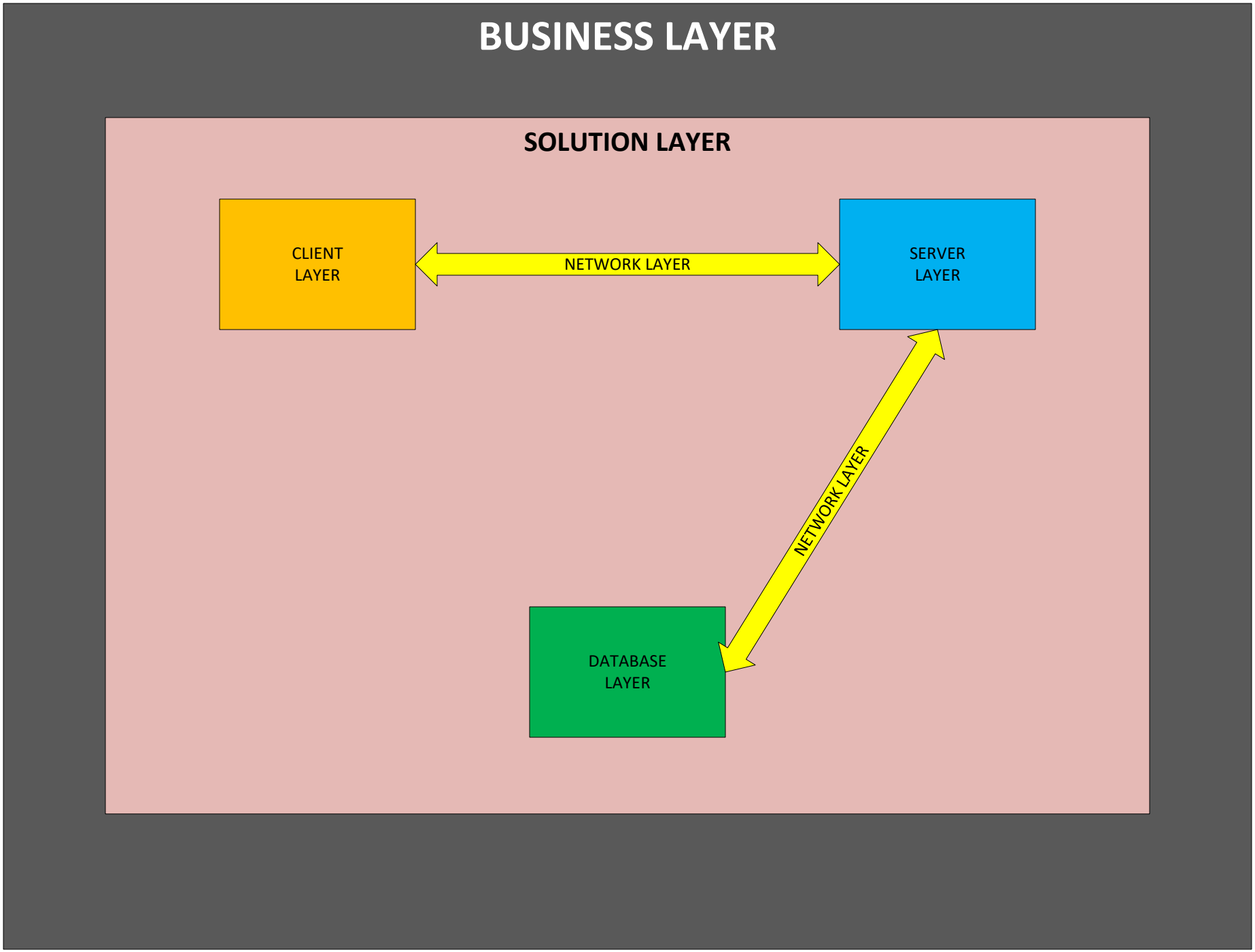
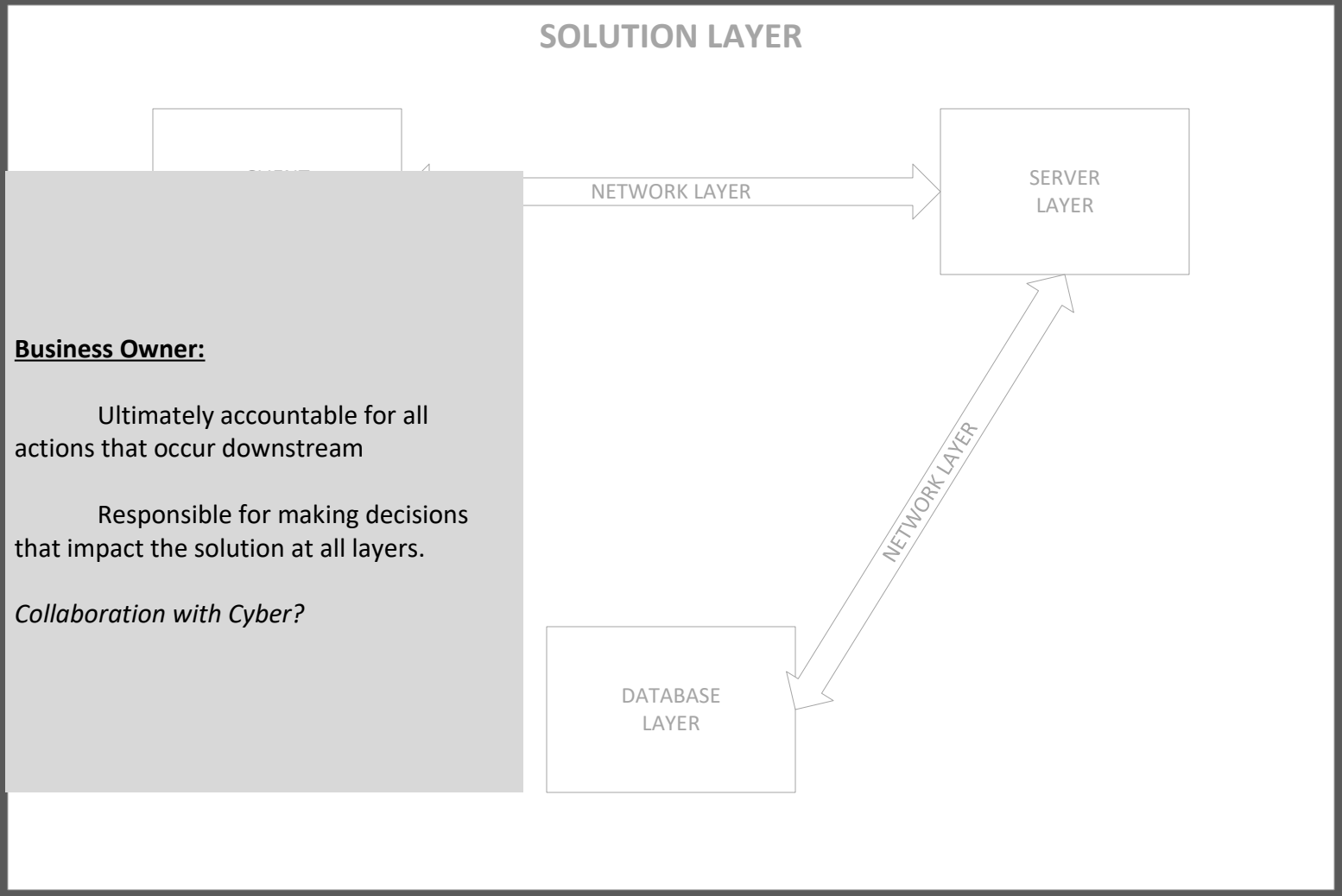

