Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Running a World Class Intrusion Detection Program: More Than Just Picking the Right Tool

In today's security landscape, Intrusion detection systems have joined firewalls as "must have" tools, but getting the greatest benefit from these devices requires much more than a deploy and move on strategy. IDS requires constant care and feeding as the environment being protected changes and new threats are being released on an ever-more frequent basis. Proper implementation, on-going support, and constant event analysis are crucial to the success of an IDS program. This paper will discuss best practices in managing...

Copyright SANS Institute
Author Retains Full Rights

AD

Running a World Class Intrusion Detection Program – More Than Just Picking the Right Tool

J.D. Aupperle

March 2, 2004
GSEC Practical Version 1.4b option 1

Abstract: In today's security landscape, Intrusion detection systems have joined firewalls as "must have" tools, but getting the greatest benefit from these devices requires much more than a deploy and move on strategy. IDS requires constant care and feeding as the environment being protected changes and new threats are being released on an ever-more frequent basis.
Proper implementation, on-going support, and constant event analysis are crucial to the success of an IDS program. This paper will discuss best practices in managing an IDS program to ensure that an organization is gaining the most benefit from the IDS.

What's the point of IDS?

IDS has a bad name. The name Intrusion Detection System invokes thoughts of keeping hackers at bay and securing your network. Intrusion detection systems are lumped into the category of must have security tools, and even more so than other security tools, are only as good as the program behind them. IDS, like firewalls, anti-virus or other mainstream security tools can in some ways be detrimental to a security program because they can provide a false sense of security. In fact, according to Jack Danahy in his article "Down With IDS", "In addition to providing a false sense of security, an under managed IDS may lead to corporate liability."[1] According to Danahy, "if a customer or partner was hurt because of the attack, and that damage could have been reasonably foreseen and prevented given the data in the IDS logs, then it's quite possible that it could result in claims of negligence."[2]

The fact of the matter is that traditional IDS systems by themselves don't keep hackers out and they don't secure anything. At their most basic level, ID systems are glorified network packet sniffers or log analyzers. So what's the allure then? Why are ID systems run by most organizations that have security programs? The answer is simple. An IDS can provide information to assist in improving the overall security posture of the organization. While the tool can glean the security-related events from the everyday network traffic, it's the analysis of these events in the context of the organization that really provides the value and defines why organizations use Intrusion Detection systems. As put by Cyrus Peikari and Anton Chuvakin in their book Security Warrior, "The main value of IDS". . ."is in knowing what is really going on. Yes, an IDS also helps with post-incident forensics, provides network and host troubleshooting, and even serves as a burglar alarm (with the corresponding limitations). However, its primary

[1] Danahy
[2] Danahy

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

function is telling you what security-relevant activities are going on inside the network and systems you control."[3]

An IDS program is a valuable asset to any Information Security program; however, there is a fine line between running a successful IDS program that provides a benefit to the organization and a program that is viewed as expensive and with questionable results.

Defining the program and getting support

Justifying the need for an Intrusion Detection program in an organization can encounter some resistance. Intrusion detection is resource intensive and expensive. Justifying the need involves getting necessary approval for this expense, which is not always an easy sell. As with most security products and programs, the return on investment is difficult to realize, unless there's been a compromise and losses to the bottom line can be directly correlated to the compromise in the form of lost sales or civil lawsuit payouts to affected customers. Security should be viewed as a cost of doing business. Security can be compared to insurance in a way. You may never need it, but your organization and its assets are attacked, you'll be glad to have it. According to Steven Northcutt and Judy Novak in their book "Network Intrusion, An Analyst's Handbook", "There is a bang for the buck using intrusion-detection systems; you can show it and you can quantify it"…"risk is part of the business equation."[4] Intrusion detection systems can help reduce the annualized loss expectancy by helping to tune a firewall and other defenses to be resistant to attacks as well as providing a compensating control for systems where vulnerabilities need to be left on systems.[5]

