Most common issues

- What are the most common defensive issues found in practice: very important problem
- Many studies, the most useful is the one made by the NSA and the CISA, they analyze a lot of organizations both for preventive purposes and for analyze/recover after an attack. They collected and shared the top ten cybersecurity misconfigurations that can affect defense significantly
- It is not a scientific work, we don't know how the rank is obtained, there is no info about impact or frequency
- A seguire lista di alcuni di questi problemi della lista

1. **Default configurations of software and applications**
   - Default credentials: many software manufacturers release network devices containing predefined default credentials for their built in administrative accounts → organizations do not change those predefined default credentials
   - Default service permissions and configuration settings: certain services may have overly permissive access controls or vulnerable configurations by default
     - Insecure active directory certificate services → if you install this and do not change the default configurations, a user can request a certificate where the user himself specifies the subject of that certificate
     - Insecure legacy protocols/services (→NTLM)
     - Insecure server message block (SMB) service → (SMB protocol for sharing folders and printers) is a problem because older versions of those servers have high impact and risk vulnerabilities, many organizations failed to patch the vulnerabilities
   - Assurdo che un software sia venduto con configurazioni di default insicure, però sicuramente un motivo c'è: active directory è molto complesso, non è facile capire che una configurazione è insicura e anche dopo averlo capito di solito non è facile cambiarle (ci sarà un motivo se le case produttrici le distribuiscono con la configurazione di default

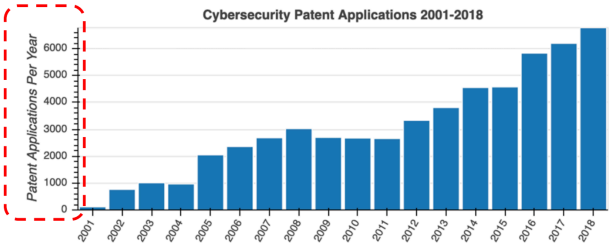
- Key general remarks: these misconfiguration illustrate
  - A trend of systemic weaknesses in many large organizations, including those with mature cyber postures
  - The importance of software manufacturers embracing secure by design and secure by default principles: manufacturers must reduce the prevalence of these misconfigurations → stop selling things that are not secure by default, the costumes cannot be the ones that fix the mistakes

2. **Improper separation of user/administrator privilege**
   - Excessive account privilege: when account privileges are overly permissive, users can see and/or do things they should not be able to, which becomes a security issue as it increases risk exposure and attack surface
   - Elevated service account permissions: applications ofter operate using service accounts to access resources. When a malicious actor compromises an application using a service account, they will have the same privileges and access as the service account
   - Non essential use of elevated accounts: using an elevated account for normal day to day, non administrative tasks increases the account's exposure and, therefore, its risk of compromise and its risk to the network
3. **Insufficient internal network monitoring:**
   - Some organizations do not optimally configure host and network sensors for traffic collection and end host logging
   - These insufficient configurations could lead to undetected adversarial compromise
   - Improper sensor configurations limit the traffic collection capability needed for enhanced baseline development and detract from timely detection of anomalous activity (and false positives)
4. **Lack of network segmentation** → in profs opinion is the most effective and most undervalued defensive action
5. **Poor patch management**
6. **Bypass of system access control**
7. **Weak of misconfigured MFA methods**
8. **Insufficient ACLs on network shares and services**
9. **Poor credential hygiene**
10. **Unrestricted code execution**

- We are not supposed to know all of them (chissà)

Reasoning about defense

- For any issue of the ten in the list, is possible to map it to a specific ATT&CK tactic (and technique), for each issue, they provide specific and detailed mitigations (ci riferiamo sempre alla pubblicazione di NSA e CISA con la lista dei 10 problemi principali, sono loro che ci danno un modo per mitigare)
- The problem: the issues are described in terms of the same framework (ATT&CK) (you can clearly understand what the role is from an attacker point of view), the mitigations are described in therms of 6 different frameworks → it is a mess, so reasoning about defense is a nightmare
- Example issue
  - → ATT&CK tactic/technique: nella descrizione di un attacco, ci sono tutti i link riferiti alla tabella MITRE, quindi tu ti puoi mettere lì, leggere la spiegazione, aprire il link e capire bene di cosa si tratta (il senso è che è tutto bello organizzato in un posto solo pronto all'uso)
  - → Mitigation: un macello, è pieno di riferimenti ad altri documenti, link a diversi framework (anche nei suggerimenti riferiti allo stesso attacco), non c'è una descrizione chiara e riferita a un modello organizzato con potrebbe essere il modello MITRE degli attacchi
- There are a lot of many best practices, frameworks → there is not a standard yet for reasoning about defense (big mess)
- Reasoning about the problem
  - Given a defensive mechanism/tool/device: how to know what does it prevent/detect, is it a help for recovering/forensics? How does it do that and with which limitations?



