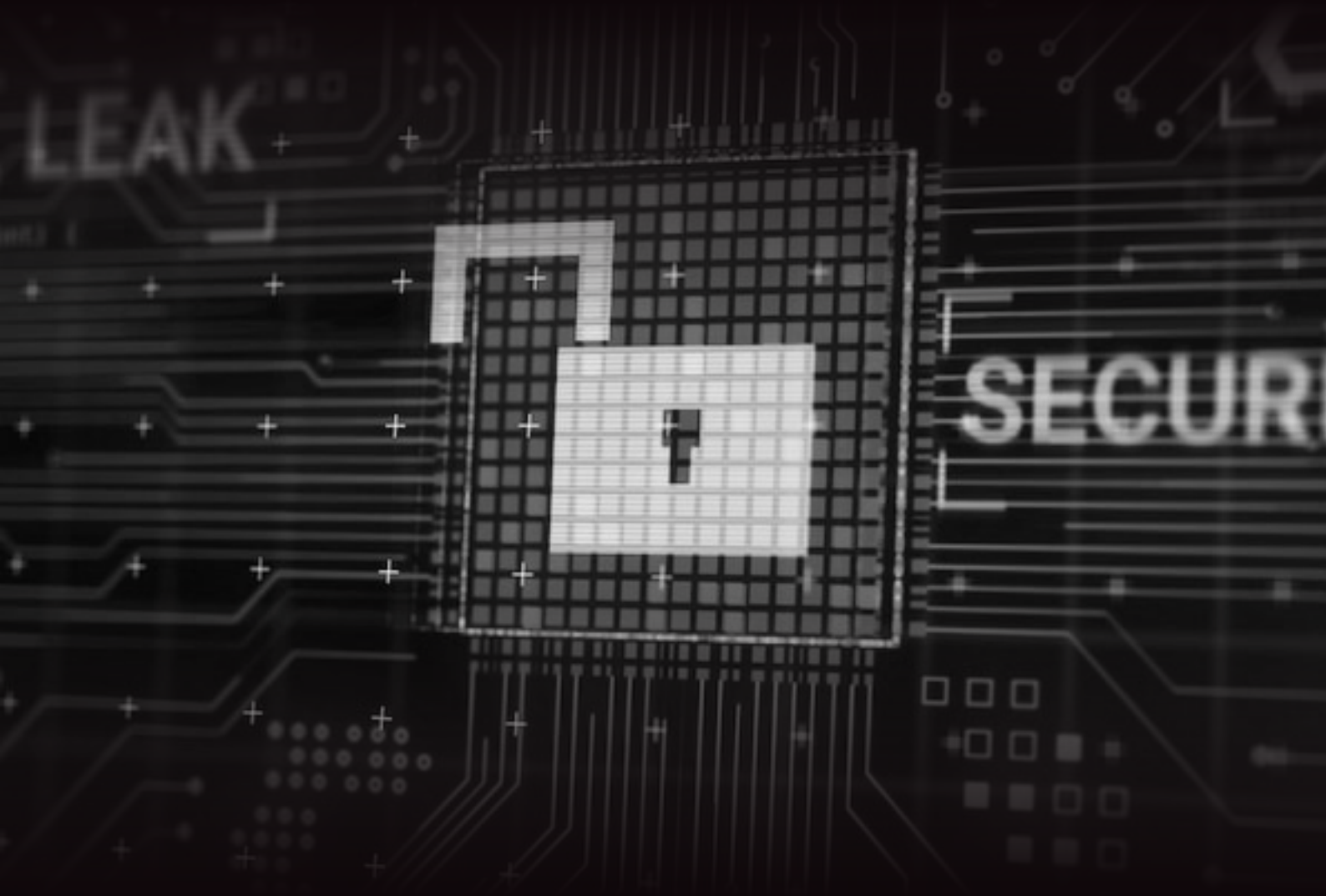
SISA



THREAT HUNTING 101

A Comprehensive eGuide

Table of Contents

What is threat hunting?

