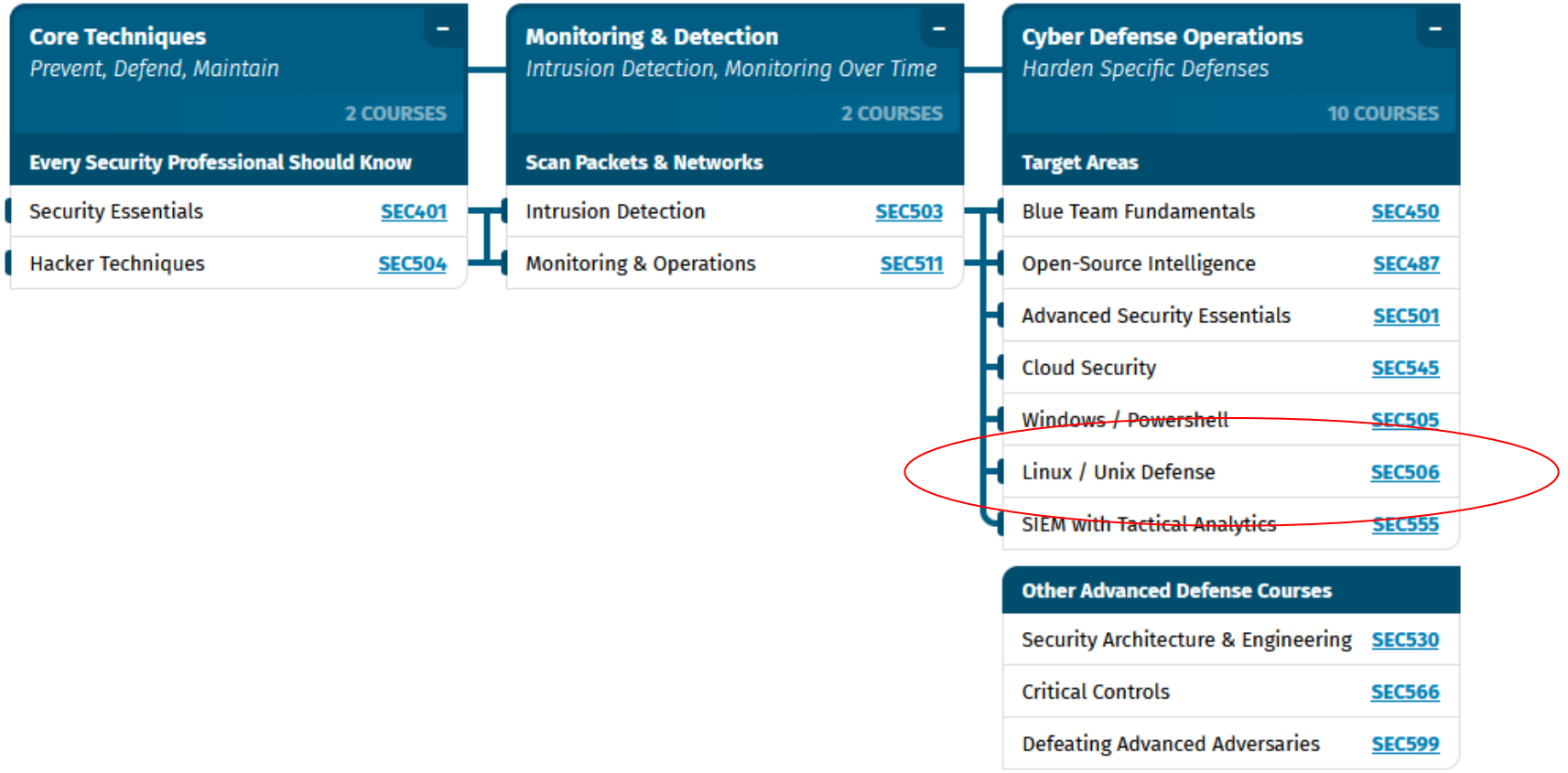
Cyber Defense Operations Roadmap



SEC505: Securing Windows and PowerShell Automation

+ SEC505.1: Learn PowerShell Scripting for Security
+ SEC505.2: You Don't Know the POWER!
+ SEC505.3: WMI and Active Directory Scripting
+ SEC505.4: Hardening Network Services with PowerShell
+ SEC505.5: Certificates and Multifactor Authentication
+ SEC505.6: PowerShell Security, Ransomware, and DevOps

