Welcome Back to the CISSP Bootcamp

Your instructors:

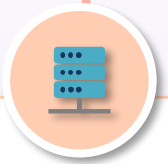
Michael J Shannon

and

Carl Mullin

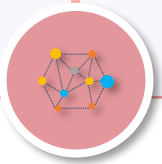
- **Class will begin at 10:00 A.M. Central Standard Time (CST)**

Data States



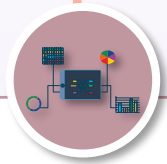
Data at rest

On hard disks, memory cards, data centers, cloud storage, archives and backups, external and removable drives



Data in transit (data in motion)

Data sent on LAN, WAN, MAN, dedicated lines, wired, wireless, etc.



Data in use (volatile data)

Data in CPU registers, RAM memory, volatile storage, Redis and Memcached elastic caches, etc.

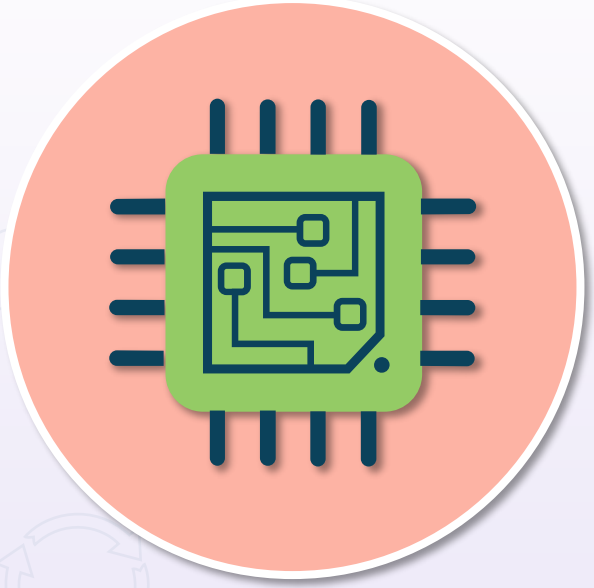
Protecting Data at Rest

- Conventional perimeter-based defenses, like firewalls, IPS, and antivirus programs
- Defense-in-depth access controls and MFA
- Secure principles, like dual operator and separation of duties
- Volume, disk, and file encryption using full disk encryption (FED) and self-encrypting drives (SED)
- Partitioned storage and hardware security modules (HSM)

Protecting Data in Motion

- Encapsulation
- Dedicated channels
- Transport Layer Security (SSL/TLS)
- IPsec Virtual Private Networks (VPNs)
- Wi-Fi Protected Access 3 (WPA3) with management frame protection
- IEEE 802.1X port-based network access control (PNAC)
- 802.11AE MACsec

Protecting Data in Use



- The least mature protection system
- Overhead due to encryption/decryption and often costly and difficult to implement
- Newer methods for protecting volatile data in memory, such as homomorphic encryption
  - Conduct calculations on encrypted data without decrypting it
- Trusted computing systems (SELinux)
- Machine learning and AI algorithms are on the cutting edge of visibility and memory protection

Data and Asset Classification

You may be using a model that has sensitivity levels and classification

- You must have a well-established tagging and labeling schema that maps to a configuration management database (CMDB), such as ServiceNow
  - Facilities, equipment, physical assets
  - Data and information assets
  - Human resources (people assets)
  - Intangible assets and intellectual property
  - Can be on-premises, in the cloud, or used as disaster recovery sites

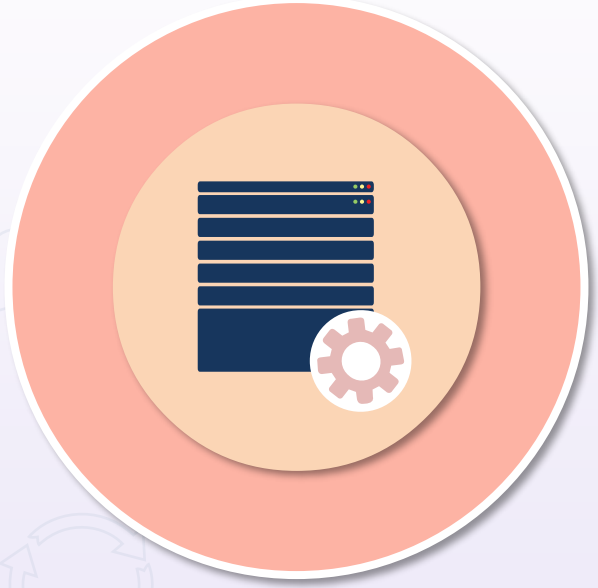
Configuration Management Database (CMDB)

- 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)
- Helps various IT services to better align with business needs by providing current and accurate data to
  - change and patch management
  - incident and problem management
  - availability management, and
  - release and deployment management

Configuration Management Database (CMDB)

- Configuration management practices offer the required data about assets and their configurations, including their interactions with other assets, which assists administrators and managers with
  - problem resolution
  - incident response
  - network component deployment
  - strategy formulation
  - budgetary forecasting, and
  - overall decision-making

Information and Asset Handling Requirements



- Labeling concerns the classification and prioritization of data, systems, and assets to determine the level of protection and how the asset should be handled
- Handling controls who has access to assets and what actions they can take
- Handling is based on labeling and how it has been classified

Choose a Classification Level

- Value – the most common criteria – if it is valuable, it should be protected
- Architecture – the subjects and objects are restricted by a mandatory access control model
- Age – the value of data lowers over time – i.e., automatic de-classification
- Useful life – if the information is made obsolete it can often be de-classified
- Personal association – if the data involves personally identifiable or health information

Sample CMDB Schema

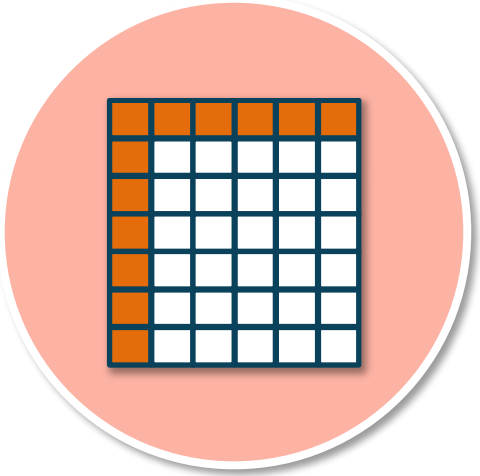
Field (Key)	Value
Collector (_collector)	The name of the collector
Source (_source)	The name of the Source entered when the Source was generated
Source Category (_sourceCategory)	A tag determined by your entry to the Category field when you configure a Source (e.g., sensor, syslog, NetFlow)
Source Host (_sourceHost)	A fixed value determined by the hostname you enter in the Hostname field
Message Count (messageCount)	A unique sequence number (per Source) added by the Collector when the message was received

Asset Management

- Tracking all physical and logical assets for location, modification, and disposition leads to improved risk management and asset recovery for business continuity
- Whether an asset is real estate or software, the asset manager's main task is to supervise all the activities related to asset management
- Digital asset manager is a growing enterprise role
- Automation and orchestration systems are vital for medium to large organizations

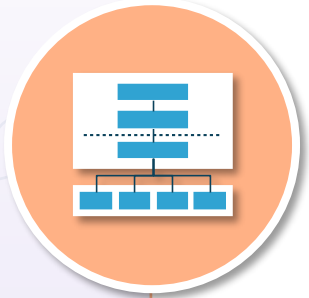
Asset Inventory Control

Just-in-Time (JIT) is prevalent



- Managing inventory helps you keep corporate budgets in line and allows for better security and more efficient management of operating capital
  - Assess the type of inventory you keep
  - Determine the quantity of goods you need to keep on hand
  - Track market trends of competitors
  - Identify minimum stock level
- Just-in-time (JIT) is an inventory strategy used to increase efficiency and decrease waste by acquiring goods only as needed in the production process

Asset Inventory Control



- Best practices for fixed asset inventory software:
  - Realize the scope of your project
  - Assign responsibility for your asset management
  - Learn basic fixed asset procedures
  - Rely on automated software in the future
  - Look for emerging technological trends
  - Clear out ghost assets (ghost IT)

Data Roles

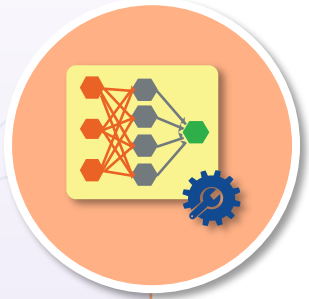
- Owner
  - Owns the information in a DAC model
  - Determines the tagging and classification level
- Steward
  - Manages the data and metadata from a business perspective
  - Ensures compliance (standards/controls) and data quality

Data Roles

- Custodian
  - Is the keeper of the information from a technical perspective
  - Ensures CIA is maintained
- Processors
- Officer (CIO, CPO, CTO)

Data Lifecycle Management

Data Collection



- This is also called data capture, and there are three key methods through which data can be captured:
  - Data acquisition: the consumption of readily obtainable data that has been produced by an entity outside the organization
  - Data entry: the generation of new data values for the organization by human operators or devices that produce data for the enterprise
  - Data reception: the capture of data generated by devices
    - Examples: SIEM systems, NetFlow collection, logs, industrial control systems, SCADA, and information systems linked to the Internet of Things (IoT)

Data Collection

- Unless data is collected, it cannot be analyzed, matched for patterns, or used for data-driven business decisions
- Only data necessary for organizational or business needs should be collected
- Article 25 of the General Data Protection Regulation (GDPR) mandates that many companies protect data by design and by default
- Enterprises should integrate data protection principles into business activities in the beginning and throughout the data life cycle

Data Location: Object vs. Block Storage

	OBJECT STORAGE	BLOCK STORAGE
PERFORMANCE	Performs best for big content and high stream throughput	Strong performance with database and transactional data
GEOGRAPHY	Data can be stored across multiple regions	The greater the distance between storage and application, the higher the latency
SCALABILITY	Can scale infinitely to petabyte and beyond	Addressing requirements limit scalability
ANALYTICS	Customizable metadata allows data to be easily organized and retrieved	No metadata

Data Location: Databases

Database type	Use cases
Relational	Traditional applications, ERP, CRM, e-commerce
Key-value	High-traffic web apps, e-commerce systems, gaming applications
In-memory	Caching, session management, gaming leaderboards, geospatial application
Document	Content management, catalogs, user profiles
Wide column	High scale industrial apps for equipment, fleet management, and route optimization
Graph	Fraud detection, social networking, recommendation engines
Time series	IoT applications, DevOps, industrial telemetry
Ledger	Systems of record, supply chain, registrations, banking transactions

Data Maintenance

- Maintenance is initiated once the data has been collected
- It involves offering data to points where usage and synthesis happen
- Some models have this as the transition from raw data to information
- Data maintenance is about processing the data without yet deriving any value from it for the enterprise (that is where information becomes knowledge and ultimately wisdom)
- Involves processes such as movement, integration, cleansing, augmentation, and the familiar extract-transform-load (ETL) functions
- Maintenance is the goal of a far-reaching array of data management activities and because of this, data governance faces many challenges in this area

Data Remanence

- Data remanence is the data, metadata, and artifacts that are leftover after a software deletion process
- This is a known residual risk when handling data during the lifecycle
- To counter the risk of malicious data recovery, physical destruction is always the best choice, however, there are other methods
- There are fundamentally three categories of ways to handle data remanence:
  - Clearing – involves wiping or overwriting the data with zeroes or ones; data may be recoverable under this method
  - Purging – a stronger enduring form that can include methods such as sanitizing or degaussing; data is not considered recoverable by any known methods
  - Destruction – the strongest technique, which includes shredding, pulverizing, burning, and encryption

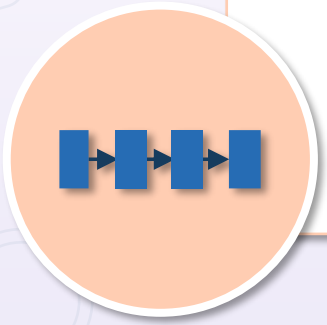
Data Retention

- In some organizations, how long a particular document or record is stored can be just as important as what is being stored
- A data retention policy helps to define what is stored, how it is stored, how long it is stored, and how it is disposed of when the time arrives
- Periodic audits help to ensure that data records or documents are removed when they are no longer needed
- You should implement an automated disk or object storage lifecycle on-premises or in the cloud

Asset Disposal

- In the asset disposal process/phase, plans are developed for discarding system information, hardware, and software and making the transition to a new system
- The information, hardware, and software may be moved to another system, archived, discarded, or destroyed
- If performed improperly, the disposal phase can result in the unauthorized disclosure of sensitive data
- When archiving information, organizations should consider the need and methods for future retrieval

Asset Disposal



- The disposal activities ensure the orderly termination of the system and preserve vital information about the system so that some or all of it can be reactivated in the future, if necessary
- Emphasis is given to proper preservation of the data processed by the system so that data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access
- The removal of information from a storage medium, such as a hard disk or tape, should be done in accordance with the organization's security requirements

Destruction and Sanitization

- Burning, shredding, pulping, and pulverizing for paper records
- Pulverizing for microfilm or microfiche, laser discs, and document imaging applications
- Magnetic degaussing for computerized data
- Shredding or cutting for DVDs
- Demagnetizing magnetic tapes

Destruction and Sanitization

- Degaussing – removing the magnetic field
- Purging – clearing everything off the media
- Wiping – overwriting every sector of drive with 1 and 0
  - The DoD 5220.22-M sanitization method is one of the most common sanitization methods used in data destruction software, and in general, is still perceived as an industry standard in the U.S.
- Encryption – encrypting all files before deleting or disposing of media

Destruction and Sanitization

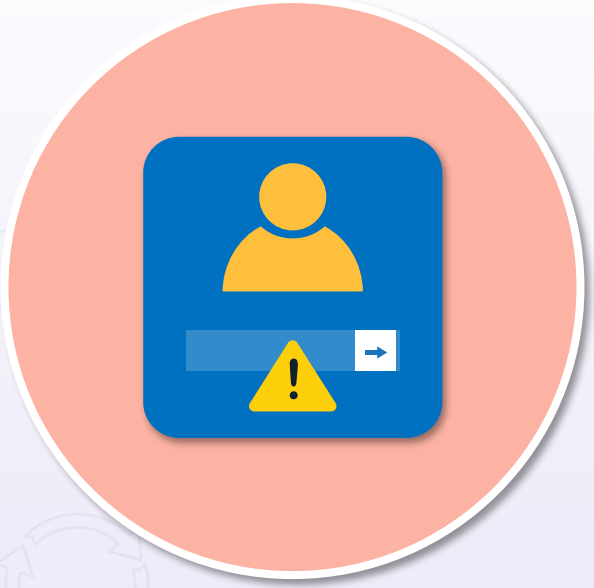
Example: medical offices should maintain documentation of the destruction of health records, including the following:

- Date of destruction
- Method of destruction
- Description of the disposed records
- Inclusive dates
- A statement that the records were destroyed in the normal course of business
- The signatures of the individuals supervising and witnessing the destruction

Inherent Risk

- Inherent risk is an assessed level of raw or untreated risk
- Can be defined as the natural level of risk inherent in a process or activity without doing anything to reduce the likelihood or mitigate the severity of a mishap
- Another definition is the current risk level given the existing set of controls, which may be incomplete or less than ideal, rather than an absence of any controls

Residual Risk



- The amount of risk or danger associated with an action or event remaining after natural or inherent risks have been reduced by risk controls
- The general formula to calculate residual risk is:

Residual risk = (inherent risk) − (impact of risk controls)

Risk Treatment (or Handling)

Risk avoidance – stopping or rejecting the activity that introduces the risk

Risk reduction/mitigation – risk is reduced to an acceptable level by implementing controls

Risk transference (sharing) – the risk is transferred to the insurance company or cloud provider

Risk acceptance – tolerating the potential loss by introducing no countermeasures or controls

Assessing Vulnerability

Begins with the definition

- It should be quantified as a percentage of probability and not just a vague list of "scary things"
- The likelihood that a threat agent's actions will result in a loss (frequency and magnitude)
- It can be a derived value from the threat capability of actors combined with the resistance of existing security controls

Assessing Vulnerability

Asset assessment and labeling

- All client and server operating systems and versions/builds
- Posture of patches, updates, and security fixes
- Browsers and types of endpoints
- Methods of access – wired, wireless, VPN, and remote teleworkers
- Control types and categories
- Access control methodologies (2FA)

Indicators of Compromise (IoC)

These are network or host-based cyber observables

Forensic artifacts of an incursion or disturbance

A measurable event or stateful property in the cyber domain

Registry entries, compressed and encrypted files on disk and in-memory, etc.

Vulnerability Information Gathering

- Various logs (system, application, firewall, etc.)
- Simple Network Management Protocol (SNMP) traps
- NetFlow collection
- Security information and event management (SIEM) systems
- Next-Generation Intrusion Prevention System (NGIPS) alerts and logs
- Cloud-based visibility tools
- Machine learning and artificial intelligence data analysis

Vulnerability Databases

- A collection and distribution of information about exposed computer security vulnerabilities
- It typically categorizes and defines an identified vulnerability (and variants) with a timeline and coding
- The database usually assesses the potential impact on affected systems based on a qualitative scale (1-5)
- May also provide mitigations, workarounds, and updates

Vulnerability Databases

These are two of the most used resources

Common Vulnerabilities and Exposures (CVE)

- A list of entities from MITRE.org that represents publicly known cybersecurity vulnerabilities
- Consists of an ID number, description, and public references
- Used by the National Vulnerability Database (NVD)

Common Vulnerability Scoring System (CVSS)

- Open standard for weighing the severity of computer system vulnerabilities
- Uses a uniform and consistent scoring method ranging from 0 to 10, with 10 being the highest severity

Vulnerability Databases

- Common Vulnerabilities and Exposures (CVE) with MITRE
- National Vulnerability Database with NIST
- ISS X-Force database
- Symantec/SecurityFocus BID database
- @Risk from SANS.ORG

Vulnerability Scanning

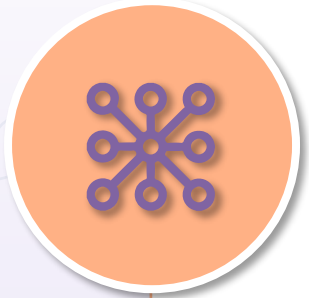
HTTP/S is the most common traffic

- Web application vulnerability scanners are most common due to heavy usage of HTTP (e.g., Burp Suite and OWASP ZAP)
- Automated tools can scan web applications and look for these security vulnerabilities:
  - Cross-site scripting
  - Cross-site request forgery
  - SQL and command injection
  - Path traversal
  - Insecure server configuration

Dark Web

- Also called overlay networks or darknets
- Need special software, configs, or authorization
- Deep web not indexed by search engines
- Peer-to-peer networking
- Tor, Freenet, I2P, and Riffle

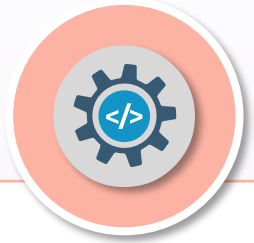
Open-source Intelligence (OSINT)



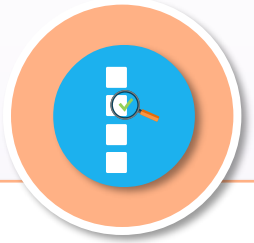
- OSINT is any data or information that can be collected legally from free, public sources concerning an individual or organization
- It is usually information found on the Internet, but can be sourced from books or reports in a public library, articles in a newspaper/magazine, statements in a press release, and FOIA reports
- Can be gathered using tools like Maltego, sharing centers, and code repositories like GitHub, among others

Threat Intelligence Sources

Automated Indicator Sharing (AIS) – Cybersecurity and Infrastructure Security Agency (CISA) capability, enables the real-time exchange of machine-readable cyber threat indicators



Structured Threat Information Exchange (STIX) – standardized language developed by MITRE (in a collaborative way) to represent structured information about cyber threats



Trusted Automated eXchange of Indicator Information (TAXII) – transport vehicle for services and message exchanges to allow the sharing of information about cyber threats

Predictive analysis and threat maps – uses cutting-edge machine learning engines and artificial intelligence tools to predict future threats

