FUNDAMENTAL SECURITY CONCEPTS

Objectives

- Learn about gap analysis
- Define zero trust initiatives
- Explore deception technologies
- Examine preventative and detective physical controls
- Look at change management business and technical processes
- Describe documentation and version control

GAP ANALYSIS

- To know where you are and where you need to go as a secure organization, you must conduct gap analysis
- This technique will be applied to several security projects, plans, and initiatives throughout an entire career
- Information security gap analysis is a comprehensive appraisal that helps organizations determine the difference between the current state of their information security to specific industry requirements guidance and best practices

GAP ANALYSIS

- When performing a security gap analysis, one will better understand the status of the cybersecurity risks and vulnerabilities in the organization
- This type of risk assessment indicates where the technical, physical, managerial, and continuing operation controls need to be deployed
- It involves knowing what the residual risks are and what further physical and logical safeguards (if any) need to be acquired and implemented

COMMON SECURITY GAPS

- Weak and/or shared credentials
- Lack of tested patch management
- Violation of the least privilege principle
- Having no/unenforced acceptable use policies
- Poor physical security
- Configuration and deployment errors due to lack of change and configuration management
- Poor visibility and lack of proper auditing

ZERO TRUST

- Zero trust (ZT) is the term for an evolving set of cybersecurity initiatives that move defenses from static, network-based perimeters to focus on users, assets, and resources
- ZT assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership

ZERO TRUST

- Authentication and authorization (both subject and object) are discrete functions performed before a session to an enterprise resource is established (TCP/TLS)
- ZT embraces the principle of least privilege consistently across all resource classes and locations
- Segregation (separation) of duties and high visibility (SIEM/SOAR) are also emphasized

ZERO TRUST ADAPTIVE IDENTITY

- Adaptive identity is another key ZT component
  - It is also called adaptive authentication or risk-based authentication
- It is a method of access to data that matches user credentials with the risk of the requested authorization
- It delivers support for multiple classes of consumers and participants, whose roles and identity may evolve to meet rapidly evolving ecosystems and environments
- Offers ease of maintenance and operation while being agile and easy to modify

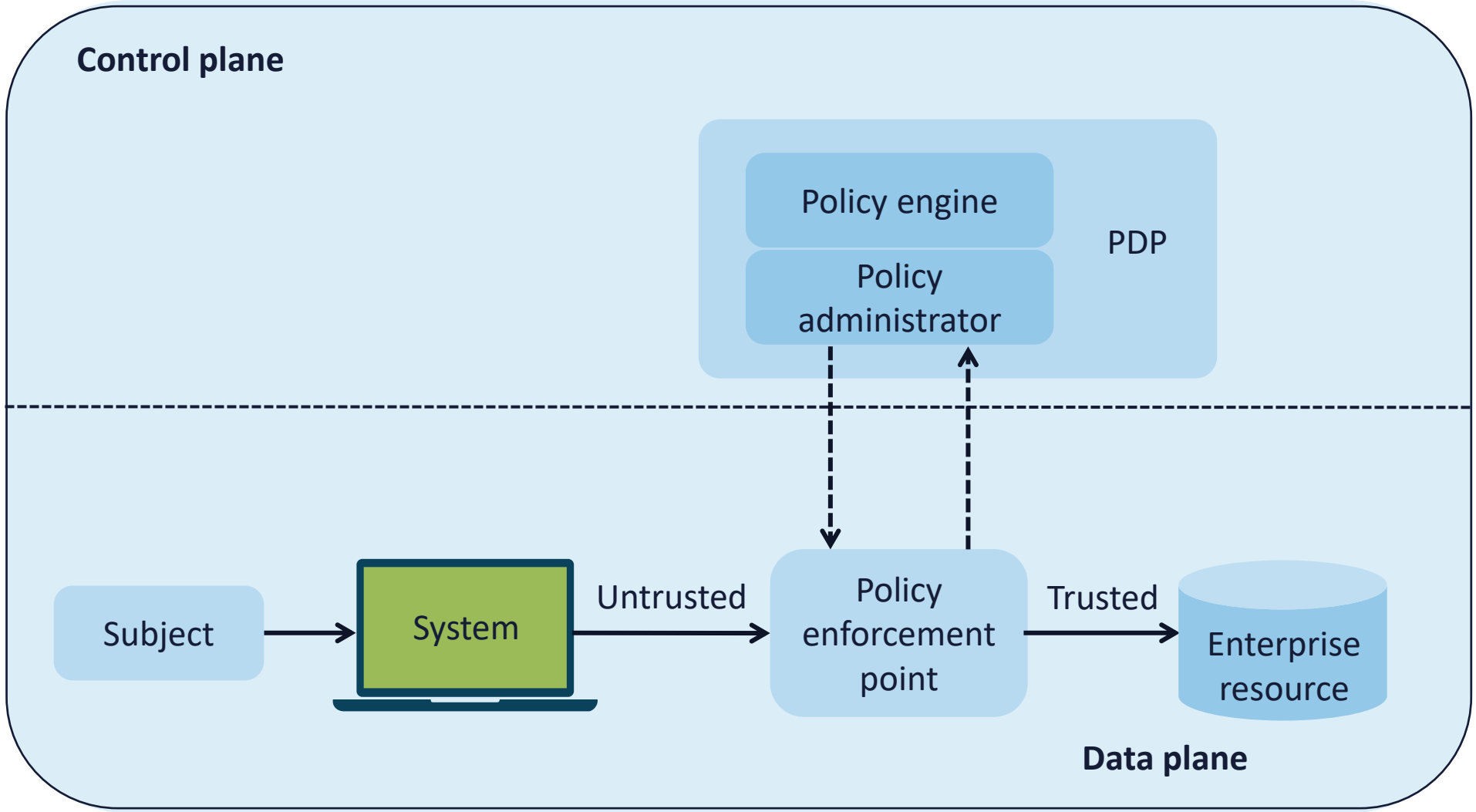
ZERO TRUST THREAT SCOPE REDUCTION

- Another main goal of ZT is threat scope reduction and risk avoidance
  - Reduced scope of threats to support agility and support complexity
  - Increased complexity and number of communication patterns, increasing difficulty of addressing through a data and asset-centric approach

ZERO TRUST CONTROL PLANE

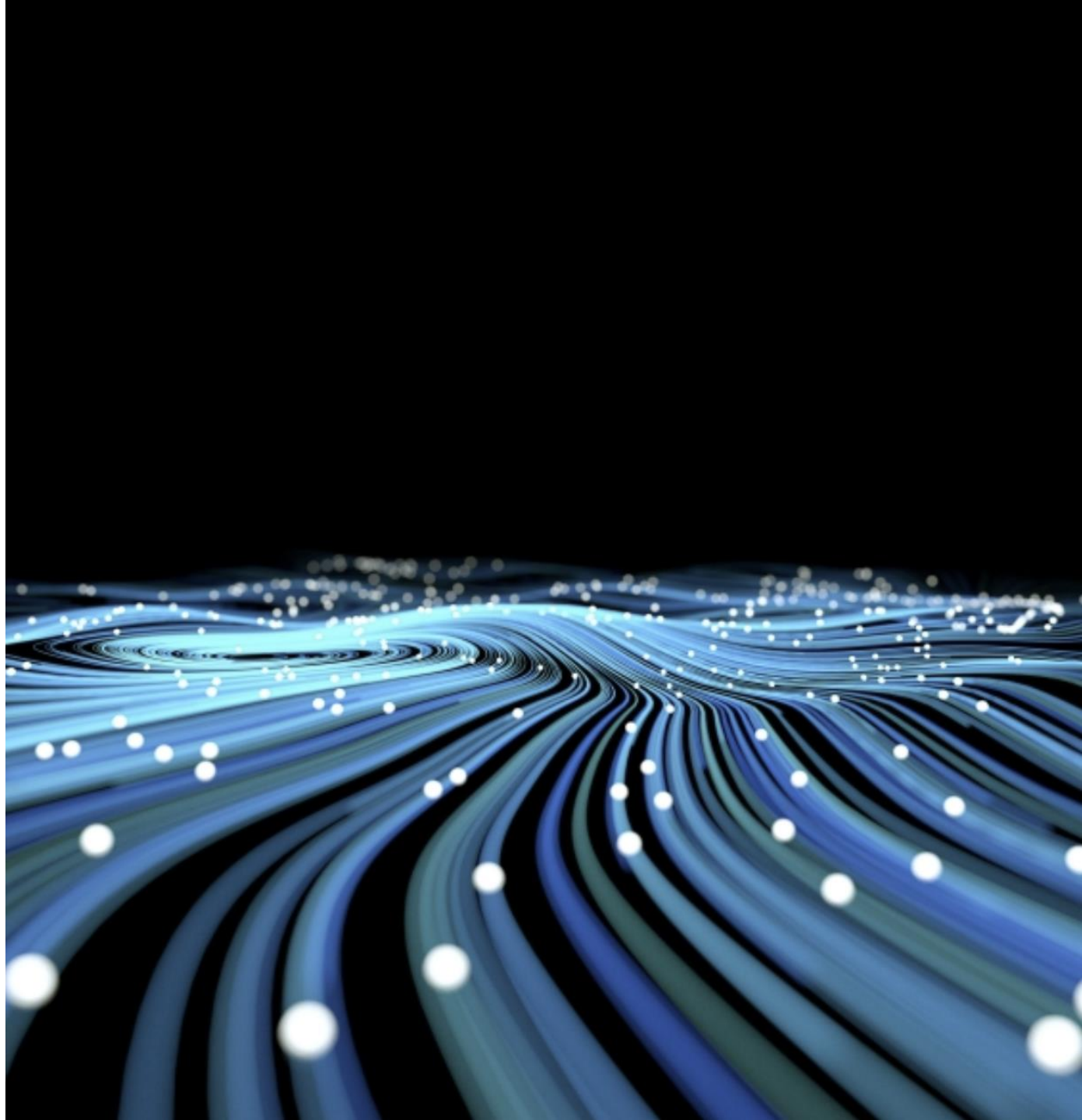
- The ZT control plane is separate from the data plane and contains the **policy decision point (PDP)**, which includes:
  - The **policy engine (PE)**, which uses the enterprise policy-driven access control (as well as input from external sources) to grant, deny, or revoke access to resources
  - The **policy administrator (PA)**, which enables and/or shuts down the communication path between a subject and a resource via commands to associated **policy enforcement points (PEPs)**
  - The PA communicates with the PEP when creating the communication path via the control plane

