PRESENTS

THE PRACTICAL THREAT HUNTING SERIES

The Practical Threat Hunting Series is a series of publications followed by review discussions

WHAT YOU SHOULD EXPECT

Monthly Publications for the next 8 months

+

Quarterly Review Discussions

PRESENTED BY

MAOR AKNIN

CHAPTER-0: PREFACE

ABSTRACT

To try helping, or even solving, one of the most challenging cyber-security situations, which I call “The Vicious Cycle of Cyber”, I decided to write this series of publications about Proactive Threat Hunting. Hopefully, this series will be used as a guide for cyber-security professionals and companies who wish to break the Vicious Cycle of Cyber, build advanced and scalable threat hunting capabilities, and take an extra step into safer environments.

The Internet is full of tutorials, guides, examples, and tools to assist in threat hunting. I am profoundly grateful for all of them! This series of publications couldn't have been written without said materials, contributions, and the contributors and colleagues that are chasing the sun, in order to develop the threat hunting community.

WHAT IS TO COME

After dealing with hundreds of high-profile cyber incidents on both national and commercial scales, building many threat hunting organizations within the most complex enterprises, and offensively testing countless systems and environments, I developed a unique process of developing threat hunting capabilities. Every month I will publish a new chapter that will be focused on a different scope and aspect of how to build scalable threat hunting capabilities and break the Vicious Cycle of Cyber.

This series is all about being **Practical** and **Proactive**. I will explain the methods, frameworks, and methodologies required for launching successful threat hunting operations. However, the main focus of this series is to instill the necessary capabilities, help to hone the skills and techniques, and to share some of the tools for launching practical and proactive operations.

From my experience and previous projects, launched within large-scale organizations, I concluded that threat hunting is the process of proactively searching for unknown adversaries on a system or network, whether it’s on-premises, in the cloud, or hybrid environments. Accordingly, this is what this series is all about, and this is its core context.

Within this series I will try to provide all the answers regarding threat hunting operations, including the Who, What, Where, When, Why, and obviously, How, practically.

Before I go any further, I want to be crystal clear about one thing: this series is a guide. It is not intended to be a tutorial or a technical manual. I want to avoid any misunderstandings and unnecessary disappointments. If you wish to learn and get the guidance that is needed for building successful and scalable threat hunting capabilities, I am welcoming you to follow this series and the next chapters.

Let’s get a deeper look at what is to come within the next chapters, and what answers I aim to provide:

What. There are a lot of definitions for Threat Hunting. Not all of them share the same definition, nor should they be treated the same way. The next chapters will cover the broad definition of threat hunting, what a threat hunting operation is, what it is based on, and the different types and approaches of threat hunting operations.

Why. The following chapters will give you answers regarding why threat hunting operations need to be executed, the various uses of threat hunting, the benefits of mature threat hunting capabilities, and various threat hunting use-cases.

Who. We do a deep dive into who should take part in threat hunting operations. The operation is commonly executed by analysts and security professionals. However, just like any other field, there are various professionals with varying expertise. This series will also explain the best structure for a threat hunting team, their roles, and responsibilities.

When. In this series, you will find answers to explain how threat hunting operations fit into your business at hand and become an integral part of your security measures. It also explains when you should consider launching specific threat hunting operations and which operations are the most suitable for each mission and task.

How. This series will explain how to plan, build, and execute the development of your threat hunting capabilities. The next chapters will show you how to assess your threat hunting readiness level and how to identify gaps, how to write threat hunting playbooks, and, eventually, how to execute these playbooks that you've created and conduct a threat hunting operation from start to end to reveal unknown adversaries in your environments.

NEXT CHAPTERS OUTLINE

As mentioned above, every month I will publish a new chapter that is focused on a different aspect of the threat hunting capabilities development process. I will try to do my best to keep these chapters as focused and summarized as possible. Here are the next chapters to come:

CHAPTER-1: EAT LUNCH OR BE LUNCH

The first chapter will explain **WHY** you should have threat hunting capabilities in place, what threat hunting is here to solve, and how did we get this situation in the first place. In this chapter, I explain what I used to call "the Vicious Cycle of Cyber". Or in other words – the reason that threat hunting is so needed.

CHAPTER-2: EXAMINE YOURSELF

The second chapter will detail how to perform a threat hunting readiness assessment for your organization, or your situation. You can be the CISO of a public large conglomerate, or a security engineer with one server. In any case, you cannot manage what you don't measure. The same goes for threat hunting capabilities. How would you manage your threat hunting capabilities if you can't measure them and know what your status is? This chapter will show you what and how to assess in order to identify the gaps and measure your status.

CHAPTER-3: BUILD YOUR TEAM

In this chapter, I will explain the key functions and skills needed for your threat hunting team. It can be a one-man show or a 100-person team. Either way, there are some key skills needed in order to perform successful threat hunting operations and develop threat hunting capabilities.

CHAPTER-4: MAP YOUR NETWORK SOURCES

This chapter is about getting to the technical side with how to map the different sources that you will use while executing your threat hunting operations. I will show you the different types of sources, and what to look for in each one of them. I obviously cannot specify every possible source, however, I do provide a decent list of sources, and more importantly, I go through the logic behind these sources, so you will be able to apply and execute it on your particular environments and scenarios.

CHAPTER-5: KNOW YOUR ENEMY

In this chapter your will get to know different terms, such as TTP, Threat Landscape, Adversarial Groups, Hypothesis (in regards to threat hunting), etc. in addition, I will guide you through the process of how to create a tailored threat intelligence map that is specific for your organization. This map will be your navigator for running your threat hunting operations as efficiently and effectively as possible.

CHAPTER-6: HYPOTHESES DEVELOPMENT

After reading this article, you will master the hypotheses development and creation process, as well as how to tailor your hypotheses to your specific threats based on your threat intelligence map built in CHAPTER-5.

CHAPTER-7: WRITE YOUR PLAYBOOKS

Within this chapter, I will show you how to get things practically and create your threat hunting playbooks. These playbooks are the field manuals for your operators, analysts, or threat hunters. By having threat hunting playbooks, you get two major accomplishments – you build your threat hunting operations fundamentals, and you can practically delegate the threat hunting operations to other parties.

CHAPTER-8: EXECUTE AND SCALE

The last chapter will close all open edges and will provide you with the capabilities to execute your well-defined, well-planned, and well-written threat hunting playbooks. This chapter is the most exciting one because after reading this chapter you can run and scale your own threat hunting operations.

FINAL WORDS

If you want to learn the exciting vertical of threat hunting from scratch, the best thing you can do is to follow this series and the next chapters. Alternatively, if you are already an experienced threat hunter, incident handler/responder, or digital forensic investigator, I encourage you to use these chapters as references for specific needs, tasks, or missions.

LET THE HUNT BEGIN!

ABOUT THE AUTHOR

Maor Aknin is a cyber-security executive, strategist, and architect with hands-on operational experience and a deep technological background originating in 2006. His expertise is in the broad range of strategic information security, proactive defensive and offensive operations, and emergency cyber incident response. Maor's vision is to create value for society and make the world a safer place to live in.

As a founder of the global cyber-security company Cyber Way, Maor helps government and private sector clients across the globe to break the Vicious Cycle of Cyber by proactively and constantly mimicking real-world threats, providing concrete and quantified information, and producing consistent results.

Maor is the former head of the Cyber Emergency Response Team (CERT) at the Israel Defense Forces (IDF), where he also worked as a contractor and helped them with incident response activities and advanced cyber-attacks investigations. In addition, he taught digital forensics and incident response at the IDF Academy.

Maor is also the former head of the Threat Hunting and Incident Response Department at the Israeli National Cyber Security Directorate (formerly known as the National Cyber Security Burau). Maor established the department from scratch, where he oversaw the entire establishment process, including developing the technical capabilities, recruiting the staff, and building the processes and methodologies. His department handled all national-level cyber threats, incident response, and proactive threat hunting activities.