

Questionnaire – Demographic Questions

1. What is your current role in the company?

Network so I'm actually mainly network administrator and firewall security administrator.

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

If there really are vulnerabilities, let's say, in the firewall or some switch, or if there are security holes through which attack may go, then I have to patch them for example.

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 with my state of knowledge that would be feasible. It's more effort, because you have to model all the switches and the nix and whatever you use there, but we can answer that later at the end. Maybe it helps you there just certainly at that time to go into more depth, but if you had enough time now yes you can understand the architecture of application systems, yes with such a code, script or technology or something already made perfect.

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

I know all that and we've also, we've looked at that, but we're already actually doing that mostly by hand, I have to say honestly.

You can go automated on the switch, read out things and make changes, but it's individual steps.

I then read out the config of all the switches that check for certain values or something and then either change them manually or if there are hundreds, then they have to be automated.

(Overall experience in company: 6 years)

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

250 .. 2k

Questionnaire – Compliance Rule Modeling and Checking

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

So we use Qualis for example. That's a manufacturer has scanner appliances, which we have on the internal networks differently, also from external and that simply scans, so is also agents installed on the computers and that simply scans the machines, and feeds Qualis with vulnerability data. And then you just see CVEs so and so, but it's just of course, it's just monitoring, (it) can't do anything (by itself).

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

It would say yes here (for rules predefined in the Qualis tool).

- a) If so, how do you define them?

Predefined

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

Yeah, so it covers a lot of gaps. So every month thousands are added, this can be automated.

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

it's also raising awareness, above all, that you have a little bit of back of your head and that you have to do something and that you also have to take action.

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

every month thousands are added (from answer 8)

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

3

Now times with maybe 3 or 4, because I must say, it is indeed really good and I would also support that, but it is already real, if I think about, I have now my boss here 169 rules that must be checked now and I want them first of all the 169 created! If you would have you now automatic import gives somehow simply get the rules and then that would be of course a 5.

A 3 because it does have each for each. So if I think about, these are with us for example, that has 1000 security gaps and if I now want to check security somehow, I would need first to create all of them manually!

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

It is like 4.

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

A 4.

Questionnaire – Architectural Reconstruction

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

So we have network plan drawn by hand times.

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

No, actually. But our entire network infrastructure is going to be completely rebuilt in the next few months. And there's a DNA center from Cisco monitoring and distribution. That is, there is actually so, there would be then templates for the switch written, for the different locations, so best are actually all the same, but then you plug switch and it then finds your network automatically. The center then gets all its config settings automatically.

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

4

(If there are) thousands of machines running or so or applications, (manual reconstruction) is of course already very difficult.

Questionnaire – Compliance Violation Fixing

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

Manually: First, we search for solutions or if these are policies or group policies on Windows domains then it is simply ironed over, but that is then done individually for each case

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

Fixing is done manually.

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

Yes, that's it, 5 yes. When it is configured, then all the machines are fixed in one step swoop. I find this super.

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?*

A 4.

Questionnaire – General Questions

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

I think it is good, but a lot of effort.

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

So for my use case, of course, would be nice. Like I said, for the Cisco IOS to be supported somehow. But the most important point is, the reporting.

24. Would you use the framework in your work?

I guess I would also use it. I would just have to get into the Winery all the stuff and take everything. Interesting it becomes in the area of Windows, one is so deeply on rather on Linux, with us is so, we have almost let's say 90% Windows server.

a) If so, in which areas?

For patching (fixing violations)

25. What is your general impression?

I find this whole process very good.