Sombrero Dynamic Honeynet Defense

STO-CSO Systems, Concepts and Integration
SCI-300 Specialists' Meeting
'Cyber Physical Security of Defense Systems'
University of Florida, Research & Engineering Education Facility (REEF)
8-9 May 2018

Ken Yu (ICF), Daniel Sullivan (Raytheon) and Edward Colbert
Network Security Branch, CISD
U.S. Army Research Laboratory (ARL)

Definition

Definition from Whatis.com

A **honeynet** is a network set up with intentional vulnerabilities; its purpose is to **invite attack**, so that an attacker's activities and **methods can be studied** and that information used to increase network security.

Definition from techopedia.com

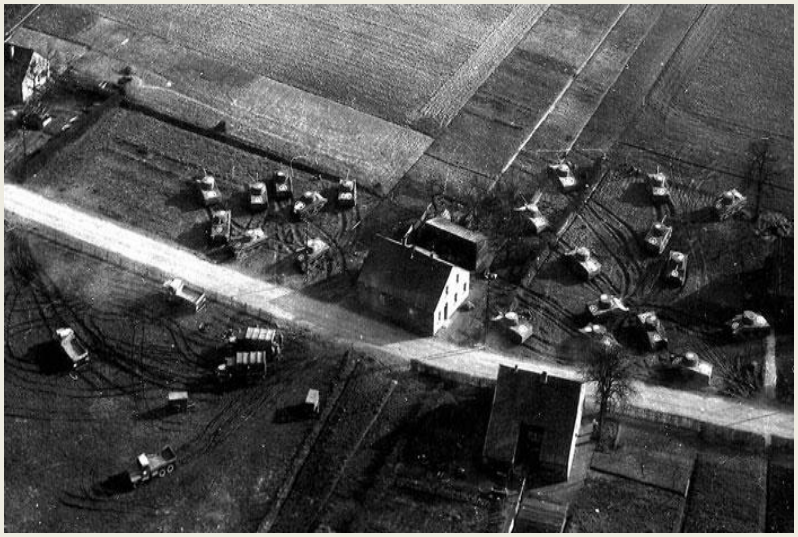
A **honeynet** is a vulnerable and simulated computer network using a **decoy** server designed to test network security. Honeynets are developed in order to help computer security experts to **improve security** for networks and systems.

History of Deceptions

D-Day Landing at Normandy, 1944 – Allies
Operation Bodyguard

Inflatable Tank

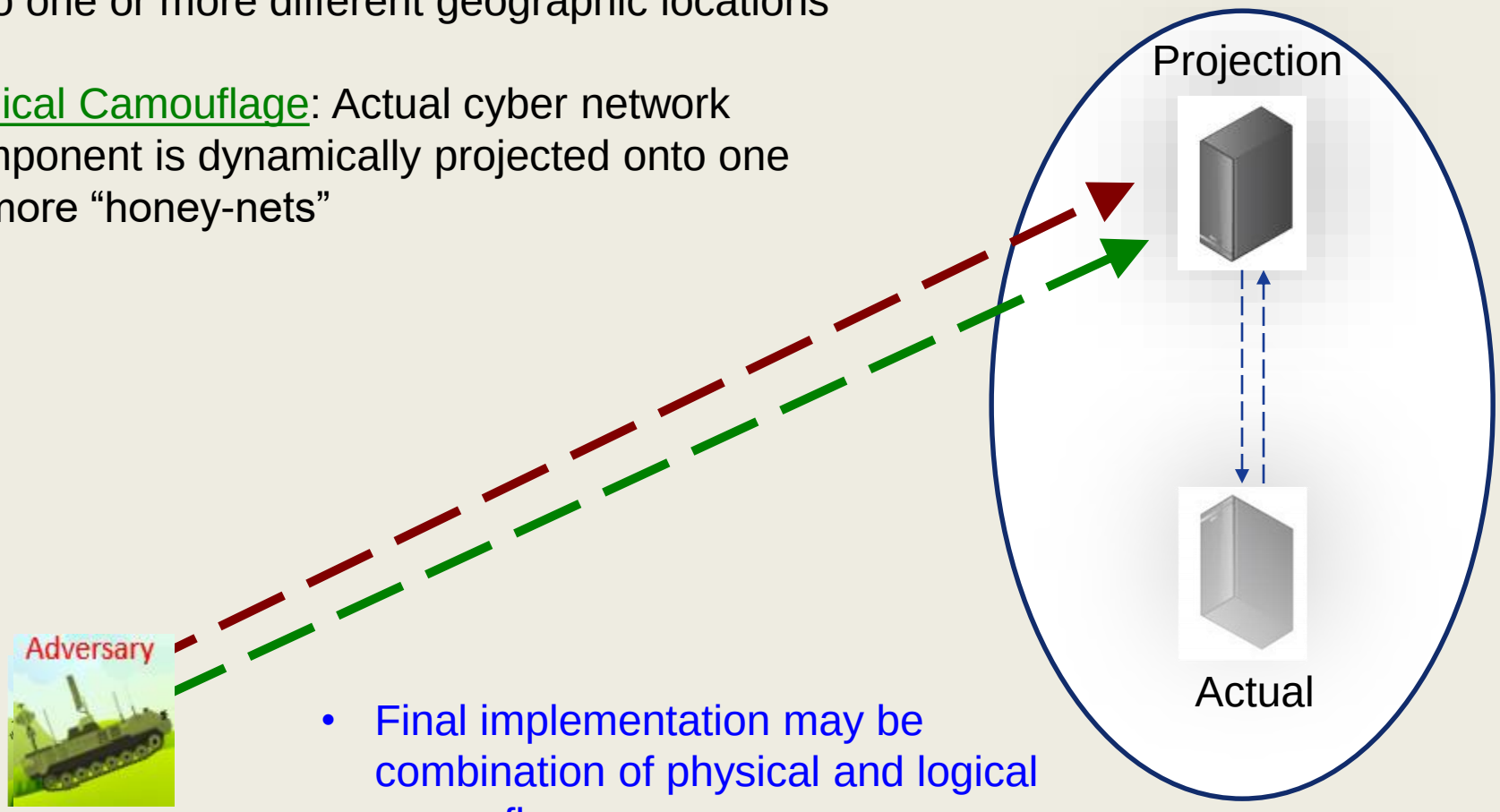
Ghost army



Sombrero System Overview

From afar, Adversary observes:

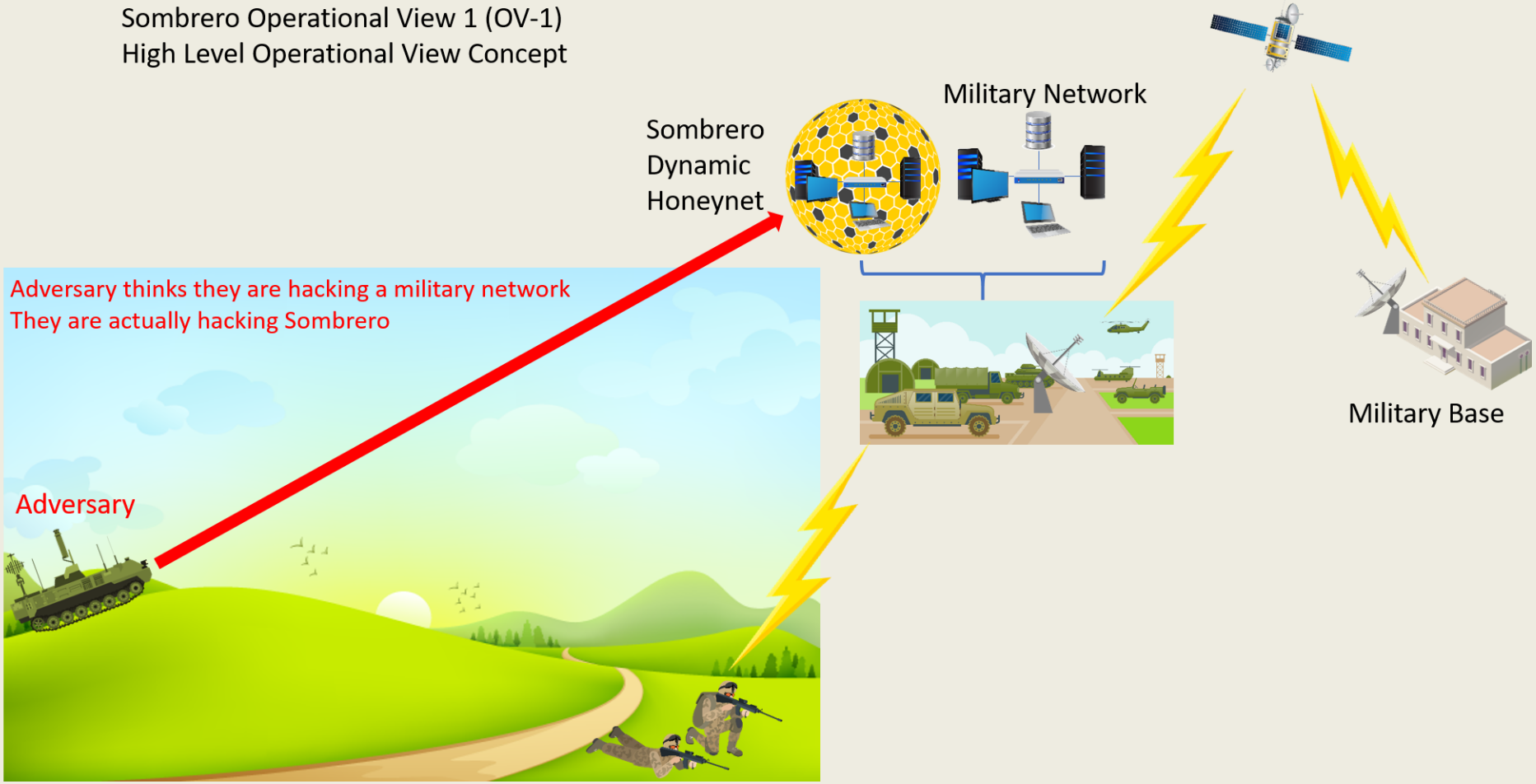
- Physical Camouflage: Actual target is projected onto one or more different geographic locations
- Logical Camouflage: Actual cyber network component is dynamically projected onto one or more “honey-nets”



- Final implementation may be combination of physical and logical camouflage

Example Sombrero Implementation

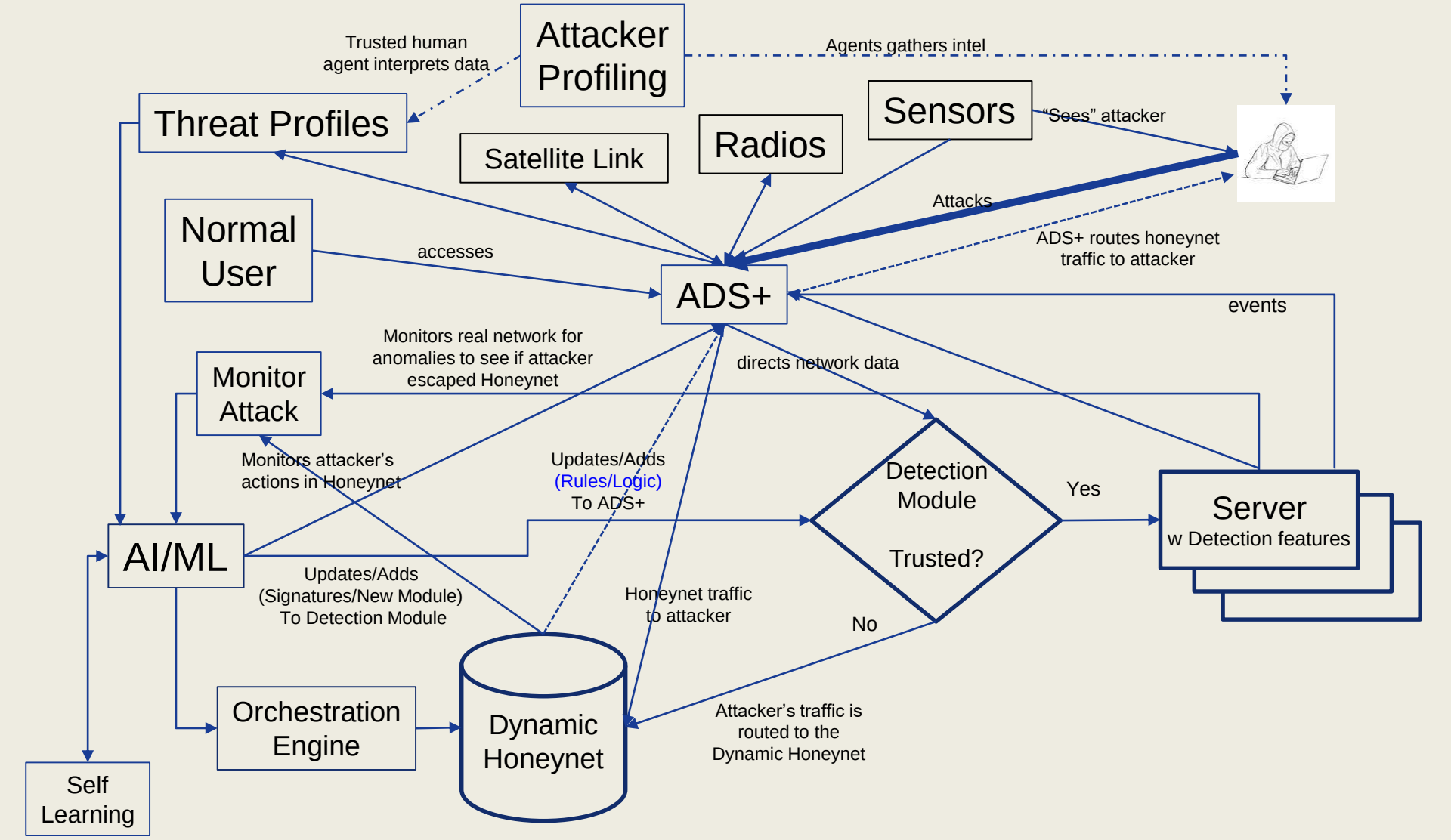
Sombrero Operational View 1 (OV-1)
High Level Operational View Concept



Critical Questions to be Answered

- How do we validate which communication is trusted?
- How to detect intrusion?
- How do we handle insider threats?
- How to build an AI/ML machine to handle attacker?
- How to build a system that is capable of performing self-learning and self-updating?
- How do we entice the attacker to pursue the honeynets instead of the real system?
- How to we interpret INTEL gathered on an attacker and feed it back to Sombrero?
- How to build an adversarial model to handle irrational attacker?

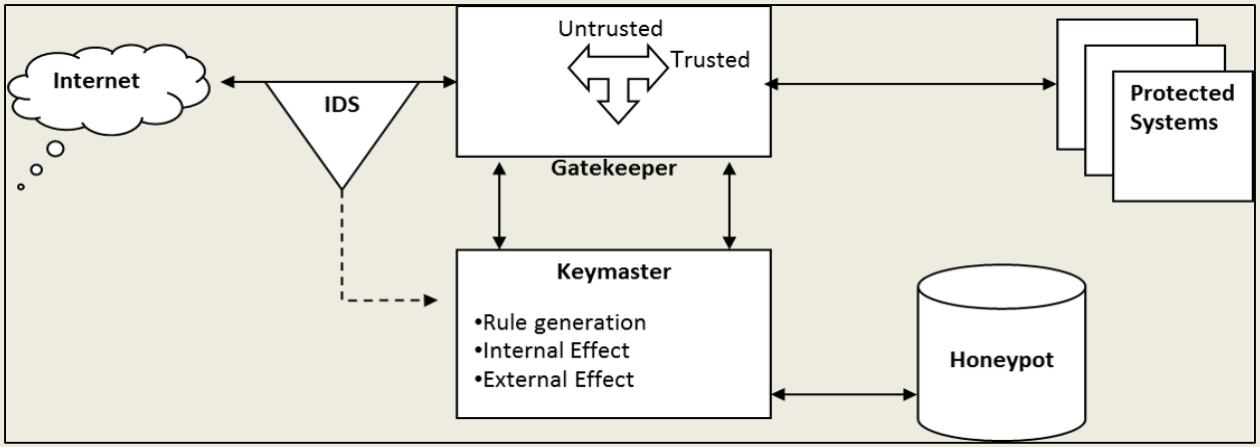
Sombrero Conceptual Architecture



Current ADS

Current Version of ADS (Active Defense System) Framework

- Has been developed at the US Army Research Laboratory
- Functional Active Defense System prototypes are currently operational on testbed networks
- Active Defense System has successfully defended against a modeled data exfiltration attempt
- Active Defense System framework components have been employed to research the targeting of malicious network traffic

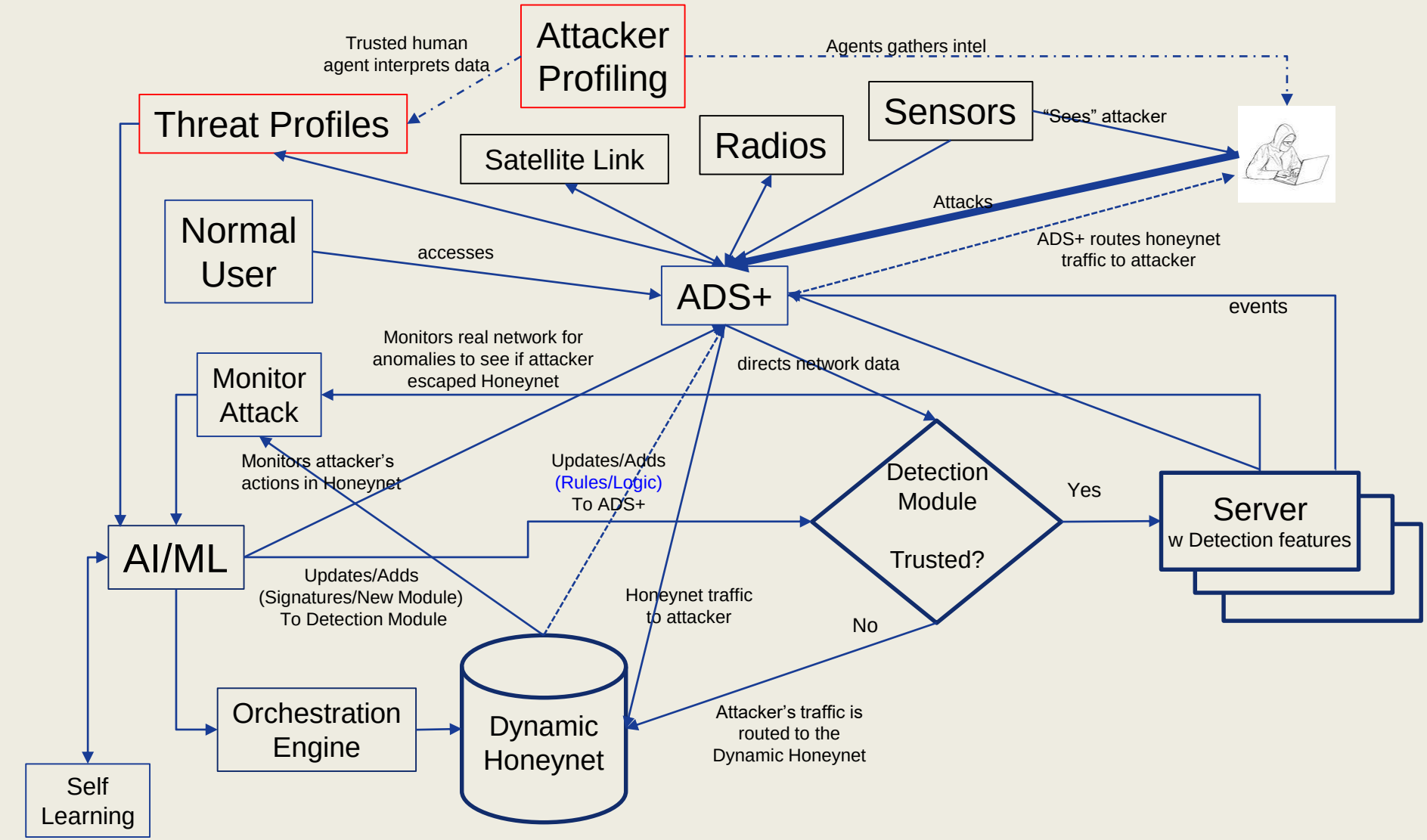


ADS+ Module

ADS+ (Next-Gen Advance Defense System)

- Leverage the current ADS Framework
- Includes software module that filters and screens incoming traffic (radios, sensors, servers, satellite links)
- Validates certificates of incoming traffic
- Establishes rules to forward or block traffic
- Sends all traffic to Detection Module (except outgoing trusted network traffic) to evaluate trustworthiness
- Routes traffic from the honeynet to the attacker
- Receives anomalous events from regular network and re-routes suspicious traffic to the honeynet
- Sends all abnormal/malicious traffic to the honeynet

Sombrero Conceptual Architecture



Attacker Profiling Modules

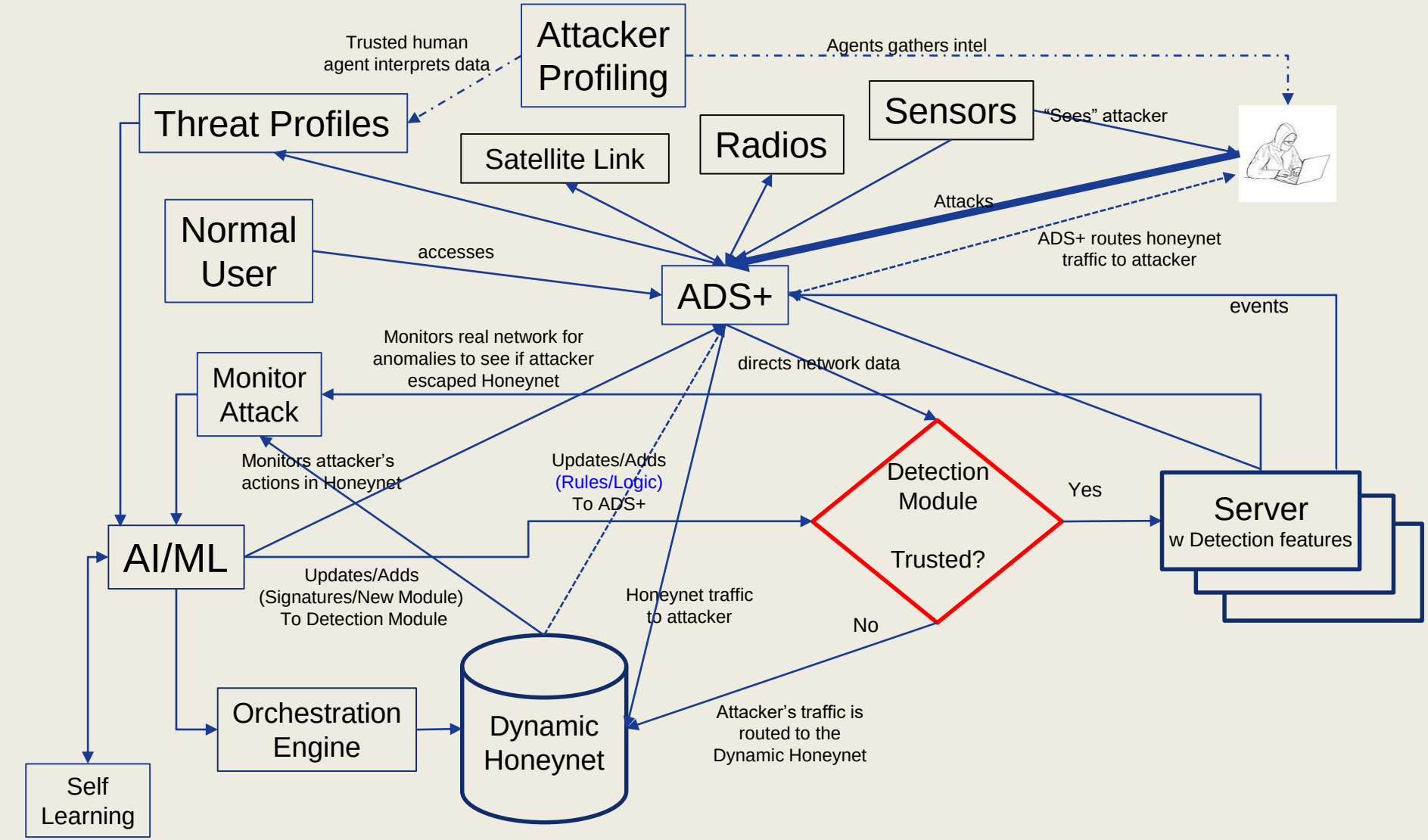
Sensors

- Detects threat data from robots, RFID attacks, GPS signal spoofing, impersonation, etc. on the battlefield
- Feeds data to ADS+ to ensure the data is not tampered
- May include “intelligence report” information

Threat Analysis

- Data gathered INTEL from various sources are collected and analyzed for threat vectors, motivation, enemy objectives, etc.
- Threat analyst interprets the data and feed the data to Threat Profiles module

