Blue Team
ivan notes 2022

- **1. Fundamentals**
  - Storytelling
    - defense is all about stories
      - what questions to ask?
      - when to ask those questions?
      - how do we answer those questions?
      - what story is the evidence telling?
      - who needs to hear this story?
      - what story do i tell this person?
  - NIST CSF
    - I P D R R
      - Identify
        - develop org understanding to manage cyber risk to systems, people, assets, data, and capabilities
          - what is inside/outside your org?
          - who are the actors?
          - what assets do you have?
          - how do you model your threats?
      - Protect
        - develop and implement appropriate safeguards to ensure delivery of critical services
          - how do you secure systems?
          - how do you configure and read logging?
          - what tools and tech can you leverage?
          - how do you lock down networks, access controls, mobile, and cloud?
      - Detect

- develop and implement appropriate activates to identify the occurrence of a cyber event
  - now that defense is breached, how do you catch attacker?
  - what do these logs mean, whats normal vs anomalous?
  - what are the IOCs and TTPs?
  - what is the timeline of events
  - how do you link different types of logs together?
- Respond
  - develop and implement appropriate activities to take action regarding a detected cyber incident
    - how do you manage a security incident?
    - how do you react to live attackers?
    - who needs to be notified and when?
    - how do you collect forensic evidence that's admissible?
    - how do you build a legal case?
    - what goes into an IR report?
- Recover
  - develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber incident
    - how do you recovery from an incident?
    - whats a postmortem?
    - how do you secure your systems for next attack?

- CIA
  - confidentiality
    - is this private?
  - integrity
    - is this real?
  - availability
    - is this usable?
- AAA

- Authentication
  - who are you?
- Authorization
  - what can you do?
- Accounting
  - did you do this?

- Risk
  - vulnerability
    - a weakness, something we control
  - threat
    - can exploit the vulnerability, something we cant control
  - risk
    - combo of vulns and threats
      - Threat likelihood * Vuln Impact

2. Threat Modeling

- Threat Categories
  - Adversarial
    - deliberate undermining of orgs security
  - Accidental
    - mistakes, especially during routine work
  - Structural
    - something fails because of resource exhaustion, capacity, age, etc.
  - Environmental
    - natural or man-made disasters
- Threat actors
  - disgruntled employees
  - corp spies
  - thieves, vandals, etc.
  - Cyber
    - script-kiddie

- hacking groups
  - hactivists
  - black hat pros
- organized criminals
- nation states

- Threat models
  - define your scenario
    - what are your business reqs
    - what are your assets
      - what do you care about
      - what might attackers value
  - list out as many threats as you can
    - how does each threat target an asset
    - how does each threat attack CIA or AA
  - narrow your list of threats
    - what are you afraid of
    - categorize and prioritize threats
  - vulnerability-first
    - enumerate vulns, possible with scanners
    - create a threat model based on relevant threats
  - tool-based
    - Microsoft threat modeling tool
      - Define > diagram > identify > mitigate > validate
    - create data flow diagram, tool suggests common threats
  - Summary
    - we use categories to label threats
      - categorizing threats will help with assessing severity and likelihood
    - threat models help define what's in scope
      - you'll defend against what's in the threat model

3. Asset Mgmt

- Identify 1
  - who/what are you protecting?
    - why are you protecting that?
  - what threats are you afraid of?
  - what vulns do your systems have?
  - what are your risks?
  - who needs to know these answers?
  - who do you need to inform?
    - why?
- Identify 2
  - people
  - asset inventory
    - network maps
      - dependencies
  - vulns
    - threats
      - risk
- Mgmt
  - track assets and associate identifiers from all sources
    - many vendors and solutions
    - link identifiers across different layers and different sources
  - given some info (hostname, IP, etc.) can we find all associated devices?
  - time is a key aspect for many fields
    - computer may be wiped and re-issued
    - DHCP leases may change on renewal
  - record any changes with timestamps
- Identifiers
  - asset unique ID
    - we create this
  - device/hardware info

- asset tags
- people and authorized users
  - who was this device issued to? connect to org chart
- physical location
  - which dept or office was this device issued to?
- OS and installed software
  - what is running on this machine?
  - what software licenses are active?
- network identifiers
  - MAC address
    - hostname
      - security log status
  - IP address
    - certificates (user and device)
  - authenticated users
    - backup or patch status

- Recon
  - active
    - activity that can be seen or logged
      - port scanners: nmap, angry, IP, other tools
    - external vs internal
      - vulnerability scanners
  - passive
    - packet analysis
      - netflow
    - log analysis
      - routers, switches, DHCP, DNS, firewalls
    - config files
      - network devices
    - host config

