Global Information Assurance Certification Paper

Six Steps to Procuring Security Products for Your Company

A Beginners Guide to Making Informed Purchasing Decisions

Gideon Malino

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b, Option 1
February 29, 2004

Table of Contents

Summary

As you advance your career in Information Security, eventually you will be looked upon to provide your company with the tools to keep your systems and your network secure. This is not a task that should be taken lightly. If a security breach is severe enough, you could end up exposing confidential data, losing your job, or worse, watching your company go out of business.

This guide attempts to make the purchasing process more understandable and manageable for those who are new to this type of assignment. It is not meant to provide you with the exact answer on what to do, but point you in the right direction for making the most appropriate security purchases for your company.

Assumptions

Every company is different, with unique processes in place for making corporate purchases. This document has been written using general guidelines that should be applicable for almost everybody, regardless of those differences. However, there were some assumptions made that should be verified.

- **You have a budget to work with**. If you need to procure free tools, this guide will not help you. You can still use some of the evaluation techniques described below, but this was written with the expectation that you will be given a significant dollar amount with which to procure your security products.
- **Your involvement goes beyond simply suggesting what to buy**. This guide is geared towards the end result of you making a purchase. There are some parts of this guide that will be helpful in researching the best security products for your situation, but it is ultimately about purchasing a solution.
- **You are able to commit to the time necessary to make an informed purchasing decision**. A smart purchase is not made overnight unless blind luck is heavily involved. You will need time to research, document, discuss, test, purchase, and deploy your solution. This can take anywhere from a few weeks to several months, depending on your situation.

As long as these assumptions are true, then you should find this guide helpful and informative. At the very least it will provide you with the first steps towards procuring the best security products for your company.

Step 1 – Clearly define the problem to define the solution

To solve any problem, the best way to begin is to know exactly what the problem actually is[1]. Typically, you will be told to either purchase a specific product ("We

[1] Ohio Literacy Resource Center

need firewalls on our DMZ") or given a general order ("We need our laptops to be more secure"). In either case, you need to know exactly what the problems are that need to be resolved. Do you need to restrict specific ports from accessing your DMZ? Are laptop users not using any passwords on their accounts? Make a list of every problem you can think of. You will find that lists are the greatest way of organizing your thoughts. Write down everything that you believe is a security issue that needs to be addressed.

Once your list of problems is complete, you now need to come up with a solution statement. The best solution statements are only one or two lines long that cover all the problems you listed, but in a non-specific manner. If you are too specific in your solution statement, you will be severely limiting yourself. Take a look at this example:

You need to purchase a product that will be able to scan all 10,000 systems on your network. This product will have to determine if these systems contain the latest patches, make sure no one has set up blank root or administrator password, and no one is running remote control software.

From this statement, you could list these problems as needing resolution:

- You need to scan all systems on your network
- You need to verify all software currency is up to date
- You need to make sure the systems are configured correctly
- You need to discover if any unauthorized software has been installed

Notice how these problem statements are more generalized than in the example. This is a good practice to get into to obtain a "bigger picture" of the security issues you need to solve[2]. Likewise, if your solution statement is "I need to be able to scan 10,000 systems for the latest patches, make sure their administrator or root passwords are not blank, and that no one is running remote control software", you have just left yourself with no room for change or improvement. What if you acquire a new company of 5,000 more systems? What if remote control software becomes necessary to use within your company? The product that would be purchased based on such a strict solution statement would be incredibly limited, and will probably be useless in a few years

A better solution statement for our example would be:

"Procure a scanning tool capable of discovering known vulnerabilities on all networked systems as well as a system's adherence to corporate standards".

In that sentence, the entire network is addressed, whether it's 10,000 systems now or 30,000 systems next week. Patch levels and software currency is

[2] Kalvar, Shannon T.

covered by ‘known vulnerabilities’, and blank passwords and remote control software is covered by ‘adherence to corporate standards’. The best part of this solution statement is that it can change as requirements change. If the network does grow, or more system configuration issues need to be discovered, a product that is purchased based on this solution statement will be able to adapt.

Step 2 – Make this an official project

Determining what security products to use will take up almost all of your time until the products are purchased and deployed. Your management needs to be aware of this, and you will also need to commit yourself to spending the appropriate amount of time and energy. By stating that this is a project, you are appropriately conveying the idea that this will be something your time will be devoted to, will most likely require other corporate resources, and will finish with a well thought out and appropriate end result.

Almost every company has a process in place for starting a project and for making corporate purchases. You need to familiarize yourself with these processes, the last thing you want is to have all your efforts derailed because you forgot to get a Non-Disclosure Agreement signed or never got your budget approved. Speak to individuals in your company who work on enterprise wide projects similar to what you are trying to accomplish. Find out what they did to start their projects and see if you can either work with them or obtain the documentation they used to make your project a reality. Try to list out all the organizations that might have to be involved in your project. Here is a sample list:

- **Information Security** – The security team that you are most likely a part of.
- **Legal/Contracts** – If any purchases are to be made, they will be the ones making sure you aren’t signing away more than you bargained for.
- **Technical Committee** – Many companies have an organization devoted to new products being integrated into the enterprise. If you have one, they will be one of your biggest resources.
- **Engineering** – If you think that the product you will deploy will either run on every system as an agent, or affect the bandwidth of your network, you will most likely have to inform and work with your engineering team. They will make sure the products you purchase don’t break anything.
- **Support** – If you have an organization devoted to break-fix, maintenance, and general support of computer systems, they will almost certainly be affected by many of the security products you procure. They need to be made aware of what is being purchased and what their future involvement will be, as well as what will be expected from them should a security alert be generated.

Of course, your number one resource will be your management. Talk to them about making this a bona fide project. Good management will work with you to make this a success.

Step 3 – Research the Product Space

In Step 1 you created a solution statement. Now it's time to find out what products can provide you with that solution. External research is the best way to create an initial list of products. There are many security magazines and websites that publish reviews on security products. Go through these and write down *all* the products they tested, not just the one or two products they considered to be the best. You will make your own determination as to what is the best solution for your company. An example of this is Network Computing's review on Vulnerability Scanners[3]. They listed 17 different products, but only reviewed 11 of them, and ultimately gave just three products semi-decent reviews. Security products are always improving, so if you were using the Network Computing article as a resource, it would be better to list every product that was referenced, then go through your own weeding process. Alternatively, ComputerWorld maintains an excellent list of Security Vendors that is very comprehensive, but does not provide any reviews[4] on their products. Regardless of where you go to create your list of Security products, be sure to cite all your resources, as documentation will be extremely important to your project (see Step 4). Once you feel you've gathered enough product names through external sources, if there are other security experts at your company, you can then ask them if they know of any other products that would provide you with the solution you are searching for. Many times this will generate a list equally as large as the external list you had previously created.

Now that you have finished compiling a list of products (and of the Vendors offering those products), you can now create an Initial Product Criteria list. This list will allow you to narrow down the products you will consider to make sure you are only focusing on those products that will truly fit your needs. Here are some ideas you can use to create your Initial Product Criteria list:

- Vulnerability Analysis – The product must be able to scan a host system and determine if known vulnerabilities exist
- Patch Management – The product must be able to scan a host system and determine if the software currency is at the latest level. The product must also be able to remotely update software that is found to be delinquent
- Policy Compliance – The product must be able to determine if a host system is configured to meet security policies.

[3] Novak, Kevin
[4] Computerworld

- Intrusion Detection/Prevention – The product must be able to unobtrusively monitor the network and determine if any network anomalies exist, and pin point those anomalies when discovered.
- Distributed Deployment – To complete a scan of the entire network within the shortest amount of time, product nodes should be dispersed geographically across the network. Each node would scan a small section of the network and report the results back to the product's main console.
- Agent Based Software – To complete an in-depth scan of every system on the network, software that will run in the background will be installed on each system and report back to the product's main console.
- Professional Service – An external company will scan and monitor the environment and produce security reports.
- Commercially Supported and Actively Developed - Any products that cannot provide immediate technical support will not be considered.
- Run against Multiple Operating Systems - The product must be able to perform vulnerability and compliance scans against all operating systems in use.

You can also reverse these statements to make negative criteria, such as "Must *not* be a Professional Service". The more criteria you list, the easier it will be to filter the number of products down to only those that will fulfill your needs.

Step 4 – Document Everything

The purchase and use of any product within a corporation is fraught with legality. To make sure that you are not setting yourself or your company up for a legal fall, you need to make sure that all communications you have with the Vendors is documented and saved. Here are two things that you will no doubt experience while purchasing a security product for your firm.

Vendors tend to say what you want to hear. This is not to imply that Vendors are dishonest by any means. In fact, most Vendors want to provide you with the best products available to build an ongoing relationship with your company. However, most Vendors are not technically savvy, or only possess an "old school" knowledge of their products without knowing the newer technologies involved. Vendors rely on their technicians for their information, and sometimes mistake what is being said. There have been many times when Vendors claim their product posses a feature that in fact won't be included for another year or two. They say this because they heard their technicians talking about it, and you happened to ask for that very feature.

The product does not perform well in your environment. It is nearly impossible for developers and manufacturers to think about and test within every possible environment. If you are working in an extremely large or unique network, or have deployed uncommon systems, it's very possible that the products you purchase will not perform as advertised, or even cause system problems.

The best defense against these is to write down all the features, requirements, and concerns you have about a product and have the Vendor respond to it in writing[5]. This is usually called a "Request for Information", or RFI (many people also call this a Request for Proposal or RFP). If the Vendor claims in writing that their product contains a feature that it really doesn't, then your RFI will give you a legal way to break the contract if you've already purchased the product, and even get your money back.

Writing an RFI is no easy task. You need to be extremely clear about what you expect the product to do and how you expect it to perform. Unfortunately there is no standard format for RFIs, and there are many differing opinions on how they should be written. Some would argue that a good RFI should be no more than four pages long[6], while you can find examples of well written RFIs in excess of 20 pages[7]! If you are unfamiliar with writing an RFI, Vendors are actually a great resource for providing you with samples. Realize that the RFIs the Vendors provide you will be geared towards their product, but if you get two or three Vendors to send you samples, you will get an excellent idea of how an RFI should look and what it should contain. To help you further, here is a list of sections a good RFI should include:

- Instructions to Vendors – This details what your goals are (a great place for your solution statement from Step 1), what the timeline for the Vendors are, and how the Vendors should respond (e-mail, fax, print).
- Overview of the Company – This will give a brief summary of what your company does and detail how its network is set up. This is vital to give the Vendors a good idea of how they need to scale their product to customize a solution specifically for you.
- Product Details – This section should contain open ended questions about what the product is capable of and how it should be deployed. This is where questions such as "What Platform does your product run on" and "What type of training do you provide" should appear. This is where Vendors can write about how their product works and why it is the best solution for you.
- Product Requirements – This is where you will list product features and requirement you are looking for. These should all be Yes/No questions. Allow the vendor to also respond with "Partial" if necessary, and then have them explain why they could not answer Yes or No. This section should be where the bulk of your questions reside as it is much easier to evaluate RFIs with quantitative responses (yes/no) versus qualitative responses (open ended). This will be explained more in Step 5.
- Request for Quote (Optional) – This section will detail how you would think the product would need to be deployed in your environment, but would

[5] Watson Jr., James K. and Andrews, Linda
[6] Howlett, Dennis
[7] Pearson, Mike

also ask the Vendor what their opinion is of how the product should be deployed. Feel free to give or ask for several different deployment scenarios (for example, one scenario emphasizing speed of results, one emphasizing accuracy of results, one being a combination of speed and accuracy, etc.). For each scenario, request the Vendor to provide you with the Capital Expense (cost of purchasing the software/hardware), as well as the Operating Expense (cost of maintaining the software/hardware) for one year.

- Legal – Your legal department will need to have a section in the RFI that the Vendor will need to warrant and sign. This is the section that will allow you to back out of the contract if it turns out that any of the answers the Vendors provide are untrue.

Extensive documentation also shows that you performed your due diligence in all your tasks. If management asks you "how did you select a list of Vendors to send your RFI to", you can respond by showing them the research you performed to make your selection (see Step 3). If an auditor comes to you and asks why you didn't purchase a scanner from an already established business partner, you could show them the RFI results from that company and explain why they were not an appropriate choice. In fact, the more documentation you create, the more you can immediately answer questions, explain your reasoning, and even cover yourself legally if need be. You can never have too much documentation.

One thing I would highly suggest is to limit any type of verbal communication with Vendors until you have narrowed down your selection to just two or three of them. Simply request that all communication be handled through e-mail, and also alert your staff not to speak to any of the considered Vendors until after the purchase decision is made.

Step 5 – Select Two Products

The number of products you are left with from Step 3 is usually no more than ten. Contact each of the vendors and send them the Request for Information document you created in Step 4. Make sure to give them a deadline of when to respond, or else you might be waiting for a while for every vendor to return a completed RFI.

While you are waiting for the RFIs to be returned, go through every question that you asked in the RFI and give it a weighted score. A weighted score is a way of assigning points to each question. Let's say you asked the following questions in your RFI:

"Can the product support customized OS fingerprints from the user?"
"Can your product look for a specific UDP or TCP port?"
"Can you pause currently running jobs?"

It would not be prudent to say that each of these questions is equally important. Based on the examples above, you might say that looking for specific UDP or TCP ports is an absolute must for the product, while customized OS fingerprints would be nice but not necessary, and pausing currently running jobs is an expected feature. From that simple description, you've just created a scoring system that could look something like this:

- 1 point = Nice to Have
- 2 points = Expected Functionality
- 3 points = Requirement

So if a Vendor responds to those questions stating that their product allows customized OS fingerprints (1 point), doesn't look for specific ports (0 points), and allows jobs to be paused (2 points), that would score 3 points. If another Vendor responded that their product didn't support customized fingerprints (0 points), allowed specific ports to be discovered (3 points), and allowed jobs to be paused (2 points), that would yield 5 points. The product scoring the higher points would be the more desirable.

Assigning a weighted score to all of your questions can be difficult and time consuming, especially when it comes to qualitative questions (open ended) rather than quantitative questions (yes/no). The questions in the example above were quantitative and easy to score. How would you score the following question?

"What types of vulnerability scanning can your system perform?"

In all actuality, you can't. The best way to score qualitative questions is to simply ask yourself "Did they answer the question" and "How well did they answer the question". This will usually generate a scoring system that looks like:

- 0 points = Did not answer question
- 1 point = Answered question poorly
- 2 points = Answered question well

It is because of the difficulty in scoring qualitative questions that you want to ask as many quantitative questions as possible. I have found that one of the best ways to create quantitative questions is to base them on the qualitative questions that you asked. In other words, if you ask:

"What types of vulnerability scanning can your system perform?"

You can then follow up with questions like:

"Can your product scan Windows systems?"

"Can your product scan UNIX systems?"
"Can your product scan for blank administrator/root passwords?"
"Can your product scan for installed Trojans and backdoors?"

The more quantitative questions you ask, the easier it will be to score the RFI and quickly determine the top two products.

Create a scoring sheet template that lists every question asked and the weighted score of each question. As you receive responses to your RFI, score each one using that template. Once the scoring is completed for all the RFI responses, tally up the scores and choose the top two products. Send back the completed scoring sheet to each Vendor that responded, with an explanation of why you did or did not choose them. Only send the scoring sheet that was used for the Vendor's RFI response, you do not need to send each Vendor the scoring sheets for all the RFI responses. Your explanation of "your product did not meet our needs as well as other products on the market" is good enough. For the products that did score the highest points, request to have the Vendors send you evaluations so you can test their products.

If you find that several vendors scored exactly the same, go through the qualitative responses to determine which product more appropriately fits your needs. If you had included a Request for Quotes section in your RFI, look at who had the better pricing structure. As stressed in Step 4, document how you came to all your conclusions. This can be reflected in a Notes section in your scoring template.

Test the two highest scoring products to make sure they perform as advertised. As with every security product, all tests should be performed in a lab and not on any systems that are in production. A good test plan will be based on the RFI you had created to make sure the product behaves as the Vendor indicated. If you have an Engineering or Technical Support department, work with them to set up a test lab. As always, document how you set up the lab, what tests were performed, and what the product's results were from those tests. If a product performs poorly, let the Vendor know in case there is a setting or configuration issue that you did not take into account. If it turns out that the product does not perform as it should even after the Vendor tried to help, eliminate that product from your project and test the product that scored the next highest points. Be sure to send the test results to the Vendor you are eliminating and explain to them that the performance of the product was the deciding factor to not purchase it.

Step 6 – Negotiate

The reason you selected two products in Step 5 is to make sure you are not locking yourself into dealing with just one Vendor. By negotiating between two products, you give yourself a lot of room for making deals and getting price

breaks[8]. Feel free to let the Vendors know that you are working with other Vendors and considering other products. They will compete against each other to give you the best price they can offer. Be sure to take into account the points they scored in the RFI, and which product you feel really is better for you. It is almost always worth it to pay more money for a superior product, unless the price is absolutely outrageous.

If you have a Legal or Contracts department, make sure they are heavily involved in the negotiations[9]. Let them sign all contracts and agreements if at all possible. They will make sure everything is above board and in the best interest of your company. Your Legal department will also need a copy of the responses from your RFI in case the product does not perform as advertised. Be sure to stay in constant contact with your Legal department in case negotiations break down. The minute they do, you can always contact another Vendor, test their product, and bring them to the negotiation table. This should rarely happen since it is always in the Vendor's best interest to make a sale, but in case it does, you do not want to find yourself dealing with only one Vendor since this will seriously reduce your company's ability to negotiate. Once a Vendor does agree to a price and all contracts are signed, then any dealings with other Vendors should be terminated immediately. Let them know who the Vendor was that you selected with a brief synopsis of why you chose them.

Conclusion

By following these six steps, you will undoubtedly purchase the best security products for your company. Management will praise the efficient manner in which you made your purchasing decisions. Contracts will applaud you for giving them all the documentation they require. Audit will reward you with excellent ratings for purchasing the best products to keep your company secure. Most importantly, you will establish yourself as a serious purchaser and will most likely create long lasting relationships between yourself and the Vendors you work with.

[8] Baby Shop
[9] Melymuka, Kathleen

List of References

1. Ohio Literacy Resource Center “Problem Solving”. July 12, 2002. URL: http://literacy.kent.edu/salt_fork/prob_solv/intro.html (February 21, 2004)

2. Kalvar, Shannon T. “How to assess new hardware needs”. TechRepublic February 19, 2004. URL: http://techrepublic.com.com/5100-6315-5157098.html (February 21, 2004)

3. Novak, Kevin “VA Scanners Pinpoint Your Weak Spots”. Network Computing Magazine June 26, 2003, Vol. 14. URL: http://www.nwc.com/1412/1412f2.html (February 07, 2004)

4. Computerworld “Security Buyer’s Guide”. URL: http://www.computerworld.com/services/buyersguide/cat/0,4846,KEY73,00.html (February 28, 2004)

5. Watson Jr., James K. and Andrews, Linda “Dealing with Technology Vendors: a Buyer's Methodology”. Insurance Technology Online April 09, 2002. URL: http://www.insurancetech.com/it2/story/IST20020409S0001 (February 21, 2004)

6. Howlett, Dennis “How to... write an applications RFI”. Techworld January 28, 2004. URL: http://www.techworld.com/features/index.cfm?fuseaction=displayfeature&featureID=305 -requires free membership (February 29, 2004)

7. Pearson, Mike “Authentication for e-government: Request for Information”. e-government October 31, 2003. URL: http://www.e-government.govt.nz/authentication/authent-rfi-200311.pdf (February 29, 2004)

8. Baby Shop “Getting Your Best Deal from Vendors”. URL: http://www.babyshopmagazine.com/fall99/bsf9914.htm (February 21, 2004)

9. Melymuka, Kathleen “How Will You Manage Your Vendors?”. Computerworld January 06, 2003. URL: http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,76968,00.html (February 07, 2004)