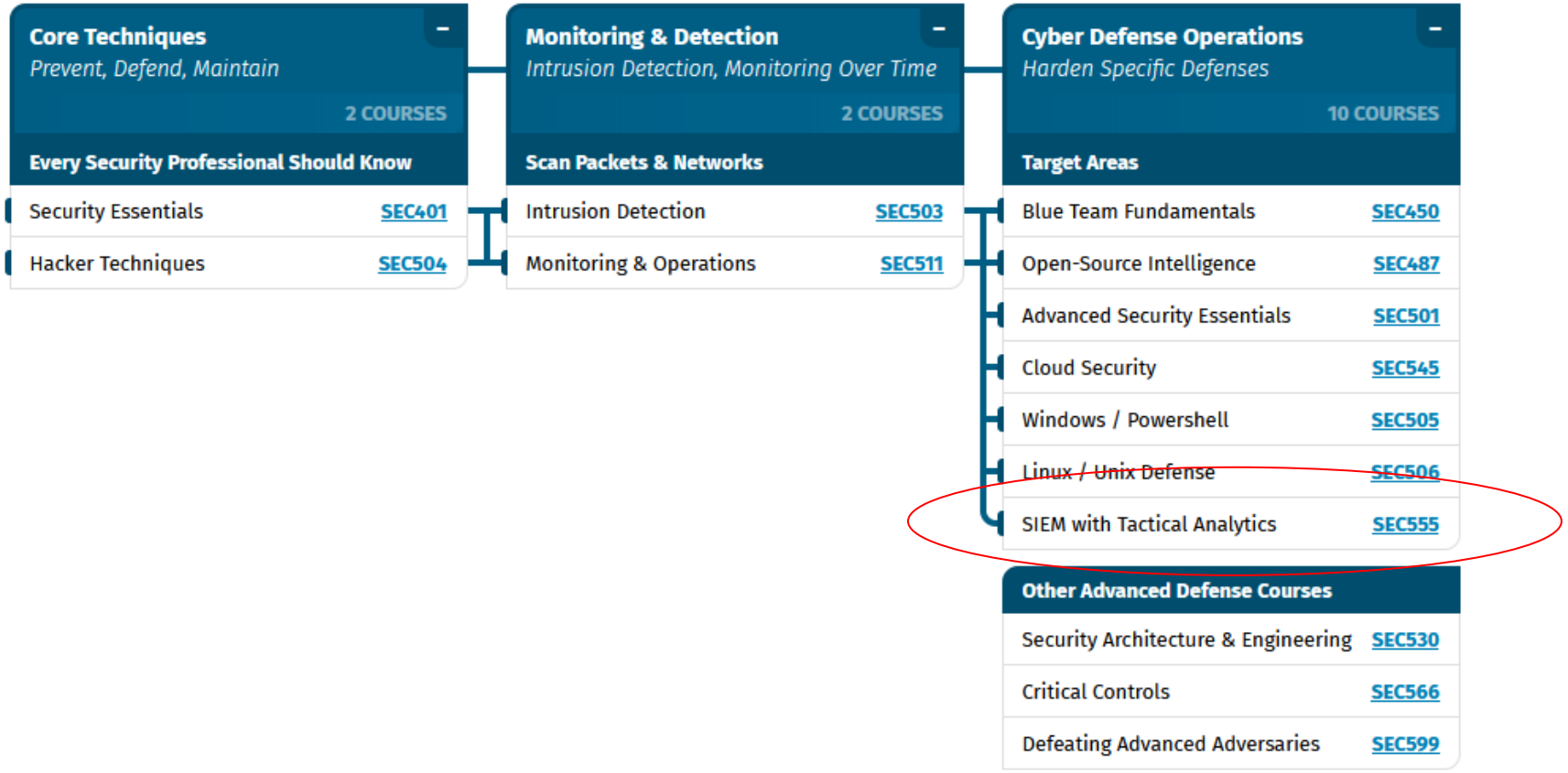
Cyber Defense Operations Roadmap



SEC506: Securing Linux/Unix

+ SEC506.1: Hardening Linux/Unix Systems, Part 1
+ SEC506.2: Hardening Linux/Unix Systems, Part 2
+ SEC506.3: Hardening Linux/Unix Systems, Part 3
+ SEC506.4: Linux Application Security, Part 1
+ SEC506.5: Linux Application Security, Part 2
+ SEC506.6: Digital Forensics for Linux/Unix

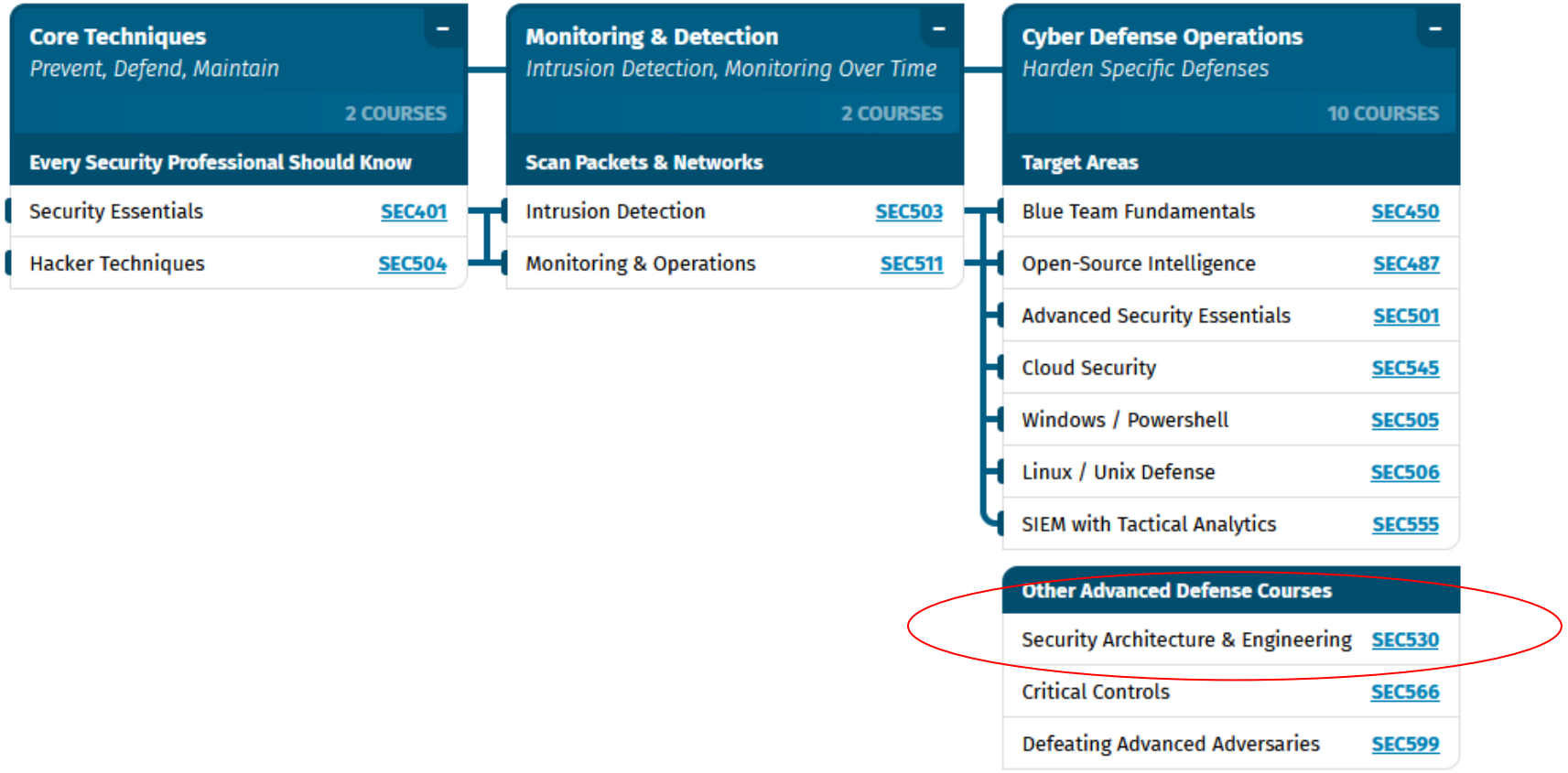
Cyber Defense Operations Roadmap



SEC555: SIEM with Tactical Analytics

+ SEC555.1: SIEM Architecture
+ SEC555.2: Service Profiling with SIEM
+ SEC555.3: Advanced Endpoint Analytics
+ SEC555.4: Baselining and User Behavior Monitoring
+ SEC555.5: Tactical SIEM Detection and Post-Mortem Analysis
+ SEC555.6: Capstone: Design, Detect, Defend

