Maximizing the Benefits of Intrusion Prevention Systems: *Effective Deployments Strategies*

Charles Iheagwara[1], Farrukh Awan[2], Yusuf Acar[3], Calvin Miller[4]

1. Computer Emergency Response Team Coordinator, Citywide IT Security, Office of the Chief Technology Officer, District of Columbia Government, USA
2. Security Architecture & Engineering Manager, Citywide IT Security, Office of the Chief Technology Officer, District of Columbia Government, USA
3. Security Operations Manager, Citywide IT Security, Office of the Chief Technology Officer, District of Columbia Government, USA
4. Director, Citywide IT Security, Office of the Chief Technology Officer, District of Columbia Government, USA

Abstract

This paper discusses general intrusion prevention systems concepts and provides a context-based analysis of the techno-economic imperatives as the driver of this technology. Further, in light of the Gartner 2004 recommendations, the paper examines the security needs and functional requirements for enterprise network IPS deployments. Given the complexity of the implementation environment, the paper will seek to demonstrate the value associated with a well thought out deployment strategy. To this end, the paper introduces performance measures and proposes effective deployment strategies to enhance the performance the IPS. Using field data, we measure the financial benefit of an IPS deployment.

Keywords: Intrusion Prevention Systems; Return on Investment

1 Introduction

In the last eight to seven years, intrusion detection systems (IDS) have been recognized as an essential and indispensable layer within enterprise security formation and architecture. The continued growth and complexity of cyber threats and increasing liability costs of cyber threats have led to wide adoption of network IDS products in Fortune 500 organizations. Yet, despite popular adoption, there remains significant dissatisfaction regarding the current crop of network IDS products. Central to this is the numerous issues confronting many security administrators in successfully deploying and deriving value from current IDS technology. Among the most pressing issues are six basic drawbacks of current IDS products that limit its effectiveness as a security solution [1]:

- Performance Barriers
- Detection Accuracy
- Product Complexity
- Growing IDS Evasion
- Passive Device
- Enterprise Scalability

The drawbacks were put squally in front of the burner when research firm Gartner Inc. provided another nudge when it declared IDS will be obsolete by 2005 [2]. The report accelerated the call by some industry analysts to kiss a final goodbye to the IDS as an essential security technology. And since then, the death knell for intrusion detection has been getting louder.

Gartner provides three reasons for this:

1. “99 out of 100” alerts mean nothing
2. Plethora of false positives
3. Voluminous amounts of data

Instead of using IDSes, Gartner recommends that businesses invest their security dollars on firewalls that block attacks, rather than alert administrators to them. "The underlying problem with IDS is that enterprises are investing in technology to detect intrusions on a network. This implies they are doing something wrong and letting those attacks in," said Gartner vice president of research Richard Stiennon [3]. "Enterprises investing money to alert them when the next SQL Slammer worm arrives is a waste of money."

Thus, according to Gartner's Information Security Hype Cycle, intrusion detection has failed to deliver value relative to its costs. Enterprises have been quick to decry IDS for the plethora of false positives it generates, for the voluminous amounts of log data administrators have to pore over and for its inability to monitor at speeds of more than 600 Mbps.

Instead of IDSes, Gartner advocates firewalls that work both on the network and application levels will supplant intrusion detection and intrusion-prevention systems within two years.

In the aftermath of Gartner’s assertions, many industry analysts have risen to the defense of IDSes; and calls for improvement of existing technologies. For example, Andre Yee, NFR Security [4] writes:

“The Silver Bullet Syndrome… In view of these perceived limitations, some industry pundits are writing off IDSs altogether in favor of newer network intrusion prevention systems (NIPS). However well intended, casting NIPS technology as a remedy to all that ails the IDS is an unfortunate oversimplification. There are three reasons for this. First, as noted in the prior section, many of the issues regarding current generation IDS products are unrelated to the issue of "prevention versus detection". For example, the distinct challenge of scaling IDS from a point product to an enterprise solution have more to do with good design than with the benefits of prevention over detection. A poorly designed NIPS product will undoubtedly encounter similar scalability problems as a poorly designed IDS product…”

Thus, the prevailing concerns about IDS provides the need and is an impetus for a new kind of network intrusion management product that comprehensively addresses the limitations of current products while delivering better detection, enterprise manageability, and prevention.

