Volume 11, Issue 8, August – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

Integrated Threat Hunting and SOAR Workflow for Autonomous Cybersecurity Operations

Ekangwo Hernadez Ebolo[1]; Kum Bertrand Kum[1];
Tagne Poupi Theodore Armand[2]; Austin Oguejiofor Amaechi[3*]

[1]The ICT University, Cameroon
[2]POEM Digital Intelligence Lab, Cameroon
[3]ISD, University College, London

Corresponding Author: Austin Oguejiofor Amaechi[3*]

Publication Date: 2026/08/21

Abstract: The cyber-security ecosystem has undergone a paradigm shift, moving from opportunistic, automated malware attacks to targeted, human-operated campaigns known as Advanced Persistent Threats (APTs). These threats, characterized by their stealth, persistence, and adaptability, frequently evade traditional perimeter defenses such as vulnerability assessment and penetration testing (VAPT) security information and event management (SIEM), firewalls, anti-spam/anti-malware solutions and system patches. This paper provides analysis of the modern threat landscape, and evaluates the efficacy of established frameworks, including NIST, ISO/IEC 27001, and MITRE ATT&CK in the face of these evolving dangers. It argues that while compliance-based frameworks provide a necessary governance foundation, they are insufficient without the integration of proactive strategies like Threat Hunting and Threat Intelligence. In this paper, we present the *Integrated Threat Hunting and Security Orchestration, Automation and Response (SOAR) Automation Workflow (THSAW)* highlighting the necessity of shifting from a reactive "alert-driven" posture to a proactive "hunt-driven" methodology to ensure organizational resilience. Using a design science paradigm, we describe the solution design rationale and artifact development. The proactive approach can be used to develop the offensive security-aware environment for organizations to uncover advanced attack mechanisms and test their ability for attack detection. Experimental results demonstrate the workflow's effectiveness in autonomous threat detection, behavioral analysis, and automated incident response.

Keywords: *Cyber-Security, Advanced Persistent Threats (APTs), Threat Hunting, Security Operations Center (SOC), MITRE ATT&CK, Cyber Kill Chain, Threat Intelligence.*

How to Cite: Ekangwo Hernadez Ebolo; Kum Bertrand Kum; Tagne Poupi Theodore Armand; Austin Oguejiofor Amaechi (2026) Integrated Threat Hunting and SOAR Workflow for Autonomous Cybersecurity Operations. *International Journal of Innovative Science and Research Technology*, 11(8), 1283-1296. https://doi.org/10.38124/ijisrt/26aug526

I. INTRODUCTION

In the contemporary digital ecosystem, information has become the most valuable currency. The rapid integration of cloud computing, Internet of Things (IoT), and interconnected enterprise networks has created an attack surface of unprecedented scale (Kintis et al., 2017; Almutairi, & Sheldon, 2025; Singh et al., 2016). Consequently, cyber-security is no longer a peripheral IT concern but a core pillar of national security and economic stability.

Despite massive investments in defensive technologies, firewalls, Intrusion Detection Systems (IDS), and Endpoint Protection Platforms (EPP) which rely on signatures (known patterns of malicious code) to detect threats, organizations continue to suffer catastrophic breaches. Historically, cyber-attacks were often the work of isolated individuals ("script kiddies") seeking notoriety or minor financial gain. However, the landscape has matured into a domain of warfare and high-stakes espionage. Today's adversaries are organized, well-funded, and often state sponsored. They employ military-grade strategies to infiltrate critical infrastructure, financial systems, and government networks. The emergence of Advanced Persistent Threats (APTs) represents the apex of this evolution (Alshamrani et al., 2019). Unlike traditional "smash-and-grab" attacks, APTs are designed for long-term residency within a victim's network, allowing attackers to exfiltrate sensitive data over months or years without detection. Traditional security measures often fall short against these threats because they rely on 'known signatures,' whereas APTs constantly modify their Tactics, Techniques, and Procedures (CrowdStrike, 2024). The 2024 Global Threat Report identified over 230 active adversaries and reported the fastest eCrime breakout time recorded at just 2 min and 7 s in 2023. According to the report, this underscores the pressing need for rapid detection and response capabilities to mitigate

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

these swift intrusions. The report highlights a significant rise in covert cyber activities, with substantial increases in data theft, cloud breaches, and malware-free attacks. These trends indicate that adversaries are continuously evolving and adapting despite advancements in detection technologies (CrowdStrike, 2024). APTs utilize "Zero-Day" exploits (vulnerabilities unknown to vendors) and "Living off the Land" (LotL) techniques, where legitimate system tools like PowerShell are used for malicious purposes (Barr-Smith et al., 2021). As a result, the "dwell time", the time between a breach and its discovery, remains unacceptably high, often averaging over 200 days (Rahman, 2024). This paper posits that to close this gap, the industry must pivot from passive reliance on frameworks to active, intelligence-driven threat hunting. According to Ashby's Law of Requisite Variety, a system must match the complexity of its environment to remain viable (Ashby, 1970). In human organizations, this regulatory capacity is enacted through self-organizing mechanisms that structure and coordinate behavior (Stafford Beer, 1981). Based on this perspective, this study explores three core questions:

- *RQ1: What are the primary limitations of compliance-based security frameworks (for instance, NIST, ISO/IEC 27001) in mitigating the risks posed by modern Advanced Persistent Threats (APTs)?*
- *RQ2: How can a unified workflow integrating Threat Hunting, Cyber Threat Intelligence (CTI), and SOAR be architected into a Threat Hunting and SOAR Automation Workflow (THSAW) to bridge the detection gaps inherent in traditional* Security Operations Center *(SOC) models?*
- *RQ3: To what extent does the implementation of the THSAW artifact improve an organization's operational resilience, specifically regarding the acceleration of detection rule generation and the reduction of Mean Time to Respond (MTTR)?*

II. BACKGROUND AND RELATED WORK

The literature review was conducted across a defined search scope focusing on the evolution of cyber-security defenses against Advanced Persistent Threats (APTs) and the necessity of shifting from compliance-based governance to proactive security operations. Sources were selected from a range of authoritative materials, primarily peer-reviewed academic journals, major industry threat reports (e.g., CrowdStrike), and foundational framework documentation (e.g., NIST, MITRE). To support the claim of the analysis, literature was chosen based on its direct relevance to operational execution, empirical data regarding detection efficacy, and its focus on the behavioral tactics and procedures (TTPs) of modern adversaries, contrasting technical limitations with governance structures. In addition, a SOC does not have a universally accepted precise definition and components (Vielberth et al., 2020). While some researchers have interpreted SOC as solely an entity responsible for monitoring the network, others see it as an organizational unit encompassing all security operations, such as incident management and threat intelligence, and some others see SOCs as typically responsible for detecting security incidents and responding to them through various measures Consequently, the term SOC can refer to a wide range of configurations. In some organizations, a SOC may consist of a small team of two to three individuals responsible for information security monitoring, maintenance, and development. In systematic review paper, Mahboubi et al (2024) provided a detailed analysis of the current state and future directions of threat hunting. The systematic review emphasized the importance of hypothesis-driven approaches and iterative detection methodologies. In another recent study, Maciel Paz Milani, Anderson, & Storey (2026) proposes six design heuristics that form a solution-evaluation framework for assessing cognitive support in threat hunting tools.

