Security of Networks, Services, and Systems

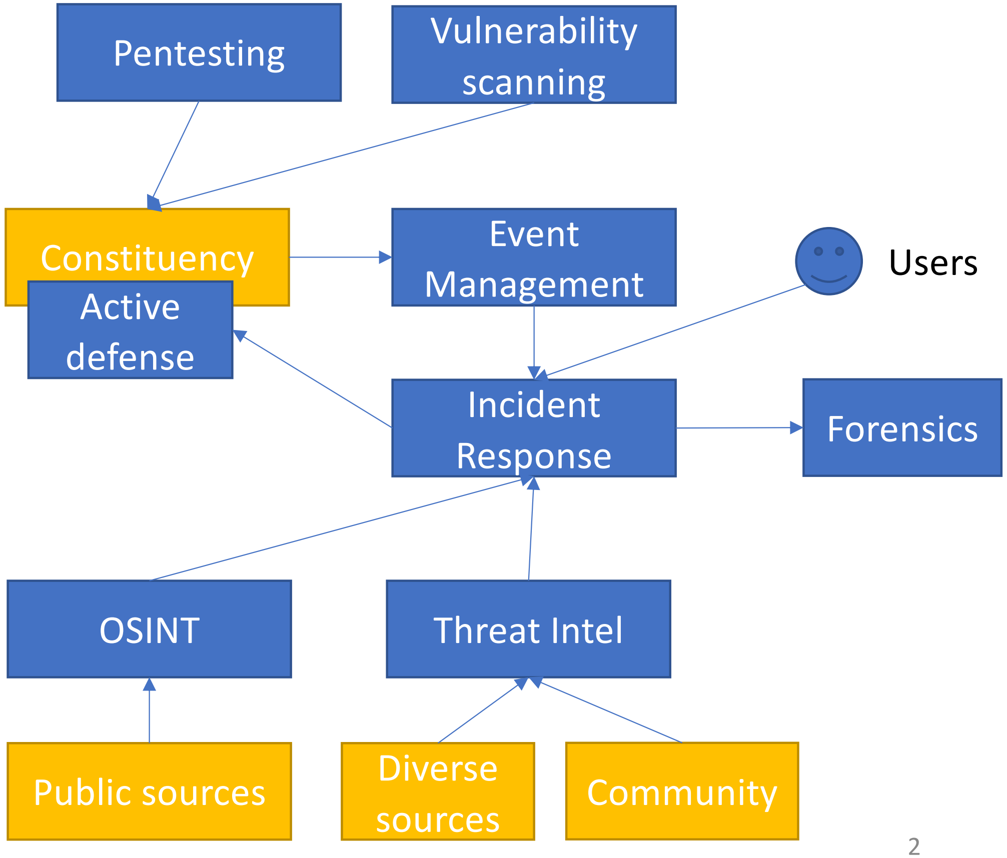
Security Operations

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC

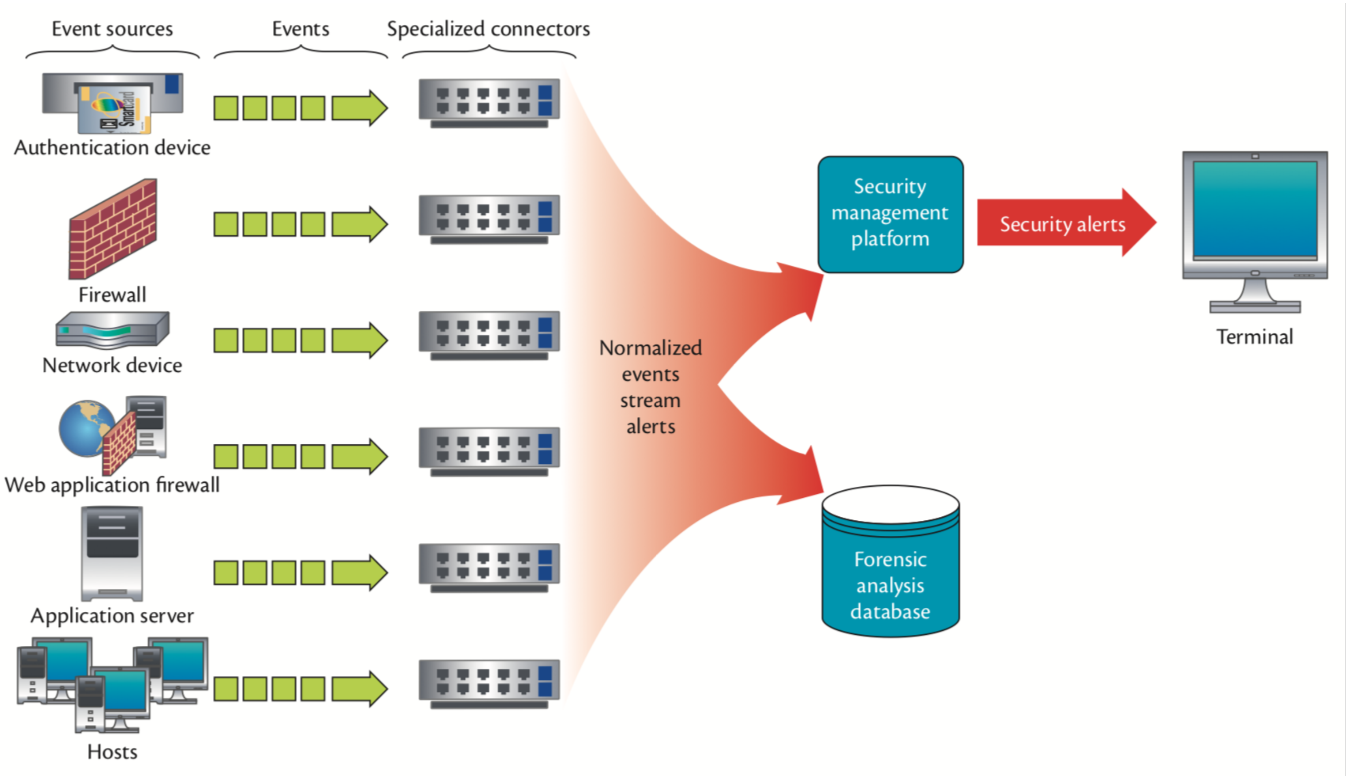
Some aspects of security operations

- Event management
- Incident response
- Cyber threat intelligence
- Open source intelligence
- Forensics
- Vulnerability scanning
- Pentesting
- Active defense



