1. **1. SEC555.1: SIEM Architecture**
   SEC555.2: Service Profiling with SIEM

- Detection methods and relevance to log analysis
  - Attacker patterns
  - Attacker behaviors
  - Abnormalities
- Analyzing common application logs that generate tremendous amounts of data
  - DNS
    - Finding new domains being accessed
    - Pulling in addition information such as domain age
    - Finding randomly named domains
    - Discover domain shadowing techniques
    - Identifying recon
    - Find DNS C2 channels
  - HTTP
    - Use large datasets to find attacks
    - Identify bot traffic hiding in the clear
    - Discover requests that users do not make
      - Find ways to filter out legitimate noise
    - Use attacker randomness against them
    - Identify automated activity vs user activity
    - Filter approved web clients vs unauthorized
    - Find HTTP C2 channels
  - HTTPS
    - Alter information for large scale analysis
    - Analyze certificate fields to identify attack vectors
    - Track certificate validity
    - Apply techniques that overlap with standard HTTP
    - Find HTTPS C2 channels
  - SMTP
    - Identify where unauthorized email is coming from
    - Find compromised mail services
    - Fuzzy matching likely phishing domains
    - Data exfiltration detection
- Apply threat intelligence to generic network logs
- Active Dashboards and Visualizations
  - Correlate network datasets
  - Build frequency analysis tables
  - Establish network baseline activity

SEC555.3: Advanced Endpoint Analytics

- Endpoint logs

        - Understanding value
        - Methods of collection
            - Agents
            - Agentless
            - Scripting
        - Adding additional logging
            - EMET
            - Sysmon
            - Group Policy
        - Windows filtering and tuning
        - Analyze critical events based on attacker patterns
            - Finding signs of exploitation
            - Find signs of internal reconnaissance
            - Finding persistence
            - Privilege escalation
            - Establishing a foothold
            - Cleaning up tracks
        - Host-based firewall logs
            - Discover internal pivoting
            - Identify unauthorized listening executables
            - See scan activity
        - Credential theft and reuse
            - Multiple failed logons
            - Unauthorized account use
        - Monitor PowerShell
            - Configure PowerShell logging
            - Identify obfuscation
            - Identify modern attacks

SEC555.4: Baselining and User Behavior Monitoring

- Identify authorized and unauthorized assets
    - Active asset discovery
        - Scanners
        - Network Access Control
    - Passive asset discovery
        - DHCP
        - Network listeners such as p0f, bro, and prads
        - NetFlow
        - Switch CAM tables
    - Combining asset inventory into a master list
    - Adding contextual information
        - Vulnerability data
        - Authenticated device vs unauthenticated device
- Identify authorized and unauthorized software
    - Source collection

        - Asset inventory systems
        - Patching management
        - Whitelisting solutions
        - Process monitoring
    - Discovering unauthorized software
- Baseline data
    - Network data (from netflow, firewalls, etc)
        - Use outbound flows to discover unauthorized use or assets
        - Compare expected inbound/outbound protocol
        - Find persistence and beaconing
        - Utilize geolocation and reverse dns lookups
        - Establish device-to-device relationships
        - Identify lateral movement
        - Configure outbound communication thresholds
    - Monitor logons based on patterns
        - Time-based
        - Concurrency of logons
            - # logons by user
            - # logons by source device
            - Multiple geo locations
    - Endpoint baseline monitoring
        - Configure enterprise wide baseline collection
        - Large scale persistence monitoring
        - Finding abnormal local user accounts
        - Discover dual-homed devices

SEC555.5: Tactical SIEM Detection and Post-Mortem Analysis

- Centralize NIDS and HIDS alerts
- Analyze endpoint security logs
    - Provide alternative analysis methods
    - Configure tagging to facilitate better reporting
- Augment intrusion detection alerts
    - Extract CVE, OSVDB, etc for further context
    - Pull in rule info and other info such as geo
- Analyze vulnerability information
    - Setup vulnerability reports
    - Correlate CVE, OSVDB, and other unique IDs with IDS alerts
    - Prioritize IDS alerts based on vulnerability context
- Correlate malware sandbox logs with other systems to identify victims across enterprise
- Monitor Firewall Activity
    - Identify scanning activity on inbound denies
    - Apply auto response based on alerts
    - Find unexpected outbound traffic
    - Baseline allow/denies to identify unexpected changes

        - Apply techniques to filter out noise in denied traffic
    - SIEM tripwires
        - Configure systems to generate early log alerts after compromise
            - Identify file and folder scan activity
            - Identify user token stealing
            - Operationalize virtual honeypots with central logging
            - Allow phone home tracking
    - Post mortem analysis
        - Re-analyze network traffic
            - Identify malicious domains and IPs
            - Look for beaconing activity
        - Identify unusual time-based activity
        - Use threat intel to reassess previous data fields such as user-agents
        - Utilize hashes in log to constantly re-evaluate for known bad files

SEC555.6: Capstone: Design, Detect, Defend

Defend-the-Flag Challenge - Hands-on Experience