Global Information Assurance Certification Paper

GSEC Practical Assignment - version 12.d

Managed Security Services: an IDS solution

Esperanza Lopez-Wilkin
May 20, 2001

In this age of highly networked computers, e-business success can only be achieved by protecting valuable business assets: from the organization's information, or research and development projects and highly skilled professionals that make it happen, to the IT infrastructure that we all have grown to depend on for all aspects of e-business. Protecting the organization's assets is a matter of saving money and protecting well-guarded prestige. Such protection can only be achieved with a forward-thinking approach of planning, prevention and timely implementation of security measures.

Intrusion detection systems (IDSs) form an important component of this prevention and protection effort, as one layer in the defense in-depth approach, by aiding with automated monitoring and analysis of events in computer systems and networks. Like any other IT-based solution, it is only as good as the organization's effort to implement, maintain and operate it. The core component for this operation is the analyst who actually makes sense of the numerous outputs and builds on previous experience to achieve the best tool of defense in this prevention/protection mechanism.

Outsourcing as a solution

Companies face a variety of challenges with the ever changing technology on which their communications infrastructure is based, and fulfilling the staff requirements to support it. Some organizations do not have enough IT staff, especially in the security arena, to spare even a few individuals to administer yet another system of computers. Network and system administrators are just too busy keeping the operations working. Other security professionals have their resources prioritize looking at the bigger picture and planning other e-business initiatives, such as VPNs and PKI, essential to many organizations.

For the highly enterprising security professional, going about doing the research to find the solution that best suits the organization's needs for an intrusion detection system implementation, procuring the needed hardware and software and, installing IDS components is just the beginning. The initial research, acquisition and deployment is followed by numerous hours of data and correlation analysis, and keeping up with IDS system updates, technology and the infrastructure that it is designed to protect. For the organization, owning the implementation of an intrusion detection systems means capital investment on hardware and software and, requiring staffing support around the clock to respond to intrusions as real-time emergencies, a problem resolution escalation procedure and specialists to fill the various levels of expertise required for this

operation, analysis and problem resolution.

Acquiring services from a managed security services provider (MSSP) comes as an alternative to the corporate investment in specialized hardware and software. Also, with staffing limitations that many organizations face, the implementation of an intrusion detection system, given what was discussed earlier, may seem more a burden than a necessary step toward a comprehensive security solution.

There is always room for entrepreneurial efforts that provide something that is needed to the organization that does not have the resources to implement and support an intrusion detection system. Still, management needs to task the security professional to find the solution to defining what is wanted and required, and how to go about obtaining and supporting it.

A word of caution for those exploring acquiring a managed security services provider as the IDS solution for the organization: do not be confused between managed security services providers (MSSPs) and managed security providers (MSPs). The latter may provide many security related services, but not necessarily installation, administration and monitoring of sensors, data analysis and incident forensics. Still managed security providers may support the development and implementation of many security initiatives for which the organization does not have resources or in-house know-how.

Managed Security Services Providers as a Solution

Managed security services providers facilitate hardware, software and services to manage and improve on the organization's network and system security. Hardware and software provide the basis for sensors or data collectors. Sensors may be network-based which collect network packets as data, or host-based which collect system log entries and/or operating system audit trails data. MSSPs provide services to design, deploy, manage and monitor an intrusion detection system for a customer organization that does not possess the staff or other resources to provide such essential service for themselves.

At the core of managed security services monitoring is the security operations center (SOC) where data collected from the sensors is merged, normalized and analyzed. SOCs are staffed 24x7 with analysts as the first step in the escalating process of evaluating suspicious events registered by the intrusion detection system and determining an appropriate handling response. There are various levels of analysis done to the data in the effort of determining if an event is an actual intrusion incident: data mining and correlation techniques are performed including aggregation of events and incidents recorded from other customer sites as well as global incident response centers.

By the way, when it comes to monitoring, alert and incident handling coverage provided by the SOC, don't think that services are any more comprehensive if a

managed security services provider happens to mention that they provide 24x7x365 monitoring as opposed to simply 24x7. The 365 sounds impressive, but it adds no additional meaning nor coverage. Actually, this could be a dangerous thing: consider what would happen to the 366th day in a leap year…

Considerations When Selecting an MSSP

There are many aspects to consider when selecting a managed security services provider. The organization must identify its security needs to find a provider that can meet them. Not all considerations may be important to an organization because it will depend on resources needed and wanted.

