

Questionnaire – Demographic Questions

1. What is your current role in the company?

see 2

2. What kind of tasks do you usually do in your work?

Right now I'm doing automation for our service elements, so I'll try to get from our pools of host management controllers information out of them to do some kind of a state analysis where we are with driver versions and stuff like that Basically, I'm working with Ansible as the automation language and I have had nice journey automating provisioning from build workers and different flavors for C systems for x86 systems with Ubuntu with Red Hat with What else Centos, well, basically Red Hat, but the low cost version of it Yeah, and then we made up a quite nice role-based Suite of things which are bringing up a machine Installing everything on to the machine make it secure provision user management as well with some of our homegrown tools and Well doing as well some kind of analysis of states of the build workers by seppics That's not my main area. We have a specialist for it and But you need to take care of your environment if it's still sane and Responsive all the machines. So Basically what I left behind now to get our pool of service elements being automated.

3. Given enough time, can you understand the architecture of an application system that is described using an IaC script of an IaC technology you are familiar with?

Yes

4. For how many years have you worked on tasks associated with IaC tools?

6 years

5. How large is the company you currently work for?

>100K

Questionnaire – Compliance Rule Modeling and Checking

6. How do you check the compliance of the software applications of your company?

Company-provided tool, which is calling a pearl script, which is looking at table-based Database which RPMs should have which version so we do daily a completely scan of installed RPMs on the machines and feed this back against the table of the suggested Versioning they expect us to have And as well with this versioning and there is some kind of security vulnerability messages with it.

7. Do you use well-defined models for the compliance rules applicable to the software applications of your company?

No, definitely no, okay, this is this is one of our endeavors we daily have in terms of what do they want from us in terms of security.

a) If so, how do you define them?

8. Do you think having a well-defined and machine-readable format for compliance rules reduces the complexity associated with checking them?

The magic is to map the machine readable stuff into this risk-based approach process

9. Do you think having a well-defined and machine-readable format for compliance rules reduces the uncertainty associated with interpreting them?

Yeah (also look at answer 7)

10. How often do you have to deal with new compliance rules?

Sometimes three months, but I would expect that this is now going into this range of half a year.

11. How much do you agree with the following statement: *using IACMF reduces the effort associated with defining and checking compliance rules?*

I do have to build up my own Catalog (of compliance rules)? Each and everyone needs the same kind of catalog. So why not doing this in library for everybody? If there is a library I would have I would totally agree. If I do it if I have to do it on my own, I would go into the direction of a disagreement

12. How much do you agree with the following statement: *using IACMF reduces the complexity associated with defining and checking compliance rules?*

A four

13. How much do you agree with the following statement: *using well-defined models for compliance rules reduces the uncertainty associated with interpreting them?*

With a well-defined I would say five

Questionnaire – Architectural Reconstruction

14. How do you reconstruct the architecture of running application instances you need to understand?

For configuration: The security tool is querying the package manager of the operating systems so they are able to look into windows. They are able to look into Ubuntu, Centos You name it.

For architecture: It was the hardest time in our Docker environment to get the clue about of how many images are stacked together into one container and which container is interacting with another one. We did this by asking around and by going into Docker and having a look what is stacked upon and I thought that's really reverse engineering at its most painful state.

15. Do you use any (semi-)automated tools for this purpose?

No

16. How much do you agree with the following statement: *using IACMF reduces the effort associated with reconstructing the architecture of running application instances?*

so, I would expect that this is this is this is something everybody's needing so there are lots of homegrown environments and if this is taking the rate the right corporation part so I expect that this will flourish like this Ansible stuff that the community supporting and growing these plugins as they are needed and helping

(Interviewer: So if there is such a community and you have something like a repository of plugins you would totally agree that the effort will be reduced?)

Okay. Definitely. Yeah

And even though if you if you invest first and have your plugin afterwards you do have it so Can work with this tooling and some time that it needs to be invested.

(Interviewer: Okay, so it's not “totally disagree” if you don't already have the plugins. Yeah, it's a bit better than one?)

Yep

Questionnaire – Compliance Violation Fixing

17. What do you do if you find out that a running application instance violates a compliance rule?

The security tool gives a point or two one of the CVE databases for example to have a look here in terms of what should be done to this problem. Sometimes we have some complex situations where we need to evaluate ourselves to get a solution.

Then, we go into our Ansible roles where we set up the manipulations of the setting sort of configurations. Feed in the right way of doing things. So the most likely there are some variables which have to be set differently. Then you you feed this into our submission code and then get a first glance with a trial run and then afterwards you push it to the repository and have your fix in.

18. Do you use any (semi-)automated tools for this purpose?

See 17.

20. How much do you agree with the following statement: *using IACMF reduces the effort associated with fixing compliance violations?*

Would say we go to four because (we will have to) go and change our process in a way that we don't go in a controlled forward ways: We go in a default forward way and then we are going in a second round and fixing everything. it is some kind of this “You better make it safe the first time”. You will need to feed back this information in your setting up of the provisioning. That's the last point. I would say to not reaching the five.

21. How much do you agree with the following statement: *having well defined models for compliance jobs reduces the uncertainty associated with handling detected compliance violations?*

Nearly totally agree because of whenever you are in a hurry to get something fixed and you can fall back to something which was predefined or already has shown that it's on other installations is working you get close to this totally agree and there is no uncertainty anymore.

Questionnaire – General Questions

22. How do you evaluate the novelty of the framework?

I feel like there is something out which I'm not aware of already, so I think at least if you go and buy something you will find the one or the other opportunity to get something like this. (But not sure) if it is that flexible as I have seen so far and the big question behind this is how much of supporting libraries are there. (Furthermore, IACMF has) positive effects because of now somebody is able to get through stacks of information and applications and then there hierarchy and I would say yes, it's for me I would say a very new novel way of of going going this route.

23. How do you evaluate the extensibility of the framework?

Extensibility is always a nice thing to have. Oh no, it's a must have I would say because everything's changing all the way. So you want to adapt to the change and therefore, it's absolutely a must and yeah, (extensibility) is the concept of plugins is well known in terms of of this mechanism. I would say yeah, that's that's the way to go.

24. Would you use the framework in your work?

If you would give me a car with four wheels steering wheel and an engine no matter if it's electric or combustion. Yeah, would do a test ride.

a) If so, in which areas?

So you would go all the options in your test environment and then you can say okay evaluation of this was worthwhile or this was too much effort to get to the point. so I think, you can afterwards say no doubt we would or wouldn't apply this.

25. What is your general impression?

I would say there is a quite potential and (it) depends very hard on how much of this configuration work is on my own shoulders or there is support in terms of libraries and interaction with existing mechanisms like for example this export plug-in that you get your fixes as well into Ansible for example.