Architecture and Design

- Configuration Management
    - The only constant is change
        - Operating systems, patches, application updates, network mods, new app instances
- Identify and document hardware and software setting
    - Manage the security when changes occur
- Rebuild those systems if a disaster occurs
    - Documentation and processes will be critical
- Diagrams
    - Network diagrams
        - Document the physical wire and device
    - Physical data center layout
        - Can include physical rack locations
    - Device Diagrams
        - Individual cabling
- Baseline configuration
    - The security of an application environment should be well defined
        - All application instances must follow this baseline
        - Firewall settings, patch levels, OS file versions
        - May require constant updates
    - Integrity measurements check for the secure baseline
        - These should be performed often
        - Check against well documented baselines
        - Failure requires an immediate correction
- Standard naming conventions
    - Create a standard
        - Needs to be easily understood by everyone
    - Services
        - Asset tag names and numbers
        - Computer names - location or region
        - Serial numbers
    - Networks
        - Port labeling
    - Domain configurations
        - User account names
        - Standard email addresses
- IP Schema
    - An IP address plan or model
        - Consistent addressing for network devices
        - Help avoid duplicate IP addressing
    - Locations
        - Number of subnets, hosts per subnet
    - IP ranges

        - Different sites have a different subnet
    - Reserved addresses
        - Users, printers, routers/default gateways

- Protecting data
    - A primary job task
        - An organization is out of business without data
    - Data is everywhere
        - On a storage drive, on the network, in a CPU
    - Protecting the data
        - Encryption, security policies
    - Data permissions
        - Not everyone has the same access
- Data sovereignty
    - Data that resides in a country is a subject to the laws of that country
        - Legal monitoring, court orders etc
    - Laws may prohibit where data is stored
    - GDPR
    - Data collected on EU citizens must be stored in the EU
    - A complex mesh of tech and legalities
    - Where is your data storeD?
        - Your compliance laws may prohibit moving data out of the country
- Data masking
    - Data obfuscation
        - Hide some of the original data
    - Protects PII
        - And other sensitive data
    - May only be hidden from view
        - The data may still be intact in storage
            - Control the view based on permissions
        - Many different techniques
            - Substituting, shuffling, encrypting, masking out, etc.
- Data encryption
    - Encode information into unreadable data
        - Original information is plaintext, encrypted form is ciphertext
    - This is a two way street
        - Convert between one and the other
        - If you have the proper key
    - Confusion
        - The encrypted data is drastically different than the plaintext
- Diffusion
    - Change one character of the input, and many characters change of the output
- Data at-rest
    - The data is on a storage device

        - Hard drive, SSD, flash drive, etc.
    - Encrypt the data
        - Whole disk encryption
        - Database encryption
        - File- or folder-level encryption
    - Apply permissions
        - Access control lists
        - Only authorized users can access the data
- Data in transit
    - Data transmitted over the network
        - Also called data in motion
    - Not much protection as it travels
        - Many different switches, routers, devices
    - Network based protection
        - Firewall, IPS
    - Provide transport encryption
        - TLS (Transport Layer Security)
        - IPsec (internet protocol security)
- Data in use
    - Data is actively processing in memory
        - System RAM, Cpu registers and cache
    - The data is almost always decrypted
        - Otherwise, you couldn't do anything with it
    - The attackers van pick the decrypted information out of RAM
        - A very attractive option
    - Target Corp Breach of credit cards
        - Attackers picked the credit card numbers out of the point of sale RAM
- Tokenization
    - Replace sensitive data with a non sensitive placeholder
    - Common with credit card pro cessing
        - Use a temporary token during payment
        - An attacker capturing the card numbers can't use the matter
    - This isn't encryption or hashing
        - The original data and token are not mathematically related
        - No encryption overhead
- Information Rights Management (IRM)
    - Control how data is used
        - Microsoft Office
        - Email messages
        - PDF’s
    - Restrict data access to unauthorized persons
        - Prevent copy and paste
        - Control screenshots
        - Manage printing

        - Each user has their own set of rights
            - Attackers have limited options

- Data Loss Prevention (DLP)
    - Where's your data?
        - Social security numbers, credit card numbers, medical records
    - Stop the data before the attackers get it
        - Data "leakage"
    - So many sources, so many destinations
        - Often requires multiple solutions in different places
    - On your computer
        - Data in use
        - Endpoint DLP
    - On your network
        - Data in motion
    - On your server
        - Data at rest
- USB blocking
    - DLP on a workstation
        - Allow or deny certain tasks
    - Nov 2008 - US DoD
        - Worm virus agent.btz replicates using USB storage
        - Bans removable flash media and storage devices
    - All devices had to be updated
        - Local DLP agent handled USB blocking
    - Ban was lifted in 2010 Feb
        - Replaced with strict guidelines
    - Cloud Based DLP
        - Located between users and the internet
            - Watch every byte of network traffic
            - No hardware, no software
        - Block custom defined data strings
            - Unique data for your organization
        - Manage access to URL's
            - Prevent file transfers to cloud storage
        - Block malware and viruses
    - DLP and email
        - Email continues to be the most critical risk vector
            - Inbound threats, outbound data loss
        - Check every email inbound and outbond
            - Internal system or cloud based
        - Inbound
            - Block keywords, identify imposters, quarantine email messages
        - Outbound

            - Fake wire transfers, W-2 transmissions, employee information
        - Emailing a spreadsheet template
            - Boeing employee emails spouse a spreadsheet to use as a template
        - Contained the personal info of 36,00 boeing employees
            - Hidden columns
            - SSN, Date of Birth
        - Boeing sells its own DLP software
            - But only uses it for classified work

- Geographical considerations
    - Legal implications
        - Business regulations vary between states
        - For a recovery site outside of the country, personnel must have a passport and be able to clear immigration
        - Refer to your legal team
    - Offsite backup
        - Organization owned site or 3rd party secure facility
    - Offsite recovery
        - Hosted in a different location, outside the scope of the disaster
        - Travel considerations for support staff and employees
- Response and recovery controls
    - Incident response and recovery has become commonplace
        - Attacks are frequent and complex
    - Incident response plan should be established
        - Documentation is critical
        - Identify the attack
        - Contain the attack
    - Limit the impact of an attacker
        - Limit data exfiltration
        - Limit access to sensitive data
- SSL/TLS inspection
    - Commonly used to examine outgoing SSL/TLS
        - Secure Sockets Layer/ Transport Layer Security
        - For example, from your computer to your bank
    - Wait a second. Examine encrypted traffic?
        - Is that possible?
    - SSL/TLS relies on trust
        - Without trust, none of this works
    - Im SSL
        - Your browser contains a list of trusted CA's
            - My browser contains about 170 CA's certifications
        - Your browser doesn't trust a website unless a CA has signed the web server encryption certificate

        - The web site pays some money to the CA for this
        - The Ca has ostensibly performed some checks
            - Validated against the DNS record, phone call, etc
        - Your browser checks the web server's certificate
            - If its signed by a trusted CA cert, the encryption works seamlessly
- Hashing
    - Represent data as a short string of text
        - A message digest
    - One way trip
        - Impossible to recover the original message from the digest
        - Used to store passwords / confidential information
    - Verify a downloaded document is the same as the original document
        - Integrity
    - Can be a digital signature
        - Authentication, non repudiation, and integrity
        - Will not have a collision (hopefully)
            - Different messages will not have the same hash
    - A Hash example
        - SHA256 hash
            - 256 bits / 64 hexadecimal characters
- API Considerations
    - API (Application Programming Interface)
        - Control software or hardware programmatically
        - Secure and harden the login page
            - Don't forget about the API
        - On Path Attack
            - Intercept and modify the API messages, replay API commands
        - Api Injection
            - Inject data into an API message
        - DDoS (Distributed Denial of Service)
            - One bad API call can bring down a system
    - API Security
        - Authentication
            - Limit API access to legitimate users
            - Over secure protocols
        - Authorization
            - API should not allow extended access
            - Each user has a limited role
            - A read only user should not be able to make changes
        - WAF (Web Application Firewall)
            - Apply rules to API communication

- Site resiliency
    - Recovery site is prepped

        - Data is synchronized
    - A disaster is called
        - Business processes failover to the alternate processing site
    - Problem is addressed
        - This can take hours, weeks, or longer
    - Revert back to the primary location
        - The process must be documented for both directions
- Hot Site
    - An exact replica
        - Duplicate Everything
    - Stocked with hardware
        - Constantly updated
        - You buy two of everything
    - Applications and software are constantly updated
        - Automated replication
    - Flip a switch and everything moves
        - This may be quite a few switches
- Cold site
    - No hardware
        - Empty building
    - No data
        - Bring it with you
    - No people
        - Bus in your team
- Warm site
    - Somewhere between cold and hot
        - Just enough to get going
    - Big room with rack space
        - You bring the hardware
    - Hardware is ready and waiting
        - You bring the software and data

- Honeypots
    - Attract the bad guys
        - And trap them there
    - The “attacker” is probably a machine
        - Makes for interesting recon
    - Honeypots
        - Create a virtual world to explore
    - Many different options
        - Kippo, Google Hack Honeypot, Wordpot
    - Constant battle to discern the real from the fake
- Honey Files and honeynets
    - Honeynets

        - More than one honeypot on a network
        - More than one source of information
    - Honeyfiles
        - Bait for the honeynet (passwords.txt)
        - An alert is sent if the file is accessed
        - A virtual bear trap
- Fake telemetry
    - Machine Learning
        - Interpret big data to identify the invisible
    - Train the machine with actual data
        - Learn how malware looks and acts
        - Stop malware based on actions instead of signatures
    - Send the machine learning model fake telemetry
        - Make malicious malware look benign
- DNS sinkhole
    - A DNS that hands out incorrect IP addresses
        - Blackhole DNS
    - This can be bad
        - An attacker can redirect users to a malicious site
    - This can be good
        - Redirect known malicious domains to a benign IP addresses
        - Watch for any users hitting that IP address
        - Those devices are infected
    - Can be integrated with a firewall
        - Identify infected devices not directly connected