



#### About Unisys Corp.

Unisys is a worldwide technology services and solutions company. Its consultants apply Unisys expertise in consulting, systems integration, outsourcing, infrastructure, and server technology to help its clients achieve secure business operations. Unisys builds more secure organizations by creating visibility into clients' business operations. The company has a strong Managed Security Services (MSS) practice and currently operates three primary Security Operations Centres (SOCs) worldwide, along with a dedicated Federal SOC in Reston, Virginia. In 2005, the Gartner Managed Security Services Provider Magic Quadrant ranked Unisys second in their ability to execute throughout the MSS industry.

#### About Tristan Morel L'Horset

Tristan Morel L'Horset is the Director of Managed Security Services within the Unisys Federal Government Group. As such, he supports numerous federal and civilian agencies in providing enterprise-wide security services. Prior to joining Unisys, Tristan was an agent with the Air Force Office of Special Investigations where he led some of the largest criminal and counterintelligence cyber-investigations in the nation.

## Unisys Corporation SANS What Works in Intrusion Prevention

### *Defending Government Security with Unisys*

***Information overload from thousands of Intrusion Detection Systems (IDSes), firewalls and malicious logic sensors prompted Unisys to look for technology that would help it weed out noise from millions of alerts per day and turn events into actionable information. Key criteria included manageability, correlation technology and open-architecture.***

#### INTERVIEW

*Q. What was happening at Unisys that led you to look for an Intrusion Prevention System (IPS)?*

A. We support several medium to large federal government contracts with 5-10,000 users or more, hundreds of IDSes, AV data, firewalls and other security systems resulting in over 100 million events per day. The challenge any large deployment is information overload in that it is difficult to hone in on the significant events. These are common issues with very large organizations.

As an industry leader in MSS, we use event monitoring and correlation tools (also referred to as Security Event Management – or SEM) in order to reduce the total amount of events deemed critical. As a result, 100 million events a day may result in 1,000 high alerts that should be reviewed. Although correlation tools are effective, evaluating 1,000 alerts a day for a single customer can still be a daunting task.

Our efforts to find technologies that would allow us to reduce the total number of false positives are what initially sparked our interest with Sourcefire. Used in conjunction with its passive vulnerability scanning product, RNA (Real-Time Network Awareness) Sensor, Sourcefire allowed us to better rate the alarm level of an event, and thereby render our overall SEM system more effective. This technology has allowed us to focus on the better quality information from the IDS itself resulting in actionable intelligence on which our incident responders can quickly work.

*Q. WhatWorks is about the experience end users have with products. You are providing your services to the federal government, what qualifies you as an end user in this case?*

A. End users of an IDS product are typically security professionals who need to understand the threats within their environment and identify violation of policies or standards which can result in incidents. These security professionals often spend countless hours determining what the real threats and violations are amidst all the network noise that can be present.

As such, we – in the Unisys Federal SOC – are end users of IDS products as our core business is to perform this very function for our customers. We very much care about the efficiency by which we can determine an incident from a false positive as it directly translates into a better service to our customers.

*Q. How did you approach finding a new solution?*

A. Our global solutions team constantly evaluates security products to include IPSes, and as such started evaluating the Sourcefire technology along with several other IPS products. Using criteria such as manageability, technology and integration within our overall SOC strategies, Sourcefire received a positive evaluation, resulting in our decision to pilot the product in a live environment within one of our existing federal customers.

---

*"...Sourcefire's RNA Sensor helped its IPS rate the criticality of an event. As a result, we saw a reduction by roughly 50% in the amount of events that were initially rated as high. Since the SOC staff spends most of its time evaluating high events, this significantly reduced the workload of our incident responders."*

---

*"Additionally, the ease of management of the product along with the superior time to deploy new signatures from Sourcefire's Vulnerability Research Team (VRT) were also very positive factors in our evaluation."*

---

It is important to note, that we always recommend deploying two or more types of technologies in any one environment in order to provide effective defense in depth. No one product can be successful in identifying all different attacks and attack vectors.

Sourcefire was selected alongside several others and the pilot was conducted in a live environment using a defense-in-depth strategy with one other product.

During the specific testing of the different devices Unisys used a live link and put a number of devices watching the same traffic. This really helped us make a final decision on the product we wanted to move forward with because in testing the competitive product, they had six times the number of false positives and actually caught 16 less real security issues.