In the last two years, there has been some noticeable progress in the development of intrusion prevention systems (IPS). Some of the developments are in the beta testing stage and others have made their debut in the IPS in the market place.

Against this background, this paper presents the business and technical imperatives of the IPS and reviews IPS concepts and implementation, analyzes performance factors and proposes effective deployment strategies.

Finally, this paper presents the benefits associated with a few IPS deployments that are implemented based on the proposed deployment strategies.

2 Business (Techno-economic) Imperatives

There are always two aspects – technical and economic - to consider when making a decision to deploy a security device. Collectively, these become the imperatives. Iheagwara et al [5] demonstrate that the performance of IDS for many organizations is not just measured in their ability of the IDS to capture or prevent attacks but on its value when expressed in economic terms. This is more so because when choosing a security product, companies tend to justify their investments based on both economic returns and technical performance. Further, Iheagwara demonstrate that in the selection of an IDS product, performance is measured using such factors as scalability, availability, ROI and the total cost of the system relative to the price of the system the IDS is protecting, just to mention a few. The above assertions holds true for IPS implementation considering that both the IDS and IPS have similar technological structure and are mutually complimentary.

Therefore, in considering implementation of an IPS, there is the need to demonstrate both the business and technical needs or imperatives. As for the technical needs, the IPS compliments IDSes and other network security devices. Section 2.1 presents the business imperatives.

2.1 Business Demands of Security

The business needs for intrusion prevention systems (IPSes) and other security devices arose out of the need to protect enterprise IT infrastructures. Three basic premises define the needs:

1. Mission critical applications and systems must be available
   - What are my mission critical applications and systems?
   - Which critical assets are at risk? Under attack?
2. Regulatory compliance and risk mitigation are a modern business reality
   a. Are we compliant with rules and regulations?
   b. We've invested all this money – how secure are we?
3. Resources are constrained
   a. Turn-key, real-time, 24*7 security infrastructure.
   b. Cost-effectiveness is paramount.

Statistics from different sources present the picture of the nature and scope of security breaches and the collateral effects on enterprise infrastructures. For example, The Computer Economics Journal [6] states that the costs associated with Virus'/Worms and other outbreaks are enormous and our ability to defend hasn't gotten better same staff and technologies that haven't increased or improved. The journal estimates the worldwide 2004 financial impact of major virus attacks to be $17.5B. This figure includes the following 2004 virus attacks: Sasser - $3.5B, NetSky - $2.75B, Bagle $1.5B, MyDoom - $4.75B, Etc

Here, we note a few grim trends and some (very real) problems for enterprise security systems:
Multiple points of vulnerability:

- Networks have multiple points of vulnerability based on the dissolving perimeter, also
  - Vulnerabilities & Exploits have ballooned

"

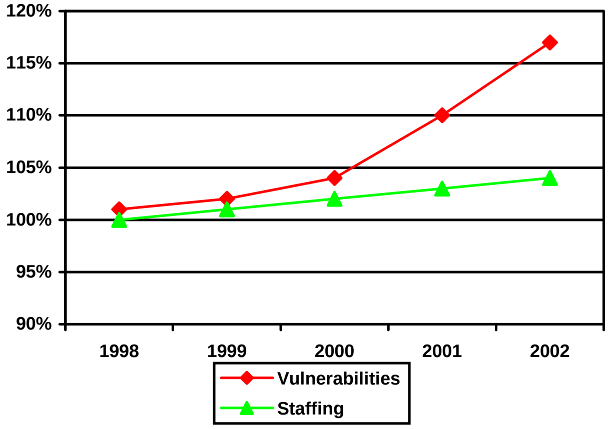

Figure 1: Resource Gap

- Everyone is suffering from the consequences

Relentless:

- The time between vulnerability disclosure and exploitation has dropped from 288 days in 1999 to less than 6 days by mid 2004 *(Secure Computing Magazine)*
- During the first half of 2004, 4,496 new Windows viruses and worms were released - four and a half times the same period in 2003 *(Symantec Security Report)*

Pervasive:

- Last year, 94% of organizations surveyed experienced security-related downtime *(Network World)*

Expensive:

- Resolving external disruptions (e.g. a hacker) cost business an average of $54,380 per event *(OMNI Consulting)*
- The total cost per security incident, not including incidental loss, exceeds $2M *(Aberdeen)*

Thus, the above security risks are the primary motivation for the decision to deploy a security mechanism such as IDS, and also make the case for the constant evolution of security technologies to keep up with the continuously increasing scope and breadth of security breaches. But the addition of the IDS as an enterprise security device has raised several questions in view of the operational problems.

The pitfalls of IDS deployments led to all sorts of hue and cries. In fact, Gartner [2] asserts, "IDS is dead." The contention is that:

- "99 out of 100" IDS alerts mean nothing
- There is a plethora of false positives
- There is a voluminous amounts of data to be processed
- And therefore, not workable

Of course the problems exist and the "First generation IDS" is somewhat considered dumb, lacks precision and the staffing needs are huge. This presents the business case to refine the IDS. The approach is to deploy the IDS in line (as an IPS) instead of out of band. The Gartner report articulates (Section 2.2) the requirements to make the technology workable.

2.2 Needs specification

Gartner [2] made *"Action Recommendations for 2004"* for second IDS generation approach.

"

The Table below presents the recommendations and the expected functionality the IDS must have to realize the recommendations.

Table 1: Second Generation IDS Requirement for Real-time Network Defense.

Number	Gartner Requirements	Useful Functionality of the IDS
1	Near Continuous Scanning	Real-time Discovery
2	System Change Alerts	Real-time notification
3	Identify unmanaged “nodes on network	Real-time notification
4	Receive frequent vulnerability updates	Real-time vulnerability database
5	Ongoing monitoring for baseline compliance, vulnerabilities, and threats	Real-time monitoring for baseline compliance, vulnerabilities, and threats
6	Standards-based interface to firewall, anti-virus and intrusion prevention systems to support rapid shielding	ABC’s of Defense – Alert, Block, or Correct

Item 6 in Table 1 specifies the need for IPS addition into the technology mix in the enterprise.

3 Overview of Intrusion Prevention System Technologies

3.1 Definitions

Intrusion Prevention is the act of dropping detected bad traffic in real-time by not allowing the traffic to continue to its destination, and is useful against denial of services floods, brute force attacks, vulnerability detection, protocols anomaly detection and prevention against ‘Zero day” (unknown) exploits.

Although some organizations have integrated the products and technologies - especially at the network level (NIPS) - into their enterprise security architecture, it's still too early to say exactly what an intrusion-prevention system is because companies use the term a half-dozen different ways. Some use the term to describe next-generation IDS systems that can block certain kinds of attacks. Others use the term more broadly and include firewalls since they can block certain attacks. Whatever the context and the actual meaning in the security lexicon, intrusion prevention technologies combine features of a standard IDS, an IPS and a firewall and is sometimes known as an In-line IDS or IPS.

A basic distinction is that the IDS is an out of band technology whereas the IPS sits in-line on the network. In this case, the IPS monitors the network much like the IDS but when an event occurs, it takes action based on prescribed rules. Security administrators can tweak such rules so the systems respond in the way they would.

3.2 Intrusion Prevention Approaches

"Intrusion prevention" can be achieved through three main approaches:

1. Secure engineering - building systems with no vulnerability,
2. Taking perfect remediation steps to uncover vulnerabilities and patch them, and
3. Detecting the exploit attempts and blocking them before serious damage is done.

