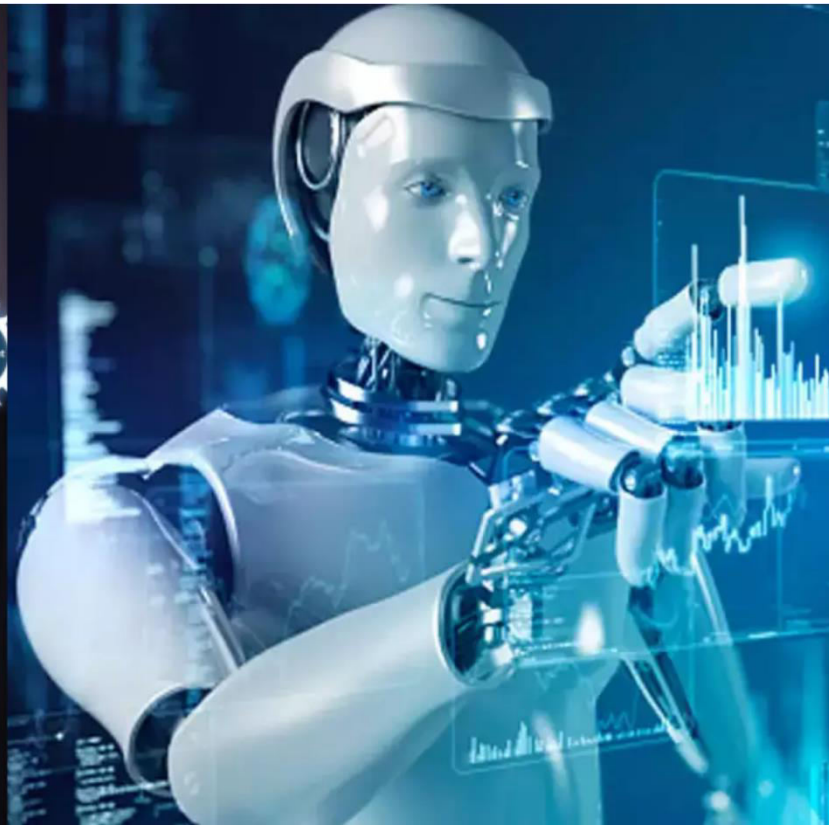
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503211|

The Paradigm Shift in Proactive Threat Hunting: Synergizing Agentic Orchestration, Neuro-Symbolic Reasoning, and Post-Quantum Resilience

Nikhil S. Khatri, Dr. Sneha Patel

Student of M.Sc. Cybersecurity, Bhagwan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, India

Asst. Professor, Bhagwan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, India

ABSTRACT: The global cybersecurity landscape of 2026 is defined by a fundamental structural transformation, moving away from the reactive, signature-centric paradigms of the previous decade toward a model of autonomous, intelligence-driven proactive defense. This evolution is necessitated by an adversarial environment where the "hands-on-keyboard" intrusion has become a professionalized, AI-accelerated enterprise. As digital ecosystems transition into "cyber-enabled hyper worlds," the integration of cyber-physical systems, autonomous agents, and massive-scale telemetry has rendered traditional perimeter-based security architectures largely obsolete.[1] Contemporary threat hunting research focuses on bridging the gap between high-volume data ingestion and high-fidelity reasoning, leveraging the convergence of Large Language Models (LLMs), agentic orchestration, and neuro-symbolic logic to maintain a defensive advantage.[2]

KEYWORDS: Proactive Threat Hunting, Synergizing Agentic Orchestration, Neuro-Symbolic Reasoning, and Post-Quantum Resilience

I. THE CONTEMPORARY ADVERSARIAL LANDSCAPE: PROFESSIONALIZATION AND GENAI WEAPONIZATION

The shift in threat hunting methodologies is a direct response to the unprecedented professionalization of threat actors observed between 2024 and 2026. Analysis of frontline data from 2025 indicates that interactive intrusions—those involving direct human-led manipulation rather than automated malware delivery—have risen by 27% year-over-year.[4] Most significantly, 81% of these interactive intrusions are now "malware-free," relying on legitimate administrative tools, living-off-the-land (LotL) techniques, and stolen credentials to bypass conventional detection systems.[4] This necessitates a move from indicator-based hunting toward behavioral and provenance-based analysis, as traditional file-based signatures no longer provide a reliable detection signal.[1]

The weaponization of Generative AI (GenAI) has scaled social engineering to a point where human trust is the most vulnerable component of the enterprise perimeter. Adversaries like FAMOUS CHOLLIMA, a DPRK-nexus actor, have demonstrated the ability to use GenAI to automate the creation of synthetic identities and perform complex technical tasks under false identities, infiltrating over 320 organizations in a single year—a 220% increase in scale.[4] Furthermore, "vishing" (voice phishing) attacks increased by 442% between 2024 and 2025, with attackers using AI-generated voices to deceive help desk personnel into resetting MFA credentials.[4]

II. HISTORICAL AND CONTEMPORARY THREAT DYNAMICS (2021-2026)

The following table contextualizes the shift in attack vectors and the corresponding impact on global organizational security.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503211|

Metric	2021	2023	2024	2025 (Projected)	2026 (Reported)	Research gap
Interactive Intrusions	Baseline	+15%	+27%	+35%	+42%	Existing systems lack real-time behavioral detection for a interactive, human-driven attacks, limited research on adaptive threat hunting models.
Malware-Free Ratio	62%	75%	81%	84%	88%	Traditional security tools fail to detect a fileless and malware free attacks. need for AI-driven anomaly detection and memory-based analysis.
Cloud Intrusion Surge	Baseline	+85%	+110%	+136%	+165%	Insufficient research on cloud native threat hunting frameworks and multi-cloud monitoring mechanisms.
Targeted Sectors (Rank 1)	Technology	Technology	Technology	Technology	Technology	Lack of sector-specific threat intelligence models and customized defence strategies for a high-risk industry.

This surge in sophistication is not limited to enterprise networks. The automotive and smart mobility sector has witnessed a 66% increase in incidents targeting telematics and cloud-based vehicle APIs.[9] Threat actors now exploit weak authentication protocols to manipulate vehicle companion apps, starting engines or altering ownership records within seconds.[9]

III. THEORETICAL FOUNDATIONS OF PROACTIVE THREAT HUNTING

Threat hunting is defined in modern research as the proactive, iterative search through networks or datasets to detect and isolate advanced threats that evade existing security solutions. Unlike traditional detection, which is alert-driven, threat hunting is hypothesis-driven, leveraging Cyber Threat Intelligence (CTI) to anticipate adversary Tactics, Techniques, and Procedures (TTPs). The evolution of this field can be categorized into three distinct phases: the Signature Era (IoC-based), the Behavioral Era (UEBA/TTP-based), and the current Agentic Era (Autonomous/Reasoning-based).[1]

IV. THE ROLE OF CYBER THREAT INTELLIGENCE (CTI)

Modern threat hunting is increasingly "intelligence-driven." This involves extracting actionable insights from

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503211|

unstructured CTI reports and aligning them with structured system telemetry. The primary challenge in this domain is the "modality gap"—the structural disconnect between the natural language descriptions of attacks found in reports and the low-level events captured in provenance graphs or audit logs.[11] Advanced NLP techniques, including Transformer-based models and Hybrid CNN-BiLSTM-DNN architectures, are currently employed to automate the extraction of entities and relationships from CTI feeds.[13]

V. MULTI-MODAL LEARNING AND PROVENANCE-BASED HUNTING

A significant breakthrough in 2025 is the development of systems like **APT-CGLP** (Advanced Persistent Threat hunting via Contrastive Graph-Language Pre-training). This system addresses the modality gap by framing threat hunting as a cross-modal alignment task between textual CTI and system-level provenance graphs.[11] Provenance graphs are essential because they provide the causality and contextual link between disparate system events—such as a file write followed by a network connection—which are often lost in isolated log entries. APT-CGLP facilitates end-to-end semantic matching without human intervention, allowing a system to "read" a new CTI report and immediately search the infrastructure for described patterns.[11]

The mathematical foundation for this alignment involves a contrastive loss function, ensuring that a textual representation of an attack pattern **T** and its corresponding graph representation **G** are mapped closely in a high-dimensional latent space:

$$\mathcal{L} = -\log \frac{\exp(\text{sim}(T_i, G_i)/\tau)}{\sum_{j=1}^{N} \exp(\text{sim}(T_i, G_j)/\tau)}$$

VI. REGAIN: HIERARCHICAL REASONING FOR NETWORK TRAFFIC

Similarly, the **ReGAIN** framework integrates network traffic summarization with LLM-driven reasoning to support forensic investigations.[18] By transforming raw packet captures (PCAPs) and flow records into descriptive embedded summaries stored in a multi-collection vector database, ReGAIN enables evidence-grounded retrieval of historical patterns. In evaluations against ICMP ping flood and TCP SYN flood scenarios, ReGAIN achieved accuracy rates between 95.95% and 98.82%, with near-perfect recall.[18] Its hierarchical retrieval and re-ranking mechanisms, combined with an abstention strategy, help mitigate the risk of LLM hallucinations.[18]

VII. THE RISE OF AGENTIC AI: AUTONOMY AND DECISION-MAKING

By 2026, the cybersecurity industry has moved rapidly from simple chatbots toward an agent-driven approach. "Agentic AI" refers to systems that do not merely respond to prompts but act autonomously to achieve high-level goals.[2] These systems possess planning capabilities, memory, and the ability to use external tools (APIs, sandboxes, EDR queries) to execute complex investigative workflows.[3]

VIII. MULTI-AGENT ORCHESTRATION: MAS-HUNT AND COLLABORATIVE DEFENSE

A single agent is often insufficient for enterprise-scale hunting. Modern research introduces architectures like **MAS-Hunt**—a novel multi-agent system architecture that operates directly on live telemetry within the Elastic Stack.[19] MAS-Hunt follows a compact three-layer hierarchy:

1. **Governance Board:** Sets objectives and safety constraints.
2. **Manager Agents:** Decompose goals into intelligence, detection, and hunting tasks.
3. **Executor Agents:** Operate against external APIs and ELK to collect intel, create rules, and validate signals.[19]

The system incorporates security-first design with built-in defenses for memory integrity and cross-agent validation to prevent a single compromised agent from triggering systemic failure.[19]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503211|

IX. NEURO-SYMBOLIC AI: THE INTEGRATION OF LOGIC AND PATTERN RECOGNITION

A fundamental limitation of purely neural approaches is their lack of conceptual grounding and "brittleness" when encountering novel attacks.[16] Neuro-Symbolic (NeSy) AI emerges as a solution, synergistically combining neural pattern recognition (Deep Learning) with symbolic reasoning (Logic/Rules).[17]

X. THE G-I-A FRAMEWORK FOR NESY CYBERSECURITY

The **Grounding-Instructibility-Alignment (G-I-A)** framework has been introduced as a systematic method to evaluate these hybrid systems [16]:

- **Grounding Quality:** Measures the system's ability to connect neural pattern recognition with real-world cybersecurity concepts and logical constraints.[16]
- **Instructibility:** Assesses how effectively a system adapts its behavior in response to analyst feedback without requiring extensive retraining.[20]
- **Alignment:** Ensures that the AI system's actions remain consistent with organizational security objectives and ethical principles.[20]

By integrating causal reasoning, NeSy systems move from simple correlation to understanding attack causality and counterfactual threat scenarios.[16]

XI. POST-QUANTUM CYBERSECURITY: THREATS AND TRANSITION

The horizon of 2026 is increasingly shadowed by the progress of quantum computing. While current quantum processors are not yet large enough to break RSA or Elliptic Curve Cryptography (ECC) in real-time, the threat of "Harvest Now, Decrypt Later" (HNDL) is an immediate concern.[5] Attackers intercept encrypted traffic today with the intent to decrypt it once cryptographically relevant quantum computers (CRQCs) become available.

The transition to **Post-Quantum Cryptography (PQC)** is a multi-year endeavor. By 2026, organizations must achieve "crypto-agility"—the ability to rapidly switch between cryptographic standards as new vulnerabilities are discovered or as PQC algorithms stabilize.[5] NIST standards such as the module-lattice key encapsulation mechanism (ML-KEM) and digital signature algorithm (ML-DSA) form the basis for these new defenses.

XII. ETHICAL GOVERNANCE AND ALGORITHMIC BIAS

As defense systems gain increasing autonomy, the risk of unethical algorithmic decision-making becomes a central concern. Research indicates that AI models used in network threat detection can experience a "precision gap" or inherit systemic biases from training data.[18] For example, studies have shown that biased training data can cause unrepresentative false-positive rates across different user groups, with some groups experiencing false-positive rates (FPR) nearly twice as high as others.[21] Ethical threat hunting requires representative datasets, differential privacy, and regular fairness audits to ensure that users are not incorrectly blocked based on their digital footprint.[21]

XIII. CONCLUSIONS AND PRACTICAL RECOMMENDATIONS

The shift toward proactive threat hunting in 2026 is not merely a technological upgrade but a fundamental change in security philosophy. To maintain a defensive posture, the following strategic priorities are recommended:

- **Invest in Agentic Architectures:** Transition legacy tools toward agentic orchestration platforms like MAS-Hunt that support autonomous reasoning.[19]
- **Adopt Standardized Context Protocols:** Utilize the **Model Context Protocol (MCP)** to standardize how AI agents interact with tools, APIs, and memory, ensuring interoperability and auditability.
- **Implement Risk-Based AI Governance:** Establish clear oversight mechanisms and adopt frameworks like G-I-A to prioritize transparency and fairness.[16]
- **Accelerate PQC Readiness:** Begin cryptographic asset discovery immediately to prepare for the HNDL threat.[5]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503211|