Cyber-Security

Cyber-security is a "complex dynamic field, and the production of cyber-security is a knowledge-intensive task" (Amaechi, 2025) and "is defined as the protection against unwanted attacks, harm, or transformation of data in a system and also the safety of systems themselves" (Kuhl et al., 2007). It is concerned with the security and privacy of digital assets, including networks, computers, and data that are processed, stored, and transferred via Internet-based information systems, according to ISACA. The Worldwide Telecommunications Union defines cyber-security as the set of methods, guidelines, protocols, best practices, and procedures used to safeguard users' online assets and organizations (Farraj, Hammad, & Kundur, 2017). Cyber-security may be viewed as a defense against unwanted access to the assets of people and organizations. Threats, attacks and human behavior are key tripod or core pillar structure of modern cyber-security (Amaechi, 2025). Threats are the kinds of things done to take advantage of security weaknesses in an infrastructure and make it worse. Attacks are the steps taken to use different tools and techniques to attack vulnerabilities in a system to harm it or interfere with its regular operations. Attackers carry out these attacks to fulfill their malevolent objectives, which may include monetary gain or self-gratification. To anticipate future threats, it's crucial to understand where the highest risks may lie.

Anatomy of the Modern Threat Landscape

Cyber-security means understanding your systems and processes, your personnel's capabilities and limitations, as well as thoroughly evaluating your threat landscape (Jorgensen and Kevin, 2018). To design effective defenses, one must first deconstruct the adversary. A "cyber threat" encompasses any malicious act that attempts to gain unauthorized access to data, disrupt digital operations, or damage information. Modern threats, particularly in the context of cyber-security and digital infrastructure, can be broadly categorized into several key areas based on their methods, targets, and motivations.

- Malware (Malicious Software): This remains the most pervasive tool in the attacker's arsenal. It includes viruses, worms, and trojans. However, the delivery mechanisms have evolved. Modern malware is often polymorphic, changing its code signature with every infection to evade antivirus detection.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

- Ransomware: A specific and highly destructive form of malware. Ransomware encrypts user data and demands payment for the decryption key. The evolution of "Double Extortion" ransomware involves attackers not only encrypting data but also stealing it, threatening to leak sensitive information if the ransom is not paid. High-profile incidents, such as the Colonial Pipeline attack, demonstrate the kinetic impact of these digital threats on physical infrastructure.
- Phishing and Social Engineering: Despite technical advancements, the human element remains the weakest link. Phishing involves fraudulent communications designed to deceive users into revealing credentials or installing malware. "Spear Phishing" targets specific individuals with highly customized messages, often achieving success rates where technical exploits fail.
- Distributed Denial of Service (DDoS): These attacks aim to overwhelm a target's resources, rendering it inaccessible. The rise of insecure IoT devices has fueled the creation of massive botnets (e.g., Mirai), capable of launching terabit-scale attacks.
- Insider Threats: Perhaps the most difficult threat to detect, insider threats originate from authorized users. Whether malicious (corporate espionage) or negligent (falling for a phishing scam), insiders bypass the perimeter defenses that most organizations rely on.

➢ *Understanding Advanced Persistent Threats (APTs)*

The term “advanced persistent threat" was coined by the United States Air Force in 2006 to describe complex cyberattacks targeting national security. An APT is a stealth threat actor that obtains unauthorised access to a device network (Alshamrani et al., 2018). An APT attack is sophisticated and tailored to the target's vulnerabilities. An APT is defined by three key characteristics:

- Advanced: The adversary possesses sophisticated technical capabilities, often developing custom malware and zero-day exploits.
- Persistent: The objective is not immediate disruption but sustained access. If one entry point is blocked, the attacker attempts others until successful.
- Threat: The attack is executed by a coordinated human team with a specific objective, rather than automated, indiscriminate code (Alshamrani et al., 2019).

APT attacks are multi-stage, stealthy campaigns designed to gain long-term access to a network (Salim, Singh & Keikhosrokiani, 2023). They typically follow five to seven stages: reconnaissance, initial infiltration, establishing a foothold (persistence), lateral movement/privilege escalation, and finally, data exfiltration while avoiding detection. APT attackers differ based on the intent or motive of their attack. The limitations and realities of modern defense against APTs have been discussed in the literature (Salim, Singh & Keikhosrokiani, 2023).

➢ *Critical Evaluation of Threat modelling (TM)*

The objective of TM is the ability to identify, classify, and describe threats that reveal an assailant or a campaign of attacks. Many cyber-security frameworks have been defined for easy analysis of threat modelling. Frameworks provide the structural scaffolding for an organization's security posture. They offer a "common language" for discussing risk and compliance. In this section, we analyze selected approaches or frameworks, including the Cyber Kill Chain model; MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework; the National Institute of Standards and Technology (NIST) guidelines; and ISO/IEC 27001.

- *NIST Cyber-Security Framework (CSF):*

Developed by the US National Institute of Standards and Technology, the NIST CSF is arguably the most widely adopted framework for critical infrastructure. It discusses a four-step qualitative methodology for threat modelling (Souppaya and Scarfone, 2016). It organizes security activities into five concurrent and continuous functions:

- ✓ Identify: Understanding the cyber-security risks to systems, assets, data, and capabilities. (e.g., Asset Management, Risk Assessment).
- ✓ Protect: Outlining safeguards to ensure delivery of critical infrastructure services. (e.g., Access Control, Awareness Training).
- ✓ Detect: Defining the appropriate activities to identify the occurrence of a cyber-security event.
- ✓ Respond: Taking action regarding a detected cyber-security incident.
- ✓ Recover: Maintaining plans for resilience and restoring capabilities after a breach (NIST, 2018).

In our opinion, NIST is excellent for strategic communication with C-suite executives and board members. However, it lacks the tactical granularity required for a SOC analyst. Telling an analyst to "Detect Anomalies" (NIST Subcategory DE.AE) does not explain how to detect a specific Golden Ticket attack.

- *ISO/IEC 27001:*

ISO/IEC 27001 is the international standard for Information Security Management Systems (ISMS) (Disterer, 2013). It adopts a process-based approach using the Plan-Do-Check-Act (PDCA) cycle. *While ISO 27001 is a compliance heavyweight as it ensures that policies, procedures, and legal requirements are met. However, it is often criticized for being "document centric." An organization can be fully ISO 27001 compliant having perfect policies on paper while still being technically vulnerable to a sophisticated APT due to poor operational execution.*

- *The Cyber Kill Chain:*

Developed by Lockheed Martin, the Cyber Kill Chain model revolutionized security by breaking an attack down into linear stages (Hutchins et al., 2011). According to Tatam et al (2021) it refers to the sequence of events during an attack, and the goal is to defend against or exploit the opponent's attacks as they go through their different stages of life (Lockheed Martin, 2015). This allows defenders to focus on breaking the chain at any point to stop the attack. Core features include:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

- ✓ Reconnaissance: The attacker selects targets and gathers intelligence (e.g., harvesting email addresses).
- ✓ Weaponization: Coupling a remote access trojan with a deliverable file (e.g., a PDF).
- ✓ Delivery: Transmitting the weapon to the target (e.g., via email attachment).
- ✓ Exploitation: Triggering the weapon's code by exploiting a vulnerability.
- ✓ Installation: Installing the malware on the asset.
- ✓ Command and Control (C2): Establishing a channel for the attacker to control the victim.
- ✓ Actions on Objectives: The attacker achieves their goal (e.g., data exfiltration).

It is the opinion of this study that while foundational, the Kill Chain is often viewed as too rigid for modern threats. It focuses heavily on perimeter defense (stopping the "Delivery"). Once an attacker is inside (past step 4), the Kill Chain offers less guidance on lateral movement within the network.

