Detection

- IDS
    - Intrusion Detection System (signature based (eg. snort) or behaviour based).
    - Snort/Suricata/YARA rule writing
    - Host-based Intrusion Detection System (eg. OSSEC)
- SIEM
    - Security Information and Event Management.
- IOC
    - Indicator of compromise (often shared amongst orgs/groups).
    - Specific details (e.g. IP addresses, hashes, domains)
- Security Signals
    - Things that create signals
        - Honeypots, snort.
    - Things that triage signals
        - SIEM, eg splunk.
    - Things that will alert a human
        - Automatic triage of collated logs, machine learning.
        - Notifications and analyst fatigue.
        - Systems that make it easy to decide if alert is actual hacks or not.
- Signatures
    - Host-based signatures
        - Eg changes to the registry, files created or modified.
        - Strings in found in malware samples appearing in binaries installed on hosts (/Antivirus).
    - Network signatures
        - Eg checking DNS records for attempts to contact C2 (command and control) servers.
- Anomaly or Behavior Based Detection
    - IDS learns model of “normal” behaviour, then can detect things that deviate too far from normal - eg unusual urls being accessed, user specific- login times / usual work hours, normal files accessed.
    - Can also look for things that a hacker might specifically do (eg, HISTFILE commands, accessing /proc).
    - If someone is inside the network- If action could be suspicious, increase log verbosity for that user.
- Firewall Rules
    - Brute force (trying to log in with a lot of failures).

  - Detecting port scanning (could look for TCP SYN packets with no following SYN ACK/ half connections).
  - Antivirus software notifications.
  - Large amounts of upload traffic.

- Honeypots
  - Canary tokens.
  - Dummy internal service / web server, can check traffic, see what attacker tries.

- Things to Know About Attackers
  - Slow attacks are harder to detect.
  - Attacker can spoof packets that look like other types of attacks, deliberately create a lot of noise.
  - Attacker can spoof IP address sending packets, but can check TTL of packets and TTL of reverse lookup to find spoofed addresses.
  - Correlating IPs with physical location (is difficult and inaccurate often).

- Logs to Look at
  - DNS queries to suspicious domains.
  - HTTP headers could contain wonky information.
  - Metadata of files (eg. author of file) (more forensics?).
  - Traffic volume.
  - Traffic patterns.
  - Execution logs.

- Detection Related Tools
  - Splunk.
  - Arcsight.
  - Qradar.
  - Darktrace.
  - Tcpdump.
  - Wireshark.
  - Zeek.

- A curated list of awesome threat detection resources