CompTIA SECURITY+ Day 01

SECURITY GOALS AND CONTROLS

Objectives

- Provide an overview of confidentiality, integrity, availability, and non-repudiation
- Describe the concepts of authentication, authorization, and accounting (AAA)
- Describe control categories
- Define control types

THE CIA TRIAD

CONFIDENTIALITY

AVAILABILITY

INTEGRITY

CONFIDENTIALITY

- Measures an attacker's ability to get unauthorized access to data or information from an application or system
- Involves using techniques, often cryptography, to allow only approved subjects with the ability to view information
- Includes preserving authorized restrictions on information access and disclosure

CONFIDENTIALITY

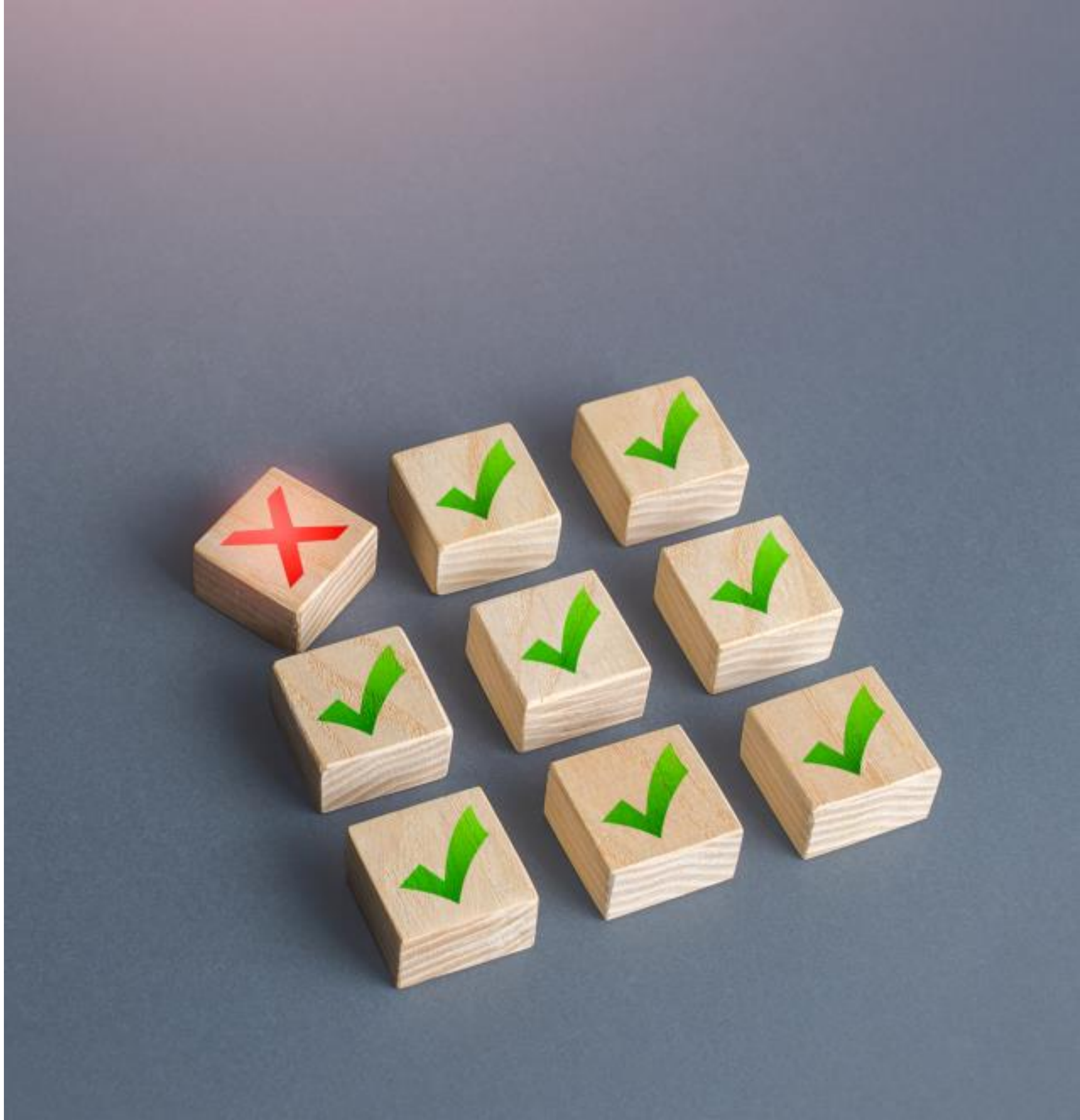
- It is a means for protecting personal privacy and proprietary information
- Confidential information can include passwords, cryptographic keys, personally identifiable information (PII), personal health information (PHI), intellectual property (IP), or other sensitive information

EXAMPLES OF CONFIDENTIALITY

- Using an IPsec virtual private network (VPN)
- Leveraging mutual Transport Layer Security (TLS) between a web browser and web server or controller
- Storing sensitive data or credentials in a mobile device partition or secure enclave
- Implementing Advanced Encryption Standard (AES) encryption on data at rest in storage (file, block, object, databases, etc.)

INTEGRITY

- Involves safeguarding against improper information modification or destruction
- Is a property that data or information have not been altered or damaged in an unauthorized way
- Is the quality of an IT system that reflects:
  - The logical correctness and reliability of the operating system
  - The logical completeness of the hardware and software that implements the protection mechanisms
  - The consistency of the data structures and occurrence of the stored data



EXAMPLES OF INTEGRITY

- An operating system that performs a mathematical checksum when a file is moved or copied from one volume to another
- A frame check sequence conducted on an Ethernet frame when sent from one MAC address to another
- A hashed message authentication code applied to advertisements sent between neighbor systems such as routers or gateways
- Implementation of a mandatory access model technique such as Biba or Clark-Wilson

AVAILABILITY

- Availability is the process of ensuring timely and reliable access to and use of information
- It is a property of data, information, applications, systems, or services that are accessible and usable upon demand by an authorized subject
- "High availability" is a failover feature to ensure availability during device or component interruptions both, planned and unplanned

