How Machine Learning Enhances Cybersecurity and Mitigates Threats

Carl Lochstampfor Jr

Department of Cybersecurity, Old Dominion University,

CYSE 420 — Applied Machine Learning in Cybersecurity

January 24, 2026

How Machine Learning Enhances Cybersecurity and Mitigates Threats

Exploring ML Benefits

Machine learning (ML) processes large amounts of data in real time, uncovering patterns that many traditional tools would not detect. In particular, ML models detect anomalies—ranging from unusual login hours to lateral movement and data exfiltration—by establishing behavioral baselines for users, endpoints, and networks. Unsupervised anomaly detection and behavioral analytics models are particularly effective in this context, as they identify deviations from normal activity without relying on predefined signatures. As cyberattacks become more sophisticated, these capabilities are game changers; thus, demonstrating the power of ML in countering specific threats underscores its value.

Mitigating Cyber Threats: Phishing

Phishing remains one of the most prevalent cyber threats. Supervised ML models trained on large datasets of malicious and legitimate emails can identify phishing attempts by analyzing sender reputation, URL structures, email metadata, and linguistic patterns. Building on these capabilities, natural language processing (NLP) further improves detection by recognizing social engineering techniques such as urgency, impersonation, and emotional manipulation. Furthermore, the 2025 Verizon Data Breach Investigations Report (DBIR) notes phishing and related attacks are increasingly aimed at people, underscoring the need for machine learning to support rapid detection and response. However, organizations should also understand that deploying these ML tools introduces additional challenges.

Challenges and Considerations

While advances have been made, machine learning poses new problems. Quality and unbiased data are critical, and although governance and ongoing retraining can help models adapt, bias can negatively affect performance. With the help of explainable AI and feature analysis, security teams can better understand model decisions, pulling back the “black-box” curtain and increasing their trust and accountability in ML models. S&P Global reports that weak AI infrastructure causes operational problems: scalable cloud and hybrid setups are solving some of these issues. Furthermore, defenses against adversarial manipulation include adversarial training, model ensembles, and layering machine learning with older controls. Organizations are responding to these challenges by turning to pragmatic cybersecurity based on machine learning.

Real-World Applications

Security analytics and threat intelligence platforms are now powered by machine learning. For instance, an S&P Global Market Intelligence (2024) profile shares a firm that uses AI to quickly extract insights from SEC filings, illustrating how ML can help parse unstructured data for quick decision-making. In addition, NIST (2024) frameworks highlight machine learning as a significant key enabler of flexible, risk-informed defenses. Together, these examples demonstrate how machine learning has evolved from an emerging capability into a foundational component of modern, risk-informed cybersecurity operations.

References

National Institute of Standards and Technology (NIST). (2024). *Cybersecurity framework 2.0*. Retrieved on January 24, 2026 from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

S&P Global Market Intelligence. (2024). *A professional services firm leverages AI to uncover insights from SEC filings*. Retrieved on January 24, 2026, from https://www.spglobal.com/market-intelligence/en/news-insights/research/a-professional-services-firm-leverages-ai-to-quickly-uncover-actionable-insights-from-sec-filings

S&P Global Market Intelligence. (2025). *AI infrastructure divide defines generative AI success*. Retrieved on January 24, 2026, from https://www.spglobal.com/market-intelligence/en/news-insights/research/ai-infrastructure-divide-defines-generative-ai-success-highlights-from-vote-ai-machine-learning

Verizon. (2025). *Data breach investigations report*. Retrieved on January 24, 2026, from https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf