Introduction to Cybersecurity

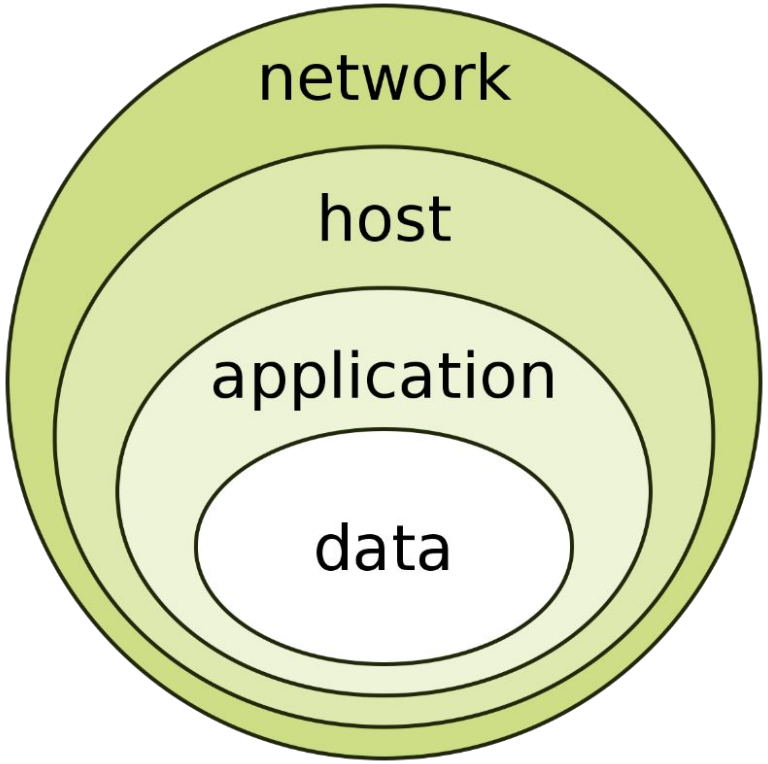
Course Incharge: **Yahya Batla**

Course Instructor: **Instructor_Name**

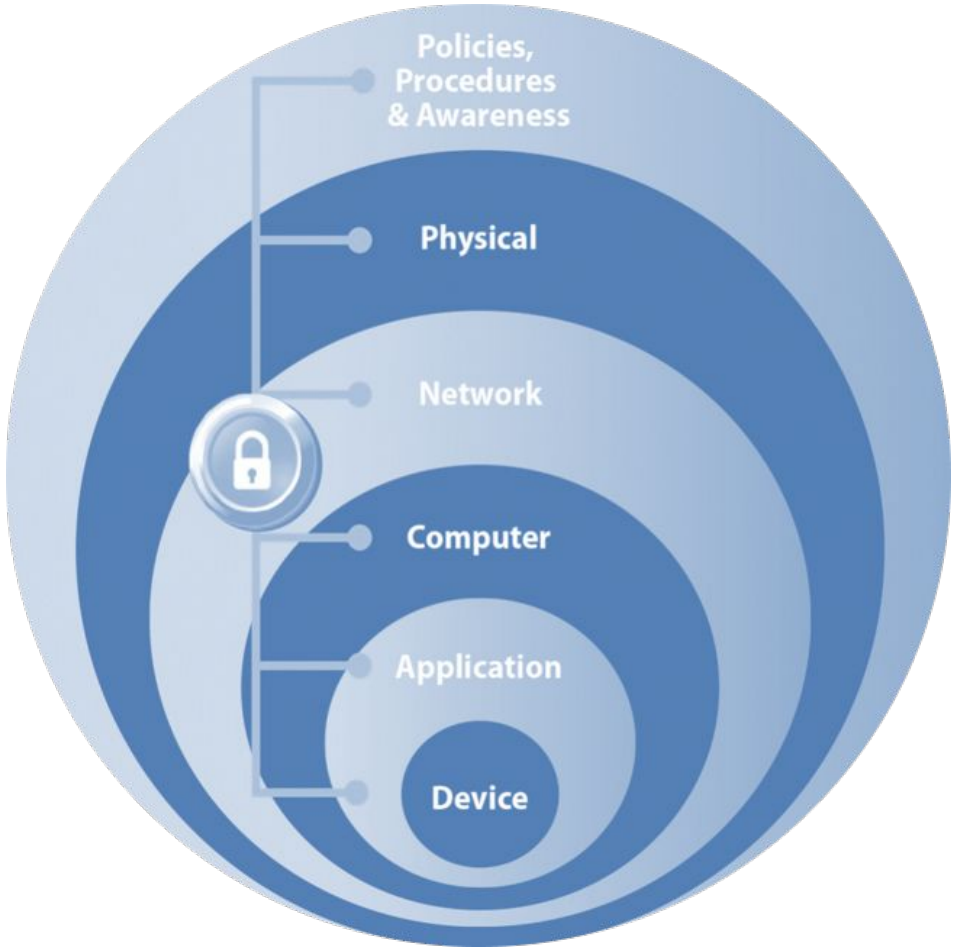
1. Defense in Depth
2. Separation of Duties
3. Privileged Access
4. Access Control
5. MAC, DAC & RBAC