EXAMPLES OF AVAILABILITY

- Implementing security controls that protect systems and services from spoofing, flooding, denial-of-service (DDoS), poisoning, and other attacks that negatively affect the ability to deliver data, content, or services:
  - Vulnerabilities that impact availability can affect hardware, software, and network resources, such as flooding network bandwidth, consuming large amounts of memory, CPU cycles, or unnecessary power consumption

EXAMPLES OF AVAILABILITY

- Assuring that technical controls such as firewalls, intrusion prevention system (IPS) sensors, anti-virus, and endpoint protection are always reliable and deployed in a failover group or cluster
- Determining the best disaster recovery site solution for every scenario or situation for an organization

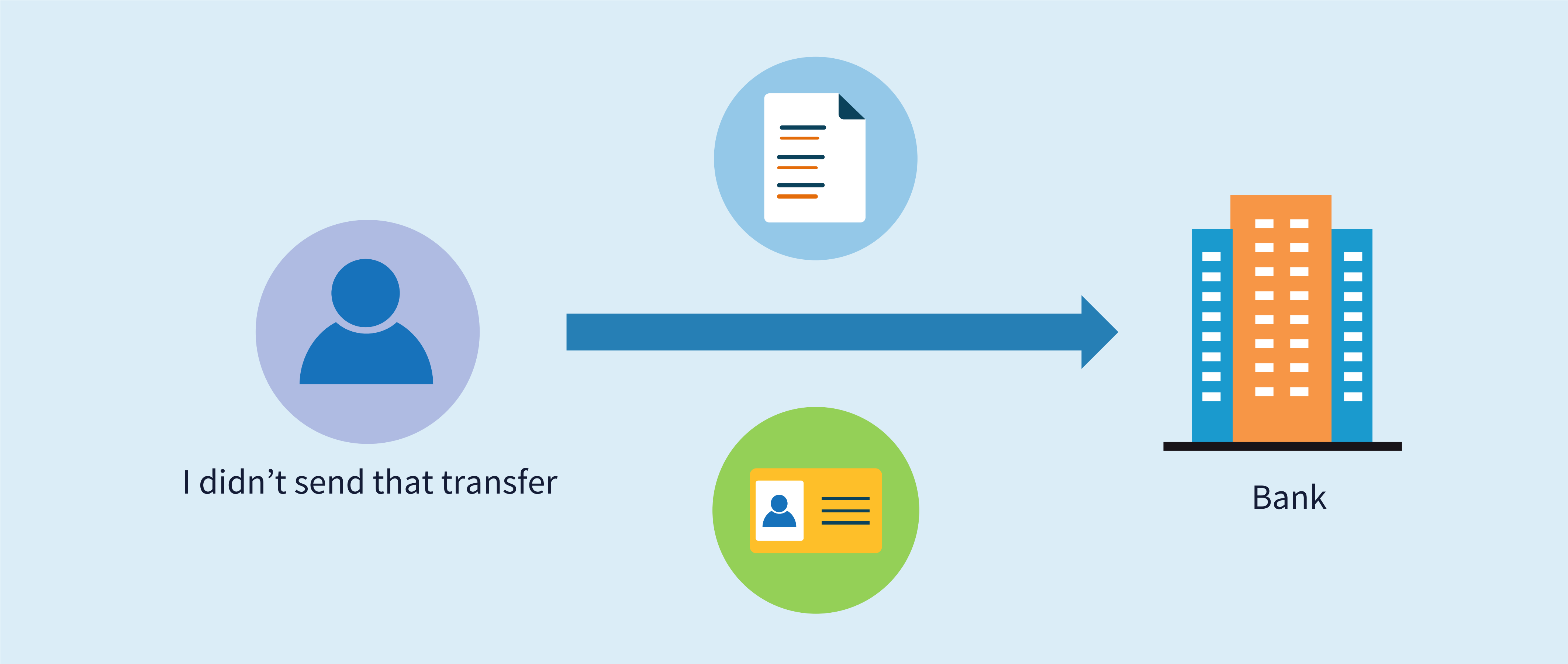
NON-REPUDIATION

- Non-repudiation refers to enforcing the inability of a subject to deny that they participated in a digital transaction, agreement, contract, or communication such as an email
- Non-repudiation is the property of agreeing to adhere to an obligation:
  - More specifically, it is the inability to refute responsibility

NON-REPUDIATION

- For example, if you take a pen and sign a (legal) contract, your signature is a non-repudiation device
- In IT, non-repudiation is usually accomplished with a public/private key pair cryptosystem and digitally signed certificates between the sending and receiving parties

REPUDIATION OF ORIGIN



AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA)

