#MissionBeforeMoney

2021 CISSP MENTOR PROGRAM

Class 1 – April 12, 2021

Instructor: Evan Francen, FRSecure & SecurityStudio CEO

Welcome!

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

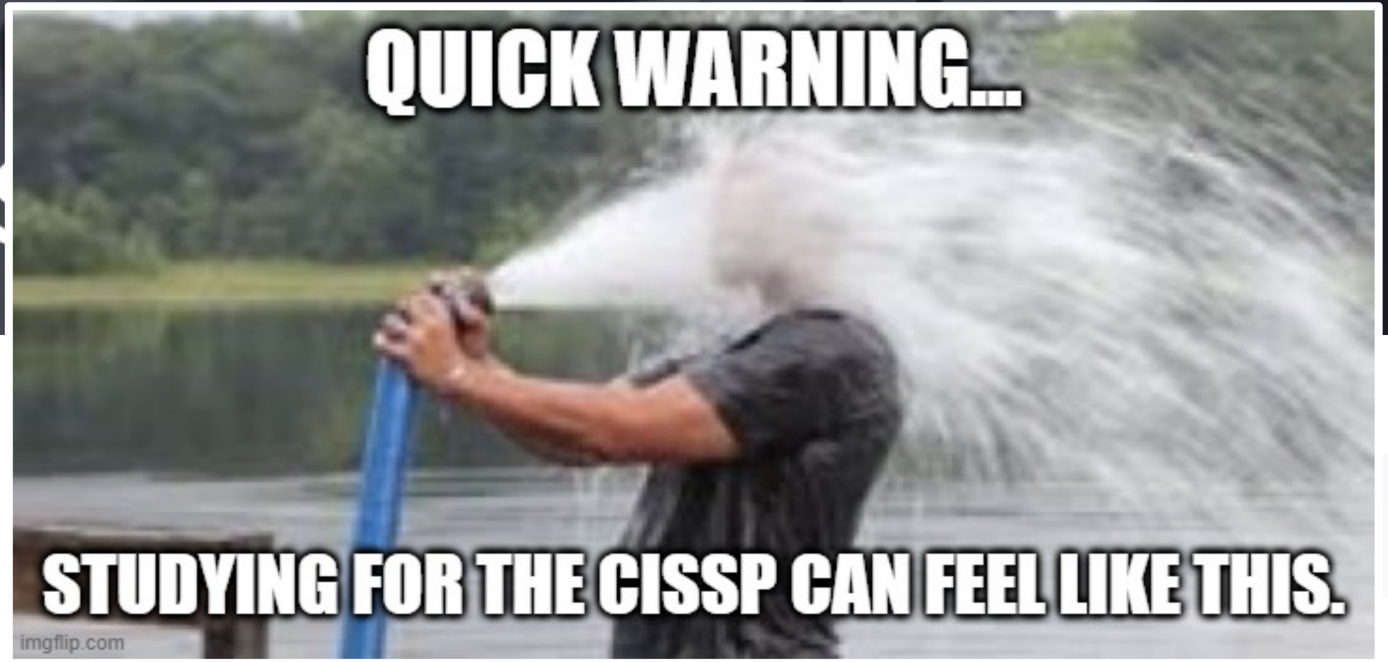
2021 FRSecure CISSP Mentor Program

CAUTION

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

CAUTION



CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

CAUTION

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

Welcome!

- What is the CISSP Mentor Program?
- History
  - 2010 – 1st Class – 6 students
  - Today – 12th Class – 5,900+ students!
- Why do we do it?
- Success stories
- Heck, it's free! What have you got to lose?

Remember when this guy was thought to be the worst the 2010's had to offer?
He was just a warmup

We have a severe talent shortage problem in our industry. Good news for you…

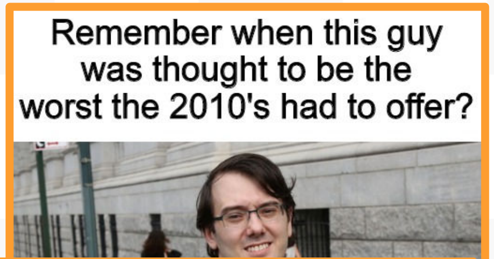
CISSP® MENTOR PROGRAM – SESSION ONE

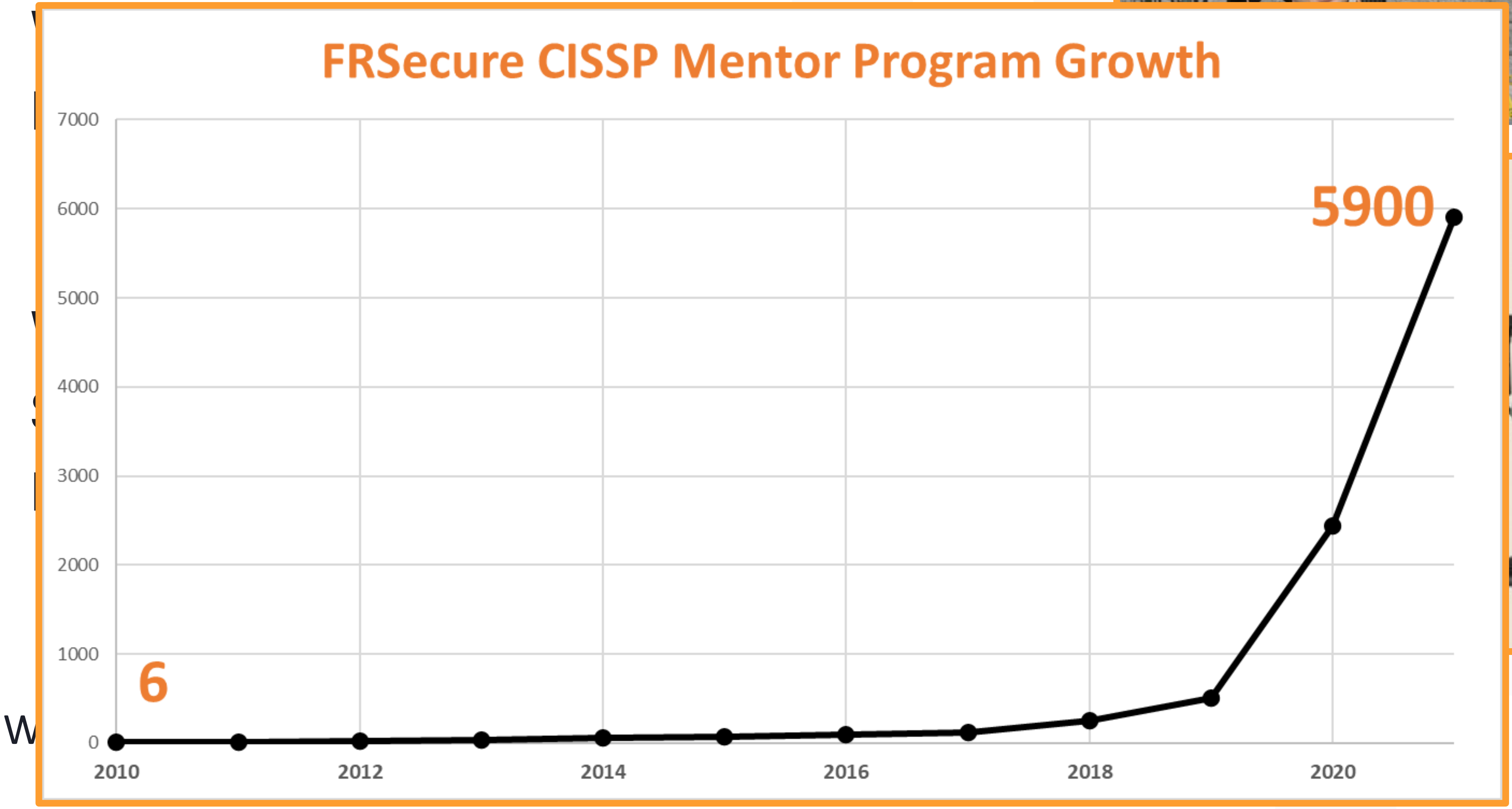
INTRODUCTION

Welcome!

- V
- I
- V
- S
- I

W


Remember when this guy was thought to be the worst the 2010's had to offer?



CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

Why do we do it?

Mission:

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

Why do we do it?

Mission: To fix the broken industry

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

Why do we do it?

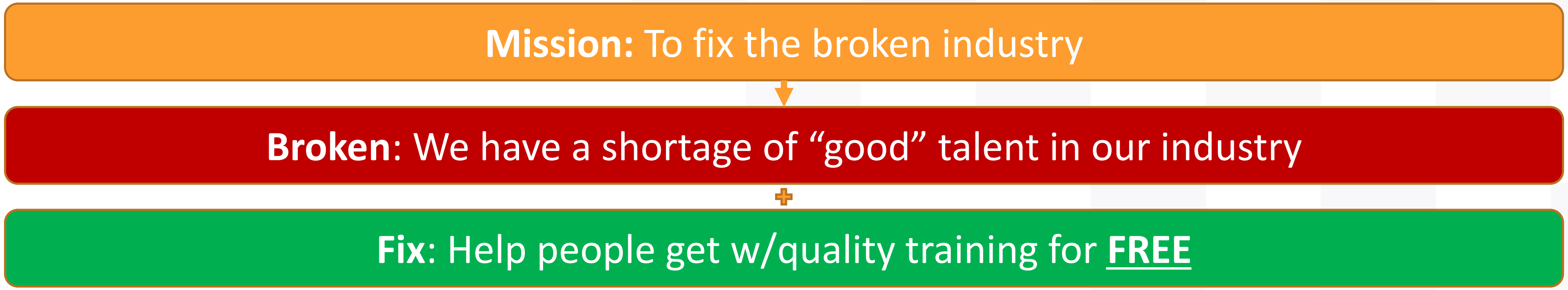
Mission: To fix the broken industry

Broken: We have a shortage of "good" talent in our industry

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

Why do we do it?



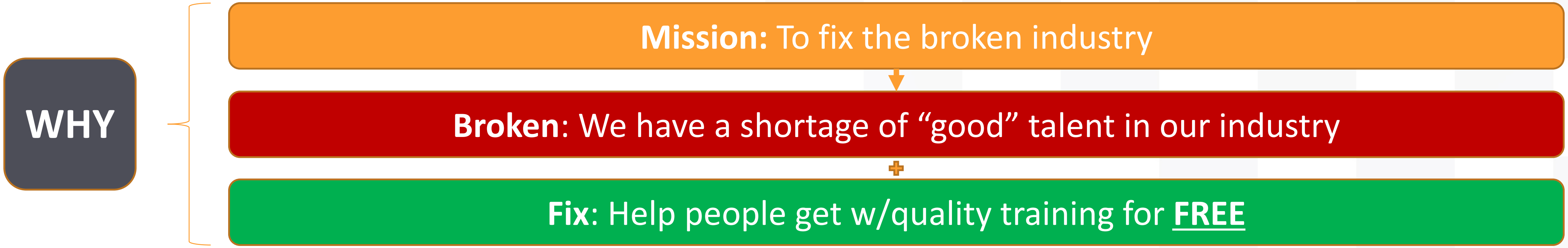
Mission: To fix the broken industry

Broken: We have a shortage of “good” talent in our industry

Fix: Help people get w/quality training for **FREE**

INTRODUCTION

Why do we do it?



WHY

Mission: To fix the broken industry

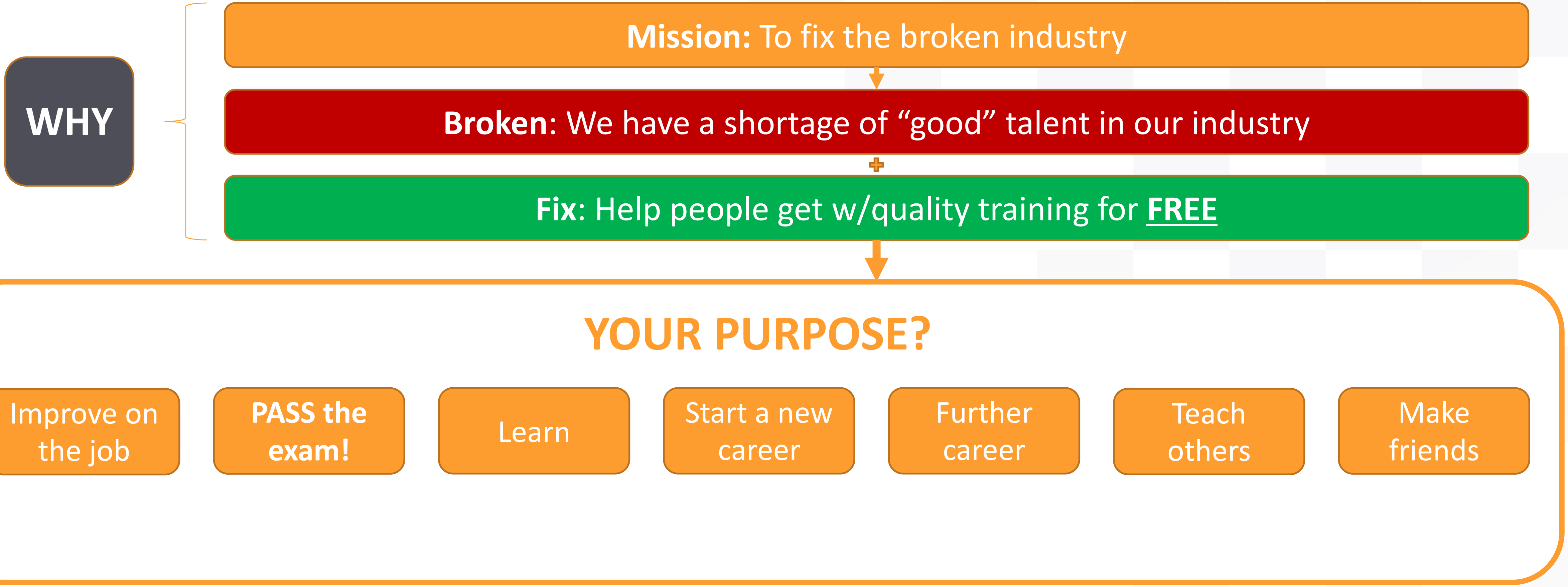
Broken: We have a shortage of “good” talent in our industry

Fix: Help people get w/quality training for **FREE**

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

Why do we do it?



WHY

Mission: To fix the broken industry

Broken: We have a shortage of "good" talent in our industry

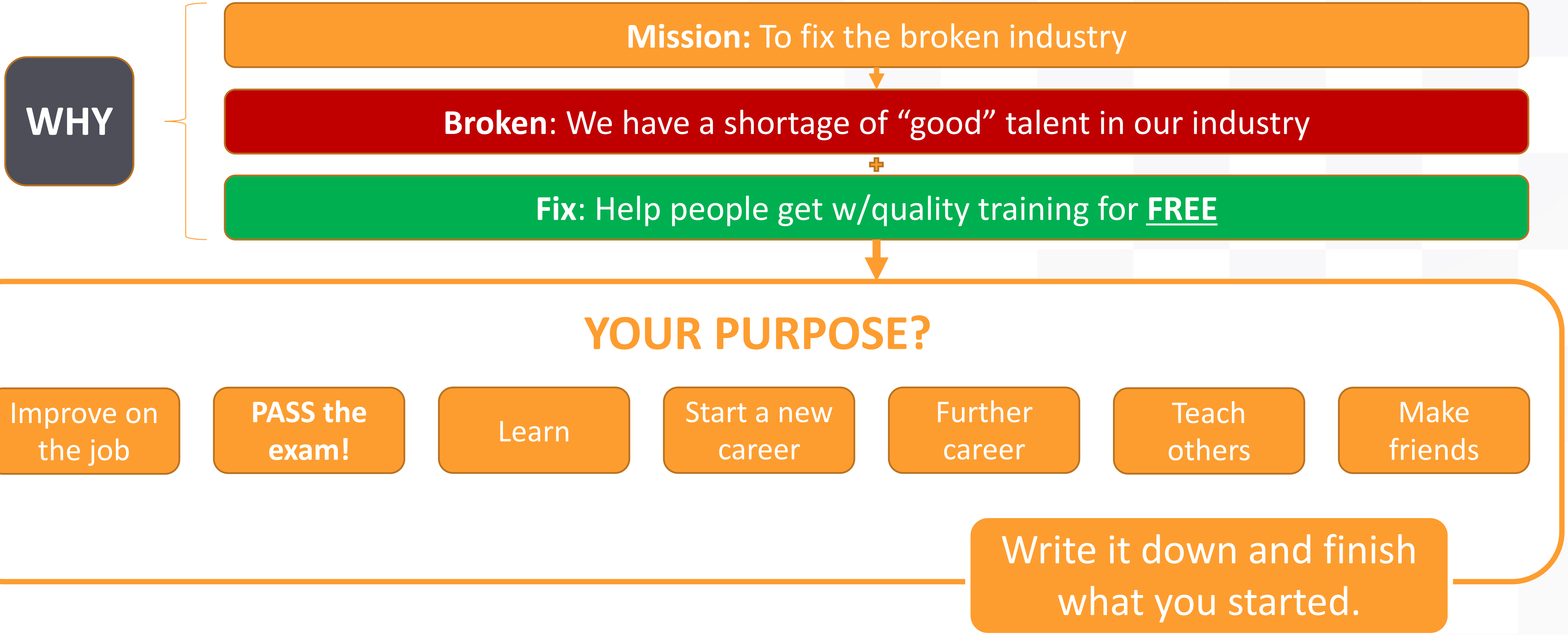
Fix: Help people get w/quality training for **FREE**

YOUR PURPOSE?

- Improve on the job
- **PASS the exam!**
- Learn
- Start a new career
- Further career
- Teach others
- Make friends

INTRODUCTION

Why do we do it?



WHY

Mission: To fix the broken industry

Broken: We have a shortage of "good" talent in our industry

Fix: Help people get w/quality training for **FREE**

YOUR PURPOSE?

- Improve on the job
- **PASS the exam!**
- Learn
- Start a new career
- Further career
- Teach others
- Make friends

Write it down and finish what you started.

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

Success stories

- The first class.
- The growth.
- People who want to pass the exam, do.
  - We don’t specifically track this.
  - If 40% take the exam and 90% pass = 3,400+ new CISSPs!
  - Avg. cost of training = $2,750 = $26m+ FREE training!
- We get messages all year long.

Restored some trust in our industry. This is **FREE** and there are **NO STRINGS**!

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

Welcome – Today's Agenda

- Introduction – Getting to know us.
- Our severe talent shortage problem…
- Mentor Program Schedule & Class structure
- What is a CISSP?
- The book. **TIPS**
- Chapter 1 – Introduction (the other one).

The better you know us, the better you'll use us.

There is space for **<u>YOU</u>**!

Organizational stuff.

BACON IS THE ANSWER

I Don't Remember The Question

INTRODUCTION

2020 CISSP MENTOR PROGRAM

But first a joke.

Why is it a bad idea to iron your four-leaf clover?

INTRODUCTION

2020 CISSP MENTOR PROGRAM

But first a joke.

Why is it a bad idea to iron your four-leaf clover?

You don't want to press your luck!

INTRODUCTION

2020 CISSP MENTOR PROGRAM

One more…

Why do fathers take an extra pair of socks when they go golfing?

INTRODUCTION

2020 CISSP MENTOR PROGRAM

One more…

Why do fathers take an extra pair of socks when they go golfing?

In case they get a hole in one!

@evanfrancen

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About Evan

I do a lot of security stuff.

SECURITYSTUDIO®

- CEO and Co-founder of FRSecure and SecurityStudio
- Co-inventor of SecurityStudio (or S²), the platform for managing information security risk.
- Co-inventor of S²Org, S²Vendor, S²Team, and S²Me.
- Co-inventor of S²Score, a quantitative measurement of information security and vendor risk used by 4,500+ organizations.
- Co-host a couple of shows; UNSECURITY Podcast and the Security Sh!t Show.
- Tell the truth (always), simplify (everything), and serve (everyone).

Me, on most days

I think I look better as a cartoon.

> *"Evan's straightforward analysis of information security risk as fractured, incomplete and disconnected is spot on."* – CISO, University of Miami

@evanfrancen

INTRODUCTION

About Evan

I do a lot of security stuff.

- Advised legal counsel in high-profile breaches including Target and Blue Cross/Blue Shield.
  - 2014/2015 - Consultant to the Special Litigation Committee of the Board of Directors of Target Corporation; derivative action related to the "Target Breach".
  - 2015/2016 – Consultant to legal counsel and Blue Cross/Blue Shield related to remediation efforts (post-breach).
  - Served as an expert witness is multiple federal criminal cases, mostly involving alleged stolen trade secrets
- Served 100s of companies; big (Wells Fargo, Target, US Bank, UnitedHealth, etc.) and small.
- Lots of television and radio, lots of information security talks at conferences, and 750+ published articles about a variety of information security topics.

> *"I don't think I've met a more successful guy in this industry with less bullshit."* – Roger Grimes

Me, on most days

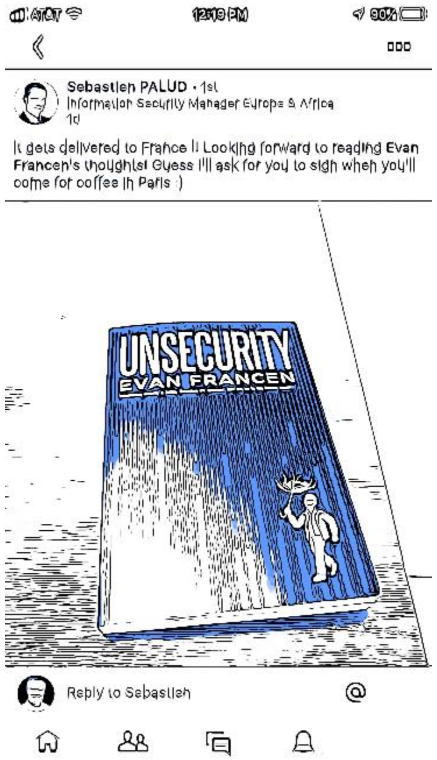
I think I look better as a cartoon.

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About Evan

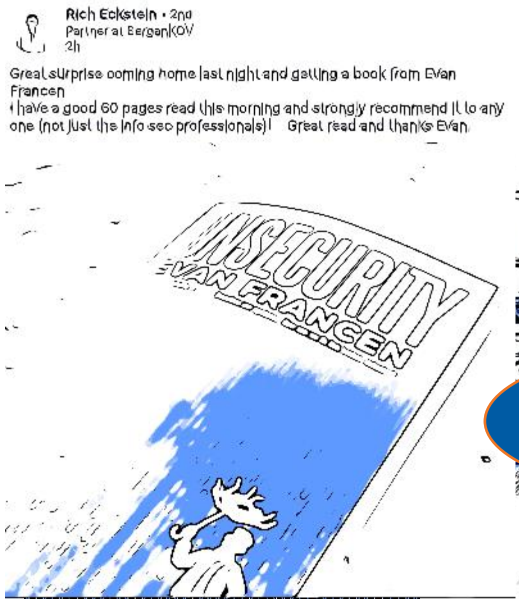
And then…



Sebastien PALUD • 1st
Information Security Manager Europe & Africa
1d

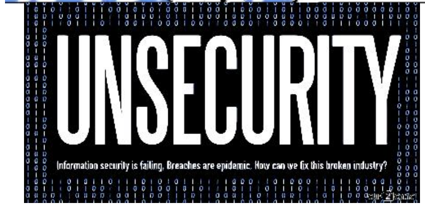
It gets delivered to France !! Looking forward to reading Evan Francen's thoughts! Guess I'll ask for you to sign when you'll come for coffee in Paris :)

Reply to Sebastien

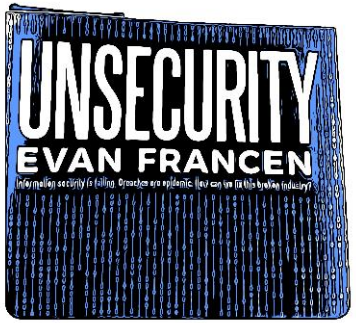


Rich Eckstein • 2nd
Partner at BerganKDV
2h

Great surprise coming home last night and getting a book from Evan Francen
I have a good 60 pages read this morning and strongly recommend it to any one (not just the info sec professionals)! Great read and thanks Evan


UNSECURITY
Information security is failing. Breaches are epidemic. How can we fix this broken industry?

Russian friend

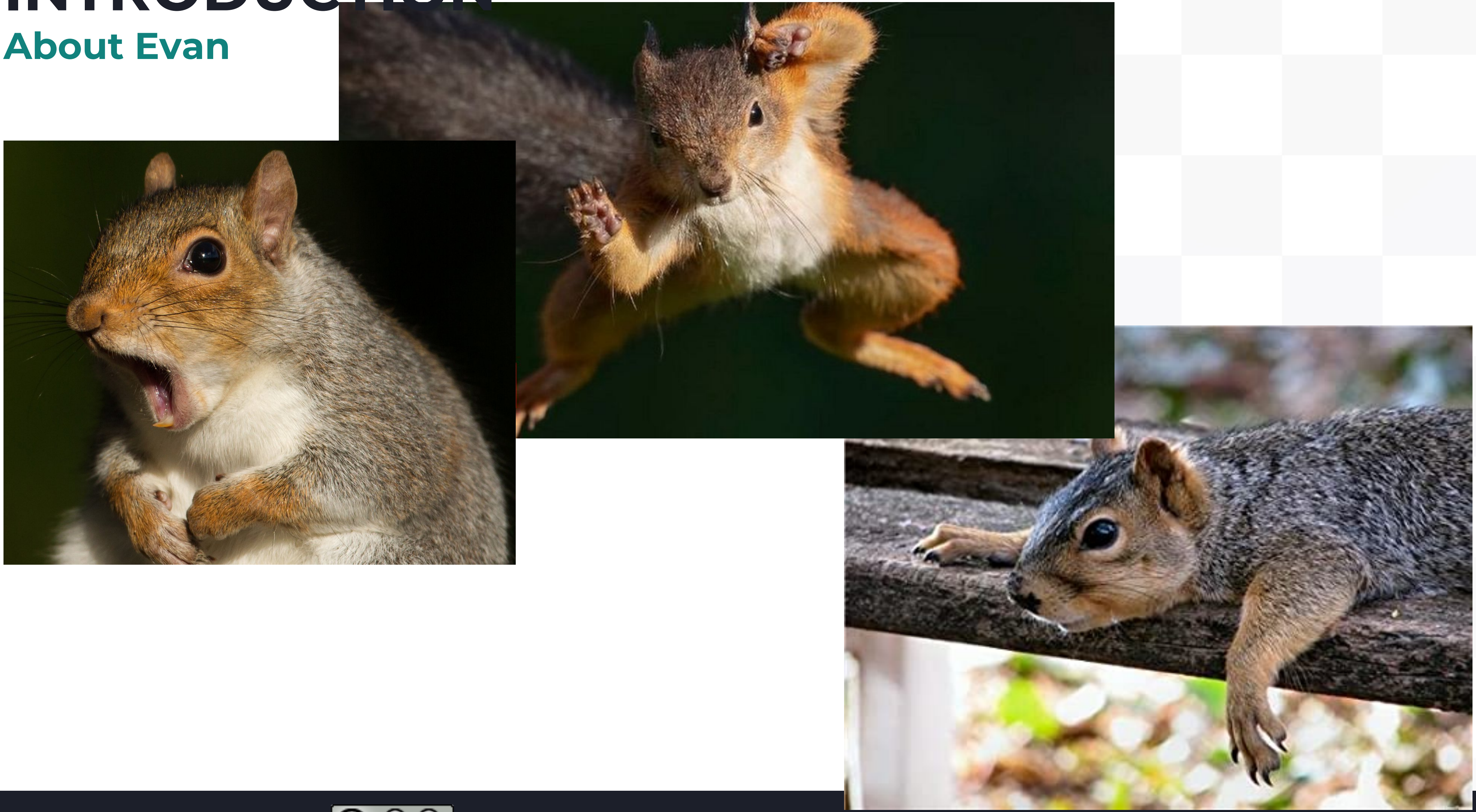

UNSECURITY
EVAN FRANCEN
Information security is failing. Breaches are epidemic. How can we fix this broken industry?

Chinese friend

https://www.amazon.com/Unsecurity-Information-security-failing-epidemic/dp/164343974X/

INTRODUCTION

About Evan



INTRODUCTION

About Evan

ADD is my superpower!

@evanfrancen

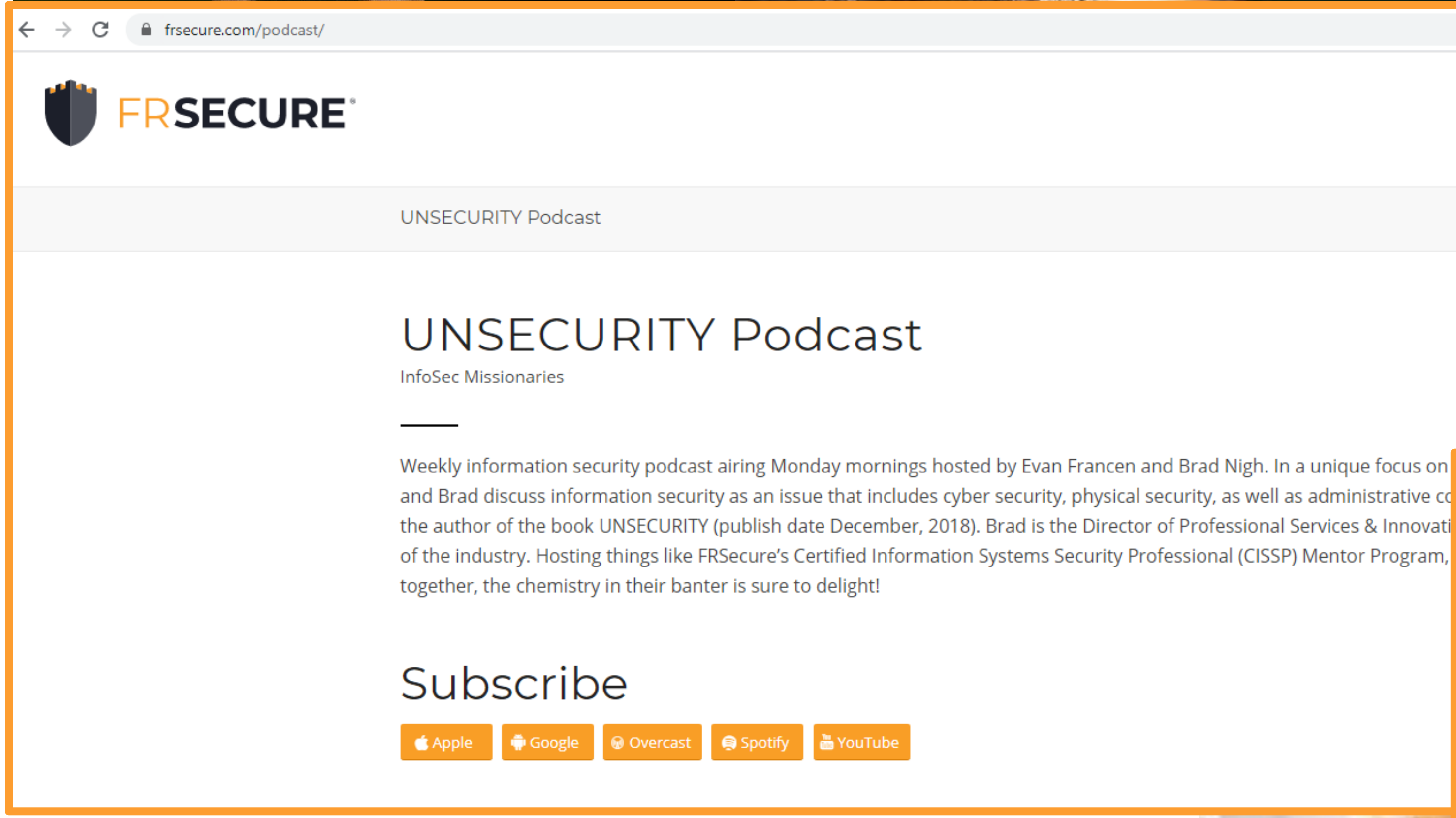
#MissionBeforeMoney

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About Evan

UNSECURITY Podcast



frsecure.com/podcast/

FRSECURE

UNSECURITY Podcast

You are here: Home / UNS

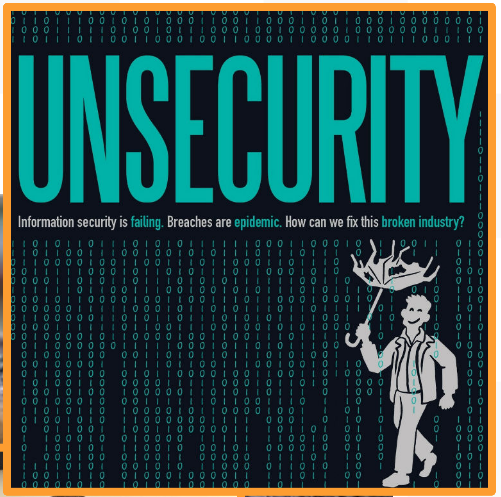
UNSECURITY Podcast

InfoSec Missionaries

Weekly information security podcast airing Monday mornings hosted by Evan Francen and Brad Nigh. In a unique focus on
and Brad discuss information security as an issue that includes cyber security, physical security, as well as administrative co
the author of the book UNSECURITY (publish date December, 2018). Brad is the Director of Professional Services & Innovati
of the industry. Hosting things like FRSecure's Certified Information Systems Security Professional (CISSP) Mentor Program,
together, the chemistry in their banter is sure to delight!

Subscribe

Apple
Google
Overcast
Spotify
YouTube



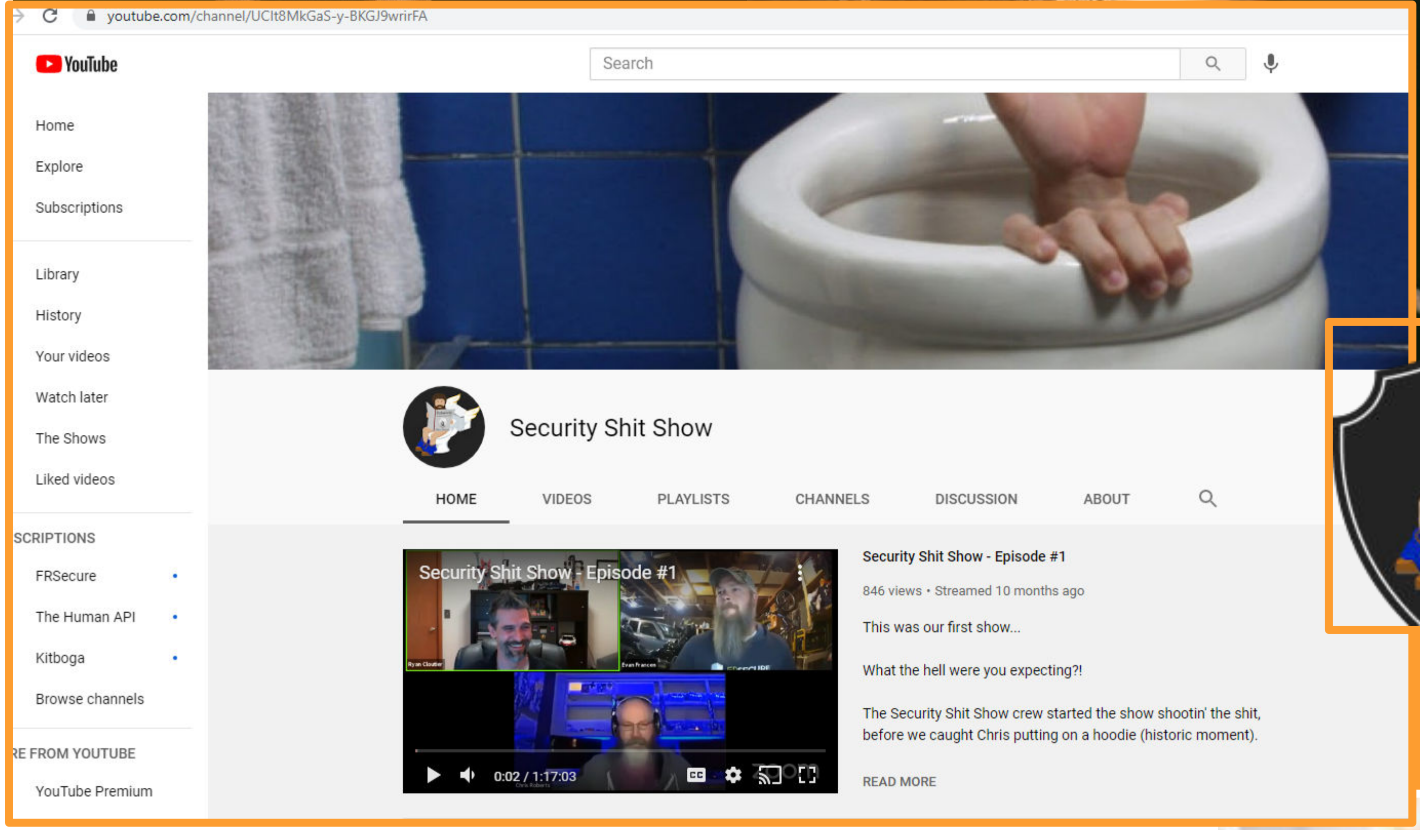
UNSECURITY
Information security is failing. Breaches are epidemic. How can we fix this broken industry?

