

IDS isn't dead, your implementation of it is!

Lessons learned from an enterprise deployment: how to maximize your detection capabilities and investment

Rohan M. Amin



26 January 2007

Abstract

In 2003, Gartner said, "IDSs have failed to provide value relative to its costs and will be obsolete by 2005." Fast forward to 2006, their end conclusion has still not been realized; however, many of the shortcomings they noted in their controversial paper are not shortcomings of the technology but rather of the implementation. This presentation reviews a case study of IDS implementation from the world's largest defense contractor and demonstrates why Intrusion Detection, correctly implemented, is still a core component of enterprise security.

About your presenter

Rohan Amin is the Manager of Security Intelligence and Incident Response at Lockheed Martin, one of the world's largest defense contractors. Rohan leads the enterprise team that provides Incident Response, Intrusion Detection, Situational Awareness and Security Intelligence capabilities for the corporation. Rohan has a Bachelor's Degree in Computer and Telecommunications Engineering and a Master's Degree in Telecommunications and Networking from the University of Pennsylvania. Rohan is also, currently, a doctoral student at George Washington University in the NSA Information Assurance program.

Introduction

Disclaimers

- Majority of the lessons apply to a large enterprise, not a small business running IDS for a DSL line.
- Presentation discusses Intrusion Detection in the broadest sense, not just signature-based network intrusion detection tools
- There are no right answers, you need to consider the spectrum of options, adapt and develop the right solution for your organization

What many large enterprises do today

- 24 x 7 x 365 security operations center
- "lots of monkeys staring at a screen" (Dave Aitel, 26 Oct 2006)
- IDS a la Ron Popeil (also known as Checkbox Security) - "Just set it and forget it!"

Key Focus Areas



Too often, implementation is technology specific without much consideration for people or process. Often, technology and process are considered first, people last. Implementation should consider all three.

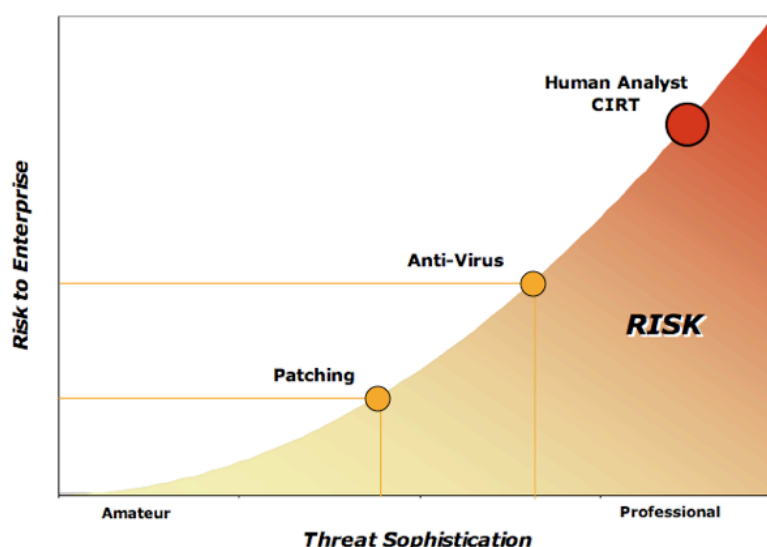
Contact Information:
Rohan Amin, rohan.m.amin@lmco.com

People

Key Challenges

- Leveraging the right talent - Your most qualified analyst will not want to be pigeonholed into looking at security event data all day, categorizing all of the various events. Your entry level analysts might be ok with staring at a screen all day but can they uncover any real threats or can they only understand the “red, yellow, green” output from your tool?
- “Toolitis” - Many large organizations suffer from “toolitis”, a phenomena where the organization believes that the solution to security problems is more and more tools. While tools are important, you don’t want to develop a culture where the analysts are supporting tools – you want the tools to support the analysts.
- Situationally Unaware Analysts - Analysts who only consider security events on a event-by-event basis instead of within a broader activity context will not be able to uncover serious threats.

Before you invest in another security tool, invest in your people!



Patching and Anti-Virus are necessary but no longer sufficient. To combat professional threats, you need qualified analysts.

False Metrics of Success

- “We have processes” - While processes are important, there is no process for “how to uncover a true threat.” Skilled analysts will devour data and understand the real threat. No process can walk an analyst completely through that thought process.
- “We have training” - Training is important, but you don’t want to create analysts who can click all of the buttons in your tool but have no clue what they are looking at. Fundamental understanding is important. When you provide training, make sure you provide a balance of vendor agnostic and vendor specific training.

Key Takeaways

- Size of your IDS team - The number of sensors and data feeds into your IDS is not linearly related to the number of people you need on your IDS team. For example, if you add 3x the number of sensors, does not mean your team needs to be 3x in size.
- Automate, automate, automate! - If you need to write a detailed step-by-step SOI for your analysts, then you can write a script to perform that function.
- Hire talent, not warm bodies - A single, highly qualified analyst will understand and uncover more real threats than a team of entry level analysts who can only tell you what the tool tells them.
- Talent begets talent - Technical individuals are drawn to other technical teammates. Additionally, a technical manager is best suited to identify top technical talent.

