

Better Risk Management via Converged Security, IT and Business Expertise

By Sharon J. Watson on August 26, 2009 11:40 AM

AlertEnterprise CEO Jasvir Gill on Creating a Clear Portrait of Risk

For more perspective about what elements enterprises need to fully understand their real-time security posture as well as potential or emerging risks, Sharon J. Watson spoke earlier this month with Jasvir Gill, CEO, and Pan Kamal, director of marketing, for AlertEnterprise.

In addition to real-time event monitoring and automating employee on- and off-boarding, AlertEnterprise literally shows a company its risk. With a click, a business user can drill down to see the precise risk factors associated with an employee and her role and physical/logical access rights, such as access to ingredients in a warehouse plus ability to alter production controls that, in combination, potentially could enable the employee to sabotage the company's product.

This year, AlertEnterprise won the RSA Conference's Innovation Sandbox Most Innovative Company award as well as "most innovative" CyberSecurity and Security Tool at The Security Network's Security Summit, where it was also the runner-up for "Best of Show."

We spoke with Gill (pictured) and Kamal about taking a preventive approach to security, monitoring risk at the enterprise application level, showing end users the value of converged systems, bringing business user expertise to security decisions and more. What follows is a transcription of our conversation, edited for length and clarity.

Sharon J. Watson: Where does AlertEnterprise fit into the security information and event management and physical security information management (SIEM/PSIM) world?

Jasvir Gill: Our solution is used right when people are being onboarded and offboarded, when you're hiring people or changing their jobs and getting new roles, whereas all the SIM/SIEM solutions come much later. They basically monitor what is happening but they are not involved in the whole process of doing risk analysis when you're giving people access.

That is one of our biggest differentiators, that we actually prevent these problems from happening rather than detecting them. Detection is always too late, it's after the fact, the damage is already done, the company's reputation has already been ruined and so on.

So that's our biggest difference--prevention. The second difference is we have the unfair advantage of knowing the real application context. Let's say now I'm hired by Dow Chemical, I've been given access to one warehouse. Let's say I am disgruntled, I've been denied a bonus, or promotion. I try to misuse my access.

If you are just looking at logs, you may not be able to catch me...looking at logs you cannot find what assets have been moved, which assets have been scrapped and so on. That's an advantage we have because we don't look at logs, we look at the actual application transaction context. We say, oh, someone is adjusting inventory for an asset, scrapping this asset. Then we look at what assets. If that asset is an asset that you really care about, a sensitive asset, yes, you want security to be alerted about that. Otherwise, you soon lose credibility sending all kinds of alerts, and they end up ignoring a genuine alert. So those are two main differentiators.

The third main differentiator is giving the business context. Today all the SIM/SIEM solutions are too technical for business people to understand. The business person cannot really understand those logs, they will always have to rely on IT. And many times that becomes an issue, because IT could be part of the problem. If I'm a super-user for a company, and I am disgruntled, there's no way management will be able to catch me. They're going to rely on me to review those logs and really point out the problems--whereas I am the problem.

So providing that business context, hiding the complexity, giving very intuitive pictures of what is happening in a company is very, very important. We're enabling executives, business people, the stake holders to really know, understand the risk. So that is the third layer. We provide the business layer on top of all the risk, something that business users can understand, can take action on. So they can say by giving Jasvir this access, this is the risk we are taking, and they can basically remediate the risk right there.

SJW: Let me go over some of this to make sure I understand. You look at the actual application, an actual asset. From what vantage point? Where are you plugged into the enterprise network to do that?

JG: What we do is interface, we call it the adapter framework. We can connect with all different business applications, like SAP, Oracle, PeopleSoft, JD Edwards and so on. We built an adapter framework to connect with them, and our rule engine has the intelligence to look at the sensitive transaction context.

So let's say you worry about somebody making payments. Processing payments is one of the big things. You could be creating a fictitious vendor, paying them a few million dollars -- that's how easy it is to do a fraud -- and retire. All you need to do is one transaction.

We were talking to a company....they told us this kind of fraud was going on with the company for a long time. Guess how they found out? They found somebody working, processing payments, with a very fancy lifestyle who retired early. The person didn't feel they needed to work any more because they made so much money doing this.

But if you're just looking at logs, you say oh, you process millions of payments every month, now you're sending a payment, you're processing a payment. That payment is made to which vendor? Is it a real vendor or is this something fake, a one-time vendor someone created? So we can act with applications to identify those kinds of scenarios, those kinds of problems.

JW: So while you are very strong in preventive measures, you are a real-time monitoring solution as well.

JG: Yes, absolutely.

Pan Kamal: SIM and SIEM work very well when you're looking at threats from the outside, the presence of malware on the network, worms, hacker attacks. Incident management tools and security automation tools have a very valid place in the organization. But what they deliver is very arcane-looking text reports, lines and lines of text, very technical numbers and characters. The business function requires a security expert to look at that and tell them what it means.

JG: It is not that we are trying to undermine the SIEM solution value. They have their own value. I think your question is, do people see the value in physical and logical security convergence.

SJW: Right.

JG: They really don't see the value if you just do the technical integration or just look at the surface or network-level issues. They see the value if you show them.

I'll give you an example. You have an employee who has been denied a bonus or promotion. Now all of a sudden you see a change in behavior of that employee--if you see it at all [because it's not just an IT system]. That's HR, we connect with HR and we see, oh this person has been denied a bonus, and all of the sudden he or she is going to the control room in the middle of the night where before she always worked from 8 to 5. So there is a change in the behavior that could be a potential threat.

So when we technically integrate IT with physical, [business users] feel, so what, what's the big deal? But if you show them these kind of examples, it's -aha! Because this risk--there's no way you can find it if you don't connect IT and physical security.

SJW: On the physical side, what are your natural connection points? Do you want to see a PSIM solution in place or just work with the disparate systems people have?

JG: We can do both. The adapter framework I was talking about can connect with an ERP system, applications, physical access control systems. Or if they already have something in place, certainly, we can connect with that. Same way on the application side, if they have some kind of middleware, we can leverage that.

PK: We have the ability to take live video feed from existing video surveillance cameras, pull that in. We have the ability of either automating, so that if an incident occurs in some part of a building, there is an automatic video switch over, or it could be on a command prompt that says let's go look at this video. Because we have interfaces to building automation systems, etc., we can actually create tags on the screens that allow you to click on the camera, look to see what's going on and if you see some suspicious activity, you could in fact lock the doors by going through the building automation system.

JG:The solution can automatically inform the first responders, police, whatever. You can configure the system so it's not only about finding alerts and problems. It's also real command and control and incident management.

SJW: You've spoken a number of times about making that event data, the risk data, intelligible to business users. When do the business users see that data? Are they looking at it on a day-to-day basis?

JG: It's mostly when you when you hire someone. When the manager hires someone, our solution finds the risk of giving some access to a person....If you provide that whole picture of the risk analysis in a way that is intuitive to them and they see the risk they are taking and of monitoring or mitigating controls they can have in place, then they are enabled to do this on their own. Leaving all of that to IT is just not practical, it's just not sustainable. That is where I think intuitiveness really helps.

Also there is now...user access review is a new audit requirement--[done] every few months, depending on the criticality of the roles. Your super-users, you have to review them every month, you have to see the access they have and whether it's needed, because many times you give people a lot of access.

Now imagine you are a business user. There is no way you will understand the

technical language of security. In SAP, security is very different; in Oracle, it is different. Understanding authorization objects, fields, values, responsibilities, menus, there's no way you'll be able to understand it. So you have only two choices: One is that you just ignore it; secondly, you just trust your IT. My IT must be doing a good job. This is not a good thing to do.

....The problem that is there today is that when companies find the risk, you need business and IT to sit together to resolve it. IT cannot work on its own because IT doesn't know. If they removed somebody's access, they could actually stop businesspersons from doing their jobs. Then business gets very upset: how dare you remove my people's access? They have not been able to process 10 transactions worth \$5 million. You've ruined my day.

So IT is really scared of taking somebody's access away. They want to be good guys.

Now if somebody is demanding access, saying 'I can't do something, I need access right away' and IT gives that access, that access could also be misused. How do you solve this problem?

