Building an Intelligence-Based Organization

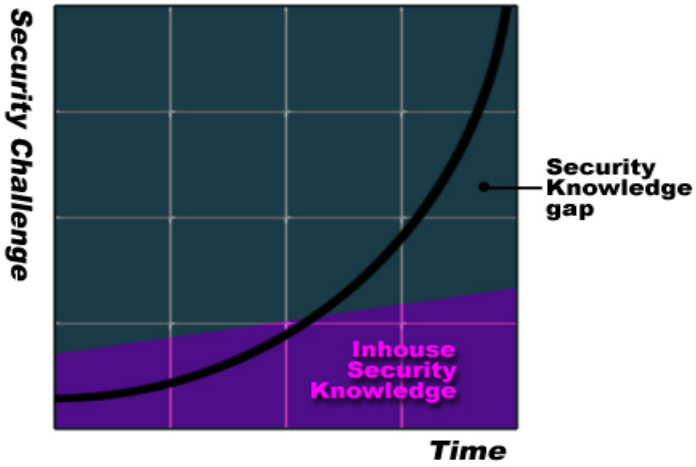
By Colin J. Tuggle

In the military, intelligence systems multiply the effectiveness of military strength by providing insight into the most precise and efficient application of that strength. Likewise, security intelligence makes enterprise security teams more efficient and increases their effectiveness in applying security safeguards, better enabling them to take the appropriate security actions at the right time.

Corporate personnel simply cannot keep up with all the sources of information reporting on security threats. Substantial savings can be realized by implementing a solution that will overcome these inefficiencies and reallocate resources in favor of proactive security solution implementation. Security intelligence provides a cost-effective means of mitigating risk by reducing the danger that an organization will be unprepared for a high-risk threat or will divert key personnel to fix low-risk threats.

The Case for Security Intelligence

Technology is insufficient to keep up with today's threats. Passive technology solutions only provide defense against known techniques; they are either incapable of evolving to handle new threats or are not timely in doing so. Technology will never evolve to handle all computer-borne threats. This is because technology is not one-sided. Technology continues to advance for hostile forces as quickly as it does for security professionals. Adversaries are constantly seeking out new vulnerabilities and apply more effective attack methods. Intelligence fills the void left by traditional security products and services.



Without security intelligence, there is a lack of knowledge and focus on proactive response to emerging security threats. This can produce information overload, lost productivity, a lack of coordination, difficulty in prioritizing security response, and impeded decision-making. Security intelligence makes order out of chaos. It helps an organization to prioritize their security response, and task individual end users and audit their actions.

Turning Information into Intelligence

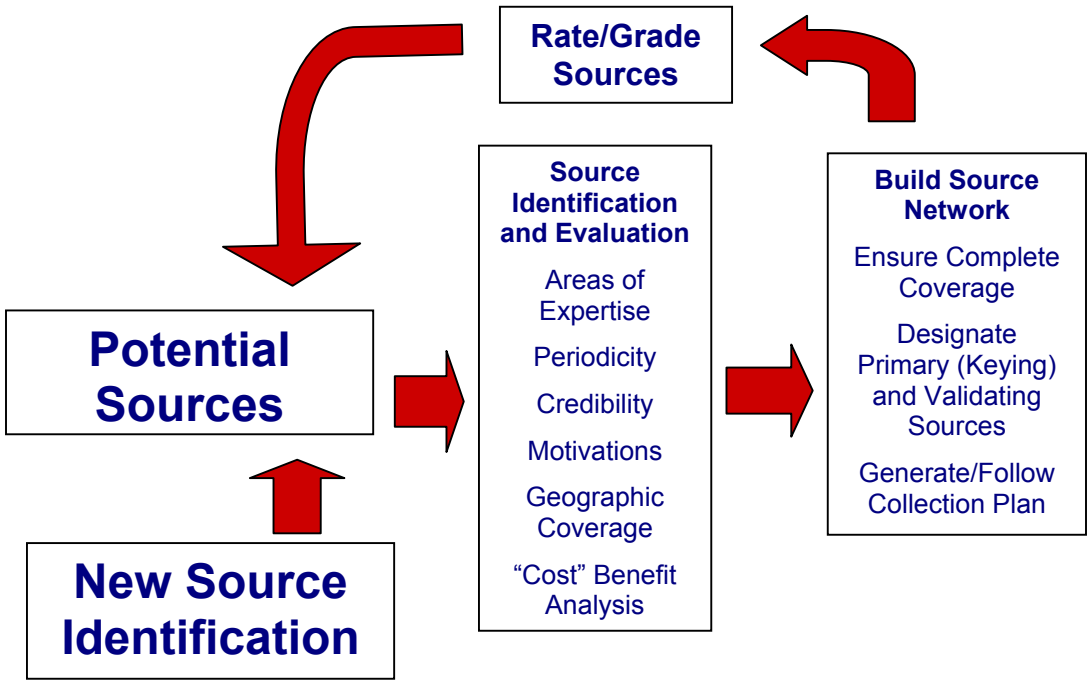
Intelligence is more than just a collection of data or bits of information. Intelligence is information that has been evaluated, analyzed, and correlated. This level of processed data is as important to IT security as it is for military operations; providing information that has been fused and filtered based upon an organization's specific needs. The goal of security intelligence is to provide early notification and analysis to the right people covering the full spectrum of security vulnerabilities, malicious codes, hacker tools and techniques, and global security trends.