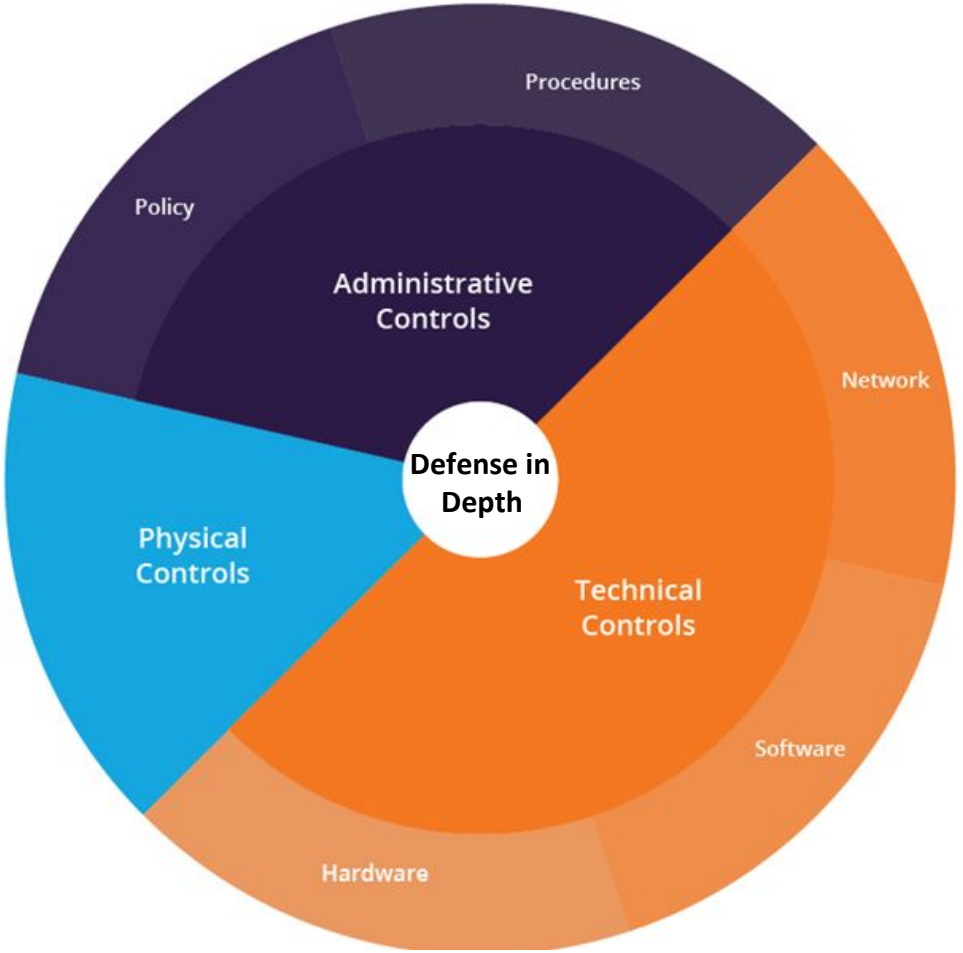
Defense in Depth (DiD)

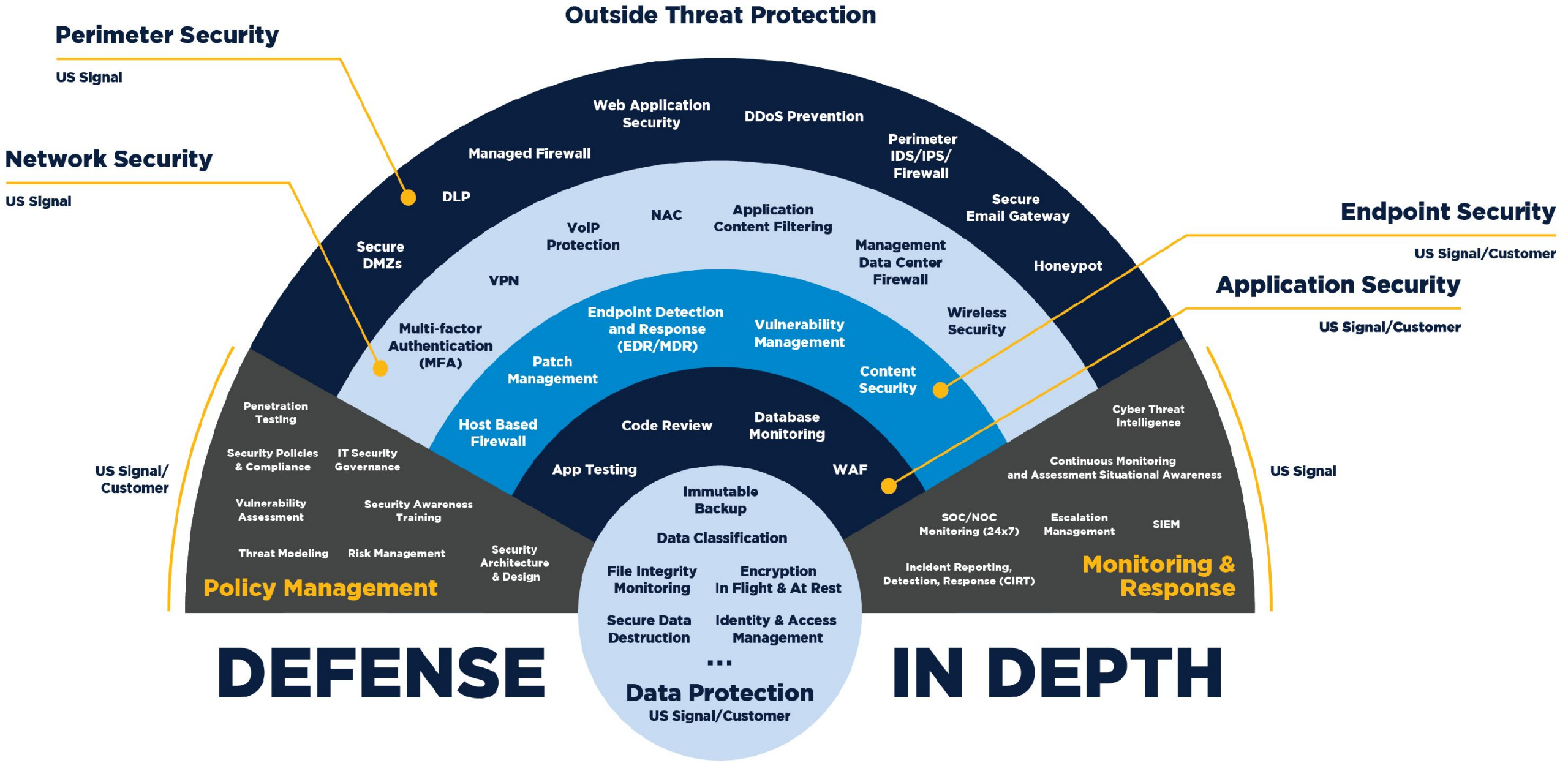
It is a comprehensive approach that employs a combination of advanced security tools to protect an organization's endpoints, data, applications, host and networks.