- apps (installed/running)
- domains, IP blocks, certificates
  - org data

4. Vulnerability Mgmt

- Servers & Apps
  - missing patches
    - outdated, unsupported systems or apps
  - buffer overflows
    - priv esc
      - arbitrary code exec
  - insecure protocols
    - debug info
      - injection
- Networks
  - firmware updates
    - outdated ciphers (SSL/TLS)
      - dont use TLS.12
  - cert issues
    - mismatched names, expiration, unknown CA
  - DNS
    - zone transfers, open resolvers, amplification
  - NAT IP exposure
  - VPN, SSH, RDP
- VMs
  - VM sandbox escape
    - patches
  - mgmt interfaces
  - virtual guests, virtual networks
- IoT and other
  - firmware never gets udpates

- hardcoded passwords
- smart power gris
- microphones and cameras
- indicators of home presence
  - smart locks/bulbs/alarms

- Scanning
  - scanners
    - nessus, nikto, openVAS, WpScan, etc.
    - vulnerability reports
  - credentials and agents
  - CVSS score
- Why?
  - regulations
    - PCI DSS, FISMA, HIPAA
  - business impacts
    - CIA: limited, serious, severe/catastrophic
  - security and privacy
    - GDPR
    - internal & external policies
- How?
  - detection > testing > remediation
  - prioritization
    - criticality, difficulty, severity, exposure
  - documentation
    - exceptions, false positives, processes
  - SLO's and SLA's

5. Firewalls

- Prevent Recon
  - limit services/attack surface
    - block ping

- IDS/IPS
  - snort, bro
- harden DNS servers
  - dont allow zone transfers to just anyone
- whois privacy services
- social media policies

- Firewalls
  - device or software designed to filter network traffic
    - allow, block, other
  - packet filtering
    - stateful inspection
  - app specific firewalls
    - NGFW

- Placement
  - on your host
    - between your apps and the network
  - at network segment boundaries
    - between 1 network segment (LAN) and another (DMZ)
  - on your home router
    - between your LAN and the internet (WAN)

- Host based
  - Windows
    - defender
    - group policy
  - Mac
    - security preferences
    - Lulu
  - Linux
    - iptables
    - ufw

6. IDS/IPS

- IDS/IPS almost interchangeable
  - actions
    - allow, deny, alert
  - network vs host based
  - deeper packet inspection
    - trade-offs with resource usage
  - Detections
    - signatures
    - anomalies
  - IPS= active, can prevent
    IDS = passive, only detect & alert
- Snort
  - NIDS
  - inspects packets over a network and make decisions; signature based
    - alert
  - rule vs heuristics
    - threshold can still be rule-based
  - rules
    - rule header
      - Action, 5-Tuple, (direction)
      - always start with the 5-Tuple
        - src IP, src port, dest IP, dest port, protocol
        - the direction will generally be src -> dest
        - may be "any"
    - rule options
      - option keyword, protocol arguments, ...
      - SID = unique identifier, user large numbers (>1,000,000)
      - msg = human-readable msg
      - others: flags, thresholds, packet bytes, etc

- Example rule
  - Alert when the word "hacked" appears in the contents of a packet"
    - sudo vi ~/snort/example.rule # make a new rule file

      i # enter insert mode

      alert tcp 192.168.56.100 any -> 192.168.56.200 any (msg:"'hacked' detected!!!"; content:'hacked'; sid: 1000001)

      :wq # save and close

7. Defense in Depth

- Security layers
  - Data
    - App
      - Endpoint/System
        - Network
          - Perimeter
  - physical
    - gates, manned roadblocks, lobby reception, badging, guards, biometrics
  - network
    - firewalls, segmentation, DMZ, jump boxes, NIDS/NIPS, web proxy, VPN, NAC, logging
  - host
    - firewalls, HIDS/HIPS, TPM, passwords, MFA, logging
  - software
    - secure code, code reviews, security assessments, SAST, DAST
- controls
  - types
    - administrative
    - physical
    - technical
  - internal types

- preventative
- detective
- corrective

- Assess
  - single points of failure
    - cascading failures
  - views of architectures
    - operational
    - technical
    - logical
  - Human elements

8. Logs

- Detection stories
  - start with an alert, or single IOC
    - create hypothesis about what could explain it
    - gather additional context and evidence
    - revise hypothesis
      - document everything
    - write conclusions and cite supporting evidence
  - Hypotheses > evidence > revise > conclusions
- what are they?
  - an official record of events
    - contain semi structured data about what happened
    - timestamp & message
      - actors, actions, errors
  - types
    - network, host, app, physical
- why collect them?
  - CIA, AAA
    - tracking who, when, and what resource

- nonrepudiation
  - actors cannot refute actions taken
- laws
  - data retention laws and policies
    - presidential records
- historical records - we may get new info

- how to read them?
  - determine what sort of system created these logs
    - network, host, app, physical, access, etc
    - narrow this down as much as possible - use context clues
  - map out the structure
    - timestamp, message, delimeters, fields
    - is each line separate, or are groups of lines for a single log message
  - identify additional related info
    - network models, OS, types of apps
  - parse content
    - what is the story that the logs are telling?
    - make sure TIMESTAMPS are config'd properly

- IOCs
  - evidence left behind by attacks
    - logs
      - requests made, errors, actions taken
    - artifacts
      - user accounts, services, machines
    - metrics
      - service degradation, strange activity upticks, failure rates
  - MITRE ATT&CK - industry standard language

- detecting attacks
  - how do we know we've been breached?
    - alerts, anomaly detection, reports, service issues

- get report > investigate issue
  - hypotheses > evidence'
  - conclusion with reasoning and supporting evidence
- network detection
  - routers
    - Netflow, RMON, SNMP
  - scanners
    - ping, iPerf, network mapping
  - network taps
    - pcap, other analyses
  - firewalls
    - dropped vs allowed packets
  - issues and attacks
- host detection
  - host device/machine
    - system resources, software/apps, access/privilege
  - monitoring tools
    - Win - perfmon, resmon, sysinternals
      Lin - ps, top, df, w
  - where are alerts coming from?
    - SCCM - central logging tools
      AC, authentication/access logs
- app detection
  - service status, failures, actions
  - what type of errors to catch?
    - anomalous activity
      - new accounts - AAA
    - unexpected output
      - unexpected outbound comms (networks)
    - service interruptions

- memory overflows

- Triage
  - example: network issues and attacks
    - scans/probes, DOS, rogue devices, link failures, beaconing
    - how do we triage and deal with these issues?
      - use tools, help identify and prioritize alerts
      - IPS - block/drop traffic
      - 3p providers, sinkhole traffic from DOS
      - use network maps to identify what is working
      - think about CIA - is it even a security issue?
  - SIEM
    - Splunk
      - investigations that correlate logs from different sources
        - type of tool defenders use to correlate logs across time and other dimensions

9. File Systems

- what?
  - ways to store and organize info on a disk
    - has a structure and a filing system
- data categories
  - file system
    - general file system information - a map
  - content
    - actual data that it stored - data units
    - deletion will sometimes not actually delete the content, just the pointers to the content
  - metadata
    - data that describes data
      - localization, size, timestamps, etc
      - slack space: commonly used to hide information

- file name
  - human interface/names for files
- application
  - other, special features

- Forensics
  - handling evidence - chain of custody
  - SIFT - toolkit of forensic software
    - classes of tools
      write blocker, memory analyzer, etc.

10. Incident Response

- What is an incident?
  - event
    - any observable occurrence in a system or network
  - adverse event
    - any event that has negative consequences
  - security/privacy event
    - any event that relates to a security/privacy function (CIA, AAA, etc)
  - security/privacy incident
    - a violation of security/privacy policies or practices
- Phases
  - 1. prep > 2. detection & analysis <> 3. containment eradication & recovery > 4. post-incident activity > (loop)
  - Prep
    - encompasses identify & protect
    - creating org policies
      - staff members & authority
      - partner teams (legal, PR, etc)
    - hardware, software, info required
      - forensics (hardware, bootable images, backup/cloning device)
      - logging/monitoring and alerting systems

- procedures and playbooks - training
- continuous improvement

- baseline normal behaviors
  - understand expected behaviors
- establish logging policies
  - synchronize clocks
- maintain org knowledge base
  - asset inventories

- Detection & Analysis
  - encompasses Detect
    - validate event -> incident
  - where do we get detection indicators?
    - alerts, logs, public info, people
  - start finding context and stories
    - perform event correlation to combine sources - SIEM
  - capture network traffic or other evidence
    - consider storage and bandwidth
  - filter info/noise
  - escalate - seek assistance from internal/external resources
- Containment, Eradication, Recovery
  - encompasses respond & recover
  - escalated a detection into an incident
  - choose and implement a containment strategy
    - trafeoffs between CIA, acting too early vs acting too late
  - gather more (legal) evidence
    - know all of the things that happened
  - identify attackers
    - actos, systems, infra
  - eradicate indicent
    - recover normal business operations

- evidence preservation
- consider SLA and other business proccess
  - this is what makes money
- costs and effectiveness of the strategy
  - time, money, degradations of the business process - how much can you stop the attack?
- segmentation - proactive
  - isolation
    - removal
- re-imaging is the only way to be certain about sanitizing
  - patch vulns
    - restore system from backups
- audit accounts and permissions
  - verify logging systems
- conduct vuln scanning
  - continuous, tack changes over time
- verify business processes

Post-incident Activity

- lessons learned review
  - reports and meetings
    - timeline of events
      - evidence retention
    - root cause, evidence details, actions taken in IR, impact of incident, validation efforts
- blameless culture
  - dont attach shame to the errors
    - encourage learning and growing
  - engage humans to fix issues
    - accountability, empowerment
- postmortems

- whenever there is impact above a certain threshold
  - larger security incidents (data loss, prolonged efforts, actions were taken)
- state facts, dont point fingers
  - gather learnings and share them for the future
- action items to change stuff that went wrong
  - focus on fixes on processes
- root cause
  - how did this incident start
- detections
  - how did we catch the incident
- action items
  - how can we improve defenses or processes