



# Threat Hunting

## INTRODUCTION TO THREAT HUNTING

### Module 1



## 1.1 Introduction

## 1.2 Incident Response

## 1.3 Risk Assessments



# INTRODUCTION

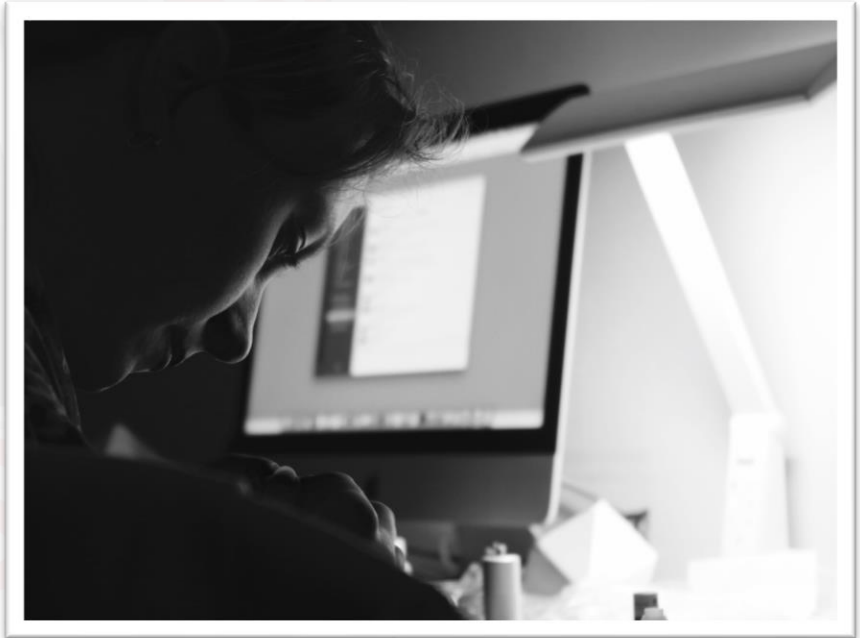
eLearnSecurity  
Forging security professionals



So you want to be a threat hunter.

You have chosen wisely.

**Threat Hunting** is one of the latest buzzwords circling throughout the industry and it has quickly become one of the hottest fields in cybersecurity.





# 1.1.1 Introduction



**VB** NEWS ▾ EVENTS ▾

How does your company respond to perceived threat?

What's stopping financial services firms from embracing digital evolution?

**DARKReading** | Join us live at **black hat** **Interop ITX**

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News

**ANALYTICS** **ATTACKS / BREACHES** **APP SEC** **CAREERS & PEOPLE** **CLOUD** **ENDPOINT** **IoT** **MOBILE** **OPERATIONS**

**VULNERABILITIES / THREATS**

2/9/2017 03:00 PM

## Threat Hunting Becoming Top Of Mind Issue For SOCs

BROUGHT TO YOU BY **IBM**

**SecurityIntelligence**  
Analysis and Insight for Information Security Professionals

Home > News >

**NEWS** February 13, 2017 @ 12:00 PM

## Threat Hunting Is a Top Security Priority for 2017

By Mark Samuels

**SECURITY** **GUEST**

## As hackers become syndicates, it's time to go threat hunting

BEN JOHNSON, CARBON BLACK MAY 8, 2016 7:15 AM

## 1.1.1 Introduction

Based on a recent poll conducted earlier this year by the Information Security Community on LinkedIn, threat hunting already is, or should be, a top-level initiative.

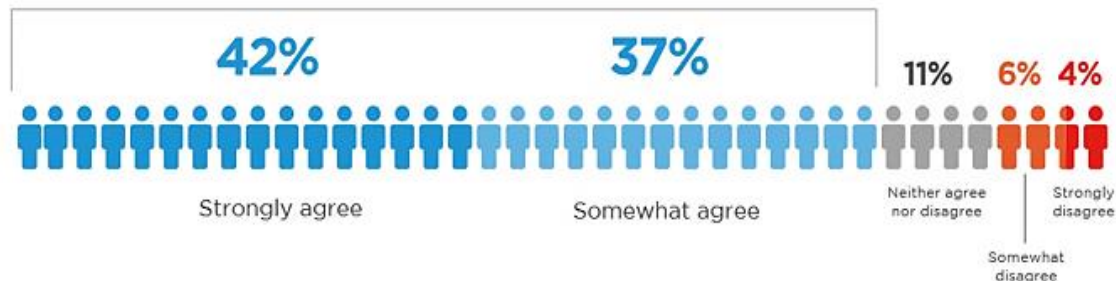
### THREAT HUNTING PRIORITY

Nearly four out of five respondents said that threat hunting should be or will be a top security initiative in 2017 with 42% saying that they strongly agreed with the statement. Over three-quarters of respondents believe threat hunting is of **major importance**.

Q: What is your level of agreement with the statement "Threat hunting should be or will be a top security initiative in 2017"?

**3/4 of respondents**

believe threat hunting is of major importance





---

The same poll asked the 330 participants the following question:

**What keeps you up at night?**

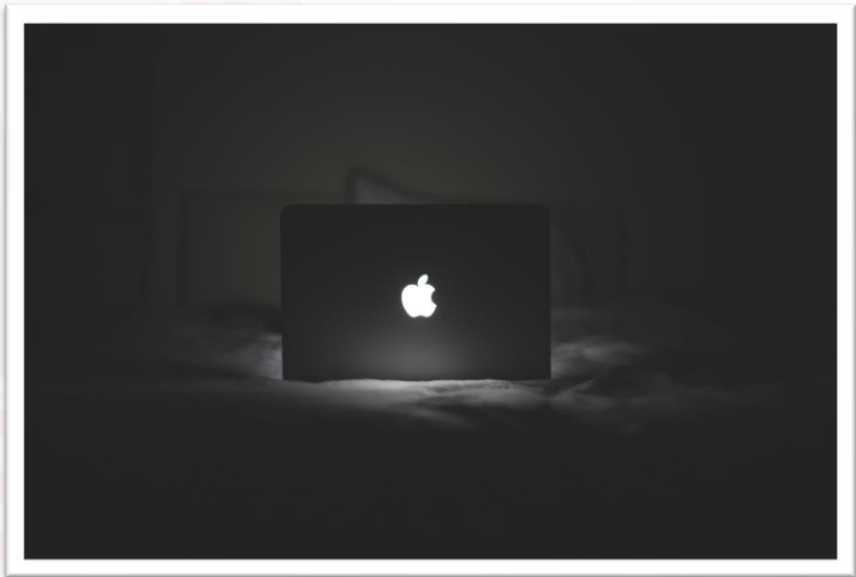
---

**ANSWER:** The thought of unknown, or undetected, threats slipping pass an organization's defenses.



Why would “unknown threats” still keep them up at night?

(Even considering their organization has spent tens, or even hundreds, of thousands of dollars on equipment to help keep their network safe and thwart any intruder.)



LearnS  
Forging security professionals





The answer is because the traditional approach to securing the network helps, but doesn't completely stop a skilled intruder from entering your network.

With all the security measures in place, we are still hearing about companies (of all sizes) being breached at a large scale. That means that small to medium-sized businesses are not exempt.



**Dwell time** is the time from the point of infiltration to the point of detection. This is a term that you'll hear often in incident response, threat hunting, and maybe even threat intelligence.

It is an important word to add to your IT Security vocabulary.

