Consolidating Vulnerability Management (with Jeff Gouge)

[00:00:00]

[00:00:10] **G Mark:** Hello and welcome to another episode of CISO Tradecraft, the podcast to provide you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy and today we're going to talk about risk-based vulnerability management. Now, as always, please make sure you're following us on LinkedIn as we provide real useful updates during the week and let your fellow security professionals know about us as well.

[00:00:32] **G Mark:** Thought I'd share with you something I found very interesting. One of my close friends is a world class ciso. He often sits on hiring panels for security professionals in his company, and he uses the same question to ask us applicants. It's one of the best hiring questions I've seen for cybersecurity professionals.

[00:00:49] **G Mark:** Imagine a new intern joins a development team. The intern is tasked with building a job, a web application that runs on Red Hat. The intern comes to you for advice and says, what do I need to do [00:01:00] to ensure my java web application is secure? What advice do you give him on how to make a secure Java Web application?

[00:01:08] **G Mark:** Now, this simple question seems to perplex security professionals, yet it shouldn't be hard to answer. The question really separates IT Professionals from those who've only gotten certification smart from ones that can give helpful advice to developers. See, developers want to detailed how to guide to follow.

[00:01:25] **G Mark:** They don't want to hear vague fluff about protecting the confidentiality, integrity, and availability of the system. Now, if you ever built a web server from scratch, you know that you'd need to install a fair amount of software to make everything. First, you need an operating system such as Red Hat or Ubuntu.

[00:01:40] **G Mark:** Then you'd need to install a Java runtime environment for Java, such as open jdk. Since most operating systems won't have an interpreter to run Java code Runtime java environments include a virtual machine, a Java class library, and a Java compiler that allows developers to run custom Java code. And once you can run Java code, we then need to install an [00:02:00] application server such as Apache Tomcat or nginx or node js.

[00:02:03] **G Mark:** And this allows you to host and implement servers and web sockets to handle remote connections. Now that users are connecting to your application, you need to add a web application framework such as Spring or Apache struts. Then you're going to need to install custom libraries for your Java web application.

[00:02:20] **G Mark:** For example, most Java web applications install jdbc, which is a Java database connector. And after you install all of this software, you finally get the opportunity to put in the custom Java source code at your organization. Okay, you're probably asking why did I just give you all kinds of technical detail about building a Java, web application that runs on Linux?

[00:02:42] **G Mark:** The answer is you need to understand there are multiple layers of software to build a Java web application, and these layers mean that no one single security tool can perform a security assessment. If you want to build a secure web application, you must ensure three different things routinely occur.

[00:02:59] **G Mark:** Number [00:03:00] one, software at every layer is patched and free from known CVEs. Number two, all software is checked against a standard or benchmark to ensure correct configuration. Now, note that most organizations use the CIS benchmarks or DISA stakes. And number three, if you want to find vulnerabilities in your custom code, then you need to perform custom code scans for common vulnerabilities like cross site scripting, url traversal attacks, and SQL injection.

[00:03:27] **G Mark:** Looking at our question of securing a Java web application, you'll generally observe that organizations assess a Java web application with at least four different tools. First, you need to make sure the operating system, runtime environment, and middleware all patched and configured correctly. So you'll leverage a vulnerability management tool like Nessus Rapid 7, or Qualys these tools find common vulnerabilities in your operating system.

[00:03:52] **G Mark:** And indicate whether you need to patch to the next version of software or change a TLS setting to be more secure. Next, you'd realize that [00:04:00] those tools don't actually scan the Java Web frameworks. Therefore, you need a second tool that is known as a software composition analysis or SCA tool. Examples include Snyk, Black Duck, or GitHub depend bot, which.

[00:04:13] **G Mark:** Scan for vulnerable versions of Apache struts. Remember, that's what got Equifax and vulnerability management and SCA tools. Don't know how to scan your organization's custom Java code, so you need a static application security testing or SAST tool like Fortify, Coverity, Vericode or GitHub code QL to analyze your custom code.

[00:04:34] **G Mark:** Now, most organizations also run a dynamic application security testing or DAST tool on web applications such as Web inspect or Detectify, OWASP Zap or Burp Suite to find vulnerabilities the way attackers do on a website. And these four classes of tools vulnerability management, SCA, SAST, and DAST will likely each have different findings.

[00:04:57] **G Mark:** There may even be some overlap where both the [00:05:00] vulnerability management tool and the SCA tool say you need to patch the same operating system packages. So now that you know you have at least four security tools providing recommendations to the developer, is that the only thing a developer has to look at?

[00:05:14] **G Mark:** And the sad answer is no. If a developer puts passwords, encryption keys, or other credentials into their code, that can also cause a security issue. So we need to add in another security scanning tool known as secret scanning tool. If the developer uses technology such as IoT devices, containers, Terraform scripts, or kubernetes, then you need to add additional security scanning tools that can assess the relevant technology. The end result is that there are usually at least six different security scanning tools in most large organizations. If you want to find as many vulnerabilities as you can. Now, let's say you want the developer to implement all the security scan recommendations from the various tools, you can expect the developers to ask how should I prioritize remediating the findings?[00:06:00]

[00:06:00] **G Mark:** Essently. The developers want to know how to rank each vulnerability finding according to risk. And since every tool can have a different finding, there needs to be a common vulnerability scoring system and the first major scoring system to emerge across the industry. And really the dominant one still, it's a common vulnerability scoring system, or CVSS and CVSS uses a 0 to 10 scoring system where none is a score of 0.

[00:06:26] **G Mark:** Low is up to 3.9. Medium is from 4 to 6.9. High is seven to 8.9, and critical is nine to 10.0. Now the best way to think about CVSS is think of a quote from Sun Tzu. If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat.

[00:06:54] **G Mark:** And if you neither the enemy nor yourself, you will succumb in every battle. [00:07:00] To know the enemy, you need to understand the likelihood of a vulnerability being leveraged in an attack. CVSS asks security teams answer a few questions to select a base score the attack vector. Does the attacker need network, local or physical access to perform the attack?

[00:07:15] **G Mark:** If you think about it, physical access is a much lower risk than network attack. Therefore you get a higher score for network versus physical access attack complexity. The second component, its metric defines the conditions beyond the attacker's control that must exist to exploit the vulnerability. You can think of this as how likely is a configuration setting to be wrong in the attacker's ability to find it.

[00:07:40] **G Mark:** If the complexity is high, it requires a great deal of skill to find it. If the complexity is quite low, it's more likely to be found and therefore higher risk. Starting to see how these combined together as a score. Privilege is required. Does the attacker already need to be a user on the system or an admin to perform the attack?

[00:07:59] **G Mark:** Or could the attack be [00:08:00] done at a higher risk with no privileges whatsoever? How about for scope? If you exploit this piece of software, does that software have run with permissions that allow it to attack other applications or even other systems? If you can change scope, if you can use this to get into something else, it's a higher risk.

[00:08:18] **G Mark:** Then the impact metrics, does it have the ability to impact confidentiality, integrity, and availability of your software or of your system? Now, if you just use the BASE CVSS score, you'll see that they only communicate the technical severity. Not the actual risk. So CVSS scoring can be problematic and it gets worse because 50 to 60% of all vulnerabilities are high severity according to the CVSS scores and of the CVSS high severity scores.

[00:08:47] **G Mark:** Roughly 75% of them are never exploited. So this means if you have a cybersecurity policy or directive that says we patch all higher critical vulnerabilities in less than 30 days, and 75% of your [00:09:00] patching is lightly wasted effort, which harms revenues to the company and also detracts you from doing other activities that perhaps might give you a better yield.

[00:09:09] **G Mark:** So we're seeing a shift to switch away from CVSS to vulnerability management, which levers vulnerability intelligence data. Here are the three important questions vulnerability intelligence data can assist with. The first question is, do you know which vulnerabilities are being actively exploited by various nation state actors or ransomware operators and malware groups?

[00:09:30] **G Mark:** If not, then you should really start with a cisa known exploited vulnerabilities catalog, vulnerability intelligence feeds and exploited sites in marketplace. Now, if you haven't checked out the CISA known Exploited Vulnerabilities catalog, please take some time to look. It's an awesome free resource where you can receive alerts on vulnerabilities that are actively exploited, and there's a link to it in our show notes.

[00:09:54] **G Mark:** The second question is, do you know which vulnerabilities are being exploited in targeted attacks against your [00:10:00] organization or industry? If not, you should really be paying attention to your IDS, sensors, and Honey Pots Endpoint monitoring and incident Response. And the third and final question is, do you know which vulnerabilities will be exploited soon?

[00:10:15] **G Mark:** Monitoring the dark web hacker forums and social chatter can be a great way to see actor interest and code availability as vulnerabilities are proof built into proof of concept code. But another key area to look at is EPSS. EPSS is the exploit prediction scoring system. Which focuses on coverage of a vulnerability across the internet and effectiveness of an exploit.

[00:10:37] **G Mark:** So in executive terms, you can look up a CVE and get a score, which has shown as a percentage. For example, CVE 2021-40438, an Apache Server vulnerability. Returns an EPSS score of 0.97, which means there's a 97% chance of the CVE becoming weaponized or exploited in the near future if it hasn't happened already.

[00:10:57] **G Mark:** These are excellent threat predictions which you can [00:11:00] use to better prioritize patching on where the bad actors focus their exploitation development efforts versus CVEs that never become weaponized. Now another key thing you really want to look at, in addition to threat intelligence data, is your configuration management database system.

[00:11:15] **G Mark:** Essentially, most organizations have information about each application in their enterprise. This system needs to identify the attributes of applications which are critical to the business. Critical applications are also referred to as crown jewels because the embarrassment of a country losing its prize possession is like unto a company's critical applications being exploited.

[00:11:35] **G Mark:** Critical applications can usually be defined as applications, meaning one or more of the following criteria. The applications have a lot of exposure, so for example, the customer web portal that all customers use. The applications contain valuable or sensitive data. For example, a core banking database, which contains customer account information and the applications host mission critical [00:12:00] services.

[00:12:00] **G Mark:** For example, GitHub and Jenkins are usually internal applications that don't contain customer data, but they play a critical role to deploy and restore important applications. Okay, so now that we know about six security scanning, CVSS scores, threat intelligence informed vulnerability management, and how to define critical applications or crown jewels.

[00:12:21] **G Mark:** We should know that there are tools in the marketplace that consolidate all of this information into a central repository, which can provide risk triage for our developers. This category of tool is generally known as risk based vulnerability management software. And today I've got a special guest who can give us a lot more information on this, so let's find out.

[00:12:46] **G Mark:** Today we're bringing on an expert that can tell us more about risk based vulnerability management software. Jeff Gouge is a CISO at Nucleus Security. And can you tell us a little bit about yourself?

[00:12:58] **Jeff Gouge:** You bet G Mark. Thank you first for having [00:13:00] me on today. I really appreciate the opportunity. So I'm Jeff go here at cisso at Nucleus Security. I am one of the first eight people, new employees at Nucleus Security. We 're a newer company started in 2018 but one of the first few to help join the company.

[00:13:16] **Jeff Gouge:** My career itself goes back not very long. I would consider myself still a newbie starting back in 2008. Started in very many different fields. I've worked my way through software development, support, qa, and then eventually worked my way into database and server administration before starting my cybersecurity career in 2013.

[00:13:37] **Jeff Gouge:** And then really focusing on that ever since. So through those times I've worked in a few different fields, working in the private sector, working in the public sector, state public sector, which is always fun with new challenges and worked my way up from there. My career in cybersecurity started as an analyst.

[00:13:53] **Jeff Gouge:** I got to do the dirty work. I moved in the public sector. I've had the opportunity to work with a [00:14:00] few people. People were, it's a problem, right? And for me, the, what we had to do is we had to do more with less. So we started doing the, nitty gritty work, working with tools working my way up to cloud and working my way from there into it security with the many cybersecurity domains that are out there, right?

[00:14:19] **Jeff Gouge:** And so that's a little bit about my career personal life, family guy, three kids living outta sunny Florida and enjoying it here.

[00:14:28] **G Mark:** And that sounds pretty good. Yeah. It's interesting when you say you're in the first eight of the company, it usually means your employee, number eight. You don't, if you're like the third employee and say I'm in the top 12 and things like that, but it sounds like you've done quite a bit of cybersecurity.

[00:14:40] **G Mark:** Even in the time from you've been involved in your career and the accomplishments that you've made and what I've heard about in prior conversation. Really impressive. Now. What do you wish all CISOs knew about this type of cybersecurity product space? When we're talking about risk based vulnerability management software?

[00:14:57] **Jeff Gouge:** Yeah, great question. Great question there. There's a lot of things, because [00:15:00] for me, when I first heard about it, I was like, what is this? What is this? What? What are the benefits here? So there's a few things that come to mind, when defining risk based vulnerability management. We have asset scanners.

[00:15:12] **Jeff Gouge:** Maybe your team has a web application scanner, maybe they have a code scanning tool. Do you have assets in the cloud? Are you scanning those? Are you using cloud scanner tools? Now what, right? If I have a critical vulnerability in each of these tools each week, which one is the most important in my career? I'd have to go to each one of those scanner tools.

[00:15:32] **Jeff Gouge:** I'd have to use this wonderful tool called Excel, which is critical for all businesses, right? That's a problem. So what do we do to fix each one of them? Now? Can one of them just be monitored until we get to. Enter risk based vulnerability management. The goal of these software solutions is to bring together vulnerabilities, assets, and threat intelligence into one relational system that allows you to automate, notify, and report on your [00:16:00] VM program. Like I mentioned before, get your business outta spreadsheets. Get 'em into a software system, right? This could be something that you thought of when you're in the security industry, and the first thing that came to mind was let's just put it in some type of database, and that way we could just throw it all together.

[00:16:14] **Jeff Gouge:** Guess what? That's hard. There's a reason this software space exists. Ingest your data from all your scanners, not only scanners. Go into your asset tools. We talked about that triad. Asset tools have their own problems and their own limited capabilities. Bring all that in. Threat intelligence, same thing.

[00:16:33] **Jeff Gouge:** It's a newer space. When I first started, it was a brand new thing. It was, and we'll talk, for me that's something that I think about is ah, threat intelligence. That's something that, everybody, you can just ignore that You can just detect things. Now things have gotten, security.

[00:16:47] **Jeff Gouge:** Has it stopped growing? No. Security vulnerabilities. Keep growing. Slice and dice the data the way you want. Another topic that I think is key is I think we need to I think we need to score and prioritize each vulnerability for the first time in a long time. [00:17:00] Phishing is no longer the top attack vector in IT security.

[00:17:03] **Jeff Gouge:** It's now vulnerability exploitation. Why spend all these hours of manpower trying to patch the latest CVSS bug of eight or more when there's no exploit or nothing on the horizon about that actually being a problem with your company? Our assets are classified by business priority, and that should affect the priority of a patch.

[00:17:22] **Jeff Gouge:** It's time to use all of this data to implement automated decision trees and score with something like SSVC, which is a newer term stakeholder specific vulnerability categorization. Using a risk-based vulnerability management software allows a company to prioritize risk based on their own decision trees.

[00:17:38] **G Mark:** So you've laid out this triad of vulnerabilities and assets and threat intelligence, and we look at it from a perspective instead of saying, yeah, just assets, rank order them in terms of the business priority, which makes for a lot of sense when you think about it, you don't gain a lot of points in the long run.

[00:17:54] **G Mark:** Guarding the trash can. And it, it tells a disconnect between the cybersecurity function and the [00:18:00] CISO or the cybersecurity leader when they come back and they report that they've done all this great work and they've protected certain assets that quite honestly aren't barely key to the business. And sometimes organizations figure that out the hard way when they realize that yeah, the crown jewels weren't protected correctly, and things such as that.

[00:18:16] **G Mark:** Now, When you think about patching and vulnerability management, how should cyber executives think about that and what trade offs do they need to make when you're thinking about this vulnerability, asset threat, Intel triad as we go through and say, Hey, we gotta keep this thing up to going. And of course, I think everybody knows the difference between vulnerability management and vulnerability discovery, as well as vulnerability discovery.

[00:18:42] **G Mark:** It's a whole world out. Let's just focus right now about what CISA should really know about the patching and vulnerability management.

[00:18:49] **Jeff Gouge:** Yeah, sure thing. This always to me comes down to manpower and priorities. Just like the SANS top 20 critical security controls, you should always start with inventory. You mentioned this already, right? [00:19:00] Are you gathering vulnerabilities from all of your assets and asset types? If not, to me, start there.

[00:19:07] **Jeff Gouge:** Start filling those gaps. Patching is always going to be a manpower problem. I mentioned before, I worked in the public sector. The one or two people we had was the same budget we had year after year. It didn't matter how many vulnerabilities were coming. That same problem exists in the private sector, right?

[00:19:22] **Jeff Gouge:** There's always going to be more and more coming. You have to do more with less. So start with making sure you're you make your decisions on what you can patch how quickly you can patch them, and making sure that those are efficient decisions.

[00:19:34] **G Mark:** Now, by the way the SAN'S top 20 not to try to correct anything. It's now the CIS critical controls. There's only 18 of them. Cause I remember when I was at SANS, I said, Sans we're thinking like we gotta get the top 20 outta there because there's talk about changing that number and the latest version has 18.

[00:19:52] **G Mark:** That number could change from time to time. But you're absolutely right, though it represents a standard of excellence. That everybody should know and that we should monitor. Now, we did talk a little bit [00:20:00] earlier that organizations that only focus on CVSS base scores are really spending time maybe patching the wrong things.

[00:20:06] **G Mark:** Now, how big of a problem is this and how could this problem actually go away with risk based scoring systems?

[00:20:12] **Jeff Gouge:** Yeah, great. Great question. It's a big problem in my opinion, to start. CVSS scores, communicate technical severity, not risk. So take some tip, simple statistics from Mandiant and Tenable. For example. 50 to 60% of vulnerabilities are high severity according to CVSS. 75% of those CVSS high risk vulnerabilities are never exploited.

[00:20:37] **Jeff Gouge:** Think about all the wasted manpower that you could be having. If you have compliance that says every high vulnerability that you have to patch within 30 days. That's a lot of wasted manpower. But our SLAs are VM plans and our compliant commitments say we have to patch them, right? So we have this struggle.

[00:20:55] **Jeff Gouge:** As I mentioned before, SSVC decision trees help prioritize [00:21:00] fixing what matters most using a tool like Nucleus or another in this risk based vulnerability management space. You can automate those decision trees by combining your asset data with your vulnerability intelligence and enrichment data that allows you to aggregate, normalize, and remediate your vulnerability management data.

[00:21:16] **G Mark:** That's good to know. Now, when you're looking at various products in this space, I know there's a variety of things that companies are going to look for. For example, what application security scanning vendor would products like your support? And I've also seen organizations ensure the tool can create tickets in things like a Jira or a ServiceNow.

[00:21:33] **G Mark:** Now, what other features do you see CISO commonly asking for during these vendor bakeoffs of risk based vulnerability management software?

[00:21:41] **Jeff Gouge:** Everybody has their own tool they use. It's so true and it's impressive to see the lists of requests that come in. For new features and new scanners, new asset tools, new ticketing tools. There are more and more open source tools used every day, and thus the requests never stop. But for [00:22:00] us, that comes with the balancing act because what in this space, what are we trying to do?

[00:22:03] **Jeff Gouge:** We're trying to integrate with those and what comes with integration, loads of support. So yeah these never stop. So the request for those come in right from the triad. You mentioned ticketing. Those come in all the time too. The thing about ticketing systems is typically the ones most commonly used are cloud systems.

[00:22:20] **Jeff Gouge:** And just like us as a SaaS tool, what do they do? Literally weekly in agile development, they change. And with that change that makes integration hard. The other request we get very often is talking about teams and department type support. People want to classify risk and they want to put risk and assign it to different areas of the business so that they can start tracking that based on department or based on, who is actually responsible.

[00:22:46] **Jeff Gouge:** For that area of the business that can help really drive that risk down. That's another one of the features that get asked very common in this industry, but the features never stopped and they always come in. There's always something new that you didn't know that [00:23:00] you didn't think of before, or what happens a whole lot is.

[00:23:04] **Jeff Gouge:** Just like the problem with development is, you develop this beautiful horse based on those requirements. People use these tools differently throughout the year. One customer could be using tool A and another customer could be using that same tool a, but using it in a completely different way which creates a challenge.

[00:23:21] **Jeff Gouge:** Ticketing. That's something I, I find very interesting, right? For me I learned the hard way when I first started vm, way back not way back when, but a few years back, right? And when I first started vm I was like, you know what? We should just ticket everything. Talk about a nightmare and creating a needle in the haystack.

[00:23:35] **Jeff Gouge:** You want your ticketing tools to go nuts, turn on ticketing for vulnerabilities and see what happens, right? If you don't have, if you just use CVSS, for example, It's a nightmare. So ticketing is a great thing usually for more mature companies that they want to get to signing that out and working on it.

[00:23:51] **Jeff Gouge:** But that's something that I think everybody wants to get to, right? That's part of the maturity process.

[00:23:55] **G Mark:** I just want an API that works with Excel and I'd be fine.

[00:23:59] **Jeff Gouge:** You know [00:24:00] what, one of the key features we have and most companies are going to have in this space is that export button. I want to filter it on the different ways. Filtering is a big thing. It's obviously dashboards that always comes to, but I also want that beautiful button that says Export to Excel.

[00:24:14] **G Mark:** Got it. Hey, CSV is never going to go away. Hey, so earlier we highlighted knowing about our vulnerabilities are key, but it's just, it's important to know what vulnerabilities the attackers are actually using. To attack companies. And as you would point out, 50 to 60% of the vulnerabilities that are scored that way in CVSS three quarters of them never get exploited.

[00:24:33] **G Mark:** And so in a way, it's wasted time, wasted effort. As you say, you're going to light up your ticketing system if you were to do that. Now can you talk a little bit more about how threat intelligence is changing the game on the risk-based vulnerability management software?

[00:24:46] **Jeff Gouge:** You bet. Yeah. Back when I first started in it, threat intelligence feeds first started getting some buzz. I used to roll my eyes If you were doing the right things and having to focus on detection, you know what, to me, what benefit did threat intelligence have? Our detection [00:25:00] mechanisms would pick up on those issues before threat intelligence even had it in the feed.

[00:25:03] **Jeff Gouge:** So well, things have changed a lot since then. The sheer number of vulnerabilities reported and released each year continues to rise. Many of us are faced with having to combat growing threats and the same resources we had for the last few years. This is where threat intelligence really comes to light.

[00:25:17] **Jeff Gouge:** As we discussed before, focus on what is important to improve efficiency. Risk-based vulnerability management software helps CISOs define severity. SLAs, we haven't talked about that a lot. Reporting typically threat intelligence tools are another expense. So another thing to keep in mind here, check what your risk vulnerability management software company can support.

[00:25:40] **Jeff Gouge:** Which ones they have built in, because that could be a potential savings if you're, paying for another one in the space. But all of a sudden this space could include that tool with it, a two for one.

[00:25:50] **G Mark:** Well, That makes a lot of sense now. Now, one of the things I know that CISOs get excited about is pretty dashboards, and we're talking about maybe exporting stuff to excel, but you [00:26:00] can't really export a dashboard to Excel. You can get a single panel, but not a whole bunch of 'em. So what metrics do you see these tools showing that CISOs might share with the other executives within the company?

[00:26:11] **Jeff Gouge:** Dashboard's so hot right now, right? So hot. But but by fully leveraging a vulnerability software solution that can integrate with each of your scanner and asset tools. You can get a clear picture of the top risk in your org. I try to avoid, because I used to roll my eyes too about when startups would say the single pane of glass, right?

[00:26:28] **Jeff Gouge:** But everybody has to have that single pane of glass. Not only will it show you the big numbers that can scare others, not insecurity like critical. And high vulnerabilities. The totals of those. It could also show you things like uniques of the, each of those vulnerabilities scenarios. You also get things like enrich data where that you can drill down into.

[00:26:49] **Jeff Gouge:** That's the other thing. Dashboards typically and some tools are just, that's it. They're a dashboard and you get, see the number. This space allows these software solutions, the real power of [00:27:00] this is that power to drill down, filter, move down. How many of those are rated as zero days? How many of those are being exploited in the wild?

[00:27:10] **Jeff Gouge:** Does malware exploits exist for those? Do your active vulnerabilities have a critical risk rated by a vulnerability, a threat intelligence as well, right? So not only does your scoring system and your vulnerability enrichment data say that it's important, but has an analyst actually looked at this and go, you know what?

[00:27:26] **Jeff Gouge:** This is bad. We're actively seeing this exploited in the wild today with these dashboards, you can get that quick snapshot, single pane of glass into not only what you have wrong, but also what you're remediating and have fixed. Trend lines and reports over time, show progress and you and how long your teams are taking to move on some of these vulnerabilities.

[00:27:46] **Jeff Gouge:** And I think that's something key here too. A lot of VM programs and scanner tools really don't talk about remediation and your trends over time. What are you doing right? They focus on, the next bad thing and let's keep fixing the next bad thing. So I think that's [00:28:00] important.

[00:28:00] **G Mark:** Well, It's interesting you talk about the remediation, because of course that ultimately ends up the actions that we need to take. It. It doesn't help you to know, yeah, this is the reason we went bankrupt last Saturday at two 30 in the morning. That's not useful information. It's better to say, Hey, we blocked and stopped that.

[00:28:16] **G Mark:** So what goals or target objectives do you see CISOs and security leaders setting for an organization once they get this single pane of glass dashboard in place?

[00:28:26] **Jeff Gouge:** Yeah. One big goal that I always want to achieve, and this is the same not only for security, but other aspects is visibility and observability. One of the things that keep me up at night, What am I missing? What are the things that I don't know, those false negative, those, those things that are out there always shooting for, finding the needle in the haystack, right?

[00:28:47] **Jeff Gouge:** The only way we can get to finding those urgent or important issues in our organization is either by changing our priorities. or discovering what we can change to get better. Once you're there, I think automation and a learning are your best [00:29:00] friend to help you target those key issues and then monitor for the others so that you can start changing that cause the most constant In our industry.

[00:29:08] **G Mark:** That's true. And I guess if something gets flagged as you go through your threat intel and you prioritize a vulnerability a little bit lower than others because hey, it's not being actively exploited. You can't just forget about it though, right? Because it still could come back and bite you three months, six months, a year later.

[00:29:23] **G Mark:** In fact, we've seen some vulnerabilities that have literally been around over a decade before somebody finally figured it out

[00:29:31] **Jeff Gouge:** Yeah, that, and that's an interesting, that's an interesting point too. It's kinda like the definition of a zero day. Once it's a zero day, is it always a zero day? At what point does it fall off as a zero day? It's the same type of things. You want to keep these on your radar, but some of 'em very easily could fall off.

[00:29:46] **Jeff Gouge:** But you always want to keep those on that radar because you never know when that change could occur.

[00:29:50] **G Mark:** And then trying to keep track of that manually with an Excel spreadsheet. It's just not going to work. And guess there are all these CVSS scores that are out there that you could be inundated with them, but [00:30:00] it requires constant monitoring, a constant update of things in terms of the threat intel, and then matching that up.

[00:30:06] **G Mark:** And of course, The users need to know where their vulnerabilities are. And also, as you had said previously, what are your most critical assets? That becomes really important. Now, as you look at this entire product space, what are the most exciting things you start to see coming in the future?

[00:30:23] **Jeff Gouge:** Yeah that's a great question that some of the things I don't even think I can think of right now, but tools that can help you adapt right to this ever growing change in the changing landscape of security are critical, right? Tools that can help you, create automation based on your own rules.

[00:30:37] **Jeff Gouge:** So we don't want to, the software, we shouldn't define what you want to look for. We can help and we can recommend, and maybe that's something that, can drive your success, but something that would allow you to change on your, just like SSC talks about changing on your stakeholder specific type what you really care about is key, in my opinion.

[00:30:54] **Jeff Gouge:** Cause. Blind spots are always developed. Another thing that I find intriguing is the [00:31:00] ability to segregate and scale your company's data as it grows. That I mentioned that securities are constantly rising. You don't see 'em usually dropping. So that means these tools need to be able to keep up with that.

[00:31:09] **Jeff Gouge:** Do you want to see your organization's data in different silos? What about buckets? About there's how those teams grow, right? As your team grows as security. Can they begin to focus in different areas? Can you break those up? Instead of having one giant, monolithic project, for example, in your org, as your team grows and as your company grows, can you be able to split those up?

[00:31:29] **G Mark:** All right. That sounds, seems interesting. So that's what's coming. What's the hardest. To get right in the vulnerability management.

[00:31:38] **Jeff Gouge:** Keeping up and maintaining focus VM is a pain to focus on as the security team grows and expands. I think about my time back in the public sector, right? We had those same two people and we started with having no VM right when we first started the security team. So we started that up and then we, we moved to Endpoint and then we would move to firewalls and then the cloud.

[00:31:59] **Jeff Gouge:** [00:32:00] And we've all seen the, I, the cybersecurity domains thought, The areas, the domains of which they're in cybersecurity, and there are hundreds that you can dive into and each one of them have their sub expertises. When a firewall issue is causing an outage, it's very easy to lose focus on vm, right?

[00:32:16] **Jeff Gouge:** Those VM ones are still there. And if you didn't have all these things telling you what's important, then the person screaming in your ear that the website is. It's very important. So once you get back to your VM workflows, can you rely on those manual process that usually boil down to exporting to Excel, to send to a board?

[00:32:35] **Jeff Gouge:** With those older methods, it's hard for any engineer to maintain focus on the many sexy security tools that are released each and every week.

[00:32:43] **G Mark:** Yeah, and there's a lot out there. And so in many ways ever been to rsa, you just kinda get lost in the sea of all these vendors out there. And yet, instead of having products sold to you, it's important sometimes to buy that is to say you come up with your own criteria. And [00:33:00] one of the things that a lot of CISOs want to be able to do is show some quick wins to be able to demonstrate.

[00:33:05] **G Mark:** That the return on investment for a particular product or product category will occur fairly quickly, maybe six months, not six years or something like that, because there's probably better places for the organization to invest their money. Are there any quick wins that you can think of that you can do with this type of technology?

[00:33:22] **Jeff Gouge:** Yeah, you bet. And you mentioned this six months thing. A lot of these tools that you're buying are cloud software, so you're actually incentivized to try to make sure you have those six months wins, because when it comes to budget next year, why would you keep renewing a product that's not going to give you those wins in that time period?

[00:33:36] **Jeff Gouge:** So, Speaking from my experience that this type of tool helps keep your scanner. Risk based vulnerability management software help you confirm the integrity of your scan data coming from your scanner tools, right? Have you been seeing duplicates for a long time? Was your scanner tool not aware, right?

[00:33:52] **Jeff Gouge:** Of a change or maybe allowed right? Could be a security issue to your assets. And thus now have a gap in your scan coverage. This type [00:34:00] of software will give you clear metrics and data on scan coverage, right when you need to look into those gaps that you didn't even know you had. Many scanner tools rely on manual methods about, updating the scans.

[00:34:11] **Jeff Gouge:** So it's easy to make mistakes or miss something. Moving over to a tool with automation will allow you to see and alert on those gaps automatically so quickly, while reducing the risk, without having to rely upon manual methods and people. Another key goal that I see is change the way you classify severity, right?

[00:34:27] **Jeff Gouge:** Don't rely on just. CVSS to tell you what is critical. Cause if you can change the way severity is, then this can have that downstream effect that. Now, if you're classifying it differently than the ways that you need to, upon compliance could change. The SLAs that you keep your teams and business to could change, which would, lead to a better efficiency.

[00:34:47] **Jeff Gouge:** So change, change the game, right? Change the game on VM work and make sure that tool helps you change the game.

[00:34:53] **G Mark:** And you mentioned SLA, and so what improvements in SLA might we be able to see with the [00:35:00] ability to automate a lot of the stuff which previously had been either excelled or manual or hodgepodge together?

[00:35:06] **Jeff Gouge:** Yeah it, it's really making sure, if you can change the severity, then all of a sudden the things that aren't important. Or that are important, dwindle down, right? You can now maintain focus on those areas, right? So your efficiency gets better. So thus you can actually meet those SLAs without just having to either, put other POAMs in place or something like that to say that, we can't just, we cannot get to this sheer number of high things this month cause we have a 30 day SLA.

[00:35:34] **Jeff Gouge:** So by changing the game on how you're defining severity, you're improving your efficiency on, you know what, now I have three. And that's attainable, right? And I can knock those out. So it's not always necessarily changing your SLAs. This could, in fact lead to those changes, right? Your VM management plan should be something that you change every year.

[00:35:51] **Jeff Gouge:** It should be a living, breathing document. So if you have a tool like this, enter into your lap, and all of a sudden you can start working on these type of [00:36:00] issues, then all of a sudden, when it's time to review that VM management plan, that's going to lead to some changes in SLAs.

[00:36:07] **G Mark:** That's a good point. So it's actually going to allow us to do a better job at what we need to do because we've got more efficient information collection, categorization, organization. We can apply it where it needs to be applied. Because we're prioritizing effectively instead of just trying to have to guess where things might like to go.

[00:36:24] **G Mark:** Now, there's one other term you had mentioned almost in passing, and I thought I'd come back to it, the SSVC, which is not a typo by the way. It's not, but CVSS backwards, which is probably deliberate, but tell me a little bit about SSVC, because some people may not have heard about it.

[00:36:40] **Jeff Gouge:** Sure. It's something newer to me as well. It came out from a white paper, right? And now it's fast being adopted. But for me the big thing that this comes is it's stakeholder specific. So gmark, your priorities of your org may be very different from mine and for us. Why are we going to let others come in and tell us what we think is [00:37:00] important? So Sspc aims for that. It basically allows you to create decision trees, based on the asset classification exploits, vulnerability, intelligence, and really start whittling out the noise, right?

[00:37:13] **Jeff Gouge:** It allows you to make a decision tree based on is this being exploited in the wild? Yes or no? And now I can either act or I can, basically just ignore honestly or just mark, right? Basically put back there in the, back into the docket to, reprioritize if something changes.

[00:37:29] **Jeff Gouge:** But things that I can basically just monitor and put into monitoring mode. And that's really the game changing thing from that is that it's no longer. Man, another mountain and we got another, 400 high severity vulnerabilities that we somehow have to patch and get done. This is just going to lead to my POAM getting longer.

[00:37:45] **Jeff Gouge:** Now with SSVC, I'm able to, go and say, okay, new Month came in. Now applying this decision, tree Logic with automation, I easily have my few targeted things that I need to do right now and I can now report on.[00:38:00]

[00:38:01] **G Mark:** Got it. Okay. That's fascinating. So the stakeholder specific vulnerability, categorization, now that's something that right now people have to do themselves, or are there tools to help out with that? Or is that something that may, that's a feature it's coming next year to a product near you?

[00:38:16] **Jeff Gouge:** It's a feature. Yeah, no, it's a great feature. No we actually, so here, speaking personally at Nucleus, we just came out with a blog post specifically on this in ways that you can actually automate this directly into a tool in the risk based vulnerability management software category. So if the automation lives in that tool, We have the ability to take, because essentially what you're doing is you're breaking down metadata from your assets, metadata from your vulnerabilities and metadata, from your vulnerability intelligence feed to make those decisions, right?

[00:38:48] **Jeff Gouge:** So as long as the software can support those metadata and then use those metadata fields to help make decisions or change severity or change risk, then you can actually automate that and you can actually implement that today with the [00:39:00] same tool

[00:39:01] **G Mark:** Interesting. So it all does come together as well. That's pretty neat. Anything else you got on your mind? Anything else that you think you'd share? Words of wisdom or advice or things like that?

[00:39:10] **Jeff Gouge:** Yeah. Yeah, there's a few things. We are also in this space myself, right? I'm CISO for a company that's in this space and we eat our own dog food, right? So I use it myself. Anyone that may be having to keep up with this compliance or other compliance control should consider a tool in this space, right?

[00:39:26] **Jeff Gouge:** Instead of having to report on trends in each of your scanner tools consolidate that into one tool that will allow you to report and trend on all your assets and vulnerabilities. To me that's something. It was a game changer for me. It was one of the reasons I came to work for this company because I, it was something that I wanted myself in my last role.

[00:39:45] **Jeff Gouge:** Why not try to change that space and help others do that? Another thing that that comes to mind and that to me, this is just one of my personal things you'll notice on this CISO that smiles a lot. I know this is an audio podcast, but hopefully you can hear it through my voice. But last, but not least

[00:39:59] **Jeff Gouge:** keep up [00:40:00] the good work. It's easy to get lost in the backlog and constant stress and pain and challenges of security. Remember that your work is making a difference while stopping attackers daily.

Smile more often. Take that extra time to celebrate your wins. You're doing a great job

[00:40:17] **G Mark:** And that sound like a great way to kind of wrap up with a nice positive message. Jeff, thank you. It's been fascinating talking about risk based security, vulnerability management, and what it can really do and how looking at things such as vulnerabilities and assets and threat intelligence and ranking our assets in terms of business priority allows us to do a much better job of figuring out where should we apply our time, attention, and effort instead of just simply blind.

[00:40:40] **G Mark:** Blindly following CVSS scores, using some sort of scoring system that disregards whether or not this vulnerability A has ever been exploited, and usually B, if it's you in your enterprise, that's an easy filter. Okay? It's a Linux vulnerability. We're all running all windows. Okay? That part is easy. But you've mentioned that being able to [00:41:00] focus more on your own environment is really key and winnowing out the things that don't matter, because quite honestly, there's academic generated or academically generated vulnerabilities.

[00:41:11] **G Mark:** You'd say specifically this could take place, but. No one's bothered to do it. And in fact, the privileges that you gain from it might not even be important enough. But somebody needed some money on a Friday night and they said, Hey, if I could turn a bug report, I might be able to get a hundred bucks. I get some beer money and off we go.

[00:41:25] **G Mark:** And things such as that. And then of course, integrating with the ticketing system so we're not ending up with just a whole list of laundry items that we have a cram into Excel spreadsheet, but we can work them out in a way that we're managing our activities and things like that. And and here's my new acronym, SPOG. Single Pane Of Glass that I think a lot of vendors are looking for, and a lot of executives are too, in CISOs as well. It's one of the business issues that I've looked at is I'm tired of having to go fishing down and running my trap lines, if you will, to go find 3, 4, 5, 6 sources to be able to [00:42:00] come back and answer question from senior management or to be able to provide effective tasking or.

[00:42:04] **G Mark:** That something has been done and that looks like it's working pretty well. So thank you again for your time and for your energy on Jeff, you're the CISO at our sponsor nuclear security, which is really great. So we'd like to say thank you to your marketing team for setting us up and making this happen.

[00:42:18] **G Mark:** And for audience, if you've liked today's show. Give us a favor and give us thumbs up, or a five star review or something like that, why? It's not just we're grubbing for grades, but rather it helps us improve our visibility and it helps other people find our show. And so if you like this show, please let us know and let other people know as well.

[00:42:36] **G Mark:** This is your host, G Mark Hardy. It's been a privilege to be with you, and thank you for your time and listening. Until next time, stay safe out there.