v2

Threat Hunting Professional

Introduction to Threat Hunting

Section 01 | Module 01

Table of Contents

MODULE 01 | INTRODUCTION TO THREAT HUNTING

Learning Objectives

By the end of this module, you should have a better understanding of:

- ✓ What Threat Hunting is and why it is important
- ✓ Threat Hunting's association with other practices
- ✓ Different Threat Hunting teams

1.1

Introduction

1.1 Introduction

Even though businesses continuously put a lot of money into cybersecurity, the losses caused by cybercrime are significantly increasing.

For example, according to a recent IC3 report, business email compromise scams alone have led to losses of over $26 billion in the past three years.

https://www.ic3.gov/media/2019/190910.aspx

1.1 Introduction

Why is that happening, or how is it possible, you may ask?

Cybercriminals are constantly evolving and becoming better at bypassing traditional defenses. While they help, they don't completely prevent a skilled intruder from entering your network. Automated detection tools alone are not enough to detect advanced, stealthy attacks.

1.1 Introduction

Based on FireEye's M-Trends 2019 Report, the average time for an organization to discover that they have been breached (also known as dwell time), for the investigations Fireeye were part of, was 78 days; this means that an intruder could be in your network for nearly three months before you know about it.

1.1 Introduction

While there is a significant decrease compared to 2011, 78 days is still a long time.

The report specifically outlines external notification as a means to identify a compromise, with a dwell time of 184 days in 2018.

1.1 Introduction

The dwell time demonstrates that the traditional approach to defend the network is no longer adequate.

It’s time to go hunting!

1.1 Introduction

Threat hunting is the human-centric process of proactively searching data and discovering cyber threats.

It is a drastic change from the traditional reactive approach of waiting for an internal system, such as an IDS, or law enforcement, to notify them that they have been breached. The hunter detects threats that nothing else detected.

1.1 Introduction

Threat hunting aims to reduce the dwell time by identifying threats in a very early stage of the infection.

By doing so, it may be possible to prevent attackers from gaining a stronger foothold in the environment and remove them from the network.

1.1 Introduction

The hunting process begins by identifying potentially targeted systems or data and categorizing which behavioral techniques the attackers may use. The hunter attempts to locate and confirm abnormal activity.

Threat Intelligence is often utilized during the hunt to develop techniques and carry out necessary actions to protect systems from compromise.

1.1 Introduction

Hunting:

- Is an offensive-based strategy
- Requires the hunter to think like an attacker
- Requires strong practical understanding of cyber threats and the cyber-kill chain
- Requires you to know your environment
- Is easier with quality data and resources

Incident Response

1.2.1 Incident Response Process

Even though this course does not go deep into incident response, we felt it is necessary to mention what incident response (IR) is and its association with threat hunting (TH).

NOTE: From this point on, you might see the abbreviations IR and TH.

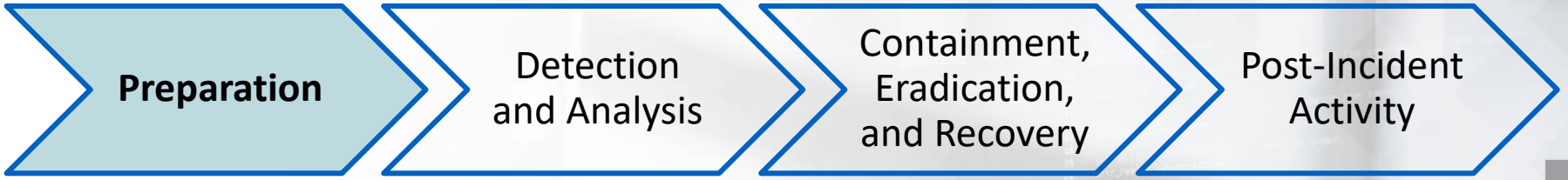
1.2.1 Incident Response Process

According to the *Computer Security Incident Handling Guide, Special Publication 800-61 Revision 2*, created by NIST (National Institute of Standards and Technology), the IR process is defined in 4 steps.

Let's briefly go over each phase of the incident response process defined by NIST.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

1.2.1 Incident Response Process



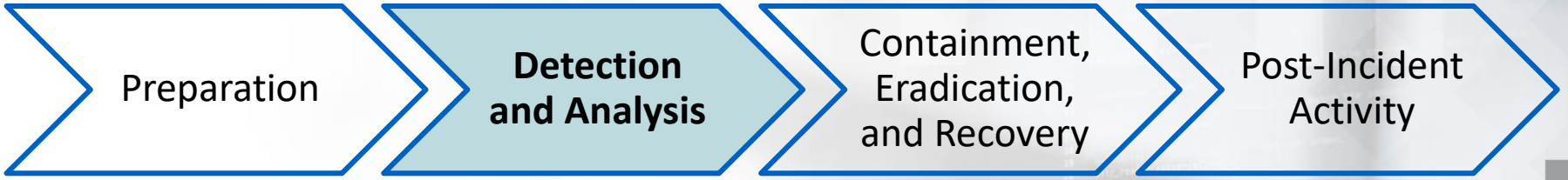
The **Preparation** phase involves preparing your organization to handle incidents and involves:

- Outlining everyone's responsibilities, hardware, tools, documentation, etc.
- Taking steps to reduce the probability of an **incident** from ever occurring

1.2.1 Incident Response Process

According to NIST, an **incident**, or a ***computer security incident***, is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

1.2.1 Incident Response Process



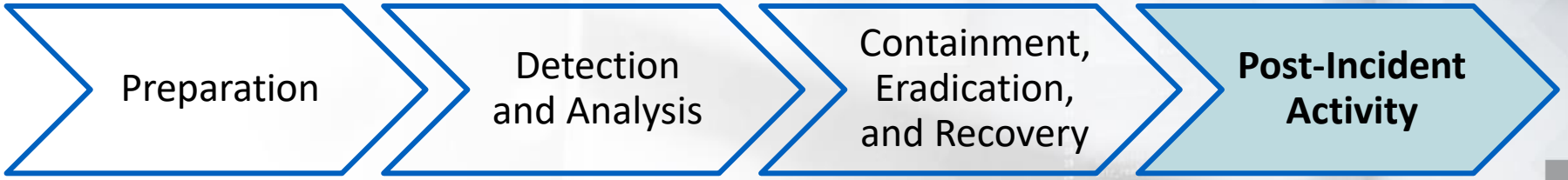
In the **Detection and Analysis** phase, the IR team would confirm if a breach took place.

They would analyze all the symptoms which were reported and confirm if the situation would be classified as an incident.

1.2.1 Incident Response Process

The **Containment, Eradication, and Recovery** phase is where the IR team would gather intel and create signatures that will aid them in identifying each compromised system. With this information, countermeasures can be put in place to neutralize the attacker and attempt to restore systems/data back to normal.

1.2.1 Incident Response Process



The **Post-Incident Activity** phase is a “lessons learned” phase.

In this phase, the goal is to improve the overall security posture of the organization and to assure that a similar incident will not happen again.

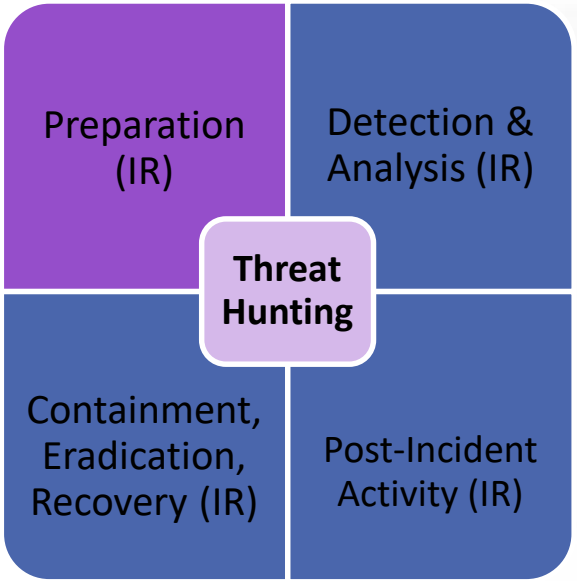
1.2.1 Incident Response Process

Now that you know what IR is, have you realized how it is connected to threat hunting?

