INSIGHTCYBER: SOLVING REAL-WORLD CHALLENGES FOR TODAY'S SECURITY PROFESSIONAL

A conversation with CSO Curtis Blount

InsightCyber Chief Security Officer Curtis Blount has spent decades leading cybersecurity and risk management organizations across multiple industries. In this in-depth discussion, he examines the differences between OT (Operational Technology) and IT cybersecurity, and how InsightCyber's new solution bridges the gap between the two worlds in an entirely new way.

Q: What is the business problem that InsightCyber is addressing?

A: The technology we're delivering solves a set of very important problems for modern businesses who invest in cyber-physical systems. The first one is what I call the convergence of technology pillars. We always hear about IT and OT converging, and while that's technically true, it's not the whole story. There are other pillars that are also merging.

From a real-world standpoint, you've got IT merging with cyber security, data governance, physical security. And then the mixed cloud, where companies are using AWS, Azure, and Google Cloud as part of their overall infrastructure.

All of these pillars are converging and all of them have distinct security issues and concerns, and distinct security controls. From an IT perspective, we're pretty accustomed to all this. We deal with it on a day-to-day basis. But in the OT world, things are fundamentally different. The mindset is different, the operations are different.

Q: What are the key differences between the two?

A: In the IT world, we focus on security through a particular framework called the CIA Triad, which stands for Confidentiality, Integrity, and Availability. In the OT world, that gets flipped completely around, and the focus is on SAIC, or Security, Availability, Integrity, and Confidentiality. So, while confidentiality is priority number one for IT, in OT it's the lowest priority. OT is primarily focused on safety and availability. When I talk about converging pillars, that's the first industry issue we need to contend with.

The second one is how IT Operations and IT Security managers manage actual security threats. In the IT world, it's about vulnerabilities – patching, firewalls, controlling network access, controlling user access, things like that. We're conditioned to think that the only way to reduce risk is to address vulnerabilities associated with a recognized database of publicly disclosed cybersecurity vulnerabilities, called the CVE List. All the security tools and the things we do from a security program standpoint are based on that. In the OT world, it is completely different.

Q: So, there's a difference in everyday security vigilance?

A: For people like plant operators or automation engineers, the focus is on operational anomalies. Safety and availability are at the core of what they do. It's almost the opposite from the IT side of the house. So, with this convergence, we have to come up with a way that handles both—being able to flip and say, okay, if I'm looking at an asset on the OT side of the house, my primary concern is availability and safety, whereas if I'm looking at something on the IT side of the house, my concern is confidentiality.

Another important aspect is that in the OT and IOT world, the concept of patching is simply out of the question. You cannot patch a SCADA (Supervisory Control and Data Acquisition) device. That's just not going to happen. And more than likely, you're not going to patch a POC module or a Raspberry PI or something like that, because it breaks the maintenance and, especially if you talk about automation, the controls are based upon the specific manufacturer and operating system version. So how do you get a handle on the OT world without patching, without doing vulnerability scans, all those things that we would normally do on the IT side of the house?

Q: It sounds like the entire mindset is completely different.

A: One important but somewhat controversial difference here is that IT and IT security are typically operational expenses (OPEX) and are tied to internal company operations. But on the industrial control side of the house, for example, a PLC—a Programable Logic Controller—is a capital expense (CAPEX), which is tied to revenue. So yes, it's a different mindset. Again, it's all about availability and security instead of confidentiality. I'm going to keep referring to that because as I go through this list, you'll see that this is really the nuts and bolts of it.

Another big consideration is asset and inventory management. This is critical, regardless of where you sit in the converging pillars. If I'm on the OT side of the house, I obviously need to know what my assets are. I also need to know what my assets are on the IT side—though in the IT world, assets are generally desktops, laptops, servers, networking, equipment, things like that. Very traditional. And, depending on the size of the organization, there could be a few thousand of those assets.

Q: What are the considerations for security assets in OT environments?

A: On the OT side, we're talking about things like legacy SCADA devices, connected and non-connected PLCs, Raspberry Pi's, connected HVAC systems, and many others. We're not talking about a thousand assets; we're talking hundreds of thousands of assets. Also keep in mind that in the OT world, you could have a manufacturing plant in California, a distribution plant in Texas, and a corporate office in Iowa.

And one plant can have 20 different buildings in it. How do you gain visibility into a massive environment and distributed infrastructure like that?

There's also the fact that IT operations and OT operations have been typically siloed. In most cases they don't talk to each other. When they start to converge and the people in IT need to see what's happening on the OT side of the house, they approach it like IT, using their existing security operations center (SOC) or network operations center (NOC). And they try to protect the OT environment the same way they protect IT—with vulnerability scans, patching, installing security software agents and so on. To which the OT manager says: No, you're not! You're not touching my environment. Because if you do, you could potentially—and most likely—bring it down, and that has a very direct impact on revenue.

Those are just like some of the real-world issues we have to contend with.

Q: So, given these differences, what approach did you take at InsightCyber with the opportunity to build a new solution from scratch?

When we looked at building the technology with InsightCyber, all of those conditions came into play. Ultimately, what we've built is a technology that solves real-world problems. First, how to you get an accurate inventory? What assets you have? What are they doing? What is the connectivity associated with them? And once you have a fundamental understanding of all that, then you can examine the vulnerabilities and the operational anomalies associated with your assets. That's the second piece of it. And the third piece is: what are the risks associated with those individual assets and those networks? From there, we get into measuring assets against industry best practices, regulatory and contractual obligations, as well as impact to revenue.

Q: What do you say to the customer who asks, "How is this technology going to make my life better?"

A: I would remind them of the old question, "How do you know where you're going if you don't know where you came from?" What we're offering is a technology that allows you to get from point A to point Z by providing a new kind of visibility into complex environments that minimizes risk and is relatively cost-effective.

We're giving customers a new option that provides a detailed understanding of what's in their environments and what the threats and vulnerabilities are. It also creates reports that can help build a very comprehensive security program that addresses both the IT side of the house and the OT side of the house, without a lot of screaming and hollering.

Q: Talk about this idea that you're going to spot problems—that you're going to have a proactive security posture that finds the tiny anomaly and keeps end-customers from getting attacked.

A: Let's look at it this way. Traditional security tools rely very heavily on vulnerability databases and logs. But logs are "post"—they're after the fact. If your network gets breached, it's likely you won't know about it until either A, something bad happens, or B, you finally get a chance to review logs to say, wait a minute, something is wrong here. That fundamental approach of logging and patching vulnerabilities just doesn't cut it anymore.

Look at all the security solutions out there, like firewalls and AV and malware detection, all that stuff. It's all based on us knowing about a particular vulnerability or malware, creating an index, and then adding that index to a security tool. Again, it's all "post." You're always fighting yesterday's war. What we're saying is, let's look at it from more of a real-time standpoint. We now know everything that's in your inventory, and, thanks to AI, we can continuously monitor your device behaviors and spot the tiny anomalies that signal the early stages of a new attack—and nip a problem in the bud before it turns into an expensive disaster.

Q: How do you implement that?

Thorough our 26-point blueprint for success—which is our model for implementing the service to meet a given customer's needs—we start by validating the assets, the connectivity, and the networks that are associated with your environment, all down to a very granular level. Because we have that, we can monitor each asset individually and create a sort of an avatar for each one that says: Your normal operating condition is "this." If we see something that is outside of a normal operating condition, we classify it as an anomaly and send an alert.

So, instead of combing through, you know, a gig's worth of data, trying to find out a particular issue, what we're saying is: cut all that out and just look at behavior. Long-term, if an asset operates the same way every single day and has the same connectivity every single day, and then all of a sudden, it's sending more packets than it should be, or it has another connection that is brand new—that's something you want to want to be aware of. That's an alert which you can actually address in real-time and say, okay, this is a brand-new device that's being attached, and I know what that is, or this is actually a threat that's impacted me, and I can remediate it right now.

Q: That sounds great, but aren't other vendors doing more or less the same thing? What's what makes InsightCyber unique?

A: We focus on behavioral analytics in a specific new way. If you're on the IT side of the house, you're familiar with behavioral analytics because that's what you do with employees and identities—basically, you monitor the behavior of people. When you see someone downloading confidential files off a share site on the corporate network, that's a behavior.

We're taking that concept and applying it at a very fine-grained level to OT devices. We identify assets and watch their behaviors continuously, and we know immediately when they deviate from what they're supposed to be doing. No one else can do this at the speed, scale, and precision that we can do it, and that's because of the AI we've developed. The second piece is that we're able to not only capture an anomaly based off a cyber threat, but we're also able to capture the anomaly based off an operational threat. And that's very important from an OT standpoint, because they're more concerned with availability and safety than they are with confidentiality, which is IT's chief concern. There is a big, unique difference between us and other technologies and their mindsets, because they focus on confidentiality more than safety and availability. We do both.

Q: What is it about InsightCyber's AI that is unique?

A: What it essentially does is “capture” your assets, meaning that it validates every single asset and creates an index of its behavior over time and against a range of expected operations. I call this the asset’s “bubble’’—the range of normal operations on a day-to-day basis. There is a threshold; you don't go above the bubble, and you don't go below it. If you do, it suggests you have a problem.

Our AI captures that information not only from a device or asset perspective but also from a network perspective. We know, for example, that across this particular network or that particular sub-net, we should see this type of connectivity, that amount of traffic generated, these particular ports open. And if we see something outside of the norm, we automatically alert on it.

Q: How does InsightCyber do it?

A: Effectively, we’re scaling down what we call the noise. In traditional IT, there’s a technology called SIEM, which is Security Information and Event Management. A SIEM solution captures all kinds of logs from multiple log sources, centralizes everything, and then generates alerts based on specific conditions, which the customer must define. We're cutting all of that out and saying that, from a behavioral standpoint, you don't need logs. All you need to do is observe the behavior of an asset and then generate an alert based on that asset and its non-condition.

We're viewing this technology as a next generation displacement for SIEM, because we're creating that behavioral aspect and incorporating that into day-to-day operations. And that's something that's really, really new in the world.

You'll hear other companies talk say that they do behavioral analytics. But their behavioral analytics are based on logs, instead of looking at the asset and basing the behavior off the asset itself. The genius here is in the AI. It does behavioral analytics in a way that’s entirely new. It gets smarter as it goes, and we're going to incorporate other intellectual property around risk that's going to strengthen the capability over time.

Q: How does this integrate with an organization’s SOC?

A: Well, it’s interesting because, again with SOC, it's very traditional. In the SOC industry and the technology associated with it, we're seeing a lot of change and a lot of fluidity. With that convergence I spoke about earlier, companies now need to be able to know what's happening on both the IT and the OT sides of the house. And that’s what we enable.

We take anomalous behavior reporting and incorporate it into the customer’s SOC, whether they're using a traditional SIEM or what we call the next generation SIEM—XDR, threat detection and remediation, and MDR, managed detection response. Instead of sending logs, we generate alerts that are easily incorporated to a SIEM.

A SOC can now have one view, or one UI, that covers both what they're already doing on the IT side of the house plus what’s happening in the OT and OT world, which is relatively new for them. So, we're able to give a SOC operator some real world understanding of both IT and OT/IOT, converging the two in a way that really works and is cost effective.

Q: How does this help with staffing?

A: From a SOC perspective, you typically have an analyst that is tied to either a certain number of IPs or a certain number of users, if you're talking about, say, a desktop environment. From a helpdesk perspective, you might need one individual per every1,500 users, or one individual per every 150 class C subnets.

Something to that effect. The more technology, the more assets, the more individuals you need, the greater number of SOC resources you have to fulfill. What we say is: let's automate a lot of that process. Because the reason you need that number of people is because you have to go through all those logs and filter out all that noise to figure out, okay, "This is an actual alert, confirmed," versus "This is something that I don't need to worry about."

Q: To that specific challenge of having people constantly sorting through the noise, how major is that for a customer?

A: It's huge. Absolutely huge. One of the biggest issues is burnout. It's very difficult to keep and maintain people in a SOC. The job involves long hours, lots of analytical work, and very little recognition, unfortunately.

Creating a satisfying career path for security professionals is hard. Today, there are typically three tiers. Tier one is the person who is just starting off, doing customer service for the most part. Tier two is more analytical work. And tier three is where the data scientists and data analysis operate, doing threat hunting and assessment. In most cases, you don't see movement from tier two to tier three. There's no worthwhile progression from a career standpoint. And that's a constant challenge that managers have to contend with.

Q: When you think about what it takes to convince the technical evaluator (and that person's boss) that InsightCyber is worth taking a risk on, what's your best pitch?

A: I think the best pitch is that we know you're just starting off in this world of building out a security program for your OT environment. At the same time, we know you also have resource constraints to contend with—that you have to do the job with what you've got in-house right now. What we provide is a solution that gives you the visibility you need and delivers the operational conditions that you're looking for from both an OT and IT perspective.

We can give you the vulnerabilities and the risks associated with all of your assets. And we can also give you the reporting that you need from a senior management standpoint, to go back to your board and say, okay, I now have a fundamental understanding of what's in our OT environment.

I know and understand what the risks are. And here is my plan to bring that environment up to a level and standard that matches what we have on the IT side of the house.

We can do that all through one solution, at a fraction of the cost of what you currently pay right now for any of your current security tools. And if you give us a chance, we can prove that to you relatively quickly.

Q: How do you respond to the executive who says, "Yeah, that all sounds great, but I'm really worried about the Colonial Pipeline incident and I'm worried about ransomware?"

A: I would go to the heart of what happened with Colonial Pipeline. I'm not going to go into the details of the actual breach itself, but essentially what came out of that situation was that if the company had had more visibility, they would've captured the breach and known about it immediately, and they would have been able to prevent it. From the very beginning, InsightCyber has always been about visibility, visibility, visibility–understanding what the customer has.

Again, going back to that old saying, how do you know where you're going if you don't know where you came from? You need to start somewhere. And that somewhere is understanding what assets you have, what they're doing, what they're connected to, and what vulnerabilities and operational anomalies are associated with them. That is fundamentally what InsightCyber delivers. So, from a Colonial Pipeline standpoint, had we actually been installed in their network, we would have given them that critical visibility, in real time, using behavioral analytics.

Q: How would InsightCyber have done that?

A: What happened in the Colonial Pipeline had to do with segmentation. You know, on the IT side of the house, we talk about zero trust and ACL tables and firewalls and all the other good stuff. On the OT side, we look at Purdue models to define the different levels of critical infrastructure that are used in production environments and how to secure them. But even with that, you have to understand what your connectivity is. And that's what we can provide because we're gaining those insights and we're documenting and recording everything based off of behavioral analytics.

When I talk to companies about building out their OT security program, I start by pointing out that you can't do it until you have a deep understanding of what you have and what it's connected to, and then what the associated vulnerabilities are. Once you have those three pieces, as a security officer, you can go back to the board and say, okay, here are the issues, here are the risks, this is going to be the direct impact to revenue if a breach occurs. That's what they need to do in order to build out a security program to minimize risks.

About InsightCyber

InsightCyber is on a mission to keep the world's critical infrastructure, supply chains, and manufacturing operations cyber-safe, preventing attacks that can have catastrophic human and economic impact. The company's AI-powered security service continuously monitors an industrial enterprise's environment, providing insight and protection against a wide range of cyberthreats. To learn more, please visit https://insightcyber.com.