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About Evan

Security Sh!t Show



youtube.com/channel/UCIt8MkGaS-y-BKGJ9wrirFA

Security Shit Show

Security Shit Show - Episode #1

846 views • Streamed 10 months ago

This was our first show...

What the hell were you expecting?!

The Security Shit Show crew started the show shootin' the shit, before we caught Chris putting on a hoodie (historic moment).

READ MORE

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

Ab

Th

I love people!

Except when they're on the road with me.

The best security people in the world are people who love people.

Information security isn't as much about information or security…

as much as it is about people.

@BradNigh

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About Brad

- 20+ years of overall IT experience, started with FRSecure in 2016
- FRSecure's Principal Security Consultant
- CISSP Mentor Program Lead
- FRSecure Workshop Series Lead
- Co-host of UNSECURITY Podcast with Evan
- CISM, CISSP, CCSFP, CSSA, MCSA: Windows Server 2012, ITIL v.3 Foundations
- ISC²® Safe and Secure Online volunteer
- Wayzata Schools COMPASS program CyberSecurity Mentor
- Passionate about information security and happy to be here!

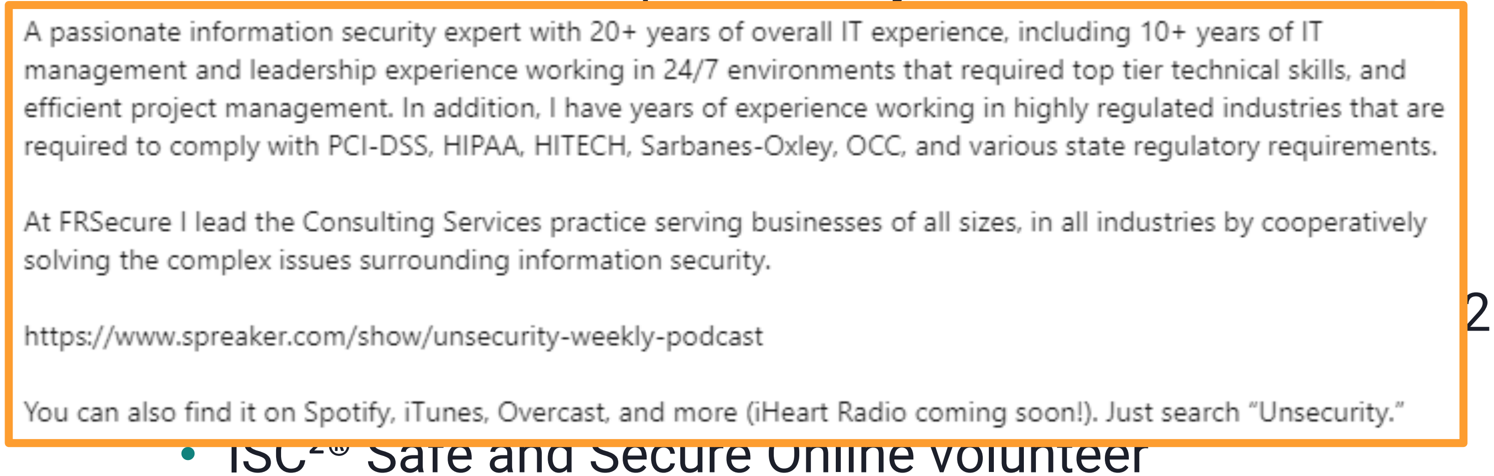
@BradNigh

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About Brad

- 20+ years of overall IT experience, started with FRSecure in 2016
- FRSecure's Principal Security Consultant



A passionate information security expert with 20+ years of overall IT experience, including 10+ years of IT management and leadership experience working in 24/7 environments that required top tier technical skills, and efficient project management. In addition, I have years of experience working in highly regulated industries that are required to comply with PCI-DSS, HIPAA, HITECH, Sarbanes-Oxley, OCC, and various state regulatory requirements.

At FRSecure I lead the Consulting Services practice serving businesses of all sizes, in all industries by cooperatively solving the complex issues surrounding information security.

https://www.spreaker.com/show/unsecurity-weekly-podcast

You can also find it on Spotify, iTunes, Overcast, and more (iHeart Radio coming soon!). Just search "Unsecurity."

2012, ITIL v.3

- ISC²® Safe and Secure Online Volunteer
- Wayzata Schools COMPASS program CyberSecurity Mentor
- Passionate about information security and happy to be here!

#MissionBeforeMoney

@BradNigh

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

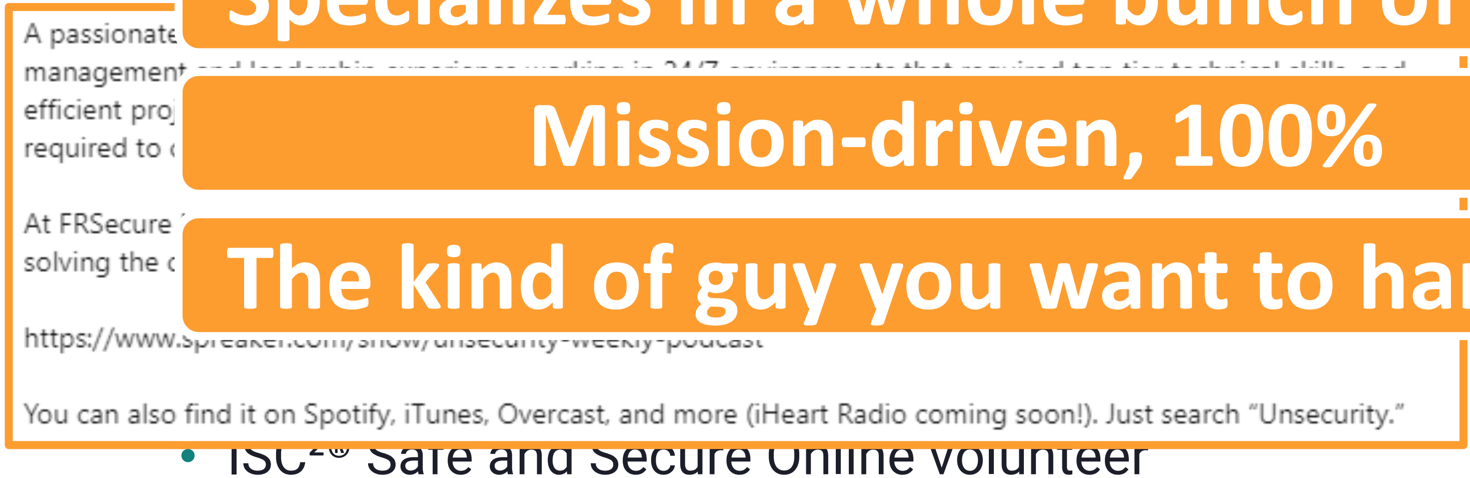
About Brad

- 20+ years of overall IT experience, started with FRSecure in 2016

Specializes in a whole bunch of stuff.

Mission-driven, 100%

The kind of guy you want to hang with!



A passionate
management and leadership experience working in 24/7 environments that required top tier technical skills and
efficient proj
required to

At FRSecure
solving the

https://www.spreaker.com/show/unsecurity-weekly-podcast

You can also find it on Spotify, iTunes, Overcast, and more (iHeart Radio coming soon!). Just search “Unsecurity.”

- ISC^{2}® Safe and Secure Online Volunteer
- Wayzata Schools COMPASS program CyberSecurity Mentor
- Passionate about information security and happy to be here!

@CLOUTIERSEC

INTRODUCTION

About Ryan

SECURITYSTUDIO®

- SecurityStudio's Principal Security Consultant
- The "right hand **and** left hand".
- Seasoned IT Security professional with over 15 years of experience
- Certified Information Systems Security Professional CISSP®
- Held a variety of IT roles during his career including multiple architect and security roles, cloud security, Dev-Ops/Sec-Ops methodology, policy, process, audit and compliance, network and application security architecture
- Performed expert-level work for several fortune 500 companies in health care, financial, and agriculture sectors
- Heavily immersed in K-12 and SLED for the last 3 years

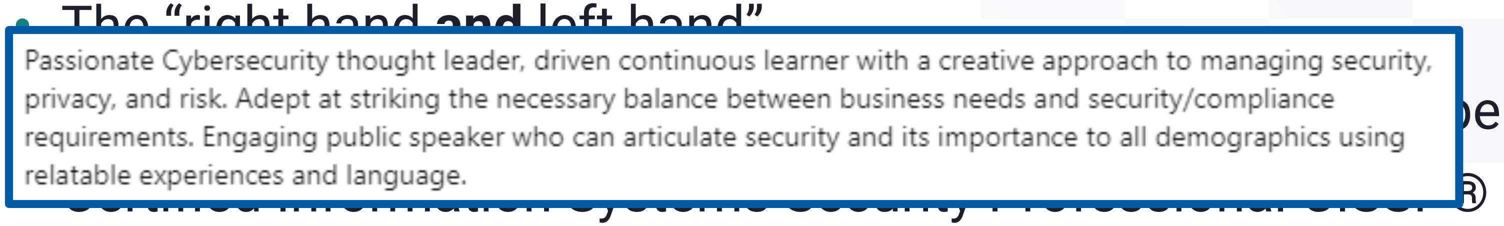
CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About Ryan

SECURITYSTUDIO®

- SecurityStudio’s Principal Security Consultant
- The “right hand **and** left hand”
- erience
- Certified Information Systems Security Professional CISSP®



Passionate Cybersecurity thought leader, driven continuous learner with a creative approach to managing security, privacy, and risk. Adept at striking the necessary balance between business needs and security/compliance requirements. Engaging public speaker who can articulate security and its importance to all demographics using relatable experiences and language.

- Held a variety of IT roles during his career including multiple architect and security roles, cloud security, Dev-Ops/Sec-Ops methodology, policy, process, audit and compliance, network and application security architecture
- Performed expert-level work for several fortune 500 companies in health care, financial, and agriculture sectors
- Heavily immersed in K-12 and SLED for the last 3 years

@CLOUTIERSEC

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About Ryan

SECURITYSTUDIO®

- SecurityStudio's Principal Security Consultant

Prolific keynote speaker.

Mission-driven, 100%

The kind of guy you want to hang with!

policy, process, audit and compliance, network and application security architecture

- Performed expert-level work for several fortune 500 companies in health care, financial, and agriculture sectors
- Heavily immersed in K-12 and SLED for the last 3 years

CISSP® MENTOR PROGRAM – SESSION ONE

YOUR INSTRUCTORS

Nifty group, eh?

@BradNigh

@CLOUTIERSEC

@evanfrancen

Special thank you to the dozen (or so) people who made this happen behind the scenes!

We couldn't be happier that you're here! Thank you for letting us be part of your journey!

FRSECURE®

SECURITYSTUDIO®

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About FRSecure

Expert-level, product agnostic information security management and consulting firm.

- Established in 2008 but didn’t really start until 2010.
- All mission, all the time.
- Information security is about people, and it’s a lot of hard work.
- Seven core values, and ten security principles.
- **Core services include:**
  - vCISO (and related)
  - Information Security Risk Assessment & Management
  - Incident Response (the best!)
  - Technical Services
  - PCI QSA Services
  - Information Security Training & Awareness
  - Whole bunch of other stuff…

100 BEST COMPANIES TO WORK FOR 2018 | minnesota BUSINESS magazine

WE TELL THE TRUTH
ARE COLLABORATIVE
WE ARE COMMITTED TO CONSTANT IMPROVEMENT
ARE SUPPORTIVE & DRIVEN TO SERVE
HAVE BALANCE
WE
WORK HARD & PLAY HARD
ALL BUY INTO WHO WE ARE, WHAT WE DO & WHERE WE'RE GOING
WE DO WHATEVER IT TAKES
ARE DRIVEN TO SERVE OUR CUSTOMERS
FRSECURE

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About FRSecure

Expert-level, product agnostic information security management and consulting firm.

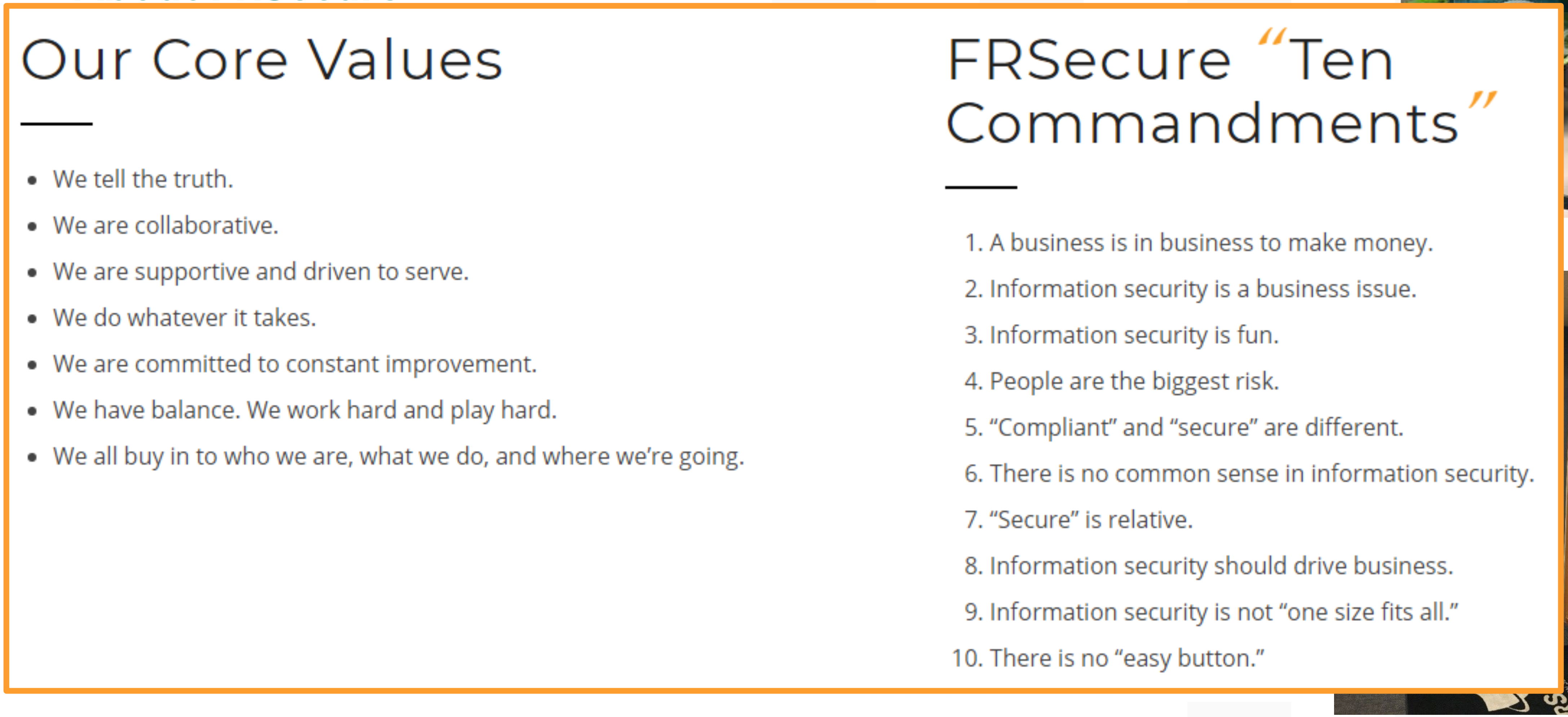
- Established in 2008 but didn't re
- All mission, all the time. ← **Fix the broken industry.**
- Information security is about people, and it's a lot of hard work.
- Seven core values, and ten security principles.
- **Core services include:**
  - vCISO (and related)
  - Information Security Risk Assessment & Management
  - Incident Response (the best!)
  - Technical Services
  - PCI QSA Services
  - Information Security Training & Awareness
  - Whole bunch of other stuff…

WE TELL THE TRUTH
ARE COLLABORATIVE
WE ARE COMMITTED TO CONSTANT IMPROVEMENT
ARE SUPPORTIVE & DRIVEN TO SERVE
HAVE BALANCE
WE
WORK HARD & PLAY HARD
ALL BUY INTO WHO WE ARE, WHAT WE DO & WHERE WE'RE GOING
WE DO WHATEVER IT TAKES
ARE DRIVEN TO SERVE OUR CUSTOMERS
FRSECURE

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About FRSecure



Our Core Values

- We tell the truth.
- We are collaborative.
- We are supportive and driven to serve.
- We do whatever it takes.
- We are committed to constant improvement.
- We have balance. We work hard and play hard.
- We all buy in to who we are, what we do, and where we're going.

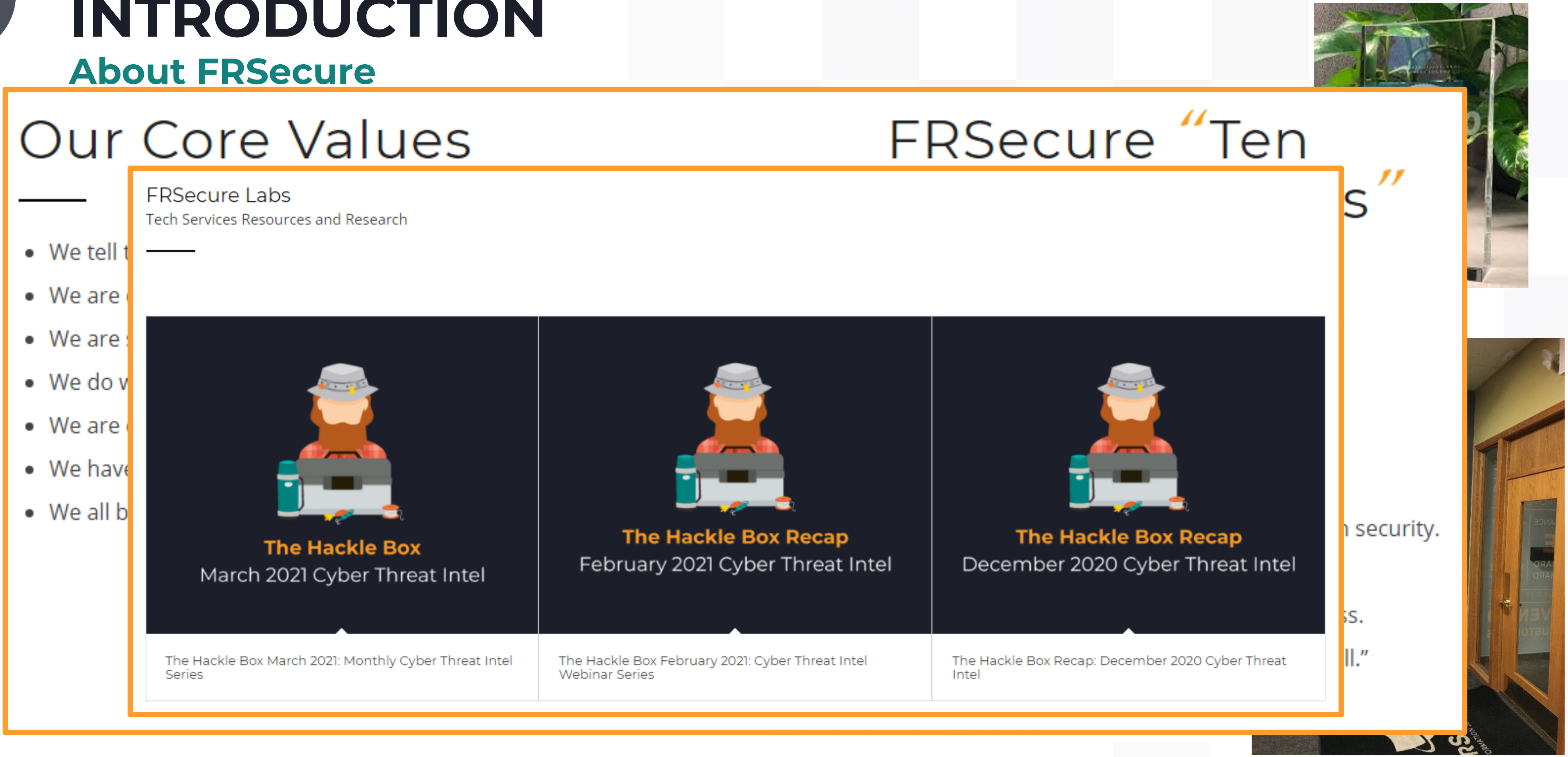
FRSecure "Ten Commandments"

1. A business is in business to make money.
2. Information security is a business issue.
3. Information security is fun.
4. People are the biggest risk.
5. "Compliant" and "secure" are different.
6. There is no common sense in information security.
7. "Secure" is relative.
8. Information security should drive business.
9. Information security is not "one size fits all."
10. There is no "easy button."

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About FRSecure



Our Core Values

- We tell t
- We are
- We are
- We do w
- We are
- We have
- We all b

FRSecure "Ten

s"

n security.

ss.

ll."

FRSecure Labs

Tech Services Resources and Research

The Hackle Box
March 2021 Cyber Threat Intel

The Hackle Box March 2021: Monthly Cyber Threat Intel Series

The Hackle Box Recap
February 2021 Cyber Threat Intel

The Hackle Box February 2021: Cyber Threat Intel Webinar Series

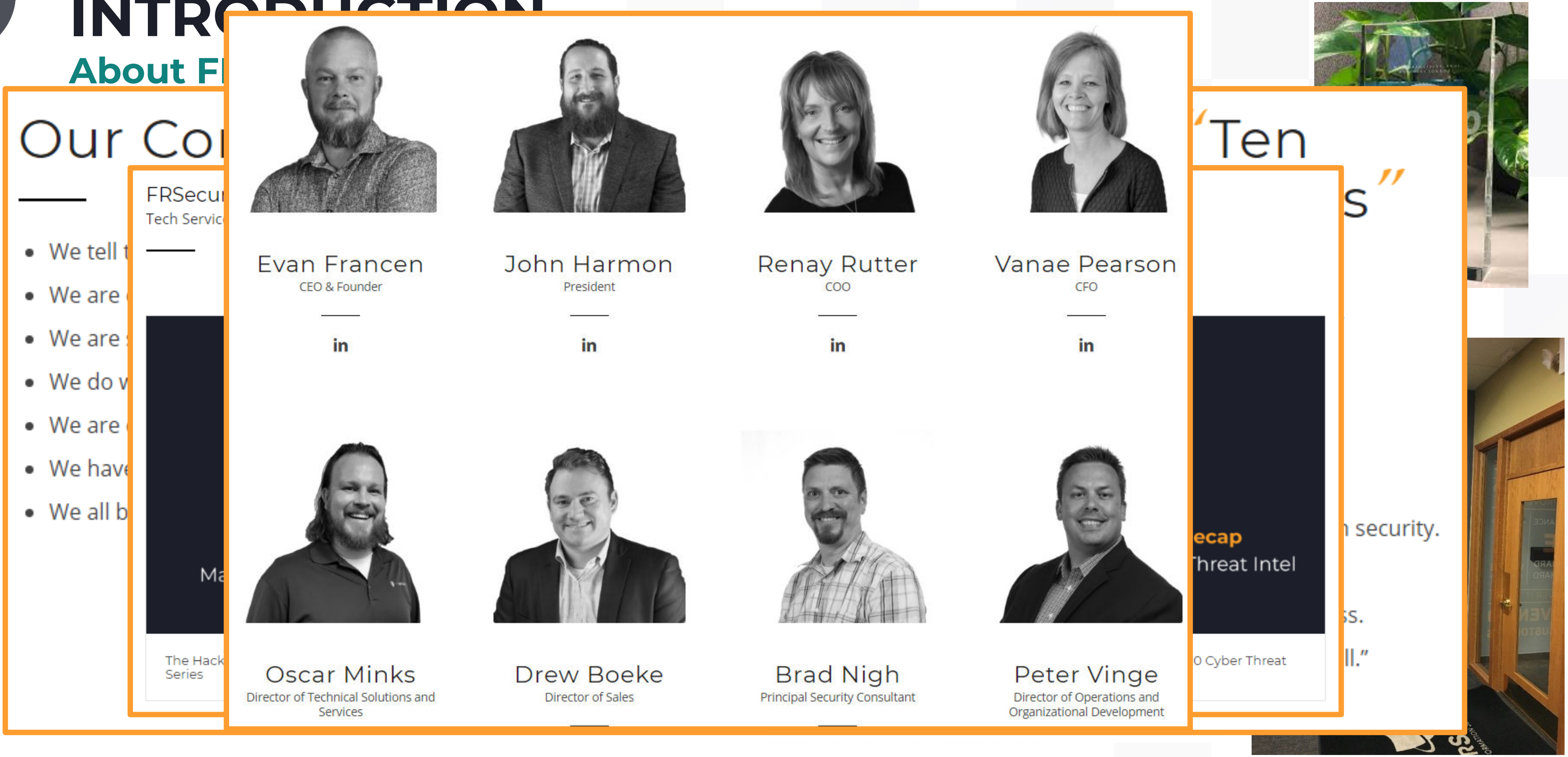
The Hackle Box Recap
December 2020 Cyber Threat Intel

The Hackle Box Recap: December 2020 Cyber Threat Intel

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About FR



Our Co

- We tell t
- We are
- We are
- We do w
- We are
- We have
- We all b

FRSecur

Tech Servic

Ma

The Hack Series

Evan Francen
CEO & Founder
in

John Harmon
President
in

Renay Rutter
COO
in

Vanae Pearson
CFO
in

Oscar Minks
Director of Technical Solutions and Services

Drew Boeke
Director of Sales

Brad Nigh
Principal Security Consultant

Peter Vinge
Director of Operations and Organizational Development

"Ten

s"

ecap

Threat Intel

0 Cyber Threat

security.

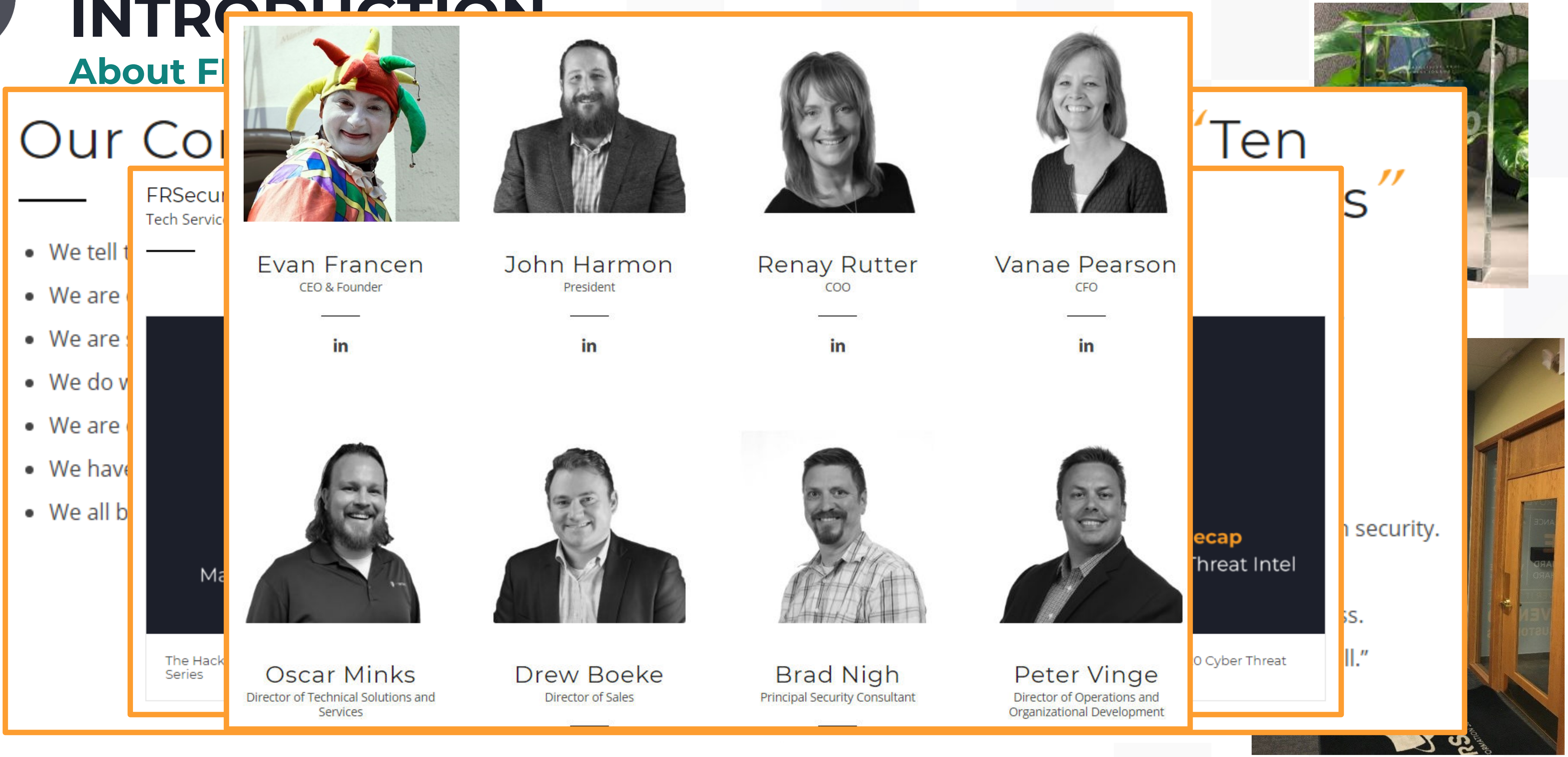
ss.

ll."

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About FR



Our Co

- We tell t
- We are
- We are
- We do w
- We are
- We have
- We all b

FRSecur
Tech Servic

Ma

The Hack
Series

Evan Francen
CEO & Founder

in

John Harmon
President

in

Renay Rutter
COO

in

Vanae Pearson
CFO

in

Oscar Minks
Director of Technical Solutions and Services

Drew Boeke
Director of Sales

Brad Nigh
Principal Security Consultant

Peter Vinge
Director of Operations and Organizational Development

“Ten
s”

ecap
Threat Intel

0 Cyber Threat

security.

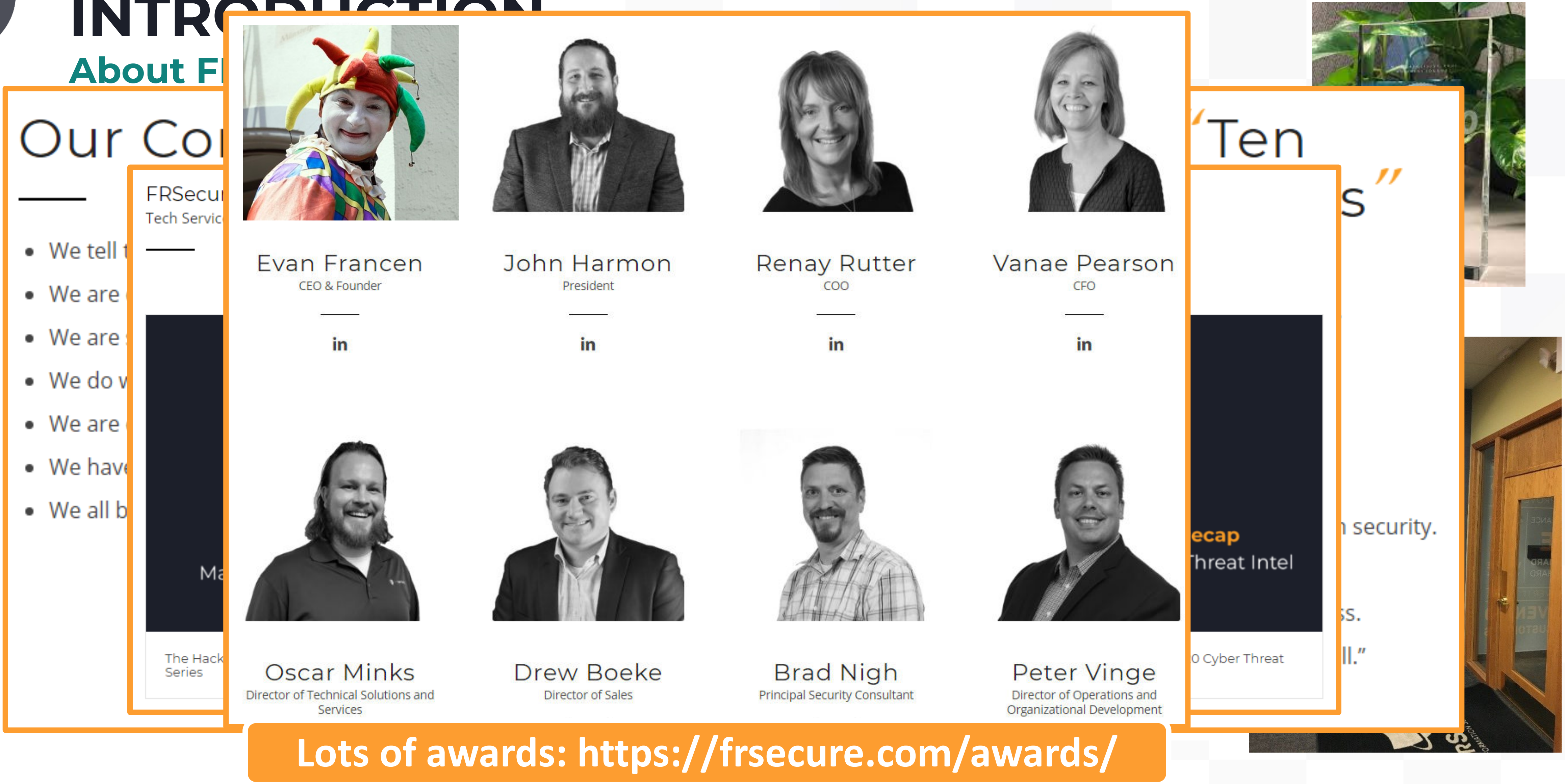
ss.

ll.”

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About F



Evan Francen
CEO & Founder
in

John Harmon
President
in

Renay Rutter
COO
in

Vanae Pearson
CFO
in

Oscar Minks
Director of Technical Solutions and Services

Drew Boeke
Director of Sales

Brad Nigh
Principal Security Consultant

Peter Vinge
Director of Operations and Organizational Development

Lots of awards: https://frsecure.com/awards/

#MissionBeforeMoney

Did you notice this?

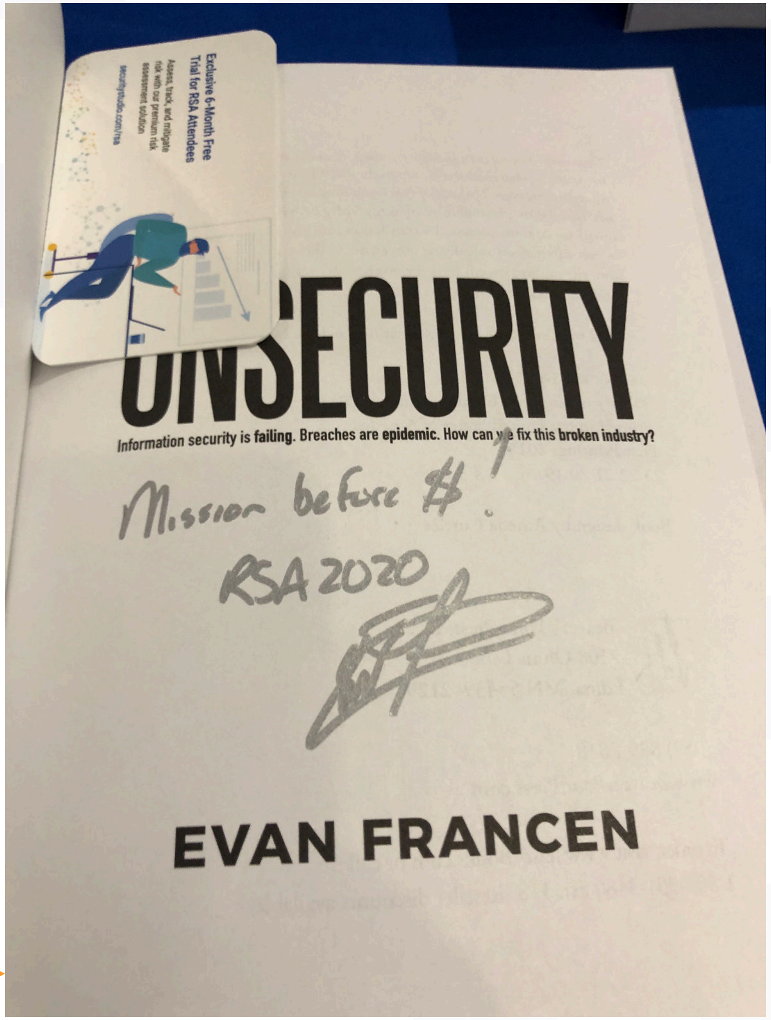
CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About FRSecure

What's the #MissionBeforeMoney thing?

