SANS

WHAT WORKS™

Increasing Vulnerability Management Effectiveness While Reducing Cost

WITH

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know about? Let us know.

www.sans.org/whatworks

ABOUT THE USER

The user interviewed for this case study has requested anonymity to maintain confidentiality, but has allowed us to refer to him as a Senior Enterprise Security Architect at a global healthcare services firm. The SANS WhatWorks program can help our security community at large make more informed decisions by encouraging seasoned professionals from major user organizations to share their stories without revealing the name of the organization.

SUMMARY

The senior security architect at a healthcare services firm needed to upgrade the organization's vulnerability management processes to both close gaps in security and to provide stronger reporting when IT operations was outsourced to an external contractor. They selected SecurityCenter Continuous View™ from Tenable Network Security and found that they met all their security goals while actually reducing licensing costs by 75 percent as well as reducing security administrative time by using Tenable's automated reports. Tenable SecurityCenter Continuous View also enabled them to reduce the time to perform critical scans from six hours to 45 minutes, and they are able to run virtual instances of the Nessus® scanner out at cloud services. They also used Tenable's passive vulnerability scanning capability (a feature of SecurityCenter Continuous View) to monitor Internet egress points and detect vulnerabilities in workstations where scanning was not practical. The bottom line was a significant increase in security while reducing both procurement and staffing costs.

Q Tell us a bit about your company and what role you have at your organization.

A I'm the Senior Enterprise Security Architect at a global healthcare services firm. My role encompasses overseeing all the non-compliance aspects of security – technical security applications, security infrastructure and so forth.

Q Do you report to the CISO?

A We don't have a CISO role. I report to the architecture organization, and I have three roles: Quality, Architecture and Security.

Q And is that in the IT organization?

A Yes, it's in what we refer to as Business Technology.

Q What sort of problems were you facing that caused you to look at these types of solutions?

A There were a couple of problems we were facing. The first one was we were rolling off of our existing vulnerability management product, which was Nexpose®. We had hit the end of our three-year initial buy on it – and having mixed emotions about it, weren't considering renewal.

In addition, in May 2011, management decided to outsource about 95 percent of IT services and application development to Hewlett Packard Enterprise Services. The reporting and the ability to track vulnerability management, and track existing vulnerabilities in the network that I got from our existing solution in Nexpose was not suitable for the outsourcing arrangement. So, not only did we need to track things just from a security perspective and maintain a particular posture, we now had financial ramifications due to things HP committed to do in their contract with us – keeping servers patched and keeping the organization free of vulnerabilities and so forth.

There were things I couldn't report back to the appropriate parties particularly well with Nexpose. In addition, we had some other gaps in our vulnerability analysis around workstation scanning, and around correlating event logs with the vulnerability from the network; it was sort of a home run solution when we looked at Tenable's SecurityCenter Continuous View™ (CV).

...we had some other gaps in our vulnerability analysis around workstation scanning, and around correlating event logs with the vulnerability from the network; it was sort of a home run solution when we looked at Tenable's SecurityCenter Continuous View.™

Q Did you look at other things besides Tenable SecurityCenter CV when you were looking at alternatives to Nexpose?

A Honestly, no, we did not. That was the first solution we looked at. I had been pretty familiar with Nessus in the past, and we actually had the Nessus scanner prior to bringing Nexpose in. It was prior to the existence of Tenable SecurityCenter CV; so, we really wanted to rollback. We tried Tenable SecurityCenter CV on an evaluation basis for 30 days, and after about a week we were sold on it.

Q From a funding point of view, did you have a budget for Nexpose and you were able to just use it with Tenable?

A Yes. We ended up with a 75 percent cost savings at the time with Nexpose versus Tenable SecurityCenter CV.

Q You saw a 75 percent cost reduction when you went to Tenable SecurityCenter CV?

A Yes. It was a quarter of what Nexpose cost. Even with all the add-ons and extension of the license – our Tenable costs are only about half of what we were paying for Nexpose.

Q Tell us about the scope of the solution; how it's deployed, how many/what sort of products and sensors, etc., you're using.

A We have kind of an interesting environment in that we're moving the way everybody else is. We're distributed between a physical co-located data center down the street from our office in which we have a dedicated environmental space and a large set of services on Microsoft Azure™, and then we're going to be moving some services to AWS soon as well.

This environment is the major factor that makes this the most cost-effective, appropriate solution for what we're doing. With my deployment of Tenable SecurityCenter CV, I get 512 Nessus scanners. I don't use nearly that many, but I can actually build scanners in my data centers, scanners on infrastructure of the service on Azure, scanners on AWS, and I can backhaul all the data back into Tenable Security Center CV, which runs locally, into a co-located data center.

