Threat Hunting for Cybersecurity Defense

Using threat hunting as part of a cybersecurity defense plan can help you identify attackers, their tactics, and their goals which allows for continuous improvement of security. It can also help you understand the trends in your security environment. This article will outline how to conduct threat hunting, how to identify threats, and how to defend against possible threats.

What is Threat Hunting

Threat hunting is actively seeking indicators of potential cyber incidents that could adversely affect your company. A threat hunt could take many different turns and result in days of hunting following many different paths. Threat hunting is never a singular process, you need to be continuously hunting for a variety of threats and trying to predict potential cyber threats to your business.

Identifying & Defending Against Threats

The Internet has evolved dramatically. As a result, it has become a critical communications infrastructure. It is also a target of advanced adversaries, who continually develop and use malicious techniques. Therefore, threat hunters must be aware of and stay on top of quickly changing software and infrastructure. You are only able to defend against a threat if you’re able to identify them. Being able to identify threats requires you to have adequate threat intelligence, in-depth knowledge of your network, ongoing security testing, and proper procedures and technology in place. With these defenses

in place you gain knowledge that allows you to determine which activity is potentially malicious and which activity is normal. Only with this in place are you able to identify and defend against threats.

Potential Indicators of a threat include:

- Spear Phishing
- Multiple Failed log-in attempts
- Somebody downloading massive amounts of company files
- Program or user attempting to gain access to unauthorized areas

Conducting a Threat Hunt

Conducting a threat hunt is not an easy 3 step process as it takes a lot of preparation learning and observing before the threat hunt process can even begin. Identifying and collecting information about an attacker's tactics, methods, and goals are critical to cybersecurity defense. If you don't have some background knowledge of how cyber criminals work, it's incredibly difficult to predict their next move. Also, information gathered at this stage can be used to gather details about an organization, such as who has access to specific information and how that information is being used. After obtaining background knowledge then you're ready to begin the first step in threat hunting.

1. The first step in threat hunting is knowing what you're looking for. For example, you want to make sure there is no unauthorized access within your network. You can then use threat intelligence and your own prior knowledge to hypothesize how a cyber criminal may achieve gaining access to your network.

2. After hypothesizing, you then need to gather as much

information as you can. Information is collected in various ways, including social media, public information services, and emails. The information you gather helps you make decisions on combating future attacks or it can help you prevent attacks altogether. There are two main types of information gathered: the information a criminal requires to commit a crime and the information an attacker needs to take control of a target system. It’s important to know how a criminal may hack into your computer system so that you can test and prevent that method before it happens. For example, an attacker may perform a port scan to discover if a system is available and configured for telnet. By knowing this information, you can then conduct your own port scan to look for vulnerabilities before a cyber criminal does.

3. After gathering information about the different methods of attacks or current vulnerabilities within different systems the next step would be to hunt for evidence of the threat within your company.

4. After conducting searching and conducting tests within your own system, if you find any vulnerabilities you’ll want to immediately remediate them.

5. Lastly, and an equally important step as the rest is to record any findings. Write down what the threat was, how you found it, and what steps you took to prevent it.

Example of a Threat Hunt:

1. You gather cyber intelligence based on media reports, cyber crime groups, and breached data. Based on the information you determined that an account takeover is the biggest threat to your company.
2. You now need to list all of the accounts you have and begin reviewing

the account activity looking for indicators of potential compromise, such as login attempts. You find multiple failed login attempts from the same IP Address to one of your accounts.

3. Now, you check the account is secure by reviewing the accounts security measures such as updating the password or enabling 2FA (2-Factor Authentication) and insuring maximum security measures are in place.
4. After securing the account, you can use the data you gathered from the IP Address to reinforce other aspects of your cyber security such as blocking the IP Address from accessing your company's online assets.
5. Lastly, you make a record of this threat hunt because it showed indicators of a threat.

Making threat hunting a priority is imperative to your company's cybersecurity defense plan. Knowing what threats may arise and how your company is equipped to handle them could be the difference between whether your company succeeds or not. With adequate threat intelligence knowledge and constant monitoring you will be able to identify any threat that your network(s) or device(s) are susceptible to and be able to combat those threats before they are an issue. Also, keeping all software updated protects you from many known vulnerabilities.