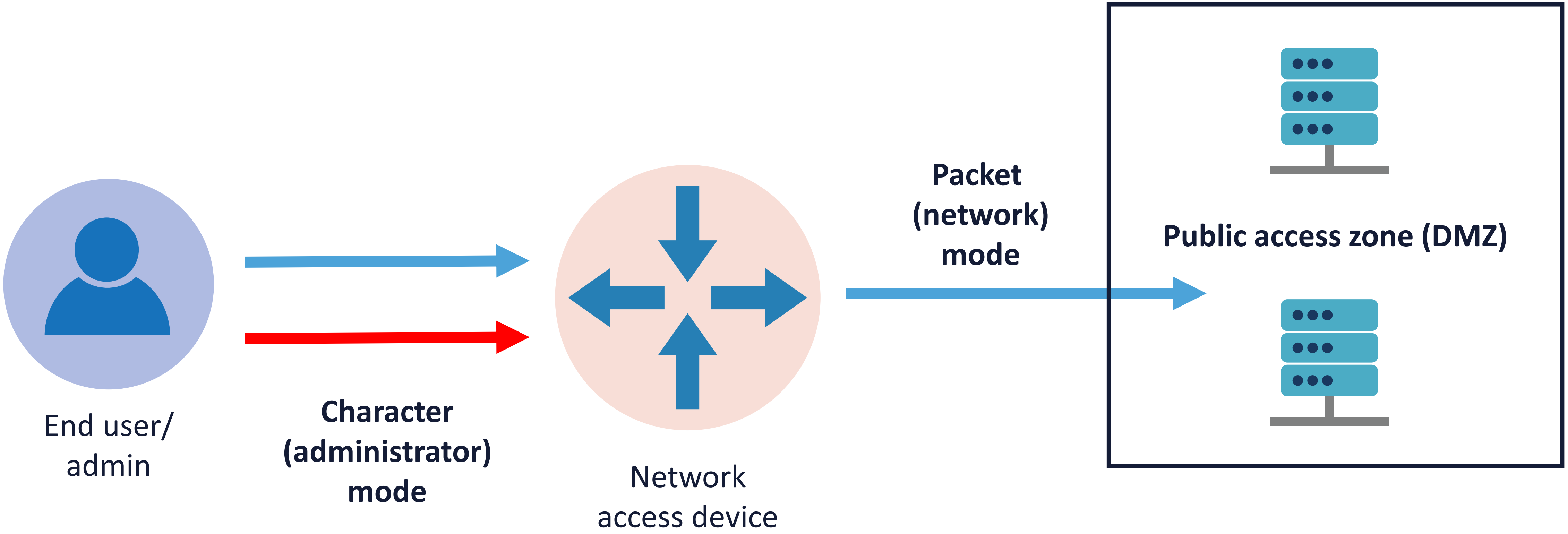
- **Authentication** – the process of validating that an entity (user, application, or system) is who or what they claim to be
- **Authorization** – the process of granting an authenticated entity permission to access a resource or perform a specific function
- **Accounting** – basically, when did the entity begin, when did it end, and how long did they do it?

CHARACTER MODE VS. PACKET MODE

Character mode sends keystrokes and commands (characters) to a network admission device for the purpose of configuration or administration on THAT same device

Packet (or network) mode occurs when the network admission device serves as an authentication proxy on behalf of services in other networks such as the web, File Transfer Protocol (FTP), domain name system (DNS), etc.

CHARACTER VS. PACKET MODE



End user/ admin

Character (administrator) mode

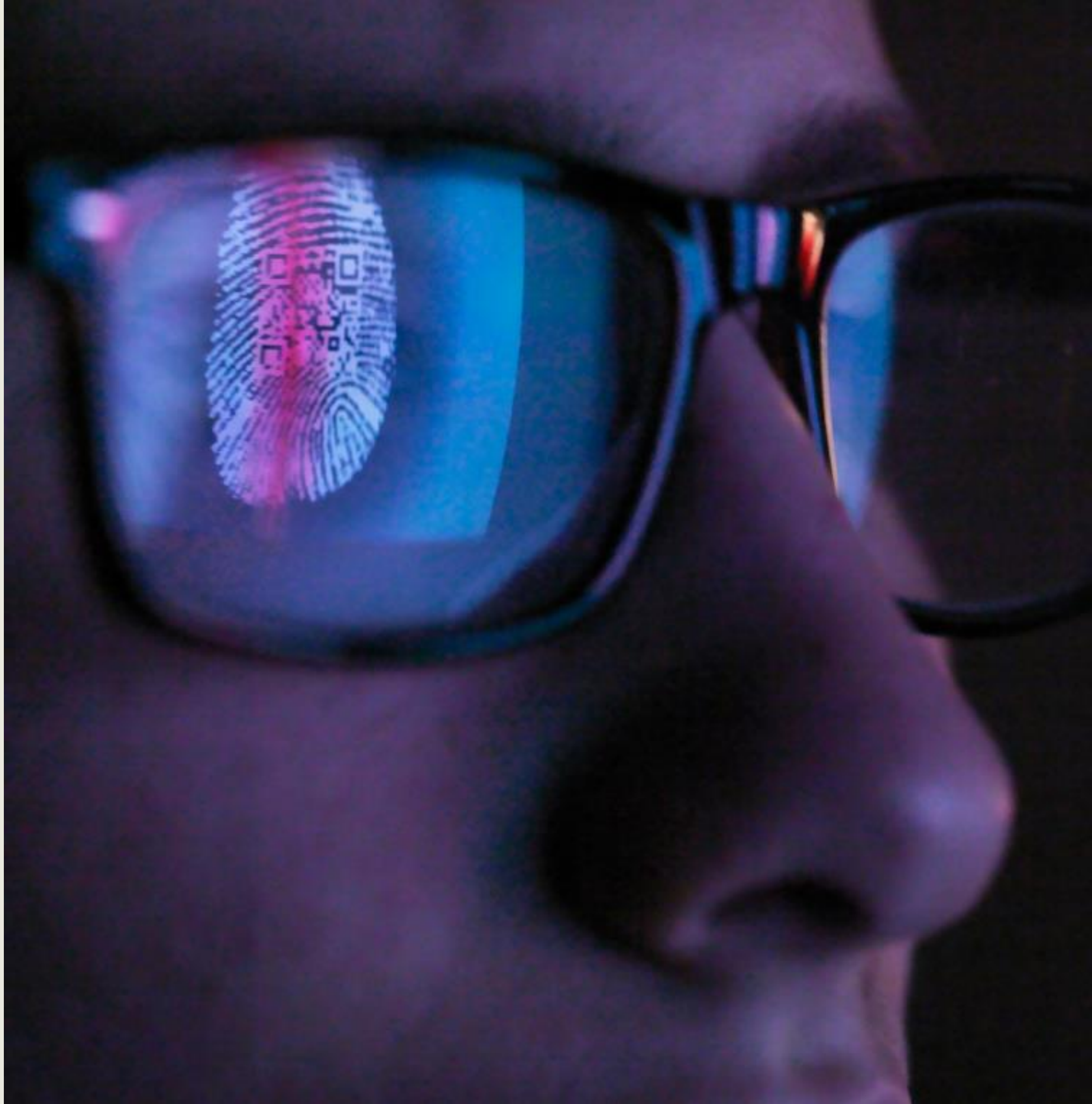
Network access device

Packet (network) mode

Public access zone (DMZ)

