Preparation Stage (Part 1)

In the preparation stage, we have two separate objectives. The first one is the establishment of incident handling capability within the organization. The second is the ability to protect against and prevent IT security incidents by implementing appropriate protective measures. Such measures include endpoint and server hardening, active directory tiering, multi-factor authentication, privileged access management, and so on and so forth. While protecting against incidents is not the responsibility of the incident handling team, this activity is fundamental to the overall success of that team.

Preparation Prerequisites

During the preparation, we need to ensure that we have:

- Skilled incident handling team members (incident handling team members can be outsourced, but a basic capability and understanding of incident handling are necessary in-house regardless)
- Trained workforce (as much as possible, through security awareness activities or other means of training)
- Clear policies and documentation
- Tools (software and hardware)

Clear Policies & Documentation

Some of the written policies and documentation should contain an up-to-date version of the following information:

- Contact information and roles of the incident handling team members
- Contact information for the legal and compliance department, management team, IT support, communications and media relations department, law enforcement, internet service providers, facility management, and external incident response team
- Incident response policy, plan, and procedures
- Incident information sharing policy and procedures
- Baselines of systems and networks, out of a golden image and a clean state environment
- Network diagrams
- Organization-wide asset management database
- User accounts with excessive privileges that can be used on-demand by the team when necessary (also to business-critical systems, which are handled with the skills needed to administer that specific system). These user accounts are normally enabled when an incident is confirmed during the initial investigation and then disabled once it is over. A mandatory password reset is also performed when disabling the users.
- Ability to acquire hardware, software, or an external resource without a complete procurement process (urgent purchase of up to a certain amount). The last thing you need during an incident is to wait for weeks for the approval of a $500 tool.
- Forensic/Investigative cheat sheets

Some of the non-severe cases may be handled relatively quickly and without too much friction within the organization or outside of it. Other cases may require law enforcement notification and external communication to customers and third-party vendors, especially in cases of legal concerns arising from the incident. For example, a data breach involving customer data has to be reported to law enforcement within a certain time threshold in accordance with GDPR. There may be many compliance requirements depending on the location and/or branches where the incident has occurred, so the best way to understand these is to discuss them with your legal and compliance teams on a per-incident basis (or proactively).

While having documentation in place is vital, it is also important to document the incident as you investigate. Therefore, during this stage you will also have to establish an effective reporting capability. Incidents can be extremely stressful, and it becomes easy to forget this part as the incident unfolds itself, especially when you are focused and going extremely fast in order to solve it as soon as possible. Try to remain calm, take notes, and

? Go to Questions

Table of Contents

Introduction

Incident Handling

Cyber Kill Chain

The Incident Handling Process

Incident Handling Process Overview

Preparation Stage (Part 1)

Preparation Stage (Part 2)

Detection & Analysis Stage (Part 1)

Detection & Analysis Stage (Part 2)

Containment, Eradication, & Recovery Stage

Post-Incident Activity Stage

ensure that these notes contain timestamps, the activity performed, the result of it, and who did it. Overall, you should seek answers to who, what, when, where, why and how.

Tools (Software & Hardware)

Moving forward, we also need to ensure that we have the right tools to perform the job. These include, but are not limited to:

- Additional laptop or a forensic workstation for each incident handling team member to preserve disk images and log files, perform data analysis, and investigate without any restrictions (we know malware will be tested here, so tools such as antivirus should be disabled). These devices should be handled appropriately and not in a way that introduces risks to the organization.
- Digital forensic image acquisition and analysis tools
- Memory capture and analysis tools
- Live response capture and analysis
- Log analysis tools
- Network capture and analysis tools
- Network cables and switches
- Write blockers
- Hard drives for forensic imaging
- Power cables
- Screwdrivers, tweezers, and other relevant tools to repair or disassemble hardware devices if needed
- Indicator of Compromise (IOC) creator and the ability to search for IOCs across the organization
- Chain of custody forms
- Encryption software
- Ticket tracking system
- Secure facility for storage and investigation
- Incident handling system independent of your organization's infrastructure

Many of the tools mentioned above will be part of what is known as a `jump bag` - always ready with the necessary tools to be picked up and leave immediately. Without this prepared bag, gathering all necessary tools on the fly may take days or weeks before you are ready to respond.

Finally, we want to stress the importance of having your documentation system completely independent from your organization's infrastructure and properly secured. Assume from the beginning that your entire domain is compromised and that all systems can become unavailable. In similar fashion, communications about an incident should be conducted through channels that are not part of the organization's systems; assume that adversaries have control over everything and can read communication channels such as email.

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

+1 What should we have prepared and always ready to 'grab and go'?

jump bag

Submit

+1 True or False: Using baselines, we can discover deviations from the golden image, which aids us in discovering suspicious or unwanted changes to the configuration.

True

Submit