Working to be stronger

Many companies in the Middle East are missing out by not gaining valuable intelligence from threats. Security information and event management (SIEM) has arisen on the enterprise scene as the latest must-have in not only protecting your business environment, but providing you with tools to analyse each threat. Ben Rossi dissects the ins and outs of SIEM.

When it comes to figuring out how many organisations in the Middle East are engaging in active SIEM, it's no easy feat. Companies are notoriously, and understandably, reluctant to reveal any information about their security environments. As a result, when industry experts are quizzed on the subject, answers are quite varied.

"Around 25% and that will double this year," says Jude Pereira, MD at Nanjgel Solutions.

Bulent Teksoz, chief security strategist at Symantec, reckons more. "I think most of them right now either have a project running now or are thinking about running it," he says.

Simon Carvalho, principal security architect at Paramount, draws upon the company's personal work in the field. He claims that Paramount was the first to introduce the concept of SIEM to the market in 2005 and in the last seven years has done around 30-35 implementations.

"I would say there have been about 150 SIEM implementations in organisations from the Middle East. In terms of the number of organisations that have engaged in a true

active SIEM in the right manner, I would say probably only a handful, very low – less than 5%," he says.

Explosion

SIEM's name derives from the convergence of the formerly disparate products of security information management (SIM) and security event management (SEM).

"It's a centralised security monitoring technology where you can have all threats and risks defined in a single location. With SIEM you can rely on the single platform to understand your threat risks and security levels at any given time," Pereira says

Nicolai Solling, director of technology services at helpAG ME, refers to the "explosion" of security devices and solutions in the last few years leading to the necessity of SIEM to control the increase in "events".

Jude Pereira, MD at Nanjgel Solutions

"We used to just have a firewall to take care of network security and maybe an antivirus for the clients. But on top of that, today, we have things like IPS, quality of service devices and network access control devices," Solling says.

"As we saw an explosion in all of these devices, we also had an explosion in the number of events. Each of these devices would feed in information and say, we have a problem. The security team needs to react to these. A SIEM solution is very important because it takes those events and analyses them based on the risks they present to the enterprise," he adds.

Carvalho says SIEM provides insight into threats before, during and after an attack takes place.

"A lot of organisations in the Middle East invest a lot in security infrastructure, but unfortunately nobody is looking at the logs. On a typical day a typical firewall will generate 10 to 20 thousand lines of logs. It is manually not possible for a human being to sit and look at these," he says.

"So if your organisation is going to be under attack, SIEM can give you a heads up on that. It gives you the ability to understand when an attack is going to happen. An effective SIEM solution also has the capability to give you real-time information when an attack is happening. It tells you in real time how you were attacked, what is being attacked and what the impact is. A SIEM solution also makes it possible to investigate and understand what exactly happened during an attack. SIEM makes it possible to investigate exactly what happen after an attack occurs.

> "A lot of organisations in the Middle East invest a lot in security infrastructure, but unfortunately nobody is looking at the logs. On a typical day a typical firewall will generate 10 to 20 thousand lines of logs. It is manually not possible for a human being to sit and look at these."

Justin Doo, security practice director at Symantec MENA

Basic requirements

Before starting out on a SIEM implementation, a company's current security environment does not require much more than a basic existing infrastructure.

"Most enterprises have already invested in significant infrastructure technology from a security perspective. The idea of a good SIEM is that it should be able to utilise the right technology that's already within the business," says Justin Doo, security practice director at Symantec MENA.

"Things like firewalls, VPNs, antivirus, IPS, web content and email filtering are the basic things that need to be there before embarking on SIEM," Carvalho says. Solling refers to these as "bread and butter" security requirements. "There's no need to look at a SIEM solution if you haven't matured as a security organisation already," he adds.

Once all the security requirements are in place, it is time to choose a vendor. Pereira provides some insight into who the major vendors of SIEM are and what he believes they offer.

"I would say there are five mature vendors, and then three more that are kind of jack-of-all, master-of-none. The vendors are very close, but each one is unique based on the concept, the architecture or where it started from. The top vendors in the SIEM

space are RSA, Arcsight, NitroSecurity, Log Logic and Q1 Labs," Pereira says.

"When you look at Log Logic, the name itself is an indicator of what they are, which is pioneers in log management. But in order to enter the SIEM space they needed some events management – so I would say they give customers 80% in log management and 20% in SIM. Nitro, on the other hand, are trying to become 50% SIM and 50% log, but they're still not quite there. I would say Arcsight, Q1 Labs and RSA are the guys that have nearly got it right," he adds.

Solling expands on the varying offerings of SIEM solutions from vendors.

"There are different levels of SIEM. There are companies that are just focused on log management who are now rebranding themselves as a SIEM solution providers, which is correct that they correlate logs and understand logs from different kinds of devices.However, they're not necessarily a SIEM solution in the sense that they can add intelligence to how to react and report on a specific incident," he says.

Selection

With different vendors offering different things, it makes it difficult for companies to choose the right solution for their business. Pereira says the lack of understanding organisations have on the subject of SIEM can lead to them making the wrong decision.

"Since the customer is not educated enough to understand and to qualify the vendor, he ends up going into, say, Axel Ops or EIQ Networks, which at the end of the day are not really correlation management tools. Since they can do a bit of security they convince a customer on that, and it's only later that the customer realises that they've lost the value of SIEM," he says.

All of the industry experts questioned on SIEM agree the first thing companies should do when choosing a SIEM vendor is to set down the objectives of what they want to achieve and expect from the solution.

"If your initiatives are purely compliance based then there are several SIEM solutions that can do that. If your objectives are to enhance existing security operations then there are fewer solutions that can do that," Carvalho says.

"Then you have to figure out how much time and money you can devote to the SIEM. There are some SIEM solutions that require you to have a lot of people dedicated, and some that can be managed with just one of two people. Also, a lot of time it makes sense to go for a solution from a vendor that you already have products from. Finally, all organisations should do a proof of concept before they buy a SIEM solution. They have to do trial, pilot and test what the best solution is," he adds.

Doo says it is important to examine the track record and also training offerings of vendors. "You should look at how each vendor has evidenced success in similar implementations in the region or vertical markets similar to the one you are in. Then, since building a team internally is integral to getting the most out of the solution, for me the vendor should be able to help train those teams in terms of identifying possible organisational structures, and how to respond to and help rate critical incidents," he says.

It is this "team" that is constantly emphasised in discussions with our SIEM experts as the most important aspect of making the solution successful, and the most common pitfall in failed implementations.

"It's one thing to have a SIEM deployed, but it's another to actually derive all of the information out of it. You need trained people that understand what it is they're seeing and to benchmark that against the risk within the business. That is something that has traditionally been harder to achieve in the local market," Doo says.

Simon Carvalho, principal security architect at Paramount

Bulent Teksoz, chief security strategist at Symantec

> "A lot of organisations in the Middle East invest a lot in security infrastructures, but unfortunately nobody is looking at the logs. On a typical day a typical firewall will generate 10 to 20 thousand lines of logs. It is manually not possible for a human being to sit and look at these."

Antievasion Readiness Test™

aet.stonesoft.com

There is just one way to know if you're protected against AETs.

Test your security device.

The Antievasion Readiness Test will put your Intrusion Prevention and Detection devices to the ultimate field test. Your devices will be tested with actual evasion attacks. No punches are pulled. Nothing is cooked in a lab. The test is as real as can be.

Stonesoft KSA
Al Khozama Center, 2nd floor, Office no.: 211
P.O. Box 53215, Riyadh 11583
+966 1 4654650 (office no.: 211)
info.emea@stonesoft.com

STONESOFT

Stonesoft UAE
Dubai Internet City
Building 15 office 214, Dubai
+971 50 627 4230
www.stonesoft.com

"People play a very important role. In order for companies to derive maximum benefit their SIEM they have to invest in people, because at the end of the day these are the people that are managing the solution and taking action from what the solution tells you. Human action is a necessity," Teksoz adds.

Pereira believes that a lack of training will create further issues for organisations and go beyond limiting the benefits realised from SIEM. "The challenge is to be able to educate the customer. Often they are not trained enough to understand the technology and the engineers just say, that's not the right way or let's not do this thing, which can lead to problems," he says.

Phased approach

In terms of best practices, Carvalho says

Waseem Hattar, operations security manager at eHDF

implementing in stages is essential to get the most out of SIEM.

"Start small and grow as you see success. Start off with basic use cases that address your pinpoints and then try to integrate all the devices. Some organisations try to start off with everything and they end up getting lost. Get the main 20 to 50 pinpoints down and then address the next pinpoints in further stages," he says.

"Any organisation looking to deploy SIEM has to integrate all devices under SIEM, but typically it is not possible for logistical reasons. Typically a medium sized organisation in the Middle East would have between 300 and 500 devices, so you should first focus on network and security devices, servers, databases and operating systems. Then do things like business applications – it is very important to integrate these because that's where you get the real value out of SIEM," he adds.

Whilst undoubtedly requiring a lot of invested work and time for an organisation, if all devices are not integrated and all logs not collected, it will be a "wasted" solution, Carvalho says.

"Many organisations try to be stingy in SIEM and only want to collect certain important logs, but the problem with that is once you start collecting and analysing you won't know what's important. When the time of an investigation comes after an attack and you realise you weren't collecting the right logs, then it will be a wasted process," he says.

"You can't make a SIEM solution better than the data it receives - you have to have support from the different departments

Nicolai Solling, director of technology service at help AG ME

within the IT infrastructure - your server side, security side and client side. You need to make sure that you correlate information from everything," Solling says.

Waseem Hattar, operations security manager at eHDF (eHosting DataFort), adds that companies must be prepared to completely commit to SIEM, as the costs and efforts to make it work will be high.

"The main challenge is the cost that can be very high even without management and engineering costs. Enterprises also need to remain updated with the current attacks and need to have a deep insight on creating alert rules on the system. If alerts are not generated, the SIEM system will only log data and archive the logs without any assessment," Hattar concludes. ■

✱ BY THE NUMBERS

Source: Source: Gartner (2011)

$858m
Cost of SIEM market at the beginning of 2010

$987m
Cost of SIEM market at the end of 2010

15%
Growth rate of SIEM market during 2010

80%
Amount of initial deployments in North America funded to close a compliance gap