Sinkholes:

Sinkholing refers to the practice of setting up dedicated servers to rerouting unexpected traffic to for further analysis

In plant we know very well what is expected communication – we can redirect all non-expected traffic to one of these.

For this we will need an internal DNS server (per plant? Or can we use the ones we already have?)

Same for outbound -> redirect suspicious outbound traffic to sinkholes for analysis

How do we keep the DNS servers ready and updated with the Ips of known botnet C&C servers?

Sink Hole is used to describe a technique that does more than the individual tools we’ve had in the past:

n Black Hole Routers – one router advertising dark IP space.

n Tar Pits – A section of a honey net or DMZ designed to slow down TCP based attacks to enable analysis and traceback

n Shunts – redirecting traffic to one of the router’s connected interface.

n Honey Net – a network designed to analyze and capture penetrations.