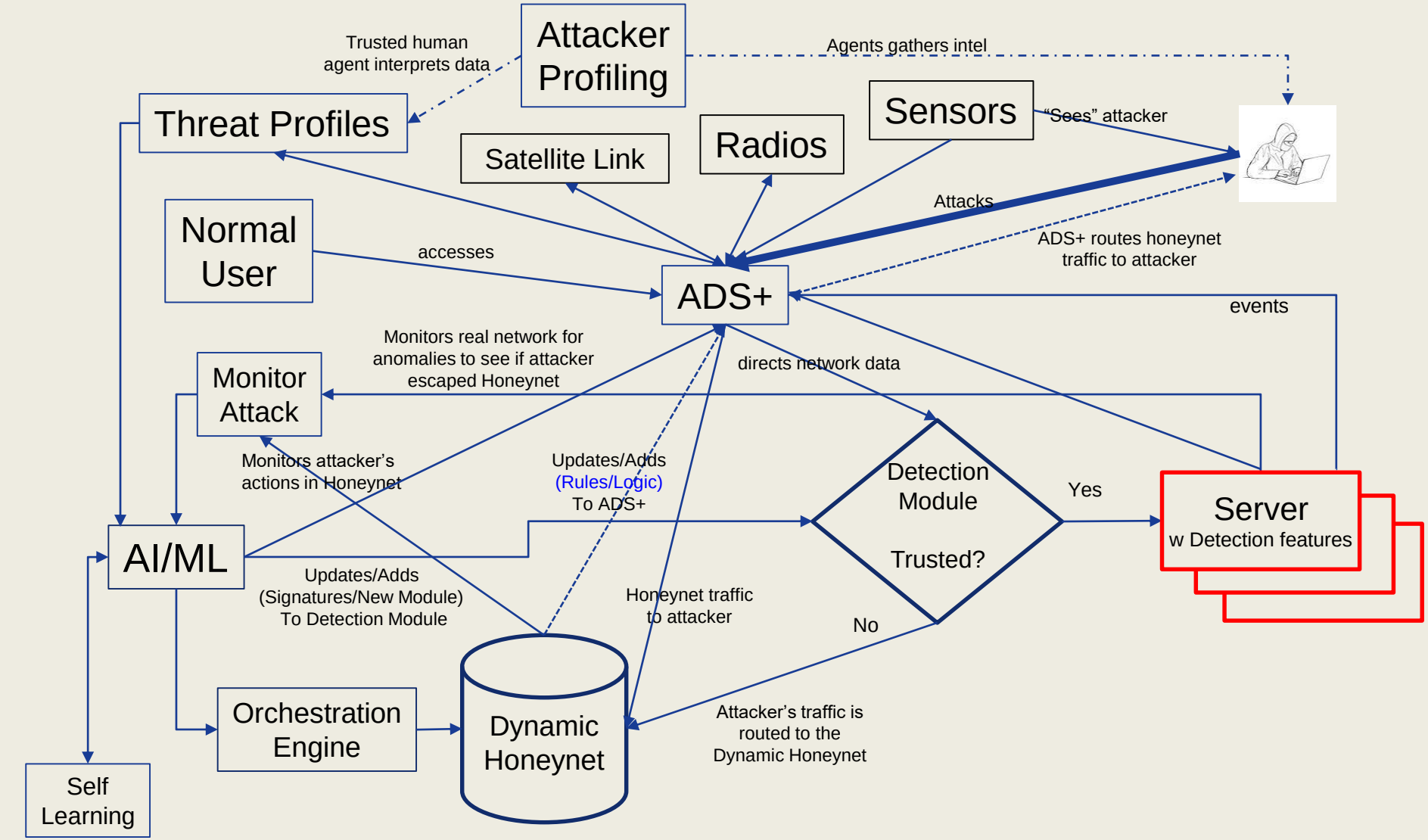
Sombrero Conceptual Architecture



Detection Module

- Accepts traffic data from ADS+
- Owns multiple detection modules
  - Signature based detection module
  - Anomaly based detection
    - Supervised learning based on historic events
    - Unsupervised learning predict intrusion
  - DoS/DDoS detection module
- Sends traffic to intended server if “approved”
- Sends traffic to honeynet if “unapproved”
- Allows ability to add/update signatures and add/update new modules

Sombrero Conceptual Architecture

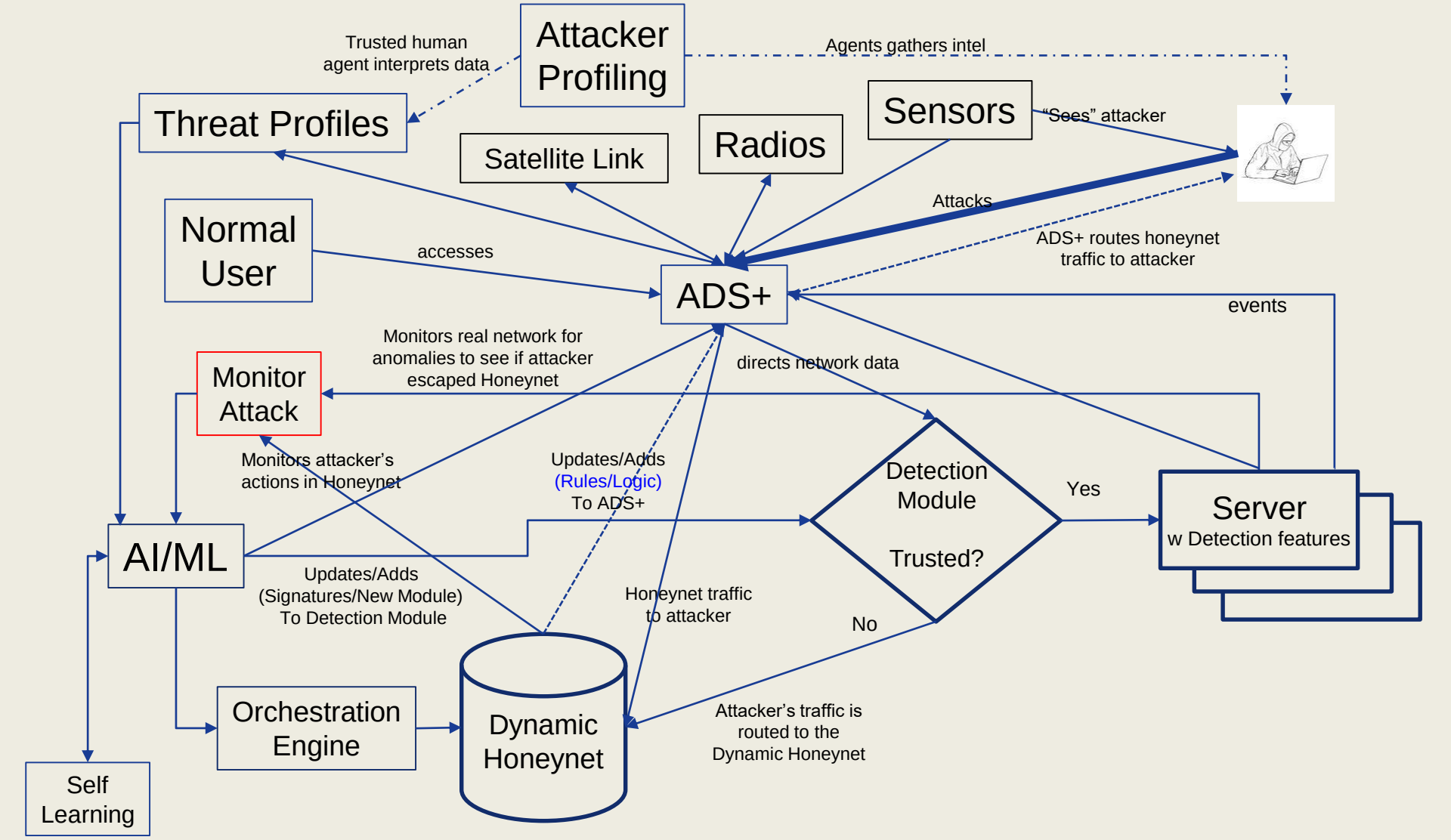


Server with Detection Features

Detection Features on Server Responsibilities

- Accepts incoming network traffic from another node
- Validates certificate of the incoming traffic
- Generates event based on some triggering rules and sends event to ADS+ Module
- Allow decoys to be deployed

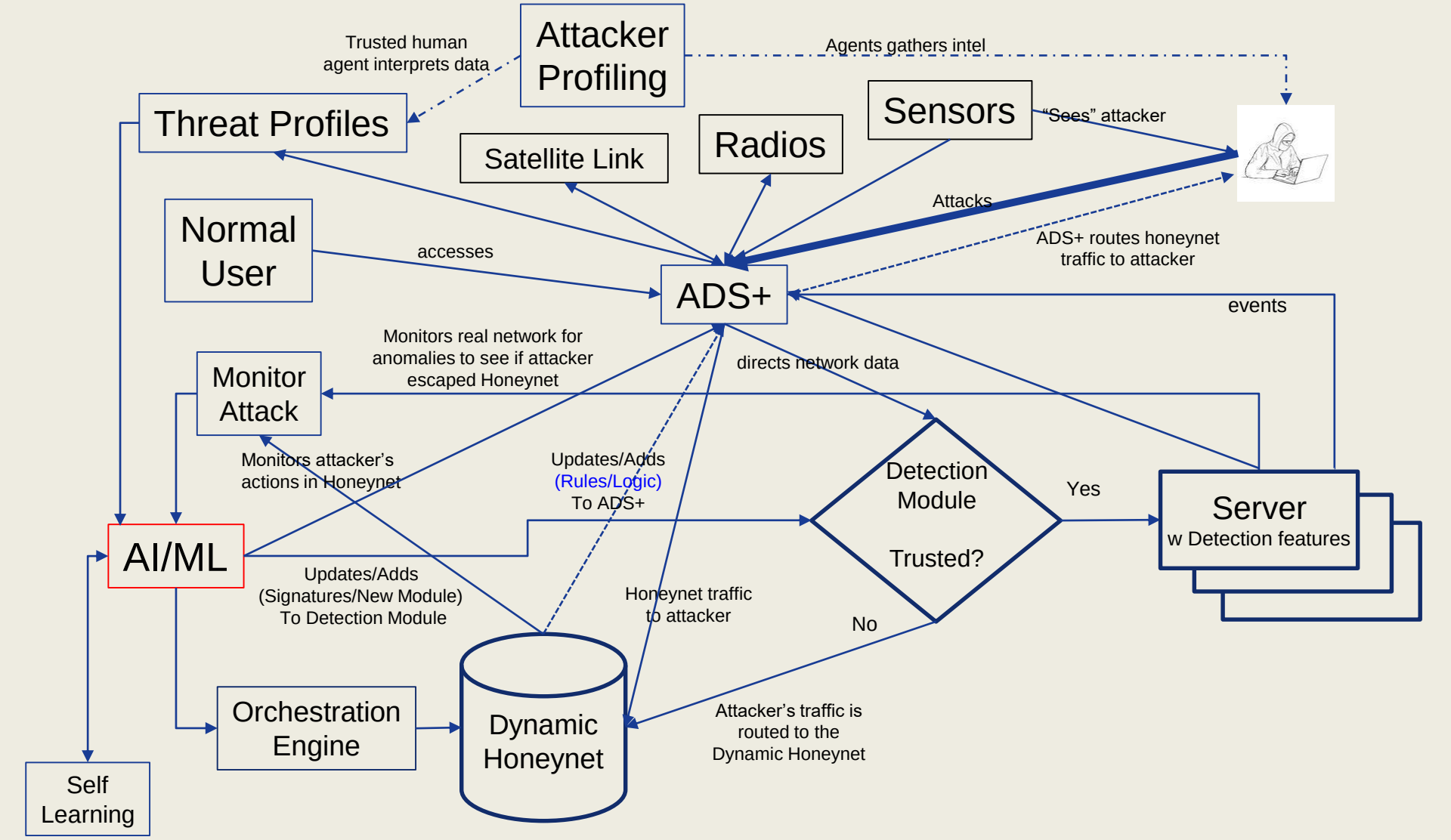
Sombrero Conceptual Architecture



Monitor Attack Module

- Monitors activities on regular networks
- Monitors attacker's actions on the honeynet
- Interprets the attacker's actions in the honeynet and sends data to AI/ML module for analysis
- Interprets anomalous events from the regular network. If events are suspicious, sends data to the AI/ML module for analysis

Sombrero Conceptual Architecture



Sample AI/ML Module Overview

Accepts data from

- Monitor Attack module data(1)
- attacker profile info(2)
- server activities data from network servers(3)

Data from (1)

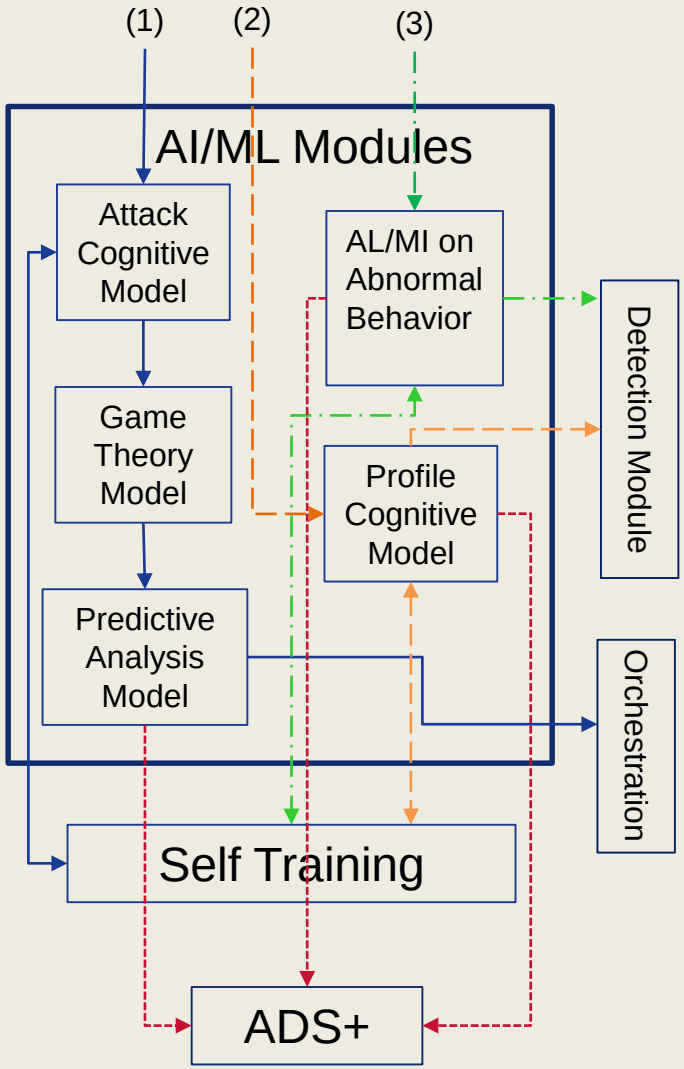
- Uses cognitive models to predict and update its AI/ML Self Training if attack method not found previously
- Passes data to Game theory model to plan countermeasures
- Predict attacker's next move using predictive analysis model
- Passed output to Orchestration Engine to configure the honeynet to keep the attacker's interest
- Updates are sent to Detection Module and/or ADS+ after new training is done

Data from (2)

- Uses cognitive models to analyze new profile info updates its AI/ML Self Training
- Passes the output to Detection Module and/or ADS+ after new training is done

Data from (3)

- Uses the AI/ML on abnormal behavior to update its AI/ML Self Training if not found
- Passes the output to Detection Module and/or ADS+ after new training is done



AI/ML Modules (cont'd)

Attack Cognitive Model Module

- Uses deep learning and/or other machine learning techniques to predict human behaviors

Game Theory Model Module

- Uses game theory technique as a probabilistic model to identify courses of actions based on attacker's utility

Predictive Analysis Model Module

- Predict the attacker's next move
- Orchestrates a set of rules for attacker to follow to
- Sets new training dataset to Self Training Module to updates its dataset if new attack has been learned
- Updates are sent to Detection Module and/or ADS+ after new training is done

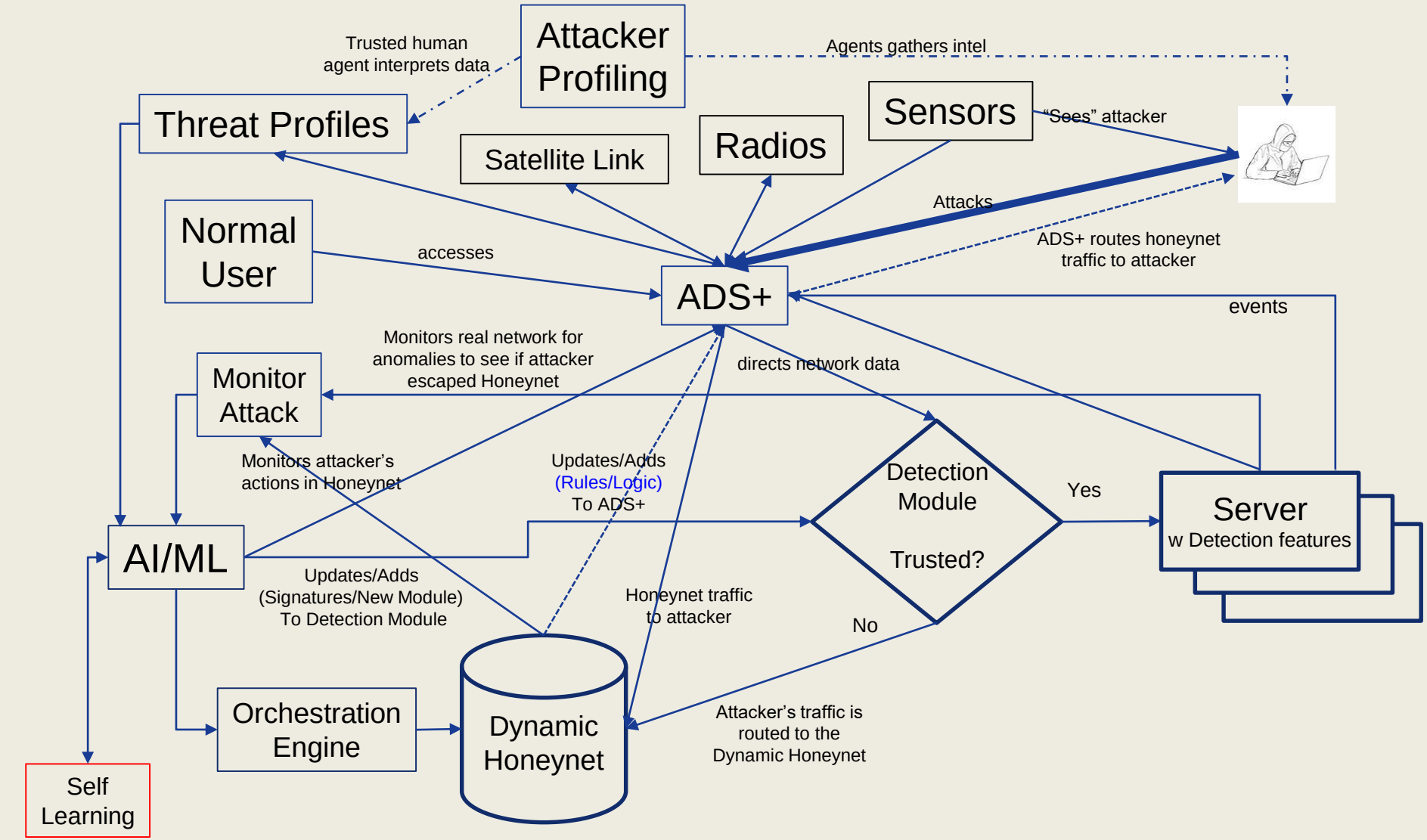
Abnormal Behavior Module

- Detects user's abnormal behavior on a trusted network servers
- Sets new training dataset to Self Training Module to updates its dataset if new attack is learned
- Updates the Detection Module to reflect new signature or module
- Updates (rules/logics) are sent to ADS+ after new training is done

Profile Cognitive Model Module

- Accepts data from the threat model
- Analyze attacker profile
- Sets new training dataset to Self Training Module to updates its dataset if new attack is learned
- Updates are sent to Detection Module and/or ADS+ after new training is done

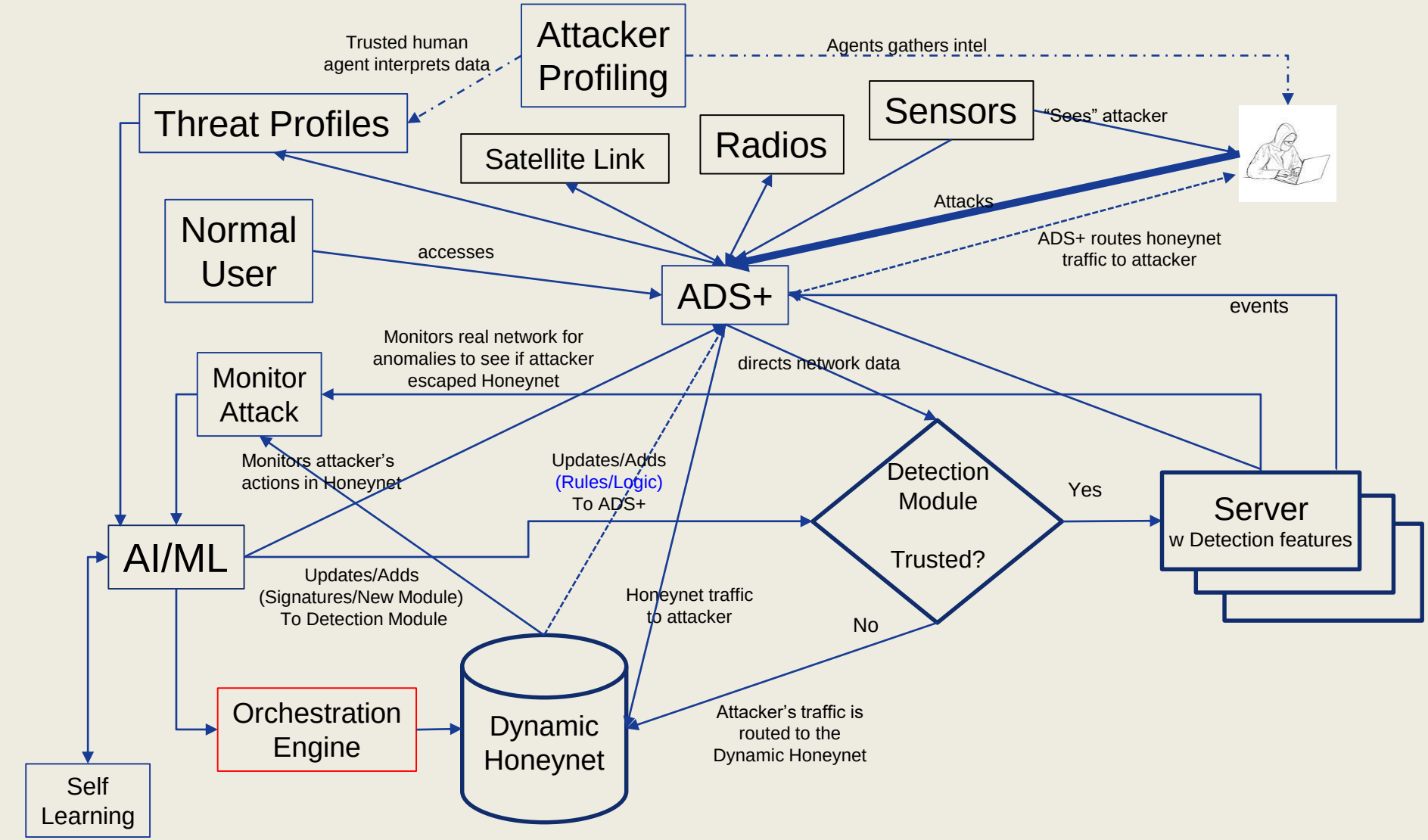
Sombrero Conceptual Architecture



Self-Training Module

- Self-Training module can use offline training to feed the data back to AI/ML module
- Accepts abnormal behavior data from AI/ML Abnormal Behavior module
  - Uses reinforcement learning AI/ML algorithm to train abnormal behavior data
  - Updates Abnormal Behavior indications of compromise after training
- Accepts attacker profile info data
  - Uses reinforcement learning AI/ML algorithm to train attacker profile data
  - Updates AI/ML cognitive models after training
- Accepts feature set of attack vectors
  - Uses reinforcement learning AI/ML algorithms to train based on attacker's feature set
  - Updates AI/ML on cognitive model signatures after training

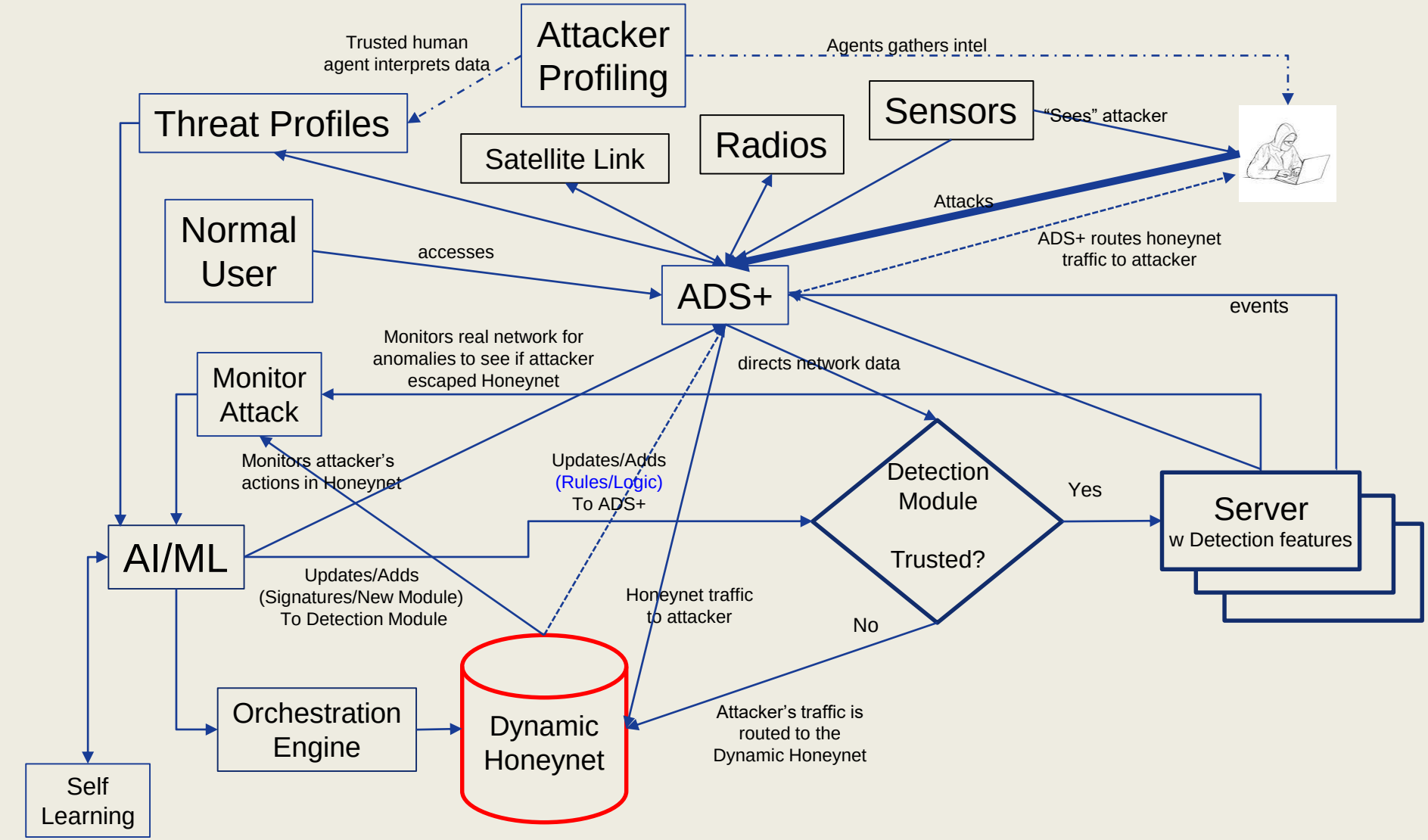
Sombrero Conceptual Architecture



Orchestration Engine

- Orchestrate Engine re-configures the honeynet based on course of action selected by AI/ML module
- Goal is to lure the attacker deeper into the honeynet

Sombrero Conceptual Architecture



Sample Honeynet Features

- Initially creates a small subset of VM servers and Mission Command applications to simulate the actual tactical network
- Simulates human interactions with Mission Command applications
- Simulates real network to lower and higher echelon communications
- Inputs:
  - Accepts traffic directly from ADS+
  - Accepts traffic from Detection Module for untrusted traffic
  - Accepts configuration changes from Orchestration Engine to draw attacker's attention
- Outputs:
  - Feeds data to Monitor Attack Module to monitor attacker actions
  - Deflect attacker traffic or invite the next attacker action back to ADS+

Questions?

ken.f.yu.ctr@mail.mil