Risk Assessment Document

- Record the processes used to identify probable threats and propose subsequent action plans if the hazard occurs
- Document assets at risk (people, buildings, information technology, utility systems, machinery, raw materials, and finished goods)
- Many templates and prototypes available online

Risk Assessment Document Inputs

Hazard Identification

Hazards

- Fire
- Explosion
- Natural hazards
- Hazardous materials spill or release
- Terrorism
- Workplace violence
- Pandemic disease
- Utility outage
- Mechanical breakdown
- Supplier failure
- Cyber attack

Property & Magnitude

Vulnerability Assessment

Assets at Risk

- People
- Property, including buildings and critical infrastructure
- Supply chain
- System/equipment
- Information technology
- Business operations
- Reputation of or confidence in entity
- Regulatory and contractual obligations
- Environment

Vulnerability

Impact Analysis

Impacts

- Casualties
- Property damage
- Business interruption
- Loss of customers
- Financial loss
- Environmental contamination
- Loss of confidence in the organization
- Fines and penalties
- Lawsuits

https://www.ready.gov/risk-assessment

Risk and Threat Matrix

	Event type								
	Accidental leak	**Espionage**	**Financial fraud**	**Misuse**	**Opportunistic data theft**	**Physical theft**	**Product alteration**	**Sabotage**	**Violence**
Nonhostile									
Reckless insider	X			X			X		
Untrained/distracted insider	X			X			X		
Outward sympathizer	X			X					
Unknown (nonhostile or hostile)									
Supplier	X	X	X	X	X		X		
Partner	X	X	X	X	X		X		
Hostile									
Irrational individual	X			X		X		X	X
Thief		X	X		X	X			
Disgruntled insider	X	X	X	X	X	X	X	X	X
Activist		X		X	X	X	X	X	
Terrorist						X		X	X
Organized crime		X	X		X	X	X		
Competitor		X			X		X	X	
Nation state		X			X		X	X	

Classic Qualitative Analysis

		Negligible	Minor	Moderate	Critical	Disastrous
		1	2	3	4	5
Frequent	5	Medium	Medium	High	High	High
Likely	4	Medium	Medium	Medium	High	High
Occasional	3	Low	Medium	Medium	Medium	High
Seldom	2	Low	Low	Medium	Medium	Medium
Improbable	1	Low	Low	Low	Medium	Medium

Classic Semiquantitative Analysis

Impact

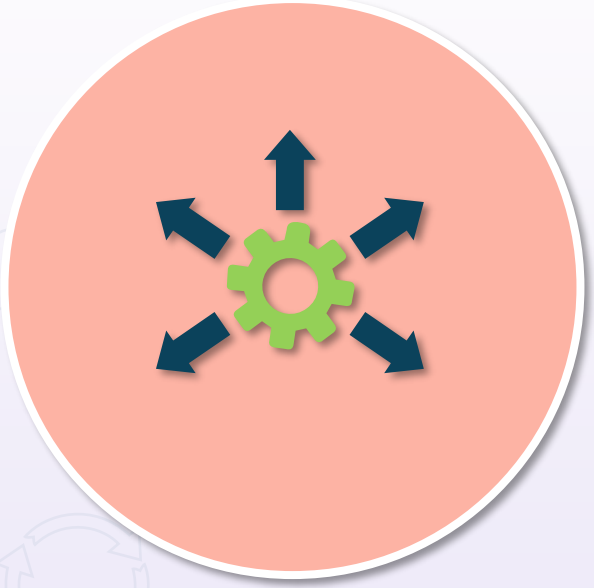
- Negligible = 1 (no impact)
- Minor = 2 (< $1 million)
- Moderate = 3 (≥ $1 million)
- Critical = 4 (≥ $100 million)
- Disastrous = 5 (complete)

Likelihood

- Improbable = 1 (almost never)
- Seldom = 2 (not in 5 years)
- Occasional = 3 (once in last 5 years but not in last year)
- Likely = 4 (once in last year)
- Frequent = 5 (several times a year)

Risk of event = 4 (material impact) X 3 (moderate likelihood) = 12

Classic Quantitative Analysis



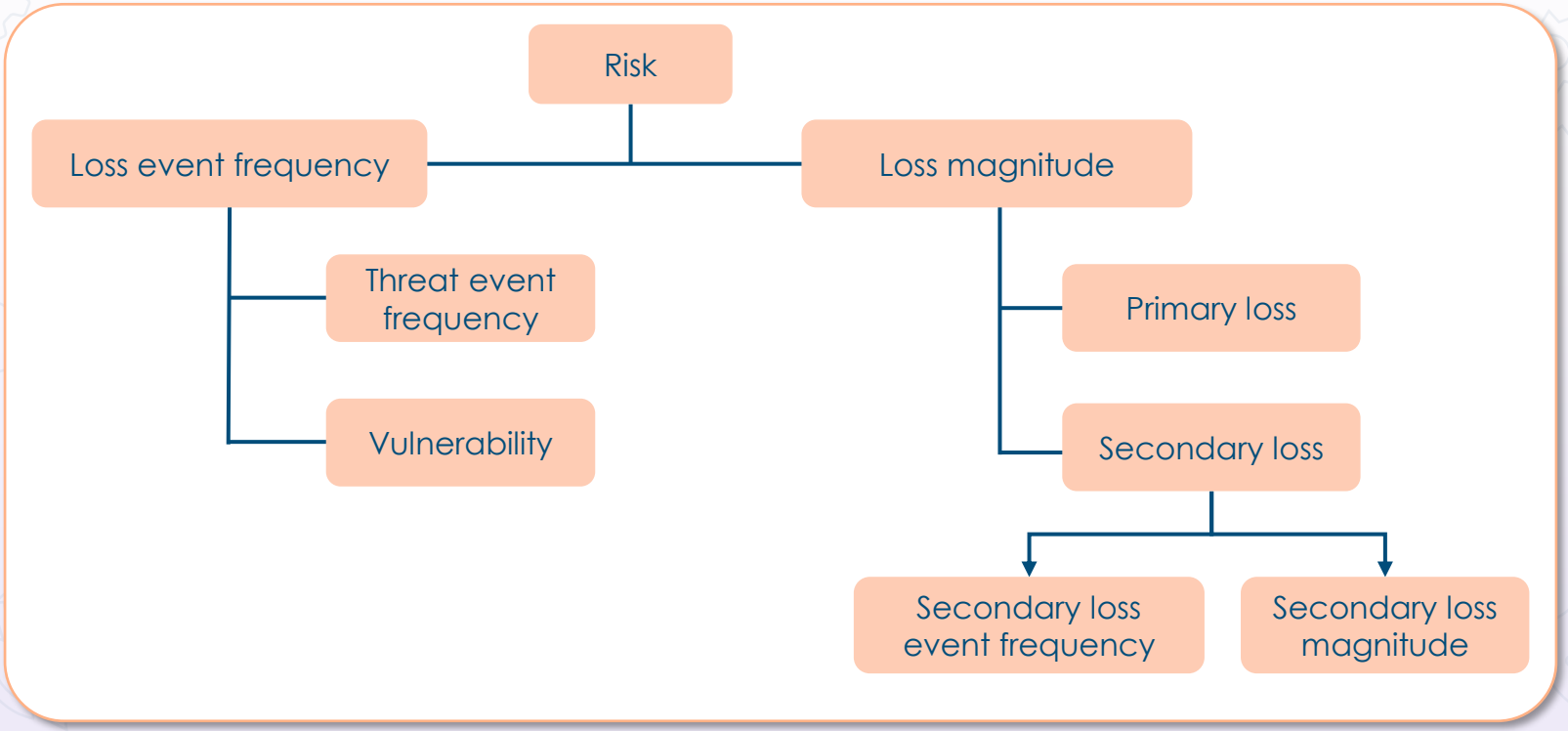
ALE = (AV x EF) x ARO

(if SLE = AV x EF), then

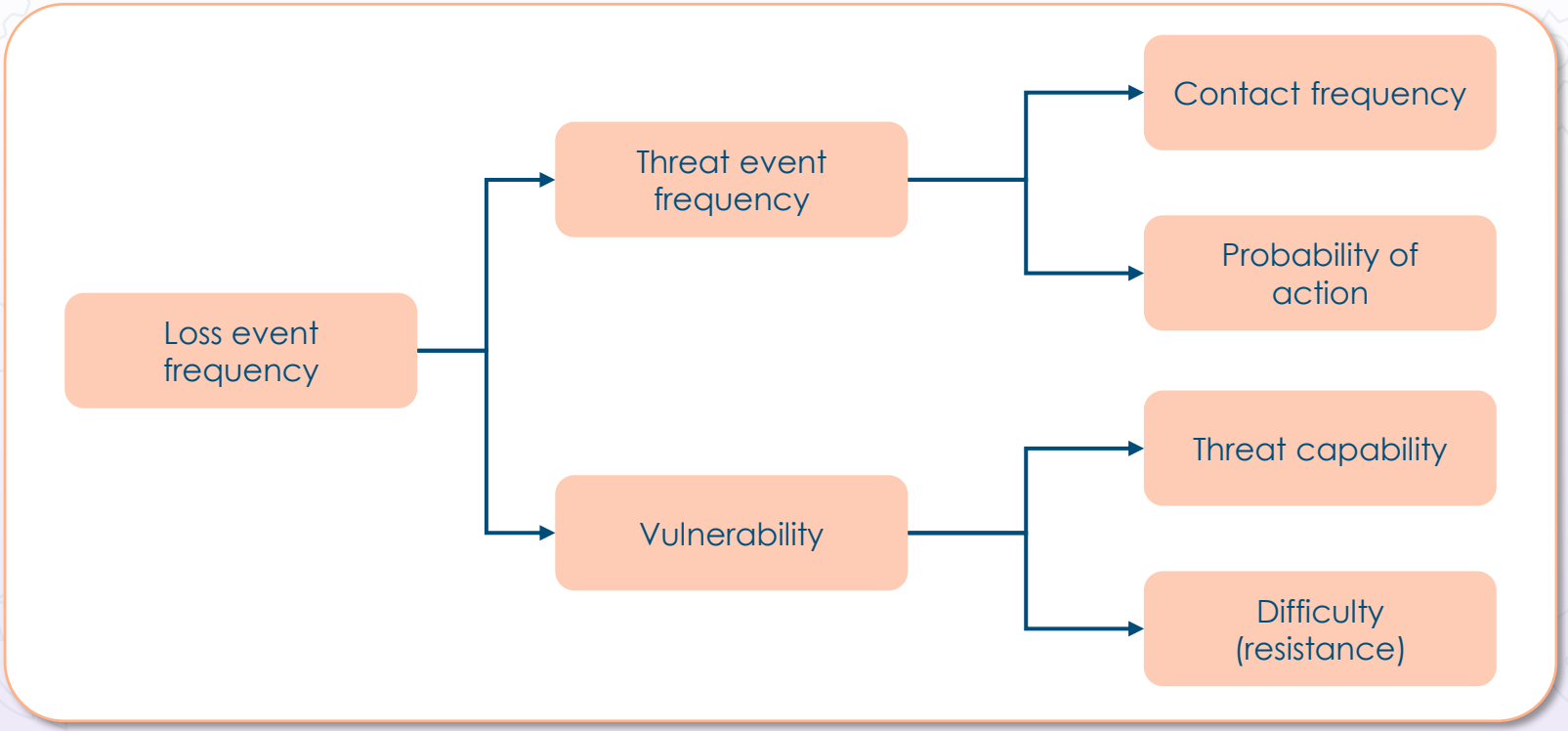
ALE = SLE x ARO

- **ALE** is annualized loss expectancy
- **AV** is asset value
- **EF** is exposure factor
- **SLE** is single loss expectancy
- **ARO** is annualized rate of occurrence

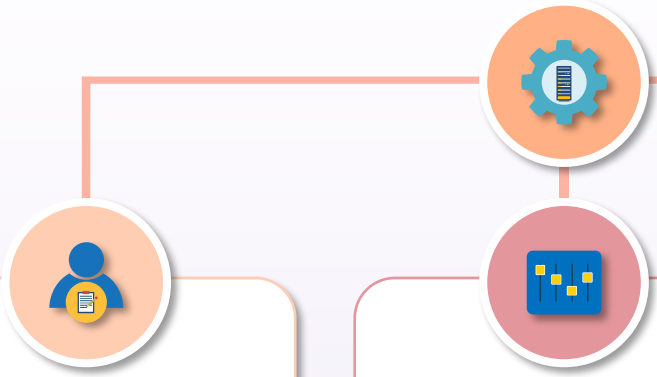
Factor Analysis of Information Risk (FAIR) Methods



Further Decomposition to Determine Risk



Security Control Categories



Administrative (or Managerial – defines policies, procedures, best practices, and guidelines

Technical – controls access to a resource using hardware and software components

Physical – controls access to campus, facilities, or specific areas and rooms

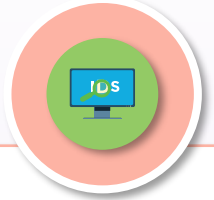
Security Control Categories

Administrative	Technical	Physical
Effective hiring practices	Controlled user interfaces	Guards
Effective termination practices	Password, tokens, OTPs	Fences
Classification of data based on levels of sensitivity	Firewalls	Motion detectors
Supervision of employees	Routers that filter traffic	Locks
Tracking of employee activity	Antivirus software	Cable conduits
Separation of duties	Access control lists	Swipe cards
Rotation of duties	Intrusion detection/prevention systems	Badges
	Smart cards	Dogs
	Biometrics	Cameras
		Alarms

Security Control Types

Preventive

Stops attacker from performing attack



Detective

Identifies an attack that is happening

Corrective

Restores a system to state before attack

Deterrent

Discourages attacker from performing attack

Compensating (recovery)

Aids controls already in place

NIST Cybersecurity Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• Asset management • Business • Environment • Risk assessment • Risk management	• Awareness control • Awareness and training • Data security • Info protection and procedures • Maintenance • Protective technology	• Anomalies and events • Security continuous monitoring • Detection process • Communications	• Response planning • Communications • Analysis • Mitigation • Improvements	• Recovery planning • Improvements • Communication

Center for Internet Security (CIS)

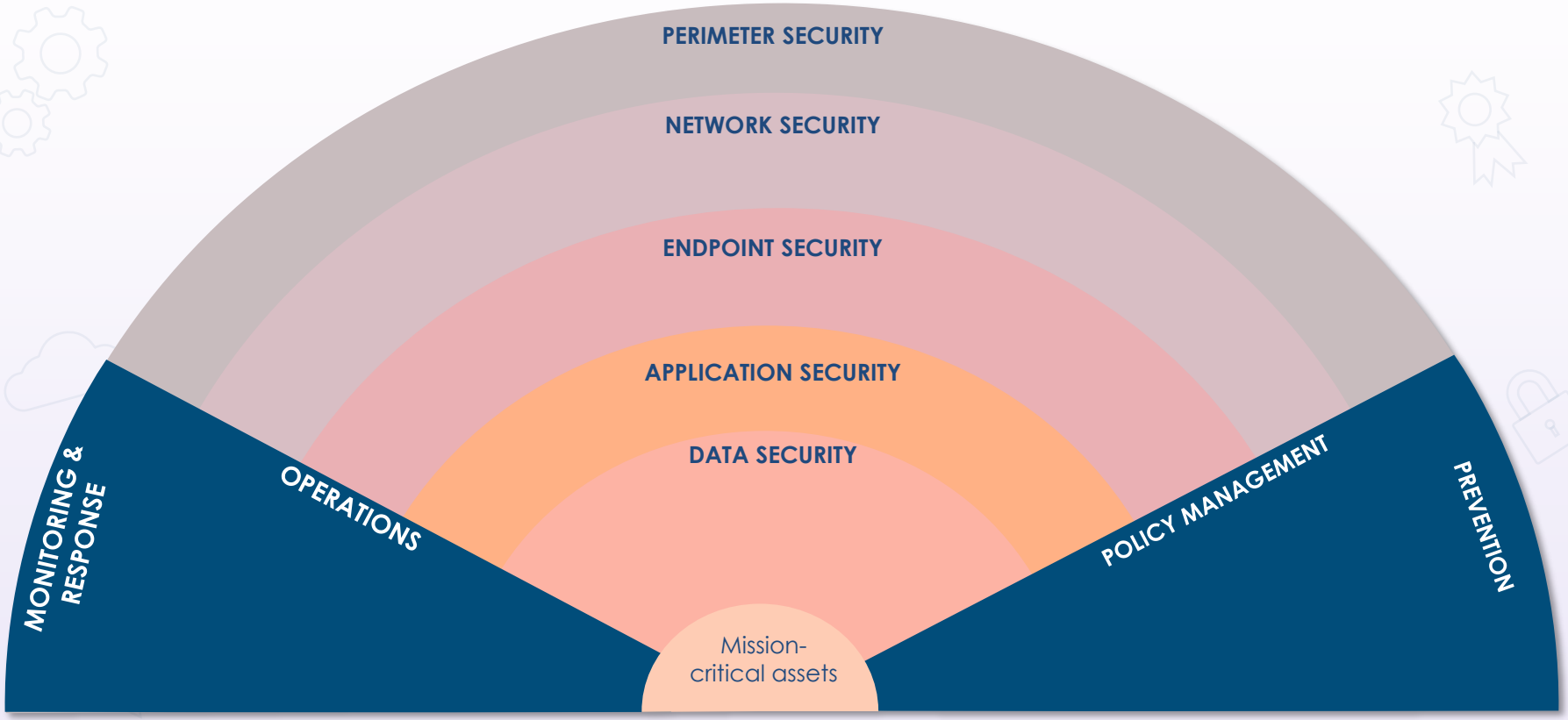
- Repository for cybersecurity best practices, tools, and threat assessment and awareness
- CIS leverages the power of a global IT community to defend public and private organizations against various cyber threats with:
  - CIS Benchmarks™ - consensus-created secure configuration guidelines for hardening data, systems, and applications
  - CIS Controls® – a strict, ordered, and simplified set of cybersecurity best practices and guidelines
  - CIS SecureSuite® - membership program that offers an automated combination of CIS Benchmarks, CIS Controls, and CIS-CAT Pro into a commanding and efficient cybersecurity resource
    - CIS-CAT Pro allows users to evaluate conformance to best practices and expand compliance scores on an ongoing basis

Cloud Security Alliance (CSA)

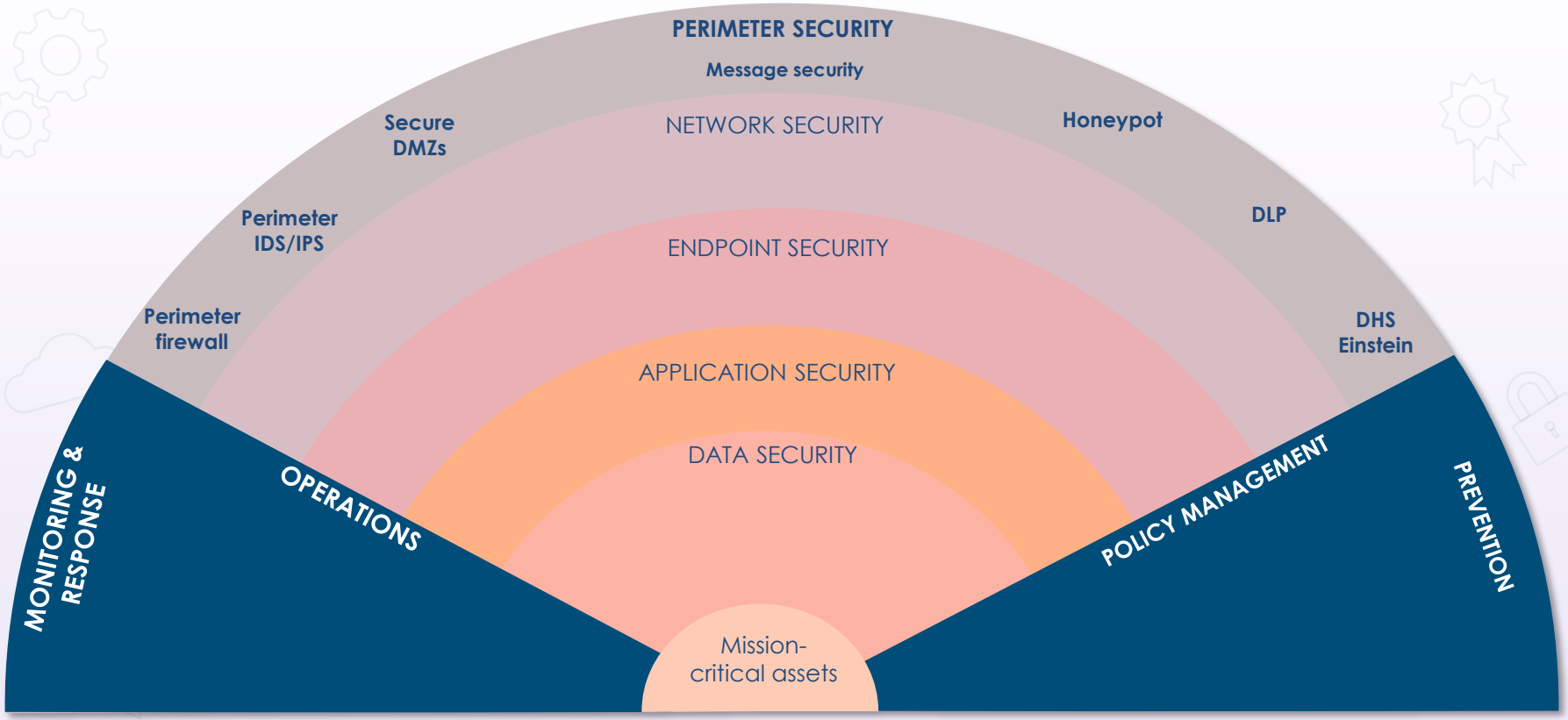
- An organization committed to defining and raising awareness of guidance for organizations of all types and sizes to guarantee a secure cloud computing experience
- Offers the Cloud Control Matrix (CCM) Version 4 to ensure handling of requirements stemming from
  - new cloud technologies
  - new controls and security responsibilities
  - necessary auditability of controls, and
  - interoperability and compatibility with other standards

Other Risk Frameworks

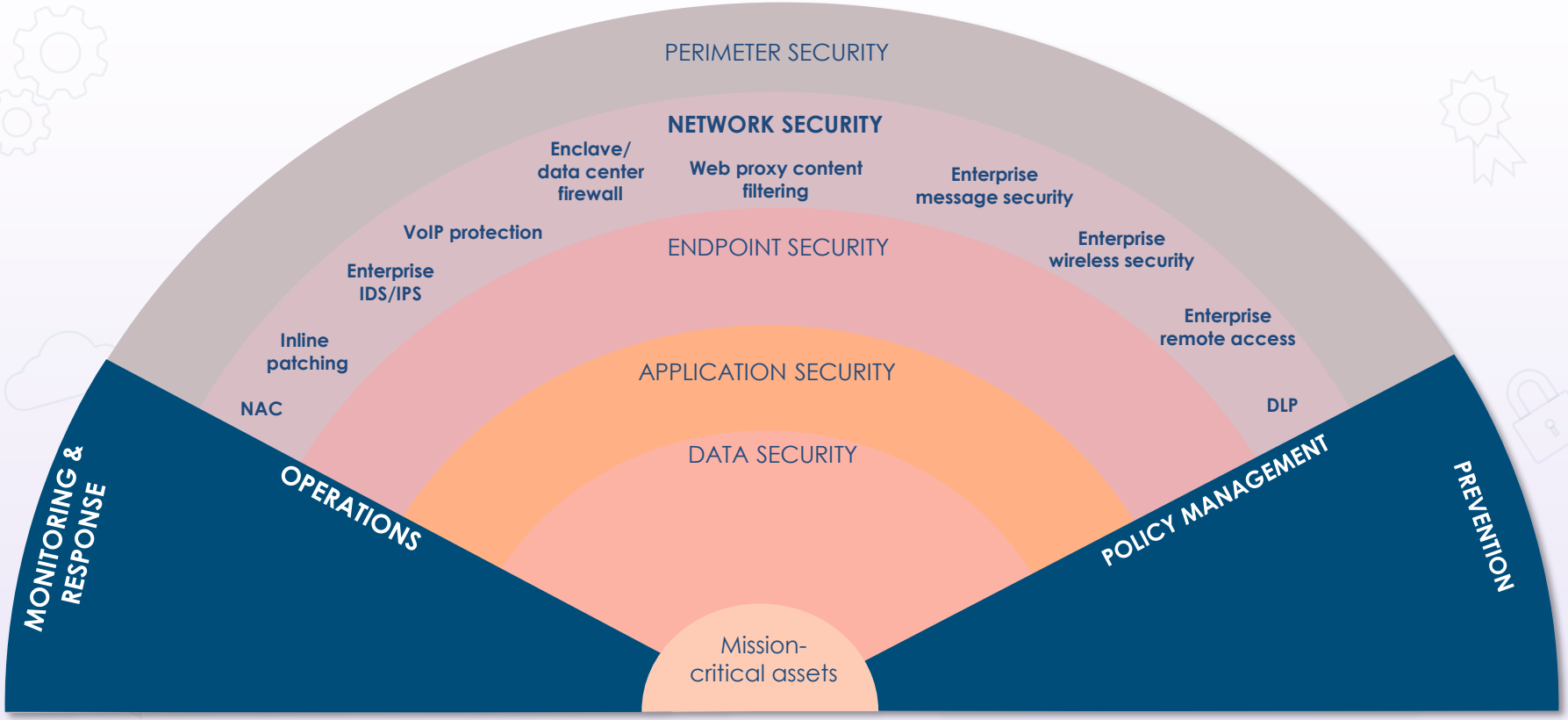
Countermeasure Selection and Implementation



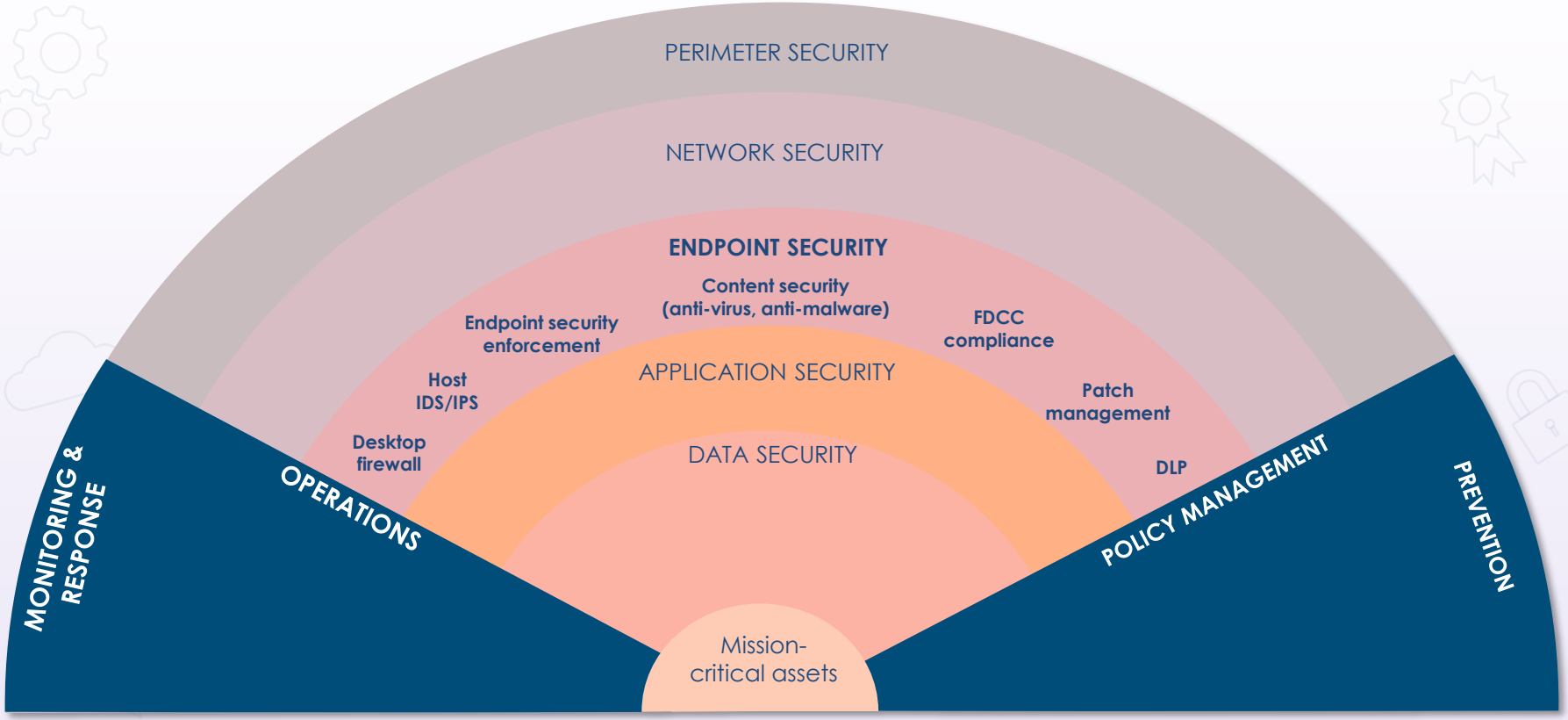
Countermeasure Selection and Implementation



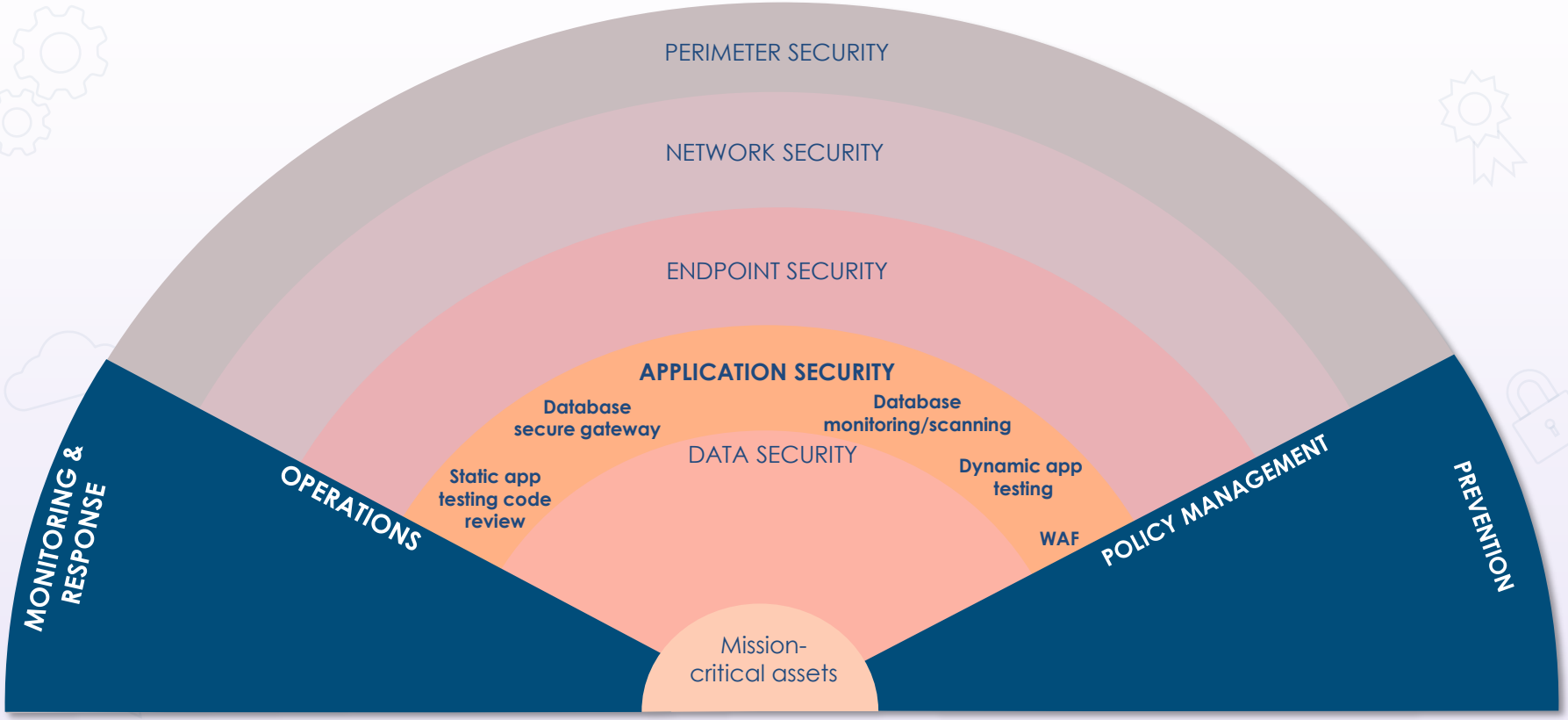
Countermeasure Selection and Implementation



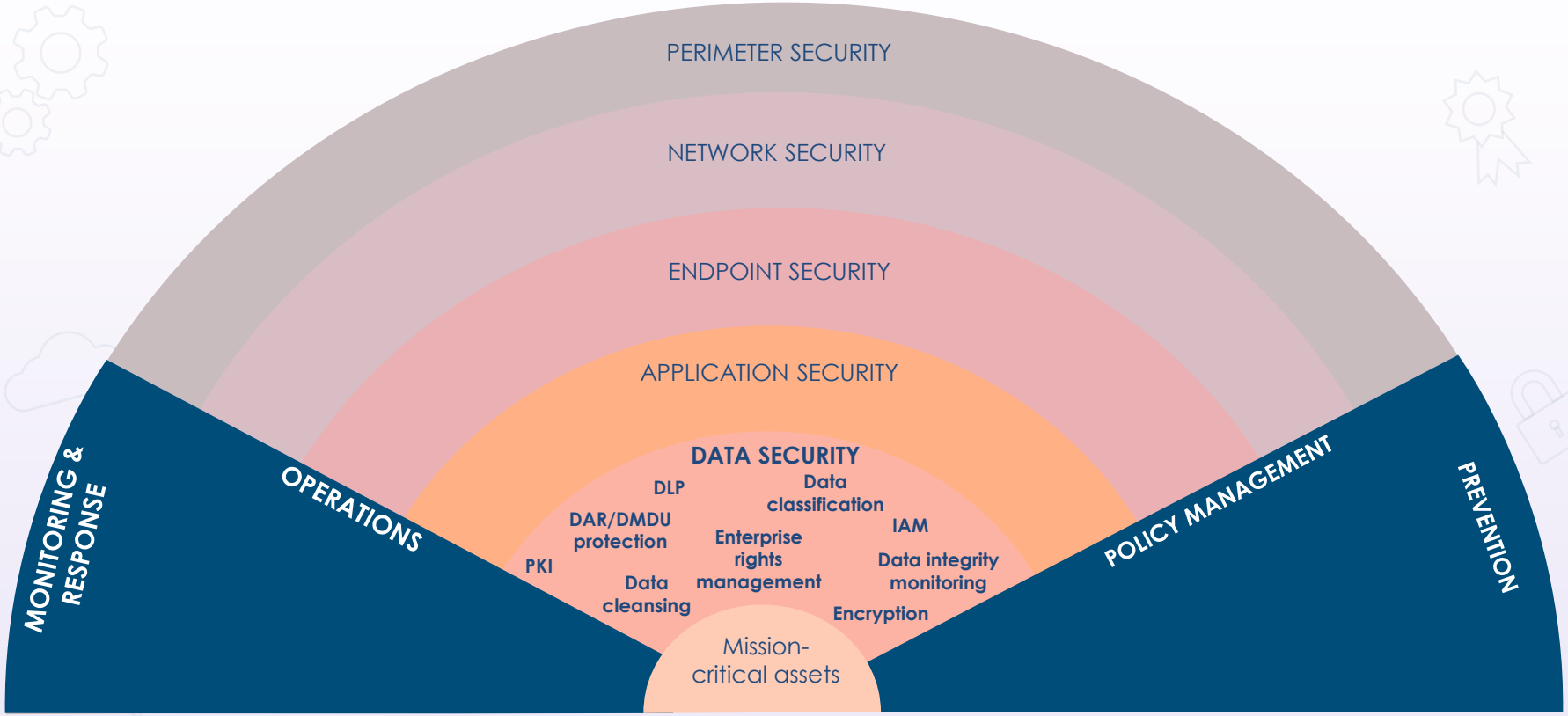
Countermeasure Selection and Implementation



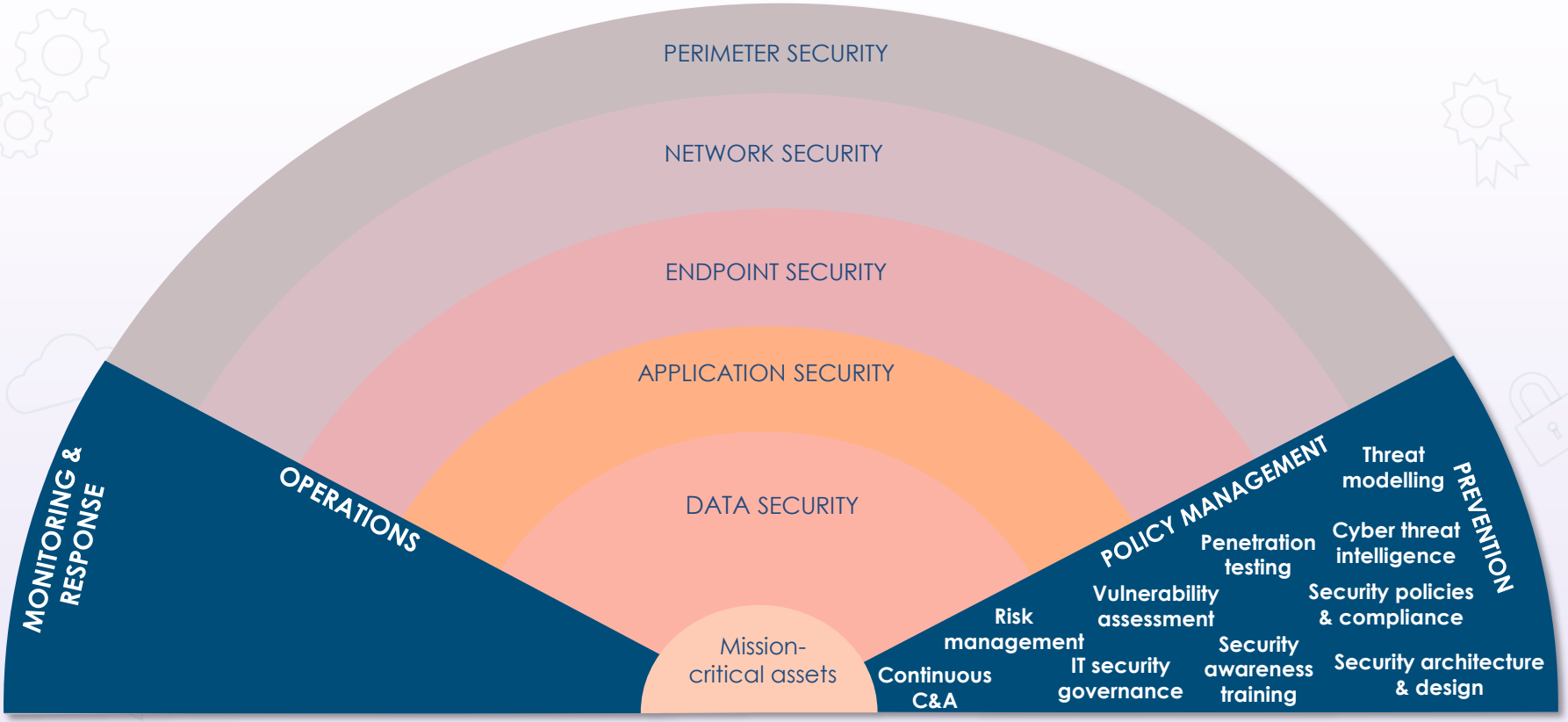
Countermeasure Selection and Implementation



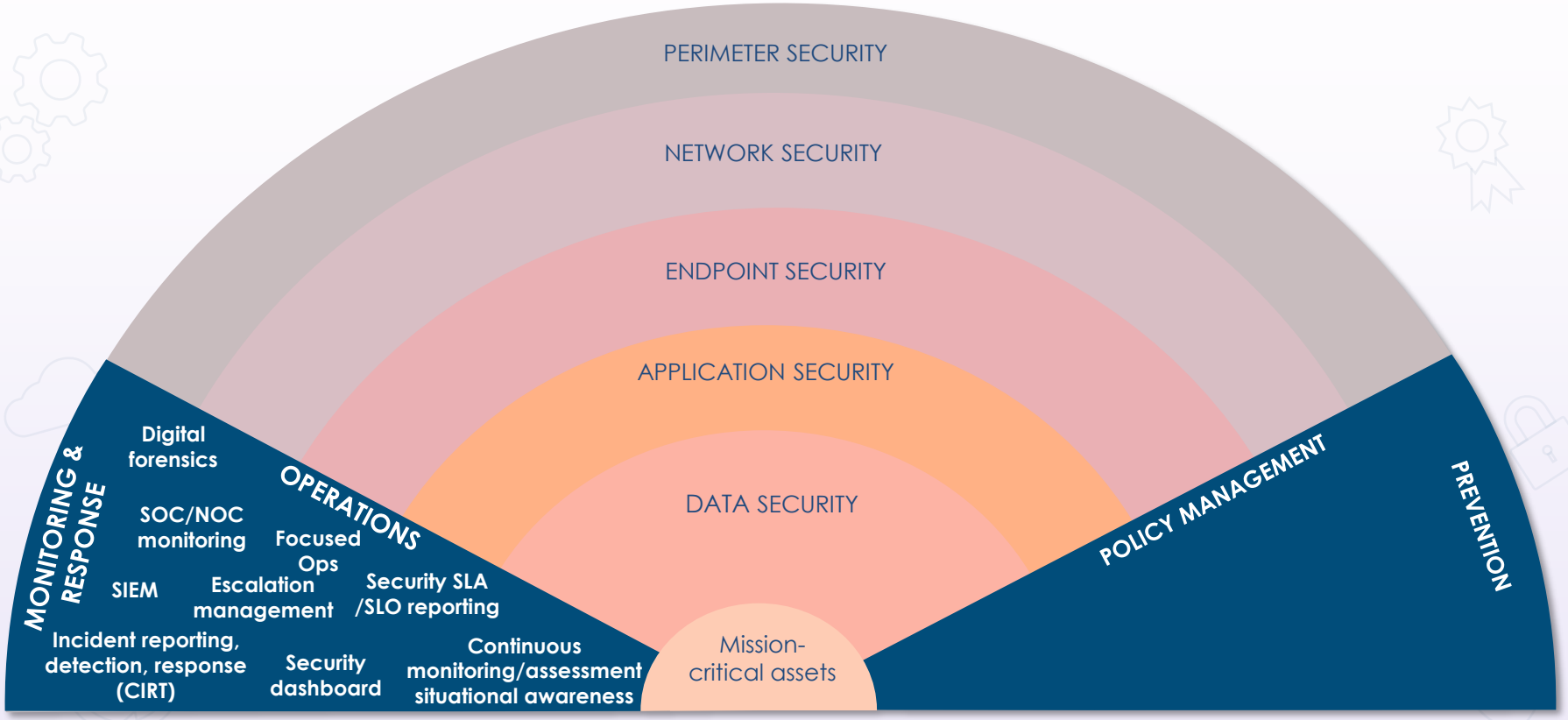
Countermeasure Selection and Implementation



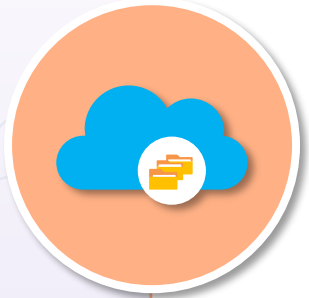
Countermeasure Selection and Implementation



Countermeasure Selection and Implementation



Security Control Assessment



- An SCA is a formal evaluation of a system against a pre-defined set of controls
- It is performed in, with, or independently of a full Security Test and Evaluation (ST&E), which is performed as part of an official security authorization
- The SCA and ST&E will appraise the operational plan (or planned implementation) of controls
- The results are a risk assessment report that represent a gap analysis documenting the system, application, or data risk
- Tests conducted should include audits, security reviews, vulnerability scanning, and penetration testing

Capability Maturity Model (CMM)

Initial (Chaotic)
Chaotic, ad hoc, Individual heroics

Level 1

Repeatable (Implicit)
Process is not codified or defined and is still vulnerable to inconsistency

Level 2

Defined (Early Explicit)
Process is defined and documented as a standard business process

Level 3

Managed (Mature Explicit)
Process is controlled and can be adjusted or adapted to particular projects without measurable losses in quality

Level 4

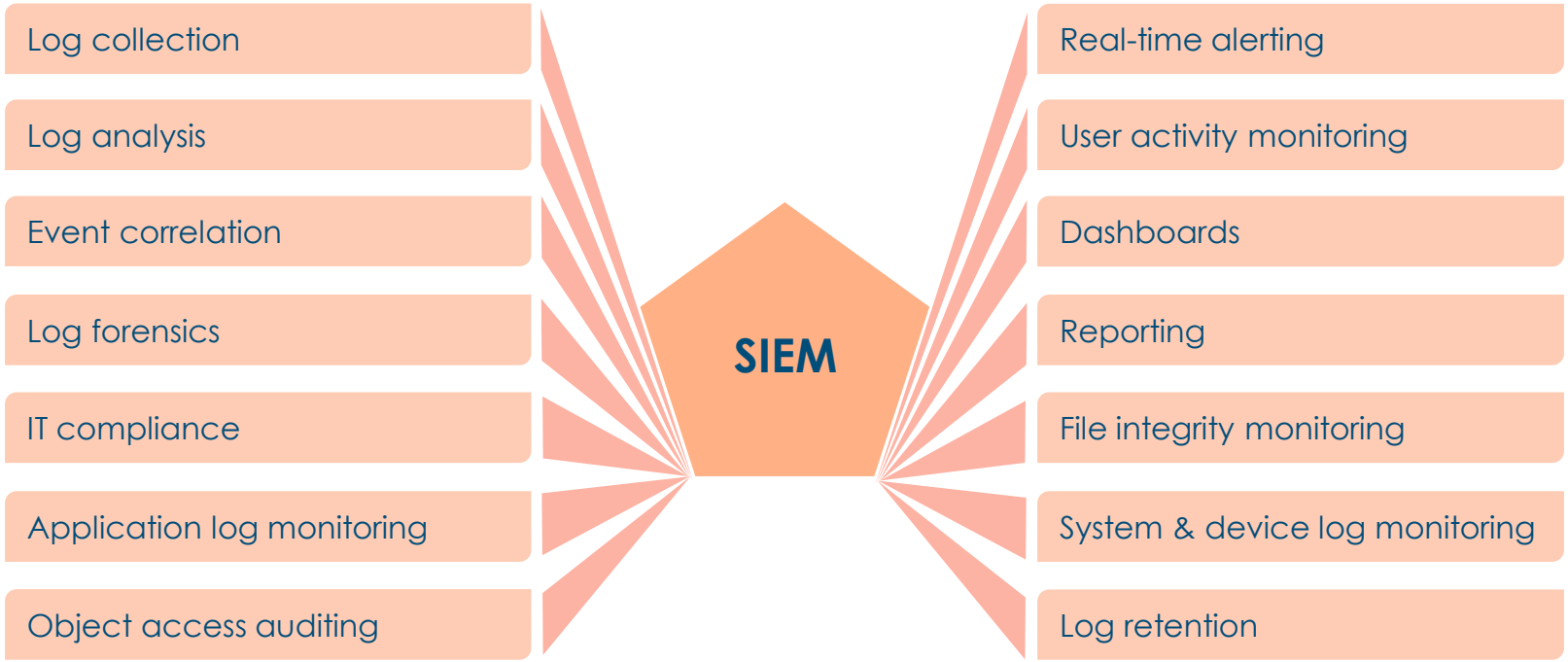
Optimized (Purely Explicit)
Process management results in deliberate process optimization and improvement

Level 5

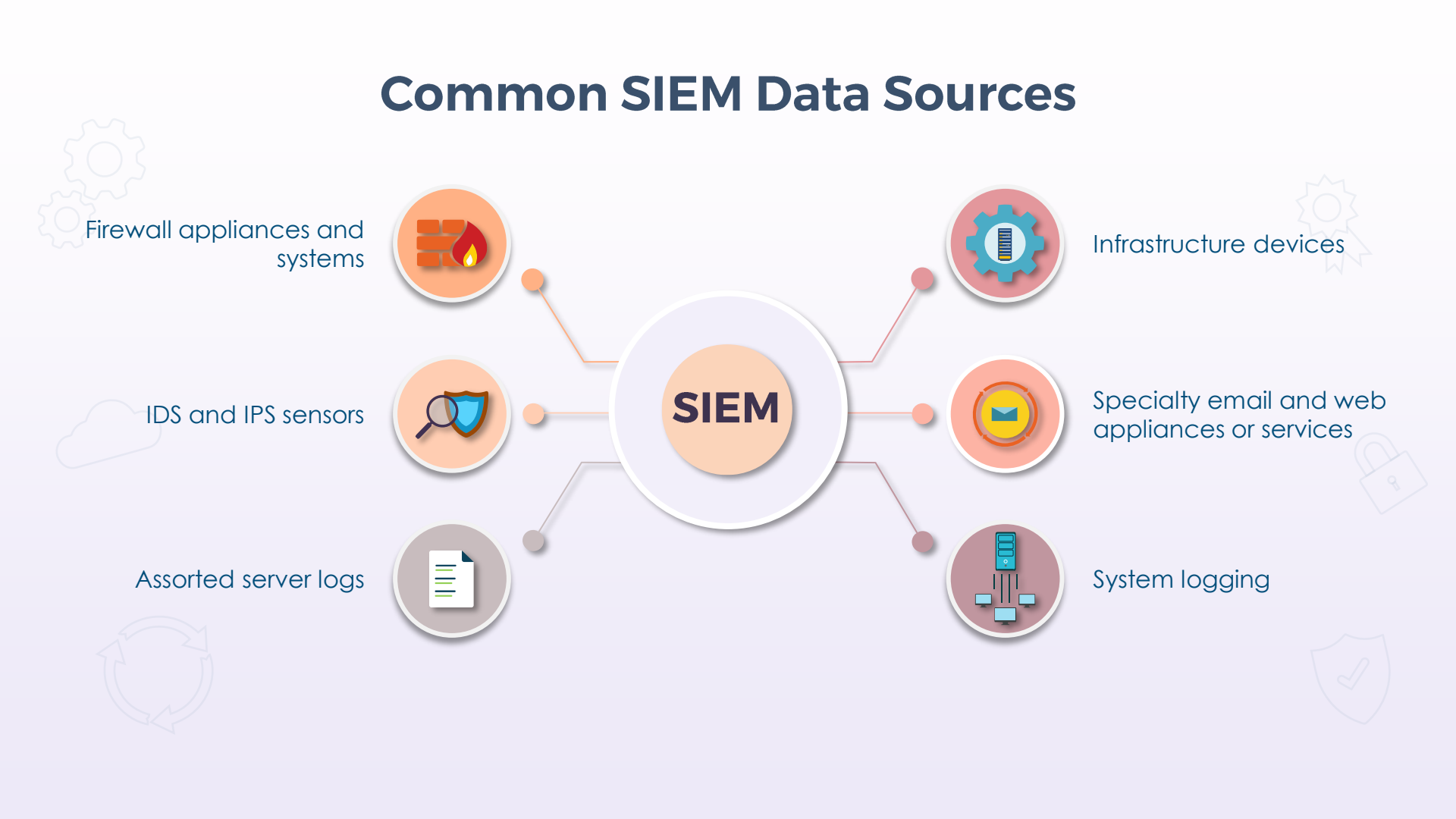
Monitoring with SIEM

- The term SIEM is a combination of security event management (SEM) and security information management (SIM)
- Centralizes the storage and analysis of logs and other security-related documentation to perform near real-time analysis
- Optionally sends filtered and processed data to mining, big query, and data warehousing servers in a data center or at a cloud service provider
- Allows security and network professionals to take countermeasures, perform rapid defensive actions, and handle incidents
- Microsoft Azure Sentinel is a cloud-based SIEM solution

SIEM Systems



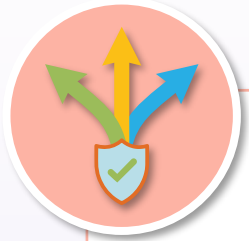
Common SIEM Data Sources



Automation vs. Orchestration

Automation

- IT automation involves generating a single task to run automatically without any human intervention
- Automation could involve sending alerts to a SIEM system, dynamically triggering a serverless function at a cloud provider, or adding a record to a database when a batch job is run
- Enterprises often automate both cloud-based and on-premises tasks



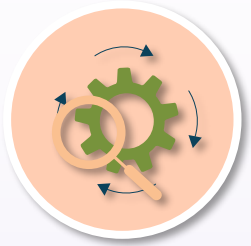
Orchestration

- Orchestration involves managing several or many automated tasks or processes
- As opposed to focusing on one task, orchestration combines all the individual tasks
- Orchestration occurs with various technologies, applications, containers, datasets, middleware, systems, and more

Security Orchestration, Automation, and Response (SOAR)

- SOAR is an assortment of software services and tools
- It allows organizations to simplify and aggregate security operations in three core areas:
  - Threat and vulnerability management
  - Incident response
  - Security operations automation

SOAR



Security automation involves performing security-related tasks without the need for human intervention

SOAR can be defensive detection, response, and remediation, or offensive vulnerability assessment and penetration testing

You should automate if the process is routine, monotonous, and time-intensive

Generating Reports

Meaningful metrics

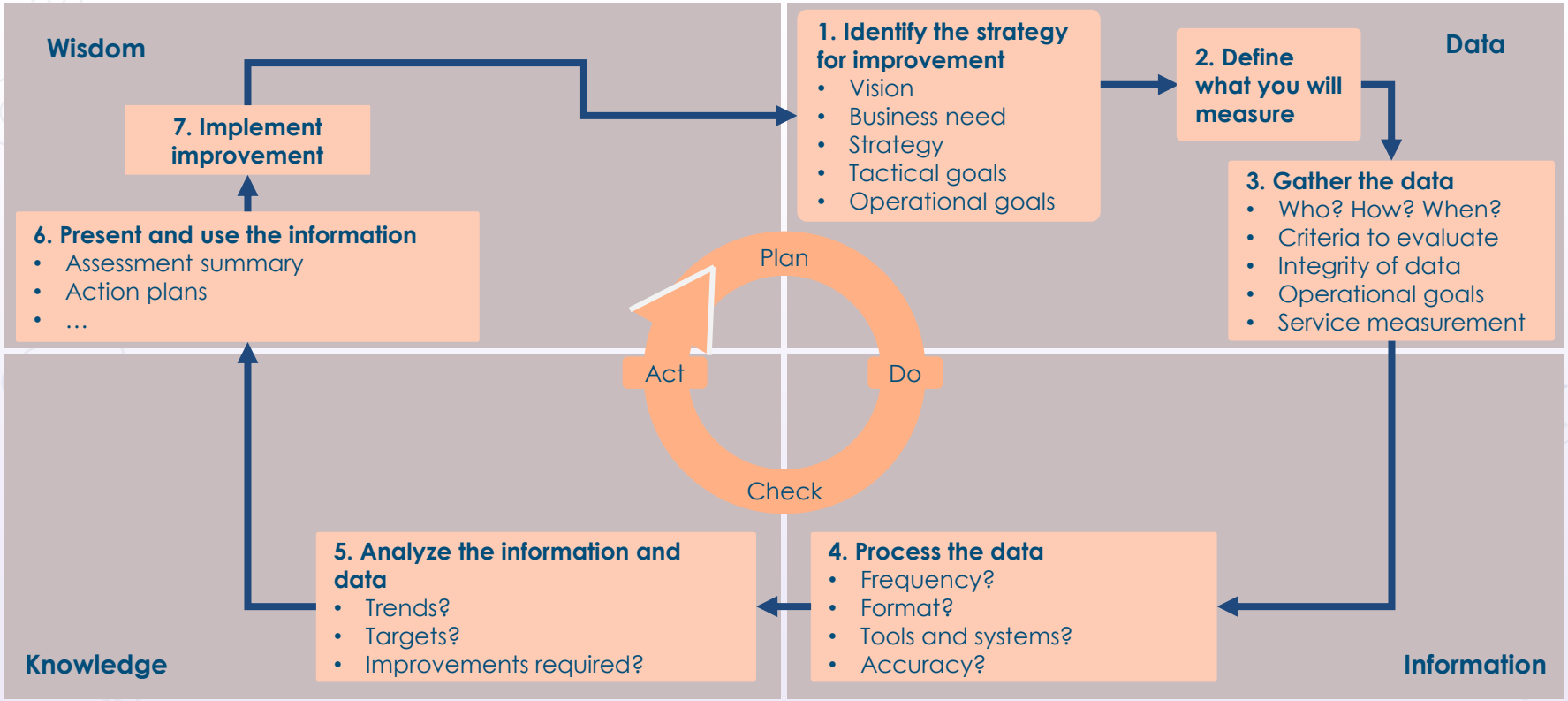
- Reports should have as much information as necessary but not a "data overload"
- May need to express in simpler terms or have different reports for different target audiences
- Dashboards are very effective (R programming)
- Understand components of visual communications
  - Avoid three-dimensional representation
  - Use a palette of sequential colors
  - Avoid pie charts for scatterplots, bars and bubble charts, histograms, density plots, and boxplots

Generating Reports

Utilize tools that deliver meaningful and digestible results

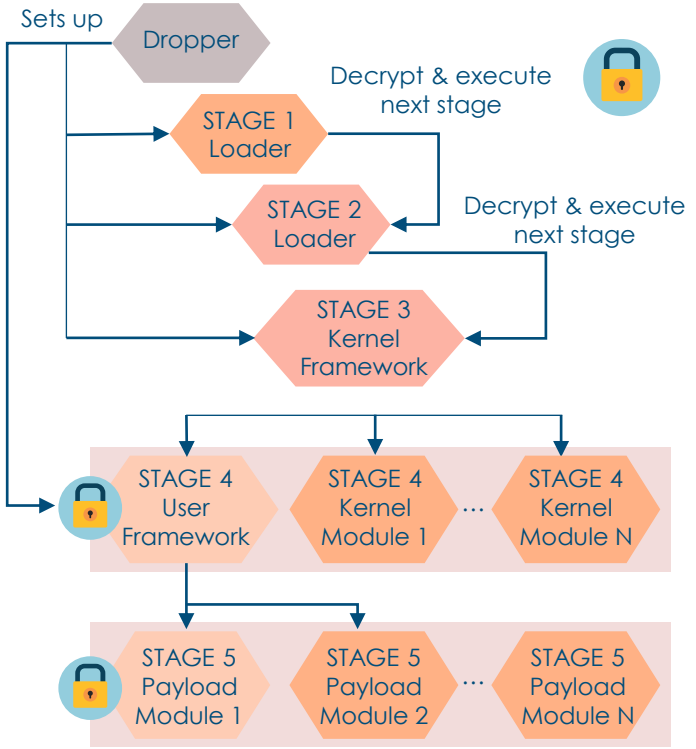
- CSP tools – CloudWatch, CloudTrail, Operations Insights
- Dashboards for visibility created with R programming and Python
- Automated system reports
- Written PDF summaries
- Engaging charts and graphs
- After-action reports including "lessons learned" sections

Continual Improvement Models Overlay



Threat Modeling

- Involves creating an abstraction of a system to identify risk and probable threats (private cloud/sandboxing)
- When cyberthreat modeling is applied to systems being developed, it can lower vulnerabilities and risk
- With the widespread adoption of threat intelligence technologies, most enterprises are trying to adopt a threat-focused approach to risk management
- Provides visibility, increased security awareness and prioritization, and understanding of posture



Threat Modeling Methodologies

Stride and PASTA are common threat modeling methods

STRIDE stands for: Spoofing of user identity, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation

It is a threat model initially developed by Microsoft in 1999 that classifies these attacker's prevalent goals

PASTA stands for Process for Attack Simulation & Threat Analysis

It is a risk-oriented method that endeavors to link business objectives to technical requirements

PASTA has seven stages with the goal of delivering a dynamic process ranging from identification and enumeration to scoring

Threat Modeling Methodologies

Trike and VAST are two other common modeling solutions along with DREAD

Trike is a technique frequently used as a risk management tool during security audits

It is a unique, open-source threat modeling method focused on enhancing the security auditing process from a cyber risk management perspective

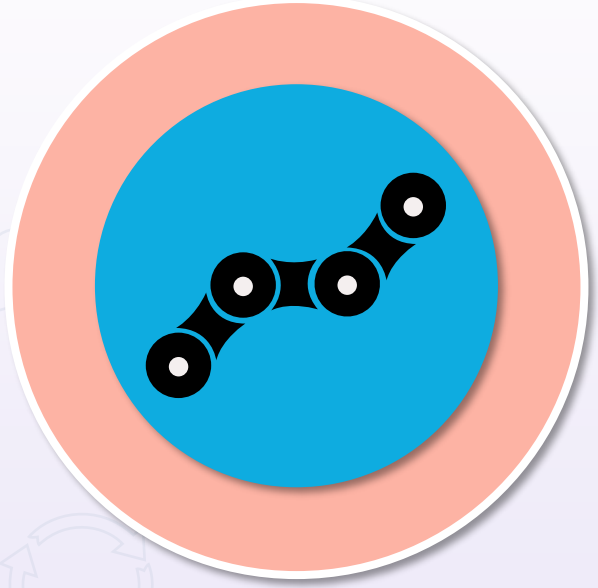
VAST is Visual, Agile, & Simple Threat Modeling

It attempts to address the limitations of other threat methodologies by using a more practical approach

Founding principle is that, in order to be effective, threat modeling must scale across the infrastructure and entire DevOps portfolio

It has separate operational and application models

Supply Chain Risk Management (SCRM)



- Challenge to modern supply chains is that several (thousands) of suppliers can contribute to a single product
- Many risks exist because vendors' employees can introduce cybersecurity vulnerabilities with hardware, software, and services
- Some tiers of the supply chain may be considered proprietary so that a lack of visibility impedes the security life cycle and this can make third-party assessment and monitoring more difficult

Supply Chain Risk Management (SCRM)

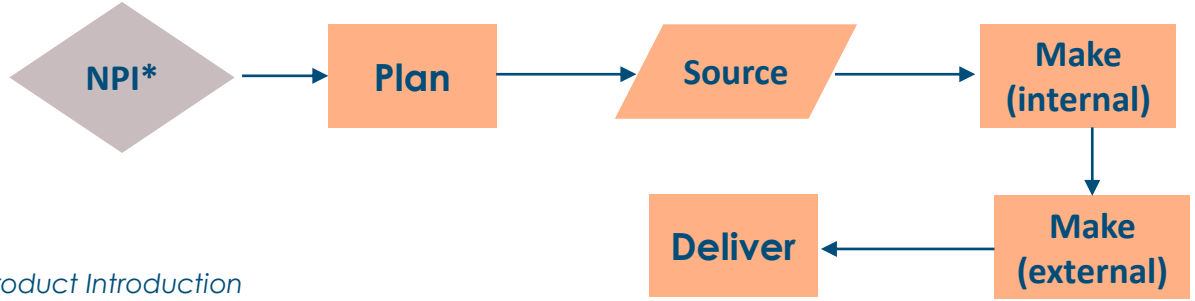
- Delivering meaningful metrics and analysis related to specific supply chain exposures
  - Cargo disruption trends
  - Transit modality exposure
  - Threats posed by terrorist/activist groups and other criminal elements
  - Country risk variables, such as the rule of law and the effectiveness of local law enforcement

Supply Chain Risk Management (SCRM)

- Governments continuously work with the trade community to manage and mitigate supply chain security risk
- US Customs and Border Protection (CBP) and Customs-Trade Partnership Against Terrorism (C-TPAT) programs
- Initiatives involve third-party assessment and monitoring and setting minimum security requirements and service-level requirements

SCRM Process

1. Identify and document risks
2. Create a supply-chain risk management framework
3. Monitor risk using customized tools
4. Implement governance and regular audits
5. Manage unknown risks by building strong defense-in-depth in a security-aware culture



*New Product Introduction

Symmetric Key Algorithms

- Same secret key is used for encryption and decryption
- Secret key must be shared between sender and receiver securely
- Strength is related to management and size of keys and how they are shared
- Key is typically from 40 to 512 bits in length
- Longer keys are less susceptible to a successful brute force attack

Symmetric Key Algorithms

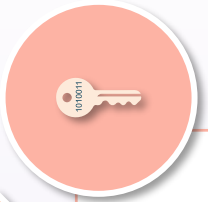
- Provide wire-speed encryption
- Used for bulk data encryption (e.g., VPNs and CMKs at a CSP)
- Deploy confusion and diffusion techniques
- Can be accelerated by hardware
- Use stream and block ciphers (most often)

Symmetric Modes

ECB (Electronic Codebook)

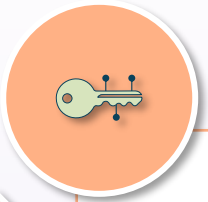
The simplest mode, where each block of data is simply encrypted with the same key

Rarely used anymore



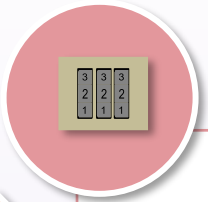
CBC (Cipher Block Chaining)

CBC improves on ECB by making the encryption of each block dependent on ciphertext of the previous block



CTM (Counter Mode)

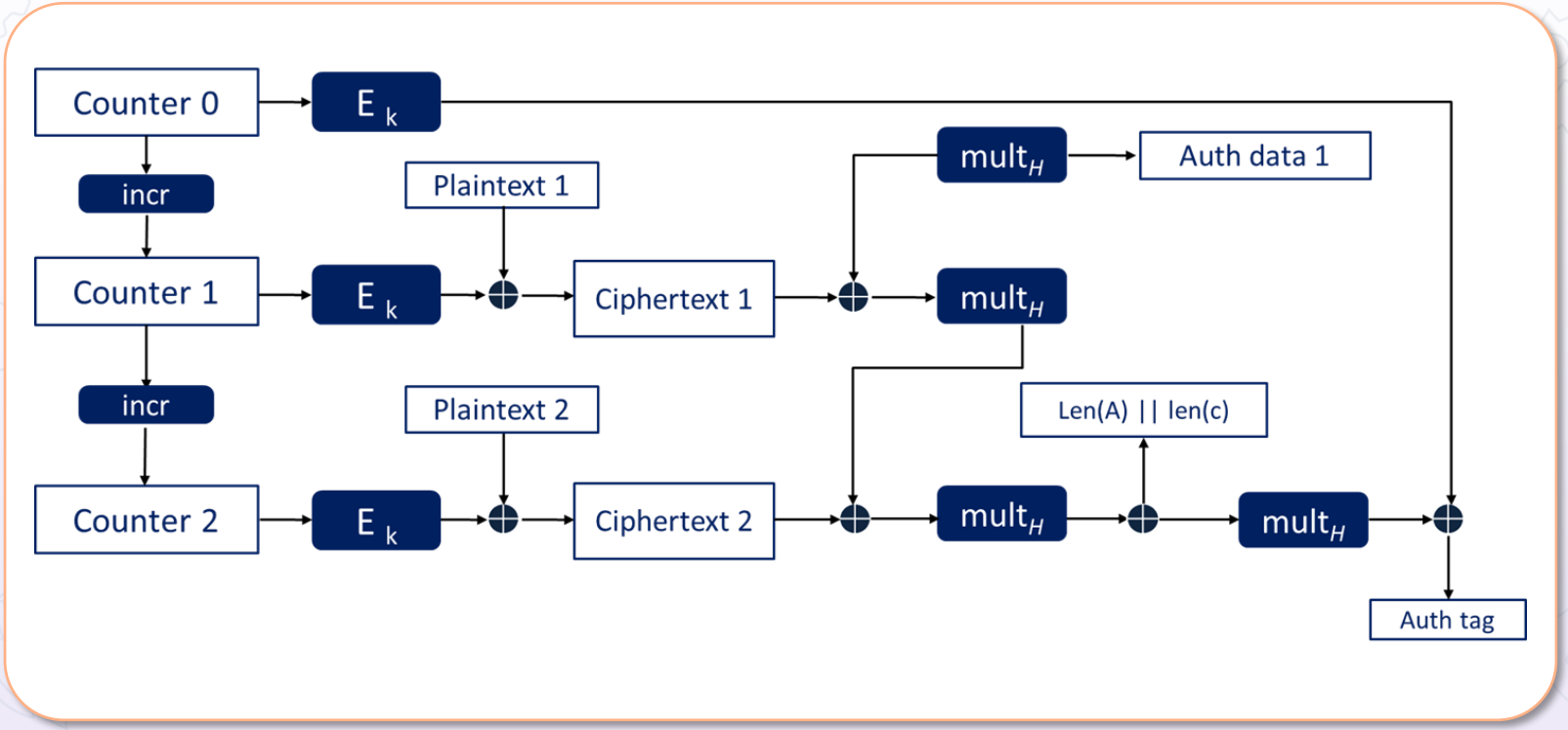
CTM generates the next keystream block by encrypting successive values of a counter



GCM (Galois Counter Mode)

Authenticated encryption mode that concurrently combines confidentiality, authenticity, and integrity

Galois Counter Mode (GCM)

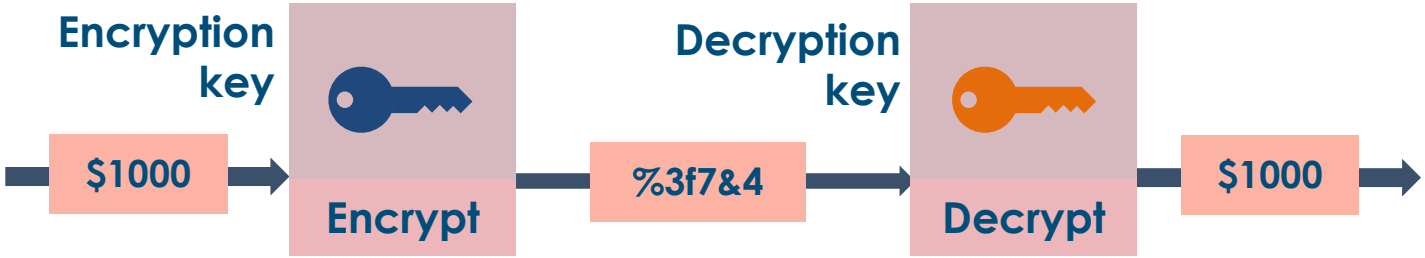


Advanced Encryption Standard (AES)

- AES became effective as a federal government standard on May 26, 2002, after approval by the Secretary of Commerce
- AES is included in the ISO/IEC 18033-3 standard
- It is available in many different encryption packages and is the first (and only) publicly accessible cipher approved by the NSA for top secret information when used in an NSA-approved cryptographic module

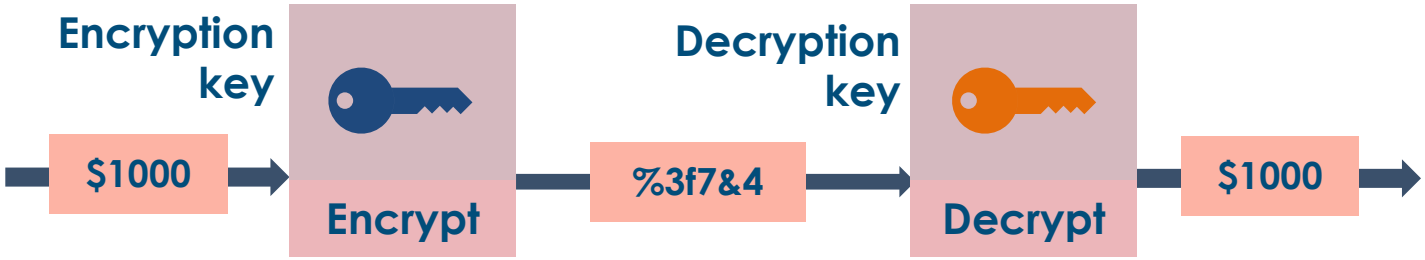
Asymmetric Key Algorithms

- Different keys are used for encryption and decryption
- They are generated together and mathematically related
- The public key is shared with many
- The private key is kept secret by owner
- Keys range from 512 to 4,096 bits in length



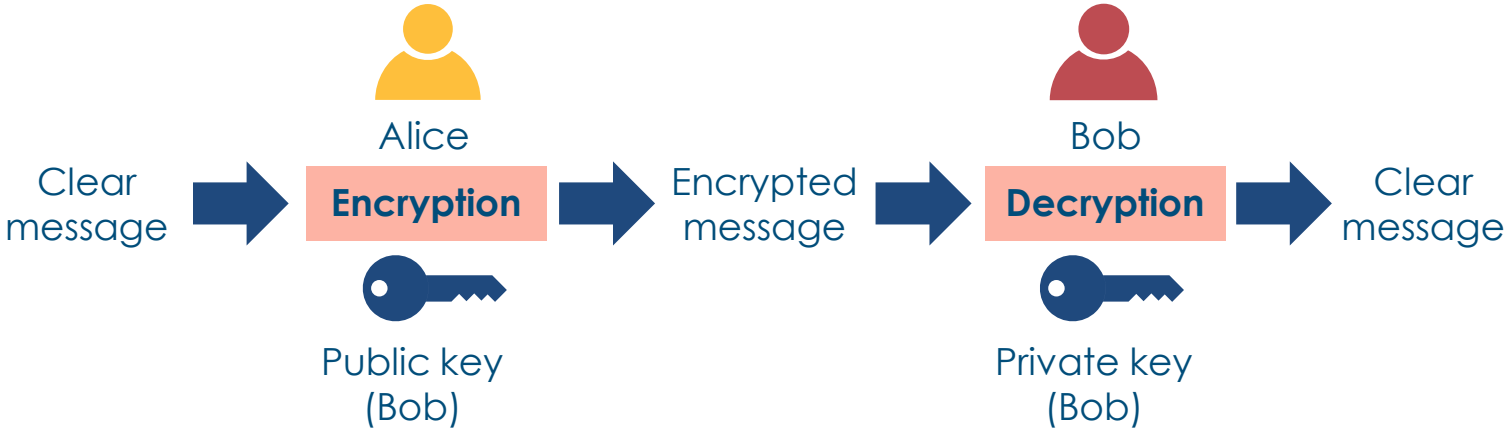
Asymmetric Key Algorithms

- Slower (not suitable for bulk data encryption)
- Design is based on factoring the product of large prime numbers
- Key management is simpler and more secure
- Best suited for digital signatures and session key exchange or agreement protection services
- RSA (most popular commercial), DSA, Elliptic curve DSA, PGP/GPG, Diffie-Hellman



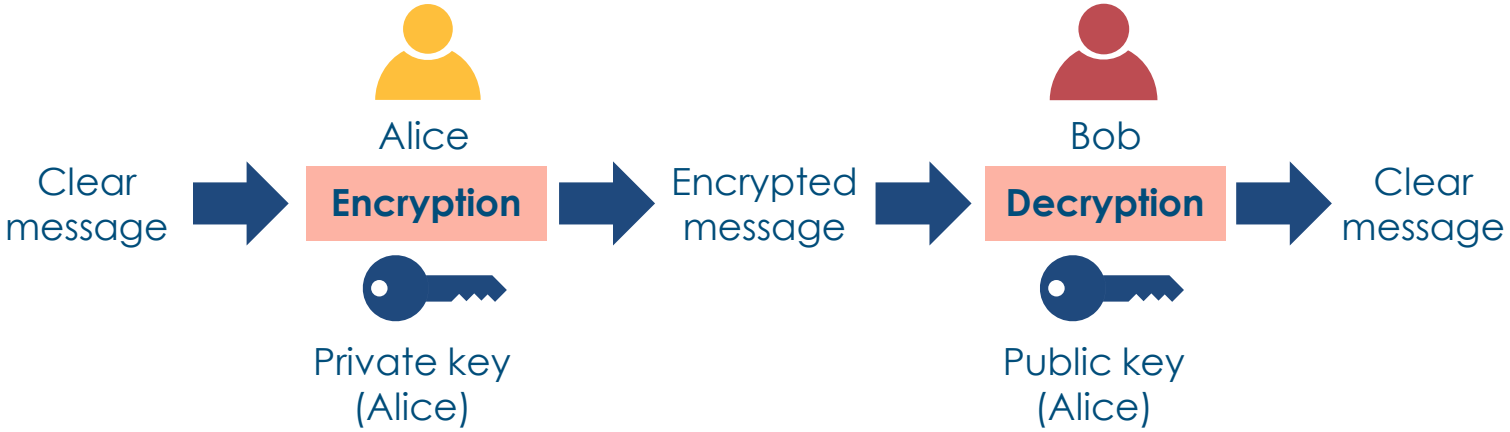
Asymmetric Key Algorithms

Privacy (confidentiality) = Alice encrypts with Bob's public key, then Bob decrypts with his private key



Asymmetric Key Algorithms

Origin authentication = Alice encrypts with her private key, then Bob decrypts with Alice's public key



Diffie-Hellman Key Exchange

- The first key agreement asymmetric algorithm used for generating shared secret keys over an untrusted channel
- Once the two parties securely develop shared secrets, then they can use the keys to derive subsequent keys
- These keys can then be used with symmetric-key algorithms to transmit information in a protected way

Diffie-Hellman Key Exchange

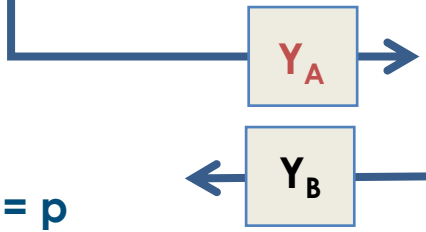
- DH can also be used to establish public and private keys; however, RSA tends to be used instead
- The RSA algorithm is also capable of signing public-key certificates, whereas the Diffie-Hellman key exchange is not
- DH is used by TLS, IPsec, SSH, PGP, and many others

Diffie-Hellman Key Exchange

Private value, X_A

Private value, Y_A

$Y_A = g^{X_A} \bmod p$



$(Y_B^{X_A}) \bmod = p$

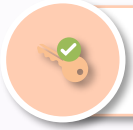
Private value, X_A

Private value, Y_A

$Y_A = g^{X_A} \bmod p$

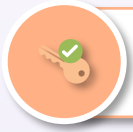
$Y_B = g^{X_B} \bmod p$

Diffie-Hellman Groups

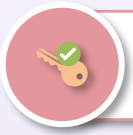


Diffie-Hellman group 14: 2048-bit modulus – MINIMUM ACCEPTABLE

Diffie-Hellman group 19: 256-bit elliptic curve – ACCEPTABLE



Diffie-Hellman group 20: 384-bit elliptic curve – Next Generation Encryption



Diffie-Hellman group 21: 512-bit elliptic curve – Next Generation Encryption

DH group 24: Modular exponentiation with a 2048-bit modulus and 256-bit prime order subgroup – Next Generation Encryption

Diffie-Hellman Modes

DH (Diffie-Hellman)

Same shared secret used all the time between parties

Original DH by itself does not provide authentication of the communicating parties

DHE/EDH (Ephemeral Diffie-Hellman)

Different shared secret used each time between parties

A cryptographic key is called "ephemeral" if it is generated for each execution of a key establishment process

ECDH (Elliptic-curve Diffie-Hellman)

Uses EC public/private key pair

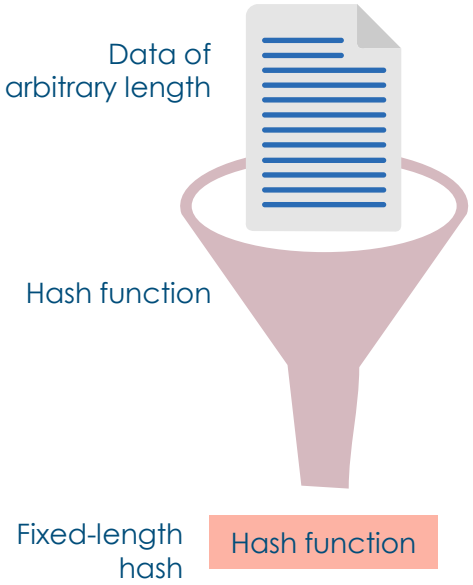
The same shared secret is used all the time between parties

ECDHE/ECEDH (Elliptical-curve Ephemeral Diffie-Hellman)

Uses EC public/private key pair

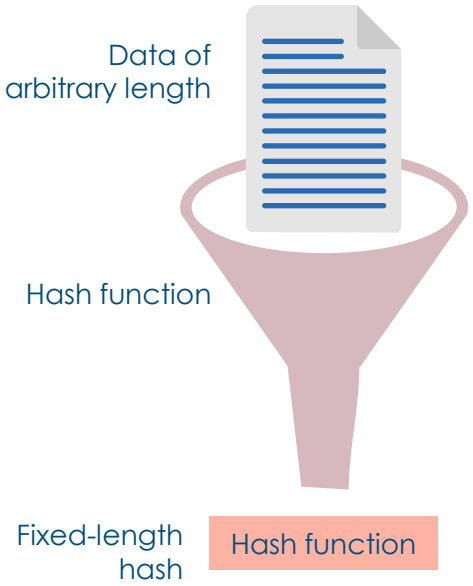
A different shared secret is used each time between parties

Cryptographic Hashing



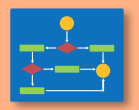
- Also known as hash value, message digest, fingerprint, checksum
- Hashing maps data of any size to a fixed-length string (SHA 256 bits)
- Produces a digest 128 to 512 bits in length
- It is an irreversible one-way mathematical function

Cryptographic Hashing



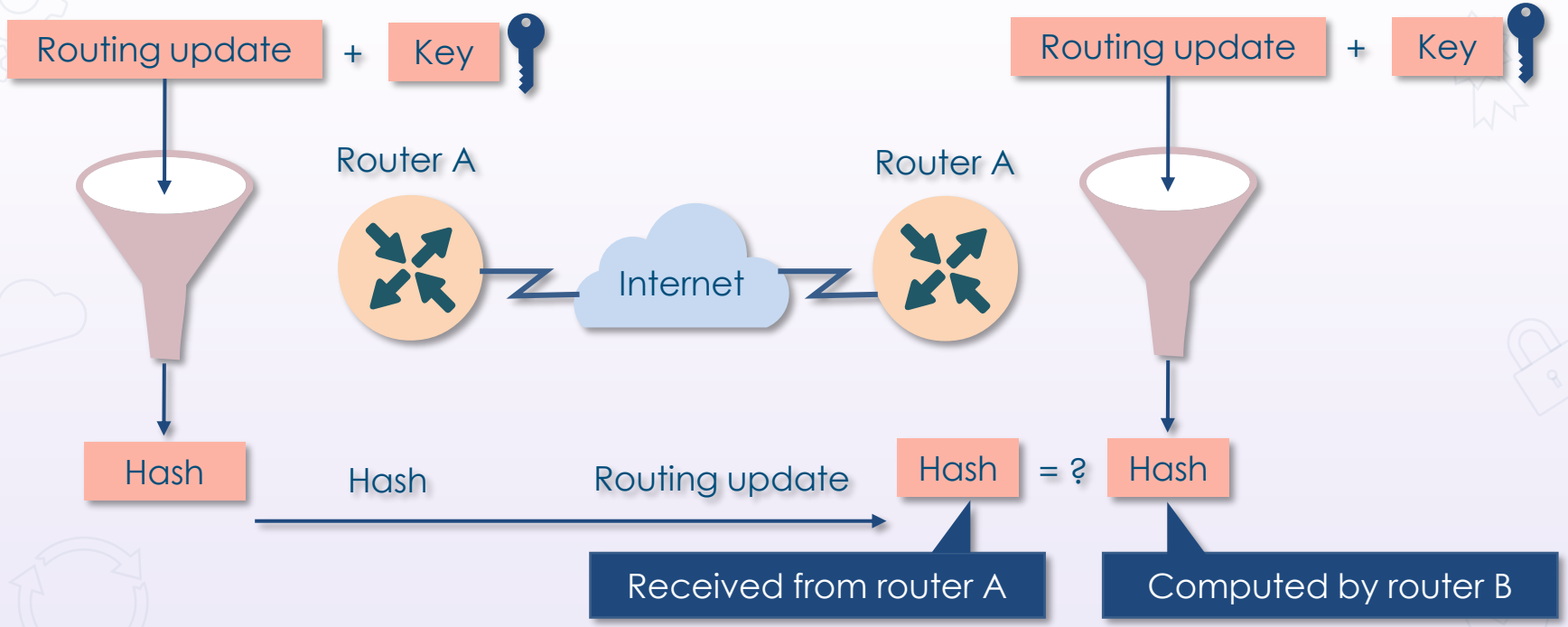
- Unfeasible to generate original from hash value
- Deterministic and quick to compute
- A small change results in the avalanche effect
- No two message inputs should generate the same hash value (collision)

Hashing Algorithms

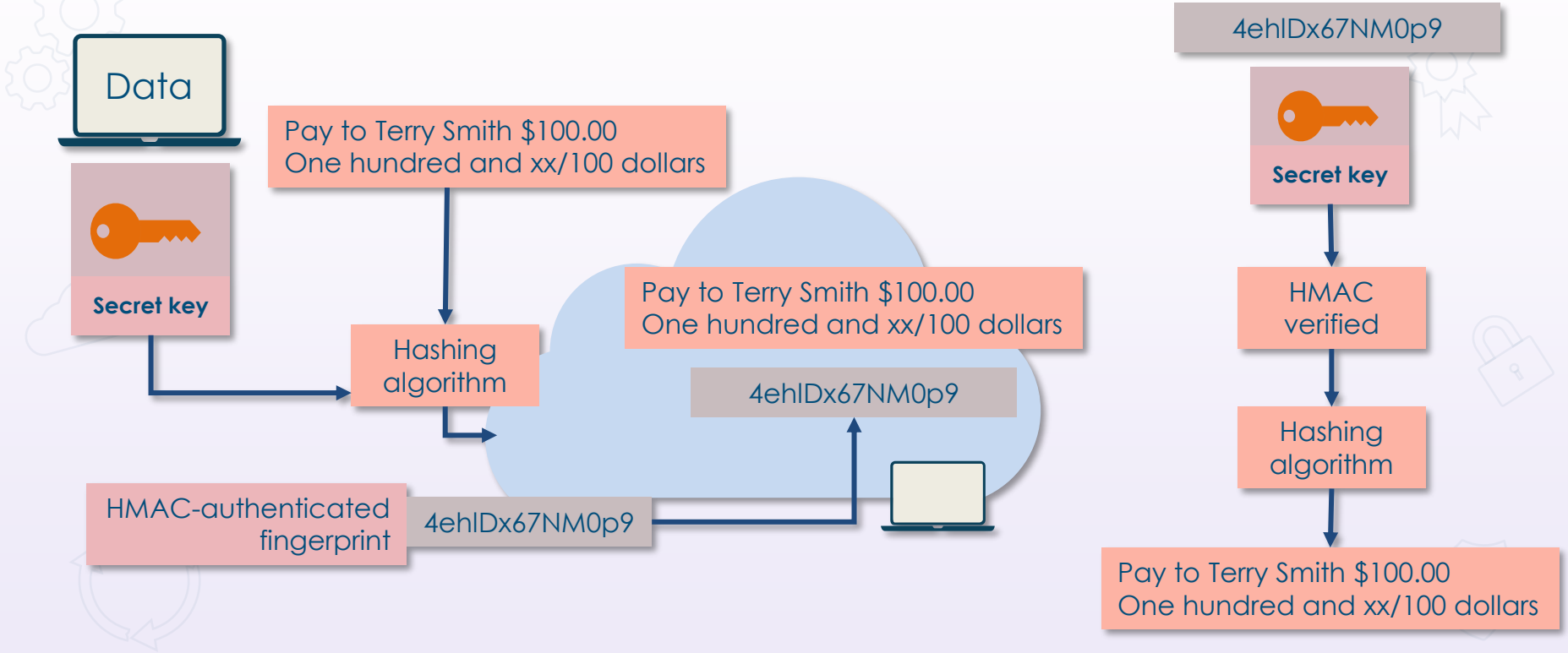


- MD5 (128-bit digest produced)
- Has been deprecated
- SHA-1 (160-bit digest produced)
- SHA-2 (256-bit)
- SHA-3 (not meant to replace SHA-2)
- RACE Integrity Primitives Evaluation Message Digest (RIPEMD) with 128-, 160-, 256-, and 320-bit versions

HMAC for Integrity and Origin Authentication



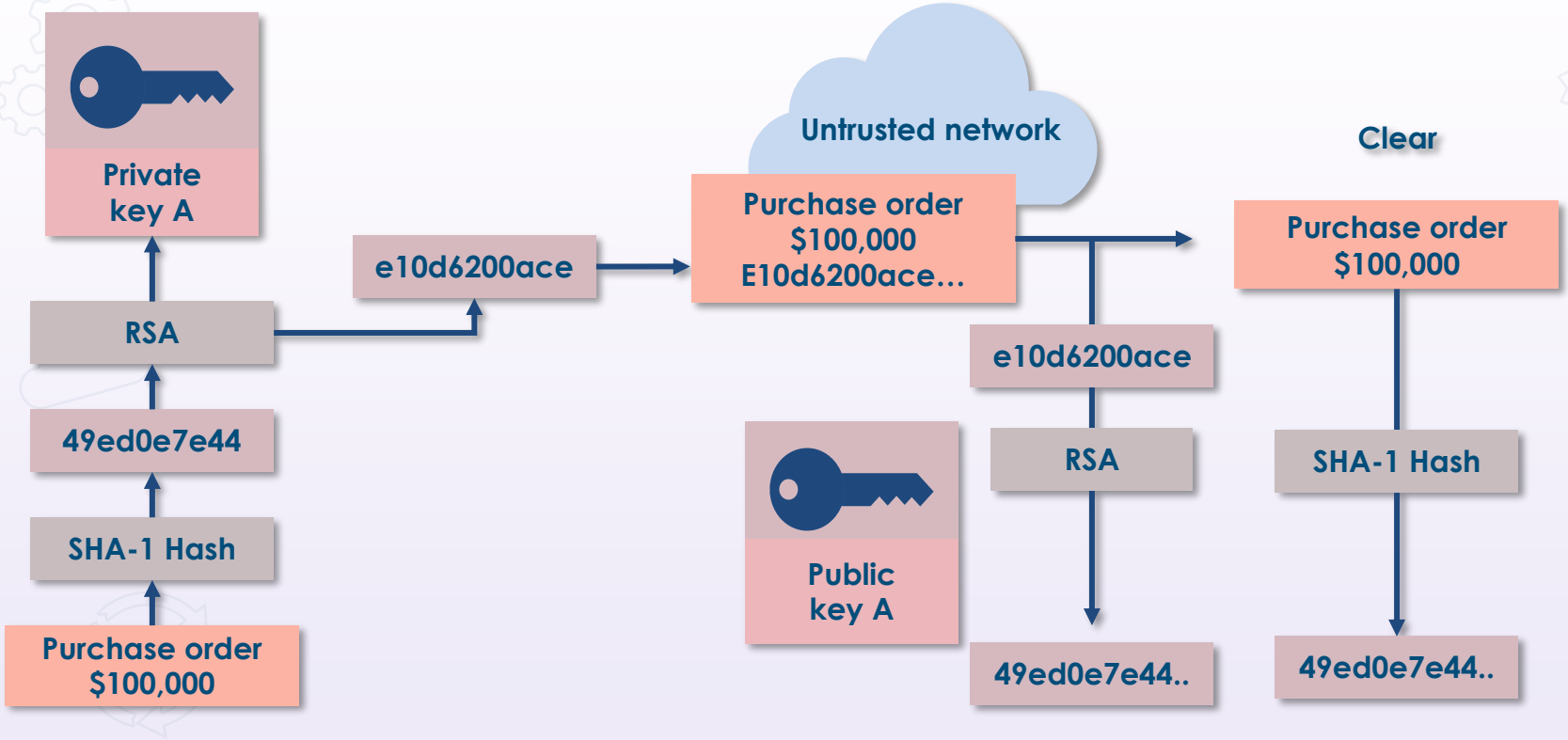
HMAC for Integrity and Origin Authentication



Digital Signatures

- Are a form of electronic signature that was designed to replace and/or augment a physical handwritten signature
- Are a mathematical algorithm commonly used to validate the authenticity and integrity of a message, such as an email, a credit card or online transaction, or some form of digital document
- Generate a virtual fingerprint that is unique to an entity and used to identify users and protect information in digital messages or documents
- Digital signatures are more secure than other forms of electronic signatures

Digital Signatures



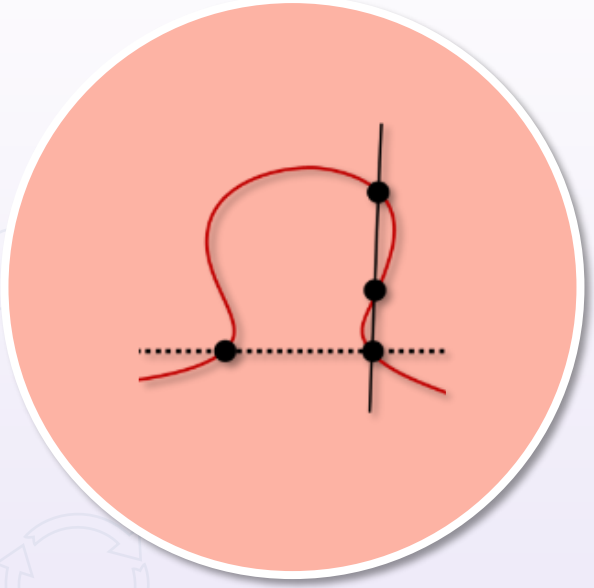
Digital Certificates

- A digital certificate is a form of file used to tie cryptographic key pairs to entities such as individuals, web sites, or organizations
- If public trust is needed, then a trusted Certificate Authority (CA) will assume the role of a third party to validate, identify, and associate them with cryptographic pairs using the digital certificates
  - The key pair consists of a public key and a private key
  - The public key is included in the certificate, while the private key is kept secure
  - The owner of the private key can then use it to sign documents, and the public key can be used to verify the validity of those signatures

Digital Certificates

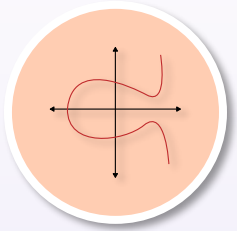
- A common format for digital certificates is based on the X.509 standard, which consists of the following:
  - A public key
  - A digital signature
  - Other metadata (serial number) about the entity linked to the certificate, such as a serial number
  - Information about the issuing CA

Elliptic Curve Cryptography



- Rich math functions based on points on a curve
  - The algorithm computes discrete logarithms of elliptic curves, which is different from calculating discrete logarithms in a finite field
- The smaller and more efficient keys offer exceptional speed and strength (e.g., a 256 elliptic curve key equals a 3,072 normal key)
- Used in digital signatures, key distribution, and encryption
- Excellent for mobile devices and IoT

Elliptic Curve Cryptography



There are two common public applications of EC

Elliptic Curve Digital Signature Algorithm (ECDSA)

This introduces a variant of the Digital Signature Algorithm (DSA) by utilizing elliptic curve cryptography

There exists political and technical concerns with ECDSA

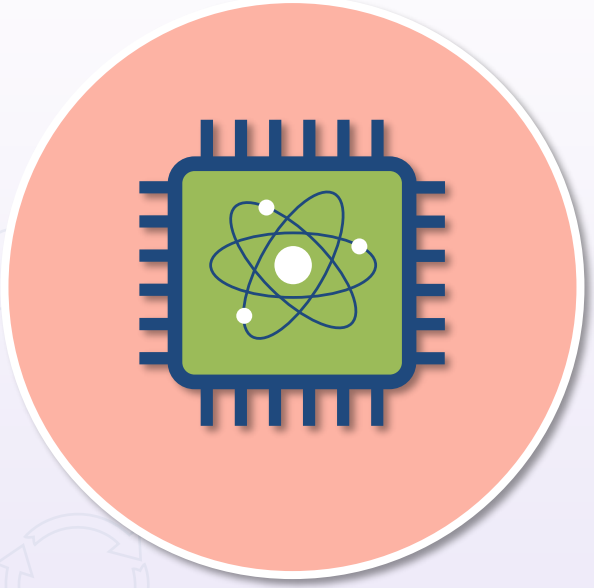
Elliptic-curve Diffie–Hellman (ECDH)

A key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to generate a shared secret over an insecure channel

This shared secret may be directly used as a key or to derive another key

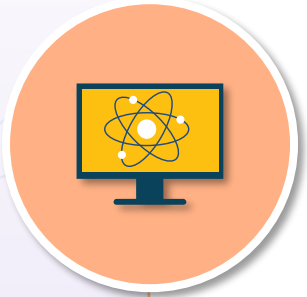
The key (or the derived key) can then be used to encrypt successive communications using a symmetric-key cipher

Quantum Computing



- Personal computers use bits (1s or 0s) whereas quantum computers use qubits
- These are typically subatomic particles, such as electrons or photons
- Quantum computing derives its power from the fact that qubits can represent numerous possible combinations of 1 and 0 at the same time
- This ability to simultaneously be in multiple states is called superposition

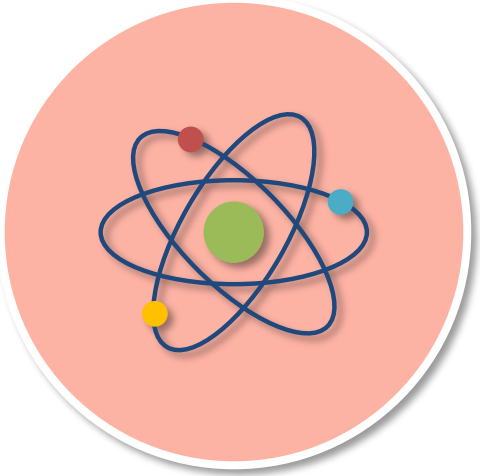
Post-quantum Computing



- Post-quantum cryptography involves developing new cryptosystems that can be implemented using today's existing computers but that will be resistant to attacks from tomorrow's quantum computers
  - Increase the size of digital keys
  - Develop more complex trapdoor functions
  - Lattice-based cryptography
  - Supersingular isogeny key exchange

Quantum Communications

Quantum physics and computing

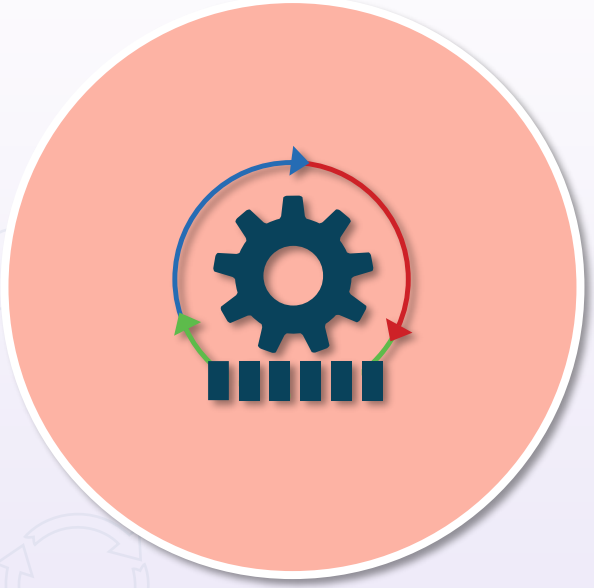


- Quantum communication leverages the laws of quantum physics and quantum computing to protect data
- Some organizations are transmitting highly sensitive data using quantum key distribution (QKD)
- QKD sends encrypted data as normal bits over the network, while the decryption key information is encoded and transmitted in a quantum state using qubits
- These networks are theoretically ultra-secure

Homomorphic Encryption

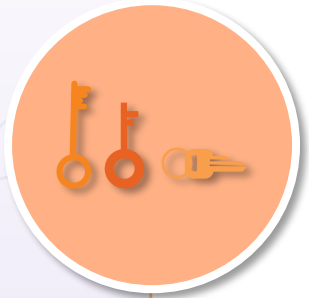
- Helps to protect data-in-use
- Data remains encrypted while being processed
- CSPs can apply functions on encrypted data
- Commonly uses public/private keypair
- Uses algebraic operations on ciphertext

Key Generation



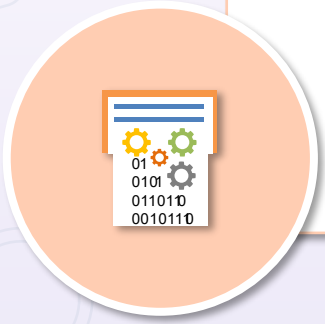
- Keys can be generated through the key manager or by a trusted third party, which must use a cryptographically secure random bit generator
- The keys, along with all their attributes, will then be stored in the key storage database (which must be encrypted by a master key)
- Attributes include name, activation date, size, and instance
- A key can be activated upon its creation or set to be activated automatically or manually later

Key Distribution and Loading



- The objective is to install the new key into a secure cryptographic device, either manually or electronically
- For manual distribution, keys must be distributed and loaded in key shares to avoid the full key being viewed in the clear
- When symmetric keys are installed, it is recommended that they be encrypted by a public key or key-encryption key prior to being delivered for deployment
- The key should be deployed and tested for a certain time period to ensure that operations are successful in order to avoid any potential data loss or theft

Key Backup and Storage



- In order to recover a key that has been lost during its use, a secure backup copy should be made available
- Backup keys can be stored in a protected form on external media (CD, USB drive, etc.), a hardware security module (HSM), or by using an existing traditional backup solution (local or networked)
- When a symmetric key or an asymmetric private key is being backed up, it must also be encrypted and stored

Normal Use and Replacement

- The key management system should allow an activated key to be retrieved by authorized systems and users
- It should also effortlessly manage current and past instances of the encryption key
- The key manager will replace a key automatically through a previously established schedule or if it is suspected of compromise
- When replacing keys, the goal is to bring an extra key into active use by the system and to convert all stored, secured data to the new key

Archiving Keys

- Archival refers to off-line long-term storage for keys that are no longer in operation
- Long-term storage (i.e., Gemalto HSM or CloudHSM)
- These keys usually have data associated with them that may be needed for future reference, such as long-term storage of emails
- There may also be associated data in other external systems
- When archiving a key, it must be encrypted to add security
- Before a key is archived, it should be proven that no data is still being secured with the old key

Key Disposal

Also called "disposition"

- The last phase is the end of the key's life cycle, where all instances, or certain instances, are completely removed
- The end of life for a key should only occur after an adequately long Archival phase and after adequate analysis to ensure that loss of the key will not correspond to loss of data or other keys
- There are three ways to remove a key from operation:
  - Key destruction
  - Key deletion
  - Key termination

Key Stretching

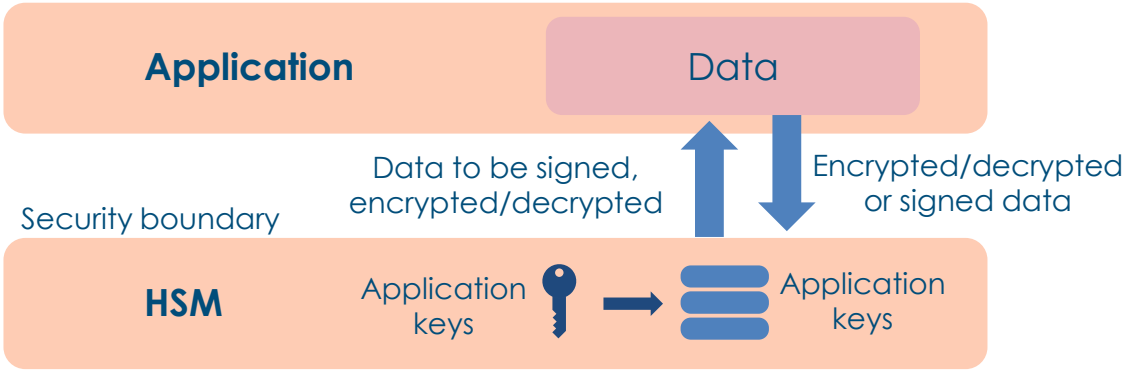
- Lengthens symmetric keys to at least 128 bits
- An initial key (password or passphrase) is fed into algorithm and an enhanced key is produced after many iterations
- Increases the time it takes to perform brute-force attack on key
- Common algorithms are Bcrypt and PBKDF2

Key Escrow

- **Third party has copy/access to private keys**
  - Only allowed access under strict conditions – for example, a court order
- **Issues can arise:**
  - The request for access process
  - The legitimacy of request
  - Granting the access
  - How many systems are not vulnerable?

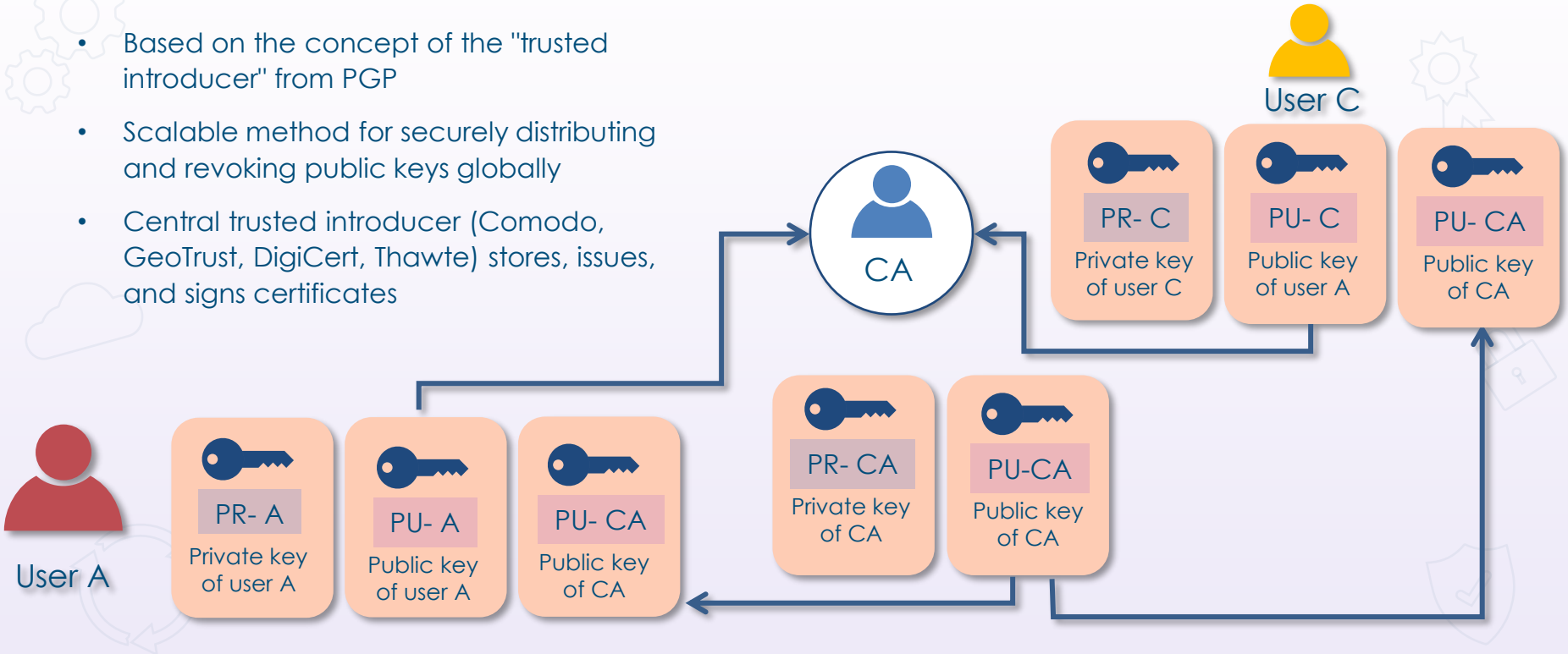
Hardware Security Module (HSM)

- Uses tamper-proof, hardened devices to provide crypto processing and protection of cryptographic keys and functions
- Involves partitioned administration and security domains
- Applies corporate key use policies
- Can be used in place of software crypto libraries and accelerators



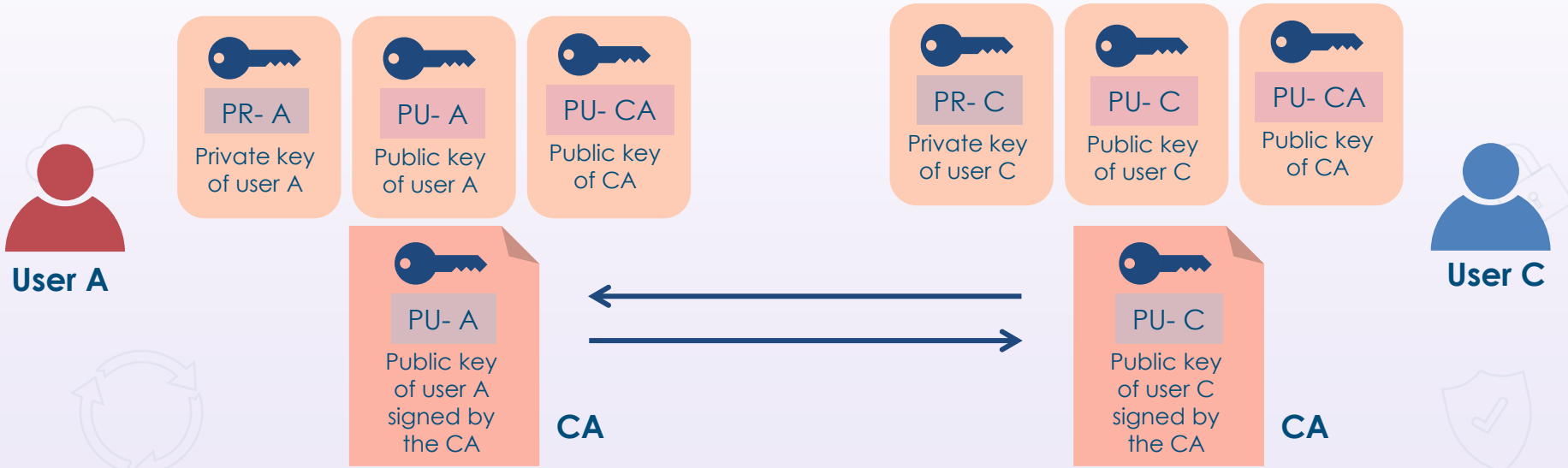
Public Key Infrastructure

- Based on the concept of the "trusted introducer" from PGP
- Scalable method for securely distributing and revoking public keys globally
- Central trusted introducer (Comodo, GeoTrust, DigiCert, Thawte) stores, issues, and signs certificates



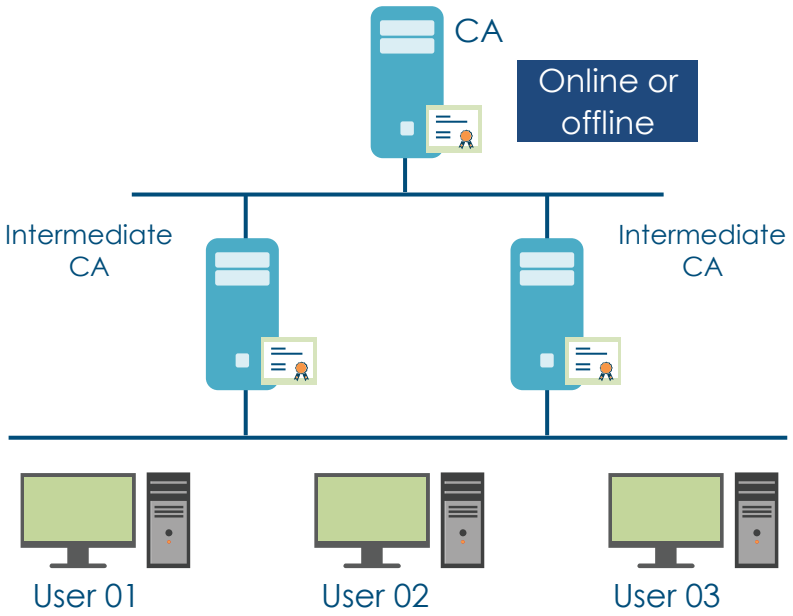
Public Key Infrastructure

- Certificates can now be exchanged over untrusted networks as the certificates/public keys of entities are now verified with the public key of a CA
- Two public key algorithms are involved: the one within the certificate, the subject's public key algorithm (e.g., some 160-bit elliptic curve mechanism) AND the one that was used to SIGN the certificate (like RSA 2048)



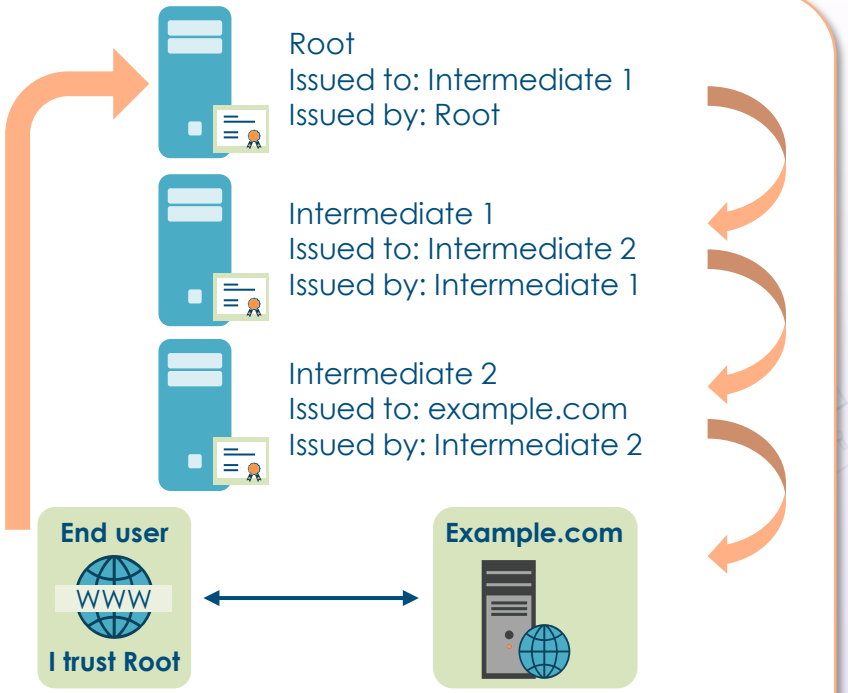
Hierarchical CA Trust Models

- Root provides certificate to intermediate CAs
- Intermediate CAs provide certificates to users or other intermediate CAs
- Root can be online or offline
  - Online – connected to network
  - Issues certificates over the network
  - Offline – not connected to network
  - Issues certificates on removable media



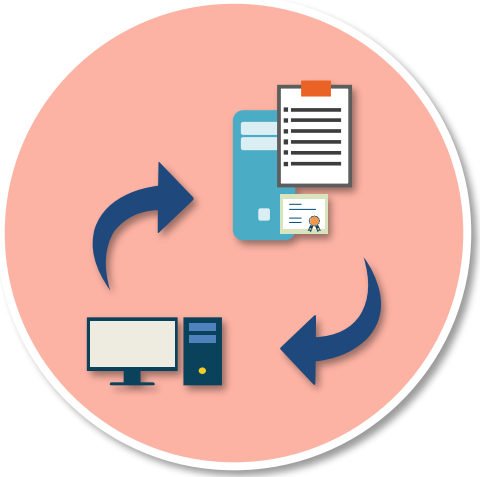
Certificate Chaining

- This is referred to as trust delegation, where each CA signs the public key of the CA one level below
- Alternatively, it is very common for CAs to cross-certify each other without some strict hierarchical relationship being in place
- The CA must be in trusted store, but it's not possible to include all CAs
- Chain of trust is established by
  - "Issued To" field, and
  - "Issued By" field



Expiration, Revocation, Suspension

Certificate Revocation List (CRL)



- Original method using a list of certificates that are invalid based on serial numbers
- Issued by the CA who granted the certificate
- Generated and published periodically
- Defined intervals or immediately - not real-time
- Downloaded by client regularly but also not in real-time
- Suspension of a certificate does NOT place the serial number on the CRL

Expiration, Revocation, Suspension

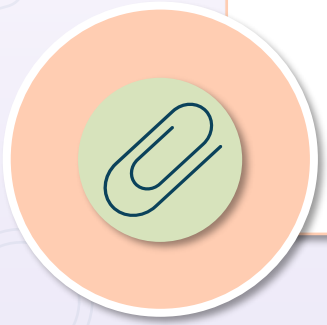
Online Certificate Status Protocol

- OCSP is a method for a web browser to determine the validity of an SSL/TLS certificate by verifying with the vendor of the certificate
- An online transactional database of serial numbers that is generated and published immediately
- Clients query database anytime, although many will bypass
- OCSP improves security, but causes websites to load slower

OCSP Stapling

- OCSP stapling is a method for quickly and safely determining whether a TLS server certificate is valid
- Stapling involves the web server downloading a copy of the vendor's response, which it can then deliver directly to the browser or other web client
- The web server can provide information on the validity of its own certificates instead of requesting the information from the certificate's vendor

OCSP Stapling



- A status_request_extension in TLS 1.2+ is used by the web client to indicate support for this feature
- The TLS server will send fresh certificate information in the TLS handshake
- Supports only one OCSP response and is used to check the status of the server certificate only

Certificate Pinning

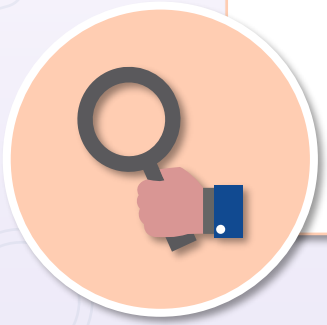
- A security method for associating a service with certificates and public keys
- Offers three key improvements:
  - Reduces the attack surface by letting owners pin the CAs that are allowed to issue certificates for their domain names (Google preloaded public key pinning for most of their sites in Chrome 13 browsers)
  - Provides key continuity without relying on public CAs
  - Pinning can be used for authentication using a secure channel

Cryptanalysis

- Cryptanalysis is the study and practice of exploiting weaknesses in communication protocols and cryptosystems
- Most known methods, like brute force, are ineffective on most modern cryptographic algorithms due to
  - lack of time
  - lack of computing power, and
  - good key management and life cycles
- Most weaknesses are found in the implementation and key management as opposed to the algorithm itself

Classical Cryptanalysis

- Classical cryptanalysis typically involves 2 disciplines:
  - Mathematical analysis that involves analytical attacks which exploit the internal structure of the encryption methods
  - Brute-force analysis, which treats the algorithm as a black box and tries all possible keys in the keyspace



Implementation Attacks

- The most common is a side-channel attack where one measures the electrical power consumption of a processor operating on a secret key
- The power trace is used to determine "0s" and "1s" and ultimately give information about plaintext or keys
- Typically needs physical access, such as Smart Card