Defense in Depth






Outside Threat Protection
Perimeter Security
US Signal
Network Security
US Signal
Endpoint Security
US Signal/Customer
Application Security
US Signal/Customer
US Signal/ Customer
US Signal
Web Application Security
DDoS Prevention
Managed Firewall
Perimeter IDS/IPS/ Firewall
DLP
Secure Email Gateway
NAC
Application Content Filtering
VoIP Protection
Management Data Center Firewall
Secure DMZs
Honeypot
VPN
Wireless Security
Endpoint Detection and Response (EDR/MDR)
Vulnerability Management
Multi-factor Authentication (MFA)
Patch Management
Content Security
Penetration Testing
Cyber Threat Intelligence
Host Based Firewall
Code Review
Database Monitoring
Security Policies & Compliance
IT Security Governance
App Testing
WAF
Continuous Monitoring and Assessment Situational Awareness
Immutable Backup
Vulnerability Assessment
Security Awareness Training
Data Classification
SOC/NOC Monitoring (24x7)
Escalation Management
SIEM
Threat Modeling
Risk Management
Security Architecture & Design
File Integrity Monitoring
Encryption In Flight & At Rest
Incident Reporting, Detection, Response (CIRT)
Policy Management
Secure Data Destruction
Identity & Access Management
Monitoring & Response
...
Data Protection
US Signal/Customer
DEFENSE IN DEPTH

4-Key Layers of Defense in Depth

The four key layers of the defense in depth security model are:

Layer 1: Perimeter Defense: This layer is like the four walls and the roof of a secure house. It includes firewalls, routers and proxy servers.

Layer 2: Host Protection: Another threat from the internal workstations connected to the network. We use workstation endpoint security for two reasons:

- ✔ To protect against someone trying to attack from within the network.
- ✔ To protect the data stored on workstation from someone coming from outside i.e. through the firewall.

Advantage of Adopting Defense in Depth Approach

Layer 3: Operating Systems and Application Protection: This layer holds protection of operating system, the application servers, web servers, and mail servers. An abuse of operating system privileges can potentially compromise network security.

Layer 4: Data/Information Protection: Data protection can be broken down into two distinct categories:

1. Sensitive data storage practices.
2. Data encryption.

Advantage of Adopting Defense in Depth Approach

A defense-in-depth cybersecurity strategy provides a strong and resilient defense system. Its several layers of security increase the chances of staying secure.