*Q. What product did you finally select and why?*

A. The specific product was Sourcefire's IPS solution alongside their RNA Sensor, though we tested it as an IDS using its advanced features and not a fully deployed the IPS solution. Our experience has shown that our customers are hesitant in using the automatic blocking feature of IPS technology. We will reevaluate that again later on as the technology matures and customers are more ready for it. By conducting a constant and systematic inventory of vulnerabilities within the environment, Sourcefire's RNA Sensor helped its IPS rate the criticality of an event. As a result, we saw a reduction by roughly 50% in the amount of events that were initially rated as high. Since the SOC staff spends most its time evaluating high events, this significantly reduced the workload of our incident responders.

The pre-processing capability that RNA has brought to the table was one of the most critical factors in our evaluation of the tool. Additionally, the ease of management of the product along with the superior time to deploy new signatures from Sourcefire's Vulnerability Research Team (VRT) were also very positive factors in our evaluation.

One of the differentiators on Sourcefire's product is the fact that they write rules that look for the vulnerability that is exploited, not the specific exploit itself. For example, Sourcefire's rules were in place that protected against the vulnerability that Zotob exploited, before Zotob came out. The rules were also able to protect against all the variances of it before Zotob that came out during the next week.

*Q. What were the criteria you decided were most important? Why?*

A. The three main criteria we look at are manageability, technology and integration. The manageability of the product looks at how easy it is to manage different policies across a large environment, and how well it allows the analysts to review the data. Technology obviously looks at how the device works and handles network traffic. Items such as signature-based vs. behavioral based mechanisms, integration with vulnerability data and the amount of false positives that the product generates, handling of large throughput or bursts, detection versus protection mechanisms, etc. The integration aspect deals with how the specific product integrates within our overall SOC strategy and tools – including our customer portal and security dashboard. We utilize several tools to provide monitoring, correlation, and long-term storage and reporting, therefore solutions selected must be able to integrate within that model. Finding infrastructure agnostic solutions is very important to us in order to leverage our existing investment and see a smoother integration.

Sourcefire ranked well in all areas with ease of management, solid technology and its open architecture.

---

*“One of the differentiators on Sourcefire’s product is the fact that they write rules that look for the vulnerability that is exploited, not the specific exploit itself. For example, Sourcefire’s rules were in place that protected against the vulnerability that Zotob exploited, before it came out.”*

---

*“Once inside the manager—in this case, the Sourcefire Defense Center—we can view more details about the alert and even start packet captures if necessary. Packet captures are very beneficial tools that we used as part of this pilot which are not always available on other products.”*

---

*Q. How do the needs of Federal SOCs differ from commercial SOCs?*

A. Well it clearly starts with different legislative compliance requirements. With the Federal Information Security Management Act (FISMA), government agencies have to comply with different requirements than most commercial entities. A derivation of this legislation does present some segregation of data issues which had to be considered as we built the SOC in order to support multiple customers. As such, specific security controls had to be applied to our systems above and beyond what is traditionally applied in other commercial SOCs.

The other component (and challenge) is that specific agencies may have different policies and specific hardening requirements. As such we had to look at some of the more common hardening procedures across government agencies (DoD, Intel, and DHS) and applied those to our systems.

The overall result of these legislations and policies is that we provide much more visibility into our systems than we would for commercial Managed Services Providers (MSPs). This helps our customers meet their certification and accreditation requirements.

*Q. What was the deployment process like?*

A. The pilot was a medium-sized deployment and ran for six months. Just as in any other deployment, the key component is to pre-configure the sensors prior to the actual deployment. Once the sensors were preconfigured, we separated key parts of our customer’s infrastructure and used distinct deployment groups which proved very effective. In terms of the Sourcefire product itself, we found the deployment process very easy following a carefully laid out plan. Sourcefire was alongside us throughout the deployment in case of problems, but frankly, we did not run into any significant issues.

*Q. Are there any challenges you found in such deployments?*

A. The largest challenge which we encounter with a deployment of this size is not necessarily related to the product selected, but rather to the underlying infrastructure. Auditing the switch fabric can be a big issue to tackle in order to accurately determine which switch are in the environment, whether they are capable of supporting SPAN ports and how to properly configure SPAN ports.

*Q. Where did you deploy the IDS/IPS Solution?*

A. We typically deploy IDS at all perimeter points to monitor both inbound and outbound traffic on both sides of the firewalls. This allows us to differentiate between attempted attacks and those that made it through the firewalls. Additionally, we recommend deploying IDS at other points in the network, specifically around internal firewalls and server subnets in order to ensure that all traffic is monitored. This is where the Intrusion Sensors were deployed. Insider threats can often be more dangerous and monitoring internal traffic can be as important or more as external traffic.