Social Engineering

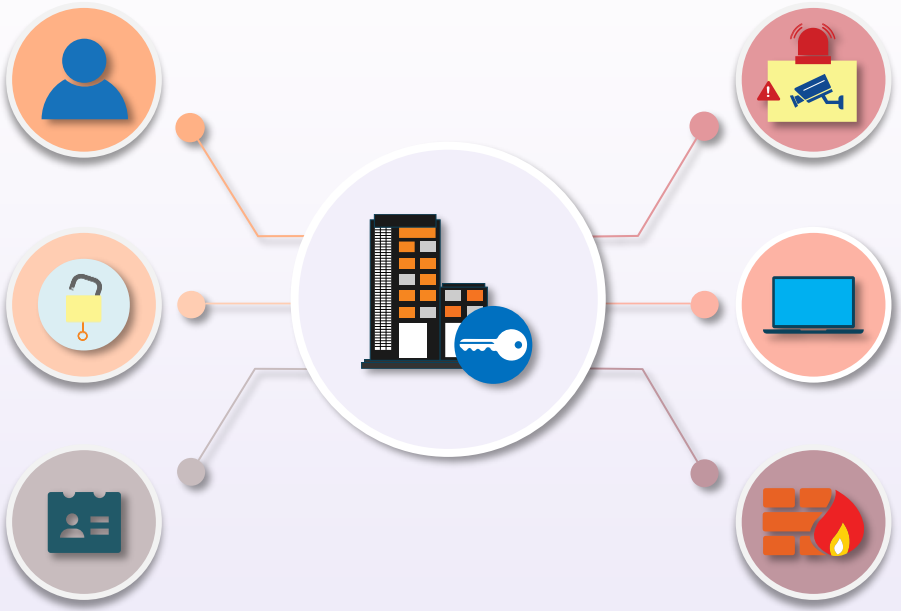
- Involves the exploitation of human weaknesses by leveraging the ability to trick, coerce, or extort a subject for information
- Involves spoofing, hoaxing, shoulder surfing, dumpster diving, phishing attacks, and more
- Most attackers will attempt to find vulnerabilities through social engineering before using other methods

Attacking RSA

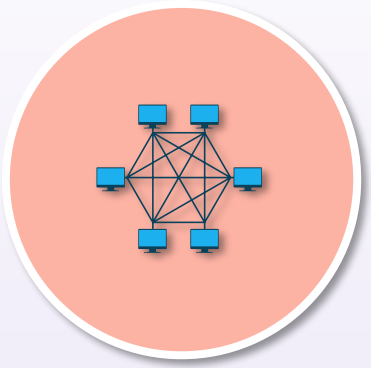
- Protocol attacks – exploit weaknesses in the way RSA is used
  - Padding and proper implementation mitigate these
- Mathematical attacks
  - Best example is factoring the modulus
  - Although 1024-bit RSA is adequate, a modulus of 2048-4096 bits is highly recommended today
- Side-channel attacks
  - Information about the private key is leaked via physical channels, such as power consumption (SPA) and timing behavior

Controlling Physical Access

Controlling Physical Access

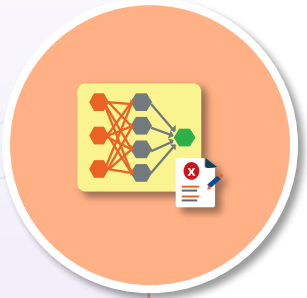


Controlling Logical Access



- IPsec and SSL/TLS VPN gateways
- IEEE 802.1X (PNAC)
- Identity and access management MFA
- Identity providers (AD and Kerberos)
- Access keys and secure logical tokens (JSON)

Fundamental Concepts of Security Models



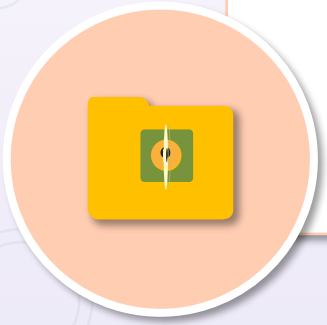
- Security models are used to decide which subjects can access particular objects – the specification of a security policy
- Typically implemented by enforcing integrity, confidentiality, origin authentication, and nonrepudiation controls
- Designer determines how the models will be used and integrated into specific designs
- May be done by individual or committee
- Security is best enforced with a multilevel or hierarchical security system

Bell-LaPadula Model

Confidentiality

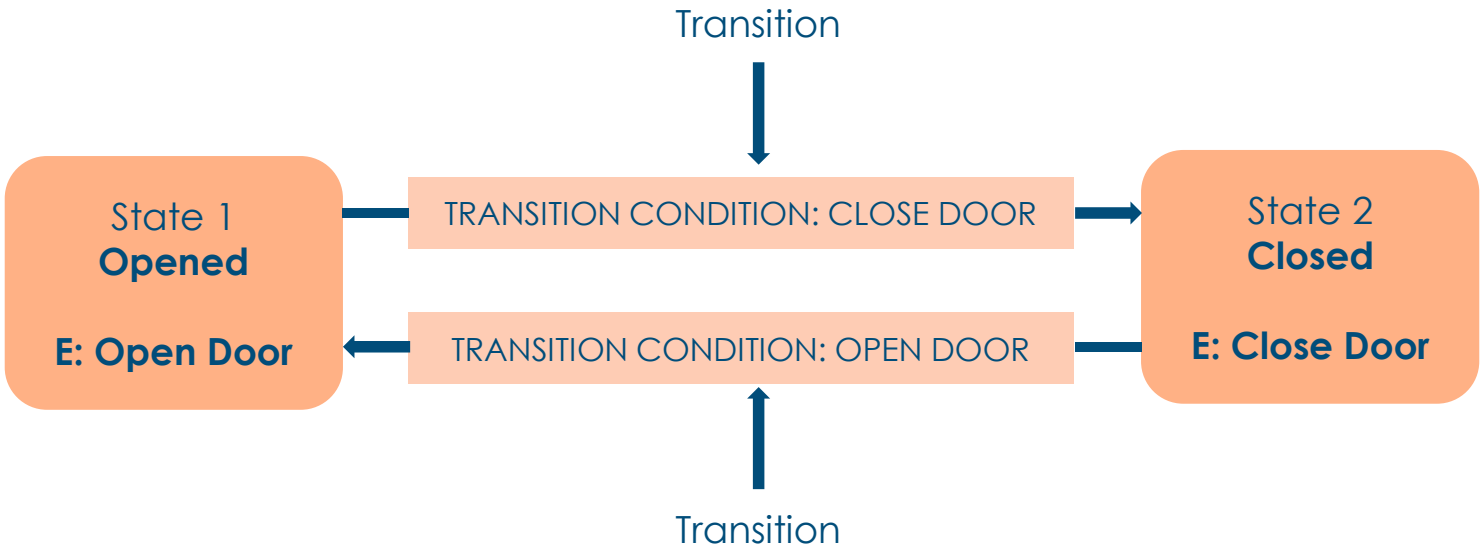
- First mathematical model with a multilevel security policy used to define the concept of a secure state machine, models of access, and outlined rules of access
- Focuses on ensuring that subjects with different clearances are properly authenticated by having the necessary security clearance, need to know, and formal access approval before accessing an object under different classification levels
- All Mandatory Access Control (MAC) systems are based on the Bell-LaPadula model because of its multilevel security – and it's been adopted by most government agencies

Bell-LaPadula Model



- Bell-LaPadula is a state machine model and is used to control access in complex systems
- The state of a machine is collected to verify the security of a system as it defines the behavior of a set number of states, the transitions between those states, and the subsequent actions that can take place
- A particular state typically consists of all current permissions and instances of subjects accessing objects
- If a subject can access objects only in adherence with the security policy, then the system is considered secure

State Machine Models



The Bell-LaPadula Ruleset

Simple security rule: a subject at a given security level cannot read data that resides at a higher security level (no read-up rule)

Strong star property rule: a subject who has read and write capabilities can only perform those functions at the same security level – nothing higher and nothing lower

Star property (*) rule: a subject at a given security level cannot write information to a lower security level (no write-down rule)

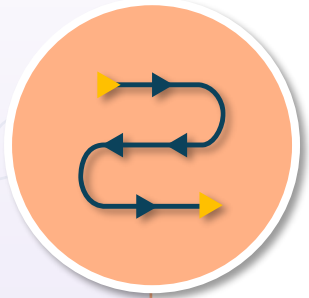
Tranquility principle: subjects and objects cannot change their security levels once they have been instantiated (created)

Biba Model

Integrity

- Developed after Bell-LaPadula, it uses a lattice of **integrity** levels (unlike Bell-LaPadula)
  - Simple integrity rule (no read down): states that a subject can not read data from a lower integrity level
  - Star integrity rule (no write up): states that a subject can not write data to an object at a higher integrity level
  - Invocation property: states that a subject cannot invoke (call upon) a subject at a higher integrity level
- Is also an information flow model (like Bell-LaPadula) because they are most concerned about data flowing from one level to another

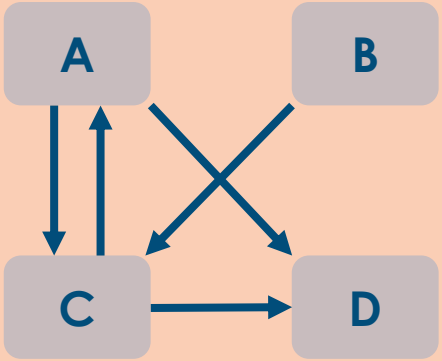
Information Flow Models



- Observes info flows in a state machine
- Data is considered in individual discrete compartments based on classification and need-to-know principles
- Subject clearance overrules the object classification, and the subject security profile must contain one of the categories listed in the object label that enforces need to know
- Example: Bell-LaPadula model prevents information flowing from higher source level to lower source level
- Example: Biba model prevents information flowing from lower integrity level to higher integrity level

Information Flow Models

Object	A	B	C	D
A	N/A		X	X
B		N/A	X	
C	X		N/A	X
D				N/A

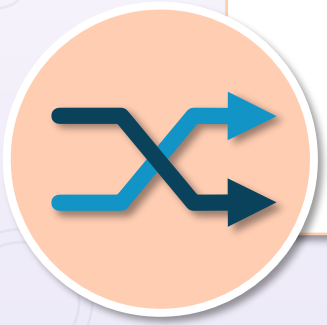


Clark-Wilson Integrity Model

- Developed after Biba and deals with information integrity
- Objects can be modified by subjects using read/write operations
- Integrity verification procedures (IVPs) are programs that run periodically to check the consistency of CDIs (integrity rules that are usually defined by vendors)

Clark-Wilson Integrity Model

- Integrity goals of Clark-Wilson model are
  - prevent unauthorized users from making modifications
  - ensure separation of duties prevents authorized users from making improper modifications, and
  - ensure well-formed transactions; maintain internal and external consistency



Role-based Access Control (RBAC)

- Access decisions rely on org chart, roles, responsibilities, or location in a user base
- Role is typically set based on evaluating the essential objectives and architecture of the enterprise
- RBAC framework is determined by security administrators and officers, and is not at the discretion of the user

Role-based Access Control (RBAC)

- For example, in a medical center, the different roles may include doctor, RN, PA, specialist, technician, attendant, receptionist, etc.
- We are seeing companies with a lot of turnover or lots of transient, temp, and contractor users move from DAC to role-based due to flexibility and easier management

Role-based Access Control (RBAC)

Advantages

- Easy to implement and control
- Roles are assigned using written security policy
- Built into many security frameworks
- Aligns accepted security principles

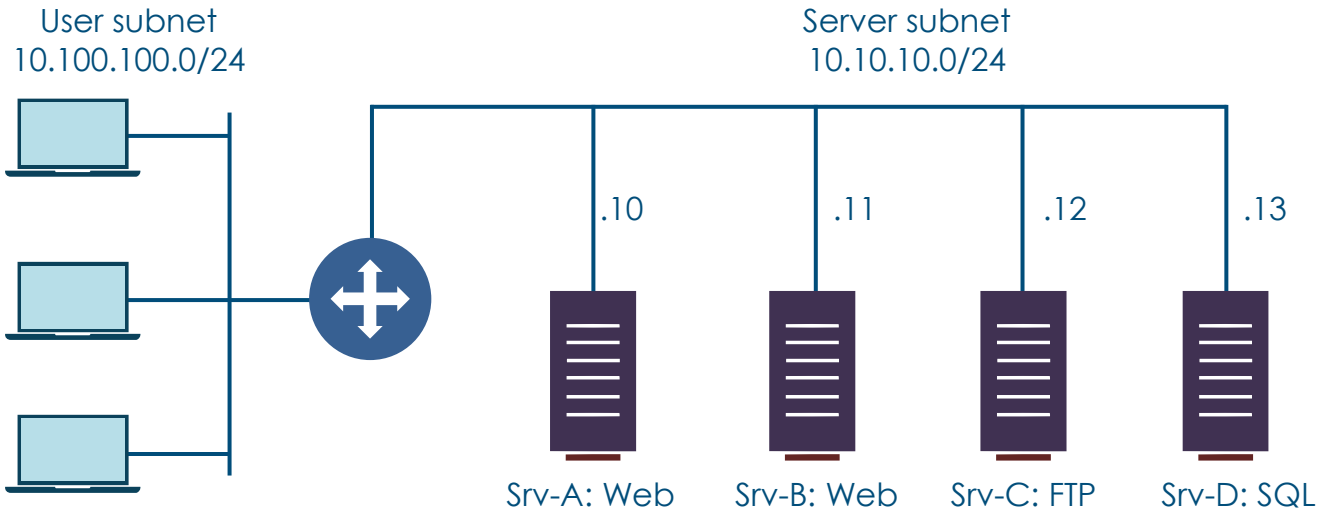
Disadvantages

- Scope creep can take place over time
- Roles and access must be audited rigorously
- Multi-tenancy capabilities need things like AD OUs

Rule-based Access Control

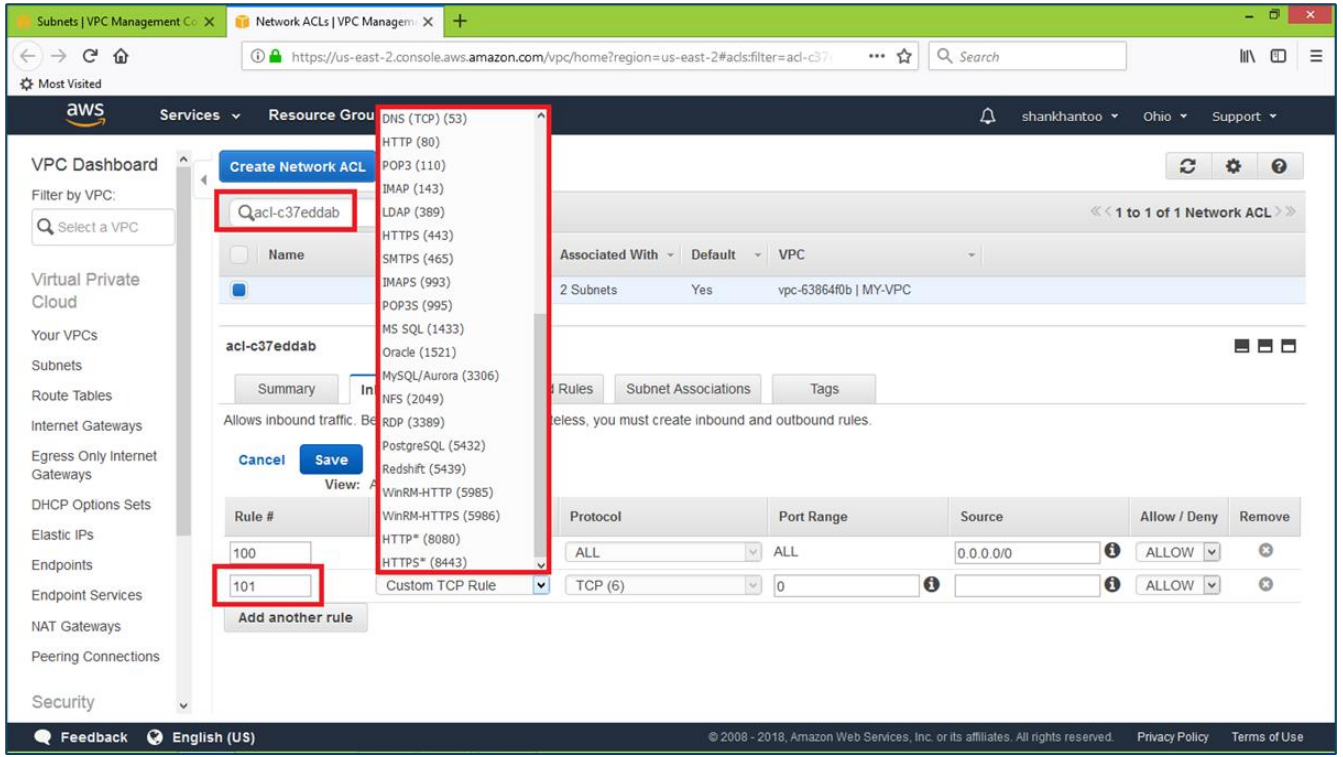
- Rule-based access control uses the acronyms RBAC or RB-RBAC
- It can dynamically assign roles to users based on criteria defined by the custodian or system administrator
- It could also be a time-based ACL if NTP is being used
- Example: a user is only allowed access to a drive on a server from 6 a.m. to 6 p.m. Monday through Friday
- It is common for infrastructure devices like routers, switches, and firewalls to use rule-based access controls

Rule-based Access Control




```
access-list 100 permit tcp any 10.10.10.10 eq www
access-list 100 permit tcp any 10.10.10.10 eq 443
access-list 100 permit tcp any 10.10.10.11 eq www
access-list 100 permit tcp any 10.10.10.11 eq 443
access-list 100 permit tcp any 10.10.10.12 eq ftp
access-list 100 permit tcp any 10.10.10.12 eq ftp-data
access-list 100 deny ip any any log
```

Rule-based Access Control



Mandatory Access Control (MAC)

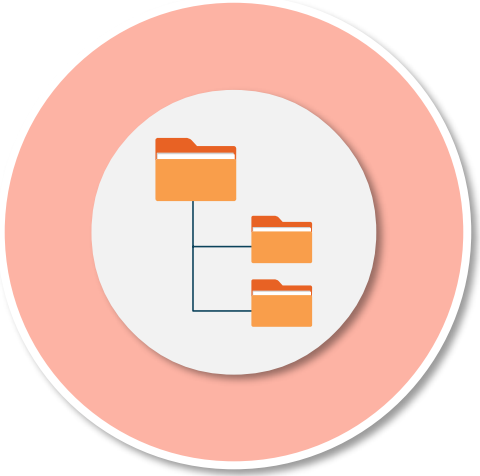
- MAC is strictly nondiscretionary and secures data by assigning sensitivity labels, then compares labels to the level of user sensitivity
- It is appropriate for extremely secure systems, such as multilevel secure military applications
- Its main advantage is that access based on "need to know" is strictly adhered to and scope creep is minimized

Mandatory Access Control (MAC)

- Main advantage is that access based on "need to know" is strictly adhered to and scope creep is minimized
- All MAC systems are based on the Bell-LaPadula model for confidentiality
- This was the first mathematical model with a multilevel security policy used to define the concept of a secure state machine and models of outlined rules of access

Discretionary Access Control (DAC)

Active Directory



- DAC restricts access to data and systems based on the identity of users and/or their group membership
- Access results are usually based on authorization granted to a user based on the various forms of credentials presented at the time of authentication
- In most DAC implementations, the owner of the resource can change its permissions at their discretion
- A DAC framework can deliver the capability for granular access control

Discretionary Access Control (DAC)

PROS

Advantages

- Easy to implement and operate
- Aligns with the least privilege security principle
- Object owner has control over granted access

CONS

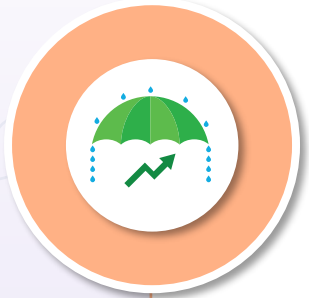
Disadvantages

- Documentation of the access must be strictly maintained
- There is a propensity for privilege (scope) creep to occur

Attribute-based Access Control (ABAC)

- Controls access to entities by weighing rules against the attributes of the subject's actions and the request environment
- ABAC relies upon evaluation of
  - people's characteristics
  - attributes of IT components
  - heuristics
  - environmental factors, and
  - situational variables
- ABAC systems are capable of enforcing both Discretionary Access Control (DAC) and Mandatory Access Control (MAC) models

Risk-based Access Control



- Also referred to as risk-adaptable access control (RAdAC)
- Considers the obstacles of traditional access control approaches to sharing of information
- Is a model that seeks to imitate real-world decision-making while considering operational needs and security risk together with every access control decision
  - Realizes that situational conditions will drive the relative weight of these two factors when authorizing access
- Can support extremely restrictive policies as well as those that offer the broadest sharing, with added risk, under specific conditions

Risk-adaptable Access Control (RAdAC)