The Rise of Proactive Threat Hunting

Kiauna Newman

2019

Kiauna J. Newman

Advance Ethical Hacking

05 May 2019

The purpose of this paper is to educate companies on what proactive hunting is and what it is not. It will also detail the benefits of adopting a proactive hunting operation. In addition a list of solutions will be explained and a list of companies who can provide those solutions. In conclusion of reading this paper, organizations will be better informed on what security approach they want to take in reference to proactive hunting.

Introduction

Consider the question; what is the difference between a company that gets attack by hackers and companies who do not get hacked? An answer in the simplest form is Proactive actions in comparison to reactive actions identifies the difference between both companies. Most companies take action to incidents and alerts once they are already formed and start the process of resolving the data breach or attacks against their systems. This may resolve the problem, but in reality the situation could have been prevented before the incident occurred. This could be done by ensuring they are prepared for certain breaches or attacks through knowledge and awareness of threat hunting. Threat hunting is defined as “the process of proactively searching and discovering cyber threats — regardless of whether they pose as yet unexploited network vulnerabilities or have already bypassed defense solutions.” (*The Anatomy of Threat Hunting: What You Need to Know and Why*)

It is also a hybrid of forensic investigation, malware, and incident response. It is a category that became popular in the last few years. As black hat hackers become more advanced in their attacks, the more there will be the need for a special group of freedom fighters or elite white hat hackers as one article called them. These elite white hat hackers are also called threat hunters. (Grimes)

There also has been some confusion on whether threat hunting was similar to incident response. *Searchsecurity.techtarget.com* defines incident response as, “an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident or security incident.” (*What is incident response? - Definition from WhatIs.com*) “

Differences between Incident response and threat hunting.

* Incident response focuses on containment and recovery in the aftermath of a cyber incident, while threat hunting aims to catch threats before they hit. (Bolzoni)
* CSIRTs follow procedures and employ tools to detect and contain a threat. Threat hunting is centered around analysts, aided by tools, to proactively look for indicators of compromise. (Bolzoni)
* Incident response is all about the now and seeks to mitigate a detected threat. Threat hunting may require analyzing historical information to identify early indicators of potential threats. (Bolzoni)
* Incident response occurs after the discovery an intrusion, effective threat hunting informs an organization's need for additional security before an event occurs. (Bolzoni)

Threat hunting Process

The process of threat hunting can be done in a variety of different ways. Some vital steps associated with the threat hunting process begin with the gathering of information, the process of the hypothesis being formed, the scope creation, and finally the threat hunt being executed. (SANS 2018 Threat Hunting Survey Results)

A company can begin the process by gathering of information. This process can be done by using reconnaissance tools, social engineering and open source software to complete an detailed observation of the intended target. The objective is to think like a black hat hacker who is oblivious to information on the company or the individual that they are going after.

The next step of the process is forming the hypothesis as it relates to threat hunting. This is done by analyzing the results from the information gathering process and formulating a question of what if. The what if question is formulated from the scenario of; ‘what if a hacker gets access into the company based of an identified vulnerability?”

The third process of creating a scope, is done by defining how long the test will take and what results the threat hunter is seeking. This process can take weeks and sometimes months depending on the complexity of the company’s system.

The final step of the process is executing the hunt which is done by two things vulnerability assessment and exploitation. Vulnerability assessment is accomplished through the initiation of scanning. Exploitation is accomplished by looking at the company’s system from an outsider’s point of view and identifying ways to attack and the system. This will give the company an idea on how to handle such threats should they occur in the future.

Recommendation for companies considering Threat Hunting operation.

Companies considering threat hunting need to do three things:

First: The company needs to search for individuals with the skills and knowledge needed to be a threat hunter. This process needs to be done with high regards to the future of the company’s security in mind.

Second: Implement a threat hunting methodology and stick with that method. As Mentioned earlier the threat hunting process can be done in a variety of different ways. If the company instills a concrete system in place the threat hunting process should run smoothly.

Third: The Company needs to establish a strong threat hunting team or consult and hire a company that specializes in threat hunting. Below are a list of companies who provide threat hunting. There is also a summary of each company’s strategy.

Companies who provide threat hunting:

Sqrrl threat-hunting: allows organizations to target, hunt, disrupt and investigate advanced cyberthreats. The Sqrrl solution detects adversaries’ behavior through the use of machine learning, peer-group analysis and behavioral baselining. In addition, it identifies threat actor tactics, techniques and procedures (TTP). (Imam)

IBM i2 Enterprise Analysis: provides threat hunters and analysts with a set of specific tools to detect, disrupt and defeat advanced threats. It is designed to gain actionable intelligence, unearth hidden connections with visual displays, and accelerate data to the point of decision.’ (Imam)

Cb Response: is built specifically for organizations’ security operation centers (SOCs) and incident response (IR) teams. Unlike other solutions, this platform performs unfiltered data gathering and captures more information about endpoint events. (Imam)

Endgame is a threat-hunting solution that eliminates the protection gap by preventing sophisticated attacks at earliest stages of the threat chain. It is one of the oldest threat-hunting tools on the market, and the experience of the company is shown in the power of the tools they offer. (Imam)

Works Cited

Bolzoni, Damiano. “Successful Threat Hunting in ICS Networks.” *Successful Threat Hunting in ICS Networks*, www.secmatters.com/blog/successful-threat-hunting-in-ics-networks.

Grimes, Roger A. “Who Wants to Go Threat Hunting?” *CSO Online*, CSO, 8 May 2018, www.csoonline.com/article/3269779/who-wants-to-go-threat-hunting.html.

Imam, Fakhar. “Threat Hunting Solutions.” *Infosec Resources*, resources.infosecinstitute.com/category/enterprise/threat-hunting/threat-hunting-solutions/#gref.

“SANS 2018 Threat Hunting Survey Results.” *Infosecurity Magazine*, 1 Nov. 2018, www.infosecurity-magazine.com/white-papers/2018-threat-hunting-survey-results/.

“The Anatomy of Threat Hunting: What You Need to Know and Why.” *Threatpost English Global Threatpostcom*, threatpost.com/the-anatomy-of-threat-hunting-what-you-need-to-know-and-why/143663/.

“What Is Incident Response? - Definition from WhatIs.com.” *SearchSecurity*, searchsecurity.techtarget.com/definition/incident-response.