Understanding Cyber-Attacks

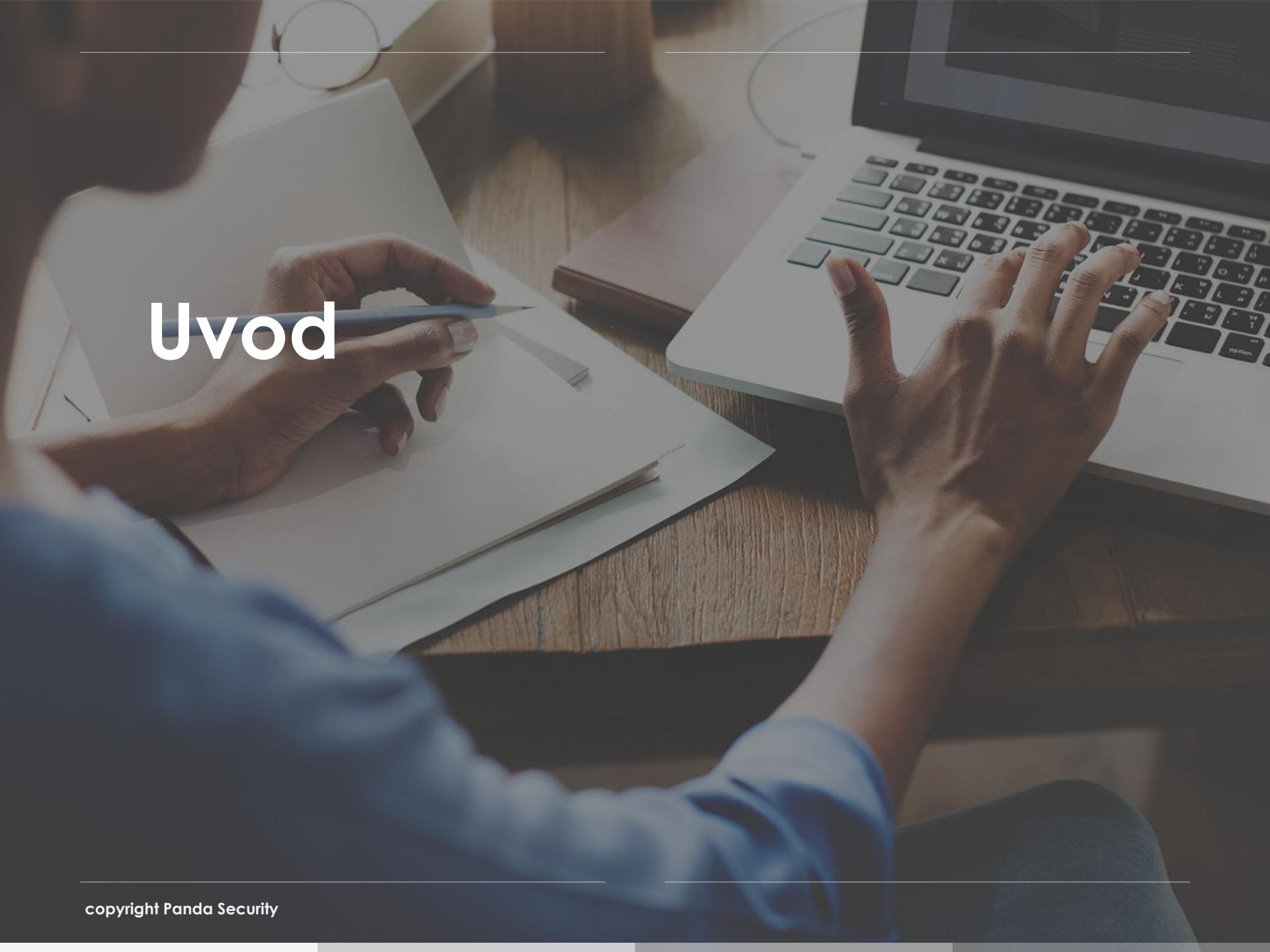
The Cyberkill Chain

Vladimir Stanković – BDM West Balkans

panda

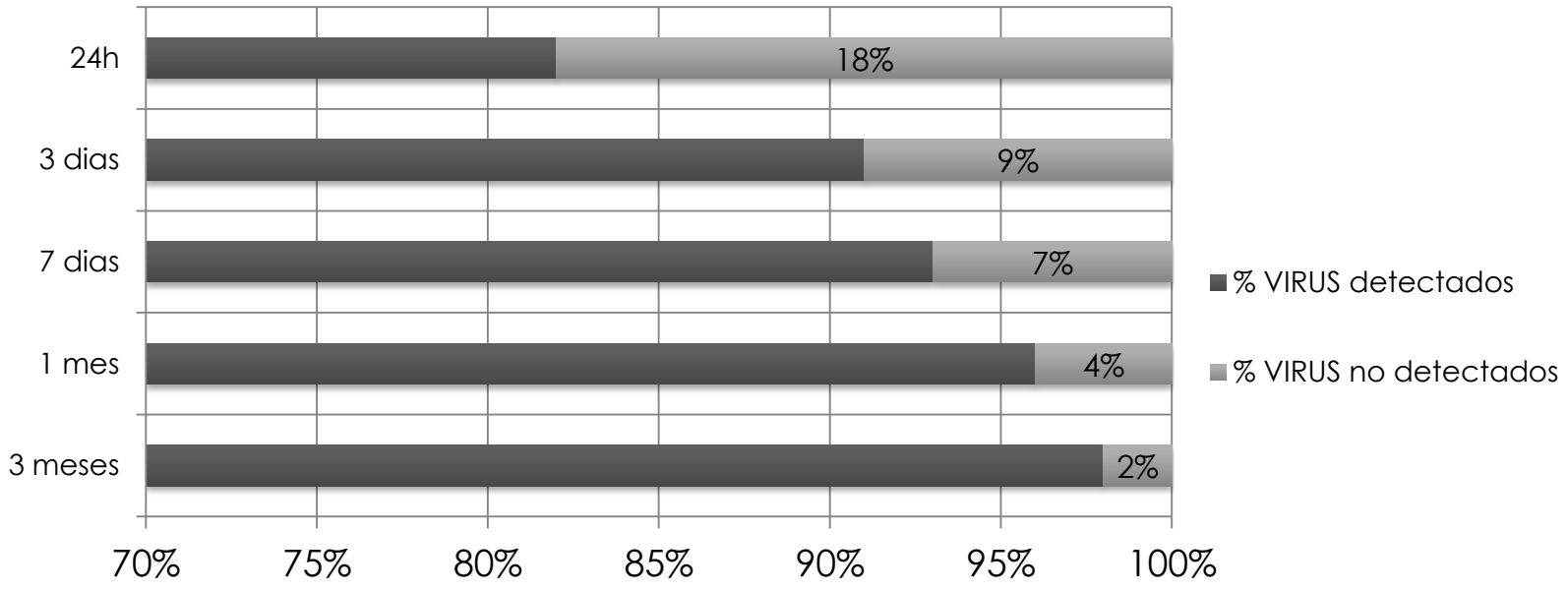
pandasecurity.com

Sadržaj:



Uvod

- **Tradicionalne antivirusne tehnologije** (signatures, heuristics, content filtering, behavioral analysis) su **reaktivne**.



- Prevencija
- Detekcija
- Reakcija

Razumevanje Cyber-Kill lanca

Lockheed Martin – Inteligence Driven Defense

model for the identification and prevention of cyber intrusions activity

Bolje razumevanje napadača i njihovih tehnika u cilju razvoja efikasnijih sistema odbrane

External Reconnaissance

Weaponization and Packaging

Delivery

Exploitation

Installation

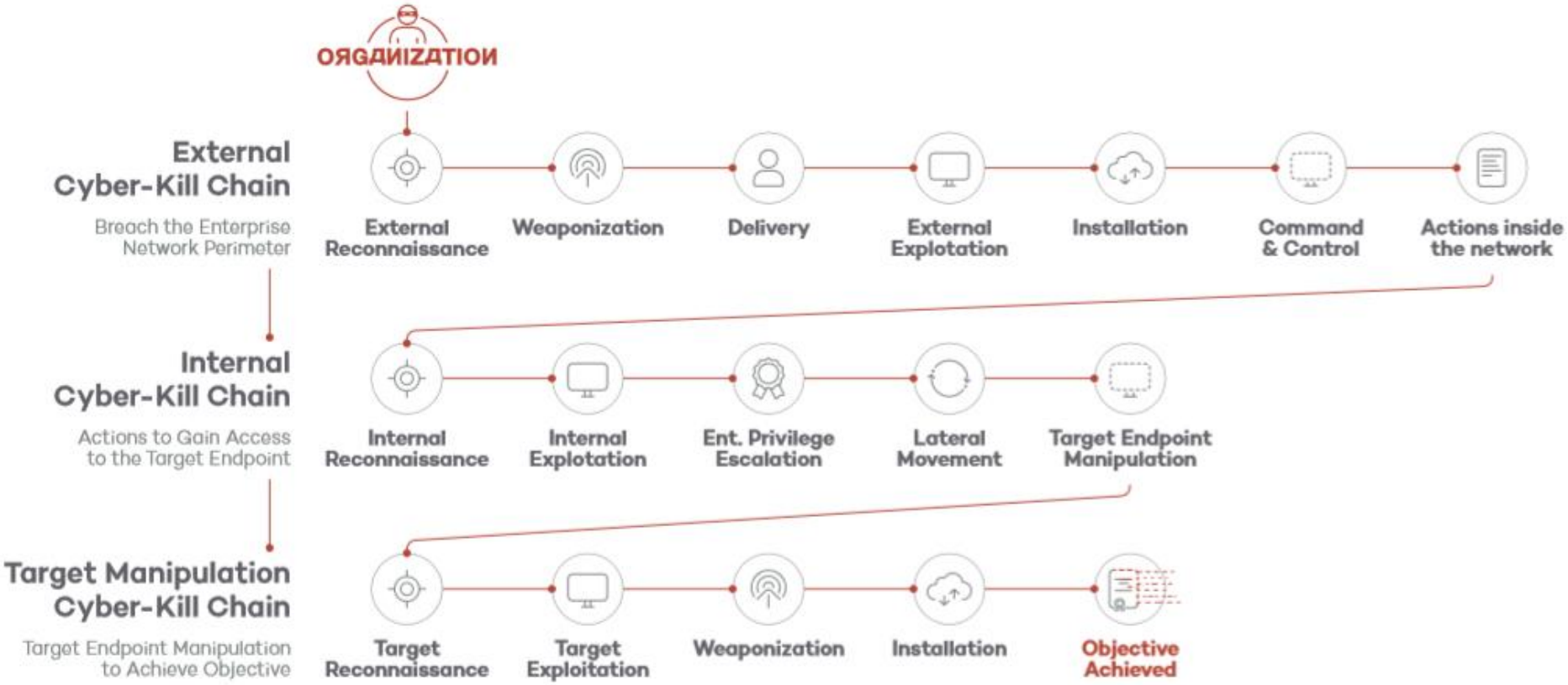
Command and Controle

Actions on Targets

External Cyber-Kill Chain

External Cyber-Kill Chain
+ Internal Cyber-Kill Chain

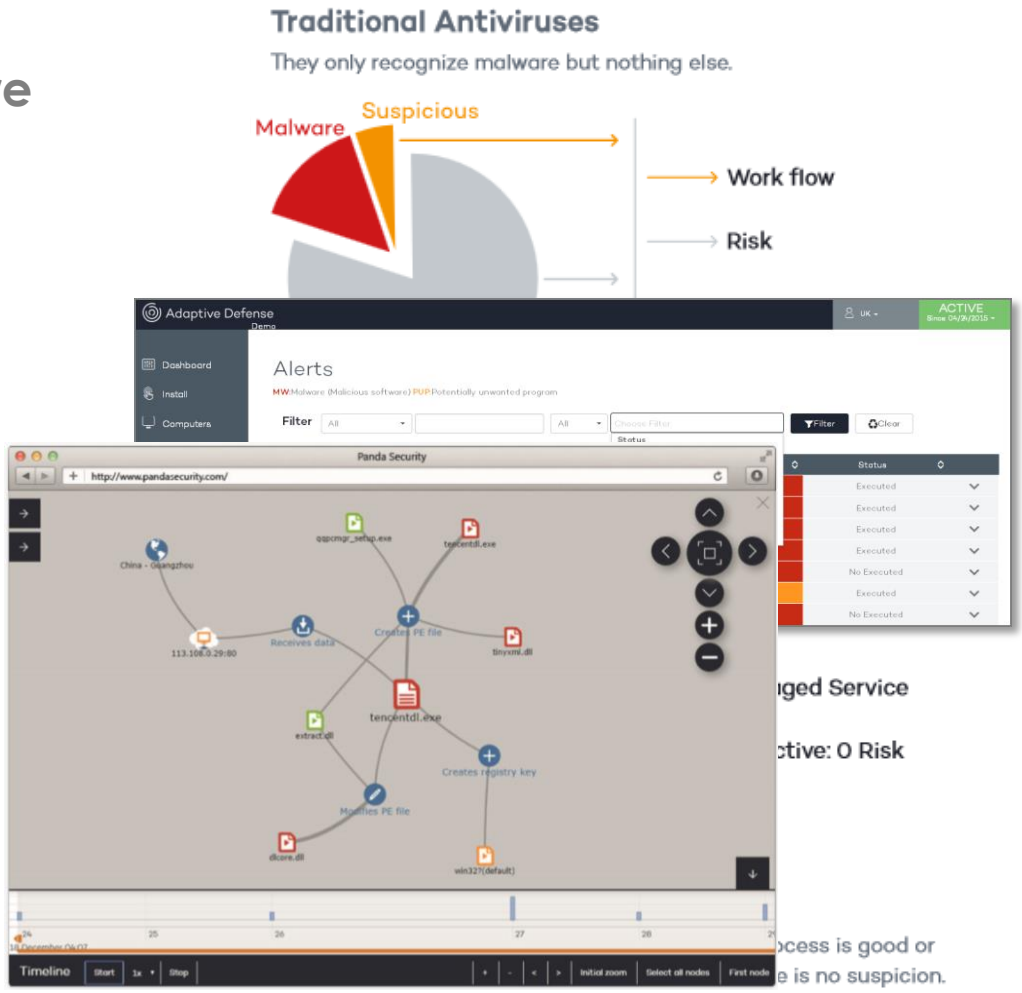
Extended Cyber-Kill Chain