Process

Tuning is critical

You must tune your IDS. Furthermore you must be able to look back and understand the tuning decisions that you made. That means you need to document your tuning parameters and understand the impacts of your tuning (you might have more false negatives or false positives, for example).

IDS is only as good as your network tapping points

Large enterprise environments are highly dynamic and a successful IDS implementation requires that your IDS team is well integrated into the network change management process. The smallest network changes such as routing, bandwidth upgrades and new firewalls can significantly impact your ability to analyze the right traffic.

Outside vs. Inside - Both!

There is lots of debate in IDS literature about the pros and cons of inside-the-firewall vs. outside-the-firewall deployment. Make sure your process and implementation account for both. Your IDS inside the firewall can tell you what is successfully bypassing your firewall and your IDS outside the firewall can tell you what compromised machines you have internally that are successfully beaconing or “phoning home”.

Your response process should not include your vendor

Some vendor implementations require you send traffic samples to the vendor for analysis (those same vendors don't allow you to view their signature details). If your response process relies on your external IDS vendor for support for event resolution, you will never be able to keep up.

A 24x7 operations center isn't needed for success

Where in the IDS manual does it say you need to have a 24 x 7 operations center? Such centers drive tremendous cost and complexity, mainly because of the large labor requirement. Assuming you are able to even staff an around-the-clock operation with the appropriately qualified staff, is the rest of your enterprise also available 24 x 7 to respond? If your third shift analysts are only able to respond to 'red, yellow, green' on your tools, why not just script your tools to page you if something in the late hours occurs?

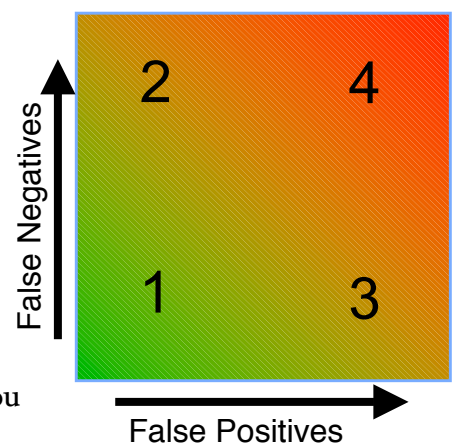
Technology

Most Vendor Signatures Stink

Vendors strive to give you signatures which have 100% detection with no chance of false negatives. A “quadrant 3” solution has virtually no false negatives but inundates the analyst with false positives. Be sure to understand the limitations of your signatures.

Custom Signatures are a MUST

You must be able to create robust custom signatures with your tool of choice. With today's threat being highly dynamic and surgical, your vendor won't see the attacks that you do and won't have the turnaround you need. With custom signatures you can also try to develop “quadrant 1” signatures which balance false negatives and false positives.



You MUST be able to see the internals of a vendor signature

Some vendors don't allow you to see the signature details, instead having you rely on some generic documentation. When you don't have the detail to analyze, your only course of action

is to ask the system administrator of the target system for an impact analysis -- that severely hampers your ability to rapidly analyze data.

Leverage existing tools before deploying new

Organizations that suffer from 'toolitis' deploy more and more tools without exploiting the full capabilities of the tools they have in place. Investigate the full capability of tools you have before you look to deploy something new -- you might be surprised.

Don't be obsessed with a 100% solution

Some are quick to dismiss IDS because it can't detect everything or that it can be evaded. Anti-Virus has long been able to be evaded but security professionals are not recommending that it be removed from your systems. IDS won't always catch new attacks, just like Anti-Virus. Use it for detection once you know what the problem is and you are trying to determine how much of your enterprise is affected. IDS is a reactive technology.

Your IDS implementation should not be limited to signature based IDS

A complete capability for detecting intrusions should include flow analysis tools and, to the extent possible, a full packet capture and reconstruction capability. The "network TiVO" is needed to understand the full context of an attack.

Understand the limitations of your IDS and complement it

Today's attackers who leverage gzip compression, base64 encoding and other evasion techniques can trivially evade detection. Be sure to understand the limitations of your IDS. IDS isn't good, for example, at detecting 'file-based' exploits (e.g. WMF) or at detecting trojans embedded in email, both of which traverse your network.

Your IDS is not a VDS

If you use your IDS primarily to function as a VDS (Virus Detection System) you are not leveraging your investment. There are also several non-intrusion related applications for IDS that should be considered. IDS is also useful for detecting already compromised machines, do not forget that!

People are more important than technology

Absolutely nothing can replace a qualified analyst who is able to decipher the myriad of data you have and convert it into actionable intelligence.

Summary

In 2003, Gartner said, "IDSs have failed to provide value relative to its costs and will be obsolete by 2005." The key of their famous statement is "relative to its costs." For your IDS implementation, keep in mind the following:

- 24 x 7 x 365 isn't absolutely necessary and it drives huge cost
- Fewer more qualified analysts are better than many unqualified analysts. Hire the right talent, not just warm bodies.
- Implement technologies which your qualified analysts can customize and tune for your environment.
- Deploy technologies that when implemented together provide a combined value greater than the individual value of each tool (signature based IDS, flow analysis, full packet capture).
- Don't be obsessed with 'real-time' response and 100% initial detection. Understand your tool limitations and maximize your investment.