DCSO Whitepaper

Technology Scouting and Evaluation

Evaluating Security Products – Honestly

Technology Scouting and Evaluation

Across industries, companies invest time and budget into IT-security solutions. Still, data leaks and compromised environments hit the news daily. Either, IT-security products do not work correctly (and an entire industry is basically selling snake oil), or somehow companies tend to buy the wrong security products for their needs. We believe in the latter. This whitepaper documents our experience on how to tackle this issue and identify solutions that work within enterprise environments.

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF Campus 22, 10829 Berlin, Germany

Takeaways

Companies should validate that they have an actual demand for a new IT-security capability before starting a product evaluation. If a new product is ultimately required, the selection process needs to be treated like a custom project. It should base on precise and use case driven criteria, which allow product comparison and ranking. The use cases should include critical non-functional aspects, like integration capabilities and maintainability. Solution pricing can be a criterion on its own, but should not mix with functional or non-functional capabilities. The evaluation itself must cover multiple products, and should strictly adhere to the predefined criteria. Instead of guided evaluations with permanent vendor supervision, we recommend to test products independently with regular vendor touchpoints. When a single suitable solution is not available, defined use cases help to identify integration synergies between multiple products.

1 Intrinsic and external triggers

Almost all product decisions start with a trigger event. To our experience, many of these triggers are notoriously leading to wrong product decisions down the line. Evaluations that were started for the wrong reasons lead to unsatisfying results, and challenging the trigger for a product evaluation is usually easier than stopping the process later. Therefore, it makes much sense to investigate whether a product decision should be taken at all. In the following, we list two common triggers that notoriously lead to poor product decisions:

- The sales representatives of a security vendor invite themselves for a product presentation. These presentations have many benefits for the vendors, but their value for a potential customer is somewhat limited. In our experience, a product always seems appropriate in such presentations. However, well-designed presentations do not necessarily correlate with well-designed products.
- An executive board member noticed a new security product and is excited to purchase it. From an operational perspective, there is no distinct need for a new solution in this area.
- Promising marketing indicates that the publishing company has much capital to invest in marketing. Promising marketing does not necessarily indicate better or worse product maturity - and it does not indicate any intrinsic demand for a new product either.

All listed triggers indicate an alleged and unnecessary demand and should be avoided. Instead, we strongly recommend sticking to triggers that indicate an actual intrinsic demand:

- An ending contract opens the window of opportunity to replace an existing solution.
- A new architecture or concept, like Office 365, macOS workstations, or BYOD is introduced.
- Red-teaming exercises, penetration testing results, or new compliance requirements show gaps in the existing security infrastructure.

2 The evaluation process

The following sections outline a six-step process for IT-security product decisions. It builds on our experience during real-world TSE customer buying decisions and how those have evolved over the past years.

2.1 Use-Cases

Each product evaluation should start with requirements, documented as use cases. We recommend to split those into functional and non-functional use cases, like compliance requirements, administration, and documentation. Depending on the scope of the evaluation, it can also make sense to split the requirements into main and auxiliary use cases. Product evaluations are always an opportunity for consolidation. To leverage consolidation synergies, we recommend taking the entire security architecture into account during the requirements definition. Maybe a new product can cover tasks that are currently dealt with by a dedicated tool. The use case definition is an often neglected phase, but we consider it crucial for a fact-driven product decision.

We document our use cases in a tool originating from software quality assurance. For smaller evaluations, it might be feasible to use a spreadsheet, but specialized tools have various benefits regarding result documentation, progress reporting, and multi-user capabilities. Therefore, we recommend considering a dedicated tool, especially since they are relatively cheap and rather mature.

2.2 Responsibilities & Stakeholders

Proper product evaluations are nearly impossible to conduct in parallel to daily business. Especially for highly-loaded administrators and analysts, an additional evaluation is usually not feasible or sensible. We recommend treating evaluations as individual projects. Therefore they should be subject to project management and require a committed budget, team, and capacity. If that commitment cannot happen, it is probably better to postpone the evaluation or outsource parts of it to a third-party contractor. To our experience, three to four person-weeks suffice to evaluate a single solution in depth. Naturally, this duration depends on the number of tested use cases.

Treating the evaluation as a proper project also includes the identification of stakeholders. Those can be part of the evaluation process, like the IT-provisioning team, or potential future users of the product. Ideally, all stakeholders sign off the use cases and commit to the evaluation process before starting the actual evaluation. If a works council exists, it also makes sense to inform them about the evaluation during this stage. Empirically, works councils decide rather slowly, and the earlier they can participate in the process, the higher chances for a smooth process are.