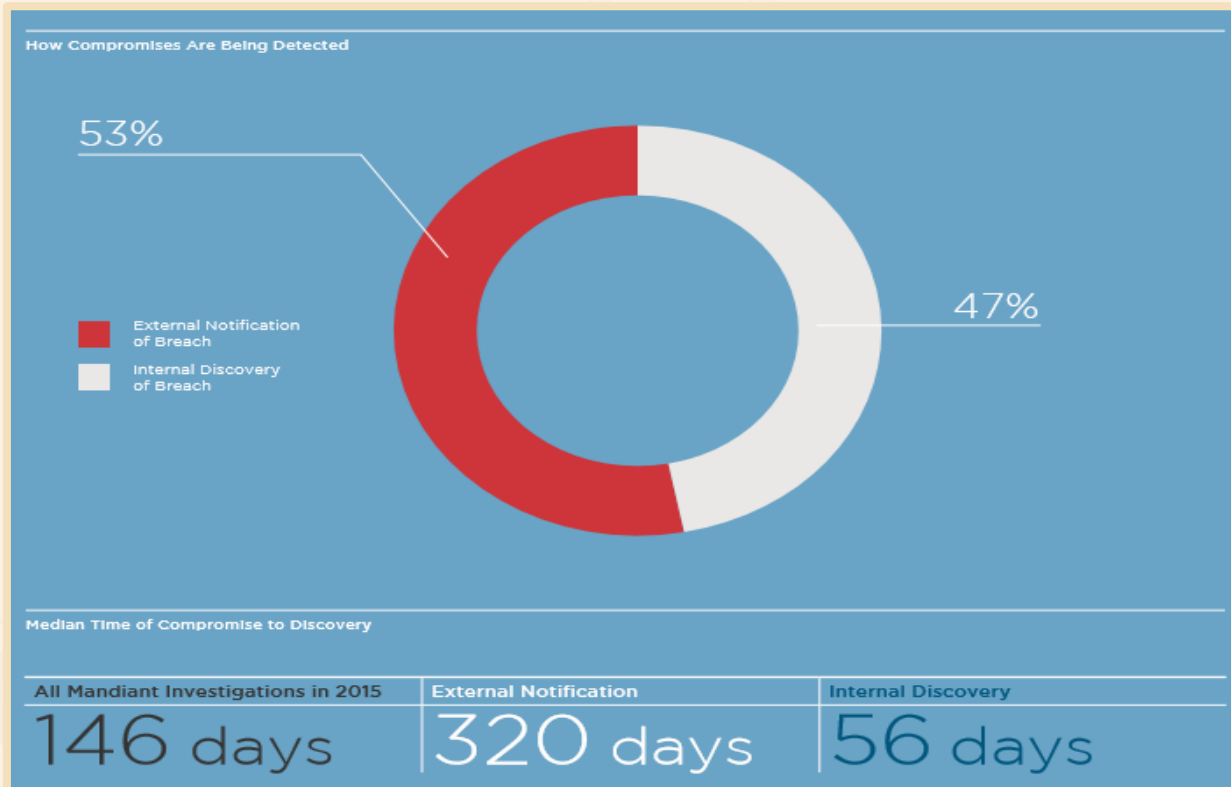


# 1.1.1 Introduction



Based on [Mandiant's M-Trends 2016 Report](#), the average **dwell time** for the investigations they were part of, was nearly 6 months. Meaning an intruder could be in your network for nearly half a year before you know about it.

External notification (the public) is listed as much as **320 days**!





Going back to Mandiant's M-Trends Report, it's obvious that the traditional approach to defend a network is no longer adequate. So what can we do differently?

That is where **threat hunting** comes in.



Individuals often think that threat hunting simply involves sifting through system logs hoping that something will “jump out” at them.

Yes, analyzing system logs is one aspect or level of threat hunting, but only if the hunter knows what he/she is looking for. Fortunately, there is more involved in threat hunting.



---

**Threat Hunting** is when the defenders, or the blue team, takes a proactive defensive posture. They are not waiting for an internal system, such as an IDS, or from law enforcement, to notify them that they have been breached.