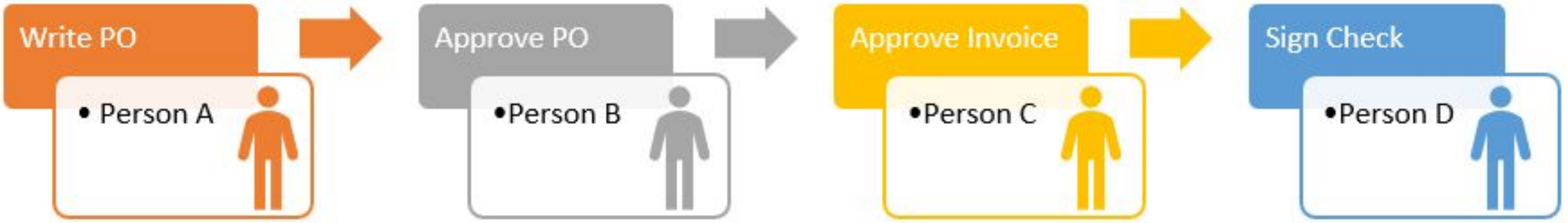
1. **Enhanced Protection:** Implementing a combination of security controls creates a robust security posture. Each layer acts as a barrier. If one layer fails, the others remain intact.
2. **Early Detection and Rapid Response:** This minimizes the impact of a potential breach. It also reduces the time an attacker has to access critical assets.
3. **Reduces Single Point of Failure:** A defense-in-depth strategy ensures that there is no single point of failure. It's better to diversify your security controls.

Separation of Duties in General

Separation of duties (SoD), also known as **Segregation of Duties**, is the concept of having more than one person required to complete a task. It is an administrative control used by organizations to prevent fraud, sabotage, theft, misuse of information, and other security compromises.

Separation of Duties in Cybersecurity

Separation of Duties (SoD) in **cybersecurity** is **a form of risk management** that is often used in cybersecurity **to mitigate insider threats** and reduce the risk of errors or accidents when it comes to mission-critical data. By having more than one person responsible for key duties, organizations can prevent conflicts of interest and better maintain data integrity and availability.



Primary Objective of Separation of Duties

Separation of duty, as a security principle, **has as its primary objective of preventing the fraud and errors.** This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users.

Fraud = Intentional

Error = Unintentional

Primary Objective of Separation of Duties

Separation of Duties is a loss-control measure designed to reduce the risk of accidental or intentional damage to the integrity, confidentiality, and availability of a transaction or process. Following are the 4 primary objectives:

1. Reduce the risk of conflict of interest OR the appearance of conflict of interest.
2. Reduce the risk of errors, fraud, abuse, theft, or other wrongful actions.
3. Comply with regulatory mandates *(e.g., SOX, HIPAA, PCI DSS, GDPR)* and industry-specific regulations *(e.g., ISO 17799)*
4. Following the **four eyes principle** helps maintain the integrity & availability of your organization's data by ensuring any data entered by employees is truthful and accurate.

Separation of Duties Video

Separation or Segregation of duties is an important concept in cyber security

https://www.youtube.com/watch?v=_rb0ITdmRtc

Privileged Access

In an enterprise environment, “Privileged Access” is a term used to designate special access or abilities above and beyond that of a standard user.

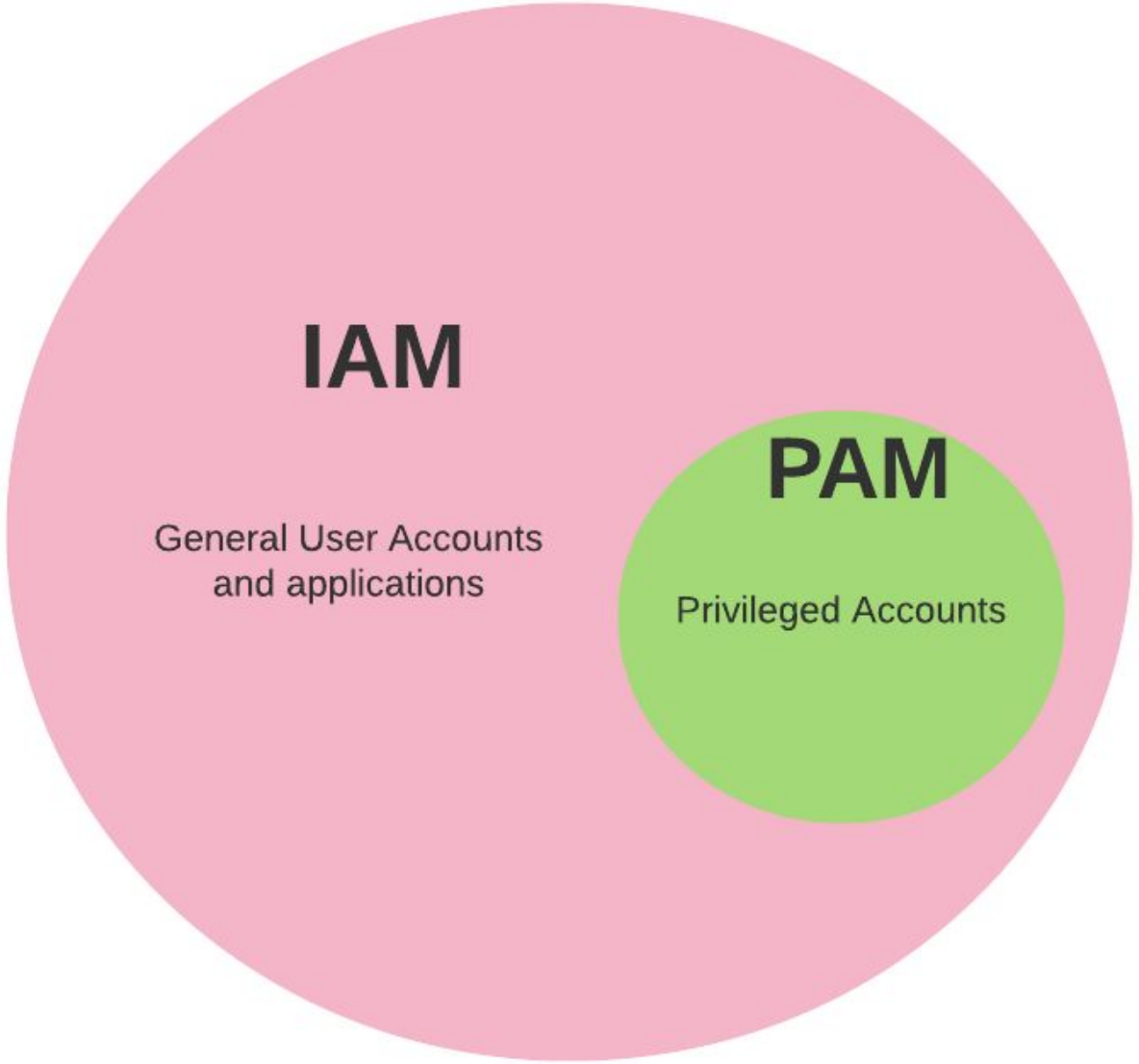
Privilege Access Management

Privileged Access Management (PAM) is an identity security solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources.

IAM vs PAM

Identity Access Management (IAM) aims to define the role and scope of every single person within an organization to ensure they can do their job correctly and efficiently.

Privileges Access Management (PAM), on the other hand, is more about monitoring and limiting access by creating a system of privileged vs. non-privileged accounts.



Types of Privileged Accounts

Type	Privileges
Superuser Accounts:	These are top-of-the-pyramid accounts with unparalleled access to systems across the network.
Administrative Accounts:	Administrative accounts can control all devices and users within a local setup (or a specific domain.
Emergency Accounts: (Break the Glass)	These are fallback accounts that administrators can turn to if their original accounts are compromised or face any issue.
Application & Service Accounts:	Applications and servers need accounts to access the operating systems, databases, etc., to function as required.
Secrets and SSH Keys:	These are mostly used by programmers and DevOps to connect to servers where codes run.

Benefits of PAM Solution

Control Access to Privileged Accounts: A PAM solution allows organizations to regulate and restrict access to privileged accounts, ensuring that only authorized individuals can use these accounts. This helps prevent unauthorized access and misuse of sensitive systems and data, enhancing overall security.

Prevent Privileged Account Attacks: PAM solutions employ security measures, such as strong authentication and session monitoring, to thwart malicious activities targeting privileged accounts. By preventing or detecting privileged account attacks, organizations can mitigate the risk of data breaches and system compromises.

Regulate Access in One Location: PAM centralizes the management of privileged access, allowing administrators to define and enforce access policies from a single location.Centralized control simplifies administration, reduces the risk of configuration errors, and provides a unified view of privileged access across the organization.

Benefits of PAM Solution

Review Risky Behavior Notifications in Real-Time: PAM solutions often include real-time monitoring capabilities that generate alerts for suspicious or risky behavior related to privileged access. Organizations can respond promptly to potential security threats, investigate incidents, and take corrective actions to prevent further risks.

Integrate with Identity & Access Management Systems: PAM solutions can integrate seamlessly with Identity and Access Management (IAM) systems, providing a cohesive approach to managing user identities and their access privileges. Integration streamlines administrative processes, enhances interoperability, and ensures consistency in access controls across the organization.

Uphold IT Compliance: PAM solutions help organizations meet regulatory and compliance requirements by enforcing strict controls over privileged access, maintaining audit trails, and facilitating regular access reviews. Upholding IT compliance not only mitigates legal and regulatory risks but also enhances overall cybersecurity practices.

PAM Software

- ✔ Beyond Trust
- ✔ Cyber Ark
- ✔ Delinea Secret Server
- ✔ JumpCloud
- ✔ Microsoft EntraID
- ✔ One Identity
- ✔ ARCON
- ✔ FoxPass
- ✔ Manage Engine
- ✔ Ermatic

PAM Video

Protect Your Business with Privileged Access Management (PAM)

https://www.youtube.com/watch?v=IJhGKez5LLY

Access Control

Access Control involves identifying a user based on their credentials and then authorizing the appropriate level of access once they are authenticated.

Identity & Access Management

Identity & Access Management (IAM) is a security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay.

