**Literature Review and Case Study**

**1. Research and Literature Review**  
  
**(a)** The last digit of my CWID is 8,   
  
Two Cybersecurity AI Computer System/Tool Instances:

Deep Instinct

Darktrace

**(b) Functions of Each Program:**

**1. Deep Instinct:**

Prevention-First Approach: Deep Instinct emphasizes a proactive stance against cyber threats, particularly ransomware. It boasts the capability to halt threats in less than 20 milliseconds, which is a staggering 750 times quicker than the fastest known ransomware encryption process.

Deep Learning Framework: Founded in 2015, Deep Instinct introduced the world's first deep learning cybersecurity framework. This framework is adept at understanding the intricate digital nuances of an organization, thereby discerning normal activities from potential threats.

Rapid Threat Classification: The platform is renowned for its swift classification and decision-making prowess. It significantly reduces false positives, allowing cybersecurity teams to focus on genuine threats and bolster their security posture.

**2. Darktrace:**

Self-Learning AI: Darktrace's AI is unparalleled in its ability to learn and understand an organization's digital environment. It discerns regular activities and can swiftly identify anomalies, making it adept at tackling even the most sophisticated cyber-attacks.

Instant Threat Visibility: Darktrace DETECT offers immediate insights into threats, even those that employ novel malware strains or innovative techniques.

Responsive Action: Upon detecting an ongoing threat, Darktrace RESPOND intervenes with surgical precision to halt unpredictable and swift attacks. It enforces a sense of 'normalcy', containing the threat without hampering regular business operations.

**(c) AI Technologies Leveraged:**

**1. Deep Instinct:**

Deep Learning: The core of Deep Instinct's platform is its deep learning framework, which offers a profound understanding of an organization's digital operations.

Automated Static Analysis: This technology is grounded in raw data, enabling comprehensive protection against an array of threats and file types without the need for human intervention.

Fast Classification: Deep Instinct's rapid classification mechanism is instrumental in reducing false positives, ensuring that genuine threats are promptly addressed.

**2. Darktrace:**

Self-Learning AI: Darktrace's AI continuously evolves, offering a bespoke understanding of an organization's digital environment.

Cyber AI Loop: This is an always-on, AI-driven feedback system that fortifies and hardens the entire security ecosystem. It's a holistic set of cybersecurity capabilities that addresses the need to reduce business risks.

Deep Learning: Darktrace employs deep learning to provide faster and more accurate malware classification. This not only prevents threats but also augments the Endpoint Detection and Response (EDR) with superior data to speed up investigations.

In terms of data utilization, both platforms harness vast amounts of organizational data to train their AI models. This data encompasses regular digital operations, user behaviors, network traffic, and more. By analyzing this data, the AI models can discern patterns, recognize anomalies, and predict potential threats.

**(d) Performance:**

**1. Deep Instinct:**

Deep Instinct prides itself on its deep learning capabilities, which is a subset of machine learning. The system's performance is often compared to traditional antivirus solutions, and it has been reported to exhibit a remarkable 99.78% accuracy rate for detection and prevention across unknown and custom attacks source. While it's challenging to draw a direct comparison between AI systems and human capabilities, the sheer speed and vast data processing abilities of Deep Instinct give it an edge in real-time threat detection.

**2. Darktrace:**

Darktrace employs a unique approach, leveraging self-learning AI to detect and combat cyber threats. Customers have given Darktrace's capabilities high ratings, with an average of 4.7 out of 5 stars source. Again, while comparing AI to human performance can be nebulous, Darktrace's real-time threat detection and rapid response times showcase its prowess in the cybersecurity realm.

**(e) Experimental or Fielded:**

**1. Deep Instinct:**  
Deep Instinct is not merely an experimental tool; it has been fielded and is operational. The platform has been adopted by various organizations, emphasizing its prevention-first approach source. The exact number of users is proprietary, but given its market presence, it's safe to assume a substantial user base. As for expertise, while the underlying technology is complex, the user interface is designed to be intuitive, allowing professionals with varying levels of cybersecurity knowledge to utilize it effectively.

**2. Darktrace:**

Darktrace is a fielded program, with its AI technologies being adopted by numerous organizations worldwide. The exact number of users is proprietary, but given its acclaim and market presence, it's evident that it has a significant user base. As for user expertise, Darktrace is designed to be intuitive, allowing users with varying levels of cybersecurity expertise to harness its capabilities effectively.

**(f) Why intelligence:**

**1. Deep Instinct:**

The intelligence of Deep Instinct stems from its deep learning framework, which is specifically tailored for cybersecurity. This allows it to predict and prevent a wide range of cyber threats, distinguishing it from traditional reactive security tools.

**2. Darktrace:**

Darktrace's intelligence is rooted in its self-learning AI, which continuously adapts to new threats and the evolving digital environment of an organization. This dynamic learning capability, paired with its ability to detect anomalies in real-time, sets it apart as an intelligent system.

**(g) Programming Languages and Environments used, UI:**

**1. Deep Instinct:**

From the information available, Deep Instinct has been associated with the Go programming language, particularly when researching specific malware variants source. However, the primary programming language and environment used for the core development of Deep Instinct's platform aren't explicitly mentioned in the sources. As for the user interface, while the exact details are not provided, one can infer from the company's website and other materials that it's designed to be intuitive and user-friendly, catering to both technical and non-technical users.

**2. Darktrace:**

Darktrace utilizes a variety of technologies, including Microsoft Azure, JavaScript, and Laravel source. However, the core programming language and environment for Darktrace's primary development remain unspecified in the available sources. Darktrace's product is known to employ unsupervised machine learning techniques to understand the "pattern of life" for every network, device, and user source. Regarding the user interface, while specific details are not provided, Darktrace's platform is designed to be intuitive, with visualizations and insights that allow users to quickly understand and act upon potential threats.

**h. References**

6Sense. (n.d.). Darktrace Company Insights, Tech Stack, and Competitors. 6Sense. https://6sense.com/company/darktrace/5b8916d37c866675e5114dd1

Bradley, T. (2022, July 25). Proof is in the pudding for Deep Instinct. Forbes.

https://www.forbes.com/sites/tonybradley/2022/07/25/proof-is-in-the-pudding- for-deep-instinct/?sh=2bf6d4c76f19

Darktrace. (n.d.). Cyber security that learns you. Darktrace. Retrieved from

<https://darktrace.com/>

Darktrace. (n.d.). Darktrace named a customers' choice in Gartner Peer Insights™ voice of the customer for network detection and response. *Darktrace*.

<https://darktrace.com/news/darktrace-gartner-peer-insights>

Deep Instinct. (n.d.). Arid Gopher Definition. Deep Instinct.

https://www.deepinstinct.com/glossary/arid-gopher-definition

Deep Instinct. (n.d.). The deep learning cybersecurity platform. Deep Instinct. Retrieved from <https://www.deepinstinct.com/>

**2. Case Study**

**(a) Supermarket Barcode Scanners:**

How can a simple barcode scanner be an instance of AI? These scanners are designed to recognize patterns (barcodes) and convert them into meaningful information (product details and prices). However, their functionality is pretty deterministic and rule-based. They don't "learn" or adapt over time. So, while they're incredibly efficient and useful, I'd argue that they don't quite fit the bill of what we'd traditionally consider as AI. They're more of a tool with a specific function rather than an intelligent agent.

**(b) Voice-activated Telephone Menus:**

The classic "Press 1 for English" systems. These systems employ speech recognition, which is a subset of AI. They're designed to understand and interpret human voice inputs and route the call based on the user's needs. Given that they can interpret and act upon auditory data, they exhibit a level of artificial intelligence. However, their intelligence is somewhat limited to the predefined commands they're programmed to recognize. Still, I'd say they're a step closer to AI than our barcode scanners.

**(c) Spelling and Grammar Correction in Microsoft Word:**

Microsoft Word's spelling and grammar checkers are more advanced than one might initially think. They don't just match words against a dictionary; they analyze sentence structures, context, and even offer style suggestions. Over time, with updates and user feedback, these features have evolved and improved. Given their ability to process natural language and provide context-aware corrections, I'd confidently categorize them as an instance of AI.

**(d) Internet Routing Algorithms:**

These algorithms are the unsung heroes of our daily internet browsing sessions. They dynamically determine the best path for data packets to travel from one computer to another. By considering factors like network congestion, failures, and latency, they adapt in real-time. This adaptability and responsiveness to a changing environment align well with our understanding of AI. They're not just following a set script; they're making decisions based on the current state of the network. So, in my book, they're a solid example of AI in action.

**(e) Virtual Assistants like Siri, Google Assistant, and Alexa:**

The heavy hitters of the AI world! These virtual assistants are designed to understand, process, and generate natural language. They can answer questions, control smart home devices, play music, set reminders, and so much more. Their capabilities are continually expanding as they learn from vast amounts of user data. They're not just reactive; they can proactively assist users based on patterns and preferences. Given their deep learning capabilities and the breadth of tasks they can perform, they’re prime examples of advanced AI systems.

**3. Agent and Environment**

**(a) PEAS Description of the Task Environment:**

Performance Measure: The primary goal is energy efficiency. So, the performance would be measured by how effectively the thermostat maintains the desired temperature while minimizing energy consumption.

Environment: The room or space where the thermostat is located, including factors like external temperature, insulation, number of occupants, and other heat sources.

Actuators: The switch or mechanism that turns the Air Conditioner (AC) on or off.

Sensors: Temperature sensors that detect the current room temperature and compare it to the desired setting.

**(b) Characterization of the Environment:**

Fully observable vs. Partially observable: Fully observable. The thermostat can directly sense the temperature, which is the primary factor for its decision-making.

Deterministic vs. Stochastic: Deterministic. Given the current temperature and the setting, the thermostat has a clear rule to decide whether to turn the AC on or off.

Episodic vs. Sequential: Sequential. The thermostat's decision at one time can affect future decisions, especially if the AC's effects aren't immediate.

Static vs. Dynamic: Dynamic. The temperature can change even if the agent doesn't take action, especially due to external factors.

Discrete vs. Continuous: Discrete in terms of the decision to turn the AC on or off, but continuous concerning the range of temperatures it can sense.

Single agent vs. Multiagent: Single agent. Only one thermostat is making decisions about the AC.

**(c) Possible States:**

Considering the thermostat's function, the possible states can be defined by:

1. Current temperature (relative to the setting: more than 3 degrees below, between 3 degrees below and 3 degrees above, more than 3 degrees above).

2. AC status (On or Off).

So, combining these factors, we have:

Temperature >3 degrees below setting & AC On

Temperature >3 degrees below setting & AC Off

Temperature between 3 degrees below and 3 degrees above setting & AC On

Temperature between 3 degrees below and 3 degrees above setting & AC Off

Temperature >3 degrees above setting & AC On

Temperature >3 degrees above setting & AC Off

That gives us a total of 6 possible states.

**(d) Type of Agent:**

The thermostat can be classified as a simple reflex agent. Here's why:

* It directly maps current percepts (temperature readings) to actions (turning AC on or off) based on predefined rules.
* It doesn't maintain an internal model of the world (like a model-based agent would).
* It doesn't have explicit goals that it plans to achieve (like a goal-based agent).
* It doesn't maximize a utility function (unlike a utility-based agent).
* And it doesn't learn from past experiences to improve performance (unlike a learning agent).

The thermostat simply reacts to the current temperature without considering past states or predicting future ones.