Glossary: Generative AI for Cybersecurity

Welcome! This alphabetized glossary contains many of the terms you'll find within this course. This comprehensive glossary also includes additional industry-recognized terms not used in course videos. These terms are important for you to recognize when working in the industry, participating in user groups, and participating in other certificate programs.

Terms	Definition	First Introduced
Adaptability of AI-powered Systems	The continuous learning and adaptation of AI-powered systems to changing environments and evolving threats. Over time, these systems improve their accuracy and effectiveness, ensuring they remain up-to-date and capable of addressing new and emerging threats in the cybersecurity landscape.	Video: Enhancing Vulnerability Management with Generative AI
Adaptability to Novel Threats	Generative AI's capacity to respond to emerging and evolving cybersecurity threats, generating adaptive strategies for a robust defense system.	Video: Transition from Conventional AI to Generative AI and its Benefits in Cybersecurity
Advanced Threat Detection	The capability of SIEM solutions, enhanced by machine learning, to identify complex, polymorphic, and previously unseen threats. Unlike traditional rule-based approaches, machine learning algorithms recognize patterns and characteristics not captured by static rules, facilitating continuous learning and adaptation to emerging threats. This results in improved detection of advanced and targeted attacks in the cybersecurity landscape.	Video: Advanced Threat Detection with Generative AI in SIEM
Adversarial Attacks	Adversaries manipulate input data to deceive Generative AI models, causing misclassifications, generating misleading information, or other undesirable outcomes. This poses a significant challenge in ensuring the robustness of model predictions.	Reading: Threats on Generative AI Models
AI Arms Race	A competitive race among tech businesses globally to develop cutting-edge generative conversational AI models and advanced AI systems, driven by rapid growth in the global AI market, consumer reliance on AI technologies, and substantial investments.	Video: Concerns & Considerations Using Generative AI in Cybersecurity
AI Lifecycle	The stages of the artificial intelligence development process, from data collection and model training to deployment and ongoing monitoring. Prioritizing security in AI development involves measures to verify data accuracy, eliminate bias, and continuously monitor performance.	Video: Concerns & Considerations Using Generative AI in Cybersecurity
AI-based Vulnerability Management Systems	Systems powered by Artificial Intelligence (AI) that introduce automation, efficiency, intelligent prioritization, continuous monitoring, advanced analytics, and adaptability into vulnerability management processes. They address the limitations of traditional approaches, providing proactive, scalable, and context-aware solutions.	Video: Enhancing Vulnerability Management with Generative AI
Alert Fatigue	The result of excessive and unnecessary alerts, causing cybersecurity professionals to become desensitized to genuine threats.	Video: Leveraging AI for Advanced Threat Detection and Prevention
Algorithmic Bias	Unintended bias in AI algorithms, often resulting from biased training data, leading to discriminatory outcomes.	Video: Leveraging AI for Advanced Threat Detection and Prevention
Anchoring Bias	Bias occurring when an LLM relies too heavily on initial information, incorporating early biases in the training data and perpetuating them throughout generated content.	Video: Generative AI and LLM Risks
Anomaly Detection	The process of identifying deviations from standard patterns, aiding in the early recognition of threats.	Video: Leveraging AI for Advanced Threat Detection and Prevention
Automated Playbook Creation	Utilization of Generative AI to automate the creation and adaptation of cybersecurity playbooks, ensuring real-time effectiveness in incident response.	Video: Transition from Conventional AI to Generative AI and its Benefits in Cybersecurity
Automated Security Alerts	The role of generative AI in monitoring and analyzing evolving threat patterns to automate the generation of timely and accurate security alerts. Ensures real-time responses to potential security incidents, maintaining cybersecurity defenses' integrity.	Reading: Applications of Generative AI on Different Tasks of Cybersecurity
Automation Bias	The tendency of individuals to unquestioningly trust AI-generated outputs without critical evaluation, posing a significant concern for generative AI systems as users assume their infallibility.	Video: Generative AI and LLM Risks
Automation in Cybersecurity	The use of automated processes, driven by AI, to perform routine tasks, respond to threats, and enhance overall cybersecurity posture.	Video: Leveraging AI for Advanced Threat Detection and Prevention
Availability Bias	Bias resulting from LLM exposure to large amounts of publicly available data, favoring readily available content and neglecting less prevalent perspectives and information online.	Video: Generative AI and LLM Risks
