

# Managed Security Services and the Incident Handling Process

By Joe Stewart, GCIH and Steven Drew, GCIA

## Introduction

This article looks at the incident handling process as it relates to managed/outsourced security. Often companies find it more economical to outsource or partner with a managed security services provider (MSSP) with the advanced skills needed to ensure a strong information security posture. When an incident occurs, the responsibilities are shared between the IT staff of an organization and the MSSP's security experts working remotely. In this scenario, steps must be taken to ensure effective communication and cooperation between the two entities for the smoothest possible recovery from an incident.

## Incident Handling

It is important to distinguish incidents from events. An event is any observable occurrence on a network. An incident is an event that has potential for damage to the company. The SANS Institute has defined a set of steps in the incident handling process in its excellent guide *Computer Security Incident Handling: Step-by-Step*. We will use the steps defined by SANS to illustrate the process and considerations when dealing with managed security.

### **Step 1: Preparation**

While it is impossible to prepare for every possible contingency, having a plan ahead of time should be your number one priority. This is a crucial step, and it requires the forethought of someone experienced in incident handling. Your MSSP should have identified and handled many incidents in the past, and you can draw on this experience to help formulate a plan for your company. They will likely have suggestions you would not have even considered.

In addition, you should provide your MSSP with as much information as possible to help them understand your environment. Network diagrams and host profiles that describe the types of services running on critical hosts are especially beneficial. If your MSSP offers managed vulnerability scanning, you can allow them to periodically scan your infrastructure and use the information to build network and host profiles in addition to proactively identifying potential vulnerabilities.

### **Step 2: Identification**

Your MSSP should be watching events on your network 24 hours a day in near real time. If they are an effective MSSP, they should quickly identify an incident. Without constant monitoring, it could be a considerable amount of time after an incident occurs that you are able to identify it. With each minute that passes, the potential for damage grows. You should make sure your MSSP has skilled analysts on staff at all times. A good indicator of skill are SANS certifications. Experienced network professionals consider many certifications "fluff". However, the GIAC Certified Intrusion Analyst (GCIA) certification requires a lengthy written practical

assignment and two written tests that measure the capability of an individual to conduct effective intrusion analysis. It is one of the best certifications out there, and achievement of it is no small task.

Notification of the incident in progress can occur in many ways including email, telephone, or pager. You should expect to be notified by telephone or pager when a high-threat incident is identified since time is of the essence.

Mature MSSP's offer secure web-based portals that dramatically facilitate communications during the incident handling process. Features you should look for include:

- Encrypted, strongly authenticated access to the portal for members of your incident handling team.
- Real-time view of security events and incidents. This will enable to your incident handling team to view the forensic details of the individual events related to the incident.
- Reporting tool that enables your incident handling team to generate reports on-demand.
- Ability to specify and modify escalation procedures for your organization.

These features will help ensure efficient communication between you and your MSSP during this and subsequent steps in the incident handling process.

### ***Step 3: Containment***

At this point your MSSP has alerted you to a situation. You need to initiate procedures to bring the incident under control and allow it to spread no further. Once again, the experience of your MSSP should be called into play. You should expect your MSSP to be more than a glorified escalation service. The MSSP should be able to recommend procedures to contain the incident. Your MSSP may also be able to dispatch incident handling experts (probably for an additional fee) to assist with the incident handling process.

Prior to this step, and before making any changes to any machines, you must decide what approach you are going to take in the incident handling process. Will you try to eliminate the problem and restore operations as soon as possible? Or do you want to prosecute the responsible parties? While prosecution is often the preference of many victims of a compromise, it forces a whole new level of handling to come into play. Steps must be taken to preserve evidence and chain-of-custody, otherwise you may find yourself in court without a leg to stand on. If you choose to go this route, ask your MSSP to help in suggesting proper procedures for maintaining the evidence for use in a court of law.

### ***Step 4: Eradication***

Although they may seem like similar steps, eradication differs from containment. In the containment phase, you are merely trying to prevent the problem from getting worse. In the eradication phase, you eliminate the threat from your network. Your MSSP should be able to point you to the proper resources (patches, scanning tools, AV updates, virus removal tools) before you even ask for them. It is the MSSP's job to stay current on the latest vulnerabilities and recommended remediation.

## ***Step 5: Recovery***

The recovery phase is where you restore your business to full working order as it was before the incident. This usually involves restoring from backups and testing the network to make sure no traces of the threat remain. The MSSP's role in this step will vary depending on the service they are providing for your organization. If the MSSP remotely manages any firewalls, IDS, AV, or content scanning systems for you, they should maintain configuration backups. Should any of these systems be impacted by the incident, the MSSP engineers will be able to work with you to quickly restore an impacted system under their management.

If your MSSP offers managed vulnerability scanning in its suite of services, such a scan can help verify the recovered systems have been properly patched and locked down.

## ***Step 6: Lessons Learned***

This is a step that is often overlooked even when not working with a managed security services provider. There should always be a follow-up meeting to discuss the incident and make suggestions to improve the incident handling plan. It should not be a time for placing blame, but instead a time to focus on preventing future occurrences of the incident that just happened. It is crucial for your MSSP to be involved in this step. Not only can the MSSP offer unbiased suggestions from an outsider's perspective, they should incorporate feedback from the incident into their service delivery to offer a more effective service. If you keep your MSSP in the dark, they may be hindered in mitigating risk for a similar incident in the future.

## **Conclusion**

Incident handling is a very detailed subject that cannot be fully covered in the scope of this article. Because of the complexity of incident handling, many companies choose to partner with a Managed Security Provider to assist. This is especially valuable to organizations lacking the human or financial resources needed to focus on information security.

If your company does not have a trained incident handler on staff, you should look to your MSSP to take the lead in an incident. Look for a company that has both Certified Incident Handlers (GCIH) and GIAC Certified Intrusion Analysts (GCIA) and you are probably in good hands.

Many MSSP's have portals designed to facilitate the flow of information between the MSSP and your organization. Regardless of the skill of the MSSP's staff, they cannot be effective without good communication from you. The key to effective outsourced security is good communication. You should consider your MSSP as more of a partner rather than an outsourced provider.

Don't forget to transmit as well as receive.

## **About the Authors**

Steven Drew, GCIA, is the VP of Managed Security Services with managed security services provider [LURHQ Corporation](#). He may be reached at [sdrew@lurhq.com](mailto:sdrew@lurhq.com).

Joe Stewart, GCIH, is a Senior Information Security Analyst with managed security services provider [LURHQ Corporation](#). He may be reached at [jstewart@lurhq.com](mailto:jstewart@lurhq.com).