- Threat Hunting
    - The constant game of cat and mouse
        - Find the attacker before they find you
    - Strategies are constantly changing
        - Firewalls get stronger, so phishing gets better
    - Speed up the reaction time
        - Use tech to fight
- Intelligence fusion
    - An overwhelming amount of security data
        - Too much data to properly detect, analyze and react
    - Many data types
        - Dramatically different in type and scope
    - Separate teams
        - Security operations, security intelligence, threat response
    - Fuse the security data together with big data analytics
        - Analyze massive and diverse datasets
        - Pick out the interesting data points and correlations
- Fusing the data
    - Collect the data
        - Logs and sensors, network information, internet events, intrusion detection
    - Add external source
        - Threat feeds, governmental agents, advisories and bulletins, social media
    - Correlate with big data analytics
        - Focuses on predictive analytics and user behavior analysis
            - Mathematical analysis of structured data
- Cybersecurity maneuvers
    - In the physical world, move troops and tanks
        - Stop the enemy on a bridge or shore
    - In the virtual world, move firewalls and operating systems
        - Set a firewall rule, block an IP address, delete malicious software
- Automated maneuvers
    - Moving at the speed of light
    - The computer reacts instantly
- Combine with fused intelligence
    - Ongoing combat from many fronts
- Tomorrow its a different fight

- Vulnerability scanning
    - Usually minimally invasive
        - Unlike a penetration test
    - Port Scan
        - Poke around and see what's open
    - Identify systems

        - And security devices
    - Test from the outside and inside
        - Don't dismiss insider threats
    - Gather as much information as possible
        - We'll separate wheat from chaff later
- Scan types
    - Scanners are very powerful
        - Use many different techniques to identify vulnerabilities
    - Non-intrusive scans
        - Gather information, don't try to exploit a vulnerability
    - Intrusive scans
        - You'll try out the vulnerabilities to see if it works
    - Non-credentialed scans
        - The scanner cant login to the remote device
    - Credentialed scan
        - You're a normal user, emulates an insider attack
- Identify vulnerabilities
    - The scanner looks for everything
        - Not everything – specifically the signatures are the key
    - Application Scans
        - Desktop, mobile apps
    - Web application scans
        - Software on a web server
    - Network scans
        - Misconfigured firewalls, open ports, vulnerable devices
- Vulnerability research
    - The vulnerabilities can be cross referenced online
        - Almost all scanners give you a place to go
    - National Vulnerability Database: http://nvd.nist.gov/
    - Common Vulnerabilities and Exposure (CVE) cve.mitre.org
    - Microsoft security bulletins
    - Some vulnerabilities cannot be definitively identified
        - You'll have to check manually to see if a system is vulnerable
        - The scanner gives you a heads up
- National Vulnerability DB
    - Synchronized with the CVE list
    - Enhanced search functionality
- CVSS (Common Vulnerability Scoring System)
    - Quantitative scoring of 0 to 10
    - The scoring standards change over time
    - Different scoring for CVSS 2.0 vs CVSS 3.x
    - Industry collaboration
        - Enhanced feed sharing and automation
- Vulnerability scan log review

        - Lack of security controls - no firewall, no av, no anti spyware
        - Misconfigurations
            - Open shares, guest access
        - Real vulnerability
            - Especially newer ones
            - Occasionally the old ones
- Dealing with false positives
    - False positives
        - A vulnerability is identified that doesn't really exist
    - This is different than a low-severity vulnerability
        - Its real, but its not to be your highest priority
    - False negatives
        - A vulnerability exists, but you didn't detect it
    - Update to the latest signatures
        - If you don't know about it, you can't see it
    - Work with the vulnerability detection manufacturer
        - They may need to update their signatures for your environment
- Configuration review
    - Validate the security of device configurations
        - Its easy to misconfigured one thing
        - A single unlocked window puts the entire home at risk
    - Workstations
        - Account configurations, local device settings
    - Servers
        - Access controls, permission settings
    - Security devices
        - Firewall rules, authentication options

- SIEM
    - Security Information and Event Management
        - Logging of security events and information
    - Log collection of security alerts
        - Real time information
    - Log aggregation and long term storage
        - Usually includes advanced reporting features
    - Data correlation
        - Link diverse data types
    - Forensics analysis
        - Gather details after an event
- Syslog
    - Standard for message logging
        - Diverse systems, consolidated log
    - Usually a central log collector
        - Integrated into the SIEM

        - You're going to need a lot of disk space
            - No, more. More than that
            - Data storage from many devices over an extended timeframe
- SIEM data
    - Data inputs
        - Server authentication attempts
        - VPN connections
        - Firewall session logs
        - Denied outbound traffic flows
        - Network utilizations
    - Packet captures
        - Network packets
        - Often associated with a critical alert
        - Some organizations capture everything
    - Security Monitoring
        - Constant information flow
            - Import metrics in the incoming logs
        - Track important stats
            - Exceptions can be identified
        - Send alerts when problems are found
            - Email text call etc
        - Create triggers to automate responses
            - Open a ticket, reboot a server
- Security reports
    - Big data analytics
        - Analyze large data stores
        - Identify patterns that would normally remain invisible
    - User and entity behavior analytics (UEBA)
        - Detect insider threats
        - Identify targeted attacks
        - Catches what the SIEM and DLP systems might miss
    - Sentiment analysis
        - Public discourse correlates to real world behavior
        - If they hate you, they hack you
        - Social media can be a barometer
- SOAR
    - Security orchestration, automation, and response
        - Automate routine, tedious, and time intensive activities
    - Orchestration
        - Connect many different tools together
            - Firewalls, account management, email filters
        - Automation
            - Handle security tasks automatically
        - Response

- Make changes immediately