Behavioral Analysis	Security teams use generative AI to identify patterns indicative of insider threats or unusual activities. This proactive approach enables the monitoring of user behavior for potential security incidents, facilitating early detection and response.	Reading: Application of Generative AI in Content Filtering and Monitoring

Terms	Definition	First Introduced
Bias Amplification	The risk associated with Generative AI models inheriting biases from their training data leads to the amplification of these biases in the decision-making processes of cybersecurity systems. Bias amplification may result in disproportionate consequences for certain individuals or groups, emphasizing the importance of scrutinizing and mitigating biases to maintain the accuracy and fairness of AI systems in cybersecurity.	Reading: Generative AI and Cybersecurity: Balancing Benefits and Ethical Concerns
Bias and Unfairness	The potential for AI algorithms, if trained on biased data, to inadvertently discriminate against certain individuals or groups, amplifying existing social biases and leading to unfair treatment in threat detection and decision-making processes.	Video: Ethical Concerns of AI in Cybersecurity
Collaborative Approach with Traditional Systems	The recognition that AI is not a standalone solution but a complementary component to traditional vulnerability management systems. The collaborative approach between AI and existing frameworks creates a robust defense against evolving threats, combining the strengths of both approaches for comprehensive cybersecurity.	Video: Enhancing Vulnerability Management with Generative AI
Compliance and Reporting	Supports regulatory compliance by providing detailed reports and logs of security events, easing the process of compliance audits.	Video: Cybersecurity Analytics Using Generative AI
Confirmation Bias	A psychological tendency reflected in LLMs where they generate content confirming existing beliefs, ignoring evidence challenging those beliefs.	Video: Generative AI and LLM Risks
Content Analysis	Generative AI employs trained models to analyze content for potential threats and detect patterns linked to malicious websites, phishing attempts, or violations of security policies. Enhancing content filtering, it effectively flags or blocks harmful content.	Reading: Application of Generative AI in Content Filtering and Monitoring
Content Filtering	The process of screening and restricting access to specific internet content in order to decrease the risks associated with harmful websites, phishing, and inappropriate information within cybersecurity.	Reading: Application of Generative AI in Content Filtering and Monitoring
Contextual Bias	Bias arising when an LLM struggles to understand or interpret the context of a conversation or prompt accurately, leading to inappropriate or misleading responses.	Video: Generative AI and LLM Risks
Contextual Remediation	A process facilitated by generative AI in cybersecurity, where identified risks or issues can be communicated to relevant personnel for remediation. Generative AI assists in setting up remediation responses, reducing coordination efforts, and enabling certain commands or actions to be executed promptly for temporary mitigation before permanent actions are carried out.	Reading: Incident Response Using Generative AI
Continuous Monitoring and Detection	A real-time or near-real-time approach in AI-based systems for identifying and addressing vulnerabilities as soon as they arise. This minimizes the exposure window and enhances overall security by providing ongoing vigilance against emerging threats.	Video: Enhancing Vulnerability Management with Generative AI
Conventional AI	Traditional artificial intelligence operating within predetermined constraints, relying on fixed models for task execution and data analysis.	Video: Transition from Conventional AI to Generative AI and its Benefits in Cybersecurity
Cybersecurity Analytics	Advanced techniques employing diverse data sources like event logs, network packets, and user behavior with big-data technologies to identify, monitor, and safeguard digital environments.	Video: Cybersecurity Analytics Using Generative AI
Data Anonymization Techniques	Techniques employed during training to ensure that Generative AI models do not memorize specific details that could compromise privacy. These techniques safeguard sensitive information and prevent its accidental exposure in the generated content.	Video: Security Risks Associated with Using Generative AI Tools
Data Leakage	Occurs when an LLM unintentionally or maliciously reveals sensitive information, proprietary algorithms, or customer data, leading to unauthorized access, privacy violations, and security breaches.	Video: Generative AI and LLM Risks
Data Loss Prevention	Monitors data flows and user interactions to prevent data breaches and unauthorized exfiltration of sensitive information.	Video: Cybersecurity Analytics Using Generative AI
Data Poisoning	Compromised or manipulated training data that can lead to the generation of inaccurate or malicious outputs. This threat is particularly concerning in applications where precision and accuracy of data are paramount, such as cybersecurity scenarios.	Reading: Threats on Generative AI Models
Data Validation and Preprocessing	Procedures applied to ensure the integrity of training data for Generative AI models. Thorough validation and preprocessing help prevent risks associated with incomplete or biased data, contributing to the model's ability to generalize to real-world scenarios.	Video: Security Risks Associated with Using Generative AI Tools
Deception Technology	The use of AI-driven tactics to mislead attackers, such as generating false information about network assets. While effective in thwarting cyber threats, ethical concerns arise due to potential collateral damage, disruption to legitimate users, and the need to balance the effectiveness of deception with potential harm.	Video: Ethical Concerns of AI in Cybersecurity
Dwell Time	The duration between a cyberattack occurring and its detection and mitigation, reduced through swift reactions enabled by AI-driven automation.	Video: Leveraging AI for Advanced Threat Detection and Prevention
Dynamic Threat Hunting	The continuous analysis of network and system data by generative AI to identify and neutralize potential threats before escalation. Enables proactive defense against emerging threats, maintaining a vigilant security posture.	Reading: Applications of Generative AI on Different Tasks of Cybersecurity
Endpoint Detection and Response (EDR)	An AI-driven cybersecurity solution that monitors and analyzes the behavior of devices connected to a network. EDR helps detect and respond to potential threats rapidly, allowing organizations to understand the	Video: Unleashing the Power of Generative AI

Terms	Definition	First Introduced
	root cause and enhance overall security.	for Cybersecurity
Ethical AI Practices	Practices that involve the responsible use of Generative AI, considering ethical considerations in the development, deployment, and ongoing evolution of AI models in cybersecurity. These practices aim to mitigate risks and foster trust in AI technologies.	Video: Security Risks Associated with Using Generative AI Tools
Explainability	Involves providing transparency into how Generative AI models process information and make decisions. Enhancing models with explainability through interpretable AI techniques ensures that decision-making processes are transparent and easily understood by stakeholders.	Video: Security Risks Associated with Using Generative AI Tools
False Positives	Incorrect alerts or warnings generated by security systems, indicating a threat that does not actually exist.	Video: Leveraging AI for Advanced Threat Detection and Prevention
Forensic Analyses	A cybersecurity process involving the systematic collection, preservation, and analysis of digital evidence to fully understand security incidents. It focuses on uncovering cyber attack methods, identifying timelines, and determining threat actors. Performed after managing incidents, it supports legal proceedings, regulatory compliance, and enhances overall cybersecurity knowledge.	Video: Overview of Incident Response and Forensic Analysis
General Data Protection Regulation (GDPR)	A European Union regulation designed to protect individuals' privacy by regulating the processing of personal data.	Video: Leveraging AI for Advanced Threat Detection and Prevention
Generative AI	Advanced AI with a unique ability to create novel content, including images, text, and simulations. Known for adaptability, continual learning, and human-like comprehension in natural language processing tasks.	Video: Transition from Conventional AI to Generative AI and its Benefits in Cybersecurity
Generative AI for Incident Response and Forensic Analysis	The application of Generative AI in incident response and forensic analyses to enhance capabilities. Generative AI can improve automation, anomaly detection, and pattern recognition, providing valuable insights in managing and understanding security incidents.	Video: Overview of Incident Response and Forensic Analysis
Generative AI in Natural Language Understanding	The capability of Generative AI to detect and understand natural language, empowering security analysts to communicate with security tools seamlessly. This ensures that analysts can perform tasks and gather information without the need to learn intricate UIs or query languages.	Reading: Incident Response Using Generative AI
Group Attribution Bias	Bias emerging when an LLM attributes specific characteristics or behaviors to an entire group based on the actions of a few individuals, perpetuating harmful generalizations and prejudices.	Video: Generative AI and LLM Risks
Hallucination	The phenomenon where LLMs produce text that is factually inaccurate, overly indulgent, or nonsensical due to incomplete or conflicting training data.	Video: Generative AI and LLM Risks
Human Oversight	The necessity of human involvement and supervision in cybersecurity decision-making processes involving AI. Human oversight ensures a check on autonomous responses, preventing unintended consequences and errors that may arise from the actions of AI-driven cybersecurity systems.	Video: Ethical Concerns of AI in Cybersecurity
