DARKHORSE

Why Managed Triage Is A Poor Economic Proposition

A DarkHorse Security Research Paper

The Setup

In today's crowdsourced security landscape, managed triage is almost a given. Every major provider includes it by default as part of their bundled offering - and on the surface, that seems like a great thing. However, upon further evaluation, we've come to the conclusion that paying for managed triage is (generally) not in the financial best interest for most organizations.

This sheet will explain our position and how we arrived at this conclusion. A more detailed write-up is available here.

The Facts

Managed Triage Requires You To Duplicate ~50% Of All Triage Work

Managed triage still requires a significant amount of work from your team: validating all triaged issues, responding to questions, false positives / false negatives, and more.

The reports that triage does remove are also the easiest (duplicates, not applicable, out of scope, etc); leaving you to have to replicate the hardest and most time consuming reports. In the end, you have to do approximately 50% of the same work that the external triage team already "did".

Managed Triage Is ~10x More Expensive Than Self-Triage

The above inefficiency, combined with a high average cost per report, results in most organizations paying at least 10x more for managed triage, then it would cost to self-triage.

NOTE: we believe these averages are low, but are based off the best public information available.

The Numbers

Inherently Inefficient

- Duplicate, not applicable, and out of scope reports make up the majority of reports, but take significantly less effort on an effort-adjusted basis.
- Valid reports, as well as those with nuance, all require client input before acceptance. These more time intensive reports equal nearly 50% of the total effort around triage.
- This means that despite paying 100% of the cost for managed triage, one still has to re-do ~50% of the work.
- If one is already performing nearly 50% of the effort relating to triage, the relative cost to do the other half of the work is *ten times* lower than paying for managed triage.

Running The Averages

- The average contract through HackerOne or Bugcrowd is ~$40k.
- The average program receives ~190 reports, annually.
- This puts the average cost per report at $210; $160 of which is allocated to triage costs.
- At this rate, the cost for managed triage on 100 reports is ~$16,000.
- Meanwhile, we estimate the cost to self-triage the remaining 50% of work is $1,700... *one tenth* the cost.

Get In Touch

Read the full report here

🌐 https://darkhorse.sh