Advanced threat actors slip past the initial security defenses set up by organizations. These **malicious attack vectors** can remain in the network for months trying to move laterally across the environment with the help of **confidential data** or login credentials. Threat hunting is a process usually followed by Security Analysts to search for such anomalies in an organization's environment to identify cyber threats that may be **lurking undetected** in a network. This approach is an essential component of a robust cyber defense strategy and combines a proactive methodology, innovative technology, and **threat intelligence** to stop attacks before they successfully penetrate an organization's defenses.

Why threat hunting?

The third quarter of 2022 witnessed a 70% increase in breaches compared to the previous quarter. The rapid and alarming rate of increase in cyber-attacks is only expected to accelerate further in 2023. The increasing sophistication of cyber-attacks leaves no room for doubt - it is important now, more than ever, for organizations to stay one step ahead of cyber threats and respond to them proactively. Organizations will need an arsenal of tools that include antivirus, firewalls and SIEM platforms along with new and emerging technology to hunt adversaries, detect anomalies and identify vulnerabilities in their network environment.

Proactive threat hunting is a critical component of a robust cyber defense strategy and enables organizations to stay one step ahead of the ever evolving and rising sophistication of cyber-attacks.

A proactive threat hunting approach enables threat hunters to become familiar with the organization's environment, network, and architecture to filter out and closely monitor key events by leveraging both **emerging technologies and** human skills. It also helps identify the potential target of the attacks as well as their patterns and the steps followed at a very initial stage. Threat hunting reduces the time taken to detect an anomaly after the occurrence of an incident, thereby **minimizing its impact on core systems,** thus facilitating **quick patches** to vulnerabilities. With the right tools, techniques and training, threat hunters can **formulate a hypothesis** around a malware, threat group or any other possible attack vector to determine whether it is present in the organization's environment. Threat hunters can then leverage the hypothesis generated from various sources like zero-day vulnerabilities, threat intelligence or incident reports, as a starting point for further investigation.

Types of threat hunting

When threat hunters start to search for unknown threats present in an organization's environment, they first investigate all the events to detect suspicious activities or system vulnerabilities that can disrupt our put the environment as risk. Threat hunting investigations are classified into three key categories:

1 Structured

Structured threat hunts are built around a central hypothesis relating to specific threat actors, their **tactics, techniques, procedures (TTPs)** and attack patterns. This enables threat hunters to identify a threat actor before it can damage the targeted systems.

2 Unstructured

Unstructured hunting is based on the logs or the alerts that are triggered by monitoring tools. Triggered alerts such as **indicators of compromise (IOC),** blacklisted IPs, or unknown executables work as a cue for threat hunters to further dig and analyze older as well as upcoming logs and take necessary action to mitigate the risk.

3 Situational

Situational investigation is based on the hypothesis unique to an enterprise that is developed from an organization's **internal risk assessment, vulnerability analysis** or **latest threat intelligence.** Threat hunters reference this internal and crowdsource data to search cyberattack trends and reveal the latest TTPs of a potential threat.

Threat hunting tools

The process of threat hunting is usually built on the foundation of planning, baselining, and testing based on the hypothesis formulated by experienced cybersecurity professionals. Besides these, a threat hunter can also use automated tools or platforms to boost threat analysis and identify any suspicious patterns and relationships on a large scale. These tools help them investigate existing logs and ensure that relevant alerts are triggered when a suspicious event occurs.

Some of these tools are:

Security information and event management (SIEM)

A combination of security information management (SIM) and security event management (SEM), SIEM solutions provide **real-time analysis** of security threats and offer tracking and logging of security data. It helps threat hunters to conduct an in-depth investigation of any anomalies and irregularities to find the root cause of an incident and take swift action. Recognized as a staple in modern-day security operations centers (SOC), SIEM has evolved to automate many manual processes associated with threat detection and incident response with the use of technologies such as **Artificial Intelligence (AI) and Machine Learning (ML)**. Some of the prominent SIEM tools available in the market are Splunk, IBM Qradar, ArcSight, LogRhythm, and SolarWinds.

Managed Detection and Response (MDR)

MDR is a cybersecurity platform that remotely monitors, detects, and responds to threats. By combining both human expertise and technology, MDR helps organizations identify threats and limit their impact. It offers analysts with threat intelligence, **advanced analytics,** and **forensic data** to detect anomalies, respond to alerts and restore the affected endpoint to its normal state. MDR enables threat hunters to identify and alert on the threats that might have been missed by the automated layers of security defenses.