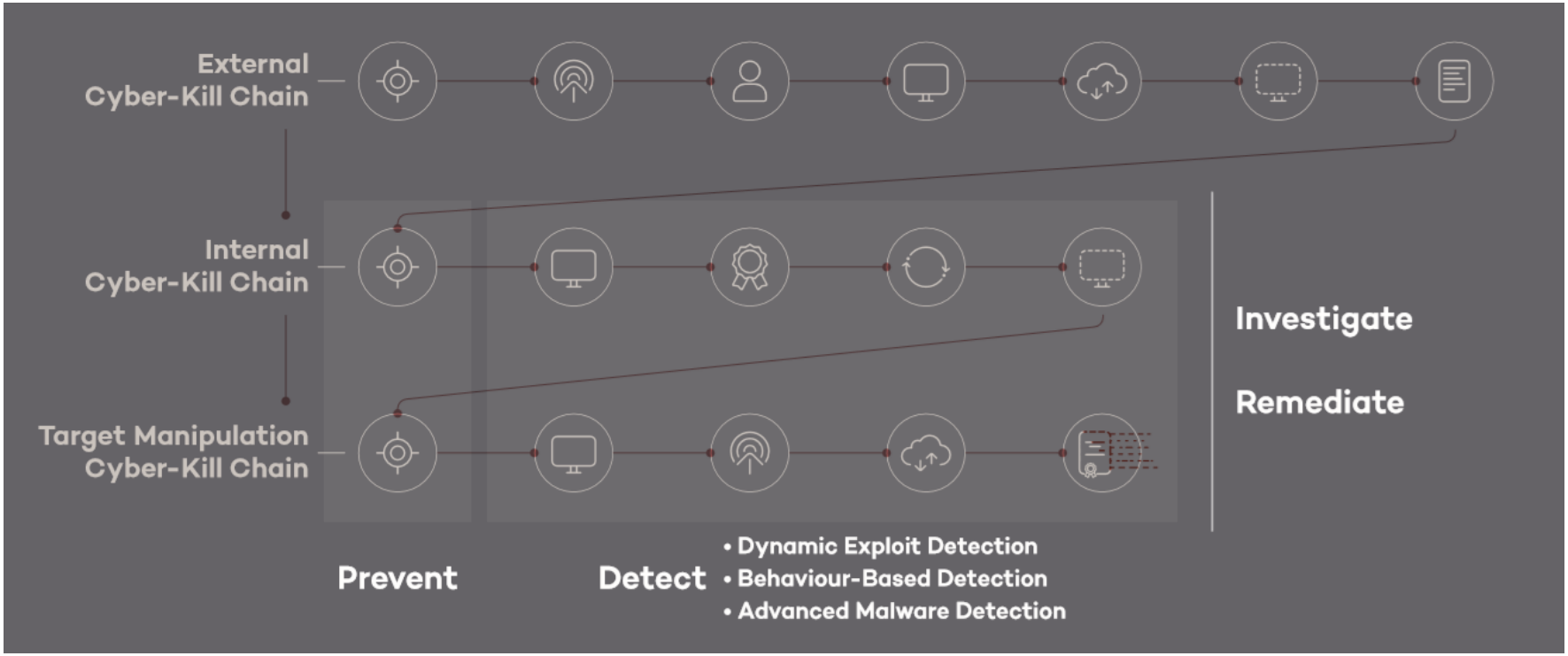
Adaptive Defense tehnologija i Panda Adaptive Defense u CKC

Glavni oslonci EDR tehnologije

- Zaštita od poznatog malware
- Napredna detekcija
- Dynamic exploit detection
- Ublažavanje (Mitigation)
- Remedijacija
- Forenzika



Panda Adaptive Defense u Cyber-Kill lancu




Hvala!
panda
pandasecurity.com