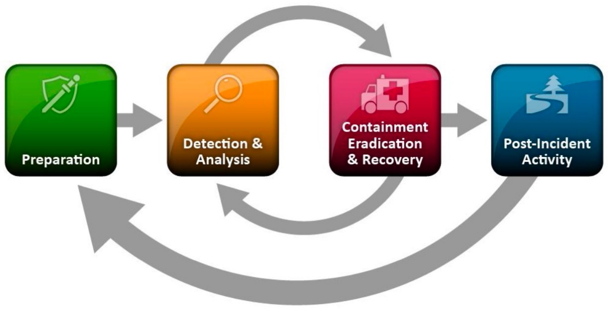
Event management

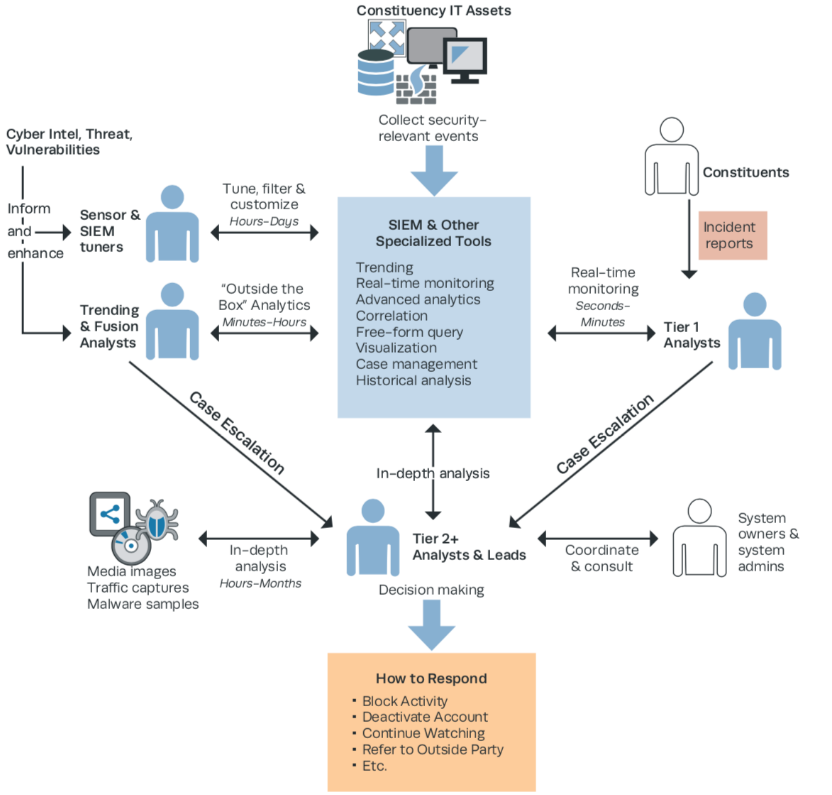
- Monitoring and detection
  - host, network, servers, etc
- Event processing, correlation, logging (SIEM)



Incident Response

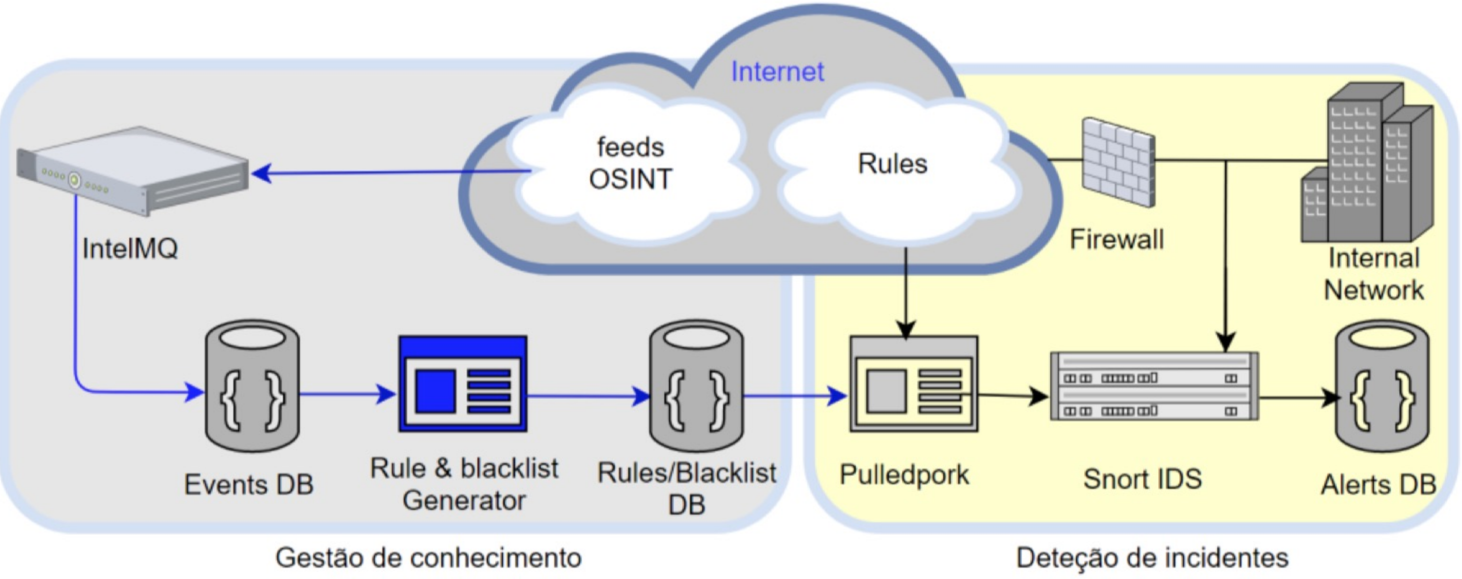
- Tier 1 – incident triage
- Tier 2 – incident investigation
- Tier 3 – threat hunting





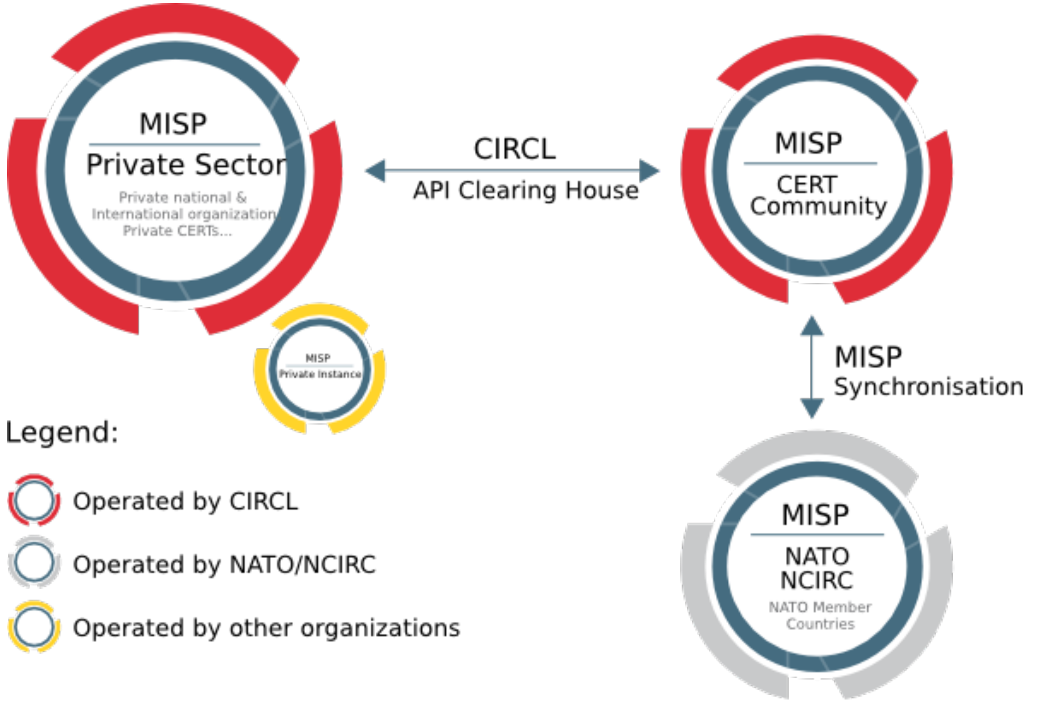
Cyber threat intelligence

- Collect and process IoC feeds, and pushing them to SIEM, IDS, firewall, etc
- Open IoC, STIX, YARA, Snort formats to express IoCs



MISP – intelligence sharing

- Develop intelligence
- Share it with your trusted partners
- Filter what intel you want
- Add what intel you want

