

# People, Process and Technology: The Foundation for Effective Incident Handling

## Executive Summary

### The Business Problem

Most organizations have focused their security efforts on deploying technology to protect them from malicious activity. While deploying an appropriate security architecture is important, it should not be viewed as an absolute solution to securing your environment. Security will never be a passive activity. Skilled attackers will continue to develop new, complex methods to wreak digital havoc. As these attack methods evolve, so must security defenses and procedures. Unfortunately, the one constant in this world of change is the fact that at some point in time the organization will be attacked. At that point, the only safeguard that will prevent damage is having a solid method of incident handling.

### The Solution

Effective incident handling is dependent on the appropriate combination of People, Process and Technology. The way these components interact and build off each other will directly impact the amount of damage that will occur during an attack. When designing an incident handling program encompassing these three critical elements, it is important for organizations to plan for the worse. By designing a program around worst-case scenarios, you will be assured the best possible results under any set of circumstances.

Elements to consider in each of the three components are:

#### *Technology*

- Security architecture is about intelligence, not absolute prevention
- Aggregation and correlation technology must be implemented
- Real-time and historical reporting are necessary components
- Options available to organizations are Buy, Build or Partner

#### *People*

- Must be properly trained
- Focused on detecting and responding
- Proper rotation avoids burnout
- Intrusion Analysts must be properly empowered
- Options available to organizations are Buy, Build or Partner

#### *Process*

- Event categorization
- Threat assessment
- Appropriate response
- Archive
- Measure and report
- Options available to organizations are Buy, Build or Partner

Incorporating the elements mentioned above will lay the foundation for an effective incident handling program. As with all other security programs, it will be important to continue to communicate the value of incident handling throughout the enterprise. Only through awareness and training can organizations be ensured success.

## Technology

### Security Architecture

Technology is the first component necessary for effective incident handling. Most organizations have already deployed an extensive security architecture consisting of Firewalls, Anti-Virus and Intrusion Detection Systems. This “defense-in-depth” architecture provides a basic level of protection from malicious activity. However, many organizations view their security infrastructure as the key to prevention. Unfortunately because of the evolving nature of attacks and the fact that humans are at the root of the attacks, these systems will never provide the absolute prevention desired.

There are no “silver bullets” in the security technology space. This fact is reinforced with each new report showing incidents and resulting damage constantly on the rise. There needs to be a shift in mindset towards security architecture. Organizations must regard the primary purpose of their security infrastructure as a provider of security intelligence, rather than security prevention. Only an effective incident handling program will provide enterprises with the ability to prevent damage from cyber-attacks.

Deploying an appropriate “defense-in-depth” security architecture is critical to conducting effective incident handling. An incident handling program needs to be fed with the right information at the right time. The various components of a security infrastructure each provide a piece of the puzzle that, when assembled, enable rapid, effective incident handling decisions. The table below provides examples of the information you can attain from the various technologies that make up a typical security architecture:

Device	Incident Information
Firewalls	<ul style="list-style-type: none"><li>• Activity transmitted to and from trusted and untrusted networks</li><li>• Attempts to circumvent firewall policies</li><li>• Check URL requests for malicious activity</li></ul>
Intrusion Detection Systems	<ul style="list-style-type: none"><li>• Detection of known exploits</li><li>• Information on exploit attempts</li><li>• Extensive packet level decoding for in-depth attack analysis</li></ul>
Anti-Virus	<ul style="list-style-type: none"><li>• Early warning data regarding potential virus outbreaks</li><li>• Visibility into attempts to launch Trojan horse programs or other malicious code</li></ul>
Operating Systems/Applications/Databases	<ul style="list-style-type: none"><li>• Detection of unknown exploits</li><li>• Identify failed login attempts</li><li>• System resource issues</li><li>• Information into the state of applications</li><li>• Log information needed to interpret unusual activity as malicious</li></ul>
Authentication Servers	<ul style="list-style-type: none"><li>• Identify password grinding</li><li>• Discover other exploit attempts</li></ul>
VPNs	<ul style="list-style-type: none"><li>• Repeated unauthorized attempts to initiate VPN tunnels</li></ul>
Routers	<ul style="list-style-type: none"><li>• Reports network traffic that fails ACL permissions</li><li>• Unauthorized access attempts</li></ul>

The above systems produce a wealth of information that can be analyzed and used to stop attacks before damage is done. The next step organizations must take is to implement technology that will consolidate this critical information from its various silos into a seamless view. The implementation of this Security Monitoring Platform is critical to being able to discover and react to threats as soon as they occur.

## Security Monitoring Platform

A Security Monitoring Platform is critical to rapid incident identification and response. To be totally effective, this system must perform the following duties:

- Event collection
- Data standardization
- Event filtering
- Event correlation
- Real-time alerting
- Trouble ticketing
- Reporting

The Security Monitoring Platform must be able to collect security event information from any relevant device, including all those listed in the above table. There are a variety of methods one can use to obtain this information such as SMNP, syslog, SMTP, etc. Multiple data collection methods should be used in order to attain the best data possible. For example, some devices may report security events more robustly using the SMTP protocol whereas with other devices it may only be possible to get all the information necessary from syslog. The ability to collect security data from any device is also critical to the technology's ability to adapt to changing environments.

The second area of functionality necessary for a Security Monitoring Platform is data standardization. Because there are few widely adopting standards for reporting security events, the information collected will be in a variety of formats. Consequently, the platform must be able to translate all these proprietary event codes into a common format to enable correlation, filtering and easier visibility into the security event that is occurring. Data standardization can be accomplished by mapping the security event information contained in the native alert, for example SNMP, to fields in the underlying database, such as Source IP. The end result is a standardized alert made up of the critical information necessary for incident handling and response.

Event filtering is another important element necessary for a Security Monitoring Platform. Security devices are inherently "chatty" and produce voluminous amounts of non-critical information. The platform must be able to filter out this noise so that organizations can focus on the actionable alerts. Filtering also reduces the impact on network bandwidth as events are communicated back to the underlying database over the LAN or WAN. Filters should be behavior-based and created after evaluating the events occurring throughout the enterprise. This enables a continuous process of improvement as more and more intelligence is built into the platform.

Event Correlation provides the fundamental analysis capability of the Security Monitoring Platform. Correlation is necessary to determine the path and extent of an attack. Typical attacks will trigger events on the Firewall, Intrusion Detection Systems and multiple host systems. Correlation can link these events to a single attacker. Additionally, correlation can pinpoint frequently attacked hosts, signaling potential security holes that can then be fortified. Event correlation further reduces non-critical information, enabling faster detection of threatening events. The ability of the Security Monitoring Platform to conduct correlation is critical to gaining the context necessary to properly evaluate the threat and conduct rapid, effective incident response.

The Security Monitoring Platform must provide real-time alert information. Discovering an attack even minutes after it has occurred will result in increased damage. The goal of this platform is to reduce the amount of exposure the organization faces during an attack. Exposure is measured by the amount of time that lapses between the start of the attack and the response to this malicious activity. The less exposure the enterprise faces, the less damage will be caused by an attack. Real-time information is critical to reducing this exposure time to a minimum.

Trouble ticketing functionality is necessary to track incidents through to their resolution. Trouble tickets should map to the event categorization and threat assessment processes that are developed to handle incidents. Using trouble tickets, incident handling teams can work together to resolve any malicious activity discovered. Organizations can then measure the effectiveness of their incident handling program based on resolution times, severity of incidents and other important metrics.

Measuring results will be critical to the success of any incident handling program. The Security Monitoring Platform must contain reporting functionality to facilitate the creation of a variety of reports. Additionally, reports should also be used to conduct trend analyses that will help organizations proactively fortify their infrastructure. Reports will also be critical to demonstrate the status of the security environment to management and auditors.

A Security Monitoring Platform that contains the above functionality will facilitate an effective incident handling program. This technology is important for the scalability, event analysis and measurement necessary for a comprehensive program. The Security Monitoring Platform must reflect the incident handling processes put in place and must be able to adapt to new processes and an evolving infrastructure. A superior Security Monitoring Platform will result in superior incident handling.

### **Technology Options**

Options available to organizations seeking to implement a Security Monitoring Platform are:

- Buy off-the-shelf Security Management software
- Build this platform internally using development resources
- Partner with a Managed Security Service Provider who uses such a platform to monitor customer environments

## People

People are the most important component of an effective incident handling program. Process and technology can only supply the necessary information to conduct incident response. Ultimately the decision to respond and the method that it is accomplished will be up to skilled Intrusion Analysts. Behind every attack, even ones that are automated, are people. The only way to counter these attacks is by deploying an organizations' human talent against it.

Training and focus are critical elements when building a team of skilled Intrusion Analysts. These analysts need the proper training that will enable them to quickly identify, categorize and respond to a variety of threats. There are a variety of security training courses and certifications available to organizations, such as CISSP, GIAC and CCSP among others. The SANS Institute's Global Information Assurance Certification (GIAC) program offers the most in-depth training on intrusion handling. This specialized training should provide Intrusion Analysts with the basic skill sets they need to conduct effective incident handling. Once trained, these team members should be focused solely on incident analysis, research and response. This will avoid the temptation to utilize them for other initiatives, which tends to lead to neglecting the incident handling program. Also, by having them focus on incident handling, their experience in dealing with malicious events will grow exponentially resulting in improved response times.

There is no substitute for incident handling experience. Attacks occur using many different methods, generating a variety of different indicators. An Intrusion Analyst must be able to quickly decipher malicious activity from normal events and make quick decisions based on what they see. The only way to accomplish this is through the experience of handling thousands of events both benign and malicious.