Let's review the brief descriptions for each phase to see the connection.

1.2.2 Incident Response & Hunting

How does threat hunting correlate to the Preparation phase of IR?



A threat hunter or team can't operate without rules of engagement.

They need predefined terms on how to operate, when to operate, what to do in a particular situation, etc.

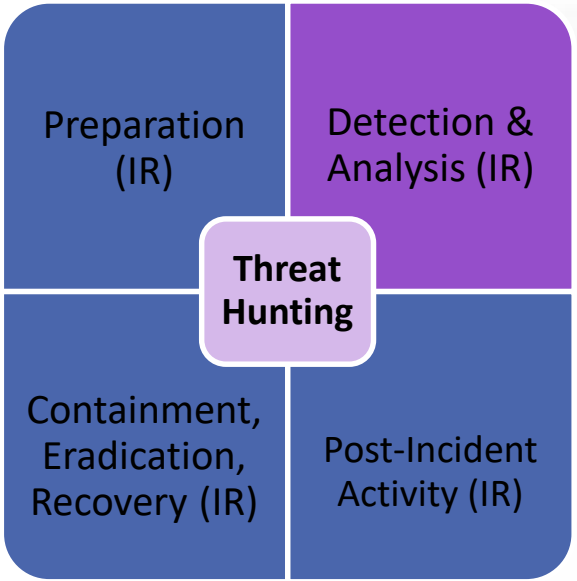
1.2.2 Incident Response & Hunting

Organizations might include threat hunting in their IR documents or simply update existing ones to cover it, as they do not necessarily have to create separate threat hunting documents.

Note: By documents, we are referring to policies and procedures.

1.2.2 Incident Response & Hunting

How does threat hunting correlate to the Detection & Analysis phase of IR?

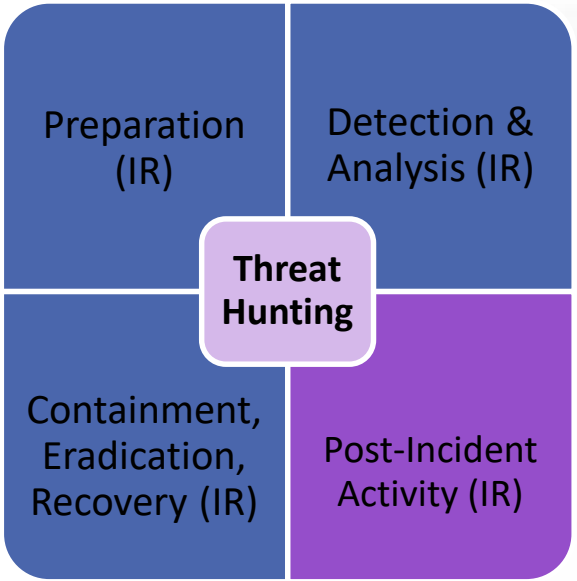


A hunter is useful in this phase because he/she will be able to assist in the investigation, to determine whether the indicators presented point to an incident or not.

The hunter can also assist in obtaining further artifacts that might have been overlooked because the hunter is able to think like an attacker.

1.2.2 Incident Response & Hunting

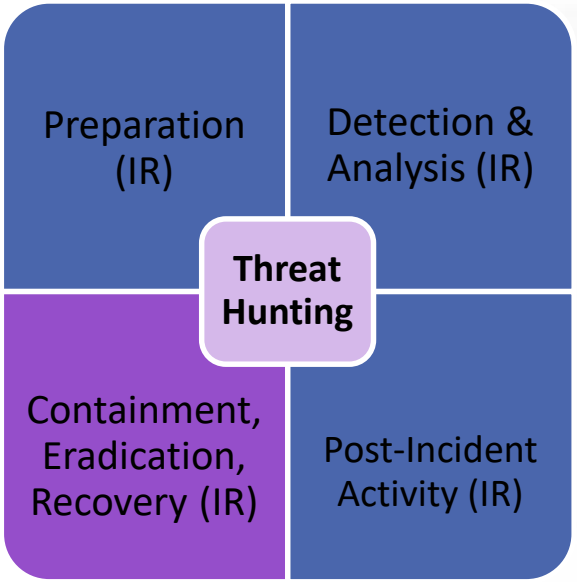
How does threat hunting correlate to the Post-Incident Activity phase of IR?



