#211 - Allowlisting and Ringfencing (with Kieran Human)

[00:00:00] **G Mark Hardy:** We're going to talk about something that you're probably using today or should be using today that really started about the time that John McAfee started doing it. Are you doing what John was doing? Find out. Stick around for CISO Tradecraft.

[00:00:12] **G Mark Hardy:** Hello, and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. I'm your host, G Mark Hardy. On today's episode, we're going to talk a lot about Endpoint protection and how we can do that better.

But before I get going, let me mention something real quickly. In February, I'm going to be getting a chance to go out to sea on something called CruiseCon, and you can too! CruiseCon 2025 will be departing from Port Canaveral, Florida from the 8th to the 13th of February. And if you're interested in joining us, go to cruisecon.

com. And if you sign up, use the [00:01:00] discount code CISOTRADECRAFT10, and you get a 10% discount. Looking forward to seeing you there. If you can make it, you're gonna meet a whole bunch of interesting cybersecurity leaders in a relatively low-key environment where you're not gonna be hit with a ton of vendor pitches and phone calls and people interrupting you.

So think about that. So anyway. Talking about endpoint protection, I've got my guest here, Kieran Human, which you'll introduce in a moment. But lemme do a little bit of a preamble here because I a little bit of research and found out, if you look at the history of endpoint protection, really the first real software tool for that was what we called antivirus.

And in 1987, for those of you who remember, John McAfee founded his eponymously named company selling a tool called Virus Scan. And I remember that in the early days it had a running count of the number of viruses that it prevented. Considering the number of malware instances we have today, it was

like the scene in Blazing Saddles where an early Howard Johnson restaurant featured one flavor of ice cream.

Now, for those of you who don't remember the sixties or seventies, Howard Johnson's was the biggest restaurant chain in the [00:02:00] world back then. It had prominently featured 28 flavors of ice cream on the road signs. And their last restaurant, however, closed in 2016, so you're forgiven if that isn't part of your memory.

But anyway, Peter Norton followed three years later with his version of Norton Antivirus. And I was an early user of the Norton Utilities, and in researching this episode, I found my 1988 versions of Version 4. 5 of these tools, which are definitely not going to work on a 64 bit machine. And anyway, these two companies duped it out for market share as PCs became fixtures in the 1980s in both businesses and homes.

Essentially, these companies would capture a sample of malware. Analyze it, determine the signature, which is usually a unique string of bytes, pretty much toward the beginning of the file, then add it to the next update. And then you'd run a scan against the files, and they would be checked against the library of known bad stuff.

And if there was a match, you get an alert. It would also check for infected boot sectors, as that was a common virus programming technique at the time. how about some advancements? In 1993, [00:03:00] Norton Antivirus 3.0 introduced a new feature, scanning for viruses in memory before loading. Wow! imagine that!

The boot process would halt, now you have to go dig out an uninfected floppy disk and then you'd boot from that. Because remember, back then, Most PC users are running MS DOS 6.0, which really wasn't a ginormous operating system like Windows 10 or 11 today. Somewhere in the box, I still have a bootable, single sided, 5.25 inch floppy that has DOS 2.11 and WordPerfect and even room for a few document files. Times certainly have changed. Now in this first generation of antivirus, which is populated McAfee, Norton, and Avast, advancements in software went beyond just alerting to the presence of viruses to be able to quarantine them so they wouldn't cause any harm.

So you scan against the database of several thousand signatures, that was a good approach when the number of viruses was small. However, bad actors got wiser to this type of defensive activity and introduced new techniques like

polymorphism. Now a polymorphic virus [00:04:00] could change itself every time a copy was made.

And now the 10,000 variants quickly became 100 million variants, which meant checking against a signature database was just not going to scale. So antivirus vendors were in a constant tail chase trying to capture, identify, define a signature, and then push updates to their customers. The industry needed a new solution to this problem. The second wave of endpoint security solutions were called Endpoint Detection and Response Software, or EDR, and here the goal is to log activity on the endpoint and associate the actions of the logged activities with known bad techniques, tactics, and procedures, what we call TTPs. Now today, an authoritative list of these TTPs is the MITRE ATT&CK Framework.

For example, if your tools detected log activity and it matched MITRE ATT&CK Framework Technique T1558, known as Kerberoasting, you know that some bad actor is trying to steal credentials in your environment. Now, while this methodology can find a lot more malicious software, it can also have a lot [00:05:00] more false positives.

MITRE ATT&CK Most industry reports would say that the best EDRs are 99, maybe even 99.5 percent accurate. That sounds pretty good, but if you miss 1 percent of ransomware in your environment, you could still have a material impact on your company. So if generation 1 antivirus and generation 2 EDR don't get you to that last 1%, then what should CISOs and security leaders look at to protect their company today?

And we think the answer is the next generation endpoint protection platforms that restrict what runs on devices by using a technique called allowlisting. Now, for many years in the cybersecurity community, we use the term whitelisting and blacklisting to refer to a list of allowable and unallowable software.

But in today's politically correct environment, some people have associated these terms with skin color and race. in the modern workplace, the trend is to use the term allowlisting and blocklisting. Now, what is allowlisting, and why should you as a CISO, as a leader, care? Instead of trying to identify which of the [00:06:00] thousands of potential software instances is malicious, which is computationally infeasible, why not take the opposite approach?

Now, instead of saying, allow to run anything that has not yet been labeled as bad, how about we use the approach, only allow to run those things we have specifically labeled as good? Now this aligns nicely with zero trust and least

privilege guidance. Any new software is denied the ability to run until it's been labeled as good.

And this includes malware, as well as crypto miners, games, shadow IT, and other scourges of IT departments. Now when it comes to Microsoft Superpatch Tuesday, the key of course is for these companies to get advanced copies of changes from Microsoft and push them to the endpoints before the update is applied, otherwise you might end up bricking your box.

if that is my intro, Let me welcome our sponsor Kieran Human from ThreatLocker to the show who's going to talk about why tools that have a default deny approach are much more suitable for protecting today's IT. Kieran, thanks for coming on today's show and can [00:07:00] you tell our listeners about yourself a little bit and about your background?

[00:07:03] **Kieran Human:** Hi, yes, thank you for having me. I'm a special projects engineer at ThreatLocker. I recently got my master's in cyber security and privacy from UCF and then I wrote my thesis on the intersectionality of cryptocurrency and cybercrime.

[00:07:17] **G Mark Hardy:** Oh, that sounds interesting. I might actually want to read that because I've got a long background in looking at cryptocurrency. But thanks for telling us a little bit about your background and it seems you've had a fun career just starting out. I noticed I went ahead and looked at your LinkedIn.

And it looks like your degrees are fairly recent. So well done in terms of getting on board while they've got educational. And UCF, University of Central Florida, by the way, if people are wondering, it's got an excellent program, both undergraduate and graduate. So we talked a little bit about antivirus and EDR software, and despite their best efforts, they still can't really detect every piece of malicious software, plus they're noisy.

If I'm a CISO at a fortune 1000 company, I could have millions of alerts from an EDR tool saying something malicious is happening. maybe not, but something might be happening. And as a result, [00:08:00] incident responders are going to tune out these alerts because of all the false positives. They're going to miss when something actually does go bad.

Now talk to me a little bit about default deny or the allow listing. What's that all about? And how does that flip the script for safeguarding the enterprise?

Alert Fatigue is a Real Issue

[00:08:15] **Kieran Human:** Yeah, alert fatigue is definitely a real issue in the industry. Having to try and figure out what is good and what is bad can take a lot of work and have many false positives like you said. Think about it like this, Compare the number of applications that you want to allow, versus the number of applications that you want to block.

Which is bigger, which is easier to manage, easier to control. with application allow listing, where you deny by default and permit by exception, it does all the heavy lifting for you. If the application is not on the list, it doesn't run. Simple as that. You don't have to chase down the latest malware and vulnerability in order to be secure.

but like you mentioned, it has traditionally been quite difficult for companies to deploy that, application allow listing. like with the patch [00:09:00] Tuesday, you don't want to cause issues where it's not allowed and then issues with the machine. Threatlocker has learning mode where it will learn what's running in your environment and then built in applications where we will track the updates for thousands of applications and update them for you so that.

It's a seamless process and you're not getting a bunch of denies and your workflow just continues like usual. we then take that further with ring fencing where we can limit what applications do, whether that's interacting with another application, your files, data, internet, registry, just a lot of granular control.

[00:09:34] **G Mark Hardy:** Okay, so ring fencing, that's a term for it might be new for some people. So as you said, it limits what applications can do.

[00:09:41] **Kieran Human:** Yes,

[00:09:42] **G Mark Hardy:** And so what that is in for each application. that you are aware of, because this is an allowless type of approach, you can say that, yep, this thing can access the internet, but perhaps this one can't.

This one can go ahead and do it. Okay, so that's the concept of ring fencing. I got it. So if vulnerability scanners and antivirus [00:10:00] tools can't detect a malicious PowerShell script, then you wouldn't be able to stop that attack. And given that ransomware happens pretty quickly, that could be problematic.

However, if we haven't approved PowerShell scripts to run, or a particular PowerShell script to run, it's blocked by default. Which sounds like it's a lot more secure, and I like that. Now, allow listing of applications has been around for a while, that concept. I can remember that even the Australian Essential Eight said it was one of the top eight safeguards that they wanted every company to adopt.

Are you seeing other guidance recommending this type of required approach in government standards and regulations?

[00:10:34] **Kieran Human:** Yes, we are seeing more guidance come out around the world requiring application allow listing. Governments are starting to realize that detection and response just isn't enough. Antivirus isn't enough. Australia has the Essential 8, the UK has Cyber Essentials, and there's just many other requirements and suggestions around the world, and everyone's moving towards that more default deny approach.

[00:10:56] **G Mark Hardy:** because when I started researching this episode, I looked [00:11:00] about this concept of allow listings and said, wow, this is pretty good. So you're telling me about, application containment and ring fencing. You, mentioned that a little bit before I dug into it a little bit. Let's go a little bit more detail just to make sure everybody understands exactly what we're talking about here.

Allow Listing ad RingFencing

[00:11:13] **Kieran Human:** Of course, so allowlisting, like we've been saying, it's extremely powerful, it's great, you should absolutely use it. you only allow what's approved, nothing else, but you also want to then limit what those approved applications can do. any application that you run has the same access that you have.

So if you can access all of your files, so can any program. if you can reach out to the internet. So can they. If you can edit the registry, so can it. so ThreatLocker ring fencing extends application allow listing by limiting the behavior of those approved applications. A user may need access to PowerShell scripts, but maybe those PowerShell scripts don't need to reach out to the internet.

Or maybe those PowerShell scripts don't need to reach out to your backup files.

[00:11:57] **G Mark Hardy:** Got it. So let me summarize this. So we've got [00:12:00] Microsoft Windows Environments. It'll run a lot of different software instances. Now there might be older software there, and it often is vulnerable to discovered weaknesses that may not have yet been patched. A good example might be Windows print drivers for old legacy devices.

Now if those print drivers can be exploited, then a bad actor could use them to read files that they shouldn't, or outright exfiltrate data. Now, neither of those is a good outcome, and so that's why I think having endpoint protection that would block old drivers from being exploited would be really helpful.

And suddenly it seems that, if it detects something that's malicious, like an open outbound network connection, it's trying to go ahead and attach to something, shared storage that it should not, you can stop that from happening and save our bacon. Is that right?

[00:12:44] **Kieran Human:** Yes, it's crucial to block all drivers and software that isn't needed. Rather than ThreatLocker seeing what it's trying to do as malicious, like what those detection and response will do. We just block by default. You don't need it, why should it be allowed to run. It really simplifies the process of securing the endpoint when you are [00:13:00] certain nothing malicious can run including old vulnerable drivers

[00:13:07] **G Mark Hardy:** So a combination of restricting things that you haven't approved, which is going to be all that old stuff. Plus the concept of ring fencing, which says of the things that we do say, okay, they don't get everything that we get. They only get those privileges that they're going to need to be approved. That kind of gives you a double one, two punch that really helps out.

And I can see how these types of approaches can really help. you look at an attack chain such as phishing, for example, you get a Microsoft Excel or PDF document and that could spawn and potentially run a PowerShell script and that could be pretty bad. So if you can use application containment safeguards to ring fence Excel from calling any external software, then you can stop a lot of these potential attacks.

Have you seen any customers use this type of next generation safeguard to further enhance their Microsoft security?

[00:13:53] **Kieran Human:** We do see those Microsoft Office files be restricted from accessing PowerShell, accessing the internet. we can [00:14:00] also limit it so that it can only access those Excel pages. So your Microsoft Excel doesn't

need to access a Word doc. Your Word doc doesn't need to access PowerShell and the Excel scripts.

It just really limits, only give it the access it needs. Nothing else. It takes that default to deny approach further.

[00:14:18] **G Mark Hardy:** I like that. I've got a friend who says it seems like every day his Chrome browser is now asking to scan his network or connect to Bluetooth. Now, we're back and forth and talking about that, and I can't get mine to do that, but his does, and it's no, stay in your lane, Chrome browser. You're there to help me surf the internet, not find unpatched OT devices like my home thermostat.

I'm pretty sure bad actors are going to start finding ways to use this Chrome functionality that Harm people in organizations. so what are your thoughts about that with respect to browsers?

[00:14:46] **Kieran Human:** Yeah, you'd be surprised at how much more applications can do and access than people realize. there's this one coupon Chrome extension that's from China that has access to your Chrome passwords and we see this on numerous [00:15:00] corporate devices all the time. it really drives home the point that you need to allow what is needed and block everything else.

That's applications, that's extensions, and then block those, the behaviors that you don't want. Chrome shouldn't be scanning your network.

[00:15:16] **G Mark Hardy:** Yeah. And by the way, I had been probably foolishly, but I like to think I know what I'm doing using the Chrome password for a number of years, actually. I finally got religion this year and I moved over to a password manager. It's just there's just too many horror stories about the browser that's really convenient.

Like pop, pops up the user password, but the way it's stored and the way you can access it, because it's stored, shared between my laptop And my cell phone and all you really need is a pin on your cell phone to get access to the entire password store and that to me is We found out that, of course, you always remember the enemy of security is convenience.

And sometimes being too convenient is a problem. But when you take a look at things such as keeping [00:16:00] software from scanning the network or trying to connect places that you shouldn't, another common attack I see is bad actors

that are going to name their malicious service is to have the same or maybe a very similar name to a legitimate Microsoft service.

So it, it's a problem. This kind of blends in. So if an administrator is casually going through a bunch of logs, they're looking at this service, their process, it's yeah, this looks normal. It looks like a reasonable thing. It's not, you don't notice that there's a one there or the I versus the L or something like that.

Now, what should endpoint protection systems be doing to look at the data lineage in Providence to say, this thing, which has the same name or all the same name is a Microsoft service really didn't come from Microsoft.

[00:16:41] **Kieran Human:** Yeah. So oftentimes they will verify certificates, but even that isn't bulletproof. you can look at the Kaseya attack in 2021. The only way to be sure is to use application allow listing. Even if a new program is signed by a reputable company, block it. If I don't need it [00:17:00] yesterday, why do I suddenly need it today?

You only need to allow what you need block everything else. It's much easier to manage a small curated list of programs that are needed rather than trying to find the bad programs amongst thousands of unknown ones.

[00:17:14] **G Mark Hardy:** Yeah, now, throw a little war story in here, for a company that was known as Bit9. You may have heard of it, and what had happened was this, is they did a similar sort of thing with the allow listing, and somebody hacked into them, and so they did two things. Number one is they grabbed their customer list.

Number two is they added their malware to the allow list. And then they went ahead and made sure that they waited until everybody updated their version of the software. Then they pushed their malware out to the customer unless they knew exactly who to email it to, and it worked like its champ. And so at that point in time, that really didn't go too well.

So presumably when we hear scary stories about early adopters in some of these spaces like that, we say we try to avoid things like that today. But another interesting threat that I'm hearing more about [00:18:00] is fileless malware. And it will run in memory. But it never saves a copy of itself on the hard drive.

Essentially, if there's no file, how is antivirus or EDR going to detect it, let alone determine that it's malicious? can you talk a little bit about fileless malware and how application containment might even stop those types of attacks?

[00:18:19] **Kieran Human:** Yeah, so fileless malware uses applications and tools already on the machine to run the malware. these can be more difficult to detect because it doesn't rely on malicious files, like traditional antivirus could then scan for malware. Application allow listing can block common tools that they try to use, like PowerShell or, Anything else, while the application may be on the computer, the adversary cannot use it if it hasn't been explicitly allowed.

And then ring fencing can block that lateral movement. So if the user tries to run a malicious office macro that calls PowerShell, it can't. ThreatLocker Detect also has some pre built policies to alert you to common violence malware behaviors.

[00:18:59] **G Mark Hardy:** [00:19:00] Interesting. let's think about how this might relate to something like ransomware. Essentially, we don't want malicious scripts writing over all of our backup data, especially things that might be externally connected, like a storage device, tape backup, cloud storage, etc., something like that. what should administrators be doing to control bad actors from writing over important backups and storage devices?

[00:19:21] **Kieran Human:** There's a few things that can be done. The first is that users shouldn't have access to other people's backups. To be even more secure though, administrators should not allow the user to even access their own backups. ThreatLocker Storage Control can block the user from accessing their own backup while still allowing your backup software the access that it needs.

I saw a recent statistic that 94 percent of ransomware in 2023 tried to compromise backups. It is a real threat that really does need to be taken seriously.

[00:19:51] **G Mark Hardy:** So of course I would think that if the user does back something up, there's got to be a process to get the information back. but you're right. They shouldn't be able to overwrite [00:20:00] what's been pushed up there. and being able to control that seems like a really good control. So, let me summarize some of the things that we've been saying here.

It sounds like this third generation. of endpoint protection tools do at least three different things that we typically don't see in an EDR. So first, they're going to provide allow listing. That's going to give you a proactive approach to cybersecurity by stopping everything from running unless it's on that approved list.

Second, they prevent the weaponization of existing drivers, applications, services, and we mentioned how bad actors might leverage malicious print drivers, or Microsoft Excel, or Chrome to harness that. harm your computer. And third, a third generation endpoint protection tool allows you to create and enforce policy based data access decisions.

For example, I don't want something using my external storage device unless it's my DR application, and that way a bad actor can't just come in and wipe my external storage or my backups. So these three features do seem like something that would stop a lot of these targeted [00:21:00] cyber intrusions, ransomware, from happening.

Or even a malicious insider. Now, if a CISO or a security leader were interested in deploying this type of solution, how hard is that to get started? can you talk a little bit about what it would take to get an application allow listing off the ground?

[00:21:14] **Kieran Human:** Getting started with ThreatLocker is really much easier than you may expect. Unlike other solutions, ThreatLocker does the heavy lifting for you, especially with learning mode where it'll learn what's running in your environment, and then you can book a free demo with us to try ThreatLocker in your environment and meet with our dedicated solution engineers to get it set up.

They'll meet with you, often starting with around once a week, and then eventually it'll be once a month or as needed as it progresses, and make sure that using ThreatLocker is a smooth experience and they address any question that you may have. there's also, 100 percent US based, 24 7, 365 cyber hero support with an average of under 60 seconds response time for any questions you may have.

[00:21:56] **G Mark Hardy:** That is absolutely awesome. nobody can that does that [00:22:00] these days. I love that. Now I have to imagine after this initial investment upfront, it's going to get a lot easier. to have the helpdesk work with employees and developers to add things to the allow list, correct? Because you've got to do that learning mode, you've got to get things set up.

Are you seeing any best practices to make this a good experience? Or how do we get from start to production?

[00:22:20] **Kieran Human:** The initial setup process and time isn't that big due to the learning mode and the solution engineers. It's really good at learning

what's already in your environment and then creating custom rules according to your specific needs. And then that solution engineer or threat locker will go over those rules and just make sure that you do want to allow those questions.

Make sure that what is running in your environment, you want to be running because so many times there'll be, there was one where they had about six different remote access tools running in their corporate and running, not downloaded, not, they're running in their environment. we'll go over and make sure, Hey, do you want these tools running?

You probably don't. so then we [00:23:00] can just block all of those for you.

[00:23:01] **G Mark Hardy:** Yeah, and a lot of times this could be shadow IT, that IT departments aren't even aware that these things are in their environment until it's surprise! You've just created a huge increase in our tax service. are there any mistakes that you see security leaders making when trying to implement these kinds of tools?

For example, if you really didn't have a good change management program or a rollout strategy, could this approach even be useful?

[00:23:26] **Kieran Human:** Inertia is probably the biggest obstacle, whether because of a fear of pushback or. Any other reason, really. The longer it takes to implement a tool, the bigger the problem of unauthorized or unneeded software becomes. You may have 200 users running a remote access tool like TeamViewer today. In a month or two, it could be 220, 250, even more.

This is a good saying. The best time to plant a tree was 20 years ago. The second best time is today.

[00:23:53] **G Mark Hardy:** So just get started. I, like it. Now, are there any types of metrics that you see CISOs and other [00:24:00] security leaders sharing with their leadership teams on how endpoint security tools are helping to defend the organization.

[00:24:07] **Kieran Human:** Before metrics, you need data, and then to get the data, you need visibility. There are countless organizations that have no idea what software, good and bad, is running in their environment, or what network activity is occurring. The first stage in applying controls and securing an environment is knowing what is present.

Then you can decide what is needed and what is not. Visibility of what software is running, what network activity is taking place, etc. is the first step in the journey to real security.

[00:24:36] **G Mark Hardy:** Amazing. Now, are there any other lessons learned or good war stories on the topic that you might want to share with our listeners and our viewers?

[00:24:45] **Kieran Human:** Yeah, so like I was saying earlier, there was an environment with six remote access tools running on their machines. Environments with dozens of machines with RDP exposed to the internet due to firewall misconfigurations. they were just [00:25:00] a single brute force attack away from being a victim of ransomware and a data breach.

we saw two or three attacks for massive companies who have work machines at home with RDP open to the internet. There were government entities with machines communicating with TikTok and active connections to Russian IP addresses. so Soft, ThreatLocker has a free software health report that everyone should check out that can give you visibility of what's going on in your environment.

You really would be amazed at what people find in their environment. It's crazy what goes on without IT knowing.

[00:25:39] **G Mark Hardy:** Wow. And I have seen maybe not this crazy as that, but I have seen a lot of things that are out there. any kind of thoughts that you have as we wrap up here about, for our listeners, which they keep in mind here,

[00:25:55] **Kieran Human:** People just need to be aware that you're only as strong as your weakest link in security. Threat [00:26:00] actors don't really care what size your business is. They will see you as a target. Whether it is with ThreatLocker or someone else, you need to have complete visibility and control of your environment.

[00:26:12] **G Mark Hardy:** yeah, I would agree with that. So Kieran. Thank you for coming on the podcast today to talk about the next generation of endpoint protection tools. I got to say to our listeners and our watchers, if you're not using allow list technologies, you're leaving out a very helpful safeguard that can stop a lot of malware from running in your environment.

And I think this is one of those things that is going to be absolutely essential in enterprise. And that's probably why the Australians put it in their essential eight.

So if any of our subscribers want to learn a little bit more or get in touch with you, what's the best way to do that?

[00:26:42] **Kieran Human:** The best way to get in touch with us is to just go to our website. That's ThreatLocker. com. We have a ton of great resources. And you can book a free demo to get started and get that free software health report that I mentioned. Thank you very much for having me. I really enjoyed it.

[00:26:58] **G Mark Hardy:** Kieran, thank you again for [00:27:00] coming. And thank you to our listeners for, or watchers for tuning into CISO Tradecraft. We hope you've enjoyed learning something about the third generation of endpoint protection tools. Now, remember, if you learn something new, share it with a friend or a colleague, and we'd love to see your LinkedIn posts.

hey, this time we're going to do something different. Make a post on LinkedIn about this episode. And after about a week, we're going to go ahead and select one person with whom to do a free 30 minute call to help you on your journey to become a better cybersecurity leader. It's pretty easy to write a LinkedIn post on the topic.

Make sure you tag us with the @CISOTradecraft, point to this episode, and we might be in touch. So thanks again for listening. This is your host, G Mark Hardy. Appreciate you being part of the show. And until next time, stay safe out there.