Of course all the three approaches are mutually inclusive. It needs to be noted that the failure to use secure engineering to prevent intrusion is the main reason for introducing intrusion detection. Equally, remediation while useful in mitigating vulnerabilities has never been an end-all solution either due to associated difficulties including lack of automated deployment tool in some cases and the unusually high number of vulnerabilities that are prevalent in IT systems both on the hardware and software sides. And the failures of the two approaches outlined above have given rise to the third approach intrusion prevention.

Although intrusion prevention is new and its relative importance and place is still being debated, critiques point to it as en extension of firewalls. This is because application firewalls and IDSs are usually marketed as an intrusion prevention solution rather than a traditional IDS solution. While there are some similarities between the two, there are obvious differences. One of the main differences is that firewalls are implemented using packet-based technologies. In other words, each traffic that passes through is examined on a packet-by-packet basis. And inherently, firewalls are not able to track sessions. On the other hand, IDS/IPS technologies are session-based, i.e. traffic flow is examined based on session flow. Thus, the main issue is that today's firewall does not offer the granularity to differentiate a normal instance of application session from one that is delivering the attack. From this perspective, prevention is a natural new capability available from newer IDS technologies.

Depending on the deployment environments, IDS as we know it - monitoring only will continue to play an important role in implementing security policies. As Martin Roesch [8] puts it “Intrusion prevention is access control. Intrusion detection is monitoring." With inline blocking capability (IPS as interpreted in this context), we now have a much more effective policy enforcement tool.

3.3 In-line Mode Vs. Out of Band Concepts

As stated before, the IPS operates on the In-line mode i.e. the sensor is placed directly in the network traffic path, inspecting all traffic at wire speed as it passes through the assigned port pair. In-line mode enables the sensor to run in a protection/prevention mode, where packet inspection is performed in real time, and intrusive packets are dealt with immediately – the sensor can drop malicious packets (defined though policy) because it is physically in the path of all network traffic. This enables it to actually prevent an attack reaching its target.

Thus, given the mission defined for it and in contrast to the IDS, the IPS mode of operation enables it to provide preemptive protection.

4 Strategies for Effective Deployment

4.1 IPS Performance Metrics

The basic performance indicator of the IPS is reflected in the success or failure of the IPS detecting and preventing attacks which are quantifiable.

“

There are performance studies [9, 10, 11] that demonstrate the different aspects to this, although for related technologies. For example, the performance metrics for IPS can be expressed in terms of those expressed for the IDS. Iheagwara et al [10] demonstrate that the performance of IDS is not just measured in their ability to capture or prevent attacks (when in reactive mode) but on its value when expressed in economic terms. This holds true for the IPS. And given the functional requirement for the IPS, the performance metrics should be measured in terms of:

- The IPS's dynamic alerting capability,
- The IPS's dynamic blocking capability, or
- The IPS's ability to correctly identify attacks.
- The IPS's ability to identify if a system's patch level makes it susceptible to impending attacks,
- The IPS's Accuracy of dropping packets
- The number of false positives
- The IPS's Fail open and fail safe capability
- The IPS's High availability and redundancy architecture

4.2. Effectiveness Measures

The decision to invest on the IPS hinges on the ability to demonstrate a positive ROI. In essence, this entails quantifying the IPS's value prior to deploying it. A positive return on security investment (ROSI) is dependent upon an organization's deployment strategy and how well the successful implementation and management of the technology helps the organization achieve the tactical and strategic objectives it has established [12]. ROI has traditionally been difficult to quantify for network security devices, in part because it is difficult to calculate risk accurately due to the subjectivity involved with its quantification. Also, business-relevant statistics regarding security incidents are not always available for consideration in analyzing risk.

Therefore, the effectiveness of the IPS will be tied to a positive ROI value. A case can be made by manipulating risk equations [5] that the ROI depends on how the IPS is able to prevent and mitigate threats to the protected network segment and resources.