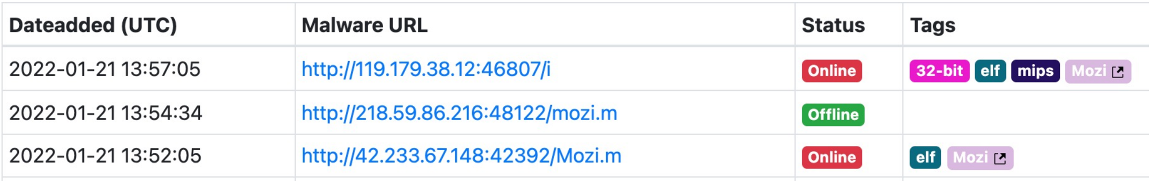


Sandboxing, honeypots, honeynets

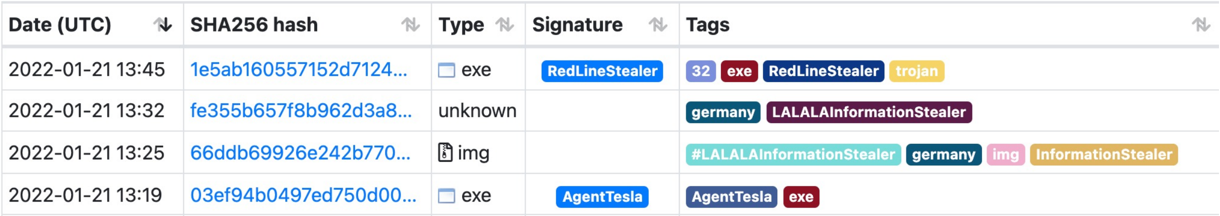
- Collect threat intelligence from attackers
  - That can be actionable on the defense
  - Namely signatures and TTPs
- Sandboxing
  - E.g. Isolated VM runs malicious payload (binary, URL)
  - Payload can check for evidence of sandboxing
- Honeypots
  - Vulnerable system deployed on the Internet

Public listings of threat intel

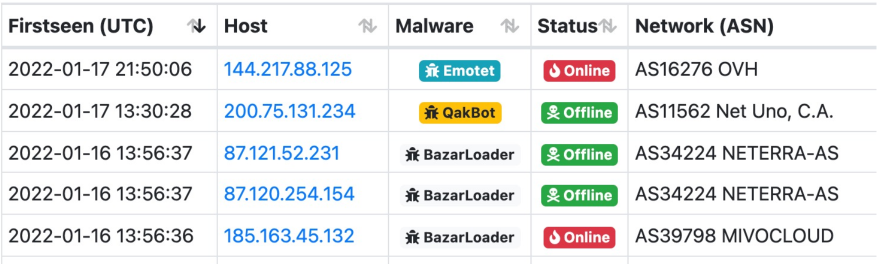
- abuse.ch
  - URLs
  - Binaries
  - C2
- virustotal
- malc0de
- vxvault.net
- Many others



Dateadded (UTC)	Malware URL	Status	Tags
2022-01-21 13:57:05	http://119.179.38.12:46807/i	Online	32-bit elf mips Mozi
2022-01-21 13:54:34	http://218.59.86.216:48122/mozi.m	Offline	
2022-01-21 13:52:05	http://42.233.67.148:42392/Mozi.m	Online	elf Mozi



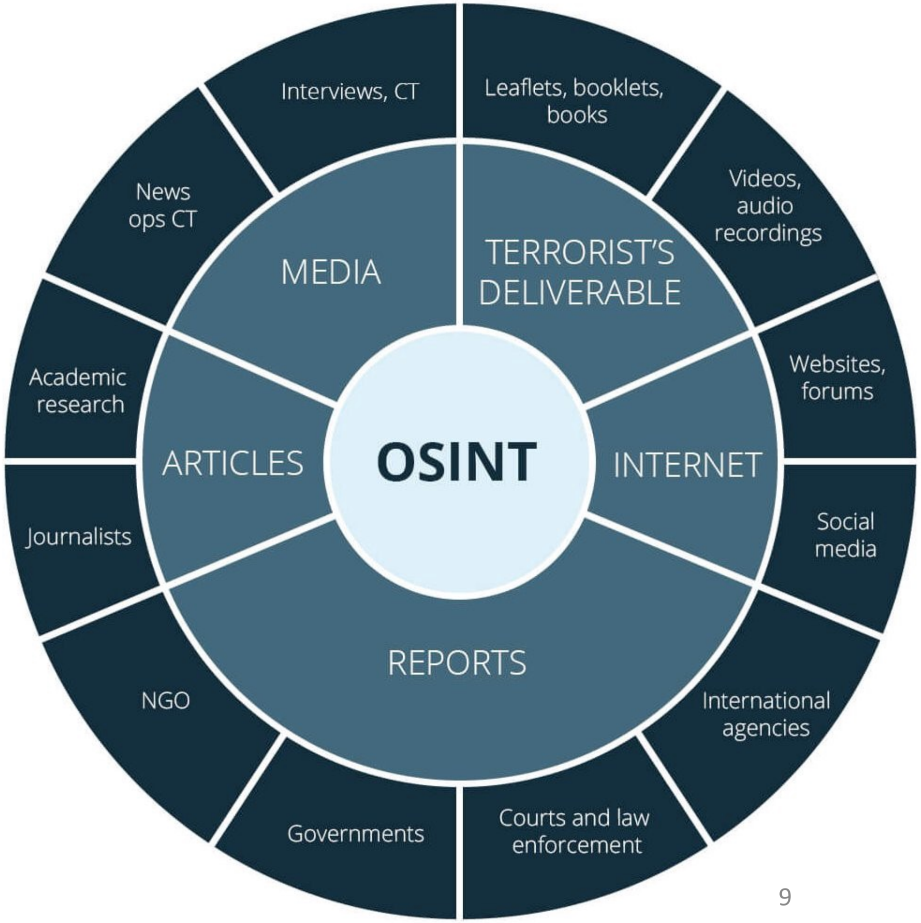
Date (UTC)	SHA256 hash	Type	Signature	Tags
2022-01-21 13:45	1e5ab160557152d7124...	exe	RedLineStealer	32 exe RedLineStealer trojan
2022-01-21 13:32	fe355b657f8b962d3a8...	unknown		germany LALALAInformationStealer
2022-01-21 13:25	66ddb69926e242b770...	img		#LALALAInformationStealer germany img InformationStealer
2022-01-21 13:19	03ef94b0497ed750d00...	exe	AgentTesla	AgentTesla exe