So, that's the deployment for the vulnerability scanning piece of it, as I mostly use several distributed scanners. I also have some local scanners at remote sites with low bandwidth since it doesn't make sense to scan across their connections, and it doesn't work very well. The ability to distribute scan load is very, very important to me, so I take advantage of that in the solution.

As far as the logging, the Tenable Log Correlation Engine™ (LCE)™ is great. We have one. I call it my Master, which has the aggregation and one log collector on it. I also have a second log collector, so I've been able to collect logs on about 1,400 servers on two machines, which is not a bad value for your money.

I just have one passive scanner (PVS)™ right now, and I span the egress traffic from the network. All my locations backhaul their Internet access through my data center, and I span all that egress traffic back into the passive scanner. PVS handles about 85 to 100 Mbs of traffic a second without any resource constraints. I'm barely pushing it.

Q So, to understand – where you have some things running on Azure and AWS™, you're running instances of the scanner out there or you're scanning from a central location through connections out to those services?

A I'm running instances of the scanners out there, because we have sites like VPNs with IPs basically cut-off from our data center. So, they act like extensions of our own internal datacenter. I don't like scanning across VPN. I've had some issues, and also the VPNs are not tremendously reliable. I don't feel that if I scanned across VPN, I would necessarily get a full scan, or the tunnel might die in the middle of the scan. So I run local scanners there and then send the results back to Tenable SecurityCenter CV, which is a much smaller transaction.

PVS handles about 85 to 100 Mbs of traffic a second without any resource constraints. I'm barely pushing it.

Q When you talked about the Log Correlation Engine, 1,400 servers – do those include things running out at AWS or Azure? Or are those all local or a mixture of both?

A It's all local right now. I'm probably going to build some more collectors soon and start back porting to or backhauling the events to LCE.

Q You said your license goes up to 512 scanners. Do you have a rough number of how many you're actually using?

A Yes. I have 18.

Q How frequently do you scan?

A Everything gets scanned weekly. I have a set of scans that runs every night on a subset of the environment.

Q Do you have no-scan zones or no-scan times or is everything scanned pretty much every night?

A I take a portion of the servers, scan them on Monday, a portion of the servers, scan them on Tuesday, and so forth; but every server gets touched a minimum of once a week.

I had scans that would take six hours in Nexpose that run in 45 minutes in Nessus.

Q Are you scanning production servers at least once a week as well?

A Yes. We have a designated time that they're allowed to be scanned.

Q When you made the decision, "Okay, we're going to go from Rapid7 to Tenable," what process did you use and how long did it take you to switch over and get fully operational?

A It wasn't bad. I mentioned the cost savings we had before. And even with that cost savings, I got more IPs than what I had licensed with Nexpose. It took maybe a week to get everything moved. I had mentioned we outsourced to HP. I used their master list of all the things in the datacenter, and built repositories and asset groups in Tenable SecurityCenter Continuous View to match up with what's in their list, since HP uses that as their source of truth for what servers belong to what.

I built the repositories in groups to mimic how HP structures their data. I set up scans. We had some scans in Nexpose, so I was able to port that schedule over, which is another thing that's great with Nessus. I had scans that would take six hours in Nexpose that run in 45 minutes in Nessus. So, I was actually able to cram more scans into one night or bring in some new checks I hadn't been doing before because of the accelerated scan times. I could do different things, allowing me a little more flexibility.

Other than that, it was pretty much "turn everything on and get it up and running." We had only one application which broke with Nessus. Oracle® Coherence was a problem. Coherence will accept data on a particular port and try to process whatever data it gets, and if it doesn't like it, it crashes. That was easy enough to troubleshoot and figure out with Tenable.

Q In your case, you're using Tenable's SecurityCenter CV, but HP's essentially responsible for maintaining the servers and whatnot. How do you get information over to them? Is it reports? Is there some integration? How are you doing that?

A We have a custom report we wrote and we call it the TAP Report, which is an acronym for threat, age and prevalence. We'll take the data out of Tenable's SecurityCenter CV and write a logarithmic function that incorporates how Tenable SecurityCenter CV has scored the vulnerability, how old the vulnerability is, and how many servers are affected by the vulnerability. Then, it spits a score out. It's just something that made sense for our environment. In the past that had been done with spreadsheets, which wasn't reliable, since they can get lost in email. So we've been converting that into our own web application, where you can upload the spreadsheet. It will parse their ports. And then, when Tenable SecurityCenter CV 5 is released, the plan is to go to using the new REST API and a web app we wrote to grab the data itself so there's no upload process.

Q Is there some trouble ticket integration? How does vulnerability information get over to HP to cause remediation action?

A We don't directly integrate. Like I said, we had that report, and we distributed the report on a bi-weekly basis. And now with the new web application we developed, they're actually able to enter their responses directly in the web application, such as "We think this is a false positive/We're going to patch this in the next patch cycle/We want a security exception for this one" and that sort of thing. So, we don't have the integration right now, but that's where I'm really looking for that REST API in version 5. We started writing some stuff and then we realized it was all going to change in Version 5, so we decided to wait until that comes out. So, it's still a very manual process right now, but I think we'll be able to automate some things in the future.

Q You said you're using the Passive Vulnerability Scanner™ (PVS) at that egress point. So any vulnerabilities it indicates are simply integrated in with everything from the scanners?

A Workstation scanning has always been hard for us. Before I came to this organization, there was a principle that everybody should have a laptop, even people who probably didn't need a laptop, since they never take it home. But, people do take them home even for their children to do homework on. We're a fairly progressive company internally as far as technology goes. We have a lot of folks who like to use company issued tablets or use their own cell phone instead of company issued equipment, so it's difficult to catch things on the network or catch things on the wired network if they move to wireless and so forth.

So, the PVS really addressed the need for us to just span all the egress Internet traffic out. We'll pull vulnerabilities out of it, then we do the same sort of process with HP. A different team manages the workstations than the servers, but we send them that same report with the logarithmic function: how many workstations are affected, what's the threat and vulnerability, how old is the vulnerability. And then, they're required to address those vulnerabilities as well.

Q So, how do you think it compares to what PVS finds that way versus where you could do an actual scan of an endpoint on the wired network? Do you think you're getting the equivalent visibility at the vulnerability?

A I think we're getting a very good visibility into the vulnerabilities that have the highest likelihood of exploitation or being the initial entry point into the internal network, and those are the things I'm most concerned about. Now, I'm going to start actually shipping some local Nessus scanners out to my sites that are going to backhaul some data into Tenable SecurityCenter CV soon, but I'm still considering that at best a point-in-time analysis of what's on the network. If people shut down their laptops, take them home, move them to wireless in the middle of scanning, I'm kind of out-of-luck, so, PVS is still going to be very, very important to us. I think the data for PVS will be more complete than what I would get from just regular vulnerability scanning.

Q Are there reports you're using out of Tenable's SecurityCenter CV; whether its PCI compliance, HIPAA compliance or any other reports you're using out of SecurityCenter?

A Yes, there are. So, even though I try to stay away from the compliance stuff, I do the HIPAA compliance audits as part of my weekly scans of every server on the network. We send them along with the TAP Report, as well as a templated HIPAA compliance report for each application.

I think the data for PVS will be more complete than what I would get from just regular vulnerability scanning.

Q You said you have 1,400 servers or so. How many endpoints are involved – user endpoints?

A 2,300 to 3,500.

Q So, to cover that and to run your install and everything, what sort of staffing do you have? Is it a full-time equivalent or a part-time job for somebody?

A It was me only until a year ago. The more we do with it, the more we are going to need to an additional technical resource. I would say its equivalent of one FTE. Right now there's myself and a junior person I hired who administers/does the care and feeding for the product. We probably spend half our time dealing with it apiece. So, it equates to one FTE.

Q Nexpose has web application-type scanning functionality. Were you using that? Are you finding the equivalent in Nessus?

A I'm not a big fan of automated web app scanners. We have our own web testing methodology. We write a lot of web apps and a lot of mobile apps. Right now, I've got 400 and some odd websites exposed out of the cloud and internal datacenters that are variants of about 34 web applications, web and mobile applications, I should say.

I don't think automated scanners find logic flaws. I don't think they find authorization failures. I think there are a lot of things they don't find. And so, the testing methodology I've developed, and that I've trained my junior counterpart to do is about 30 percent automated. We do use Nessus to look for vulnerable components in web applications, but we don't use it to find any application specific vulnerabilities. It's about 30 percent automated and 70 percent manual what we do. That's not a byproduct of not being good at it; it's simply that I don't believe in them as an application testing solution.

Q You said you started this transition in 2011. So, you've been using Nessus for close to two years now?

A Yes. It was three years in August this year. We purchased it in August 2011.

Q So, thinking back to when you got started and even the past couple of years, are there any lessons you've learned now that you know/would have done anything differently that we can pass on to others?

A I probably would have organized the assets a little bit differently in Tenable SecurityCenter CV. There were a lot of things that we didn't take advantage of in Tenable SecurityCenter CV, like the dynamic asset groups that we should have. The product has changed so much from where we started. I think we started with version 4.2 or 4.3.

There's been so much integration. I've spent a lot of time writing reports in it and learning the query engine and learning how to build dashboards. That was one of the differences in Tenable SecurityCenter CV versus Nexpose. Nexpose gave you, so to speak: "Here's the house. It's painted this way. Here are the walls and the siding. This is the way it is. This is what you get – and you get what you get." With Tenable SecurityCenter CV, it's more like: "Here are the nails and the wood and the paint. You build it the way you want it."

There were a lot more manual build-in things. But the introduction of the ability to search for pre-built dashboards and reports that Tenable introduced in 4.8 has actually been very, very helpful. A lot of the things I spent time doing manually and tearing my hair out writing when we started out are now already built for you.

...pre-built dashboards and reports that Tenable introduced in 4.8 have actually been very, very helpful. A lot of the things I spent time doing manually and tearing my hair out writing when we started out are now already built for you.

The biggest thing that I've learned was that perhaps if it doesn't have a feature, that Tenable's probably going to write it in the next release. So, they're very perceptive as to the challenges people have with the product and addressing them and trying to streamline things.

Q And you said you had a few low speed links where you put local scanners and forward the information. Did you know of that issue beforehand or is that something you found out once you started trying to do the scans over those lengths?

A Basically, I found it out with the first one that I tried. I worked with Tenable support, and they are always very helpful. I probably opened more tickets with them than anyone; since I'm paying for the support, I may as well use it. First of all, I found we couldn't get the scans to run right. After that, I decided it was going to be our standard practice to put a local scanner everywhere we needed to deploy. Anywhere we weren't going to be able to deploy, we just put a local scanner out there.

Q Are there any features or requirements you've asked Tenable or told Tenable you'd like to see added?

A One thing that has created some security issues, or rather come up on our third-party pen test when they come internal to network is credentialed scans. I use a domain admin account as opposed to trying to manage individual credentials for each server, which would be impossible. I use a domain admin account to log in to Windows machines that are targets of scans.

The problem is when you log out, you have that residual session, which can be used in pass-the-hash or token-replay attacks. The account stays in the machine. That's one of the negatives about it; you do have to leave. If you want the credentialed scan, you can either scan over the network and not log in the machine and run a higher likelihood of breaking things. Or you can log into the machine and get more insight into what's on the machine and the vulnerabilities on the machine. You don't break things, which is great, but you do leave that residual administrative session on there because of the rights the scanner needs for analysis.

Q Does passive scanning of user endpoints over the network give you the same results as credentialed scanning?

A I feel pretty good about it. Like I said, with PVS you're not going to get the locally exploitable things on the machine, and that's just the way it is. I'm more concerned about that on servers than workstations to a degree. But, if I can pick off some of the remotely exploitable items and codes of vectors where someone might get the foothold in the machine and then use something local or some privilege escalation – it makes me happy. I don't feel like the vulnerability scanning's ever going to be 100 percent, regardless of what you do. But, if you can systematically identify as many risks as possible given the time that you have to scan, I think that's where the value is.

Q You're using the product side tech support. And you're happy with their support?

A Yes. If I have a quick question, I have the chat function. If it's something severe – like it's completely broken – I'll call in. But they're always very responsive. They're always very helpful.

I recall when first installing PVS, I couldn't get the web console to load. I couldn't figure it out. I sat with a tech support guy for about an hour, and he couldn't figure it out. Then, he said, "Well, hang on – let me see what I can do." I got a phone call and there were three or four developers, the Product Manager, and two or three tech support guys all in a conference room with WebEx™ up on the screen looking at my stuff saying, "Okay, well, show us this, show us that." They were trying to figure it out with me. So, they're always good to escalate when necessary. I've only had one or two times when the tier 1 or tier 2 tech support hasn't been able to solve things. So I have had really good experiences with it.

Q Have you had to use any paid professional services from Tenable outside the product support you're paying for?

A No, I haven't. It's easy to install and deploy.

SANS bottom line on Tenable SecurityCenter Continuous View:

- Reducing how long vulnerability scanning takes is key to moving towards more continuous vulnerability assessment and mitigation.
- Adding passive vulnerability assessment to active scanning reduces assessment gaps and enables higher fidelity vulnerability assessment.
- The use of virtualized scanners supports integrated assessment of cloud-based servers.
- Automating standard reports reduces administrative time and eases integration with IT asset management systems.
- To make mitigation easier, where possible group your assets the same way IT operations does.
- Tenable's integration of Nessus, passive vulnerability scanning and Tenable SecurityCenter Continuous View reduced licensing and operating costs while supporting more frequent and more accurate vulnerability assessment and mitigation.