

*WhatWorks in Vulnerability Management:  
Wrangling Vulnerabilities in the Wild West of Websites*

October 2010

## 2. About the Speaker

The user interviewed for this case study has requested anonymity to maintain confidentiality. The WhatWorks program can help more users make more informed decisions if we allow seasoned professionals from major user organizations to share their stories without revealing the name of the organization.

# 3. What tools are selected for inclusion in SANS WhatWorks?

- Only tools that...
- Can be proven to significantly improve the defenses
- Are cost-effective, and
- Presented by an independent user willing to share the lessons learned

## 4. Can you tell me a little bit about your environment?

We have a very complex environment: We're distributed, not only geographically, but also into almost 30 different departments with hundreds of websites and web applications running varieties of technologies on different platforms. Following some major publicized security breaches, we revisited our security program with relation to application security, web security, vulnerability management, and where those items converge in an effort to see where the enterprise was overall. We collapsed a few security teams from different departments, took some resources from internal IT and other departments, and consolidated them to work across those boundaries to clean up the situation.

# 5. How did you begin?

- The first step was building a governance structure to try and encapsulate the situation we had at hand and bring all those parties into some sort of control.
- We had pretty good security policies, but there weren't effective enough enforcement mechanisms.
- We took a modernized view of the web and designed a framework that could be more of a living document over time: overall conceptualized ideas, and sub-policies and procedures that define the specifics.
- We also brought together the governance structure starting at the senior management level to make sure they're endorsing those changes.

## 6. Buy-in was key?

- It's a painful process whenever there's any sort of change. Consulting the people affected certainly slows down the effort, but it was critical to getting traction on the issue.
- Having senior management involved in the governance structure, endorsing those changes, and steering the direction so it wasn't an IT-led initiative, was critical. The web stakeholders were leading the initiative and they had the ultimate say in it.
- We made it clear that we were there to advise how to best protect this investment and lay down some groundwork for the rules of the road. It was much more successful in a sustainable fashion than taking a purely authoritative approach.

# 7. How did their buy-in influence the process?

- When you don't have buy-in and you try to set up a meeting, they often decline and it's off their radar.
- Once you flip the tables, and the accountability isn't so much on security but on who owns the problem areas, they become a lot more attentive and responsive.
- When you have a bad problem and you get senior management attention, there's a limited opportunity to take advantage of the situation and implement a systemic change in the process that enables security to succeed.

# 8. How did you go about finding a solution?

- Coming from zero it was a big gray area that we were heading into--today there are a lot more resources available.
- We started by just looking at what was out there: the major players on the market then were SPI Dynamics, Watchfire, Cenzic and WhiteHat.
- We picked up some standalone web vulnerability testing tools to get us off the ground, but the problem is really beyond just being able to scan a website.
- You don't have any intelligence that you can supply upstream or downstream to really make any significant decisions--we really needed a much more powerful tool that could help us organize and prioritize the thousands of issues we were discovering.

# 9. How did you narrow the field?

- We developed technical requirements as well as reporting, metrics and data management requirements.
- We were able to get around our normal RFP process and go directly to Cenxic because they had some unique features that met both our functional and business requirements and left room to grow. It was also the only solution that met all of our needs and fit within budget.
- Originally, we wanted to outsource because we didn't have the staff, knowledge, skills and ability, but the budget just wasn't there.
- Cenxic had a flexible solution where we could go on a subscription basis, start out small and get what we need for the first year to get off the ground. We went that route and then augmented our staff and scaled up as needed.

# 10. Why did Cenzic win out?

- We tested all the scanners against a variety of applications with known vulnerabilities to see which worked best.
- We focused on the business requirements and advanced features where Cenzic was far ahead of the other candidates that met the technical requirements.
- We use all three to cover the bases. Besides Hailstorm, our security group also uses WebInspect standalone (we'd already bought it) and our Dev/QA team uses App Scan for their IBM technologies. Hailstorm provides a great portal environment where we can import those scan results too.
- Acquisitions scare us to some degree because we wanted web vulnerability management from a company that would stick to its core function.
- Cenzic's feature set was a little bit ahead of the curve, including more intuitive reporting.

# 11. How was the initial set up?

- We got it up and running very quickly. They were able to come on site and provide assistance as needed.
- The hard part is finding your websites if you don't have them cataloged. We had to really get creative and come up with some ways to mine existing data: DNS records, queries against network logs, etc.
- We put some responsibility on the units themselves. Part of the new governance structure created new roles and responsibilities for individuals to manage that type of information.
- All new websites have to go through a pre-production assessment from security, editorial and governance angles before they are approved for launch.

