



Beyond Passwords and Firewalls: Cybersecurity Tactics for Today's Co-op

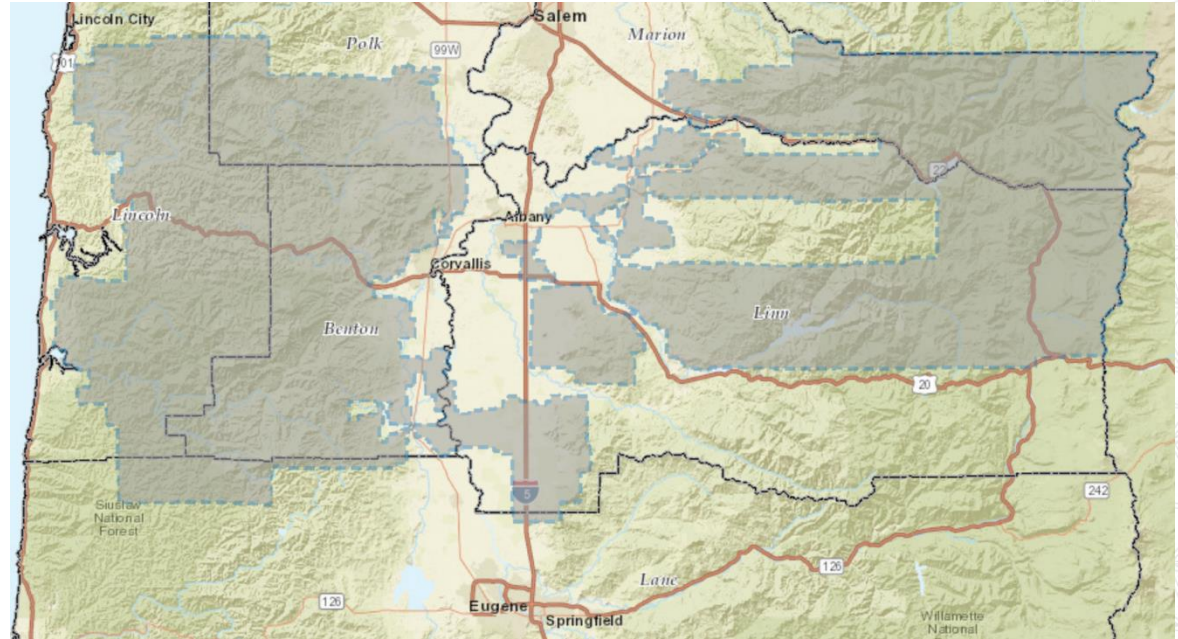
Taylor Cox
Network Security Administrator
Consumers Power Inc.





Consumers Power Inc.

- Philomath, OR
- 22,000 members
- 3,500 sq mi
- 6 counties
- 3,000 miles of line
- 6.7 customers/mi
- 68 employees
- 7 IT staff



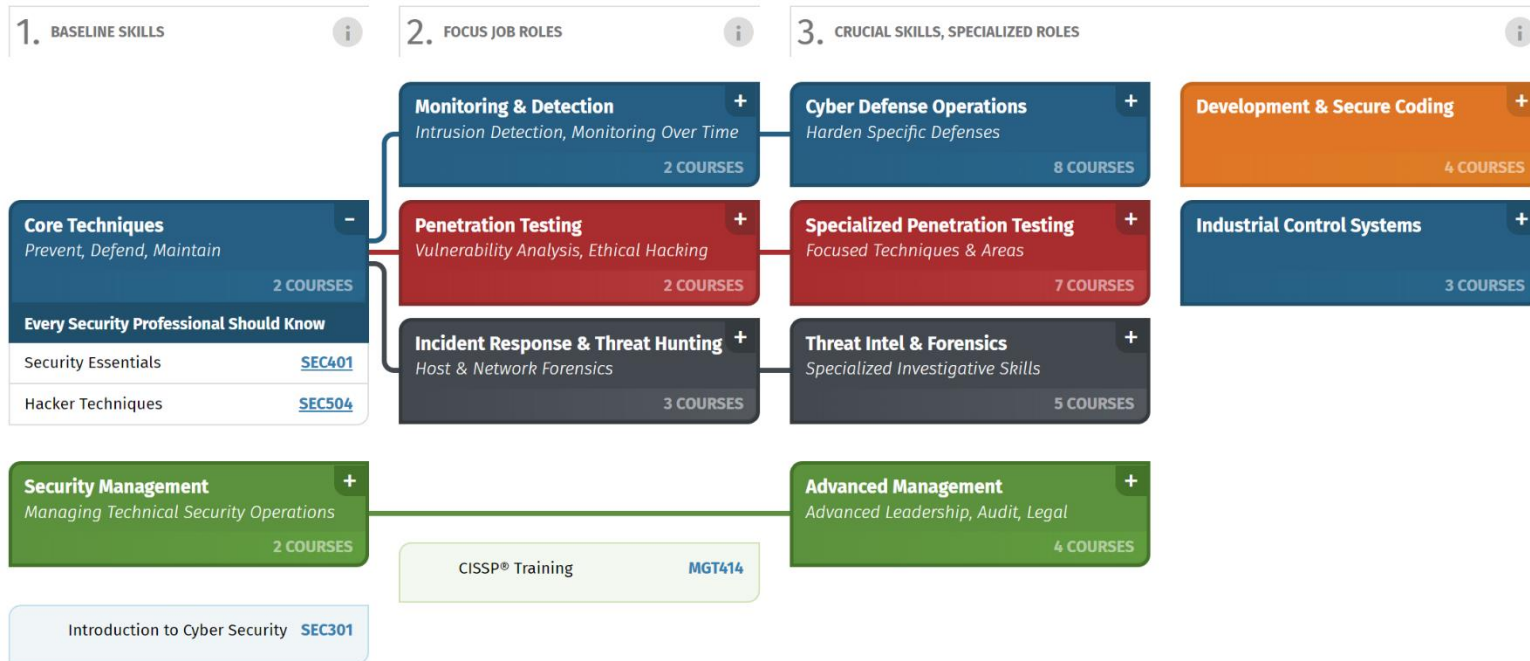


Before RC3

- Oregon State University
 - B.S. Finance
- CompTIA Security +



SANS Cyber Security Skills Roadmap



SANS Cyber Security Skills Roadmap

Core Techniques

Prevent, Defend, Maintain

2 COURSES

Every Security Professional Should Know

Security Essentials

[SEC401](#)

Hacker Techniques

[SEC504](#)

Before RC3

- Oregon State University
 - B.S. Finance
- Security +
- SEC 401: Security Essentials Bootcamp Style
 - GIAC GSEC
- SEC 504 Hacker Tools, Techniques, Exploits, and Incident Handling
 - GIAC GCIH

RC3

- Two categories:
 - Category A
 - SEC 301, SEC 401, SEC 503
 - SEC 301, MGT 512, MGT 514
 - Category B
 - Any available online class

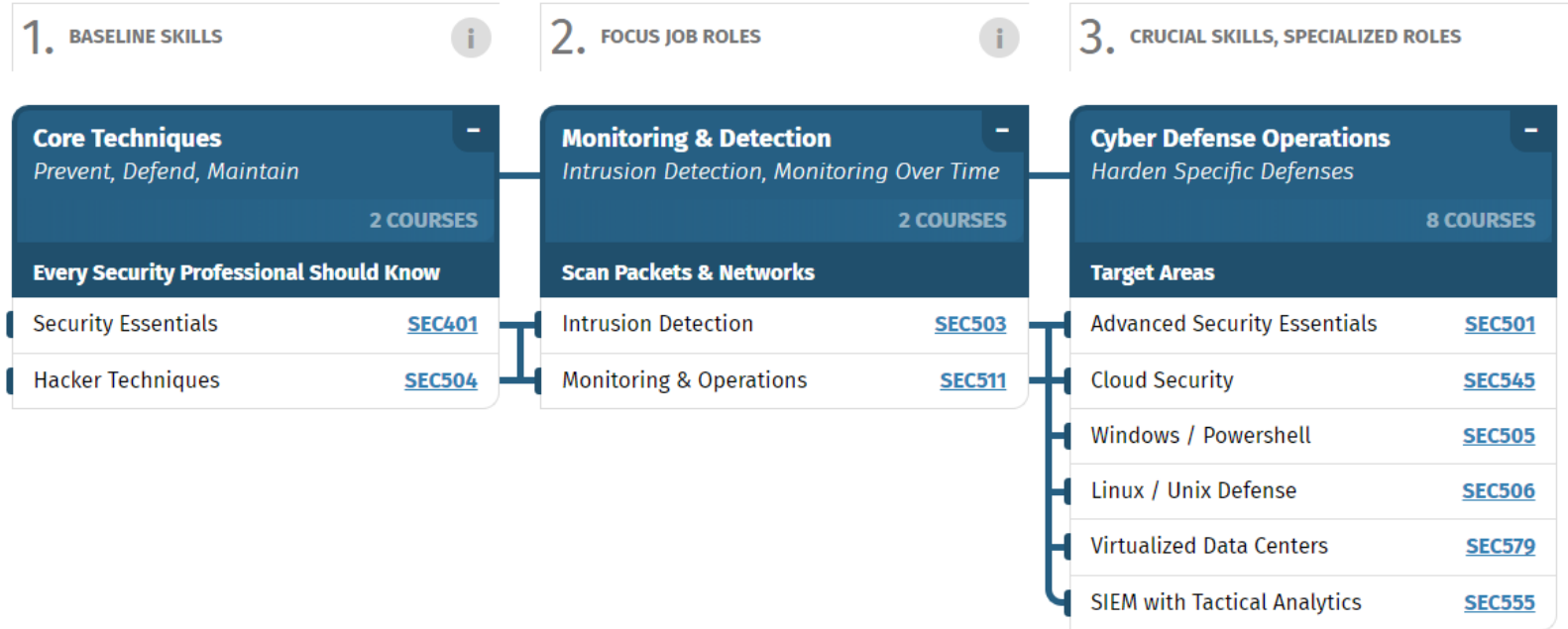


RC3

- Three SANS classes
 - Who else would benefit?
 - AMI Administrator
 - SEC 401, GSEC
 - Now taking SEC 504, GCIH (Not RC3)



