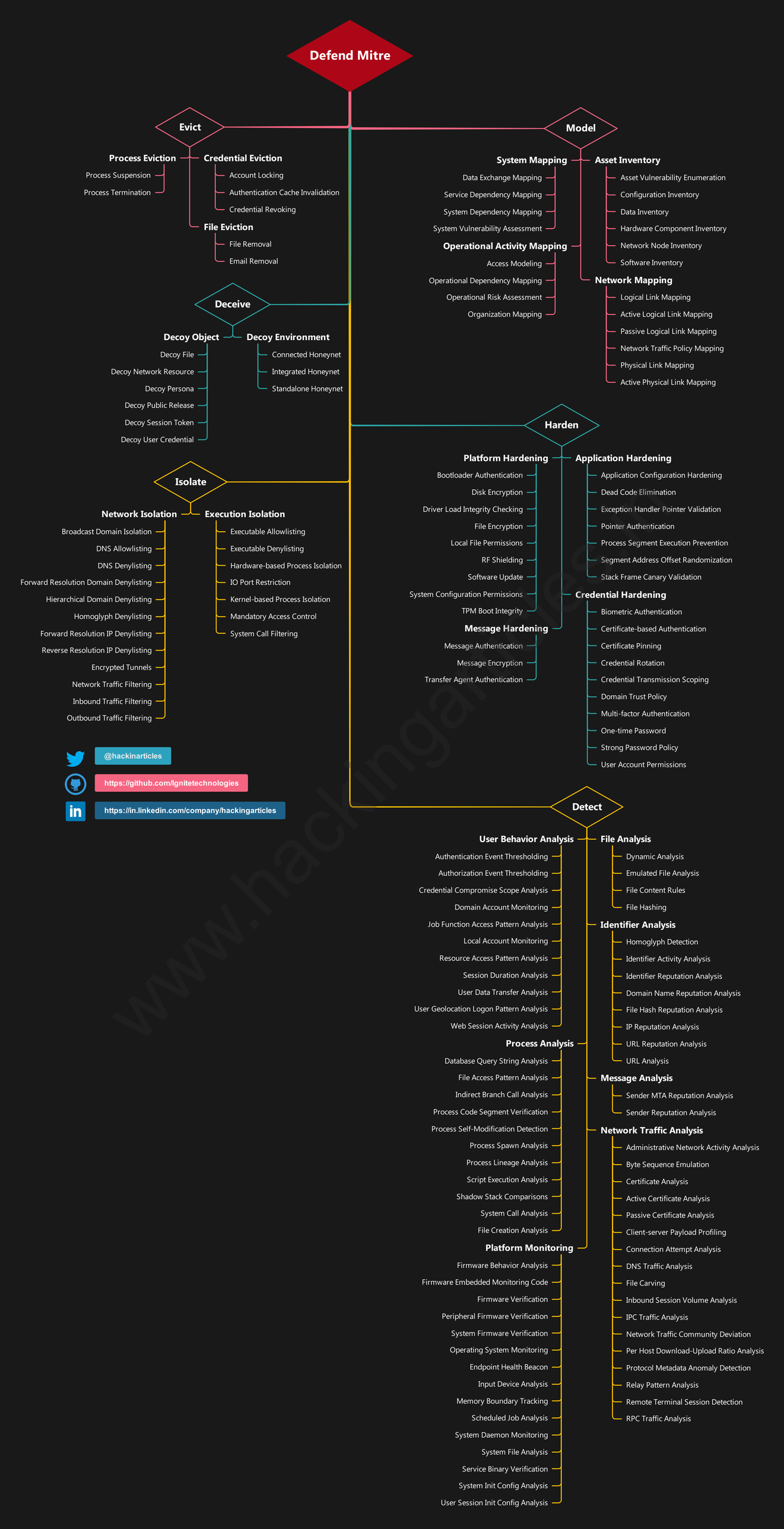
Defend Mitre
Evict
Process Eviction
Process Suspension
Process Termination
Credential Eviction
Account Locking
Authentication Cache Invalidation
Credential Revoking
File Eviction
File Removal
Email Removal
Model
System Mapping
Data Exchange Mapping
Service Dependency Mapping
System Dependency Mapping
System Vulnerability Assessment
Operational Activity Mapping
Access Modeling
Operational Dependency Mapping
Operational Risk Assessment
Organization Mapping
Asset Inventory
Asset Vulnerability Enumeration
Configuration Inventory
Data Inventory
Hardware Component Inventory
Network Node Inventory
Software Inventory
Network Mapping
Logical Link Mapping
Active Logical Link Mapping
Passive Logical Link Mapping
Network Traffic Policy Mapping
Physical Link Mapping
Active Physical Link Mapping
Deceive
Decoy Object
Decoy File
Decoy Network Resource
Decoy Persona
Decoy Public Release
Decoy Session Token
Decoy User Credential
Decoy Environment
Connected Honeynet
Integrated Honeynet
Standalone Honeynet
Harden
Platform Hardening
Bootloader Authentication
Disk Encryption
Driver Load Integrity Checking
File Encryption
Local File Permissions
RF Shielding
Software Update
System Configuration Permissions
TPM Boot Integrity
Message Hardening
Message Authentication
Message Encryption
Transfer Agent Authentication
Application Hardening
Application Configuration Hardening
Dead Code Elimination
Exception Handler Pointer Validation
Pointer Authentication
Process Segment Execution Prevention
Segment Address Offset Randomization
Stack Frame Canary Validation
Credential Hardening
Biometric Authentication
Certificate-based Authentication
Certificate Pinning
Credential Rotation
Credential Transmission Scoping
Domain Trust Policy
Multi-factor Authentication
One-time Password
Strong Password Policy
User Account Permissions
Isolate
Network Isolation
Broadcast Domain Isolation
DNS Allowlisting
DNS Denylisting
Forward Resolution Domain Denylisting
Hierarchical Domain Denylisting
Homoglyph Denylisting
Forward Resolution IP Denylisting
Reverse Resolution IP Denylisting
Encrypted Tunnels
Network Traffic Filtering
Inbound Traffic Filtering
Outbound Traffic Filtering
Execution Isolation
Executable Allowlisting
Executable Denylisting
Hardware-based Process Isolation
IO Port Restriction
Kernel-based Process Isolation
Mandatory Access Control
System Call Filtering
@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles
Detect
User Behavior Analysis
Authentication Event Thresholding
Authorization Event Thresholding
Credential Compromise Scope Analysis
Domain Account Monitoring
Job Function Access Pattern Analysis
Local Account Monitoring
Resource Access Pattern Analysis
Session Duration Analysis
User Data Transfer Analysis
User Geolocation Logon Pattern Analysis
Web Session Activity Analysis
Process Analysis
Database Query String Analysis
File Access Pattern Analysis
Indirect Branch Call Analysis
Process Code Segment Verification
Process Self-Modification Detection
Process Spawn Analysis
Process Lineage Analysis
Script Execution Analysis
Shadow Stack Comparisons
System Call Analysis
File Creation Analysis
Platform Monitoring
Firmware Behavior Analysis
Firmware Embedded Monitoring Code
Firmware Verification
Peripheral Firmware Verification
System Firmware Verification
Operating System Monitoring
Endpoint Health Beacon
Input Device Analysis
Memory Boundary Tracking
Scheduled Job Analysis
System Daemon Monitoring
System File Analysis
Service Binary Verification
System Init Config Analysis
User Session Init Config Analysis
File Analysis
Dynamic Analysis
Emulated File Analysis
File Content Rules
File Hashing
Identifier Analysis
Homoglyph Detection
Identifier Activity Analysis
Identifier Reputation Analysis
Domain Name Reputation Analysis
File Hash Reputation Analysis
IP Reputation Analysis
URL Reputation Analysis
URL Analysis
Message Analysis
Sender MTA Reputation Analysis
Sender Reputation Analysis
Network Traffic Analysis
Administrative Network Activity Analysis
Byte Sequence Emulation
Certificate Analysis
Active Certificate Analysis
Passive Certificate Analysis
Client-server Payload Profiling
Connection Attempt Analysis
DNS Traffic Analysis
File Carving
Inbound Session Volume Analysis
IPC Traffic Analysis
Network Traffic Community Deviation
Per Host Download-Upload Ratio Analysis
Protocol Metadata Anomaly Detection
Relay Pattern Analysis
Remote Terminal Session Detection
RPC Traffic Analysis