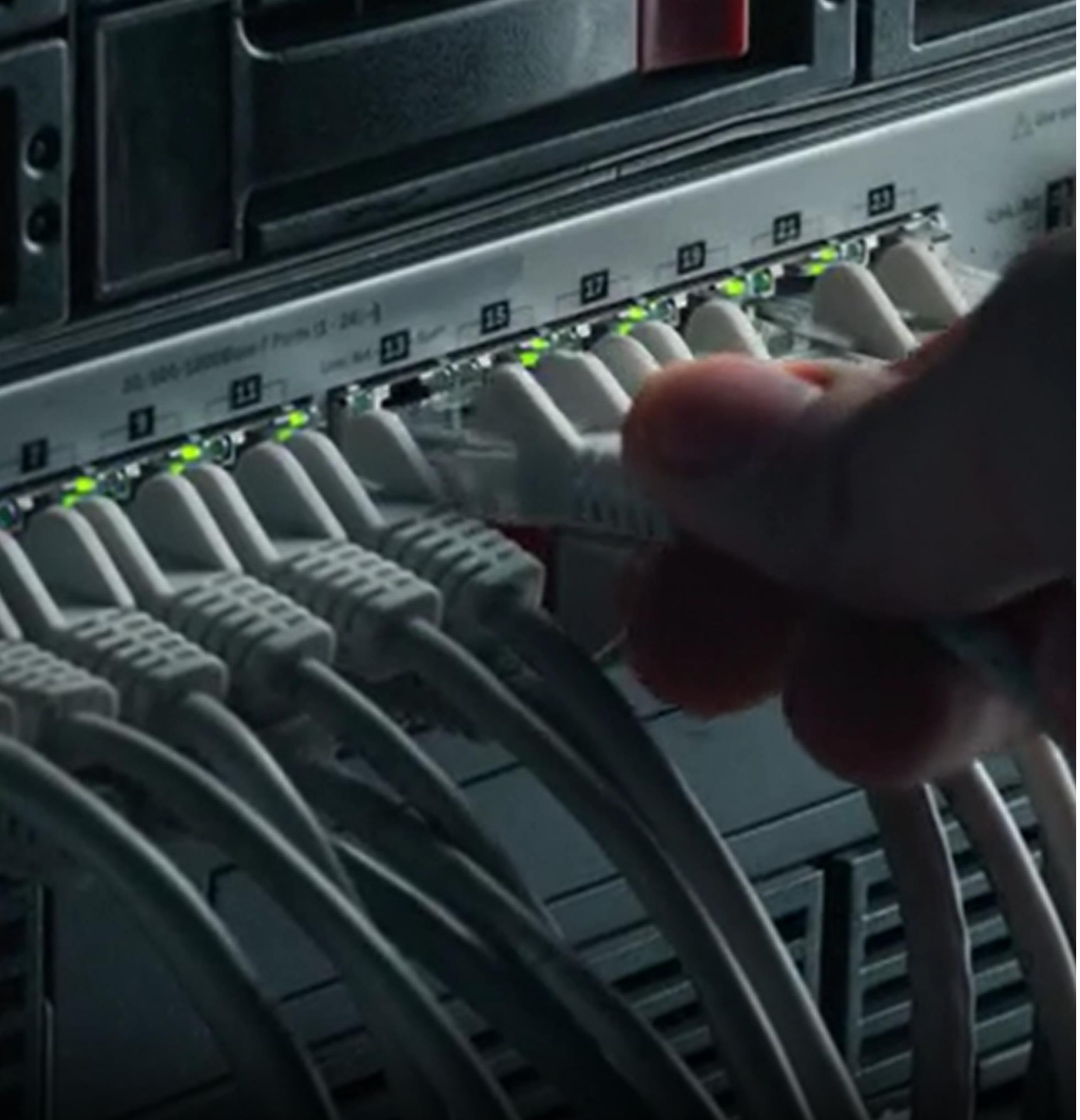
ZT ARCHITECTURE



ZERO TRUST DATA PLANE

- The zero trust data plane is defined by explicit trust zones, which could include
  - Data centers
  - DMZs (public access zones)
  - The public Internet
  - Cloud computing subnets such as private or VPN-only
  - Honeynets

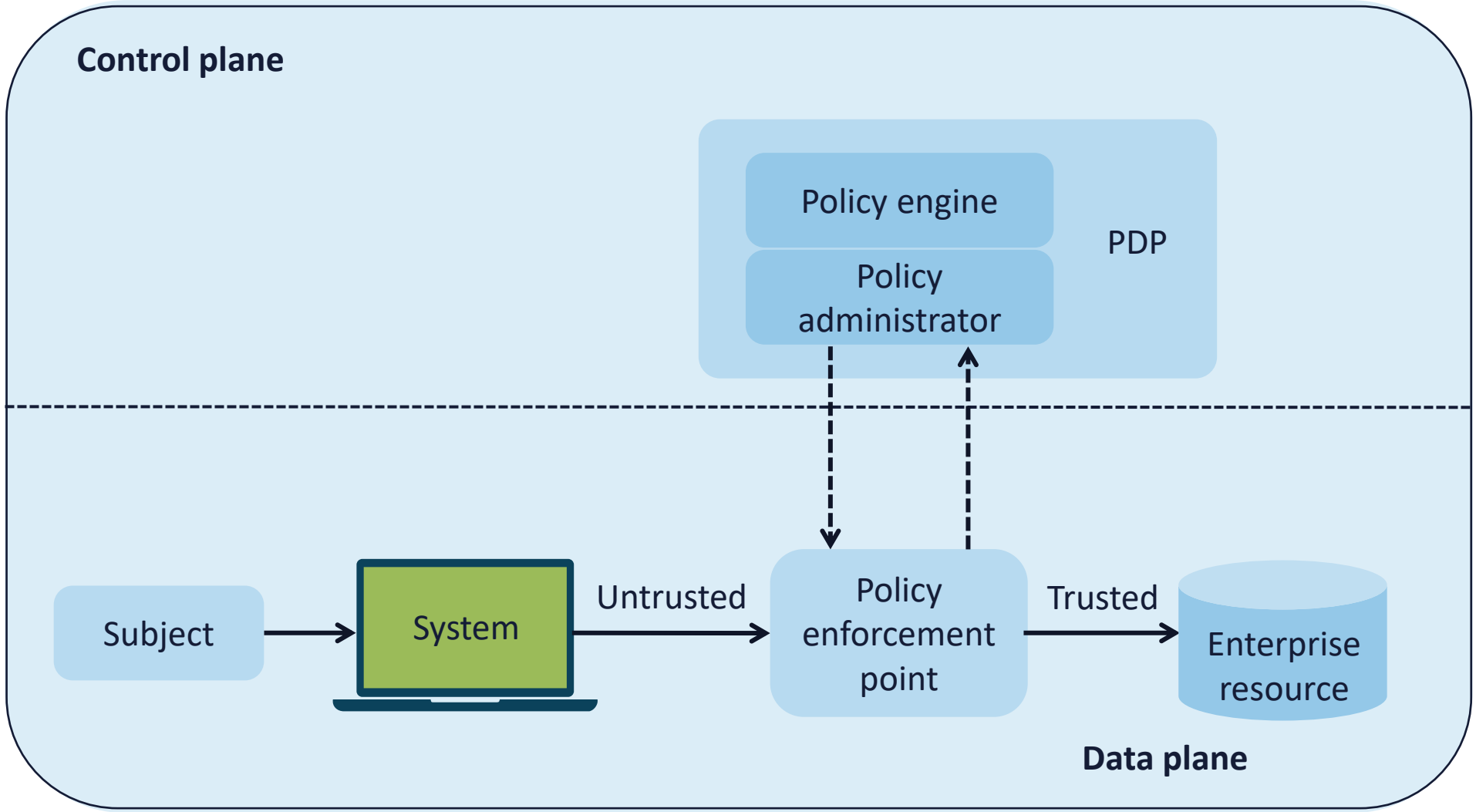




POLICY ENFORCEMENT POINTS (PEP)

- Network PEPs:
  - Edge routers
  - Edge firewall appliances
  - SDP access gateways
  - Network L2/ML switches
  - Authentication proxy servers
- Application PEPs:
  - API gateways
  - Resource groups
  - Network VLANs
  - Code repositories
  - Cloud services

ZT ARCHITECTURE



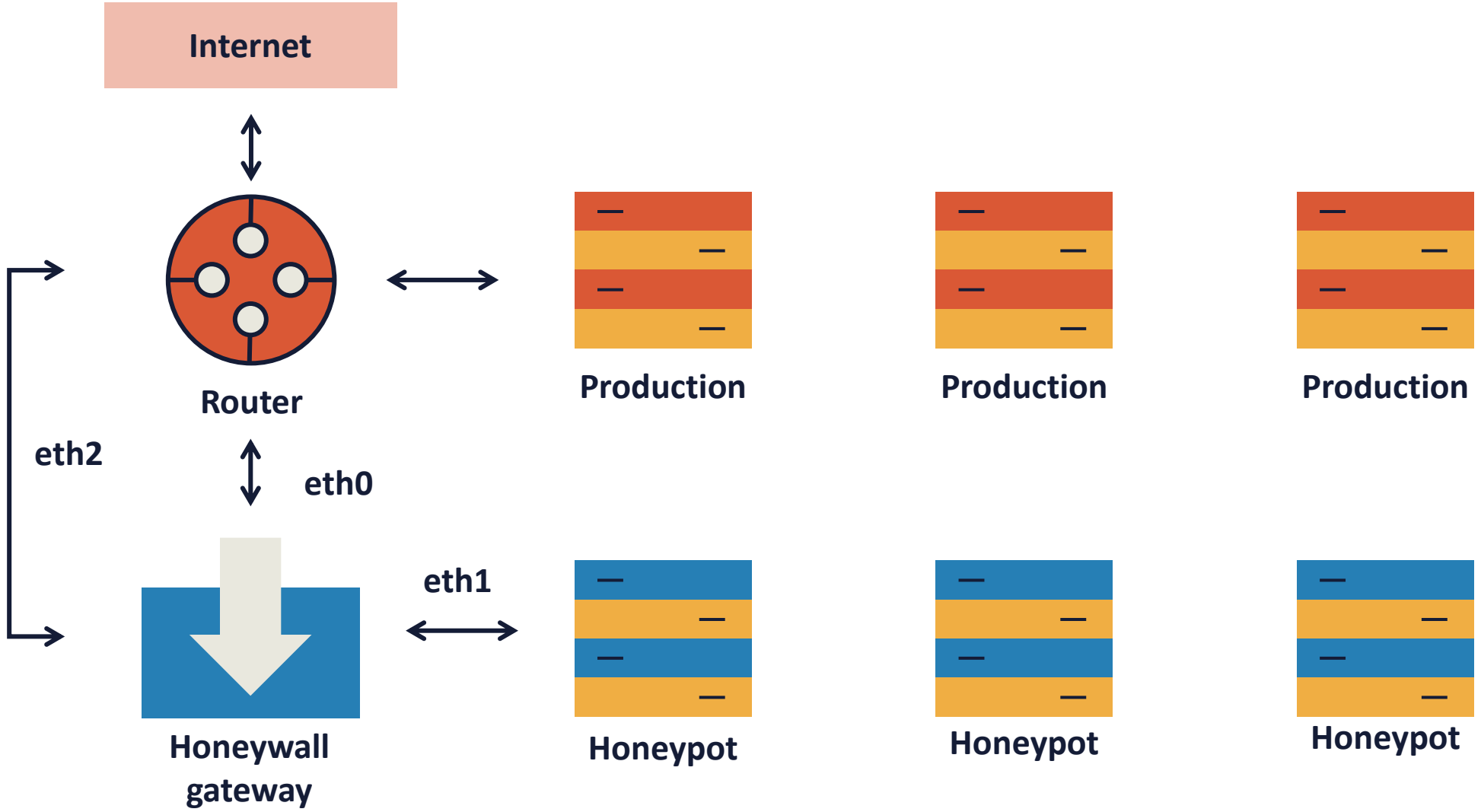
DECEPTION TECHNOLOGIES: HONEYPOT

- A honeypot is a system (e.g., a web server) or resource (e.g., a file on a server) that is designed to be attractive to potential attackers and intruders, like honey is eye-catching to bears
- Modern systems are often running as a virtual machine in a type 1 hypervisor such as a VMware solution
- They are strategically placed in parallel to public access or demilitarized zones where public-facing servers are typically placed

HONEYNETS

- A honeynet can simply be considered a "network of honeypots"
- It is also set up with intentional vulnerabilities hosted on decoy servers and services to attract or redirect attackers
- The primary purpose is to test network security by inviting attack patterns and "kill chains"
  - This helps security teams analyze an actual attacker's activities and methods to improve network security