REFERENCES

1. IEEE Cybermatics Congress. (2025). *The 2025 IEEE Cybermatics Congress – Cyber-Enabled World Program*. Retrieved February 7, 2026, from https://ieee-cybermatics.org/2025/2025%20IEEE%20Cybermatics%20Congress%20at%20Program.pdf
2. DLA Piper. (2025). *Key insights from the CrowdStrike 2025 threat hunting report*. Retrieved February 7, 2026, from https://privacymatters.dlapiper.com/2025/08/key-insights-from-the-crowdstrike-2025-threat-hunting-report/
3. CyberProof. (2025). *CyberProof 2025 mid-year cyber threat landscape report*. Retrieved February 7, 2026, from https://www.cyberproof.com/cyber-threat-intelligence/cyberproof-2025-mid-year-cyber-threat-landscape-report/
4. Intezer. (2026). *Top 15 AI SOC tools for 2026: SOC automation compared*. Retrieved February 7, 2026, from https://intezer.com/blog/top-15-ai-soc-platforms-in-2026/
5. Google Cloud Community. (2026). *Operationalizing Google agentic threat intelligence: Transforming defense workflows*. Retrieved February 7, 2026, from https://security.googlecloudcommunity.com/community-blog-42/operationalizing-google-agentic-threat-intelligence-transforming-defense-workflows-6618
6. Right-Hand AI. (2025). *Adopting agentic AI in cybersecurity: What CISOs expect in 2025*. Retrieved February 7, 2026, from https://right-hand.ai/blog/agentic-ai-in-cybersecurity/
7. Authors unknown. (2026). *A survey of agentic AI and cybersecurity: Challenges, opportunities and use-case prototypes*. arXiv. Retrieved February 7, 2026, from https://arxiv.org/html/2601.05293
8. Flobotics. (2025). *The hottest agentic AI examples and use cases in 2025*. Retrieved February 7, 2026, from https://flobotics.io/uncategorized/hottest-agentic-ai-examples-and-use-cases-2025/
9. TierPoint. (2026). *Cybersecurity trends in 2026: Rising threats & strategies*. Retrieved February 7, 2026, from https://www.tierpoint.com/blog/cybersecurity/cybersecurity-trends/
10. CrowdStrike. (2025). *2025 threat hunting report: Latest cybersecurity trends & insights*. Retrieved February 7, 2026, from https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/
11. Authors unknown. (2025). *APT-CGLP: Advanced persistent threat hunting via….* arXiv. Retrieved February 7, 2026, from https://www.arxiv.org/pdf/2511.20290
12. Kellton. (2026). *Agentic AI trends 2026: Key innovations transforming business operations*. Retrieved February 7, 2026, from https://www.kellton.com/kellton-tech-blog/agentic-ai-trends-2026
13. Palo Alto Networks. (2025). *2025 Unit 42 global incident response report*. Retrieved February 7, 2026, from https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report
14. iOPEX Technologies. (2026). *Agentic AI workflows in threat detection*. Retrieved February 7, 2026, from https://www.iopex.com/blog/agentic-ai-workflows-in-threat-detection
15. EvoAI Labs. (2026). *The rise of agentic AI in cybersecurity: A new era of autonomous defense*. Retrieved February 7, 2026, from https://evoailabs.medium.com/the-rise-of-agentic-ai-in-cybersecurity-a-new-era-of-autonomous-defense-899c9dd46481
16. Authors unknown. (2025). *Neuro-symbolic AI for cybersecurity: State of the art, challenges, and opportunities*. arXiv. Retrieved February 7, 2026, from https://arxiv.org/html/2509.06921v1
17. Upstream. (2025). *Mind the cyber gap: Key insights from Upstream's 2025 automotive cybersecurity report*. Retrieved February 7, 2026, from https://upstream.auto/blog/insights-from-upstreams-2025-automotive-cybersecurity-report/
18. Authors unknown. (2026). *ReGAIN: Retrieval-grounded AI framework for network traffic analysis*. arXiv. Retrieved February 7, 2026, from https://arxiv.org/html/2512.22223v1
19. Authors unknown. (2026). *MAS-Hunt: A resilient AI multi-agent system for threat hunting*. MDPI. Retrieved February 7, 2026, from https://www.mdpi.com/2673-4591/123/1/26
20. Authors unknown. (2025). *Neuro-symbolic AI for cybersecurity: State of the art*. arXiv. Retrieved February 7, 2026, from https://arxiv.org/abs/2509.06921
21. RSIS International. (2025). *Bias and data privacy: Challenges in AI-driven network security*. Retrieved February 7, 2026, from https://rsisinternational.org/journals/ijriss/uploads/vol9-iss11-pg8093-8101-202512_pdf.pdf

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details