Application of AI in CyberSecurity

Kanishk Thamman

6/18/2024

PURDUE UNIVERSITY

Kanishk Thamman

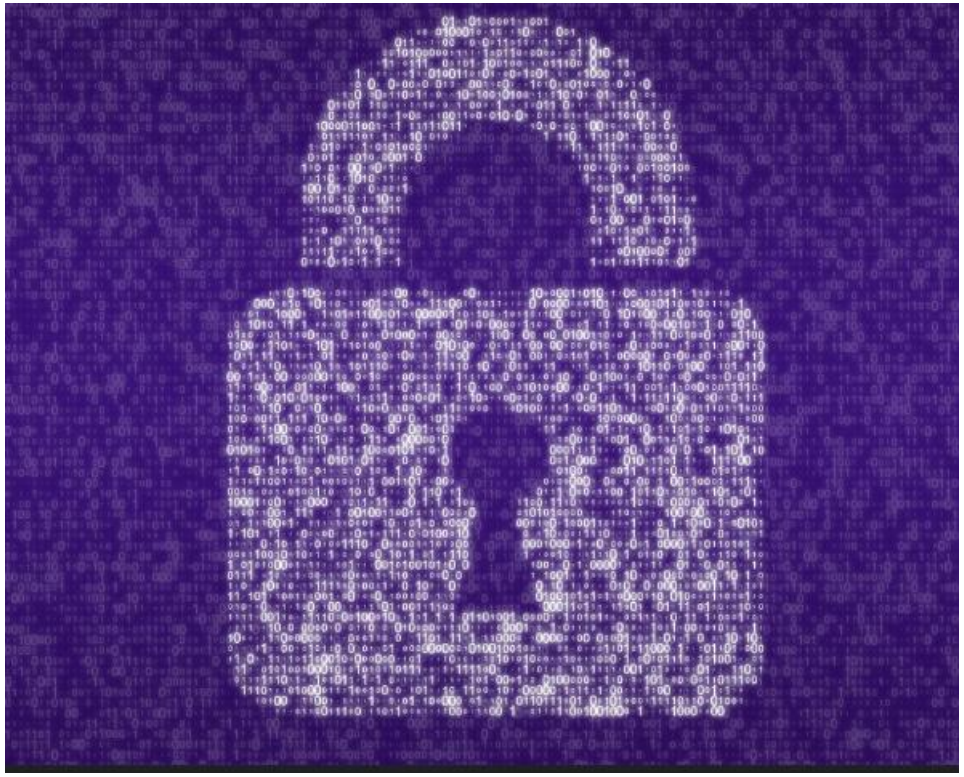
Junior at Wakeland High, TX

- CCST Cybersecurity
- IT Specialist - Cybersecurity
- I love AI and Cyber Security
- In my free time, I help with audio and lights for shows

What is Autonomous CyberDefense ?

Autonomous Cyber Defense describes systems capable of protecting organizations and users through system hardening, network and endpoint management, threat detection, and intrusion response and recovery, without direct human tasking.

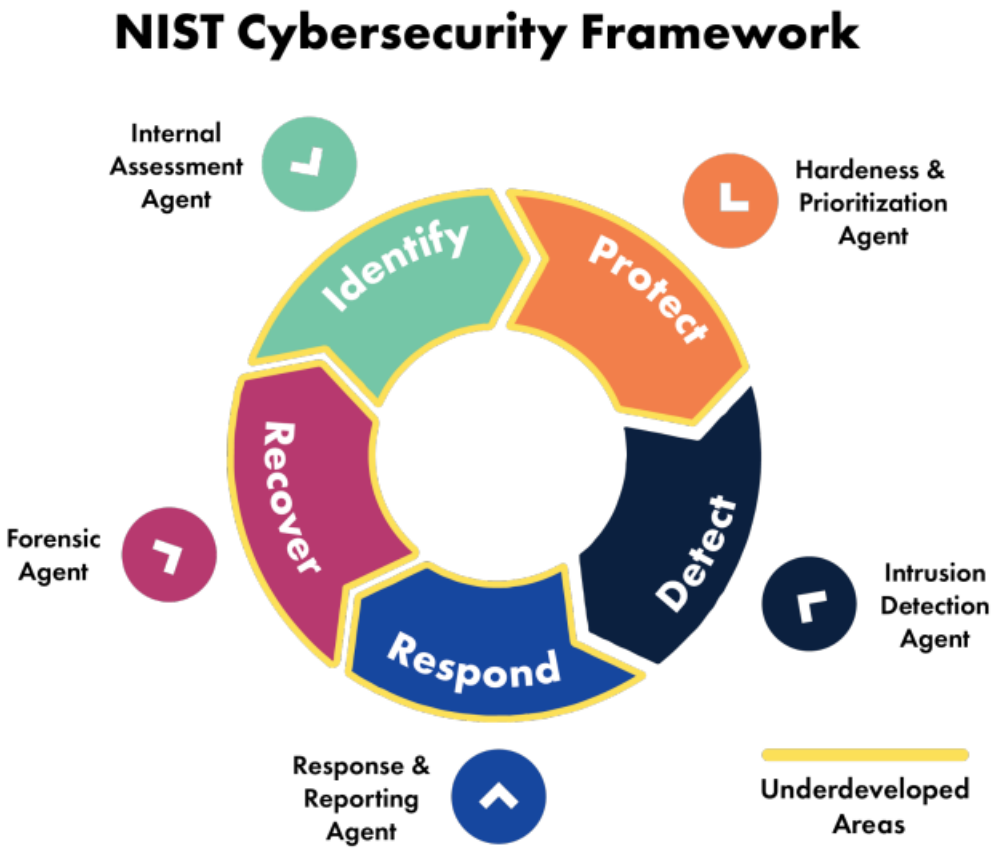
(Lohn et al.)



