

About Arlan McMillan

Arlan McMillan, First Vice President/Director is the Global Head of Information Security Operations for ABN AMRO Bank. He leads a globally dispersed team which monitors the bank's global network for suspicious and malicious traffic. The ABN AMRO enterprise consists of over 250,000 nodes spanning more than 50 countries. To oversee the enterprise, Arlan's team monitors an environment which consists of over 200 NIDs, 60 firewall complexes and vulnerability information of over 95% of all network attached devices, numerous proxy logs and antivirus data. The over 1 billion events that these monitor as well as other data sets generated monthly are fed into a centralized collection system which in turn provides automated correlation and triage for the Information Security Analysts.

About ABN AMRO

ABN AMRO Holding N.V. (ABN AMRO) is the ultimate parent company of the ABN AMRO consolidated group of companies. The Company provides a range of financial services on a worldwide basis, including consumer, commercial and investment banking.

SANS Summary

Seeking help to correlate and make sense of the massive volumes of security data coming from its global network, ABN AMRO chose to collaborate with an existing vendor to improve their product to dramatically improve workflow processes, accuracy and depth of intelligence. The enhanced product allows them to process more than a billion events a month in real time with greater accuracy and introduced the ability to rapidly perform ad-hoc investigations to determine complex traffic patterns.

~~~~~

#### Interview

Q. What was going on that led you to look for a new solution?

A. The primary motivation which got us looking down this road was actually an organizational change within ABN AMRO. Like many large enterprise organizations we are global, we're in 65 countries. We had at the time over 110,000 employees, about 300,000 nodes on the globally dispersed network and we had a change in the organization that went from a federated model into shared services. So it went from vertical tiers to horizontal layer and I was asked to head up a group which was given the responsibility to monitor the bank's global network for suspicious and malicious activity.

*\* To hear Arlan McMillan expand on his answers, view his presentation slides, and listen to his answers to many more detailed questions asked by other users from around the world, go to <http://www.sans.org/webcasts/archive.php>.*

Q. What gave you the opportunity?

A. Two things primarily – right time and right place. As part of the reorganization, the numerous existing security organizations which were spread across the globe were evaluated for their overall maturity and vision. Of these 20 or so groups, two stood out well above the rest. One was located in Chicago, USA and the other Sao Paulo, Brazil. In the end, the Chicago group was given the lead to develop how the new Global group would be developed and what their oversight responsibilities would be.

**"Intellitactics can save significant amounts of time and cost."**

In support of that decision, in 2005 I was asked to take over one of the three divisions that made up this new group. Due to numerous successes that were had with the development and implementation of the log correlation system, in 2007 I assumed leadership over all globally focused operations.

Q. What were you in your earlier life? Were you in security at all or were you in operations?

A. I was in security, though for a much smaller organization. My background is IT-specific as opposed to IS. I've grown into IS. Like many, my career began as a desk-side technician in a Novell environment. After a number of years in the trenches, in 2000 I was asked to be part of a small team within ABN AMRO that was working on building what rapidly became an industry leading eCommerce Treasury Management solution. After performing in various roles within that space, I was given the opportunity to help shape the newly created Global Information Security Operations group.

Q. Development too? Were you actually in development or you did more of the systems engineering?

A. For a year I was a project manager for an Application Development group at First Union Bank before it was bought out by Wachovia. Most of my experience however is on the systems side with a tight partnership with developers and the business – all working together to develop new products. We were a small, very highly talented team that built up a treasury management solution. So while I was OS or system side focused, sitting two desks away from me was a team of developers. I didn't do development but I worked very closely with them in helping test their creations and then supporting the products.

Q. And you grew up all through it, learned from the challenges.

A. Grew up all through it – from a senior systems engineer to production support manager. We were processing over ten billion dollars a month through this environment. So you can imagine the downtime costs associated with something like that. And in working in that arrangement, that was a web focused, e-commerce, treasury management solution, I became very interested in security, I think for obvious reasons. And it was that interest in security that then acted as the stepping stone for the next couple of positions that I had,

one of which was heading up a security compliance group that worked with the development teams on this in other systems. I became a security and compliance person at that point and then from there I moved into the global role.

Q. The security world has gone from all compliance to actually having to do security and it's challenging a lot of people. Your background's good because it's got this real heavy technical arena and then compliance and then you

brought it all together in the new job. You didn't just start out in compliance, as if that were the beginning and end of security.

**"Intellitactics offers a highly capable centralized management console that presents all the data you have collected."**

A. If you wish to be successful in IS you really need to come out of IT. You can do risk management, you can do compliance and not come out of IT, but if you want to be successful in the running of IS you have to come out of IT because you must understand what you're securing and why you're doing it.

Q. Yes, not only why but how, because otherwise you get misled. And you don't know you're getting misled because you have no language and no experience.

A. Absolutely. You have to have an ability to feel it rather than just knowing how to follow a script.

Q. That's an old, old goal of ours, to get people to think that way, but the compliance push the last five years kind of pushed us off. We lost that argument over and over and over again.

A. And I firmly stand behind the idea of IT out of IS. Now I don't believe that the IS organization ought to be a subset of IT, they ought to be separate organizations. Governance is a different topic. With that said, I have never met a skilled and successful innovator within IS that did not come out of IT. The ability to sustain compliance - to be secure - requires focus and process. Our focus is security and demonstrating compliance is a by-product.

Q. So you're sitting there with a new job and you need global visibility. Everybody's got some tools already or there are no tools in place? Are there lots and lots of little tools?

A. There's lots and lots of little tools. So the first step is to develop a standard. Get it all underneath one umbrella, standardize on platform, standardize on deployment methodology and philosophy. We standardized on the SNORT Sourcefire product for our NIDs, as the very first step. There were a variety of different products out there. We decommissioned all of those and deployed the Sourcefire boxes all reporting into central management, our Defense Centers, and distributed those globally. Obviously I'm speaking

specifically within my arena. There were many more activities within our organization at that time, but specifically within the operational field that was our first step.

Q. And about when was all this? When did you get the job, roughly?

A. Well, the real deployment work began around 2005 and 2006 and continued until early 2007.

Q. So it was a lot of time to do this because it's a big company. What about management tools?

A. Sourcefire SNORT. It's part of their package. It's called the Defense Center so you have all of these SNORT boxes reported to your central reporting station.

Q. But that wasn't complete visibility?

A. No it wasn't. This is where the rubber hits the road. If you're only looking at IDS you're only getting a slice of your security picture. The real value, which drives the need for information security professionals, is bringing in multiple data sources and correlating all of those data sources together in real time or near real time, to get a more complete threat posture of the network of your organization. IDS is wonderful. IDS, just like every other type of product, is positioned to look a particular way. So for example, how about antivirus, antivirus is going to tell you wonderful things. How about firewall logs, how about proxy logs. In most organizations, each of the data-sets remains independent. Take firewall or proxy data for example. These logs are huge not only in raw size but also in the wealth of information that they contain. The challenge though is being able to do something with the firewall or proxy data that is comprehensive and near real time as opposed to what most organizations do which is either to do nothing or to cobble together some sort of shoot-from-the-hip response. Without a well rehearsed work-flow processes and a comprehensive correlation toolset that allows for quick queries and automated correlation, it is impossible for IT or IS professionals to be anything except reactive and therefore well behind the curve with any detection or forensic activities.

**"A tool like this is all about enablement - if you don't have one, you can't claim to do security."**

Q. Is it because the search tools are slow or because they're a little arcane to use or because very few people know how to use them? What makes one thing slow and Intellitactic's tools not slow?

A. Well, there's two things that become very important. The first is that most data sources don't format their data in a way that is conducive to perform investigations. Again to use the firewall data set as example, it's important to appreciate that in a large organization there are typically many egress and ingress points within your network. This is rather standard in a flat WAN or GAN - especially one that has grown organically over time. What that means is anybody from Singapore can come into my North American network from

many different points if they know how to do it, it's not very hard. So if I want to investigate some activity and I don't have a centralized tool, I now must search each and every one of my border firewalls. Even if all of the devices are using NTP and GMT, which we all know is hardly ever the case in environments that are not centrally managed, the time that it would take to manually search all firewalls for even just one query would take so long and eat up so much effort that it quickly becomes prohibitive except for the most egregious and high profile investigations. Centralized log storage helps a great deal but doesn't solve the problem. The only thing that does is to get that massive amount of data out of their flat files and into a database. Intellitactics has an efficient security data warehouse.

This leads us into the second issue. It's not enough to have multiple, albeit good central management consoles. Other data sets like IDS format their data much better. For a very

**"It's reliable and relatively flexible."**

long time we only, and very successfully, leveraged Sourcefire's central management consoles. After two or three, the probability that human analysts will be able to look at screens of cascading and disparate data and derive intelligible data from them becomes basically nill. That only

happens in the Matrix. It's impossible. Not only is that technically impossible, it's impossible to develop repeatable and consistent methodologies. So you never can guarantee your quality of service, you can never baseline your quality of service and you can never measure your quality of service. Intellitactics offers a highly capable centralized management console that presents all the data you have collected.

Q. And you feel you can measure all your service with these tools?

A. Absolutely. And we're starting to be able to touch on network behavioral analysis as well because we can do this type of baselining.

Q. Right, it's not just security issues. It's operations and the network, right?

A. Absolutely. There are a lot of exceptionally talented people out there that can do some incredibly complicated forensic work. They're great and they're expensive. A correlation system will not replace those people. What a correlation system brings to the table is the ability to do information security on a daily basis with measurable and repeatable processes. You go from IS being the bastion of the monks on a hill to something that has day to day value. You could say that Intellitactics enables you to leverage the skills you have on your team.

Q. Now, you decided you wanted to look at more than the SNORT stuff, the Sourcefire stuff, you had to look for one of the SIMS, what was the critical criteria? At the end when you were done with all the criteria and all the testing, what mattered most in choosing one over the other?

A. I'll be very honest with you, we did not choose Intellitactics in that way, we had Intellitactics in house already so that's where we started. The problem was that at the time it didn't work – we're looking back three years.

I think most people, most analysts out there can appreciate that Intellitactics today is significantly different than what it was a couple of years ago. The quality of the product is almost 180 degrees different. Even though the product before didn't do what we needed it to do, I engaged the vendor because the initial investment was already made by my predecessor. The vendor heard me out, thought what I wanted to do was interesting and was aligned with their already determined strategic direction. We partnered up and after significant changes to the product we made it happen. That took over a year of effort by both my teams and Intellitactics. In some ways that effort paralleled the work that was done in my prior groups where systems people partnered with developers to build a new product. I understand that a significant amount of what we all put together is now part of their standard build.

Q. If you were talking to the other users and they said, are you the guy that caused it to go from A to B what would be the biggest changes from the old to the new?

A. From a technical perspective they introduced significant architectural changes to all three of the tiers – database, application and the web component. So they completely recoded their product and their reporting module from the ground up and that's why I say the product a couple of years ago is not what it is today. What you can buy off the shelf is actually very similar to what we've spent thousands of man hours over the past few years configuring an effective solution in our environment. We've got a product that works and they help maintain it for us.

Q. So it was already in house so we didn't have to talk about an implementation, how long did it take?

A. If you can import firewalls into a correlation system and you can do real time reporting that's a major milestone. We have five regions, roughly 35 firewall complexes in each region, that needed to go into this system and be actively correlated against vulnerability management information, NIDs information and anti virus information. I needed a 24 by 7 system alerting my human analysts about threats it's identified. When I inherited the product it was struggling with the heavy firewall data. I think I've got over 60 firewalls in it now and more than that, I'm processing over a billion events a month.

**"...creating reports of technical data is pretty easy to do."**

Q. How long did it take you to go from not being able to handle the firewall data to 60 of them? Was that the years?

A. Yes, and this is where it becomes difficult for a large organization. For us it was a very developmental process. For most organizations, despite the fact that all environments are unique and thus all implementations will require tuning, time from conception to production will be significantly shorter.

Q. Right, because you were rebuilding the tool while implementing it and you were also developing your internal processes.

A. Exactly. While it has been in production as the primary tool for our 24x7x365 Security Operations Center for some time, we continually work to improve the environment through tuning the logic, building new types of reports that examine data in new ways and of course by bringing in new and different data sets into the correlation engine.

Q. So how does that affect security?

A. It does a few things. While a system like will this absolutely boost an organization's overall security posture, one of often overlooked and very real benefits is the operational efficiencies that can be realized. For example, we can now do trending. We have a far better understanding of what is not normal traffic. We have a quicker turn around time, a quicker response time. Let's consider one example: One of the best tools to uncover suspicious or malicious traffic are NIDs. There are many positives to that technology. Two negatives however are relatively high false-positive rates and a diminished ability to provide reliable criticality ratings in complex environments. As you're able to get more data into a correlation system that leverages good logic to interrogate the data, that system

**"... to get all of that data takes them a fraction of the time that it did before we implemented Intellitactics."**

will become more and more able to filter out false-positives and to more accurately triage the events and thus greatly increase overall accuracy and ability to separate false-positive events from real incidents / confirmed-positives. We get that with Intellitactics and that's what it's all about. From there, the humans take over and put eyes on and do the

real investigation. Without that initial effort being automated by your SIEM, you can't do security. When a way to automate your process becomes holistic and repeatable - then you can take it to the next step and develop baselines. The types of baselines that you need to develop are numerous and span across all three of the service delivery triangle of people, process and technology. There's baselines for analyst accuracy and response time - in other words you can determine if you have a people or process issue. Then there's network behavior and traffic patterns - you can determine if this level or type of traffic from these segments or from these systems is typical - even determine if they are typical from one system to another. A tool like this is all about enablement - if you don't have one, you can't claim to do security.

Q. What's the job of the analyst?

A. In my organization, the job of the analyst is to investigate events which have been elevated by your central correlation tool and then to escalate reviewed events to and partner with direct support personnel to perform the detailed secondary analysis. Many organizations give the analysts IDs that have elevated rights on the target systems so that they can perform in depth investigations. We don't. We don't for a number of reasons ranging from maintaining segregation of duties principles to the simple and pragmatic. When I was supporting critical systems, I'd raise hell if anyone even physically, no less logically, touched any of mine. No one knows a system better than those that are charged with supporting them. In other words, that's not going to be your security analyst. We broadly define these two stages as monitoring/alerting and validation/remediation where the analyst performs the monitoring and alerting phase and assists with validation and remediation if requested. Whatever information you can package from the SIEM that will assist the validation and remediation phase is a bonus.

Q. And giving the analysts the raw data so they're investigation is successful.

A. And to get all of that data takes them a fraction of the amount of time that it did before we implemented Intellitactics. An investigation that we do today that takes ten minutes would have taken days in the past. On top of that it's repeatable and demonstrable. Repeatable and demonstrable are critical requirements if you want to take anything to law enforcement or the courts.

**"The Intellitactics  
SIM is a good  
product."**

Q. Can you give us one example of the type of thing that the correlation enables you to find?

A. Absolutely. One of the easiest things to find is something like Slammer – it lights up the tool. Slammer lights up any tool for that matter. Large automated attacks in general are fairly easy to detect, especially if you're looking for them. What become more difficult are "low and slows", coordinated or unexpected attacks. Take the issue that we all had with the Russian Business Network a few months back. There you had many web sites that were designed to perform drive-by downloads. Once you became aware of an issue like that, you could take a hatchet approach. After you block their whole network manually rummaging through all of your proxy and firewall logs and identify all of your systems that might have had contact with one of those sites directly or via one of their hosted banners via a third unsuspecting site. At this point, if you don't have correlation there are a couple of choices, but none of them are particularly effective. First, you can do nothing and hope that nothing got installed. Second, you can choose to not trust them and reimage them all. Or third, you can send out a team of techs or analysts with detailed instructions on what to look for and hope that everybody followed the instructions properly and had the technical skills.

All three options are expensive whether you measure cost by the amount of risk that you have to accept and/or the pure dollar value of hours that need to be invested. That cost only goes up if you discover at a later time... say a day after you complete your desk-side investigations, that there was something else that you needed to look at.

