## PT Model Cryptography Public KEY Infrastructure Blacklisting Encryption 0.8 **Deception Technology** Access Control ML/DL Multi Factor Authentication Mutual Authentication 0.6 NLP/LLM Password Strength Meters Password Hashing Password Management **Password Policy Graphical Authentication** IDS/IPS **ONE Time Password** Penetration Testing CAPTCHA **Behavior Based Detection** 0.2 Formal Verification Split Manufacturing Game Theory — Anomaly Detection Vulnerability Assessment Patch Management 0.0 Vulnerability Management 2013 2015 2016 2018 2019 2025 2026 2014 2017 2020 2022 2023 2024 SIEM 2021 Standardized Communication — Control Flow Integrity **Vulnerability Scanner** User Behavior Analytics Data Loss Prevention Network Segmentation Risk Assessment Dynamic Resource Management Least Privilege Continuous Authentication Distributed Ledgers Blockchain Data Provenance Source Identification Image Recognition Hypergame Static Analysis Dynamic Analysis Taint Analysis DNSSEC Data Leakage DETECTION/PREVENTION Activity Monitoring Moving Target Defense **Keystroke Dynamics** Attack Tree **Data Sanitization Outlier Detection Adversarial Training** Trustworthy AI Bayesian Network Strong Authentication SSL/TLS Https Identity-Based Encryption (IBE) Session Management Rate Limiting — Traffic Shaping Packet Filtering Blackholing Rank Correlation Application Whitelisting — Data Backups — Statistical HMM --- Identity Management File Integrity Monitoring — VPN — Privacy Preserving Sandboxing --- Honeypot **Darknet Monitoring** — Virtual Keyboards — Secure Boot Code Signing — Dynamic Binary Instrumentation Graphical Model Software Defined Network Certificate Pinning — Secure Simple Pairing Data Augmentation — Dimensionality Reduction **Defensive Distillation RRAM** — Spatial Smoothing Noise Injection

Supply Chain Risk ManagementMerkle Signature

3D Face Reconstruction

Liveness Detection

BiometricsDigital Watermark