---

They are actively searching the network for any indication of a threat or breach, whether known or unknown.




The hunt is an offensive-based strategy.



A threat hunter needs to think like an attacker.



They will need to have an attacker's mindset in order to be an effective hunter.



Forging security professionals



The threat hunter will need to understand:

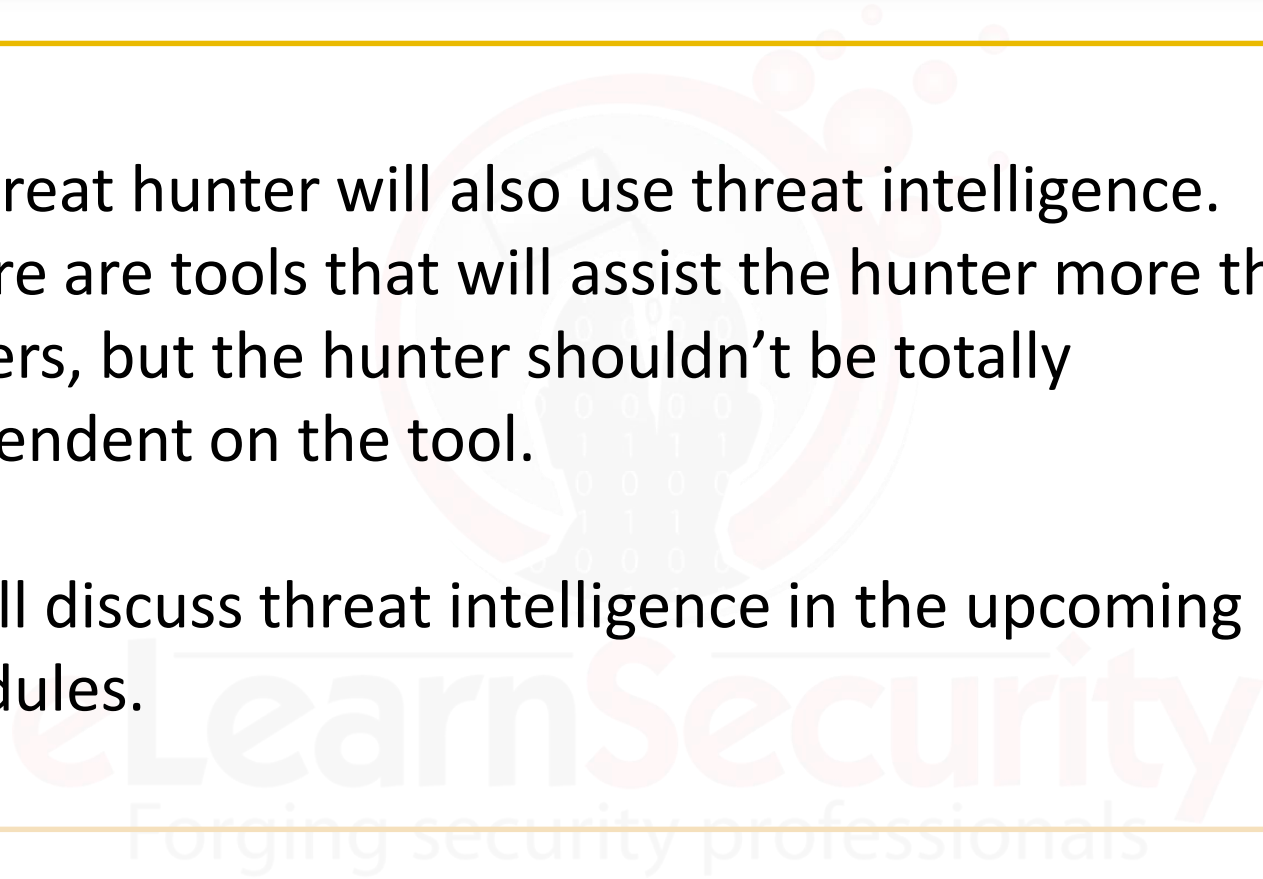
- All points within the **Cyber Kill Chain**, which we'll see in a later module.
- What tools/techniques will be used at a particular point in the kill chain and how to prevent successful progression up the chain.





A threat hunter will also use threat intelligence. There are tools that will assist the hunter more than others, but the hunter shouldn't be totally dependent on the tool.

We'll discuss threat intelligence in the upcoming modules.





The objective of the threat hunter is to:

Detect the intruder

Prevent them from  
gaining a stronger  
foothold within the  
network

Eventually remove  
them from the  
network.

In summary, the goal is to prevent the intruder from achieving it's objective or mission, and ultimately reduce both detection time and response time.



# INCIDENT RESPONSE

eLearnSecurity  
Forging security professionals



Even though this course will 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 IR and TH as abbreviations



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.



Caendra Inc  
Forging security professionals



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





## 1.2.1 Incident Response Process



The **Preparation** phase involves preparing your organization to handle incidents.

This step involves outlining everyone's responsibilities, hardware, tools, documentation, etc.

This phase also involves taking steps to reduce the probability of an **incident** from ever occurring.



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.

Forging security professionals



## 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 whether or not 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 & 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 more like 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 won't happen again.

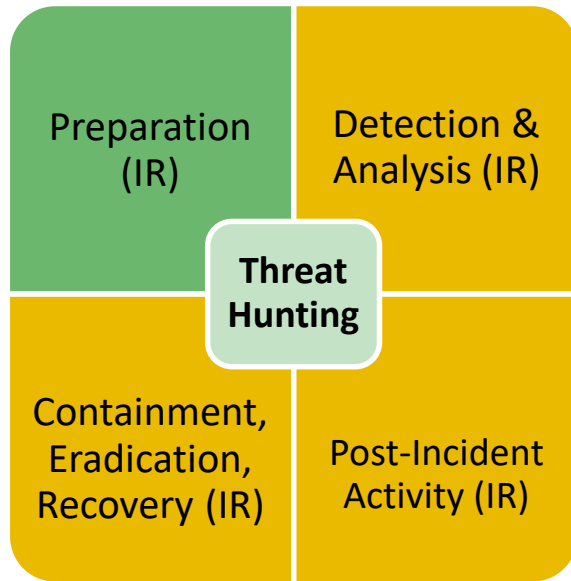


Now that you know what IR is, have you made the connection as to how it is connected to threat hunting?

Don't worry, by reviewing the brief descriptions for each phase, you can see the connection.



### 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.



Organizations might include threat hunting in their IR documents or simply update existing documents to include it.

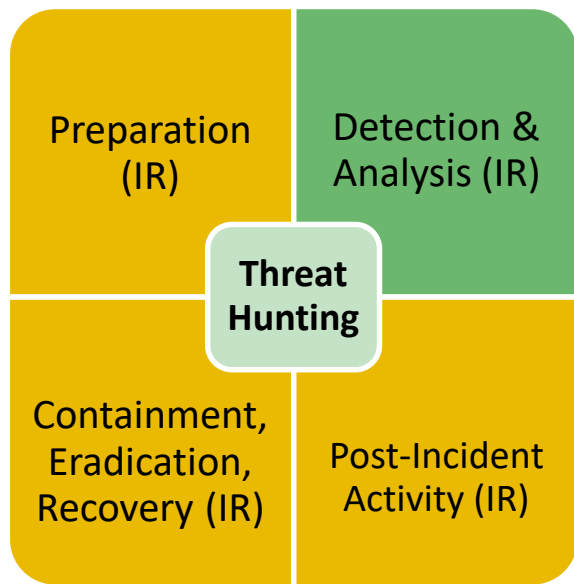
They don't necessarily have to create separate threat hunting documents.

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

LearnSecurity  
Forging security professionals



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

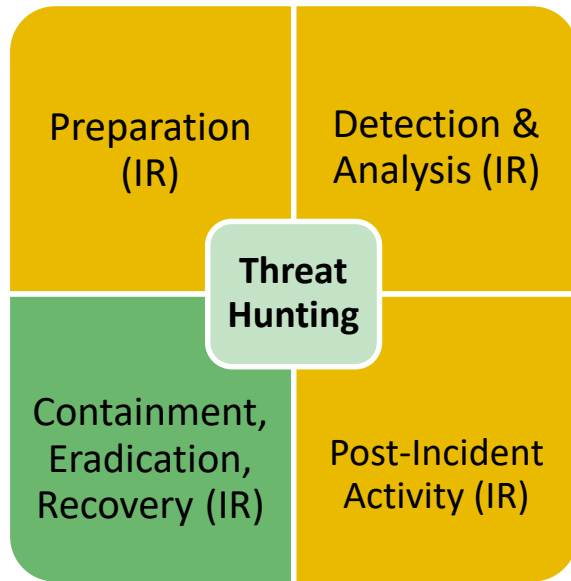


A hunter is useful in this phase because he/she will be able to assist in the investigation, to determine whether or not the indicators presented, in fact, point to an incident or not.

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



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



In certain corporations, a hunter might already be expected on conducting the tasks covered in the Containment, Eradication, & Recovery phase, but it's not mandatory.

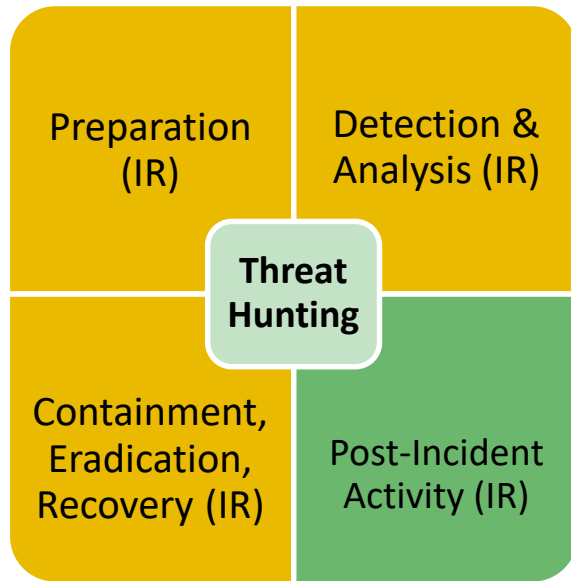
The hunter can pass this task to another member of the IR team.

This will be defined in the documentation outlining the policies and procedures for the hunter or hunting team.





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



Hunters have 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 their overall security posture.

That recommendation can either be a quick implementation or a future implementation.



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.

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 it correlates to threat hunting.





## 1.3 Risk Assessments



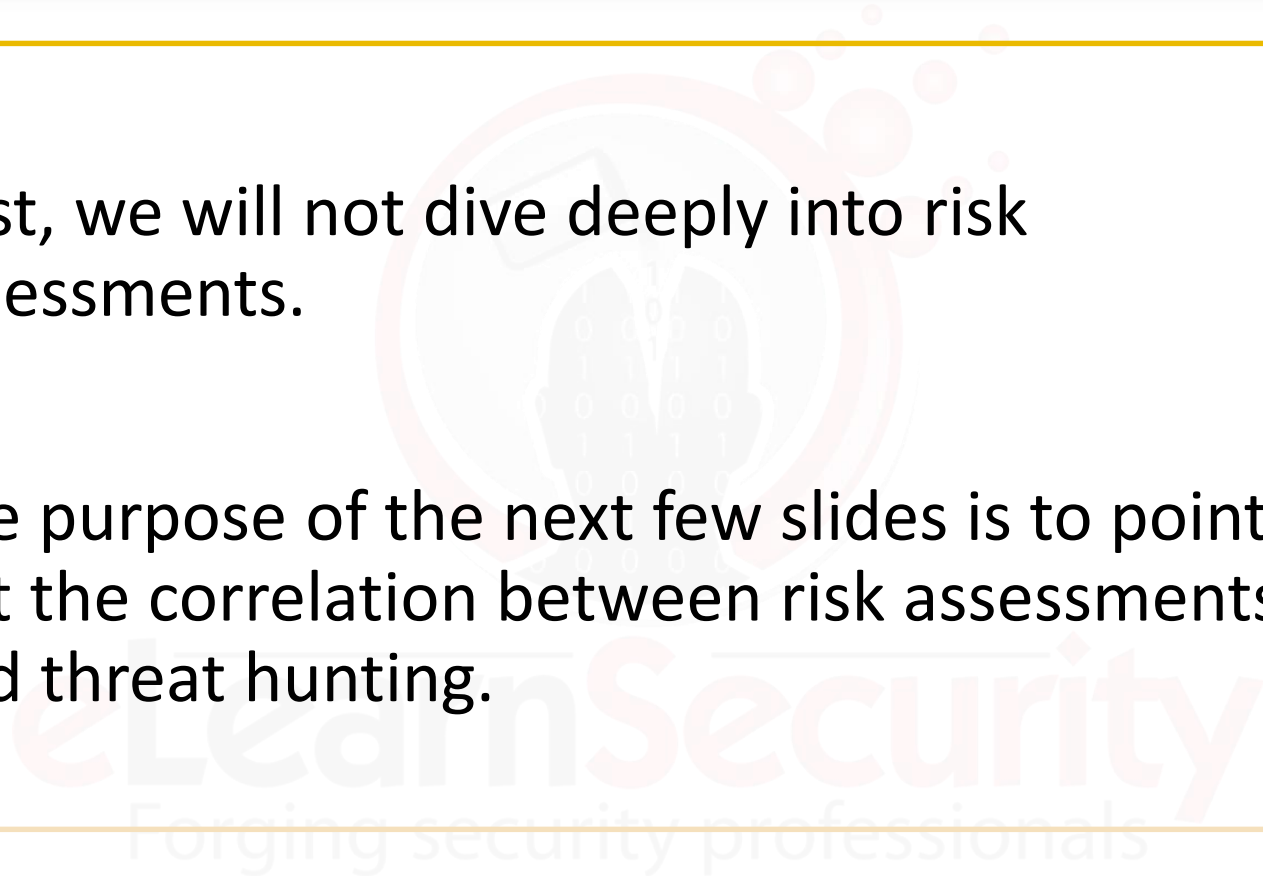
# RISK ASSESSMENTS

eLearnSecurity  
Forging security professionals



First, we will not dive deeply into risk assessments.

The purpose of the next few slides is to point out the correlation between risk assessments and threat hunting.





We'll start off with:

What is a risk assessment?

- In a risk assessment, an organization assesses any threats and vulnerabilities to their assets.
- This report will list all the vital systems/processes and the impact, to the organization, if anything would happen to these systems.



With this report, it will give the hunter an idea as to what systems/processes an intruder would most likely go after.

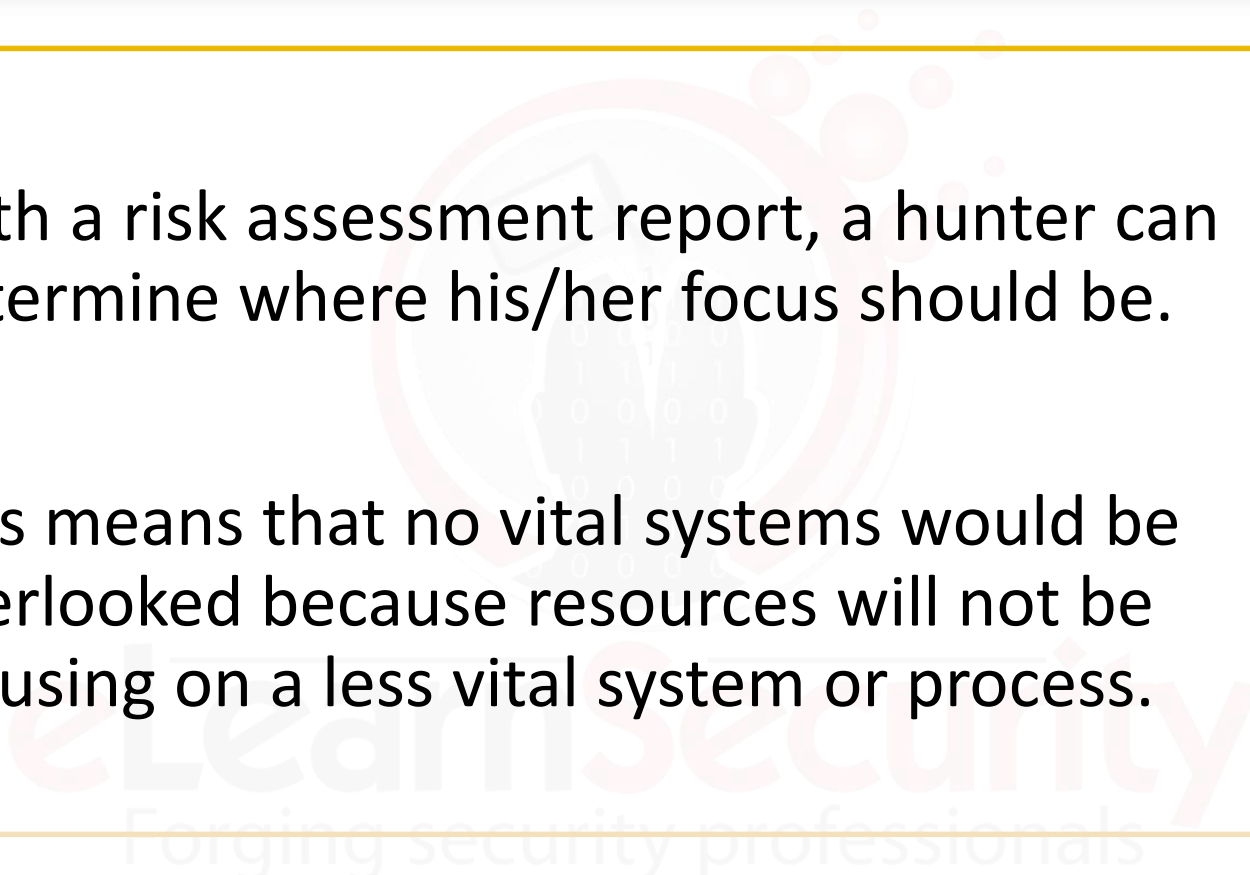
Remember, a key to be a successful hunter is that you have to think like the attacker.

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



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 focusing on a less vital system or process.







There are other documents that might assist the hunter, in determining which systems/processes requires more focus than others.

Those documents would be a threat assessment report or a business impact analysis report.

Threat Hunting - © Caendra Inc 2017 - All Rights Reserved



In large corporations, it is not the job of the hunter to conduct the risk assessments.

But 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 1x a week or even 1x a month.

On the other days of the week he/she may conduct different tasks on the IT Security team.



This concludes this module, Introduction to Threat Hunting.

We have covered:

- ☒ What is threat hunting?
- ☒ Why it's important?
- ☒ What is its association with incident response and risk assessments.



# REFERENCES

eLearnSecurity  
Forging security professionals



[Venture Beat](#)



[Dark Reading](#)



[Security Intelligence](#)



[NIST Guide](#)



[Annual M-Trends Report](#)

eLearnSecurity  
Forging security professionals