* Security Architecture

**3.1 Architecture Model**

* **Architecture and infrastructure concepts**
  + Cloud
    - Responsibility matrix
    - Hybrid considerations
    - Third-party vendors
  + Infrastructure as code (IaC)
  + Serverless
  + Microservices
  + Network infrastructure
    - Physical isolation
    - Air-gapped
    - Logical segmentation
    - Software-defined networking (SDN)
  + On-premises
  + Centralized vs. Decentralized
  + Containerization
  + Virtualization
  + IoT
  + Industrial control systems (ICS)/ supervisory control and data acquisition (SCADA)
  + Real-time operating system (RTOS)
  + Embedded systems
  + High availability
* **Considerations** 
  + Availability
  + Resilience
  + Cost
  + Responsiveness
  + Scalability
  + Ease of deployment
  + Risk transference
  + Ease of recovery
  + Patch availability
  + Inability to patch
  + Power
  + Compute

What is the Cloud?

* The cloud is a network of remote servers that are used to store and process data and apps.
* It's like a remote computer that can store your files, run your programs, and do more tasks without needing to be physically near you.
* When you use the cloud, you are renting computing resources from a cloud provider.
* This allows you to access the resources you need, when you need them, without having to invest in your
* own hardware and software.

Why we need the Cloud?

* **1990s**
  + Companies used to have an on-prem approach.
  + Servers, Hard drives, routers, physical hardware, everything managed in their datacenters, etc.
  + They needed to maintain those datacenters (cooling systems), purchase more devices than needed, oversize, etc.
* **2000s**
  + The cloud model came and outsourced the infrastructure and management part (patching, cooling, availability, etc.)
  + You as a user only care about developing your app.
  + The cloud provider gives you storage, computing, processing, etc. You only worry about your tasks.

Use Cases

* **Storage**: Store data, such as documents, images, videos. A cost-effective way to store large data, as you only pay for the storage you use.
* **Compute**: Run apps and process data. A cost-effective way to run apps.
* **Identity & Access Management**: Manage user authentication and access. Testing: Test applications before they are deployed.
* **Backup and disaster recovery:** This is a critical service for businesses of all sizes, as it can help to minimize the impact of a disaster.

Shared Responsibility

* Defines the division of responsibilities between providers and customers.
* Both parties play crucial roles in ensuring the security and compliance.
* The provider is responsible for the security of the cloud, the customer is responsible for securing their data.

Hybrid Considerations

* Integrating on-premises infrastructure with cloud services.
* Offers flexibility and maintains control over local sensitive data.

Infrastructure as Code

* Managing cloud infrastructure through code instead of manually.
* Automate processes, reduce human error, ensure consistency.

Serverless

* A model where the cloud provider manages the allocation of resources.
* Developers focus on code while the cloud provider handles server management.
* Reduces operational overhead.

Microservices

* Monolithic applications are apps built as a single, large code. All of the code, data, and more are stored in a single unit.
* Microservices: A style that structures an application as a collection of loosely coupled services.
* Each service is responsible for a specific function, and the services communicate with each other through APIs. Each service is independent and manageable. Enhances flexibility. Updating one part of the app will not affect other parts.

Network Infrastructure

* **Physical Isolation**: Separating network components physically to prevent unauthorized access.
  + Ensures critical systems are inaccessible from public networks.
  + **Air-gapped Networks**: Completely isolating a system from any external connections.
* **Logical Segmentation** (VLAN): Dividing a network into **distinct segments**.
  + Group devices together and isolate network traffic for each group.
* **Software-defined Networking** (SDN): For efficient network configuration. Rather than fixing and configuring issues manually, logically fix that with the SDN (control plane).

Infrastructure Concepts

* **Virtualization**: Creating virtual versions of physical resources, such as servers. Allows multiple VMs to run on a single physical machine.
* **Containerization**: Packaging applications into isolated units (containers).

loT

* **IoT (Internet of Things) Devices**: Network of **interconnected devices**, such as refrigerators, thermostats, cars equipped with internet connectivity.
  + IoT devices include smart home devices (lights, cameras, etc.), wearable devices (watches, trackers).
  + Each device is connected to the Internet and is uniquely addressable.
  + Security issues here include authentication and updates.

Infrastructure Concepts

* **Industrial Control Systems and SCADA systems** are designed to control and automate industrial processes.
* **Real Time Operating Systems (RTOS)**: An OS designed to process data as it comes in, time-sensitive.
  + Ensures timely and deterministic responses for critical applications.
  + Always need to be available.
* **Embedded Systems**: Devices that have a dedicated function and use a computer system to perform that function.
  + Embedded into hardware and often perform real-time computing tasks.

Considerations

* **Availability**: The degree to which a system or app is operational and accessible when required. We typically want high availability.
* **Resiliency**: Ability of a system to recover quickly from failures and keep operating.
* **Cost**: Includes initial setup, ongoing maintenance, and operational costs.
* **Scalability**: The ability of a system to handle increased load or expand in capacity.
* **Responsiveness**: The speed at which a system responds to user inputs.
* **Ease of deployment**: The simplicity and speed with which a system can be deployed.
* **Ease of recovery**: Ability to restore systems to normal operation after a failure.
* **Patch availability**: Frequency of updates to fix bugs and improve functionality.
* **Compute**: The processing power available to handle workloads and run applications.

Cloud Considerations

* **Amazon Web Services (AWS)**
  + 100+ data centers
  + 5 continents
  + 200 million computers
  + UPS for every server
  + High Performance Servers
  + 100,000 RAID and backup servers
  + 100+ Patch Management teams
* **Kevin Little Cloud (KLC)** 
  + 2 data centers
  + 1 continent
  + 80 computers
  + No UPS
  + Regular Servers
  + 10 backup servers
  + 1 Patch Management team

**3.2 Infrastructure Consideration**

* **Infrastructure considerations** 
  + Device placement
  + Security zones
  + Attack surface
  + Connectivity
  + Failure modes
    - Fail-open
    - Fail-closed
  + Device attribute
    - Active vs. passive
    - Inline vs. tap/monitor
  + Network appliances
    - Jump server
    - Proxy server
    - Intrusion prevention system (IPS)/intrusion detection system (IDS)
    - Load balancer
    - Sensors
  + Port security
    - 802.1X
    - Extensible Authentication Protocol (EAP)
  + Firewall types
    - Web application firewall (WAF)
    - Unified threat management (UTM)
    - Next-generation firewall (NGFW)
    - Layer 4/Layer 7
* **Secure communication/ access** 
  + Virtual private network (VPN)
  + Remote access
  + Tunneling
    - Transport Layer Security (TLS)
    - Internet protocol security (IPSec)
  + Software-defined wide area network (SD-WAN)
  + Secure access service edge (SASE)
* **Selection of effective controls**
* **Device Placement**: The strategic positioning of devices within a network. It ensures optimal performance and security.
* Segmented networks with varying level of security (**security zones**).
* Minimize the **attack surface** to reduce the potential points of compromise.
* **Active Devices** actively interact with the network traffic (firewalls, routers, etc.)They are inline with traffic. They directly influence traffic flow and security.
* **Passive Devices** monitor network traffic without altering it (IDS, sensors).
* **Failure Modes**: How does a system behave after a failure?
  + **Fail-Open**: A system continues to operate in its default state during a failure.
    - A firewall that allows all traffic if it fails.
  + **Fail-Closed**: A system blocks all operations during a failure.
    - A firewall that blocks all traffic if it fails.

Network Appliances

* **Jump Server**: A computer used to manage access to a different security zone.
* **Proxy Server**: An intermediary server that forwards requests from clients to other servers.
  + Instead of directly connecting to a website, you connect to the proxy, and then the proxy connects to the website for you.
  + Proxies are used for security to filter and block access to certain websites or content.
* **Sensors**: Monitor network traffic and collect data for analysis and alerting.