Your organization and the selected MSSP will draw a service level agreement which determines the level and quality of service to be provided by the MSSP and expected from the organization. The service level agreement needs to be negotiated in advance for a clear understating of services and cost.
MSSPs offer various pre-packaged service level agreements that might fit your organization's needs or can be customized to the specific needs.

Here are some aspects to consider on the road of identifying the organization requirements and selecting a managed security services provider:

- Technology. Managed security services providers offer a variety of technical solutions through software and hardware from various vendors. The solution that is best for your organization will be largely dependent of how much control or hands-on your organization wants, requires and can afford. Another aspect of the same issue is how much the managed security service provider is able to provide. The two hold an inversely proportional relationship. The systems and network infrastructure where the IDS will reside is a deterministic factor as well.

  Consider some details on the technical requirements:

  - Network-based sensors deployment and support. Network speed must be taken into consideration since sensors need to keep up with the data that are trying to collect.

  - Host-based sensors deployment and support. Host-based sensors analysis is another aspect of defense in-depth, therefore it should be an integral part of the IDS and the data correlation analysis performed.

  - Sensor management. Hands-on support in your organization and the MSSP's technical capacity to remotely manage sensors are factors in this matter.

- Sensor signature upgrade capabilities and timing. Depending on the specific implementation, the product(s) deployed may have capabilities for signature development. Signatures updates can be supplied by the IDS software vendor or by MSSP support for quick implementation and protection.

- System tuning. System tuning is an on-going process to minimize false-positives, which is essential to focus efforts on actual intrusions. MSSPs may consider a pilot phase to establish a base level of event activity that would be used for an initial fine-tuning of the system.

- System scalability. Even in a modest IDS initial deployment, the planning for future sensor deployment and integration should be considered from the start by the organization.

- Technical training. If your MSSP provides basic monitoring and alerting, based on your service level agreement, technical training may be required for your organization's analyst who is left with many tasks to support hardware and software components, signature updates and development, and basic sensor maintenance.

- Reporting. There are two types of reporting that an organization should consider:

  - Alert reporting. There are some choices or requirements that may need to be implemented to comply with the organization's policies: phone notification, e-mail notification, paging, SNMP trap and web portal notification. Timing of alert notification must certainly be considered and can be related to already developed incident handling policies and procedures.

  - Statistical and other reporting. Even when the managed security services provider is doing the analytical work and correlation, still as a conscious analyst in your organization, there are many benefits from knowing what type of events are being detected by the intrusion detection system to plan for better security measures. A secured web portal interface can aid the analyst on this task by providing statistical reporting while protecting the information being shared.

    Incident handling reporting also may help the analyst in the effort to document the organization's intrusion incidents and to justify future acquisition and implementation of security measures, in

addition to the current MSSP expense.

Regular monthly reports are a good way to keep abreast with IDS upgrades and can provide security advisories for newly discovered threats.

- Incident handling and forensics. Support may be beyond monitoring and alerting. Data forensics is needed to understand the event, the extent of any damage done, possible fixes and mitigation steps. This aspect will depend on the organization's incident and escalation procedures for intrusion incidents. The organization may also need on-site support in case of an intrusion incident and possible legal counseling and support.

- Company's assessment.

    - On their own or with a partner. Various MSSPs provide the whole range of services or partner with another company to supplement the security services for the customers.

    - Corporate history and growth. Knowing how long the company has been established as a MSSP, number of employees, and growth over time may give the organization some prospective on what to expect, especially if the organization plans to expand services beyond the initial deployment. Also, having an idea of other corporate customers would provide some comfort level on the MSSPs background and capabilities to satisfy the organization's needs.

    - Location and operations. Location may be a factor if your organization requires on-site support because travel expenses will be reflected in services' cost. Inquire about SOC redundancy of operations since your organization will entrust a critical component of security to the MSSP.

