BLUE LANCE

Making Security Monitoring a Part of Your Best Security Practices

An Executive White Paper

By

BLUE LANCE, Inc.

Do you want to have some fun with your information security experts? Start by asking each one to characterize the single most important information security-related goal that their company needs to achieve. Follow up this first question by asking your expert to explain the "best way" to achieve the goal. You are now drawing out a view of a "best practice", as seen through the eyes of an information security expert. Now lets start having even more fun. Present the same two questions to your C-level executives, Information Risk Managers, Business Managers, Information Technology Administrators, Information Owners, Attorneys, and Administrative Assistants.

Carefully consider your survey results. The concept of best practices could vary wildly depending on whose views are being canvassed, the respondent's background, and the level of experience with information security. The concept of "best" is relative and will even vary among your experienced security professionals.

We may fail to agree on what constitutes a "best practice" since we may fail to agree on what goals are important and what behavior is effective in achieving stated goals. "Best" for some may be seen as "not enough" or "settling for less" by others. "Best" depends on money -- what is the best level of security that you can afford to implement with the funding that you have available? "Best" may depend on regulatory pressures, if your business is regulated -- what minimum "standard" of acceptable security does your company need to comply with? "Best" should depend on the risk of being attacked. One would expect the "best practice" that can be implemented to protect sensitive information at your community Bank will be considerably "better" than the "best practice" that can be implemented to protect an inventory control system at your local automobile parts store.

This paper introduces a process that can be followed to develop a best information security practice, considers the impact of organization structure on the ability to develop best practices, evaluates the role of two types of security monitoring practices, and identifies particular features in LT Auditor+ that Blue Lance customers leverage in building a best security monitoring practice.

The Process of Developing a Best Information Security Practice

Before we examine the subject of security monitoring, lets reflect on the process of developing a best information security practice. In many respects, developing a best information security practice is not terribly different than refining other elements of your company's operations.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

Step 1: Assign a Practice Champion that will lead the effort to develop the information security practice.

Step 2: Convene a Practice Development Working Group consisting of representatives from stakeholders in your company that will ultimately be affected by the practice. Select working group participants to leverage a blend of backgrounds and perspectives. Clearly, you will need information security expertise on the working group, but welcome other backgrounds from the enterprise to increase buy-in and generate excitement throughout your company. Through effective consensus building and syndication of ideas, the practice champion uses the working group to develop the practice.

Step 3: Define the goals of the practice by expressing the benefits that the practice is intended to achieve.

Step 4: Develop procedures that are designed to achieve the desired goals of the practice. Procedures should clearly define permissible and prohibited behavior and include a compliance procedure to validate that prohibited behavior is not occurring. Permissible behavior should be adequately defined to make it clear if the behavior is mandatory, conditional, or discretionary.

Step 5: Select and implement tools to address specific processing requirements defined by the procedures.

Step 6: Assign roles and responsibilities, as needed, to address administrative tasks defined in the procedures. Ensure that there is an adequate separation of duties to increase the likelihood that procedures will be followed. Separation of duties creates dependencies between individuals, strengthens teamwork, and reduces the likelihood that an inattentive employee can drag down a practice.

Step 7: Assess the effectiveness of the Practice by collecting information to determine if the goals of the practice have been met and to ensure that the procedures are effective.

Step 8: Refine the Practice by using the Power of I2 (incremental innovation) approach, keeping your initial goals modest and enhancing goals to build upon your early stages of success.