- This graph shows the number of patent applications in cybersecurity defense issued every year → there is no way for reasoning systematically about every of these mechanisms/tools
- Now we will look at the defense support in ATT&CK (data sources, mitigations) and then we will see an experimental (very promising) framework for defense: D3FEND (developed by MITRE)

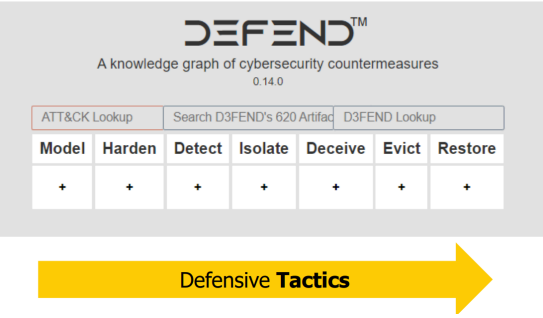
Defenses in ATT&CK

- Data sources:
  - There is a categorization of data sources in ATT&CK, that represent the various subjects/topics of information that can be collected by sensors/logs
  - It is a predefined list, each data source is mapped to techniques that may potentially be detected (with a specific information collected)
  - Data source examples:
    - Firewall: They describe what a firewall is (more or less), then which attack techniques can be detected by using a firewall and the attack techniques that may operate on a firewall (quindi dicono cos'è, cosa può rilevare e come può essere attaccato)
    - User Account
  - Collect informations is just the preliminary step, not really a defensive concept
- Mitigations:
  - Security concepts and classes of technologies that can be used to prevent a technique form being successfully executed
  - Also a predefined list, each mitigation is mapped to a technique that may potentially be prevented
  - The description of mitigations is very high level (very general), quite far away from operational suggestions and not useful for understanding pros/cons

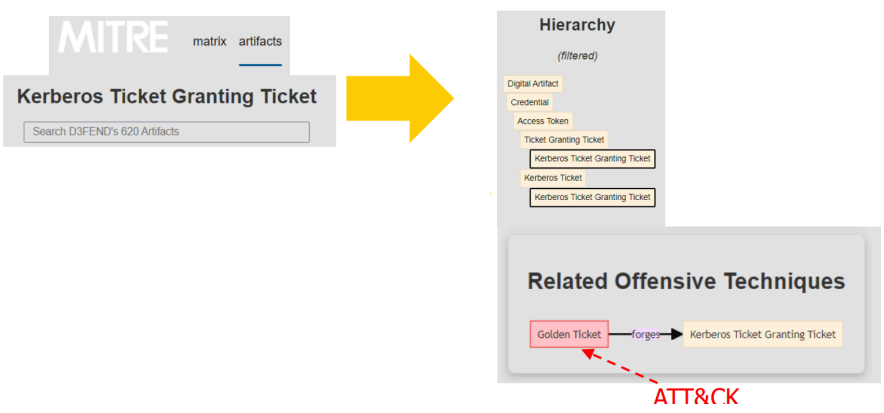
MITRE D3FEND

- Currently the most interesting framework
- It is a knowledge base (compilation) of defensive techniques and their relationship to adversary techniques
- The ATT&CK framework is a standard, mature and used, the D3FEND framework is a maturing research project started in 2021, version 1 release planned for this year