Cyber Defense Operations Roadmap



SEC530: Defensible Security Architecture and Engineering

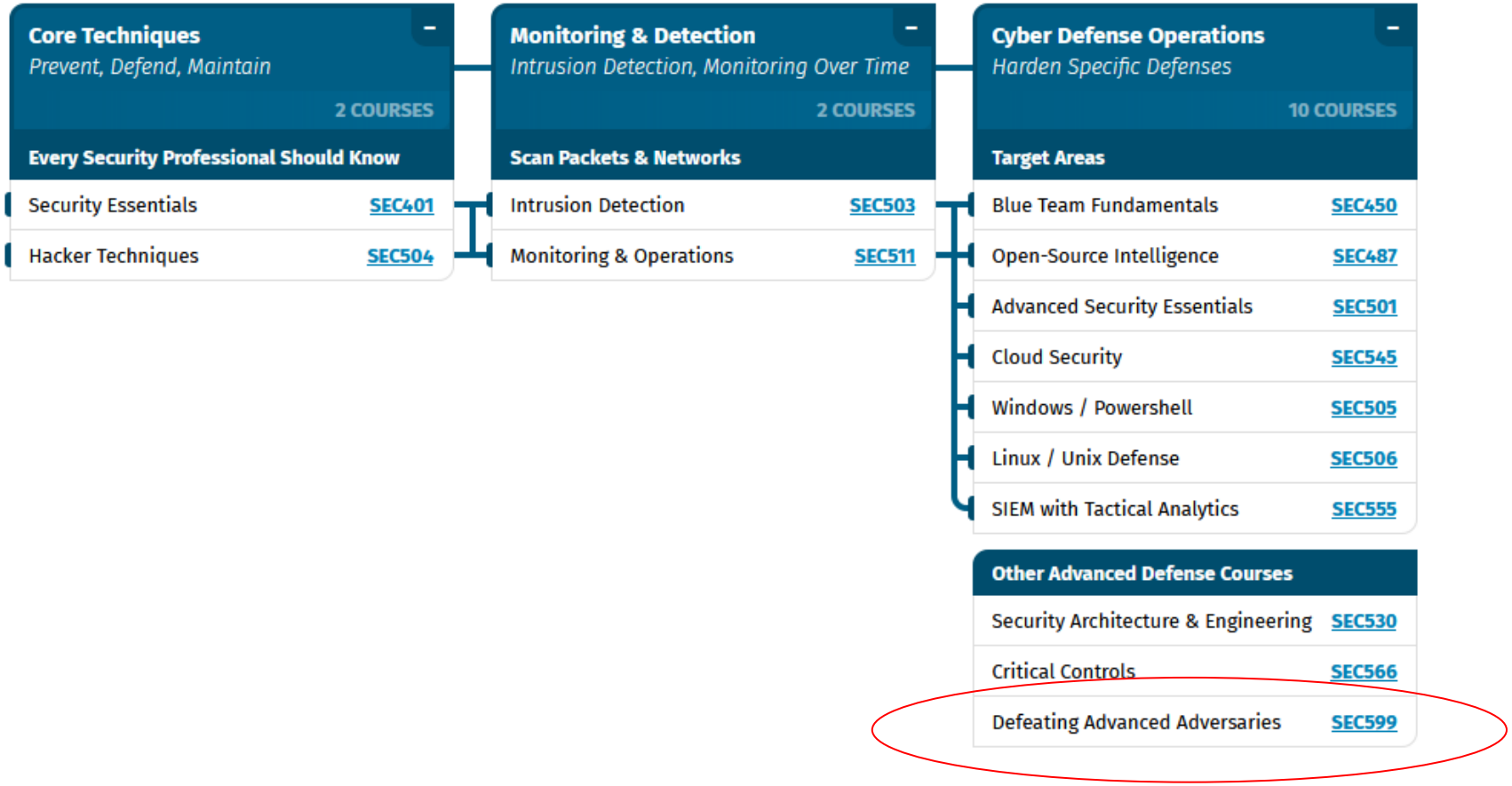
+ SEC530.1: Defensible Security Architecture and Engineering
+ SEC530.2: Network Security Architecture and Engineering
+ SEC530.3: Network-Centric Security
+ SEC530.4: Data-Centric Security
+ SEC530.5: Zero-Trust Architecture: Addressing the Adversaries Already in Our Networks
+ SEC530.6: Hands-On Secure-the-Flag Challenge

Cyber Defense Operations Roadmap

SEC566: Implementing and Auditing the Critical Security Controls - In-Depth

+ SEC566.1: Introduction and Overview of the 20 Critical Controls
+ SEC566.2: Critical Controls 3, 4, 5 and 6
+ SEC566.3: Critical Controls 7, 8, 9, 10 and 11
+ SEC566.4: Critical Controls 12, 13, 14 and 15
+ SEC566.5: Critical Controls 16, 17, 18, 19 and 20

