Document Title: Cybersecurity Defense Strategy & Team Directory
Date: October 26, 2025
Subject: Operational Guide for Threat Detection and Defense
Compiled By: Lionel Chikuku

---

1. Operational Methodology: The Three Phases

This section outlines the strategic approach for implementing our AI defense system.

Phase 1: Feature Extraction (Translating "Human" to "Math") [1]

Objective: Convert raw data into numerical vectors that the AI can process.

Action: This phase involves breaking down unstructured data (like email text or login attempts) into specific, measurable attributes.

Phase 2: The "Normalcy" Baseline (Defining Safety) [2]

Objective: Establish a mathematical standard for "normal" behavior.

Action: Before detecting threats, the system must learn standard patterns (e.g., typical login times, usual file access volume) to avoid false positives.

Phase 3: Signal vs. Noise (The Boundary) [3]

Objective: Distinguish between harmless anomalies and actual malicious threats.

Action: This phase focuses on tuning the decision boundary to separate the "noise" of daily operations from the "signal" of a cybersecurity attack.

---

2. Directory of Defense Algorithms (Encryption & Hashing)

These algorithms form the defensive backbone, securing credentials and data against unauthorized access.

Primary Hashing Standard: Argon2 [4]

Status: Winner of the Password Hashing Competition[5].

Variants:

Argon2d: Offers resistance to GPU cracking but is vulnerable to side-channel attacks[6].

Argon2i: Optimized to resist side-channel attacks but is slightly less resistant to time-memory trade-off attacks[7].

Argon2id: A hybrid version using Argon2i for the first pass and Argon2d for subsequent passes[8].

Alternative Hashing Tools [9]

Bcrypt: Uses the Blowfish cypher[10].

Scrypt: A specialized algorithm designed to be resource-intensive[11].

PBKDF2: A standard key derivation function[12].

Key Capabilities & Compliance

Key Stretching: Algorithms are designed to be deliberately slow and resource-intensive to thwart brute-force attacks[13].

Defense Against Specific Attacks:

Rainbow Table Attacks [14]

FPGA Attacks: Resists cracking attempts using Field Programmable Gate Arrays[15].

Regulatory Standard: Adheres to FIPS-140 compliance[16].

---

3. Directory of Detection Features (AI Inputs)

These specific features [17] serve as the inputs for the AI model during Phase 1.

Levenshtein Distance: Used to mathematically measure the similarity between strings (e.g., detecting domain spoofing)[18].

Sentiment/Urgency Score: Quantifies the tone of a message to detect social engineering tactics relying on panic[19].

URL Mismatch Boolean: A binary check (True/False) determining if a hyperlink's text matches its actual destination[20].

Time Delta from Baseline: Measures the deviation in time (e.g., login hours) compared to the user's established history[21].