SE6014: SECURITY MONITORING & THREAT DETECTION

[PRELIMS FROM PROF. ANWIT]

informationsecurity.wustl.edu/vulnerabilities-threats-and-risks-explained/

Security — process of maintaining acceptable level of perceived risks
- achieved using controls

Threat → **Relations to:**
- Risk: potential for threat agent to exploit a vuln.
- Vulnerability: flaw/weakness in asset's design, implementation, or op. & mgmt that could be exploited by a threat

party w/ capabilities & intentions to exploit vulnerability
- structured (ex., organized criminals, terrorists, spies) or unstructured

Assessment
- Response (corrective ctrls)
- Protection (preventive ctrls)
- Detection (detective ctrls)

Types:
- Human errors
- 3rd party failures
- System failures
- Malicious actions
- Natural & social phenomena

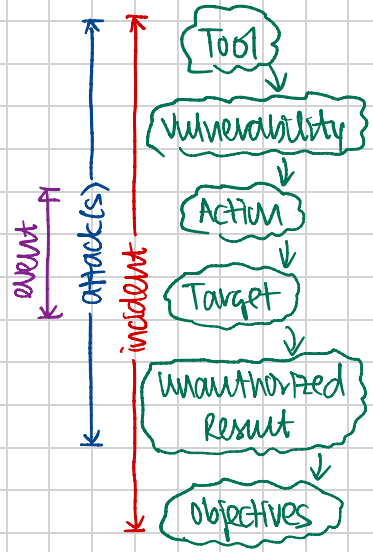
- insider threats (ex., data theft, data manipulation)
- physical threats (ex., terrorist atk, document fraud, unauthorized entry)
- cyber threats (ex., malware, DoS, penetration atks)

Cyber Threat Intelligence
- systematic collection, analysis & dissemination of info abt company's op. in cyberspace & physical space (to an extent)

evidence-based knowledge abt existing/emerging menace or hazard to assets used to inform decisions regarding subject's response to menace/hazard

Threat Intelligence → **Validities:**

- **Strategic**
  - * long-term changes in threat landscape
  - * long-term objectives of adversaries
- **Operational**
  - * shot to medium changes in threat landscape
  - * current techniques used by adversaries
- **Tactical**
  - * current events w/in threat landscape



Monitoring
- threat-centric
  - network security monitoring op. is designed to detect adversaries, respond to their activities & contain them before they can accomplish their mission
- vulnerability-centric
  - continuous monitoring op. strives to find an org's computers, find vulnerabilities, & patch those holes if possible

Cycle
- Planning, Requirements & Direction
- Collection
- Analysis & Processing
- Production
- Dissemination

Stages
- Ad-hoc — orgs handle tasks manually w/ little/no defined process; tasks may be handled inconsistently
- Formal — expectations, capabilities & processes are documented & understood; tasks at this level are repeatable & have consistent outputs, but largely handled manually
- Efficient — automated processes streamline handling of tasks & data, incl. prioritization; increased visibility into ops. thru reporting metrics
- Proactive — orgs can identify intelligence gaps & anticipate future needs

I. FOUNDATIONS OF CYBER SECURITY FRAMEWORKS

- Lacks visibility
- Limited telemetry
- Static rule-based detections
- Lack of automation
- Lack of integrations

Legacy SOC

Modern SOC
- Tech stack
  - NG Analytics
  - AI/ML-based solutions
  - Integrations btwn tools & solutions
- Telemetry: threat logs fm various solutions
- Threat Intel collections
- Orchestration & automation

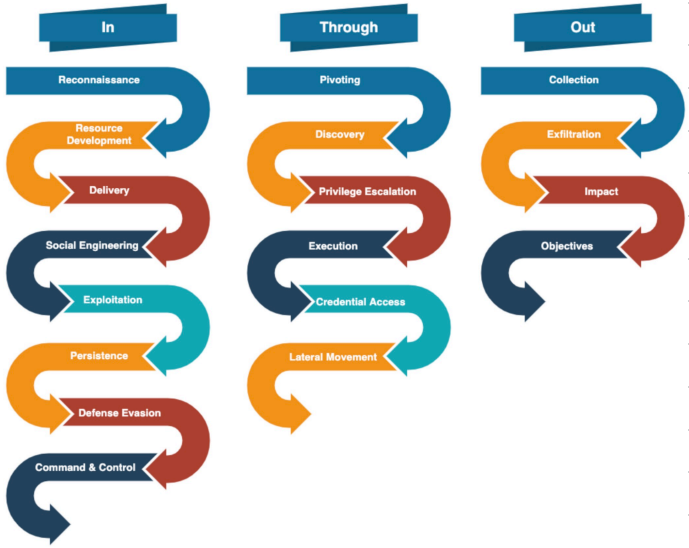
Security Ops Center (SOC)
- Security Architecture
- Threat Intel
- DFIR Incident Response

Cyber Defense
- FXS
  - Offensive Security
  - Vuln. Mgmt
- Red-teaming: atk against BLUE
- Pen-testing (BLUE team): defence against RED
- Purple-teaming: RED + BLUE team aspects

to safeguard & defend an org's digital assets, infrastr. & info fm cyber threats

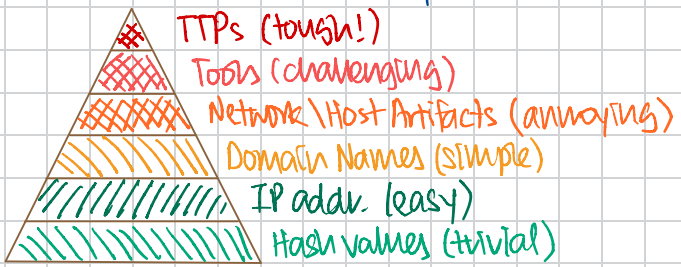
Critical Frameworks & Concepts
1. Cyber Kill Chain
2. Unified Kill Chain
3. Diamond Model
4. Pyramid of Pain
5. MITRE ATT&CK
   - use cases
     - detection
     - threat intelligence
     - assessment & engineering
     - adversary emulation

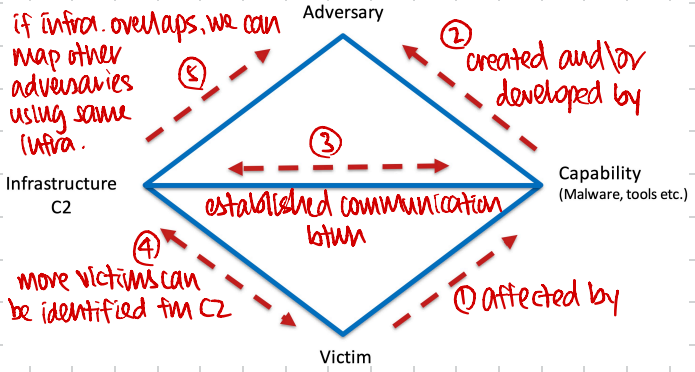
1. Reconnaissance — Gather info
2. Weaponization — Develop weapon
3. Delivery
4. Exploitation — of vuln.
5. Installation
6. Cmd + Ctrl (C2)
7. Actions on Objectives



Threat Actors

1. script kiddies: unskilled indvs using scripts/progs developed by others for malicious purposes
2. hacktivists: criminal groups united to carry out cyberatks to support political causes; ∞ & motivated
3. cybercriminals: criminal groups carrying out cyberatks; financially motivated
4. APT/nation state:
   - * APT: well-resourced adversary engaged in sophisticated malicious cyber acts.; targeted & aimed at prolonged network/sys. intrusion
   - * APTs are often nation-state actors or state-sponsored groups
5. Insiders: adversary originating fm w/in org.





Cyber Kill Chain — Martin, L., 2011

* series of steps that trace stages of cyberatk
  ↳ emphasizes atker's steps for successfully compromising target
  ↳ breaking chain at any stage ⇒ atk disrupted
* 1° focus: understand & disrupt atk process instead of analyzing adversary's motivations or capabilities

Stages

① Reconnaissance (Observation Stage)
* atkers identify targets & make plan of action
* activities
  - researching potential targets
  - determining vulns.
  - exploring potential entry pts.

② Weaponization
* atkers create atk vector to use in cyberatk
  ↳ exploit vuln. identified in reconnaissance phase
* may also try to ↓ likelihood of being detected by any security solutions in place

③ Delivery (atker officially launches target)
* atk vector delivered thru medium (ex., phishing email) or hacking into target's sys./network

④ Exploitation
* malicious code executed w/in target's sys.
* atkers can further exploit target sys. (ex., install tools, run scripts, mod security certs)
* ex. exploitation atks.: scripting, dynamic data exchange, local job scheduling

⑤ Installation
* atk vector installed on target sys.

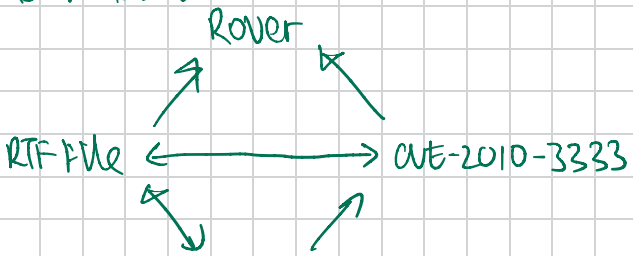
⑥ Command & Control (C2)
* atker uses installed atk vector to ctrl devices or identities remotely w/in target's network
  ↳ may also move laterally during C2 phase to avoid detections & est. more pts. of entry

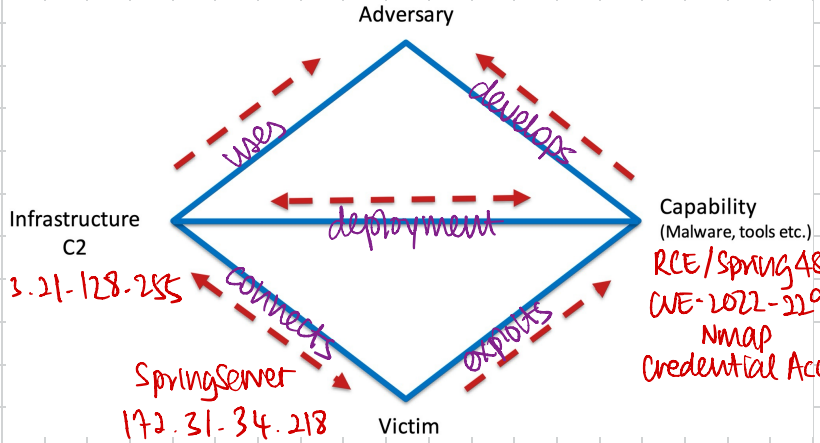
⑦ Actions on Objectives
* atker takes final steps to carry out original obj. (data theft, destruction, encryption, exfiltration)

Diamond Model — Caltagirone et al., 2013

* framework for investigating & analyzing cybersec incidents
* 4 main components
  ↳ adversary: atker/group responsible for cyber incident
  ↳ infrastructure: tech resources/assets used by adversary during atk (ex., servers, domains, IP addrs.)
  ↳ capability: method/tool/technique used by adversary during atk (ex., malware, exploits)
  ↳ victim: indv/org. targeted by adversary
* benefit
  ↳ provides clear, organized way to structure & process data relating to cyber threats & atks

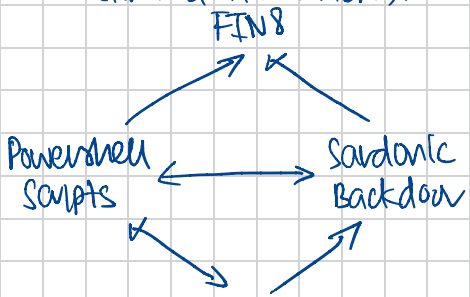
Rover Malware:





The FIN8 attacks in 2021, targeting organizations in the financial, hospitality and entertainment space with a goal of financial gain, were a diamond event.
↳ The adversary (FIN8) used infrastructure (Powershell scripts) to deploy a capability (Sardonic Backdoor) while attacking victims (financial institutions).

Ex: securityboulevard.com/2023/04/a-guide-to-the-diamond-model-of-intrusion-analysis



Ex: linkedin.com/pulse/diamond-model-mitre-attck-advanced-cybersecurity-guzmán-mercado/

detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

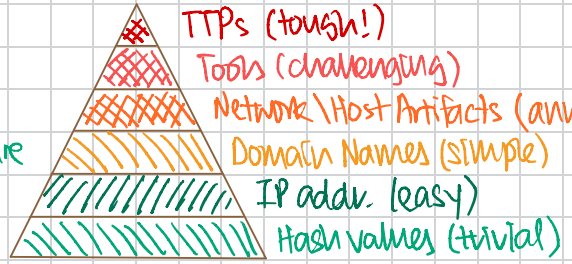
Pyramid of Pain (by David Bianco)

* shows relship btwn types of indicators used to detect adversary's activities & how much PAIN caused to them if you can deny those indicators to them
* emphasis on ↑ adversaries' op. costs (ie., PAIN)

Types of Indicators

Hash Values → hashes (SHA1, MD5, etc.) corresponding to specific sus. or malicious files
↳ often used to provide unique refs. to specific samples of malware or files involved in an intrusion

* most accurate indicators (odds of 2 files w same hash v. low)
* problem: any change to file results in completely diff. & unrelated hash value



IP Addresses → atks require network connections; network connections est. btwn IP addrs.

* problem: ∃ a lot of IP addrs, adversary can change used IP addr. at will easily
  ↳ IP changing more frequent if adversary uses anon. proxy service (ex., Tor)

Domain Names → domain name itself or a subdomain

* slightly more of a pain to change
  ∵ domain names need to be registered, paid for, & hosted somewhere
* domain name changes take ~1-2 days to reflect thruout Internet
* problem: ∃ many DNS providers w lax registration stds.

Network Artifacts → observables caused by adversary acts on network \ network bytes as a result of adversary's interaction
ex., URI patterns, C2 info embedded in network protocols, distinctive HTTP User-Agent or SMTP Mailer values

Host Artifacts → observables caused by adversary acts. on ≥1 of your hosts
ex., registry keys\vals. known to be created by specific pieces of malware, files\dirs dropped in certain places or using certain names, names\descs.\malicious srvcs.\anything distinctive

focus: pieces of activity that might tend to distinguish malicious acts. frm those of legit users

* detection & response to network\host artifacts → atker needs to reconfig and\or recompile tools

ex., Atker's HTTP recon tool uses a distinctive User-Agent str. when searching Web content
↳ block this User-Agent → atker needs to — find out how you found recon tool, then fix it

User-Agent request header: characteristic string that lets servers & network peers identify app\OS\vendor\ver. of requesting agent.

Tools → software used by adversary to accomplish mission
ex., utils - to create malicious docs for spearphishing, backdoors to establish C2, pswd crackers, other host-based utils (post-compromise)

* adversaries need to expend time & resources in
  ↳ research (find existing tool w same capabilities),
  ↳ development (create new tool if they are able), &
  ↳ training (figuring out how to use tool & gain proficiency in using it)
* ex. tool indicators: AV or YARA signatures

Tactics, Techniques & Procedures (TTPs) → how adversaries accomplish their mission frm recon → data exfil. & every step in btwn
ex., "spearphishing w trojaned PDF file", "spearphishing w link to malicious .SCR file disguised as ZIP", "dumping cached authentication creds. & using them in Pass-the-Hash atks"

* detection & response at this level = operating directly on adversary behavior, & their tools
  ex., detect pass-the-hash atks themselves (ex., by inspecting Windows logs) instead of tools used to carry those atks
  ↳ adversaries forced to learn new behaviors (MOST CONSUMING THING POSSIBLE!)
* Tactic → highest-level description of actor's behavior
  Technique → more detailed desc. of behavior in context of tactic
  Procedure → lower-level, highly detailed desc. of behavior in context of technique

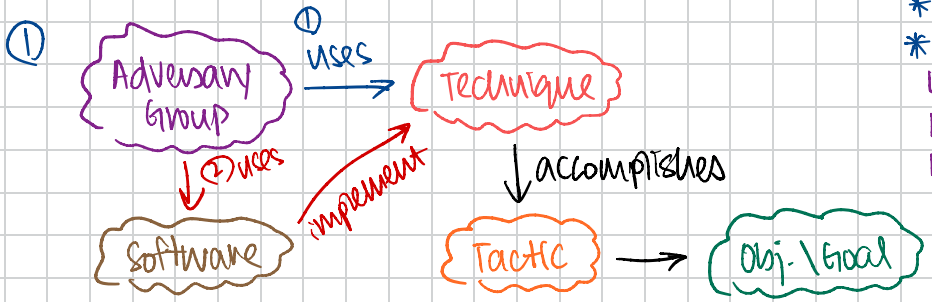
Adversarial Tactics, Techniques & common Knowledge

ATT&CK Framework

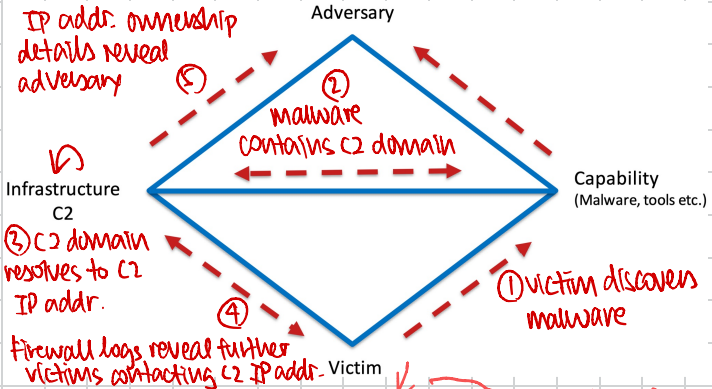
↳ knowledge post of adversary behavior \ "playbook"
↳ based on real world cases & observations
↳ common language in industry
↳ driven by the community

attack.mitre.org/resources/attack-data-and-tools
mitre-attack.github.io/attack-navigator/ → primarily using Enterprise Layer

attack.mitre.org/groups → list of APTs

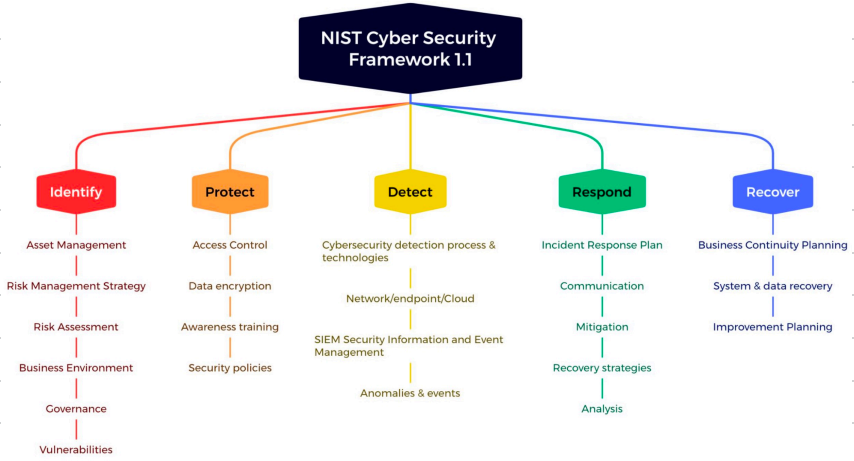


ex., Ocean Lotus → uses → Credential Dumping
Ocean Lotus → uses → MimiKatz
MimiKatz → implements → Credential Access
Credential Access → accomplishes → Obj. \ Goal



NIST Framework NIST: National Institute of Standards & Technology

* ver. 1.1: Apr 16, 2018 ; ver. 2.0: Aug 6, 2023
* core fxs:
  ↳ Govern (GV) — establish & monitor org's cybersec. risk mgmt strategy, expectations, & policy
  ↳ Identify (ID) — help determine the current cybersec. risk to the org
  ↳ Protect (PR) — use safeguards to prevent or reduce cybersec. risk
  ↳ Detect (DE) — find & analyze possible cybersec. attks & compromises
  ↳ Respond (RS) — take action regarding a detected cybersec. event
  ↳ Recover (RC) — restore assets & ops. that were impacted by a cybersec. incident



(ChatGPT)

Strengths

* comprehensive analysis of atk
  ↳ provides structured framework for analyzing intrusion events fm multiple perspectives
* attribution
  ↳ by examining adversary component, model facilitates attribution of atks to specific threat actors \ groups (crucial fo determining appropriate response measures)
* contextual understanding
  ↳ helps contextualize intrusion events by considering technical aspects + motivations & capabilities of adversaries

Weaknesses (ChatGPT)

* high complexity (esp. fo inexperienced analysts)
  ↳ may require significant expertise to apply
* strict data requirements (accurate & comprehensive)
  ↳ needed fo real-time \ sophisticated atks, but ✕ always available
* interpretation of model may vary btwn analysts
  ⇒ subjective assessments of intrusion events