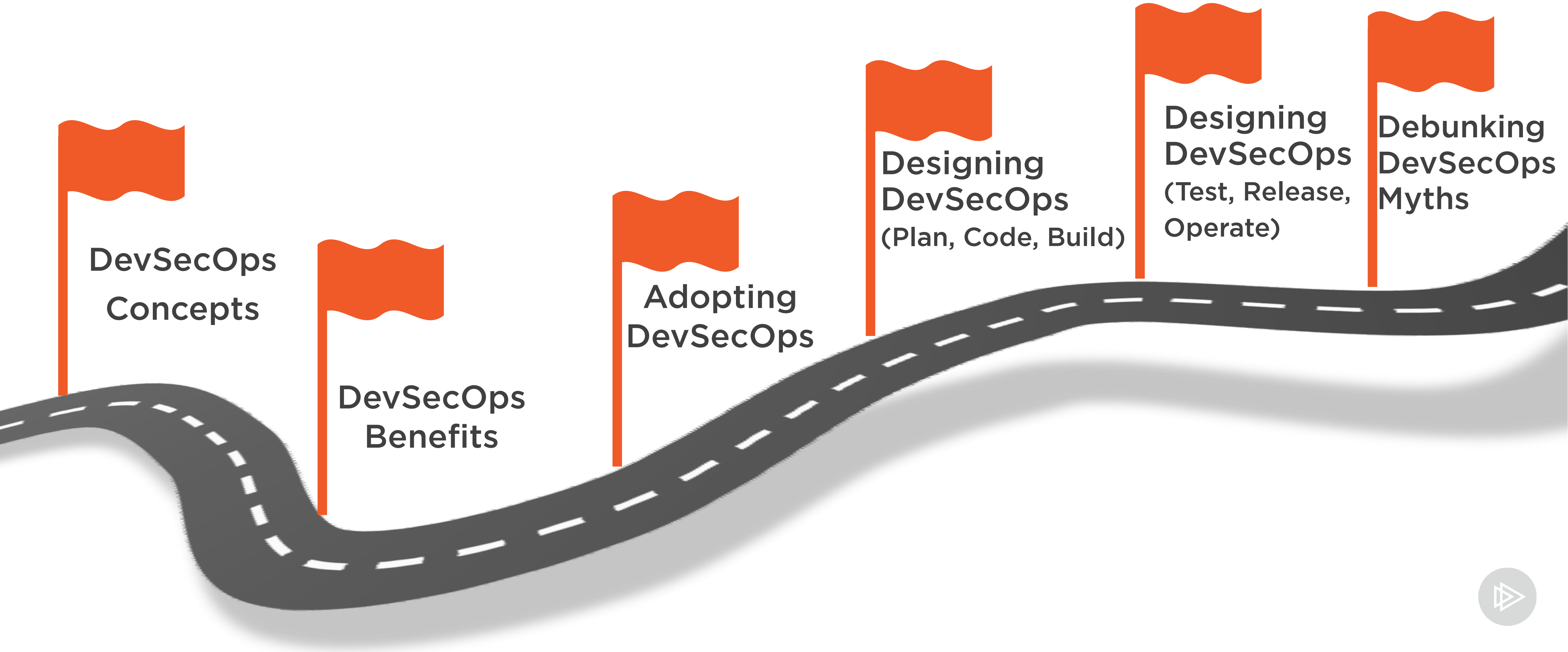
Debunking DevSecOps Myths

Richard Harpur

INFORMATION SECURITY PROFESSIONAL, CISM

@rharpur www.richardharpur.com

Continue Our DevSecOps Journey



DevSecOps Concepts

DevSecOps Benefits

Adopting DevSecOps

Designing DevSecOps (Plan, Code, Build)

Designing DevSecOps (Test, Release, Operate)