BUSINESS LAYER
SOLUTION LAYER
CLIENT LAYER
NETWORK LAYER
SERVER LAYER
NETWORK LAYER
DATABASE LAYER

BUSINESS LAYER



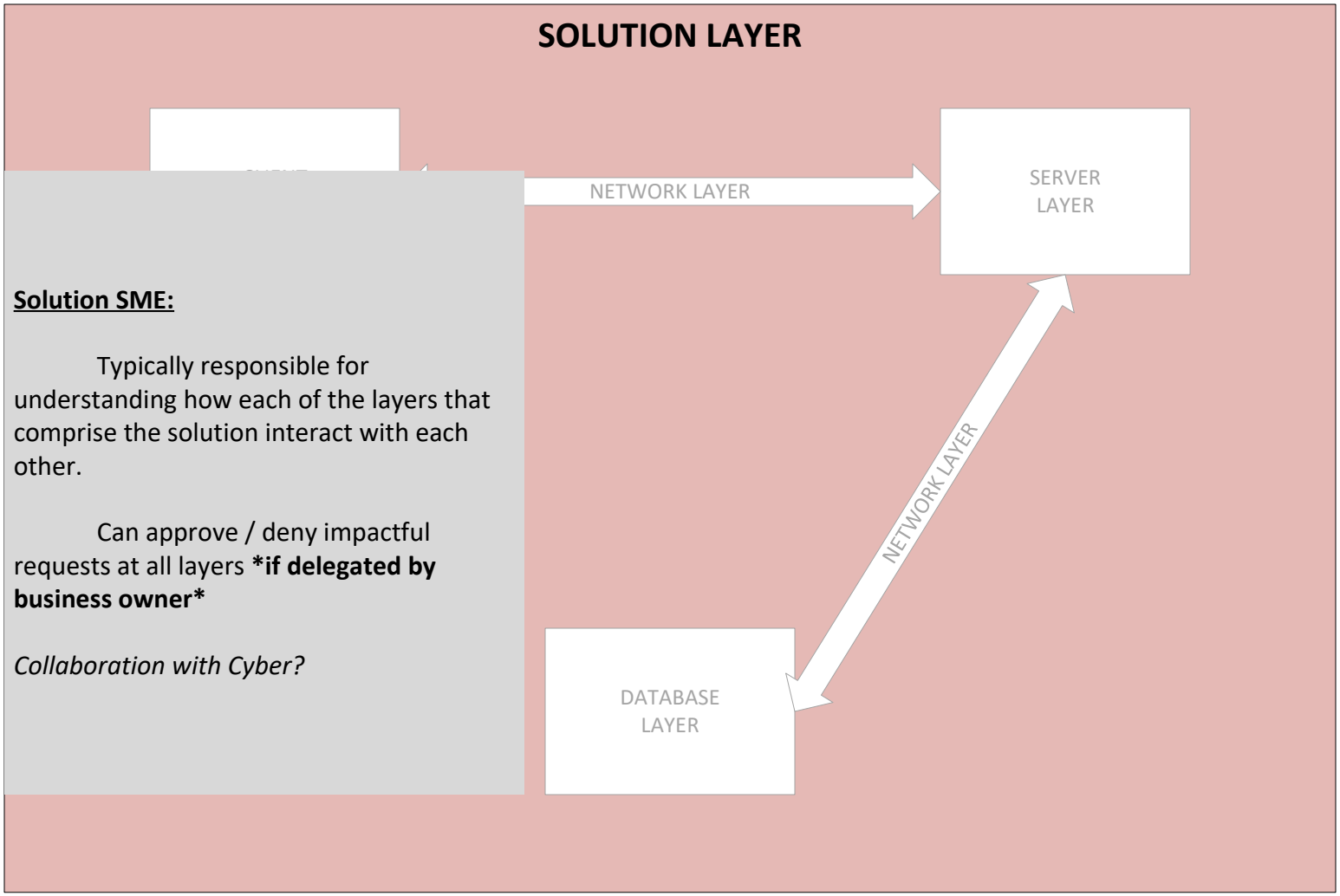
Business Owner:

Ultimately accountable for all actions that occur downstream

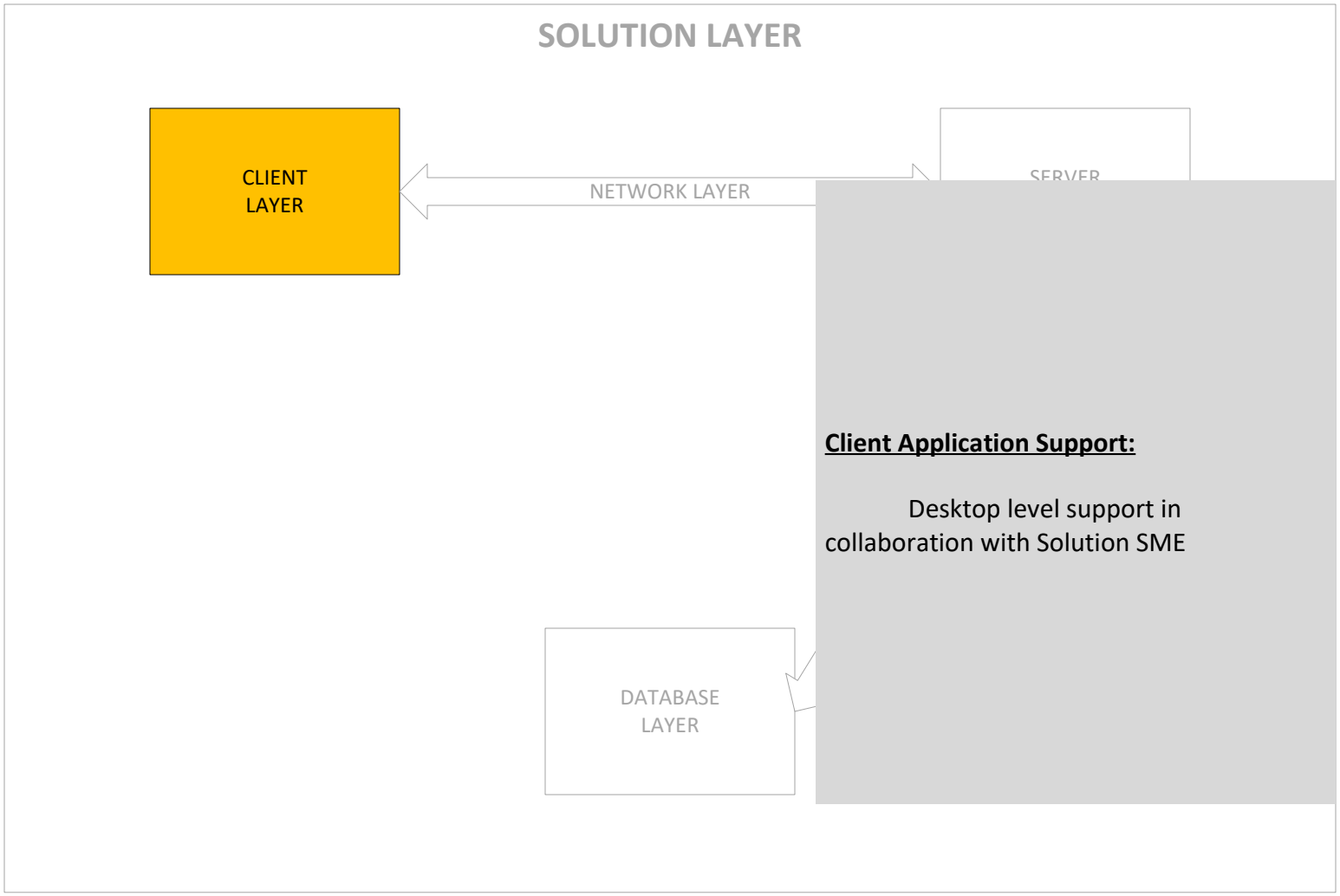
Responsible for making decisions that impact the solution at all layers.

Collaboration with Cyber?