HONEYNETS


Internet
Router
eth2
eth0
eth1
Honeywall gateway
Production
Production
Production
Honeypot
Honeypot
Honeypot

HONEY FILES AND HONEY TOKENS

- The compromised privileged insider is the number one internal structured threat for most organizations
- Honey files and tokens are strategically placed artifacts and files meant to allure the suspect into exposing themselves as part of an internal investigation
- They are also valuable in the discovery of attackers who are deep into the kill chain phases
- Common examples are access keys and credentials to valuable cloud-based assets and database entry points

PREVENTATIVE PHYSICAL SECURITY CONTROLS

- Before security professionals can focus on technical and operational countermeasures, they must be certain that these are deployed in a physically secured property, facility, and environment
- Although detective and deterrent controls are important, prevention is critical for protecting all types of assets

FENCE BARRIERS

- Most organizations will have protective fence barriers around the perimeter to deter or prevent individuals from unauthorized entry and exit
- Fences may only be used in certain zones or areas to protect junction boxes, generators, dumpsters, and shredding service pickup points
- Fences can be of varying heights and barbed depending on the locale
- Electrified fences and signage are also common for high security properties and facilities (e.g., airports, prisons, military installations)

GATES

- Fences are often combined with entry/exit gates of varying strength and guarding
- Barricade gates and tire shredders are common
- Types of gates in the U.S. include
  - Class I: Residential gate operation
  - Class II: Commercial, such as a parking lot or garage
  - Class III: Industrial/limited access (e.g., warehouses, factories, docks)
  - Class IV: Restricted access operation requiring supervisory control

BOLLARDS

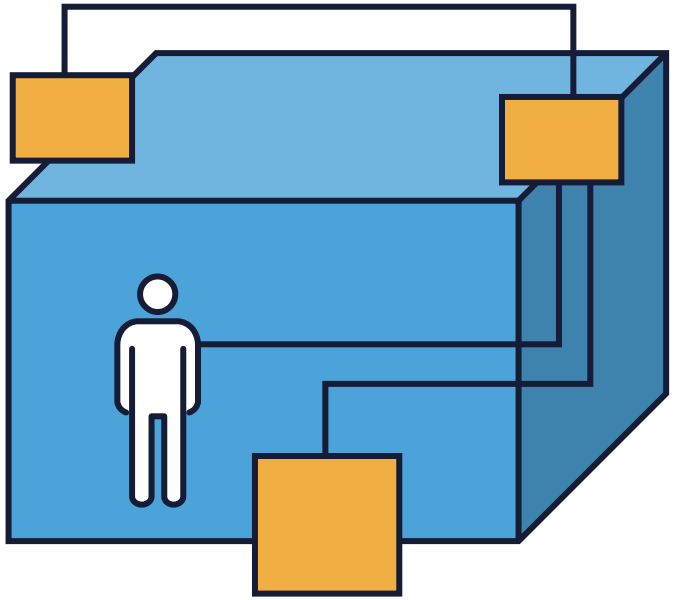
- Bollards are strategically placed pylons meant to redirect pedestrian traffic or prohibit vehicles from entering certain areas, such as the foyer of an office building
- They can be permanent or temporary pillars
- They are typically made of concrete or strong metal
- High-tech bollards can be mechanical and include cameras and sensors

ACCESS CONTROL VESTIBULES

- Access control vestibules are typically areas that are fortified with forced entry-resistant and bullet-resistant security glazing
- These fortified entryways serve as formidable barriers to unauthorized access that go beyond traditional security measures
- Access control vestibules are also known as security or mantrap vestibules and are a highly effective means of hardening commercial security, typically through a series of interlocking doors

MANTRAPS

- There is an entry and exit door but only one door can be open at a time
- One person at a time – no piggybacking (tailgating):
  - Person can be identified and authenticated
  - Provide credentials and license or passport
  - Can include biometric readers
  - CCTV and intercom systems are often used
  - Security guard behind bullet-proof glass
  - Person is eventually allowed in through a strong door with electronic locks

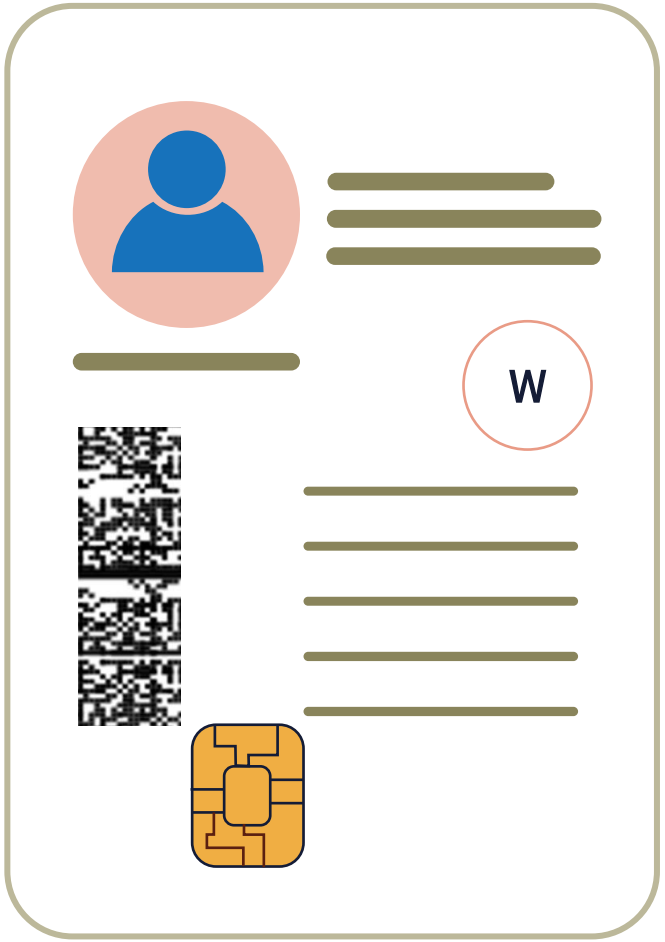


ACCESS BADGES AND CARDS

- Access badges and cards represent another "something you have" authentication factor
- Many organizations will have all guests register at a reception area security desk:
  - Collect and input identification information in a visitor log
  - Distribute temporary access cards or badges
  - Have a camera station for pictures for a temporary badge
- There should be a "no tailgating (piggybacking)" policy at all access points