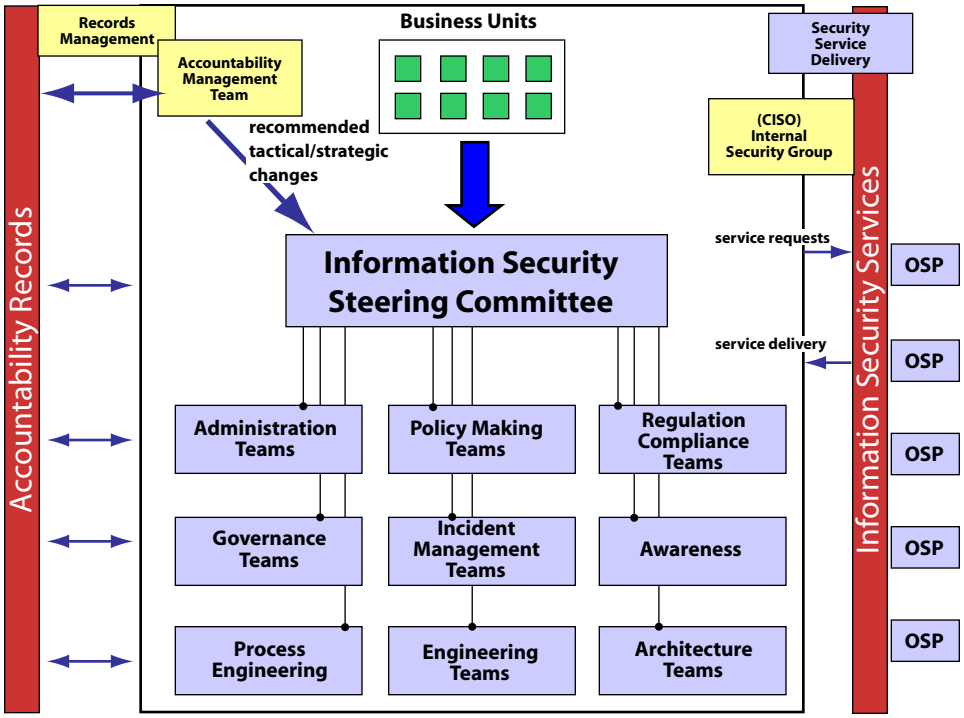
BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

An Organizational Framework for Developing Your Best Practices

Many companies may end up fumbling through the process of developing best practices or may find it very difficult to get suitable traction because of inadequate organization. Regardless of the size of a company, the process of developing best practices can run smoother with the right organization structure in place. The following diagram illustrates an organization structure that makes the effort highly participatory and business driven.



The organizational model represented by this diagram is a "participatory model" with an accountability system backbone that helps the program mature over time. The model recognizes that information security is likely to require the introduction of different types of operational processes, with the mix of needed processes varying from one organization to another.

To keep the participatory process under control, it is recommended that an enterprise-wide security steering committee be put in place and be given the following charter: (1) facilitate the creation, population, and decommissioning of needed working groups; (2) ensure that working groups are operating effectively; (3) facilitate the exchange of information between working groups and support the working groups in ways that are needed; (4) assume responsibility for the development, refinement and dissemination of

BLUE LANCE
410 Pierce Street
Suite 300
Houston, TX 77002
www.BlueLance.com

enterprise-wide security policies; (5) set direction and priorities, if needed, to ensure that pressing security issues are being addressed by assembled working groups; (6) evaluate and approve proposals coming out of the working groups. The mission of the security steering committee is primarily high-level information security program management.

Under this organizational model, various working groups are set up to develop different information security practices. The internal Information Security Group acts as a clearinghouse for delivering needed security services, rolling out services by leveraging internal resources or outsourcing (if business-justified), to qualified outside service providers (OSPs). A separate accountability management team operates in an ongoing review capacity to ensure that the operations of the virtual security organization is effective, and when appropriate recommends improvements to achieve greater efficiencies.

When business units are driving information security through the participatory approach advocated by this organizational model, you end up with a far greater number of information security stakeholders and a far better chance of distributing ownership of security to the employees that are ultimately responsible for processing data and have the greatest stake in how well data is protected. More people get involved in helping navigate the organization to a more comfortable security level. More people get sensitized. More people get inspired to contribute. Programmers start writing secure code. You increase the chances that security practices will be accepted and respected.

The Role of Security "Event" Monitoring in Your Best Practices

It will be difficult for a company to achieve information security objectives without security event monitoring. Security event monitoring is derived from the general practice of monitoring activities that occur on a computer system. Security event monitoring involves (1) recording information that represents activity and (2) analyzing recorded information to identify and respond to questionable activities (i.e.; possible security events).

Without security event monitoring, a company effectively operates on faith that all activity against a computer system is within the company's best interests. Without security event monitoring, a company denies itself the ability to identify disruptive or otherwise undesirable activity, reducing the ability to validate that confidentiality, integrity and availability requirements are being effectively met. Without security event monitoring, a company has no means of keeping administrators accountable for the quality of their administrative activities.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

The maturity of a company's security event monitoring practice depends on 5 critical factors:

1. The breadth and depth of activity that can be monitored. A company will need to consider various ways in which information can be compromised in determining the most effective level of monitoring. Opportunities may exist to monitor activity from a number of vantage points including:

    - The operating system's perspective (using available system level auditing capabilities).

    - The network communication perspective (using network traffic monitoring tools).

