Security Vendor Management

Justin Hall
CBTS

First - a brief exercise...

What's a good vendor look like?

Or - how can you tell a good vendor from a bad one?

A good vendor is recognized by the community

- Smart guys talk about the vendor's products
- They're referenced on top tools lists (i.e. sectools.org)
- Analysts put them in their "magic quadrants"

A bad vendor is one you've never heard of

- They've been around for about six months
- They have no customers you're familiar with

What's a good vendor look like?

Or - how can you tell a good vendor from a bad one?

A good vendor is known for their research team

- Members of team speak at conferences
- They discover significant vulnerabilities
- They contribute to the community as a whole

A bad vendor has no research team

- You only hear about them in press releases

What's a good vendor look like?

Or - how can you tell a good vendor from a bad one?

A good vendor is focused on solving a particular problem

- Recognizes their place in a defensive strategy
- Maps to a single critical control (or two)
  - See http://www.sans.org/critical-security-controls/

A bad vendor tries to fix everything

- They claim their product will "make you secure" and that it's "all you need"
- You aren't sure exactly what they do

What's a good vendor look like?

Or - how can you tell a good vendor from a bad one?

A good vendor is standards-based

- They conform to ISO, COBIT, NIST, etc
- They can tell you where they fit into those guidelines
- Their products use IETF's RFC standards
  - File types
  - Protocols / communication

A bad vendor is 100% proprietary

- "We can't tell you how that works"

How do you choose a vendor?

- Ask your peers
- Ask the community
- Ask the analysts
- Ask consulting companies, salespeople
- Check out the news

Case Study - Admiral Power - SIEM

- Global energy company - 100k users worldwide
- Highly diverse IT infrastructure
- Somewhat mature security architecture
- Small incident response team
- No centralized logging

"We need a SIEM product. Everyone's talking about them. I hear they can help us with compliance. At least, that's what the <ENORMOUS SECURITY VENDOR> sales guy told me yesterday when we were playing golf. You should check it out."
- Admiral Power's CISO to you

How do you choose a product?

Or: Don't just rely on the vendor

Why do you want it in the first place?

- What problem does it solve for you?
- What controls does it provide?
- How does it provide C,I,A?

How will you use the product?

- Who in your organization will design its implementation? Who will do the actual install? Who will administer/maintain the product?
- How will it fit in your security team's day-to-day work?
- What does a successful implementation look like?
- What are your use cases?

Admiral Power - SIEM Use Cases

You: "So, what kind of activity do you want to detect with this SIEM?"
CISO: "You know... bad guys. Evil stuff."
You: "Okay. Which of our log sources do you want to analyze to detect this 'evil stuff'?"
CISO: "Anything you think we should look at. All of it. All the important stuff, anyway."

A real use case:
If we see an attempt to visit a known malicious web page from our proxy logs by an internal host, followed by at least five failed login attempts to our directory service, or ten block alerts from our firewall, from the same host, fire an alert.

Plan your evaluation

- Assemble your use cases
- Gather stakeholders
- Lay out your decision criteria and prioritize
  - What HAS to be in this product for us to choose it?
  - What SHOULD be there?
  - What's "nice to have" but not necessary?
  - Assign quantitative score to each requirement for apples-to-apples comparison
- Choose your initial set of vendors
  - Remember our criteria from earlier!
  - Request short sales pitch & product demonstration

Admiral Power - SIEM Requirements

- Security staff gathers representatives from management, desktop support, server team, network team, and compliance
  - Documents use cases and log sources that will be required to identify activity from cases
- Creates list of 60 requirements, broken down into eight high-level categories
  - Assigns ranking (low/medium/high) priority to each requirement as well as numerical score
  - Chooses ten SIEM vendors for initial round of sales pitches

Product Evaluation

- Weed out the weak vendors
  - Which ones showed off the product (not just slides)?
  - Which ones appeared to match closely with your requirements?

- Bring in the good ones for a hands-on demo
  - Assemble an evaluation team
  - Develop an assessment plan
    - Goal is to measure how well each product meets your requirements
    - What's your capability to evaluate the products? How much time, equipment, talent, etc. are at your disposal?
    - Cost is a factor but shouldn't overtake / exclude your other requirements

Admiral Power - SIEM Evaluation

- Eval team sees demos from ten SIEM vendors
- Team has enough time and resources to evaluate four of them
    - Each vendor is given two weeks to build evaluation system on-site
    - Eval team works with vendor to provide requirements, use cases, sample data
    - Once system is built, team spends remainder of evaluation period testing, documenting and scoring
- Once testing period is complete, eval team assembles results and reports to CISO
- CISO takes results to business to work out budget & negotiate cost, support, etc. with vendor

Maintaining vendor relationships

- Does the vendor want a relationship?
    - If not - should you really be doing business with them?
    - Do they treat you like you're important?

- Meet regularly with your contacts
    - Technical Sales Engineers -> Technical Security Staff
        - Discuss technical issues, suggest features, etc
    - Account Managers -> Security Management
        - Discuss strategy, roadmap, viability of vendor

- Leverage support team
    - Don't be afraid to bring issues - large or small - to the vendor's attention
    - Be aware of their long-term strategy, R&D goals, etc

Maintaining vendor relationships

- Keep your products up to date!
  - Avail yourself of vendor communication - newsletters, vulnerability bulletins, blogs, etc
  - Make sure they know how well their patches / feature updates are working (or not working)

- Join User Group, Community, etc
  - Look for official UG's or ad-hoc user forums
  - Trade horror stories, ask questions
  - Sometimes, far more valuable than talking to vendor
  - Does the vendor participate?

Questions?

Justin Hall
Security Architect
Cincinnati Bell Technology Solutions
justin.hall@cbts.cinbell.com