VERSA

Security Use Cases for AI

July 2024

General Disclaimer

Although Versa Networks has attempted to provide accurate information in this guide, Versa Networks does not warrant or guarantee the accuracy of the information provided herein. Versa Networks may change the programs or products mentioned at any time without prior notice. Mention of non-Versa Networks products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

Security threats are increasing in both volume and sophistication. Traditional security measures alone often fall short. Artificial intelligence (AI) enhances cybersecurity by providing advanced tools for threat detection, incident response, user behavior analytics, malware detection, and data loss prevention. Discover the top five AI use cases in cybersecurity and how they strengthen traditional approaches.

1. Threat Detection and Prevention

Artificial intelligence enhances threat detection and prevention by analyzing vast amounts of network traffic, user behavior, and system activities in real-time to identify potential threats. By leveraging machine learning models, AI systems can detect anomalies and patterns indicative of malicious activity, providing early warnings and automated responses to mitigate cyberattacks.

Key Features:

- Real-time monitoring
- Anomaly detection
- Machine learning algorithms
- Automated threat response

Key Benefits:

- Improved threat detection accuracy
- Reduced false positives
- Faster incident response
- Enhanced protection against sophisticated threats

Why AI is an Enhancement: Traditional threat detection methods are effective at identifying known threats using predefined signatures and rules. AI enhances these methods by continuously learning from new data, enabling the detection of emerging threats and sophisticated attacks. Real-time monitoring and anomaly detection provide faster identification of potential threats, while automated responses reduce the time to mitigate attacks, enhancing overall security.

2. Accelerated Incident Response

AI-driven tools streamline the incident response process by building correlating disparate data points, building detailed context around incidents, automating routine tasks, and reducing the time and effort required to address security incidents. These systems isolate affected systems, block malicious traffic, and provide comprehensive context in real-time, allowing security teams to make informed decisions quickly.

Key Features:

- Context building and correlation
- Automated workflows
- Real-time action
- Comprehensive incident analysis

Key Benefits:

- Faster resolution of incidents
- Reduced manual workload
- Improved decision-making
- Enhanced operational efficiency

Why AI is an Enhancement: Traditional incident response relies heavily on manual processes, which are thorough but can be time-consuming. AI enhances these processes by building detailed context around incidents through data correlation and analysis, ensuring rapid and consistent responses. By automating routine tasks, AI allows security teams to focus on strategic decisions. This comprehensive context and automation not only reduce the workload on security teams but also accelerate incident resolution and improve the organization's resilience to future threats.

3. User Entity Behavior Analytics (UEBA)

User Entity Behavior Analytics (UEBA) powered by artificial intelligence is a critical component in modern cybersecurity strategies. AI-driven UEBA systems monitor and analyze user activities to establish a baseline of normal behavior. By continuously learning from these patterns, AI can detect deviations that may indicate insider threats, compromised accounts, or other security issues. The ability to identify unusual or suspicious activities in real-time allows organizations to respond swiftly to potential threats.

Key Features:

- Behavioral baselines
- Anomaly detection
- Real-time monitoring
- Insider threat identification

Key Benefits:

- Early detection of insider threats
- Improved account security
- Enhanced visibility into user activities
- Reduced risk of data breaches

Why AI is an Enhancement: Traditional UEBA methods effectively monitor user activities using static rules and thresholds. AI enhances these methods by continuously learning from user behavior, adapting to new patterns, and detecting anomalies more accurately. This dynamic approach provides better detection of insider threats and compromised accounts, offering real-time insights and reducing the risk of data breaches, while also ensuring compliance with security policies.

4. Malware Detection and Analysis

Artificial intelligence has transformed malware detection and analysis, providing advanced capabilities to identify and mitigate threats. AI-driven systems utilize machine learning models to analyze files, network traffic, and system behavior for patterns indicative of malware. Unlike traditional signature-based approaches, AI can detect previously unknown malware by recognizing malicious behaviors and characteristics.

Key Features:

- Machine learning models
- Pattern recognition
- Behavioral analysis
- Automated malware analysis

Key Benefits:

- Detection of zero-day threats
- Faster malware identification
- Comprehensive threat analysis
- Enhanced protection against sophisticated malware

Why AI is an Enhancement: Traditional malware detection methods are proficient at identifying known malware using signature-based techniques. AI enhances these methods by using behavioral analysis and pattern recognition to detect malicious activity, including zero-day threats. This proactive approach allows for faster identification and mitigation of malware, providing comprehensive threat analysis and enhanced protection against sophisticated attacks.

5. Data Loss Prevention

Artificial intelligence plays a pivotal role in enhancing data loss prevention (DLP) strategies within cybersecurity frameworks. AI-driven DLP systems continuously monitor and analyze data movements across the organization to identify and prevent unauthorized data exfiltration. By leveraging machine learning algorithms, AI can detect anomalies and patterns indicative of potential data breaches, ensuring sensitive information remains secure.

Key Features:

- Real-time data monitoring
- Anomaly detection
- Machine learning algorithms
- Automated data protection

Key Benefits:

- Proactive data breach prevention
- Improved data security
- Enhanced compliance with data protection regulations
- Reduced risk of data exfiltration

Why AI is an Enhancement: Traditional DLP methods effectively protect data using static rules and keyword matching. AI enhances these methods by employing machine learning to detect anomalies in data usage and transfer, providing a more dynamic and accurate approach to data protection. This allows for real-time monitoring and automated responses to potential data breaches, improving overall data security and ensuring compliance with data protection regulations.

Learn more at www.versa-networks.com
Follow us @versanetworks.

2550 Great America Way, Suite 350 | Santa Clara, CA | 95054