AUTHENTICATION

- Authenticating subjects is technically mandatory, even if using open or anonymous techniques
- Historically, clients would initiate a Transmission Control Protocol (TCP) three-way communication handshake before the authentication process
- This is now considered sub-optimal and a violation of "zero trust" principles



AUTHORIZATION

- Authorization is technically optional for authenticated entities and is mandatory from a practical policy standpoint
- In modern security deployments, it is desirable to implement session-based (tokens) and attribute-based authorization mechanisms

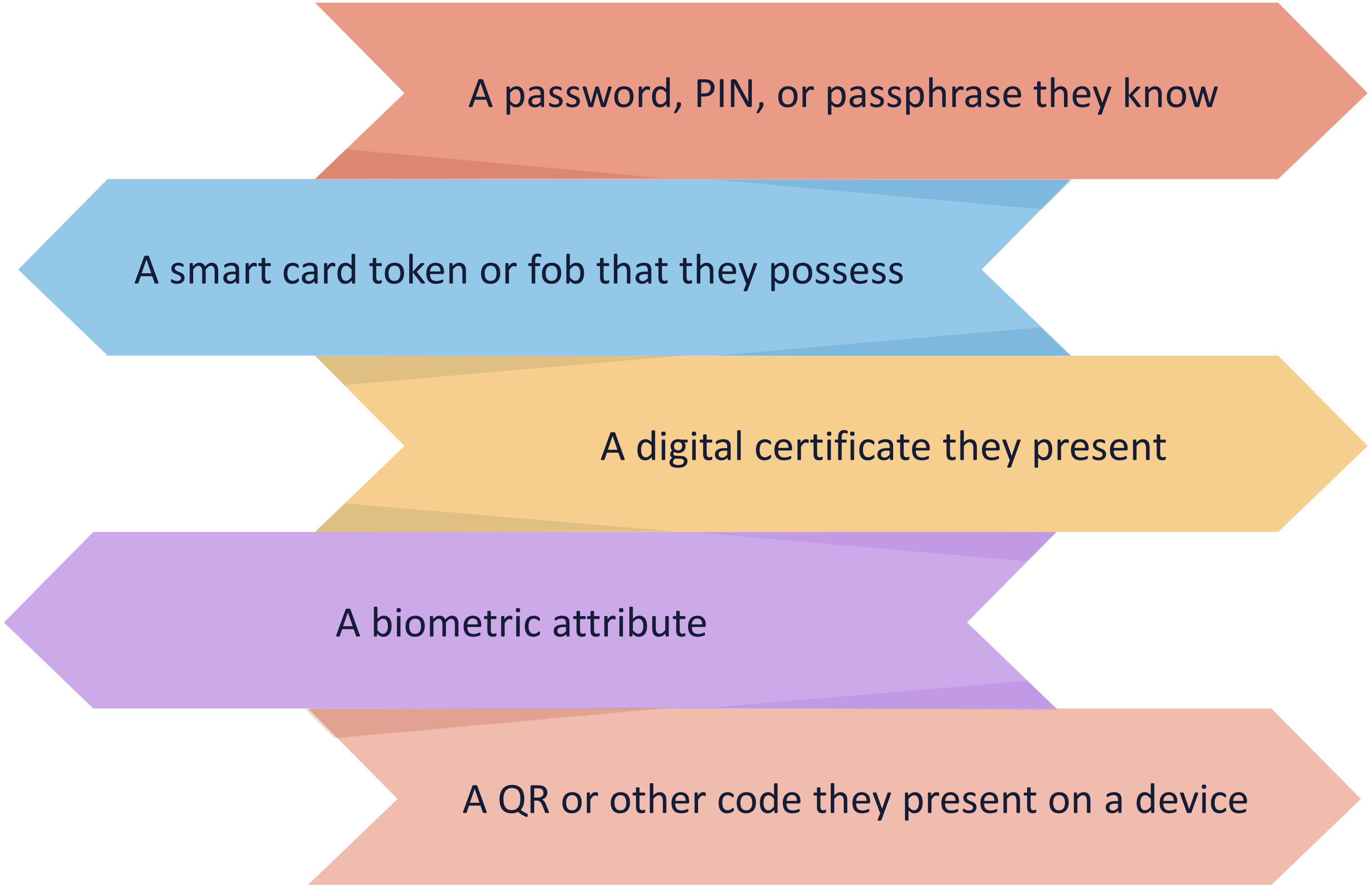
ACCOUNTING

- Accounting is generally implemented for two use cases:
  - Monitoring, visibility, and reporting
  - Billing, chargeback, and reporting
- Remote Authentication Dial-in User Service (RADIUS) is one of the most popular Internet Engineering Task Force (IETF)-based AAA services, and it is known for exceptional accounting capabilities
- Diameter is the next generation of RADIUS

AUTHENTICATING PEOPLE

- Authenticating a person entity means confirming that they are who they claim to be
- This confirms only those with authorized credentials gain access to secure systems
- Usernames/webmail/email and a password is still the most common factor for authenticating people
- There should always be another robust factor added to a simple credential today

