**Press Release**

**Threat Services Market (TSM) Goes Live!**

**TSM is a first of its kind pay per use security service that allows users to choose, customise and combine Security as a Service offerings from main stream vendors in a single console and make use of them in a variety of ready-made apps & plugins.**

TSM comes supported by collection of open source plugins for popular SIEMs, forums, browsers, web site builders, OS’s and other tools and hooks. Via the central TPM console users can then pick, choose and combine security services from main stream SaaS vendors to power those plugins. The TSM console is then used to monitor activity, review performance and provide centralised billing. Today TPM aggregates services from Reversing Labs TitaniumCore, CrowdStrike Hybrid Analysis and Sophos Intelix but more are promised.

We see continuing growth in diversity with niche platforms popping up all over the place accompanied by an eco-system of plugins and extension. Each of these platforms would benefit from some kind of security value add delivered via a custom plugin. However, these niche markets are often to small and fluid for mainstream security providers to invest the time to integrate with via a custom plugin. Also, to provide compelling security value add, many platforms require a spread of security services that no single vendor does well. Because of this and because platform communities want to be vendor neutral you rarely find open source plugins available and where you do they offer a single low brow solution.

TSM aims to cater for this ‘long tail’ of niche markets by releasing plugins and integrations that call home to a market place of security services. Crucially these plugins are released as open source so that the niche platform’s community can update and enhance them as they see fit. Out of the box, each TSM plugin will use custom fit default vendor services to best do its function, but the user is free to tweak and tune that selection at any time. As a simple example, for a site builder plugin like (e.g. WordPress ), a user may choose to use Reversing Labs to check URL links in users posts but scan file up loads with Hybrid Analysis. Users are free to review that decision and change it, a la carte, at any time.

To try out the Threat Service Market, you can quickly get a feel via the web portal that allows you analyse URLs, files and other items across the different vendors. Then take a look at the plugin gallery to see how you could use the services on your website, browser, desktop or you SOC. The TSM plugins will also be available in the platforms plugin repository / store and this is typically where most users will find them.

*“Security solutions have two halves’, one half hooks into the system or platform and the other half is the secret sauce – so that’s the security content or service itself. The former is powered by the later and for years major vendors couple the two together. TSM breaks this model by making the hook a part of the platforms plugin eco system, open sourcing it so the platform experts own it rather than security vendors. The secret sauce remains with the vendors but the user gets to pick and choose and blend them. This new paradigm is a natural next step as we seeing increasing numbers of diverse and niche platforms that security vendors can’t create and maintain hooks for” TSM Business Manager.*

*“This is a win, win, win since vendors get exposure to new niche markets, niche platforms get industry leading security tailored for their eco-system and users get security availability and an a la carte choice.”* TSM Product Manager.

*“I am the technology lead in a start-up creating a new platform that allows b2b customers in the underwater basket weaving industry to share content and discuss ideas. I have created a TPM plugin for the platform so that I can scan content submitted in particular on the end user areas of the portal.”* Joe Finsbury Platform Developer.

*“ I run a small underwater basket weaving company. We have a slack forum for user to discuss our products, we use Basecamp for my internal team project management and I run a web site and blog on Weebly. I use TSM plugins for all three platform, this is great as I can monitor activity in a single place. Initially I used Clam AV for file scanning as its cheaper I have now added Hybrid Analysis for Basecamp because I want to be sure my internal documents are virus free. We also use the TSM plugin for Chrome, Edge and Safari at home for the kids and have that switched it to Sophos Intelix as they have great web site categorisation” .* Jane Ashes small business owner and tech savvy Mother.

*‘I lead the IT infrastructure team for a mobile sales team. The sales guys always complain about any Anti-Virus installed so we’ve gone with Windows Defender and to also built a custom TSM plugin for Microsoft AMSI interface. As a TSM have open sourced there AMSI plugin it was easy for us to modify to fit with our in-house deployment tools. We select* Hybrid Analysis Quick Scan service for document scanning and full-blown Sophos Intelix Dynamic analysis for any executables the sales guys download’. Henry Savage Tech Lead, Infrastructure, Underwater Baskets Inc.

**FAQs**

Q: You don’t have a plugin for the platform I used - can anyone modify or create an application that uses TSM?

A: The TSM plugin SDK is welcome documented and has an active support forum and there are many examples out there in open source which would serve as a great

Q: Why can’t I develop my own plugin and call the vendors API directly?

A: You can do, but you will need to start from scratch, be tied to one vendor and will have no open source. Since we are geared up for plugin development, we hope you find the TSM SDK, example s and support easier to use.

**Internal FAQs**

Q: There are 1000s of niche eco systems out we can’t possibly write a TSM plugin for all of them?

A: To get started we should target carefully and choose a couple in each area that we think has potential. We deliver only simple MVP style plugins no more than the ‘Hello World’ example for the niche area. We then market and watch the uptake and re-invest only in areas with good update. For example, we choose OS Tools, Browsers and SIEM, we do a plugin for one vendor platform watch for up take. Similar to Multivariable Calculus optimization problem.

Q: If we create a large enough number of plugins wont maintenance become a constraint?

A: Since we will open course the code for plugins we hope that the community can help take on some of that burden.

Q: Aren’t we at the mercy of the big SaaS vendors. They could pull their services from us.

A: Indeed, this is a risk but we hope to mitigate it as vendors would see this as a potential revenue stream. Also, there are enough of them we hope to maintain good relations with some of them.