Dear Avi:

On behalf of Palo Alto Networks, I am responding to your e-mail of July 13, continuing an exchange that you began in June regarding what you claim are Orca's findings of security vulnerabilities in Palo Alto Networks' Prisma Cloud Security suite. As we informed you on July 11, your assertions do not amount to vulnerabilities in Palo Alto Networks' Prisma Cloud Security suite.

As you know, the Palo Alto Networks Product Security Incident Response Team (PSIRT) regularly assesses, identifies, and remediates security vulnerabilities. Palo Alto Networks has been an innovator in empowering external researchers, vendors, customers and other organizations to identify material vulnerabilities in PAN products, and to publicly congratulate them for reporting such vulnerabilities to us before the vulnerabilities could result in harm. A complete description of this process is available here: Palo Alto Networks Product Security Assurance and Vulnerability Disclosure Policy - Palo Alto Networks. We have routinely acknowledged those who have discovered or have helped fix vulnerabilities with an acknowledgment statement on our security advisories. And, even if an advisory is not published, we have included the researcher on our hall of fame page. Therefore, we have a long-established track-record of acknowledging independently identified vulnerabilities in PAN products and of publicly congratulating those who find them.

You purport to have initiated this process with your June correspondence. Pursuant to this process, the PSIRT evaluated your videos, identified shortcomings with your analysis, and determined it is incomplete with inaccurate conclusions. Your most recent response provided no additional substantive information. The PSIRT has thoroughly considered all information provided and the information does not constitute a reportable vulnerability under our disclosure policy.

Let us be clear. If the PSIRT had determined that you had identified any actual vulnerabilities, it would have thanked you, addressed those vulnerabilities, and notified affected customers if necessary. However, nothing you have provided to date rises to that level and our analysis did not find any negative impact on the system's confidentiality, integrity, or availability.

Finally, you seek our confirmation that Orca is "not subject to any responsible disclosure guidelines." We do not agree and would consider it irresponsible for Orca to publish an incomplete analysis as credible research. If you intend to publish the findings despite our good faith assessment, at a minimum you prominently state these facts: (1) the videos depict an older version of the Prisma Cloud that does not take advantage of the industry leading WildFire cloud-based malware detection; (2) threat data (IP reputation lists, DNS block lists, malware signatures) was out of date by nearly two months; and (3) the videos do not depict malicious activity typically seen in real-life compromises.

Sincerely,
Chandan