Debunking DevSecOps Myths

Overview

Debunking DevSecOps myths

- Special teams
- Delays to deployments
- Buying DevSecOps

Course wrap up

- Future learning

DevSecOps Manifesto Reminder

DevSecOps Manifesto

Leaning in over Always Saying “No”
Data & Security Science over Fear, Uncertainty and Doubt
Open Contribution & Collaboration over Security-Only Requirements
Consumable Security Services with APIs over Mandated Security Controls & Paperwork
Business Driven Security Scores over Rubber Stamp Security
Red & Blue Team Exploit Testing over Relying on Scans & Theoretical Vulnerabilities
24x7 Proactive Security Monitoring over Reacting after being Informed of an Incident
Shared Threat Intelligence over Keeping Info to Ourselves
Compliance Operations over Clipboards & Checklists

Source: https://www.devsecops.org/

Common Myths

Helping Ben

Ben is a software developer

He has worked for Globomantics for 3 years now

Ben wants to introduce DevSecOps practice

We will help Ben identify the benefits of DevSecOps so that he can get support from his manager and peers ✓

We will help Ben respond to myths his team are raising ✓

We Cannot Introduce DevSecOps Because…

We Cannot Introduce DevSecOps Because…

We need a special team dedicated to DevSecOps

> "DevSecOps is…
> empowered engineering teams taking ownership of how their product performs all the way to production, including security."
>
> *Larry Maccherone*

We Cannot Introduce DevSecOps Because…

The security team still needs to do all security checks for us

By handing over security checks to other teams we introduce delays and time lag into our agile process, instead we should ask the security team to codify their checks so we can build them into our development process automatically.

We Cannot Introduce DevSecOps Because…

We don't have enough resources to do DevSecOps, just buy a tool that does it for us

DevSecOps is not about a capability, it is about a culture, buying a tool is not culture changing. Whilst tools are required to make DevSecOps possible these tools supplement the existing development process and help you deliver DevSecOps, if you have the correct culture in place.

We Cannot Introduce DevSecOps Because…

DevSecOps will just slow down our developers

DevSecOps is about empowering developers to ensure their product gets to production with appropriate security built-in. Traditional approaches to security required testing after developers complete coding and before deployment to production.

Because this is so late in the lifecycle it takes longer to fix and retest software compared to identifying the issue at an earlier stage in the lifecycle, so DevSecOps can save time and increase developer speed.

We Cannot Introduce DevSecOps Because…

DevSecOps will result in our developers giving up control and won’t be able to plan

With DevSecOps developers gain control by running security checks at the best possible opportunity to help developers fix the issues quickly and easily. No longer are developers dependent on external teams, and gain control of the work and schedule.