If an organization does not currently have an intrusion detection program in place, the first question that should first be answered is "Is an IDS program needed?" An intrusion detection program is going to provide the most benefit to an organization if the security program has matured to the appropriate level. In "Network Intrusion Detection, An analyst's handbook", the authors list "The Seven Most Important Things to do if Security Matters" (see below). Of these items, Intrusion detection and incident response come last on the list. This list is a good set of guidelines to help determine if an organization is at an appropriate point to start an ID program. It is not logical to spend the money for intrusion detection if security policies have not been defined to help determine what is acceptable versus unacceptable activity. Likewise, money may be better spent in areas that provide an immediate improvement in security posture such as deploying firewalls or implementing a vulnerability assessment program.

[3] Peikari, p 434
[4] Northcutt, p. 387
[5] Northcutt, p. 387

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The Seven Most Important Things to Do If Security Matters[6]

1. Write the security policy (with business input).
2. Analyze risks, or identify industry practice for due care; analyze vulnerabilities.
3. Set up a security infrastructure.
4. Design controls, and write standards for each technology.
5. Decide which resources are available, prioritize countermeasures, and implement the top priority countermeasures you can afford.
6. Conduct periodic reviews and possibly tests.
7. Implement intrusion detection and incident response.

It is vitally important for the individual championing the program to understand the business and that choosing security is a business decision. The focus of the business case should be on risk and how the implementation of the program will contribute to the mitigation of risks like doing business on the Internet or allowing network connectivity to business partners and vendors. Industry statistics surrounding attack activity towards organizations in your industry can be found on the Internet and should be included. The "sky is falling" syndrome should be avoided while relaying the fact that attacks and intrusions do in fact occur at a certain level for organizations in the industry. These statistics will help the business understand the risk and make informed decisions regarding the approval of the program. Lastly, it is important that the expenditure is placed in the context of an overall program. Management will be more likely to approve the institution of a new program and associated expenditures if they understand that the methodology. That is to say, it is part of an overall strategy with finite and measurable goals that can be communicated throughout the organization to show progress. According to Northcutt and Novak, "senior management does not have the time to accept information piecemeal; it is responsible for broad business strategies. Take a bit of your time to make its job easier."[7]

Host-based vs. Network-based

The first question to be answered is what type of IDS to run. While there are multiple variations of intrusion detection systems, most can be broken down into two major categories – host based and network based. In their whitepaper "Network- vs. Host-based Intrusion Detection - A Guide to Intrusion Detection Technology" Internet Security Systems define network and host-based IDS as follows:

> Network-based intrusion detection systems use raw network packets as the data source. A network-based IDS typically utilizes a network adapter running in promiscuous mode to monitor and analyze all traffic in real-time as it travels across the network. Its attack recognition module uses four common techniques to recognize an attack signature:
> · Pattern, expression or bytecode matching,

[6] Northcutt, p. 390
[7] Northcutt, p. 390

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

· Frequency or threshold crossing
· Correlation of lesser events
· Statistical anomaly detection

> Host based IDS typically monitor system, event, and security logs on Windows NT and syslog in Unix environments. When any of these files change, the IDS compares the new log entry with attack signatures to see if there is a match. Host-based IDS have grown to include other technologies. One popular method for detecting intrusions checks key system files and executables via checksums at regular intervals for unexpected changes. The timeliness of the response is in direct relation to the frequency of the polling interval. Finally, some products listen to port activity and alert administrators when specific ports are accessed.[8]

In today's networks some form of network based intrusion detection system is going to provide the most benefit with limited time and resources. It's relatively easy to deploy and the coverage achieved with the deployment of one device will outweigh deployment of multiple host-based agents. The downfall of network IDS is that as more and more network traffic becomes encrypted, there's less of the actual traffic that will be visible for inspection. Host-based intrusion detection systems resolve this issue by inspecting the activity on the host itself – after decryption. Network based IDS will have a small footprint on the network while host based will involve installing software on mission critical assets like web and application servers. The decision for which technology to deploy is going to rely on many factors, however, according to Peikari and Chavukin, the writing is on the wall:

> "The increasing use of switched networks hinders an IDS that monitors the network using promiscuous mode, passive protocol analysis. It is becoming more difficult to monitor multiple hosts simultaneously due to increased bandwidth, virtual networks, and other complications. In addition, the growing use of encrypted traffic foils passive analysis off the wire. Thus, IDSs are moving toward host-based monitoring".[9]

The ideal solution in today's environment may be some combination of host and network IDS. Due to likely longer timeframes to deploy host-based IDS, it may be beneficial to deploy network based until the same coverage can be achieved with host based.

Another question that needs to be addressed is whether the program will be run internal to the organization or whether it will be outsourced to a managed security service provider. There are benefits and downsides to both options. A managed security service provider will be expensive, but they will also have experienced intrusion analysts, 24x7 monitoring, a broad view of current attack trends based on what they see towards their overall customer base, and in many cases the

---

[8] ISS, p 3
[9] Peikari, p. 439

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

ability to correlate the attack information better than off the shelf products. Running the program internally will be less expensive which may allow for a more extensive deployment, and internal analysts will have better knowledge of the infrastructure and be able to better determine the events of interest based on this knowledge. Part of the decision may also be reliant on how the rest of the organizations' technology is managed. If technology as a whole is outsourced, it may make sense to also outsource the intrusion detection. There are some who would argue, however, that security should never be outsourced and that outsourcing security is giving away the keys to the kingdom. The ideal solution may be some combination of outsourcing and in sourcing. For example, it may make sense to outsource initially until the expertise can be developed internally. Or to outsource for mission-critical or highly visible assets only such as Internet points of presence or business partner connections.

Determining staffing requirements should be reliant on one main factor – the ability to perform due diligence in event analysis. Sounds simple, but what value is an ID program when the analysts spend more time supporting the infrastructure than performing event analysis? In many organizations, the task of running the intrusion detection program is included in the job description of network or system administrators. Conversely, in other organizations, dedicated intrusion analysts may be tasked with system administration of the ID infrastructure or managing projects to related to intrusion detection. The right level of staffing is the one where the staff has the ability to complete whatever system administration and project-related tasks while having coverage on a day-to-day basis to actually perform event analysis. One recommendation is to have analysts rotate responsibilities on a regular basis. While an analyst is "on the con", she will not be performing any other tasks other than performing event analysis and tuning the infrastructure. According to the ID manager at a large organization upon receiving more headcount for his program, "This is the year that we'll get to have someone looking at events all day long." Of course, he adds, "that doesn't always happen", but it's a noble goal to shoot for!

Depending on the scope of an IDS deployment, the simple care and feeding of the infrastructure could be a full time job in itself. Whether the ID program will support it's own infrastructure or delegate this function to another group inside or outside of the organization is usually more of a philosophical debate. Many of the arguments regarding outsourcing will also hold true for the discussion of who supports the infrastructure. The infrastructure support groups in the organization may be better suited to perform the system administration – the "leave it to the experts" argument. Then again, ID systems may be configured in a way that is non-standard for the organization due to operating system hardening and the fact that they may need to run applications the infrastructure support group is not familiar with. Moreover, there is the argument that due to the sensitivity of information on these systems, only the security group should have access to them. If part of the intent of the program is monitoring internal employees, it may be a conflict of interest for the very people being monitored to have

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

administrative access to the systems. Part of this decision will also depend on the product being deployed. While many ID solutions run on standard operating system platforms that can be readily supported by infrastructure support groups, many today are appliance based which may not require the same level of system administration as standard operating system builds. In this case, the support personnel require little knowledge of the underlying operating system and this may be more conducive to support by the ID program. The right decision will rely on placing the support with the group that can provide the best system availability while ensuring that analysts have time to perform event analysis.