When you have automated correlation tool like we have you have more options. First you can rapidly perform multiple Boolean type searches across your whole enterprise and all available data sets. Second, you can analyze traffic patterns. In other words, did two

**"What a correlation system brings to the table is the ability to do information security on a daily basis with measurable and repeatable processes."**

systems within the same subnet go out to any set of subnets for attempt to open unusual connections to uncommon systems? The third is to perform a broad and coherent investigation by logically grouping suspected systems and subjecting them to enhanced observation and interrogation. With Intellitactics we

can perform real analysis and thus provide strong data against which risk management decisions can be made. This in turn can save significant amounts of time and cost associated with any of the wide spread hatchet approaches. In the worst case scenario, when there is a breach and you're organization is being investigated as part of a legal proceeding, significant fines can be avoided if you're able to demonstrate that your tools and processes achieve the minimum regulatory requirements for proactive threat management.

Q. And have you found things you wouldn't have otherwise?

A. Absolutely. Everybody wants to talk about real attacks but the reason why these attacks are so interesting to people is because they're almost unique in a way. Every attack becomes almost unique. When you have such a large organization it becomes impossible to have any real confidence that you have an effective grasp on the activity on your network unless you're passing this type of data through a centralized, automated tool.

Q. How much work was it to create the logic that identified the kinds of things you were able to find? Meaning how much of this is because you own a tool and how much is it the brilliance of the people you have doing it?

A. The fundamental logic is built into the Intellitactics system. Every organization will need to customize the logic to fit their unique environment. For us it wasn't the tuning the logic that took/takes the longest, that in fact is rather easy to do. Less than 10 minutes for some of the basic changes. The real challenge and time comes in trying to figure out what you want to know and what you believe is important to and within your organization.

In terms of how many brilliant people do you need, well, the goal in my opinion is to be able to set up repeatable processes and to be able to do that you have to get away from requiring a whole team of brilliant people. I've got a good team of analysts that are in my SOC but they're all replaceable. They are smart, intelligent, experienced and they can all be replaced. I can get new people. We try and position ourselves to be successful by reducing the number of critical assets and by developing repeatable processes that we can automate. Any organization that expects quality of service needs to take these steps.

Q. The logic is built into the tool; it's not stuff you added in after you got the tool.

A. That's correct. Now there are add-ons that we've done, customizations about what data we want it correlated against and how we want to see it, but the core algorithms, and what goes into those algorithms are in the tool and we leverage that.

Q. What are some of the mistakes you've seen other people make, not because they've picked the wrong tool, but in using the correlation tools?

A. It's not even in the using it, it's the planning for it. The biggest mistake people make is not appreciating the up front work required and the dedication required to put this in

place. They expect, and the vendors are a little bit guilty of this (all vendors say it's going to come out of the box, it's great), but that's not exactly true. You are going to need to plan to dedicate resources, time, effort and thought about how you're going to deploy a standard type of tool into your unique environment. Every environment is unique.

**"Intellitactics has an efficient security data warehouse."**

Every organization is unique. It's impossible to take a standard out of the box tool and make it work exactly how you want in your environment and get the full value out of your investment without a some work on your part. In today's economy all investments have to be maximized and that takes planning and effort.

Q. What kind of key people do you need to help you in that?

A. From the top to the bottom you need them all if you're going to be doing a large deployment or if you have any real scope in mind. And it's going to be not only the time invested by your security staff and engineers, but also by the time invested by your product management teams and also the network teams they interface with. You need to get a buy in from your stake holders and you need to have the timeline fully laid out so that everybody appreciates the effort that's going to be required to implement this type of product. I've seen projects where there's a lot of excitement in the beginning and when results aren't exactly as expected it trails off; the buy in filters out a little bit and the product isn't realized to its greatest potential.

Q. How did you talk the network folks into helping?

A. It was extremely difficult – especially across organizational and country borders. We still have challenges today, but when you start to use the same tool for network

management and network monitoring and network visibility they become advocates. They need something, use your tool to help them get it.

Q. You talked about how Intellitactics was already in house, Arlan, did you need additional training to use the new features you requested? When they came in was there anything that you had to adapt to that was different?

