Instrumenting defense techniques via subversion of adversaries

Ryan Mills
Lancaster University
Supervisors: Nick Race & Matthew Broadbent
Coseners 2019

Context

- High profile infrastructure targeted by expert actors
- Majority financial institutions (20% - FireEye)
  - Incorporating weaponized CVE / 0day PoC (Not always needed!)
  - Actor completes objective within network
- Traditional enterprise security solutions not suitable

Challenges

- Determined and Powerful Attackers
- Long Duration of Attacks
- Correlation of Events

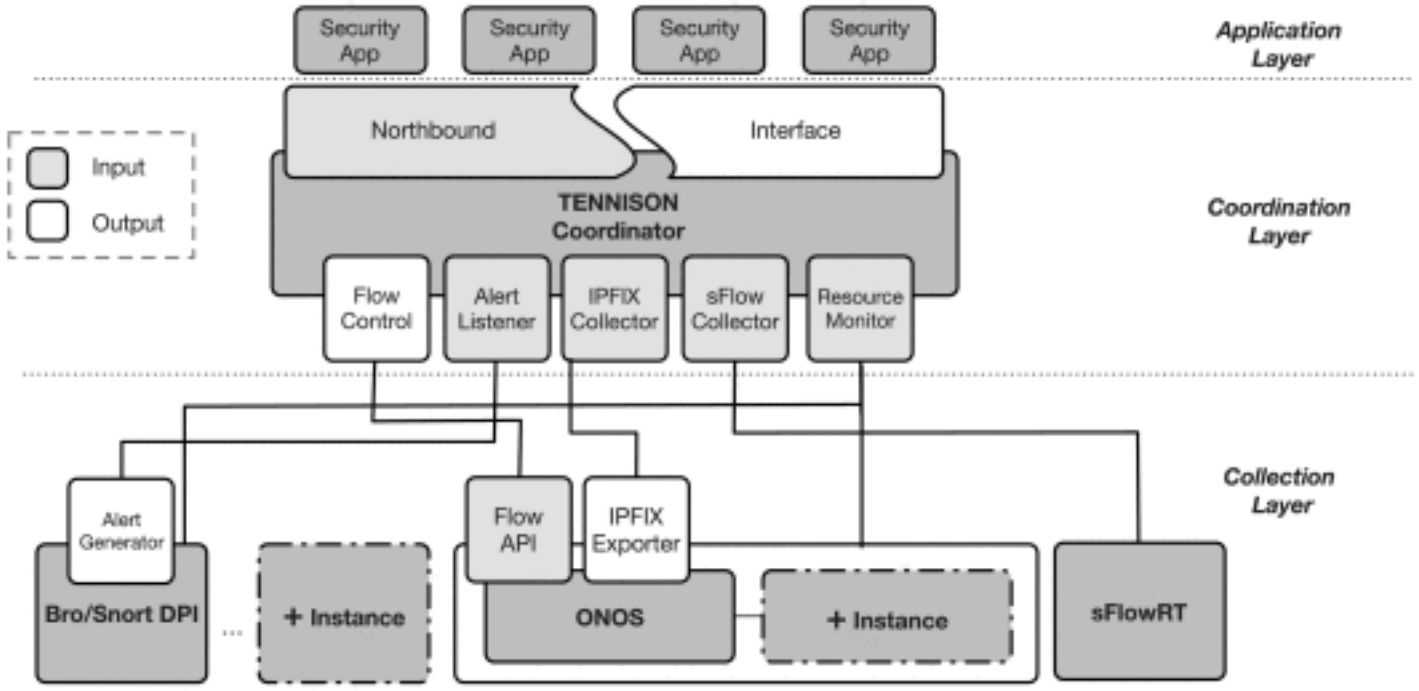
Current intelligence methods

- MISP (Malware Information Sharing Platform) [1]
- Forums & IRC Channels [2,3]
- Honeypots & Honeynets
  - Internal
  - External

1) https://www.misp-project.org/index.html
2) Proactive Identification of Exploits in the Wild Through Vulnerability Mentions Online
3) Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence

Tennison [1]

- Existing SDN framework within Lancaster University
- Network based monitoring
- Multi-level scalability
- Policy engine

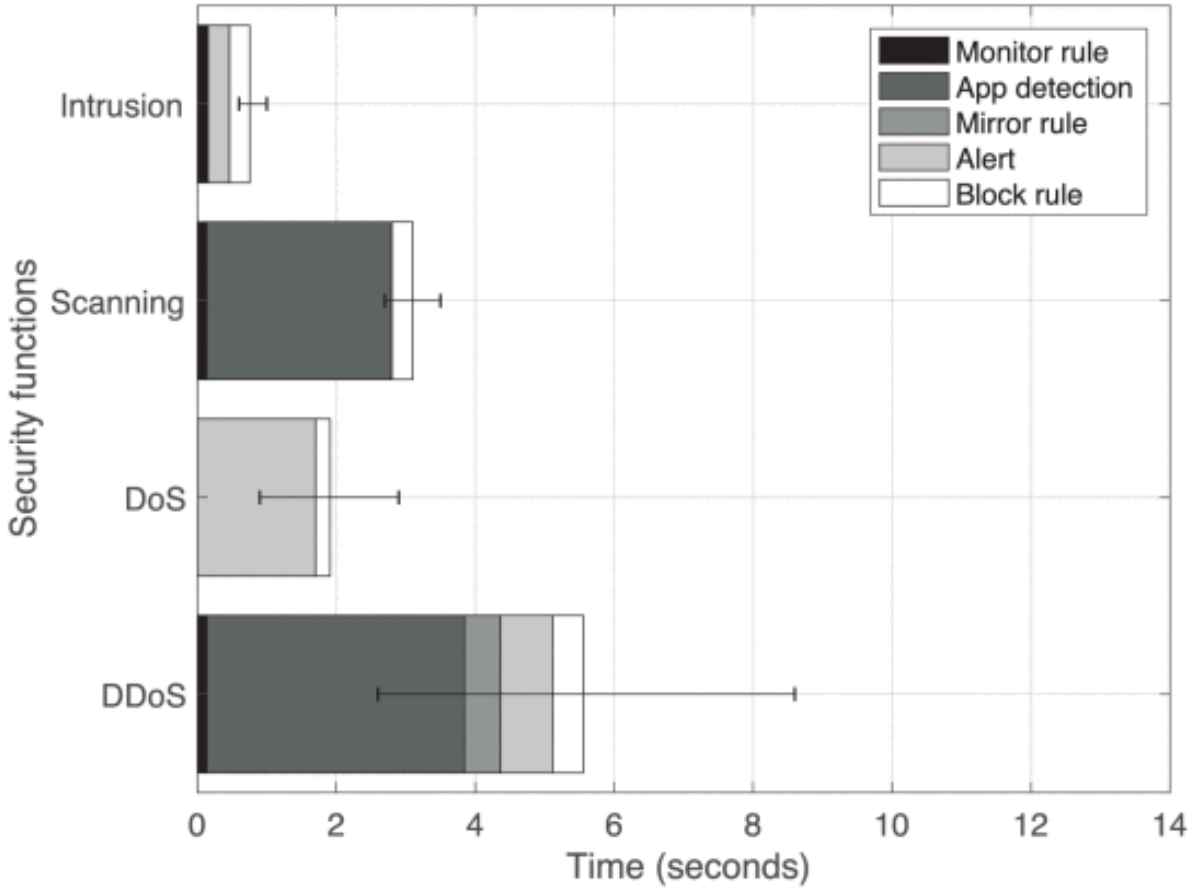


1) Lyndon Fawcett, Sandra Scott-Hayward, Matthew Broadbent, Andrew Wright, and Nicholas Race "TENNISON: A Distributed SDN Framework for Scalable Network Security." IEEE Journal on Selected Areas in Communications (2018).

vsftpd (2.3.4)