COMMON ACCESS CARD (CAC)

- Expiration date
- Federal identifier
- Affiliation
- Service/agency
- Color indicator
- Pay grade
- Rank
- Integrated circuit chip



SECURITY GUARDS

- Security guards are typically 24x7, but could just be present during business or non-business hours
- They are a security control of multiple types:
  - Detective
  - Deterrent
  - Preventative
- They can provide rapid security response if an intrusion or incident occurs
- Robot sentries are rapidly replacing humans in certain scenarios

SECURITY GUARD CONSIDERATIONS

- Are they hired, contracted, or freelance?
- Do they need to be certified/licensed?
- Will they be armed or unarmed?
- What is the impact on insurance policies?
- Is the organization directly involved with screening and background checks?
- Where are they stationed on the campus?
- Who provides the ongoing training?

VIDEO SURVEILLANCE

- Cameras and video surveillance provide a way to monitor and record the property perimeter for intruders and potential attackers
- They are considered detective physical controls, but the mere presence may also be a deterrent
- Video surveillance offers a way to record intruders in action with recordings
- Alerts should be triggered when a camera is disabled

VIDEO SURVEILLANCE CONSIDERATIONS

- The systems will be indoor and outdoor webcams or CCTV systems
- May be closed-circuit to a security operations center (SOC)/linked to a third-party vendor
- It is imperative to transfer media to a safe and secure location
- Industrial camouflage involves cameras and surveillance devices hidden in landscaping elements, statues, and tall trees
- It should be combined with various lighting solutions, both of which can have "dead spots"

LIGHTING

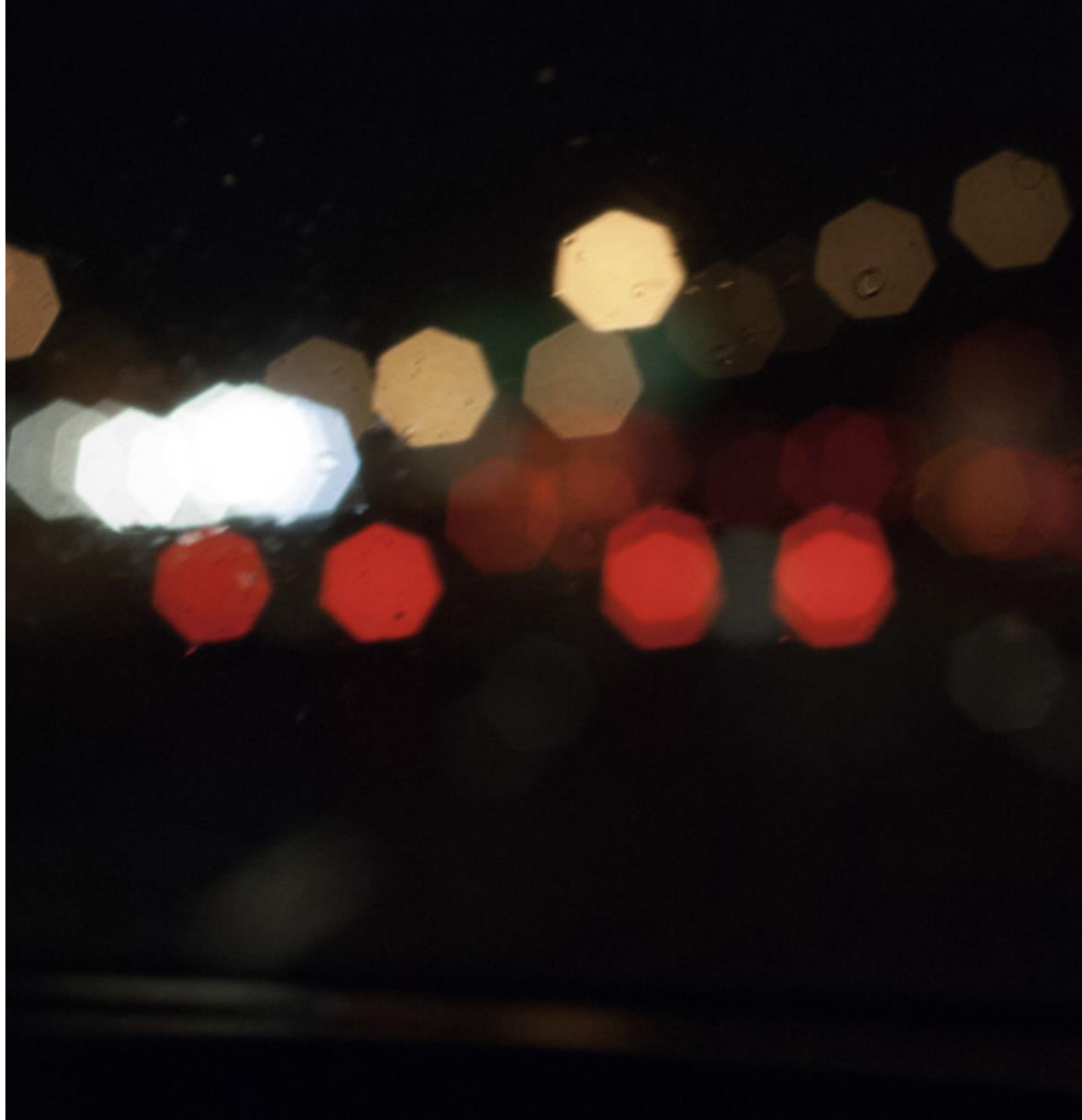
- Lighting can enhance other security controls such as cameras, security guards, and sensors
  - They should start at the perimeter and be used in every defense-in-depth mechanism
- Some modes of lighting can be mercury vapor, sodium vapor, quartz, and LEDs

