CYBER THREAT INTELLIGENCE

EMERGING TECHNOLOGIES & TECHNIQUES

AI & MACHINE LEARNING IN CTI

Artificial Intelligence (AI) and Machine Learning (ML) have become fundamental in analyzing large datasets and identifying patterns within them, especially in the context of cybersecurity.

TECHNIQUES

- **Anomaly Detection:** AI-driven systems can continuously monitor network traffic or system behaviors to identify anomalous patterns indicative of a cyberattack.
- **Predictive Analytics:** ML algorithms can predict future cyberattacks based on historical threat data, offering advanced threat forecasting.
- **Automated Threat Detection:** Machine learning algorithms are trained on vast datasets of known attack vectors, helping systems to autonomously detect zero-day vulnerabilities, phishing attempts, and other sophisticated attacks.

DECEPTION TECHNOLOGY

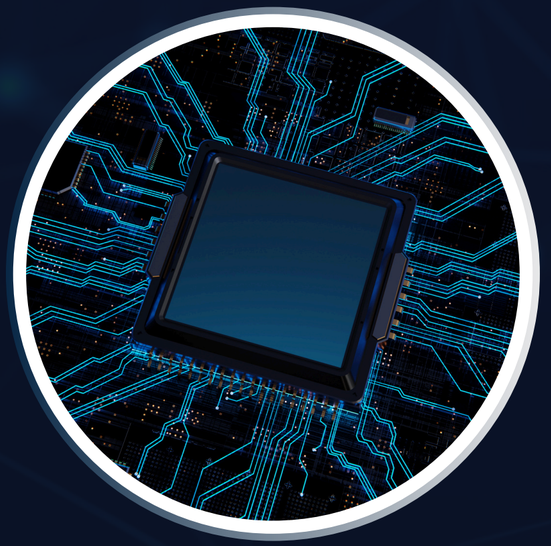
Deception technology involves setting up traps, decoys, or honeypots within a network that appear to be legitimate targets, luring cyber attackers into engaging with them. This provides organizations with early warning of a breach and an opportunity to analyze attack methods.

TECHNIQUES

- **Honeypots & Honeynets:** These are decoy systems that mimic real networks or systems but are isolated from the actual environment. Any interaction with these systems is recorded and analyzed.

- **Active Deception:** Involves the deployment of fake data, systems, or services that dynamically respond to attackers to confuse and mislead them.

ADVANCED MALWARE ANALYSIS & SANDBOXING



As malware becomes increasingly sophisticated, emerging CTI techniques are being used to analyze and understand new malware strains.

TECHNIQUES

- **Dynamic Sandboxing:** Malware samples are executed in a controlled environment to observe their behavior without risking real systems. Advanced CTI techniques track the malware's interactions with the system and network to develop defense mechanisms.

- **Automated Reverse Engineering:** AI and ML are used to automate the reverse engineering of malware, identifying attack methods, payloads, and other critical data in real time.

AUTOMATED INCIDENT RESPONSE

Automated Incident Response refers to using CTI in combination with automation tools to respond to incidents without human intervention. This enables faster containment and mitigation of threats.

TECHNIQUES

- **Security Orchestration, Automation, and Response (SOAR):** Platforms integrate CTI data with workflows to automatically trigger predefined response actions like blocking IP addresses, isolating infected devices, or issuing alerts.

- **AI-Driven Response Automation:** Leveraging machine learning models to determine the best response actions based on real-time analysis of an attack.

BLOCKCHAIN TECHNOLOGY

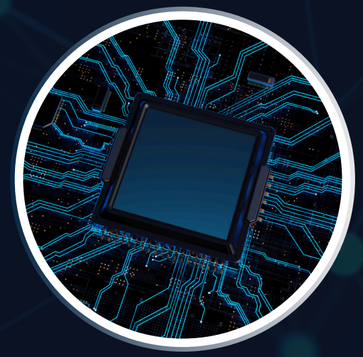
Blockchain technology, known for its secure and transparent ledger system, is emerging as a solution to ensure the integrity of threat intelligence data and combat cybercrime.

TECHNIQUES

- **Decentralized Threat Intelligence Sharing:** Using blockchain for secure, transparent, and tamper-proof sharing of threat intelligence across organizations and sectors.

- **Cryptographic Signatures:** Blockchain-based solutions ensure that the intelligence shared is authentic and hasn't been altered, which is crucial for building trust in threat data.

ZERO-TRUST ARCHITECTURE (ZTA)



Zero Trust Architecture is a security model that assumes no user or device, inside or outside the network, can be trusted. ZTA plays a critical role in CTI by continuously verifying users and devices and ensuring they meet security standards.

TECHNIQUES

- **Real-Time Risk Assessment:** Continuous monitoring of the user and device behaviors with CTI to dynamically assess risks and enforce access controls.

- **Intelligent Access Controls:** Leveraging CTI to refine user authentication and authorization, ensuring only trusted entities have access to sensitive systems.

CONCLUSION

- The field of Cyber Threat Intelligence is rapidly evolving with the introduction of cutting-edge technologies and techniques. Organizations are increasingly relying on AI, machine learning, automation, and other advanced tools to stay ahead of increasingly sophisticated cyber adversaries.

- The continuous development and integration of these technologies into CTI processes will provide a more proactive, collaborative, and effective defense against modern cyber threats.

THANK YOU!