    - From the perspective of the application processing protected information (using available application transaction logging capabilities).

    - A database management system's perspective (using available database access logging capabilities).

    The importance of a particular level of monitoring will be situational, where varying circumstances could make the information in one activity log important one day, but less important another day.

2. The ability to protect the activity data that is collected. From a confidentiality standpoint, it will be important to prevent unauthorized access to activity data, since the data can provide an adversary useful intelligence about the location of applications and identify users who are authorized to access applications. Such intelligence can be used to plan out subsequent attacks, including focused efforts to compromise the passwords of users that possess privileged access to critical applications. From an integrity standpoint, it will be important to ensure that the collected activity data has not been tampered with; otherwise the ability to reach conclusions from the data can be diminished.

3. The ability to compare activity that is recorded with activity that is authorized. Activity data that is easier to work with includes data that represents attempted activities that were denied due to access control rules. For example, a user may attempt to read confidential data that he or she was not granted permission to

BLUE LANCE
410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

read – this would typically lead to an access control system denying access and producing a record indicating that attempted access was denied. By definition, any activity that is denied would be questionable, since authorized users should only be accessing information that they are explicitly authorized to access. A "denial event" could represent an adversarial act or may reveal that an administrator has not set up access controls effectively, leading to a undesired reduction in productivity. All denial events should be investigated to assess if the event represents adversarial intent.

Activity data that is usually harder to work includes data representing successful activities, since a reviewer would need to judge if a successful activity was or was not legitimate. Illegitimate "sucessful activity" could be the result of ineffective access controls, giving a user more access than is justified, or could be the result of an authorized user's password being compromised.

The utility of the activity data depends on the ability of an activity reviewer to notice something unusual from patterns of successful activity. In many cases, a reviewer may need considerable experience with monitoring authorized use of a computer system in order to recognize a pattern of successful activity that may be indicative of misuse. Correlating activity data to independent "corroborative records" may also be important in detecting misuse. For example, many companies require creation of a separate authorization/entitlement record before a security administrator is authorized to set up an account or assign an account authorized privileges. A more mature monitoring practice will give the reviewer the ability to compare the separate authorization record to the corresponding activity record.

4. The ability to eliminate extraneous data and summarize data. Due to the way software is designed, a given activity may produce multiple activity records, with some of the records seen as offering little or no security value. The maturity of an event monitoring practice depends on the ability to filter out extraneous information and to summarize patterns of low-level events into higher-level intelligence.

5. The ability to perform monitoring in a transparent manner and avoid impairing normal operations of a monitored system. Many companies may be reluctant to perform security event monitoring for fear that monitoring activities will consume excessive resources, starving other applications of needed resources. The maturity of an event monitoring practice depends on the ability to perform monitoring without degrading the performance of the system being monitored. When implementing an event monitoring system, companies need to be prepared to perform performance tuning in order to achieve a suitable balance between the demands of the monitored applications and the demands of the monitoring system.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

The Role of Security "State" Monitoring in Your Best Practices

Security "state" monitoring is designed to complement security "event" monitoring in a number of respects. State monitoring involves (1) collecting information about the configuration of controls on a computer system and (2) analyzing the collected information to identify and correct controls that are inadequately configured.

Security state monitoring is often referred to as a vulnerabilities assessment or simply a security assessment, since inadequately configured controls introduce vulnerabilities (i.e.; opportunities to compromise security). Security state monitoring analyzes the current state of security at a particular point in time.

Security state monitoring can cover an assessment of (1) access controls, governing access to applications and files, (2) password controls, determining permissible choice of passwords and governing the requirement to change passwords; (3) connectivity controls (e.g.; open ports/ enabled protocols) influencing permissible communications to and from a computer system; (4) inappropriate files (including viruses, worms, trojan horses, bootleg software, music files, inappropriate image files); and (5) unpatched software, bringing attention to available security-related patches that have not been deployed.

An assessment consists of evaluating one or more properties of each item being assessed. For example, in order to assess the likelihood that accounts are being protected by effective passwords, applicable password content controls can be assessed. Depending on the type of password protected system being assessed, password control properties that may be analyzed can include one or more of the following: (1) A property that determines if a password is or is not required; (2) A property that determines the minimum length of the password; (3) A property that determines the maximum number of repeated characters; (4) A property that determines if a password needs to contain a mixture of letters, digits, and special characters; (5) A property that determines the maximum lifetime of a password before it must be changed; (6) A property that determines if a password needs to be different than previous passwords assigned to the account; and (7) A property that determines if a second form of authentication (e.g.; token) is needed, in addition to a password.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

Similar to security event monitoring, the maturity of a company's security state monitoring practice depends on 5 critical factors:

1. The breadth and depth of controls that can be evaluated.

2. The ability to protect the state monitoring data that is collected.

3. The ability to compare the current state of controls to a desired state of controls, specifying in the form of policy requirements.

4. The ability to eliminate extraneous data, by filtering out unimportant properties about controls that are being reported.

5. The ability to perform monitoring in a transparent manner and avoid impairing normal operations of a monitored system.

The Synergy Between Security "State" Monitoring and Security "Event" Monitoring Practices

In some respects, it may seem that security event monitoring could make security state monitoring redundant. In practice, this is usually not the case because while security event monitoring typically can reveal that a technical security control has been modified, this level of monitoring may or may not identify what the control has been modified to. Furthermore, while security event monitoring can report changes affecting technical security controls, the data is typically dispersed over time, increasing the difficulty of formulating an overall impression about the state of security. In contrast, security state monitoring focuses on the problem of sizing up the overall state of security by analyzing controls at a particular point in time and identifying gaps against a stated policy.

There may also be some thought that security state monitoring eliminates the need for security event monitoring, at least with respect monitoring changes in technical security controls. While security state monitoring can highlight inadequately configured controls, it is the security event monitoring that enables a company to explain how security controls became inadequately configured. Is it because default controls were never tightened or is it because an administrator failed to set up controls effectively or is it because an intruder deliberately relaxed controls to increase the feasibility of future unauthorized access? Security state monitoring highlights weaknesses, while security event monitoring gives you the ability to explain the origin of weaknesses – a one-two punch to improve the effectiveness of a security monitoring practice.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

Sizing your Security Monitoring Practice

Most companies that value the importance of information security will accept that some level of security monitoring is required. But, how much monitoring is enough? Do you monitor everything in an attempt to produce a comprehensive record of activity or do you attempt to be more selective in recording activity? What controls are evaluated as part of security state monitoring? How often are applicable controls evaluated?

As a general rule of thumb, the importance of monitoring depends on "the value" of what is being monitored. Less valuable systems and information are less important to monitor than more valuable systems and information. Most companies will go through a risk assessment process to rationalize how much security is needed, with the need for security directly related to (a) available funding, (b) regulatory requirements and (c) an understanding of the potential downside of a disruption to the integrity, confidentiality, or availability of important resources. Companies will prioritize the implementation of security to mitigate significant risks and potential losses from a security breach. Access controls are applied with the intent to prevent disruption or to reduce the size of the potential risk population (i.e.; population of users that may have the opportunity to disrupt). Detective controls are applied to keep administrators and users accountable for authorized activity, provide a general means of recognizing subversive activity, and provide a means to flush out vulnerabilities before they are exploited.

Part of the exercise of arriving at the optimal level of information security will involve some degree of hypothesizing; including entertaining the prospect that systems will ultimately be compromised. Such what-if scenarios tend to buttress the case for security monitoring, since active monitoring increases the likelihood that subversive activity can be recognized sooner, giving a violated company an ability to react more quickly to limit losses, recover compromised systems, and reduce the chance that an incident will lead to an embarrassing public relations event.

Although there is no optimal one-size-fits-all level of security event monitoring that is appropriate for all businesses, guidance is available from the widely respected information security management standard, ISO 17799 in order to frame what it will take to exercise "due diligence" in a security-event monitoring practice. Clause 9.7 within the standard entitled "Monitoring System Access and Use" specifically applies to security event monitoring. Requirement 9.7.1 within this clause advocates the importance of recording exceptions and other security-relevant events. This includes records of successful/rejected system access attempts (logons, logoffs, and connections) and other successful or rejected resource access attempts (including file access).

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

The ISO 17799 standard includes a number of provisions related to the role of security state monitoring; including clause 9.2.4 entitled "Review of User Access Rights" and clause 12.2.2 entitled "Technical Compliance Checking."

Applying LT Auditor+ to Help Implement Your Security Monitoring Practice

Blue Lance customers that strive to implement an effective security monitoring practice take advantage of a number of features in LT Auditor+:

- The ability to use monitoring agents that record system activities from the operating system perspective. A detailed record can be generated of access to any file containing information that needs to be protected.

- The ability to use monitoring agents to implement an effective level of security-event monitoring, achieved through the monitoring of:
    - System access (logons, logoffs, and connections),
    - Administrative activities (e.g.; account management, access control
    - management),
    - Use of privileged accounts,
    - Access to files containing confidential information,
    - Changes to access controls,
    - Changes to executable software and critical control files,
    - Suspicious patterns of activity following a successful logon,
    - Rejected attempts at accessing resources,
    - Attempts at accessing sensitive files out of a normal context,
    - Suspicious patterns of activity following exploitation of vulnerable software.

- The ability to monitor systems in a transparent manner.

- The ability to monitor Windows Servers and Workstations, NetWare Servers, eDirectory and Syslog-enabled computers/applications (including Linux/Unix Servers, Network Devices, and firewall appliances).

- The ability to evaluate the contents of any text-based log file.

- The ability to install a monitoring agent from a remote location onto a computer that needs to be monitored, provided the installer has privileged access to the

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

desired computer. This remote installation capability eliminates the need to be physically present at the computer and reduces the costs in deploying an LT Auditor+ infrastructure within an organization that has many computers that need to be monitored.

- The ability to configure and deploy a monitoring configuration from a central computer functioning as a management console to computers monitored by LT Auditor+ agents. Deployed monitoring configurations can be adjusted, on demand, from the management console, giving Blue Lance Customers the ability to throttle the level of auditing in response to changing monitoring needs.

- The ability of monitoring agents to report events in a real time manner, delivering the reports either through native operating system messaging capabilities, SNMP, or e-mail agents. Real Time Alerting can give a Blue Lance Customer the ability to recognize exceptional events (including attempted security breaches) quickly, so remedial steps can be promptly taken to contain an adversary and reduce the likelihood that information that needs to be protected will be further compromised. Real Time Alerting can be used to notify incident response teams of access to honey pot files (planted files with fake information that needs to be protected), in order to more easily identify an adversary, who has managed to penetrate an organization's infrastructure and who is searching for opportunities to compromise information that needs to be protected.

- The ability to use LT Auditor+ filtering methods in order to ignore extraneous data that is automatically recorded in native Windows logs, increasing the utility of the log files maintained by LT Auditor+ and avoiding unproductive information overload.

- The ability to archive native Windows logs for backup purposes and to enhance a Blue Lance customer's ability to investigate computer crime.

- The ability to protect the recorded activity in LT Auditor+ log files from being tampered with, including an ability to transfer log files to a separate log consolidation computer in order to simplify the management and protection of archived log files. Log file transferring can be configured to occur on a scheduled basis (e.g.; off hours) or can be configured to occur in response to an attempt at shutting down an LT Auditor+ agent (i.e.; a defensive transfer) or in response to certain detected events that may be indicative of an intruder (i.e.; another form of a defensive transfer).

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

- The ability to protect the integrity and confidentiality of communications between an LT Auditor+ agent and manager, through the use of cryptography and other control mechanisms.

- The ability to import LT Auditor+ log files into a relational database management system on the log consolidation computer, giving Blue Lance Customers a high degree of flexibility in querying activity information stored in the database using the LT Auditor+ SQL Report Generator or using other SQL oriented querying tools.

- The ability to use canned database management scripts to simplify the retention and archiving of historical data.

- The ability to audit the actions of an LT Auditor+ Administrator and to monitor the integrity of an LT Auditor+ architecture through status monitoring and transaction logging.

- The ability to perform a security assessment of controls within eDirectory or access controls protecting files stored on NetWare servers. This includes the ability to analyze password content controls, as well as other controls that determine access to resources defined to eDirectory.

Conclusion

This paper covered the role of security monitoring within a company's best security practice. Both security "event" and security "state" monitoring were presented as two complementary forms of security monitoring. Companies that desire to develop a security monitoring practice will need to follow a practice development method and will benefit by having an organizational structure that encourages broad participation from all potential stakeholders. A practice development method and proposed organizational structure were offered in the paper. Finally, the paper summarized many of the key features in LT Auditor+ that are leveraged by Blue Lance customers that strive to implement an effective security monitoring practice.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

Bill Rudolfsky is the Chief Information Security Officer for Blue Lance, and a 23 year veteran in providing Information Technology Services. Within the last 12 years, Mr. Rudolfsky held various information security leadership positions for large organizations in the banking and financial services industry including the Federal Reserve Bank and JP Morgan Chase. His credentials include obtaining Certified Information Security Professional (CISSP) status in 1999.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com