COMMON WAYS TO AUTHENTICATE PEOPLE



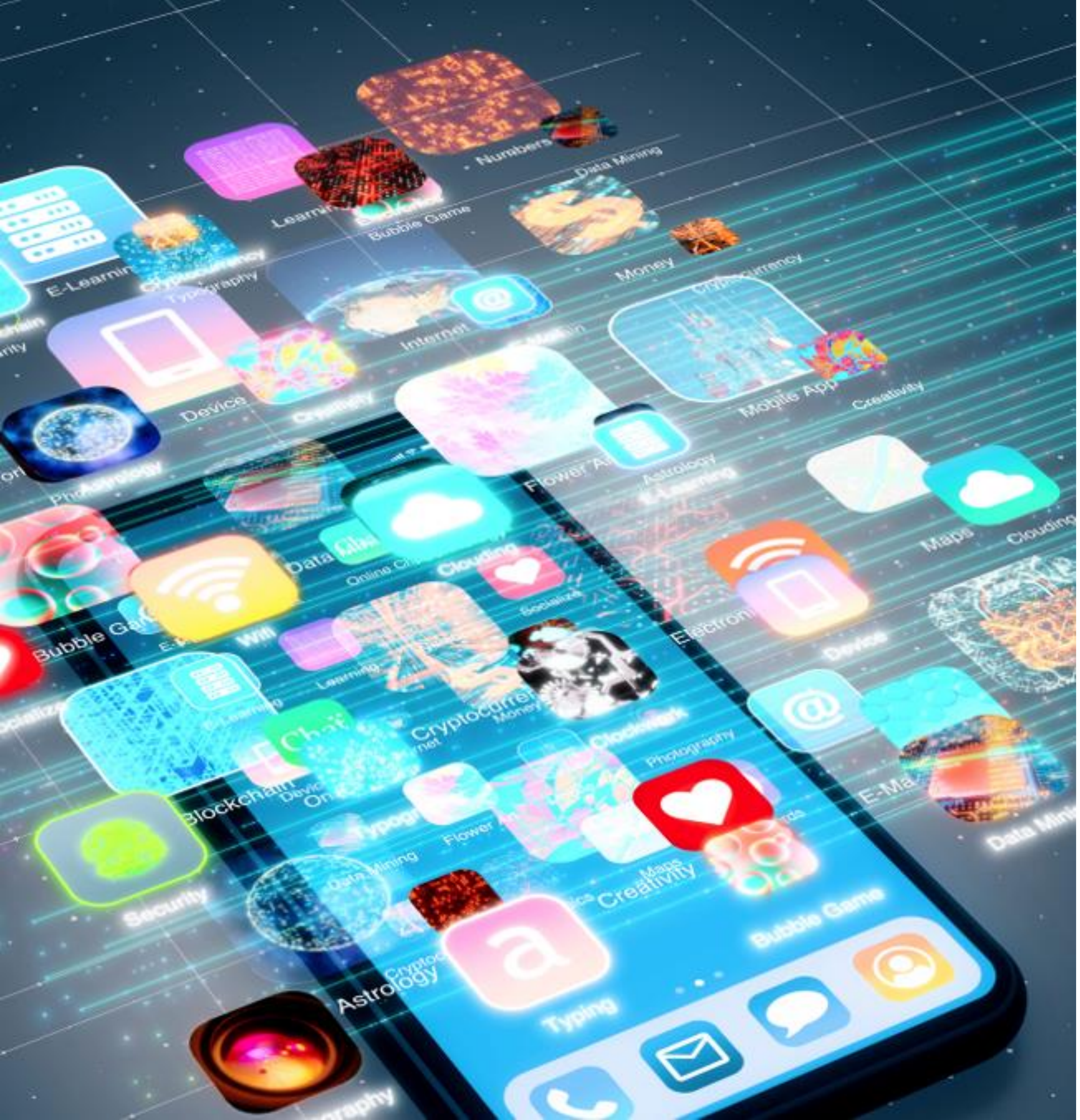
A password, PIN, or passphrase they know

A smart card token or fob that they possess

A digital certificate they present

A biometric attribute

A QR or other code they present on a device



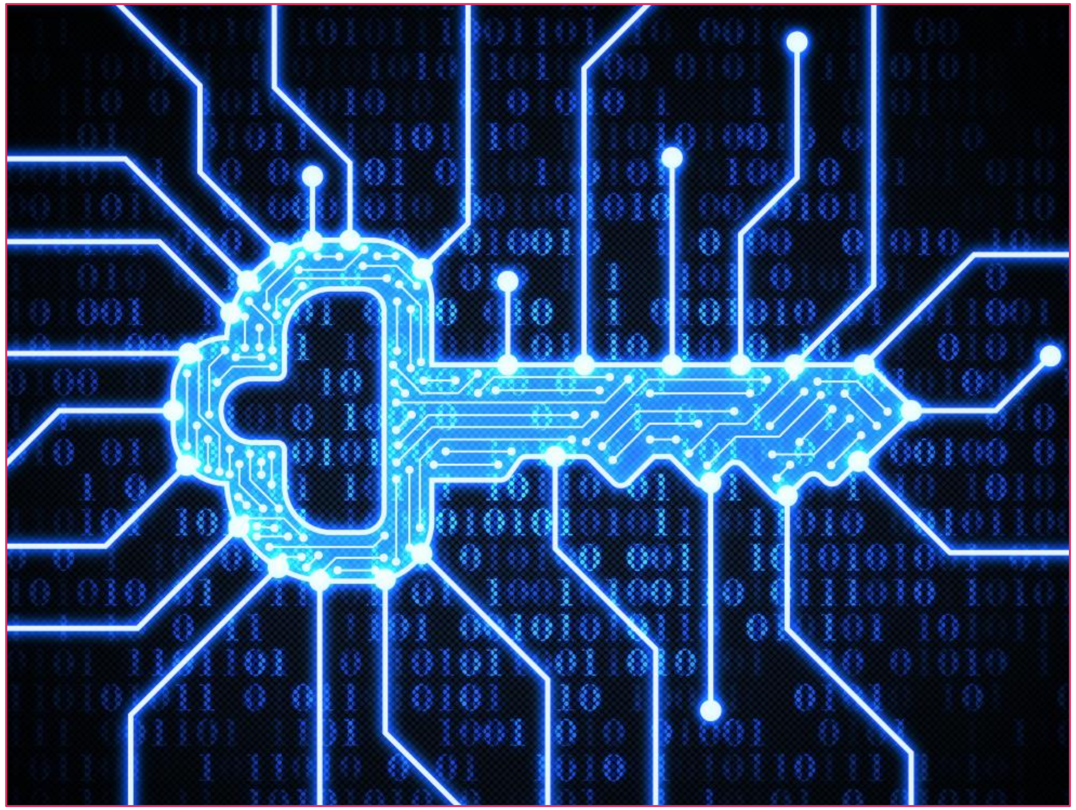
AUTHENTICATING DEVICES AND SYSTEMS

- There are many different types of entities or principals that can be authenticated other than people
- These subjects are often called "non-person entities" (NPEs):
  - Laptops and pads
  - Mobile devices
  - Gateways and load balancers
  - Robotics systems
  - Embedded devices
  - Internet of Things (IoT) endpoints

