THREATQUOTIENT™

BUILD OR BUY?
Answering the Eternal Technology Question

by Ryan W. Trost, Co-Founder & CTO

The eternal technology question seems to be, *"Build or buy?"* It is usually posed when a technology capability is mature enough that it has some open source options and there's a defined market need, but not so mature that an entire discipline exists that has evolved over many years, with a handful of vendors offering a range of solutions all ranked by industry pundits.

Threat intelligence platforms (TIPs) are at that inflection point and security teams are asking themselves, "*Should we build or buy a TIP?*" However, the better question to ask is, *"Just because we could build one, should we?"*

WHAT A TIP SHOULD BE

A threat intelligence platform empowers security operations centers (SOCs), threat intelligence analysts and incident response, risk management and vulnerability teams to not only respond to events and alerts, but to also anticipate threats and become more proactive. The key to enabling this is that the TIP serves as the single source of truth for all threat data from both external and internal sources – fostering collaboration, better decision making, proactive measures and accelerated detection and response. Whether you buy one or build one, that platform must be able to help you understand, prioritize and act upon the most relevant threats facing your organization. As the threat landscape and your internal environment changes, the TIP can also help you learn about and anticipate potential threats through continuous threat assessment so you can proactively strengthen defenses.

Streamlining threat operations and management, a TIP should provide the ability to rapidly bring together internal threat information, including security event data, malware analysis and adversary analysis, and overlay it with external insights for critical context of the who, what, when, how and why of a threat. A TIP should also help with prioritization so you can automatically filter out noise and understand what matters to your organization based on parameters you set. Through orchestration, automation and synchronization of threat intelligence, a TIP should allow you to strengthen the configuration and policies of your security infrastructure proactively and accelerate detection and response efforts. Regular updates with pre-processed, contextual and prioritized data, along with the ability to capture feedback and learnings, empowers teams to reprioritize and anticipate threats to reduce risk now and in the future.

KEY CONSIDERATIONS IN THE BUILD VS. BUY DECISION

Regardless of how many of these capabilities your security teams and management identify as critical technical and business requirements, you need to consider the following tradeoffs in the juxtaposition of build vs. buy.

RESOURCES

Does your organization have a dedicated development team available?

Finding someone, let alone a small development team, with the skillset to build a core software component for a SOC team is rare. Keeping that same resource long-term to support ongoing maintenance and deliver new functionality and integrations is even more difficult, particularly when the project is not directly driving revenue. Be wary of plans to "borrow" talent or "steal cycles" from another department, especially when you're in an environment where that developer could be reassigned as needed. The replacement developer will have to reengineer code before moving forward, which will delay, if not sink, the project.

FINANCIAL CHALLENGES

Have you accounted for all upfront and maintenance costs?

Building an internal team to support even a small homegrown application will require a minimum of four full-time employees: two developers, a dedicated database/big data engineer and a quality assurance (QA) resource. Some will balk at the need for a dedicated database/big data resource. But if you consider the aggregation of external sources, internal analysis including malware data, vulnerability data, risk management factors, as well as all the accompanying associations linking each of those objects, this instantly turns into a daunting effort. Forgoing a dedicated resource and only delivering a subset of this functionality will quickly reach a ceiling of effectiveness significantly short of your end goal. Assuming salaries of approximately $100,000 each plus 25 percent in benefits and bonuses, the annual price tag soon reaches over a half a million dollars in headcount alone. That may seem reasonable on paper, but in most organizations, getting additional headcount versus a tool is exponentially more difficult, especially when the tool has a lower price tag that satisfies 85-90 percent of the requirements and includes support and upgrades.

OPERATIONAL DISCONNECTS

Do your resources have software development and threat operations experience?

"True" software development and security operations are very different disciplines. The developer talent must be knowledgeable about software architectures, development operations (DevOps), security operations (SecOps) and security technology, which is an extremely rare combination of skills. More likely, they will need a counterpart in the security and/or intelligence discipline who can devote time to help design, explain and act as a "final stakeholder" in the development process. However, this means that the counterpart will lose productivity cycles in their core responsibilities as a security analyst, incident responder or intelligence analyst.

INNOVATION

Are you willing to commit ongoing resources for feature requests and bug fixes?

As the TIP gets more use, analysts' feature requests will naturally increase, especially if the goal of the TIP is to aggregate intelligence across several teams or departments. Will you be able to keep a development team in place for the long term to enrich the platform? What happens when feature requests get delayed due to competing priorities? Do you have the resources to really drive innovation, or will you be playing catch-up with other solutions offered by companies in the TIP business? In contrast, vendors, especially those that offer annual subscriptions, give you purchasing leverage so you can ensure the product roadmap still aligns with your needs and expectations. The vendor landscape for TIPs is robust enough that you can switch vendors if needed. Although change is never easy, the opportunity to capture business from a competitor typically motivates vendors to do everything in their power to make the transition as easy and seamless as possible.

QUALITY ASSURANCE

Is your team able to perform all necessary system, regression and integration testing?

Initially, you may be able to get away with developers performing peer reviews of code, but this approach doesn't scale. As your platform becomes more robust to meet requirements, you should expect you'll need a formalized QA process, including standard unit tests, smoke-screen tests, regression tests and labor-intensive manual tests. And don't forget about maintaining multiple environments for development, production and staging. Prepare for the reality that, as more and more analysts across the team begin to leverage the TIP and rely on it heavily, the code will grow and the tech debt of "quick code fixes" will morph into significant re-factoring efforts. This will also steal time needed to address the already long waiting list of new features, causing intra-team friction. Once you've made it to this stage, you need to be cognizant of the fact that the original developer now has highly prized security intelligence development skills that are extremely attractive to other organizations. It would be wise to consider a third developer and second QA engineer for redundancy in the event one or two are lured away.

INTEGRATION

Is your team qualified to perform all current and future integrations in a timely manner?

Most organizations are dealing with millions of threat-focused data points from commercial sources, open sources and various security vendors, not to mention the massive amount of log and event data from each point product within your layers of defense and/or your SIEM. Aggregating this data into your TIP and translating it into a uniform format for use is a huge, complex undertaking that warrants a full-time database engineer. There's also the aspect of applying the threat intelligence that you want to act on and deploy to the appropriate technologies in your sensor grid, which means integrating with your firewall, IPS, IDS, NetFlow, endpoint protection, etc. Keeping up with the idiosyncrasies of integrations is easily a full-time job.

TIME

Do you have a realistic estimate of the development and deployment duration?

Consider the time it will take you to properly design, architect and develop a platform, as opposed to evaluating third-party solutions and then proceeding down the selection, proof-of-concept and implementation process with a vendor. Also contemplate the time your team will likely need to rebuild the in-house application to account for hidden obstacles that surface when concepts and whiteboard efforts do not translate to operational routines several months after the fact. Any difference translates into additional time your threat operations program won't be able to perform as you need it to, and affords adversaries a greater window of opportunity to launch attacks.

RISK

How much risk are you willing to shoulder for internal development?

The end game is to mitigate cyber risk. Assessing how a homegrown solution will perform and mitigate risk in comparison to a commercial platform can be tricky. There's no established track record for proprietary solutions; these solutions don't undergo third-party testing to validate performance, secure coding best practices and constantly evaluate embedded open source licensing tools, and SLAs typically aren't in place. Furthermore, if an adversary leeches onto the homegrown application, the aftermath is naturally more time-consuming when the solution is built internally. Not only must you deal with incident response, but you also have to address any gaps in solution functionality that may have contributed to the success of the attack.

VENDOR MANAGEMENT

Would you like a single point of contact for platform updates and product roadmaps?

It's always easier to deal with a vendor, whether to collaborate on a new cutting-edge feature or when there's a problem, as opposed to firing and hiring an employee. SOC managers are typically the primary owner of the TIP and they tend to spend 60 percent of their time as a human referee, 20 percent as an executive translator and 20 percent dealing with technical issues. That 60 percent will creep up if they have to deal with even more personnel issues and cut into the time your SOC manager should be spending on other higher-priority activities.

CONCLUSION

Your ability to accelerate security operations through a streamlined threat operations and management program hinges on the tool that brings threat data, analysis and action all together. As you go through the list of considerations, run the cost projections of maintaining full-time employees to support the effort on an ongoing basis against a software purchase. Also, take into account the opportunity costs and risks as you divert precious security resources from the front lines to development work. Regardless of which direction an organization takes, it should be guided by a maturing strategy that is ready to shift with the organization and the threat landscape.

ABOUT THE AUTHOR

As CTO and co-founder of ThreatQuotient, Ryan Trost utilizes his 15+ years of security experience focusing on intrusion detection and cyber intelligence to help drive thought leadership as well as innovative product discussion. As a recognized leader in the cyber industry, Ryan frequently speaks at industry conferences, including BlackHat, DEFCON, SANS, HTCIA (High Technology Crime Investigation Association) and FIRST. Ryan is the author of Practical Intrusion Analysis and has also developed one of the first geospatial intrusion detection algorithms used to identify geolocation attack patterns. Prior to ThreatQuotient, Ryan managed several USG and Commercial Security Operations Centers (SOCs) and was the Sr. Director of Security and Privacy Officer for a medium-size healthcare company in Northern Virginia. Ryan also serves as Chairman of the Advisory Board for the Northern Virginia Community College cyber degree program.

ABOUT THREATQUOTIENT™

ThreatQuotient understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, empowers defenders to ensure the right threat intelligence is utilized within the right tools, at the right time. Leading global companies are using ThreatQ as the cornerstone of their threat intelligence operations and management system, increasing security effectiveness and efficiency.

For additional information, please visit threatq.com.

TQ_Build-vs-Buy-Salaries_Rev1