Load Balancer

* Load balancer is a tool that distributes network traffic across multiple servers.
* This improves performance by preventing any one server from becoming overloaded.
* It is a good way to improve the performance and ECUR reliability of apps.

**IPS/IDS** (Intrusion Prevention System/Intrusion Detection System)

* DS and IPS watch network traffic and take action based on events.
* IPS **blocks (prevents)** attacks before it reaches the target.
* IDS **detects** attacks and **alerts** users but doesn't block the attack.
* **Host-based IDS/IP**S (HIDS/HIPS) is an additional software installed on a **single system** (a computer, a server, etc.)
* **Network-based IDS/IPS** (NIDS/NIPS) monitors activity on the **entire network**.

Port Security

* **802.1X** is a protocol that is used to authenticate devices before they a to access a network.
* **Extensible Authentication Protocol** (EAP): provides a method for systems to authenticate.
* EAP prevents access to the network until authentication is successful.
* EAP can be used to create other forms of authentication.

What is Firewall

* It is a network security device that monitors and controls incoming and outgoing network traffic.
* It protects networks from unauthorized access.
* It is like a gatekeeper that sits between your network and the outside world.
* Firewalls can be software or hardware. Software RSECURIT firewalls are installed on individual computers, while hardware firewalls are standalone devices.

Type of Firewall

There are many different types of firewalls:

* **Web Application Firewall** (WAF): Protects web applications by filtering and monitoring HTTP traffic. Blocks SQL injection, XSS, and web-based attacks.
* **Next-Generation Firewall** (NGFW): A sophisticated firewall. Provides deeper packet inspection and more security.
* **Unified Threat Management** (UTM): Multiple security features into a single appliance.
* **Layer 4**: Operates at the transport layer (Layer 4), filtering traffic based on IP address, protocol, and port.
* **Layer 7**: Operates at the application layer (Layer 7), inspecting content.

Secure Communication/Access

**VPN** (Virtual Private Network)

* A tool used to connect to a private network via the internet.
* Allows users to access resources such as files, apps, streaming, as if they were physically connected to the network.
* VPNs encrypt your internet traffic and protect your online identity.
* VPN hides your IP address, making it impossible to track you.

**Site-To-Site VPN**

* A site-to-site VPN connects two sites to each other across the internet and sends data in an encrypted form.

**Remote Access VPN**

* A remote access VPN allows users to connect to a private network from a remote location.

**SSL/TLS** (Secure Sockets Layer/Transport Layer Security)

* SSL/TLS is the protocol used to protect (encrypt) web communication. It encrypts messages/data.
* HTTPS (port **443**) uses SSL/TLS to secure web pages.
* HTTPS = HTTP + SSL/TLS.

**IPsec** (IP Security)

* It is a protocol used to provide secure communication by encrypting each packet.
* IPsec has 2 key components:
  + **Authentication Header** (AH): It adds integrity to packets, ensuring that packets are not modified.
  + **Encapsulating Security Payload** (ESP): provides both encryption and authentication to packets.

Secure Communication

* **SASE** (Secure Access Service Edge): A network architecture that combines wide-area networking (WAN) and network security services.
* **Example**: Adding new branches or remote workers without significant infrastructure changes.
* Employees access corporate resources securely from home or mobile locations.

**3.3 Data Types and Data Classification**

* **Data types**
  + Regulated
  + Trade secret
  + Intellectual property
  + Legal information
  + Financial information
  + Human- and non-human readable
* **Data classifications**
  + Sensitive
  + Confidential
  + Public
  + Restricted
  + Private
  + Critical
* **General data considerations**
  + Data states
  + Data at rest
  + Data in transit
  + Data in use
  + Data sovereignty
  + Geolocation
* **Methods to secure data** 
  + Geographic restrictions
  + Encryption
  + Hashing
  + Masking
  + Tokenization
  + Obfuscation
  + Segmentation
  + Permission restrictions

Data

* Data refers to information that can be processed and analyzed.
* Data classification is the process of categorizing data based on its sensitivity and importance to the organization.
* This helps in applying appropriate security measures to protect the data.

