CUSTOMER Q&A

RSA SOLUTIONS EMPOWER MOL TO BUILD A PROACTIVE, ADAPTIVE SECURITY MODEL THAT ADDS BUSINESS VALUE

AT-A-GLANCE

Challenges

- MOL Group previously took a reactive approach to its security and its strategy lacked cohesion and focus.
- It wanted to develop its technology to combat current and future threats while managing incidents efficiently and proactively.

Results

- With RSA Security Analytics and RSA Archer, MOL Group identified suspicious activity and reacted to threats with preventatitve measures.
- The company was able to identify threats easily and bring quantative data to top executives to propose improvements.

"The measure of a relationship is not about how good you are when everything's great; it's about how you turn around when things go wrong. Every single time I have a conversation with RSA about what needs to change it's picked up, taken on board, and it's recycled back out."

JASON HAWARD-GRAU, GROUP CHIEF INFORMATION SECURITY OFFICER, MOL GROUP

MOLGROUP

RSA

As a Fortune 500 company operating in approximately 26 markets, MOL Group is one of the world's largest oil and gas companies. It operates in about 40 countries with a work force of 27,000 people, four refineries, two petrochemical plants, and over 2,000 service stations in central and South-Eastern Europe.

Why is security important to you?

Jason Howard-Grau, Group Chief Information Security Officer: Information security is being brought into everyday business discussions, from everything from deploying a bond into the marketplace, through to the due diligence that we now do on the acquisitions, so it's fundamentally become ever more important.

How are you organized to meet your security goals?

Howard-Grau: We are separated into the core functions of risk and compliance; architecture; design and insurance, and cyber defence capabilities. Then program management and governance underpin all of those areas.

However, our Information Security department actually sits outside of the IT department. We chose to do this because we wanted the indepdence to work efficiently in partnership with IT, without being tied to that department's operational goals.

What drove your decision to implement RSA solutions?

Tamás Kapócs, Head of Security and Architecture Design and Assurance: Before using RSA solutions, we only had basic analysis capabilities in the organization and we obviously wanted to develop this to face today's challenges. We needed to think about incident management as well.

Howard-Grau: The organization was focused very much on the reactive end of the spectrum, so the focus was on understanding what might have happened, rather than looking at it from a proactive threat detection perspective. Across our organizations what we were really looking at was a set of disjointed technologies that lacked cohesion and strategy, and lacked focus.

Why did you choose RSA Security Analytics and RSA Archer?

Howard-Grau: We were backward-looking as an organization. The horse was out of the stable and some were even in the next field, and we hadn't even noticed that the gate was open. By deploying the RSA suite we wanted to give ourselves the chance to actually aggregate information in the right places and drive it towards insight.

Kapócs: We deployed RSA Security Analytics back last year in 2015 and currently we are in the process of setting up our Archer framework and infrastructure and on top of it we are deploying security operations suite and vulnerability and risk management.

With RSA Archer we are looking to have a base platform for all the security orchestration, needs and processes that we have. This will be the core platform which can collect and analyze all the information we need.

Can you share an example of how you're using the tool?

Howard-Grau: We switched on Security Analytics and a lot of things suddenly started lighting up, just like a Christmas tree. For example, we were being hit by a large number of phishing emails, and as soon as we switched on Security Analytics we started to detect them. The cyber defence organization identified that this was a particular targeted type of campaign, and we moved very quickly to identify the known bad IP list and make sure that the outbound firewalls were blocking those. By having the actual facts in our hands I can sit down with the CIO and say, "We have some serious issues with our ability to update our known bad IP lists, to update and manage our firewalls effectively."

What are the benefits of selecting RSA solutions?

Kapócs: Seeing more and being able to dig into the details is helping us to really find the root cause of certain problems, and avoid missing key events that are going on in our enterprise networks and systems. We can continuously report, measure and analyze how many vulnerable hosts we have, how long those vulnerabilities have been out there and how quickly we can eliminate certain vulnerabilities. This is key for the business to understand so we can focus our resources on to those areas where there is the highest need.

What is the benefit to you of working with RSA?

Howard-Grau: The measure of a relationship is not about how good you are when everything's great; it's about how you turn around when things go wrong. Every single time I have a conversation with RSA about what needs to change it's picked up, taken on board, and it's recycled back out. For me RSA is all about partnership.

What business value were you able to generate?

Howard-Grau: Business value for us is more about risk aversion. The business wants to know they're protected but the price of that protection is hard to quantify. Most organizations recognize that information security is seen very much as the umbrella for a rainy day. It's not a great position to be in, but it's the reality in which we're currently operating in, and we're gradually changing that. However, I would say right now the value is in driving insight. It's about the moments when we can say, "Ah that's different. Didn't see that before. What do you think that is? Why is that happening?" These are all the questions that my team are starting to ask, and the value in that is massive.

One breach that we can detect and prevent, or respond and contain is worth a significant amount of value to our business. Our refineries are extremely expensive; we have a huge investment over a long period of time across multiple geographies and some of the most challenging parts of the world. Practically speaking it's really simple: if we detect it, prevent it, that's value.

How do your security insights inform conversations with the business?

Howard-Grau: By having the actual facts in our hands I can sit down with the CIO and say, "We have some serious issues with our ability to update our known bad IP lists, or to update and manage our firewalls effectively." It's not a panacea, we didn't get there completely overnight, and we're not there yet, but at least by having both the information in my hand and the insight I can draw from it, I can have those really powerful business conversations. They're not based on what I think or what I believe, but based on what I know, and those facts are very difficult to dispute.

What best practices can you share with others?

Kapócs: Looking into the enterprise security architecture was key, as was building it up in a way that is easy to understand for our top management. We can now articulate the value of it and also the risks that we can mitigate or address with all these solutions. At the same time it was crucial for us to make sure that we have the right connection points to the key business processes. Our team is engaged all the time to check any information security capability or just to make sure that the right controls are there from design.

What's the next step in your security journey?

Kapócs: The next step in our journey is to look at standardization within information security. We'd like to implement a common set of key information security capabilities, solutions and technologies in our business and this will help us drive our strategy and enterprise architecture going forward.

Howard-Grau: We've established a role structure that actually helps people from the beginning as they come into the organization understand where they want to get to, then our job is to make sure that we facilitate their growth in the right way. At the same time, we need to ensure that we have the right training budget in place. We recognize that the world we're operating in is adapting every three to six months. New technologies come on the market, new threats hit us, and the way that we did something three months ago will not be the way that we need to do it in six months' time. Being adaptive to those changes means that I need to make sure my workforce is also adaptive.

CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.rsa.com