Source: https://blogs.uwe.ac.uk/cyber-security-cyber-crime/measuring-the-suitability-of-artificial-intelligence-in-autonomous-resilience-for-cyber-defence/

PURDUE UNIVERSITY

Why Autonomous CyberDefense ?



(Lohn et al.)

Example Use Cases:

- Using AI to detect and take action against a cyber attack
- Autonomous software pen-testing to look for vulnerabilities
- Predictive approach to CyberSecurity

PURDUE UNIVERSITY

Why do I like Autonomous CyberDefense ?

(H. Jahankhani et al.)

- It can be cost effective since it is one tool for small companies
- It allows for better and faster control and incident response which will help prevent or mitigate the extent of an attack
- Its development and inception is inevitable, might as well help the Whitehat hackers implement it first
- Its an Emerging Technology which means that I can contribute and make a huge impact

How would Autonomous CyberDefense work?

Human to machine

- Highly specific allow and deny lists tailored to specific organisations.
- Categorises alert thresholds.
- Feedback loops to question and challenge decisions of autonomous agents.
- Real-time threat intelligence and example events likely to be of interest.
- Failsafe mode to intercept and reverse autonomous agent actions.

Machine to human

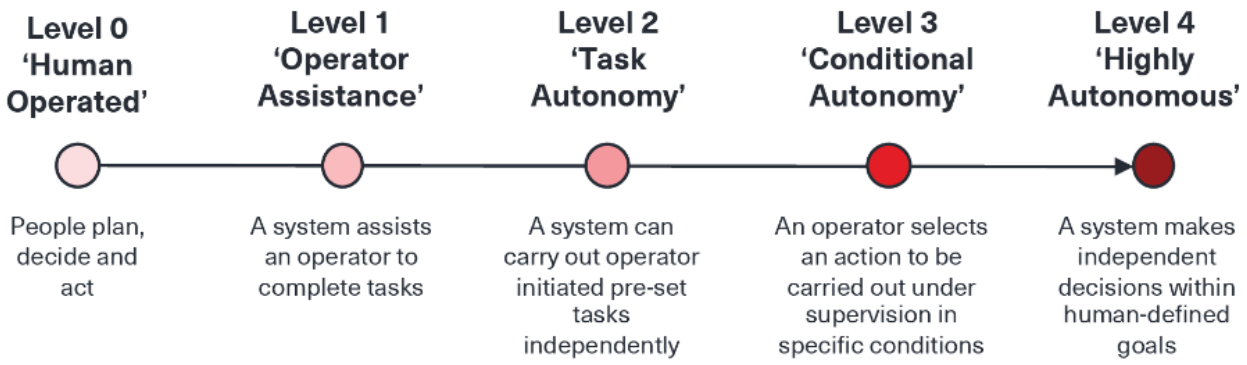
- Filters alerts to minimise noise.
- Large language models generate text-based summaries.
- Surfaces actions for review after initiating action with a human-edit loop.
- Reminder prompts for long-standing actions.

(Knack and Burke)

Future Implications of Autonomous CyberDefense

D3FEND Component	Level of Autonomy			
	L1: Operator Assistance	L2: Task Autonomy	L3: Conditional Autonomy	L4: Highly Autonomous
Harden	3.83	6.83	6.33	5
Detect	2	2	5.5	13.5
Isolate	2	7.5	9.5	4
Evict	2.75	10.58	4.58	5.08
Restore	5	7	6	6
Deceive	3.75	4.75	9.25	4.25

(Knack and Burke)



PURDUE UNIVERSITY

Thank You

Kanishk Thamman

Kanishk-Thamman

kthamman@purdue.edu

PURDUE UNIVERSITY

Work Cited

Jahankhani, H., Meda, L.N.K., Samadi, M. (2022). Cybersecurity Challenges in Small and Medium Enterprise (SMEs). In: Jahankhani, H., V. Kilpin, D., Kendzierskyj, S. (eds) Blockchain and Other Emerging Technologies for Digital Business Strategies. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-98225-6_1

Anna Knack and Ant Burke, “Autonomous Cyber Defence: Authorisedbounds for autonomous agents,” CETaS Briefing Papers (May 2024).

Andrew Lohn, Anna Knack, Ant Burke, and Krystal Jackson, "Autonomous Cyber Defense" (Center for Security and Emerging Technology, June 2023). https://doi.org/10.51593/2022CA007