Product Evaluation

When it comes time to implement an intrusion detection program, choosing the tools to use can be one of the most enjoyable and at the same time frustrating endeavors in the process. Any individual involved in hands-on intrusion detection loves getting his hands dirty with the technical aspects of the job but there's also the responsibility of performing due diligence in choosing a product that will benefit the organization the most. There is a plethora of products on the market to choose from and a good salesman will invariably profess that his product will be able to meet the needs of an organization better than any competitor's product.

It is important to enter the selection process with a list of clearly defined requirements. The list of requirements will include not only technical requirements like ability to handle certain network traffic speeds or ability to detect certain types of attacks, but may also include non-technical requirements like the financial stability of the vendor and the ability of the vendor to meet certain service level requirements in regards to technical support. Certainly one of the biggest requirements in any selection process is going to be cost. Once the requirements have been defined, they should be weighted by importance and each product should then be scored according to whether the requirement is met (see figure 2). It may be a good idea to take a first cut at the selection process with information obtained from the Internet and from speaking with Industry peers in order to narrow down the list of tools that will eventually be fully evaluated. There are some excellent web sites that can assist in the selection process like Robert Graham's IDS FAQ and "How To Evaluate Network Intrusion Detection Systems" by Michael Wilkison . Talisker Security Products and Service Website contains a good listing of the tools available in the product space.

| Requirements | Weight | Product A | | Product B | | Product C | |
|---|---|---|---|---|---|---|---|
| | | Score | Weighted | Score | Weighted | Score | Weighted |
| Requirement #1 | 10 | 5 | 50 | 8 | 80 | 3 | 30 |
| Requirement #2 | 3 | 6 | 18 | 2 | 6 | 10 | 30 |
| Requirement #3 | 1 | 10 | 10 | 8 | 8 | 4 | 4 |
| Requirement #4 | 8 | 2 | 16 | 1 | 8 | 5 | 40 |
| | | | | | | | |
| Total | | | 94 | | 102 | | 104 |

Figure 1 (Sample requirements scoring matrix)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The tools that will be chosen should fit the expertise level of the organization. In her book "Intrusion Detection", Rebecca Gurley Bace breaks the intrusion detection product space into "tools" and "applications". "Tools" characterize attacks in terms of connections, services, and port numbers, but the information produced by tools may not mean much to an analyst without a technical background. "Applications" do not require a technical background and typically involve graphical user interfaces and robust reporting functions. Whether intrusion detection tools or applications are chosen for a program should depend largely on the level of technical expertise of the intrusion analysts who will be using the product both now and in the future.[10] Many products on the market today are a good mix of tool and application. That is, they have user-friendly GUIs and good reporting features, but at the same time, the analyst can drill down to view the packet data if she so desires as well. According to Bace, the "best security solution is the one that is used and continues to be used over time. Furthermore, the best solution is the one that best fits the user's needs and capabilities while yielding a measurable improvement in security."[11]

The architecture of the intrusion detection infrastructure is for the most part going to be determined by the vendor and may not be customizable, so it will be important to ensure that architecture requirements are included in the decision matrix. It is essential for any good intrusion detection system to have the capability of viewing the events multiple ways. Correlation is key in the analysis process. According to Northcutt ""…correlation is one of the primary keys to maintaining situational awareness, one of the primary responsibilities for the intrusion analyst."[12] The analyst will want to see things like events grouped by time, source address, destination address, or reporting device. It will be necessary to see current events in the environment as well as historical ones for investigative purposes and forensic evidence if necessary. This usually involves the utilization of some type of relational database. Some products will use a proprietary data store while others will use standard off the shelf databases and still others will use a combination of off the shelf data store and proprietary code. While a proprietary data store may be efficient in how it stores the data for the application, it may not be conducive to any customized reporting needs. On the other hand, a solution that uses a standard database like Mysql, MS Sql Server, or Oracle will allow for customized queries and flexibility in reporting.

Compliance with industry standards may also play a deciding factor in choosing technology for an IDS program. While the industry is still maturing in many respects, there are emerging industry standards for intrusion detection technologies. According to Northcutt, "The goal of these specifications is to enable you to pick and choose the products that meet your needs, and also to

[10] Bace, p222-223
[11] Bace, p223
[12] Northcutt, p167

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

allow them to work together to help you detect and neutralize attacks."[13] One of the most widely accepted and used industry standards is the Open Platform for Secure Enterprise Connectivity (OPSEC). According to Network Technologies web site, "OPSEC is the industry's leading open multi-vendor security framework. OPSEC integration enables products to work together in the most efficient manner to both simplify configuration, monitoring, and tracking, and at the same time provide the highest level of performance and availability."[14] From an intrusion detection standpoint, OPSEC compliance will allow integrated network and host-based intrusion detection and prevention products to provide dynamic reconfiguration of the security policy upon intrusion alerts.[15] The ability to reconfigure firewall policies to block the source of an attack as it's occurring is a very powerful tool.

Another factor that may play a role in the product evaluation process is the open or closed nature of the product signature set. If the actual signatures are available to the analyst, determining false positives becomes much easier. Some vendors will attempt to compensate for closed signature sets by providing more extensive documentation on what the signature is looking for and the likelihood of false positives. This will suffice in most instances, however, there are going to be times when the analyst will require visibility of the actual pattern the signature is attempting to match against. Products that allow for a great deal of flexibility in modifying existing signatures or creating new signatures are also beneficial in that one can better tune the IDS to the environment in which it will be deployed. Many IDS systems today will have the ability to create new signatures, while, some even go so far as to accept open source signatures like those used for Snort, the popular open-source IDS.

Deployment

Defense in-depth is the basis of good security architecture. According to SANS, "Defense In-Depth is the approach of using multiple layers of security to guard against failure of a single security component."[16] An organization employing the defense in depth methodology may have multiple layers of firewalls between their core network and un-trusted networks as well as employing strict host based security measures. The Intrusion detection deployment will add another layer of depth. According to the authors of "Defending Yourself: The Role of Intrusion Detection Systems", "When we combine the use of multiple firewalls and sensors configured to support a mission-specific security policy with a proactive vulnerability remediation policy, the removal of unneeded services, and the regular and careful use of integrity checking tools, the intruder's task becomes much more difficult."[17]

---

[13] Northcutt, p167
[14] Network Technologies
[15] Check Point Software Technologies
[16] SANS
[17] McHugh, p5

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Determining where to focus resources for deployment of the ID program is going to rely on prioritization of target areas based on risk. Typical areas where organizations deploy network based IDS are to monitor perimeter networks, mission critical server farms, and network backbones. Host based deployments typically focus on perimeter facing hosts and mission critical systems. The NIST Special Publication on Intrusion Detection Systems recommends a staged deployment of network and host based IDS starting with Network IDS and then moving to host based IDS on critical servers.[18]

Deployment for perimeter networks will ideally have sensors on the internal and external side of the firewall. According to the authors of "Defending Yourself: The Role of Intrusion Detection Systems", "Using a network sensor outside the protected network lets the administrator sense the general threat level as indicated by probes and attempts that will be blocked by the outer firewall. Comparing the observations of sensors on both sides of the firewall lets the analyzer be configured to validate the firewall rules."[19] In an environment where multiple layers of firewalls and DMZ's separate the external network from critical assets, sensors can be deployed at each level to provide an end-to-end view of whether the attack successfully traversed each layer.

Deployment should not be considered complete until network diagrams have been updated, configurations have been documented, and support documentation and procedures are in place.

Event Analysis and Response

Event analysis and response is central to the success of any ID program. It is a job that is in most cases made extremely difficult by the plethora of data generated by an out of the box IDS. In fact, the sheer volume of data generated is one of the most frequently criticized problems with current IDS technology. Intrusion detection is not a plug and play technology. Effectiveness of an intrusion detection system is going to be determined by how well it is tuned to the environment it is monitoring. Conversely, if too much traffic is filtered, there is the risk of missing events that would normally require review. According to Julia Allen in her article "Intrusion Detection", "Most ID systems err on the side of caution by default, with the upshot being generation of lots of false alarms. Over time, the staff assigned to monitoring the systems must learn how to sort the serious attacks from the false alarms and "tune" systems to reduce the number of false alarms." [20]

There are two common methods employed in tuning intrusion detection systems. In some cases, it is acceptable to run a default configuration with all signatures

[18] Bace(NIST), p35
[19] McHugh, p5
[20] Allen

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

and filter as necessary until an acceptable level of alerts is reached. Alternatively, one can run a reduced set of signatures based on factors like knowledge of the network. For example, it may make sense to run a signature set of Unix-based attacks only against Internet facing web servers if Unix is the only operating system in use for our web servers.

The first place to begin tuning is with the security policy. If the intrusion detection system is being used as a way to enforce security policy, any events relating to the use of technologies that are acceptable under the security policy should be removed. For example, most IDS technology will have capability to detect the use of file-sharing protocols like Kazaa on the network. If the security policy permits (or does not specifically prohibit) the use of these technologies, then these signatures should be disabled in an effort to reduce the number of alerts.

One of the emerging trends in the Intrusion detection industry that shows promise in dealing with the massive amounts of data is being called target-based IDS. Joel Snyder in his article "Taking Aim" states that "Target-based IDS is a new technology that correlates knowledge about network topology, operating systems and applications with incoming attack information."[21] The idea is to "combine a normal IDS engine with post-processing tools to convert alerts from 'raw' to 'well-qualified'."[22] In this case, the "raw" events are the unfiltered IDS alerts and "well-qualified" events are those that involve an attack against a host that is vulnerable to the attack. While this is still an immature technology, as a conclusion to his evaluation of the products in the space, Snyder "saw a significant decrease in the amount of noise, helping us focus more quickly on alerts that matter."[23]

Conversely to tuning the IDS, most IDS vendors will release updates on a regular basis in order to detect against new attacks and vulnerabilities. As part of the on-going process of daily operational activities, these updates should be applied in a timely fashion to ensure the latest attacks will be visible to the IDS.

Most commercial IDS products will have the capability of automated response to certain events like sending an alert in the form of an email or page. While this feature can be powerful and lead to increased response times and awareness of certain types of events, it is also easy to become inundated with alerts. With utilization of the OPSEC standard, many ID systems are able to implement a firewall rule change to block an attacking address. While sending multiple alerts to an email address may create an annoyance, accidentally blocking legitimate traffic attempting to access the company web site can be detrimental to business and to the career of an intrusion analyst! The NIST suggests being "conservative about using them until you have a stable IDS installation and some sense of the behavior of the IDS within your environment."

---

[21] Snyder, p35
[22] Snyder, p 35
[23] Snyder, p 44

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The ID program should have well defined procedures for dealing with events. Most events are going to require further investigation in order to verify validity and determine the severity. Once this is determined, there are three main areas of response that can take place. First, it may be determined that the event was caused by faulty or poorly configured systems and the course of action may be to engage the system administrators for corrective action. Second, it may be determined that the event was triggered due to normal operating conditions. In this case, changes to the IDS infrastructure may be warranted such as filtering the system being reported, changing the signature to a more appropriate pattern, or even disabling the signature. Lastly, the event can be labeled an incident and escalated to the incident response process.

Every organization should have some type of defined procedure for handling incidents. According to the NIST Special Publication on Intrusion Detection, this procedure should "at a minimum, assign roles and responsibilities for all parties within the organization, outline the actions that are to be taken when an incident occurs, and establish schedules and content for training everyone about their responsibilities in the incident handling process."[24] Whether the intrusion detection group handles the incident handling procedures will be organizationally dependant, but it is imperative that the ID analysts understand the process and follow it accordingly in the event of an incident.

Reporting

It is important to keep appropriate parties abreast of the events generated by the intrusion detection system. Different types of reports may be appropriate for different parties. For example, a daily summary of events, sensor health statistics, and logs of changes to the infrastructure will be valuable for the intrusion detection analysts. Management would probably like to see reports on a less frequent basis of reported incidents and their outcome, as well as statistics relative to the overall threat level against the organization. If the IDS tool does not have the capability for generating the required reports for the organization, it should be the responsibility of the IDS analyst to provide these some other way.

Program Assessment

On-going assessment is necessary for the long-term success of the intrusion detection program. Depending on the organization, an internal audit group or third party will from time to time measure the program against internal policies or industry best practice. In order to prepare for these assessments and in an effort to achieve a best in class program, it is beneficial to proactively self-assess the program on a regular basis. This assessment may involve a high level look at the deployed technology suite compared to how the industry is evolving to

[24] Bace(NIST), p 40

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

determine if the products are still best in breed or if there is a need to re-evaluate technology decisions.

It is important to evaluate the deployed solution in the context of the changing environment. For example, if the network is being upgraded to handle gigabit speeds, it will be necessary for the technology and hardware deployed to be able to perform at this speed. In a host-based scenario, it is important to ensure that host-based ID technology is being included in the implementation of any new mission-critical assets. Verification of existing coverage is also necessary. It will be necessary to audit against known configurations for unknown changes to ensure that configurations allowing for the capture of the traffic are still valid. An example of this is when network intrusion detection systems are configured to monitor traffic using switch port mirroring. In the event that switch configurations are modified, the traffic monitored by the IDS could be altered or cease to be visible. As systems are verified, or changes uncovered and resolved, necessary documentation including network diagrams, network configurations, and standard operating procedures should be updated to reflect the current state of the program.

Conclusion

Intrusion detection is not a perfect technology. It is expensive and difficult to deploy and maintain, however, the benefit to an organization with a world-class intrusion detection program is going to be achieved in a more secure and diligently monitored environment.

© SANS Institute 2004, Author retains full rights.

References

Allen, Julia H. "Intrusion Detection." CIO 15 Sep 2002. URL: http://www.cio.com/research/current/intrusion.html (2 Mar 2004).

Bace, Rebecca Gurley. Intrusion Detection. Indianapolis: Macmillian Technical Publishing, 2000.

Bace, Rebecca, and Peter Mell. "NIST Special Publication on Intrusion Detection Systems." URL: http://www.netsys.com/library/papers/intrusion_detection_systems_0201_draft.pdf (2 Mar 2004).

Check Point Software Technologies. "OPSEC Partners Security Enforcement Intrusion Detection and Protection." URL: http://www.opsec.com/solutions/sec_intrusion_detection.html (2 Mar 2004).

Danahy, Jack. "DOWN WITH IDS." Information Security. February 2003. URL: http://infosecuritymag.techtarget.com/2003/feb/logoff.shtml (2 Mar 2004)

Graham, Robert. "FAQ: Network Intrusion Detection Systems." Version 0.8.3, March 21, 2000. URL: http://www.robertgraham.com/pubs/network-intrusion-detection.html (2 Mar 2004).

Internet Security Systems. "Network- vs. Host-based Intrusion Detection -A Guide To Intrusion Detection Technology." 2 Oct 1998. URL: http://www.isskk.co.jp/customer_care/resource_center/whitepapers/nvh_ids.pdf (2 Mar 2004).

McHugh, John, Alan Christie and Julia Allen. "Defending Yourself: The Role of Intrusion Detection Systems." IEEE Software September/October 2000. URL: http://www.cert.org/archive/pdf/IEEE_IDS.pdf (2 Mar 2004).