Getting the Basics Right.

Threat hunting is not just the use of SIEM and MDR tools but is the effective monitoring and management of log data across an organization's computer systems, servers, and networks.

Organizations generate massive amounts of log data and events through applications, networks, systems, and users, and therefore require a systematic process to manage and monitor disparate data across log files.

The combination of network-level security logs, authentication logs and application-level audit logs help provide complete visibility of an organization's IT infrastructure.
Logs generated from Firewalls, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), Domain Name System (DNS) and Endpoint Detection and Response (EDR), Antivirus etc., are a crucial component of forensics, compliance, and real time threat hunting. These log sources provide a detailed record of every action and thus provide insights to help identify the root cause of problems or anomalies. Correlation rules and AI/ML tools work much better in tandem with these logs as well.

- **Firewall logs**

  The firewall keeps track of all traffic entering and exiting the environment it was designed to protect. It allows access to information such as the source address, source port, and destination address and port.

- **IDS/IPS logs**

  They inspect network packets, block suspicious ones, and notify administrators of attempted attacks. The logs of these systems contain valuable network threat information about attack types, targeted devices, and malicious traffic sources.

- **DNS logs**

  It manages and secures communication between browsers and the websites and services they access. It entails regularly checking DNS records for any unexpected changes or localized outages in order to detect potential security breaches.

- **EDR logs**

  It combines continuous real-time monitoring and endpoint data collection with automated response and analysis. EDR supports custom rule mechanisms and provides threat intelligence-based detection.

- **Antivirus logs**

  It primarily employs signature-based detections to identify threats on a system, which aids in the tracking of common malware and hacking tools. It also aids in the identification of notable threats and provides insight into trends and coverage from antivirus solutions.

Analyzing an attack

Threat hunting is a proactive and challenging process, and it is not easy to document rapidly evolving adversarial techniques. Understanding how attacks work is critical to devising defense strategies and for that hunters need to use detailed threat intelligence relating to the **anatomy of an attack.** Highlighted below are some of the threat intel frameworks that are useful for a threat hunter to analyze the movement and minimize the impact of a threat actor.

- ## Cyber Kill Chain

The Cyber Kill Chain framework, developed by Lockheed Martin, underlines a step-by-step approach that attackers use to move through networks to identify potential vulnerabilities. Divided into seven stages, this model can help a threat hunter recognize these security gaps and take measures to prevent systems from getting compromised. The **seven stages** of Cyber Kill Chain model are as follows:

Figure 1: Cyber kill chain framework

Reconnaissance

The first stage includes identifying the **potential targets,** collecting data about them, spotting their security vulnerabilities, and exploring the entry points for an attack.

Weaponization

After gathering all the necessary information, the attacker starts **engineering the malware** based on the security vulnerabilities and the intention of the attack.

Delivery

The weaponized malware is then used to infiltrate the target's network via **phishing emails** or other mediums such as through hardware or software vulnerabilities.

Exploitation

The attacker breaches the perimeter and further infiltrates the target's network by **moving laterally** to achieve their objectives.

Installation

After exploiting the vulnerabilities, the attacker attempts to install malware and other cyber weapons using **backdoors** or **command line interfaces** on the target network to exfiltrate data.

Command and control

The attacker gains control over the network and systems and starts communicating through the installed malware to **gain access** to privileged accounts, search for credentials and change permissions.

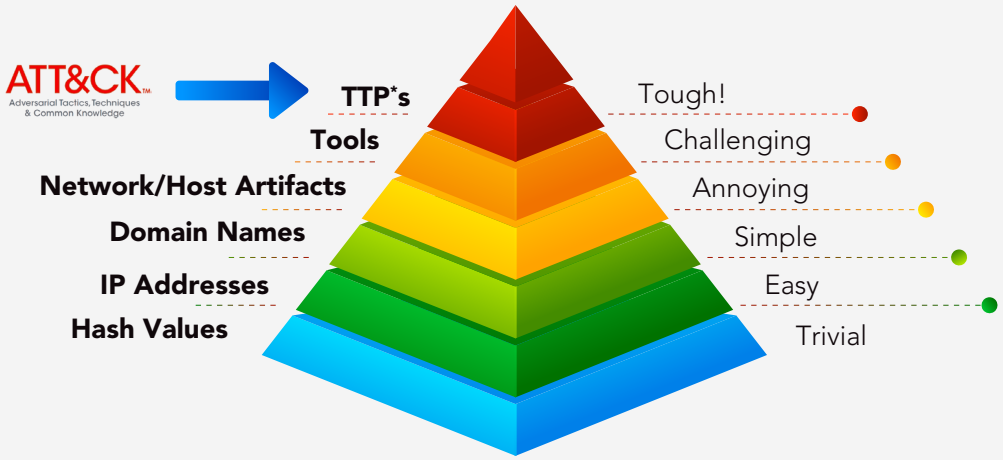
Action on objectives

The final stage includes carrying out the objectives of the cyberattack by gathering, encrypting, and extracting **confidential information.**

- ## Pyramid of Pain

In 2013, David J Bianco came up with the concept of Pyramid of Pain that represents **six types of attack indicators** that the analyst must look out for, to detect the activities of an adversary. The indicators arranged in ascending order represent the amount of pain an adversary needs, to adapt to, pivot and **continue with the attack** even when the indicators at each level are being denied. A threat hunter can employ the different types of indicators of compromise (IOC) illustrated at each level to detect an attacker's activities. While identifying and preventing the **IOCs at each level,** the hash values, IP addresses and domain names can be accessed through commercial threat intelligence feeds; network and host artefacts can be accessed via micro threat intelligence feeds; robust security programs are necessary to detect and prevent threat actor's tools and tactics, techniques, and procedures (TTPs).

Figure 2: Pyramid of pain: Six types of attack indicators



- ## MITRE ATT&CK Framework

MITRE ATT&CK Framework helps threat hunters build contextual threat models and determine the tools and techniques that an attacker can use for a successful attack.

MITRE's Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) is a threat intelligence resource and a knowledge base of attacker's TTP based on real world observations. The framework lists **11 tactics and multitude of techniques** used by threat actors to compromise any network. Threat hunters can leverage this model to build **contextual threat models** and determine the tools and techniques an attacker can use for a successful attack on their organization. It helps hunters broaden their scope of hypothesis, understand attacker's profile and behavior, gather data, and investigate the potential targets of any attack. Each step of the investigation from initial access and execution to exfiltration and command & control, hunters can feed **indicators of compromise** and **indicators of attack** that are relevant to the context of their organization. This helps improve the organization's monitoring and detection capabilities and elevates the overall security posture.

Figure 3: MITRE ATT&CK framework

INITIAL ACCESS	EXECUTION	PERSISTENCE		PRIVILEGE ESCALATION	DEFENSE EVASION	
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Port Monitors	Access Token Manipulation	Access Token Manipulation	Masquerading
Hardware Additions	CMSTP	Accessibility Features	Rc.common	Accessibility Features	BITS Jobs	Modify Registry
Replication Through Removable Media	Command-Line Interface	Account Manipulation	Re-opened Applications	AppCert DLLs	Binary Padding	Mshta
Spearphishing Attachment	Control Panel Items	AppCert DLLs	Redundant Access	AppInit DLLs	Bypass User Account Control	NTFS File Attributes
Spearphishing Link	Dynamic Data Exchange	AppInit DLLs	Registry Run Keys / Startup Folder	Application Shimming	CMSTP	Network Share Connection Removal
Spearphishing via Service	Execution through API	Application Shimming	SIP and Trust Provider Hijacking	Bypass User Account Control	Clear Command History	Obfuscated Files or Information
Supply Chain Compromise	Execution through Module Load	Authentication Package	Scheduled Task	DLL Search Order Hijacking	Code Signing	Plist Modification
Trusted Relationship	Exploitation for Client Execution	BITS Jobs	Screensaver	Dylib Hijacking	Compile After Delivery	Port Knocking
Valid Accounts	Graphical User Interface	Bootkit	Security Support Provider	Exploitation for Privilege Escalation	Compiled HTML File	Process Doppelgänging
	InstallUtil	Browser Extensions	Service Registry Permissions Weakness	Extra Window Memory Injection	Component Firmware	Process Hollowing
	LSASS Driver	Change Default File Association	Setuid and Setgid	File System Permissions Weakness	Component Object Model Hijacking	Process Injection
	Launchctl	Component Firmware	Shortcut Modification	Hooking	Control Panel Items	Redundant Access
	Local Job Scheduling	Component Object Model Hijacking	Startup Items	Image File Execution Options Injection	DCShadow	Regsvcs/Regasm
	Mshta	Create Account	System Firmware	Launch Daemon	DLL Search Order Hijacking	Regsvr32
	PowerShell	DLL Search Order Hijacking	Systemd Service	New Service	DLL Side-Loading	Rootkit
	Regsvcs/Regasm	Dylib Hijacking	Time Providers	Path Interception	Deobfuscate/Decode Files or Information	Rundll32
	Regsvr32	External Remote Services		Plist Modification	Disabling Security Tools	SIP and Trust Provider Hijacking
	Rundll32	File System Permissions Weakness	Valid Accounts	Port Monitors	Execution Guardrails	Scripting
	Scheduled Task	Hidden Files & Directories	Web Shell	Process Injection	Exploitation for Defense Evasion	Signed Binary Proxy Execution
	Scripting	Hooking	Windows Management Instrumentation Event Subscription	SID-History Injection	Extra Window Memory Injection	Signed Script Proxy Execution
	Service Execution	Hypervisor		Scheduled Task	File Deletion	Software Packing
	Signed Binary Proxy Execution	Image File Execution Options Injection	Winlogon Helper DLL	Service Registry Permissions Weakness	File Permissions Modification	Space after Filename
	Signed Script Proxy Execution	Kernel Modules and Extensions		Setuid and Setgid	File System Logical Offsets	Template Injection
	Source	LC_LOAD_DYLIB Addition		Startup Items	Gatekeeper Bypass	Timestomp
	Space after Filename	LSASS Driver		Sudo Caching	Group Policy Modification	Trusted Developer Utilities
	Third-party Software	Launch Agent		Sudo	HISTCONTROL	Valid Accounts
	Trap	Launch Daemon		Valid Accounts	Hidden Files and Directories	Virtualization/Sandbox Evasion
	Trusted Developer Utilities	Launchctl		Web Shell	Hidden Users	Web Service
	User Execution	Local Job Scheduling			Hidden Window	XSL Script Processing
	Windows Management Instrumentation	Login Item			Image File Execution Options Injection	
	Windows Remote Management	Logon Scripts			Indicator Blocking	
	XSL Script Processing	Modify Existing Service			Indicator Removal from Tools	
		Netsh Helper DLL			Indicator Removal on Host	
		New Service			Indirect Command Execution	
		Office Application Startup			Install Root Certificate	
		Path Interception			InstallUtil	
		Plist Modification			LC_MAIN Hijacking	
		Port Knocking			Launchctl	

Figure 3: MITRE ATT&CK framework

CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFILTRATION	COMMAND AND CONTROL
Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Domain Generation Algorithms
Input Capture	Peripheral Device Discovery	Remote Services	Input Capture		Fallback Channels
Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture		Multi-hop Proxy
Keychain	Query Registry	Shared Webroot	Video Capture		Multiband Communication
LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content			Multilayer Encryption
Network Sniffing	Security Software Discovery	Third-party Software			Port Knocking
Password Filter DLL	System Information Discovery	Windows Admin Shares			Remote Access Tools
Private Keys	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
Replication through removable medis	System Network Connections Discovery				Standard Application Layer Protocol
	System Owner/User Discovery				Standard Cryptographic Protocol
Securityd Memory	System Service Discovery				Standard Non-Application Layer Protocol
Two-Factor Authentication Interception	System Time Discovery				Uncommonly Used Port
	Virtualization/Sandbox Evasion				Web Service

Threat hunting techniques

Threat hunting is a human-driven and systematic process that helps reduce breaches, increase speed and accuracy of incident response, and improve security defenses. But there is more than just one way to hunt for threats and fight against adversaries. A few of the most common threat hunting techniques that security teams can use to identify the threats are listed below.

Intel-based hunting

A reactive hunting strategy, intel-based hunting is a technique based on **input sources of intelligence** such as IOCs, IP addresses, hash values and domain names, networks, or host artifacts. These predefined rules can be integrated with SIEM and other threat intelligence tools to observe and inspect the networks and systems. To identify any compromise in the environment, intelligence sharing platforms such as **computer emergency response teams (CERT)** can also be used to export automated alerts and input into the threat hunting tools as structured threat information expression (STIX) or trusted automated exchange of intelligence information (TAXII).

Hypothesis-based hunting

To identify malware attacks and persistent threat groups, hypothesis-based threat hunting technique leverages **MITRE ATT&CK framework** and threat hunting library. Using this proactive approach, threat hunters can identify the threat actors by using IOAs and TTPs, assess its attack behavior to create hypothesis, and monitor the environment to timely detect the anomalies.

Custom hunting

Custom hunting technique is based on situations and can be a combination of both **intel-based** and **hypothesis-based** threat hunting. It is customizable based on the requirements and involves using situational awareness and existing information about the environment.

Threat hunting methodology

An effective threat hunting exercise is an iterative combination of processes, tools and techniques that align with the organization's structure. While there are some basic steps and processes that one can follow for an efficient hunting program, threat hunters still need to think out of the box and **expand their scope** of investigation to ultimately outwit the attackers. A common threat hunting methodology includes:

Ensuring the right information

Just having raw data is not enough to conduct a meaningful hunt. Hunters must use tools that provide a **detailed picture of data** like network traffic patterns, file hashes, system and event logs, user activity, file operations and all other activities.

Defining the normal

Detecting abnormal activities triggered by threat actors becomes easier if threat hunters understand the **baseline normal**. Determining the organization's structure, its framework , business activities and user behaviors helps create hypothesis to investigate anomalies.

Developing a hypothesis

Hypothesis formation and testing includes leveraging tools, frameworks, threat intel and past experiences to quickly **detect the root cause** behind the threats and efficiently respond to them. Some of the widely used threat intelligence include Virus total, IBMM Xforce, and AlianVault.

Analyzing the potential threats

The next step involves discovering malicious patterns in the data cycle and uncovering the **attacker's TTPs** with the help of various tools and techniques. It helps validate the nature, impact, and scope of the generated hypothesis.

Responding to the threats

After uncovering any anomaly, it is essential to neutralize the threat with **rapid response and remediation.** In addition to protecting the system from a perceived threat, hunters must initiate measures that help prevent similar attacks in the future as well.

Automating routine tasks

The last step includes using the discoveries made during an investigation to form a basis for **automated analytics.** This improves EDR systems and helps analyze future incidents more effectively, compared to the knowledge base generated.

Challenges of threat hunting

Threat hunting is a time-consuming affair and requires around the clock monitoring along with **cybersecurity expertise.** In addition to being a time-consuming effort, lack of adequate budgets also restricts organizations from having an effective threat hunting platform. Some of the common challenges of carrying out threat hunting are mentioned below.

Human capital

Cyber threat hunting requires expert threat hunters capable of identifying the indicators of **sophisticated attacks** at a very early stage to prevent an organization from getting breached. As cybersecurity skills gap widens impacting over **57% of organizations**[II] worldwide, deploying the right workforce for the exercise becomes a part of the challenge.

Data collection

Access to both current and historical data is a key component of initiating a hunt. Missing any crucial information can lead to **lack of informed hypothesis** based on network, endpoints, or cloud infrastructure.

Latest threat intelligence

Threat hunters must stay abreast with threat intelligence to analyze IOCs and protect their organization's network, data, users and reputation from evolving adversaries. Additionally, the platform used must be capable of integrating the **latest intelligence** to develop meaningful attack hypothesis. With outdated knowledge, analyzing potential network threats can become a challenging task.

Future of threat hunting

Proactive solutions like threat hunting have proven their effectiveness amidst an exponential increase in the attack surface. The uptick in adoption is expected to continue in the coming years.

Industries across the globe are caught up in a whirlwind of massive **technological innovation** on the one hand and **exponential growth of data** on the other. As the attack surface widens at a rapid pace, it is likely to open multiple gateways for threat actors to breach networks and exploit unpatched vulnerabilities. Over the years, this **high-speed evolution** has prompted organizations to use proactive solutions like threat hunting due to its proven effectiveness. This trend is likely to continue in the coming years.

However, as we progress forward, relying only on **terabytes of threat intel** information and manual analysis of anomalies could prove to be exhausting for threat hunters. Moreover, emerging sophisticated attack vectors that are familiar with widely used **simplistic rules and analytics,** may also render most threat hunting programs less effective. It is crucial for organizations to equip threat hunting teams with advanced tools that leverage **AI and ML** algorithms to identify anomalies, and outwit evolving attack techniques used by hackers.

SISA ProACT and threat hunting

SISA ProAct, a **Forensics-driven MDR solution** is an end-to-end platform combining intuitive security analytics dashboards, scalable virtual appliances, and a proprietary all-in-one agent. It provides an integrated monitoring platform and a unified incident response solution to help organizations strengthen their cybersecurity posture. **SISA ProACT,** enabled by SISA's in-house developed machine learning algorithm, provides a comprehensive approach to reduce the false positives and relieves enterprises from alert fatigue situations.

A scalable solution that supports all platforms and deployment architectures including on-premises, cloud, co-location, and hybrid cloud deployments, SISA's MDR solution facilitates **faster integration** with enterprise network components and scales rapidly to help enterprises accelerate time to value. Some of the key differentiators of SISA ProACT are as follows:

Complete visibility into all malicious activities with **real-time situational awareness** for cyber-resilience.

Aggregation and monitoring of logs with SISA's proprietary **all-In-one agent** for preventive incident response of cyber threats.

Real-time data collection and historical analysis of security events from a wide range of **dynamic and contextual data sources**.

Inputs from **forensics engagements** converted into detection use cases and threat hunting hypothesis.

Intuitive navigation systems for incidents, exposures, health, and endpoint reports.

Combination of people, application layers, and IT infrastructure on one platform for a better **threat visibility.**

1,100+ SIEM use cases in library aligned with **MITRE ATT&CK** framework and Sigma open standards.

For a deeper understanding of how **SISA ProACT** can help you efficiently prevent, detect, and respond to cyber threats, **request a call** and we will connect you with **SISA's forensics experts.**

References:

1. https://www.infosecurity-magazine.com/news/data-breaches-rise-by-70-q3-2022/
2. https://venturebeat.com/security/studies-show-cybersecurity-skills-gap-is-widening-as-the-cost-of-breaches-rises/
3. https://attack.mitre.org/
4. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
5. https://www.sans.org/tools/the-pyramid-of-pain/

SISA INFORMATION SECURITY

SISA is a forensics-driven cybersecurity company, with offices across the globe and is trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective security services, and solutions.

1,000+ ACTIVE ENGAGEMENTS

40+ COUNTRIES

2,000+ GLOBAL CUSTOMERS SERVED

Our Offerings

Compliance

PCI Compliance

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ

Risk & Compliance

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Swift
- Cloud Security
- Risk Assessment
- Quarterly Security Audit

Security Testing

Application Security

- Application Penetration Testing
- CREST/CERT-in Approved Security Testing
- API Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- ASV Scan

IoT Security Testing

Managed Security Services

Phishing Simulation

Cyber Resilience

Managed Detection and Response Solution - SISA ProACT

Incident Response and Forensics

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation

Advanced Threat Hunting

Data Protection

Data Discovery and Classification Tool - SISA Radar

- Card Data Discovery
- PII (Privacy) Data Discovery
- Data Classification

Data Discovery as a Service

Training

Payment Data Security Implementation Programs

- CPISI
- CPISI Advanced

Security Incident Detection and Response Programs

- CIDR

Forensic Learning Sessions for Senior Management

To learn more about SISA's offerings visit us at

www.sisainfosec.com

contact@sisainfosec.com