2.3 Market Research

Identifying products worth evaluating can be a challenge. Especially when time and resources for a thorough test of several solutions are lacking, the product selection is already an essential part of the evaluation. Although it might seem tempting just to benchmark the products rated best in analyst papers, in our experience, this approach does not lead to the optimum results. Instead, we had good experiences by creating a short questionnaire that targets our main use cases. This questionaire does not need to cover the tests extensively, and should not exceed 10 to 15 concise requirements. They allow to quickly approach several promising vendors and gather precise and accountable feedback on their solution portfolio. Besides, nothing beats a thorough hands-on demo with the vendor, at best with a technical product engineer. During a demo, documented and precise use cases pay off, as many of them can already be addressed during the demo. Finally, the evaluation scope should compose of three to five promising products, selected by their proposed coverage of the defined use cases.

2.4 PoC Preparation

If not done already, the first step of PoC preparation should be the refactoring of defined use cases into test cases. Test cases need documentation on the desired functionality and how to evaluate it. As during all steps, documentation is vital and ensures that the testing can complete without delays. In our experience, the time spent during the preparation is a good investment when compared with ad-hoc tasks while the PoC is running. As mentioned before, non-functional use cases are a rather important part of testing. Many solutions fail to deliver their expected performance because of non-functional issues. Special attention should be spent on proper documentation, integrations with in-place solutions, compliance topics, and life-cycle aspects.

Besides the test cases, the required infrastructure for the test needs to be prepared. This step depends on the product, and its deployment model. Yet again, time invested during the PoC phase to have the infrastructure prepared and running is well spent. The product evaluation is conducted in an isolated environment ideally, but for some solutions this approach might not be feasible. Especially for solutions that integrate with several third-party products, production deployments might be the only viable option. In this case, all deployment steps need documentation, so a complete rollback of the process is possible.

With defined test cases and a prepared infrastructure, the testers can finally enroll the products. Before installation, we recommend defining documented test goals and periods with the vendor. Open-end testing is tempting but often leads to never-ending cycles of product improvements and configuration changes. As already mentioned, three weeks of intense testing are usually enough to gather thorough insights of the solution's capabilities.

2.5 Test Execution

In most PoC that we conducted, the vendor offered to install the product at the customer site and only required the necessary access rights. It might seem attractive to take some time off during the installation and let the vendor do their work, but we strongly recommend against it. The product installation is already part of the test and allows us to gather a lot of insights into product design, documentation, and maturity. We recommend customer's to install the product by themselves, supported by the vendor. Only when the customer itself executes all necessary steps, an honest assessment of its installation complexity is possible. If a vendor obstructs this request, because the product is too complicated or too poorly documented for a customer-driven installation, this can already be a red flag during the evaluation.

The same applies to product configuration. Vendors can usually assist with best practices and recommended settings, but the configuration itself should be set up by the tester. Changes to the settings are required during most PoCs, and the initial installation is an excellent opportunity to familiarize with them.

During the actual testing, it is rational to stay in close contact with the vendor. However, the vendor should not be present during the actual test, as they typically try to influence testing results in their favor. We recommend to test products using the provided documentation and use regular touchpoints with the vendor to discuss questions and issues. The testers should document all test results in the previously designated format.

A properly executed test inevitably points out missing features and issues. We recommend communicating these issues with the vendor and requesting their roadmap for implementation. Promises regarding added features need to be concrete, committed, and tracked. Experience has shown that vague ideas and verbal commitments cannot be relied on.

2.6 Result Documentation

We recommend splitting the result documentation into two documents. One document should contain all test results, together with short reasoning and description. Since not all test results are black or white, a scale from 0 (not implemented) to 3 (better than required) has proven to work best for our testing. As not all test cases are equally, a weighting can help to clarify which requirements are most influential. The second document contains all auxiliary information and impressions gathered during the installation, configuration, and test. By splitting the documents, facts and opinions are separated and can be treated so in the final decision process.

3 Final thoughts

The presented evaluation process is an outcome of our year-long engagement in customer product evaluations. We believe that the guidelines we presented can help companies to make better product decisions and improve their general security architecture - step by step.

About the author

DCSO is a Berlin-based cyber-security joint venture, founded in 2015 by Allianz, Bayer, BASF, and Volkswagen. We provide security services and enable synergies between our customers.

Within our Technology Scouting and Evaluation service, we provide an overview of the IT-security market and test security products in accordance with our customers' use-cases. Additionally, we support our customer base during custom evaluation projects.

Visit us on https://dcso.de/de/services/technology-scouting-evaluation/
Get in touch: sales@dcso.de