**Computer and Network Security Week 3**

* Threat Intelligence Sources
  + Pools of resource and knowledge about the latest attacks
  + Evidence of an attack is one type of shared infor
  + Key Risk Indicators
    - Metrics of upper and lower bounds of specific indicators of normal network activity
    - These indicators may include the total network logs per second, number of failed remote logins, network bandwith, outbound email traffic
  + A KRI exceeding its normal bounds could be an indicator of compromise (IOC)
    - An IOC shows that a malicious activity is occurring but is still in early stages
    - IOC info aids in prediction and discovery of attacks before they occur
  + Category of sources
    - Open Source refers to anything that can be freely used
    - Open source threat intelligence (OSINT)
    - Cyber Information Sharing and Collaboration Program (CISP)
      * Analyst-to-analyst technical exchanges
      * Digital malware analysis
      * CISCP analytical products
    - 2 concerns around public info-sharing centers are:
      * Privacy – must be careful not to share sensitive information when providing IOC details
      * Speed – Automated Indicator Sharing (AIS) enables exchange of cyberthreat indicators through computer toi computer communication
      * @ Tools
        + Structured Threat Information Expression (STIX) is a language and format used to exchange
        + Trusted Automated Exchange of Intelligence
    - Closed Source
      * Is proprietary, belongs to na organization
      * Restrict access to data and participation
  + Sources of threat Intelligence
    - Vulnerability Database is a repository of known vulnerabilities and info on how they’ve been exploited
    - Threat maps illustrate cyber threats on a diagram of a geographical area
    - File and code repositories are when victims of an attack can upload malicious files and code that can be examined
    - Dark web- security professionals and orgs use the dark web on a limited basis to look for signs that info critical to that enterprise is being sough out or sold on the dark web
  + Securing Endpoint Computers
    - Three major tasks
      * Confirming the computer has started securely
      * Protecting the computer from attacks
      * Hardening it for even greater protection
  + Confirm Boot integrity
    - Ensuring secure startup involves the Unified Extensible Firmware Interface (UEFI)
      * Early booting processes used firmware called the BIOS
      * UEFI is an improved firmware interface
      * It includes the ability to access hard drives that are larger than 2 TB, Support an unlimited number of hard drive partitions
      * Faster booting
      * Support for networking functionality
    - Boot Security
      * The ability to update BIOS in firmware opened the door for threat actors to create malware to infect BIOS
      * Boot security involves validating that each element used in each step of the boot process has not been modified
      * Begins by validating boot software, then software drivers, and so on until control is given to the OS
      * Called chain of trust because each element relies on validation of the previous element
      * The strongest starting point is hardware (known as hardware root of trust
  + Protect Endpoints
    - Protection on endpoints can be accomplished through software installed such as
      * Antivirus software
        + Antivirus (AV) can examine a computer for file-based virus infections as well as monitor computer activity
        + Signature-based monitoring = static analysis
        + Heuristic monitoring = dynamic analysis
      * Antimalware
        + Is a suite of software intended to provide protections against multiple types of malware
        + Antimalware spam protection often uses Bayesian filtering. Filters by analyzing every word in each email and determines how often a word occurs in spam pile versus nonspam pile
        + Has a component called antispyware, which helps prevent spyware infection, using pop-up blockers
      * Web Browser protections
        + Use secure cookies to send to a web server with an encrypted request
        + This prevents unauthorized people from intercepting the cookie while its being transmitted
      * Monitoring and Response systems
        + 3 Types

Host Intrusion Detection Systems (HIDS) is a software-based app that can detect if an attack has occurred

Host Intrusion Prevention Systems (HIPS) monitor endpoint activity to block a malicious attack immediately

Endpoint Detection and Response (EDR) tools are considered more robust than HIDS and HIPS

Can aggregate data from multiple endpoints to a centralized database

Can perform more sophisticated analytics that identify patterns and detect anomalies

* + Harden Endpoints
    - Involves patch management and os protections
    - Patch management
      * Involves two types of patch management tools
      * Patch distribution using an automated patch update service
    - Operating Systems
      * Securing OS involves security configs and confinement tools
      * Security config should include:
        + Disabling unnecessary ports and services
        + Disabling default accounts/passwords
        + Employing least functionality
      * In Windows, a security template is a collection of security config settings that can be used to deploy security settings to multiple computers
      * Windows 10 Tamper Protection security feature prevents Windows security settings from being changed or disabled
      * Confinement Tools – to restrict malware
        + Application whitelisting/blacklisting
        + Sandbox
        + Quarantine
  + Creating and deploying SecDevOps
    - An unsecured app can open the door for attackers
    - A directory traversal attack takes advantage of vulnerability in the web app or web server software so that the user can move from the root directory to other restricted directories
    - This could allow unauthorized users to enter commands to execute on a server known as command injection
    - Other weaknesses in apps can create vulnerabilities in computer memory or buffer
    - Poor memory management vulnerabilities result in attacks such as buffer overflow, integer overflow, pointer/object deference, and DLL injection
  + App Development concepts
    - General Concepts
      * Development, Testing, Staging, Production
      * Software diversity is a software development technique in which two or more functionally identical variants of a program are developed from the same specification but by different programmers or teams
      * Provisioning: enterprise-wide configuration, deployment, and management of multiple types of IT system resources
      * Deprovisioning in app development is removing a resource that’s no longer needed
      * Integrity Measurement is an attestation mechanism designed to be able to convince a remote party that an app is running only a set of know and approved executables
    - SecDevOps
      * Application development lifecycle model describes the stages in creating an application
      * Waterfall model – uses a sequential design process
      * Agile model – takes an incremental approach
      * SecDevOps is the process of integrating secure development practices and methodologies into app software development and deployment processes using agile model
      * Applies automated courses of action to develop code quickly and securely
      * The automation enables
        + Continuous: Monitoring, validation, integration, delivery, deployment
    - Secure Coding techniques
      * Determining how encryption will be implemented
      * Ensuring that memory management is handled correctly
    - Code Testing
      * One of the most important steps in SecDevOps
      * During the implementation and verification phases
      * Static Code analysis
        + Test ran before the source code is even compiled
      * Dynamic Code Analysis
        + Performed after the source code is compiled
        + Fuzzing is used for dynamic and provides random input to a program attempting to trigger exceptions