SECURITY LIGHTING

- **Continuous lighting** is the most familiar form of outdoor security lighting and can provide greater projection and control
  - The glare of continuous (barrier) lighting originated in prisons and correctional institutes and is still in use today
- **Stand-by lighting** systems are designed for reserve or stand-by use or to supplement continuous systems
  - These systems are engaged either automatically or manually when the continuous system is inoperative or when there is a need for extra light

SECURITY LIGHTING

- **Moveable lighting hardware** is manually operated and typically is made up of moveable search or flood lights located in chosen places, which require temporary lighting
  - The moveable system is also used to supplement continuous or stand-by lighting and is often used at construction sites
- **Emergency lights** are used in times of power failure or other emergencies when other systems are inoperative – often gas-powered generators or batteries



TYPES OF SENSORS

- Photoelectric – a break in a light beam
- Passive infrared – detecting infrared light
- Vibration – a change in the level of vibration
- Acoustical – noise detection of a change in sound waves
- Microwave – a change in high-frequency radio waves
- Electro-mechanical – a break in electrical circuit
- Electrostatic – a change in an electrostatic field
- Moisture and temperature detection – for server rooms and data center environmental control

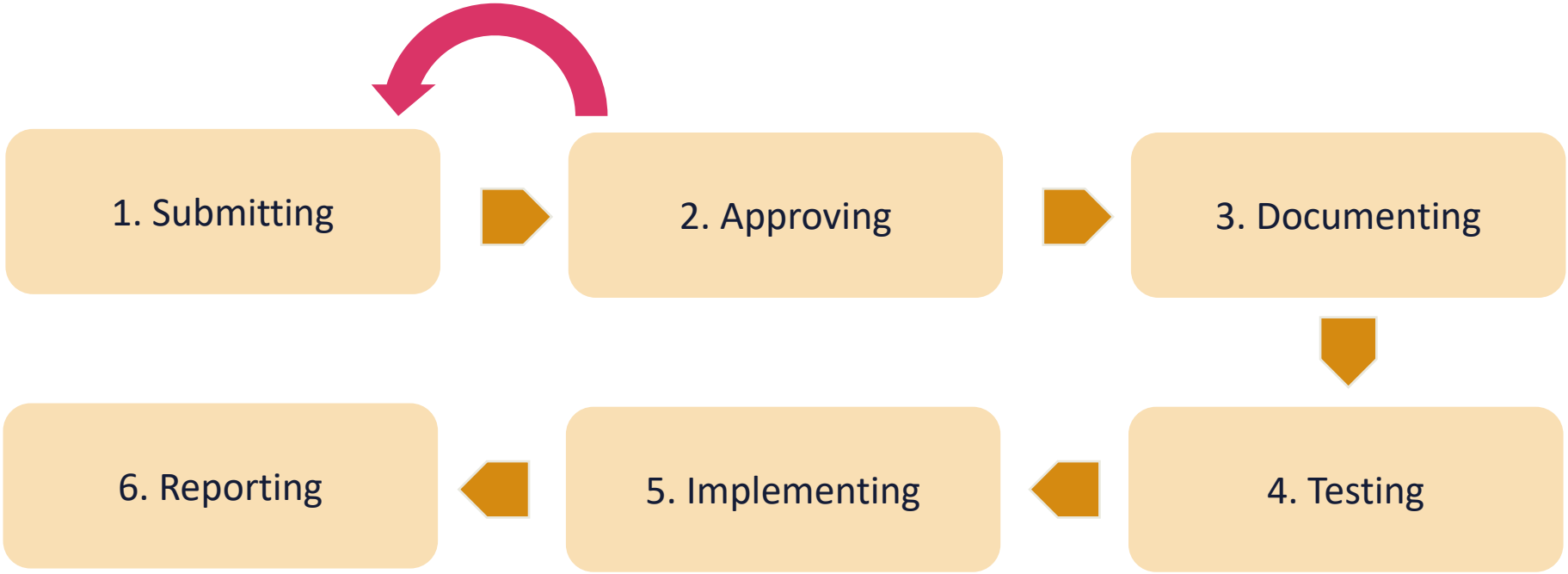
SENSORS TRIGGER ALARMS

- A static or flashing light on the display panel in the security room or operations center
- Bells ringing or horns blaring
- Sending a text notification to an interested party
- Sending an email message
- A silent alarm to a security firm or local law enforcement
- A telephone or cellular call to a software program or live attendant

CHANGE MANAGEMENT

- Change management is the methodical approach to handling the transition or modification of an organization's goals, processes, or technologies
- The purpose is to implement strategies for carrying out change, controlling transformations, and assisting individuals in adapting to change
- Change management is also referred to as the change control practice
- Typically, configuration management occurs first to establish a baseline before standard, normal, and emergency changes occur