Employed within a stringent quality assurance environment, the three fundamental elements of people, technology, and methodology must be integrated and balanced to form the foundation for consistent, high-quality, useful intelligence. The people dedicated to this process should effectively combine technical and intelligence gathering capabilities. This requires the coordinated efforts of managers, systems analysts, technicians, and intelligence specialists. Technology is not by itself a

solution, but provides the advanced analytical tools that are necessary to find, process, and manage threat information. An effective methodology ties the people and technology together; ensuring the efficient coordination between team members will deliver comprehensive and consistent reporting throughout an IT organization.

Building a Global Source Network

Compiling a comprehensive network of sources around the world is the first step in building a security intelligence solution. Effective security intelligence cannot be based on ad hoc source collection, where "favorite" sources are searched when time permits. Organizations must ensure that they have complete coverage of the entire security landscape. When identifying potential sources, evaluate their areas of expertise, periodicity of updates, credibility, underlying motivations, geographic coverage, and cost-benefit analysis. Furthermore, periodically rate and grade the effectiveness of your existing sources and potential new sources based upon these criteria.



There are hundreds of primary sources and thousands of supporting and validating sources available, including the following: professional associations, industry groups, government sources, software and antivirus vendors, media organizations, hacker groups, listservs, periodicals, subscription services, newsgroups, chat rooms, etc. Organizations must generate and distribute an effective collection plan to efficiently gather information from their selected list of sources.

Applying Intelligence

Security intelligence helps even a well-equipped enterprise IT security team increase the effectiveness of its security tools and reduce business risks. Consider its application to the threat and vulnerability management cycle of discovery, notification, action, and verification.

Managing the Cycle: Discovery

Once you have a global source network in place, you must have the appropriate processes set up to effectively discover newly emerging threats. An organization must fuse information from multiple

sources to avoid the perils of single source reporting – such as conflicting motives or inaccuracies. Organizations must also deconflict information from multiple sources to filter out redundant data and identify inconsistencies. Finally, an organization intelligence team must validate the information by assuring its quality to the end users.

Managing the Cycle: Notification

Upon fusing data from multiple sources, an organization's next step is to get the right information into the right people's hands so they can take the appropriate action. The biggest impediment to an effective notification process is the reliance upon manual intervention to forward information to the right people. The traditional methods of electronic mail or trouble ticketing are often not fast enough and an automated means of paging the correct individuals may also be required. Security intelligence must merge redundant and often fragmented data collection assets, eliminating islands of information and getting processed intelligence into the right people's hands.

Managing the Cycle: Action

In order to successfully support decision-making, intelligence must help to ensure that the correct action can be taken. Intelligence needs to minimize or eliminate the work an end user has to perform to determine if a threat is applicable. It must also clearly define and help to prioritize the threat, based upon well-defined criteria. Finally, intelligence is rendered useless unless it also provides solutions. Intelligence alerts must be continuously updated with the appropriate long-term patches or fixes and more immediate safeguards that can be taken.

In order to aid decision support and threat prioritization, intelligence alerts should use a consistent methodology to quantify the overall risk associated with the threat. Classifying a patch as "critical" or quantifying the risk based upon nebulous criteria such high, medium, or low risk simply does not tell an organization enough to aid in prioritizing threat response.

Our clients have found that it is very helpful to conduct risk analysis for threats based upon three criteria: Urgency, Credibility, and Severity. The "Urgency" rating is a factor of how quickly you should respond to a threat. A high urgency rating would be assigned to a rapidly propagating worm or a situation where tools are available to exploit a vulnerability. "Credibility" quantifies the confidence level in your sources based upon the number of sources reporting on a threat, the historical reliability of those sources, and in-house testing. Fusing information from multiple sources and validating technical solutions helps to increase the credibility of your information. The "Severity" rating would quantify the potential damage, based upon the access granted to an attacker, the damage to systems, and recoverability of damaged assets.

Managing the Cycle: Verification

Organizations should have an integrated means of verifying that a threat or vulnerability has been eliminated. Rather than passing unsecured e-mails back and forth, build a system that provides secure collaboration across an enterprise and a historical audit capability. Tying the audit capability directly to the applicable intelligence alert helps to coordinate your overall response more efficiently.

The Cycle Never Ends

The discovery process does not end after the initial publication of a security alert. A continuous update process is required to identify any changes to the threat environment: patch release, exploit tool development, patch validation or recall, improved safeguards. An effective change control process is necessary to ensure the appropriate updates are captured and disseminated out to the organization.

The Solution – Outsourced Security Intelligence

Organizations face a daunting challenge when attempting to build an intelligence-based organization. Finding all of the threats is only the beginning of this daily challenge. Organizations must analyze and validate threat information, determine its relevancy to their own specific environment, research the solutions and safeguards for protection, prioritize the response to these threats, and disseminate the information to the right people. This can require a great deal of attention from management and drain both time and resources across an IT organization. The value of security risk reduction must significantly exceed the costs incurred to acquire, evaluate, and disseminate intelligence information. Living with "business as usual" or attempting to build an effective in-house security intelligence solution are both far too costly.

Building an in-house security intelligence solution requires significant foresight, planning, and commitment to be effective. Merely pushing raw information within your organization is not enough. Effective security intelligence must be efficient, objective, accurate, consistent, relevant, and permit adequate time for implementing solutions. Outsourcing security intelligence saves an organization's scarce resources for decision-making and solution implementation. The network security environment is too large for individual companies to effectively monitor and evaluate. Companies need a Security Intelligence partner that will help them to keep abreast of ever changing network security threats. This translates into diminished financial and market risks and maximized Return on Investment (ROI) on security expenditures.

Organizations should ensure that any prospective outsourced security intelligence service is efficient, comprehensive, and unbiased. One of the most important factors to consider in today's business environment is vendor neutrality. Ensure that your vendor of choice does not withhold information on vulnerabilities and that their reporting is consistent across all vendors. You should never have to question whether a vulnerability alert is biased or has been delayed.

Additionally, a solution should provide detailed analysis that covers the entire security landscape: security vulnerabilities, malicious codes, hacker tools and techniques, and global security trends. Seek a solution that also provides advanced notification and management tools, such as streamlined workflow management, administrative account management, and robust search functionality that provides for efficient filtering of the entire alert database. Lastly, be wary of vendors that outsource their development, delivery, or support. A vendor with their own comprehensive in-house solution will better ensure the integrity and confidentiality of your data and help to assure rapid product development and immediate attention to product issues.

It takes more than great technology to build a truly effective intelligence service. It is the proper combination of people and processes – along with technology – that makes an outsourced solution appropriate for organizations of any size.

Colin J. Tuggle is the Director of the Knowledge Products Division at Vigilinx, the leading provider of independent, proactive security intelligence (www.Vigilinx.com).