NETWITNESS

Practical Approaches to Unleashing Autonomous AI Defenders

NetWitness' John Pirc on Ensuring Actionable Workflows for Incident Response Teams

ISMG
INFORMATION SECURITY
MEDIA GROUP

John Pirc

Pirc drives innovation in threat detection for global enterprises. He is a seasoned cybersecurity leader with more than 20 years of experience in threat intelligence, product strategy and national security. He previously held key roles at the CIA, Cisco and IBM, and co-founded the software company Bricata.

With cyberthreats growing more advanced, incident response and cyber defense teams must constantly adapt. “To move faster, security teams are consolidating fragmented tools into integrated platforms, streamlining workflows and using artificial intelligence and automation,” said John Pirc, vice president and head of product management at NetWitness.

But driving innovation with AI technology such as AI agents needs to be practically managed, which means “not letting them go crazy on their own and making their own decisions,” Pirc said. “Innovation is great, but if it’s too complex, then it defeats the purpose.”

Pirc pointed out that cyber adversaries are also using AI to compromise systems at greater speed and scale. “They’re using it at quick speeds. It’s like trying to out-swim a shark,” he said. That’s why autonomous AI threat detection is so crucial.

In this interview with Information Security Media Group at RSAC Conference 2025, Pirc also discussed:

- The level of SASE maturity in APAC and India
- How to balance privacy and network visibility
- How NDR helps in meeting key tenets of SASE

“With AI and ML, you have to train a model. If you train models with garbage data, that’s exactly what you’re going to get out there.”

State of Threat Detection

ANNA DELANEY: What is the current state of threat detection and why is there such an urgency to evolve?

JOHN PIRC: You have to constantly innovate, get outside your comfort zone. Innovation is great. But if innovation is too complex, then it defeats the purpose. When you look at innovation, it’s not just security vendors that are doing that, it’s also the adversaries. We’re using AI, and they’re using AI at quick speeds. How do you compete against that? AI is going to bring a lot to us, but in comes the idea of predictability, being able to stretch multiple analytics together. When you start looking at everything, its data, its data analytics. How do you apply AI to that from that perspective? It involves wanting to make things more efficient, not only from a threat detection perspective but also in terms of analyst workflows and responses.

Catalyst for Cyber Change

ANNA DELANEY: We’re seeing a shift from siloed tools to a more integrated detection ecosystem. What is driving that change and why does it matter?

JOHN PIRC: It matters because you don’t want to be context switching between different platforms. If you have three screens in front of you, that could be three different products. You need to have something more centralized. You’re not going to be that efficient, you’re not going to be able to respond to attacks if you’re constantly switching between different avenues. There are a lot of technologies today with SIM that bring all that technology together. But having one place with all that information is more efficient, reduces dwell time. Dwell time is how long a threat actor is in your organization. How can you reduce that? You reduce that by having the right information at the right time.

The AI Bandwagon

ANNA DELANEY: Early adopters have jumped into the AIdriven threat detection bandwagon. What have we learned so far? What is actually working? What’s not?

JOHN PIRC: With AI and ML, you have to train a model. If you train models with garbage data, that’s exactly what you’re going to get out there. Some think that you can just leave models unsupervised and let it go, whereas it’s going to replace my job. I hear that all the time when we talk to SOC analysts and no, “With AI and ML, you have to train a model. If you train models with garbage data, that’s exactly what you’re going to get out there.” it’s not. It’s human machine teaming. You’re always going to have to have some kind of a human action in a loop with that. When you look at AI, it’s great, but it’s training those models with the right data and not letting them go crazy on their own and make their own decisions.

Doing More With Less

ANNA DELANEY: So many SOCs are asked to do more with less. What's your advice for them and what are the go-to strategies to be more efficient?

JOHN PIRC: I just got done talking to a customer who has three individuals in their SOC, which is small, considering the large size of their organization. It's getting back to using AI in a smart way from a workflow perspective. How can I augment tier one, tier two analyst information that's coming in like a copilot? Having all that information bubbled up to where now that analysts can really focus on or triage what they need. If you're able to improve the speed of those workflows, it makes it more efficient for those analysts to run faster. But on another note, it's not just your current analysts, but when you have men and women coming out of university, they get their first job. Being a SOC analyst is by no means trivial at all. Use that role in a way that trains them, gets them to run faster, to understand. It's going to be game changing.

Blind Spots or Blindsided?

ANNA DELANEY: Threat hunters seem to be leaning more on behavioral analytics and timeline-based correlation. How are these tools helping spot those blind spots?

JOHN PIRC: When you talk about retro threat hunts, let's say you have 12 months of data. At a time slice that data was okay or maybe suspicious. But as you fastforward with new intelligence and saying, 'Okay, well this back here was bad.' Being able to go back, do these retro hunts, piece things together is really important. When you look at whether it's behavioral or whatever we want to call it, it's more from an analytical perspective, so having these analytics, having AI, having these tied from a threat hunting perspective is good. When you look at innovations on that side, threat hunting is not a science, it's an art. How I would approach it would be different to how you would approach it. But being able to leverage AI to come up with a thesis, where do I start? Because there's so much data, there's petabytes of data. Sometimes when you're doing threat hunting, you can go down a path for a day and you get nowhere and then you have to start all over again. 'Well, where do I start?' As I said before, you start in a different place than I would. That's the evolution of the SOC, the evolution of the threat hunter. I still believe a threat hunter is not an entry level job. You definitely want to promote the ranks to do that, but you have to learn. The power of AI will make that happen a lot faster.

"When you start looking at the gap, the gap is really based on the information you have. Do you have a clear picture? When you look at a lot of detection technologies, they're looking at north-south traffic. What I mean by that for those that don't understand is traffic that's coming from the internet into the organization. Now where things get tricky, where a lot of your, I would say, critical assets and critical infrastructure are going east-west."

AI Incident Response Gap

ANNA DELANEY: One of the challenges we hear about is turning AI outputs into actionable, clear insights for incident response. What's your take on that gap?

JOHN PIRC: The gap on that is being closed. We have an IR team. I work with the men and women on our IR team, and they're absolutely closing that gap by using different types of technology, different type of analytics. When you look at the gap, the gap is really based on the information you have. Do you have a clear picture? When you look at a lot of detection technologies, they're looking at north-south traffic. What I mean by that is traffic that's coming from the internet into the organization. Now where things get tricky, where a lot of your critical assets and critical infrastructure are going east-west. How do you see into that? You have endpoint detection and response that can feed up. We talked about a central platform where you can do all that. I really think that gap, based on the technology or instrumentation that the customer has, does provide that clear picture to an IR team. There's really no difference in my perspective. You have a threat hunter that's looking at something, but incident response teams are taking everything into play. Again, we started off before garbage in, garbage out. It's making sure that you have the right telemetry, the right information and the right time slices that you need to be looking at.

ANNA DELANEY: How are you at NetWitness helping customers tackle all these threats and challenges that we've been talking about?

JOHN PIRC: Our platform is one single platform where we're able to feed in NDR, so network detection and response, which is packet data. Our SIM, which we pull and log data. We have UBA, so analytics. I talked about how analytics are really important. Obviously going down the AI route as well. We have SOAR, so Security Orchestration and Automated Response. What that means is we're seeing an attack happen, we need to take that host offline, so being able to be proactive. Then our vision on where we want to go with having an autonomous SOC drives that forward, which I think is really important. Then we just recently had a partnership with a company called BforeAI, which involves all this predictive, 'in the future we're going to see X, Y and Z' AI-related responses. I'm super excited to be part of NetWitness and growing out this team.

NetWitness provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats.

For more information, visit netwitness.com.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifi cally tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to fi nd actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach Prevention. Response. Notification. TODAY CyberEd.io

CIO.inc DeviceSecurity.io PaymentSecurity.io FraudToday.io

CYBER THEORY CyberEdBoard Xtra mile LIFECYCLE MARKETING GREYHEAD

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io