happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

THREAT HUNTING

IOCs VS TTPs

www.happiestminds.com

Table of Contents

Abstract

The Threat landscape is changing with time; therefore, organizations need to adopt new threat detection capabilities to defend themselves from new and advance Threats.

The traditional way of looking at events and detecting something unusual by predefined values of signature is not very effective. Let's go deeper and get a general pattern to detect the threats and protect from any threat family or threat behavior.

THREAT HUNTING

As per SANS "Threat hunting uses new information on previously collected data to find signs of compromise evading detection".

So, we can understand it as an activity where security analysts check events both on the high and low level to make some significant deviation to identify anomalies.

It is the complete understanding of any traffic, process execution and any user activity. Analysts should know all answers **What, When, Where, Who, How and Why.**

These manual efforts of Threat Hunting pave the way for auto alert configuration. Threat Hunting in perspective to SOC or SIEM can be considered as hunting of events collected by SIEM for multiple log sources and identify unusual patterns which derive signs of Threat.

Now a day's organizations are adding pro-active Threat Hunting services and investing more on the same. Pro-active Threat Hunting helps organizations to reduce the impact of the Threat marginally. However, all of this depends on the seriousness and the efforts of the organization.

THREAT HUNTING MATURITY

To achieve a well-managed and mature Threat Hunting program, Organizations must align it with some of the external best practices, available frameworks and proper skill resources. Continuous tracking and taking corrective decisions are required to maintain the pace and accuracy. And finally, support from the management is critical to have a proper direction and enforcement.

Threat Hunting **Traditional Way**

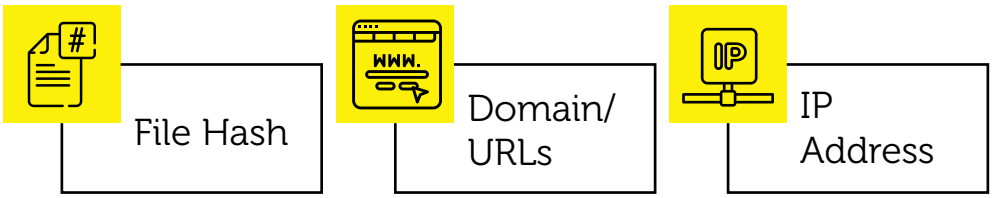
An Organization can choose many ways as per available resources and budget. This Whitepaper mainly describes Threat Hunting based on IOCs and TTPs. Let's explore more.

IOCs Based Threat Hunting

What is IOC?

As per Wikipedia, **"Indicators of Compromise (IOC) is an artifact observed on a network or in an Operating system with high confidence indicates a computer intrusion."**

Examples of IOCs (not limited to)



Sources of IOCs (not limited to)

TAXII **STIX** **OpenIOC**

IOC can be pulled manually and fed into SIEM or administrators can configure SIEM to extract latest IOCs from external sources.

Some security organizations are also releasing regular security advisories on latest IOCs and sharing with their customer to act proactively and reduce the risk of getting compromised.

Benefits of IOCs

Quick

Latest IOCs become available quickly (paid or free sources).

Easy To Implement

Many sources are available to fetch latest IOCs and add into SIEM (manually/automatic).

Challenges of IOCs

Dynamic

IOCs are not static in nature. These need to be constantly updated. The one which you added in watchlist last month may still not be bad now.

False Positive

As IOCs are dynamic so analyst cannot be sure on triggered alerts. Each time investigating all IOC based alerts causes less optimiation time and efforts.

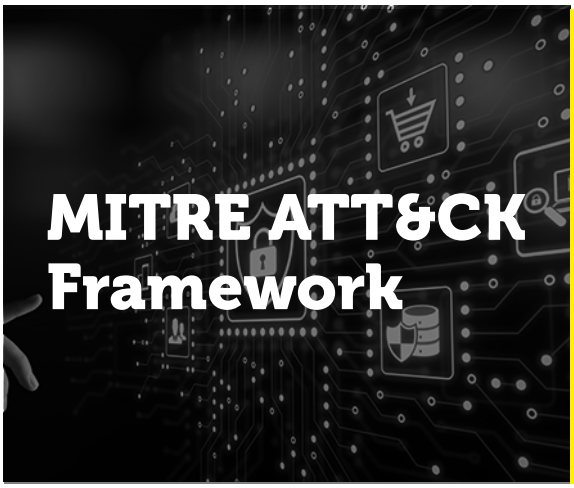
Reactive

IOC based alert are mostly reactive in nature as detects once system is compromised.

No Zero Day Detection

IOCs provide protection against only known threats

Threat Hunting **Modern Way**

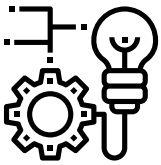


MITRE ATT&CK™ Based on the real-world observation, it is a globally accessible knowledge base of antagonist tactics and techniques. In the development of Threat models and methodologies in the private sector, in the government sector, also in the cybersecurity product and service community "Attack" knowledge base is used as the foundation.

Initial Access	Execution	Persistance	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript
Exploit Public-facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software
External Remote Services	Command -Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services
Replication Through Removable Media	Control Panel Items	AppCert DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash

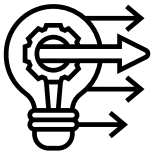
Introduction to **TTPs**

TTPs describe 'why', 'what' and 'how' of adversary behavior. Given, specific observed instances within individual-specific incidents, TTPs are abstracted so that they may be more generally applicable in developing contextual understanding across incidents, campaigns and Threat actors.



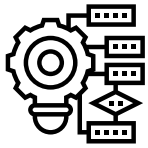
Tactics
WHY

Why attacker is trying a specific technique. What attack is going to achieve?



Technique
WHAT

Techniques are listed below each Tactic.



Procedure
HOW

How attacks achieve the desired result.

Comparison between IOCs & TTPs

IOCs	TTPs
Detective in nature	Descriptive in nature and define characterization on abnormal behavior
More false positive alert	Less false positive alerts
Specific to one attack	Covers entire attack family depending on behavior pattern
Reactive	Proactive

Let's understand the difference between TTP and IOC with simple examples –

1

Threat advisory company releases malicious hashes for ransomware - This is a type of IOC. If we go a little deeper and understand the behavior of ransomware and find the common properties and define their characteristics, then it is a Technique.

IOC – Malicious Hash

Techniques – Access to multiple files in short duration OR encryption/rename of various data in a short period.

2

Threat Advisory company releases malicious domains categorized as Command and Control or bad domains. These are simple IOCs which can be changed later. Instead of this if the organization detect behavior (Domain Generation Algorithm DGA) that will be a more stable and correct solution.

IOC – Known bad domains

Technique – Domain Generation Algorithm (DGA)

Conclusion

This is how we see both approaches of Threat Hunting. Both have their advantages, but by combining classical technique of IOCs with the new way of TTPs, will help organizations to combat with new emerging threats. Finally, whatever approach we follow, acquiring skilled resource is very critical because they are the ones who will use their intelligence to understand the attack patterns and enhance the detection capabilities.

About the Author

Gaurav Tiwari has over 13 years of experience in Security Operation Center (SOC) with multiple SIEM solutions. He is currently part of Infrastructure Management and Security Services business unit of Happiest Minds Technologies Pvt Ltd. He is primarily responsible for running security operations as well as maturing it with new detection and response capabilities. He is also involved in designing new security solutions. Gaurav is an active member of ISC2 organization.

Write to us at Business@happiestminds.com

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transfor-mation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in the U.S., UK, The Netherlands, Australia and Middle East.