Security of Networks, Services, and Systems

Cybersecurity concept overview sprint

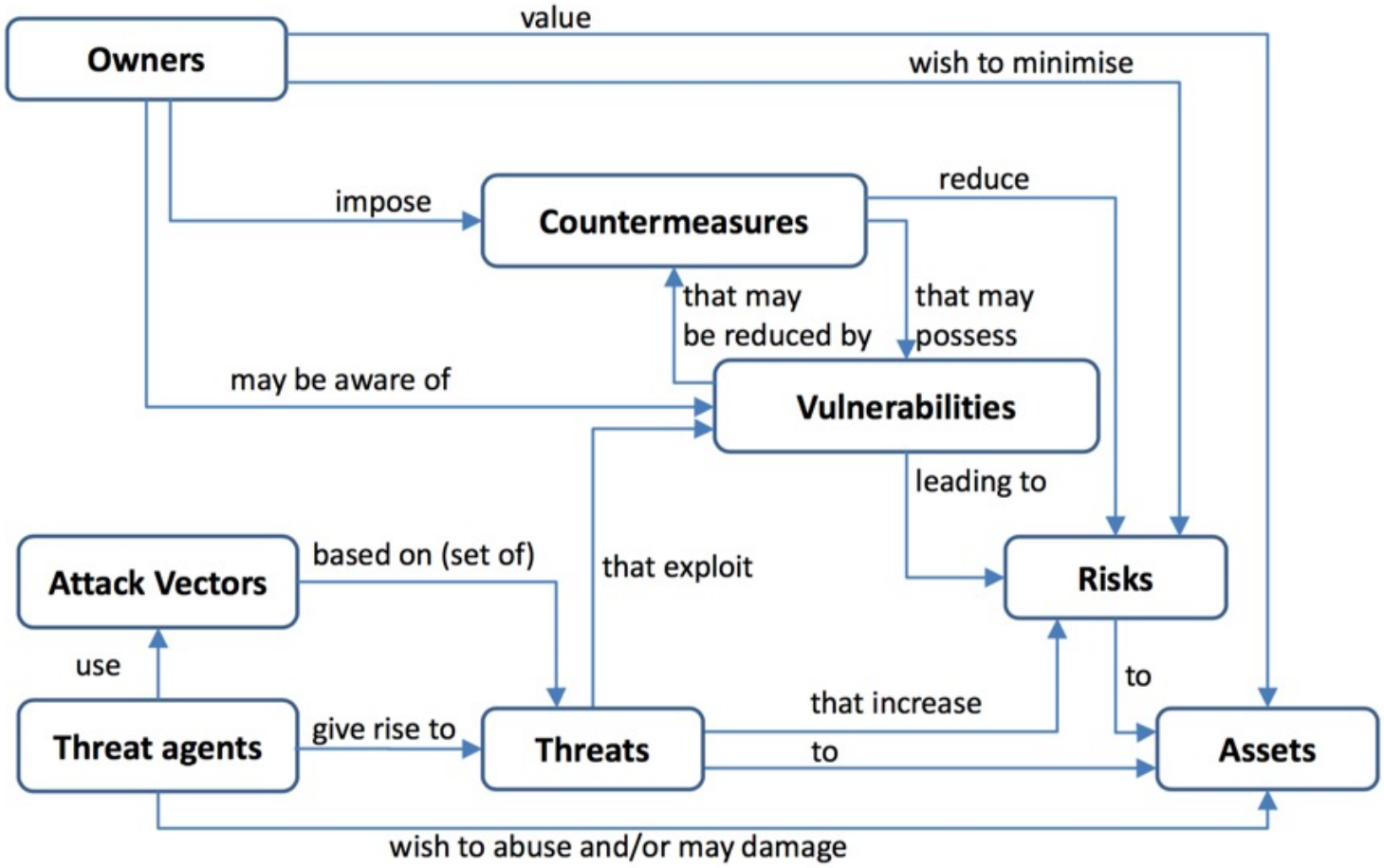
Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC

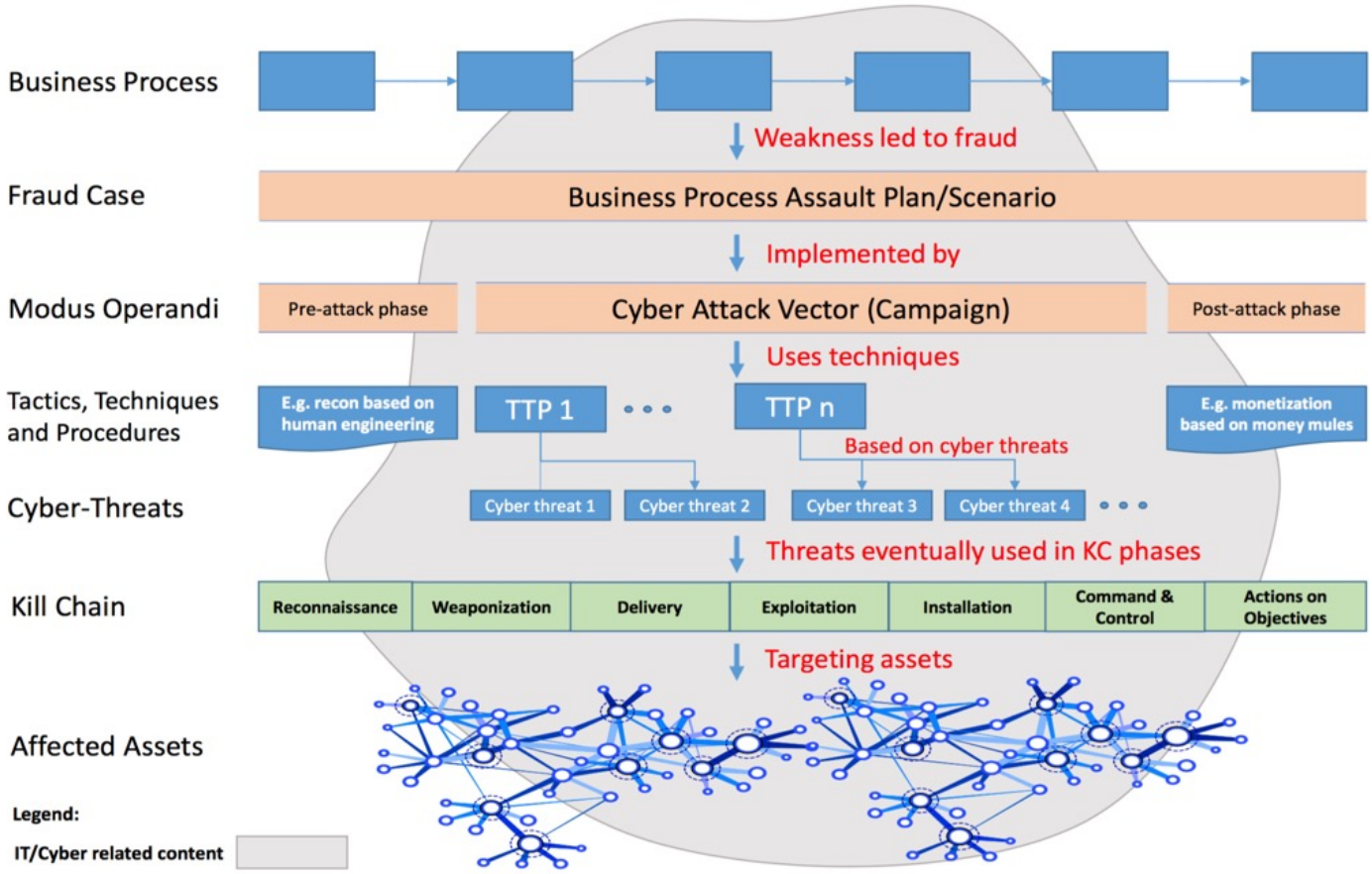
Why do we need cybersecurity?

- Greed, vengeance, stupidity – among other human qualities – do no go away in cyberspace
- Attackers are driven by the same things as in the "real world"
  - Stealing money, information, etc
  - Disrupting services
  - Destroying cyber infrastructure, crippling societies
- Layers of anonymity in cyberspace may actually encourage attackers
- And it’s not all contained in cyberspace
  - Cyber-physical systems bring disruption from cyber to physical
  - Critical infrastructure, IoT

Major players and concepts



Tools of the trade – M.O. (Modus Operandi)

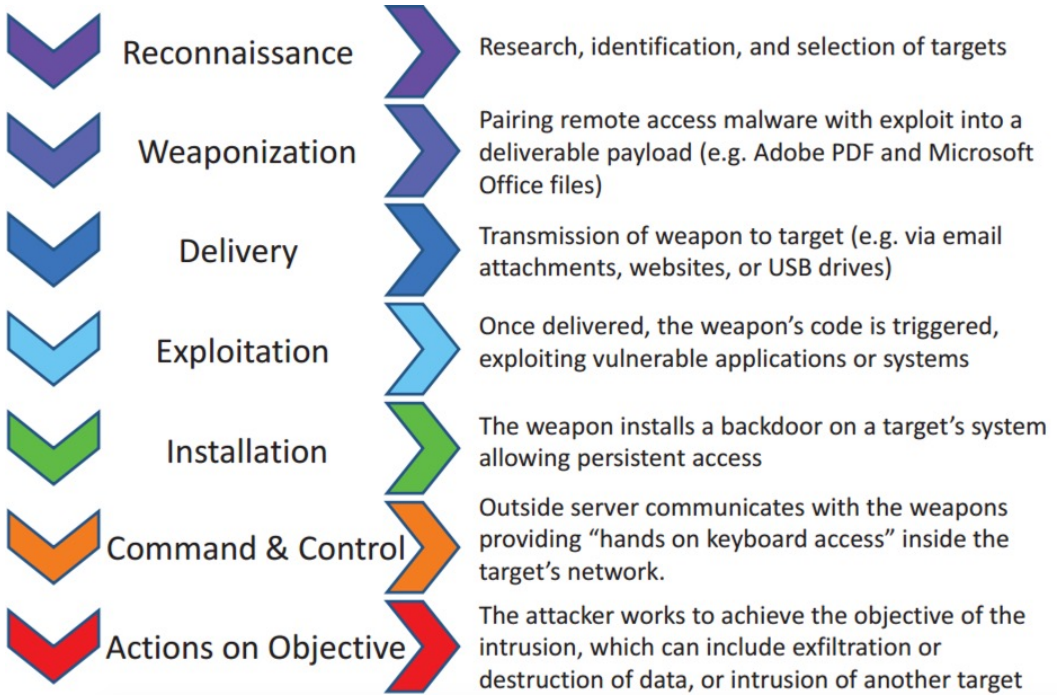


https://attack.mitre.org/tactics/enterprise/
https://attack.mitre.org/techniques/enterprise/

Mitre Att&ck enterprise tactics

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

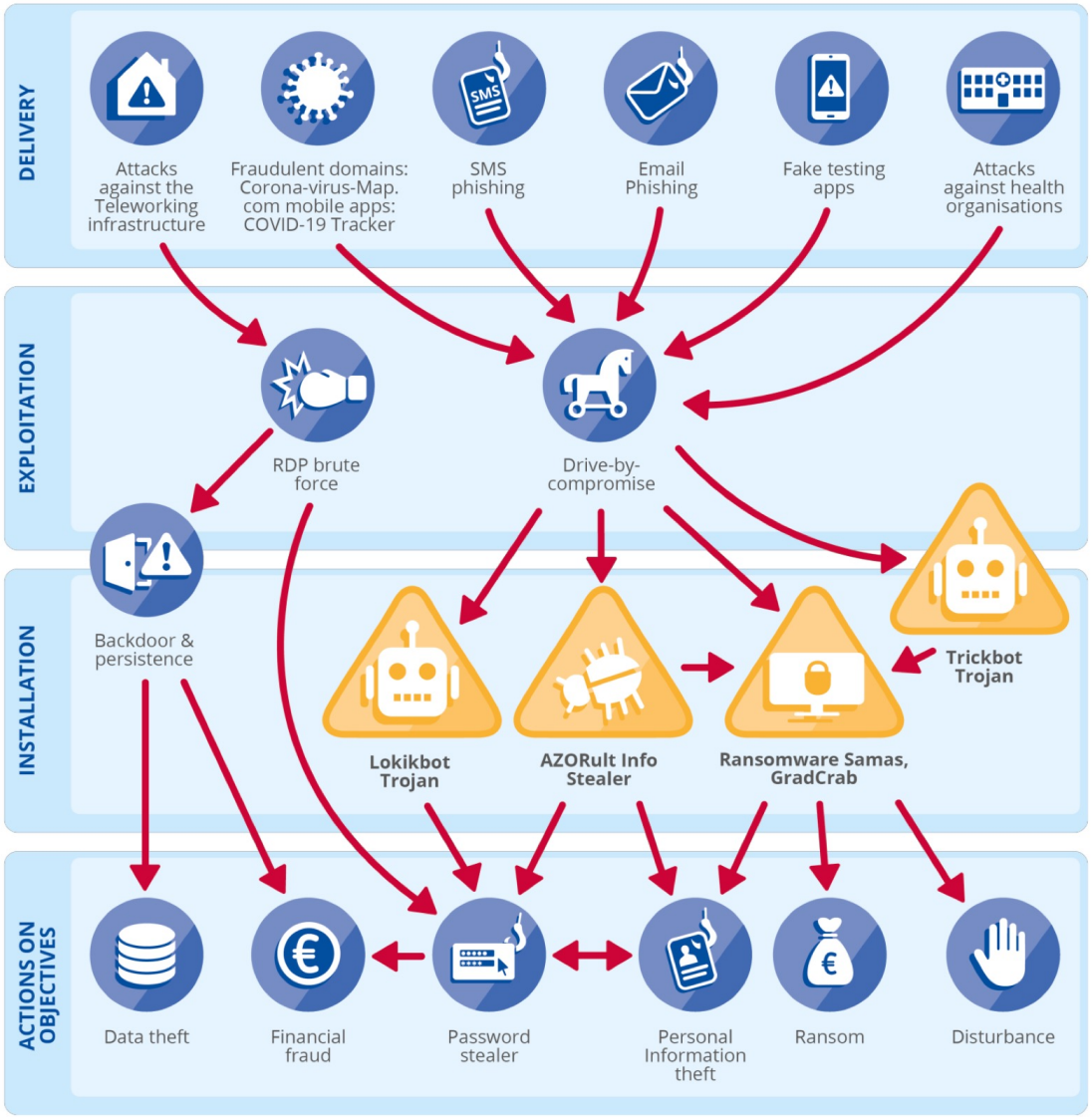
Kill chain – user desktop or mobile



Enisa threat rank 2020

https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

Enisa covid-19 exploitations



Getting a sense of cybercrime

- https://cybercrime-tracker.net
  - Date: 11-08-2021
  - URL: 37.0.10.102//rut/panel/admin.php
  - IP: 37.0.10.102
  - Malware: **AZORult**
- “spyware that can steal banking information, including passwords and credit card details as well as cryptocurrency” (*Malwarebytes*)
- Follow IP address on virustotal
  - https://www.virustotal.com/en/ip-address/37.0.10.102/information/
  - File that communicates with this IP address:
    2021-08-10, Win32 EXE, xds.exe, 9192c2363847689ba2d28c05c4c04c6c
- Look up xds.exe file on URLhaus (by hash)
  - 2021-08-12 07:23:04
  - hxxp://37.0.10.83/cxx/xds.exe
  - Status: online, on 2021-08-14
- Found: IP serving file and the IP with C2:
  - 37.0.10.83, same /24 network as C2 server

Protecting assets with threat modeling

- Threat models
  - For each asset
  - Imagine how and in which conditions an attacker could compromise the asset
- Assumptions
  - If the attacker can do x
  - x: access a private network, run privileged code, obtain username/password, sniff network packets, etc
- How likely is each assumption? What is the risk for the asset in that case?
- Develop countermeasures
  - start with the most likely and higher risk threats

Threat modeling

- Methods
  - https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/
- CIA triad
  - Confidentiality, Integrity, Availability

Threat modeling (2)

- STRIDE
  - Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
- DREAD (risk assessment)
  - Damage, reproducibility, exploitability, affected users, discoverability
- Exercise
  - https://www.coursera.org/lecture/identifying-security-vulnerabilities/the-stride-method-via-example-oVpus
  - Design a (moderately complex) target system; applies STRIDE to find threats

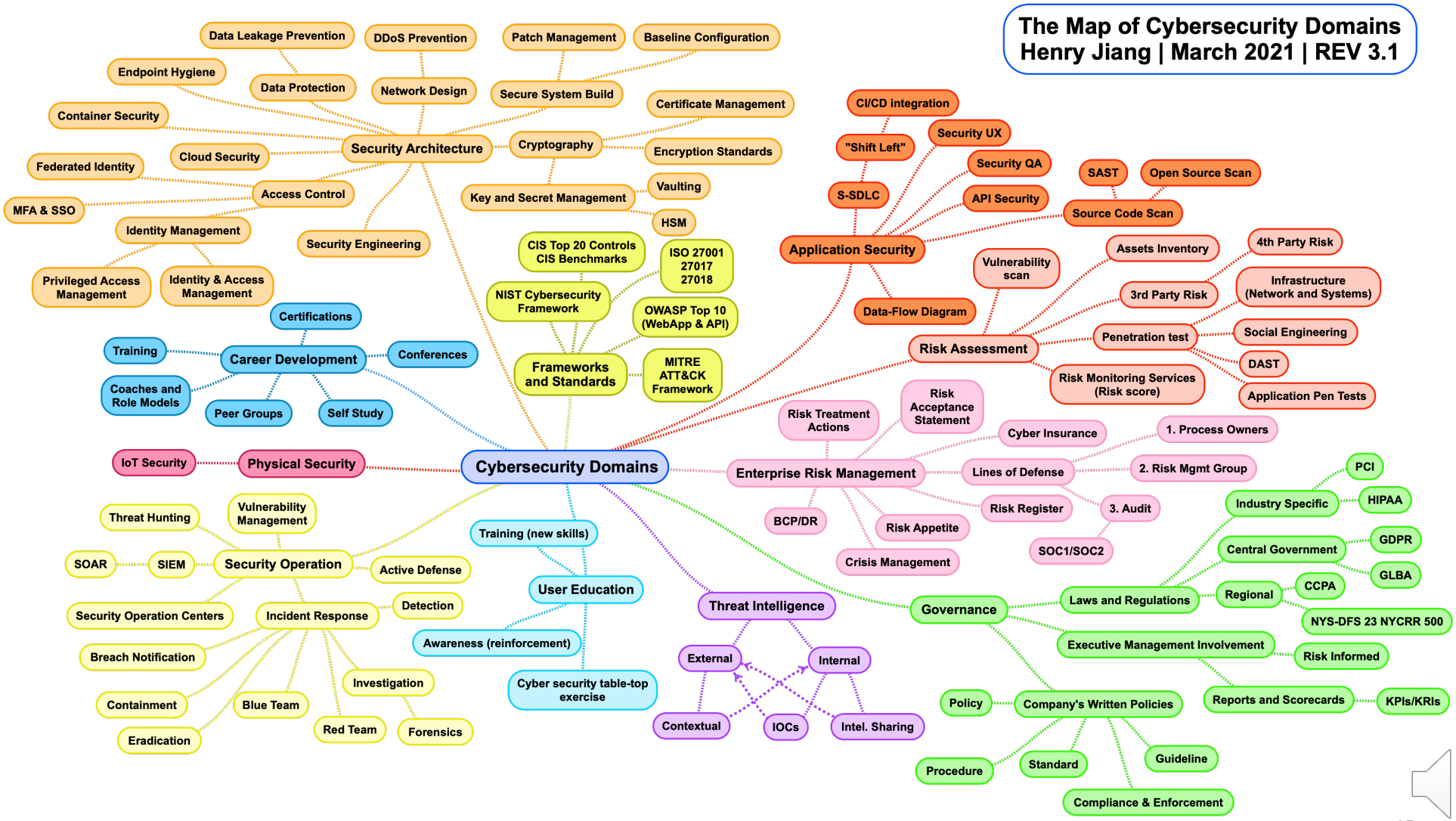
Security by design

- Include threat modeling countermeasures at design stage
- Don’t way until your system is deployed
  - High cost of redesigning
  - High cost of covering security holes

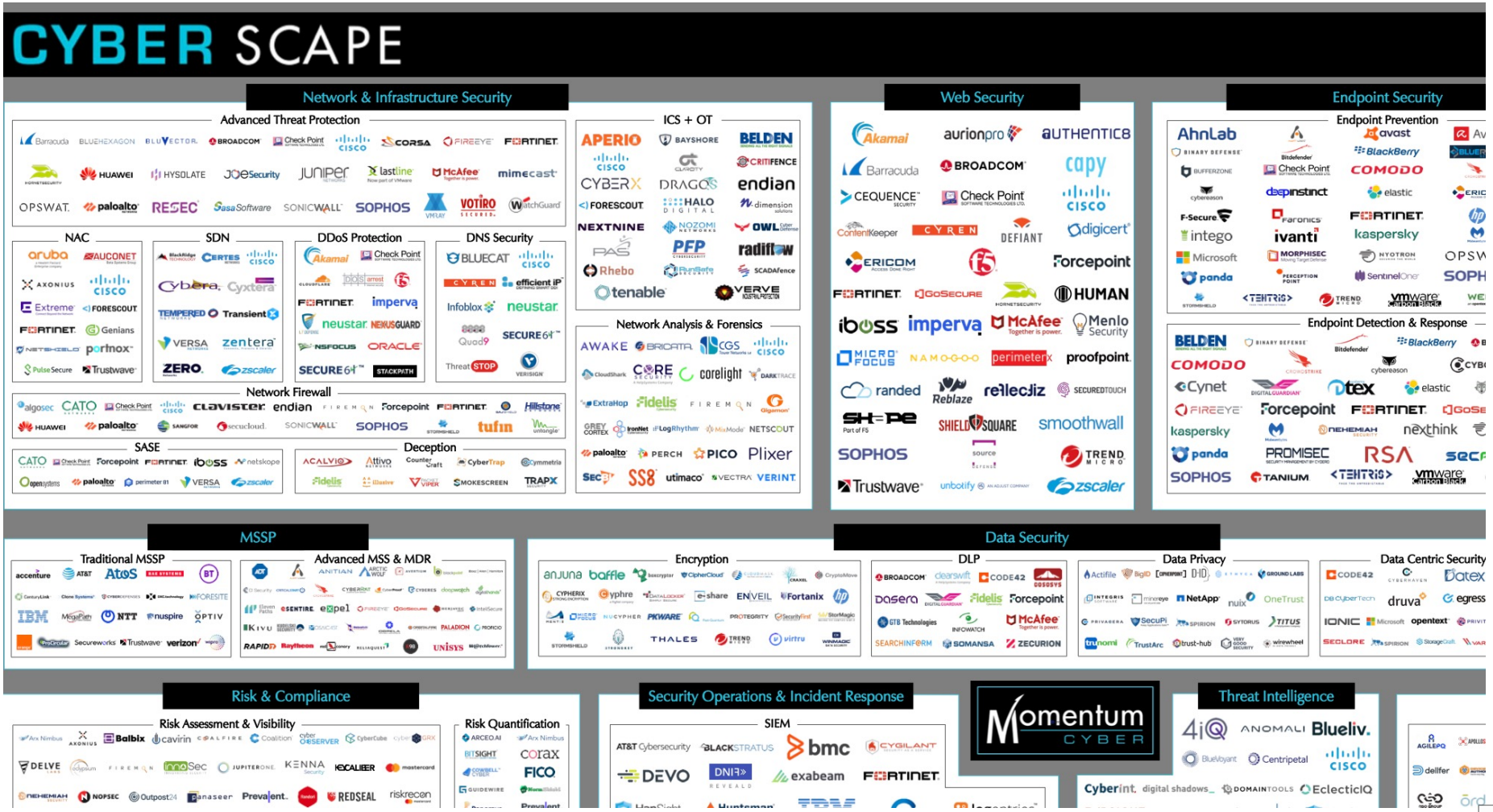
- Security by obscurity vs. open security

Securing systems

- Desiging and engineering secure systems
  - Secure hardware, software, protocols, networks
  - Cannot make a perfectly secure system
- Managing insecure systems
  - Detecting intrusions and attacks
  - Detecting, pacthing, mitigating vulnerabilities
  - Gathering intelligence



https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/



https://momentumcyber.com/docs/CYBERscape.pdf

Security of Networks, Services, and Systems

Cybersecurity concept overview sprint

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC