

Questionnaire – Demographic Questions

1. What is your current role in the company?

I'm a first line manager.

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

Well, I manage a department of, I would say, software engineers and IT specialists. I have various groups in my team. One is focused on doing continuous integration, and another one is responsible for our special purpose private cloud.

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?

So I'm familiar with the concept of infrastructure, the code.

In general, I'm familiar with Saltstack, maybe you heard about the software, and in Saltstack it uses YAML to define the model structure. And according to this definition in YAML, salt master instructs salt minion to execute some actions on the minion.

So from this perspective, I'm familiar.

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

.Infrastructure in general, I would say, 20.

And infrastructure as code 8

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

More than 100,000.

Questionnaire – Compliance Rule Modeling and Checking

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

Well, we use quite a number of different tools. And those tools, the compliance status inside the reporting tool, I would say, is not directly related to the state of a operating system.

You need someone in between.

Well, or you need to write your own automation, which is, I guess, possible, but in my area, we do not have this yet.

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

we have guidance that is human readable and needs to be translated to something that you can have to make or directly configure on the system, on the target system.

That should reach a certain compliance state.

a) If so, how do you define them?

It's human readable text.

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

Yes, I think so.

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

If we talk about relatively simple compliance rule that we need to implement, then definitely yes.

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

I would, several times a year.

So yeah, but several times a year, it happens that we need to change something.

For example, if we talk about the support of operating systems. So in some case, the CIO can make a decision. Okay. We will not tolerate any more some levels of legacy operating systems, even so they are supported. But we do not tolerate them Oh, they are, no, they are not supported for many years. And now we made a decision that we will not support them anymore. And in our case, this means that we have to identify all systems that are running.

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

by defining, if you mean by defining that I will get enough information about how to apply this new security rule, then yeah, definitely that will give me a very clear guidance

By checking, I also think that it will help a lot because, well, your system I assume will have some means of reading some new

So, yeah.

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

I would say four as well, so it will definitely help.

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

Well, I would say also, yeah, maybe even five

Questionnaire – Architectural Reconstruction

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

So, at the moment in my area, we use infrastructure, the code, and we have a certain for automation or so for deployment of operating systems and for configuration. So, that we configure operating system itself, we are installing components, open stack, for example, components. We configure them through this tool and after the execution of this tool and maybe some steps like rebooting the system, we expect that it comes up in a state that it is usable.

So, in this case, I do have existing model of the system, namely in YAML file, which is in a machine readable form.

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

I do not know this.

Okay.

So, we are using salt, well, so it's, I guess, we can look it up, but we never used any visualization.

And simple tower?

With, I think, I do not know, openly speaking, I never used Ansible Tower, but I can imagine that Ansible Tower provides you some level of graphical information, but never did this myself so I cannot comment.

So, I would say, if we talk about the inspection, ideally, we need something that, in case of Linux, reads a list of RPMs that are installed or Debian packages, whatever you name it, and identify which of them are relevant for the data model.

And then, based on this, the software can decide what needs to be patched.

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

I would say it will reduce the effort of keeping this information and using this information.

So, my understanding that this initial effort should be done most probably manually.

Questionnaire – Compliance Violation Fixing

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

I would say for us, it's already a step two. First, since as we discussed, we have our security guidance in the human readable form without any technical specific about how to implement them.

So we know what we need to achieve, but we do not know how. For this reason, we need to first analyze our systems and understand which of them are really a non compliant to this new relation

Like something is not working. We need to introduce another fix. So that might be a chain of fixes. They will be tested in the staging the environment. And then all of these changes accumulated together should be rolled out to production.

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

Well, I think we try to provide a fix for the violation as a part of our infrastructure of the code library, which not always can be the case.

Like for example, if we need to reinstall an operating system, so switch from one version to another. So this triggers some changes in the way how we deploy, but then we need to execute this.

So yes, this is somehow automated as well. So yeah, we try to automate this so that whenever we reinstall, this change is applied automatically.

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

So, yeah, it reduces, but yeah, not entirely, I would say.

eah, there are still some cases in which you still, the compliance job probably doesn't describe how to fix.

How to, well, it's not only about how to fix. Sometimes yes, fixing might be way more complex, but also the verification part after.

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?*

Well, I would say, yes, it does reduce. But I would say the level, I would say maybe three.

Questionnaire – General Questions

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

I would say for the state of the infrastructure that we manage in our team, this definitely introduced some new functionality that we do not have yet.

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

Well, I think it provides.

So you can define new operating system flavors.

You can define new security controls for each of the operating system.

So you can define new models of the systems.

So what maybe I'm missing a little bit, but I assume it could be also added easily is some kind of a classification of data.

24. Would you use the framework in your work?

Yeah, I think so.

a) If so, in which areas?

Well, I would use this framework and especially in an area where I would like to understand the state of the systems that are running, so their current compliance state, and get a report about what is missing.

So not the automatic fixing part, the checking part mostly.

25. What is your general impression?

Yeah, let me think.

I think we talked about the data classification and about the server classification from security perspective.

Yeah, we talked a lot about the integration with existing automation tools like Ansible

Assault.

We talked about the verification that the software is running as it should after applying the security ratings.

Yeah, so I would say most of my comments we already discussed.

And other than that, I think in general, this is a good initiative.

And yeah, for me, it's something that we miss, a certain piece that we miss in our implementation of the security framework.