Summary

DevSecOps = empowering developers

More consistency and control

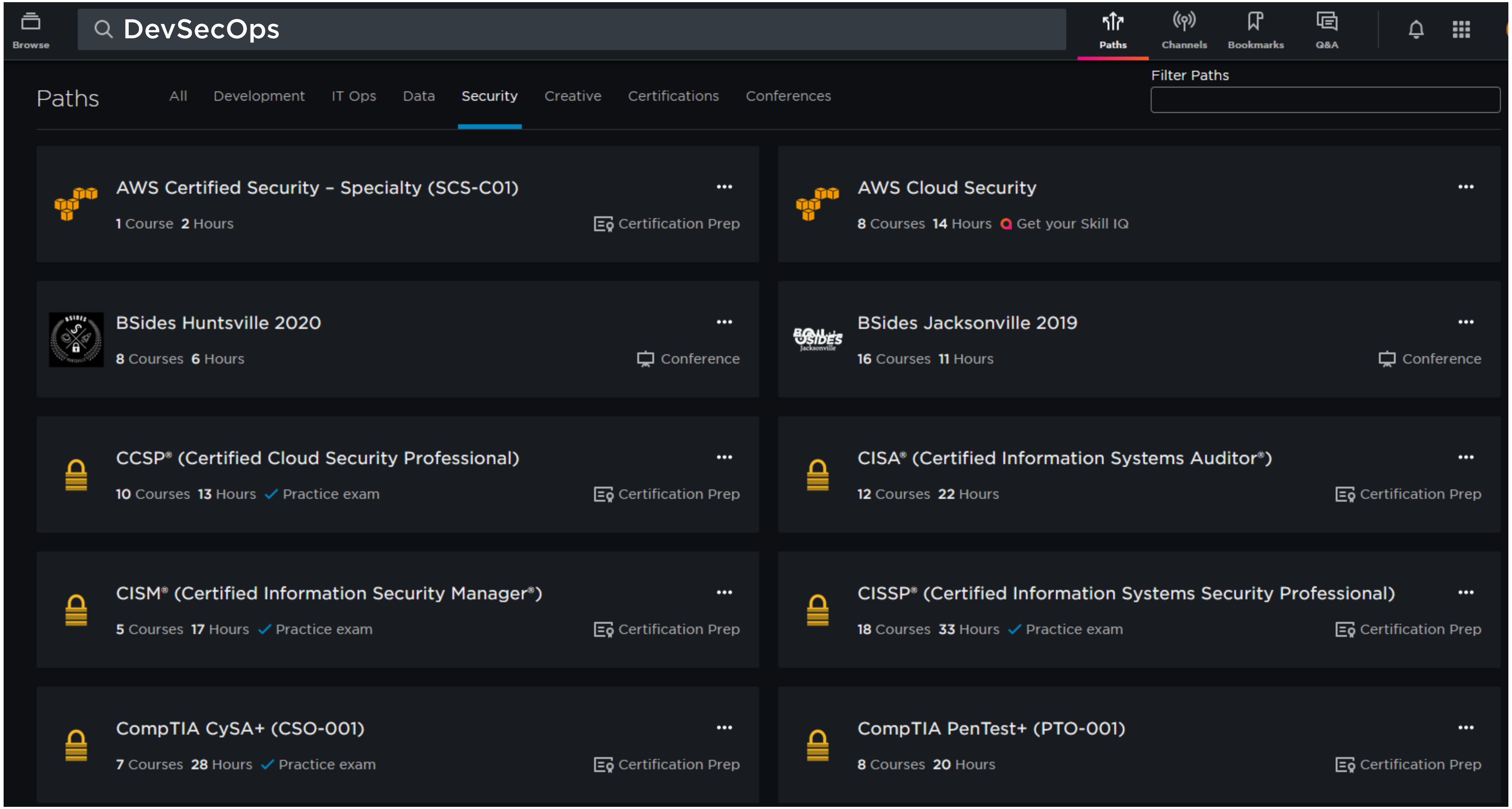
Culture

- Next steps
- Thank you

Congratulations

Further Learning

DevSecOps Path



DevSecOps

Paths

All · Development · IT Ops · Data · Security · Creative · Certifications · Conferences

Filter Paths

AWS Certified Security – Specialty (SCS-C01)
1 Course 2 Hours · Certification Prep

AWS Cloud Security
8 Courses 14 Hours · Get your Skill IQ

BSides Huntsville 2020
8 Courses 6 Hours · Conference

BSides Jacksonville 2019
16 Courses 11 Hours · Conference

CCSP® (Certified Cloud Security Professional)
10 Courses 13 Hours ✓ Practice exam · Certification Prep

CISA® (Certified Information Systems Auditor®)
12 Courses 22 Hours · Certification Prep