Also, there are various variables that factors in risk equations that are directly related to the management methods for any security device. Iheagwara [5] examines how implementation methods, management methods, and intrusion detection system (IDS) policy affect Return On Investment (ROI). He demonstrates the value associated with a well thought out implementation and effective lifecycle management of IDS technology.

In the next Section, we propose deployment strategies for "Best Practices" and effective management of the IPS that improves the ROI value.

4.3 IPS Deployment Strategies

Generally, there are several product configurable and network/system parametric variables that affect the performance effectiveness of the IPS:

- High Bandwidth Throughput
- Minimum Packet Latency
- Accuracy of Detection

- Accuracy of Dropping Packets
- Ability to detect unknown attacks (Protocol Anomaly)
- Few false Positives
- Policy based Controls
- Fail Open and Fail Safe Capability
- High Availability and Redundancy Architecture

Some the variables depend on the choice of deployment (i.e. placement location and configuration of the product’s tunable parameters) while the others depend on network/system variables such as bandwidth availability, packet latency that in turns depends on the network architecture, etc.

Given the above, optimization of these parameters is crucial to the performance of the IPS and poses serious challenges to systems and security administrators as they try to optimize the IPS implementation decisions. The following presents some useful viewpoints on deployment strategies that can help optimize the IPS deployment.

4.3.1 Area of coverage

An improper IPS deployment scheme or configuration provides little or no value in the event of an attack against the protected network segment. Therefore, to maximize the benefits of the IPS, it must be deployed in a way that positions the traffic streams to transverse through it for a wider scope of visibility such that it can perform a deep inspection of the packets and based on the pre-defined rules take appropriate actions i.e. allowing passage of the packets, sending an RST, dropping packets, etc.

Based on previous studies [10] and data from our field practice [AWAN], we propose the following deployment location to maximize the IPS effectiveness:

- Deployment where high security and protection is required
- Deployment at the defense perimeter
- Deployment where there is a high probability of an internal outbreak and attack; and
- Deployment through strategic segmentation of the network into smaller areas for better distributed architecture

4.3.2 Deployment Scenarios

Generally, the IPS can be deployed within the following scenarios:

- IPS Deployed at Ingress/Egress (like traditional Firewalls)
- IPS Deployed at Network Core Trunk
- IPS Deployed at Network Access layer Trunks

Deployment at Ingress/Egress

In considering the choice of a particular scenario over the other, it is important to consider the benefits associated with each scenario and the suitability for each environment.

The advantages of deploying the IPS at Ingress/Egress point within the network like traditional Firewalls and NIDS are few but much defined. This style of deployment allows stopping malicious traffic from entering or leaving the network perimeter and internal outbound traffic.

This type of deployment is most useful in preventing attacks against Perimeter infrastructure e.g. if some is trying to compromise Border router, Firewalls and VPN devices. This approach can also be useful in protecting Secure Zones such as DMZ.

At the same time, there is a high amount of generated alerts as the perimeter s often the starting point for attackers who are probing for vulnerable systems. Also, devices deployed at Ingress/Egress Points within the network offer little value in preventing internal outbreaks from spreading to other internal areas within the network. For instance, a single infected internal host could potentially infect every other vulnerable internal host without traversing through the IPS thereby generating a negative ROI value.

Deployments at Core switches and Access layer Trunks

IPS Deployments at Core switches and Access layer Trunks VLANS provides the most coverage area and protection against internal attacks. With this strategy it defines very small containment areas where in the event of an internal outbreak the infection will be able to propagate only within a single area. In cases where the majority of the hosts on any given access layer switch device are in dissimilar VLANs, the containment are may be reduced even further due to the necessity of traffic traveling from one VLAN to another to traverse the core switch/router device. This deployment strategy is the most effective as it is closest to the end user but not cost effective since in order to cover 100%, IPS needs to be deployed at each Access layer Switch. The Real World deployment is to deploy IPS on Core Switch Truck VLANS to provide high degree of protection against internal and external threats.

