SANS

WHAT WORKS™

Lifecycle Vulnerability Management and Continuous Monitoring with Rapid7 Nexpose

SPONSORED BY

RAPID7

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

SUMMARY

Continuously monitoring and mitigating vulnerabilities is widely accepted as basic security hygiene for any security program that will be successful in avoiding or reducing the impact of breaches. While the value is clear, the obstacles to assessing vulnerabilities more frequently and more accurately have slowed adoption. However, many security leaders have invested in improved processes, more advanced security products and threat-driven prioritization approaches to show immediate and measurable increases in both the effectiveness and the efficiency of their security programs. This case study details the steps a Global Director of IT Security took to do just that.

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 Global Director of IT Security for a manufacturing company. 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.

Q Can you tell us a little bit about your background and your role at your Company?

A I'm the Global Director of IT Security and I report to the CIO. I have been in this role for about four years and have spent the majority of an 18 year career in both infrastructure and security. Today I'm responsible for our risk and cyber security program, areas of compliance, and our disaster recovery program. The scope of all of the responsibilities is global.

Q Give us an idea of the scope and what business your company is in.

A We're a global mid-western-based industrial manufacturer. We have been around for 120 years.

Q What sort of problems drove you to look at and evaluate solutions?

A When I first moved into the role, we really looked at what was in the marketplace – what was expected, how other security programs were being built, developed. Visibility was first and foremost, something that we were lacking in many areas of our security program. We had decided from a priority perspective to look at vulnerability management. We had been patching operating systems for many years, but we weren't sure what our success rate was, what that looked like globally, and beyond just operating system patches, what did that look like for applications, databases, both desktops and server systems.

Q What was the baseline you were starting with as far as vulnerability assessment?

A We had used some open-source tools and had been able to cobble together some reporting. But, by the time we had any actionable intelligence, it was months out of date. We were looking for something that was more real-time, so when scans run, we wanted reporting to get right to the people who were operationally responsible for those areas to give them some intelligence to be able to execute and act on vulnerabilities in our environment.

Q Was there an incident, an audit event, or how did you convince management to fund the project and move forward?

A No, no specific incident. We had brought in companies to perform vulnerability assessments and penetration tests, and we really felt like a vulnerability management program, being run internally, was going to provide a significant benefit in risk reduction for our overall company and environment. So, this was looked at by management as something that would not just be cost effective, but a key cornerstone to our security program.

Q Did you have PCI exposure that required you to do quarterly compliance? Did you have any other compliance-type drivers related to this?

A The company I work for is a publicly-traded company. We do have Sarbanes Oxley (SOX) compliance, and we do have a PCI environment, but it's very small, isolated and segregated. So, we were able to, when that was built, provide all the PCI requirements around that. But, no, this was a much larger task, not just regulations or compliance driving us to move forward and better the environment.

Q Can you walk us through the process you followed to find and look for solutions that would work?

A We ran a couple of proof of concepts. We had a good idea who the market leaders were in the space and were very impressed with what we'd seen from Rapid7, not only from a product perspective, but the partnership that Rapid7, how they engage their customers. We really feel that we're not just getting a product, but when there's something that we need, something that's important to us, that the Rapid7 team listens and is able to assist us. Beyond that, their support has been phenomenal.

Q When you set out to look at vulnerability assessment management products, what were some of the critical evaluation criteria you were looking for in the products?

A We wanted something that was, first and foremost, low operational impact – where it was not going to be cumbersome for the security team or infrastructure team to manage – where it was up, and it runs. We can't spend a lot of time managing the application itself. We were also looking for something that the security team wouldn't necessarily own and operate all by itself, something that could be set up, deliver reports into different people's mailboxes; a portal that they could log into, run scans themselves once they were trained up on the application. We wanted different people, different areas of operational responsibility to be able to see what's important to them, whether it's country specific, network specific, regionally specific or even type-of-device specific. Our network team can see our network equipment as opposed to our Intel/Windows team who can see the servers and desktops.

Q **So, ease of use and operationalizing was important. On the technical constraints side, did you have to look at how much traffic would be put on the network or how many scanners would be required and where they could go?**

A We did look at architecture of the vulnerability management configuration. What Rapid7 offers are remote scanners that report back to a console, reducing bandwith requirements and business impact. That was something that we invested in as part of our primary investment. So, we had chosen to install some vulnerability scanners around the globe and have a single console on our corporate data center.

Q **Did you do bake-off of multiple products, or did you do more of an RFP paper evaluation process?**

A More of a bake-off. We had reviewed what was available in the marketplace: Tenable Nessus, Tenable SecurityCenter, Qualys and Outpost24. We picked a couple of products that we felt would fit our environment and that were considered market leaders. We'd brought them in for proof of concepts for a short period of time. We had also sought advice from some security advisors that we use.

I would say within 12 months of deployment of the product, we had seen between 65 and 75 percent reduction in vulnerabilities.

Q **So, obviously, you chose Rapid7. You mentioned the support and the operationalization. Any other factors that they stood on that led you to choose Rapid7?**

A Yes. The community forum area. It's probably a heavily underutilized offering where people can exchange information about Nexpose or other products from Rapid7. In that forum area, we found a report that someone had built and essentially opened up to the community that provided letter grades. We were trying to see how we can provide meaningful metrics not only to our staff, but to our senior management, our Board of Directors, trying to provide information to them on how well are we doing, and letter grades seemed to be the easiest way. But, most products out there will only provide counts of vulnerabilities and some risk levels, which seemingly are arbitrary numbers. It's hard to get a feeling when you see a score of 100 million or 100,000. We were looking for something that was a little more basic, and this report really provided that. And while the grade itself may be arbitrary, this was really the line in the sand that helped drive engagement in our company. When we had seen one region who was graded as a C or a D and other regions were graded as A's and B's, there seemed to be a lot more engagement and focus on the areas that we're not patching as well who had high counts of vulnerabilities. This was an easy discussion to have with our Board of Directors, with our senior management and our CIO; something that could easily be grasped, questions could be asked: what isn't getting done and why not, and it resulted in a lot of action. We had seen a great reduction in vulnerabilities in the first six months, over 50 percent. I would say within 12 months of deployment of the product, we had seen between 65 and 75 percent reduction in vulnerabilities.

Q **Can you give us an idea of the scope – a rough number of scanners, a rough number of endpoints being scanned?**

A About 12,000 endpoints around the globe. We have 15 scanners globally to accommodate our scanning schedule.

Q **Are you doing any scanning of cloud-side services or virtual environments, or is it all physical devices?**

A No, virtual environments. Physical environments, really anything that is IPV4 addressable on our network gets scanned. That includes any devices that remotely access our environment. We aren't doing anything today with any third-party-based cloud services. We are using it in our PCI environment, our hosted environments internally. We are reviewing the cloud scanning service, as we would prefer to use this on our public IP space.

Q **You said you're at roughly 12,000 endpoints. So, when you made the decision to get Rapid7 product in, how long did it take you to get up to the full capability you're at now?**

A I think this is very interesting and something that should be a great story about Rapid7 and the Nexpose product. When we looked at this, we talked to other companies about deployment time. We were hearing, realistically, for a full global deployment, of six to nine months. From purchase to full deployment, full global deployment for our Company, we had done it under three months. We were very surprised and very excited to be able to get it up so fast, and a lot of that had to do with the virtual scanner offering. So, we were able to send scanners to other sites via file transfer, stand them up pretty quickly, and connect them into the console. We had worked with Rapid7 to help configure the environment, and that's not to say that additional tuning and updates haven't happened since, but we were able to get full visibility inside of three months.

From purchase to full deployment, full global deployment for our Company, we had done it under three months.

Q You mentioned using fifteen scanners. Are those all virtual scanners, or is it some mix?

A All virtual.

Q You started regular vulnerability scanning. Do you scan everything, how frequently do you scan, and how does that work?

A We do scan everything. A lot of the focus in the maturing of the program has to do with visibility. So, some focus has been spent on when we can not log into a device, why we cannot. Is this something that we should have credentials for? So, trying to identify those and remediate the things that we cannot identify. So, it really provides the visibility into what the vulnerabilities are on systems that we can't see today. So, there are a lot of improvements along the way and maturing that aspect of the program.

Q For production systems, do you have scan windows where you can scan them or no scan times where you can't – how do you handle that?

A We had initially been scanning everything around the globe about once every two weeks. We have since moved those up to weekly, and in some areas, we're even doing daily scans. Those are sites that are changing drastically, maybe acquisitions or whatever the case, where we're trying to improve the security posture day in and day out and trying to improve those sites. But, we really settled on once a week for about 98 percent of our installed addressable network spaces. We do not differentiate if it's a shop floor type network or a printer or a workstation space. We are always trying to get full visibility.That's how we sold this program. We don't want to turn a blind eye toward any part of our network. This is a real true vulnerability view of how our network is at a given point in time. So, we want as much information as we can get about every single asset that we have the ability to scan.

We were looking to put good actionable intelligence in the hands of our operations teams where they could get these reports and say, "this is a list of things for me to do in order to make an impact."

Q Once you start doing the scanning, how do you find the quality of the results from a false negative/false positive kind of rating?

A Very good. We've had a very small number of false positives along the way. Many of those had to do with systems that could not be logged in to. But, once we had the correct credentials installed on those remote systems, we were able to fully see things. So, it may amount to "this system looks like a Windows XP machine with no vulnerabilities in it," but when we really look into it, it might be an industrial control system. We've probably had also a handful of false positives on the patches themselves or the vulnerabilities themselves. So, Nexpose might say that there is a vulnerability on a certain system when it was a patch that was superseded by another patch. But, again, those have been few and far between. We've been very happy with the results.

Q How about the quality of the information that comes along with the vulnerability as far as aiding in remediation or aiding the operations side into saying, "I understand what the problem is and we can figure out how to fix it?" How's the quality of the information that comes along?

A Very good. There are two key reports that we look at that are delivered to the bulk of our infrastructure and operational teams. Those reports are the top 25 remediation report, which show if you were able to patch these top 25 vulnerabilities – it would have this much impact on this many assets in your network. So, it really takes prioritization and provides that to the teams that are responsible in these areas. And then, the other result is in the other assets, and that is the top 10 most vulnerable systems or assets. And again, that can be done by site. So, it can be done by region, by country, by network. We may have a person who's responsible for a specific network or location or region, and this gives them or their teams the prioritization that they need to make a significant impact in vulnerabilities.

Q How do you get the information from Nexpose over to the infrastructure and operations team? Are you integrating with a trouble ticket system? Are you providing them reports, and how does that work?

A We do two things. Nexpose itself has the ability to generate reports. We do these post scan. So, once the scan is completed or weekly scan has been completed, weekly reports go out to these teams: Here's your new priorities for the week, and they can go and execute. It may be a Top 25 report saying "Chrome and Adobe Flash need to be updated." This gives them some prioritization. Once a week, we provide a scoring that goes up to our management that shows how well the teams are executing on their patch management process, how they're able to execute and reduce risk with our vulnerability management program.

Q Those people who actually do the patching, they're getting those reports, or is the scan output feeding into their trouble ticket system?

A They're actually getting the reports via email. We have not integrated with any ticketing system, so they get these reports directly. They understand what they're doing with them, easy to read, easy to execute. And again, we were looking to put good actionable intelligence in the hands of our operations teams where they could get these reports and say, "this is a list of things for me to do in order to make an impact."

Q Last operational question, especially since you said you do it on the shop floor – one fear everybody has when they start to do any vulnerability scanning is are they going to knock over any servers, i.e. self-inflicted wounds. Did you run into any problems there?

A None directly. I would say that we, like any operationally sensitive team, are going to tread lightly. This isn't something that you're going to turn the key on and just let it run its course. You're going to want to initially schedule these things for, perhaps, late at night or off-production hours to limit the health and safety issues that go along with shop floor networks. There are very few systems that are fragile enough we have chosen not to scan, but that is the rare exception.

Q How long have you been operational now?

A A little over two years.

Q Knowing what you know now after running for two years, are there some things you would have done differently in the beginning or lessons learned you can pass on to people?

A This is one of the few programs that we designed, built, implemented, and executed very well. I would say a very small number of things we would do differently. I believe this is a key cornerstone of our security program. I think getting the operations teams involved, setting expectations that this is something that they need to do, providing them with actionable intelligence, being able to get high-level meaningful metrics, not only to the operational teams but management. This product really fit for everything that we were trying to do.

Q For the fifteen scanners you're using and the scale you're doing, do you have any idea what sort of staffing it takes to do that? Is it an FTE, a part of an FTE, how does that work?

A For us, it's been part of an FTE, and minimal dedicated staffing was definitely one of our requirements. I mentioned we didn't want to spend a lot of time managing this. There are other security products we have that other companies have where it takes a DBA to administer a database. It takes some infrastructure folks or server folks time to manage the operating system or the systems themselves. This has really been a hands-off product for us, which is a win/win. We may spend two to four hours a week doing management of the Nexpose platform and all the underlying architecture, but it's largely been hands off, which is very important for my team, which is very busy doing other things. We would rather be trying to investigate security incidents or trying to improve the overall security and not trying to spend time keeping our scanners and vulnerability management console up and available.

This has really been a hands-off product for us, which is a win/win.

Q Any future requests or requirements you've asked Rapid7 you'd like to see added to the product?

A Yes. I would say there've been several down the road, and this is where that great partnership that we really feel we have with Rapid7. We feel that we're tied very closely into the product management team, that when we have either ideas or problems or things that we would like to see that may be specific to our environment or may be something that would be beneficial to other customers, as well, they're always willing to listen and put that on the to-do list. Other companies that I've worked with would allow you to submit feature requests, but Rapid7 does a fantastic job of really taking these, looking at them and rolling them into their product. We've seen great advances in both functionality and performance in the feature set because of the partnership that Rapid7 has with its customers.

We've seen great advances in both functionality and performance in the feature set because of the partnership that Rapid7 has with its customers.

Q Since you are in the manufacturing side, were there SCADA devices and industrial control systems/ process control-type of endpoints that you needed them to add or that you found in there that you were surprised that they actually covered?

A Yes. There were things in there that we have seen in our asset listing that we were surprised that they had a fingerprint for. Additionally, there were other things that came up that we knew what they were that weren't in there that we've been able to contact the team and get them added.

BOTTOM LINE

A Global security manager used Rapid7's Nexpose product to move to weekly and daily vulnerability scanning which enabled more rapid mitigation, reducing overall risk. The use of virtual scanners eased deployment and the user interface enabled direct use by operations groups, reducing the security staffing time required.