Much (not all) of our industry.



Exclusive 6-Month Free
Trial for RSA Attendees
Assess, track, and mitigate
risk with our premium risk
assessment solution
securitystudio.com/rsa

UNSECURITY

Information security is failing. Breaches are epidemic. How can we fix this broken industry?

Mission before $!

RSA 2020

EVAN FRANCEN

US

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About SecurityStudio

SECURITYSTUDIO®

Oh yeah, these guys too!

Dedicated to Simplifying Information Security for the Masses

- SecurityStudio (or **S^2**) is a Software as a Service (or SaaS) company dedicated to making safety, privacy, and cybersecurity simple and attainable for everyone.
- The **S^2** platform is built around a simple language called the **S^2Score** and we make fundamental tools available to the market including:
- **S^2Org** - the organizational information security risk management tool used by organizations of all sizes, but primarily developed for small to medium-sized businesses.
- **S^2Vendor** - the simple vendor/third-party information security risk management tool, integrated with S2Org for optimal efficiency.
- **S^2School** - the education-specific version of S2Org, used by K12 and higher education institutions everywhere.
- **S^2Team** - the information security portal leveraged by organizations to help their employees at home (and ultimately help themselves too).
- **S^2Me** - the **FREE** safety and cybersecurity risk management tool built for everyday people to use at home for better personal and family protection.

> *"Complexity is the enemy of security" - Bruce Schneier*

CISSP® MENTOR PROGRAM – SESSION ONE

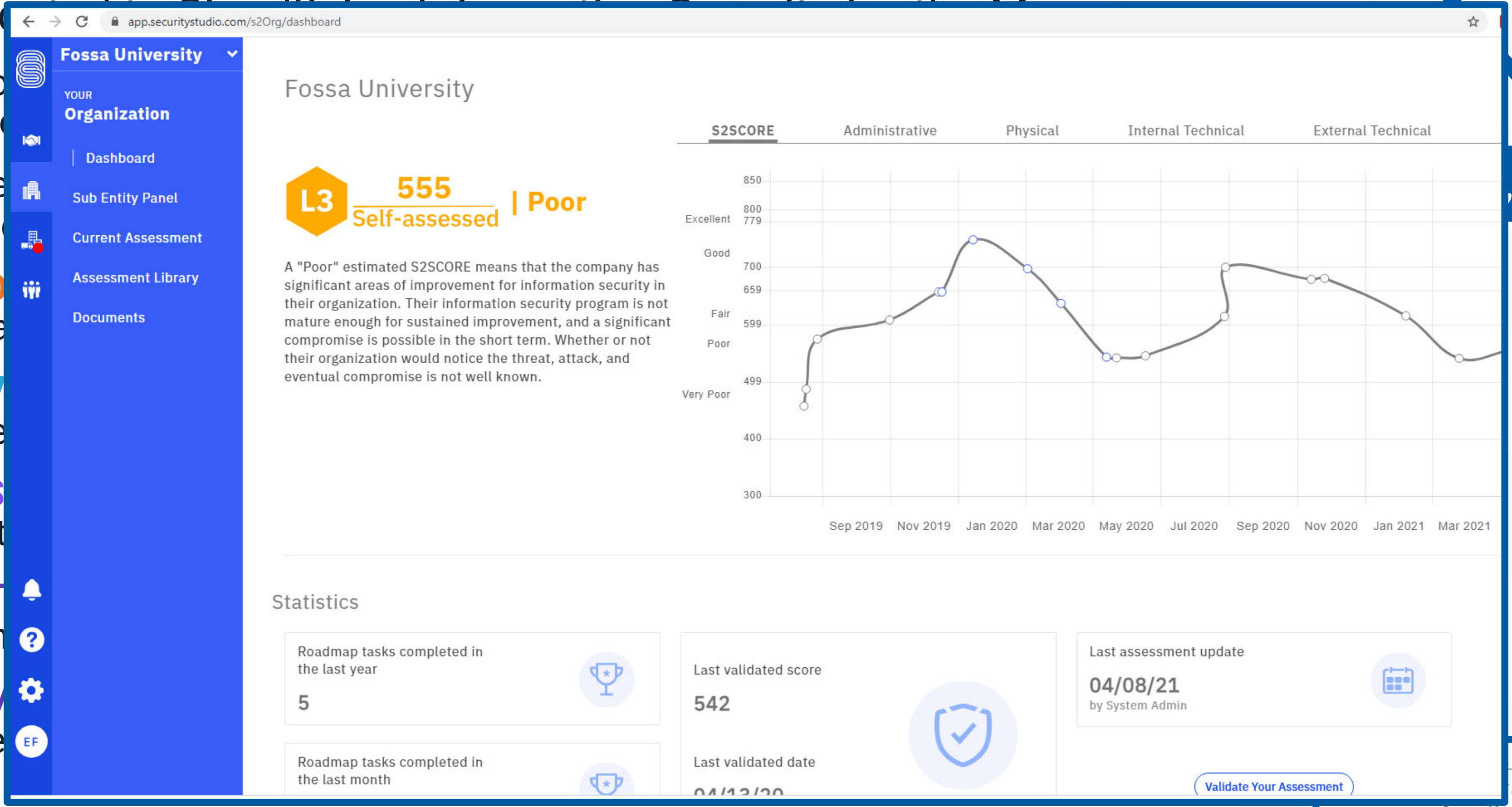
INTRODUCTION

About SecurityStudio

SECURITYSTUDIO®

Dedi

- Sec saf
- The fun
- S^2O of a
- S^2V inte
- S^2S inst
- S^2T at h
- S^2M use



Fossa University

L3 555 Self-assessed | Poor

A "Poor" estimated S2SCORE means that the company has significant areas of improvement for information security in their organization. Their information security program is not mature enough for sustained improvement, and a significant compromise is possible in the short term. Whether or not their organization would notice the threat, attack, and eventual compromise is not well known.

Statistics

Roadmap tasks completed in the last year
5

Last validated score
542

Last assessment update
04/08/21
by System Admin

Roadmap tasks completed in the last month

Last validated date
04/13/20

, these guys too!

y is the enemy of security" - Bruce Schneier

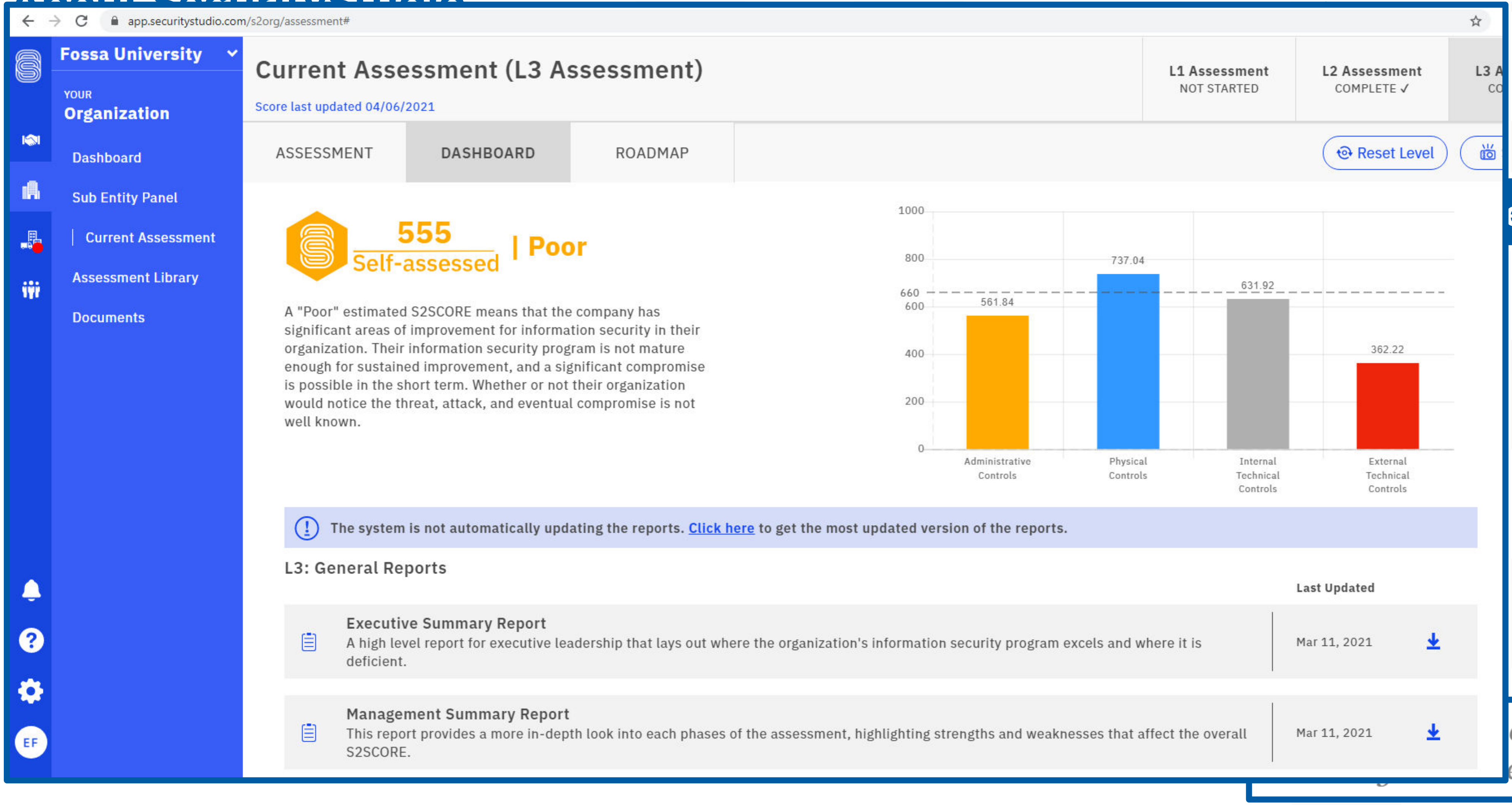
FRSECURE

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About SecurityStudio

SECURITYSTUDIO®



Current Assessment (L3 Assessment)

Score last updated 04/06/2021

555 Self-assessed | Poor

A "Poor" estimated S2SCORE means that the company has significant areas of improvement for information security in their organization. Their information security program is not mature enough for sustained improvement, and a significant compromise is possible in the short term. Whether or not their organization would notice the threat, attack, and eventual compromise is not well known.

The system is not automatically updating the reports. Click here to get the most updated version of the reports.

L3: General Reports

	Last Updated
Executive Summary Report A high level report for executive leadership that lays out where the organization's information security program excels and where it is deficient.	Mar 11, 2021
Management Summary Report This report provides a more in-depth look into each phases of the assessment, highlighting strengths and weaknesses that affect the overall S2SCORE.	Mar 11, 2021

e guys too!

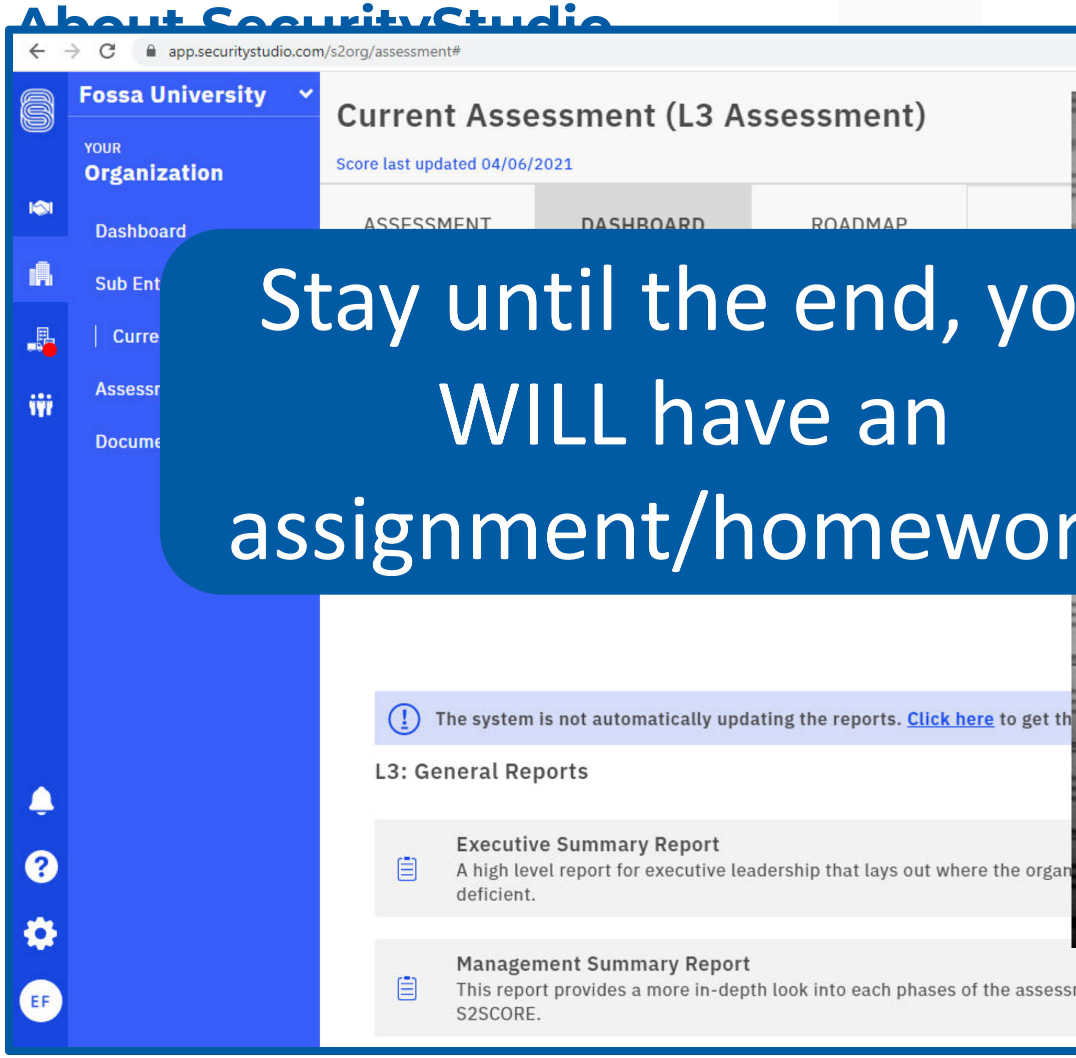
e enemy of
e Schneier

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

About SecurityStudio

SECURITYSTUDIO®



Current Assessment (L3 Assessment)

Score last updated 04/06/2021

The system is not automatically updating the reports. Click here to get th

L3: General Reports

Executive Summary Report
A high level report for executive leadership that lays out where the organ
deficient.

Management Summary Report
This report provides a more in-depth look into each phases of the assessment, highlighting strengths and weaknesses that affect the overall S2SCORE.

Mar 11, 2021

Stay until the end, you WILL have an assignment/homework!

e enemy of
e Schneier

CISSP® MENTOR PROGRAM – SESSION ONE

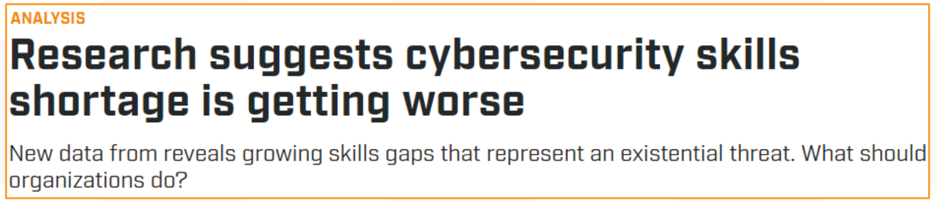
INTRODUCTION

About us.

CISSP® MENTOR PROGRAM – SESSION ONE

OUR SEVERE TALENT SHORTAGE PROBLEM…

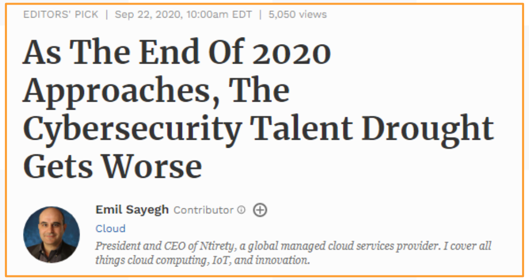
- Chapter 10 – UNSECURITY
- No shortage of stories about our impending doom.
- Another take (from me) - No Easy Button Solution To Cybersecurity's Skills Shortage (https://www.cybersecurityintelligence.com/blog/no-easy-button-solution-to-cybersecuritys-skills-shortage-4150.html)
- Some people claim that there is no shortage, or that it's overhyped.
- The truth is probably somewhere in the middle, but there is plenty of opportunity!



ANALYSIS

Research suggests cybersecurity skills shortage is getting worse

New data from reveals growing skills gaps that represent an existential threat. What should organizations do?



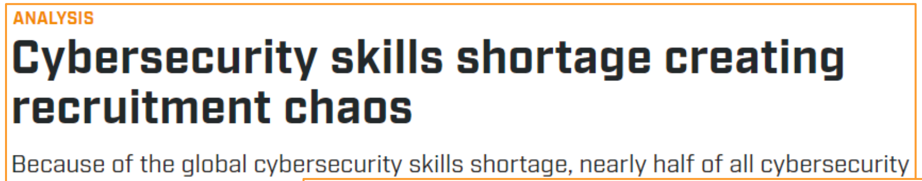
EDITORS' PICK | Sep 22, 2020, 10:00am EDT | 5,050 views

As The End Of 2020 Approaches, The Cybersecurity Talent Drought Gets Worse

Emil Sayegh Contributor

Cloud

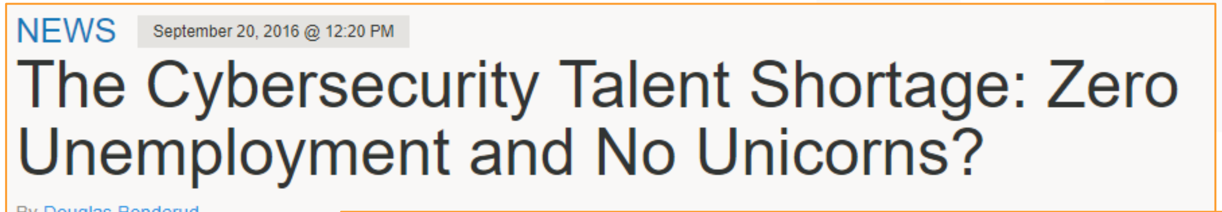
President and CEO of Ntirety, a global managed cloud services provider. I cover all things cloud computing, IoT, and innovation.



ANALYSIS

Cybersecurity skills shortage creating recruitment chaos

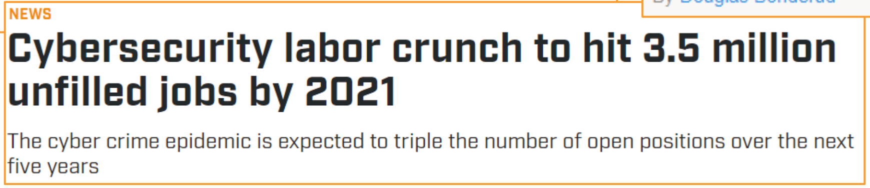
Because of the global cybersecurity skills shortage, nearly half of all cybersecurity professionals are solicited



NEWS September 20, 2016 @ 12:20 PM

The Cybersecurity Talent Shortage: Zero Unemployment and No Unicorns?

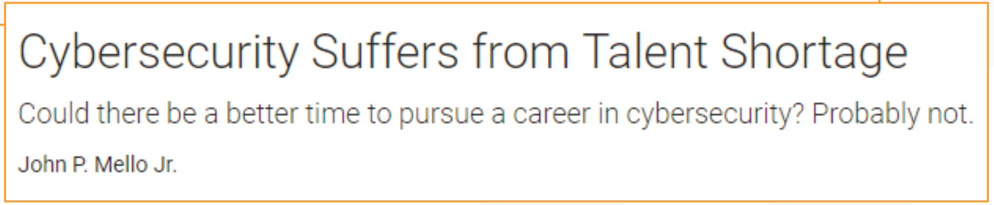
By Douglas Bonderud



NEWS

Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021

The cyber crime epidemic is expected to triple the number of open positions over the next five years



Cybersecurity Suffers from Talent Shortage

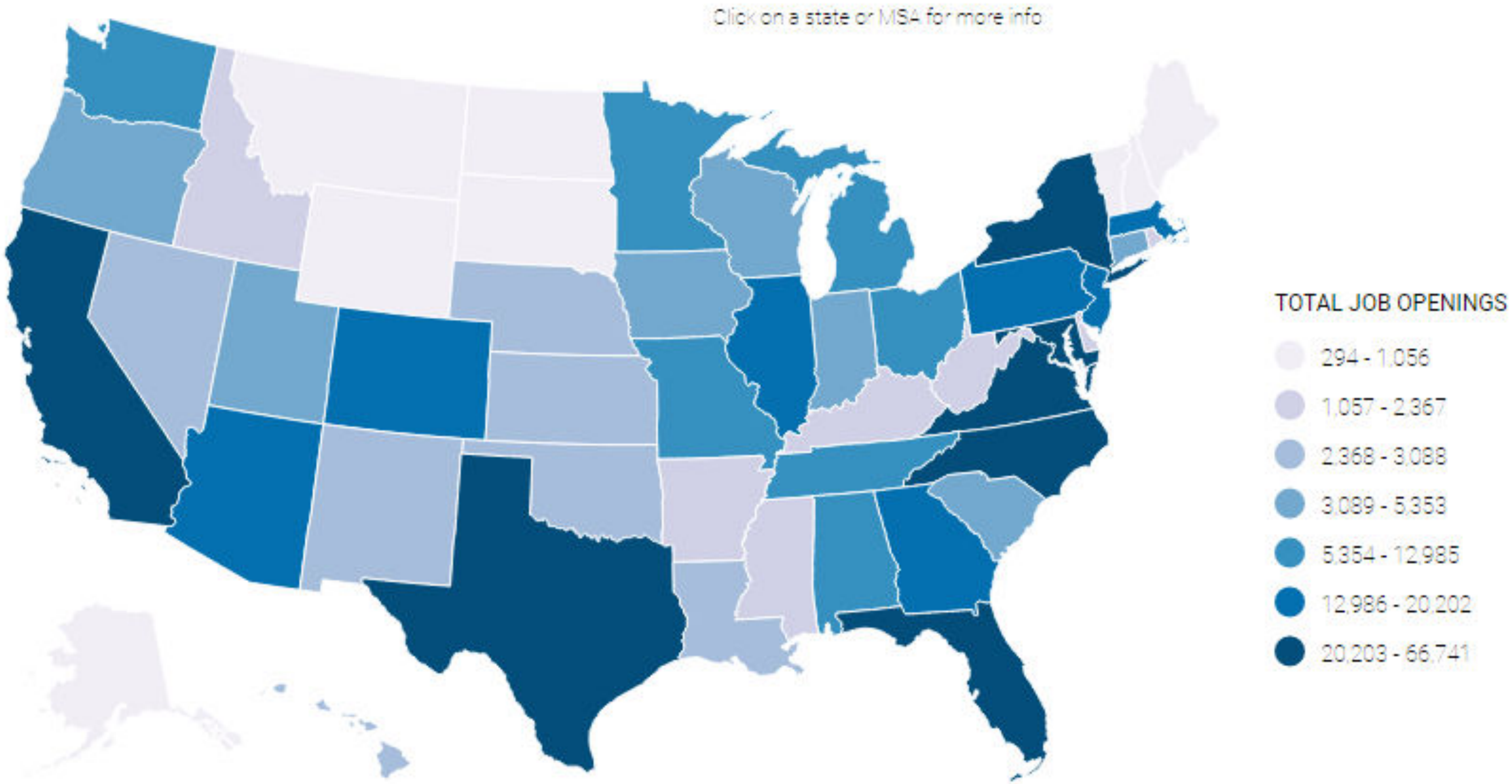
Could there be a better time to pursue a career in cybersecurity? Probably not.

John P. Mello Jr.

CISSP® MENTOR PROGRAM – SESSION ONE

OUR SEVERE TALENT SHORTAGE PROBLEM…

Some truth. Total Job Openings.

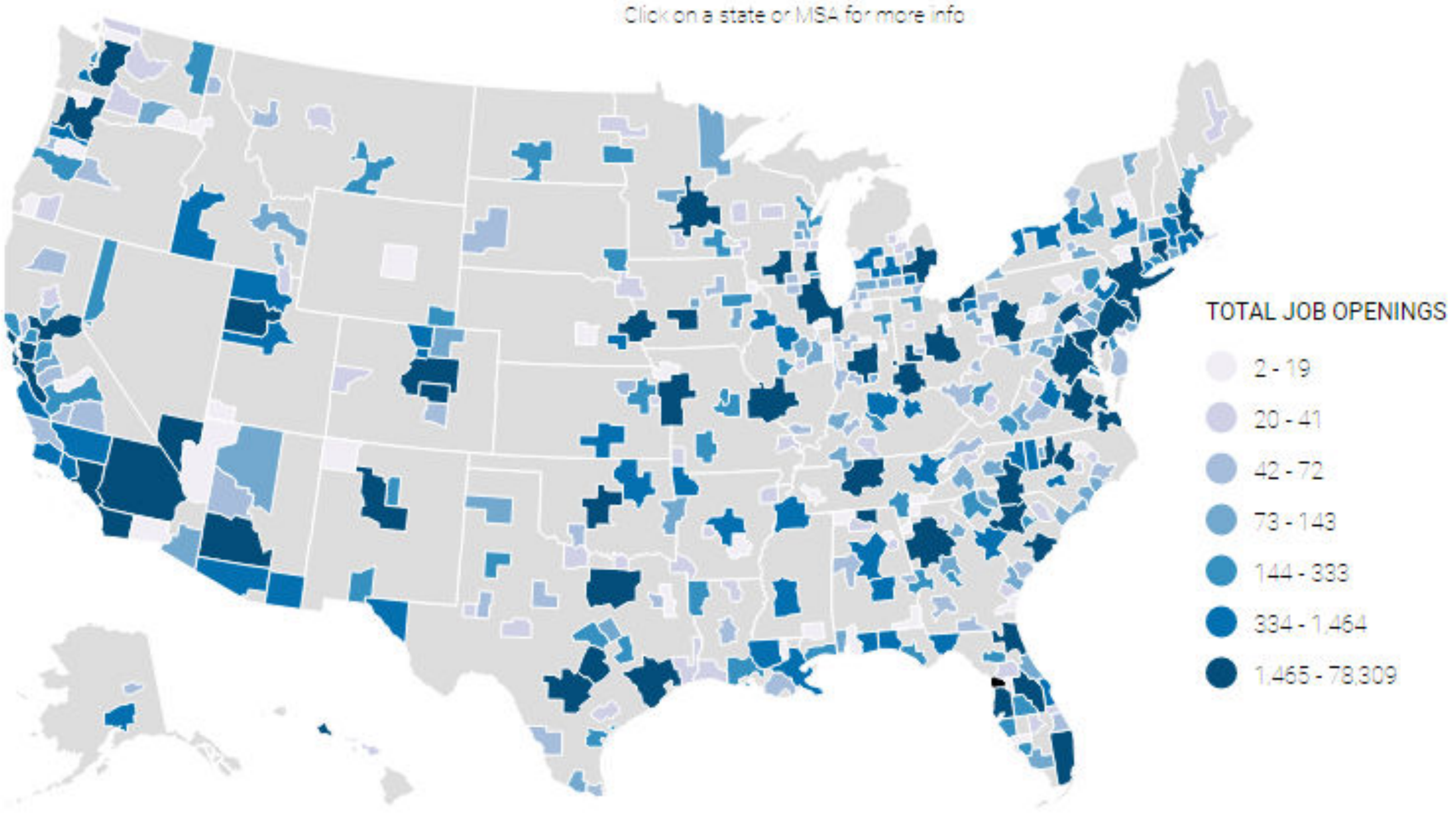


Source: CyberSeek – www.cyberseek.org

CISSP® MENTOR PROGRAM – SESSION ONE

OUR SEVERE TALENT SHORTAGE PROBLEM…

Some truth. Total Job Openings.

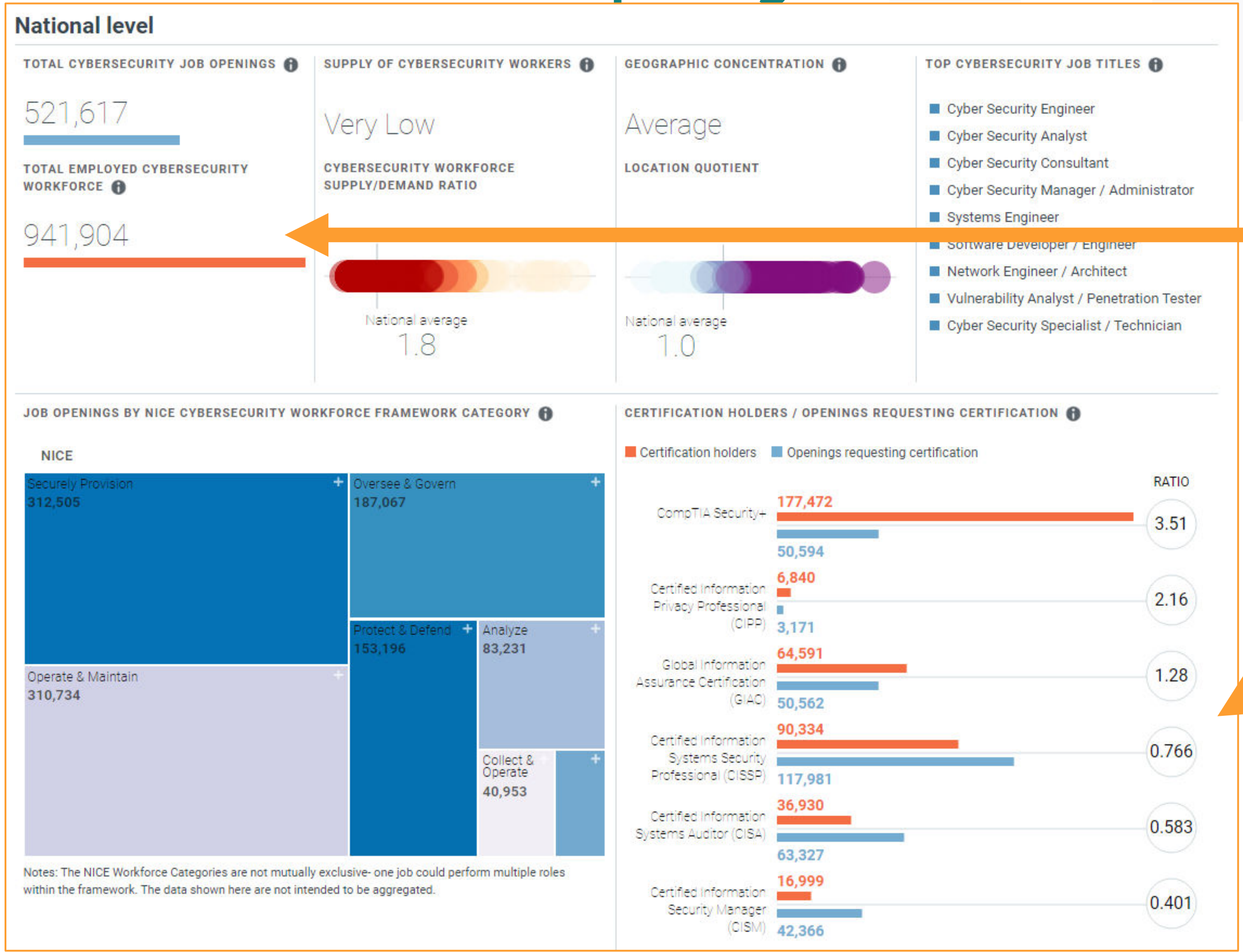


Source: CyberSeek – www.cyberseek.org

CISSP® MENTOR PROGRAM – SESSION ONE

OUR SEVERE TALENT SHORTAGE PROBLEM…

Some truth. Total Job Openings.



National level

TOTAL CYBERSECURITY JOB OPENINGS

521,617

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

941,904

SUPPLY OF CYBERSECURITY WORKERS

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO

National average 1.8

GEOGRAPHIC CONCENTRATION

Average

LOCATION QUOTIENT

National average 1.0

TOP CYBERSECURITY JOB TITLES

- Cyber Security Engineer
- Cyber Security Analyst
- Cyber Security Consultant
- Cyber Security Manager / Administrator
- Systems Engineer
- Software Developer / Engineer
- Network Engineer / Architect
- Vulnerability Analyst / Penetration Tester
- Cyber Security Specialist / Technician

JOB OPENINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY

NICE

Category	Openings
Securely Provision	312,505
Oversee & Govern	187,067
Protect & Defend	153,196
Analyze	83,231
Operate & Maintain	310,734
Collect & Operate	40,953

Notes: The NICE Workforce Categories are not mutually exclusive- one job could perform multiple roles within the framework. The data shown here are not intended to be aggregated.

CERTIFICATION HOLDERS / OPENINGS REQUESTING CERTIFICATION

🟥 Certification holders 🟦 Openings requesting certification

	Certification holders	Openings requesting certification	RATIO
CompTIA Security+	177,472	50,594	3.51
Certified Information Privacy Professional (CIPP)	6,840	3,171	2.16
Global Information Assurance Certification (GIAC)	64,591	50,562	1.28
Certified Information Systems Security Professional (CISSP)	90,334	117,981	0.766
Certified Information Systems Auditor (CISA)	36,930	63,327	0.583
Certified Information Security Manager (CISM)	16,999	42,366	0.401

This.

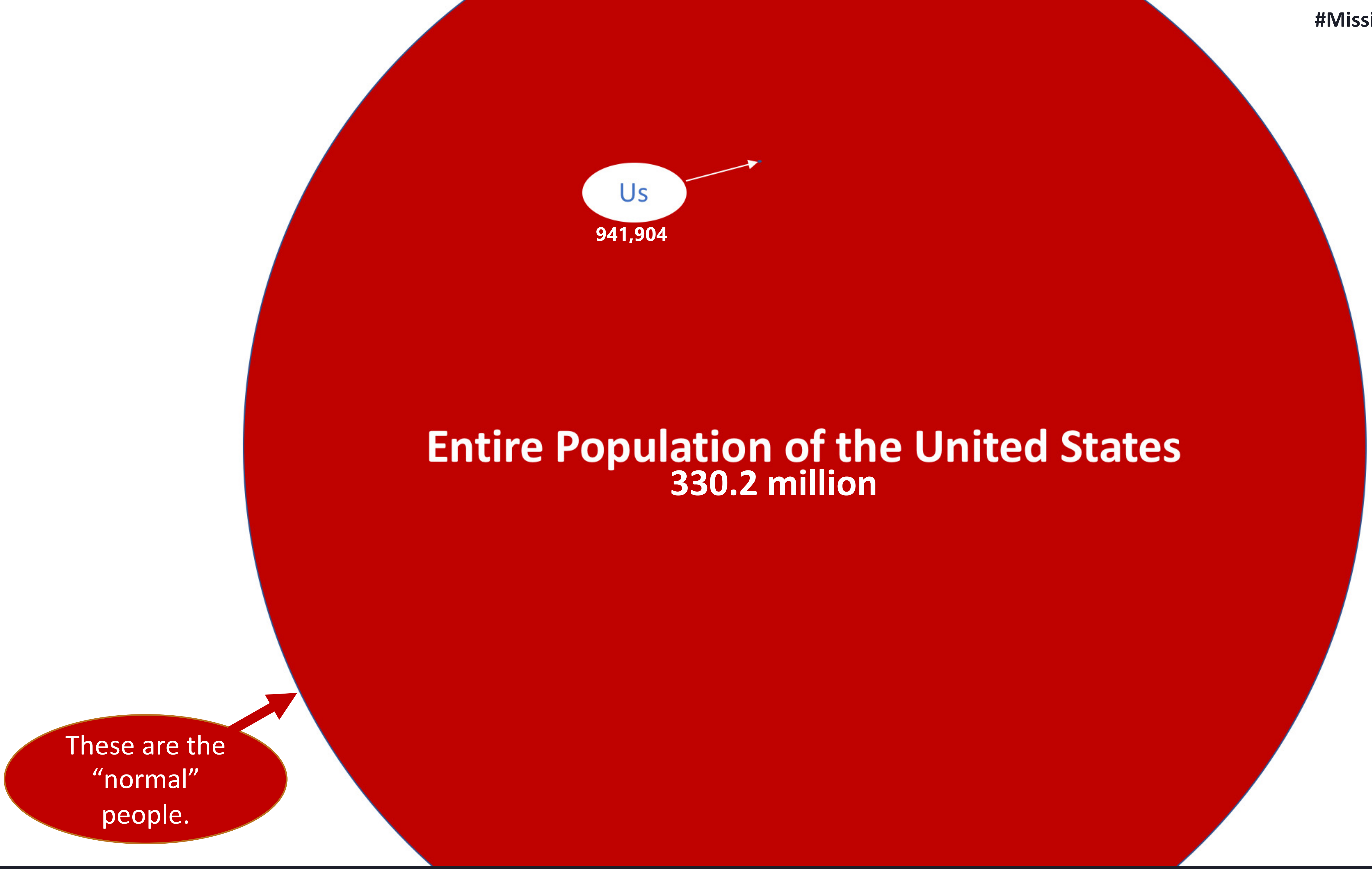
In context

This.

Source: CyberSeek – www.cyberseek.org

FRSECURE

#MissionBeforeMoney



Us

941,904

Entire Population of the United States

330.2 million

These are the “normal” people.

OUR SEVERE TALENT SHORTAGE PROBLEM…

Some truth.

- Report from Cybersecurity Ventures estimates there will be 3.5 million unfilled cybersecurity jobs by 2021, up from 1 million openings in 2019.
- ISACA predicts there will be a global shortage of two million cyber security professionals by 2019. (CAME TRUE)
- 70% of organizations report being impacted by the worker shortage
- 'We are outnumbered' — cybersecurity pros face a huge staffing shortage as attacks surge during the pandemic
- American salary for cybersecurity professionals is $90,000 a year and those who hold security certifications can make more.
- Cyber crime is expected to cost the world $6 trillion by 2021.

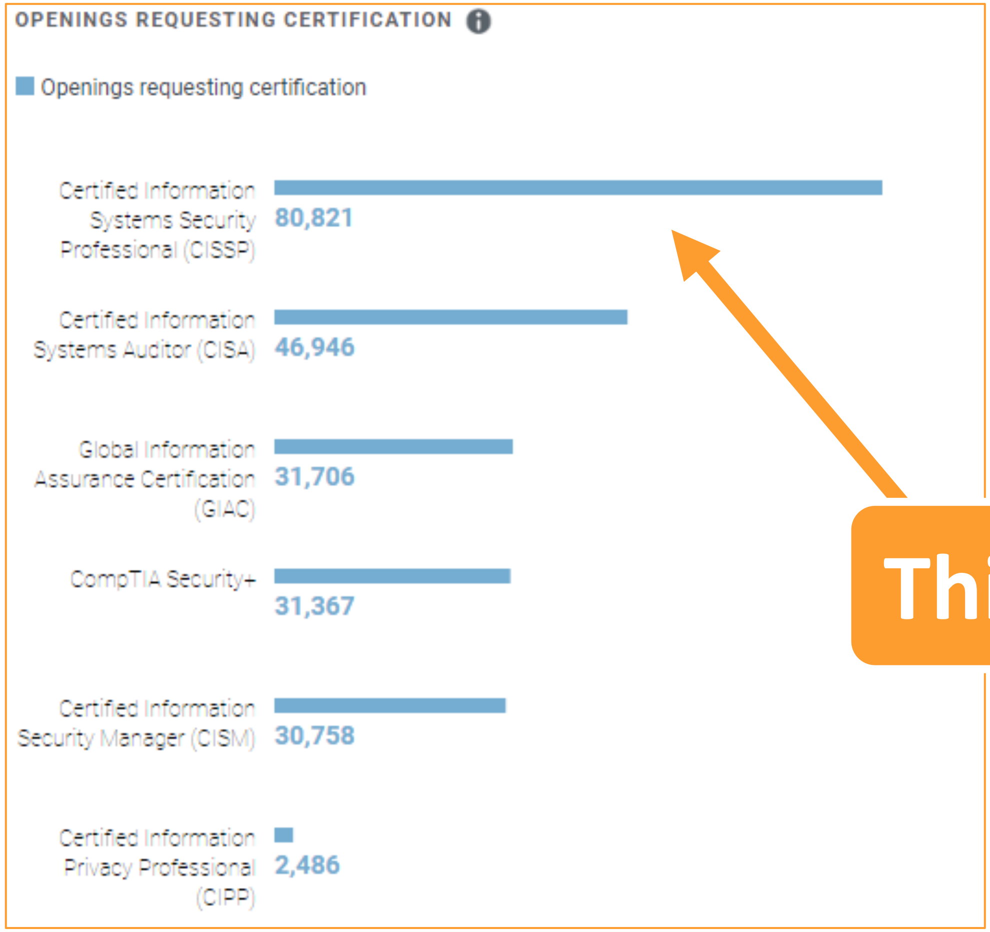
"Lack of Cybersecurity Talent is a Systemic Issue" - Dave Barton, Security Magazine

CISSP® MENTOR PROGRAM – SESSION ONE

OUR SEVERE TALENT SHORTAGE PROBLEM…

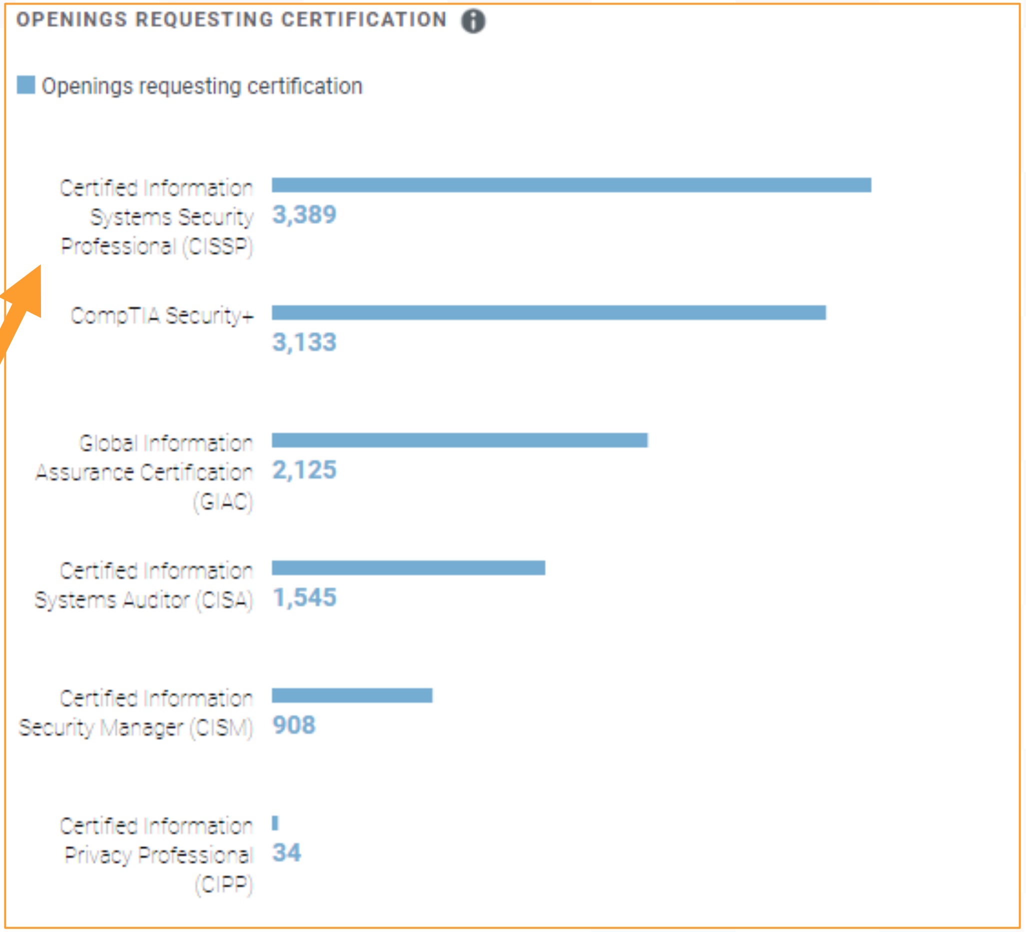
Some truth.

Private Sector



This.

Public Sector



OUR SEVERE TALENT SHORTAGE PROBLEM…

"Good" Security Talent

- What makes a "good" information security professional?
- Backlash from the Equifax Breach, noted that Susan Mauldin (former Chief Security Officer) had a music degree; therefore, she must have been unqualified.

"a problem emerges: according to LinkedIn, Mauldin's stated educational background has no security or technology credentials and consists of…. a bachelor's degree in music composition (magna cum laude) and a Master of Fine Arts degree in music composition (summa cum laude), both from the University of Georgia. Once again, this is the person who was in charge of keeping your personal and financial data safe — and whose failure to do that have put 143 million at risk from identity theft and fraud."

(Source: https://www.zerohedge.com/news/2017-09-15/another-equifax-coverup-did-company-scrub-its-chief-security-officer-was-music-major)

OUR SEVERE TALENT SHORTAGE PROBLEM…

“Good” Security Talent

- What makes a “good” information security professional?
- Backlash from the Equifax Breach, noted that Susan Mauldin (former Chief Security Officer) had a music degree; therefore, she must have been unqualified.

> *When Congress hauls in Equifax CEO Richard Smith to grill him, it can start by asking why he put someone with degrees in music in charge of the company’s data security.*
>
> *And then they might also ask him if anyone at the company has been involved in efforts to cover up Susan Mauldin’s lack of educational qualifications since the data breach became public.*
>
> *It would be fascinating to hear Smith try to explain both of those extraordinary items.*
>
> *(Source: https://www.marketwatch.com/story/equifax-ceo-hired-a-music-major-as-the-companys-chief-security-officer-2017-09-15)*

OUR SEVERE TALENT SHORTAGE PROBLEM…

“Good” Security Talent

- What makes a “good” information security professional?
- Some people believe that you cannot be “good” without a technical degree, others believe that you cannot be “good” without certifications like a CISSP, CISM, etc.
- There are thousands of awesome security practitioners who have no information security degree whatsoever.

Defining “Good”

- At FRSecure we “grow talent”.
- There are three things that create talent:
  - **Intangibles** – the things you can’t teach.
  - **Education** – the “book smarts”. Education can come in a variety of forms; degree programs, books, in-person instruction, mentorship, certification preparation, etc.
  - **Experience** – the “street smarts”. The best way to gain experience is by doing.

This is #1, non-negotiable.

The three ingredients are not mutually exclusive and there are all sorts of ways.

OUR SEVERE TALENT SHORTAGE PROBLEM…

Supply and Demand - acquisition, retention, and our culture

- **Supply** – we don't have enough information security people.
- **Acquisition** – we can't find enough good information security people for ourselves.
- **Retention** – we can't keep good information security people for ourselves (and in some cases, in our industry).
- **Culture** – we have a "bro culture" problem that isn't helping.
  - Intimidating
  - Egotistical
  - Lacking minority perspective.

Thankfully, this has gotten better the past few years, but we're NOT DONE.

OUR SEVERE TALENT SHORTAGE PROBLEM…

Supply and Demand - acquisition, retention, and our culture

- Two sources; people willing to change careers, and younger people entering the workforce.
- **Career Changers** - If you were interested in getting into our field, where would you start?
  - A bachelor's degree in cyber security will cost somewhere between $20,000 - $60,000, or more. This might get you an entry-level job. A master's degree will cost much more. (Source: https://www.onlineu.org/most-affordable-colleges/cyber-security-degrees)
  - Certification? Training to pass the CISSP® exam can range from $2,000 - $5,000, or more, and the exam itself will set you back another $699.
  - Cost is a barrier to entry. Most people don't have this amount of money lying around.
- **Younger People** – Not enough education options (getting better, but not fast enough).

OUR SEVERE TALENT SHORTAGE PROBLEM…

Supply and Demand - acquisition, retention, and our culture

- Early Education – schools are starting programs, and they're working. Many examples.
- Free Education
  - **FRSecure's Mentor Program** (https://frsecure.com/cissp-mentor-program/)
  - **SANS Cyber Aces Online** (http://www.cyberaces.org/courses/)
  - **Cybrary** (https://www.cybrary.it/catalog/)
  - **Cyber Degrees** (https://www.cyberdegrees.org/)
  - Many more showed up during the pandemic…
- Mentorship – no single dominant program; this requires more of us giving back.
- Hire Intangibles – and train/educate for the rest. Can be a good acquisition strategy too.
- Internships – becoming more popular, but we need more.

OUR SEVERE TALENT SHORTAGE PROBLEM…

Supply and Demand - acquisition, retention, and our culture

- Our industry culture is not always conducive to attracting and retaining talent.
- Some of the results of our culture are gender inequity and minority inequity.
  - Women make up 49.56% of the world's population, but only make up 24% (up from 11%) of the information security workforce.
  - 26% of our workforce is non-Caucasian (or "white") male.
  - People of color make up less than 20% of the information security analyst jobs in the U.S.
  - 8% of VC investors are women and fewer than 1% are Black

REMEMBER: Difficult problems are best solved using diverse perspectives.

"In a survey of 580 scheduled attendees of the Black Hat 2017 conference to be held in Las Vegas, Black Hat found that 71% of respondents felt their companies lacked sufficient staff to defend itself against current cyberthreats. And, although less than half of respondents (45%) were "concerned" about the shortage of women and minorities in the information security"

OUR SEVERE TALENT SHORTAGE PROBLEM…

Supply and Demand - acquisition, retention, and our culture

- Since our industry is so male dominated, there's a "bro culture" that exists.
  - *"It's a very male-dominated culture." "It can be a little more crass, a little bit more rough and maybe some … females don't like that, and it is off-putting."* – Ellison Anne Williams, Ph.D., founder and chief executive of Enveil, a Fulton, Md., data security company.
- It's not only the people in our industry that contribute to the problem. Customers, clients, and other normal people also assume that information security is a male sport.
  - *"They have clients who won't speak directly to them, It's the assumption that the woman is not the lead on the project. They just default to speaking to the men."* - Leah Figueroa, lead data engineer at Gravwell, a data analytics company out of Coeur D'Alene, Idaho (Source: http://www.govtech.com/workforce/Why-Are-So-Few-Women-in-Cybersecurity.html)
- This culture didn't start in our industry and it's not exclusive to our industry either.

OUR SEVERE TALENT SHORTAGE PROBLEM…

Supply and Demand - acquisition, retention, and our culture

- Promote and participate in more diversity initiatives and programs.
- Studies prove the more diverse work groups produce more creative a better results.
- A partial list of resources for women:
  - **SANS CyberTalent Immersion Academy for Women** - https://www.sans.org/cybertalent/immersion-academy
  - **Computer Science for Cyber Security (CS4CS) Summer Program for High School Women** - http://engineering.nyu.edu/k12stem/cs4cs/
  - **Women's Society of Cyberjutsu (WSC)** - http://womenscyberjutsu.org/
  - **Women in Cyber Security (WiCyS)** - https://www.wicys.net/

OUR SEVERE TALENT SHORTAGE PROBLEM…

Supply and Demand - acquisition, retention, and our culture

- Promote and participate in more diversity initiatives and programs.
- Studies prove the more diverse work groups produce more creative a better results.
- A partial list of resources for other underserved groups:
  - **Blacks in Cybersecurity** - https://www.blacksincyberconf.com/
  - **Black Cybersecurity Association -** https://blackcybersecurityassociation.org/
  - **International Consortium of Minority Cybersecurity Professionals** - https://www.icmcp.org/
  - **Others? Start one!**

CISSP® MENTOR PROGRAM – SESSION ONE

INTRODUCTION

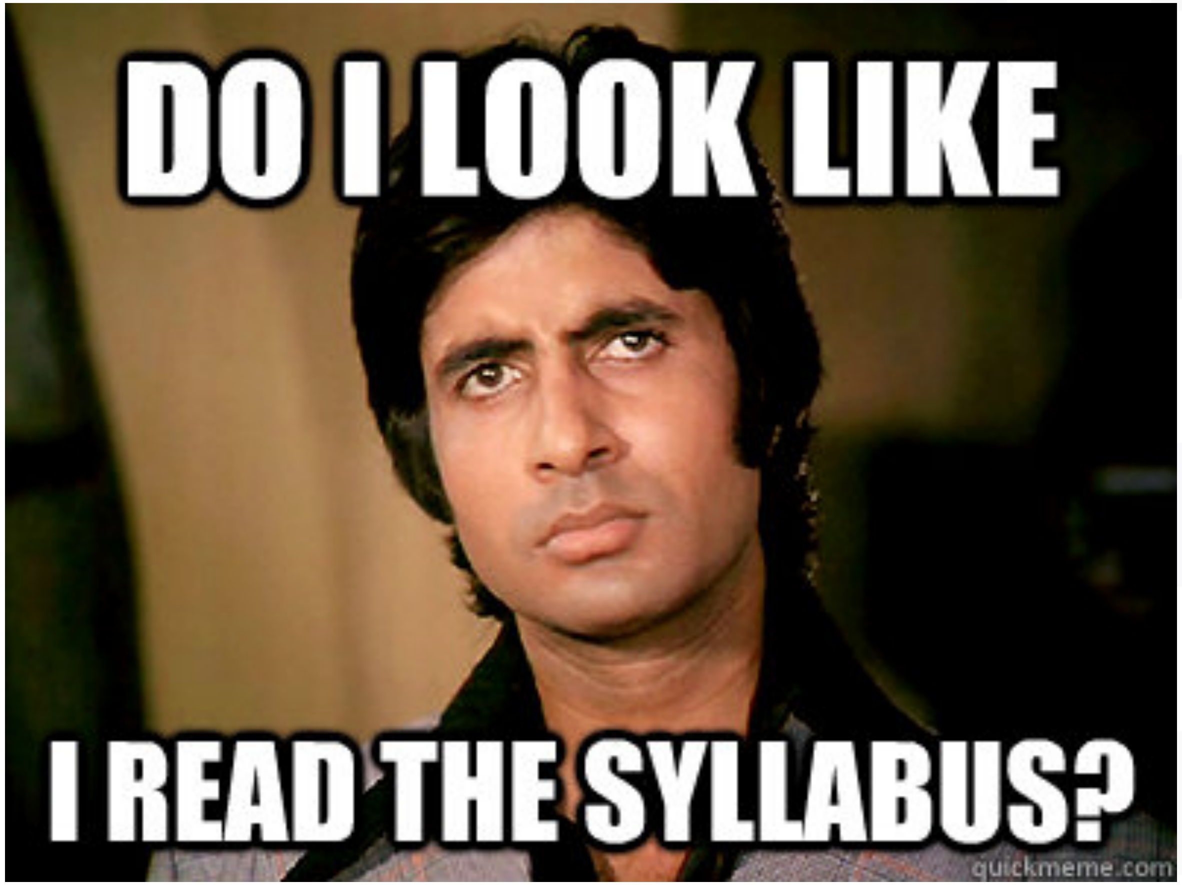
Our severe talent shortage problem…

- One more thing.
- Get this (if you want).
- It’s free (of course!).

CISSP® MENTOR PROGRAM – SESSION ONE

MENTOR PROGRAM SCHEDULE & CLASS STRUCTURE

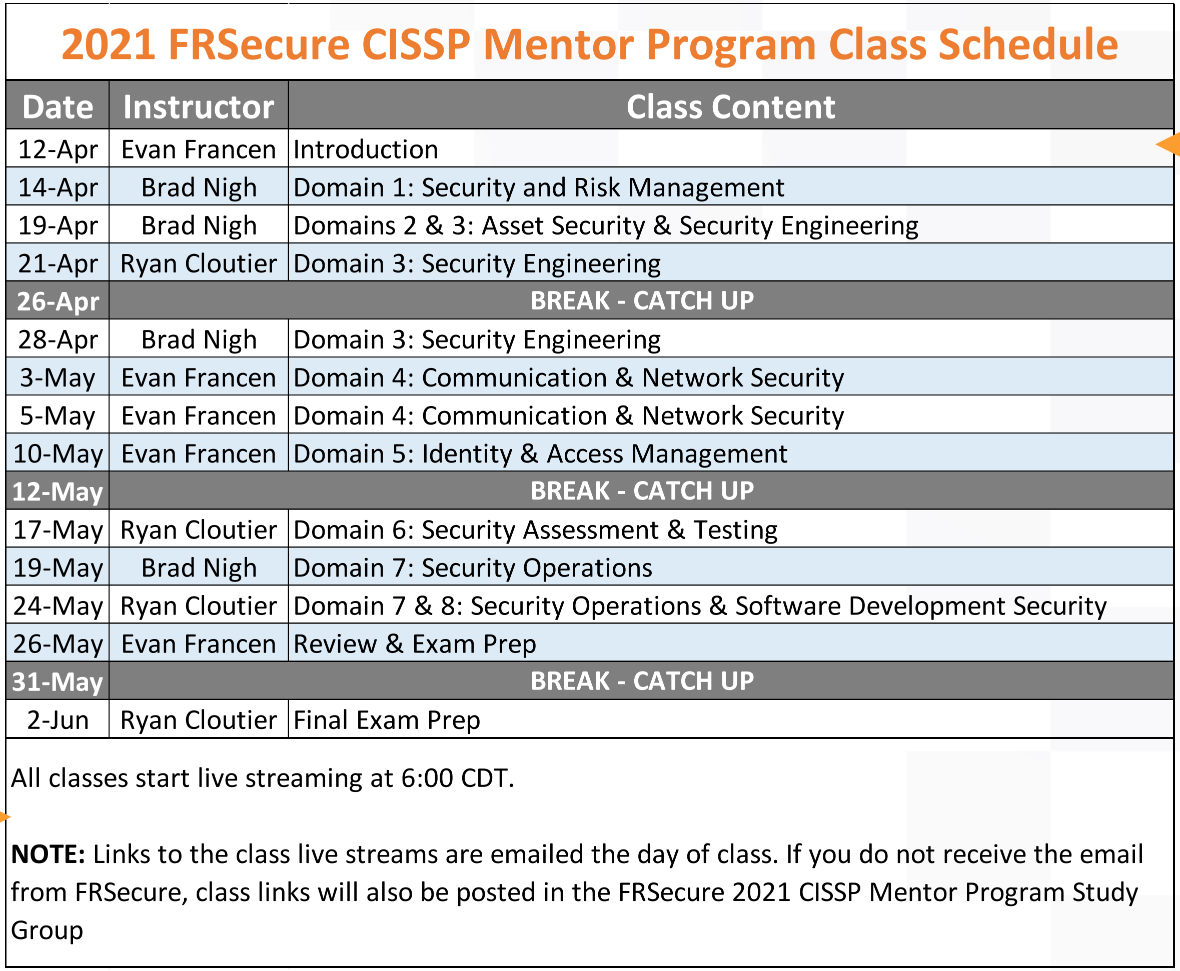
Syllabus (not really), but close.



CISSP® MENTOR PROGRAM – SESSION ONE

MENTOR PROGRAM SCHEDULE & CLASS STRUCTURE

Class schedule



2021 FRSecure CISSP Mentor Program Class Schedule

Date	Instructor	Class Content
12-Apr	Evan Francen	Introduction
14-Apr	Brad Nigh	Domain 1: Security and Risk Management
19-Apr	Brad Nigh	Domains 2 & 3: Asset Security & Security Engineering
21-Apr	Ryan Cloutier	Domain 3: Security Engineering
26-Apr	BREAK - CATCH UP	
28-Apr	Brad Nigh	Domain 3: Security Engineering
3-May	Evan Francen	Domain 4: Communication & Network Security
5-May	Evan Francen	Domain 4: Communication & Network Security
10-May	Evan Francen	Domain 5: Identity & Access Management
12-May	BREAK - CATCH UP	
17-May	Ryan Cloutier	Domain 6: Security Assessment & Testing
19-May	Brad Nigh	Domain 7: Security Operations
24-May	Ryan Cloutier	Domain 7 & 8: Security Operations & Software Development Security
26-May	Evan Francen	Review & Exam Prep
31-May	BREAK - CATCH UP	
2-Jun	Ryan Cloutier	Final Exam Prep

All classes start live streaming at 6:00 CDT.

NOTE: Links to the class live streams are emailed the day of class. If you do not receive the email from FRSecure, class links will also be posted in the FRSecure 2021 CISSP Mentor Program Study Group

This is us!

NOTE

Online, FRSecure homepage → Events → 2020 CISSP Mentor Program

MENTOR PROGRAM SCHEDULE & CLASS STRUCTURE

Class schedule

- There is a boatload of information to memorize for the exam, and you'll appreciate the breaks; we've built in three of them (4/26, 5/12, and 5/31).
- Evan, Brad, and/or Ryan will lead classes, switching things up to keep things fresh.
- We're easing into things this first week; only this introduction and one domain (Domain 1: Security and Risk Management).

No class on April 26th, May 12th, or May 31st.

Use this time to be healthy and self-study.

There are times when the material gets REALLY dry.

MENTOR PROGRAM SCHEDULE & CLASS STRUCTURE

Class schedule

- Every class is structured similarly, starting with a brief recap of the previous content/session, then:
  - Questions.
  - Quiz.
  - Current Events.
  - Lecture.
  - Homework (you'll appreciate the breaks…)

FRSecure 2021 CISSP Mentor Program Study Group

- This is yours. Please use it, and DON'T abuse it.
- We will be in and out of the study group to help when we can.

We will be removing the moderation holds tonight.

Report any/all abuse to cisspmentor@frsecure.com

CISSP® MENTOR PROGRAM – SESSION ONE

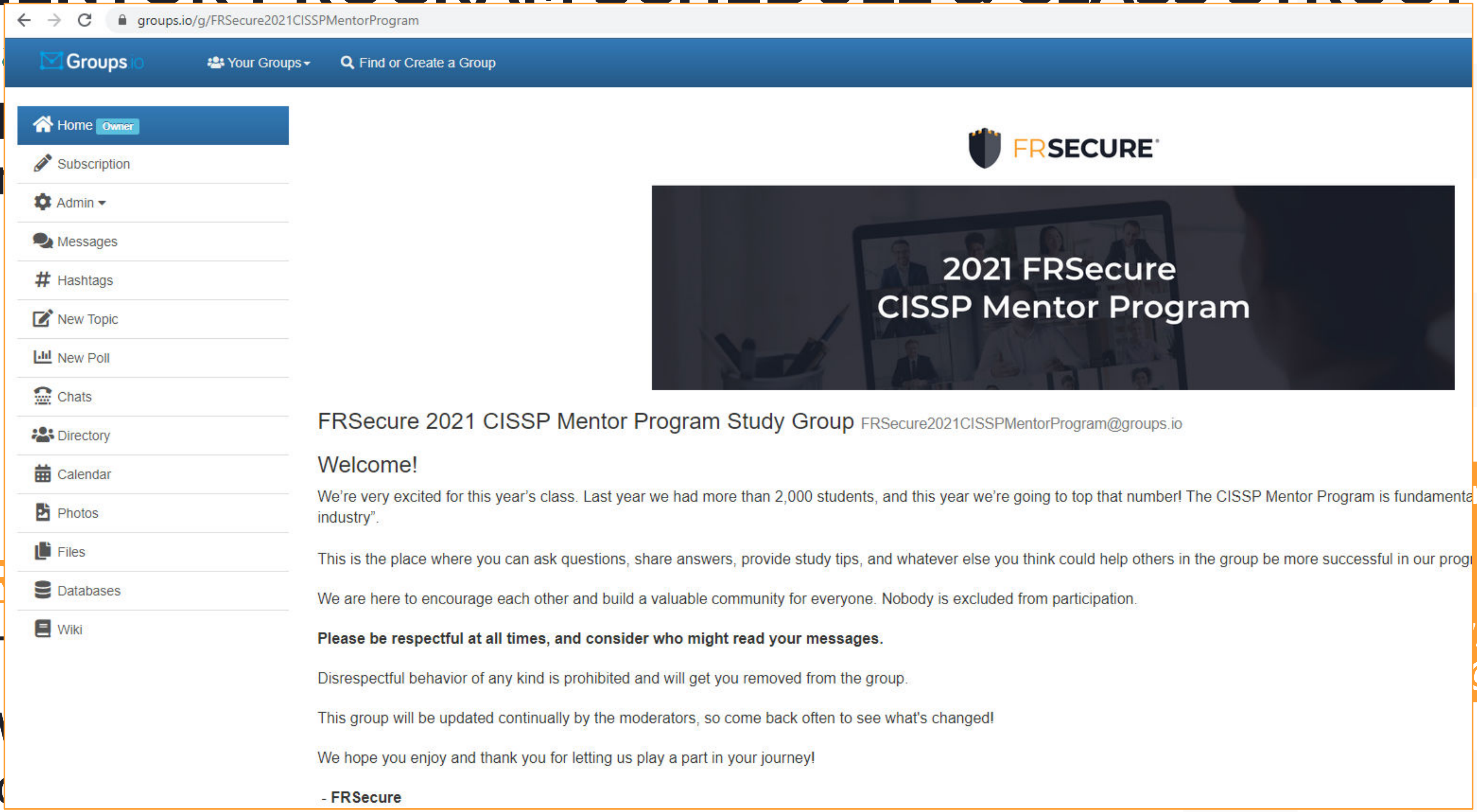
MENTOR PROGRAM SCHEDULE & CLASS STRUCTURE

Cl

- I
  I

FR

- -
- V
  (



FRSecure 2021 CISSP Mentor Program Study Group FRSecure2021CISSPMentorProgram@groups.io

Welcome!

We're very excited for this year's class. Last year we had more than 2,000 students, and this year we're going to top that number! The CISSP Mentor Program is fundamenta
industry”.

This is the place where you can ask questions, share answers, provide study tips, and whatever else you think could help others in the group be more successful in our progr

We are here to encourage each other and build a valuable community for everyone. Nobody is excluded from participation.

Please be respectful at all times, and consider who might read your messages.

Disrespectful behavior of any kind is prohibited and will get you removed from the group.

This group will be updated continually by the moderators, so come back often to see what's changed!

We hope you enjoy and thank you for letting us play a part in your journey!

- **FRSecure**

removing the
holds tonight.

/all abuse to
@frsecure.com

MENTOR PROGRAM SCHEDULE & CLASS STRUCTURE

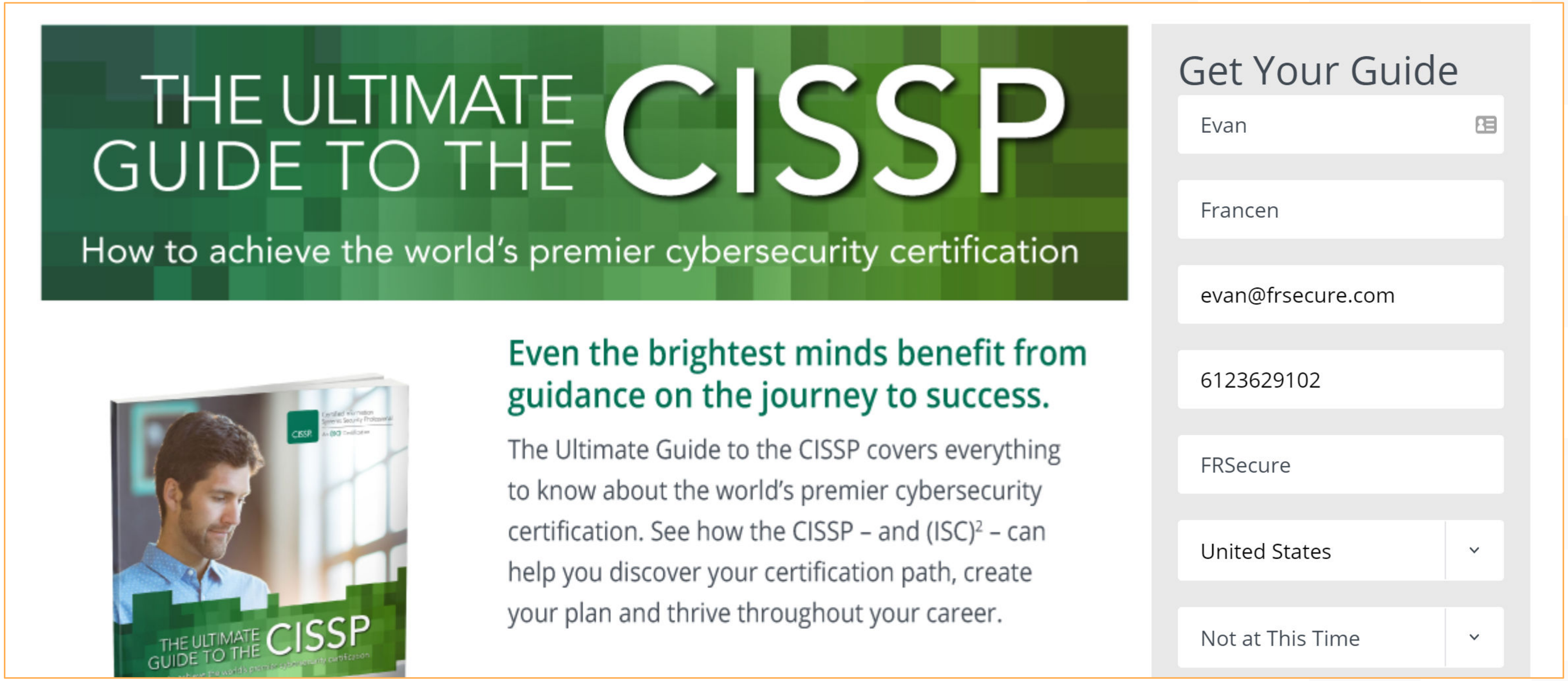
Class schedule

- We are here to help!
- If you have any questions, at any time, please send them to cisspmentor@frsecure.com.
- Please do not email any of us directly (mostly because we're slow).
- Content will be made available to all students, including (these) slides and handouts (if there are any).
- Video recordings are available immediately after class on the FRSecure YouTube channel.

WHAT IS A CISSP?

The Certified Information Systems Security Professional (or "CISSP")

Get your Ultimate Guide to the CISSP @ https://www.isc2.org/Certifications/Ultimate-Guides/CISSP?



THE ULTIMATE GUIDE TO THE CISSP

How to achieve the world's premier cybersecurity certification

Even the brightest minds benefit from guidance on the journey to success.

The Ultimate Guide to the CISSP covers everything to know about the world's premier cybersecurity certification. See how the CISSP – and (ISC)² – can help you discover your certification path, create your plan and thrive throughout your career.

Get Your Guide

Evan

Francen

evan@frsecure.com

6123629102

FRSecure

United States

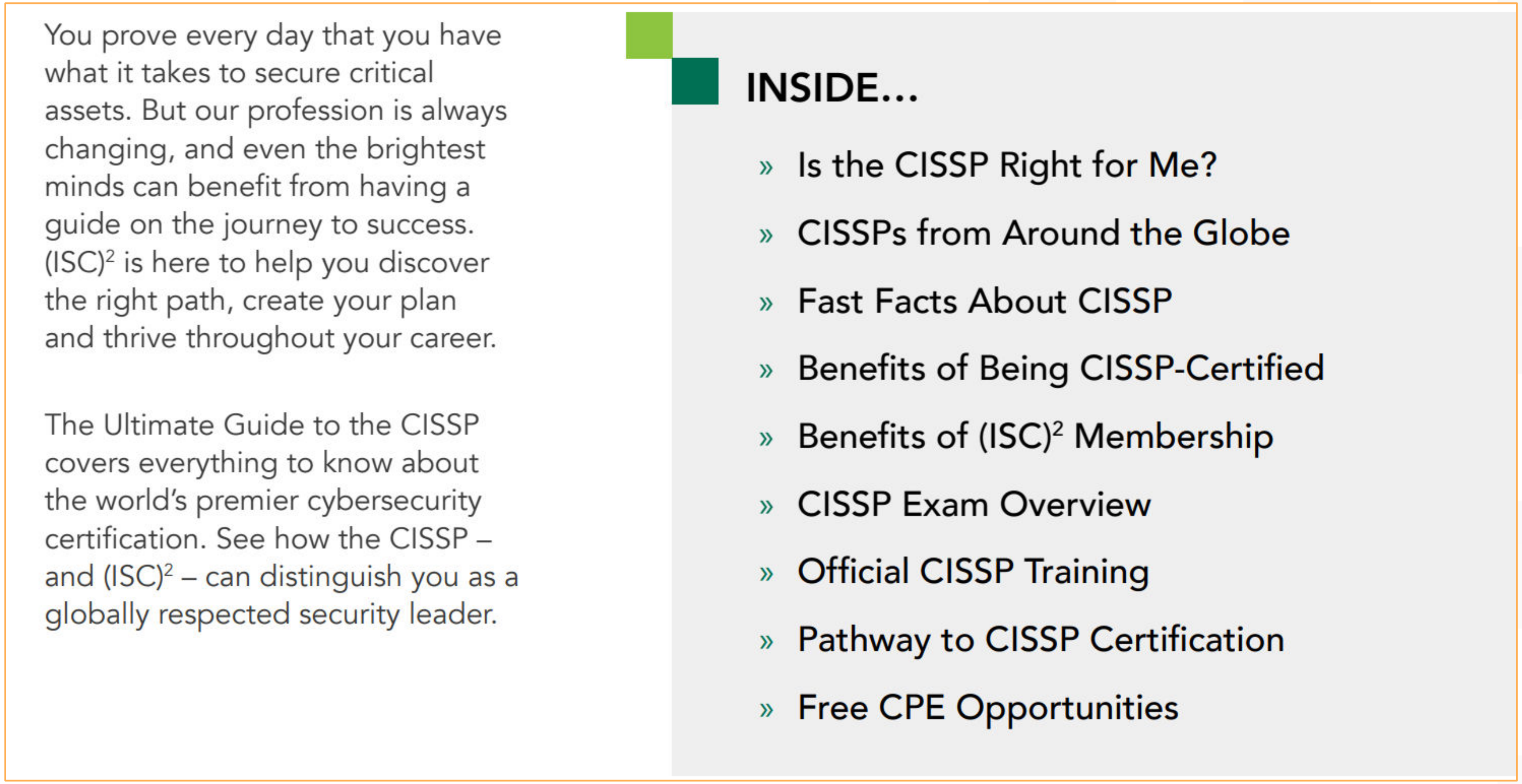
Not at This Time

CISSP® MENTOR PROGRAM – SESSION ONE

WHAT IS A CISSP?

The Certified Information Systems Security Professional (or "CISSP")

Get your Ultimate Guide to the CISSP @ https://www.isc2.org/Certifications/Ultimate-Guides/CISSP?



You prove every day that you have what it takes to secure critical assets. But our profession is always changing, and even the brightest minds can benefit from having a guide on the journey to success. (ISC)² is here to help you discover the right path, create your plan and thrive throughout your career.

The Ultimate Guide to the CISSP covers everything to know about the world's premier cybersecurity certification. See how the CISSP – and (ISC)² – can distinguish you as a globally respected security leader.

INSIDE...

» Is the CISSP Right for Me?

» CISSPs from Around the Globe

» Fast Facts About CISSP

» Benefits of Being CISSP-Certified

» Benefits of (ISC)² Membership

» CISSP Exam Overview

» Official CISSP Training

» Pathway to CISSP Certification

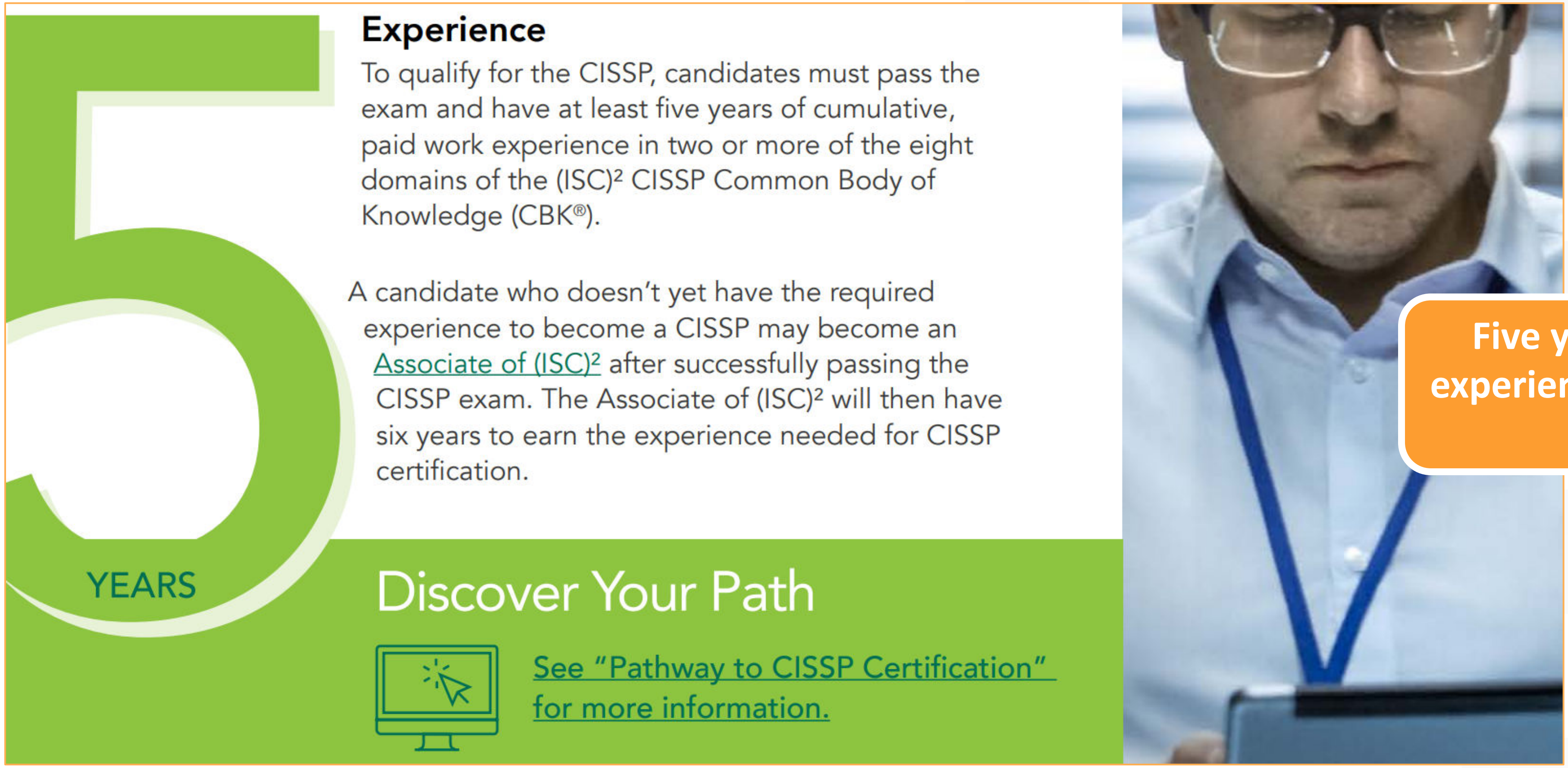
» Free CPE Opportunities

CISSP® MENTOR PROGRAM – SESSION ONE

WHAT IS A CISSP?

The Certified Information Systems Security Professional (or “CISSP”)

Get your Ultimate Guide to the CISSP @ https://www.isc2.org/Certifications/Ultimate-Guides/CISSP?



5 YEARS

Experience

To qualify for the CISSP, candidates must pass the exam and have at least five years of cumulative, paid work experience in two or more of the eight domains of the (ISC)² CISSP Common Body of Knowledge (CBK®).

A candidate who doesn’t yet have the required experience to become a CISSP may become an Associate of (ISC)² after successfully passing the CISSP exam. The Associate of (ISC)² will then have six years to earn the experience needed for CISSP certification.

Discover Your Path

See “Pathway to CISSP Certification” for more information.

Five years (cumulative) experience in two (or more) domains.

CISSP® MENTOR PROGRAM – SESSION ONE

WHAT IS A CISSP?

The Certified Information Systems Security Professional (or “CISSP”)

Get your Ultimate Guide to the CISSP @ https://www.isc2.org/Certifications/Ultimate-Guides/CISSP?

Fast Facts About CISSP

Introduced in 1994

Most Required Security Certification on LinkedIn

First information security credential to meet the strict conditions of ISO/IEC Standard 17024

DoD Approved

Exam available in 8 languages at 882 locations in 114 countries

CISSPs work in more than 160 countries globally

93% of CISSPs are lifers

More than 129,000 professionals currently hold the CISSP certification

Average CISSP Salary: US $131,030

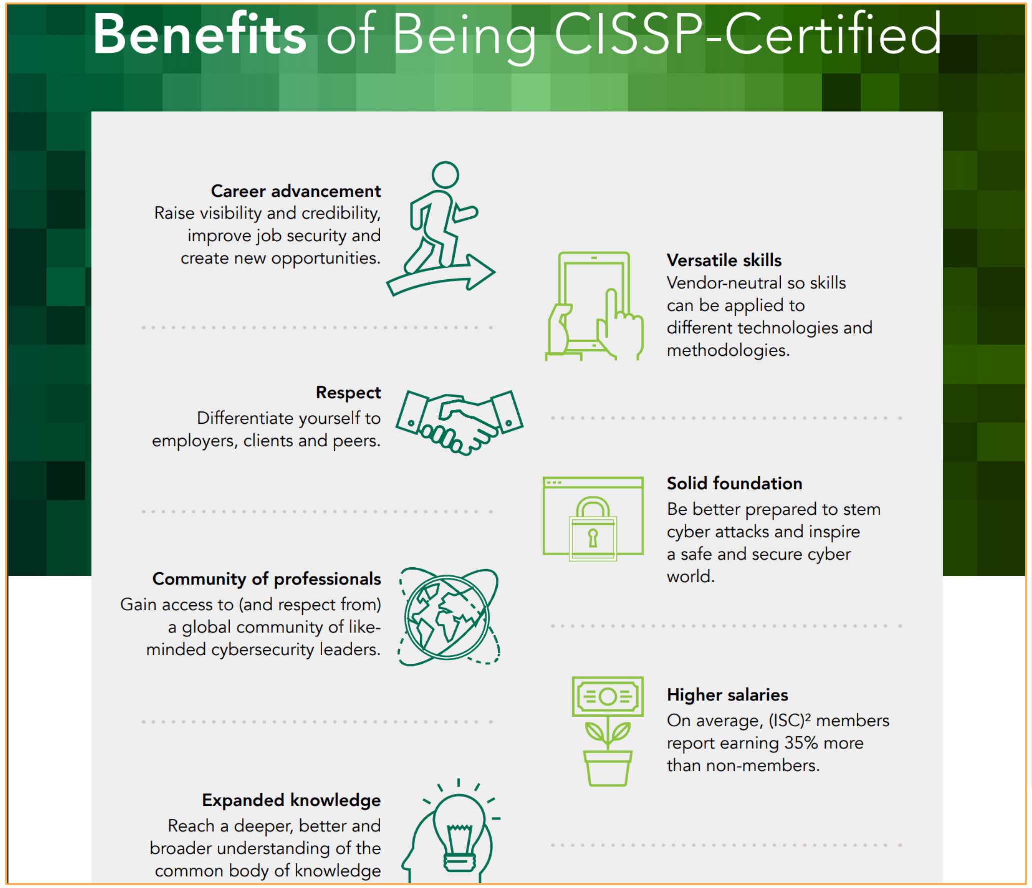
Computerized Adaptive Testing (CAT) introduced December 18, 2017

CISSP® MENTOR PROGRAM – SESSION ONE

WHAT IS A CISSP?

The Certified Information Systems Security Professional (or “CISSP”)

Get your Ultimate Guide to the CISSP @ https://www.isc2.org/Certifications/Ultimate-Guides/CISSP?



Benefits of Being CISSP-Certified

Career advancement
Raise visibility and credibility, improve job security and create new opportunities.

Versatile skills
Vendor-neutral so skills can be applied to different technologies and methodologies.

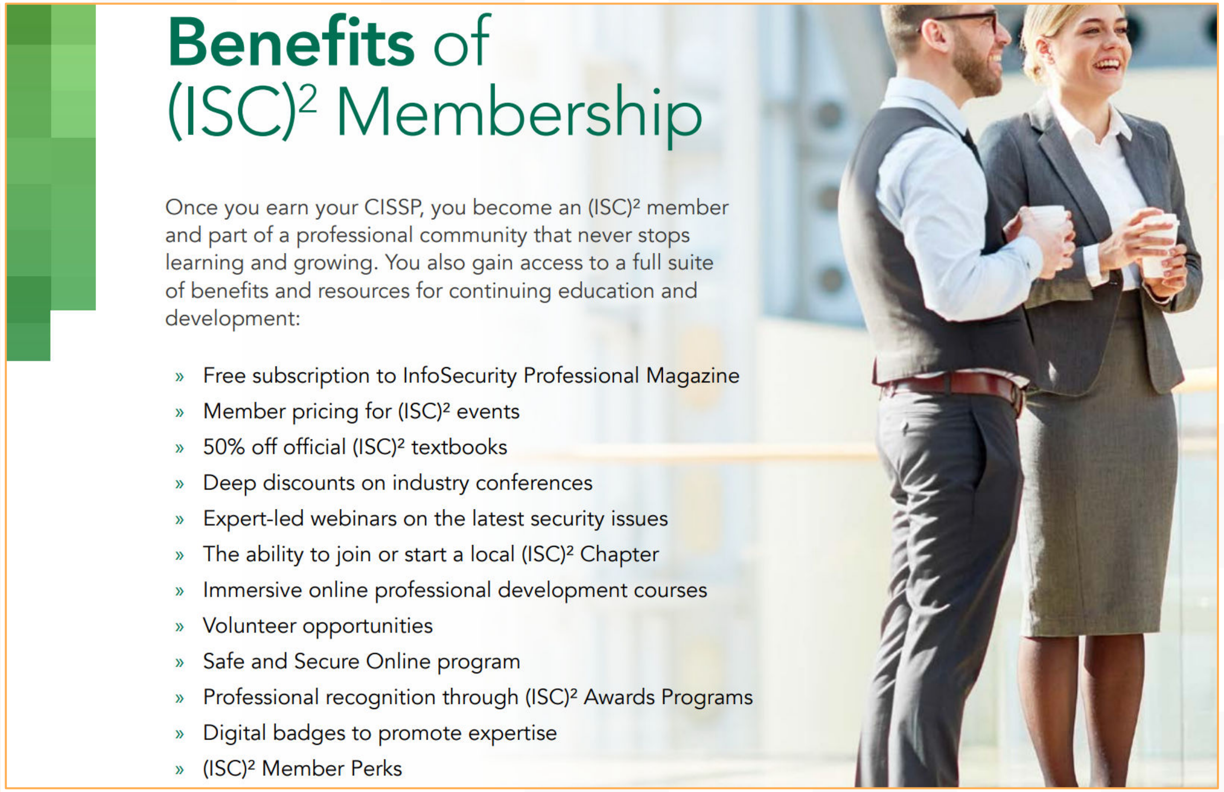
Respect
Differentiate yourself to employers, clients and peers.

Solid foundation
Be better prepared to stem cyber attacks and inspire a safe and secure cyber world.

Community of professionals
Gain access to (and respect from) a global community of like-minded cybersecurity leaders.

Higher salaries
On average, (ISC)² members report earning 35% more than non-members.

Expanded knowledge
Reach a deeper, better and broader understanding of the common body of knowledge



Benefits of (ISC)² Membership

Once you earn your CISSP, you become an (ISC)² member and part of a professional community that never stops learning and growing. You also gain access to a full suite of benefits and resources for continuing education and development:

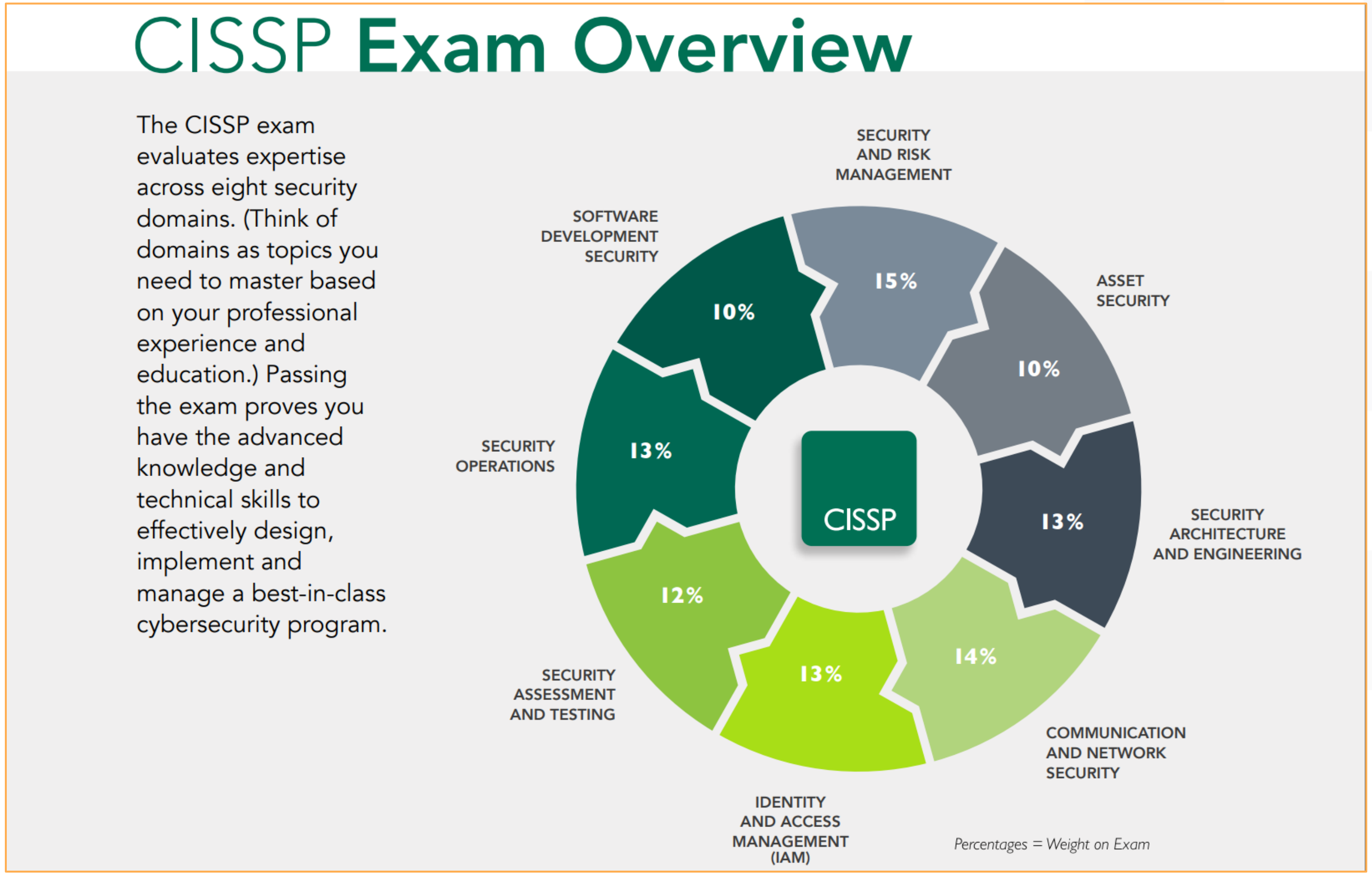
- Free subscription to InfoSecurity Professional Magazine
- Member pricing for (ISC)² events
- 50% off official (ISC)² textbooks
- Deep discounts on industry conferences
- Expert-led webinars on the latest security issues
- The ability to join or start a local (ISC)² Chapter
- Immersive online professional development courses
- Volunteer opportunities
- Safe and Secure Online program
- Professional recognition through (ISC)² Awards Programs
- Digital badges to promote expertise
- (ISC)² Member Perks

CISSP® MENTOR PROGRAM – SESSION ONE

WHAT IS A CISSP?

The Certified Information Systems Security Professional (or “CISSP”)

Get your Ultimate Guide to the CISSP @ https://www.isc2.org/Certifications/Ultimate-Guides/CISSP?



CISSP Exam Overview

The CISSP exam evaluates expertise across eight security domains. (Think of domains as topics you need to master based on your professional experience and education.) Passing the exam proves you have the advanced knowledge and technical skills to effectively design, implement and manage a best-in-class cybersecurity program.

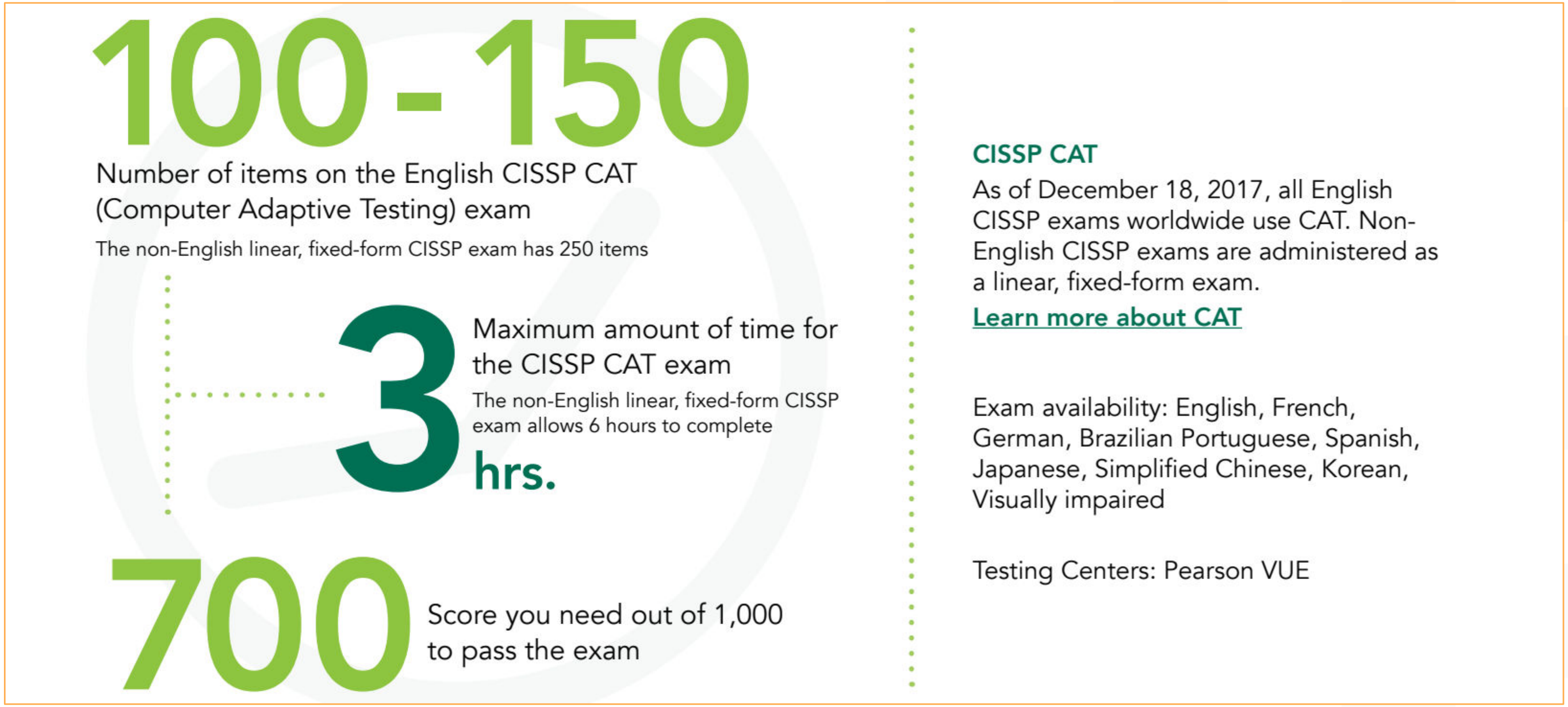
Percentages = Weight on Exam

CISSP® MENTOR PROGRAM – SESSION ONE

WHAT IS A CISSP?

The Certified Information Systems Security Professional (or “CISSP”)

Get your Ultimate Guide to the CISSP @ https://www.isc2.org/Certifications/Ultimate-Guides/CISSP?



100 - 150

Number of items on the English CISSP CAT (Computer Adaptive Testing) exam

The non-English linear, fixed-form CISSP exam has 250 items

3 hrs.

Maximum amount of time for the CISSP CAT exam

The non-English linear, fixed-form CISSP exam allows 6 hours to complete

700

Score you need out of 1,000 to pass the exam

CISSP CAT

As of December 18, 2017, all English CISSP exams worldwide use CAT. Non-English CISSP exams are administered as a linear, fixed-form exam.

Learn more about CAT

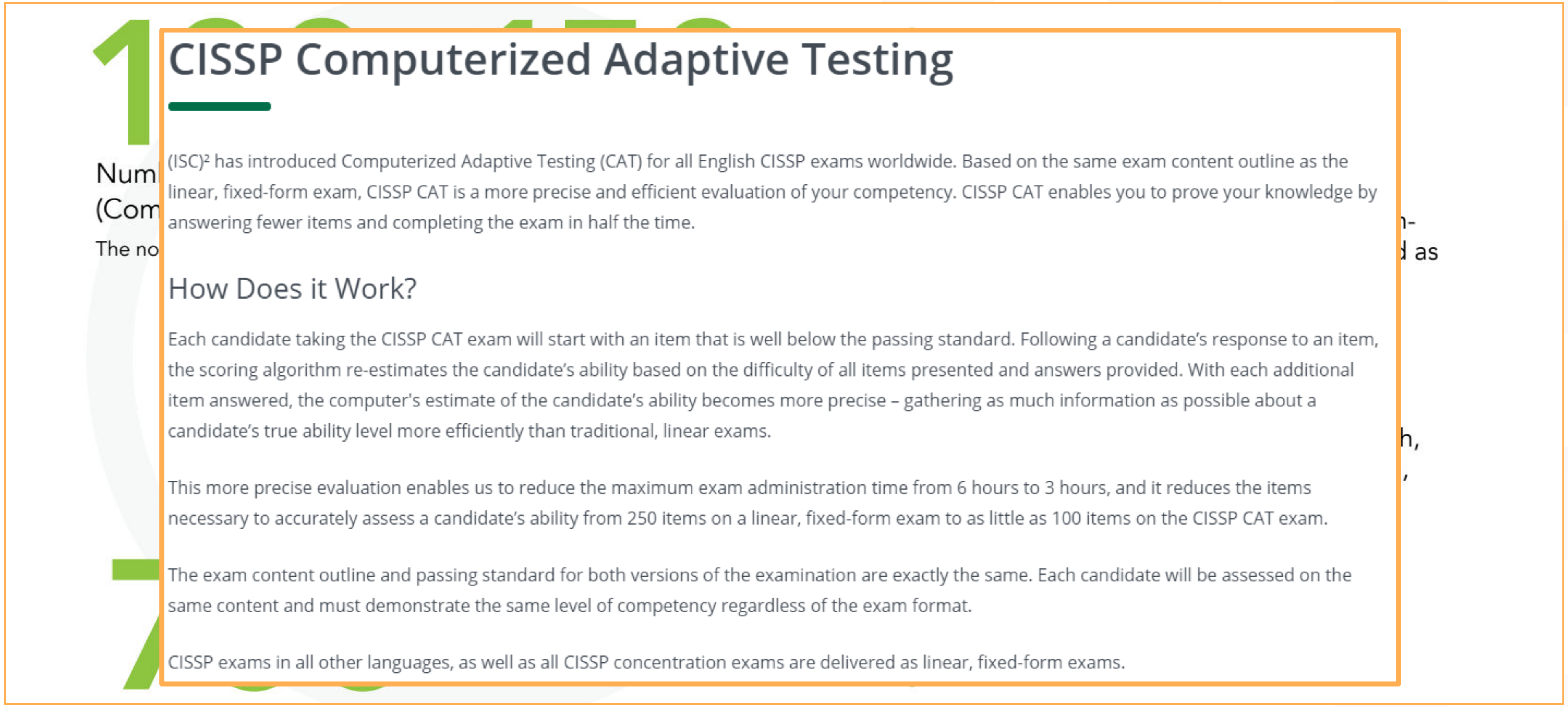
Exam availability: English, French, German, Brazilian Portuguese, Spanish, Japanese, Simplified Chinese, Korean, Visually impaired

Testing Centers: Pearson VUE

WHAT IS A CISSP?

The Certified Information Systems Security Professional (or “CISSP”)

Get your Ultimate Guide to the CISSP @ https://www.isc2.org/Certifications/Ultimate-Guides/CISSP?



CISSP Computerized Adaptive Testing

(ISC)² has introduced Computerized Adaptive Testing (CAT) for all English CISSP exams worldwide. Based on the same exam content outline as the linear, fixed-form exam, CISSP CAT is a more precise and efficient evaluation of your competency. CISSP CAT enables you to prove your knowledge by answering fewer items and completing the exam in half the time.

How Does it Work?

Each candidate taking the CISSP CAT exam will start with an item that is well below the passing standard. Following a candidate’s response to an item, the scoring algorithm re-estimates the candidate’s ability based on the difficulty of all items presented and answers provided. With each additional item answered, the computer's estimate of the candidate’s ability becomes more precise – gathering as much information as possible about a candidate’s true ability level more efficiently than traditional, linear exams.

This more precise evaluation enables us to reduce the maximum exam administration time from 6 hours to 3 hours, and it reduces the items necessary to accurately assess a candidate’s ability from 250 items on a linear, fixed-form exam to as little as 100 items on the CISSP CAT exam.

The exam content outline and passing standard for both versions of the examination are exactly the same. Each candidate will be assessed on the same content and must demonstrate the same level of competency regardless of the exam format.

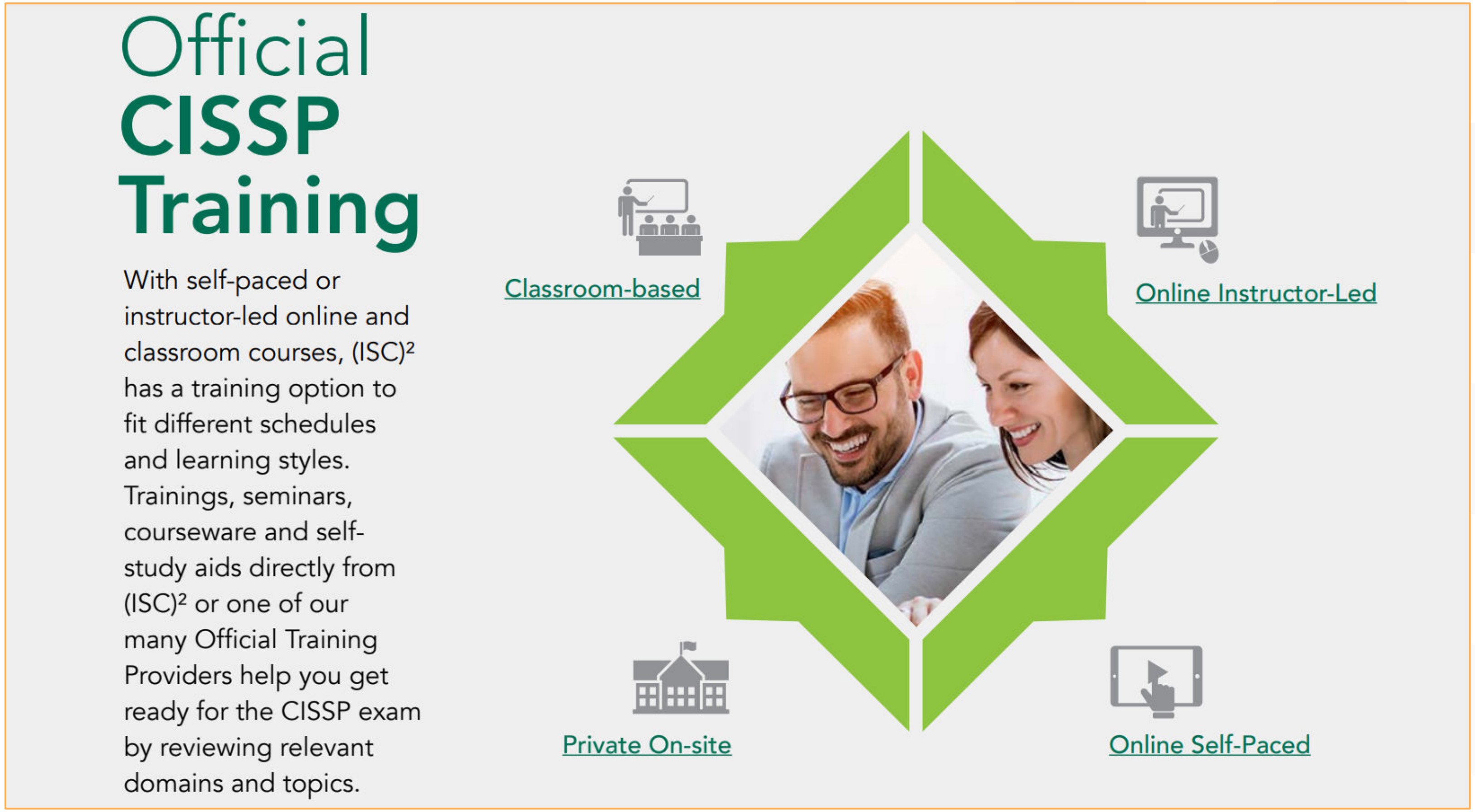
CISSP exams in all other languages, as well as all CISSP concentration exams are delivered as linear, fixed-form exams.

CISSP® MENTOR PROGRAM – SESSION ONE

WHAT IS A CISSP?

The Certified Information Systems Security Professional (or "CISSP")

Get your Ultimate Guide to the CISSP @ https://www.isc2.org/Certifications/Ultimate-Guides/CISSP?



Official CISSP Training

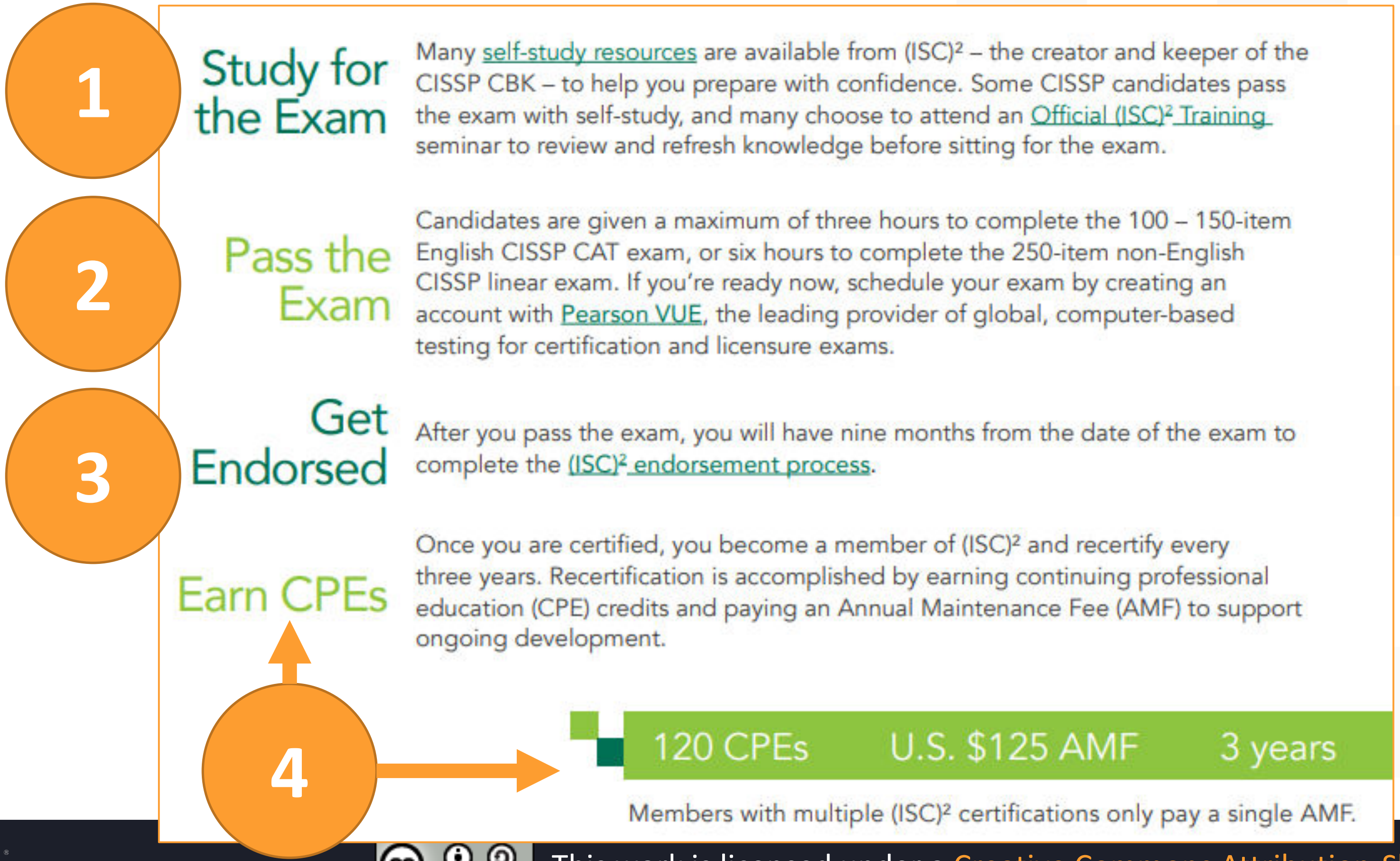
With self-paced or instructor-led online and classroom courses, (ISC)² has a training option to fit different schedules and learning styles. Trainings, seminars, courseware and self-study aids directly from (ISC)² or one of our many Official Training Providers help you get ready for the CISSP exam by reviewing relevant domains and topics.

CISSP® MENTOR PROGRAM – SESSION ONE

WHAT IS A CISSP?

The Certified Information Systems Security Professional (or “CISSP”)

Get your Ultimate Guide to the CISSP @ https://www.isc2.org/Certifications/Ultimate-Guides/CISSP?



Study for the Exam

Many self-study resources are available from (ISC)² – the creator and keeper of the CISSP CBK – to help you prepare with confidence. Some CISSP candidates pass the exam with self-study, and many choose to attend an Official (ISC)² Training seminar to review and refresh knowledge before sitting for the exam.

Pass the Exam

Candidates are given a maximum of three hours to complete the 100 – 150-item English CISSP CAT exam, or six hours to complete the 250-item non-English CISSP linear exam. If you’re ready now, schedule your exam by creating an account with Pearson VUE, the leading provider of global, computer-based testing for certification and licensure exams.

Get Endorsed

After you pass the exam, you will have nine months from the date of the exam to complete the (ISC)² endorsement process.

Earn CPEs

Once you are certified, you become a member of (ISC)² and recertify every three years. Recertification is accomplished by earning continuing professional education (CPE) credits and paying an Annual Maintenance Fee (AMF) to support ongoing development.

120 CPEs U.S. $125 AMF 3 years

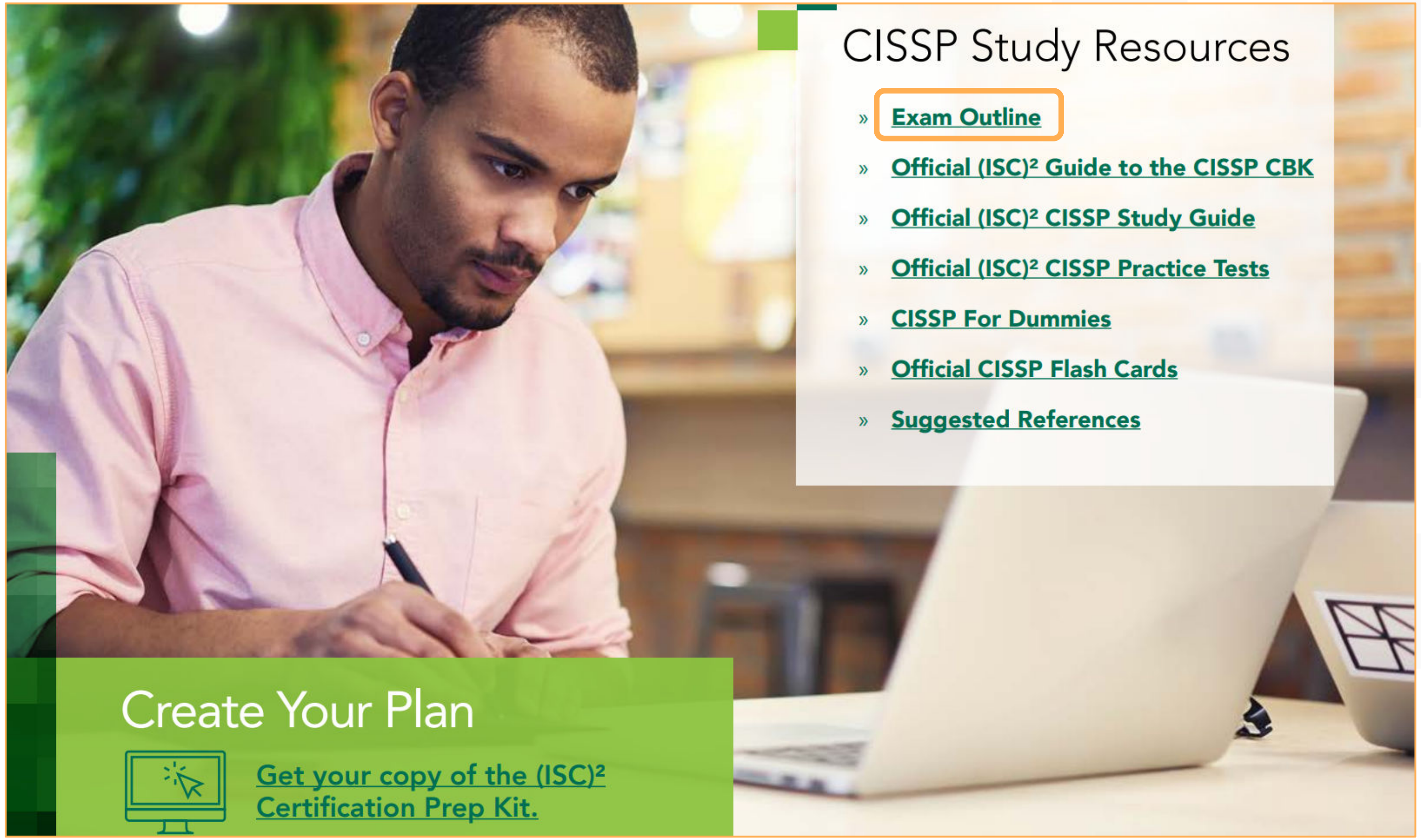
Members with multiple (ISC)² certifications only pay a single AMF.

CISSP® MENTOR PROGRAM – SESSION ONE

WHAT IS A CISSP?

The Certified Information Systems Security Professional (or “CISSP”)

Get your Ultimate Guide to the CISSP @ https://www.isc2.org/Certifications/Ultimate-Guides/CISSP?



CISSP Study Resources

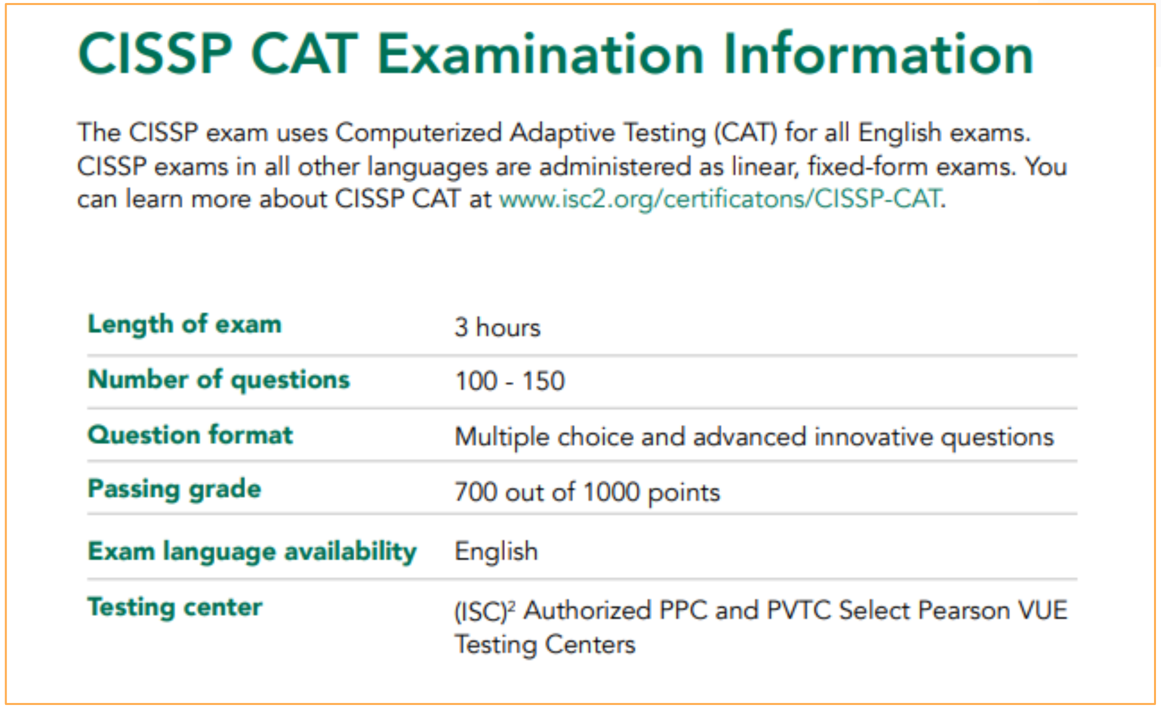
- » Exam Outline
- » Official (ISC)² Guide to the CISSP CBK
- » Official (ISC)² CISSP Study Guide
- » Official (ISC)² CISSP Practice Tests
- » CISSP For Dummies
- » Official CISSP Flash Cards
- » Suggested References

Create Your Plan

Get your copy of the (ISC)² Certification Prep Kit.

CISSP CERTIFICATION EXAM OUTLINE

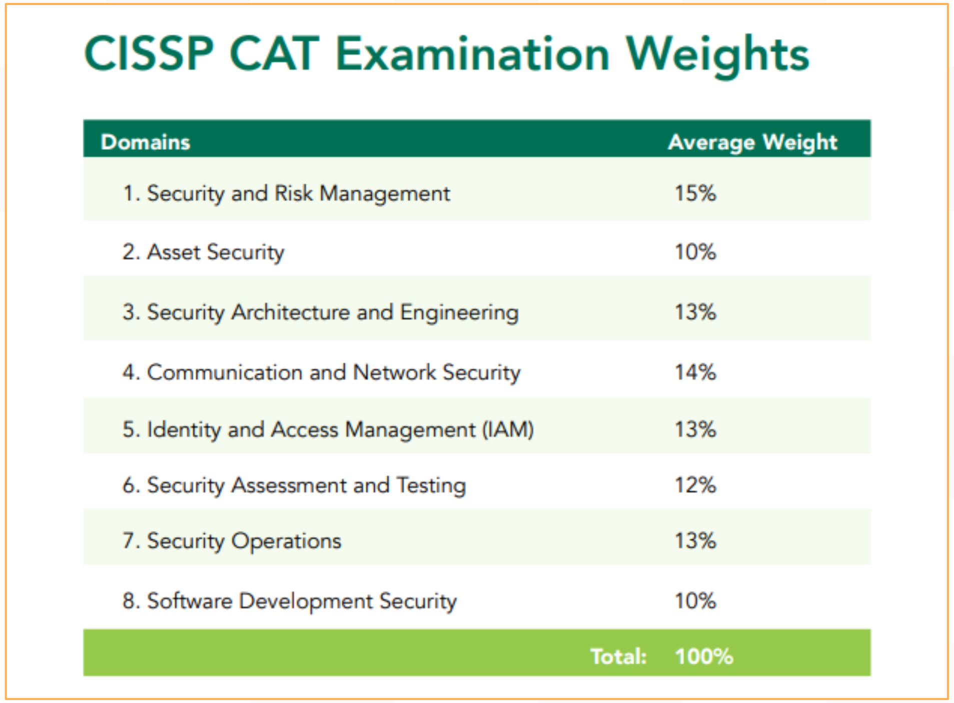
https://www.isc2.org//-/media/ISC2/Certifications/Exam-Outlines/CISSP-Exam-Outline-English-April-2021.ashx



CISSP CAT Examination Information

The CISSP exam uses Computerized Adaptive Testing (CAT) for all English exams. CISSP exams in all other languages are administered as linear, fixed-form exams. You can learn more about CISSP CAT at www.isc2.org/certificatons/CISSP-CAT.

Length of exam	3 hours
Number of questions	100 - 150
Question format	Multiple choice and advanced innovative questions
Passing grade	700 out of 1000 points
Exam language availability	English
Testing center	(ISC)² Authorized PPC and PVTC Select Pearson VUE Testing Centers

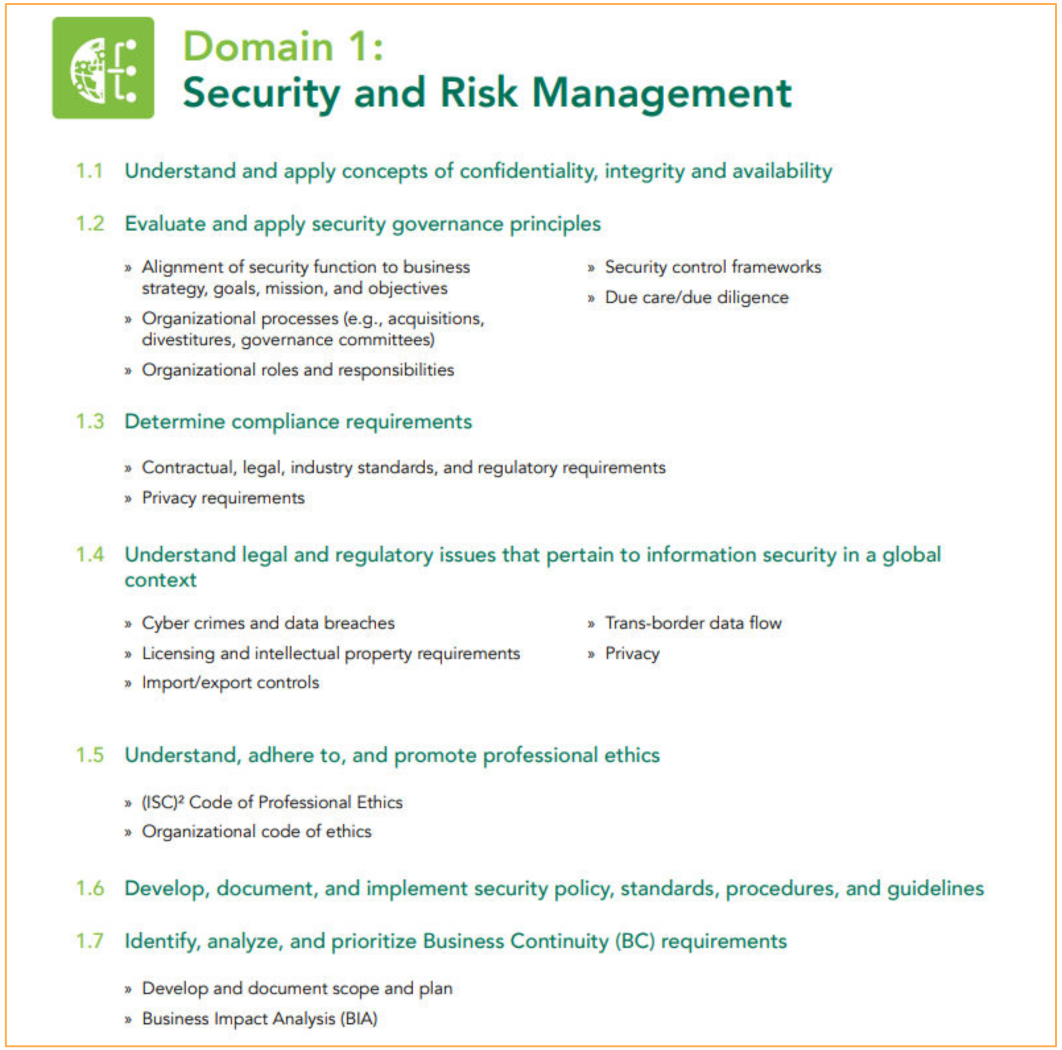


CISSP CAT Examination Weights

Domains	Average Weight
1. Security and Risk Management	15%
2. Asset Security	10%
3. Security Architecture and Engineering	13%
4. Communication and Network Security	14%
5. Identity and Access Management (IAM)	13%
6. Security Assessment and Testing	12%
7. Security Operations	13%
8. Software Development Security	10%
Total:	100%

CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE



Domain 1: Security and Risk Management

1.1 Understand and apply concepts of confidentiality, integrity and availability

1.2 Evaluate and apply security governance principles

- » Alignment of security function to business strategy, goals, mission, and objectives
- » Organizational processes (e.g., acquisitions, divestitures, governance committees)
- » Organizational roles and responsibilities
- » Security control frameworks
- » Due care/due diligence

1.3 Determine compliance requirements

- » Contractual, legal, industry standards, and regulatory requirements
- » Privacy requirements

1.4 Understand legal and regulatory issues that pertain to information security in a global context

- » Cyber crimes and data breaches
- » Licensing and intellectual property requirements
- » Import/export controls
- » Trans-border data flow
- » Privacy

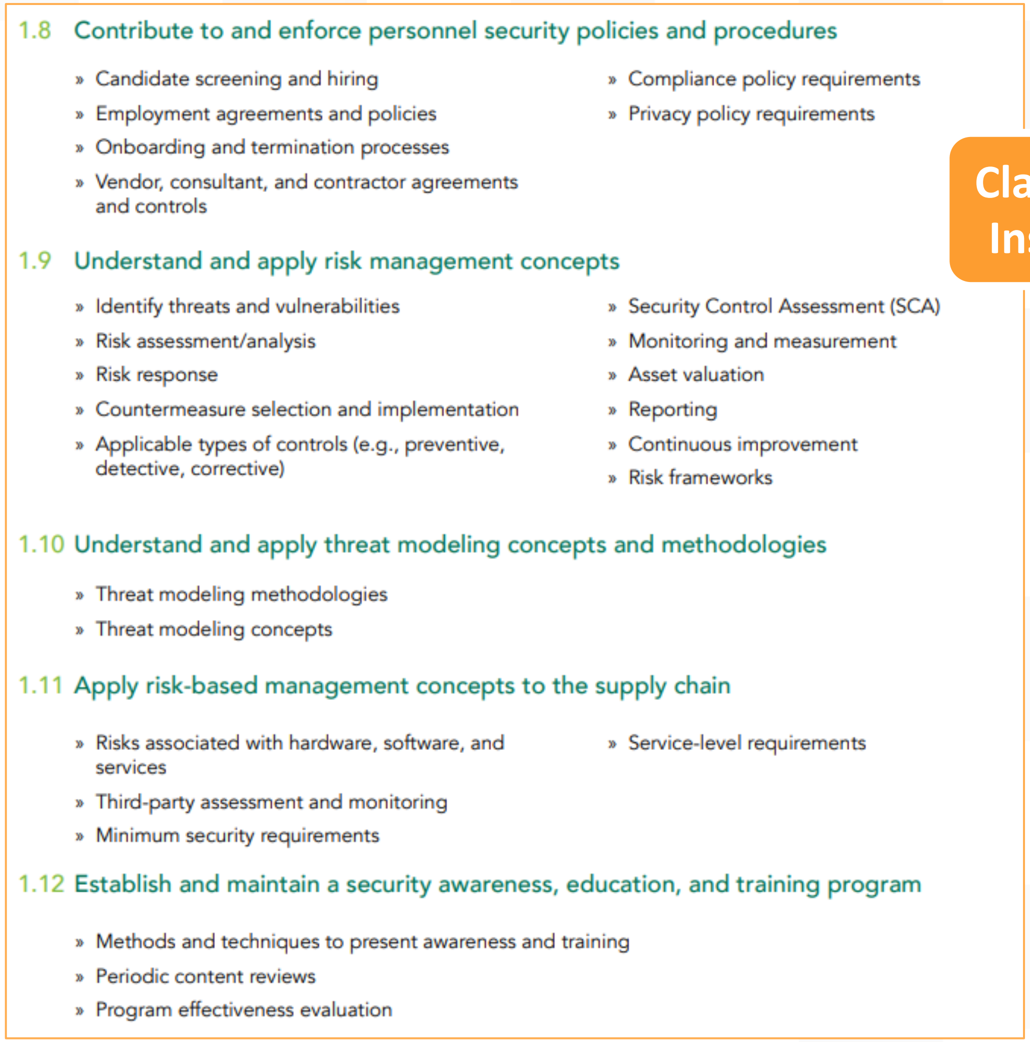
1.5 Understand, adhere to, and promote professional ethics

- » (ISC)² Code of Professional Ethics
- » Organizational code of ethics

1.6 Develop, document, and implement security policy, standards, procedures, and guidelines

1.7 Identify, analyze, and prioritize Business Continuity (BC) requirements

- » Develop and document scope and plan
- » Business Impact Analysis (BIA)



1.8 Contribute to and enforce personnel security policies and procedures

- » Candidate screening and hiring
- » Employment agreements and policies
- » Onboarding and termination processes
- » Vendor, consultant, and contractor agreements and controls
- » Compliance policy requirements
- » Privacy policy requirements

1.9 Understand and apply risk management concepts

- » Identify threats and vulnerabilities
- » Risk assessment/analysis
- » Risk response
- » Countermeasure selection and implementation
- » Applicable types of controls (e.g., preventive, detective, corrective)
- » Security Control Assessment (SCA)
- » Monitoring and measurement
- » Asset valuation
- » Reporting
- » Continuous improvement
- » Risk frameworks

1.10 Understand and apply threat modeling concepts and methodologies

- » Threat modeling methodologies
- » Threat modeling concepts

1.11 Apply risk-based management concepts to the supply chain

- » Risks associated with hardware, software, and services
- » Third-party assessment and monitoring
- » Minimum security requirements
- » Service-level requirements

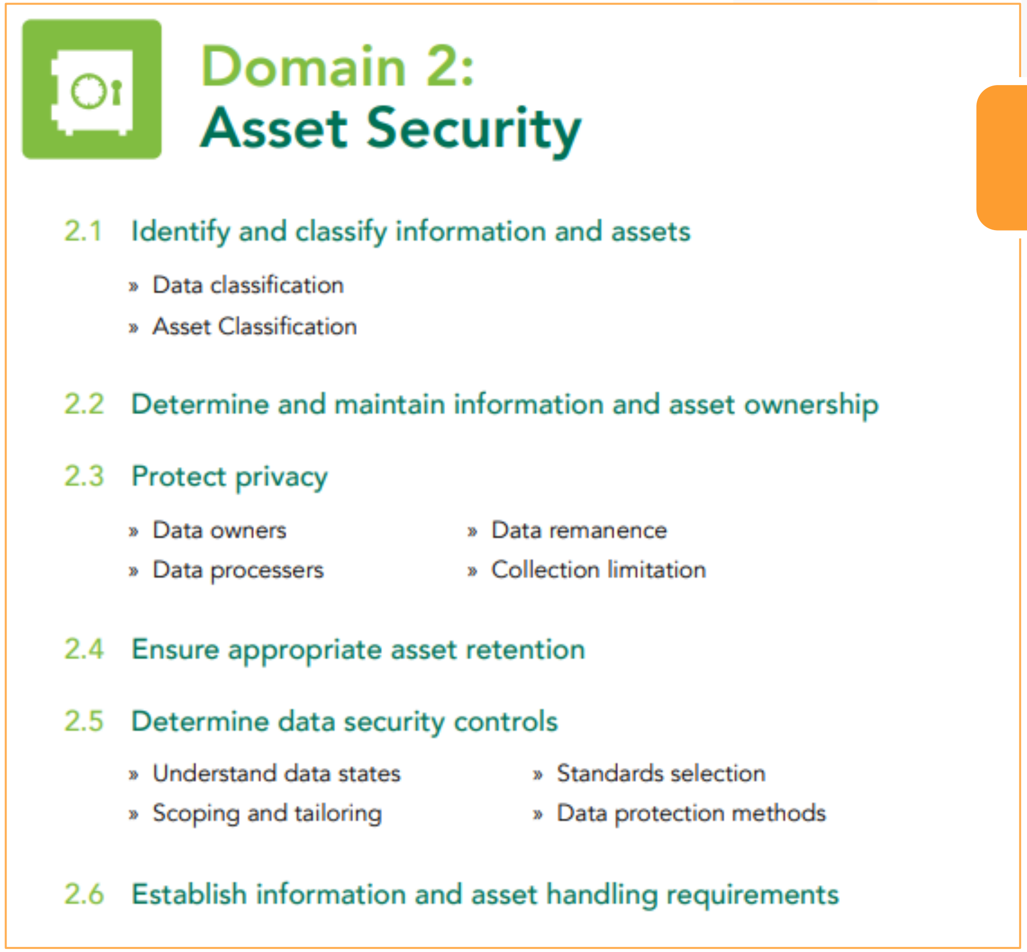
1.12 Establish and maintain a security awareness, education, and training program

- » Methods and techniques to present awareness and training
- » Periodic content reviews
- » Program effectiveness evaluation

Class 2: April 14th
Instructor: Brad

CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE



Domain 2: Asset Security

2.1 Identify and classify information and assets

» Data classification
» Asset Classification

2.2 Determine and maintain information and asset ownership

2.3 Protect privacy

» Data owners
» Data processers
» Data remanence
» Collection limitation

2.4 Ensure appropriate asset retention

2.5 Determine data security controls

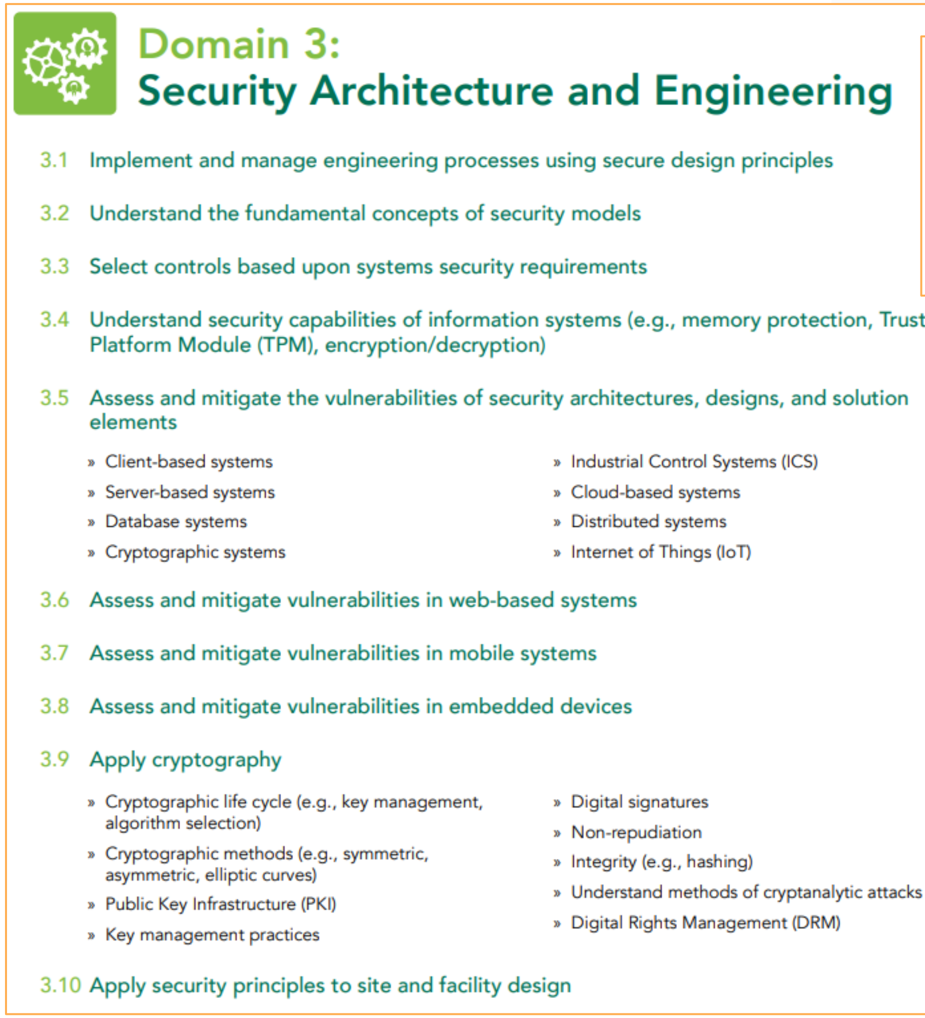
» Understand data states
» Scoping and tailoring
» Standards selection
» Data protection methods

2.6 Establish information and asset handling requirements

Class 3: April 19th
Instructor: Brad

CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE



Domain 3: Security Architecture and Engineering

3.1 Implement and manage engineering processes using secure design principles

3.2 Understand the fundamental concepts of security models

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Client-based systems
- Server-based systems
- Database systems
- Cryptographic systems
- Industrial Control Systems (ICS)
- Cloud-based systems
- Distributed systems
- Internet of Things (IoT)

3.6 Assess and mitigate vulnerabilities in web-based systems

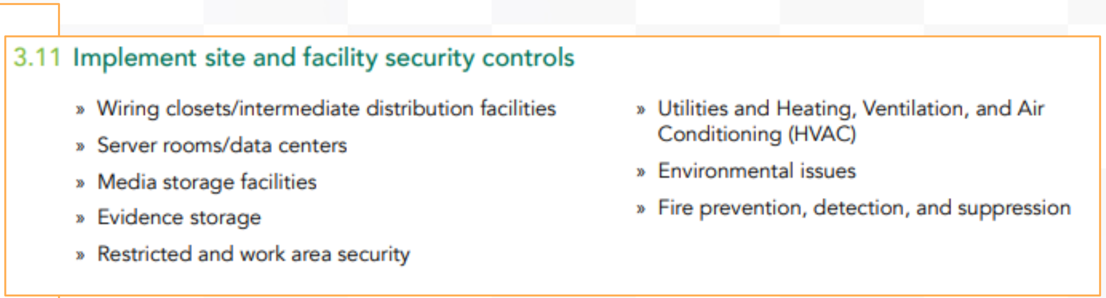
3.7 Assess and mitigate vulnerabilities in mobile systems

3.8 Assess and mitigate vulnerabilities in embedded devices

3.9 Apply cryptography

- Cryptographic life cycle (e.g., key management, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves)
- Public Key Infrastructure (PKI)
- Key management practices
- Digital signatures
- Non-repudiation
- Integrity (e.g., hashing)
- Understand methods of cryptanalytic attacks
- Digital Rights Management (DRM)

3.10 Apply security principles to site and facility design



3.11 Implement site and facility security controls

- Wiring closets/intermediate distribution facilities
- Server rooms/data centers
- Media storage facilities
- Evidence storage
- Restricted and work area security
- Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
- Environmental issues
- Fire prevention, detection, and suppression

Class 3: April 19th
Instructor: Brad

Class 4: April 21st
Instructor: Ryan

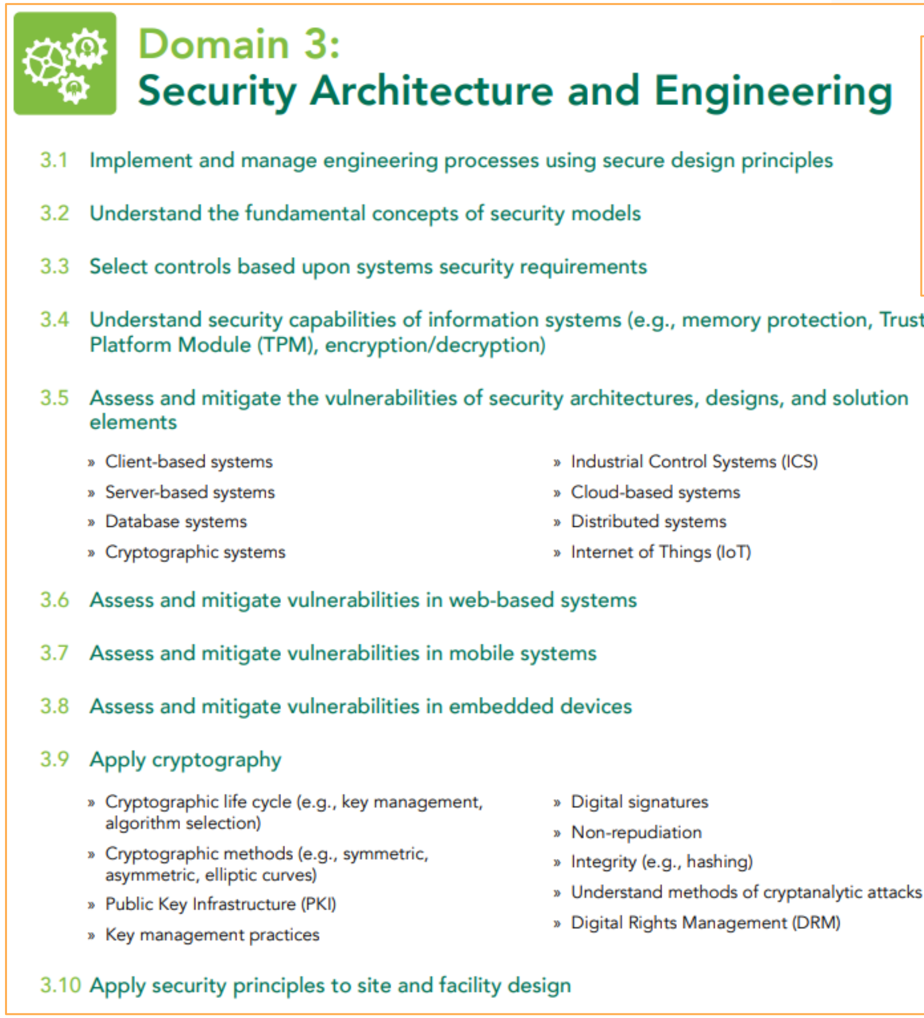
CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE

April 26th - BREAK

CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE



Domain 3: Security Architecture and Engineering

3.1 Implement and manage engineering processes using secure design principles

3.2 Understand the fundamental concepts of security models

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Client-based systems
- Server-based systems
- Database systems
- Cryptographic systems
- Industrial Control Systems (ICS)
- Cloud-based systems
- Distributed systems
- Internet of Things (IoT)

3.6 Assess and mitigate vulnerabilities in web-based systems

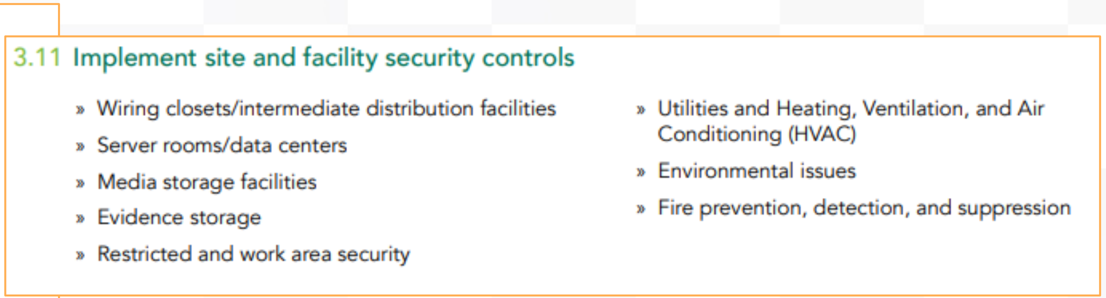
3.7 Assess and mitigate vulnerabilities in mobile systems

3.8 Assess and mitigate vulnerabilities in embedded devices

3.9 Apply cryptography

- Cryptographic life cycle (e.g., key management, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves)
- Public Key Infrastructure (PKI)
- Key management practices
- Digital signatures
- Non-repudiation
- Integrity (e.g., hashing)
- Understand methods of cryptanalytic attacks
- Digital Rights Management (DRM)

3.10 Apply security principles to site and facility design



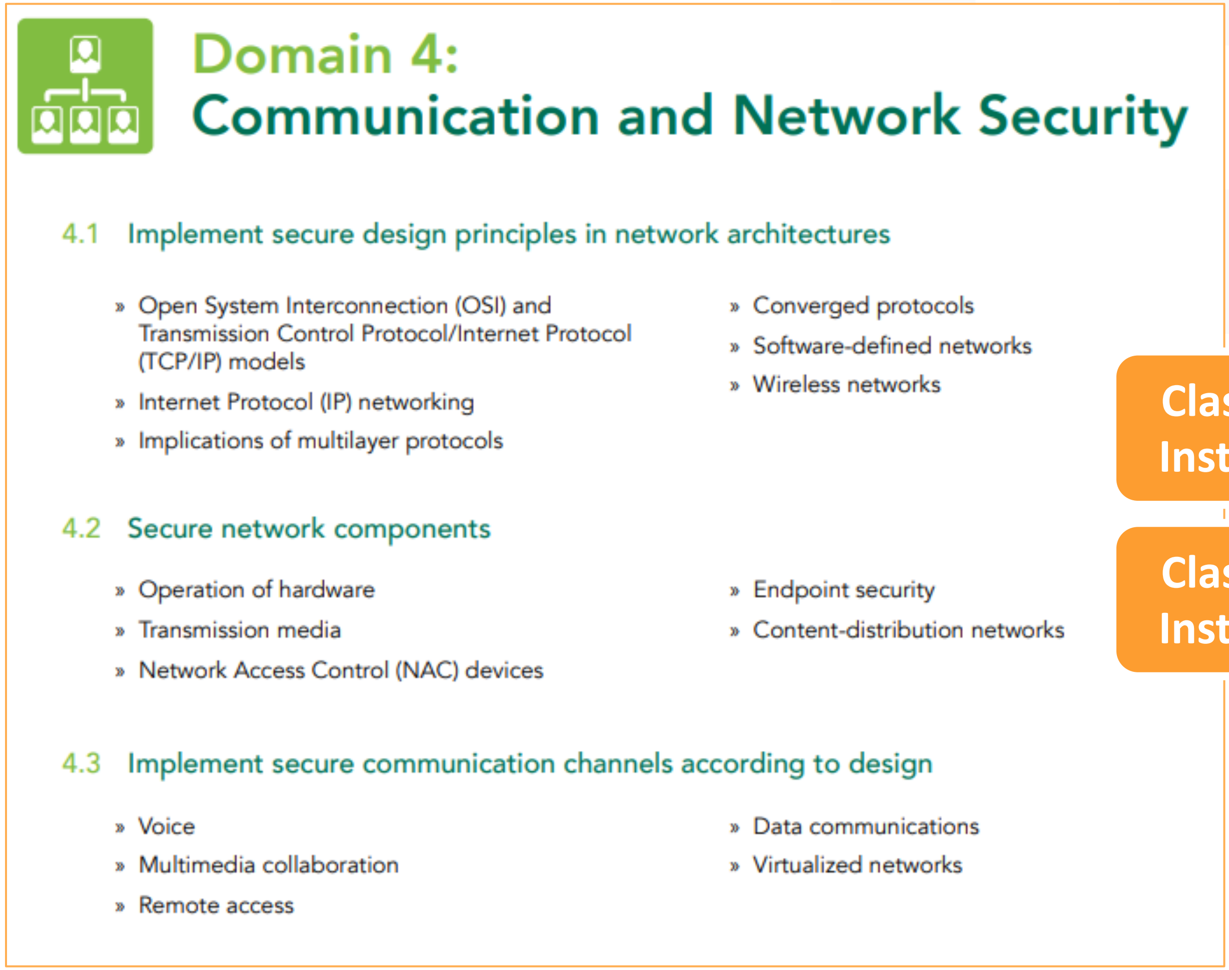
3.11 Implement site and facility security controls

- Wiring closets/intermediate distribution facilities
- Server rooms/data centers
- Media storage facilities
- Evidence storage
- Restricted and work area security
- Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
- Environmental issues
- Fire prevention, detection, and suppression

Class 5: April 28th
Instructor: Brad

CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE



Domain 4: Communication and Network Security

4.1 Implement secure design principles in network architectures

- » Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- » Internet Protocol (IP) networking
- » Implications of multilayer protocols
- » Converged protocols
- » Software-defined networks
- » Wireless networks

4.2 Secure network components

- » Operation of hardware
- » Transmission media
- » Network Access Control (NAC) devices
- » Endpoint security
- » Content-distribution networks

4.3 Implement secure communication channels according to design

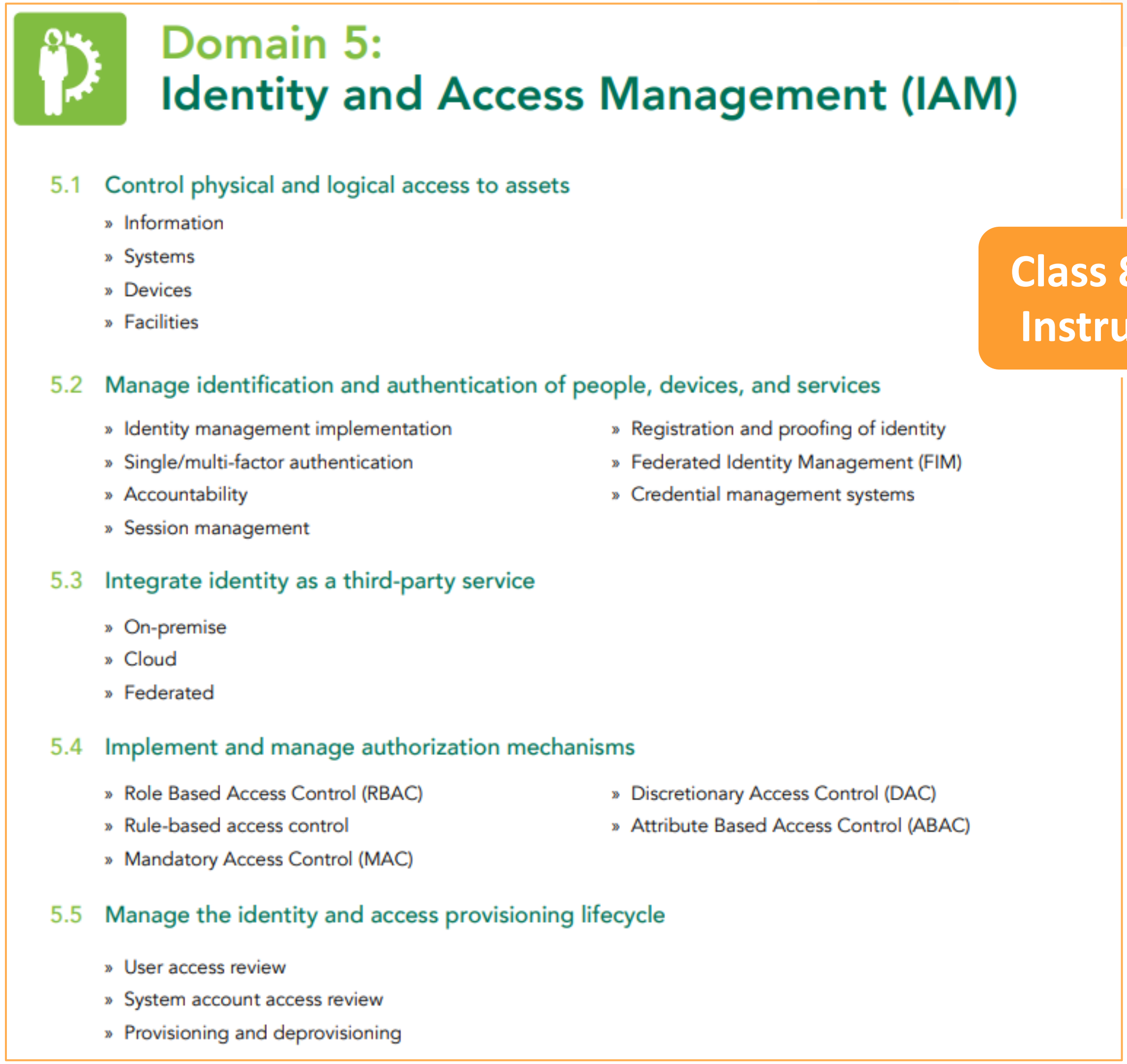
- » Voice
- » Multimedia collaboration
- » Remote access
- » Data communications
- » Virtualized networks

Class 6: May 3rd
Instructor: Evan

Class 7: May 5th
Instructor: Evan

CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE



Domain 5: Identity and Access Management (IAM)

5.1 Control physical and logical access to assets

- » Information
- » Systems
- » Devices
- » Facilities

5.2 Manage identification and authentication of people, devices, and services

- » Identity management implementation
- » Single/multi-factor authentication
- » Accountability
- » Session management
- » Registration and proofing of identity
- » Federated Identity Management (FIM)
- » Credential management systems

5.3 Integrate identity as a third-party service

- » On-premise
- » Cloud
- » Federated

5.4 Implement and manage authorization mechanisms

- » Role Based Access Control (RBAC)
- » Rule-based access control
- » Mandatory Access Control (MAC)
- » Discretionary Access Control (DAC)
- » Attribute Based Access Control (ABAC)

5.5 Manage the identity and access provisioning lifecycle

- » User access review
- » System account access review
- » Provisioning and deprovisioning

Class 8: May 10th
Instructor: Evan

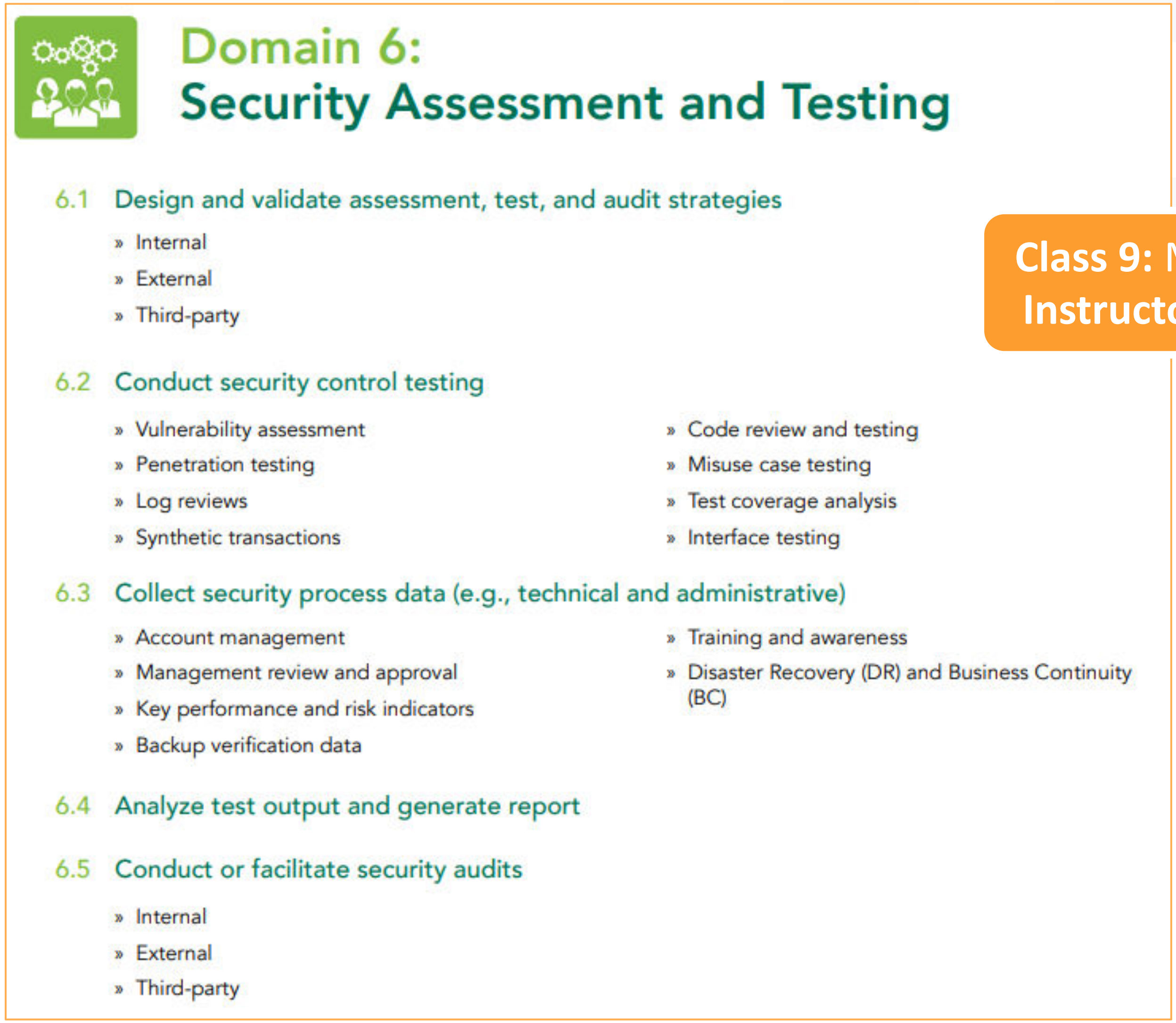
CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE

May 12th - BREAK

CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE



Domain 6: Security Assessment and Testing

6.1 Design and validate assessment, test, and audit strategies

- Internal
- External
- Third-party

6.2 Conduct security control testing

- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions
- Code review and testing
- Misuse case testing
- Test coverage analysis
- Interface testing

6.3 Collect security process data (e.g., technical and administrative)

- Account management
- Management review and approval
- Key performance and risk indicators
- Backup verification data
- Training and awareness
- Disaster Recovery (DR) and Business Continuity (BC)

6.4 Analyze test output and generate report

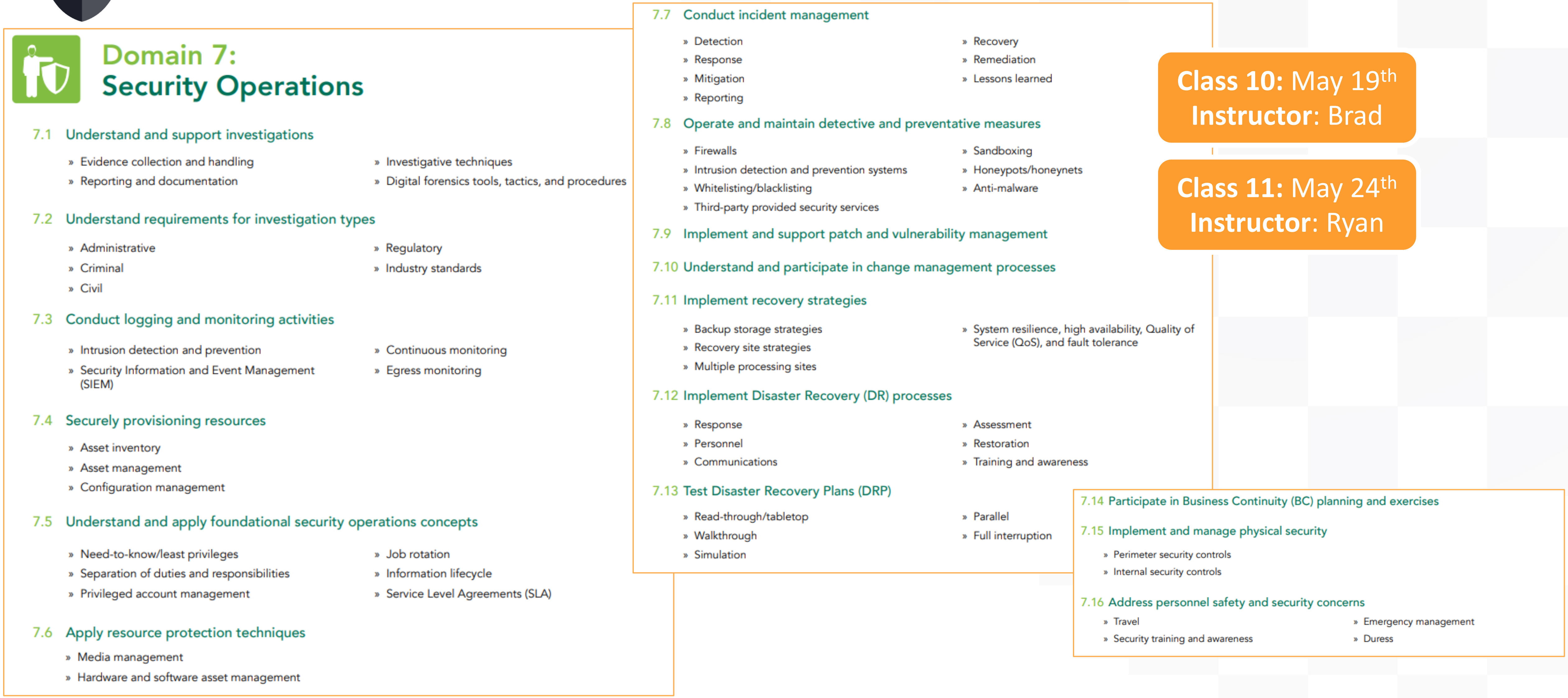
6.5 Conduct or facilitate security audits

- Internal
- External
- Third-party

Class 9: May 17th
Instructor: Ryan

CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE



Domain 7: Security Operations

7.1 Understand and support investigations

- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures

7.2 Understand requirements for investigation types

- Administrative
- Criminal
- Civil
- Regulatory
- Industry standards

7.3 Conduct logging and monitoring activities

- Intrusion detection and prevention
- Security Information and Event Management (SIEM)
- Continuous monitoring
- Egress monitoring

7.4 Securely provisioning resources

- Asset inventory
- Asset management
- Configuration management

7.5 Understand and apply foundational security operations concepts

- Need-to-know/least privileges
- Separation of duties and responsibilities
- Privileged account management
- Job rotation
- Information lifecycle
- Service Level Agreements (SLA)

7.6 Apply resource protection techniques

- Media management
- Hardware and software asset management

7.7 Conduct incident management

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

7.8 Operate and maintain detective and preventative measures

- Firewalls
- Intrusion detection and prevention systems
- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware

7.9 Implement and support patch and vulnerability management

7.10 Understand and participate in change management processes

7.11 Implement recovery strategies

- Backup storage strategies
- Recovery site strategies
- Multiple processing sites
- System resilience, high availability, Quality of Service (QoS), and fault tolerance

7.12 Implement Disaster Recovery (DR) processes

- Response
- Personnel
- Communications
- Assessment
- Restoration
- Training and awareness

7.13 Test Disaster Recovery Plans (DRP)

- Read-through/tabletop
- Walkthrough
- Simulation
- Parallel
- Full interruption

7.14 Participate in Business Continuity (BC) planning and exercises

7.15 Implement and manage physical security

- Perimeter security controls
- Internal security controls

7.16 Address personnel safety and security concerns

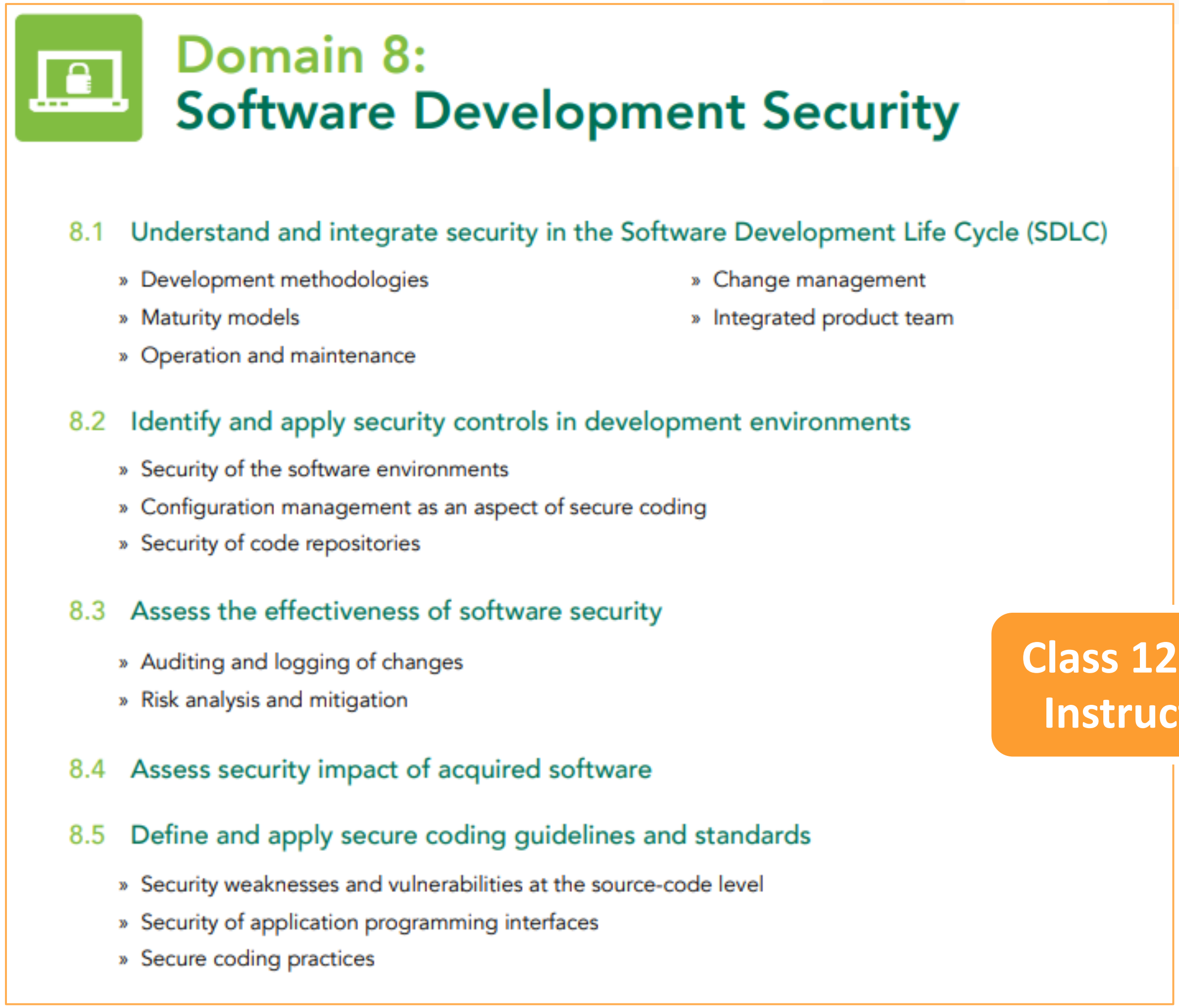
- Travel
- Security training and awareness
- Emergency management
- Duress

Class 10: May 19th
Instructor: Brad

Class 11: May 24th
Instructor: Ryan

CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE



Domain 8: Software Development Security

8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)

- Development methodologies
- Maturity models
- Operation and maintenance
- Change management
- Integrated product team

8.2 Identify and apply security controls in development environments

- Security of the software environments
- Configuration management as an aspect of secure coding
- Security of code repositories

8.3 Assess the effectiveness of software security

- Auditing and logging of changes
- Risk analysis and mitigation

8.4 Assess security impact of acquired software

8.5 Define and apply secure coding guidelines and standards

- Security weaknesses and vulnerabilities at the source-code level
- Security of application programming interfaces
- Secure coding practices

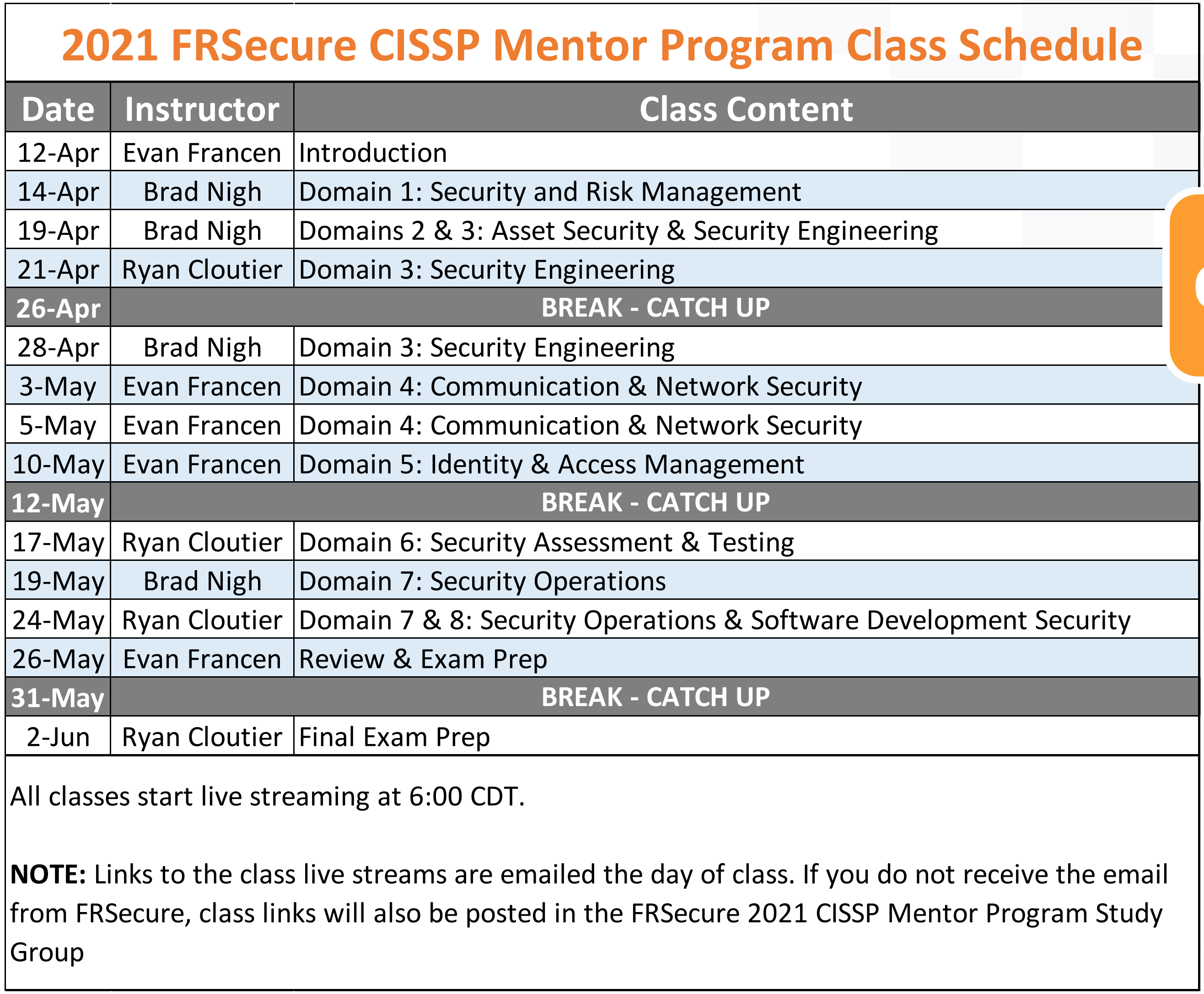
Class 12: May 26th
Instructor: Evan

CISSP Exam Final Preparation & Practice Testing

Class 12: May 26th
Class 13: June 2nd
Instructors: Evan, Brad, and Ryan

CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE



2021 FRSecure CISSP Mentor Program Class Schedule

Date	Instructor	Class Content
12-Apr	Evan Francen	Introduction
14-Apr	Brad Nigh	Domain 1: Security and Risk Management
19-Apr	Brad Nigh	Domains 2 & 3: Asset Security & Security Engineering
21-Apr	Ryan Cloutier	Domain 3: Security Engineering
26-Apr		BREAK - CATCH UP
28-Apr	Brad Nigh	Domain 3: Security Engineering
3-May	Evan Francen	Domain 4: Communication & Network Security
5-May	Evan Francen	Domain 4: Communication & Network Security
10-May	Evan Francen	Domain 5: Identity & Access Management
12-May		BREAK - CATCH UP
17-May	Ryan Cloutier	Domain 6: Security Assessment & Testing
19-May	Brad Nigh	Domain 7: Security Operations
24-May	Ryan Cloutier	Domain 7 & 8: Security Operations & Software Development Security
26-May	Evan Francen	Review & Exam Prep
31-May		BREAK - CATCH UP
2-Jun	Ryan Cloutier	Final Exam Prep

All classes start live streaming at 6:00 CDT.

NOTE: Links to the class live streams are emailed the day of class. If you do not receive the email from FRSecure, class links will also be posted in the FRSecure 2021 CISSP Mentor Program Study Group

Once again, for reference…

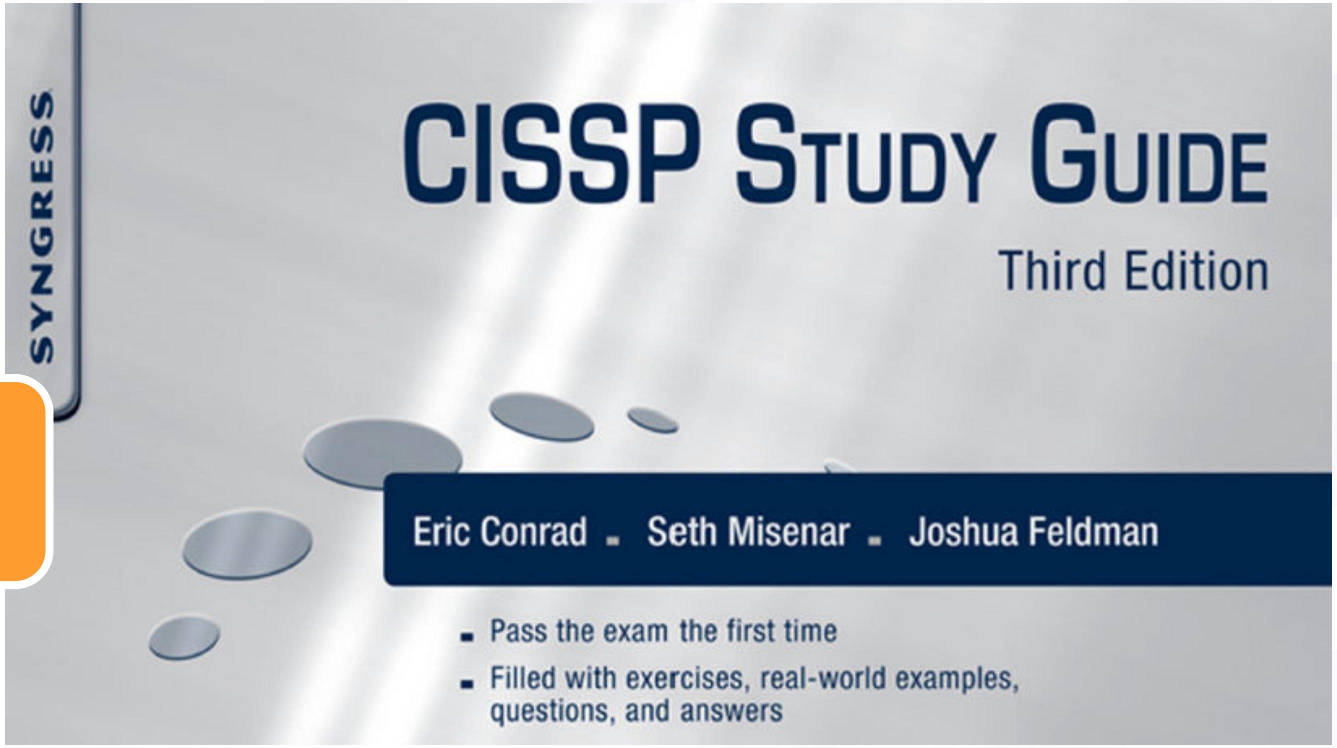
THE BOOK

CISSP Study Guide – Third Edition

Title: CISSP Study Guide, Third Edition (Paperback) by Eric Conrad, Seth Misenar, & Joshua Feldman.

- ISBN-10: 0128024372
- ISBN-13: 978-0128024379

WAIT! This book is more than five years old!

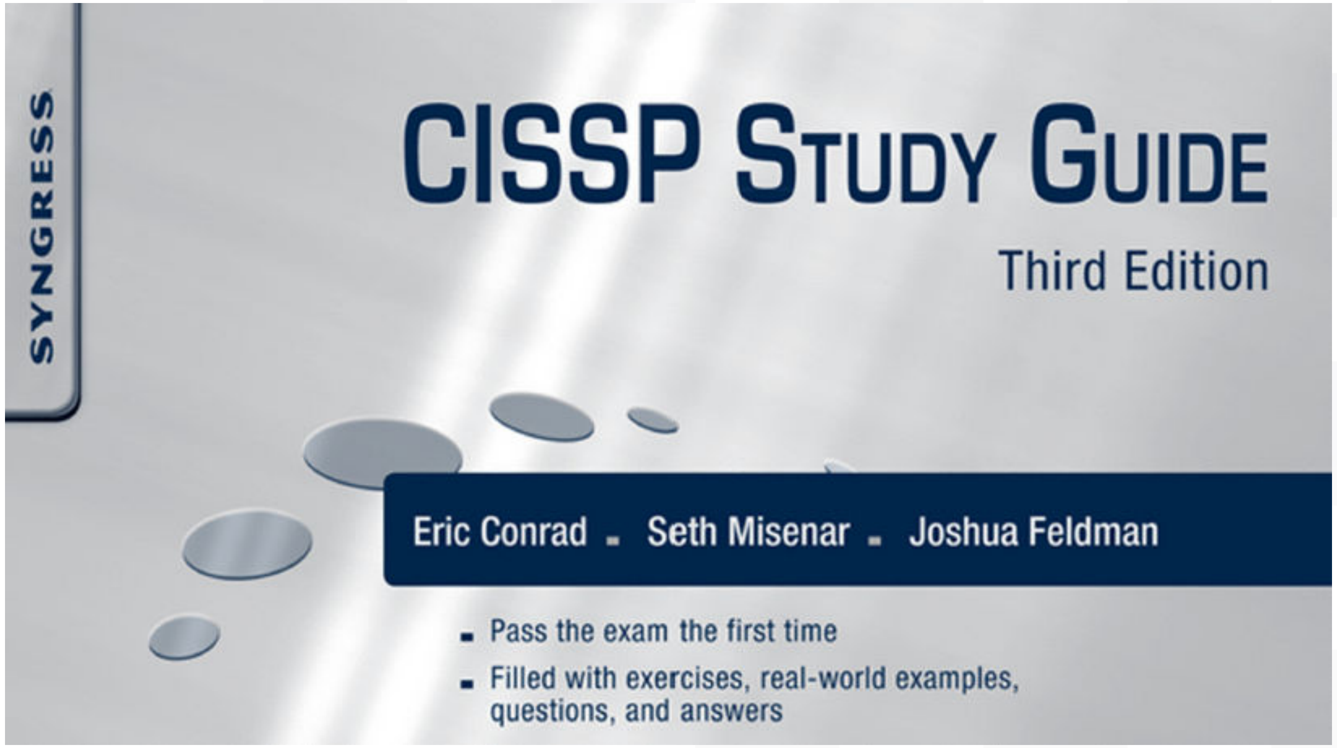

SYNGRESS
CISSP STUDY GUIDE
Third Edition
Eric Conrad ▪ Seth Misenar ▪ Joshua Feldman
▪ Pass the exam the first time
▪ Filled with exercises, real-world examples, questions, and answers

CISSP® MENTOR PROGRAM – SESSION ONE

THE BOOK

CISSP Study Guide – Third Edition

- If you don't have it, you can get it in a variety of place; Amazon, Elsevier, Borders, etc.
- I prefer the book in Adobe Acrobat format; easy reference and copy/paste capabilities.


SYNGRESS
CISSP STUDY GUIDE
Third Edition
Eric Conrad
Seth Misenar
Joshua Feldman
Pass the exam the first time
Filled with exercises, real-world examples, questions, and answers

CISSP® MENTOR PROGRAM – SESSION ONE

READY?! LET'S DIG IN.

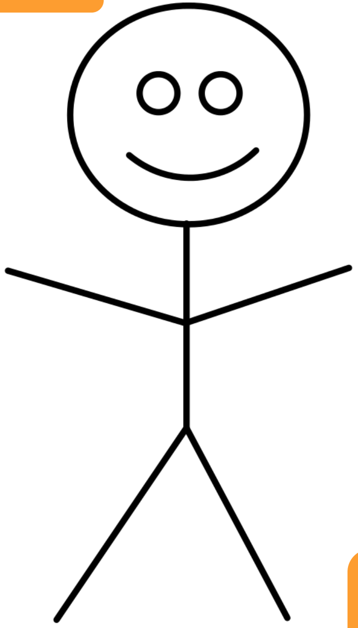
BTW. Dogs are cool.

CHAPTER 1 - INTRODUCTION

EXAM OBJECTIVES IN THIS CHAPTER

- How to prepare for the Exam
- How to take the Exam

Stick with it!



You ARE NOT required to take the exam!

Everybody has their own pace.

Everybody has their own method.

Get it?! "Stick" with it?

Sorry, that was dumb…

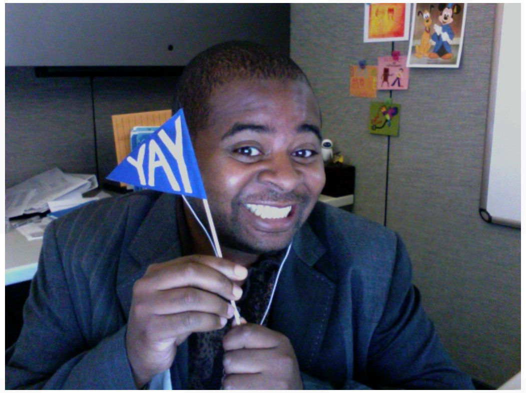
CHAPTER 1 - INTRODUCTION

How to take the Exam

- Used to be six hours and 250 questions.
- Now it's three hours and 150 questions! (**not in the book**)
- Computer-based testing ("CBT") at Pearson Vue, used to be paper and pencil (Evan's old!)
- Two (sort of four) types of questions:
  - Multiple Choice (four options, two are almost obviously wrong)
  - "Advanced Innovative"
    - Scenario
    - Drag/Drop
    - Hotspot

All this is valid, but you may have heard the CISSP exam is changing…

On May 1st, we're getting a "Domain Refresh"!



CHAPTER 1 - INTRODUCTION

CISSP Domain Refresh FAQs (https://www.isc2.org/Certifications/CISSP/Domain-Refresh-FAQ)

How is the CISSP exam changing?

"As a result of the content refresh, we have updated some of the domain names to describe the topics accurately. For details on the exam domain and subdomain changes, review our CISSP Domain Refresh guide." (https://www.isc2.org/-/media/ISC2/Certifications/Domain-Refresh/CISSP-Domain-Refresh.ashx) .

NOTE: Content HAS NOT been officially published by (ISC)² yet; however, we will cover the changes (including content) in the CISSP Mentor Program.