Dtata Types

* **REGULATED DATA**
  + Data subject to compliance requirements and regulations.
  + Requires security measures for compliance and avoid fines.
  + Example — Personal Data for EU residents, protected under GDPR.
* **TRADE SECRET** 
  + Secret information that holds economic value; not publicly known.
  + Formulas, practices.
  + The recipe for Coca-Cola is a famous trade secret.
* **INTELLECTUAL PROPERTY (IP)** 
  + Creations of the mind that are legally protected.
  + Intellectual assets, inventions, and proprietary processes.
  + Research and development data
* **LEGAL INFORMATION**
  + Related to legal matters, case files, and contracts.
  + Requires confidentiality.
  + Legal documents outlining terms and conditions.
* **FINANCIAL DATA** 
  + Related to the organization's financial statements.
  + Bank account details, balance sheets, tax information.
* **HUMAN AND NON-HUMAN READABLE** 
  + Easily interpreted by humans.
  + Text documents, spreadsheets, images, videos.
  + Non-human readable: Intended for processing by machines.
  + Binary files, encrypted data.

Data Classification

* **PUBLIC DATA** 
  + Intended for public disclosure. It doesn't require protection.
  + Its exposure does not pose any risk to the organization.
  + Public announcements, Web home pages, etc.
* **RESTRICTED DATA** 
  + Highly sensitive data, access is tightly controlled.
  + Disclosure could have severe consequences.
  + Details about power grids, transportation systems.
* **CONFIDENTIAL DATA** 
  + Secret and only accessible to authorized individuals.
  + Access should be limited to those with a need to know.
  + Trade secrets, business plans, patents.
* **SENSITIVE DATA** 
  + If disclosed, could cause harm to an organization or individual.
  + Social security numbers, addresses, credit card numbers.
* **PRIVATE DATA** 
  + Related to individuals, intended to remain private.
  + Disclosure could infringe on personal privacy.
  + Medical records, emails, personal messages.
* **CRITICAL DATA** 
  + Essential to the operation and survival of an organization.
  + Compromise could result in business failure.
  + Manufacturing processes, supply chain information.

States of Data

* **Dtat In Transit**
  + Data actively moving from one location to another
  + Emails, file transfer.
* **Data In Use**
  + Data actively processed by a computer or app
  + Most vulnerable stage
* **Datat At Rest**
  + Data stored in a non-volatile location such as a hard drive, computer, etc.

Data Security

* Data security involves implementing measures to protect data fromm unauthorized access.
* Encryption and hashing are techniques used to enhance data security.
* **Encryption** is the process of converting readable data into an unreadable format.
* The goal of encryption is to protect information from unauthorized access.
* **Hashing** is the process of converting any type of data into a fixed-length of characters.
* Hashes are unique to the data, and any change in the original results in a completely different hash result.
* Hashing is a one-way transformation. You **cannot** retrieve the original data from the hash result.
* **Data Masking** — Hiding original data with modified content. Replacing with realistic but false data.
  + Credit Card Numbers 4224-5271-9835-1410 masked to 1234-\*\*\*\*-\*\*\*\*-5432
  + Social Security Numbers: 987-65-4321 masked to 987-\*\*-\*\*\*\*
* **Tokenization** — Substituting sensitive data with a unique identifier (token) that has no exploitable value.
  + Tokens can be mapped back to the original data only through a secure system.
  + Credit Card Tokens: 4331-6171-1073-1489 tokenized to ebzw-kagr-aika-mevw
* **Obfuscation** — Making data difficult to understand. Helps protect against reverse engineering.
* **Segmentation** — dividing a network into smaller isolated segments. Limits the scope of access and exposure of data
* **Sovereignty** — Data is subject to the laws of the country where it is stored. Ensures compliance with local data protection laws.
* **Geographic restrictions** — Controlling access to data based on the geographical location of users or devices. Implemented via IP address restrictions.