CHANGE MANAGEMENT LIFECYCLE



CHANGE CONTROL BUSINESS PROCESSES

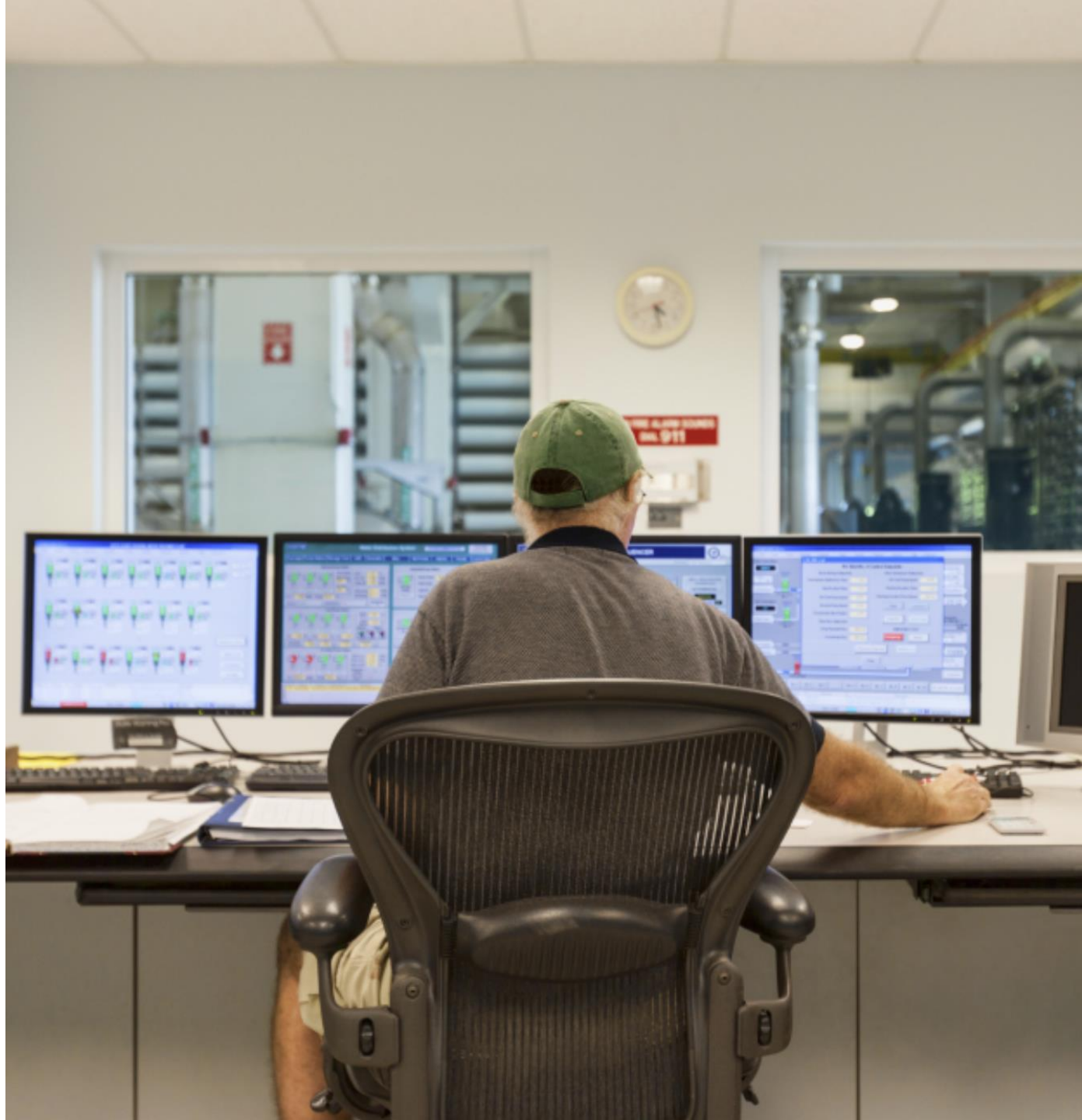
- The **approval** process should be a flexible and highly iterative phase of the lifecycle
- **Ownership** of the physical or logical asset must be considered and is driven by the access control model
- All **stakeholders** should be either involved based on the RACI model
  - Responsible, accountable, consulted, informed

CHANGE CONTROL BUSINESS PROCESSES

- A **change impact analysis** compares two states (the current and future state) of a change to identify what is changing, who is impacted by the change, and what needs to be communicated to the impacted
- The process involves identifying and categorizing who and what will be affected, assessing the degree of change occurring within these areas, and describing the change
  - This last activity folds into stakeholder analysis, communication analysis, and strategies

CHANGE CONTROL BUSINESS PROCESSES

- A change **backout or fallback plan** is a recovery point, and it must be in place during both the testing plan and implementation phase
  - Make small individual changes instead of several impactful changes
- **Maintenance windows** are typically used to show times during which changes should be scheduled
- A **standard operating procedure (SOP)** offers precise directions and detailed instructions needed to perform a specific task or operation consistently and proficiently



CHANGE MANAGEMENT TECHNICAL IMPLICATIONS

- **Allow/deny lists** are used with change control in line with the access control model to dictate which subjects are allowed to make changes or not
  - An allow list is a permissive control
  - A deny list is a restrictive control
- By implementing least privilege and separation of duties, certain activities and areas will be restricted

CHANGE MANAGEMENT TECHNICAL IMPLICATIONS

- **Downtime** relates to high availability, which is an aspect of resiliency
- **Availability** consists of planned and unplanned downtime (e.g., an outage) and must be considered with technical change management when making modifications or performing migrations
- Other considerations are a service restart, application restart, legacy applications, and all dependencies

DOCUMENTATION AND VERSION CONTROL

- Organizations must document using a well-established tagging and labeling schema that maps to a configuration management database (CMDB), such as ServiceNow
- A configuration management system (CMS) is a set of data, tools, utilities, and processes used to support configuration management
  - Relational databases have been used historically
  - NoSQL/document databases are emerging as a common solution
  - You could leverage a CSP service, such as Amazon Redshift data warehousing or DynamoDB

DOCUMENTING WITH A CMDB

- A configuration management database is not a typical data warehouse
- It plays a critical role in several IT management initiatives, like IT service management (ITSM) and IT asset management (ITAM)
- It helps various IT services to better align with business needs by providing current and accurate data for
  - Change and patch management
  - Incident and problem management
  - Availability management
  - Release and deployment management

VERSION CONTROL

- Version control and change management procedures are important to both the operations team and the security team
- Version control applies to
  - Operating system builds
  - Application updates
  - Device drivers
  - Licensing updates
  - Various upgrades and patches
  - Container packages and microservices
  - Firmware updates
  - Trusted platform modules
  - Component updates