White Paper

Ten Ways to Prepare for Incident Response

intel Security

Table of Contents

This white paper was written by:
Jim Olmstead
Senior Consultant, Incident Response and Forensic Practice
Foundstone® Services

Introduction

As a senior consultant on the Foundstone Services incident response and forensic team, I regularly respond to a wide range of security incidents at client sites. I have assisted clients with the containment and eradication of malicious code (for example: ransomware and malware infections) and responding to unauthorized access/network breaches impacting their enterprise environment. During all of the responses, there was the need to identify the nature of the incident, assess the client's security infrastructure, and work towards the identification of the threat or attack vector(s). The information gathered from the initial assessment and related analysis was then used to isolate and contain the malicious activity impacting devices within the environment.

Each response is different and presents its own challenges, which are addressed. However, there are common general security methodologies and best practices that help make the engagement a success during the containment, eradication, and recovery of the environments. To mitigate the chaos generated from an incident, we adopt and implement different security standards, such as National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), and others.

This paper focuses on various steps and processes that you can take to help prevent and/or reduce the malicious impact of commodity malware and viruses on your enterprise, as well as reduce the impact that hackers may have on your environment.

Engagement Scenario

Client engagements are initiated when Intel Security and/or the Foundstone Services team is contacted and a request is made for assistance to respond to a security breach, malware, or other malicious activity impacting the client's environment. During an Emergency Incident Response (EIR), a consultant will arrive on site within 24 hours. Remote assistance can be provided immediately. The remote support provided will depend upon various factors and according to your needs.

To be successful during any incident response (IR), companies should test their IR capabilities annually in a way that is similar to how companies test their disaster recovery plans:

- **Stress:** The stressors of reacting, as well as increased reporting requirements, that occur during an incident can substantially affect the ability of security personnel to respond both in a timely and effective manner. Additionally, the added stress of directly reporting events to senior leaders, the board of directors, auditors, and regulatory agencies will impact and/or delay the responders' ability to respond. If the required reporting times are scheduled to be close in frequency, it will impact the responder's ability to perform even simple tasks during the crisis.
- **Communication:** There is a need to have open access to the organization's computer security personnel in order to respond and perform needed work. The access and priority of the incident responders should take precedence over other previously scheduled and/or non-critical tasks. There needs to be an established channel of communication and process to ensure that IR needs are prioritized and, when necessary, escalated.
- **Training and Expertise:** The level of training and expertise varies across all industries and business types—and the lack of skills will impact the ability to respond. A training curriculum should be established to provide needed skills and expertise in advance of an incident.
- **Maturity:** The level of maturity of the organization and its IR and forensic team will play a significant factor in the ability to respond. If the team has not rehearsed or practiced their skills in advance of the response, the reaction time will lag, as the responders will be learning (or relearning) skills while reacting.

As organizations mature and are better prepared to respond, they can reduce the impact of threats on their environment. They will be better prepared to respond in a timely manner when there is a significant incident. Ultimately, preparation across many fronts is essential to enhancing your security and having the necessary capabilities and tools to respond to a crisis.

Ten Ways to Prepare for an Incident Response

1. Define Roles, Guidelines, and Procedures

During an incident it is very important for responders to understand their roles and responsibilities across the organization. Depending upon the size of the organization, there may not be the ability to divide the responsibilities over many people, so some individuals may take on multiple roles. When an individual has to assume many roles, their effectiveness diminishes. In these circumstances, it may be necessary to add additional personnel from elsewhere in the organization to assist or to temporarily augment your resources with outside contractors to either lead and/or respond during the incident.

It is very important to have a central point of command and control and to assign an incident lead or commander to be responsible for complete response activities and associated communications. The names of the departments will vary. Whatever the departments are called, they need to be in line with immediate response activities, as well as policy and communications:

- IR and forensics.
- Network and information security.
- Network engineering and infrastructure.
- Endpoint security.
- Security Operations Center (SOC).
- Legal department.
- Public relations.
- Policy or contracting.
- Corporate security.

In small organizations and in less mature organizations, a handful of people will be responsible for all aspects of response, and there will not be any division of computer security components.

2. Communicate Plans and Procedures Effectively

Preplanning considerations should be done before an incident. There is a need to include the potential need for both out-of-band communication (non-business accounts) and encrypted communications. Consideration should be given during planning for a meeting space large enough for a team of people to meet and work. This room should have working phones, network connections, internet connections, whiteboards, and/or a projector and screen. This room will act as the central point for all response activities and coordination. In advance of any incident, a current contact list with all of the relevant stakeholders should be compiled and available to the Chief Information Officer (CIO), Chief Information Security Officer (CISO), and other security managers and team leads to ensure availability and access.

The information collected can used to prepare a press release or other communications that are released to address concerns of organizational leadership, employees, regulators, or the client's outside users and customers.

3. Incorporate Thorough Intelligence and Research
During an incident, you will have to identify the true nature of the incident or the attack. All too often, the initial contact related to an incident contains inaccurate or incomplete information. This is generally caused by hastily compiled information and not interviewing the user of the victim systems.

Once you have determined the threat, you will need to understand the tools and methodologies used. Once you have this knowledge, you can perform threat intelligence research to further understand your adversary or how the malware works. You should also have the capability to further review the tools in order to use the indicators of compromise (IoCs) and attack vectors to feed back into your security applications and infrastructure in order to better defend and protect your environment. You must either have onsite capabilities for computer forensics and tools for reverse engineering or consider other resources to perform this work.

4. Isolate or Monitor Affected Systems (Virtually or Physically)
During an incident, you will identify a variety of executables, files, processes, ports, IP addresses, and other IoCs. Once you have identified these IoCs, you will have to decide whether or not to isolate systems from connecting to the network in order to protect your infrastructure from potential destructive activity, exfiltration of data, and other potential threats. This can be done by physically isolating the system, by disconnecting the network cable, by virtually severing the network connection by mean of a host-based firewall policy, or by disabling the port from the switch. The virtual isolation of a system is highly desirable, given that most businesses have remote employees and or office that are located around the world. The days of walking across the floor to locate a system are long gone.

5. Document and Maintain Records of Response of Activities
Documentation during a response is essential for a number of reasons. The ability to recall facts concerning events during an incident can prove helpful when you have to repeat your results or document that you have completed all aspects of your review. This type of recordkeeping will also prove helpful when you need to relay facts around events to other team members, to your senior management, auditors, and even regulatory bodies.

Note taking can either be done electronically or on paper. While electronic storage does have advantages, you and your team may be required to initially record information on paper and then enter it into a database later. Often, it is useful to put facts and information on a whiteboard in order to share with the group and to later record it electronically.

Ultimately, this information will help you prepare your action report and your lessons learned after the incident.

6. Document Chronology of Incident Events
Once your notes are recorded, you should keep in mind the order of events by date and time. As you record the chronology of events, often other activities and/or events are put in context. This helps to guide response activities and will help you build a easy-to-understand graphic for your final report.

7. Understand Response Phases

It is important to identify the scope of the incident, work to contain the threat(s) in your environment, and then work toward remediation. During the containment phase, you need to identify the obvious threats and work toward finding the hidden threats. This will require understanding various disciplines, including endpoint threat/data analysis, forensic and malware analysis, and network traffic analysis. As the incident response progresses, there will be back-and-forth communication among the various departments that will use the information found during the review of endpoint data, security application data, and network data. This information is fed back across the teams to help contain the threat (for example, malware or threats from human attackers) in order to contain the incident. As the initial threats to the incident are addressed, you can move towards remediation. At this time, you can take all of the information gathered from lessons learned and apply it to cleaning up any potential persistence mechanisms or close down vulnerabilities in your environment.

During remediation, you should check all of your security measures. You should be proactive about implementing and refining security measures before you have an incident and to reduce any further impact in the future.

8. Stay Vigilant by Securing Architecture, Applications, and Operating Systems

It is crucial to understand threats and vulnerabilities in your environment and work to secure those threats before they become an issue. The following areas should be addressed both as a preventative measure during an incident and enhanced during the post-response phase to ensure that your environment is secure.

1. Ensure operating systems are up to date.
2. Ensure security applications are up to date.
3. Ensure third-party applications are patched and up to date.
4. Do not allow unauthorized USB or personal devices on network.
5. Segment the network, and keep guest access separate.
6. Use two-factor authentication.
7. Ensure there is a password policy covering time-to-go-live, complexity, and length.
8. Check firewall and security policies to ensure that perimeters are secured, and use penetration testing to validate existing policies. Ensure logs are preserved and safeguarded.
9. Use network and email security products at gateways to monitor, block, and filter unwanted and/or unsafe sites and potentially harmful files before they get to the endpoint. Ensure cloud services are covered with monitoring and security protection.
10. Disable auto-run and only allow, if necessary, as an exception.
11. Disable Microsoft macros, and force users to enable only when needed.
12. Disable use of open shares and any unnecessary mapped shares.
13. Restrict use of administrative accounts and privileges, and allow only as an exception. Remove them when they are no longer necessary.
14. Follow up security enhancements with user computer security and awareness training to reinforce the notion that bad actors will attempt to trick users into disabling security enhancements. Users need to beware of suspicious or unsolicited email.

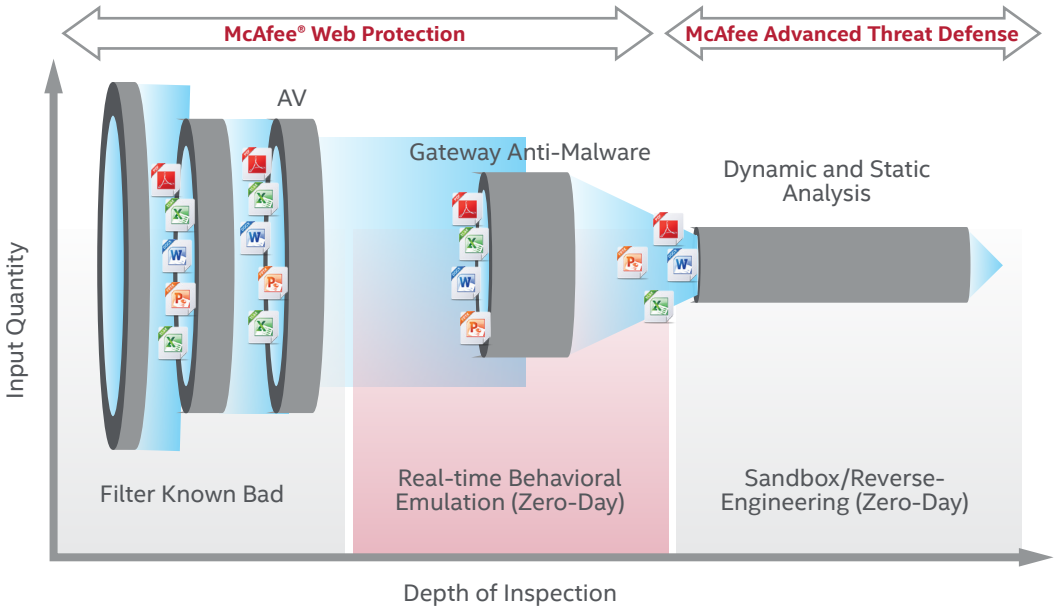

Figure 1. Reducing incoming threats to environment with automation.

9. Maintain Logs and Archives

It is extremely important to be able to review historic logs and data in order to reconstruct the activities of a hacker or the spread of malware across you network. By routinely preserving your logs and forwarding the data to an archive, you will have those records available during an incident. Also, by archiving the data to a protected system or an off-site location, you can reduce the potential for an attacker to destroy evidence.

During an incident response you will need access to many types of logs and data, including but not limited to:

- Endpoint threat and antivirus logs.
- Syslog's or other enterprise/network traffic logs.
- Network traffic captures (PCAP)
- Firewall logs, intrusion detection systems (IDS)/intrusion prevention systems (IPS.
- Web proxy logs.
- Microsoft event logs.
- VPN access logs.
- DHCP logs.
- DNS logs.
- Microsoft Active Directory (AD) logs.
- Cloud environment monitoring and protection logs.

10. Use an Endpoint Management and Monitoring Solution

It is important to be able to manage all of the assets in your environment and to have visibility and reporting of threats. Always ensure that any system that connects to your environment is installed with security software so that each endpoint is updated with threat detection signatures, access control rules, and policies. These policies will determine when the system is scanned for viruses and malware, as well as other potentially unwanted programs (PUPs). Additionally, if you contract

for cloud or other outside resources, you should ensure that the same type of monitoring and security protections are in place and maintained.

If a managed system is not updated with the current updates and policies, it increases the potential for security vulnerabilities in your environment. Also, your personnel should monitor the daily threat detections and review for any escalating or unwanted activities on your network. These are basic security considerations that organizations should follow regardless of their size and/or industry.

Summary

An effective incident response will start well in advance of an actual detection of any incident or crisis. The time an organization spends on preparation and planning before an incident occurs can minimize the impact and exposure during an incident. As more businesses are beginning to see, it is not if, but when they will need address advanced threats. This kind of preparation is essential to the future success of any response. An incident commander should be identified who can effectively manage an incident and coordinate all communication among stakeholder groups before an incident occurs.

The implementation of best security practices, patching, and updating will help minimize the impact of malicious code and hackers to the network and endpoints. If you maintain legacy operating systems, unpatched systems, and applications, you will increase the overall risk exposure to your environment. By conducting regular tabletop exercises or dry-run exercises, you can practice what you have prepared on paper.

About the Author

Jim Olmstead is a senior consultant with Foundstone Services, where he provides IR and digital forensic services to clients. His duties include responding to system breaches and malware outbreaks, performing IR gap analysis, performing forensic analysis, conducting risk-based investigations, providing IR responses, providing forensic training, and delivering customized scenario-based tabletop exercises.

Learn More

We offer an array of resources to help you improve your incident response processes—from guidance on standards and best practices to free tools and detailed threat advisories. Find out more by visiting: **https://www.mcafee.com/us/downloads/free-tools/index.aspx**

About Foundstone Services

Foundstone Services, a division of the Intel® Security Professional Services team, offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone consultants identify and implement the right balance of people, process, and technology to manage digital risk and leverage security investments more effectively. The team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military. Learn more at **www.foundstone.com**.

About Intel Security

Intel Security, with its McAfee product line, is dedicated to making the digital world safer and more secure for everyone. **www.intelsecurity.com**. Intel Security is a division of Intel.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com