

“Automated Incident Handling Using SIM”

By Anton Chuvakin, Ph.D., GCIA, GCIH

Introduction

Security professionals often learn to live by the slogan “prevention-detection-response.” Each of these three components is known to be of crucial importance to the organization’s security posture. However, unlike detection and prevention, the response is simply impossible to avoid. Sometimes the organization has weak prevention and detection capabilities, but response will have to be there since the organization will often be forced into response mode by the attackers. The organization will likely be made to respond in some way after the incident has occurred.

In light of this, becoming prepared for the incident response is to be one of the most cost effective security measures the organization takes. Timely and effective incident response is directly related to decreasing the incident-induced loss to the organization. Several industry surveys have identified that public company’s stock price may plunge several percent because of a publicly disclosed incident. Incidents that are known to wreak catastrophic results upon the organizations may involve malicious hacking, virus outbreaks, economic espionage, intellectual property theft, network access abuse, theft of IT resources and other policy violations.

Effectively responding to incidents requires knowledge of your computing environment, company culture and internal procedures, implemented security countermeasures as well as possessing incident response skills. Incident response fuses together technical and non-technical resources, bound by the incident response policy.

To build an initial incident response (IR) framework one can use SANS (SysAdmin, Audit, Network, Security) Institute Six-Step incident response methodology, which includes the following six steps of dealing with the incident:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Follow-Up

The actions defined by the plan are started even before the incident transpires (Preparation steps) and extend beyond the end of the immediate mitigation activities (Follow-Up).

Defining and implementing the process such as the above for an organization is not a trivial pursuit. Fortunately, many organizations already have an important tool to assist them with this project: a Security Information Management (SIM) product. SIM products evolved from simple event management and aggregated into advanced security centralization solutions that can help organization to optimize various aspects of security management, including incident, risk, policy and vulnerability management.

In this article, we will talk about building an effective management process for incident resolution, focusing on how it may be optimized by using SIM products.

Preparation stage covers everything one should do before handling the first incident. It involves both technology issues, such as preparing response and forensics tools, learning the environment, configuring systems for optimal response and monitoring, and process issues, such as developing response policy, assigning responsibility, forming a team and establishing escalation procedures. Additionally, the steps to increase the security posture and thus decrease the likelihood and damage from future incidents are included here. Security audits, patch management, awareness programs for employee security and other security tasks all serve to prepare the organization for the incident action.

Building a culture of security and a secure computing environment also serves as incident preparation. Here SIM products can help significantly! For example, establishing a real-time system and network security event-monitoring program will help to receive early warnings about the hostile activities as well as collect evidence after the incident. Providing a single view into your security infrastructure goes a long way towards being more prepared and equipped to deal with the incidents as they occur as well as cleaning up in the aftermath. Single evidence storage allows performing sophisticated data analysis, leading to better awareness of threats and vulnerabilities.

Identification is what happens first when the incident is detected, reported by the third parties or even suspected. Determining whether the observed event does in fact constitute an incident is of crucial importance here. Careful record keeping is also very important, since such documentation will be heavily used at later stages of the response process. One should record everything that was observed in relation to the incident, whether online or in the physical environment. Thus, increased security event monitoring is likely to help at that stage by providing information about the chain of events leading to the incident. During this stage, it is important that people responsible for the handling maintain the proper chain of custody. Contrary to popular opinion, this is important even when the case is never destined to end up in court.

Various security technologies play a role in incident identification and the SIM solution is at the center of it. For example, firewall, IDS, host and application logs reveal evidence of potentially hostile activities, coming from both outside and inside the protected perimeter. Logs are often tantamount in finding the party responsible for those activities. Security event correlation, performed by a SIM solution, is essential for high quality incident identification, due to its ability to uncover patterns in incoming security event flow. Collecting various audit logs and correlating them in near real-time goes a long way towards making the identification step of the response process less painful. Additionally, incident identification is greatly helped by “qualifying” the IDS and other alerts using other environment context, such as system vulnerabilities, running applications as well as business value. SIM solutions excel at such multifaceted analysis.

Containment is what keeps the incident from spreading and thus incurring higher financial or other loss. During this stage, the incident

responders will intervene and attempt to limit the damage, such as by tightening network or host access controls, changing system passwords, disabling accounts, etc. While completing the above steps, one should make every effort to keep all the potential evidence intact, balancing the needs of system owners and incident investigators. The backup of the affected systems to preserve them for further investigation is also essential at this step. The important decision on whether to continue operating the affected assets should be made by the appropriate authorities during this stage.

SIM solution may deploy automated containment measures in case of some security incidents, especially those on the perimeter of the organization. This is possible if security event correlation is used in the incident identification process for reliable threat identification. Correlation makes incident identification much more accurate, thus enabling automated containment measures such as firewall blocking, system reconfiguration or forced file integrity checks.

