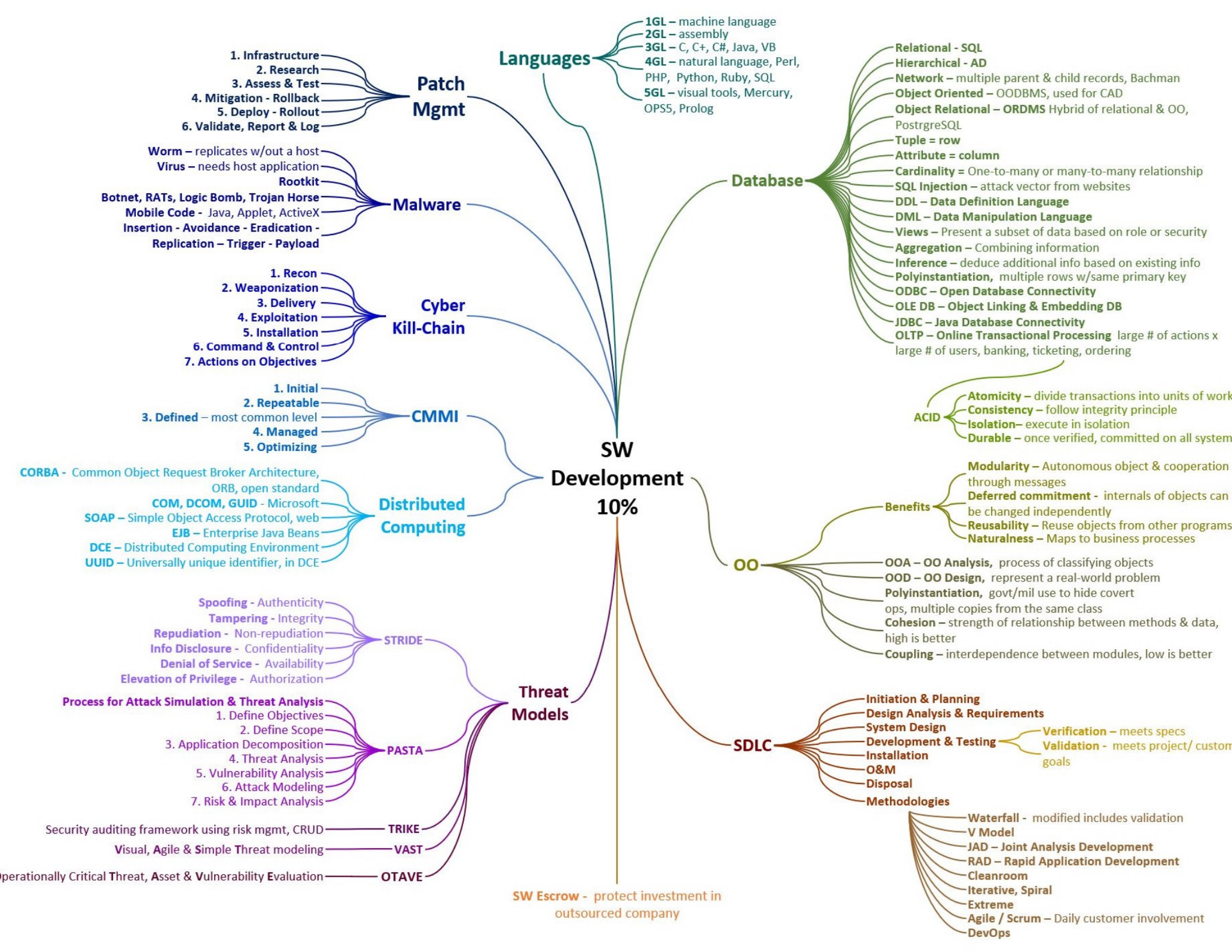
SW Development 10%
Languages
1GL – machine language
2GL – assembly
3GL – C, C+, C#, Java, VB
4GL – natural language, Perl, PHP, Python, Ruby, SQL
5GL – visual tools, Mercury, OPS5, Prolog
Database
Relational - SQL
Hierarchical - AD
Network – multiple parent & child records, Bachman
Object Oriented – OODBMS, used for CAD
Object Relational – ORDMS Hybrid of relational & OO, PostrgreSQL
Tuple = row
Attribute = column
Cardinality = One-to-many or many-to-many relationship
SQL Injection – attack vector from websites
DDL – Data Definition Language
DML – Data Manipulation Language
Views – Present a subset of data based on role or security
Aggregation – Combining information
Inference – deduce additional info based on existing info
Polyinstantiation, multiple rows w/same primary key
ODBC – Open Database Connectivity
OLE DB – Object Linking & Embedding DB
JDBC – Java Database Connectivity
OLTP – Online Transactional Processing large # of actions x large # of users, banking, ticketing, ordering
ACID
Atomicity – divide transactions into units of work
Consistency – follow integrity principle
Isolation– execute in isolation
Durable – once verified, committed on all system
OO
Benefits
Modularity – Autonomous object & cooperation through messages
Deferred commitment - internals of objects can be changed independently
Reusability – Reuse objects from other programs
Naturalness – Maps to business processes
OOA – OO Analysis, process of classifying objects
OOD – OO Design, represent a real-world problem
Polyinstantiation, govt/mil use to hide covert ops, multiple copies from the same class
Cohesion – strength of relationship between methods & data, high is better
Coupling – interdependence between modules, low is better
SDLC
Initiation & Planning
Design Analysis & Requirements
System Design
Development & Testing
Verification – meets specs
Validation - meets project/ custom goals
Installation
O&M
Disposal
Methodologies
Waterfall - modified includes validation
V Model
JAD – Joint Analysis Development
RAD – Rapid Application Development
Cleanroom
Iterative, Spiral
Extreme
Agile / Scrum – Daily customer involvement
DevOps
SW Escrow - protect investment in outsourced company
Threat Models
STRIDE
Spoofing - Authenticity
Tampering - Integrity
Repudiation - Non-repudiation
Info Disclosure - Confidentiality
Denial of Service - Availability
Elevation of Privilege - Authorization
PASTA
Process for Attack Simulation & Threat Analysis
1. Define Objectives
2. Define Scope
3. Application Decomposition
4. Threat Analysis
5. Vulnerability Analysis
6. Attack Modeling
7. Risk & Impact Analysis
TRIKE
Security auditing framework using risk mgmt, CRUD
VAST
Visual, Agile & Simple Threat modeling
OTAVE
Operationally Critical Threat, Asset & Vulnerability Evaluation
Distributed Computing
CORBA - Common Object Request Broker Architecture, ORB, open standard
COM, DCOM, GUID - Microsoft
SOAP – Simple Object Access Protocol, web
EJB – Enterprise Java Beans
DCE – Distributed Computing Environment
UUID – Universally unique identifier, in DCE
CMMI
1. Initial
2. Repeatable
3. Defined – most common level
4. Managed
5. Optimizing
Cyber Kill-Chain
1. Recon
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objectives
Malware
Worm – replicates w/out a host
Virus – needs host application
Rootkit
Botnet, RATs, Logic Bomb, Trojan Horse
Mobile Code - Java, Applet, ActiveX
Insertion - Avoidance - Eradication - Replication – Trigger - Payload
Patch Mgmt
1. Infrastructure
2. Research
3. Assess & Test
4. Mitigation - Rollback
5. Deploy - Rollout
6. Validate, Report & Log