THREAT HUNTING – HUNTER or HUNTED

By

AKASH SARODE

Threat Hunting, as the name suggest is hunting for threats and in the cyber security world, threats are evolving day-by-day. So, it becomes our responsibility as an individual to come out with new techniques to prevent or detect any kind of threats or attacks.

Let's begin with the technical definition of "**Threat Hunting**" – the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.

Let's get to my definition of Threat hunting – **FIND STUFF**, as simple as that.

Threat Hunting is not a Technology but Approach.

As a Security analyst, Threat Hunting is applying our knowledge in an effective way to look out for any anomalies in the environment.

A threat hunter uses critical-thinking skills and creativity to look at patterns of normal behavior and be able to identify behavior anomalies.

Why is threat hunting necessary?

In traditional security monitoring approach, most of the blue teamers look out for threats based on the alerts being triggered out by SIEM or other security devices. In addition to alert–driven approach, why can't we add a continuous process for finding stuff from the data without any alerts driving us for incident. That's the process of Threat hunting, proactively looking out for threats in network. Those threats which are not identified by your existing security solutions or attacks which bypassed your solutions can be hunted down using this process. So, why

can't this be alert-driven, reason is alert driven is mostly some numerical way and not behavioral way.

Ways to perform threat hunting?

- **Manual** – Analyst need to continuously looking for anything that could be evidence/indicator of intrusion.
    - Important for the threat hunter to keep current on the latest security research.
- **Automated/Machine-assisted** – Analyst uses softwares that leverages "Machine Learning" and "UEBA" to inform analyst about potential risks.
    - It helps in providing Predictive and Prescriptive analytics.
    - Threat Intelligence feeds adds to analytics.

How to perform Hunting?

Please follow the below mentioned steps:-

1. Develop Hypothesis – Hypothesis means what u want to look for, like looking out for powershell commands making connection to internet etc.
2. Gather data – Based on the hypothesis, look out for data you need to collect for hunting.
3. Test hypothesis and gather hunting – Once data is collected, look out for threats based on behavior, search queries .
4. Automate certain tasks – Threat hunting can never be fully automated but semi-automated.
5. Operationalize Threat Hunting – Now, instead of ad-hoc hunting, operationalize your hunting program so that we can perform continuous threat hunting.

How to generate Hypothesis?

It's simply obtained by reading articles, security news, new APT public report, Twitter, and some frameworks to follow. Threat hunting is carried out on every kind of data source like endpoint, network, perimeter, etc. Its just applying our knowledge in effective way to find anomalies. Critical thinking skills are required. Threat Intelligence which consists of Indicators of Compromise (IOC's) also plays important role in performing hunting.

MITRE ATT&CK

Most of the threat hunting platforms uses "Attack MITRE" adversary model. MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

Attack MITRE has also came up with a project name "CAR" Cyber Analytics Repository.

The Mitre team has listed down all those adversary behaviors and attack vectors carries out by an adversary on a victim machine. It provides you with description as well as some references regarding the threats, based on historical outbreak. It uses TTP's Tactics, Techniques and Procedures and maps it to Cyber Kill chain. Most of the threat hunting methodology uses Mitre framework to carry out hunting process.

Practical Threat Hunting -

Now, to perform hunting, we need hypothesis and after generating the hypothesis, we can hunt or search for the attack based on any platform which we use. For testing hypothesis, you can use any tools available such as Splunk, ELK Stack, and many more, but kindly take care of data before starting hunting. Florian Roth has came up with new generic format for SIEM signature – SIGMA. Most of the Mitre Att&ck techniques are mapped to Sigma rules and those rules can be directly incorporated in to your SIEM platform for threat hunting. Sigma conversion to Splunk, arcsight, ELK is also available.

Sigma rule conversion ready made list is available at google sheets:-

https://docs.google.com/spreadsheets/d/1mY6BGYZgwPH3UiVAdxU4Hraa9n1gFLXSMcR_5mhs0GE/edit?usp=sharing

Threat hunting can never be automated but some portions can be such as these sigma rules can be directly alerted in SIEM but the later part of investigation and triage needs manual touch.

Threat hunting can be analytics driven as well. Machine learning and UEBA used to perform risk score can also be used as hunting hypothesis. Most of cyber analytics platform are leveraging this UEBA , ML feature to identify anomalies.

Threat Hunting Hunts:-

1. Word or excel file opening powershell which runs mimikatz command for hash dumping – To check this hypothesis, first look for data, do we have proper data to hunt for this hypothesis, then hunt for winword.exe /execl.exe process creating powershell.exe, and command line containing (mimikatz).

2. Downloading files from internet (Other than browser) – Look out for process which are used to download files from internet other than browser, certutil.exe , hh.exe can be used for the same.

3. Powershell download cradles event_data.CommandLine:(*powershell* *pwsh* *SyncAppvPublishingServer*) AND event_data.CommandLine:(*BitsTransfer* *webclient* *DownloadFile* *downloadstring* *wget* *curl* *WebRequest* *WinHttpRequest* iwr irm "*internetExplorer.Application*" "*Msxml2.XMLHTTP*" "*MsXml2.ServerXmlHttp*")

4. Privilege escalation - Run whoami as System
   event_data.Image:"*\\whoami.exe" AND (event_data.LogonId:0x3e7 OR event_data.SubjectLogonId:0x3e7 OR event_data.User:"NTAUTHORITY\\SYSTEM")

5. Suspicious LSASS SSP was loaded event_id:4622 AND - event_data.SecurityPackageName:(*pku2u *TSSSP *NTLM *Negotiate *NegoExtender *Schannel *Kerberos *Wdigest "*Microsoft Unified Security Protocol Provider")

6. Possible logon session hijacking event_data.Image:"*\\tscon.exe" AND (event_data.LogonId:0x3e7 OR event_data.SubjectLogonId:0x3e7 OR event_data.User:"NTAUTHORITY\\SYSTEM")

7. Using certutil for downloading event_data.CommandLine:(*certutil*) AND event_data.CommandLine:(*urlcach* *url* *ping*) AND event_data.CommandLine:(*http* *ftp*)

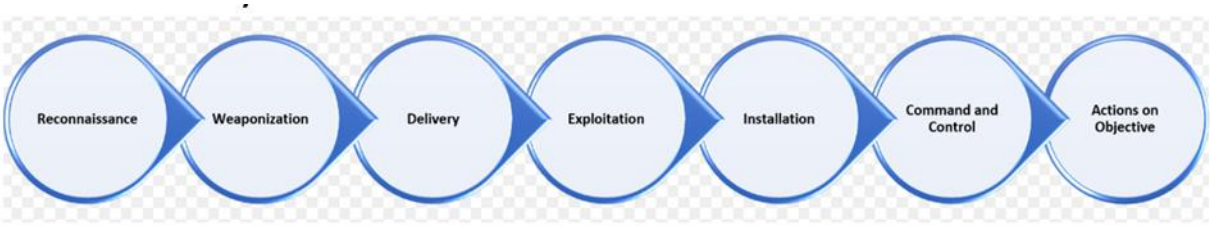
Att&ck mitre contains them all. Just we need to take care of some new techniques in the future which can be used by attacker.

Machine Learning and Threat Hunting

Machine learning plays an important role in cyber threat hunting. Multiple algorithms can be used such as classification, clustering etc. to identify any kind of anomaly and outlier based on logs in SIEM. Machine learning plays a role of

assistance to threat hunting as it provides us the outlier which will be further invested by analyst to hunt for threat.

Chain cycle for Red-blue team



Red Teamer Cyber Kill Chain

Blue Teamer Defense Chain

Resources:-

1. Sans Threat Hunting and IR summit
2. Red canary Threat Hunting resource
3. Att&ck Mitre – Att&ckon.
4. CAR by Mitre
5. Sigma project by Florian Roth – https://github.com/Neo23x0/sigma
6. Twitter
7. menasec.net

Threat Hunting is all about applying knowledge and implement it via hunts. Its like hunting out for threats after understanding the threats. So, Threat hunting is certainly not a Blue teamer Task.

You need to be RED + BLUE = PURPLE Teamer!

Let's decide whether we want to be a hunter or get hunted by a hunter!

References-

https://en.wikipedia.org/wiki/Cyber_threat_hunting

https://github.com/akky2892/Sigma-to

https://github.com/Neo23x0/sigma

https://www.threathunting.net/