A. It was in house but mostly not used so everybody got trained as a baseline. Also I was replacing the seven screens with a single screen. So there is not only training in the

**"While a system like will this absolutely boost an organization's overall security posture, one of the often overlooked and very real benefits is the operational efficiencies that can be realized."**

technical sense but also retraining in work flow and process – to give everyone a comfort level on how they were going to use Intellitactics to do their work. What you really need to do, especially for your first and second level analysts, is define a standard set of processes, methodologies and related tool sets that make up their work flow.

Q. How much did it take in the way of manpower to use it the way you're using it now?

A. Primary effort has come from a single engineer dedicated full time for about two years now, a year and a half. Additional effort has come from the

analysts as well as the manager of my SOC in marrying the processes and technology.

Q. Do you find that gets you everything you need?

A. I have a backup for him, but for the most part yes. When it hasn't, Intellitactics has proven to be a dedicated and reliable partner that we can fall back on.

Q. Have you ever had anything crop up that made you contact tech support? Anything that was particularly difficult?

A. Sure. This should be expected given the complexity of these types of products. We're implementing a new appliance from Intellitactics in another location, but our centralized solution is the software product. You can't expect to open the box, rack it and walk away like you would an appliance. You will absolutely need to establish a tight partnership with your vendor of choice for at least six months from the point of getting it in house. It is absolutely critical that you engage with a vendor who is absolutely willing to work on this and be an active partner – not just somebody who bills you hours. When performing your review, cost and technical aspects are of course critical, but don't forget to evaluate your impression of the vendors desire to get involved and participate like a real partnership with you.

Q. Are there additional features that you wish it had? Anything on the drawing board now as far as you know?

A. Absolutely. For example we want to link into our incident management system. We leverage Archer incident management system for our ticket tracking and we're close to completing an automated ticket creation link between the Intellitactics system and Archer. You'd right click on an event and say create ticket and it automatically links into Archer, propagates all the fields with all the necessary data and increases efficiencies in your work flow. This also introduces the ability to measure SLAs from creation to closure for all events and investigations.

Q. How do you feel about the Intellitactics SIM overall, both pros and cons?

A. I like it, it's a good product. Pros: it's been stable, it enables us to achieve our goals in real time, it's able to handle the volume. We have very large volumes we're pumping through it and it's able to handle it. We have very little down time. It's reliable and relatively flexible. Cons: I wish the reporting component was more robust – it's not as good as we need it to be so getting data out of it is more difficult than it ought to be. This incidentally is a common weakness across the IS space in general.

Q. Is it the granularity of the reports that's the problem or a specific type?

A. It's just how the logic is written within the reports themselves – it may provide you very interesting types of technically focused reports but if you want to get into any advanced analytical or management type reports it doesn't do that as well as I would wish it to.

**"...it's been stable and it enables us to achieve our goals in real time, it's able to handle the volume."**

Q. What kind of report would you like it to have done? Give us an example, what would a problem be where a report was needed where you had to do more work than you wanted to do.

A. Sure. One of the things is workflow – being able to quantify and qualify the work that is being done by your analysts. An example would be reporting on SLAs, everybody knows the term. How do you measure an SLA from start to finish or the full life cycle of an event. Say you have an SLA around incident resolution – an event clicks off at one o'clock, if you have an SLA to resolve this incident, you have to go through that whole process of event being created by the tool, event being identified and owned by the analyst, event being closed escalated and then finally the incident being resolved. You've got to be able to measure that life cycle every step of the way so that you can identify places where you require improved efficiencies. This is one report we'd like to get from Intellitactics. On the other hand – creating reports of technical data is pretty easy to do.

Q. Because you're managing a process and it's as much a question of what did I do on my management side of my responsibilities it was to what did I find in my security side?

A. Absolutely. Information Security is fundamentally a Risk Management focused discipline that leverages a heck of a lot of technology. It's not enough just to say you had 6 incidents in a month. That by itself means nearly nothing and is almost useless to your decision makers. You have to put that into perspective, trend it, quantify and qualify it. You have to tell your management how much any sort of activity deviates or satisfies the stated acceptable risk posture for your organization.

Q. And it's not the kind of thing the security guys think about when they built the product.

A. No, but it's terribly important because we're not talking about a product that in our case was going to cost you \$50,000. We're talking about a product that for organizations like ours is going to cost more than a half a million dollars. That kind of number may make some people blush but as soon as you start to add up people and time costs along with your hardware, software, licensing and maintenance costs, these products quickly become expensive. So when you start going to management and say you need a half a million plus, or more, you are going to have to be able to justify your expenditure and you're not going to be able to do that by simply saying, yeah, we're doing better. You need to be able to justify the spend by illustrating how you are improving from point A to point B.

Q. It allows you to measure the guys against each other. How did you do that and was reporting pretty easy?

**"... for most medium size and all large organizations where security is strategic, this type of product is a must have."**

A. You know the hardest part of this goal is determining what you want to report. And it's been a process. We're still getting there but we're doing pretty good. For example, one of the basic metrics that some organizations use is reporting on how many tickets were created. Well, you know there's a problems with metrics like that. I can create 1500 tickets and all of them are

meaningless if I have a false-positive rate of 98%. Creating a bunch of tickets doesn't mean that I did any better than the guy who created five tickets and all five of them were confirmed. So then what you have to do is you have to take it to the next step, how many of those were false positives, how many of those were confirmed positives. Look at what is your average rate of alerts during a certain period of time, during certain times of the week, during certain periods of the month? Your activity versus volume matters.

Say you have a certain number of alerts being triggered. You should measure how many tickets are being created off of those alerts and how many tickets the analysts are taking

ownership of per hour, In addition you can then look at certain categories of alerts that have a higher probability of being a false-positive. This is information you can investigate to see if there is an opportunity for improvement or refinement.

Another example is being able to determine the average number of alerts per time slice and then seeing an increase in that time slice. You can set thresholds that are outside of baseline and you can create a new ticket or a new alert out of that data. These are the kinds of things you can't possibly derive if you're looking at each one of these data sources in isolation.

Q. What's the future for the SIEM at ABN? Has ABN been able to cost justify their investment in a SIEM - what were the savings or what costs were deferred as a result of the SIEM investment?

A. My CISO was convinced early on by the richness and depth of the technical data that I was able to bring to him. I've been able to further prove the investment by proving how this product improves operational efficiencies. It's really just a slam-dunk at this point. Because of that I continue to have wide latitude to expand the number and types of datasets that I point at the system and to test with different ideas. We're looking to expand what we do with our proxy monitoring for example and this is eagerly anticipated by our APAC region.

Q. Do you use alert risk scoring to prioritize alerts based on a nine factor risk score?

A. We use the risk scoring, but we configured the scoring into five categories for easy classification.

Q. Since ABN has recently been acquired, was the SIEM data useful in communicating the impact the ABN team had on security? Is the SIEM data any value in quantifying the value of the work that the ABN team has been doing?

A. As can be expected, there are stringent controls how much I talk about the acquisition or our acquiring partners. In general, what we've done at ABN AMRO within the Information Security space is well respected within the community.

Q. Do you believe a smaller company than yours, one where the volume of events is less, would benefit from a SIEM? In what ways?

A. Small, medium and large are terms that are hard to quantify. What I can say is that I believe that for most medium size and all large organizations where security is strategic, this type of product is a must have. For medium sized companies tough questions about the depth of their bench and strategic goals have to be answered. All of my experience is within the large enterprise but my suspicion is that medium sized companies would find value with limited and targeted implementations. I know that Intellitactics is trying to address the medium sized market with their new appliance.

SANS Bottom Line on Intellitactics at ABN AMRO:

1. SIEM manages the "waterfall of data" dilemma;
2. Provides centralized correlation ability;
3. Helps focus investigators on the right things and doing it quickly (triage);
4. Excellent to enable data for process improvement; and
5. Enables repeatable processes and consistent quality of investigations.

**For more information on Intellitactics:**

**Go to: [www.intellitactics.com](http://www.intellitactics.com)**

**E-mail: [SalesInfo@intellitactics.com](mailto:SalesInfo@intellitactics.com)**

**Phone: 877-746-7658**