Summary of the Event

I arrived to the venue on Monday 20th at 7:30am, I was provided everything necessary to teach the class. There was some confusion from the audience, as some of them had received notification that the class would start at 9am, instead of 8:30am as the ASPE guidelines recommend. We agreed as a group that we would start daily at 8:30am, stop for a break in the morning, have an hour break for lunch around noon-time and then one break in the afternoon. Class would finish at 4:30pm.

This schedule worked fine for the whole week. As I explained the materials, I focused and extended over the subjects where they expressed questions or their own opinions. When the class went silent or uninterested on a particular slide, I shared experiences from my own pains or successes in order to drive them to empathize or inquire more details about the situation.

Minor detail, lunch catering interrupted the class on Tuesday, so on Wednesday and on; I decided to start the lunch break close to noon-time, based on a convenient change of topic in the slides, instead of someone calling our attention through the glass.

It's relevant to mention that I finished the material for the DevSecOps course on Wednesday afternoon, so I started with the SRE workshop right after a small break there.

If you would like more details about the session, I wrote a facilitator guide for the DevSecOps course, it has ten pages of details on how I teach the DevSecOps class. Please contact ASPE to request this, as I delivered it to them, and it's under their review.

Successes

Exercise A (Value Stream Mapping), Exercise B (Threat Modeling) and the Discussion about IAM applied to Microservices were the most engaging activities. Groups were committed to work on the exercises to their full extent and they showed and explained their diagrams.

* Most of them had not worked in a Value Stream Mapping diagram.
* None of them had worked in a Threat Model before.
* Some of them questioned why a "Threat Model" was not a requirement for their "Definition of Ready" when reviewing applications that need to be published in live environments.

Our Lab Activity involving Gitlab SaaS and passive security check in a security-weak sandbox page worked for all attendants, and it took a longer while for some. I felt relieved that I decided to focus on a lab activity without command line skills requirement, because that would've taken more time, and it might have frustrated some people in the room.

Concerns

Exercise C of the DevSecOps workshop required some walkthrough and hand-holding, the expectation of a Security Profile of an organization is a high level of abstraction that needs more analysis and familiarity with the Security Control Families. This activity was based on classifications from the Security Control Profiles for Cloud Based IT services written by the Government of Canada, which is conversely based on the NIST Cloud Computing Security Reference Architecture [SP 500-299]. In any new instance of such workshop, I would replace that exercise with an activity where the audience learns how to determine the severity of risks, according to [OWASP's Repeatable Method](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Repeatable_Method).

Exercise E was a challenge to get people involved, as the audience seemed frustrated from seeing their teams reduced in numbers in the recent past, while they're also constantly pushed to achieve more things in less time. This subject came up more than once, because the materials advocate for close feedback loops and testing closer to the left of the Development Cycle; but their experience has shown them how leaders at U. of Phoenix prefer to assign resources for new features, rather than automated testing to safely deliver and support quality products. I geared myself into "motivational mode" and drove the conversation to the fact that approving budget and 40 hours of their time for the workshop was definitely a sign that leadership wanted to good practices in place.

When it comes to the SRE workshop, exercises are heavily dependent of having the book available in physical form to read use cases, the degree of technical detail makes it impossible for the facilitator to memorize them all. When I was told that the audience would have the book available, it was my impression that each attendant would be given a hard-copy of the book. This was not the case, and the reading experience from the online book or a PDF is extremely different, because laptops are full of distractions like email notifications, Microsoft Teams, etc.

I worked around this limitation by asking some of them to read out loud paragraphs with a few SRE books that Travis Hill brought in on Thursday. I gave the cue calling someone's name at the start of a paragraph, while the rest of the audience followed reading from their laptops. Tone of voice and cadence of different readers helped me to overcome this difficulty. I'm confident that providing books to the audience will enrich the experience for the SRE book.

Discussions/Interests of Attendees

Audience was heterogenous and there was people from many different roles, but there was only one manager (Andy Kaschl). Success in a digital transformation requires continued and consistent Leadership commitment, and the notable absence of Managers was not helpful to reinforce the learning process for the Technical audience.

The broad sample of roles in the audience helped us to build rich conversations and there was a request to have more information about rollback procedures when deploying software in the SRE workshop. I consulted with ASPE and they validated that it was ok to explain this subject from my own experience with a sample on the whiteboard.

There's one thing that everyone considered important for their current transformation phase: clear goals. Exercise A helped them to pinpoint some common security goals, then Exercise E created the opportunity to find ways to incentivize themselves through : simplification of processes, consolidation of tools (e.g. the multiple helpdesk ticket systems they have) to reduce rework, and standardization of formats; among others. But they don't feel leadership budgets enough time to do things right and automate where necessary; which ends up creating more technical debt.

I was asked a couple of times if there were plans to provide training to other teams, they seemed interested to get more people trained with these methodologies.