*Q. What do you see?*

A. The SOC primarily monitors our SEM tool which is integrated with the various IDS products. Once an event deserves further investigation, we will often go to the source of the event and remotely access the management device. Once inside the manager – in this case, the Sourcefire Defense Center – we can view more details about the alert and even start packet captures if necessary. Packet captures are very beneficial tools that we used as part of this pilot which are not always available on other products.

---

*“Throughout the life of the pilot, we saw the Sourcefire devices alert on more events than the other competing product alerted on, thereby catching more threats. Additionally, the alerts that we received were ranked in such a way that we could differentiate between a low alert (unsuccessful exploit) and a high alert (successful attack).”*

---

---

*“Sourcefire is one of the market’s leading IPS/IDS solutions. The capabilities provided by the combination of real time network analysis and one of the most powerful signature detection engines are groundbreaking.”*

---

*Q. What do your clients see?*

A. Our customers have access to all the reports available to us through customized portals. In that sense they see the critical alarms that we saw and can evaluate our response. If they require more information for their investigatory purposes, we can also provide all logs pertaining to their environment. In most cases however, we serve the federal government in an advisory capacity only. While we will often go after routine things, like viruses infection and automatically clean them out, more complex incidents will be run by a government representative with our analysts acting as advisors. As a result of this, the government is notified every time a critical alarm occurs and investigates with us whether it is a false positive or an incident. When this product was piloted, we clearly saw fewer false positives and this resulted in fewer calls to the government. Of the remaining calls we made, these often resulted in more efficient and quick determination of what action had to be taken. This was a direct result of the Sourcefire deployment.

*Q. Do you have any proof it works?*

A. Of course. Like I mentioned earlier, we always recommend deploying two different types of IDS at critical junctures in order to provide verification that threats were properly identified. Throughout the life of the pilot, we saw the Sourcefire devices alert on more events than the other competing product alerted on, thereby catching more threats. This was largely due to the large sets of rules available in this product. Additionally, the alerts that we received were ranked in such a way that we could differentiate between a low alert (such as an unsuccessful exploit) and a high alert (such as a successful attack or infection).

*Q. How was technical support?*

A. They have been quick to respond and we have been very pleased. Sourcefire technical support was always available from configuration support to custom feature development.

*Q. What level of manpower does it require and how much training did your staff need?*

A. Given our Tier 1 Staff’s existing expertise in IDS/IPS they were able to get up to speed with a limited amount of training. They already know and understand how to recognize an event in our SEM console and the proper procedures to following. Sourcefire came on-site and gave a one-day training session to some of our Analysts and Engineers on some specific features of the tool. For a team that already works with various IDS/IPS technologies and products on a day-to-day basis, we found the product to be very intuitive. As a follow-on we did send one Engineer to a week long course with Sourcefire and plan to send a couple of engineers and senior analysts to become certified in the product. We would like personnel certified in the product in order to be able to use its full capabilities to include the prevention component.

*Q. Are there any features you would like to see added?*

A. Some areas of the Sourcefire product would benefit from the ability of further end user customization. For example we ran into an issue with sending emails on alerts; we were unable to remove the alert context from the email or modify the fields of the email to remove or encrypt customer data. Sourcefire was able to generate a custom solution to this problem for us within 48 hours and took our input into consideration for future feature development.

*Q. How do you feel about Sourcefire overall?*

A. Sourcefire is one of the market's leading IPS/IDS solutions. The capabilities provided by the combination of real time network analysis and one of the most powerful signature detection engines are groundbreaking. Finally, the Sourcefire team has been true Partners with Unisys and we've established an excellent relationship.

### SANS BOTTOM LINE ON SOURCEFIRE WITH UNISYS

1. Fairly painless deployment
2. Few false positives
3. Responsive customer service
4. Speedy signature deployment.

### ABOUT SANS WHAT WORKS

SANS What Works saves user organizations months of time that would be wasted in trying to uncover the truth about which Internet security tools actually work in their environments. What Works is a user-to-user program in which managers from organizations that have implemented each of the effective internet security technologies tell a complete story of why they deployed it, how it works, how they know it actually improves security, what problems they faced, and what lessons they learned. Without What Works, buyers are at the mercy of sales people who, too often, do not have sufficient security expertise to understand how their products fit into a defense in depth and what the tools can and cannot do. Only users know the answers to those questions. Smart buyers have always demanded an opportunity to talk to users directly. SANS What Works brings those users to you in written interviews and in live and recorded webcasts where you can get your questions answered.