Burnout is a common occurrence among Intrusion Analysts. This is because of the typically long periods of time between attacks. During these "quiet" periods, analysts are usually presented with volumes of low-level alerts that result in boredom and monotony. When an attack does occur, team members usually work long, stressful hours to handle the situation. To counteract burnout, organizations must rotate Intrusion Analysts regularly. Rotation should encompass incident analysis, research and response stations, allowing them to move between the monitoring console and conducting other engaging activities. Rotation should not include other aspects of security, such as patch management, in order to keep them focused on incident handling. The result will be less burnout, while increasing the experience across the incident handling team.

Empowerment of the Intrusion Analysts is very important to the success of the incident handling program. These individuals must be able to act immediately in response to any threats they discover. Every second matters when an organization is under attack and the team responsible for incident handling must be given a level of autonomy in how they resolve malicious activity. Bureaucracy, internal politics and all other hindrances must be removed from their path in order to facilitate the incident handling process. Only through empowerment will the Intrusion Analysts keep exposure time low and successfully stop attacks before damage is done.

### People Options

Options available to organizations seeking to incorporate skilled Intrusion Analysts are:

- Buy skilled expertise from the limited pool of talent available
- Build this expertise internally through training and experience
- Partner with a Managed Security Service Provider who already possess skilled Intrusion Analysts

## Process

An effective incident handling process creates a roadmap for incident identification and response. While developing this process organizations must take into consideration worst-case scenarios. Only by preparing for the worst can enterprises expect the best possible results from this process. An effective incident handling process must encompass the following steps:

- Event categorization
- Threat assessment
- Appropriate response
- Archive
- Measure and report

Event categorization is the first step in an incident handling process. Event categorization will determine the severity of the incident and how the Intrusion Analysts need to respond to the activity. Categorization should essentially follow a flow chart that walks the incident handling team through a series of levels. Initial categorization may determine whether the incident in question is a threatening security event. Another level may separate automated attacks from human-controlled attacks. This process continues down each level until a severity and associated action is determined. After completion of this step in the incident handling process, the Intrusion Analyst will know what they are dealing with and how to counter the attack.

Threat assessment is the next step in the process. Events occurring throughout organizations impact systems in a variety of ways. Therefore events must be assessed to ensure that the most threatening events are addressed immediately while less severe threats are handled over time. Threat assessment can be done in any way that makes sense to an organization. Some teams may find it easier to assign a low, medium or high severity level to events, whereas other organizations may want to assign ratings on a scale of 1 to 5. Whatever system is utilized, the end result should be to provide the Intrusion Analysts with a clearly defined threat assessment method.

Once threat assessment is accomplished, an incident handling process should define the appropriate responses to each severity level. Responses should be detailed enough to provide Intrusion Analysts with adequate direction so that when under attack they can react in a predictable, repeatable fashion. On the other hand, this process cannot possibly outline the exact method of response to every attack and should not attempt to do so. Only experience and training can drive these tactical responses. For low severity attacks, an appropriate response may be to simply log the event for historical analysis and reporting. High severity attacks may require not only countering the threat, but also contacting business unit managers, legal counsel and the authorities. These first three steps comprise the foundation of the incident handling process. This will provide a roadmap for the Intrusion Analysts to follow whenever an incident arises.

Archiving the incident and its associated category, priority level and response is necessary for future analysis. Storing all aspects of the incident is critical for forensics work. Additionally, the same attacker may be responsible for multiple events over time. These should all be stored to strengthen the case against the perpetrator if the need for prosecution arises. This information is also critical to the ongoing tuning of the incident handling program.

The final step necessary for an effective incident handling program is measuring and reporting the results. The effectiveness of the program needs to be continually monitored so that feedback is incorporated into future revisions. Over time the program should continue to reduce exposure and become extremely accurate at determining the true nature and severity of the threat. This is only accomplished through measuring results. Additionally, organizations can report these results to management and auditors.

### Process Options

Options available to organizations seeking to implement an incident handling process are:

- Buy consulting time for an outside security consulting firm to develop a process
- Build this process internally through research, trial and revisions
- Partner with a Managed Security Service Provider who has already implemented an incident handling process

## Summary

An effective incident handling program is critical for any organization that is online today. With vulnerabilities, exploits and attacks all on the rise, it is not a question of whether an incident will occur, but when. Having a plan in place will enhance an enterprise's security posture and lead to more effective overall information security. Implementing skilled people, security monitoring technology and an incident handling process will enable organizations to limit the amount of exposure time to attacks and resulting damage from those attacks. Additionally, centralized event information will provide the organization with the ability to generate performance metrics never before possible. Effective incident handling programs will also enable the enterprise to comply with various industry regulations and lead to more successful audits. Organizations seeking to rapidly implement an incident handling program should consider Managed Security Service Providers before buying the components separately or building a program internally. These providers will enable organizations to attain the enhanced security they need with minimal impact to internal resources.

## Get Started Today

Contact your local reseller at:

Or contact LURHQ Corporation at:

**843.903.4376**

[info@lurhq.com](mailto:info@lurhq.com)

[www.lurhq.com](http://www.lurhq.com)