Defense

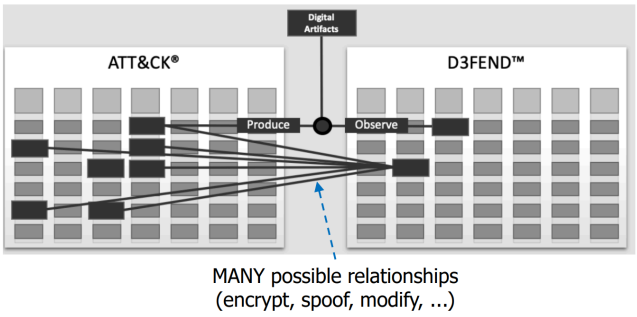


- The D3FEND framework consists in several tactics that can be used from a defender point of view, each tactic can be implemented with several techniques (e fin qua è come ATT&CK)
- Tactics:
  - Model: have an idea of the environment
    - Create and maintain a common understanding of the systems being defended, the operations on those systems, actors using the systems, the relationships and interactions between these elements
    - Techniques: assert inventory, network mapping, operational activity mapping, system mapping
  - Harden: modify the configurations of the environment to make for the attackers hard to enter
    - Increase the cost of computer network exploitation
    - Techniques: application hardening, credential hardening, message hardening, platform hardening
  - Detect: after the attack is occurred
    - Identify adversary access to or unauthorized activity on computer networks
    - Techniques: file analysis, identifier analysis, message analysis, network traffic analysis, platform monitoring, process analysis, user behavior analysis
  - Isolate: make it difficult for the attacker to move
    - Create logical or physical barriers in a system which reduces opportunities for adversaries to create further accesses
    - Techniques: Execution isolation, network isolation
  - Deceive
    - Advertise, entice and allow potential attackers access to an observed or controlled environment (questa al prof non piace, non ne parla, è in grigetto nelle slide)
  - Evict: clean up all
    - Remove an adversary from a computer network
    - Techniques: credential eviction, file eviction, process eviction
  - Restore
    - Return the system to a better state
    - Techniques: restore access, restore object
- The framework has a logical temporal evolution (le tattiche ovviamente si possono comunque usare in ordine sparso e/o andando avanti e indietro)
- Mindset: distribute the budget on multiple tactics, at a basic level the organizations have to focus on detect, isolate and restore because in most cases organizations focus only on hardening (initial access) and it is not sufficient (assumendo che la parte del model sia già stata fatta in modo appropriato, altrimenti non ha neanche senso parlare delle altre tattiche)
- In addition on the tactic, there is a list of defensive techniques, for each of these is given the definition, how it works and the related ATT&CK techniques
  - Example of MFA: what is, how works and considerations, useful whit defense evasion, initial access, impact, persistence, privilege escalation (e relative tecniche)
- D3FEND digital artifacts: knowledge of digital objects of interest in cybersecurity
  - Example Kerberos TGT is a digital artifact of interest, they describe what is and what an attacker can do with it
  - The digital artifact associated offensive techniques are in the ATT&CK framework, the countermeasure technique in D3FEND framework



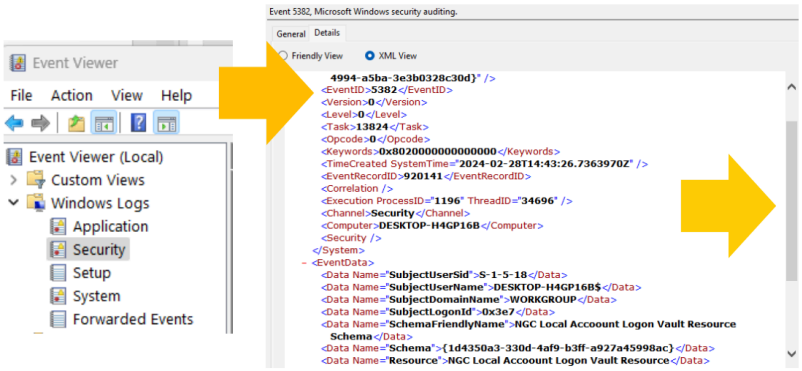
Defense

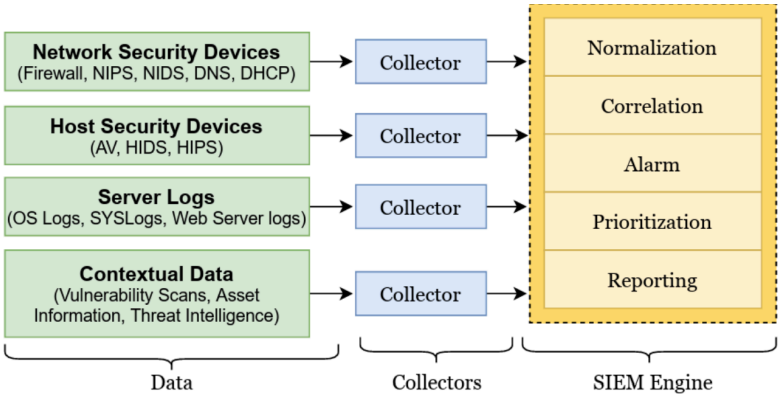
- Then there is also the mapping from the ATT&CK to the D3FEND frameworks



SIEM/SOC

- Specific defensive concept very important in practice and it's effectiveness and relevance is often misunderstood
- We know that in a system there is always at some point some informations about the activity in that systems are recorded ⟶ this point is called LOGS
- Log's:
  - In a organization there are many sources (logs) ⟶ applications, host (operating systems), networks devices
  - All the informations are extremely important for functionality monitoring, troubleshooting, security
- Think for one moment about the number and types of logs, for a given log how many events there are per time unit
- For a given log type, how many event types (event description depend on event type)
- Key fact and problem:
  - Per ogni tecnologia di log, c'è una differenza radicale tra
    - Events of interest (high level): file open, file modified, user logon, pwd changed…
    - Logged events (low level): completely different from HLE
  - Per tirare fuori un evento di interesse, bisogna raccogliere tanti eventi di log di basso livello, per fare questo bisogna essere in grado di scrivere una query molto particolare
- Un evento di alto livello, di solito corrisponde a
  - Tanti eventi di basso livello, non linkati tra loro, sono tutti isolati (problema di fondo), l'attività di un utente, non si trova in un unico log, ma è distribuita in tanti log diversi (con sorgenti diverse)
  - A volte c'è una componente informativa che facilita l'associazione tra eventi, ma non c'è sempre, non collega tutti gli eventi e non è sempre la stessa
- SIEM (security information event management)
  - Sistema per gestire informazioni degli eventi rilevanti per la sicurezza ⟶ è un sistema centralizzato che gestisce tutti i log
    - Punto in cui arrivano i log di tutte le sorgenti informative, questi vengono messi insieme in un formato uniforme e permette di correlare le loro informazioni. Permette la correlazione tra gli eventi di una macchina agli eventi su un altra, idealmente permette anche di fare analisi
  - Non funziona in modo autonomo, deve avere delle regole per capire cosa cercare, ci sono regole codificate per identificare eventi che descrivono attività anomale (alerts) or che indicano un security incident (alarms)
  - Queste regole sono delle query fatte a un database gigante in un linguaggio che dipende dal SIEM
  - Queste regole di basano sulle signatures
  - Bisogna saper correlare eventi in log diversi anche a distanze di tempo notevole
  - Le correlazioni vengono costruite in larga parte con il domain knowledge e i previously observed attacks (sviluppo query basate su attacchi conosciuti e cerco di raccogliere i log associati a quello per identificarli)
- Stupidaggine: AI can discover previously unseen attacks ⟶ problema non è rilevare un attacco, il problema è rilevare solo gli attacchi (falsi positivi)





Defense

- SIEM fa parte del detect nelle tattiche difensive
- SOC (security information center)
    - Centrale di controllo → idealmente è la stanza di controllo virtuale dove le persone analizzano il SIEM
    - Si occupano della detection, decidono che priorità dare all'alert e capire cosa sta succedendo (Prioritization e investigation)
    - Sono quelli che decidono quando un alert deve essere escalated (escalation può essere tecnica o amministrativa)
    - Containment and recovery
    - Può essere in house (organizzazione che ha delle persone in grado di gestire il soc dall'interno 24/7) oppure può essere affidato a un esterno (MSSP: managed security service provider) → è molto difficile avere all'interno le capacità per gestire i log
    - Microsoft è una degli MSSP più importanti al mondo (gestisce i log per molte organizzazioni)
- Avere un SOC è un investimento notevole
- Sono stati fatti tantissimi studi, l'esito è sempre lo stesso: gli attacchi non sono il problema, ma è individuare solo gli attacchi il problema → le AI non risolvono questo problema
- C'è un altro importante problema: explanation of the alert → investigare tutti gli alert porta via molto tempo ed è difficile
- One of the many studies: (sponsorizzato da IBM)
    - Intervista a 1000 persone che lavorano il SOC, 100 org, 10 paesi
    - Con sicuramente high budget e security awareness
    - → vengono investigati meno della metà di tutti gli alert (è praticamente impossibile riuscire a vedere tutti gli alert in tempo reale), molti di questi sono falsi positivi con priorità bassa, negli ultimi due anni il tempo necessario a investigare un alert è cresciuto