# CYBER THREAT HUNTING

## DETECT ADVANCED THREATS HIDING IN YOUR NETWORK

*A guide to the most effective methods.*

LIFARS
your digital world, **secured**

# CONTENTS

# BREAKDOWN

## Threat Hunting Defined

Cyber threat hunting is one of the best approaches to investigate potential compromises, detect advanced threats, and improve cyber defenses. It is a thorough process that combines the use of human talent and engineering to seek Indicators of Compromise (IOC) in the client environment. The industry defines cyber threat hunting as "the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions"[1]. Threat intelligence analysts familiarize themselves with an organization's environment and are able to effectively filter out key events that need closer examination. These analysts find and identify possible targets, then interpret patterns around the attack. Threat hunting usually requires tapping into sources of intelligence from the Dark Web as well as network traffic and endpoints. Since there is never a definite answer, only a stochastic probability of confirming a compromise, it is critical to examine both the false positives and negatives as well as various sources to ensure accuracy and keep the focus on the indicators of compromise.

## How it Works

Threat hunting leverages the latest data analytics algorithms, while utilizing threat intelligence to detect the zero day cyber-attacks, Advanced Persistent Threats (APTs) and the latest IOC to answer the probability of an enterprise compromise. LIFARS optimizes our experienced approach to look for threats that have gone unnoticed within the network environment. Tactics, Techniques, and Procedures of attackers are examined to analyze the potential vector of compromise entry, and the initial point of a compromise. These threats tend to be in the environment for long periods of time by escaping detection or maintaining persistence. LIFARS discovers these hidden attacks using a number of detection mechanisms—including network forensics, endpoint examination, and pattern matching to indicate compromise.

# THE NEED

## Growing Cyber Breaches

An organization should implement proactive measures to reduce the possibility of a compromise. With threat hunting, an organization can improve cyber defenses by detecting threats hiding in its network. The sooner an attack is found, the faster it can be mitigated, limiting the amount of damage.


Once sensitive information is leaked, it can be irreversible. Threat hunting can help an organization's corporate identity and integrity by decreasing the chances of private customer or company information from getting leaked or hacked.

The number of attackers without IT knowledge, such as script kiddies and insiders, is increasing at an alarming rate, and with the increased prevalence of the Internet of Things (IoTs), Bring Your Own Devices (BYODs), and the cloud, network complexity continues to grow—making it harder for organizations to keep their network secure. As a result, it becomes more difficult to monitor all the data and activity being sent or received. Moreover, attackers consider targeting networks as their top priority, because exploiting one vulnerability can harm hundreds or thousands of devices connected to that network. Choosing threat hunting can mitigate these possibilities.

# WHEN TO CHOOSE THREAT HUNTING

A business should start threat hunting as soon as possible. If a company has to ask the question, “Is my business at risk or compromised?”, chances are it’s time to start threat hunting.

More and more organizations are using threat hunting to improve their overall security. With threat hunting, not only are hidden threats found and detained, but the speed and accuracy of catching these threats increases, reducing the likelihood of an incident. The biggest challenge for many companies is to make threat hunting a viable and obtainable option that brings in a profit. However, identifying and understanding the threats to your system is the first step in dealing with potential losses.

# THE LIFARS SOLUTION

## LIFARS Threat Hunting

When choosing an expert threat hunting firm, it is important to not just evaluate their experience, but the tactics, and the tools they use as well. At LIFARS, we continuously explore the latest innovations in the cybersecurity field, and seek to stay one step ahead of tomorrow's industry landscape. LIFARS can offer your business decades of experience and lessons learned from previously conducted threat hunting investigations.

As the threat landscape evolves, keeping up with the latest threats can be a tremendous challenge. The LIFARS team stays up to date on the newest threats and will continuously monitor your network to detect existing threats – including advanced or targeted attacks that have bypassed existing perimeter controls.