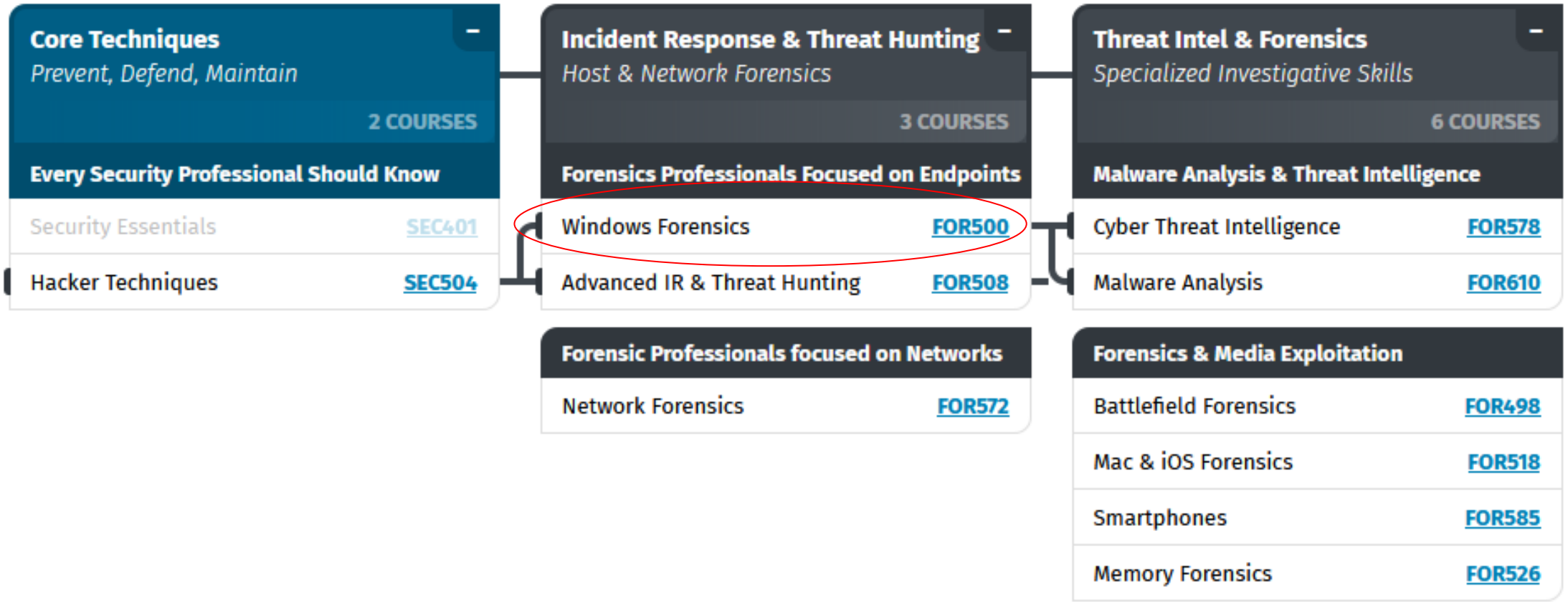
Cyber Defense Operations Roadmap



SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses

+ SEC599.1: Introduction and Reconnaissance
+ SEC599.2: Payload Delivery and Execution
+ SEC599.3: Exploitation, Persistence, and Command and Control
+ SEC599.4: Lateral Movement
+ SEC599.5: Action on Objectives, Threat Hunting, and Incident Response
+ SEC599.6: APT Defender Capstone

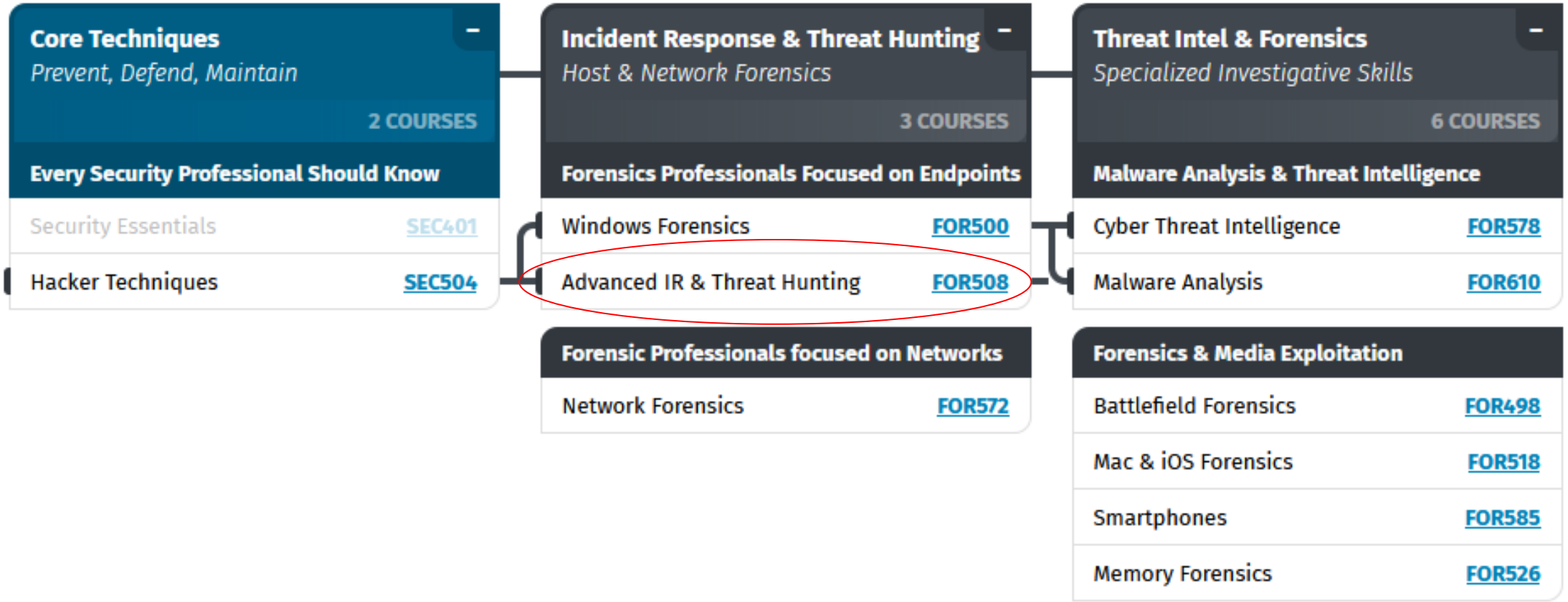
SANS Forensics Roadmap



FOR500: Windows Forensic Analysis

+ FOR500.1: Windows Digital Forensics and Advanced Data Triage
+ FOR500.2: Core Windows Forensics Part 1: Windows Registry Forensics and Analysis
+ FOR500.3: Core Windows Forensics Part II: USB Devices and Shell Items
+ FOR500.4: Core Windows Forensics Part III: Email, Key Additional Artifacts, and Event Logs
+ FOR500.5: Core Windows Forensics Part IV: Web Browser Forensics for Firefox, Internet Explorer and Chrome
+ FOR500.6: Windows Forensics Challenge

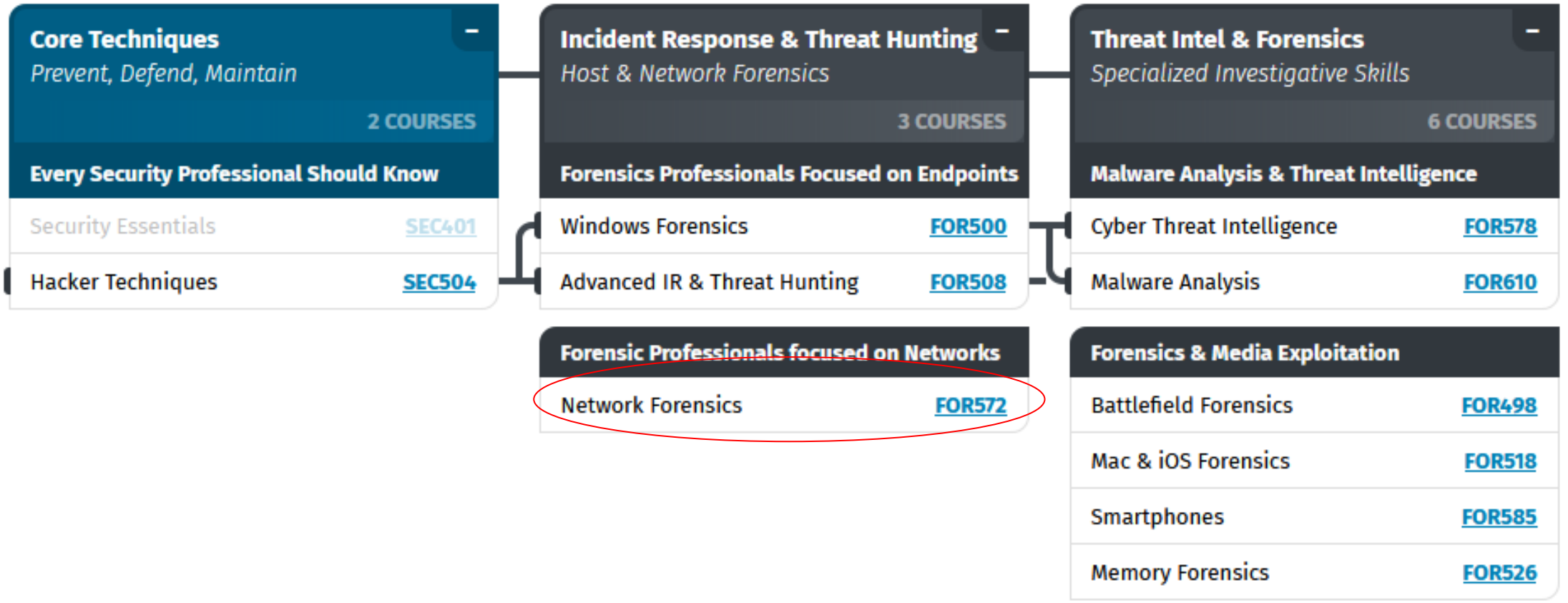
SANS Forensics Roadmap



FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

+ FOR508.1: Advanced Incident Response & Threat Hunting
+ FOR508.2: Intrusion Analysis
+ FOR508.3: Memory Forensics in Incident Response & Threat Hunting
+ FOR508.4: Timeline Analysis
+ FOR508.5: Incident Response & Hunting Across the Enterprise | Advanced Adversary & Anti-Forensics Detection
+ FOR508.6: The APT Threat Group Incident Response Challenge

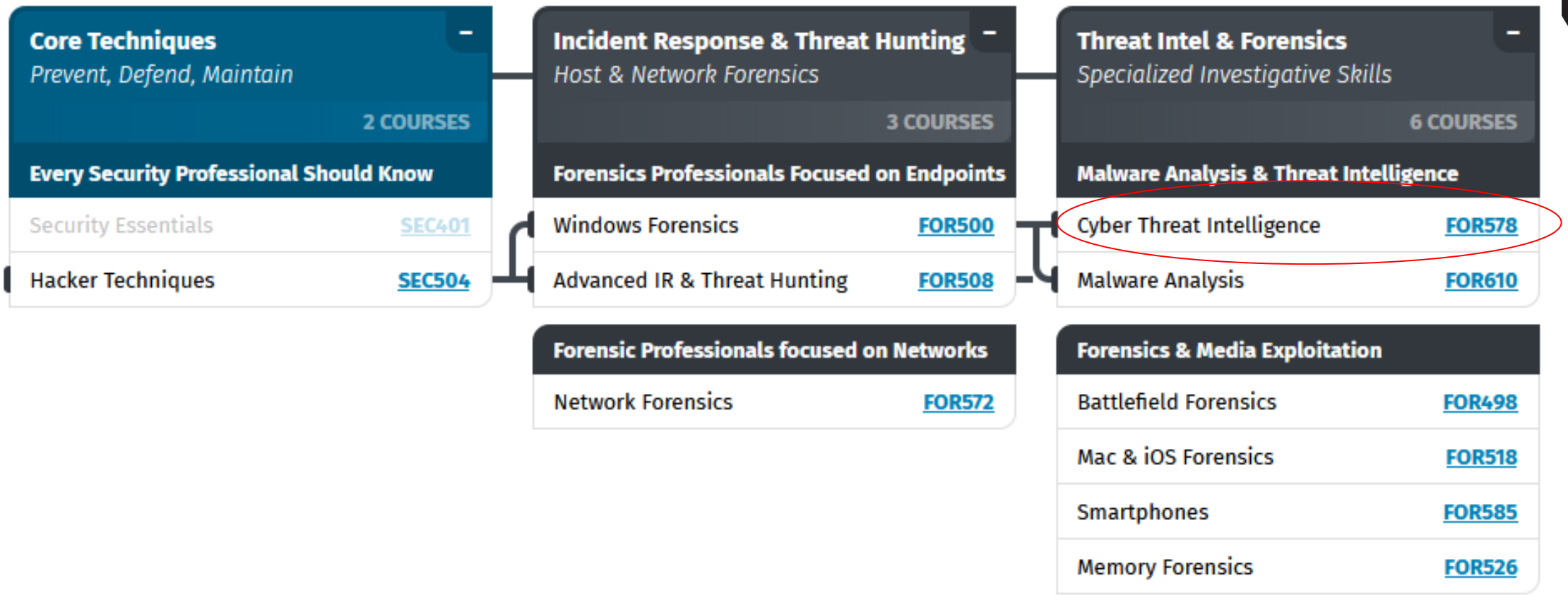
SANS Forensics Roadmap



FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

+ FOR572.1: Off the Disk and Onto the Wire
+ FOR572.2: Core Protocols & Log Aggregation/Analysis
+ FOR572.3: NetFlow and File Access Protocols
+ FOR572.4: Commercial Tools, Wireless, and Full-Packet Hunting
+ FOR572.5: Encryption, Protocol Reversing, OPSEC, and Intel
+ FOR572.6: Network Forensics Capstone Challenge