SANS Cyber Security Skills Roadmap



RC3

- **SEC 505: Securing Windows and PowerShell Automation**
 - GIAC GCWN



SEC 505

Course Syllabus

+ SEC505.1: Learn PowerShell Scripting

+ SEC505.2: Host Hardening and Active Directory Scripting

+ SEC505.3: Smart Tokens and Public Key Infrastructure (PKI)

+ SEC505.4: Protecting Admin Credentials and PowerShell JEA

+ SEC505.5: Thwarting Hackers Inside The Network

+ SEC505.6: Blue Team PowerShell: WMI, DNS, RDP and SMB



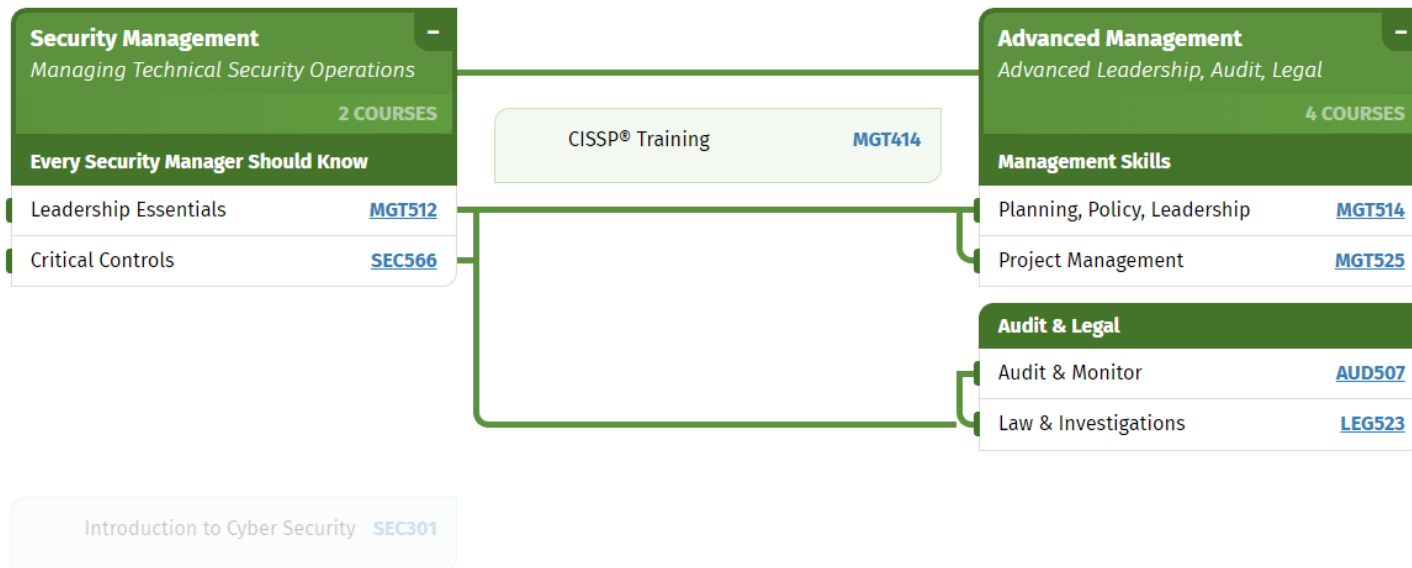


Projects

- Windows 10/Server 2016
- MFA
- Credential protections
- Patch management
- Removal of legacy Windows services
- Windows automation
- PKI/Certificates
- IPsec
- Host based firewall



SANS Cyber Security Skills Roadmap





RC3

- LEG 523: Law of Data Security and Investigations
 - GIAC GLEG



LEG 523

Course Syllabus

+ LEG523.1: Fundamentals of Data Security Law and Policy

+ LEG523.2: E-Records, E-Discovery and Business Law

+ LEG523.3: Contracting for Data Security and Other Technology

+ LEG523.4: The Law of Data Compliance: How to Conduct Investigations

+ LEG523.5: Applying Law to Emerging Dangers: Cyber Defense





Projects

- Security requirements in vendor contracts
- Incident response planning
- Law enforcement investigation
- E-discovery guidance
- What is legal, what is not, what is uncertain



Takeaways

- “Good Computer Security is nothing but an inspired application of the fundamentals.” -Ed Capizzi
- Course for every need
- Top instructors
- Impactful projects
- Expand culture of security

