# Summary

## Meeting time and location

27 August 2019 @ 11h30 in the Paris conference room

46 Ingersol Rd, Lynnwood Glen

## Participants

* Advance
  + Roelof Naude
* Dark nITes
  + Jeandre
  + Muhammed
  + Sisa

## Apologies

* Ruslynn – medical emergency
* Christo – medical emergency

## Decisions/Amendments made/adopted

* Logging system will form part of the system. A log entry will include *time*, *username*, and the *action taken*
* User accounts/Log ins will be included as a security feature
* IPv6 support not to be added now; peg as a possible future feature
* Implementation of “unique algorithm per pool” requirement to be added later

# To-do

* Metrics
  + Implement blocking calls for Metrics initialisation
  + Look at reading eBPF maps directly in Python
  + Alert manager alert rules
  + Playlist for demo
* Interfaces
  + Confirmatory (automatic action) toasts for Info, Warning and Error
  + Include a feedback/confirmation of (manual) actions
* Auditing/Logging
  + Statistical sampling of data
  + Look towards implementing Audit objects

# Overview

The purview of this meeting was to touch base and reconcile our progress with the client’s expectations.

## Metrics

* Remove sleeps, rather use a block for Metrics start-up on Defendr start-up
  + Open a socket
  + Poll Prometheus
  + Once response is received, continue
* Each backend is to expose its own metrics instead of a centralised monitor
  + eBPF maps can be used in Python (perhaps access the maps directly instead of using the command line bin)

## Confirmatory toasts

* Implement toasts that provide feedback to let a user know an action has been performed
  + Info
  + Warning
  + Error
* Also include a notice of (automated) actions, e.g. an IP that was dynamically blacklisted

## Logging

* Log statistical samples of data instead of the entire set
* Could also use linear regression on the logs to perform analysis and predictions

## Load-balancing

* Spoofing of IPs has been an issue, as one could use Defendr to perform an attack (send request, spoof response IP)
  + One layer of security is that ISPs tend not to forward requests if the source IP is not in their IP range

## Auditing

* Consider using “audit” objects
  + Objects store the data
  + We store the object
* Include a hash of the data next to the logs for verification if need be

## Alert Manager

* Set up AlertManager to provide notifications should an admin’s attention be needed, e.g. system resources running low, # of connections for an IP is reaching the limit, etc.