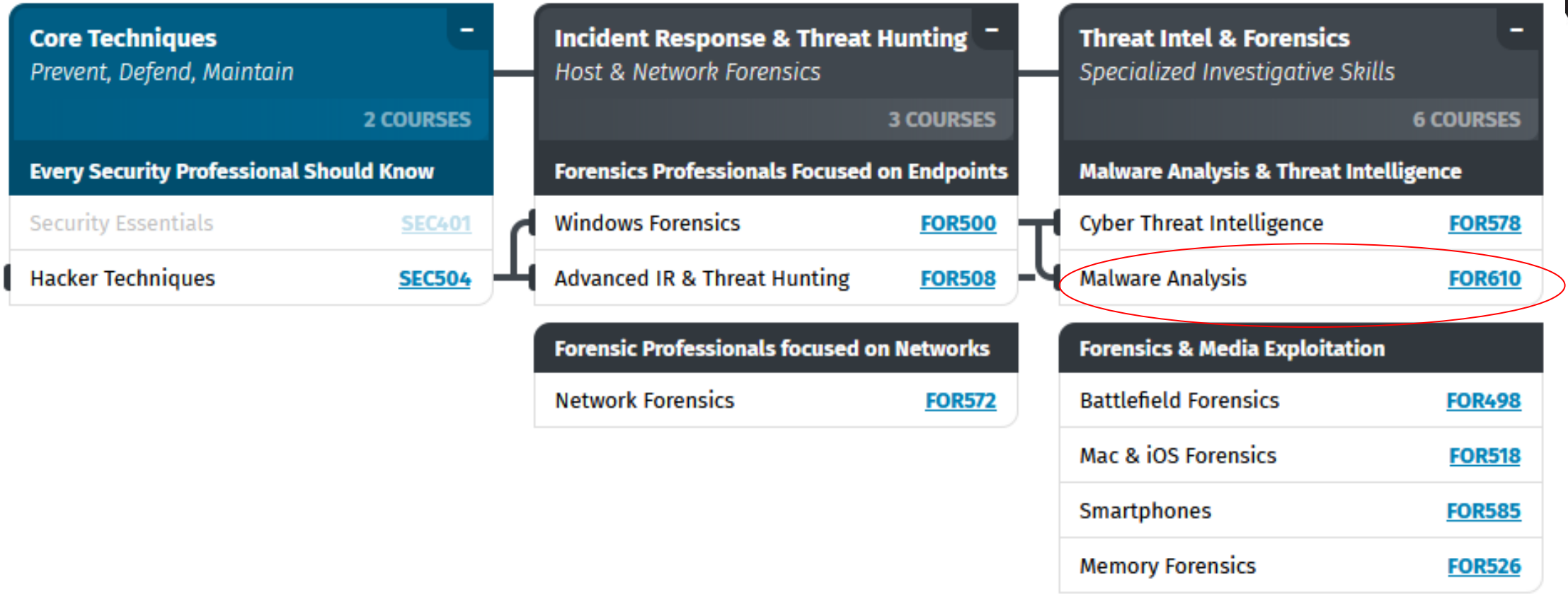
SANS Forensics Roadmap



FOR578: Cyber Threat Intelligence

+ FOR578.1: Cyber Threat Intelligence and Requirements
+ FOR578.2: The Fundamental Skillset: Intrusion Analysis
+ FOR578.3: Collection Sources
+ FOR578.4: Analysis and Dissemination of Intelligence
+ FOR578.5: Higher-Order Analysis and Attribution

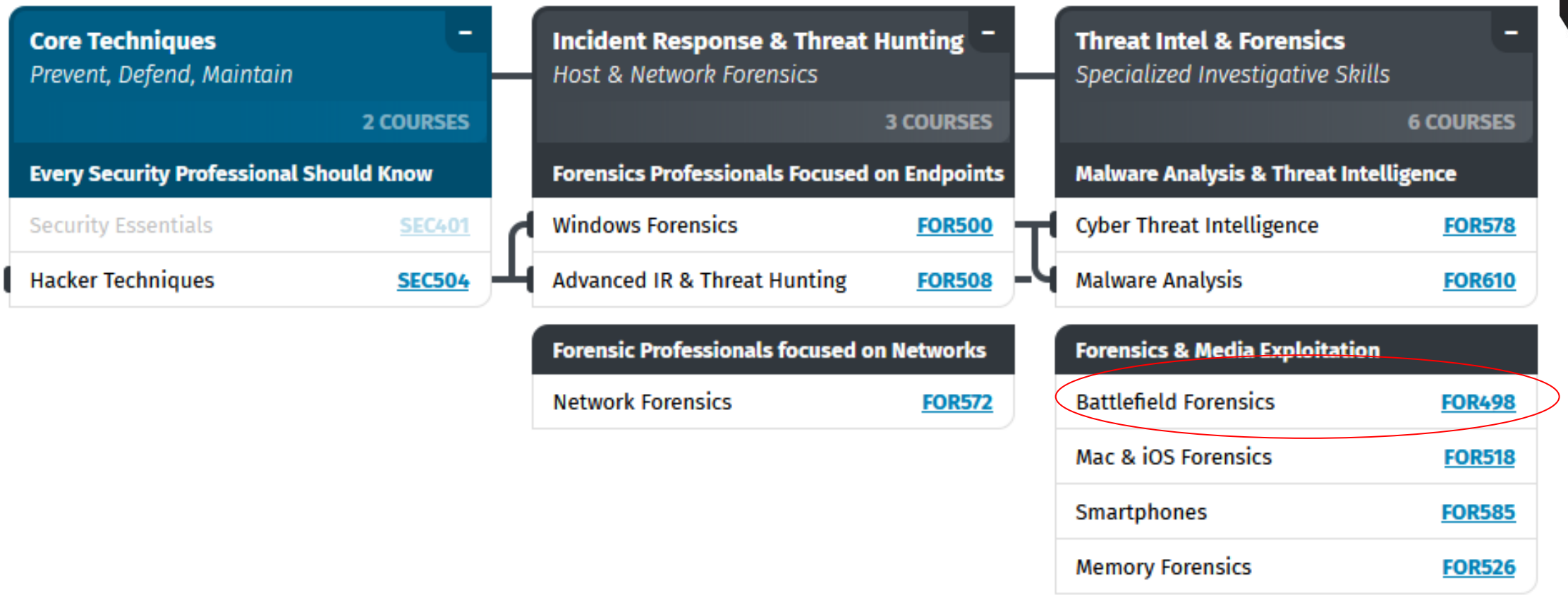
SANS Forensics Roadmap



FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques

+ FOR610.1: Malware Analysis Fundamentals
+ FOR610.2: Reversing Malicious Code
+ FOR610.3: Malicious Web and Document Files
+ FOR610.4: In-Depth Malware Analysis
+ FOR610.5: Examining Self-Defending Malware
+ FOR610.6: Malware Analysis Tournament

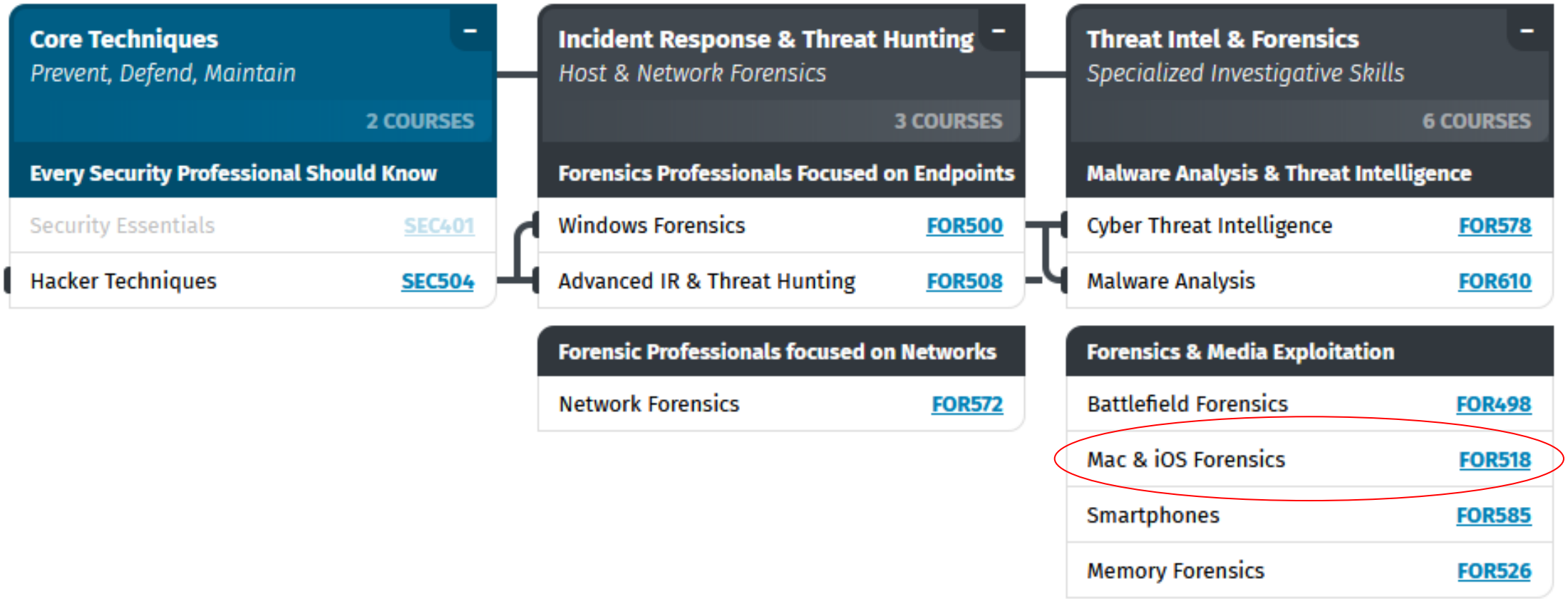
SANS Forensics Roadmap



FOR498: Battlefield Forensics & Data Acquisition

+ FOR498.1: Evidence File Quick Wins and Dealing with Smartphones
+ FOR498.2: Evidence Acquisition and Collection
+ FOR498.3: Quick Win Forensics
+ FOR498.4: Non-Traditional and Cloud Acquisition
+ FOR498.5: Apple Acquisition, Internet of Things, and Online Attribution
+ FOR498.6: Beyond the Forensic Tools: The Deeper Dive

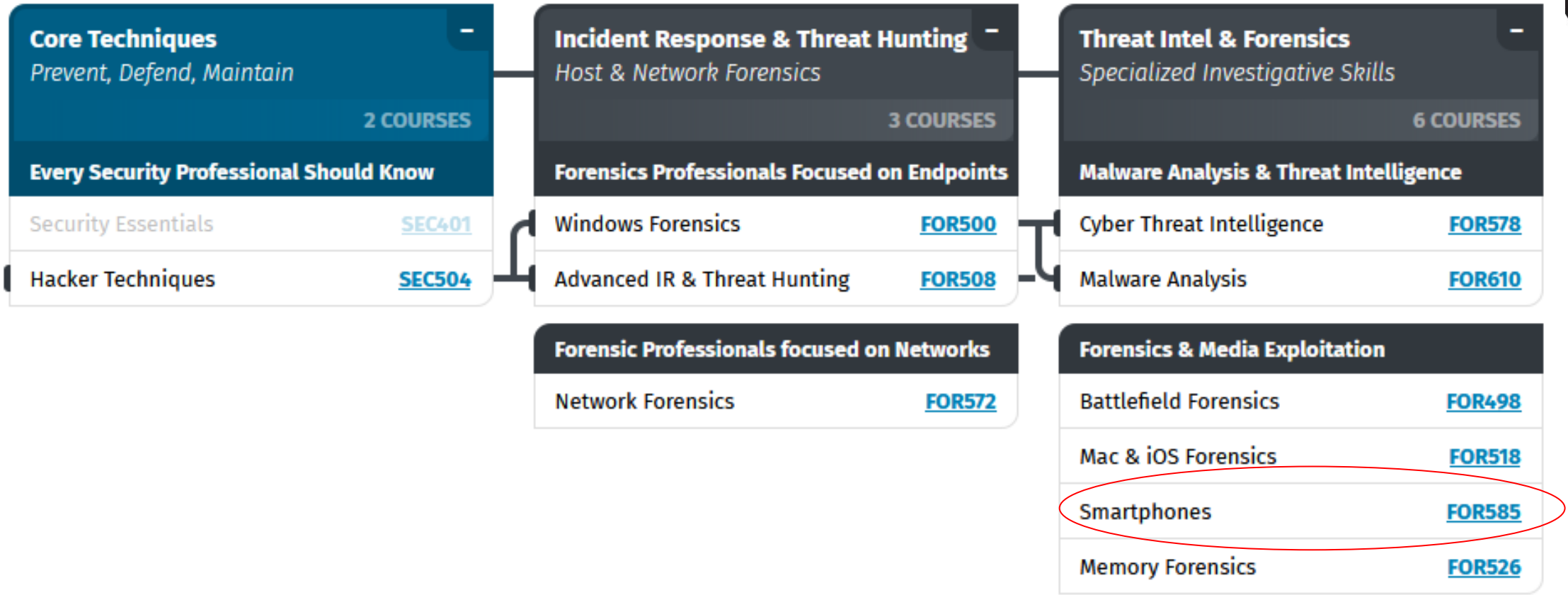
SANS Forensics Roadmap



FOR518: Mac and iOS Forensic Analysis and Incident Response

- FOR518.1: Mac and iOS Essentials
- FOR518.2: File Systems & System Triage
- FOR518.3: User Data, System Configuration, and Log Analysis
- FOR518.4: Application Data Analysis
- FOR518.5: Advanced Analysis Topics
- FOR518.6: Mac Forensics & Incident Response Challenge

SANS Forensics Roadmap



FOR585: Smartphone Forensic Analysis In-Depth

+ FOR585.1: Smartphone Overview, Fundamentals of Analysis, SQLite Introduction, Android Forensics Overview, and Android Backups