# 12. Which method was most successful in finding the sites?

- DNS--if you're not paying attention to that you're going to be missing something major, so that is a guaranteed resource.
- External hosting is difficult if all your vendor relationships aren't managed adequately. Check with your procurement and contract management folks.
- Tracking down the outliers is a difficult task and we haven't come up with an adequate solution other than following the money... eventually existing sites will need to renew domains or hosting and that is your opportunity.

# 13. How do you handle it when you find issues?

- Cenzic's multipronged approach really helps. We can provide both low-level and high level information so both managers and developers can get what they need to understand the issue.
- Some teams are on top of it and they understand it. Other teams need a lot of training and awareness. We created a separate stream of training, awareness, and education initiatives just to make sure we were making an application security program that was sustainable.
- All the reports we send out come with remediation instructions, and then we try and create working groups within the development communities, so they can learn from each other and they don't all become dependent on us.

# 14. What kind of staffers do you look for?

- To make the software give you valid and complete results you have to understand the tool and the application—it's not just reading instructions and pushing a couple buttons. It requires very advanced knowledge.
- In the defense industry, for example, they're looking for someone who is in their 50s, has 20 years of experience, knows what COBOL and IV&V are... and has been there and done that.
- If you don't have someone who has been a developer or at least understands the fundamentals of development, the software engineering process and all these complex ins and outs you're definitely not going to be getting the maximum value out of these tools. It's a different animal than running Nexus and patching your servers.

# 15. Are there any recommendations you'd give to other groups looking for solutions?

- Even if you had all of the tools available to you they're still only going to find maybe half of known vulnerabilities, so it's a very difficult space to work in.
- The advances in technology are so fast it's very difficult to keep up, so partnering with a company that is aware of those complications alleviates some of that responsibility.
- I don't think you're going to get away from using automated tools, but some folks look at them as the only thing they need and that is definitely a fallacy. They need to be complimentary to strong processes, layered defenses and competent staff or you're going to get hacked just the same.

# 16. You've put a great deal of planning and effort into this. Is there anything else to share?

- This has been a huge effort between our web, security and IT groups that has probably taken about a year and two or three iterations of remediation effort.
- We adopted a web application firewall, use a reverse proxy mechanism, egress filtering and VLANs, segregate to prevent a compromise of one box affecting other boxes, etc.
- Education, awareness and training are key support mechanisms. If developers and integrators don't understand the issues you'll soon be back where you started.
- Empower developers with the tools themselves. Hailstorm makes this fairly simple with LDAP integration and the ARC Portal.

# 17. How is tech support?

- We utilize their standard support service included as part of our subscription, but they also offer 24x7.
- The support staff are very responsive and account management is always keen to make sure issues are being followed up on and resolved as quickly as possible.
- We work with the same folks who are knowledgeable about our installation and previous support issues.
- Once or twice, we've had support issues that did require escalation and we were able to work with product engineers who quickly resolved our issues.

# 18. Are there features that you wish it had that it doesn't?

- We've provided Cenzic with probably a half dozen or so Request for Enhancements (RFEs) and probably 50% of those have been implemented in future iterations of the product. To date we've been very happy with their agility.
- We wish it had increased performance and scalability for large enterprises, and, according to their CEO, this is coming in their next release. It includes expanded OS support (64bit), improved scalability and other under-the-hood improvements.
- We are also waiting for increased scan notification options. We would like the option to send notifications when a scan gets added to the queue or just prior to starting so we could send automated messages to the site owners in case they experience any issues during the scan.

# 19. Overall, are you satisfied with the solution?

- We have definitely been satisfied with the solution to date and it has been key to our efforts in sustaining an enterprise application security program.
- Cenzic still appears to be leading the pack so we look forward to renewing our contract and continuing to work with their team.
- We also utilize Cenzic's managed service, Click to Secure, which has greatly complemented our in-house capabilities and enabled us to manage demand and respond more quickly during increased periods of activity.

# 20. SANS Bottom Line on Cenzic Hailstorm:

1. Flexible licensing options, professional services, managed service combinations allow for all organization types/sizes to find a feasible solution;
2. Pioneer in commercializing fault-injection technology, continues to provide innovative methods of web application testing techniques;
3. Integrates with VMWare Virtual Center/Lab Manager, so you can scan 'production' environments without impact;
4. Integrates with application firewall solutions like Imperva and Citrix;
5. Flexible management and reporting interfaces with built in compliance suites, as well as integration with bug tracking, static analysis tools and application firewalls;
6. Great support staff, responsive to enhancement requests.

# 21. Questions

- E-mail: [q@sans.org](mailto:q@sans.org)

- **Cenzic**

Visit: [www.cenzic.com](http://www.cenzic.com)

E-mail: [request@cenzic.com](mailto:request@cenzic.com)

Phone: 1-866-4-CENZIC (866-423-6942)