



In Conversation

In Conversation with Rob Demain

Carol Baker

Research by e2e-assure reveals over 50% of organizations now expect their Operational Technology (OT) to be targeted more than any other, but with their ability to monitor and protect their environments uncoordinated, organizations are lacking the resilience to respond and recover from an attack. As the race to secure critical infrastructure continues, we talk to Rob Demain, CEO, e2e-assure about the challenges OT environments face and how organizations can prepare for an attack while keeping downtime to a minimum.

Rob Demain
Founder and CEO
E2e-assure <https://e2e-assure.com/>

Rob has 20+ years' experience in building SOCs for large corporations and organizations, including telcos, financial institutions, national public sector, and defence organizations. Rob believes the traditional SOC was focused on inefficient, sporadic spend on technology at the expense of people and process.

Rob founded e2e on the premise that technology should be there to support analysts, but not dictate their behaviour to them. This led to the development of e2e's SOC-as-a-service platform built for analysts (Cumulo).



Tell our readers a little about yourself.

As the CEO and founder of e2e-assure, I have been running the company for about 13 or 14 years. My background in cybersecurity dates back to the late 1990s giving me nearly three decades of industry experience. Outside of tech, I enjoy challenging outdoor activities, especially riding vintage, pre-electric start motorbikes.

Your recent research shows that 51% of organizations now expect their Operational Technology (OT) environments to be targeted more than any other. Why has the "bullseye" shifted so significantly toward OT in 2026?

Traditionally OT systems have had the luxury of obscurity – being offline meant many people didn't know what the system was used for, let alone how they worked. But as OT systems become digitalized, they moved online. As such, they become more viewable to the attacker – and the impact can be huge. We now see ransomware groups carrying out very focused disruptions, which have far more impact than data theft.



In Conversation

If your job is to manufacture something, then any production stoppage – whether it be for an hour, minute or second – can come at a very big cost impact. Operating a just-in-time production line means that any failure in that production line costs a lot of money very quickly. Of course, attackers will want to hit where it hurts, therefore they see the key bullseye as being, "if we can stop them making the thing they need to make, that is going to cost them a lot of money, so they are more likely to pay us a ransom if we can achieve that."

You've mentioned in the past, that the cost for attackers to compromise systems is going down while their speed is increasing. How is this "affordability of attack" specifically impacting critical national infrastructure?

There are a couple of key things here. Previously, if an attacker wanted to break into a system in critical national infrastructure (CNI), it would take a lot of skill, time and patience to find the right type of vulnerability, and exploiting it could take months or even years. But with the advent of tools like AI, it's becoming a lot quicker and cheaper to reverse engineer key technologies and it automates much of the workflow for the attacker.

With the rise of state-sponsored "pre-positioning", how should OT leaders differentiate between a dormant presence in their network and an active, destructive threat?

A long-term motivation in espionage was to listen into what's happening, learn, copy intellectual property, etc – that has now shifted. What we are now seeing is a worrying trend emerging – one of destruction. We saw that in the recent attack in Poland, where it looks like the motivation was destruction, not eavesdropping.

So, if the attacker's goal becomes destruction then that could have a massive impact. For example, rather than understand how a power system works, the attacker's motivation changes to how can it be turned off, that has a very different impact. Organizations must think much more about resilience and recovery. After all, it takes a different mindset to address how you are going to make sure you can fix it if the whole thing is completely broken.

How has the convergence of IT and OT erased the traditional "air-gap", and what is the single most common entry point you're seeing today?

There has definitely been a change. Traditionally these systems possibly didn't even have the IP address or connectivity to function as an IP connected network. Then they became IP enabled and became like normal networks, but often these weren't connected to the internet in any way. This is what we call the 'air gap', and sometimes it's a complete air gap, which means that the only way to access the system would be to physically go in the building, and into the room, to use the system inside.

Then as OT systems developed, they needed to rely on IT much more. For example, in manufacturing, if you want to build a car, you need a specification for a



car. That specification would have been inputted into an IT system and then transmitted to OT – and that needs a connection, otherwise it takes too-long, so the commercial imperative is to make things faster and digitize. You then have IT and OT connected – sometimes in a secure way, but at other times, that connection may be less secure.

e2e-assure recently launched a 24/7 Unified IT/OT Detection solution with EmberOT. What gap in traditional SOC models does this partnership bridge for industrial clients?

Players in the market are often a specialist in IT or a specialist in OT, but often the two don't meet – at e2e-assure we converge the two. In an organization, it may be that the OT itself is never actually attacked, but that IT is so badly impacted that OT can't work because it needs information from IT.

At e2e-assure we are obsessed with being able to detect the attack as early as possible, because the quicker we can detect the attack, the less impact it will have. If the attack is coming from IT, we need to be able to ensure it can't get all the way to OT, but also vice versa, because, potentially, suppliers could bring a threat the other way. So you have to have a service that can look at the thing holistically. If you are looking at one piece in a silo, you're going to miss the bigger picture – and I think that big picture, that whole end-to-end vision of monitoring the system, is essential. That's why we have launched 24/7 Unified IT/OT Detection and Monitoring that uses EmberOT's specialist sensor technology.

EmberOT's sensors deliver continuous insight into status, vulnerabilities and threats, helping organizations address potential risks and protect industrial systems and critical infrastructure. The sensors will help customers reduce alert noise through false positives, decrease detection times, and increase asset visibility. Combined with e2e-assure's expertise and deep subject matter knowledge, this solution means customers can get ahead of threats and build resilience into a proactive cybersecurity strategy.

With e2e-assure taking a 'defensive cyber' rather than just passive monitoring approach, how does your proprietary Cumulo platform help analysts move from "alert noise" to "actionable intelligence" in an OT context?

Normally, you could do a penetration test, probing and attacking the system to see if it is safe, but you can't really do that when it comes to OT because the risk of breaking something is too high. This is why we use a digital twin analysis system, using AI and machine learning, to create a digital copy of the environment through which we can safely and proactively run threat scenarios.

How does "protocol-aware" monitoring (supporting Modbus, DNP3, etc.) differ from standard IT traffic analysis?

The depths of analysis are really important. With OT, you can't rely so much on threat intelligence as you would do in IT. In OT, there isn't such a reliable method of



In Conversation

knowing that a threat exists. For example, in IT, if a threat is identified by an IP address that's a very easy thing to understand. But in OT, the threat's probably not identifiable by an IP address. So if you want to go below that IP address, you will need to understand what the IP address does and how it communicates at a payload level.

By looking at the actual instructions in the OT protocols, we could say 'this field device normally sends a request to this controller at three o'clock every day'. That request is normally this many bytes, and it normally has this in its payload. That's a lot more detail than just the IP address. With OT, the lower that you can get down into that instruction set and payload, the better you can analyze an event.

So when you're looking at nation states attacking OT, you're not going to have the threat intelligence to know what it is they're doing. You can't assume you are going to be able to find them. So the way you look at them is by looking at changes in the underlying activity, and the deeper you can get into that underlying activity, the better you can detect the presence of something changing that shouldn't have changed.

In OT things are very, very regular. Patterns are very regular and consistent. So you are looking for any change in those patterns, and if you can go to a payload level and say, 'why has this field device just sent a strange request to this other device? That is not normal.' So you have got to go beyond the firewall logs right into the payloads, and that's what we do at e2e-assure.

How can organizations leverage passive visibility to build an asset inventory without the risk of "knocking over" sensitive legacy systems?

This goes back to the digital twin. We believe the key task with OT monitoring is to do it as safely as possible. With passive monitoring you are capturing the observable evidence from the system in a secure way so that you are not putting a device in the way of the traffic. You are looking at the system as it looks right now, and then copying everything from it into a passive observable layer. Once you have that layer, you can then identify assets in it by the nature of the communications you see within the traffic. That's how we do the asset management and discovery. It's automatic, working out what things are by the very nature of the protocols they are using. It is also using identifiers like the Mac address, or the host name, or the types of traffic. For example, we know that it is a Windows server because it's got Windows traffic, or that it is a PLC because it has got Modbus.

That passive observable asset discovery is a fundamental building block of everything in OT. Without asset management you can't understand anything. Then the digital twin enables us to leverage that data to different types of analysis so we can do more advanced AI activities with it.

The concept is to get a copy of everything in real time at a very deep level, then use that to infer what's going on. A fundamental building block of any cybersecurity program is knowing what you're defending.



You recently stated that OT security in 2026 is about "protecting uptime, not just systems". How should a CISO's KPIs change when the cost of downtime can reach millions per hour?

In OT there is a lot of great compliance and governance coming in. But the message I'm trying to articulate here is that if there is a data breach, it's terrible and compliance failure is bad, but if you go offline, it's worse. It's a mindset shift that needs to go all the way from the board.

People often talk about cyber attacks as, "Oh no, we've lost some data. We've had a data breach." That is not really the key business problem for OT – it's availability. And I think that needs to be reinforced at a board level.

The recent attack on Jaguar Land Rover is a case in point. No doubt there were lots of data stolen, but that's not the business problem they faced. The attack meant that they weren't able to make cars.

Security teams need to be talking to the board effectively about what the real impact is, and the really big impact in OT is always availability. Therefore, you have got to really adjust all your cyber security to go, "the real threat here is it something that wipes out our availability."

In an attack, the instinct is often to "pull the plug." What are the dangers of an IT-style response in an OT environment?

This comes back to mindset. You need to make sure you don't self-cause the problem that you are trying to prevent. If your response plan goes, "Oh, well, what we will do is disconnect IT from OT, then turn it on again" then you are likely to find that everything breaks because it's never really been turned on and off before. This causes a cascade of problems and suddenly you don't understand what you are causing.

Ultimately, you are causing an outage yourself just by trying to stop the outage that you are worried about. So the mindset has to shift into maintaining availability. Today, there are so many dependencies and interdependencies in systems that cutting things off can actually be a disaster.

I have seen a situation where there was a cyber attack and the security team's approach was to cut off the internet and disable a lot of the authentication. The knock-on effect was that all the Wi-Fi went down in all the factories, offices and sales areas. Then the doors wouldn't open because it needed the Wi-Fi. Then the tills wouldn't operate because it couldn't do sales because the Wi-Fi, and the Wi-Fi needed the internet, and the Wi-Fi needed the authentication. So all of a sudden they were locked out of showrooms and locked out buildings because the building system wanted to get authenticated.

The days of pulling the wire are long gone – everything now is so much more interconnected.



In Conversation

How should organizations evolve their recovery strategies to ensure that “restoring from backup” doesn’t just re-introduce the same vulnerability that caused the outage?

Attackers know about backups and a decent long-term attack will be designed to pollute backups to make sure that they don’t work properly, or they reintroduce the problem when they are restored. A lot of the time, what we see is that when attack takes place, the backup system doesn’t work because it needs a network, or it needs DNS, or it needs authentication, or it’s in the cloud, or it’s been disabled as part of the attack.

The other thing is, organizations expect to have an operating system available to restore to. But a disruptive attack will wipe the computer out so it’s not booting. Therefore, you cannot restore it without physical access to it, putting something inside it, rebuilding it in some way. At this point, the backup strategy changes into a restore from bare metal strategy.

It becomes, “Right, we might have a booting operating system. Now who’s got the firmware?” “Who can restore it?” “How do you do that?” “Is it USB?” “How do you get it on?” It becomes all about how do you physically fix systems, not how do you fix them over the network.

How can CISOs better communicate the return on investment (ROI) of OT security to a board that sees it only as a “cost centre”?

I think this is really the proverbial problem in all cybersecurity cases. Most organizations want to do the right thing and boards want to be responsible and have proper governance. So we always say to them, you have to get a board discussion going around about how “good cybersecurity practice is good business practice”, and “good cyber resilience is good business resilience”. You need to be a good and profitable business to maintain your clients, and you’re not going to want to get yourself in the news so build cyber as a key business priority that’s a non-negotiable.

Looking toward 2027, if a manufacturer could only invest in one single improvement to their OT security posture this year, what would you tell them it should be?

Implement a passive observability platform that will ensure secure, real-time data collection in both current and new OT networks. By integrating this into your OT system design, you maintain control over valuable insights, regardless of vendor or service provider.

Any closing thoughts?

A lot is changing very quickly in this space, and there’s a lot of catch-up work to be done, so it’s important that organizations don’t underestimate the significance of the changes. AI is making it easy to understand OT, but it is also making it cheaper and easier for attackers to exploit. Clearly, the impacts are huge. There are many factors, geopolitical and others that are contributing to the threat landscape – organizations have never been a bigger target than they are now.