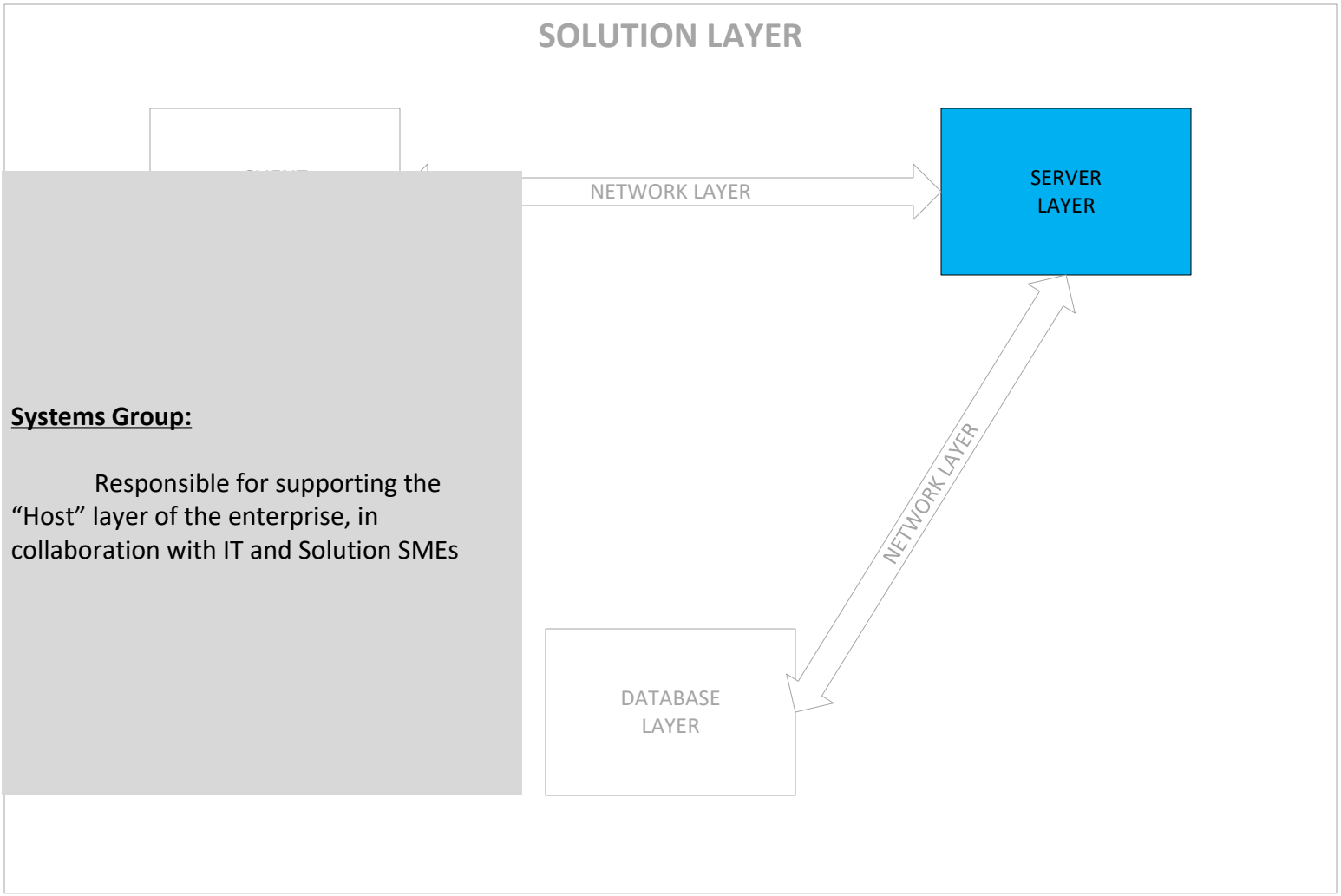
BUSINESS LAYER



BUSINESS LAYER



BUSINESS LAYER



BUSINESS LAYER

Database Group:

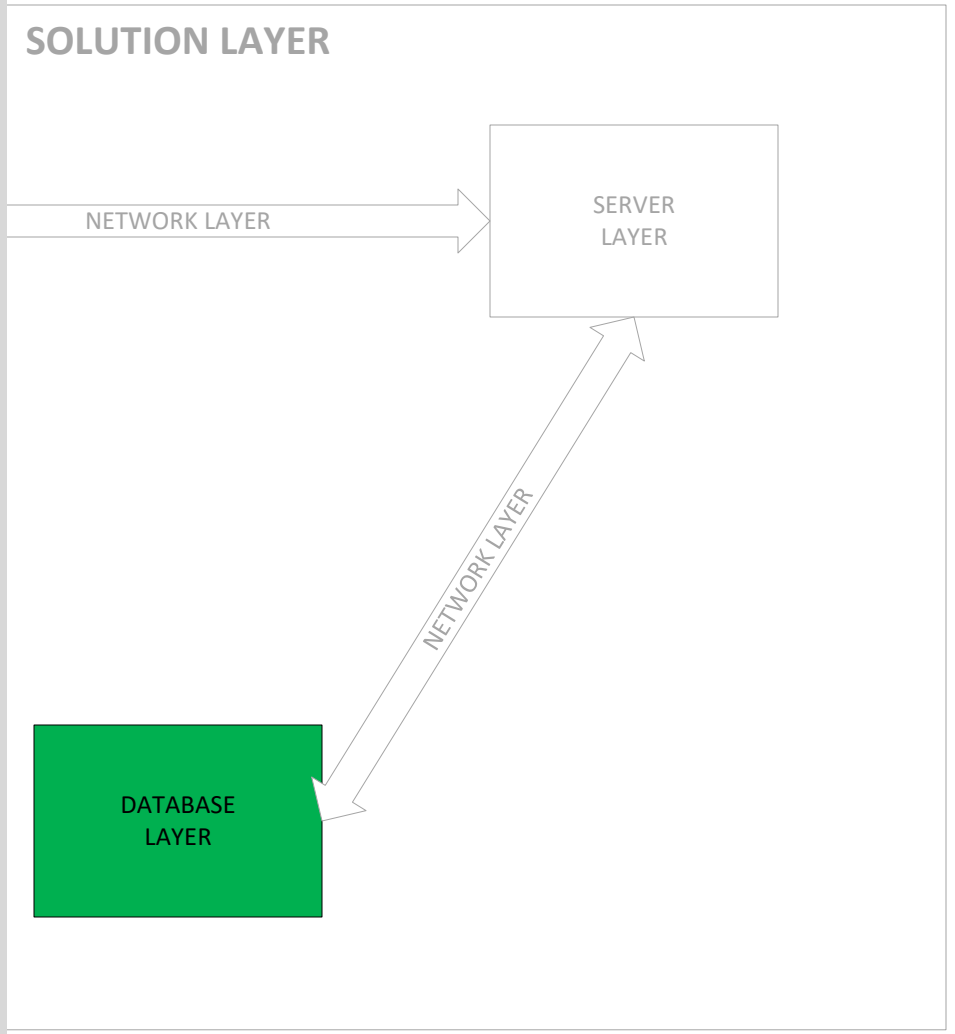
Responsible for supporting all solution artifacts that start at the DBMS Instance layer, in collaboration with Solution SMEs. *(see supporting diagram)*

Dependency on Systems Group to provision Hosts, and Network Group to provision data transport throughput.

*Dependency on Cyber(?) to provision Active Directory accounts / groups that contribute to DBMS instance layer operation.

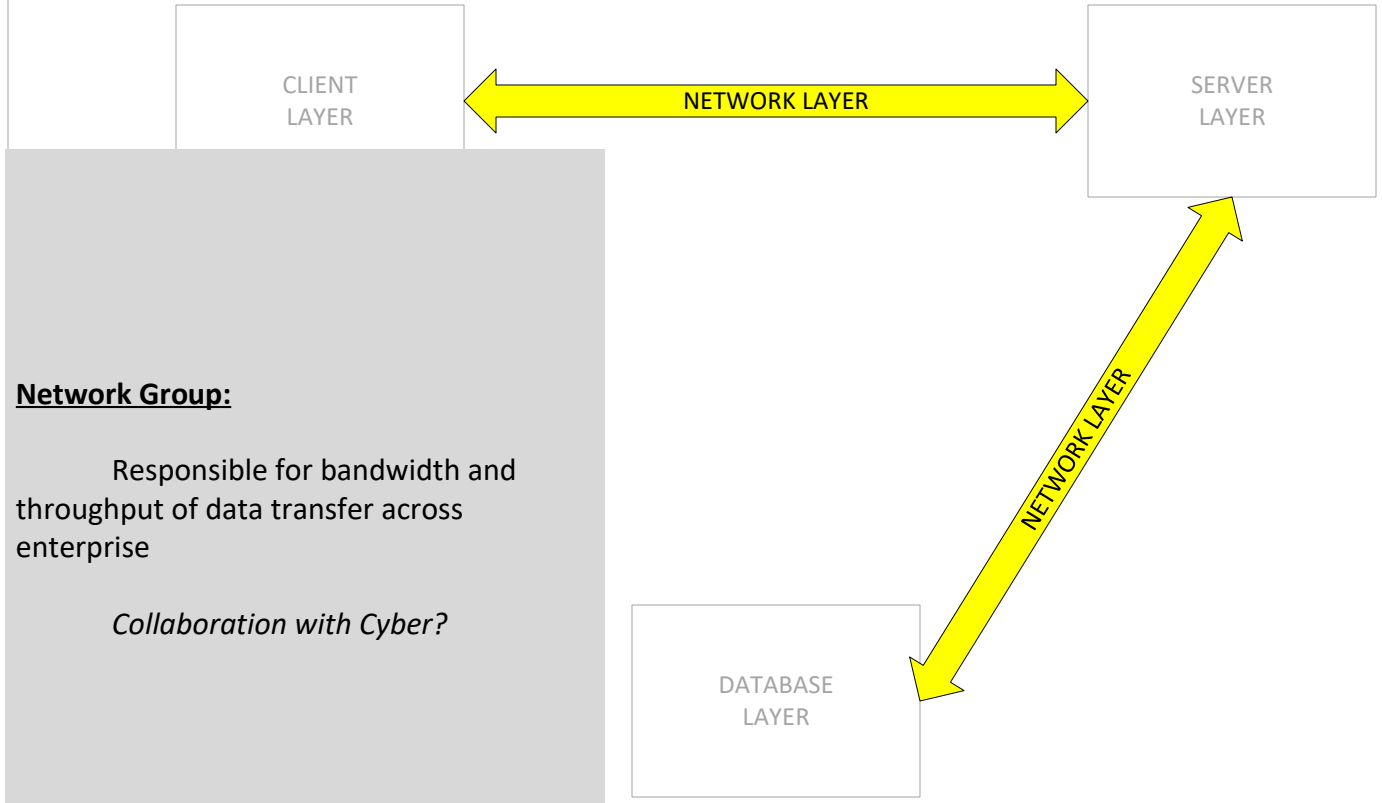
*Dependency on Cyber(?) and Business Owner / Solution SME collaboration to provision membership to Active Directory accounts / groups that provide access to DB Layer

**Current Sierra Space specific dependency*



BUSINESS LAYER

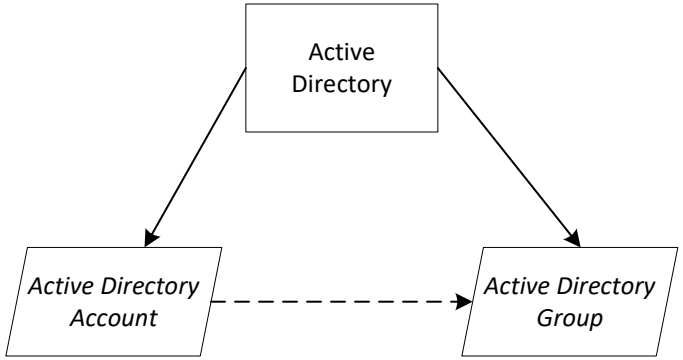
SOLUTION LAYER

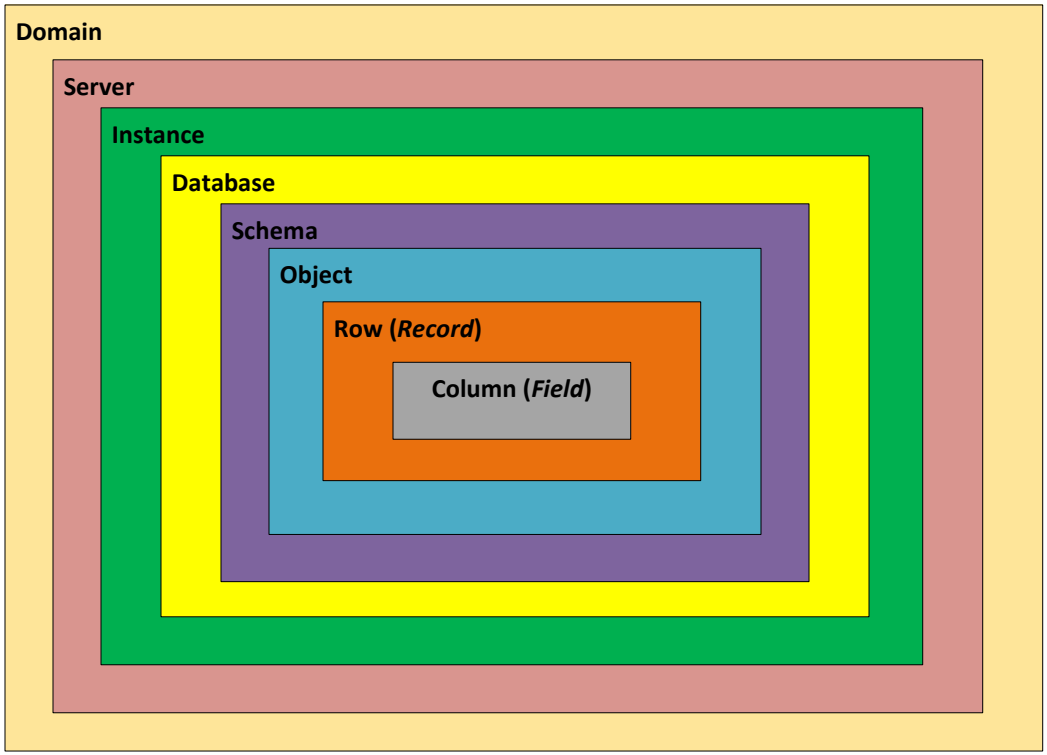


Network Group:

Responsible for bandwidth and throughput of data transfer across enterprise

Collaboration with Cyber?





(Cyber)Security Application

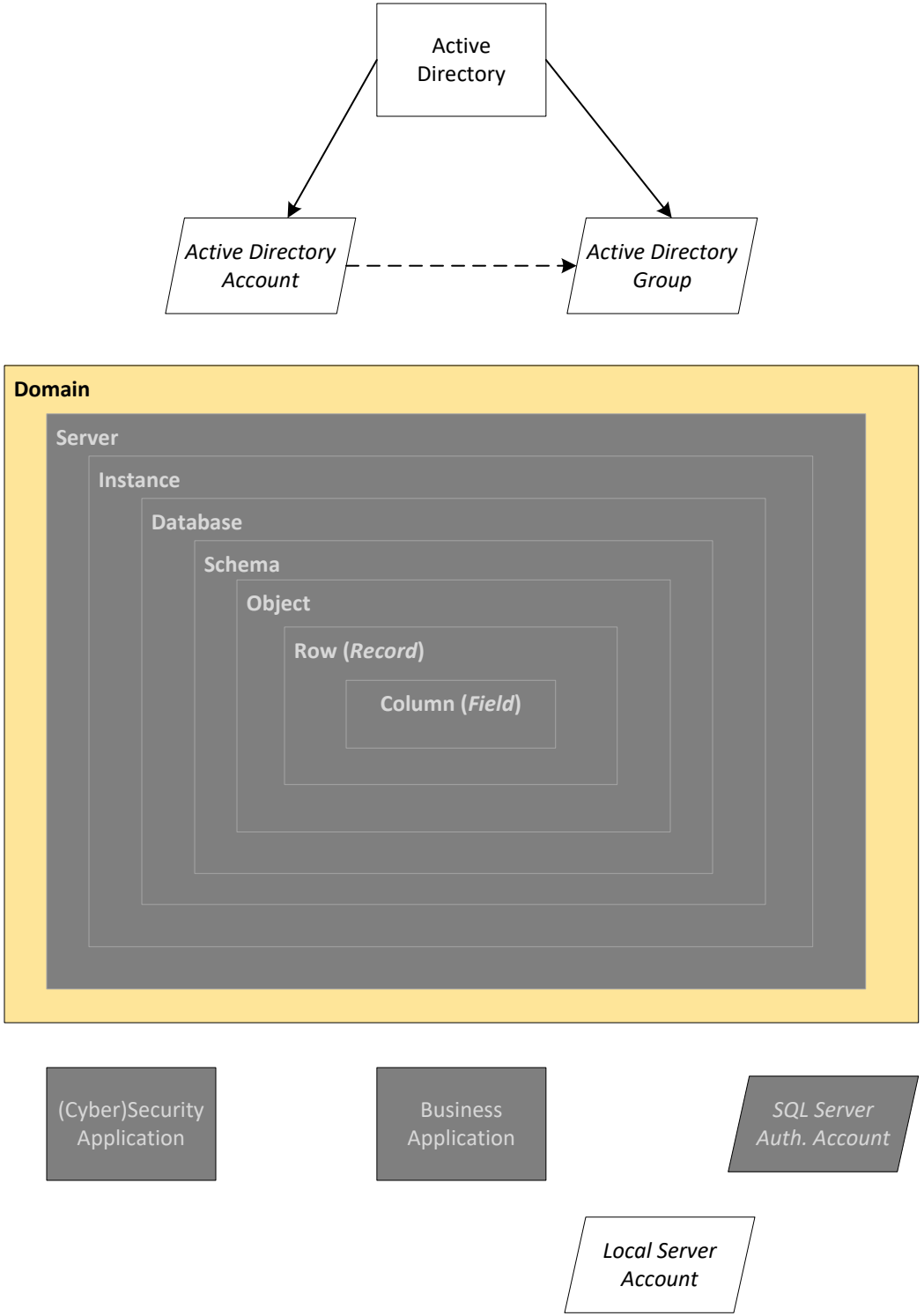
Business Application

SQL Server Auth. Account

Local Server Account

Database Environment / Dependent Objects:

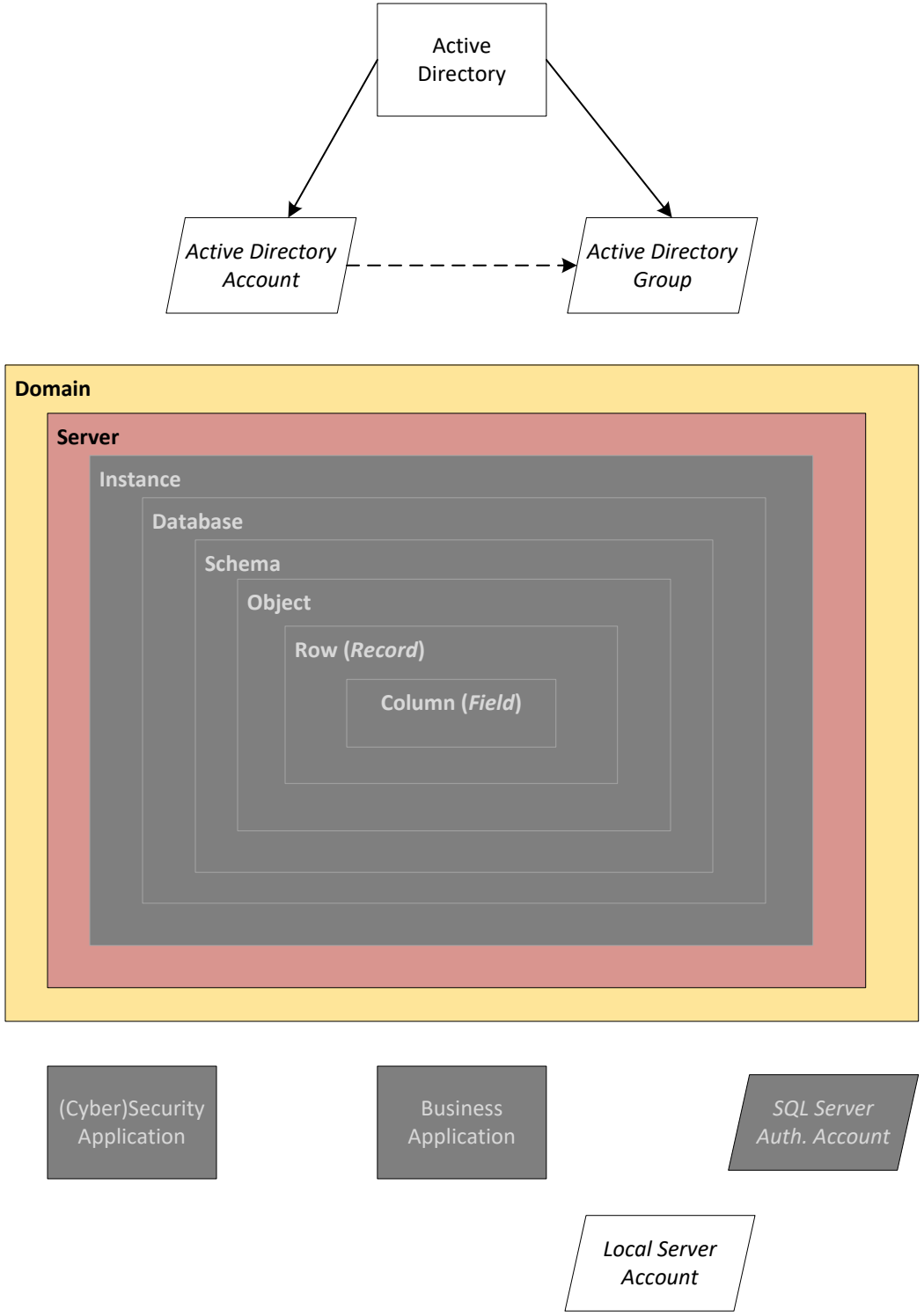
Domain *(contains servers, accounts, groups)*
Server *(contains instances, accounts, groups)*
Instance *(contains databases, accounts, groups)*
Database *(contains schemas, objects, users)*
Schema *(contains objects, users)*
Object *(contains rows, columns, data)*
Row *(contains columns)*
Column *(contains data)*



- Active Directory Accounts are created within Active Directory.

- Active Directory Security Groups are created within Active Directory, and populated with Active Directory Accounts.

- Active Directory Accounts and Groups exist on a Domain.



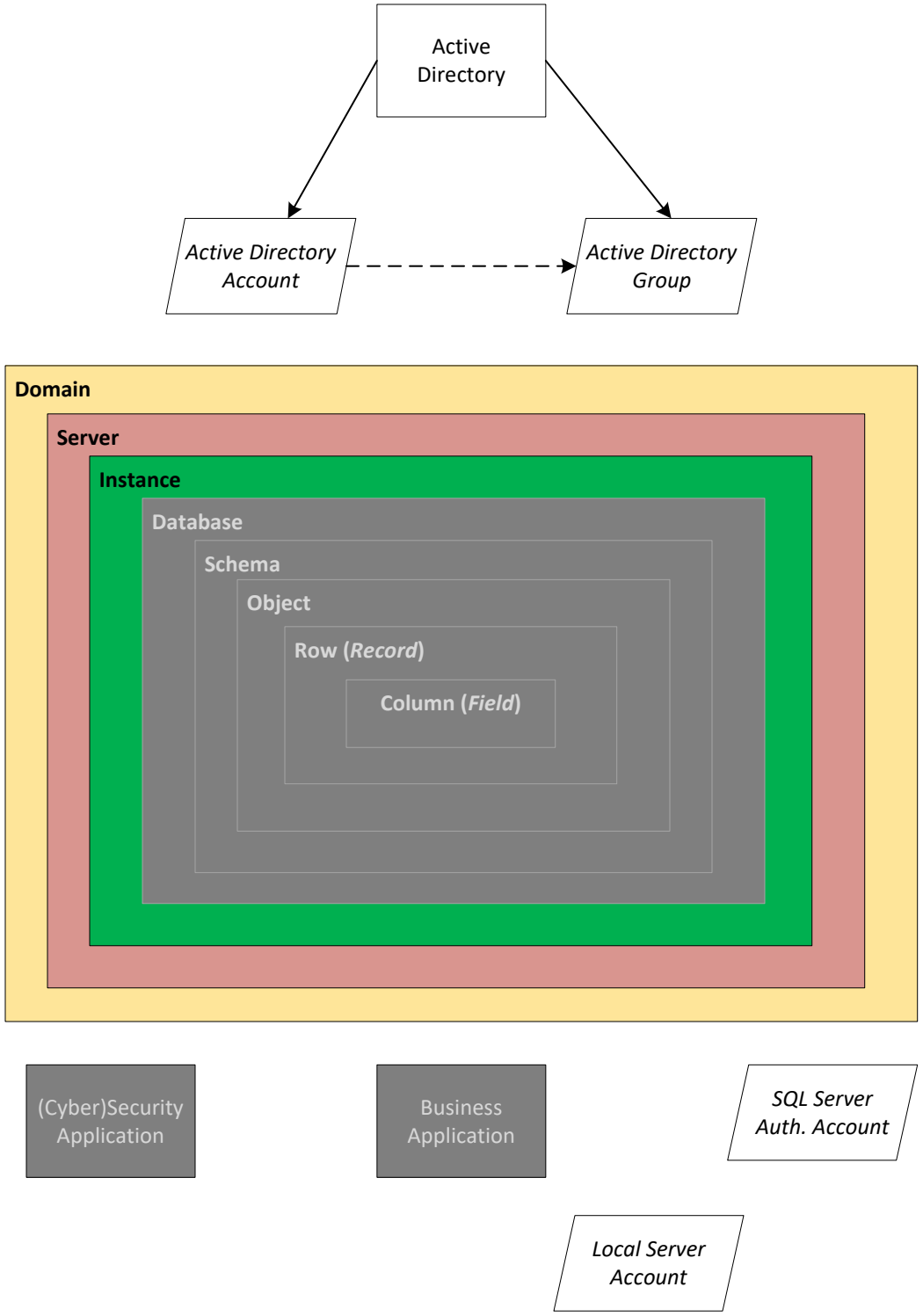
- Servers are created on, and exist within a domain.

- Active Directory Accounts and Groups that exist on a Domain, *can be* added to a Server that exists on a Domain.

- If an Active Directory Account or Group is added to a Server that exists on a domain, that Account or Group is assigned a set of permissions that apply to the Server.

- Local Server accounts exist outside of the Active Directory / Domain scope, and do not inherit any permissions.

By default, no Server level permissions are inherited by child database artifacts.



- Active Directory Account status (locked / unlocked, active / inactive, etc.) is configured at the at the Active Directory layer.

- Membership to Active Directory groups is configured at the Active Directory layer.

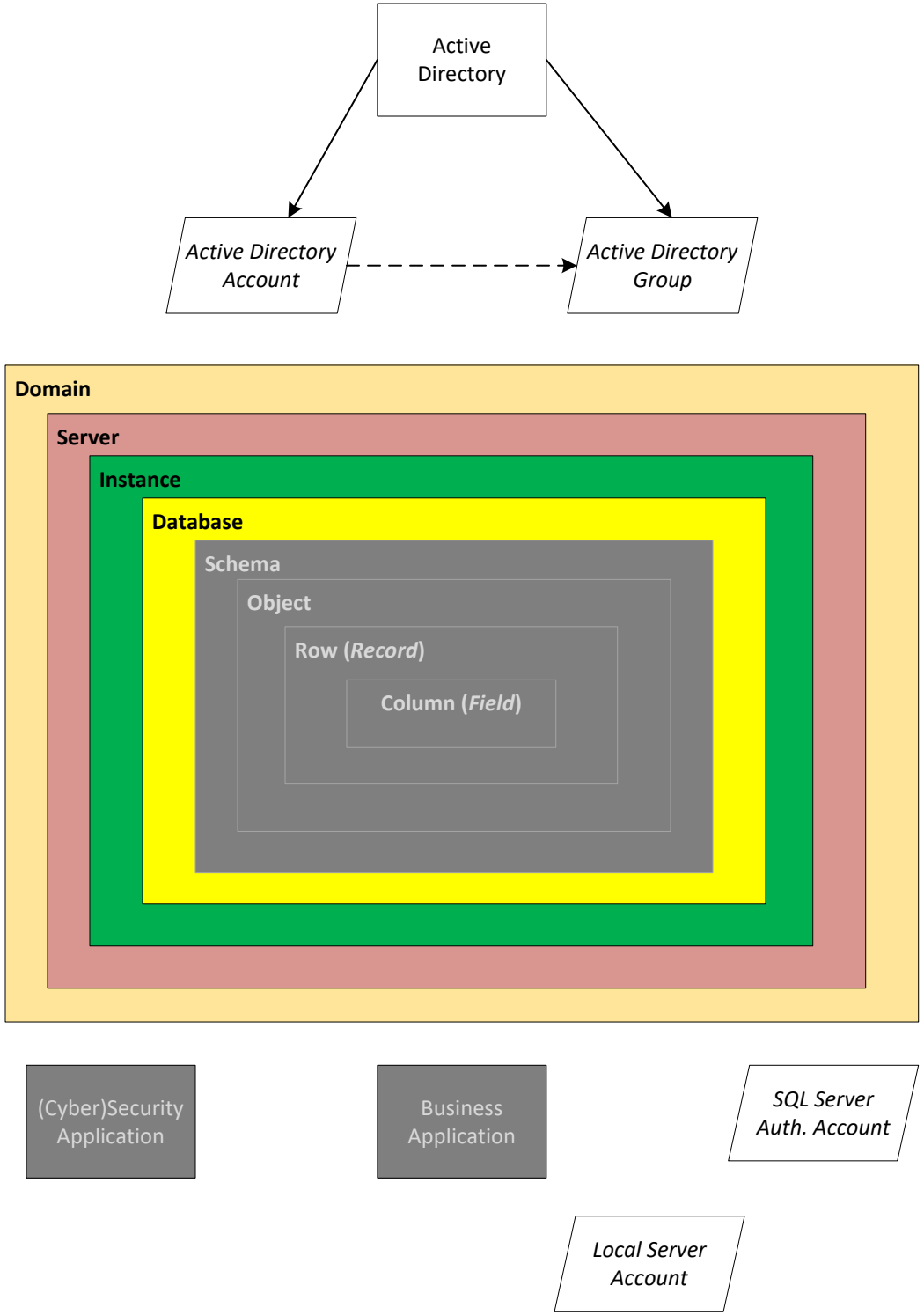
- Active Directory Accounts, *and* Active Directory Groups can be added to an Instance. By default, there are no implied permissions at the Instance layer given to an Account or Group that originates at the Active Directory layer. Permissions to the Instance for the Account or Group are configured / granted / revoked at the Instance layer.

- Local Server Accounts, *and* Local Server Groups can be added to an Instance. By default, there are no implied permissions at the Instance layer given to an Account or Group that originates at the Local Server layer. Permissions to the Instance for the Account or Group are configured / granted / revoked at the Instance layer.

- SQL Server Authenticated Accounts can be created at the Instance layer, and exist totally outside of the Domain and Server scopes. There are no implied upstream, or downstream permissions granted by default.

- “User Groups” do not exist at the SQL Server Authentication level.

- ActiveDirectory accounts, AD groups, Security Applications, Business Applications, etc. have no influence whatsoever by default.

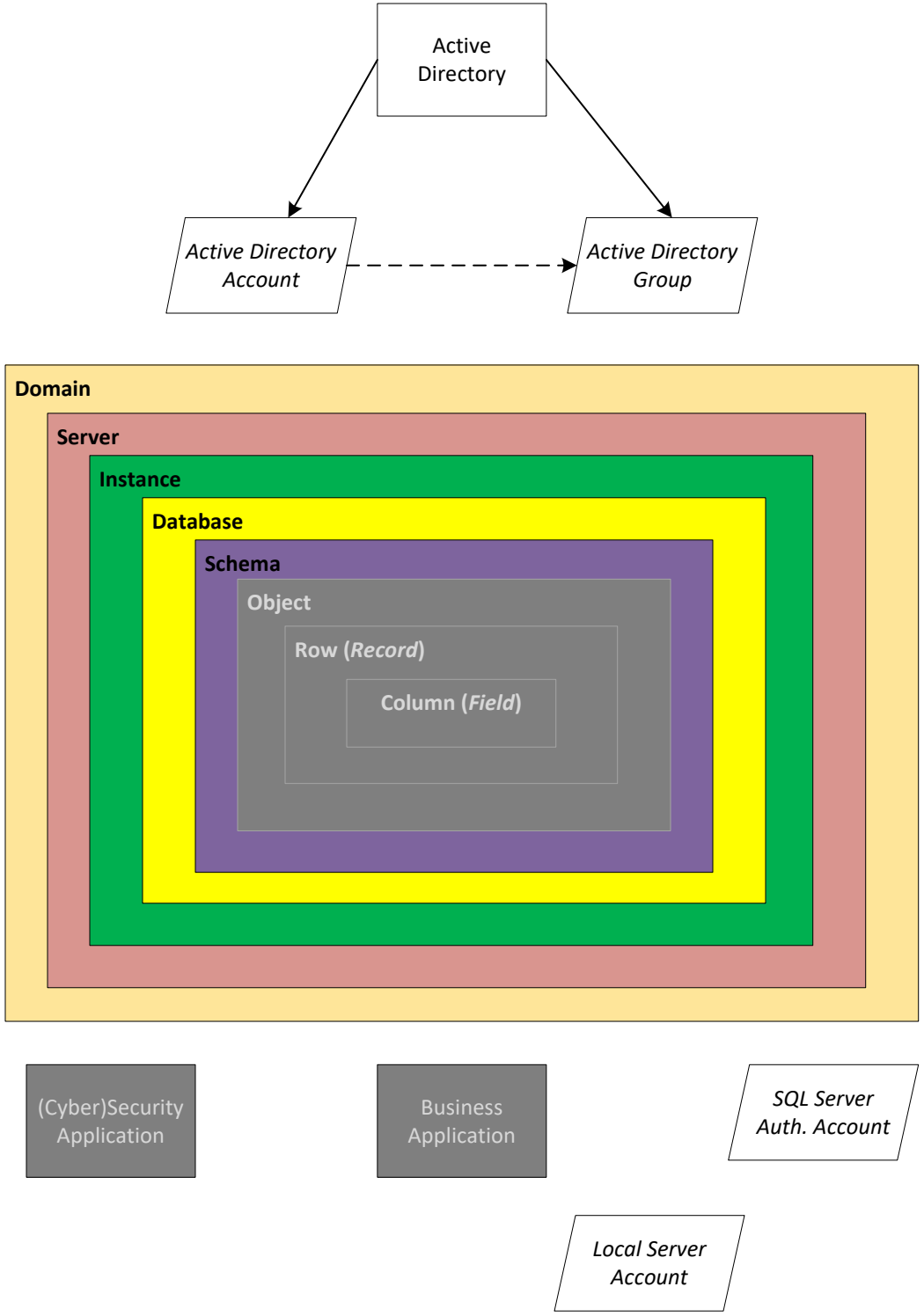


- Accounts ("*logins*") that exist at the Instance layer, irrespective of where they originate from (*AD, Local, SQL, etc.*) can be mapped to individual Users that exist at the Database level, and assigned permissions that apply to the Database level.

- There ***are*** levels of access that can be granted at the Instance layer that can supersede any permissions granted at the Database layer by default (*for example, membership to the sysadmin role at the Instance layer grants unrestricted access to **all** databases that exist within an instance*).

- Conversely, accounts that are granted rights at either the Domain or Server level (*or both*) will **NOT** inherit those rights at the Instance level by default.

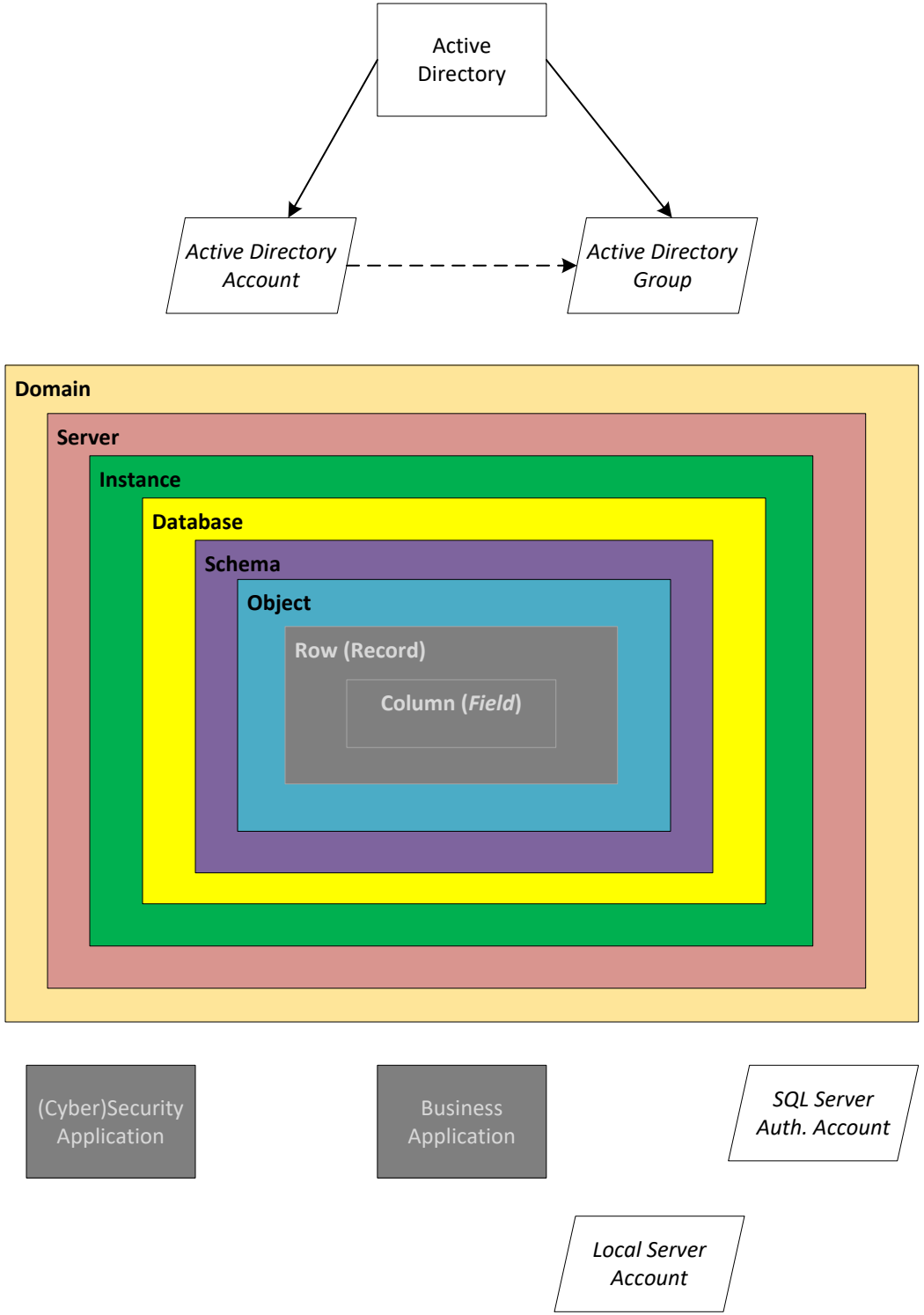
- ActiveDirectory accounts, AD groups, Security Applications, Business Applications, etc. have no influence whatsoever by default.



- Schemas exist within the Database scope, and contain logical groupings of objects. By default, permissions are inherited from the Database scope.

Fine-grained control over discrete objects within a database can be achieved through the use of schemas.

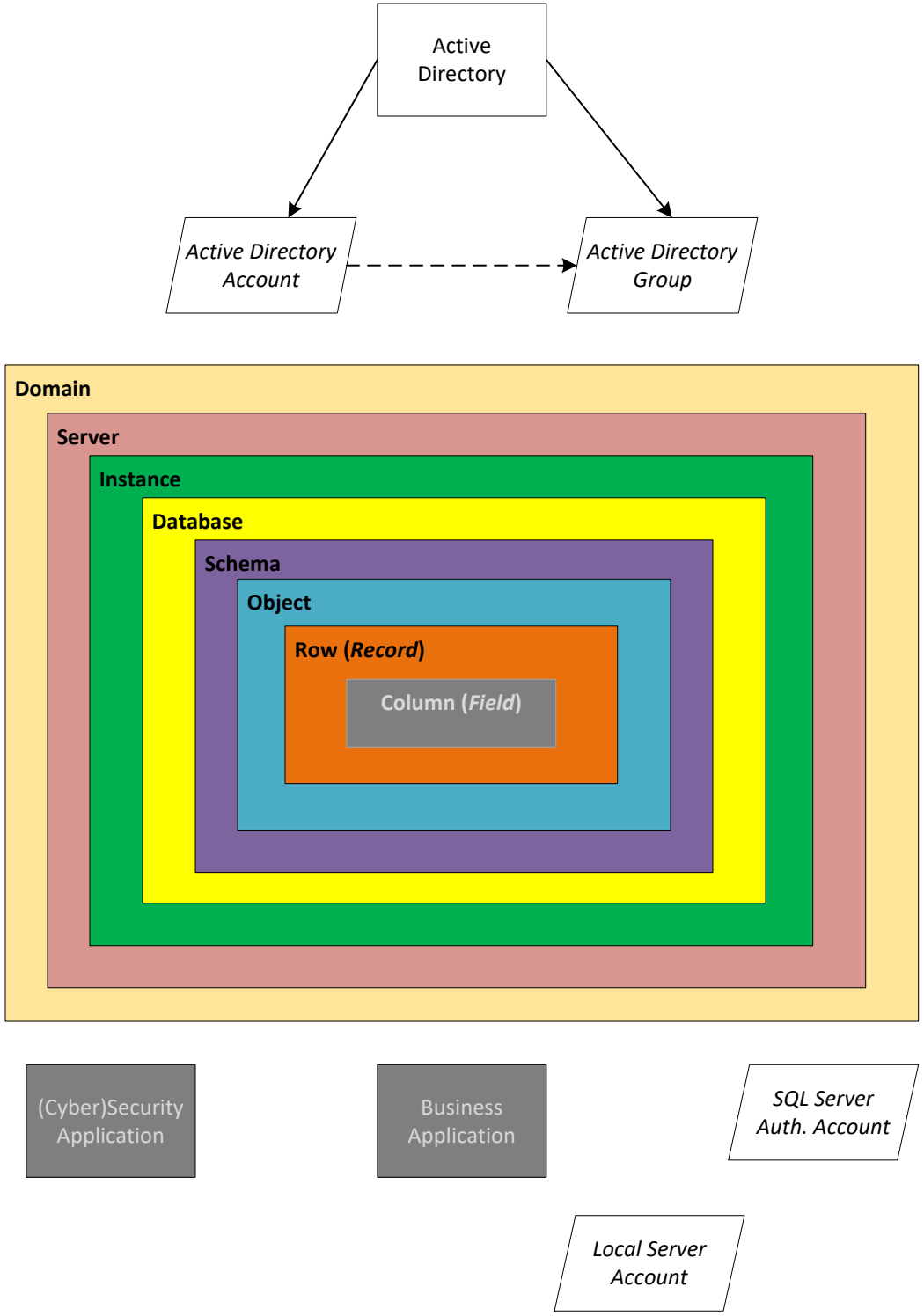
- ActiveDirectory accounts, AD groups, Security Applications, Business Applications, etc. have no influence whatsoever by default.



-Objects (tables) contain rows of data with specific attributes identified by columns.

Fine-grained control over specific objects within a database can be achieved through the use advanced security controls.

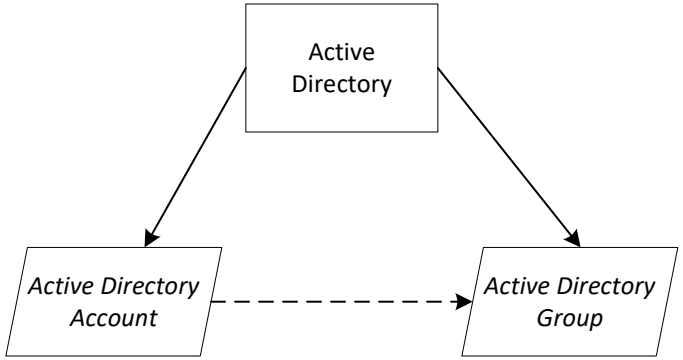
- ActiveDirectory accounts, AD groups, Security Applications, Business Applications, etc. have no influence whatsoever by default.

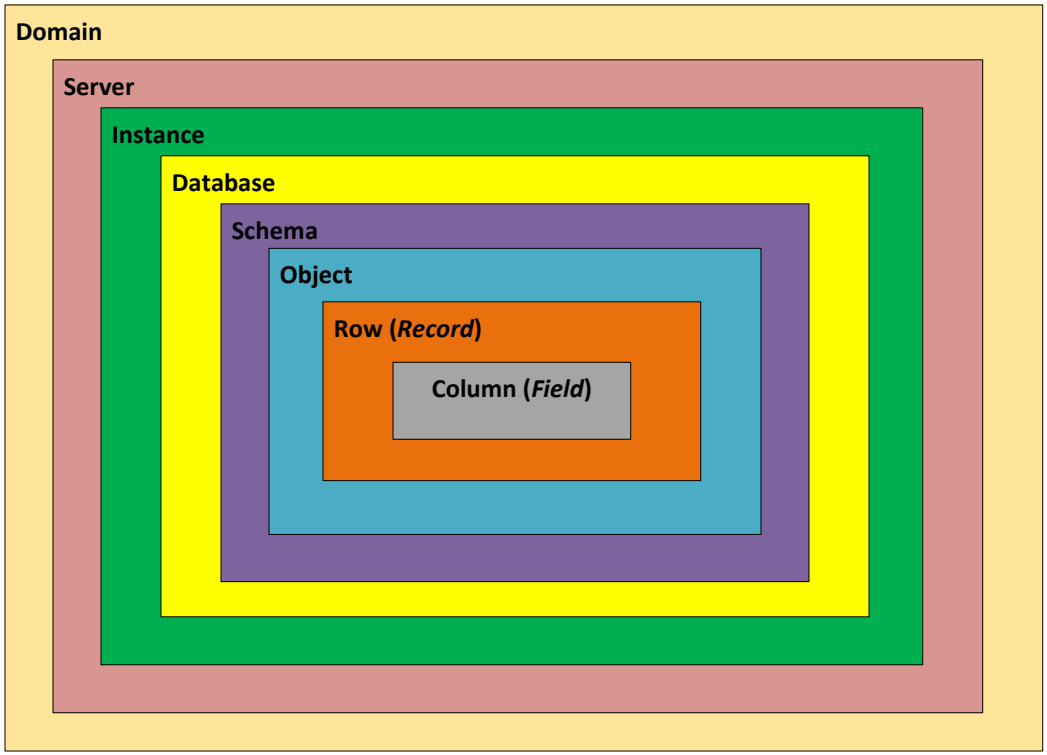


-Rows contain a collection of columns (fields) that are identified by name.

Fine-grained control over specific rows within an object (table) can be achieved through the use advanced security controls.

- ActiveDirectory accounts, AD groups, Security Applications, Business Applications, etc. have no influence whatsoever by default.





(Cyber)Security Application

Business Application

SQL Server Auth. Account

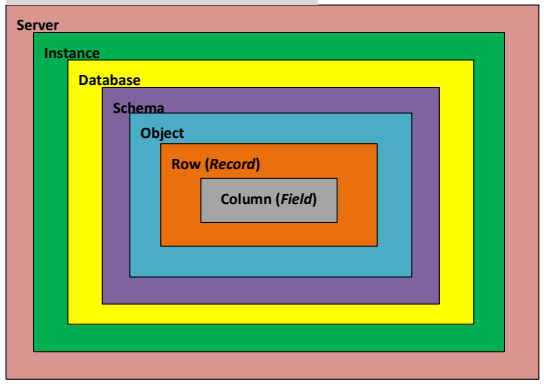
Local Server Account

-Columns (fields) exist within a row, and can contain various data attributes.

Fine-grained control over specific columns within an object (table) can be achieved through the use advanced security controls.

- ActiveDirectory accounts, AD groups, Security Applications, Business Applications, etc. have no influence whatsoever by default.

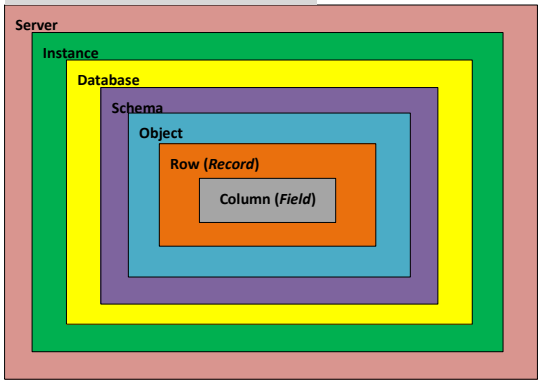
PRODUCTION



DATABASE LAYER

What's often referred to colloquially as "the database" or "SQL" is more accurately represented as shown on this page.

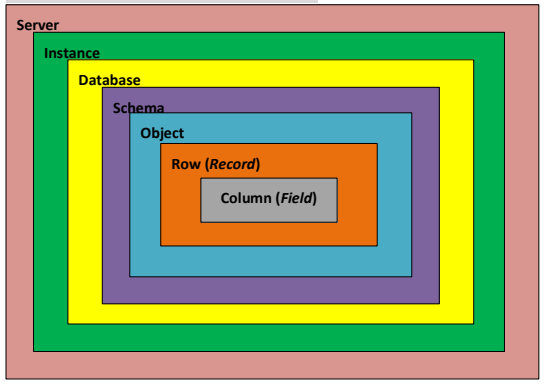
DEVELOPMENT



Relationships / Multiplicity:

Single Solution –> Multiple Apps
Single Application -> Multiple Servers
Single Server -> Multiple Instances
Single Instance -> Multiple Databases
Single Database -> Multiple Schemas
Single Schema -> Multiple Objects
Single Object -> Multiple Rows
Single Row -> Multiple Columns
Single Column -> Multiple Values

UAT



TEST