Network Technologies. "OPSEC." URL: http://www.nwt.dk/OPSEC/default.htm (2 Mar 2004).

Northcutt, Stephen, Judy Novak, Donald McLachlan. Network Intrusion Detection An Analyst's Handbook Second Edition. Indianapolis: New Riders, September 2000.

Peikari, Cyrus and Anton Chuvakin. Security Warrior. Sebastopol: O'Reilly & Associates, Inc, 2004.

Snyder, Joel. "Taking Aim." Information Security. January 2004 (2004): 35-45.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

SANS. "SANS Glossary of Terms Used in Security and Intrusion Detection." May 2003. URL: http://www.sans.org/resources/glossary.php (2 Mar 2004).

Wilkison, Michael. "Intrusion Detection FAQ - How to Evaluate Network Intrusion Detection Systems?" URL: http://www.sans.org/resources/idfaq/eval_ids.php (2 Mar 2004).

© SANS Institute 2004, Author retains full rights.

Last Updated: November 29th, 2015

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Cape Town 2015** | **Cape Town, ZA** | **Nov 30, 2015 - Dec 05, 2015** | **Live Event** |
| **SANS San Francisco 2015** | **San Francisco, CAUS** | **Nov 30, 2015 - Dec 05, 2015** | **Live Event** |
| **HIMSS** | **Boston, MAUS** | **Dec 01, 2015 - Dec 02, 2015** | **Live Event** |
| **Security Leadership Summit & Training** | **Dallas, TXUS** | **Dec 03, 2015 - Dec 10, 2015** | **Live Event** |
| **SANS Cyber Defense Initiative 2015** | **Washington, DCUS** | **Dec 12, 2015 - Dec 19, 2015** | **Live Event** |
| **SANS Las Vegas 2016** | **Las Vegas, NVUS** | **Jan 09, 2016 - Jan 14, 2016** | **Live Event** |
| **SANS Dubai 2016** | **Dubai, AE** | **Jan 09, 2016 - Jan 14, 2016** | **Live Event** |
| **SANS Cyber Defence Delhi 2016** | **Delhi, IN** | **Jan 11, 2016 - Jan 22, 2016** | **Live Event** |
| **SANS Brussels Winter 2016** | **Brussels, BE** | **Jan 18, 2016 - Jan 23, 2016** | **Live Event** |
| **SANS Security East 2016** | **New Orleans, LAUS** | **Jan 25, 2016 - Jan 30, 2016** | **Live Event** |
| **Cyber Threat Intelligence Summit & Training** | **Alexandria, VAUS** | **Feb 03, 2016 - Feb 10, 2016** | **Live Event** |
| **SANS Scottsdale 2016** | **Scottsdale, AZUS** | **Feb 08, 2016 - Feb 13, 2016** | **Live Event** |
| **SANS Secure Japan 2016** | **Tokyo, JP** | **Feb 15, 2016 - Feb 20, 2016** | **Live Event** |
| **SANS Munich Winter 2016** | **Munich, DE** | **Feb 15, 2016 - Feb 20, 2016** | **Live Event** |
| **SANS McLean 2016** | **McLean, VAUS** | **Feb 15, 2016 - Feb 20, 2016** | **Live Event** |
| **ICS Security Summit & Training** | **Orlando, FLUS** | **Feb 16, 2016 - Feb 23, 2016** | **Live Event** |
| **SANS Secure India 2016** | **Bangalore, IN** | **Feb 22, 2016 - Mar 05, 2016** | **Live Event** |
| **SANS Anaheim 2016** | **Anaheim, CAUS** | **Feb 22, 2016 - Feb 27, 2016** | **Live Event** |
| **RSA Conference 2016** | **San Francisco, CAUS** | **Feb 28, 2016 - Feb 29, 2016** | **Live Event** |
| **ICS410 London 2015** | **OnlineGB** | **Nov 30, 2015 - Dec 04, 2015** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |