0-to-hero

X/10 Mentors <> X/10 Sessions

Rashad Suleymanov

`

https://www.linkedin.com/in/rashad-suleymanov-b7293a41/

Job / Education

`

Education:

- Tallinn University of Technology, Cybersecurity (master)
- Azərbaycan Ali Hərbi Təyyarəçilik Məktəbi, Radioelectronics (bachelor)

Work experience:

- HSBC – Threat Hunter
- IBM X-Force – Escalation Engineer, Threat Analyst
- ATL Tech – System Administrator
- 118 Xidmeti – System/Network Support Engineer
- AGBank – Network Support Engineer
- HHQ – Radioelectronics Engineer

Agenda

`

1. Cybersecurity job market in Poland (EU)
2. Cybersecurity carrier plan
3. Cybersecurity frameworks
4. LAB, LAB, LAB
5. Building right mindset
6. Malware Analysis
7. Threat Hinting
8. Resources (Books, conferences)

Cybersecurity job market in Poland (EU)

`

- Cybersecurity job market spreads differently around the World.
- Cybersecurity Companies in Poland:
- - IBM, EY(Ernst & Young), Banks (HSBC, Credit Suisse,), F-Secure, Intel (Research Center)
- Visa, Work Permit, Blue Card

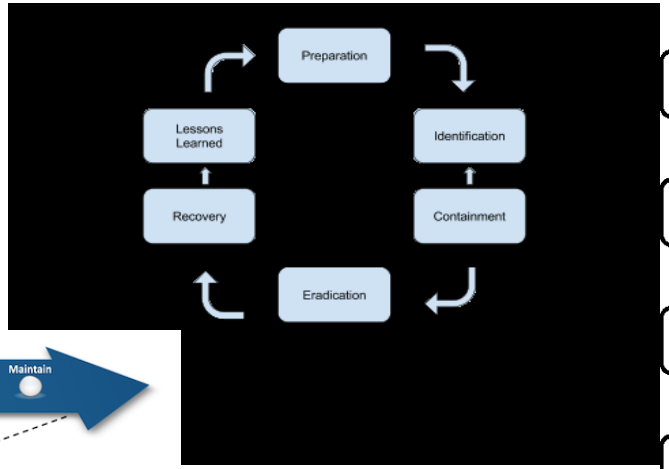
Cybersecurity carrier plan

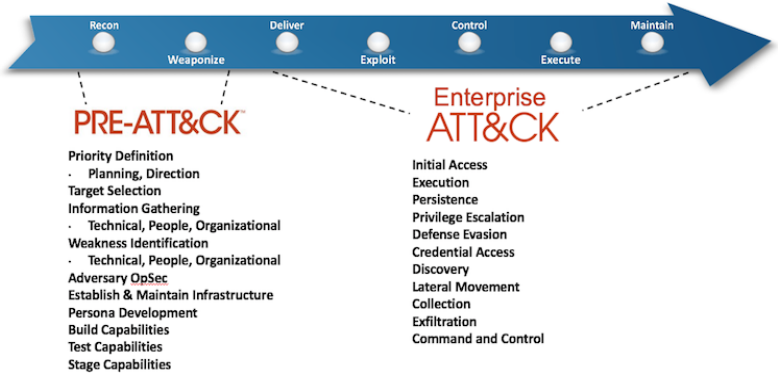
`

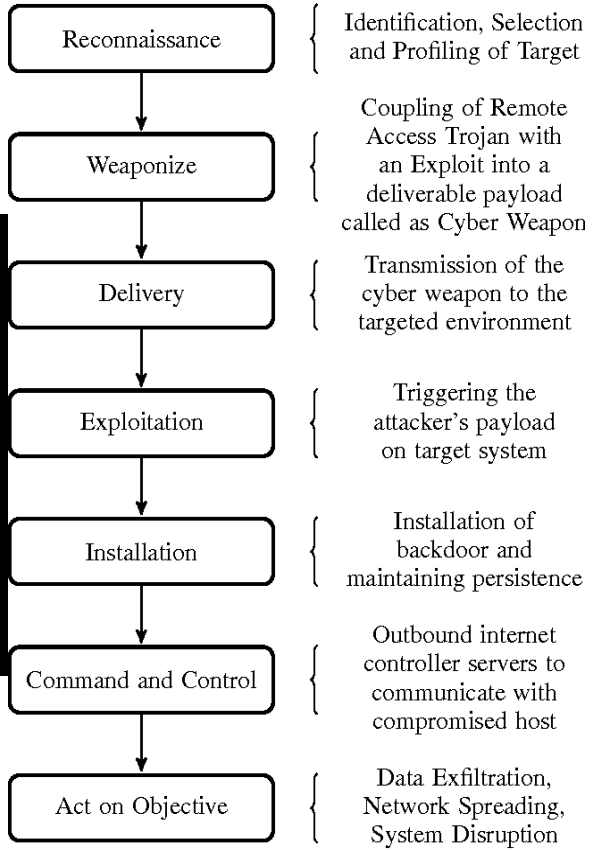
1. Know yourself (capabilities), what is your background? (Network, System, Programming?)
2. RED Team or BLUE Team or PURPLE Team???
   - RED Teaming is not Pentesting
3. Blue Teaming
4. Purple Teaming
5. Certifications

Cybersecurity frameworks

1. Incident Response Process
2. Cyber Kill Chain
3. MITRE ATT&CK framework



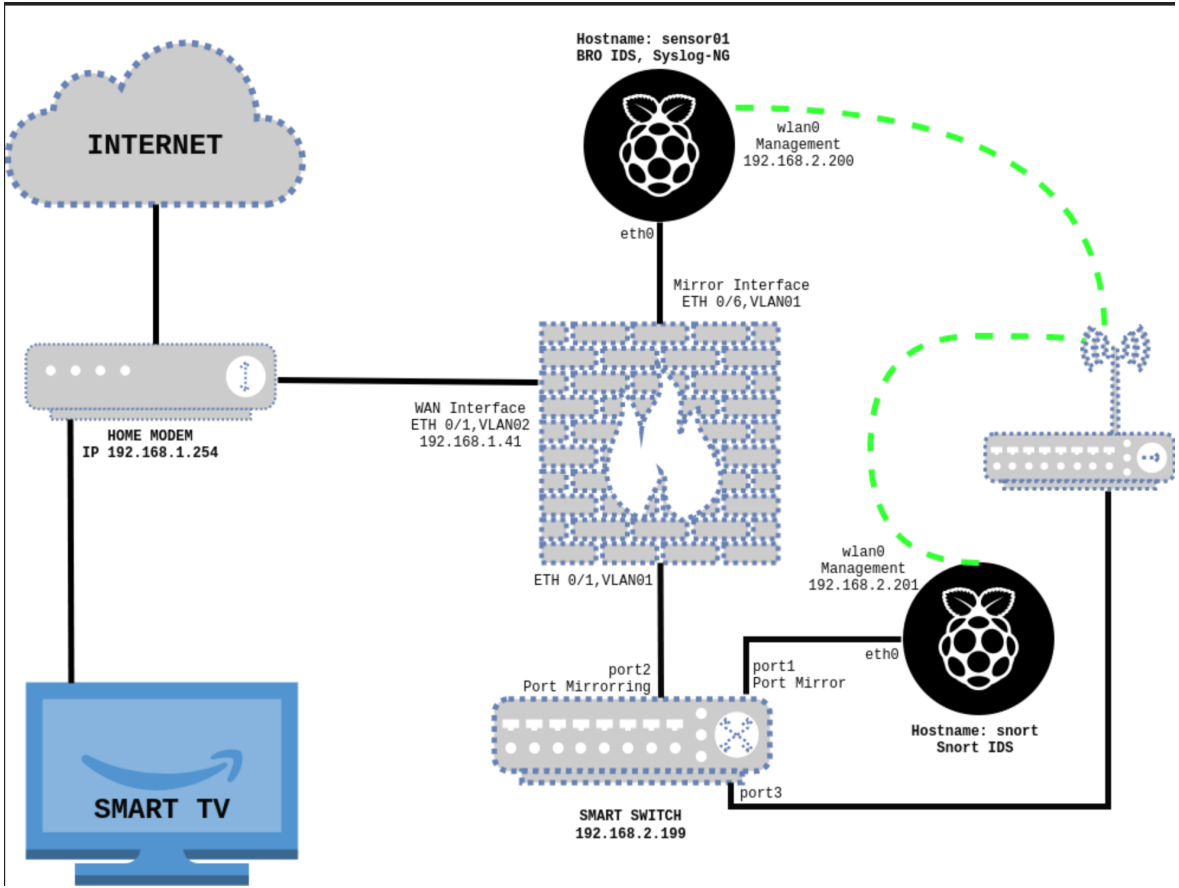




LAB, LAB, LAB

`

1. Build a LAB to simulate adversary (ESXi)
2. Build a LAB to understand home network traffic (syslog-ng, bro ids, graylog in cloud)



Building right mindset

`

1. Building right mindset
2. Learn investigation theory
3. Follow proper people:
   - David Bianco (Threat Hunting)
   - Chris Sanders (Investigation Theory)
   - Anton Chuvakin (SIEM) etc...

Malware Analysis

`

1. Dynamic Analysis
   - Sandboxing, understanding artefacts, cockoo (https://cuckoo.cert.ee)
   - Understanding Windows Internals
   - Tooling, Sysinternal (procmon, sysmon+splunk)

2. Static Analysis
   - Before RE you have to know Computer Architecture and Organization
   - IoT can be good start in terms of simplicity (MIPS architecture)
   - Not easy, still learning

Threat Hunting

`

1. Trend is changing….
   - Why Threat Hunting? (last work)
   - Zero-trust network (Firewall, IPS almost failed)
   - EndPoint Security is not AV (CarbonBlack, CrowdStrike)

2. Skills
   - You need a strong background in different domains
   - Improve researching skills
   - Learn how to create testable hypothesis
   - Methods (TaHiTi)

Study, Study, and Study again :)

`

1. Fundamentals (which one do you have?)
   - Network background
   - Sysadmin background
   - Programming background
2. Conferences
   - Try to attend at least 1 time to security conference
3. Threat Intelligence Important
   - Start to build network in twitter
   - Understand APT groups TTPs
4. Books in the next slide