Autonomous Cybersecurity

short paper

Jeffrey L Duffany, Ph.D.
Politechnic University of Puerto Rico
jduffany@pupr.edu

Extended Abstract

Autonomous cybersecurity refers to the use of artificial intelligence (AI), machine learning (ML), and automation to detect, prevent and respond to cyber threats with minimal human intervention. It aims to enhance traditional cybersecurity by improving speed, accuracy, and adaptability to emerging threats. The main benefits are faster threat mitigation, reduced reliance on human analysts, improved accuracy in threat detection and scalability across large networks. Some of the major challenges include sophisticated adversarial attacks against AI models and ethical concerns around full automation. Autonomous cybersecurity systems leverage AI, machine learning (ML) and automation to identify and neutralize cyber threats in real time. This approach significantly enhances an organization's ability to counter advanced cyberattacks.

For example autonomous cybersecurity can be used to analyze network traffic, user behavior and system logs to identify anomalies. Automated response can neutralize threats in real time for example isolating compromised devices and blocking malicious IPs. Self-Learning technologies can use ML to improve threat intelligence by learning from past attacks and by dynamically adapting security policies based on evolving attack patterns. Automated incident response can be provided using Security Orchestration, Automation, and Response (SOAR) platforms which streamline investigations and responses and are capable of rapidly mitigating threats like ransomware without waiting for human input. In addition, AI-driven ethical hacking tools can provide autonomous penetration testing which continuously test for vulnerabilities to help organizations proactively fix weaknesses before exploitation.

Autonomous cybersecurity systems are still in their infancy. They involve something called hard AI which requires capabilities similar to human cognition. To date there has not yet been developed a truly autonomous cyberdefense system. However we are currently seeing the evolution of next generation firewalls which are moving in the direction of autonomous cyberdefense systems. Key features of next generation firewalls incude deep packet inspection which analyzes packet contents rather than just source and destination while detecting and blocking threats hidden in legitimate traffic. Application-Aware filtering identifies and controls applications, e.g., blocking specific applications and preventing unauthorized applications from consuming bandwidth or being used for cyberattacks. Intrusion Prevention System (IPS) technologies are used to detect and block known attack patterns. Threat Intelligence Integration is used to continuously update databases to detect new malware, phishing attempts and botnets useing real-time threat intelligence to stop zero-day attacks. AI-powered analytics are used to prevent advanced persistent threats (APTs) and include advanced features to protect cloud environments and Internet of Things (IoT) devices from cyber threats.

References

1. Andrew Lohn, Anna Knack, Ant Burke, Krystal Jackson "Autonomous Cyber Defense: A Roadmap from Lab to Ops", Policy Brief, CETAS Centre for Emerging Technology and Security, June2023.
2. Anna Knack, Ant Burke, " Autonomous Cyber Defense: Authorized Bounds for Autonomous Agents", Policy Brief, CETAS Centre for Emerging Technology and Security, May 2024.
3. Jason Sparapani, Laurel Ruma, "Preparing for AI-enabled cyberattacks", MIT Technology Review, 2021.
4. Diego Abreu, Christian Rothenberg, Antonio Abelém, "QML-IDS: Quantum Machine Learning Intrusion Detection System", arXiv:2410.16308v1 [cs.CR] 07 Oct 2024.
5. T.Saranyaa, S.Sridevi, Tran Duc, "Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review", Third International Conference on Computing and Network Communications (CoCoNet'19), Procedia Computer Science 171 (2020) 1251–1260.