- *MITRE ATT&CK:*

The Operational Standard: While the Cyber Kill Chain provides a linear model of intrusion, it fails to capture the non-linear, adaptive nature of modern APTs. The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework addresses this gap by providing a comprehensive matrix of adversary behaviors. Unlike NIST (which focuses on *what to do*) or the Kill Chain (which focuses on *when* it happens), MITRE ATT&CK focuses on how it happens (MITRE, 2023). It is structured into three layers:

- ✓ Tactics: The adversary's technical goal (e.g., "Credential Access" or "Lateral Movement").
- ✓ Techniques: The specific method used to achieve the goal (e.g., "OS Credential Dumping").
- ✓ Procedures: The specific implementation or tool used (e.g., using Mimikatz to dump LSA secrets).

The superiority of MITRE ATT&CK lies in its granularity. For instance, where the Cyber Kill Chain might simply label an event as "Exploitation," MITRE ATT&CK breaks this down into specific sub-techniques (e.g., T1068: Exploitation for Privilege Escalation). This allows SOC analysts to map specific alerts to broader campaigns, moving from a signature-based approach ("We found a virus") to a behavioral approach ("We are seeing T1059.001 usage consistent with APT29").

➢ *Case Studies in Modern Cyber Warfare*

To fully appreciate the inadequacy of traditional frameworks, we analyze specific incidents where these frameworks failed to prevent catastrophic breaches. This section deconstructs two landmark events, the SolarWinds Supply Chain Attack and the Colonial Pipeline Ransomware Incident, through the lens of the MITRE ATT&CK framework.

- *The SolarWinds Orion Supply Chain Attack (2020)*

The SolarWinds compromise, attributed to the Russian APT group APT29 (Cozy Bear), represents a watershed moment in cyber-security history. It demonstrated that even the most secure organizations (including the US Department of Homeland Security and FireEye) are vulnerable if their trusted vendors are compromised.

- ✓ Attack Vector (T1195.002): The attackers did not target the victims directly. Instead, they compromised the build environment of SolarWinds, a software vendor used by 33,000 organizations. They injected a malicious backdoor, known as *SUNBURST*, into a legitimate software update (SolarWinds.Orion.Core.BusinessLayer.dll).
- ✓ Defense Evasion (T1027): The malware remained dormant for 12-14 days before executing (a technique to bypass sandbox analysis). Once active, it mimicked legitimate network traffic using the Orion Improvement Program (OIP) protocol to blend in with normal administrative noise.
- ✓ Operational Impact: This attack highlighted a critical blind spot in the NIST "Protect" function. Most organizations whitelisted SolarWinds software because it was a "trusted" security tool. The breach proved that "Implicit Trust" is a fatal flaw in modern network architecture, accelerating the global shift toward Zero Trust Architecture (ZTA).

- *The Colonial Pipeline Ransomware Incident (Srinivasan and Li-Kuan, 2023)*

- ✓ While SolarWinds was a masterclass in espionage, the Colonial Pipeline attack by the DarkSide criminal group illustrated the kinetic impact of cyberattacks on physical infrastructure (Cyber-Physical Systems).
- ✓ Initial Access (T1078): The attackers gained entry via a single compromised Virtual Private Network (VPN) password that had no Multi-Factor Authentication (MFA) enabled. This rudimentary failure occurred despite the organization likely adhering to basic compliance standards on paper.
- ✓ Impact (T1486): The ransomware encrypted IT systems used for billing. Although the Operational Technology (OT) systems controlling the pipeline were not infected, the company shut them down as a precaution to prevent lateral movement. This resulted in a shutdown of 45% of the US East Coast's fuel supply.
- ✓ Strategic Analysis: This incident exposed the fragility of the IT/OT Convergence. Traditional SOCs often monitor IT networks (email, web traffic) but lack visibility into OT networks (SCADA systems, PLCs). An effective Threat Hunting program must bridge this gap, correlating anomalies I n business networks with potential threats to industrial control systems.

The escalating complexity of the modern threat landscape has exposed the critical limitations of reactive, signature-based security models. CrowdStrike (2025) argue that relying solely on alert-driven mechanisms leaves organizations vulnerable to "living-off-the-land" attacks

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

where adversaries utilize legitimate system tools to evade detection. This "detection gap" has necessitated a paradigm shift toward Threat Hunting, a proactive methodology defined by (Bianco, 2015) in the *SANS Institute's Hunting Maturity Model* as "the process of iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions." However, Chatziamanetoglou and Rantos (2024) note that manual hunting is resource-intensive and unscalable without a structured framework. Their research in the *IGI Global Handbook* emphasizes that to transition from "ad-hoc" hunting to "integrated" defense, organizations must operationalize intelligence rather than simply consume it.

To fuel this proactive search, Cyber Threat Intelligence (CTI) acts as the foundational layer, providing the necessary context to distinguish malicious behavior from benign anomalies. (Sarker, 2024) posits that CTI must evolve from static indicators (IPs, Hashes) to behavioral intelligence. However, the ingestion of CTI creates its own challenges. Ontologies exist for the standardization of CTI (Tounsi and Rais, 2018), thus, for CTI to be effective, it must be normalized and mapped to a common ontology before it reaches the analyst, otherwise, the "signal-to-noise" ratio becomes too low for effective decision-making.

To solve the normalization challenge, the MITRE ATT&CK framework has emerged as the global standard for mapping adversary behaviors (TTPs). Rahman and Williams (2022) in their study concluded that MITRE ATT&CK provides the "common language" required to translate abstract CTI into concrete hunting hypotheses. By focusing on *Techniques* (e.g., T1003 - OS Credential Dumping) rather than just *Tools*, defenders can build resilient detection logic that survives changes in attacker infrastructure (Jiang et al., 2025). Recent empirical research by Mgbemele (2026) demonstrates that aligning detection engineering with MITRE ATT&CK yields measurable operational improvements, including a 40 - 65% increase in detection accuracy.

Despite the theoretical alignment of CTI and MITRE ATT&CK, the practical execution of hunting campaigns is often bottlenecked by manual processes. Al-Husain et al. (2021) identify "human latency" as the primary weakness in modern SOCs, noting that the time required to manually query SIEM logs for a hypothesis allows attackers to dwell in the network for extended periods. This has driven the adoption of Security Orchestration, Automation, and Response (SOAR). French (2024), in a study on *Hyper-Automation*, proposes that SOAR should not just be a response tool, but an "investigation engine." By automating the data collection phase of the hunt, pulling logs, enriching IPs, and running preliminary queries, SOAR allows analysts to focus purely on the "verdict" phase, effectively utilizing what (Paul-Arthur, Mindflow, 2023) describes as "Intelligence-Driven Automation."

The convergence of these four pillars, CTI, Hunting, MITRE ATT&CK, and SOAR, forms the basis of the "New Face of Cyber-security." (Tim Abdiukov, 2024) presents a unified model in the *Well Testing Journal* (Cyber-security Section), arguing that the future of detection lies in "closed loop" systems as intelligence feeds directly into automated hunting playbooks. This integrated workflow is further supported by (Kummarapurugu**,** 2024), who proposes an architectural framework where SOAR platforms act as the execution layer for MITRE-based hypotheses. This synthesis of technologies transforms threat hunting from an episodic, human-dependent activity into a continuous, machine-speed operation, addressing the scalability challenges identified by NetWitness (2025) and ensuring defenses evolve as rapidly as the threats they face.

➢ *The Paradigm Shift: Threat Hunting & Intelligence*

Findings from the literature review shows that threat hunters deploy various approaches, often mixing them and those in the know argues that flexibility in their approach helps them identify subtle threat indicators that might otherwise go undetected if using only one method (Badva et al., 2024). The core challenges in threat hunting ranges from technical challenges to people and organizational culture challenges. The failure of automated defenses to stop APTs has necessitated a shift toward "Active Defense." This paradigm assumes that the network is *already compromised* and that relying on alerts is insufficient. To further situate our study, we looked at the paradigm shift under these three categories: *Threat Hunting: Beyond the Alert, Threat Intelligence (TI): The Fuel for the Hunt, and Integrating Security Orchestration, Automation, and Response (SOAR) platforms.*

- *Threat Hunting: Beyond the Alert:*

Threat Hunting is the proactive, iterative process of searching through networks to detect and isolate advanced threats that evade existing security solutions (Bianco, 2015; Gunter, & Seitz, 2018). Unlike traditional incident response, which is *reactive* (triggered by an alarm), threat hunting is *proactive* (triggered by a hypothesis). Threat hunting methods can be**:**

✓ Hypothesis-Driven Hunting (Alghanmi et al., 2025): The hunt begins with a specific question derived from threat intelligence. *Example:* "If APT34 is targeting the energy sector using DNS tunneling (T1071), do we see high-volume DNS traffic to unknown domains in our logs?"
✓ Data-Driven (Anomaly) Hunting (Costa-Gazcón, 2021): This approach relies on Machine Learning (ML) and statistical analysis to identify deviations from the norm. *Example:* "User 'Ebolo' normally logs in from Douala, Cameroon, between 9 AM and 5 PM. Why is his account accessing the payroll server from an IP address in the Ivory Coast at 3 AM?"

Figure 1 shows a circular cycle diagram showing the phases: Establishing hypothesis> Establishing Evidence> Identify sources> Identify Fields> Query Data> Analyze Data. This illustrates that Threat Hunting *is a continuous process, not a one-time feed.*

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

Fig 1 The Threat Hunting Lifecycle

- *Threat Intelligence (TI): The Fuel for the Hunt:*

Threat Hunting cannot function in a vacuum; it requires actionable intelligence. “Threat Intelligence Sharing Platforms” is a solution created to exchange information and knowledge regarding vulnerabilities, threats, incidents and mitigation strategies in order to collectively protect against today’s sophisticated cyberattacks (Sauerwein et al., 2017). Figure 2 *shows circular cycle diagram illustrating the different the phases: Planning > Collection > Processing > Analysis > Dissemination > Feedback. The illustration shows that TI is a continuous process, not a one-time feed.* TI is categorized into three levels:

- ✓ Strategic Intelligence: High-level information consumed by C-level executives. It focuses on the "Who" and "Why." (e.g., "Nation-state actors are targeting our intellectual property to bypass R&D costs.")
- ✓ Operational Intelligence: Information about specific campaigns. It focuses on the "How." (e.g., "The adversary is using a specific strain of ransomware delivered via HR-themed phishing emails.")
- ✓ Tactical Intelligence: Technical indicators consumed by SIEMs and firewalls. It focuses on the "What." (e.g., "Block IP address 192.168.x.x and file hash MD5: 5e884...").

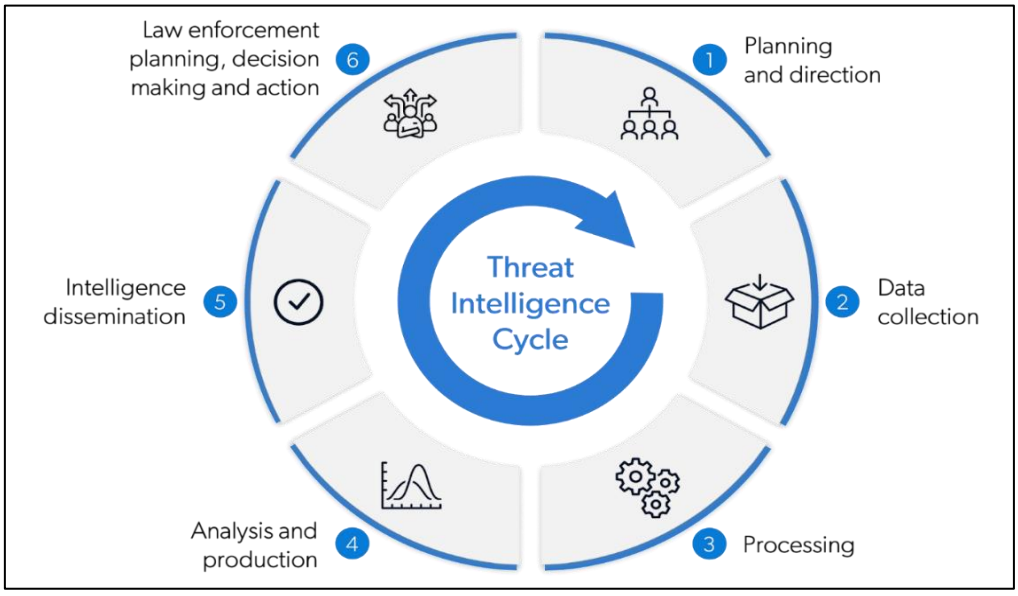

Fig 2 The Threat Intelligence Lifecycle (Adapted from https://www.silobreaker.com/glossary/threat-intelligence-lifecycle/)

- *Integrating Security Orchestration, Automation, and Response (SOAR) Platforms:*

The volume of data generated by modern networks, often terabytes of logs per day, makes manual hunting unsustainable (Chuvakin et al., 2013). Security Orchestration, Automation, and Response (SOAR) platforms bridge this gap. SOAR tools ingest alerts from the SIEM and automatically execute "Playbooks."

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

✓ *Case Example:* If a SIEM detects a "Brute Force" attempt (T1110), a SOAR playbook can automatically: (1) Block the IP at the firewall, (2) Disable the user account in Active Directory, and (3) Open a ticket for an analyst to review. This reduces the "Mean Time to Respond" (MTTR) from hours to seconds.

III. RESEARCH METHODOLOGY

Our research follows a design science paradigm illustrated in (Per Runeson, Engström and Storey, 2020), which emphasizes the creation and iterative refinement of an artifact to address a well-defined practical problem while contributing to theoretical understanding. In our case, the artifact - Integrated Threat Hunting and SOAR Automation Workflow (THSAW) - was developed to support threat hunters. The design science research process adopted in this work can be summarized through three interrelated activities: problem conceptualization, solution design, and empirical validation. The inquiry was conducted within a real-world organizational setting - a private cyber-security consulting company with approximately 10 employees. The implementation details for the THSAW artifact within this organizational setting were formalized across four key dimensions:

➢ *Data Sources:*

The THSAW ingests two primary data streams: Threat Intelligence Feeds from *Yeti, OpenCTI, and MISP*, which provide external Indicators of Compromise (IOCs) and threat reports, and the MITRE ATTACK Knowledge Base, which supplies structured adversarial Tactics, Techniques, and Procedures (TTPs). These feeds are combined with internal operational data, including SIEM logs ingested from ((Windows, Linux, macOS) servers and user systems, switches, and routers) for centralized event correlation and EDR telemetry for detailed endpoint process execution and behavioral analysis.

➢ *Security Tools:*

The THSAW utilizes an integrated stack centered on three platforms: a specialized Threat Hunting Platform that serves as the analyst workbench for hypothesis generation and querying; a SOAR Platform (n8n and shuffle) that acts as the automation engine for executing playbooks; and the existing SIEM/XDR(Wazuh) infrastructure, where new, validated detection rules are deployed.

➢ *Analyst Roles:*

Due to the organizational size, three cross-functional roles were established to manage the workflow: *The Threat Hunter* generates and validates hypotheses, translating abstract intelligence into actionable queries. *The CTI Analyst* is responsible for normalizing and mapping threat intelligence to the MITRE ATT&CK ontology. *The SOAR Engineer* is tasked with developing and maintaining the automated playbooks for response and detection deployment.

➢ *Evaluation Steps:*

Initial empirical validation focused on measuring the efficacy of the automated closed-loop system. Key steps included Hypothesis Query Testing to confirm the platform's ability to uncover hidden malicious patterns; Playbook Operationalization, ensuring SOAR successfully pushes new detection rules to the SIEM/XDR; and the observation of a reduced Mean Time to Respond (MTTR), as SOAR automates manual data collection tasks.

IV. RESULTS - WORKFLOW AND EMPIRICAL EVALUATION OF THSAW

➢ *Architecture and Operational Mechanics of THSAW*

Cyber-security increasingly relies on threat hunters to proactively identify adversarial activity. As noted in the Nour et al. study, cyber threat hunting methodologies have experienced significant evolution, transitioning from manual procedures to encompassing automated techniques (Nour et al., 2023). Todays' cyber-security adversary behaviors are known to adapts to economic, societal, political, and technological circumstances taking advantage of any vulnerability, gap or deficiency of both digital infrastructures and human operators. As a result, information security needs to grow and evolve proportionally. Building on our field experience and prior studies that examined how threat hunters construct and share mental models during investigations, this paper proposes a flexible threat hunting method or workflow (Figure 3) called *Integrated Threat Hunting and SOAR Automation Workflow (THSAW).*

As shown in Figure 3, the block flow diagram shows the progression of data: from the Threat Intelligence and MITRE ATT&CK Framework to the Threat Hunting Platform (Hypothesis Generation) to the SOAR Platform (Automation & Playbooks) to the Automated Detections and Incident Response which feeds the Feedback Loop. The illustration indicate how abstract intelligence is transformed into proactive hypotheses, which are then operationalized and scaled through SOAR to creating a continuous, closed-loop defense system. The solution aligned with the view that automation will not remove the need for human oversight. Threat hunting may be triggered by events detected by security analysts or unknown malicious behaviour or cyber threat intelligence in the input data (resulting from behavior, intent, and alerts).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

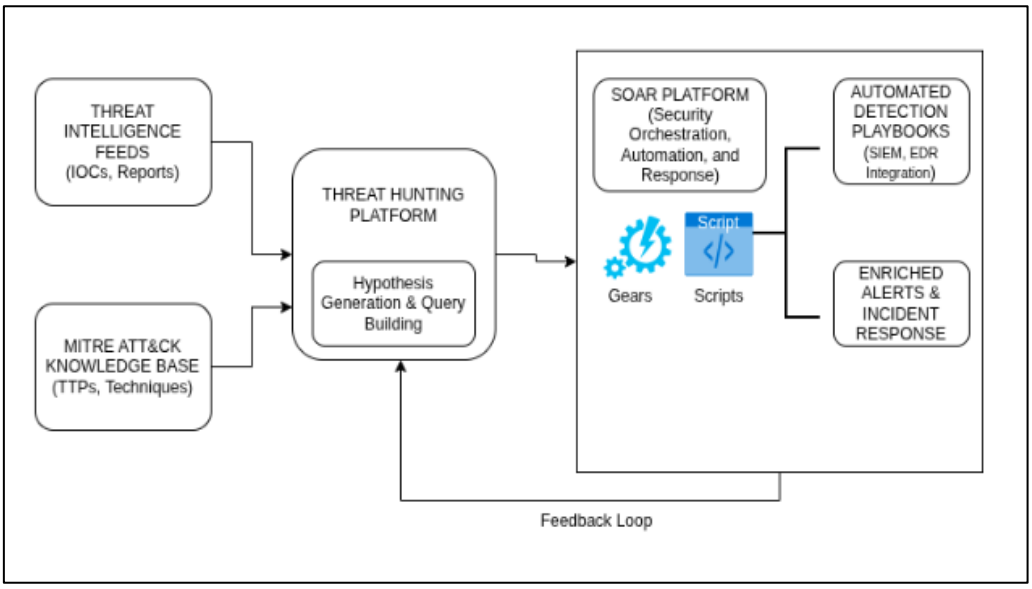

Fig 3 Integrated Threat Hunting and SOAR Automation Workflow (THSAW)

The architecture of the integrated threat hunting and SOAR automation workflow represents a critical shift from reactive incident response to proactive, intelligence-driven cyber-security. The process begins with the ingestion of two foundational data streams: Threat Intelligence Feeds and the MITRE ATTACK Knowledge Base. Threat intelligence provides the tactical "what" by supplying known Indicators of Compromise (IOCs) and external threat reports, while the MITRE ATT&CK framework provides the behavioral "how" by detailing the specific Tactics, Techniques, and Procedures (TTPs) utilized by adversaries.

These data streams feed directly into the core engine of the system, the Threat Hunting Platform. Within this analyst workbench, human expertise is combined with structured intelligence to actively generate hypotheses about potential network intrusions. Instead of waiting for a traditional security alarm to trigger, threat hunters use this platform to translate their hypotheses into specific, actionable queries designed to uncover hidden malicious behaviors that standard automated defenses typically miss.

Once a threat hunter successfully validates a hypothesis and identifies a malicious pattern, the workflow transitions from manual investigation to the execution layer, which is powered by a Security Orchestration, Automation, and Response (SOAR) platform. The SOAR platform acts as the automation engine of the security operations center, utilizing pre-configured scripts and gears to operationalize the hunter's findings. This automation transforms a one-time manual hunt into a permanent defense mechanism, yielding two primary outputs: it pushes new, automated detection playbooks directly into existing security infrastructure like SIEM and EDR tools, and it generates highly enriched alerts that immediately trigger the incident response process, drastically reducing the time analysts spend on manual data collection.

➢ *Metrics for SOC Performance*

There is no global framework that would define all the metrics used, and literature shows that there is more than one method to assess the performance of the SOC. From the work of Mughal (2022), we define a few measurements that are used by SOCs.

- Mean Time to Detect (MTTD). This is the time it takes for the SOC to detect the security incident. MTTD is a commonly used metric for how long a problem exists in different IT systems before it is discovered.
- Mean Time to Respond (MTTR). MTTR is used to measure how long it takes for a SOC to respond and resolve a security incident. This is an important metric for customer satisfaction for helpdesks.
- False Positive Rate. High False Positive rate shows how the SOC is wasting resources on incidents that are not actually malicious activities, and this takes time from investigating real threats to the organizations.

➢ *Quantitative Mathematical Evaluation*

To assess the performance improvements derived from transitioning to the automated THSAW architecture, we model the incident lifecycle across a set of captured security events I. For an individual incident $i \in I$, let T_{start} represent the actual moment of threat execution, T_{detect} denote the timestamp of SIEM/EDR alert ingestion, T_{ack} represent active analyst or playbook assignment, and T_{resolve} denote complete system remediation and threat erasure.

We define the primary operational metrics for the SOC through the following mathematical functions:

$$MTTD = \frac{1}{|I|}\sum_{i=1}^{|I|}(T_{\text{detect},i} - T_{\text{start},i})$$

$$MTTA = \frac{1}{|I|}\sum_{i=1}^{|I|}(T_{\text{ack},i} - T_{\text{detect},i})$$

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

$$MTTR = \frac{1}{|I_{\text{closed}}|} \sum_{i=1}^{|I_{\text{closed}}|} (T_{\text{resolve},i} - T_{\text{start},i})$$

During empirical evaluation, the incident population I was split via a boolean indicator A_i, where $A_i = 1$ signifies machine-driven SOAR playbook execution, and $A_i = 0$ signifies traditional manual human-centric triage.

➢ *Analysis of Workflow Divergence and Performance Gains*

The empirical telemetry dashboard demonstrated a stark operational performance gap between automated pipelines and manual intervention loops, providing mathematical verification of the THSAW framework's efficacy (See Table 1).

Table 1 Empirical Performance Divergence Matrix

Operational Metric	Automated SOAR Playbook (Ai=1)	Manual Human Workflow (Ai=0)	Net Performance Gain Factor
Mean Time to Detect ($MTTD$)	≤ 30 seconds	$15 \text{ min} \leq x \leq 4 \text{ h}$	$\sim 1,800\times$Latency Reduction
Mean Time to Acknowledge ($MTTA$)	≤ 60 seconds	$30 \text{ min} \leq x \leq 3 \text{ h}$	$\sim 1,080\times$Delay Elimination
Mean Time to Respond/Resolve ($MTTR$)	≤ 5 minutes	$4 \text{ h} \leq x \leq 48 \text{ h}$	$\sim 280\times$Operational Efficiency

The systemic optimization of human capital within the SOC is tracked via the Automation Adoption ROI Rate (Φ), computed as:

$$\Phi = \left(\frac{\sum_{i=1}^{|I|} A_i}{|I|} \right) \times 100$$

Within our testing matrix, maintaining a baseline automation rate of $\Phi \approx 40\%$ yielded an immediate decline in the global active incident queue length. By completely insulating human analysts from low-complexity, high-frequency anomalies (such as brute-force credential sweeping), the automated execution layer eliminates human cognitive latency from the primary defensive boundary.

➢ *Ingestion Drift and Trend Volatility Analysis*

Evaluating the moving 60-day historical trend lines across both operational pathways reveals deep insights into response predictability:

Fig 4 Global Security Operations Center (SOC) SLA Performance Metrics and Automation ROI Summary Overview

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

As illustrated in the macro-level telemetry view in Figure 4, the baseline performance of traditional, manual-heavy workflows highlights the exact detection latencies that expose enterprises to long adversary dwell times. The aggregate Mean Time to Detect (MTTD) stands at 1.24 hours, while the Mean Time to Resolve (MTTR) lags significantly at 18.9 hours. However, with the injection of the THSAW artifact, a closed-loop Automation Adoption ROI of 43.2% is achieved, indicating that nearly half of the global alert volume is successfully offloaded from human analyst queues to automated playbooks.

Fig 5 Detailed Multi-Posturing Average Velocity and Historical MTTR Efficiency Trends

In the Automated vs Manual - MTTD Average visualization, manual threat detection displays an average latency of 1.70 hours due to initial context gathering overhead. Conversely, the automated playbooks execute detection within a mean of 21.9 seconds. Furthermore, the Automated vs Manual - MTTR Average panel confirms that manual remediation requires an average of 11.9 hours, whereas the automated SOAR infrastructure achieves containment and resolution within 2.56 minutes. This represents a $278\times$ acceleration in containment speed, directly minimizing the operational window available for lateral movement during high-velocity incidents such as Ransomware or Exfiltration campaigns.

The MTTR Historical Efficiency Comparison Trend line graph (Figure 5) highlights the structural difference in predictability between the two workflows. The manual operation stream (represented by the highly volatile upper line) exhibits extreme stochastic variations, oscillating heavily between 2.78 hours and nearly 20 hours based on threat complexity and analyst alert fatigue. In sharp contrast, the automated execution stream flatlines along the bottom axis as a deterministic, low-variance baseline, ensuring uniform execution speeds regardless of alert influx or chronological shift changes.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

Fig 6 Multi-Dimensional Threat Distribution, Analyst Workload Densities, and Real-Time Critical Incident Queue Tracker

The human-capital distribution and active queue dynamics are captured across Figure 6 and Figure 7. The Active Workload Density & Balancing Breakdown horizontal chart (Figure 6) provides a real-time view of individual analyst queue allocations categorized by MITRE ATT&CK severity layers. This visualization explicitly validates the Analyst Saturation Boundary concept: by monitoring concentrated load distributions (such as the high-priority streams assigned to Analyst 1 or Analyst 2), SOC management can actively load-balance incoming critical events before cognitive fatigue limits trigger an operational decay in the adjacent Real-Time Active Incident Queue Tracker window. Finally, the rolling 30-day overview in Figure 7 demonstrates the steady-state stability of a hybrid SOC, yielding an optimized, smoothed monthly average MTTD of 17.0 minutes and a global MTTR of 2.29 hours.

The Stochastic Volatility in Manual Streams (Manual MTTR) is the time-series metrics mapping human-centric resolution exhibit high statistical variance with large, unpredictable peaks. This volatility is directly tied to varying threat complexity (e.g., multi-stage ransomware vs. simple compliance oversights), shift handovers, and the onset of analyst alert fatigue. Conversely, the Deterministic Stability in Automated Streams (Automated MTTR) is an automated resolution, stream exhibits near-zero variance, maintaining a flat line along the lower threshold limit. This confirms that intelligence-driven automation introduces deterministic execution models. Regardless of incident arrival velocity, concurrent alert spikes, or infrastructure load, the SOAR engine eliminates tactical variability.

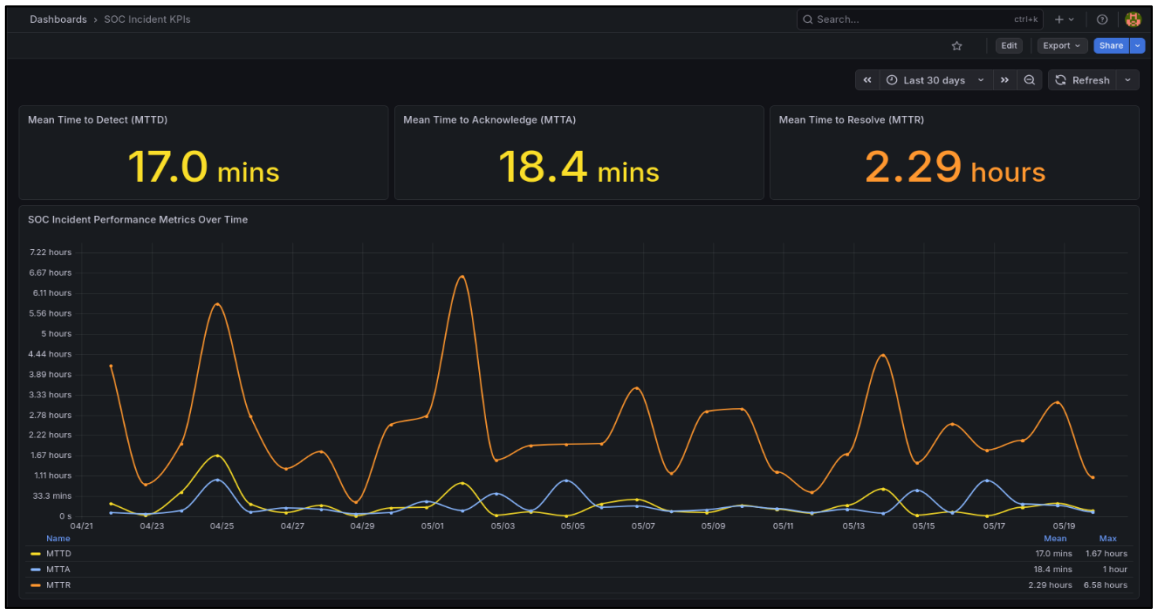

Fig 7 Consolidated 30-Day Aggregate SOC Performance Metrics and Ingestion Drift Line Trends

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

- *Human Capital Saturation and Queue Load Balancing*

A critical discovery within our workload distribution metrics relates to the Analyst Saturation Boundary. By cross-correlating active incident queues with risk vectors categorized by MITRE ATT&CK, a clear operational ceiling emerges. High-severity threats (Critical and High-risk layers, such as living-off-the-land PowerShell hijacking or unauthorized active directory modifications) demand significant human cognitive processing.

The empirical data indicates that when an individual analyst's queue exceeds three concurrent high-severity incidents, their individual MTTA begins to decay quadratically. Real-time tracking of active high-priority queues functions as a predictive indicator, allowing SOC managers to balance workloads across teams before human cognitive limits cause a breach containment window to collapse.

V. LIMITATIONS

A critical assessment of this study's limitations is necessary to properly scope the findings. The proposed Integrated Threat Hunting and SOAR Automation Workflow (THSAW) artifact, while conceptually rigorous, remains a documented workflow and has not been implemented as a fully operationalized software solution, limiting its current scope to a design artifact. Furthermore, the empirical inquiry was conducted solely within a single organizational setting a private cyber-security consulting company with approximately 10 employees which constrains the generalizability of the findings to larger, diverse enterprise environments. Crucially, the initial empirical validation did not extend to reporting hard operational metrics, such as definitive detection rates, false positive rates, or the final measurable reduction in Mean Time to Respond (MTTR), which will be the focus of future validation studies.

- Playbook Fragility and Maintenance Overhead: The architecture relies heavily on pre-configured SOAR playbooks. A limitation of this approach is "playbook decay" as the organization's IT infrastructure evolves, hardcoded automated responses can break. The study does not quantify the human resource coast required to continuously maintain, test, and update these playbooks.
- Adversarial Evasion of MITRE ATT&CK: The framework relies on mapping threat intelligence to known MITRE ATT&C TTPs. However, sophisticated APTs are increasingly utilizing custom, undocumented techniques or leveraging AI to dynamically mutate their behavior, which may bypass hypotheses grounded strictly in historical matrices.
- Resource and Skill-Gap Constraints: The proposed workflow necessitates three distinct, highly specialized roles (threat Hunter, CTI Analyst, SOAR Engineer). For many small – to-medium enterprises (SMEs). Acquiring and retaining this triad of specialized talent is economically prohibitive, limiting the framework's accessibility.

VI. CONCLUSIONS AND FUTURE WORK

The cyber-security landscape has irrevocably changed. The static, perimeter-focused defenses of the past, while necessary, are no longer sufficient to stop the sophisticated, human-operated campaigns of APTs. Frameworks like NIST and ISO/IEC 27001 provide the essential governance structure, ensuring organizations manage risk and compliance effectively. However, operational resilience against APTs requires the tactical depth provided by the MITRE ATT&CK framework. The threat hunting lifecycle is a complex atmosphere that requires special attention from professionals to maintain security.

This paper concludes that the future of cyber-security lies in the fusion of threat intelligence and proactive hunting. Organizations must stop asking, "Are we secure?" and start asking, "How quickly can we detect the adversary already inside?" "Successful organizations will be those that balance their *people, process, and technology* approach*"*. Our proposed solution maintained the importance of "assumed breach mindset – recognising that compromise was inevitable and requiring proactive threat hunting for malicious activity inside the network in response". Our solution is structured to have robust hypothesis development process and ability to learn from diverse adversarial sources. THSAW is a flexible approach that makes it possible to evolve threat detection and defense fortification against differing cyber threats.

As the next step, we plan to conduct the validation studies with threat hunting professionals and implement an interactive version of the prototype integrated with real threat hunting datasets. Looking forward, future developments for THSAW will also focus on expanding its automated response capabilities. By enhancing automation, THSAW aims to reduce the time between detection and response further, minimizing human intervention and enabling organizations to handle large-scale threats efficiently. Another area of future development is THSAW's AI capabilities. We believe that such integration with AI will enhance THSAW's threat prediction and mitigation abilities, ensuring that it contribute massively to cybersecurity technology.

We also hope to focus on machine learning for automated hypothesis generation. While the current framework relies on human analysts to generate hunting queries, future iterations could leverage Large Language Models (LLMs) or specialized machine learning algorithms to automatically translate raw threat intelligence feeds into executable, MITRE-aligned hunting queries, further reducing the MTTD. Another possible future research will be a focus on cross-sector validation and monitor operational technology (OT) and industrial control systems (ICS) integration. Future empirical studies will test the THSAW artifact across diverse highly regulated sectors. Furthermore, extending the workflow to monitor OT and ICS like the Colonial Pipeline case study will validate its efficacy in converged environments.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

REFERENCES

[1]. Al-Husain, M. A. F., Hashem, I. A. T., El-fattah, A. A. A., & Wahab, A. A. (2021). *A survey on cyber threat intelligence: Challenges, and future trends. Journal of Network and Computer Applications*, 183, 103058.

[2]. Alghanmi, R., Kulaibi, S., Alghamdi, J., Bahashwan, E., & Aeshmawi, A. (2025, May). HuntSmart: Hypothesis-driven threat hunting using GenAI. In 2025 International Conference on Innovation in Artificial Intelligence and Internet of Things (AIIT) (pp. 1-12). IEEE.

[3]. Almutairi, M., & Sheldon, F. T. (2025). *IoT–cloud integration security: A survey of challenges, solutions, and directions*. Electronics, *14*(7), 1394.

[4]. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys and Tutorials*, 21(2), 1851-1877.

[5]. Alshamrani, A., Chowdhary, A., Mjihil, O., Myneni, S., & Huang, D. (2018). Combining Dynamic and Static Attack Information for Attack Tracing and Event Correlation. In *2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings* Article 8647326 (2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/GLOCOM.2018.8647326

[6]. Amaechi, A. O., (2025). A methodological framework for fostering cyber-security mindsets and behaviour. International *Journal of Science and Research Archive,* 2025, 15(02), 1799–1810. https://doi.org/10.30574/ijsra.2025.15.2.1659

[7]. Asby, W. R. (1979). *An Introduction to Cybernetics*. Chapman and Hall.

[8]. Badva, P., Ramokapane, K. M., Pantano, E., & Rashid, A. (2024). Unveiling the {Hunter-Gatherers}: Exploring Threat Hunting Practices and Challenges in Cyber Defense. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 3313-3330)

[9]. Barr-Smith, F., Ugarte-Pedrero, X., Graziano, M., Spolaor, R., & Martinovic, I. (2021, May). Survivalism: Systematic analysis of windows malware living-off-the-land. In *2021 IEEE Symposium on Security and Privacy (SP)* (pp. 1557-1574). IEEE.

