Dear Sir / Madam,

In a blog post published by you, your team claimed that one of the main values of the Prisma suite feature set is a "robust runtime monitoring and protection mechanism", and claimed that this is a major advantage of your suite over Orca's agentless cloud security platform.

Subsequently, our research team have had a quick review of these capabilities and took note of the following extremely alarming findings:

1. Cryptominer detection is only as strong as the file name. A simple change of the file name will cause the crypto miner not to be detected. Just calling a cryptominer 'not-cryptominer' is enough to evade detection.
2. The same goes for lateral movement detection - only as strong as file names. Changing nc to 'notnc' is all that is needed to evade detection.
3. C&C communication detection is evaded when communicating using IP addresses.
4. Malware detection is extremely limited - not detecting even extremely well known malware.
5. Exploit detection doesn't work - even for well known exploits that are supposedly understood by your platform.

This is extremely alarming as organizations that rely on your marketing claims of 'robust run time monitoring platform' are at significant risk. Any novice threat actor can simply change a file name to evade detection.

We believe in transparency and plan to publish these findings to allow customers to make an informed decision when considering cybersecurity protection tools. Having said that, putting the customers' protection as the first priority, we are willing to delay the publication of the above for a reasonable period of time (up to the customary 90 day responsible disclosure duration) if you're planning to release a fix to these serious findings. Please let us know if / when you're planning to.

Detailed reproduction examples of all of the above can be found in this link (please treat the link as secret, as sharing it can allow more people to see the details before you'll be able to publish a fix - and let us know that you downloaded it so we can stop the sharing). Don't hesitate to reach out if you need any other information.

For the avoidance of doubt, this communication is not deemed confidential by us, and we reserve the right to publish the correspondence.

Yours,
Avi Shua