In certain corporations, a hunter might already be expected to conduct the tasks covered in the Containment, Eradication, and Recovery phase, but it is not mandatory. The hunter can pass this task to another member of the IR team; this will be defined in the documentation outlining the policies and procedures for the hunter or hunting team.

1.2.2 Incident Response & Hunting

How does threat hunting correlate to the Containment, Eradication, and Recovery phase of IR?



Hunters have a vast knowledge of various IT domains and IT Security, which allows them to assist in this phase of IR. They can provide recommendations and insight on how the organization can improve its overall security posture. That recommendation can either be a quick implementation or a future implementation.

1.2.2 Incident Response & Hunting

These slides were meant to cover the correlation between incident response and threat hunting. We are not saying that they need to be intermixed, nor are we saying they shouldn't be. Ultimately, it will be up to the organization as to how they will implement threat hunting.

In the next few slides, we'll look at risk assessments and how they correlates to threat hunting.

Risk Assessments

1.3 Risk Assessments

What is a risk assessment? A risk assessment is the process of assessing threats, vulnerabilities, and their likelihood of occurring to the organization's assets.

A risk assessment report will list all the vital systems / processes and the impact to the organization, if anything would happen to these systems.

1.3 Risk Assessments

This report provides the hunter with an idea as to what systems/processes an intruder would most likely go after. Remember, to be a successful hunter, you must think like the attacker.

What would he/she go after if they were infiltrating your network?

1.3 Risk Assessments

With a risk assessment report, a hunter can determine where his/her focus should be; this means that no vital systems would be overlooked, because resources will not be wasted focusing on a less vital system or process.

There are other documents that might assist the hunter in determining which systems/processes require more focus than others. Those documents would be a threat assessment report or a business impact analysis report.

1.3 Risk Assessments

In large corporations, it is not the job of the hunter to conduct the risk assessments. In smaller organizations, the hunter may not be a dedicated threat hunter, and he/she may be responsible for multiple roles within the IT Security team. This means that the hunter might be part of a team, and because of other responsibilities, he/she might only be able to hunt one time a week or even one time a month. On the other days of the week, he/she may conduct different tasks on the IT Security team.

1.4

Threat Hunting Teams

1.4 Threat Hunting Teams

There is no general definition or description of what a hunting team should be composed of, as organizations determine this based on their size, industry, and hunger to hunt.

The three most commonly encountered types are:

- Ad-hoc hunter
- Analyst and hunter
- Dedicated hunting team

1.4.1 Ad-hoc Hunter

The Ad-hoc hunter is usually responsible for multiple roles in the organization, and therefore the hunts occur less frequently. The hunts are more task-oriented, which requires a clear plan of what to hunt for on a given hunting trip.

This type of hunter is primarily found in organizations with no formal security team.

1.4.2 Analyst and Hunter

This type of hunter is the most common, in which SOC analysts also have the responsibility to perform hunting. These skills are complementary; after all, a good hunter is a great analyst.

This type of hunter is often found in small organizations or those with extremely well-developed detection and baseline capabilities.

1.4.3 Dedicated Hunting Team

This type of hunter is the most specialized one – a team of a few members whose sole purpose is to hunt. The members are well experienced and qualified.

This type of hunter is often found in a large organization or governmental organizations.

References

References

Business email compromise - the $26 billion scam

https://www.ic3.gov/media/2019/190910.aspx

Annual M-Trends Report

https://content.fireeye.com/m-trends

NIST Guide

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf