OPEN LETTER TO SECURITY RESEARCHERS

Dear Esteemed Researcher,

We write this letter to clarify our complementary roles in improving the web application and API security for our joint customers.

All improvement programs require clarity on the current state, action to address problems then verification of the result of the actions. The program that we jointly execute has these characteristics.

1. Clarification on the current state

We perform very limited vulnerability discovery hence we require you to think of new and creative ways to hack the applications under test.

Our vulnerability discovery is limited to public databases (eg Shodan), observing the hygiene of server banners-headers and weekly unauthenticated DAST scanning tools.

We encourage you report the same and more. We can ingest authenticated and unauthenticated SAST-DAST-IAST scans results plus manual penetration testing and bug bounty reports.

Your findings can be displayed, prioritized and commented in our portal.

2. Action to address the problems

After we have visibility of your findings our analysts produce a Shielding Plan. This outlines what items we can address, a brief outline of how and then an assessment of any residual risk. We are available for clarification discussions and may need to iterate the solution.

Once it is mutually agreed that we will shield a specific issue, we build and deploy the shield and make it available for you for testing. This can be done under urgency in minutes to hours.

3. Verification

We require you to be satisfied that the shield is effective. Given our shields are software, they too are subject to the laws of AppSec and hence if bypasses exist or the shield is just not effective we need to be made aware and remediate.

We trust that this clarifies our complementary roles and look forward to working with you in keeping our joint customers safe.

Regards,

RedShield Executive Team