From Prevention to Detection: Real-Time Security in a Digital World with Infosys

[00:00:00] **Mohammed:** The future of is an intelligent ERP. The company should not or doesn't have to rely on expensive third-party components, but the ERP should be self-aware and capable of identifying the issues, guiding the customers on fixes, and even blocking attacks autonomously. I envision ERP systems that resolve problems with minimal human intervention, making security and optimization native to the platform.

[00:00:29] **Richard:** Hello, I'm Richard Howells, and this is the future of ERP, a podcast where we discuss hot topics, best practices, and the latest innovations in today's global business. And I'm joined as ever by my wonderful cohost, Oyku.

[00:00:42] **Oyku:** Hello, everyone. I'm Oyku Ilgar, a marketer, podcaster, and blogger in the ERP and supply chain space at SAP. In today's episode, we are joined by Mohammed Moidheen from Infosys to discuss the importance of real-time security in today's digital world. Mo, lovely to have you here today. Could you please introduce [00:01:00] yourself and your organization for those of our listeners who do not know you?

[00:01:04] **Mohammed:** Thank you so much, Oyku and Richard, thank you for inviting me. My name is Mohammed Moidheen. I am an SAP security architect based in Germany, and I work with Infosys Consulting as a principal consultant. I bring over 12 years of specialized experience in SAP security, including the areas of SAP Access Management, SAP Hardening, and SAP. Threat detection and controls, et cetera. Throughout my career, I have worked with organizations such as Adidas, SAP, Security Bridge, and Infosys. I specialize in enabling security frameworks, implementing security controls, and designing security processes that support the digital transformation journeys that help organizations fulfill the regulatory compliance requirements from an SAP standpoint.

[00:01:59] **Oyku:** Great. Let's [00:02:00] dive straight into the question. Why is real-time security monitoring so essential in today's cloud environment?

[00:02:07] **Mohammed:** Real-time security monitoring becomes absolutely critical in cloud environments today because, as we speak, cyber attacks are happening all over the world. In fact, according to the recent global cybersecurity statistics, there are over 2,200 attacks every single day, which means one attack every 39 seconds. And these cyber attacks don't wait. They happen in seconds. Not days, not months, but in seconds. And the scarier part about these cyber attacks is that they have a financial impact on the organizations. So recent reports estimated that global cybercrime is costing businesses 1.2 to 1.5 trillion annually, by the end of 2025, making it one of the largest economic drains. And as per IBM's cost of data breach report, the average cost for [00:03:00] this single data breach is somewhere around 4.4 million globally. And in us alone, it is reaching up to 10 million per bridge. And this is why real-time monitoring matters. It's the difference between catching a threat immediately versus discovering it weeks or months later when the damage has actually multiplied exponentially. To break it down in simple terms, we can think of it like security cameras with instant alerts versus reviewing the footage like a week later or a month later. The first approach lets you stop an intruder in time. The other shows you what went wrong after the break-in. So in cloud environments, I believe this emergency or this urgency is amplified because of the shared responsibility model. The service provider and the customer both need visibility immediately without real-time monitoring. It's [00:04:00] like, you're essentially flying blind. I would say that real-time monitoring in the current world scenario is not a luxury, but I would call it a survival.

[00:04:10] **Richard:** You provided some really eye-opening statistics there. The fact that there's a security breach every 39 seconds means the risk is in the trillions. And you also talked about the difference that cloud brings and the shared responsibilities. So, what are some of the standard security monitoring blind spots that organizations should watch out for?

[00:04:34] **Mohammed:** Blind spots are areas that an organization assumes are covered, but they really are not. Let me share some blind spots in the context of maybe S/HANA Cloud or the RISE with SAP context. Many companies assume that SAP monitors everything- infrastructure, hardening OS database, network, and Hyperscaler. SAP is managed by SAP, but it doesn't monitor the access management [00:05:00] vulnerabilities in custom codes, enabling logging as per the company's audit and regulatory requirements. These are often the areas where risk originates and the customer is responsible for, right? This would be my first example, and the second is collecting the audit logs but not reviewing them. So logs are only useful if you make sense out of them or analyze them. Otherwise, they're just lines or noise. And this is what, as a consultant, I have seen in many organizations in order to comply with audits, external audits,

governance requirements, and internal audits. Everybody enabled the audit logs, but when they're asked, what do they do with the audit logs? The answer is not that great, so this is another blind spot. And third would be ignoring the third-party integrations and API connections. So these are the gateways to your environment, and the attackers know it, and there should be a stringent governance process before any third-party [00:06:00] application becomes a part of your organization. So when I say this, a real-world example comes to my mind in 2021, the attackers exploited an unsecured API in a major financial services firm, which led to millions of records being exposed. Because those APIs were not monitored. And the fourth one, I would say, is not giving extra security to privileged or admin accounts. The privilege accounts, or admin accounts, generally are keys to your kingdom. They have very, extremely high privileges, and they need continuous monitoring enabled. And this is not the case with many organizations. The fifth one I would say would be forgetting about insider threats. Many organizations focus only on external attacks, but insider misuse, whether it is intentional or accidental, in both cases, it could be as damaging. So we should also give importance to insider threats like [00:07:00] we do for external attacks. Monitoring individual events, but not correlating patterns. So a single failed login might look harmless. It doesn't indicate anything, but combined with other signals, this could potentially indicate an attack in progress. So the organization should have some capabilities in place to correlate the events and show us patterns of possible attacks. So to summarize, I would say the organization should think holistically, not just technical monitoring alone, but technical business and behavioral insights are needed to build a truly secure environment.

[00:07:41] **Richard:** There seem to be many points within a business system that could get attacked. And the more integrations you do, the more APIs you leverage, the more the risk increases. And you're only as strong as your weakest link. And sometimes many companies don't have the [00:08:00] staff in place or the skills in place to keep up with all of this. So, how are real-time monitoring systems evolving to take advantage of technologies like machine learning and AI to improve this threat detection?

[00:08:11] **Mohammed:** AI will completely reshape the preventive and detective security strategies over the next few years. To highlight a few capabilities that hold the most promise, first would be predictive threat intelligence. Imagine AI telling you you are most likely to face an attack in 30 days, and here are the reasons why. AI can easily do this by analyzing the global threat patterns and your specific environment, so you can strengthen your defenses even before an attack happens. This sounds great, right? Only AI can help in this area because we have to go through millions of lines of log to correlate and get an insight into this. And AI is very much capable of doing this.

And the next one would be automated threat response. AI is not just [00:09:00] capable of detecting the threats, but it can also respond instantly. For example, if it spots a compromised account, it can lock it, or it can trigger additional authentication and contain the threat. And if this happens in seconds, humans will still get notified, but the damage will already be prevented by AI systems. Next would be natural language security and analytics. This would be a game-changer for accessibility. Now you need consultants or security consultants to analyze the logs and to detect the flaws, et cetera. But with natural language security analytics analysis, the future that AI is offering, you will be able to ask questions like, Show me unusual financial approvals. Show me unusual login attempts. For example, in plain English, you don't need to be a technical expert. Anyone can interrogate the system meaningfully, and this is a cool and promising feature that I see is possible with AI. The next one would be [00:10:00] cross-domain correlation. So I have already explained about connecting the dots and correlating in the previous example. So AI is very much capable of connecting the dots across your IT ecosystem. For example, a badge swipe at 2:00 AM, or SAP login from an unusual location, or unusual traffic on your SAP systems. So, individually, this may not seem odd sometimes. So, together, if you connect the dots, they might reveal a coordinated attack. And AI systems can do this correlation more effectively than humans can perform, and by going through millions of lines of logs from various systems and correlating them. So, AI is not just adding speed; it's adding foresight, automation, and intelligence factors through security. It's moving the whole security from a reactive defense to predictive and proactive prevention.

[00:10:59] **Oyku:** Mo, you [00:11:00] have already given a real-world example earlier. And I would like to delve into this topic in more actual examples. Do you have any cases that you can share on how real-time threat action helps companies respond faster to breaches and reduce damage?

[00:11:16] **Mohammed:** So when it comes to threat detection, speed is the key. So, the industry average for detecting a breach is still measured in weeks, months, etc. And that's a huge problem because every hour a threat goes undetected, the damage grows exponentially. So, real-time threat detection changes the game. It means spotting suspicious activities in minutes, not weeks, not months. Acting before an attacker can do real harm to your SAP systems. So let me share a couple of examples that I know firsthand and from my colleagues. So on a Saturday evening, the monitoring system suddenly went up with an alert that it was usually downloading. Customer data tables are about 50 times 00:12:00 their usual volume and are being done at a time when nobody is actually online. This was a big red flag, and within five minutes, the system triggered an alert, and we logged the account immediately without real-time detection; the person could have spent the entire weekend pulling millions of

records. This is exactly what real-time monitoring brings in. Second is an example that I know from a colleague who is working in the same department An employee who has just been notified of termination systematically accessing competitive intelligence over several days, and the monitoring system pick ed up the pattern, late night access, frequent downloads, unusual downloads, et cetera. threat intel team intervened before the employee could walk away with confidential data. These examples show why real-time threat detection is not a nice-to-have feature. It's the difference between a minor incident and a catastrophic breach.

[00:12:55] **Oyku:** Mo, as a person who's constantly in contact with customers, what 00:13:00 advice would you give organizations to improve their real-time security monitoring?

[00:13:05] **Mohammed:** The first one would be to start with clarity before jumping into tools or alerts, et cetera. Understand your organization's governance framework and the regulations that you need to follow. The monitoring strategy that you are trying to implement with the real-time monitoring systems should be in line with those requirements. Otherwise, you would be just building something without a blueprint. And when it comes to SAP ERP, don't assume that SAP monitors everything. Read SAP SOC reports and create clear responsibility metrics so everyone in the organization is aware of who owns what. That simple step avoids confusion when something goes wrong. Next would be, don't aim to boil the ocean at first, focus on crown dwell systems. The systems and the [00:14:00] processes and the data that matter the most to your organization. If this process of the data was compromised, what would the business impact be? So this question should be able to give you the answer to which systems and which processes to protect you should be focusing on first. So start small, monitor what matters, and expand gradually. And another one would be to set your baselines correctly. Know what is normal, what normal looks like in your environment. Without a baseline, you cannot spot anomalies. AI and machine learning can help in identifying the anomalies. But for that, you need to set your baselines correctly and don't forget the human element. Train your teams, whether they are IT, security, or business users. I would say build a security mindset across the organization. It's not just good for work, but it also helps in daily life. Like how many phishing emails and scam calls we get on a daily basis, [00:15:00] right? So this security mindset would help us secure the organization, but also it'll help in our daily life, to raise awareness that it's your first line of defense. So train your teams, create awareness inside the organization. And finally connecting the dots. Correlate data across the SAP network, endpoints, hr, etc. If you cannot afford a full CM solution, even manual correlation can also help. And you can have incident response, playbooks, runbooks, et cetera, for common incidents.

[00:15:36] **Richard:** We've covered a lot of topics here around the whole concept of security, and obviously you are an expert in this area and people within your organization are also experts. So how can Infosys help companies with their cybersecurity challenges?

[00:15:52] **Mohammed:** Infosys can help you assess your situations, assess your organization security status, security [00:16:00] posture, lay the foundation and build it from there. As I mentioned, foundation building or blueprint is extremely essential. It's not like you procure a tool in the first place, switch on the controls, and build without a blueprint. So this approach is not feasible. Infosys can help you in understanding your regulatory requirements, doing the gap assessments, and laying the foundation and building the security from there.

[00:16:27] **Richard:** Okay, we're coming to the end of the podcast and, we have a standard question we ask all of our guests. From a real-time security perspective, in your mind, what's the future of ERP?

[00:16:39] **Mohammed:** The future of is an intelligent ERP. The company should not or doesn't have to rely on expensive third-party components, but the ERP should be self-aware and capable of identifying the issues, guiding the customers on fixes, and even blocking attacks autonomously. Think of how Microsoft evolved in the 00:17:00 early 2000s. We need separate antivirus packages, software, etc. But today, Microsoft Defender is a built-in proactive feature, which is capable of doing many things. Similarly, I envision ERP systems that resolve problems with minimal human intervention, making security and optimization native to the platform.

[00:17:21] **Richard:** Great summary, Mo. Thanks for a great conversation. It's been really interesting.

[00:17:25] **Mohammed:** It was nice to talk to you as well, Richard, and Oyku.

[00:17:28] **Richard:** For all the listeners, please, Marcus's favorites, and you can get regular updates and information about future episodes. But until next time, from Mo or you and me, thanks for discussing the future of ERP.