## LIFARS Threat Hunting Categories

1. Endpoint Threat Hunting
2. Networks Threat Hunting
3. Threat Intelligence & Deep Dark Web Search

# ENDPOINT THREAT HUNTING

## Breakdown

Endpoint threat hunting is a methodology designed to detect and alert if the integrity and confidentiality of endpoints are compromised. This is managed by validating forensics artifacts on the endpoint and determining if the obtained information requires further examination. LIFARS' expert team can access relevant information swiftly and integrate with existing advanced persistent threat detection solutions (APTs) to capture endpoint snapshots. LIFARS is able to verify the visibility potential of compromise indicators and potential threats, search other endpoints for the same threat, and remediate the issue leveraging Endpoint Security clean up methodology.

## Endpoint Threat Hunting Categories

Endpoint Threat Hunting forensics artifacts can be divided into three categories.

1. **Threat Hunting on Active & Recoverable Data:**
   Processing active files on the system can be a great start to endpoint threat hunting and artifacts such as prefetch, amcache, and shimcache.

2. **Examination of Unallocated Data:**
   Unallocated data, such as file systems and volatile data, can reveal impressions of tools such as mimikatz, system commands and powershell activities, and also process volatile data, such as network connections.

3. **Memory Forensics Examination:**
   On the live system or after collection—processes, their parents, and threads can be found and addressable space can be examined, likely with Yara-type signatures or other conditional statements.

# ENDPOINT THREAT HUNTING

## Techniques

### Clustering

A statistical technique in which groups of like data points established on specific aspects of a large data set are separated into groups. This is most effective when acting upon a broad group of data points that do not share behavioral characteristics. Clustering finds precise cumulative behaviors, like an unusual number of instances of a common occurrence through various applications such as outlier detection.

### Grouping

A technique in which a set of various unique artifacts are taken and identified using specific criteria. For the hunter, an input consists of a specific set of items that are of interest as well as the found groups within the items that the attacker may be using as tools. It consists of finding specific criteria used to group items, like events which happen within a specific time window. This is best used when hunting for several, similar unique artifacts.

### Searching

A simple technique in which hunters query data for specific artifacts that can be used in most tools. However, outliers may not be found in the result set since hunters only get the results they search for, making it sometimes ineffective. Too general of a search will flood the analyst with an excessive amount of results. Therefore, to prevent an overload, the search must be narrow and specific. On the other hand, a search that is too narrow might not render enough effective results.

### Stack Counting/Stacking

A common technique used to investigate a hypothesis, in which the number of occurrences for specific value types are counted and the outliers of the results are examined. This is most effective when the input is thoughtfully filtered, such as endpoints of a similar function. Also, to predict the volume of the output, the analysts must comprehend the input. When used through various unique hosts it is best to use a filtered input. When using stacking, the number of command artifact executions by hostname or account should be counted.

# ENDPOINT THREAT HUNTING

## Visualization

Visualizations are a method used to illustrate, interpret, and determine patterns in the data. There are several approaches used to visualize the data.

**Box Plots**: Used to identify outliers and determine the distribution of a dataset. They are useful for portraying extreme values and showing the differences between distributions. Entities can be grouped based on the function or type, helping analysts find inconsistencies. Also known as box-whisker plots.

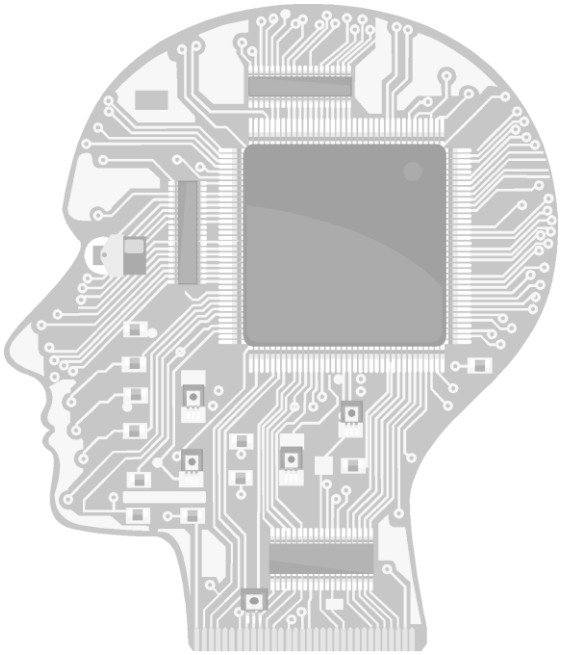
**Sparklines**: Used when displaying trends in an array of values where the values are continuously fluctuating. As data fluctuates, sparklines make it easier for the analysts to see the changes that occur, minimizing the time it takes to understand the displayed data.

**Heat Map**: Used to represent data in a color format to cater a prompt visualization of the data. With color to represent the data, distinct groups of data are visible and relationships between data sets become easier to understand. Heat maps are the most useful when the inputted data is distinct and the outliers are of interest.

# ENDPOINT THREAT HUNTING

## Machine Learning Techniques

Machine learning takes away the need for explicit coding of a system. Instead, the system learns automatically using algorithms. Random Forests, one algorithm that is the most used by data scientists, provides the least challenges and saves time when creating code. A tree, or random training data, is made when random subsamples are taken from the training data and columns. When conducted several times, numerous trees are created. Each tree has an answer, then the most consistent answer is then used.



# NETWORK THREAT HUNTING

## Breakdown

LIFARS network threat hunting analyzes network activities, such as packet captures and network flow, network IDS/IPS alerts, and network device logs.

### Network Threat Hunting Verticals

1. **Threat Intelligence for Network Communications**
2. **Network Anomalies and Pattern Machine Learning Algorithms**
3. **Volumetric Statistical Analysis**

Indicators of compromise can be examined parallel to network streams, including full reconstruction of sessions and examination. It is easy for firms to disregard monitoring potential threat vectors where the most insidious, long-term damage may be percolating. LIFARS expert team can analyze and examine network anomalies in protocols and contextual capture. Volumetric statistical analysis will focus on examining four key network features: the number and initiation (TCP SYN) of outbound network connections, the duration of connections, the amount of data exchanged, and the frequency of connections.

# THREAT INTELLIGENCE

Threat intelligence allows you to identify an ongoing cyberattack. LIFARS threat hunting team familiarizes themselves with a company's environment and are able to effectively filter out key events that need closer examination. Optimization of threat intelligence in the daily mirage of events can dramatically increase the overall effectiveness and allow a System and Organization Controls (SOC) team to focus on important tasks and real malicious incidents. LIFARS threat intelligence provides a comprehensive evaluation of the enterprise, fine-tuned for actionable intelligence.

## Deep Dark Web Search

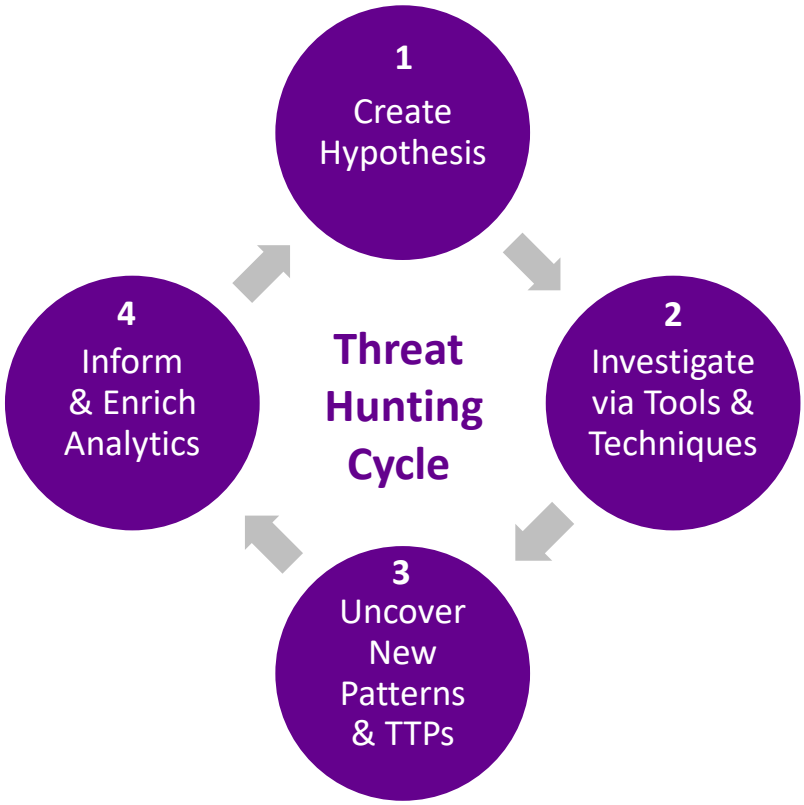
LIFARS threat hunters also monitor the Deep Dark Web where companies' data can easily be exposed. Data loss on the Dark Web cannot be prevented, however a leak can be detected and remediated. LIFARS' threat hunting team utilizes Deep Dark Web Searches to stop damage and quickly resolve the matter.

# LIFARS METHODS

## Threat Hunting Framework

LIFARS uses the first widely accepted framework for conducting cyber threat hunting operations from the Sqrrl Security Analytics Company.

Four specific milestones are performed cyclically:




The purpose of the steps is to describe the essence of conducting cyber threat hunting operations. The framework does not provide any specific details such as planning, implementation, and specific TTPs—these are left to the organization to determine.

# TWO LEVEL APPROACH

Tools like Outlier and Encase Enterprise use a two-level approach for the analysis of vulnerabilities that may be affected, such as configuration systems.

## Level One

Holistic examination is performed on the network to curtail the focus to a few sets of questionable computers with possible vulnerabilities. Analysts use the information they gather to evaluate vulnerabilities they encounter through various means. Metadata is collected and analyzed from endpoints to find usage patterns, statistical outliers, user behavior anomalies, and vulnerabilities. Automated security analytics are also used to run unknown binaries.

**CONFIGURATION/VULNERABILITY**

Versions of frequently exploited client facing programs are tested and evaluated for vulnerabilities within the system. Unpatched machines with vulnerable software pose a greater risk. These programs include Java, Adobe Acrobat, or Media Player.

**COMMAND LINE AND INTERACTIVE BEHAVIOR**

To detect questionable user or program behavior, Prefetch, superfetch, lnk, shellbags, MRU, registry entries, and file timestamps are applied.

**USER ACCOUNT ABUSE**

To recognize accounts that may have been abused through stolen passwords, the hash attacks user profiles and logon events are examined.

**PERSISTENCE MECHANISMS**

Software is examined to indicate the threat level and timestamp information to locate a starting place for a timeline analysis.

**MEMORY AND DLL INJECTION**

To find out if a program was injected into another program, the loaded memory is audited.

**CONFIGURATION/BROWSER**

Browsers are considered a higher risk when they are set with plugins, proxy ports, extensions, and helper objects.

# TWO LEVEL APPROACH

**AV QUARANTINE LOGS**

AV logs are examined to identify new or previously existing malware.

**PERIMETER EVENT LOGS**

Perimeter security devices can be used to recognize possible attacks, vulnerable machines, and existing infections.

**DNS LOGS**

Like perimeter event logs, DNS logs can help determine at risk machines.

**CUSTOMER SUPPLIED PREVIOUS HISTORY**

Determines the extent machines and user profiles should be examined.

## Level Two

High risk machines are more closely examined in Level Two of the approach. Data and digital artifacts are collected in small quantities so only the right data is found. Event logs, registry hives, memory snapshots, or master file table records are analyzed. The collected data is then “normalized” and arranged in a “timeline reconstruction”.

**CREATE ADDITIONAL QUERIES & INDICATORS**

Used to search the entire network to find threats in a quick and adept manner.

**BROWSER HISTORY**

All users and program activity and history which uses browser APIs is examined for suspicious activity.

**MEMORY ARTIFACTS**

Memory snapshots of suspicious activity, modules, strings, or code are evaluated to find malware or hidden hacking tools.

# TWO LEVEL APPROACH

### SANDBOXING AND BEHAVIORAL ANALYSIS

To ascertain runtime behavior, specific executable files are examined in a sandbox.

### EVENT LOGS, REGISTRY HIVES

Digital artifacts that contain time stamped endpoint behaviors which can be used in a forensics timeline analysis.

### NETWORK CONNECTIONS AND IP REPUTATION

Suspicious network connections are compared with an IP reputation database.

### SOFTWARE USAGE HISTORY

To find if client side software has crashed, all event logs or crash logs are inspected to use as a place for a timeline analysis.

### MFT, USN CHANGE JOURNAL, SYSTEM RESTORE POINTS

Similar to event logs–digital artifacts that contain time stamped endpoint behaviors and are used in forensics analysis to establish a timeline.

### BINARY REVERSE ENGINEERING

Binary files are used to evaluate command and control loops, find internal functions, and discover encryption methods.

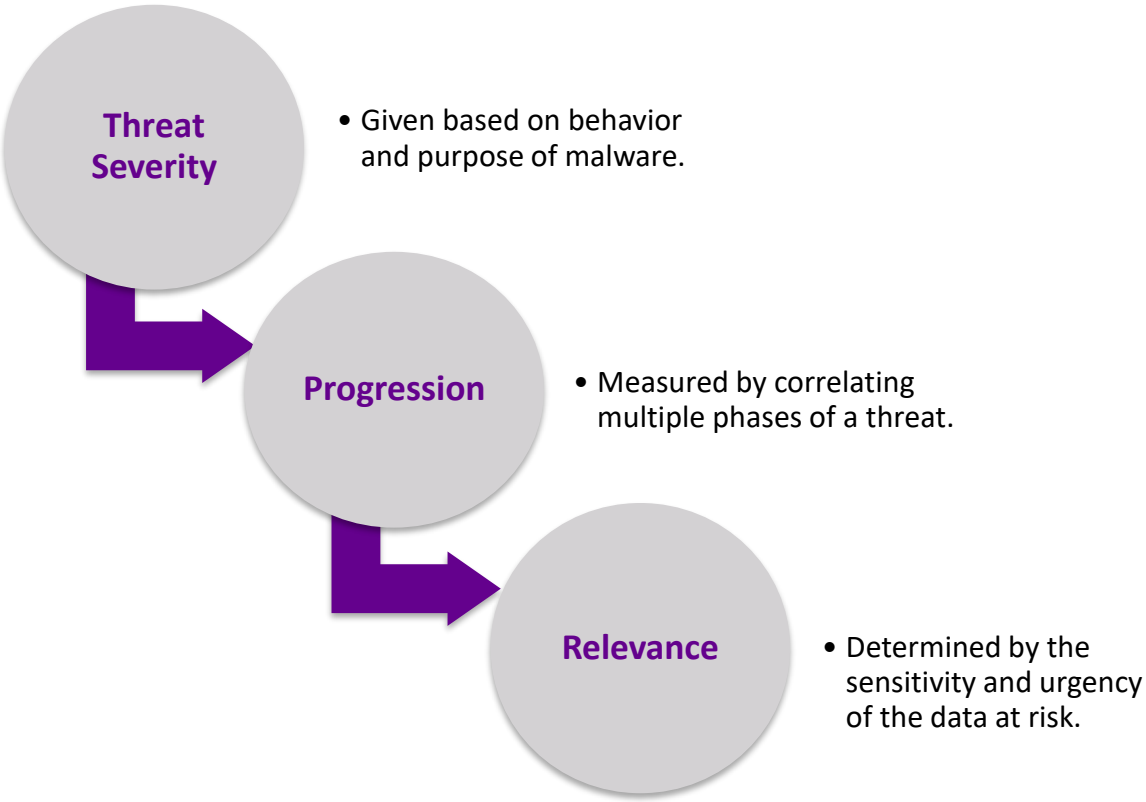
### FILE ARTIFACTS

The files deemed suspicious and, therefore, pulled for further examination.

# LIFARS METHODS

## Threat Metric Modeling

LIFARS uses Threat Metrics Modeling to enable the ranking of threats according to:



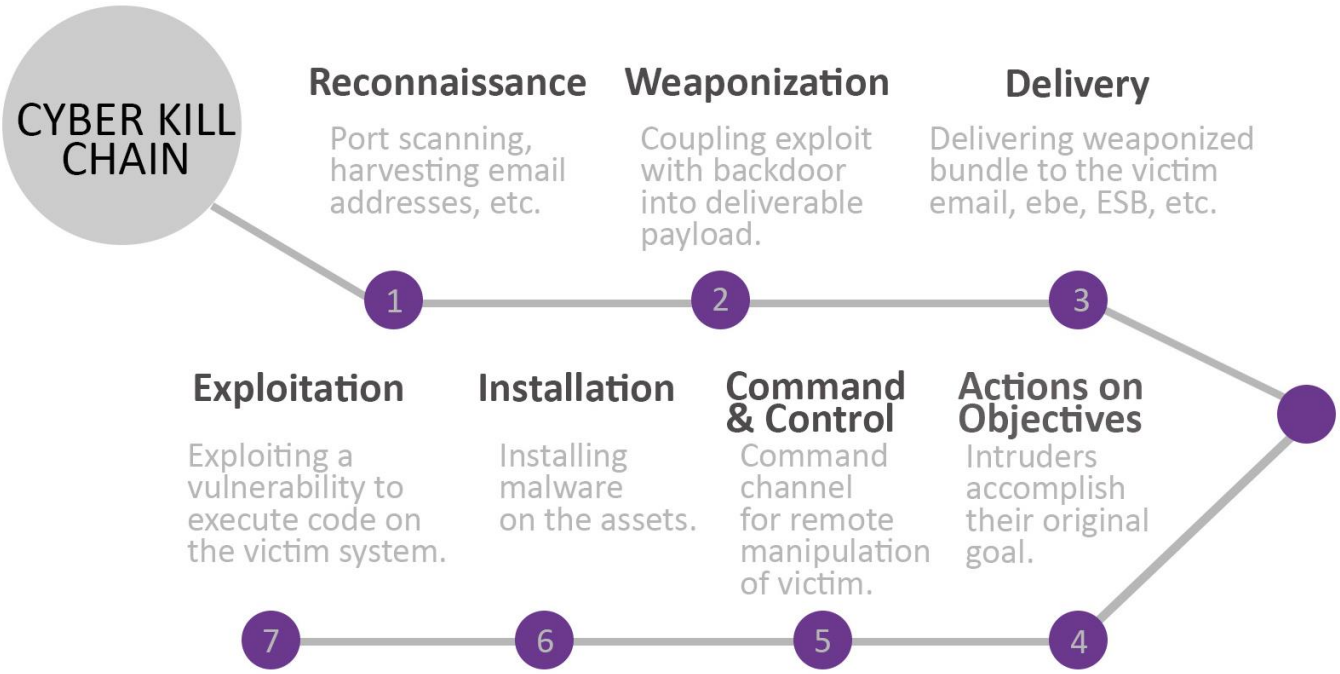

## Threat View Dashboard

LIFARS also offers Threat View Dashboard, which presents a visual view of the Threat Metric information that helps our team quickly identify which threats have the biggest risk to the organization and require immediate attention and which threats may safely be deescalated.

# LIFARS METHODS

## Attack Tree Analysis

Threat hunters focus on understanding Tactics, Techniques, and Procedures (TTPs) that are produced in the indicators through a process known as Attack Tree Analysis. Attack Tree Analysis involves modeling what steps an adversary may perform to breach an organization's systems (Schneier, 1999). Graph below is "The Lockheed Martin Cyber Kill Chain", which illustrates one method to determine where in the attack tree an adversaries' activities occurred. When attempting to get into a network or web server, attackers often follow these Cyber Kill Chain steps.



LIFARS

your digital world, **secured**

## Contact Us to Learn More

www.lifars.com | 212.222.7061 | info@lifars.com | Twitter: @LIFARSLLC

LIFARS is an Elite Cybersecurity Intelligence firm based in New York City specializing in: Incident Response, Digital Forensics, and Cybersecurity Intelligence.