Types of Access Control

Information Security Access Controls

MAC
Mandatory Access Control

DAC
Discretionary Access Control

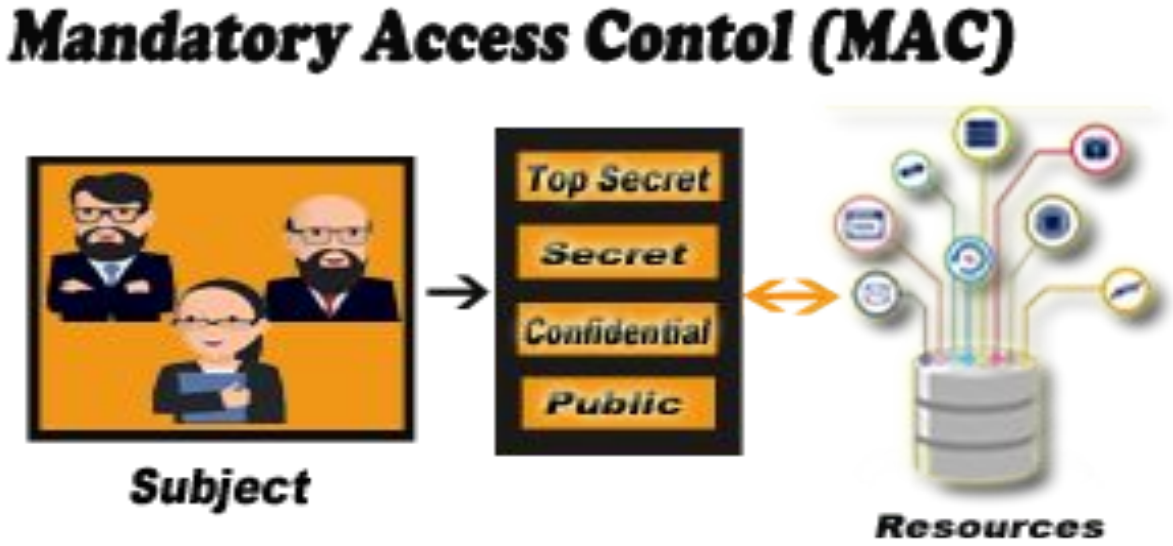
RBAC
Role Based Access Control

RuBAC
Rule Based Access Control

ABAC
Attribute Based Access Control

MAC (Mandatory Access Control)

MAC is the **most strictly enforced control** method. All the access control settings and configurations are only accessible by the administrator. You can't change anything without their permission. Often used in government and military environments, classifications are assigned to system resources and the operating system or security kernel.



MAC (Mandatory Access Control)

A mandatory access control (MAC) policy is one that is uniformly enforced across all subjects and objects within the boundary of an information system. In simplest terms, this means that only properly designated security administrators, as trusted subjects, can modify any of the security rules that are established for subjects and objects within the system. This also means that for all subjects defined by the organization (that is, known to its integrated identity management and access control system), the organization assigns a subset of total privileges for a subset of objects, such that the subject is constrained from doing any of the following:

- Passing the information to unauthorized subjects or objects
- Granting its privileges to other subjects
- Changing one or more security attributes on subjects, objects, the information system or system components
- Choosing the security attributes to be associated with newly created or modified objects
- Changing the rules governing access control

Although MAC sounds very similar to DAC, the primary difference is who can control access. With Mandatory Access Control, it is mandatory for security administrators to assign access rights or permissions; with Discretionary Access Control, it is up to the object owner's discretion.

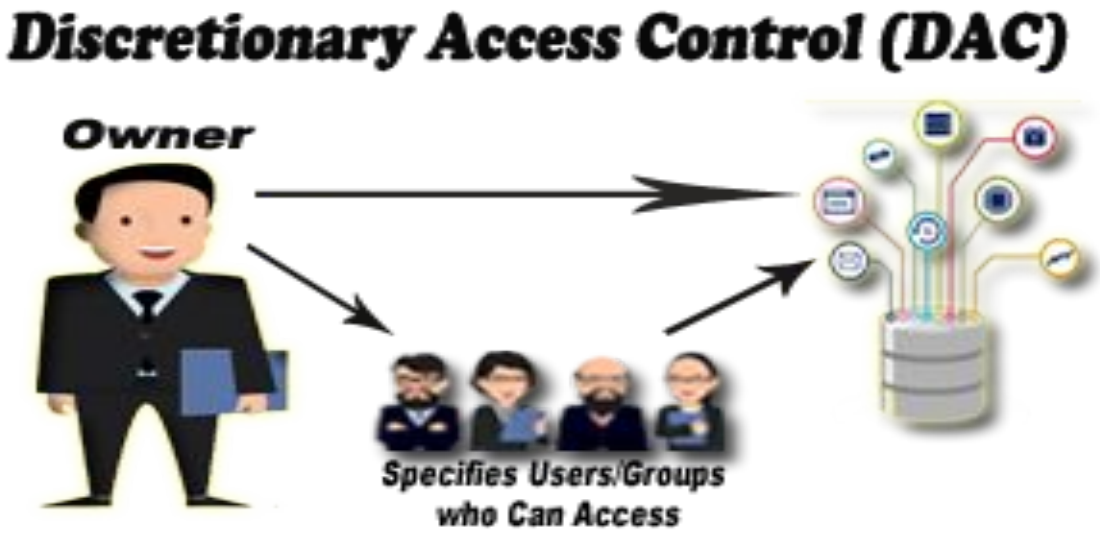
DAC (Discretionary Access Control)

It allows you to grant or restrict object access, where object in this context means **data entity**.

DAC provides granular access control that suits businesses having dynamic security needs. Firstly, DAC allows you to change or transfer ownership of an object from one user to another. Secondly, the object access in DAC uses an access control list (ACL) authorization.

DAC offers several advantages:

- ✔ minimal administrative obligations.
- ✔ great customization.
- ✔ simple role management.
- ✔ reduced costs.



DAC (Discretionary Access Control)

Discretionary access control (DAC) is a specific type of access control policy that is enforced over all subjects and objects in an information system. In DAC, the policy specifies that a subject who has been granted access to information can do one or more of the following:

- Pass the information to other subjects or objects
- Grant its privileges to other subjects
- Change security attributes on subjects, objects, information systems or system components
- Choose the security attributes to be associated with newly created or revised objects; and/or
- Change the rules governing access control; mandatory access controls restrict this capability

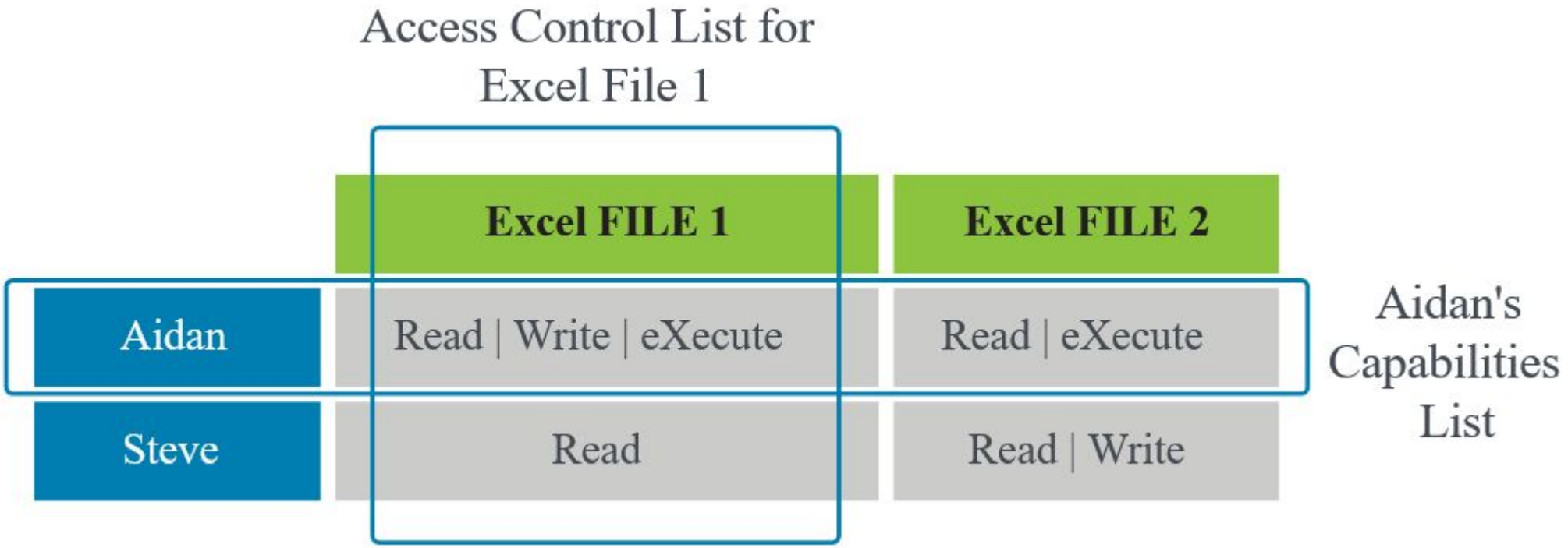
Most information systems in the world are DAC systems. In a DAC system, a user who has access to a file is usually able to share that file with or pass it to someone else. This grants the user almost the same level of access as the original owner of the file.

DAC (Discretionary Access Control)

Steve and Aidan, for example, are two users (subjects) in a UNIX environment operating with DAC in place. Typically, systems will create and maintain a table that maps subjects to objects, as shown in the image. At each intersection is the set of permissions that a given subject has for a specific object. Many operating systems, such as Windows and the whole Unix family tree (including Linux) and iOS, use this type of data structure to make fast, accurate decisions about authorizing or denying an access request. Note that this data can be viewed as either rows or columns:

DAC (Discretionary Access Control)

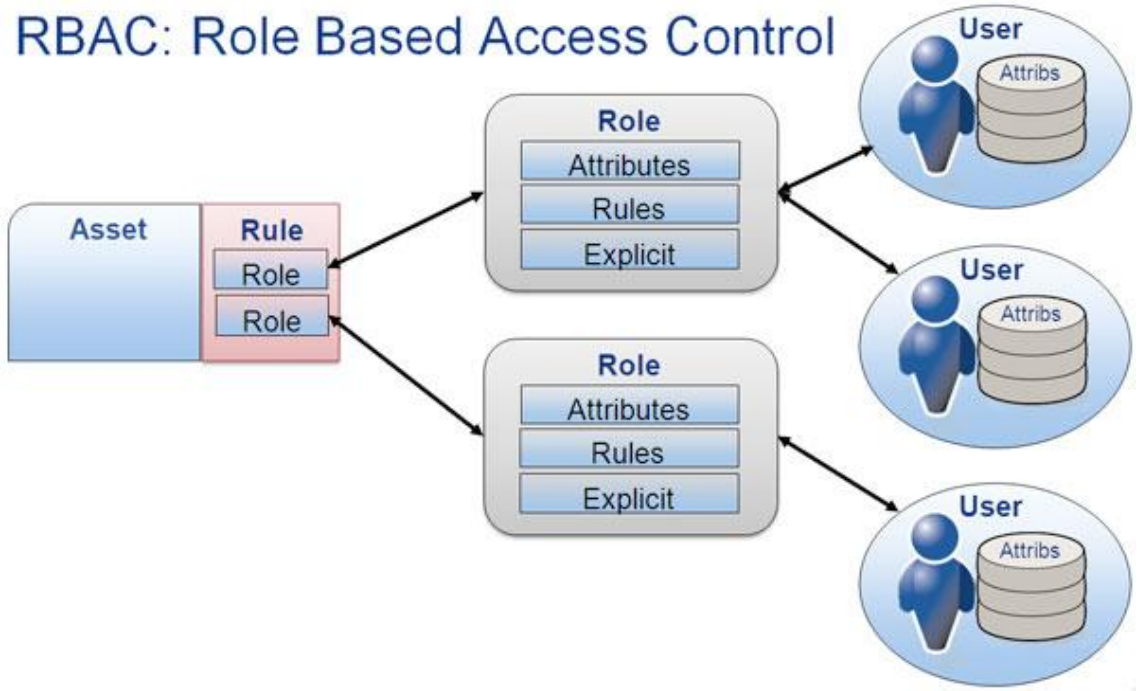
- An object's access control list shows the total set of subjects who have any permissions at all for that specific object.
- A subject's capabilities list shows each object in the system that said subject has any permissions for.



RBAC (Role Based Access Control)

It is becoming one of the **most widely adopted control methods**. RBAC allows you to group individuals together and assign permissions for specific roles. If you decide to use RBAC, you can also add roles into groups or directly to users.

RBAC makes assessing and **managing permissions** and roles easy. It utilizes the **principle of least privileges** and reduces administration costs.



RuBAC (Rule Based Access Control)

It’s based on a **predefined set of rules** or access permissions. This is regardless of the role of individuals accessing the files.

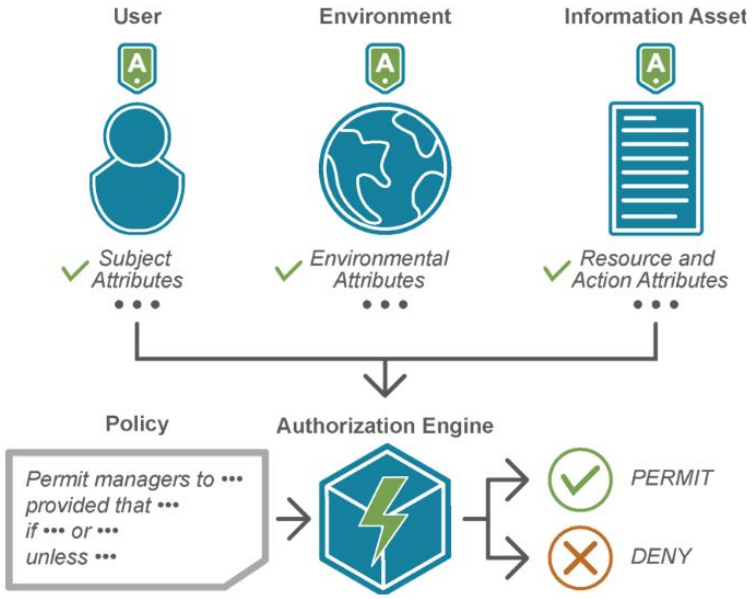
In RuBAC, a system administrator creates and controls the rules that determine the usage and access of business resources. In this type of access control, rules supersede the access and permissions.

Often RuBAC is useful for controlling access to confidential resources. This approach needs **another level of maintenance** and **constant monitoring**.

ABAC (Attribute Based Access Control)

ABAC's authorization model **evaluates attributes instead of roles** or users. It provides you with a more fine-grain approach over access controls. ABAC allows you to use user attributes such as username, role, and security clearance. Additionally, you can use environmental attributes such as **time of access** and **location of data**.

ABAC has several more controlling variables than any of the other control methods. This makes it useful in larger businesses with **complex hierarchical structures**. One of the major advantages of using ABAC is not needing to change existing rules to accommodate new users.



Select the Best Access Control For Your Set-Up

Attribute / Access Control Type	DAC	MAC	RBAC	ABAC	RuBAC
Ease of Usage	High	Varies	High	High	High
Performance	Low	Varies with Security Level	High	High	High
Reusability	Yes	No	Yes	Yes	Yes
Single Point Failure	Authorization Failure	Less	Less	-	Authorization Failure
Authentication Failure	Less	Varies	Based on Role	Less	Less

IAM Software

- ✔ Okta
- ✔ Cyber Ark
- ✔ OneLogin
- ✔ JumpCloud
- ✔ ForgeRock
- ✔ Autho
- ✔ OpenIAM
- ✔ IBM Security Verify
- ✔ Manage Engine
- ✔ Midpoint

Identity & Access Management (IAM)

https://www.youtube.com/watch?v=aNj36g7fSsU

بنو قابل

اپنی دُنیا آپ پیدا کر

THANK YOU