*Disclaimer: My focus until June is mainly on my courses. I am still very excited about the thesis, but I have given myself until January for this, while I want to finish my courses for this semester (hopefully) in June. This would mean no retake exams in August and that my focus from July onwards is fully towards the thesis. Due to the amount of deadlines and tasks for the courses my planning might not seem very ambitious until they are finished.*

# PLANNING

|  |  |
| --- | --- |
| Monday 01/05 | Updating my planning (and finalizing projects for MCS and Cybersecurity) |
| Monday 15/05 | Running the event monitoring successfully on the cluster. |
| Monday 29/05 | Piping the events to the algorithm and generating the Delta Kano matrix. |
| Monday 12/06 | Making sure the VM matrix generates correctly. |
| Monday 26/06 | Making a first working version of the algorithm |
| Monday 10/07 | Optimised version of the algorithm |
| Monday 24/07 | Deciding which tests are necessary, writing down an hypothesis about the test and setting up testing environment |
| Monday 07/08 | Running the actual tests and experiments. |
| Monday 21/08 | Draw conclusions and possible drawbacks/mistakes about the tests, algorithm and general solution |
| Monday 04/09 | Updated version where conclusions are integrated for a better end solution |
| Monday 18/09 | Extra headspace for changes. The algorithm and tests should be finalised by this date. |
| Monday 02/10 | Writing Chapter 1: Introduction and Problem statement. This does not yet include the abstract, |
| Monday 16/10 | Writing Chapter 2: More in-depth about the problem |
| Monday 30/10 | Writing Chapter 3: Describing the solution/algorithm |
| Monday 13/11 | Writing chapter 4: The testing setup, results and conclusions |
| Monday 27/11 | Writing chapter 5 and abstract: Final chapter rounding everything up including possibly open research questions. |
| Monday 11/12 | TO BE FILLED/REVISION/EXTENSION |
| Monday 25/12 | TO BE FILLED/REVISION/EXTENSION |
| Monday 08/01 | TO BE FILLED/REVISION/EXTENSION |
| Monday 22/01 | TO BE FILLED/REVISION/EXTENSION |

# 

# Research Problem:

Verifying the consistency of Kubernetes security policies between security layers

*Disclaimer: technical background information is left behind and will be more in-depth in the final thesis. This is just a short problem statement and thesis goals.*

Within Kubernetes we might have multiple nodes (Cluster layer) running on different Virtual Machines (VMs) (Cloud layer). These VMs might have rules defined between them in terms of security policies that indicate where communication is allowed or disallowed. The problem arises if we take into account the security policies defined within the Cluster layer of the Kubernetes stack. Here more specific rules might be specified that define whether or not containers and/or pods are allowed to communicate. Seeing how pods can be deployed on different nodes within the cluster, which in turn might be deployed on different VMs within the cloud layer it is not hard to see how we might have conflicts between security policies.  
  
Let me give an example. Imagine a Pod *Pa* being deployed on Node *Na*, and a Pod *Pb* being deployed on Node *Nb*. *Pa* and *Pb* have their security policies set up in such a way that they should be able to communicate. This is necessary because *Pa*pulls its data from *Pb*. However, nodes *Na* and *Nb* are deployed on different VM’s at the cloud provider: VM *Va* and *Vb* respectively. The cloud provider has set up rules that all of it’s VMs are not allowed to communicate with each other in any way, meaning that the pods deployed on them also can not communicate.

Clearly these different security rules are conflicting with each other, but are never checked. With the constant possibility of nodes, pods and containers being deleted, moved and added this needs to be checked regularly as well. Due to the enormous amount of these entities being deployed, each with possibly multiple security rules in place makes manually verifying these rules against each other unviable. So summarized: Verification needs to be done quickly, automatically and only taking into account the changes that might impact the security rules.

My thesis goal is to achieve this automatic verification. To do this I start with the Kano container matrix and by generating matrices that show (1) the relations between containers and VMs and (2) the communication relation between these VMs.   
Every event that changes one or multiple security rules must trigger an algorithm that only takes into account the affected existing rules. Conflicts, where (1) rules are not restricting enough, (2) rules are too restricting or (3) the newly added security rules creates a conflict must be outputted. Solving conflicts that I have detected fall outside the scope.