Firstseen (UTC)	Host	Malware	Status	Network (ASN)
2022-01-17 21:50:06	144.217.88.125	Emotet	Online	AS16276 OVH
2022-01-17 13:30:28	200.75.131.234	QakBot	Offline	AS11562 Net Uno, C.A.
2022-01-16 13:56:37	87.121.52.231	BazarLoader	Offline	AS34224 NETERRA-AS
2022-01-16 13:56:37	87.120.254.154	BazarLoader	Offline	AS34224 NETERRA-AS
2022-01-16 13:56:36	185.163.45.132	BazarLoader	Online	AS39798 MIVOCLOUD

Open source intelligence

- data from overt and publicly available sources
- collection, analysis
- goals
  - produce threat intelligence on specific malicious actors or for specific industry
  - assist cyberhygene and pentesting on target organization

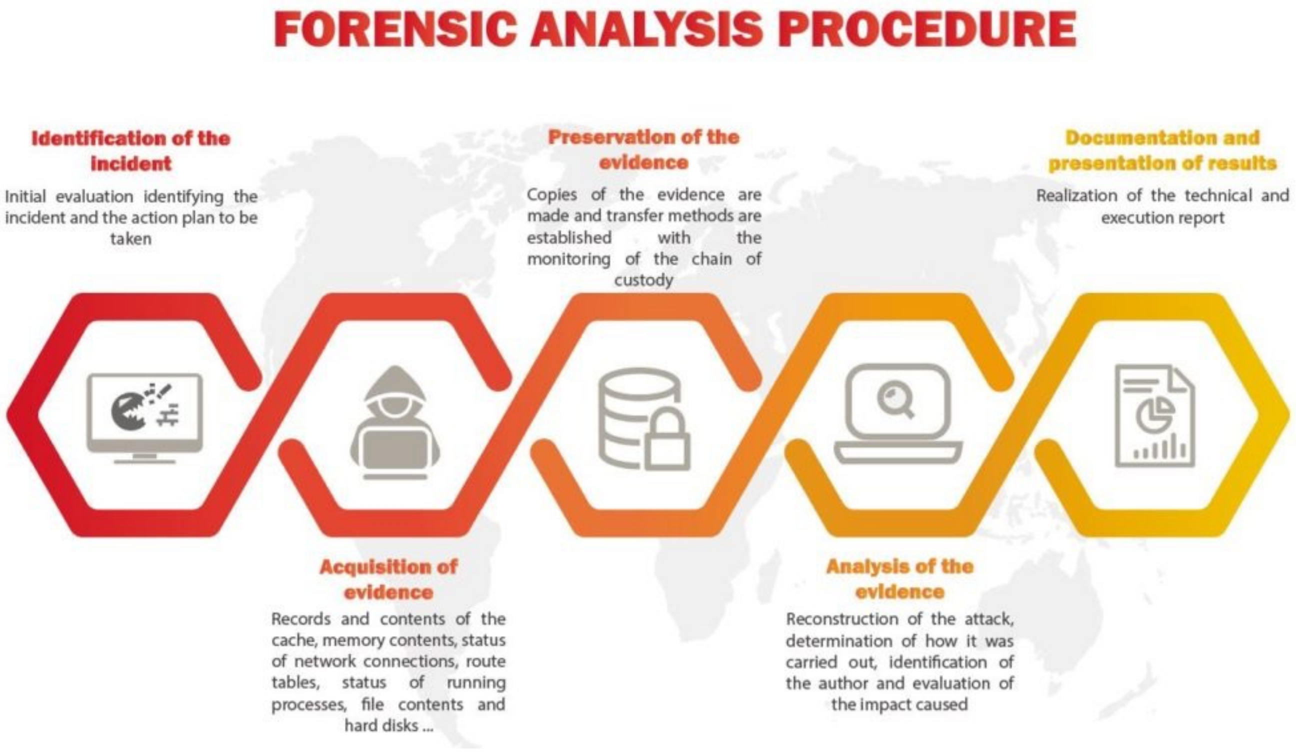


Sources of OSINT

- Google inurl, passive DNS, WHOIS, Shodan, etc
- Listings of OSINT sources and tools that query multiple OSINT sources
    - recon-ng, sn0int, theHarvester, …
- Domain names, networks, AS numbers, public hosts and exposed ports, people, exposed admin info, CPE (common platform enumeration)

Forensics

- Identification of incident
- Evidence acquisition
- Evidence preservation
- Evidence analysis
- Documentation and presentation



FORENSIC ANALYSIS PROCEDURE

Identification of the incident

Initial evaluation identifying the incident and the action plan to be taken

Acquisition of evidence

Records and contents of the cache, memory contents, status of network connections, route tables, status of running processes, file contents and hard disks ...

Preservation of the evidence

Copies of the evidence are made and transfer methods are established with the monitoring of the chain of custody

Analysis of the evidence

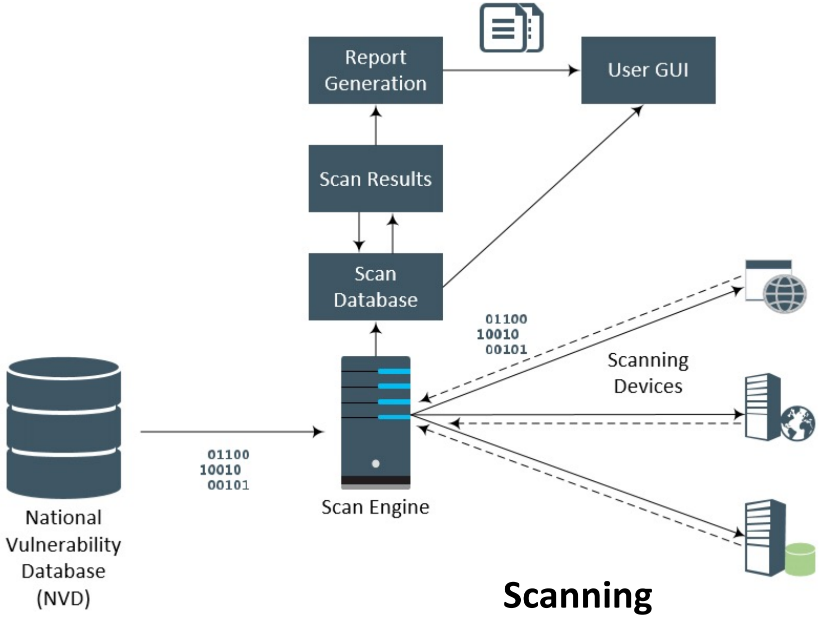
Reconstruction of the attack, determination of how it was carried out, identification of the author and evaluation of the impact caused

Documentation and presentation of results

Realization of the technical and execution report

Vulnerability detection, vulnerability scanning

- Detection – keep track of vulnerable software versions
  - List currently installed repositories, check if they're known to be vulnerable and if they can be patched
  - Often by running agent in target host
- Scanning – check if services on target host are vulnerable
  - Try list of known vulnerabilities
  - Remotely on target services
  - As if an attacker



Scanning

Security of Networks, Services, and Systems

Security Operations

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC