Threat Actors Are Targeting SAP. Are Customers Ready?

Juan Perez-Etchegoyen
CTO
Onapsis

For years, a prevailing assumption in the SAP ecosystem held that threat actors didn't know enough about SAP to target it directly. That assumption took a serious hit in 2025, when CVE-2025-31324 revealed a zero-day campaign involving a payload specially crafted for SAP—one that required deep knowledge of SAP applications and Java deserialization to build. It was, as Juan Perez-Etchegoyen describes it, the "biggest myth buster" the community has seen.

As CTO of Onapsis, a position he has held for nearly 15 years, Perez-Etchegoyen oversees the company's security research efforts, working closely with the Onapsis Research Labs, whose joint vulnerability research with SAP has helped strengthen security across the entire SAP customer base.

When CVE-2025-31324 hit, his team was among the first to identify the severity, share threat intelligence with SAP, and help SAP push patches to customers. In many cases, this helped organizations get ahead of a second wave of attacks that caught slower-moving organizations off guard.

In an interview with ASUG, Perez-Etchegoyen discussed how the SAP threat landscape has evolved, what customers still get wrong about securing cloud and hybrid environments, and why the organizations that treat security as a transformation priority—not an afterthought—tend to move faster.

This interview has been edited and condensed for length and clarity.

Q: From where you sit, how has the cybersecurity threat landscape for SAP environments shifted over the past few years, especially as more SAP customers move forward with cloud transformations?

It has definitely evolved or shifted in a number of different ways. One, from the perspective of the attackers or the threat actors. A couple of years ago, we were monitoring attacks and exploitation of SAP vulnerabilities, and it was fairly stable. Here and there, we were looking at specific, pointed campaigns, some exploitation, some incidents, of course. There have always been internal incidents where there's an insider or some more complex scenarios, but the mass scale wasn't really there.

But over time, we started seeing more and more mass exploitation of SAP applications. Threat actors are upping their game with a good understanding of SAP technology, of how to exploit and compromise systems, and of how to profit from it—by deploying ransomware, exfiltrating data, or performing financial fraud. More and more threat actors are targeting SAP directly, whereas in the past, they targeted other technologies that were more massively deployed. We know SAP is very pervasive in large enterprise organizations, but it's not as massively deployed as other technologies. So that's on one side.

On the other side is really how SAP technology has been evolving. Ten years ago, most SAP customers were running on-premises behind the firewall with little connection to the outside world. That has changed with the rapid adoption of cloud, the push

from SAP towards embracing cloud applications, public cloud, and transitioning from solutions that were only available on-premises to serving those same solutions as public cloud SaaS applications.

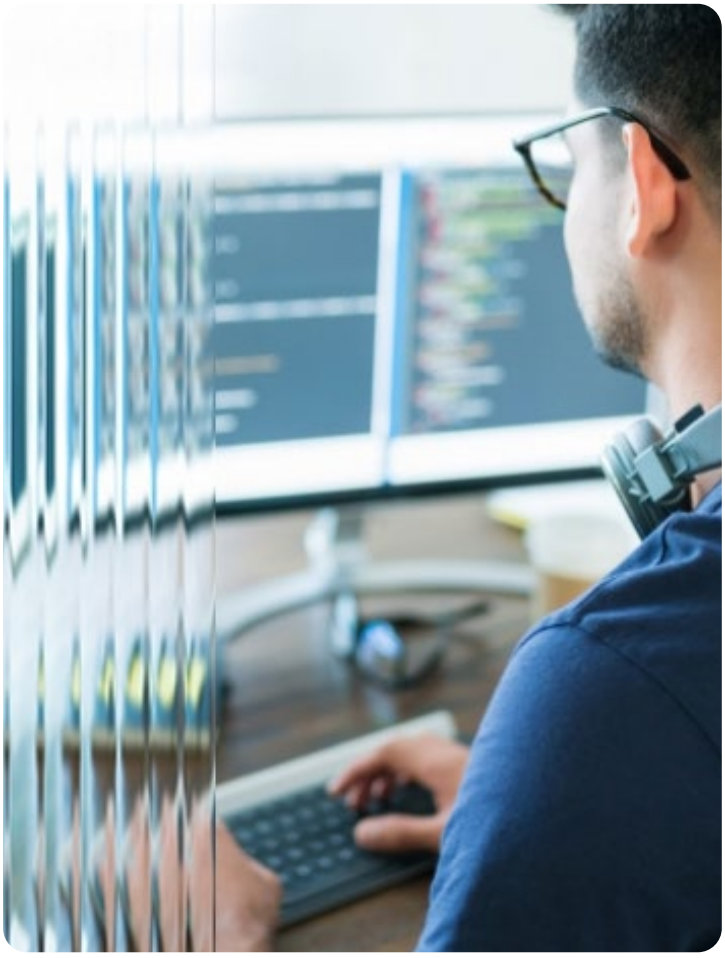
All of that transition led to organizations running completely hybrid environments where they have some systems on-premises, some systems in private cloud, some systems in public cloud, all of it interconnected through SAP Business Technology Platform (BTP). It's a very fast pace of adoption, and that's also increasing the attack surface. From those two perspectives, it has been changing a lot.

Q: What kinds of threats do you think SAP customers are most likely to underestimate right now? And why do those risks tend to slip under the radar?

I think the biggest misconception—and it's slowly changing—is that threat actors don't know about SAP and don't target SAP. With CVE-2025-31324, we saw massive exploitation of a zero-day with a payload that was specially crafted for SAP. That is showing that threat actors do know about SAP and do target these applications.

Underestimating the fact that these applications are under attack is probably the biggest problem. If you don't think that those applications are under attack, then you don't deploy the right controls, the right monitoring. You don't react fast enough until it's too late, because these are heavily regulated applications—our crown jewels, in most cases—which organizations are mandated to protect.

Connect with Juan Perez-Etchegoyen on LinkedIn



Q: How do you advise organizations to think about SAP security as part of a broader enterprise risk management framework, as opposed to treating it like a more traditional IT security domain?

The opportunity we have here is that organizations have been, for the past couple of years, constantly running through migration processes. RISE with SAP, moving to the cloud, and that's still ongoing. That's a perfect opportunity to put security front and center at the very beginning of these projects, driving the requirements and all the actions afterwards. We can plan and put a project together and really integrate security with our vulnerability management initiatives, incident response, continuous monitoring, and all of our DevSecOps initiatives.

All of those elements still have to happen to really run security efficiently across the organization, SAP included, but the unique opportunity we have today is that we are already initiating and pushing projects that will migrate SAP applications, regardless of if it's a lift and shift or a completely new implementation. Deploying new technology, migrating into new environments, and adding security there as a requirement at the very beginning makes a huge difference.

Q: As SAP customers migrate to S/4HANA, whether through RISE or hybrid architectures, how is the shared responsibility model around SAP security changing?

That has been a topic of debate across many customers for the past two to three years. Starting about a year ago, I would say there is much more transparency and understanding between SAP and its customers around this shared responsibility model. But there have definitely been a lot of hiccups along the way.

In the past, SAP customers believed SAP would do everything in regard to security, so they didn't need to worry about it. The reality is that's not the case. There is a shared responsibility model. SAP will deal with a lot of those processes and responsibilities, but there is a huge part of the responsibilities that are still on the customers.

Understanding that is important so you can actually accommodate your processes and your controls, and you don't have unmet expectations, as we have seen in many cases where, after the deployments happened, "Hey, but you told me that this was covered," and now we know that it's not, and then this back and forth with your provider.

So now there's much more clarity and much more transparency. And it's important: user authorizations, patch management, configuration management, most security-related aspects at the application layer are still the responsibility of the customer. Everything below that—OS, parts of the database and the infrastructure—is transparent to end users, managed and secured by SAP. But the application layer is still something we need to take care of. We are still accountable for ensuring that those are secure, and if something happens, it's going to be our responsibility as customers to address that.

Q: Threat intelligence gets discussed in the abstract a lot, but from your experience, what does actionable threat intelligence actually look like in practice when you're talking about SAP environments?

Threat intelligence can be many things. It's a concept that involves being able to capture signals that indicate how threat actors are behaving or evolving, if there has been a compromise, if there are conversations talking about a specific vulnerability or a specific incident, or if there are TTPs or IOCs—tools, techniques, procedures, or indicators of compromise—that should used to identify threat actors, and that we can use to detect them in our company.

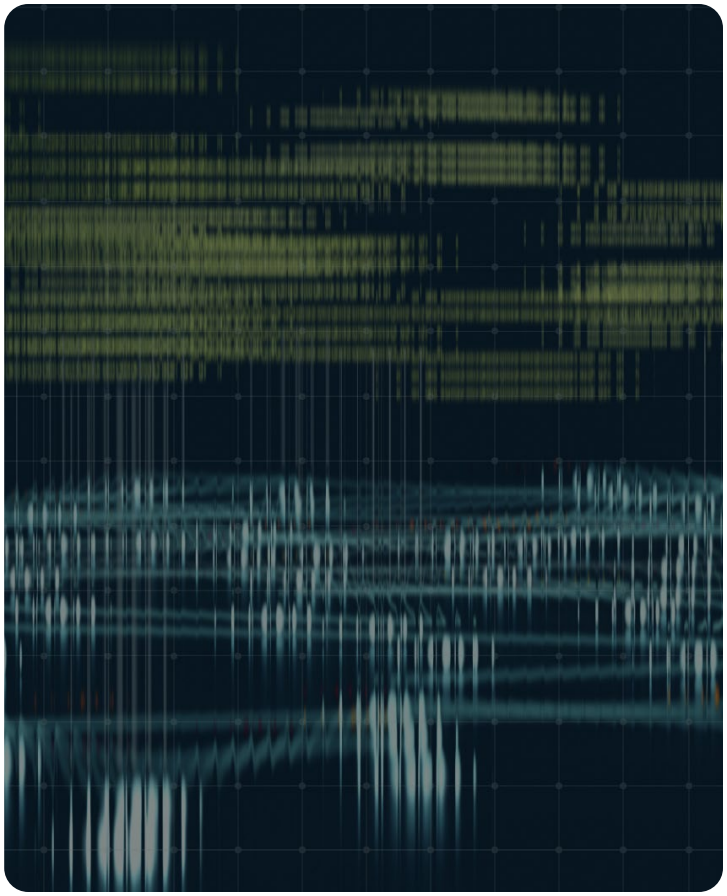
In the context of SAP, threat intelligence is really all about being able to prioritize. What are the vulnerabilities? What are the risks? What are the threats that are most timely today? Because we know that there is friction when it comes to changes in SAP environments, for many reasons, especially in heavily regulated industries.

The reality is that being able to upgrade the kernel in a production environment is a huge ordeal for organizations. So if we have the right threat intelligence allowing us to prioritize: "Hey, this is something you need to look at immediately because it's an active threat that could pose an imminent threat to your organization" versus "Yes, this is important, but you can use your existing processes and take some time to apply this security note or change this specific parameter on the system," that's what allows you to make better decisions and use your resources more efficiently.

Q: Onapsis Research Labs is widely recognized in the SAP security community. What is its mission, and why is independent SAP security research especially critical today?

We share a mission of securing SAP applications with SAP itself, at its core, ensuring that the services and products they offer are secure and delivered securely to customers. By the joint work we do at the Onapsis Research Labs, analyzing SAP applications and reporting security vulnerabilities and potential improvements from a security perspective to SAP, and SAP releasing security patches out of it, we effectively help elevate the security of SAP products across the world, across the entire SAP customer base.

Now that we know that many threat actors are targeting SAP, being ahead of them, fixing those vulnerabilities together with SAP, and preventing compromises are super important today, more than ever.



Q: Could you walk us through an example of how those insights have helped an organization get ahead of an emerging threat?

I can give you a very recent example with CVE-2025-31324, which was last year. It was a zero-day campaign. Right after the first patch release by SAP, I think it was on a Thursday, we started getting in touch with our customers. Within a matter of hours, we released support on our platform to all of our customers and started notifying them. The customers who took that and were able to quickly react prevented a whole second wave of attacks that happened over the weekend.

We made it very clear to all organizations: “Hey, this is critical, this is timely, we need to react because it’s an active threat being triggered by threat actors.” Because of that, we prevented many additional compromises that happened afterwards. And we heard of organizations that weren’t as quick to react, and they got hit after this second wave.

So that’s why time is important, quick reaction is important, but this is all driven by the right threat intelligence. The Onapsis Research Labs were uniquely positioned on this CVE because we were able to see what threat actors were exploiting and actually help SAP. We shared with SAP our threat intelligence, so they came up with another patch fixing the root cause of the vulnerability. From the get-go, we started warning everyone about the criticality, which was effectively confirmed right after that.

Q: Where does Onapsis fit within SAP customers’ broader cloud and cybersecurity strategies, both for organizations still running ECC and those operating in an S/4HANA landscape?

We’ve been in the market for over 15 years. We started supporting the older versions like ECC, even older NetWeaver versions, all the way to the newest S/4HANA, BW/4HANA, all of the latest flavors of SAP ABAP-based solutions, and other solutions as well.

As SAP technology evolved, we have been evolving, so customers can use our technology to protect their entire landscape, if they have on-premises, potentially older systems, and if they have newer S/4HANA or any newer product deployed in the cloud.

Q: As attackers become more sophisticated, what role do you see AI playing in SAP security over the next 12 to 24 months—both as a threat and as a tool for defenders?

I think the key lens we need to apply here is AI—it's a disruptive technology across the board. Threat actors are also leveraging it to have more efficiency in targeting SAP customers and organizations in general.

Because of that, defenders have to be empowered with the right level of visibility around vulnerabilities in SAP, threats on SAP, continuously monitoring SAP, and fixing any issues across the multiple domains that SAP security involves, whether it be configurations, authorizations, integrations, or custom code. Because of how fast threat actors are going, organizations need to deploy the right controls across the board on their SAP landscape.

We are also working with AI at Onapsis, implementing security use cases around AI, basically augmenting the capacity that someone will have when analyzing active threats or active monitoring capabilities on SAP systems, with AI capabilities that allow you to deal with more information in a smaller time window. Being able to prioritize and filter the noise and really take care of what could be really important.

Q: If there's one strategic step that SAP customers should prioritize this year to strengthen their cybersecurity posture, what would it be and why?

Assuming that SAP customers are not addressing security across the board in their entire landscape, I would say it starts with visibility. Understanding what the risks are and having the right visibility into potential vulnerabilities on the system, and also potential incidents that could be affecting the system.

We know that some threat actors are pervasive; they stay under the radar for long periods of time, abusing the fact that SAP systems process financial transactions, and they can profit from it. So I think it's about being purposeful around security and dedicating resources to it.

Visit the Onapsis website

Onapsis is the global leader in SAP cybersecurity and compliance, helping the world's leading organizations reduce business risk, protect revenue, and keep critical operations running as they accelerate their SAP Cloud and AI initiatives. Built for and by SAP defenders, the SAP-endorsed Onapsis Platform enables Cybersecurity and SAP teams to proactively prevent breaches, accelerate audits, and respond faster to threats across RISE with SAP, S/4HANA Cloud, and hybrid environments. Powered by intelligence from the Onapsis Research Labs, Onapsis delivers rapid time to value, measurable risk reduction, and the confidence enterprises need to innovate faster. Connect with Onapsis on LinkedIn or visit https://www.onapsis.com.

ASUG is the world's largest SAP user group. Originally founded by a group of visionary SAP customers in 1991, its mission is to help people and organizations get the most value from their investment in SAP technology. ASUG currently serves thousands of businesses via companywide memberships, connecting more than 130,000 professionals with networking and educational resources to help them master new challenges. Through in-person and virtual events, on-demand digital resources, and ongoing advocacy for its membership, ASUG helps SAP customers make more possible.