The Distributed Honeypot Project	*NoAH*
Question 1 *("Have you or are you currently running any honeypots or honeynets ?")* Most of the responses on this questionnaire came from experts on security issues, who are familiar with the honeypot (SecurityFocus Honeypot List). 95% of the respondents have used honeypot technology in the past .	NoAH questionnaire is targeting various organizations, that do not exclusively rely in the area of security (45% of the respondents have used honeypots in the past).
Question 2 *("If you have run honeypots or honeynets, were they physical ?")* **Question 3** *("If you have run honeypots or honeynets, how many of them were virtual ?")* These two questions are referring in the use of virtual honeypots and they also discriminate virtual from physical ones.	NoAH refers to honeypots in general
Question 4 ("*If you have run honeypots or honeynets, how often do your machines receive suspicious activity?"*) It is indicated that honeypots usually record suspicious traffic at an increased frequency.	It is expected that NoAH honeypots will also receive traffic at high rates. This is emphasized by the request for the minimization of fault positives on possible attacks that NoAH honeypots will produce (Figure 27)*
Question 5 ("*If you have run honeypots or honeynets, what kind of machine(s) are you imitating?*") The 58% of the respondents, run their honeypots in a production environment, while the 33% of them, are operating personal honeypots.	There is not a similar question in NoAH questionnaire.
Question 7 ("*If you have run honeypots or honeynets, what is your primary reason?"*) Most of the respondents use honeypots for personal interest.	In NoAH 's corresponding question (Figure 14), most responds came from individuals who are interested in using honeypots both for research/educational purposes and also as an alternative security mechanism, against cyber-attacks.
Question 8 *(Rate the level of interest for six future topics of honeypot research on a five-stage scale of "Not interested" to "Highly interested")* By the majority of the responses, it is indicated that honeypots are used for the detection of virus/worms, for collecting information concerning the attack, etc.	There are similar conclusions derived from NoAH questionnaire (Figure 23)

* All figures' numbers mentioned in this document, refer to the figures in the deliverable D0.2, "*Requirements Collection and Analysis."*

The Distributed Honeypot Project	*NoAH*
Question 9 ("*Are there any particular subjects of interest in honeypots or honeynets that you would like to see research in?*") Responses in this question indicate that a) current users of honeypots are highly interested in attack signature generation, as well as, in client-side applications using honeypots b) an interest for user-friendly and easy to install honeypot infrastructure c) there is a need for zero-day exploits detection	a) There is a similar interest for generating a signature concerning the detected attack, as well as for further relevant information on the attack. Furthermore, the request for honeypot client-side applications is satisfied by the development of honey@home . b) The same requirement is derived from questions 20-21 of NoAH questionnaire, as the most respondents seems to prefer configuring their honeypots by themselves. c) NoAH infrastructure will try to support detection of zero-day exploits.

Generally, the NoAH infrastructure requirements that were derived from the questionnaire, are strongly related with the overall results of this survey. This is of great interest, as the specific questionnaire is targeting experts on honeypot issues. What is more, both surveys indicate that there is great interest in using honeypots as an alternative security tool.

From this small comparison of the two surveys, we can safely assume that the NoAH project, is heading in the right way.