Let's say you find 500 violations. Imagine making IT and business sit together to solve all of those problems. People are working remotely, everyone is busy, all of those meetings are impractical. So you need a solution that business and IT can understand, and they can work separately at separate times. So business looks at the problem and says 'oh, I understand what the problem is, take this access away.' They find an action that goes to IT, and then IT takes that action. This is done at separate times. They don't need to sit together to resolve every problem. What we are doing is providing them a platform, one picture, one visual, that both teams can understand and can use.

SJW: What about the physical security professional? How often do you get involved with them? What kind of value does this sort of correlation of events provide to them or how does that get more value out of what their systems can do?

JG: We talk to them all the time. They see a lot of value in a number of ways. One is the visuals: they say today to get this information that you just showed me in one picture in one second in one click, it could take me about a week to two weeks to get that information. So that whole process is very frustrating.

Secondly, [they say] the information I get will probably be 10 pages for one user for all the access they have, the text is very hard for us to understand and by the time we get the information, it could be irrelevant because it could have already changed. So that's one value they see: providing information at their fingertips anytime you want to know who has access to your control room, to your SCADA systems, in a picture that they can understand rather than with some numbers

and schematics.

The second thing see the value of when they integrate IT and physical...the moment a person is laid off in the HR system, you have a trigger: it can automatically deactivate a person's physical access right away, instantly. That's a big problem for companies. Somebody is leaving on a Friday. If [security] doesn't hear from HR for a few days or a few weeks, the person's access is still active.

We went to one customer where we found they had 2000 active access badges for people who had already left the company. Some were employees, others consultants--2000 active badges because IT and physical are not connected.

PK: It turns out that is a very common problem. There is a Ponemon Institute research paper on this kind of access, and what they're saying is that when companies terminate employees, they may turn off their IT access--your e-mail doesn't work anymore, which is good--but 63% of those companies take at least a week and maybe up to a year to turn off their physical access. It's because they are disconnected and in silos and they're completely separate systems.

SJW: Given that so many physical access control systems don't communicate with each other, and people are provisioned by physical security people into a number of systems, how can your solution address turning them off in all those different physical systems?

JG: One is that most of these different systems follow a standard, and we also follow a standard, so we can connect with most of them using the same standard interface. All of these solutions provide you capabilities, APIs, to activate or deactivate someone's access, so it's actually not that difficult to do. The technical part is fairly simple.

As for the homegrown systems -- we have been in countries where we came across customers who had all these legacy systems, homegrown systems, which don't really follow any standards. These are file-based systems, they store all of the data in files. We don't interface to those; we provide the flexibility where you can do easy configuration, mapping of fields. There are really about 8 to 10 fields that are relevant for this whole thing, who this person is, what kind of access they have, to which facilities, from what time to what time, and so on. We can map those fields; without any programming, we can connect with those. Those connections are not that difficult.

The difficult part, the complexity is the data that you have in all these different systems, the transactions, the domain knowledge: How do you look at that data, how do you analyze it, how do you really determine what is a real risk or not. That's the real difficult part.

SJW: What should I be asking about pulling physical and logical event data together to get a really comprehensive picture of your security risks and

managing security?

JG: I think one of those questions is scalability. A lot of customers feel that their environments are too complex, they ask how would you scale, how would you connect with all of these different legacy systems....This is one of the biggest questions everyone has, I am living with a lot of legacy systems, I haven't even really solved IT problems, I haven't solved physical problems, how can I do both? You're talking to me about going to the fifth grade right from the first grade.

...I challenge them. I say, so you are telling me that you failed to solve this problem and that means you don't want to do anything? Not doing anything is not a good strategy. So when we talk to them about going in baby steps. First let's solve your IT problems, find the risk in your IT systems. Then let's go beyond IT to physical, to IT and physical and industrial control systems.

SJW: The kinds of companies bringing these issues to your attention--are most of the people interested heavily regulated or have especially sensitive data or materials?

JG: One is the people who are hit by the mandatory regulations. They definitely want a solution because otherwise there are very heavy fines. Second are people who are really worried about their companies' reputations, and they really see major threats. Imagine bioterrorism. Take a [major beverage company]-- somebody messes around with their SCADA systems, their control system, so that it turns off a preservative. The end product could be contaminated, a few people fall sick--imagine the damage to their brand. So some of the companies really worried about the potential damage to the company's reputation are willing to invest in this space.