CISSP® MENTOR PROGRAM – SESSION ONE

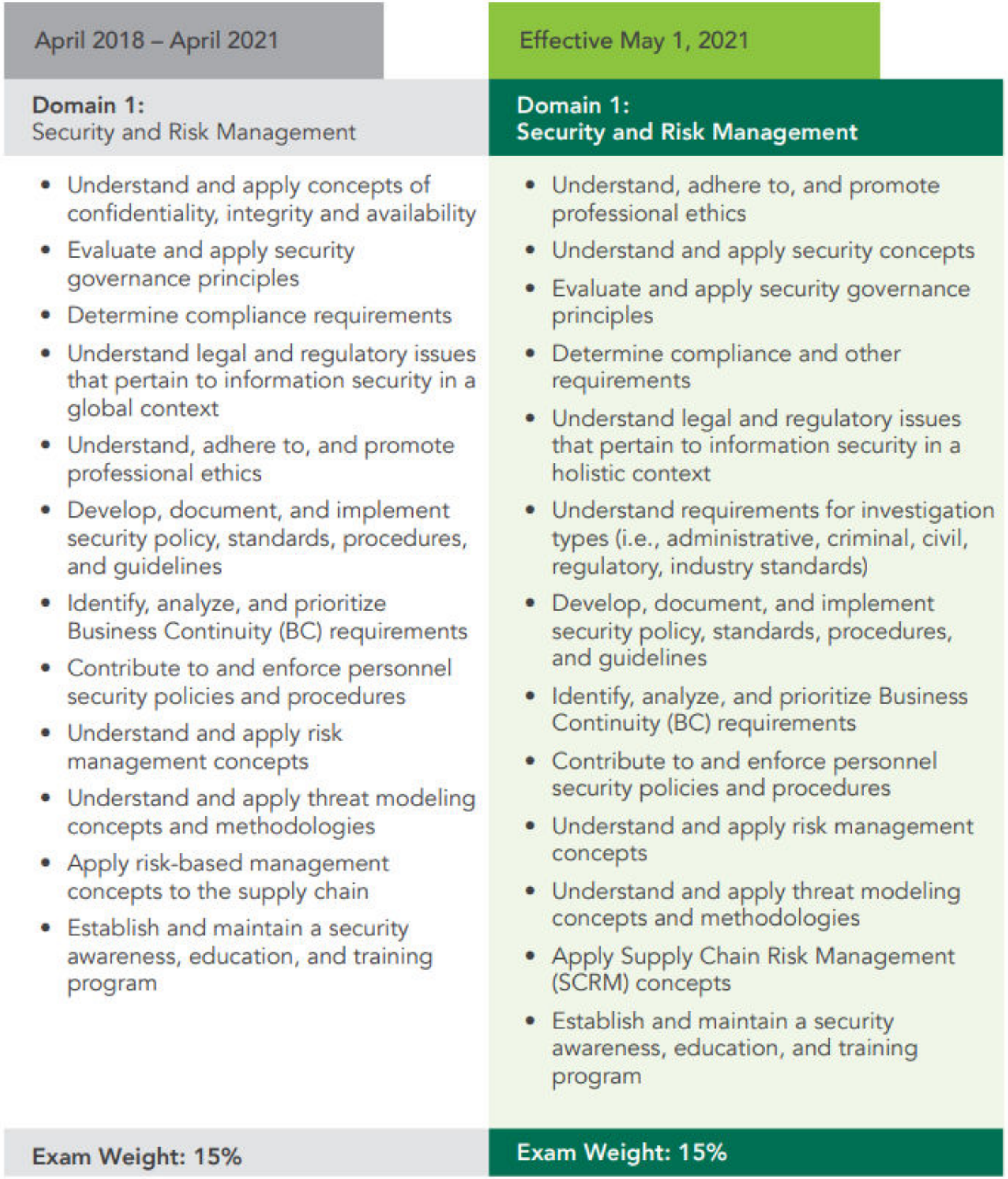
CHAPTER 1 - INTRODUCTION

CISSP Domain Refresh

CISSP® MENTOF

CHAPTE

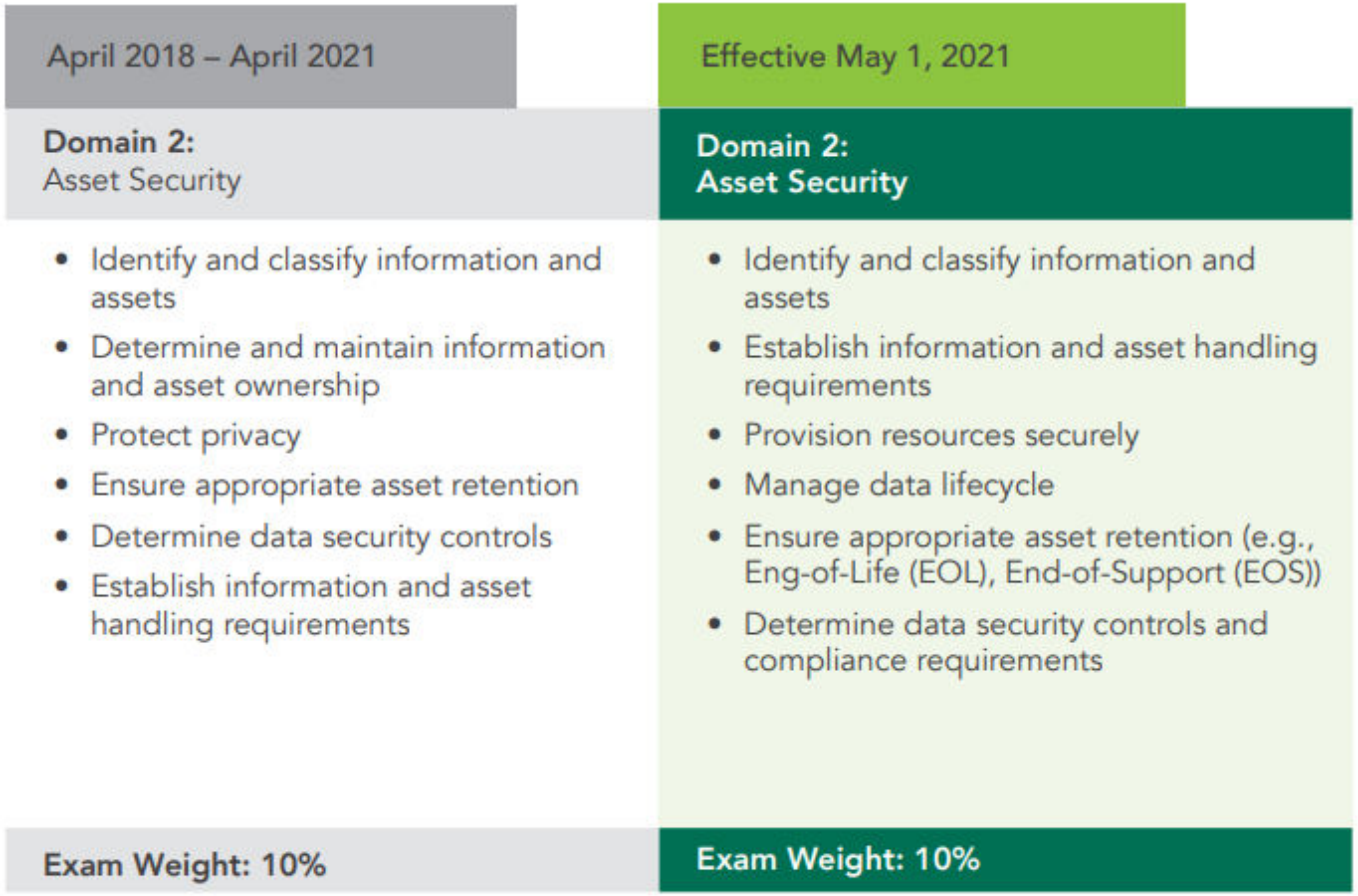
CISSP Domai



April 2018 – April 2021	Effective May 1, 2021
Domain 1: Security and Risk Management	**Domain 1:** **Security and Risk Management**
• Understand and apply concepts of confidentiality, integrity and availability • Evaluate and apply security governance principles • Determine compliance requirements • Understand legal and regulatory issues that pertain to information security in a global context • Understand, adhere to, and promote professional ethics • Develop, document, and implement security policy, standards, procedures, and guidelines • Identify, analyze, and prioritize Business Continuity (BC) requirements • Contribute to and enforce personnel security policies and procedures • Understand and apply risk management concepts • Understand and apply threat modeling concepts and methodologies • Apply risk-based management concepts to the supply chain • Establish and maintain a security awareness, education, and training program	• Understand, adhere to, and promote professional ethics • Understand and apply security concepts • Evaluate and apply security governance principles • Determine compliance and other requirements • Understand legal and regulatory issues that pertain to information security in a holistic context • Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards) • Develop, document, and implement security policy, standards, procedures, and guidelines • Identify, analyze, and prioritize Business Continuity (BC) requirements • Contribute to and enforce personnel security policies and procedures • Understand and apply risk management concepts • Understand and apply threat modeling concepts and methodologies • Apply Supply Chain Risk Management (SCRM) concepts • Establish and maintain a security awareness, education, and training program
Exam Weight: 15%	**Exam Weight: 15%**

CHAPTER 1 - INTRODUCTION

CISSP Dom

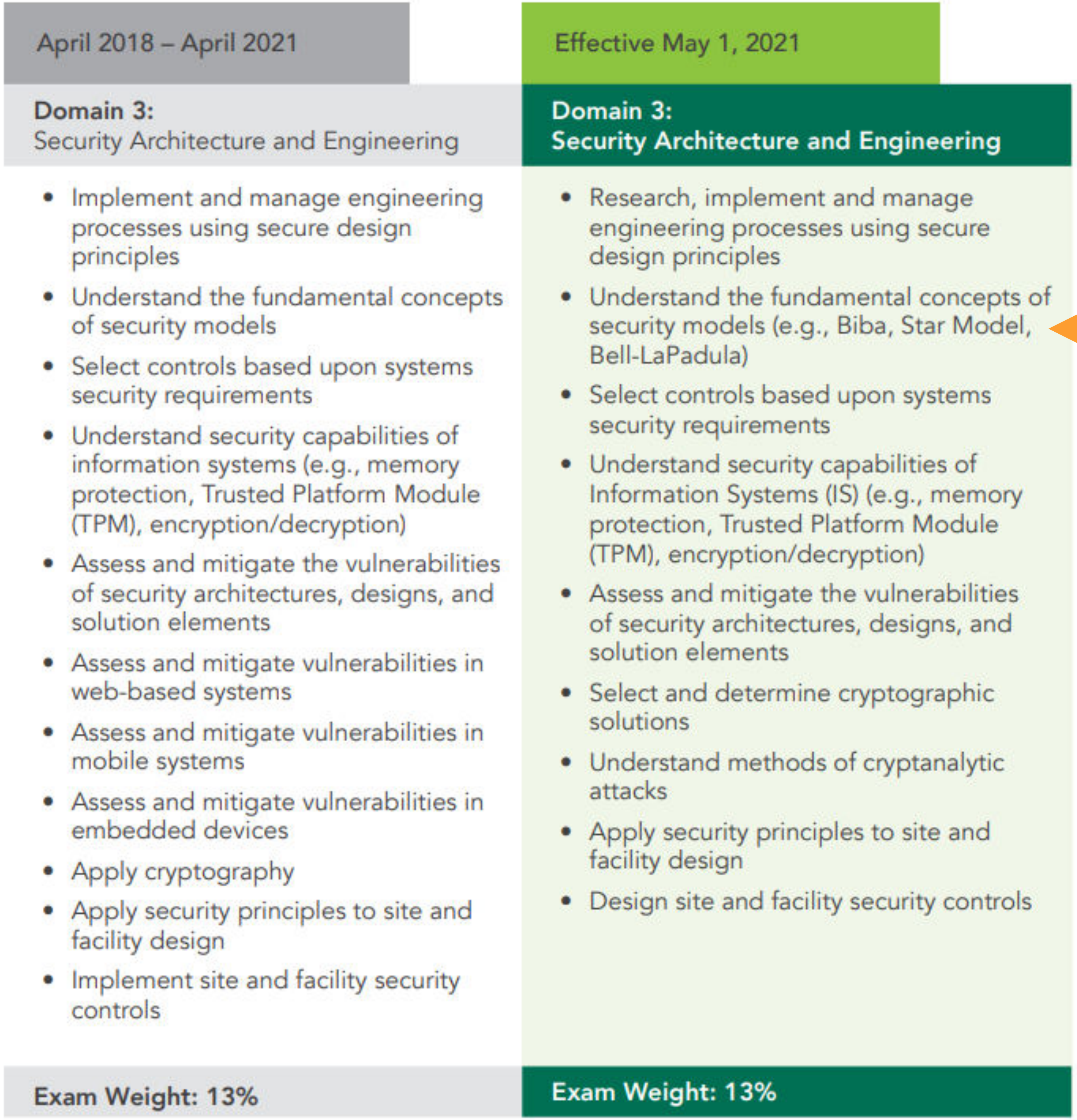


April 2018 – April 2021	Effective May 1, 2021
Domain 2: Asset Security	**Domain 2:** **Asset Security**
• Identify and classify information and assets • Determine and maintain information and asset ownership • Protect privacy • Ensure appropriate asset retention • Determine data security controls • Establish information and asset handling requirements	• Identify and classify information and assets • Establish information and asset handling requirements • Provision resources securely • Manage data lifecycle • Ensure appropriate asset retention (e.g., Eng-of-Life (EOL), End-of-Support (EOS)) • Determine data security controls and compliance requirements
Exam Weight: 10%	**Exam Weight: 10%**

CISSP® MEN

CHAPT

CISSP Don



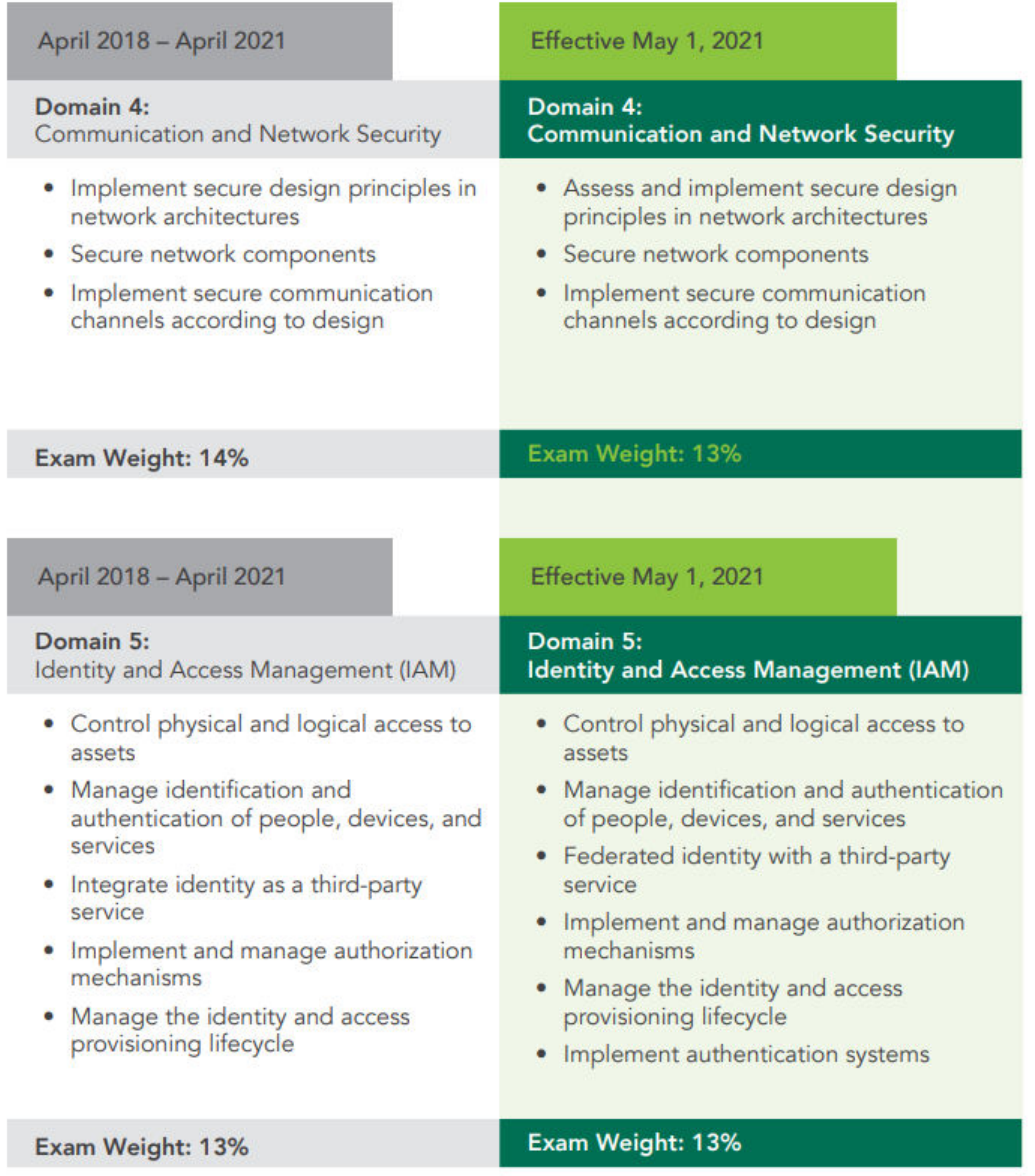
April 2018 – April 2021	Effective May 1, 2021
Domain 3: Security Architecture and Engineering	**Domain 3:** **Security Architecture and Engineering**
• Implement and manage engineering processes using secure design principles • Understand the fundamental concepts of security models • Select controls based upon systems security requirements • Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption) • Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements • Assess and mitigate vulnerabilities in web-based systems • Assess and mitigate vulnerabilities in mobile systems • Assess and mitigate vulnerabilities in embedded devices • Apply cryptography • Apply security principles to site and facility design • Implement site and facility security controls	• Research, implement and manage engineering processes using secure design principles • Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula) • Select controls based upon systems security requirements • Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption) • Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements • Select and determine cryptographic solutions • Understand methods of cryptanalytic attacks • Apply security principles to site and facility design • Design site and facility security controls
Exam Weight: 13%	**Exam Weight: 13%**

Sort of wish we could have spared you this. ☹

CISSP® MENTOI

CHAPTE

CISSP Domai



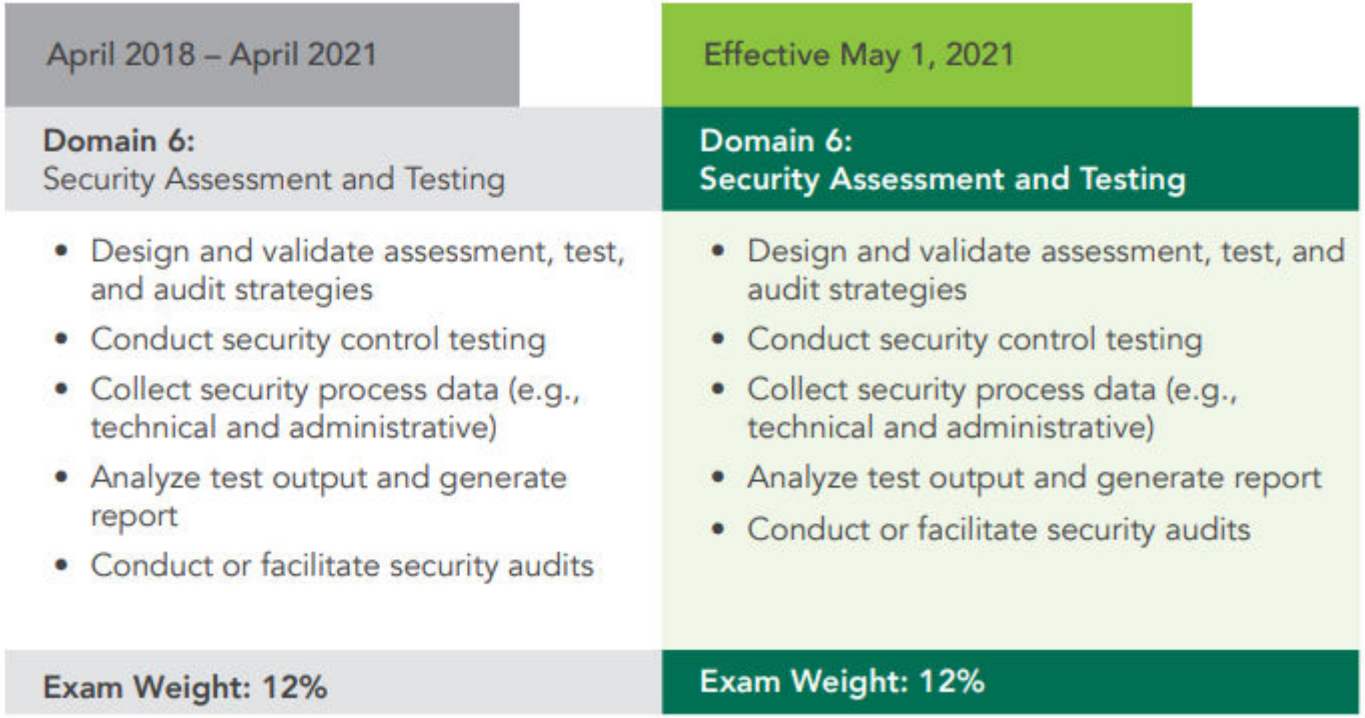
April 2018 – April 2021	Effective May 1, 2021
Domain 4: Communication and Network Security	**Domain 4:** **Communication and Network Security**
• Implement secure design principles in network architectures • Secure network components • Implement secure communication channels according to design	• Assess and implement secure design principles in network architectures • Secure network components • Implement secure communication channels according to design
Exam Weight: 14%	**Exam Weight: 13%**

April 2018 – April 2021	Effective May 1, 2021
Domain 5: Identity and Access Management (IAM)	**Domain 5:** **Identity and Access Management (IAM)**
• Control physical and logical access to assets • Manage identification and authentication of people, devices, and services • Integrate identity as a third-party service • Implement and manage authorization mechanisms • Manage the identity and access provisioning lifecycle	• Control physical and logical access to assets • Manage identification and authentication of people, devices, and services • Federated identity with a third-party service • Implement and manage authorization mechanisms • Manage the identity and access provisioning lifecycle • Implement authentication systems
Exam Weight: 13%	**Exam Weight: 13%**

CISSP® MENTOR PROGRAM – SESSION ONE

CHAPTER 1 - INTRODUCTION

CISSP Domain Refresh

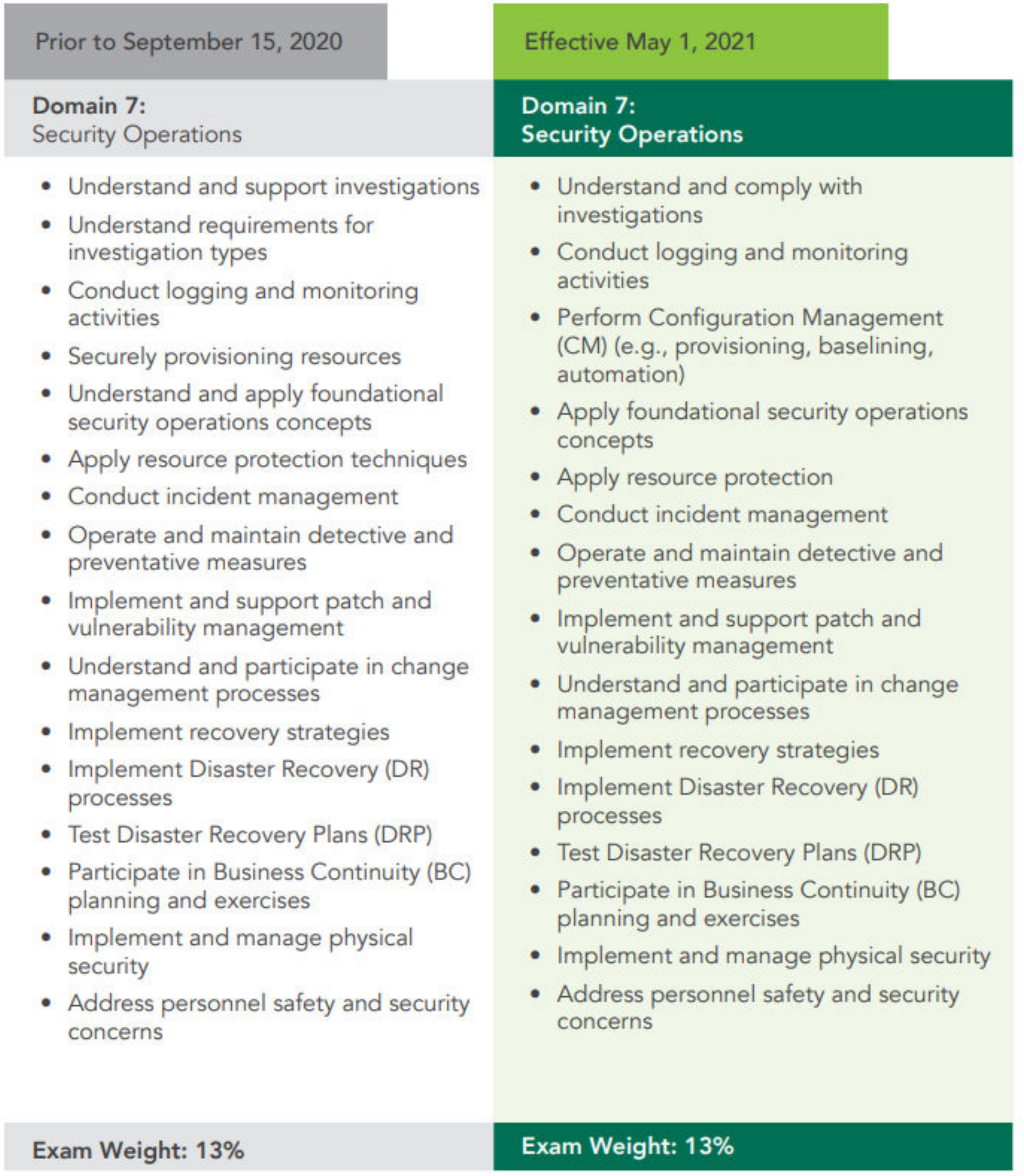


April 2018 – April 2021	Effective May 1, 2021
Domain 6: Security Assessment and Testing	**Domain 6:** **Security Assessment and Testing**
• Design and validate assessment, test, and audit strategies • Conduct security control testing • Collect security process data (e.g., technical and administrative) • Analyze test output and generate report • Conduct or facilitate security audits	• Design and validate assessment, test, and audit strategies • Conduct security control testing • Collect security process data (e.g., technical and administrative) • Analyze test output and generate report • Conduct or facilitate security audits
Exam Weight: 12%	**Exam Weight: 12%**

CISSP® MENTOR

CHAPTE

CISSP Domai

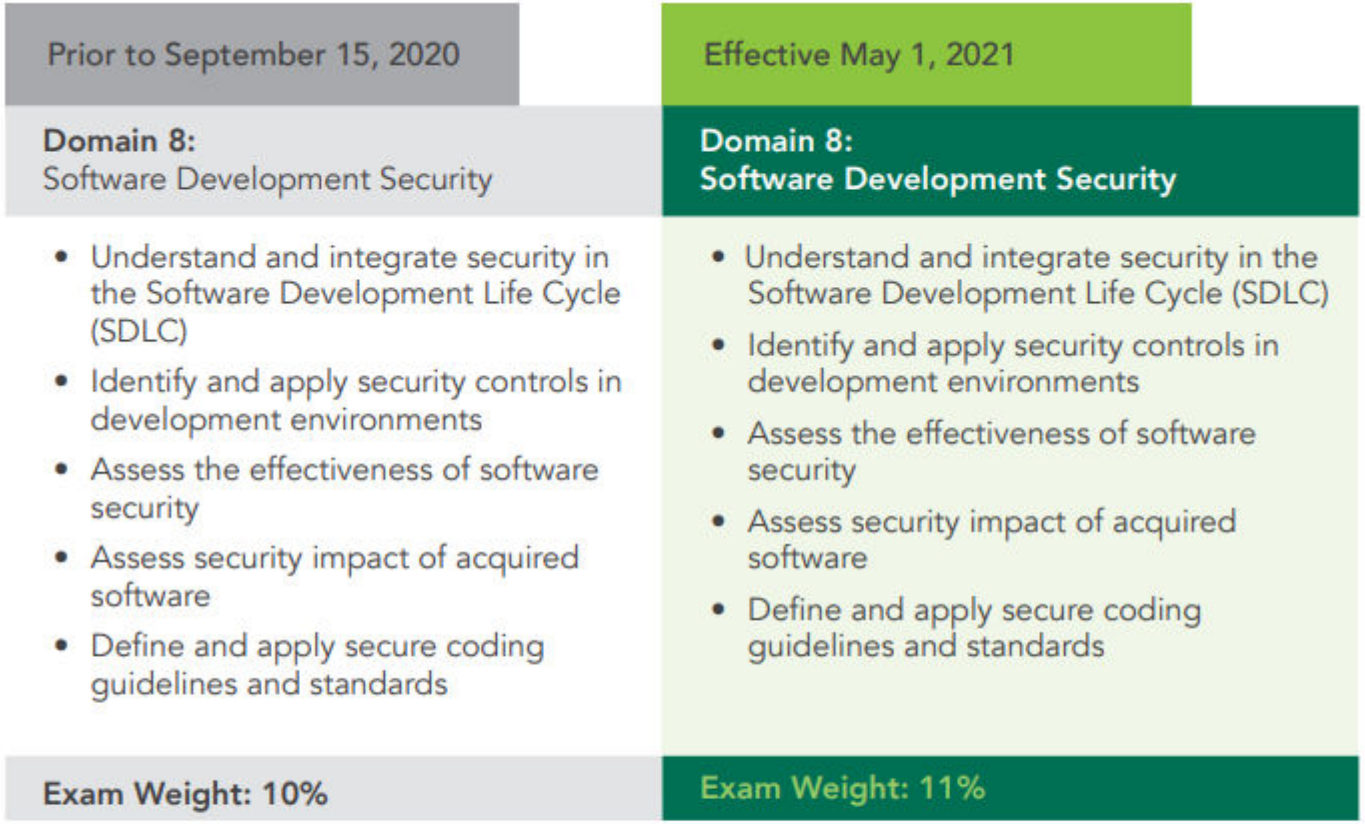


Prior to September 15, 2020	Effective May 1, 2021
Domain 7: Security Operations	**Domain 7:** **Security Operations**
• Understand and support investigations • Understand requirements for investigation types • Conduct logging and monitoring activities • Securely provisioning resources • Understand and apply foundational security operations concepts • Apply resource protection techniques • Conduct incident management • Operate and maintain detective and preventative measures • Implement and support patch and vulnerability management • Understand and participate in change management processes • Implement recovery strategies • Implement Disaster Recovery (DR) processes • Test Disaster Recovery Plans (DRP) • Participate in Business Continuity (BC) planning and exercises • Implement and manage physical security • Address personnel safety and security concerns	• Understand and comply with investigations • Conduct logging and monitoring activities • Perform Configuration Management (CM) (e.g., provisioning, baselining, automation) • Apply foundational security operations concepts • Apply resource protection • Conduct incident management • Operate and maintain detective and preventative measures • Implement and support patch and vulnerability management • Understand and participate in change management processes • Implement recovery strategies • Implement Disaster Recovery (DR) processes • Test Disaster Recovery Plans (DRP) • Participate in Business Continuity (BC) planning and exercises • Implement and manage physical security • Address personnel safety and security concerns
Exam Weight: 13%	**Exam Weight: 13%**

CISSP® MENTOR PROGRAM – SESSION ONE

CHAPTER 1 - INTRODUCTION

CISSP Domain Refresh



Prior to September 15, 2020	Effective May 1, 2021
Domain 8: Software Development Security	**Domain 8:** **Software Development Security**
• Understand and integrate security in the Software Development Life Cycle (SDLC) • Identify and apply security controls in development environments • Assess the effectiveness of software security • Assess security impact of acquired software • Define and apply secure coding guidelines and standards	• Understand and integrate security in the Software Development Life Cycle (SDLC) • Identify and apply security controls in development environments • Assess the effectiveness of software security • Assess security impact of acquired software • Define and apply secure coding guidelines and standards
Exam Weight: 10%	**Exam Weight: 11%**

CISSP® MENTOR PROGRAM – SESSION ONE

BONUS – INFORMATION SECURITY FUNDAMENTALS

What is Information Security?

- This is a question for you.
- This is a question that our industry still struggles with.
- Don't forget this…

Information security is managing risks to the confidentiality, integrity, and availability of information using administrative, physical and technical controls.

Will also accept…

Information security is the set of rules, plans, and actions taken to protect people and information.

BONUS – INFORMATION SECURITY FUNDAMENTALS

What is Information Security?

- This is a question for you.
- This is a question that our industry still struggles with.
- Don't forget this…

It is **NOT** eliminating risk!

Information security is **managing risks** to the confidentiality, integrity, and availability of information using administrative, physical and technical controls.

BONUS – INFORMATION SECURITY FUNDAMENTALS

What is Information Security?

- This is a question for you.
- This is a question that our industry still struggles with.
- Don’t forget this…

People often over-emphasize this,

Information security is **managing risks** to the **confidentiality**, **integrity**, and **availability** of information using administrative, physical and technical controls.

Balance.

BONUS – INFORMATION SECURITY FUNDAMENTALS

What is Information Security?

- This is a question for you.
- This is a question that our industry still struggles with.
- Don’t forget this…

Information security is **managing risks** to the **confidentiality**, **integrity**, and **availability** of information using **administrative**, **physical** and **technical** controls.

Who cares about your firewall if I can steal your server?

It is **NOT** (only) and IT issue!

It’s easier to go through your secretary than your firewall!

CISSP® MENTOR PROGRAM – SESSION ONE

BONUS – INFORMATION SECURITY FUNDAMENTALS

What is Risk?

- This is a question for you.
- This is another question that our industry still struggles with.
- Don't forget this (either)…

Yes, 100%, absolutely, and please.

NO!

Maybe

NO!

BONUS – INFORMATION SECURITY FUNDAMENTALS

What is Risk?

- This is a question for you.
- This is another question that our industry still struggles with.
- Don’t forget this (either)…

Risk is the likelihood of something bad happening and the impact if it did.

These are derived from threats and vulnerabilities!

BONUS – INFORMATION SECURITY FUNDAMENTALS

Ten Information Security Principles

1. A business is in business to make money.
2. Information Security is a business issue.
3. Information Security is fun.
4. People are the biggest risk.
5. “Compliant” and “secure” are different.

Not necessarily on the exam, but these will serve you well!

BONUS – INFORMATION SECURITY FUNDAMENTALS

Ten Information Security Principles

6. There is no common sense in Information Security.
7. "Secure" is relative.
8. Information Security should drive business.
9. Information Security is not one size fits all.
10. There is no "easy button".

You Dig?!

Not necessarily on the exam, but these will serve you well!

THAT’S IT. NEXT?

That’s it for today…

- We’re very excited that we get to be a part of your information security career journey!
- This will be a rewarding experience.

For most of you:

This will get hard. This will seem dry. This will seem overwhelming.

Don’t give up!

CISSP® MENTOR PROGRAM – SESSION ONE

THAT’S IT. NEXT?

That’s it for today…

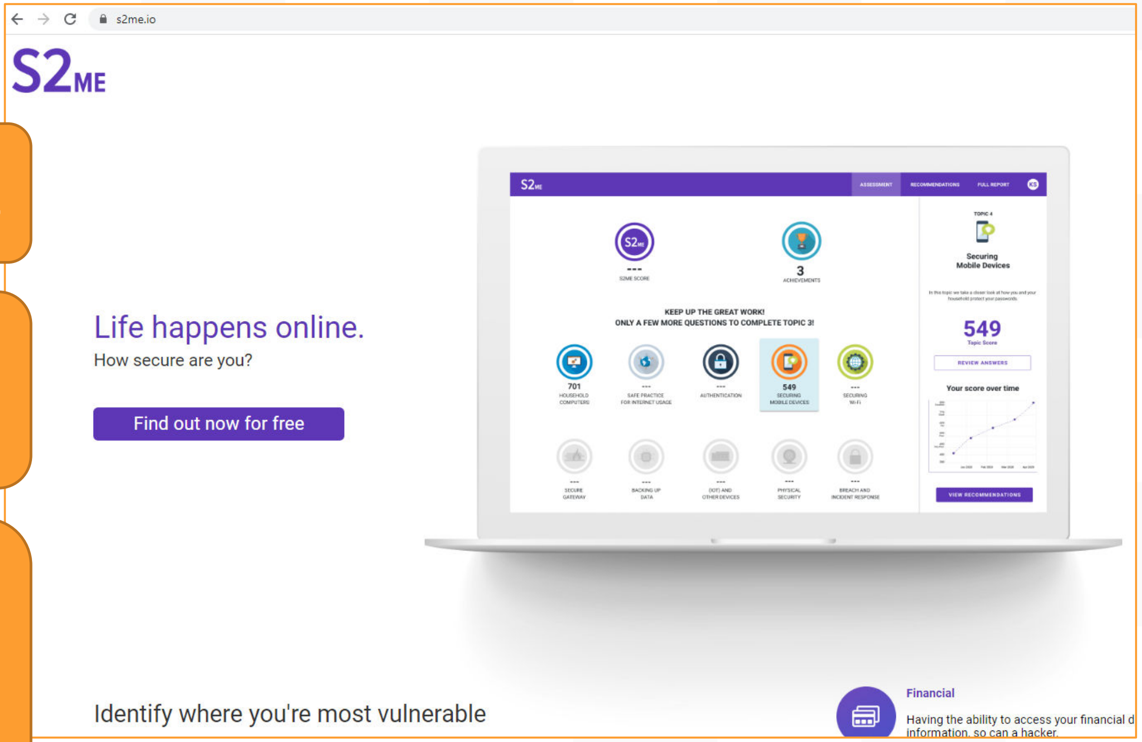
- Homework for Wednesday (4/14):
  - Do your **S²Me** – https://s2me.io. Tell at least two friends and/or family members to do it too!

Your homework.

Information security is a LIFE SKILL.

Information security, privacy and safety cannot be separated.

Telling others helps build confidence to talk to others about information security.



s2me.io

S2ME

Life happens online.

How secure are you?

Find out now for free

Identify where you're most vulnerable

Financial

Having the ability to access your financial d information, so can a hacker.

THAT'S IT. NEXT?

That's it for today…

Your homework.

- Homework for Wednesday (4/14):
  - Do your **S²Me** – https://s2me.io. Tell at least two friends and/or family members to do it too!
  - Please get the book if you haven't already.
  - Please read Chapter 1 (pages 1 – 10).
  - We will be covering Chapter 2 Domain 1: Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity) on Wednesday.

Evan Francen
@evanfrancen

Brad Nigh
@BradNigh

Ryan Cloutier ("cola")
@CLOUTIERSEC

See you Wednesday!