**3.4 Resiliency and Recovery**

* **High availability**
  + Load balancing vs. clustering
* **Site considerations** 
  + Hot
  + Cold
  + Warm
  + Geographic dispersion
* **Platform diversity**
* **Multi-cloud systems**
* **Continuity of operations**
* **Capacity planning** 
  + People
  + Technology
  + Infrastructure
* **Testing**
  + Tabletop exercises
  + Fail over
  + Simulation
  + Parallel processing
* **Backups** 
  + Onsite/offsite
  + Frequency
  + Encryption
  + Snapshots
  + Recovery
  + Replication
  + Journaling
* **Power** 
  + Generators
  + Uninterruptible power supply (UPS)

High Availability

* A technique to ensure that systems are consistently operational and accessible.
* Minimizes downtime, ensures that critical services are always available to users.
* Redundant servers or failover systems.
* **Load Balancing**: Distributing incoming network traffic across multiple servers.
* Ensures no single server becomes overwhelmed.
* **Clustering**: Grouping multiple servers to work together as a single system.
* If one server fails, others can take over its workload.

Site Resiliency

* **Cold Sities**
  + A cold site is a site where you are provided an empty building with no hardware. You bring your hardware, data and people.
* **Hot Sities**
  + A hot site is an exact duplicate of the existing environment. The hot site is operational 24/7 and takes over quickly from main site.
* **Warm Sities**
  + A warm site is just enough to get things going. It might have rack space and you bring hardware, or it might have hardware but you bring software, data.

Bussiness Continuity Planning (BCP)

* Business continuity is an organization's ability **to maintain business functions** or **quickly resume** them in the event that risks are realized.
* The events can be a power outage, loss of network connectivity, cyberattacks, earthquakes, etc.
* BCP isimportant to **minimize downtime**.
* **COOP (Continuity of Operation Plan)** Ensuring that critical Budiniess functions can continue during and after a disaster.

Resiliency

* **Platform Diversity** : Using a variety of platforms within an organization to eliminate single points of failure.
  + Different OSs like Windows, Linux, and macOS.
  + Utilizing hardware fron multiple manufacturers.
* **Multi-cloud Systems**: Using multiple cloud service providers to host apps.
  + Increases availability, a failure in one cloud provider does not disrupt services.
  + Hosting apps across AWS and Azure.

Testing

* Analyze an incident to understand what happened, and how future incidents can be prevented.
* **Tabletop Exercises**: Discussion-based sessions where team members walk through hypothetical incident scenarios to evaluate the effectiveness of their plans.
* **Simulations**: advanced and realistic exercises that replicate real-world cyber incidents.
* **Fail over**: Simulating failures to ensure systems can switch to backup resources.
* **Parallel Processing**: Test a system's ability to handle multiple tasks concurrently without degradation.

Backups

* **Onsite/offsite**: Storing backup data within local offices and at remote locations.
  + Ensures availability and recovery options in case of local disasters.
  + Local backup servers and cloud storage solutions.
* **Snapshots**: Capturing the state of a system at a specific point in time.
  + Provides a quick recovery option by restoring to a known good state.
  + VM snapshots.
* **Journaling:** Recording changes to data in a log for recovery purposes.
  + Replaying or undoing changes to recover data.

Power

* **UPS** (Uninterruptible Power Supply)
  + A UPS is a power backup system that provides a temporary power source during electrical outages.
  + It prevents data loss due to sudden power outages
* **Generators**
  + Backup generators provide a secondary power source during prolonged outages, ensuring continuous operations of systems.