ENDPOINT AUTHENTICATION

- Endpoint (or device) authentication is a security technique designed to ensure that only authorized devices can connect to a given network, site, or service
- Endpoint security management is rapidly emerging as an important area in machine-to-machine (M2M) communications and IoT
- **Endpoint fingerprinting** is one way to enable authentication of non-traditional network endpoints such as smart card readers, HVAC systems, medical equipment, and IP-enabled door locks

COMMON DEVICE (ENDPOINT) AUTHENTICATION METHODS



- A shared secret key stored on endpoints (wireless) or infrastructure devices
- An X.509 v3 device certificate stored in a software application
- A cryptographic key, certificate, or other credential stored at the hardware level in a trusted platform module
- A key stored in a hardware security module (HSM)
- A protected access file (PAC) in a Cisco infrastructure

AUTHORIZATION MODELS: DAC

- Discretionary access control (DAC) grants access control decisions to the resource owners and custodians
- Each resource typically has an owner who determines the access permissions and shares
- The owner can grant or revoke access rights for other users or groups
- DAC offers flexibility and allows resource owners to have fine-grained control over access, but it can also result in inconsistent access control decisions
- It is the most prone to "privilege creep"

AUTHORIZATION MODELS: RBAC

- Role-based access control (RBAC) grants access based on predefined roles or job titles
- Users are assigned roles, and access rights are associated with these roles
- Instead of directly assigning permissions to individual users, permissions are assigned to roles, and users inherit the access rights associated with their assigned roles, for example:
  - Various roles in a hospital or medical center
  - Built-in roles in a database management system
- RBAC streamlines access control administration by grouping users with similar job functions and offering a scalable approach to access management

AUTHORIZATION MODELS: MAC

- A mandatory access control (MAC) is a strict mathematical model where access to resources is determined by the system based on predefined security labels and rules
- Principals are assigned security clearances or classification levels (top secret, secret, confidential, etc.)
- Resource objects are labeled with sensitivity levels
- Access is granted or denied by comparing these labels and rules, ensuring strict control and preventing unauthorized access
- This is a "non-discretionary" model

AUTHORIZATION MODELS: ABAC

- Attribute-based access control (ABAC) grants access based on a combination of characteristics associated with users, resources, and environmental conditions
- Attributes can include user attributes (job title, department), resource attributes (sensitivity level, classification), and environmental attributes (time of access, location)
- Authorization policies are defined using these combinations, and decisions are made based on evaluating the attributes against the defined policies

AUTHORIZATION MODELS: ABDAC

- Attribute-based dynamic access control (ABDAC) combines the principles of attribute-based access control (ABAC) with dynamic access control (DAC)
- It considers dynamic factors such as risk assessment, user attributes, resource attributes, and contextual information to make access control decisions in real time
- ABDAC provides more fine-grained and context-aware access control needed in "zero trust" environments when compared to traditional static access control models:
  - May include dynamic machine learning techniques such as user behavioral analytics (UBA) in next-generation environments

AUTHORIZATION MODELS: RULE-BASED

- Rule-based access control (RBAC) uses rules to determine access
- Access control rules define conditions or criteria that must be met for access to be granted
- These rules can be based on several factors, such as user attributes, resource attributes, time of access, and more
- **Access decisions are made by comparing these rules against the context of the access request – usually IP transport and network layer header metadata**

RULE-BASED ACCESS CONTROL LISTS

Protocol	Port	Source	Destination	Name	Action
UDP	53	Any	192.16.10.200	Allow DNS queries	Allow
TCP	80,443	Any	192.168.10.201	Allow HTTP and HTTPS	Allow
TCP	3,389	IT_Admin_IP_Range	Any	Allow RDP	Allow
Any	Any	Any	Any	Default	Deny

SECURITY CONTROL CATEGORIES

Technical

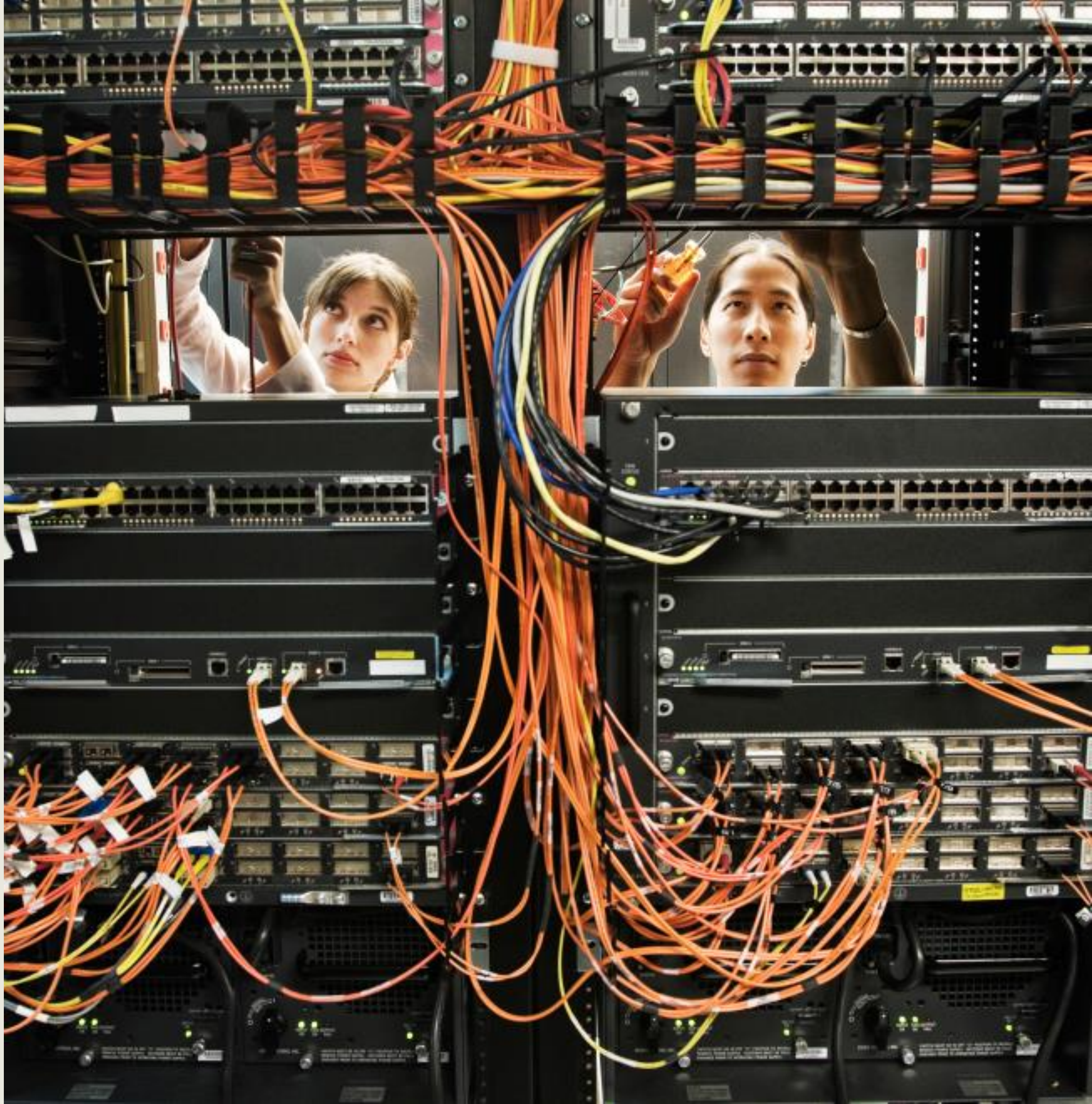
Managerial

Operational

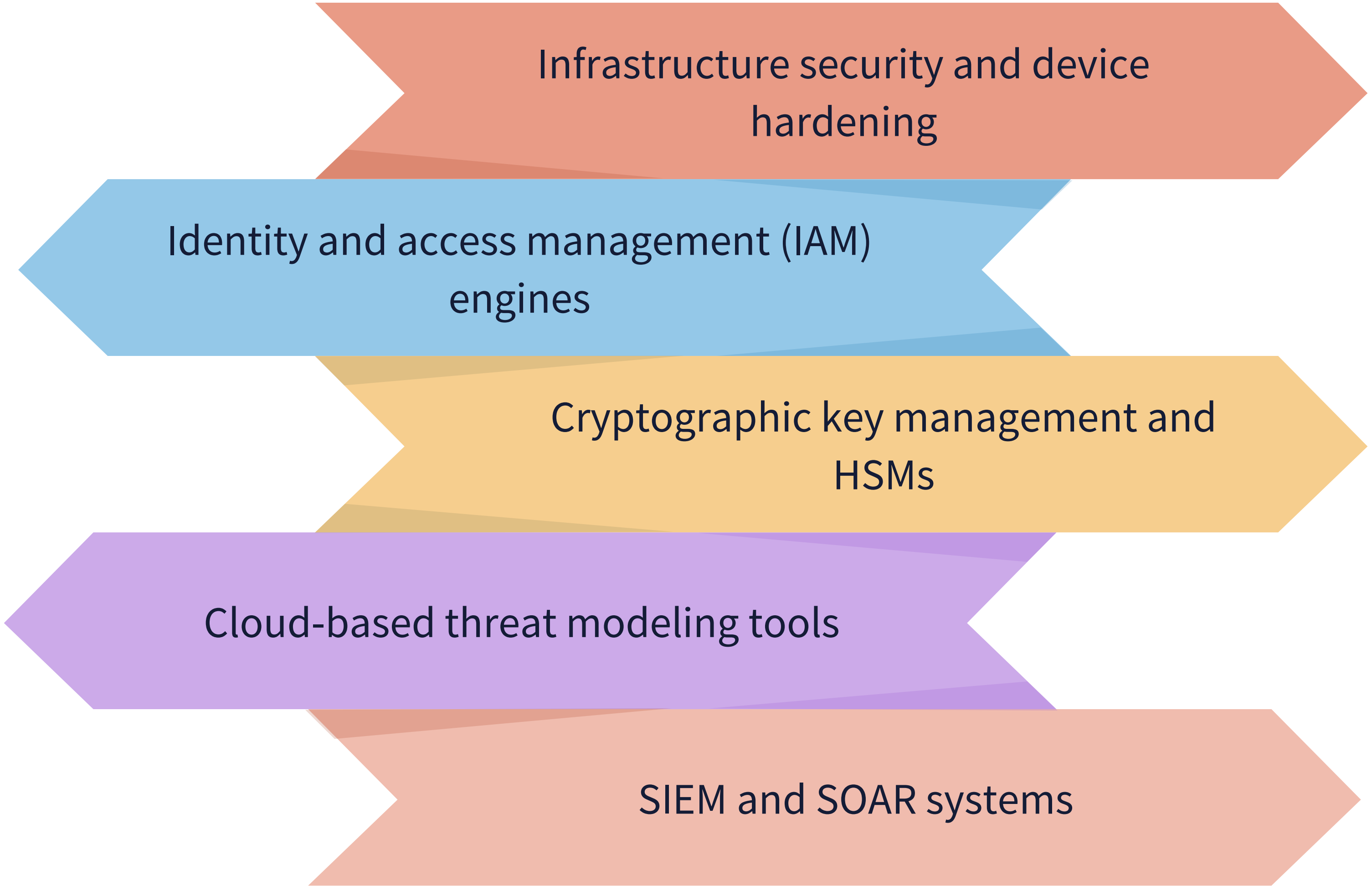
Physical

TECHNICAL CONTROLS

- Are security mechanisms that the specific systems run – either manually or, more often, automated and orchestrated
- Deliver confidentiality, integrity, authenticity, and availability protections
- Defend against unauthorized access or misuse
- Facilitate the detection of security violations and support security requirements for applications and data