The best approach is to optimize the deployment using a combination of all the above approaches with deployment at Perimeter; Core switches on Trunk VLANS and critical access layer switches. In the Figure 2 below, the IPS deployment is distributed to protect Internet Firewall, DMZ and Intranet against external attacks from Internet. The advantage of placing IPS on the Trunk VLAN between core switch give access to all VLANS as the traffic passes through Truck via trucking protocols (802.1q).

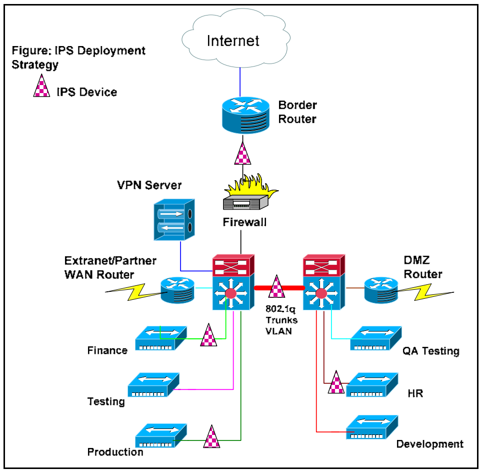

Figure 2: Distributed IPS deployment

4.3.3 Specifications for Bandwidth, Availability and Interface Type.

Two important issues to consider with respect to the IPS performance are:

1. Varying bandwidth levels for different interfaces,
2. Failover/Failopen mechanism.

With respect to the bandwidth level, one key criterion to determine in the deployment is the bandwidth requirements on the Trunk link and the type of interface i.e. the use of fiber or copper interfaces based on the core switch topology. In this regard, it is worthy to note that 802.1q Trunks often carries extremely heavy load of traffic and this may result in the saturation of the inline IPS devise causing it to drop packets it cannot handle.

As for failover mechanism, considerations should be given to configuring the IPS with fail open arrangement such that when the IPS malfunctions, it acts like a wire or the IPS needs to be configured in array so it fails secure. Thus, at a minimum the IPS should fail open, regardless of the network media to provide high availability along with low latency, which is often the most critical performance factor for Network Intrusion Prevention Systems.

5 Empirical Performance Data and IPS Value Proposition

In considering the implementation of any IDS/IPS technology, a return on investment can be understood by analyzing the difference between annual loss expectancy (ALE) without IDS/IPS deployment and the ALE with IDS deployment, adjusted for technology and management costs. The ultimate initial goal, then, should be to prove that the value proposition (re: a benefit in the form of a quantifiable reduction in ALE) in implementing and effectively managing the IDS/IPS technology is greater than the implementation and management costs associated to deploying the technology [12].

A few available statistics from implemented IPS systems present a somewhat positive picture. And, considering the limited time that IPSes have been introduced in enterprise systems, it will be a while before a clearer picture emerges on the IPS performance relative expectations since Gartner.

For now, it is known that immediate benefits have begun to accrue from current deployments. One implementation using T-1 outbound connection on a network system [13] asserts the following:

1. Prior to implementation, infected internal machines were choking bandwidth to a point of uselessness
2. IPS implementation prevented T-1 upgrade resulting to a saving of approximately $600 per month
3. The IPS identified infected machines and kept Blaster Virus traffic off the network.
4. When an IPS was implemented on outbound T-1 connection, substantial bandwidth was reclaimed (wasted bandwidth average from 3Mbps to <1Mbps) and prevented T-1 upgrade (saved ~$600 per month). The actual traffic data is presented in Figure 3.

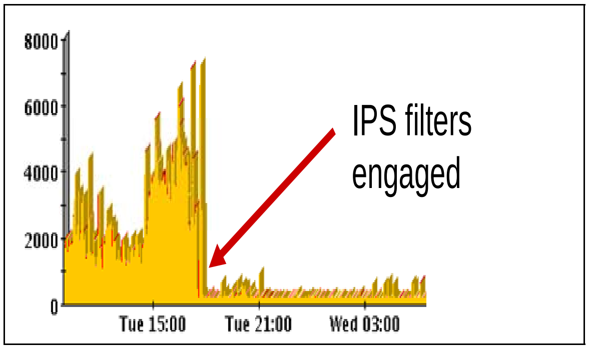

Figure 3: Bandwidth Utilization with and without IPS filters.

In Figure 3 above, bandwidth consumption is represented on the “X” (vertical) axis while the “Y” horizontal axis represents time in minutes.

Also, data obtained from implementation of the IPS on network [13] shows:

1. That the IPS is blocking over 100,000 attacks per month.
2. That estimates for prevention of Viruses, Worms, Spyware is roughly 5000 infections

For the 5000 infections prevented, we can express the economic benefit (EB) of the damages prevented in the form of:

EB= (Repair Time X Wages X Attacks Blocked) =2hrs X $40 X 5000 = $400,000
Where the time to repair an infected workstation = 2 hour; and
The Sys Admin hourly wage = $40.

The EB while not exactly an exact computation of return on investment, nevertheless, is a pointer to a positive ROI in the above case given.

Conclusion

Inline-IDS (IPS) provides real-time intrusion prevention with proactive dynamic blocking capabilities based on predefined policy, which can be adjusted accordingly to stop attacks before damage can be done. Several industry analysts have pointed out the importance of using intrusion prevention as a means of risk management. To this, we have presented the underlying concepts and mode of operation of the IPS and underscored the business imperatives for the technology.

When an IPS device is deployed in a complex environment, there are several factors/variables that influence the performance. And, hence to effectively deploy the IPS, there is the need to have a sound understanding of the environment where the IPS is deployed including, at a minimum, the impact of deployment location, area of coverage, bandwidth levels and interface type. In line with this, we have presented the factors/variables and analyzed how they affect the IPS performance.

Additionally, we proposed strategies to optimize the effectiveness of the IPS using proven deployment techniques. Thus, the contributions made by this paper are in the formulation of strategies to enhance the performance effectiveness of the IPS.

“

Finally, we measure the financial benefit of an IPS deployment from performance data obtained from field practice.

References

[1] C. Iheagwara, "The effectiveness of intrusion detection systems." Ph.D. Thesis, University of Glamorgan, Pontypridd, Wales, 2004
[2] http://www.esecurityplanet.com/views/article.php/2228631
[3] http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci905961,00.html
[4] A. Yee, "The intelligent IDS: next generation network intrusion management revealed." NFR security white paper. Available at: http://www.eubfn.com/arts/887_nfr.htm
[5] C. Iheagwara, "The Effect Of Intrusion Detection Management Methods On The Return On Investment" *Computers & Security Journal,* Vol 23, issue 3, pp 213-228, May 2004
[6] The Computer Economics Journal "Cost estimates for viruses and worms." 2004
[7] SourceFire, Inc. "Real-time Network Defense - The Most Effective Way to Secure the Enterprise." White Paper, Columbia, Maryland, 2004
[8] E. Hurley, "Intrusion prevention: IDS' 800-pound gorilla." News Article, April 8, 2003 http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci892744,00.html
[9] C. Iheagwara and A. Blyth, "Evaluation of the performance of IDS systems in a switched and distributed environment," Computer Networks, 39 (2002) 93-112
[10] C. Iheagwara, A. Blyth and M. Singhal**, "**A Comparative Experimental Evaluation Study of Intrusion Detection System Performance in a Gigabit Environment," Journal of Computer Security, Vol 11(1), January, 2003
[11] K. Richards, "Network Based Intrusion Detection: a review of technologies," Computers & Security, 18 (1999) 671-682.
[12] C. Iheagwara, A. Blyth, K. David, T. Kevin, "Cost – Effective Management Frameworks: The Impact of IDS Deployment on Threat Mitigation." Information and Software Technology Journal, Vol 46, Issue: 10, pp.651-664, May 2004
[13] TippingPoint, Inc. Case Study. Available at: http://www.tippingpoint.com/pdf/resources/casestudies/505323-001_UnivofDaytonCaseStudy.pdf

"