    - Personnel background. MSSPs take great pride in having on board former employees from the Department of Defense and other government agencies that specialize on intelligence work. Many analysts may also hold current certifications available for security professionals. In addition, it is wise to understand or require a certain level of background checks and/or clearances for analysts and staff that will be supporting your organization's security efforts.

- Security services beyond IDS. To complement intrusion detection system monitoring, MSSPs facilitate development of security policies and procedures, as well as, a more proactive approach to security measures

to determine and correct vulnerabilities before an intruder's exploit. This proactive approach include vulnerability assessment/scanning and penetration testing:

- Vulnerability assessment/scanning. Assessing the strength and implementation of security controls on systems and network can be performed with vulnerability assessment tools. Some of these tools are active in nature because they identify vulnerabilities using exploit techniques.

  Other vulnerability assessment may be performed in a passive mode, where security weaknesses may be encountered by reviewing security measures developed and implemented by the organization such as security policies and procedures, access controls and, roles and responsibilities. Even when data needs to be gathered from production systems, the tests are performed off-line without affecting the systems' performance.

  Both types of vulnerability assessment approaches may assess important security controls such as password strength, file systems protection, system security-related bug-fixes and access control lists.

- Penetration testing to find security holes before intruders do is always good practice. Your organization may prefer to have the penetration testing performed by a third party company. This will not only test for security weakness in targeted systems but a test on the intrusion detection system implementation as well.

  The scope of any penetration testing and vulnerability assessments to be performed should be identified in advance to minimize impact to the systems and networks being tested.

- Cost. This will greatly depend on the service level agreement your organization develops with the selected MSSP. Service level agreements range from simple sensor monitoring and alerting to sensor implementation design and deployment, incidence forensics, vulnerability assessments, penetration testing and others indicated in this document.

  Consider the number and type of sensors to be deployed and monitored and, the extent of the initial targeted IDS implementation. There could be a significant difference in the cost of host-based versus network-based sensors and how extensive the support requested from the MSSP to maintain the IDS.

  Also, MSSPs also provide hours of consulting services to satisfy other

security needs from customers in an effort to provide comprehensive security services.

Some final thoughts

There is a wide range of outsourcing alternatives to implement an intrusion detection solution that fits your organization's needs. Managed security services providers satisfy many requirements with specialization and solid expertise in the security field.

Selecting a managed security service provider may prove to require low initial investment and faster deployment than a solution developed and supported only with in-house resources because of the high cost of ownership.

The organization needs to decide between technical and policy requirements, in addition to budget and technical constraints to find and acquire a provider best suited for the job at hand. Maybe the major challenge on acquiring MSSP is knowing what the organization wants and needs before the organization actually gets it.

References and Resources

Amaladoss, Babu, "Managed Security Services – An Evolving Security Solution!", March 8, 2001, URL:
http://sans.org/infosecFAQ/managed/mss.htm

Bace, Rebecca and Mell, Peter, "NIST Special Publication on Intrusion Detection Systems", February 12, 2001, National Institute of Standards and Technology,
http://csrc.nist.gov/publications/drafts/idsdraft.pdf

Chetty, Synthil, "Outsourcing Security Management", April 9, 2001, URL:
http://sans.org/infosecFAQ/policy/outsourcing.htm

Counterpane Internet Security, Webpage on company's website, accessed on April 16, 2001, URL:
http://www.counterpane.com/integrated.html

DeJesus, Edmund X., "Managing Managed Security", January 2001, URL:
http://www.infosecuritymag.com/articles/january01/cover.shtml

Internet Security Systems, "Network- vs. Host-based Intrusion Detection" – A guide to Intrusion Detection Technology, accessed on March 9, 2001, URL:
http://secinf.net/info/ids/nvh_ids/

Riptech, Inc., webpages on company's website, accessed on April 20, 2001,

URL:
http://www.riptech.com/securitypro/solutions.html
http://www.riptech.com/technology/features.html

Polk, W. Timothy, “Automated Tools for Testing Computer System Vulnerability”,
December 1992, National Institute of Standards and Technology, Special Publication No. 800-6, URL:
http://csrc.nist.gov/publications/nistpubs/800-6/800-6.txt

Proctor, Paul E., “The Practical Intrusion Detection Handbook”, 2001, Prentice Hall PTR

Last Updated: July 27th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event