THERE ARE MANY FACTORS TO TAKE INTO ACCOUNT WHEN DECIDING WHETHER TO BUILD OR BUY A **THREAT INTELLIGENCE PLATFORM.**

Build or Buy?

HERE ARE 5 KEY CONSIDERATIONS

1. FINANCIAL AND RESOURCE CHALLENGES

Finding someone, let alone a small development team, with the skillset to build core software components of a threat intelligence platform (TIP) is rare.

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 resource.

Foregoing a dedicated resource and only delivering a subset of this functionality will quickly reach a ceiling of effectiveness significantly short of your end goal.

2. INNOVATION

As a threat intelligence platform 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.

Resources are needed to drive real innovation, or you'll be playing catch-up with other solutions offered by companies in the TIP business.

3. INTEGRATION

Aggregating internal and external threat data, logs and events into your TIP and translating them into a uniform format for use is a huge, complex undertaking that warrants a full-time database engineer.

Applying the threat intelligence that you want to act on to the appropriate technologies in your sensor grid means integrating with your firewall, IPS, IDS, NetFlow, endpoint protection, etc. with multiple APIs from multiple vendors.

4. TIME

Consider the time it will take you to properly design, architect, develop and test a fully functional threat intelligence platform.

Evaluating and implementing third-party solutions with a vendor can get you up and running in a matter of weeks versus months.

Additional time means your threat operations program won't be able to perform as you need it to, and this affords adversaries a greater window of opportunity to launch attacks.

5. RISK

There's no established track record for proprietary solutions; these solutions don't undergo third-party testing to validate performance, and SLAs typically aren't in place.

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.

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

To learn more, download our guide

Build or Buy?

Answering the Eternal Technology Question.

DOWNLOAD