COGNITIVE SECURITY INSTITUTE

Introduction to the Cognitive Security Institute

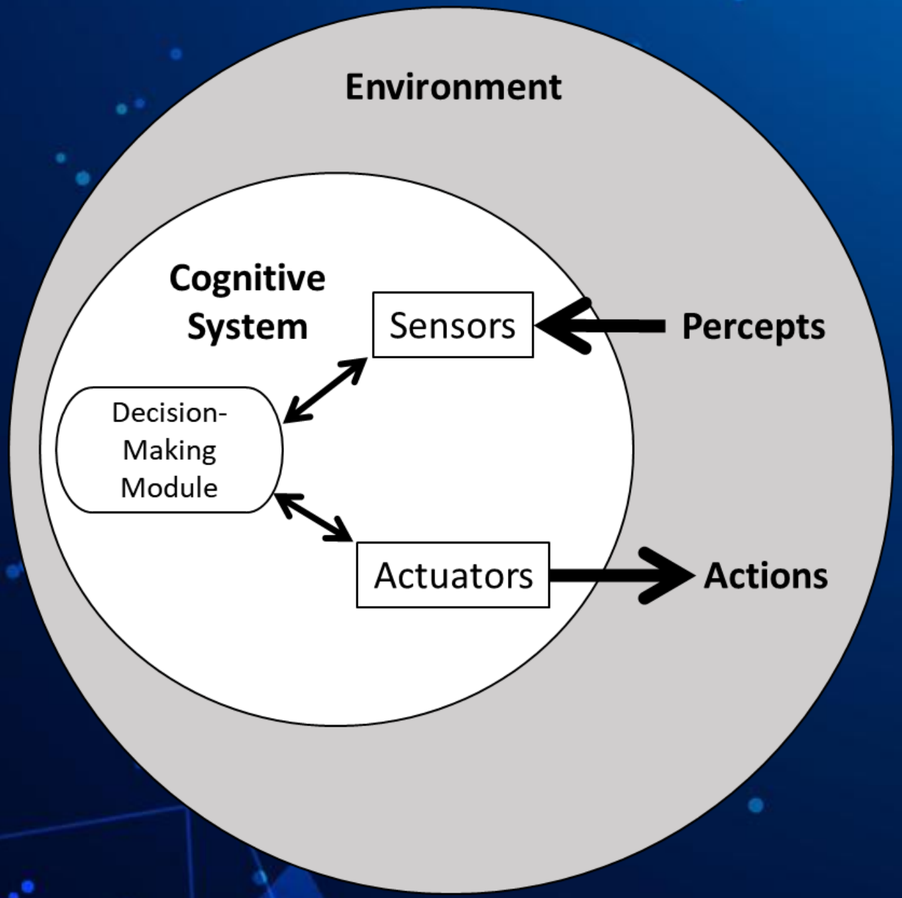
Dr. Matthew Canham
Cognitive Security Institute
mcanham@cognitivesecurity.email

Dayton Security Summit

Dec. 20, 2024

COGNITIVE SECURITY INSTITUTE

Cognitive Systems



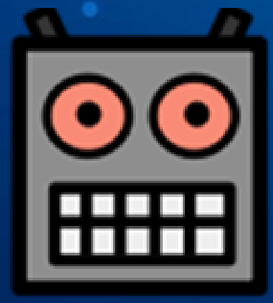
ΨΦ

COGNITIVE SECURITY INSTITUTE

Cognitive Security

Ψ

Φ




COGNITIVE SECURITY INSTITUTE
COGNITIVE ATTACK OF THE DAY
Sleeper Agent Attack
CAT_ID: CAT-2024-002 | Security Layer: AI | Category: TTP
An AI model acts in a benign capacity, accurately carrying out assigned tasks until a trigger event causes it to suddenly act in a malicious manner (essentially becoming an insider threat). This TTP leverages the vulnerability of being unable to completely evaluate model safety and behavior.
https://cognitiveattacktaxonomy.org/

COGNITIVE SECURITY INSTITUTE

Hackers: a Community, a Culture, a Movement	Ed Skoudis
Human-Centered Cybersecurity	Julie Haney
Cyber Warfare	Dr. Chase Cunningham
Deceptive Patterns	Harry Brignull
A Forensic Cyberpsychology Approach to Cyberbullying	Marshall Rich
PRC Hybrid Warfare	Gen. Robert Spalding
Infostealer Malware	Leonid Rozenberg
Sneaky War and the Dark Arts	Sean McFate
Decoding AI Deception in Our Hyperreal World	Perry Carpenter
AI and Power	Bruce Schneier
Integrating Human Factors Engineering in Cybersecurity	Calvin Nobles
Linguistic Analysis of a Ransomware Gang	Dalya Manatova
Shifting Security from FUD to Flourish	Dr. Margaret Cunningham
Defending National Cognitive Infrastructures	Winn Schwartau
Goals and methods of cognitive warfare.	Dr. Torvald Ask
The Next Disinformation Frontier	Dr. Rand Waltzman

COGNITIVE SECURITY INSTITUTE

Weekly Online Meetings

Presentations uploaded to YouTube Channel

YouTube Channel:

https://www.youtube.com/@cognitivesecurityinstitute/videos

Cognitive Attack Taxonomy

https://cognitiveattacktaxonomy.org/

Contact:

mcanham@cognitivesecurity.email