- ‘:)’ payload
- Shell access on port 6500

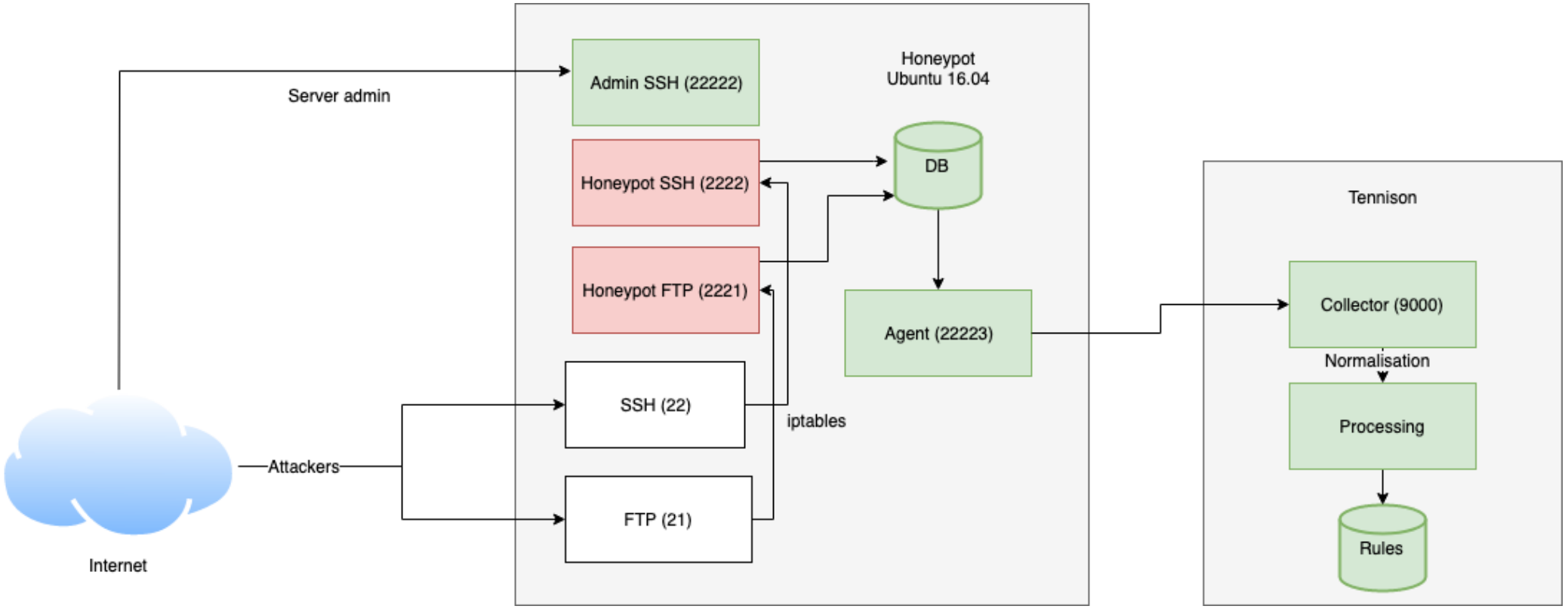
- Problems?
  - TLS
  - Encoding
  - Redirection
  - Unknown exploit



- Solution requires context and knowledge

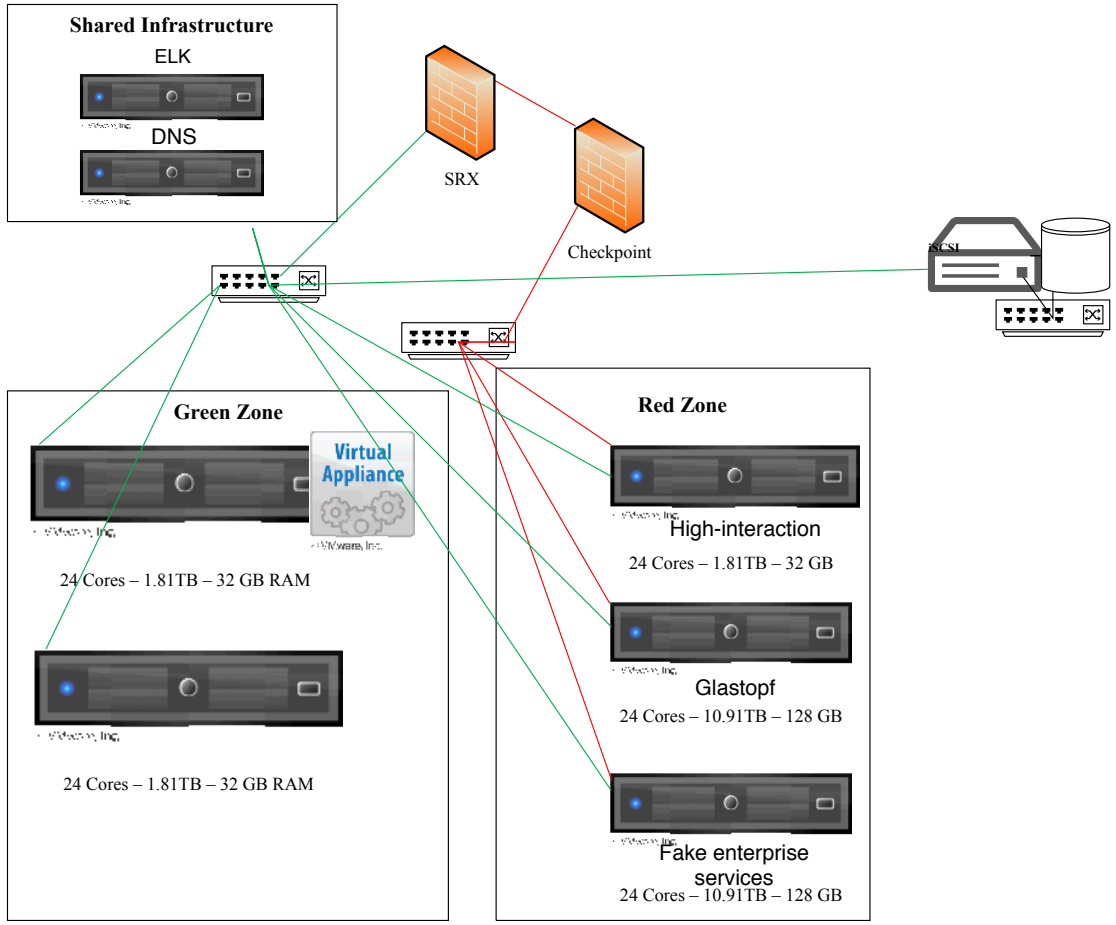
Tennison v2

- Honeypot with exposed FTP service
- Agent identifies malicious event
- Create actionable rules



Intelligence gathering

- Low interaction
  - tcpdump
- Medium interaction
  - Authentication credentials
  - Shell input
  - Malware
  - Payloads
  - Further compromise attempts
- High interaction
  - Syslogs
  - Agent

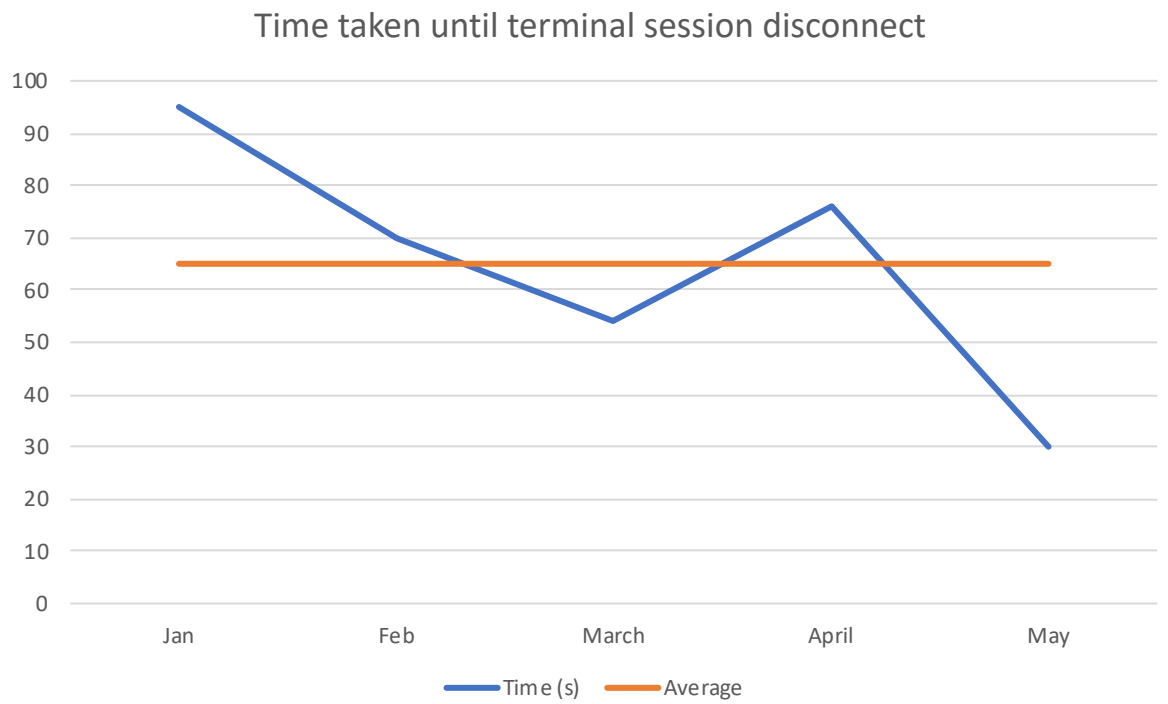


Directors:
Angelos Marnerides <angelos.marnerides@lancaster.ac.uk>
John Couzins <j.couzins1@lancaster.ac.uk>

The emulation question

- Manual attackers stay connected to medium interaction SSH honeypots for an average of 65 seconds
- Bots last even shorter
- 99% never login again

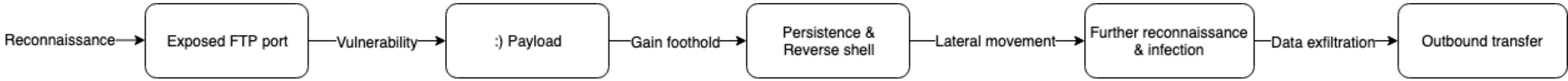
- Why?
  - Unrealistic environment
  - Commands
  - Network setup