+ FOR585.2: Android Forensics

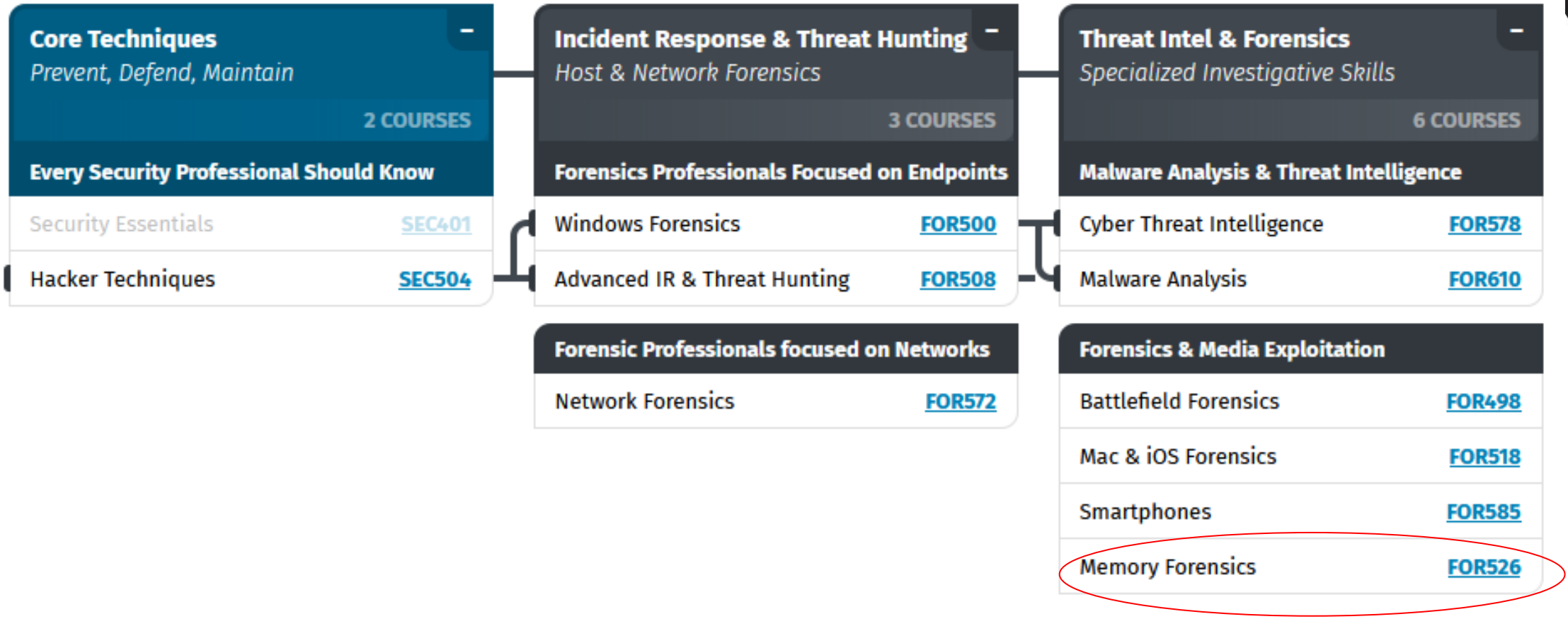
+ FOR585.3: iOS Device Forensics

+ FOR585.4: iOS Backups, Malware and Spyware Forensics, and Detecting Evidence Destruction

+ FOR585.5: Third-Party Application Analysis

+ FOR585.6: Smartphone Forensic Capstone Exercise

SANS Forensics Roadmap



FOR526: Advanced Memory Forensics & Threat Detection

+ FOR526.1: Foundations in Memory Analysis and Acquisition
+ FOR526.2: Unstructured Analysis and Process Exploration
+ FOR526.3: Investigating the User via Memory Artifacts
+ FOR526.4: Internal Memory Structures
+ FOR526.5: Memory Analysis on Platforms Other than Windows
+ FOR526.6: Memory Analysis Challenges

Cloud Security & DevOpsRoadmap

SEC488: Cloud Security Essentials

+ SEC488.1: Welcome to the Cloud
+ SEC488.2: Securing the Cloud Environment and Infrastructure Security
+ SEC488.3: Application Security and Securing Services
+ SEC488.4: Cloud OPs and Architecture
+ SEC488.5: Legal/Compliance, Penetration Testing & Incident Response

Cloud Security & DevOpsRoadmap

SEC522: Defending Web Applications Security Essentials

+ SEC522.1: Web Fundamentals and Security Configurations
+ SEC522.2: Defense Against Input Related Threats
+ SEC522.3: Web Application Authentication and Authorization
+ SEC522.4: Web Services and Front-End Security
+ SEC522.5: Cutting-Edge Web Security
+ SEC522.6: Capture-and-Defend-the-Flag Exercise

DOURAN GROUP

Cloud Security & DevOpsRoadmap

SEC534: Secure DevOps: A Practical Introduction

+ SEC534.1: Introduction to Secure DevOps

+ SEC534.2: Moving to Production

Cloud Security & DevOpsRoadmap

Cloud Security	5 COURSES
Every Developer Should Know	
Cloud Sec Essentials	SEC488
Development Security Essentials	SEC522
Secure DevOps	SEC534
Secure DevOps and Cloud	SEC540
Cloud Sec Architecture & Ops	SEC545

SEC540: Cloud Security and DevOps Automation

+ SEC540.1: Introduction to DevSecOps
+ SEC540.2: Cloud Infrastructure and Orchestration
+ SEC540.3: Cloud Security Operations
+ SEC540.4: Cloud Security as a Service
+ SEC540.5: Compliance as Code

Cloud Security & DevOpsRoadmap

SEC545: Cloud Security Architecture and Operations

+ SEC545.1: Cloud Security Foundations
+ SEC545.2: Core Security Controls for Cloud Computing
+ SEC545.3: Cloud Security Architecture and Design
+ SEC545.4: Cloud Security - Offense and Defense
+ SEC545.5: Cloud Security Automation and Orchestration

Industrial Control Systems Roadmap

ICS410: ICS/SCADA Security Essentials

+ ICS410.1: ICS Overview
+ ICS410.2: Field Devices & Controllers
+ ICS410.3: Supervisory Systems
+ ICS410.4: Workstations and Servers
+ ICS410.5: ICS Security Governance

Industrial Control Systems Roadmap

ICS515: ICS Active Defense and Incident Response

- ICS515.1: Threat Intelligence
- ICS515.2: Asset Identification and Network Security Monitoring
- ICS515.3: Incident Response
- ICS515.4: Threat and Environment Manipulation
- ICS515.5: Active Defense and Incident Response Challenge

Industrial Control Systems Roadmap

ICS612: ICS Cybersecurity In-Depth

+ ICS612.1: The Local Process
+ ICS612.2: System of Systems
+ ICS612.3: ICS Network Infrastructure
+ ICS612.4: ICS System Management
+ ICS612.5: Covfefe Down!

Industrial Control Systems Roadmap

ICS456: Essentials for NERC Critical Infrastructure Protection

+ ICS456.1: Asset Identification and Governance
+ ICS456.2: Access Control and Monitoring
+ ICS456.3: System Management
+ ICS456.4: Information Protection and Response
+ ICS456.5: The CIP Process