COMMON TECHNICAL CONTROLS



Infrastructure security and device hardening

Identity and access management (IAM) engines

Cryptographic key management and HSMs

Cloud-based threat modeling tools

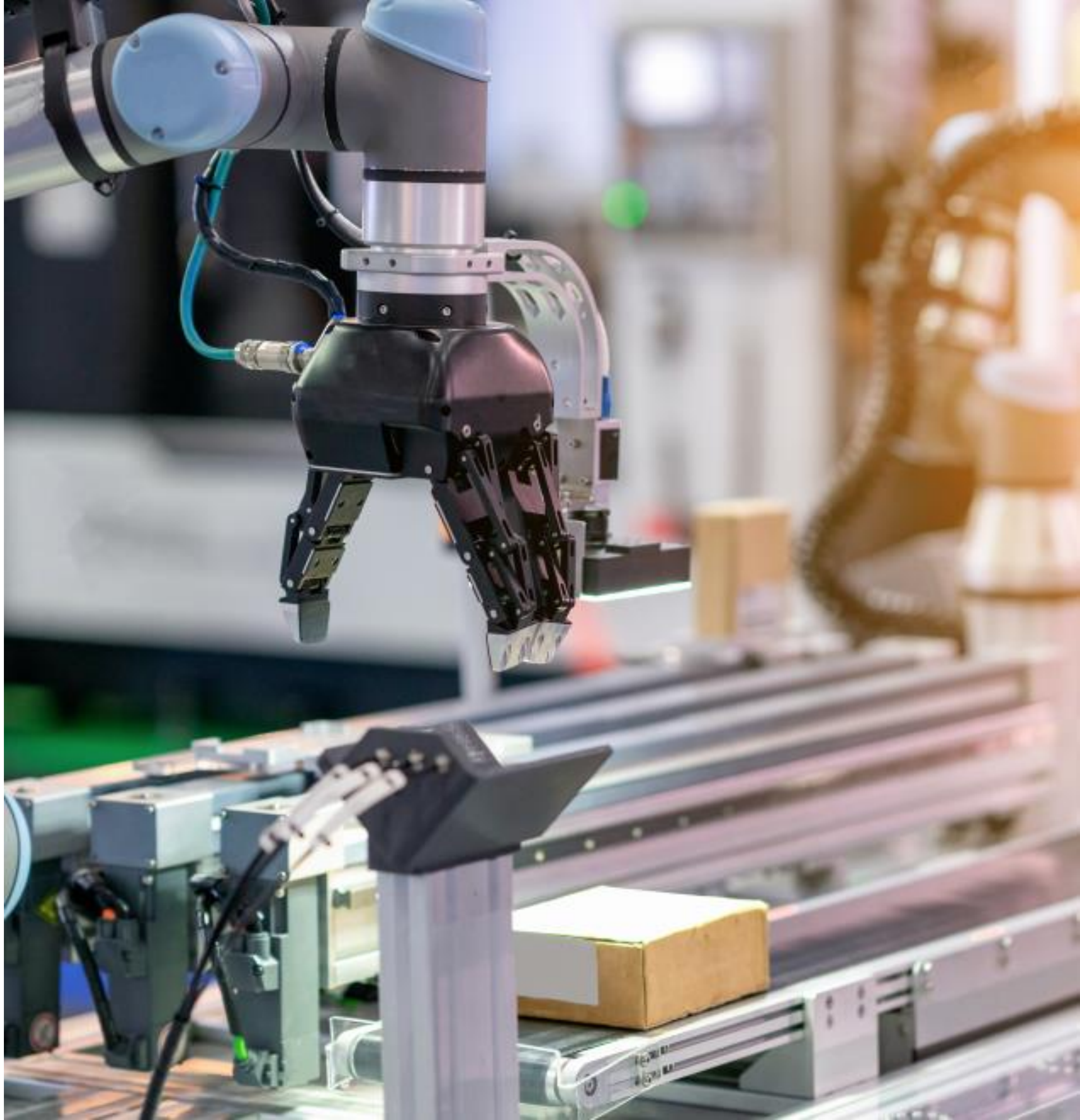
SIEM and SOAR systems

MANAGERIAL CONTROLS

- Managerial (also administrative) controls define policies, procedures, best practices, and guidelines
- They are usually more logical in nature
- Should be a published or printed definition of policies:
    - No piggybacking (tailgating)
    - Acceptable use policies
    - Best practices and guidelines
    - Password policies
    - Screening, hiring, and termination procedures
    - Mandatory vacations
    - Training and awareness

OPERATIONAL CONTROLS

- Operational controls support ongoing maintenance, due care, and continual improvement:
  - Optimizing the change and configuration management database
  - Performing tested patch management
  - Conducting awareness and training
  - Monitoring physical and environmental controls
  - Conducting incident response and disaster planning testing and drills
  - Performing software assurance initiatives
  - Managing mobile devices and mobile applications on an ongoing basis



PHYSICAL CONTROLS

- Physical controls are introduced to protect the campus, facility, environment, and people:
  - Various physical barriers
  - Guards and security teams
  - Cameras and surveillance equipment
  - Different types of sensors and alarms
  - Locking mechanisms
  - Secure safes, cabinets, cages, and areas
  - Mantraps and Faraday cages
  - Fire detection and suppression systems
  - Environmental controls

SECURITY CONTROL TYPES

Preventive

Deterrent

Detective

Corrective

Compensating

Directive

SECURITY CONTROL TYPES

Preventative

Stops an attacker from successfully conducting an exploit or advanced persistent threat

Deterrent

Discourages an attacker from initiating or continuing an attack

Detective

Identifies an attack that is occurring as well as the steps of the kill chain

SECURITY CONTROL TYPES

Corrective

Restores a system to state before the negative event occurred; can simply rectify or correct an identified problem

Compensating

Aids controls that are already in place or provides a temporary stopgap solution

Directive

Consists of mandatory policies and regulations that are in place to maintain consistency and compliance