Fractional CISO's Cybersecurity Workshop Series

Weekly Syllabus

1. External Technical Evaluation

- Fractional CISO performs a technical evaluation of your external network and reviews results
- Receive actionable advice on how to harden your external-facing environment
- Preview AWS Security Hub

2. AWS Security Hub Initial Assessment

- Enable AWS Security Hub and get initial scores
- Set risk-optimized goals for Security Hub score improvements
- Compare AWS Security Hub assessment results to CIS Controls

3. Essential Controls and Workspace Eval

- Turn on multi-factor authentication (MFA) on all high-value accounts
- Evaluate Google Workspace security configurations
- Harden Google Workspace instances

4. Key Security Processes

- Learn about key cybersecurity processes including employee off-boarding, vendor management, and patch management.
- Use templated procedure documents to implement key practices in your organization

5. AWS Security Hub Assessment 2

- AWS Identify and Access Management (IAM) review/rollout
- Explore functionality of AWS security services including CloudTrail and GuardDuty
- Continue improving AWS security settings

6. Cyber Insurance Evaluation

- Learn what makes good and bad cyber insurance coverage
- Determine what risk-optimized coverage looks like for your organization
- Advise on how to improve coverage

7. Incident Response Plan Draft

- Learn about high-quality incident response plans
- Determine likely risks at your organization
- Begin drafting an incident response plan tailored for your organization

8. External Technical Evaluation 2

- Perform another external technical evaluation and compare to Week 1 results
- Discuss how things have changed, and how to continue improving external-facing posture

9. Incident Response Tabletop

- Whole group performs a collaborative incident response tabletop exercise
- Learn how to practice incident response at your own organization

10. Phishing, Training, and Testing

- Learn about the importance of phishing, the most common cyber attack
- Evaluate different phish training vendors
- Decide which phishing training vendor is correct for your organization

11. Finalize Incident Response Plan

- Review several different incident response plans from the group
- Make recommendations to improve all plans to a high-quality standard

12. Final Assessment

- Review AWS Security Hub and make a roadmap for future improvements
- Help plan for future cybersecurity and compliance goals

Interested? Click here to request pricing.