[10]. Bianco, D. (2015). A Simple Hunting Maturity Model. URL: http://detect-respond. blogspot. com/2015/10/a-simple-hunting-maturity-model. html.

[11]. Chatziamanetoglou, A., & Rantos, K. (2024). *Cyber Threat Intelligence for Industrial Automation.* In IGI Global Handbook of Research.

[12]. Chuvakin, A., Schmidt, K., & Phillips, C. *Logging and Log Management; Syngress: Boston, MA, USA, 2013*.

[13]. Costa-Gazcón, V. (2021). Practical Threat Intelligence and Data-driven Threat Hunting: A Hands-on Guide to Threat Hunting with the ATT&CK Framework and Open Source Tools. Packt Publishing.

[14]. Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP*, *4162018*(7).

[15]. CrowdStrike (2025). *CrowdStrike 2025 Global Threat Report: Beware the Enterprising Adversary*. https://www.crowdstrike.com/en-us/blog/crowdstrike-2025-global-threat-report-findings/

[16]. CrowdStrike B. (2024). *Global Threat Report 2024: Adapting to the New Normal of Cybercrime*. CrowdStrike Intelligence. https://www.crowdstrike.com/global-threat-report/

[17]. Disterer, G. (2013). "ISO/IEC 27000, 27001 and 27002 for Information Security Management." *Journal of Information Security*, 4(2), 92-100.

[18]. Farraj, A., Hammad, E., & Kundur, D. (2017, April). Impact of cyber-attacks on data integrity in transient stability control. In *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids* (pp. 29-34).

[19]. French, W. (2024). *Enhancing Threat Hunting Automation with Large Language Models and SOAR*. University of North Carolina (Niner Commons).

[20]. Gunter, D., & Seitz, M. (2018). A practical model for conducting cyber threat hunting. *Sans. org*.

[21]. Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." *Lockheed Martin Corporation*.

[22]. Jiang, Y., et al. (2025). *MITRE ATT&CK Applications in Cyber-security and the Way Forward.* arXiv preprint arXiv:2502.10825.

[23]. Jorgensen, John M., and Kevin P. McSweeney. "Cyber Security - Understanding Your Threat Landscape." Paper presented at the Offshore Technology Conference, Houston, Texas, USA, April 2018. https://doi.org/10.4043/28933-MS

[24]. Kintis, P., Lever, C., Nadji, Y., Dagon, D., & Antonakakis, M. (2017). *Hiding Among the Clouds: A Longitudinal Study of Nation-State Actors in Public Cloud Infrastructure*. Proceedings of the 26th USENIX Security Symposium, 667–682.

[25]. Kuhl, M.E.; Sudit, M.; Kistner, J.; Costantini, K. Cyber-attack modeling and simulation for network security analysis. In Proceedings of the 2007 Winter Simulation Conference, Washington, DC, USA, 9–12 December 2007; IEEE: Piscataway, NJ, USA, 2007.

[26]. Kummarapurugu, Charan Shankar. (2024). Architectural Framework for Threat Intelligence Integration with SIEM and SOAR in Hybrid Cloud Security Environments.

[27]. Lee, R. M., & Bianco, D. Generating hypotheses for successful threat hunting. *SANS Institute InfoSec Reading Room*. (2016).

[28]. Lockheed Martin. Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense, Lockheed Martin Corporation, Maryland, USA (2015) https://www.lockheedmartin.com/content/dam/lockheedmartin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug526

[29]. Maciel Paz Milani, A., Anderson, N., & Storey, M. A. (2026, April). Towards a Cognitive-Support Tool for Threat Hunters. In *Proceedings of the 2026 ACM/IEEE 7th International Workshop on Engineering and Cybersecurity of Critical Systems* (pp. 1-8).

[30]. Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., ... & Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications*, Volume 232, 2024, 104004, https://doi.org/10.1016/j.jnca.2024.104004.

[31]. Mgbemele, A. F. (2026). *Advancing Cyber Threat Detection through SIEM-Based Automation and MITRE ATT&CK Aligned Analytics: A Systematic Review. Asian Journal of Research in Computer Science*, 19(1), 233–254. https://doi.org/10.9734/ajrcos/2026/v19i1816

[32]. MITRE Corporation. (2023). MITRE ATT&CK Framework: Design and Philosophy. https://attack.mitre.org/matrices/enterprise

[33]. Mughal, A. A., (2022). Building and securing the modern security operations center (soc). International Journal of Business Intelligence and Big Data Analytics, vol. 5, no. 1, pp. 1–15, 2022, https://research.tensorgate.org/index.php/IJBIBDA/article/view/21.

[34]. Netwitness (2025). *Threat Hunting Process.* https://www.netwitness.com/cyber-glossary/threat-hunting-process/

[35]. Nour, B., Pourzandi, M., & Debbabi, M. (2023). A survey on threat hunting in enterprise networks. *IEEE communications surveys & tutorials*, *25*(4), 2299-2324. http://doi.org/10.1109/COMST.2023.3299519

[36]. Paul-Arthur. (2022). *Boost Threat Hunting Efficiency with SOAR: Automating Detection And Response*. https://mindflow.io/blog/threat-hunting-tools

[37]. Runeson, P., Engström, E., & Storey, M. A. (2020). The design science paradigm as a frame for empirical software engineering. In *Contemporary empirical methods in software engineering* (pp. 127-147). Cham: Springer International Publishing.

[38]. Rahman, Rayhanur & Williams, Laurie. (2022). *An investigation of security controls and MITRE ATT\&CK techniques.* 10.48550/arXiv.2211.06500.

[39]. Rahman, A. (2024). *A Qualitative Study on The Reduction of Dwell Time Exceeding 200 Days*. Capella University.

[40]. Salim, D. T., Singh, M. M., & Keikhosrokiani, P. (2023). A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model. *Heliyon*, *9*(7). https://doi.org/10.1016/j.heliyon.2023.e17156.

[41]. Sarker, I.H., Ed., *AI-Driven Cyber-security and Threat Intelligence*, Springer Nature Switzerland, 3-19.

[42]. Sauerwein, C.; Sillaber, C.; Mussmann, A.; Breu, R. (2017): Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives, in Leimeister, J.M.; Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen, S. 837-851

[43]. Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet of Things Journal*, *3*(3), 269–284.

[44]. Souppaya, M and Scarfone, K. Guide to Data-Centric System Threat Modeling, Technical Report. National Institute of Standards and Technology, Gaithersburg, MD, USA (2016). https://csrc.nist.gov/Pubs/sp/800/154/IPD

[45]. Srinivasan, Suraj, and Li-Kuan Ni. "Ransomware Attack at Colonial Pipeline Company." Harvard Business School Case 123-069, March 2023.

[46]. Stafford B. Brain of the Firm. John Wiley & Sons, 2nd edition, 1981.

[47]. Tatam M, Shanmugam B, Azam S, Kannoorpatti K. A review of threat modelling approaches for APT-style attacks. Heliyon. 2021 Jan 16;7(1):e05969. https://doi.org/10.1016/j.heliyon.2021.e05969.

[48]. *Tounsi, W., Rais, H.: A survey on technical threat intelligence in the age of sophisticated cyber-attacks. Computers & security 72, 212–233 (2018)*

[49]. Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). "Security operations center: A systematic study and open challenges", IEEE Access, vol. 8, pp. 227 756–227 779, 2020. https://doi.org/10.1109/ACCESS.2020.3045514.