High interaction indicators

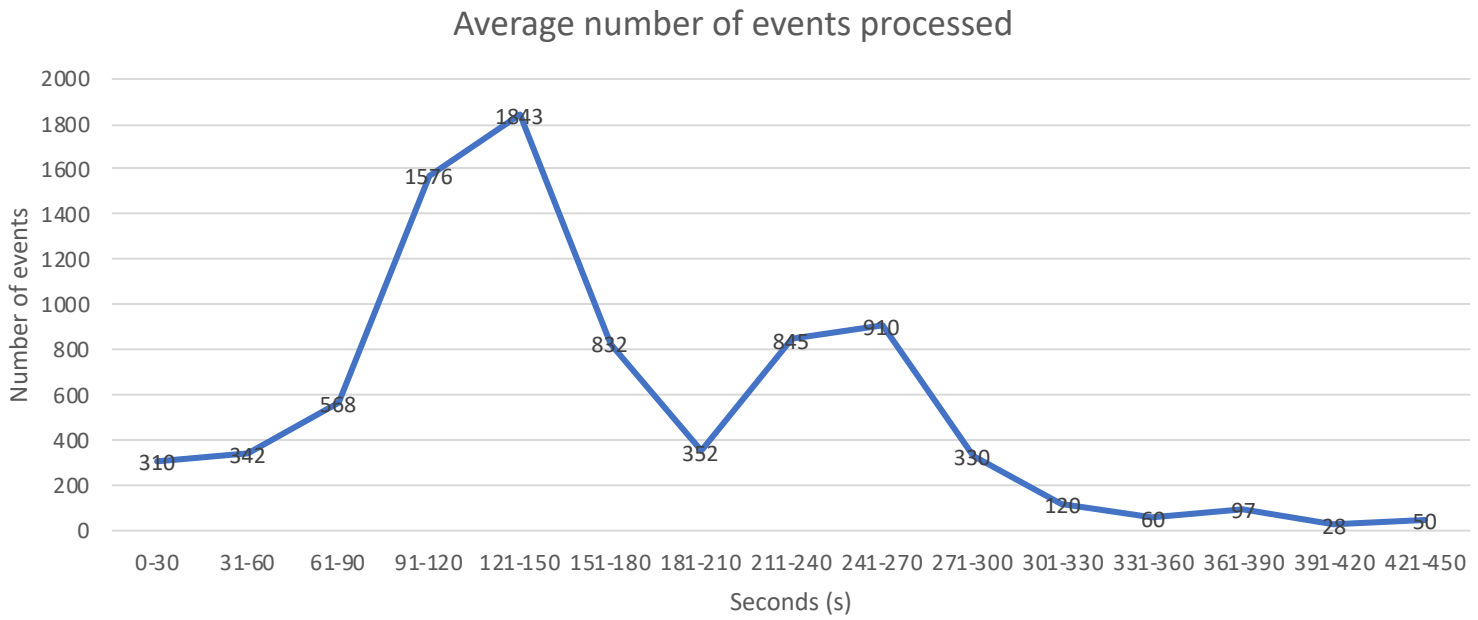
- Agent
- Docker logging
- MiTM (Man in The Middle) proxy
- VMI (Virtual Machine Introspection)

- Attack patterns through entire chain of events
  - vsftpd use case



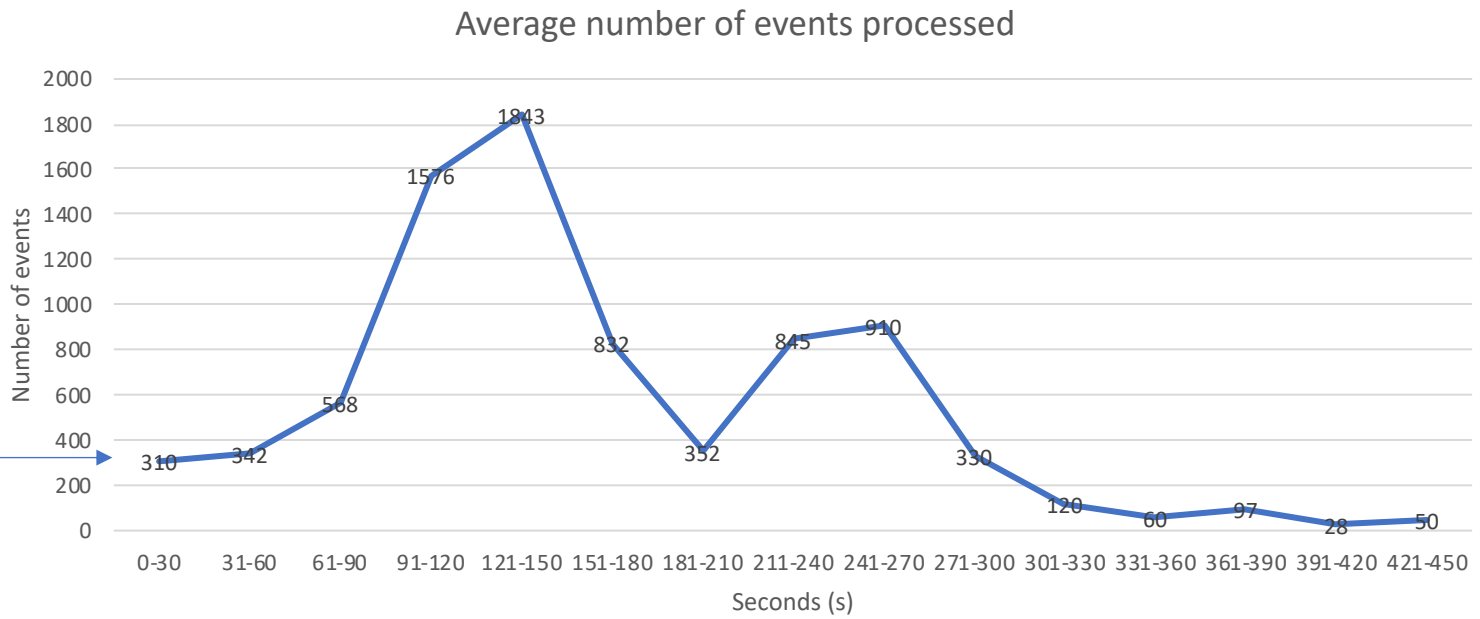
- Important to gather rich amount of data

Gaining indicators



Gaining indicators

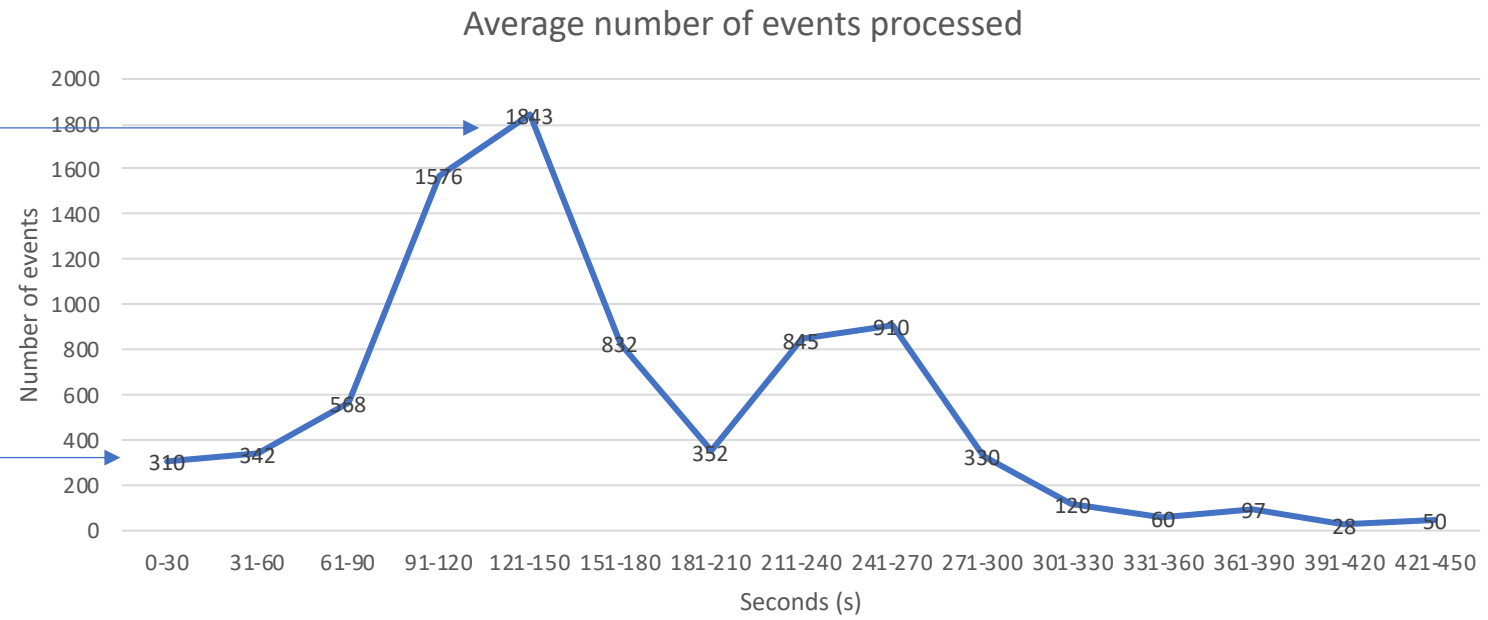
Bruteforce



Gaining indicators

Malware

Bruteforce

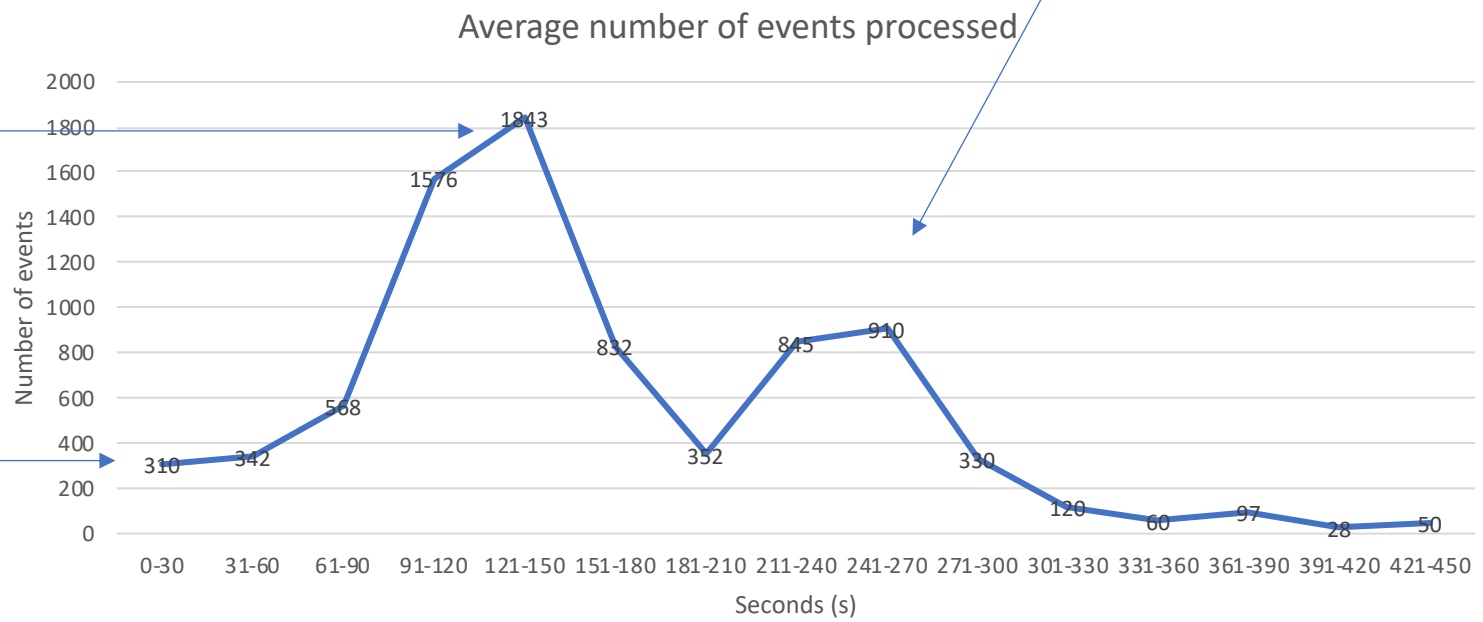


Gaining indicators

Lateral movement

Malware

Bruteforce

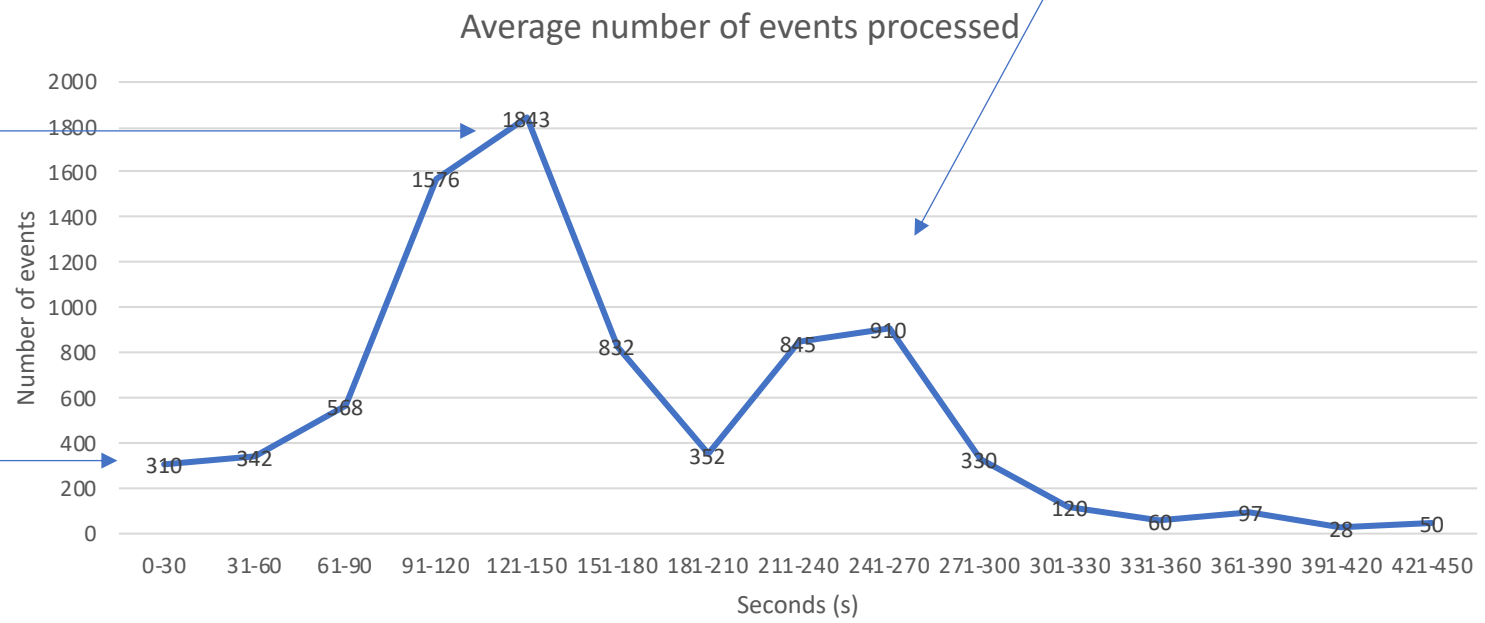


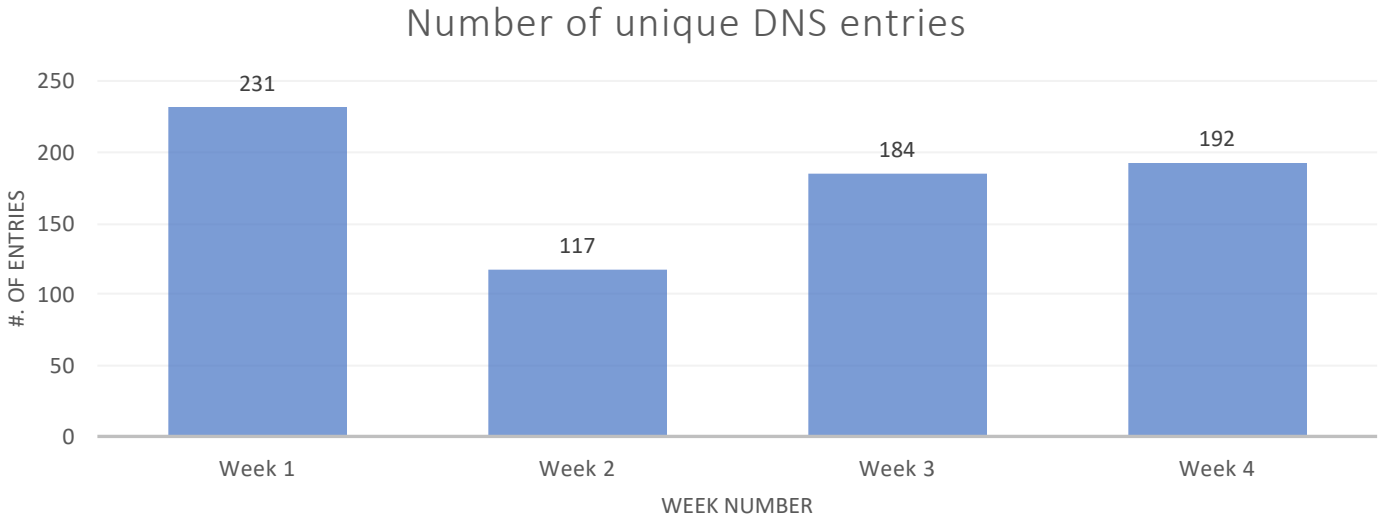
Gaining indicators

Lateral movement

Malware

Bruteforce





Future work

- Mining attack data
- Policy application
- Internal network topology
  - Containernet
  - Honeyd
- Attack surface
- Share data

Thank you

- Any questions?