Eradication is a stage when the factors leading to the incident are eliminated or mitigated. Such factors often include system vulnerabilities, unsafe system configurations, out-of-date protection software or even imperfect physical access control. In addition, the non-IT controls such as building access policies or key card privileges might be adjusted at this stage. Because of this stage in case of a hacker-related incident, the affected systems are likely to be restored from last clean backup or rebuilt from the operating system vendor media with all applications reinstalled.

Time is critical during the eradication stage. The first response should satisfy several often-conflicting criteria, such as accommodating the system owners' requests, preserving evidence, stopping the spread of damage while complying with all the appropriate organization's policies. SIM products centralized incident resolution capability helps to streamline

Recovery is the stage where the organization's operations return to normal. Systems are restored, configured to prevent recurrence and are returned to regular use. To insure that the newly established controls are working, the organization might want to maintain the increased monitoring of the affected assets for some period.

SIM products provide increased and optimized monitoring, which, if implemented before the recovery stage, will not only lead to increased protection of the affected assets, but also might be adopted as a new baseline for the whole organization, especially if such monitoring helps to uncover new threats. Thus, SIM solution will drive security for the entire enterprise, contributing to future incident prevention.

Follow-Up is an extremely important stage of the incident response process. Just as in the preparation stage above, proper incident follow-up helps to ensure that lessons are learned from the incident and that the recurrence of similar incidents is prevented. Reports on the incident are often submitted to the senior management. It covers the taken actions, summarizes the lessons learned and serves as a knowledge base in case of similar incidents in the future. It might also summarize the intruder's actions; tools used, summarize details of vulnerabilities exploited, and contain other information on the perpetrator. More in-depth changes to the organization's handling of security are also performed at this step.

Follow-up steps often need to be distributed to a wider audience than the rest of the investigation process. Enterprise-wide security knowledge base, such as provide by a SIM solution, helps to address this challenge. It will ensure that IT resource owners will be more prepared to combat future threats. To optimize the distribution of incident information, one can use various forms and templates, prepared in advanced for different types of incidents. Incident cases should also be added to an organization-wide security knowledge base, in addition to the industry security resources and vulnerability knowledge. A summary of suggested actions might also be sent to the senior management.

Overall, the SANS process facilitated by a SIM solution allows one to give structure to the otherwise chaotic incident response workflow. It defines the steps that will then be followed under incident-induced stress with high precision. In fact, many of the above steps may be built from the pre-defined procedures.

Following the steps will then be as easy as selecting and sometimes customizing the procedures for each case at hand. Incident handling workflow will become relatively painless and the crucial steps will not be missed and documented properly. Using pre-defined procedures also helps train the incident response staff on proper actions for each process step. The automated system may be built to keep track of the response workflow, to suggest proper procedures for various steps and to handle incident evidence securely. Additionally, such a system will facilitate collaboration between various response team members, who can share the workload for increased efficiency. Some SIM solutions provide security team collaboration and reporting capabilities.

What is even more important, monitoring incident resolution activities allows the organization to implement effective security metrics. It is one thing to count number of alerts or events flowing from various sensors, but to take security assessment to the next level one needs to measure the performance of the whole security process, involving both people (such as security team members working on the incident cases) and technologies.


SIM and Incident Handling Integration

The incident handling system is thus a natural component of the Security Information Management (SIM) solution, since properly deployed SIM solution holds most evidence of the information security incident. Incident handling is SIM product functionality aimed at gathering and organizing security event data around incidents and enforcing proper response workflow in order to facilitate effective and prompt response to security incidents. General trouble ticketing systems simply do not have the workflow optimized for security incidents and incur a steep learning curve as well.

Tight integration of Security Information Management and incident handling provides many important benefits to the system users. It establishes a single control point of the security response capabilities by combining the major potential evidence storage (a SIM solution) with the investigative platform. In addition, it enables users to create incidents from detected event data with just a few mouse clicks or even automatically.

Moreover, due to sensitive nature of both incident data and security event data, a SIM solution can provide a secure way to store case evidence and apply tight and granular access controls to case data, while still allowing investigators to work together on a case.

Conclusion

Security Information Management (SIM) systems such as netForensics have an incident handling component to assist the system users with the crucial part of the security triad—incident response. Such a component should not only simplify and optimize the response process, but also serve as a security knowledge repository and be useful for security staff training. Having a highly efficient incident response program will help organizations save money by limiting the damage from security incidents and increasing the efficiency of the existing security infrastructure investments. 

Anton Chuvakin, Ph.D., GCIA, GCIH is a Senior Security Analyst with netForensics, a security information management company, where he is involved with designing the product and researching potential new security features.