Human-Centric Approach	An approach to decision-making in cybersecurity that emphasizes the importance of human oversight and intervention, especially in complex and sensitive scenarios involving Generative AI. A human-centric approach provides a check against potential biases, errors, and ethical dilemmas that may arise in the autonomous operation of AI systems. It recognizes the indispensable role of human judgment in ensuring ethical conduct and aligning AI-driven cybersecurity practices with societal values.	Reading: Generative AI and Cybersecurity: Balancing Benefits and Ethical Concerns
IBM Endpoint Detection and Response (EDR)	IBM's Endpoint Detection and Response (EDR) is a sophisticated security solution designed to fortify organizations against evolving cyber threats at the endpoint level. It excels in real-time threat detection by continuously monitoring endpoint activities, employing behavioral analytics to identify anomalies, and integrating with threat intelligence feeds for up-to-date threat information. EDR supports detailed forensic analysis, ensures comprehensive endpoint visibility, and provides automated response actions based on predefined playbooks, empowering organizations to proactively defend against threats.	Video: Ways to Integrate Generative AI into SIEM
IBM QRadar	IBM QRadar is a prominent Security Information and Event Management (SIEM) system known for its robust capabilities in aggregating and correlating security event data from diverse sources. It provides real-time monitoring, threat detection, and incident response. IBM QRadar exemplifies the integration of advanced technologies, including Generative AI, to enhance cybersecurity capabilities. It is designed to offer comprehensive visibility into an organization's cybersecurity landscape and is adaptable to both on-premises and cloud-native architectures.	Video: Ways to Integrate Generative AI into SIEM
Impersonation	The act of pretending to be someone else with the intent to deceive or trick others. In the context of cyberattacks, generative conversational AI can be used for impersonation to trick employees into revealing sensitive information or to harm a business's reputation.	Video: Concerns & Considerations Using Generative AI in Cybersecurity
Inadequate Sandboxing	When an LLM lacks proper isolation during interactions, posing risks of exploitation, unauthorized access, or unintended actions.	Video: Generative AI and LLM Risks
Incident Response (IR)	A systematic method in cybersecurity for managing and resolving security incidents. It involves activities such as identification, containment, eradication, recovery, and learning from security incidents.	Video: Overview of Incident Response and Forensic Analysis
Incomplete Training Data	If the training data is incomplete or not representative of actual scenarios, the Generative AI model may struggle to generalize effectively. This can result in inaccurate or insecure outputs, impacting the reliability of the model in real-world applications.	Reading: Threats on Generative AI Models

Terms	Definition	First Introduced
Insecure Innovations	AI innovations developed without sufficient security considerations, leading to challenges such as loss of sensitive data, damage to credibility, business disruption, reputational harm, and financial losses.	Video: Concerns & Considerations Using Generative AI in Cybersecurity
Insufficient Access Controls	Occurs when access controls or authentication mechanisms are not correctly implemented, allowing unauthorized users to interact with the LLM and potentially exploit vulnerabilities.	Video: Guarding against NLP-based Attacks on Generative AI
Intelligent Prioritization	The ability of AI algorithms to analyze vulnerabilities based on severity, exploit likelihood, and business impact. It enables security teams to focus on the most critical issues, maximizing the effectiveness of remediation efforts.	Video: Enhancing Vulnerability Management with Generative AI
IoT Security	Monitors and protects IoT devices and networks, identifying vulnerabilities and unusual device behavior.	Video: Cybersecurity Analytics Using Generative AI
Lack of Transparency	Risks associated with the complexity of Generative AI models, where there is a need for more transparency into how they process information and make decisions. The lack of clear reasons for decisions makes it challenging for cybersecurity professionals to interpret and validate outputs.	Video: Security Risks Associated with Using Generative AI Tools
Large Language Model (LLM)	A machine-learning neural network trained on unlabeled or uncategorized text data, using a self-supervised or semi-supervised learning approach. LLMs, such as GPT-3 and GPT-4, have parameters ranging from millions to trillions and generate text predictions.	Video: Generative AI and LLM Risks
Leveraging Historical Data	The process of utilizing historical security event data sets within SIEM to train machine learning algorithms. This allows algorithms to understand normal behavior in an organization's IT environment, identify deviations and anomalies, and signal potential security threats. The leveraging of historical data is foundational to the effectiveness of machine learning in enhancing threat detection and response capabilities in SIEM.	Video: Advanced Threat Detection with Generative AI in SIEM
Linguistic Bias	Bias favoring certain linguistic styles, vocabularies, or cultural references over others, resulting in more relatable content to specific language groups or cultures while alienating others.	Video: Generative AI and LLM Risks
