Appendix G – Survey Responses from Testers

SIAAS SURVEY FOR TESTERS

Methodology:

A survey was replied via video call or text survey: https://forms.microsoft.com/e/t47we3fNCf

Participants:

Trilio Data: Video call (with Matt Golden, Customer Success Engineer), on April 21, 2023, at 17:00 UTC
Altice Portugal: Video call (with Ricardo Ramalho, Head of Cybersecurity Behaviour Analytics and Automation), on April 24, 2023, at 18:30 UTC
VTXRM – Software Factory: Video call (with Jorge Teixeira, IT Team Lead), on May 5, 2023, at 21:00 UTC
David Negreira: Video call, on May 12, 2023, at 18:30 UTC

Replies:

Technical aspects (10 sentences, rate 1-5):

1. It is easy to install and configure the components of this vulnerability scanner.
   Trilio -> 4
   Altice -> 5
   VTXRM -> 5
   David -> 5

2. The CLI usage and help menus are user-friendly.
   Trilio -> 5
   Altice -> 5
   VTXRM -> 4
   David -> 4

3. The agent correctly discovers neighborhood hosts.
   Trilio -> 5
   Altice -> 5
   VTXRM -> 4
   David -> 5

4. The vulnerability scan results are accurate.
   Trilio -> 5
   Altice -> 4
   VTXRM -> 5
   David -> 3

5. The vulnerability scans do not impact network or targeted hosts negatively.
   Trilio -> 3
   Altice -> 5
   VTXRM -> 5
   David -> 5

6. The e-mail reports are reliable.
   Trilio -> 4
   Altice -> 3
   VTXRM -> 3
   David -> 3

7. The existing documentation is useful.
   Trilio -> 4
   Altice -> 5
   VTXRM -> 4
   David -> 5

8. It is easy to customize the scanner for one's specific environment.
   Trilio -> 4
   Altice -> 5
   VTXRM -> 3
   David -> 5

9. It is easy to integrate the API with existing tools and workflows.
   Trilio -> 3
   Altice -> 5
   VTXRM -> 3
   David -> 3

10. You are satisfied with the performance and functionality of the vulnerability scanner.
    Trilio -> 4
    Altice -> 5
    VTXRM -> 5
    David -> 4

Organizational aspects (5 sentences, rate 1-5):

11. This vulnerability scanner is a valid approach to an organization which has no access to paid commercial solutions or cybersecurity human expertise.
    Trilio -> 5
    Altice -> 5
    VTXRM -> 5
    David -> 4

12. When compared with other paid tools like Nessus, considering human expertise and configuration time, this scanner saves time/money/resources while keeping an acceptable performance.
    Trilio -> 4
    Altice -> 4
    VTXRM -> 3
    David -> 5

13. The vulnerability reports generated by the scanner help with the process of addressing, prioritizing, and remediating vulnerabilities.
    Trilio -> 4
    Altice -> 4
    VTXRM -> 5
    David -> 5

14. This vulnerability scanner helps an organization complying with relevant security standards and regulations.
    Trilio -> 4
    Altice -> 4
    VTXRM -> 4
    David -> 5

15. This vulnerability scanner increases an organization's posture and ability to detect and mitigate vulnerabilities.
    Trilio -> 5
    Altice -> 5
    VTXRM -> 5
    David -> 5

Overall aspects (2 sentences, rate 1-5):

16. This vulnerability scanner helps improving the security auditing process of an organization.
    Trilio -> 4
    Altice -> 5
    VTXRM -> 5
    David -> 5

17. You would recommend this vulnerability scanner to other organizations.
    Trilio -> 4
    Altice -> 4
    VTXRM -> 5
    David -> 4

Open-ended questions (3 questions, text response):

18. What were the main technical or organizational-related shortcomings found (technical issues, false positives, or others)?
    Trilio -> Technical problems regarding the DB file limits (16MB BSON limit in MongoDB), which disappeared after disabling one of the scripts. This was the only technical problem observed.
    Altice -> (Empty.)
    VTXRM -> As it relies on ARP to discover hosts, the scanner might be sensitive to ARP spoofing from a malicious actor in the network. An easier installation process for the test scenario would be nice, as it requires some Linux expertise as it is (suggestion: containerization).

David -> The scanner does not detect vulnerabilities already fixed by server patching. Some confusion in understanding what the agent IDs meant (clarified with the author).

19. What features would you like to see added or improved in future versions of the scanner?
    Trilio -> GUI interface, with possibility of configuring the agents, and a way one can go through a list of targets and select them from a drop-down list to filter the scanning outputs. Also, this GUI should have the ability to mark false positives in order to remove them from the reports.
    Altice -> Docker release, especially for the server component. This would also be quite useful for testing.
    VTXRM -> Graphical interface. More details in the CVE descriptions (current information is too technical). These details could be presented in the graphical interface itself.
    David -> Detecting backported vulnerabilities by patching. Identifying the distribution of the neighborhood hosts (example: Ubuntu) and other aspects related to it, per example, if an OS version was already discontinued.

20. Any other comments?
    Trilio -> Popular tools have most of their features hidden behind their paid version, which makes this an interesting project overall. Regarding statement 5: no negative impact was observed, score of 3 just because the tests didn't drill down on this specific point; statement 9: score of 3 because it was not tested.
    Altice -> It is a very interesting and useful project. Has the potential to become a product. Regarding statement 6: score of 3 because it was not tested; statement 13: prioritizing is a different matter from addressing or remediating, and even the most expensive and complex solutions have difficulties in helping with this; statement 16: the tool helps but does not necessarily guarantee by itself that, for an audit, all requirements are passed; statement 17: the alternatives were not thoroughly explored.
    VTXRM -> Interesting project. Increased interest in cybersecurity and what CVEs are. Will use it for own projects. Regarding statements 6, 8, 9, and 12: score of 3 because those statements could not be tested or assessed.
    David -> It's a good product. Possibility of being widely adopted. It's easy to install, configure, and set up. Regarding statement 4: score of 3 because it does not detect vulnerabilities solved by patching; statement 6: score of 3 because it was not tested; statement 9: JSON output looks easy to parse and integrate, but score of 3 because this was not tested.

Technical Note G1 - Survey results from the testers of the artifact