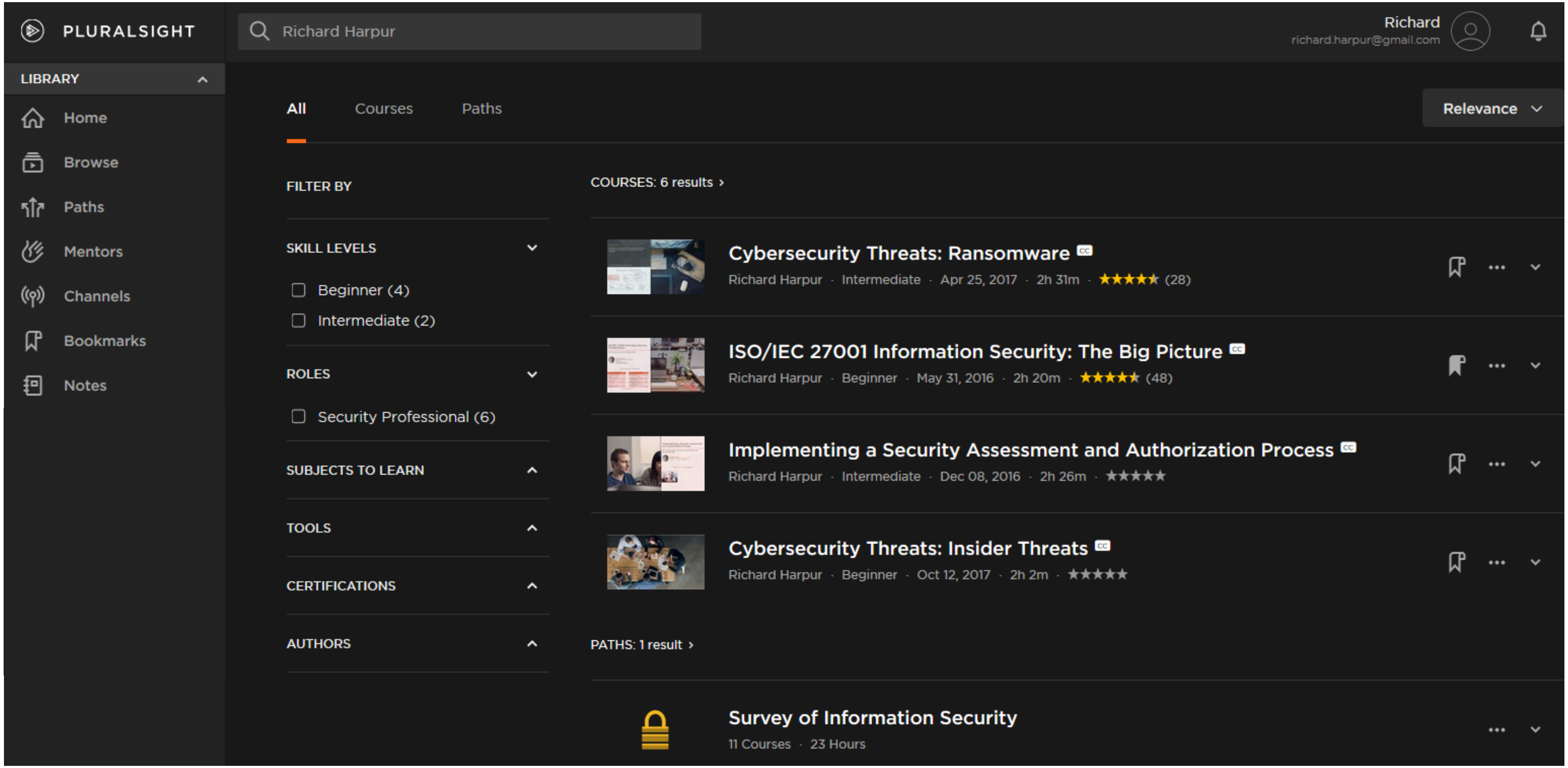
CISM® (Certified Information Security Manager®)
5 Courses 17 Hours ✓ Practice exam · Certification Prep

CISSP® (Certified Information Systems Security Professional)
18 Courses 33 Hours ✓ Practice exam · Certification Prep

CompTIA CySA+ (CSO-001)
7 Courses 28 Hours ✓ Practice exam · Certification Prep

CompTIA PenTest+ (PTO-001)
8 Courses 20 Hours · Certification Prep

Where to from Here?



□ Beginner (4)
□ Intermediate (2)

□ Security Professional (6)

COURSES: 6 results ›

Cybersecurity Threats: Ransomware
Richard Harpur · Intermediate · Apr 25, 2017 · 2h 31m · ★★★★★ (28)

ISO/IEC 27001 Information Security: The Big Picture
Richard Harpur · Beginner · May 31, 2016 · 2h 20m · ★★★★★ (48)

Implementing a Security Assessment and Authorization Process
Richard Harpur · Intermediate · Dec 08, 2016 · 2h 26m · ★★★★★

Cybersecurity Threats: Insider Threats
Richard Harpur · Beginner · Oct 12, 2017 · 2h 2m · ★★★★★

PATHS: 1 result ›

Survey of Information Security
11 Courses · 23 Hours

“Thank you”

@rharpur

www.richardharpur.com