Machine Bias	Bias in LLMs originating from biases in the training data, perpetuating stereotypes and discriminations related to race, gender, ethnicity, and socioeconomic status.	Video: Generative AI and LLM Risks
Malware Detection and Analysis	The use of generative AI algorithms to analyze malware code structure, behavior, and signatures. This helps identify similarities and anomalies, enabling proactive protection of systems and networks against potential cyber threats.	Video: Unleashing the Power of Generative AI for Cybersecurity
Mitigating False Positives	Addressing the challenge of false positives in security alerts by using machine learning algorithms in SIEM. These algorithms establish baselines and learn from historical data to distinguish normal activities from abnormal or suspicious behavior. By reducing false positives, security teams can focus on genuine security incidents, avoiding alert fatigue and optimizing resource allocation for effective threat response.	Video: Advanced Threat Detection with Generative AI in SIEM
Model Bias	Inherent biases in LLMs further subdivided into various categories, including machine bias, availability bias, confirmation bias, selection bias, group attribution bias, contextual bias, linguistic bias, anchoring bias, and automation bias.	Video: Generative AI and LLM Risks
Natural Language Search	A search approach that allows security analysts to interact with security tools using natural language, eliminating the need to learn specific workflows or query languages. It enables analysts to focus on tasks by expressing queries or commands in a language they understand, improving efficiency and reducing the learning curve associated with different tools.	Reading: Incident Response Using Generative AI
Network Traffic	Involves the analysis of network traffic patterns and anomalies to detect intrusions, malware activity, and other network-based threats.	Video: Cybersecurity Analytics Using Generative AI
Phishing Detection	Generative AI excels in simulating authentic phishing attacks, aiding organizations in assessing and fortifying defenses against phishing threats. Monitoring responses to these simulations helps identify vulnerabilities and educates users on recognizing phishing attempts.	Reading: Application of Generative AI in Content Filtering and Monitoring
Playbooks in Cybersecurity	A cybersecurity response playbook is a detailed plan outlining the steps to be taken in the event of a security incident. Organizations often keep incident response plans simple and supplement them with specific cyber response playbooks for different types of incidents.	Video: Using Generative AI for Cybersecurity Report Summarization and Playbooks
Policy and Compliance Management	The responsibility of generative AI in automating the generation and adaptation of security policies. This includes aligning policies with compliance requirements and adapting to emerging threats, contributing to robust policy and compliance management	Reading: Applications of Generative AI on Different Tasks of Cybersecurity
Potential for Offensive Use	The acknowledgment of Generative AI technologies having a dual-use nature, where they can be repurposed for offensive activities. This recognition underscores the need for constant vigilance to stay ahead of evolving threats and emphasizes the importance of ethical considerations in the development and deployment of AI technologies in cybersecurity. Balancing defensive capabilities with ethical concerns is crucial for responsible technology use and deployment.	Reading: Generative AI and Cybersecurity: Balancing Benefits and Ethical Concerns
Predictive Analytics	The use of historical data and trends to forecast potential cybersecurity threats, enabling organizations to implement preemptive defense strategies.	Video: Leveraging AI for Advanced Threat Detection and Prevention

Terms	Definition	First Introduced
Prompt Injection	Bypassing filters or manipulating the LLM with crafted prompts to make the model ignore previous instructions, leading to unintended consequences like data leakage or unauthorized access.	Video: Guarding against NLP-based Attacks on Generative AI
Quality of Training Data	Risks arising from the heavy dependence of Generative AI tools on the quality and diversity of training data. Models trained on incomplete or biased data may fail to generalize to real-world scenarios, leading to security vulnerabilities.	Video: Security Risks Associated with Using Generative AI Tools
Real-Time Threat Analysis	The capability of AI systems to continually monitor network traffic, user behavior, and system logs in real-time for immediate detection and insights into potential threats.	Video: Leveraging AI for Advanced Threat Detection and Prevention
Reduced False Positives	Utilizes machine learning algorithms to decrease false positive alerts, enabling focused efforts on genuine threats and avoiding wasted time on harmless events.	Video: Cybersecurity Analytics Using Generative AI
Reduced Response Time	Contribution of Generative AI to swift incident responses, minimizing the impact of security breaches through automated analysis and recommendation processes.	Video: Transition from Conventional AI to Generative AI and its Benefits in Cybersecurity
Scalability	The ability of AI systems to handle large volumes of data and adapt as organizations grow, emphasizing efficiency and adaptability.	Video: Leveraging AI for Advanced Threat Detection and Prevention
Security Information and Event Management (SIEM)	A comprehensive solution that combines Security Information Management (SIM) and Security Event Management (SEM) to provide real-time analysis of security alerts generated throughout an organization's IT infrastructure. SIEM collects and aggregates log data, correlates events, performs analysis, and generates reports to help organizations meet compliance requirements and enhance their cybersecurity posture.	Video: Advanced Threat Detection with Generative AI in SIEM
Security-by-Design Approach	A proactive approach to AI development that integrates cybersecurity seamlessly into every stage of the AI development lifecycle. It involves prioritizing data integrity, implementing measures like access controls, encryption, security audits, and timely vulnerability remediation.	Video: Issues, Concerns & Considerations Using Generative AI in Cybersecurity
Selection Bias	Bias arising when training data does not represent the entire population or target audience, leading to a lack of knowledge for unbiased and comprehensive content generation.	Video: Generative AI and LLM Risks
SSRF Vulnerabilities	Server-Side Request Forgery vulnerabilities that enable attackers to manipulate an LLM to execute unintended requests or gain unauthorized access to restricted resources.	Video: Generative AI and LLM Risks
Threat Detection	Recognizes diverse threats, such as malware, phishing attacks, and insider threats, by analyzing network traffic and system logs for anomalies and suspicious activities.	Video: Cybersecurity Analytics Using Generative AI
Threat Intelligence	Involves collecting and analyzing external threat intelligence feeds, examining IoCs and TTPs used by threat actors.	Video: Cybersecurity Analytics Using Generative AI
Traditional Vulnerability Management Systems	Conventional approaches that rely on manual efforts, making them time-consuming, error-prone, and limited in scale and speed. They focus mainly on identifying vulnerabilities, lack contextual analysis, and operate reactively, addressing vulnerabilities only after discovery.	Video: Enhancing Vulnerability Management with Generative AI
Triage in Cybersecurity	The process of prioritizing and categorizing security incidents for efficient responses. Analysts assess incidents based on severity, impact, and relevance, assigning priority levels and allocating resources accordingly. This optimization ensures critical incidents receive immediate attention. Automated tools and AI, such as Generative AI, can enhance the triage process.	Video: Triage Potential Incidents, Analyze Logs, and Assist Investigations
User and Entity Behavior Analytics (UEBA)	Monitors and analyzes user and entity behavior, detects anomalies and potential security threats, and identifies insider threats and compromised accounts.	Video: Cybersecurity Analytics Using Generative AI
Unauthorized Code Execution	Description: Occurs when an attacker exploits an LLM to execute malicious code or actions on the underlying system through natural language prompts.	Video: Guarding against NLP-based Attacks on Generative AI
Unified Interface (UAX)	A modern and consolidated interface in the QRadar Suite, developed with input from security analysts. It provides a consistent experience for investigating threats across various security tools, enhancing efficiency in responding to and hunting for threats.	Reading: ChatGPT with QRadar/any SIEM tool
Vulnerability Assessment and Patching	The use of generative models to simulate diverse cyberattacks, identifying potential weaknesses in systems. Guides security administrators in prioritizing and implementing necessary patches and updates to address vulnerabilities proactively.	Reading: Applications of Generative AI on Different Tasks of Cybersecurity
Vulnerability Management	A continuous process involving the identification, categorization, mitigation, and monitoring of vulnerabilities in software, networks, and computer systems. It aims to safeguard digital assets, prevent cyber threats, and maintain a secure and resilient IT infrastructure.	Video: Enhancing Vulnerability Management with Generative AI
Vulnerability to Adversarial Attacks	The susceptibility of Generative AI models to manipulations through adversarial attacks. Adversarial attacks involve making slight modifications to input data, leading to misclassification and raising doubts about the reliability and robustness of AI-driven cybersecurity measures. Safeguarding against adversarial attacks is crucial for ensuring the trustworthiness and effectiveness of generative models in cybersecurity.	Reading: Generative AI and Cybersecurity: Balancing Benefits and Ethical Concerns

Terms	Definition	First Introduced
Zero-Day Exploit	A tactic where hackers exploit previously unknown vulnerabilities in software or systems, posing a serious threat as there is no pre-existing defense.	Video: Leveraging AI for Advanced Threat Detection and Prevention

Author: Manish Kumar