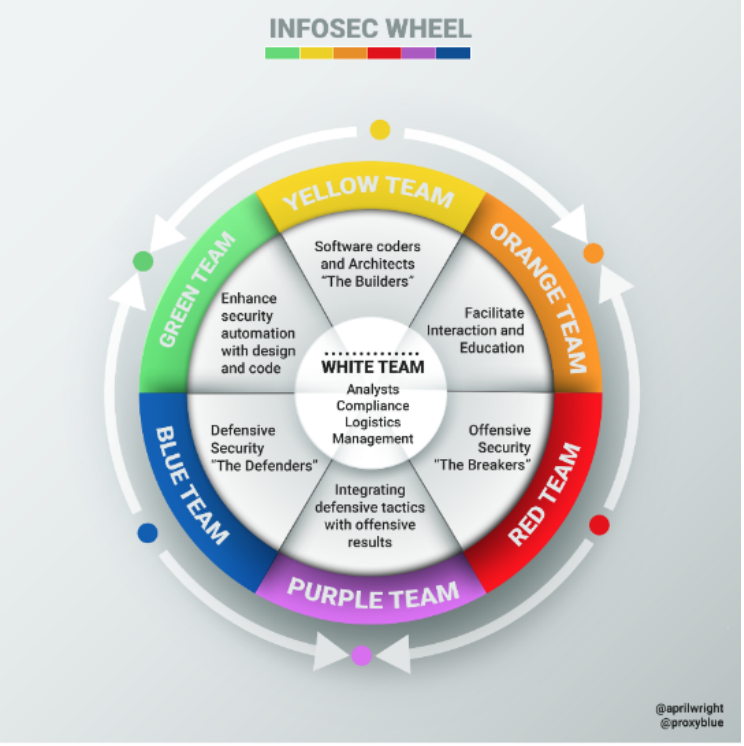
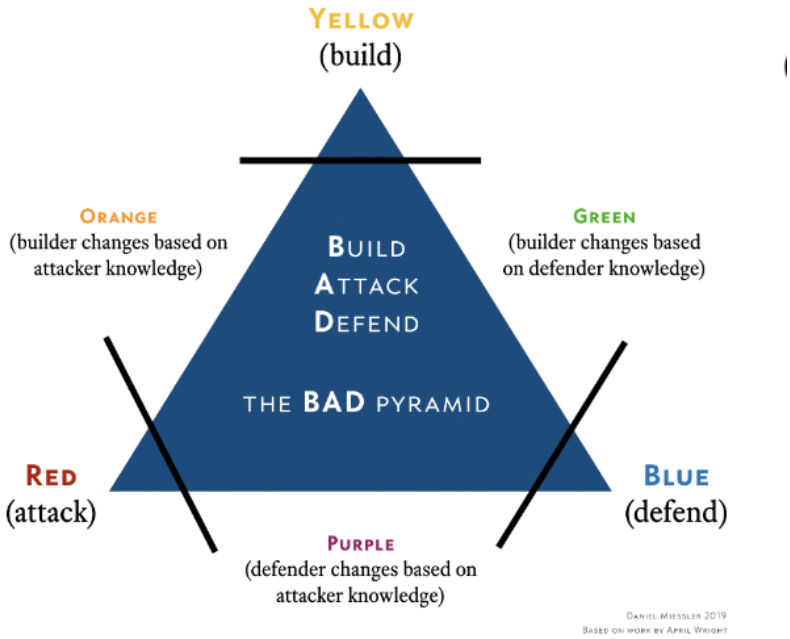
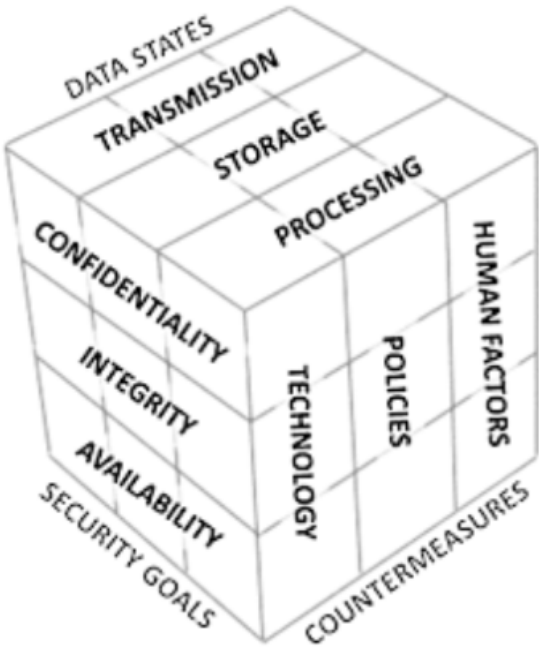
Security samenvatting:

White team





Security cube



BLUE TEAM

1. Preparation
2. Detection & Analysis
3. Containment, Eradication, Recovery
4. Post-Incident Review
5. Update the plan !

Phase 1: Preparation

Condensed steps to prep and create a plan

1. Identify and prioritize your assets
2. Identify your potential risks
3. Establish procedures
4. Assemble a response team
5. Train your employees

NIDS: Network Intrusion Detection System:

Dit is netwerk niveau

Veel logs

3 manieren hoe detectie gebeurt:

- Signature based detection: Hierbij zal om de bepaalde tijd (uur,dag,etc.) van de centrale server signature gedownload worden. Gekende fouten zullen door dit getecteerd kunnen worden

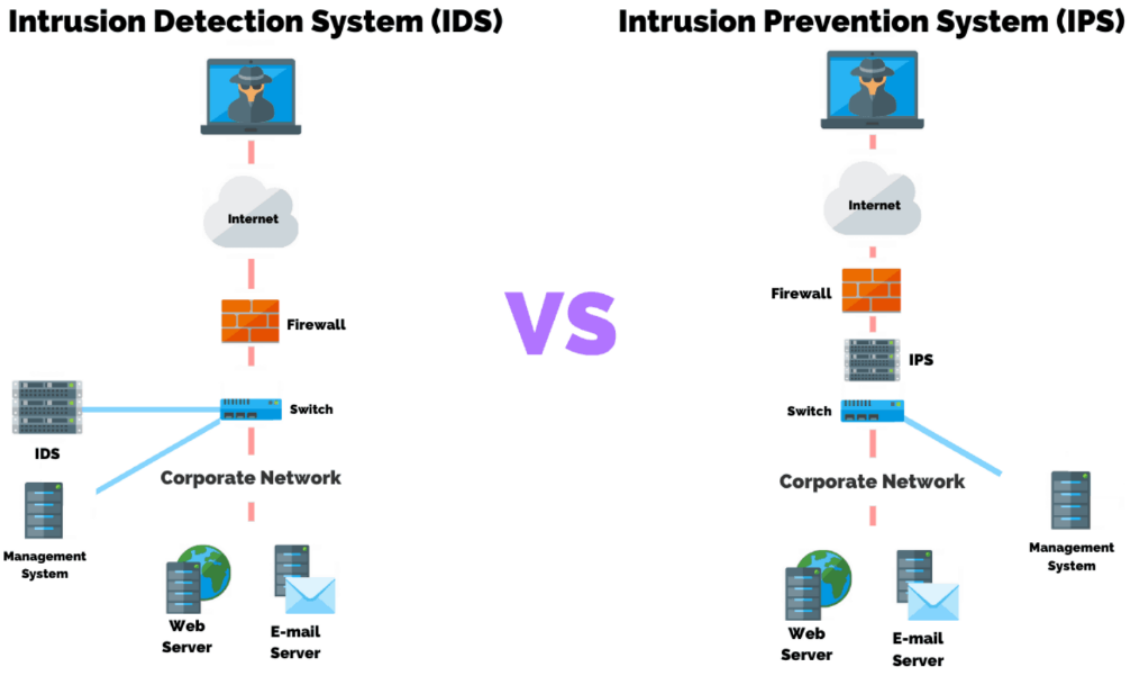
- Statistical anomaly based detection: Hierbij zal onbekende traffic gedetecteerd worden. Het gaat hier dan over potentieel gevaarlijke trafiek dat gedecteerd wordt.
- Stateful protocol analyses detection: Je gaat hierbij verdan dan tcp/ip en kijkt binnen de pakketjes. Met https zie je dit wel niet.

HIDS: Host Intrusion Detection System: (andere benaming: Endpoint security)

Een soort virusscanner dat scant op systeem, memory,ram,… er worden metrics terug vertuurd.

NIPS en HIPS: Network/ Host intrusion Prevention Systems

Hierbij zal er gepreventeerd worden ipv alleen detecteren. Bij detection systems zal de data overgekopieerd worden naar de detection systeem en zal dat systeem het verder afhandelen (analyseren , monitoren). Prevention systeem zal onmiddellijk gedetecteerde stoppen.



NIDS Tools: Snort, suricata

HIDS Tools: Wazuh, ossec

Tool Examples:

NIDS

HIDS

Wat is honeypot:
Een systeem dat zich voordoet als een echte systeem (Zoals geeft een fake shell) maar logt informatie van aanvaller. Waarom? 2 redenen: Signatures te maken. En aanvaller af te leiden van de echte servers. Dit is meer nuttig dan endpoint detection

Visualisatie (En aggregeren) tools voor de logs:

Splunk en Security onion

“Supertools”
Combining it all - Aggregate data and correlate “With AI and Blockchain”

DFIR: Digital Forensics & Incedent Response

File system forensics: (Het gaat hier dan om persistent data)

Disk to image: Dat je van een disk een image maakt. Dit is het beste scenario omdat je alles een copy hebt waarin je alles in kan bekijken.

Disk to disk: Hier analyseer je de schijf zelf → iets beperkder dan disk to image

Logical: Toegang dat je hebt op een aantal files.

Sparse : Snippet van data (Klein stukje waar je toegang op hebt)

Write block (zie apparaat) is er effectief een read only van een bepaalde schijf en dat ook kan dienen als bewijs. Dit help tegen evidence tempering bijvoorbeeld.

DFIR skills

PXL DIGITAL

Technical Skills

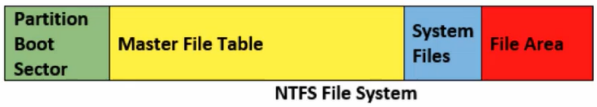
- File System Forensics

  Extraction

  Involves the retrieving of unstructured or deleted data

  Deleted != gone: Deleting files only removes it from the disc contents table.

  Other hiding techniques: encryption, steganography, file obfuscation...

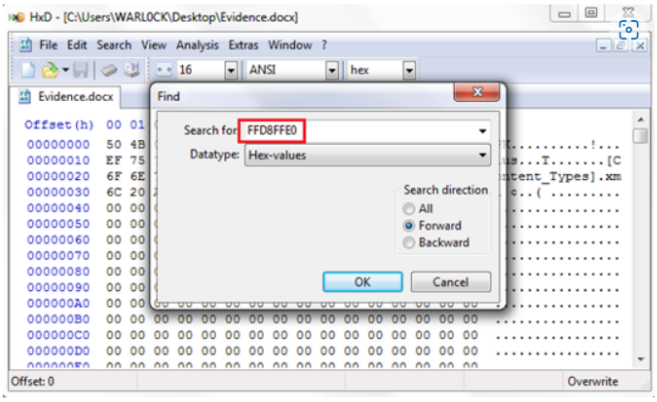


In deze slide gaat het over indexatie. Alles in een file system werkt eigenlijk met indexatie. Als je iets wilt opvragen kan je via de master file table refereren en de data opvragen. Bij het verwijderen van een bepaalde data zal niet effectief de data verwijderd worden maar zal de index alleen verwijderd worden van de master file table. Er bestaan tools dan om handmatig de verwijderde bestanden terug op te vragen door de index dan terug te zetten.

Hiding techniques:

- Steganography: data verstoppen in bv. images zoals jpg,…
- File obfuscation: De extentie veranderen van een file zodat je niet weet welk bestand dat het is. → easy te vinden though
- Encryption: Encrypteren van harde schijf. Waarschijnlijk de beste manier en sterkste manier omdat het ook het gebruiksvriendelijkste is. Als je container wel sluit dan ben je wel alles kwijt.

File carving: Van raw data een data proberen te achterhalen. Bv. een jpg file start altijd met zelfde header en eindigt met trailer. Je kunt in een word document dit achterhalen door met bv. Hxd (tool) te zoeken en kopieren van header tot en met trailer. En kan dit dan verder opslaan.



Memory System Forensics: (Hier gaat het dan om werkgeheugen (RAM Geheugen)

Malicious software kan ook in het werkgeheugen verstoppen.

We kunnen een snapshot maken van ons memory geheugen en dat noemt dan **Memory Dump.**

Van wat kan je snapshots maken :

Rawformat: Rechtstreeks een snapshot van een misschien nog zelfs draaiende systeem

Crash dump: wanneer je os crasht en je van hieruit een snapshot maakt.

Hibernation file: Wanneer je basically je systeem in standby gaat en een snapshot gemaakt wordt.

Pagefile: een deel/blok van de ram/werkgeheugen van een snapshot.

Vmware snapshot spreekt voorzich.

Mimikatz (van werkgeheugen credentials ophalen). (KENNEN?)

Technical skill

Log analyses:
ELK Stack : Elasticsearch, Logstash, kibana

Security onion is een ELK Stack tool.

Het analyseert jou logs. En creert een aantal default dashboards al vr jou. Geautomatiseerd dus.

Technical skill

Intelligence analyses:

Hier gaat het om al de relaties tussen entiteiten te ontdekken. Tussen mensen of technische relaties. Bv. chain of custody voorbeeld: Wie wat wanneer heeft wat gedaan of mocht hij dat doen. Omgekocht ? of phishing targeted persoon ?,… Technisch hetzelfde, welke files zijn gepasseerd in het netwerk, of ip adressen, …

Technical Skills

- Intelligence Analysis

  determine the relationships between the following entities:

  - People.
    - Names.
    - Email addresses.
    - Aliases.
  - Groups of people (social networks).
  - Companies.
  - Organizations.
  - Web sites.
  - Internet infrastructure such as:
    - Domains.
    - DNS names.
    - Netblocks.
    - IP addresses.
  - Affiliations.
  - Documents and files.

Sounds a lot like OSINT! But more organized and with a bigger goal (most of the time)

Maltego is dan een intelligence analyses tool.

Malware triage: Malware recognize, analyze en reverse engineering skills.

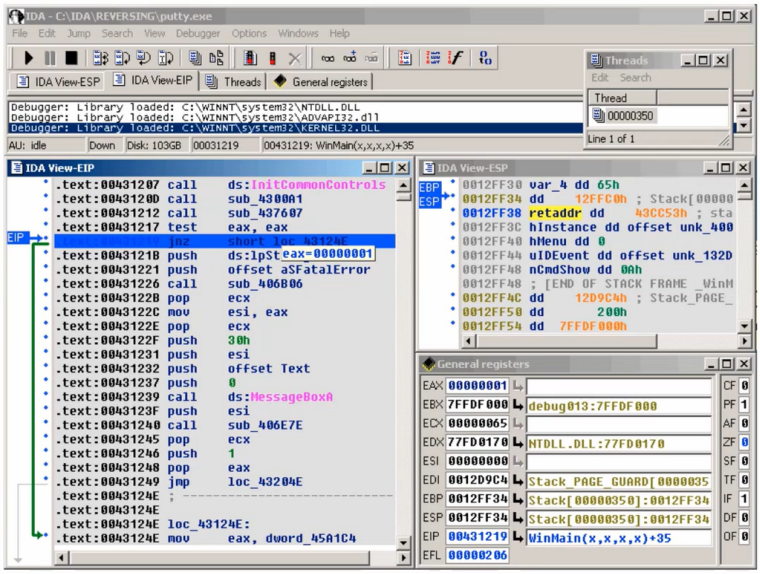
DFIR skills

Technical Skills

- Malware Triage

Recognize, analyse and reverse-engineering

https://resources.infosecinstitute.com/category/certifications-training/malware-analysis-reverse-engineering/



Decompilers: IDA, ghydra

Technical skills
Soft skills:

Communicatie, working in team, ….

YELLOW TEAM:

Pro active controls: Een soort security checklist waaraan je je best je applicatie aan voldoet.