

# Understanding Cyber-Attacks

## *The Cyberkill Chain*

Vladimir Stanković – BDM West Balkans



[pandasecurity.com](https://www.pandasecurity.com)

---

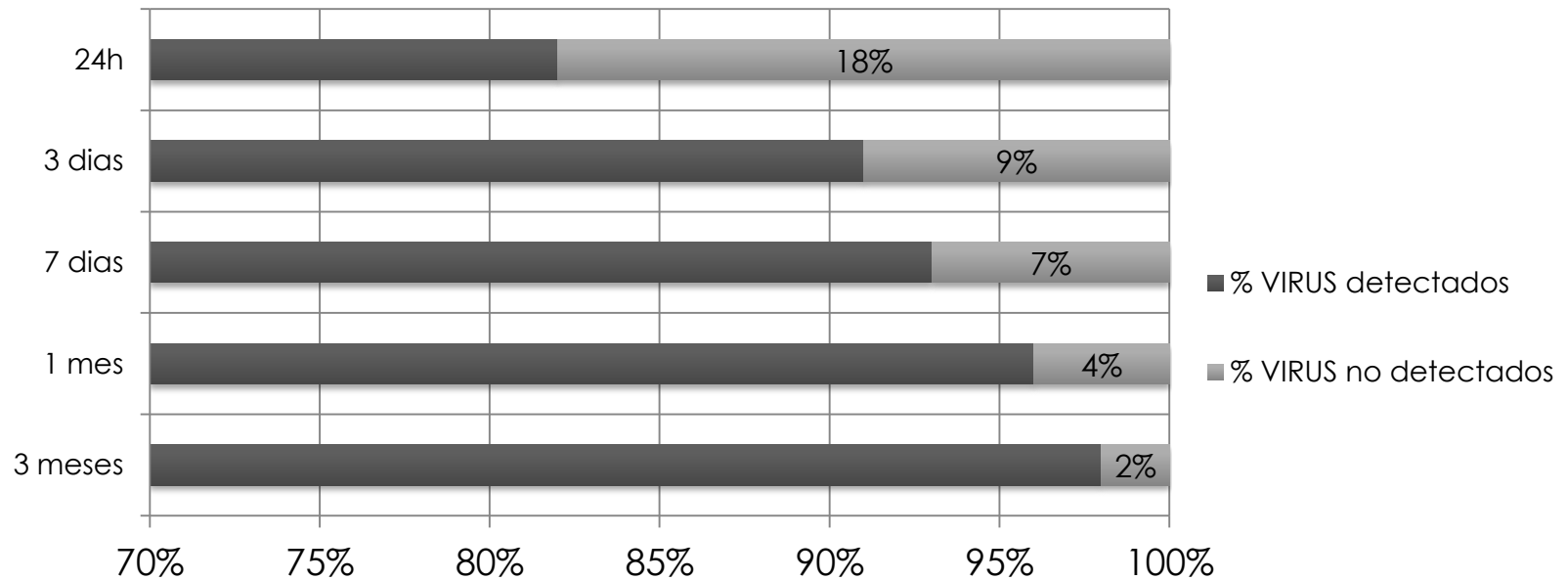
# Sadržaj:

- **Uvod**
- **Razumevanje Cyber-Kill lanca (CKC) i proširena verzija Cyber-Kill lanca**
- **Endpoint Detection&Response tehnologija i Panda Adaptive Defense u CKC**

A person is sitting at a wooden desk, working. They are holding a blue pen over a white sheet of paper. To their right is a silver laptop with their hand on the keyboard. The scene is dimly lit, with a warm, blue-toned light. The word "Uvod" is overlaid in white text on the left side of the image.

# Uvod

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



---

➤ **Prevensija**

➤ **Detekcija**

➤ **Reakcija**



A person is sitting at a wooden desk, working on a laptop. Their hands are visible, one typing on the keyboard and the other holding a pen over a piece of paper. The scene is dimly lit, with a soft glow from the laptop screen. The text 'Razumevanje Cyber-Kill lanca' is overlaid in white, bold font across the center of the image.

# Razumevanje Cyber-Kill lanca

---

## Lockheed Martin – Intelligence 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 Control**



**Actions on Targets**





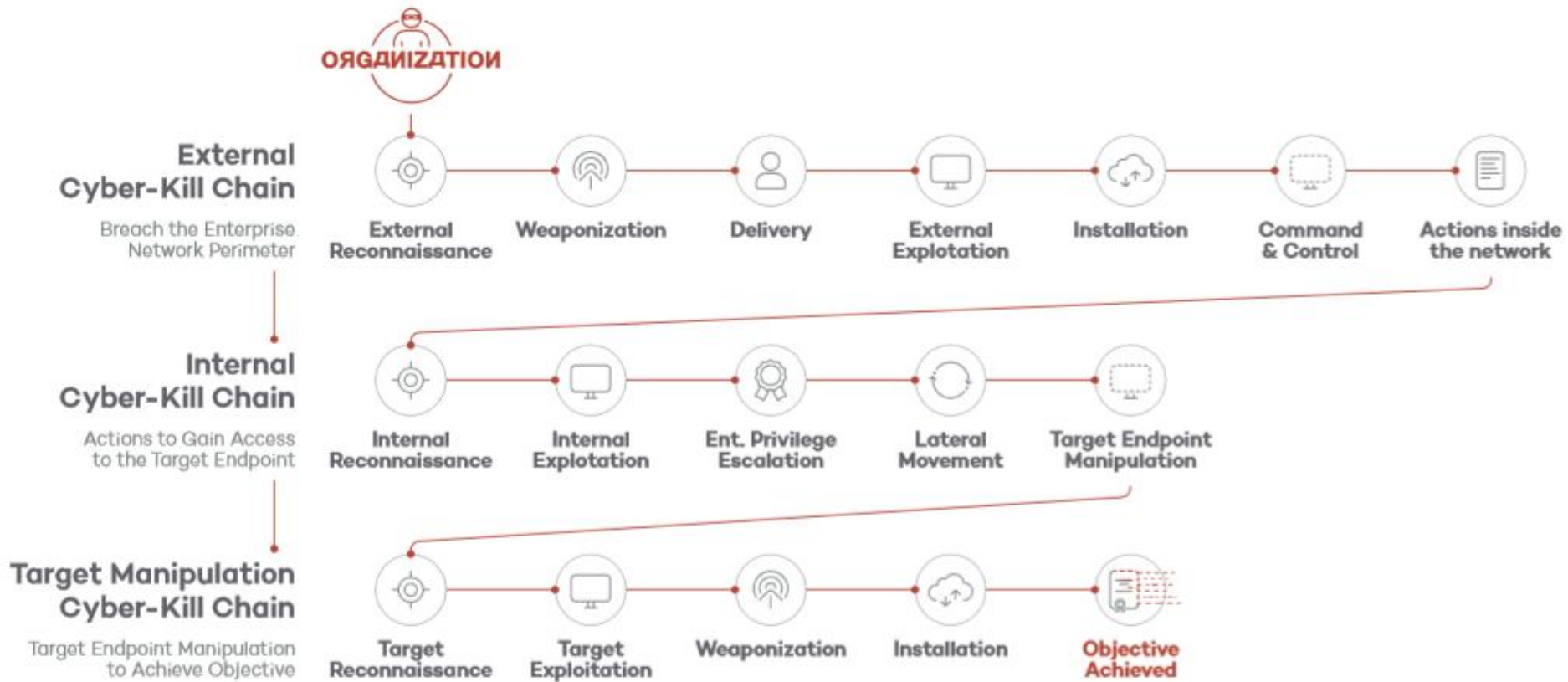
# External Cyber-Kill Chain



# External Cyber-Kill Chain + Internal Cyber-Kill Chain



# Extended Cyber-Kill Chain



A person is sitting at a wooden desk, working on a laptop. Their hands are visible, one typing on the keyboard and the other holding a pen over some papers. The scene is dimly lit, with a soft glow from the laptop screen. The overall atmosphere is professional and focused.

# 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

## Traditional Antiviruses

They only recognize malware but nothing else.

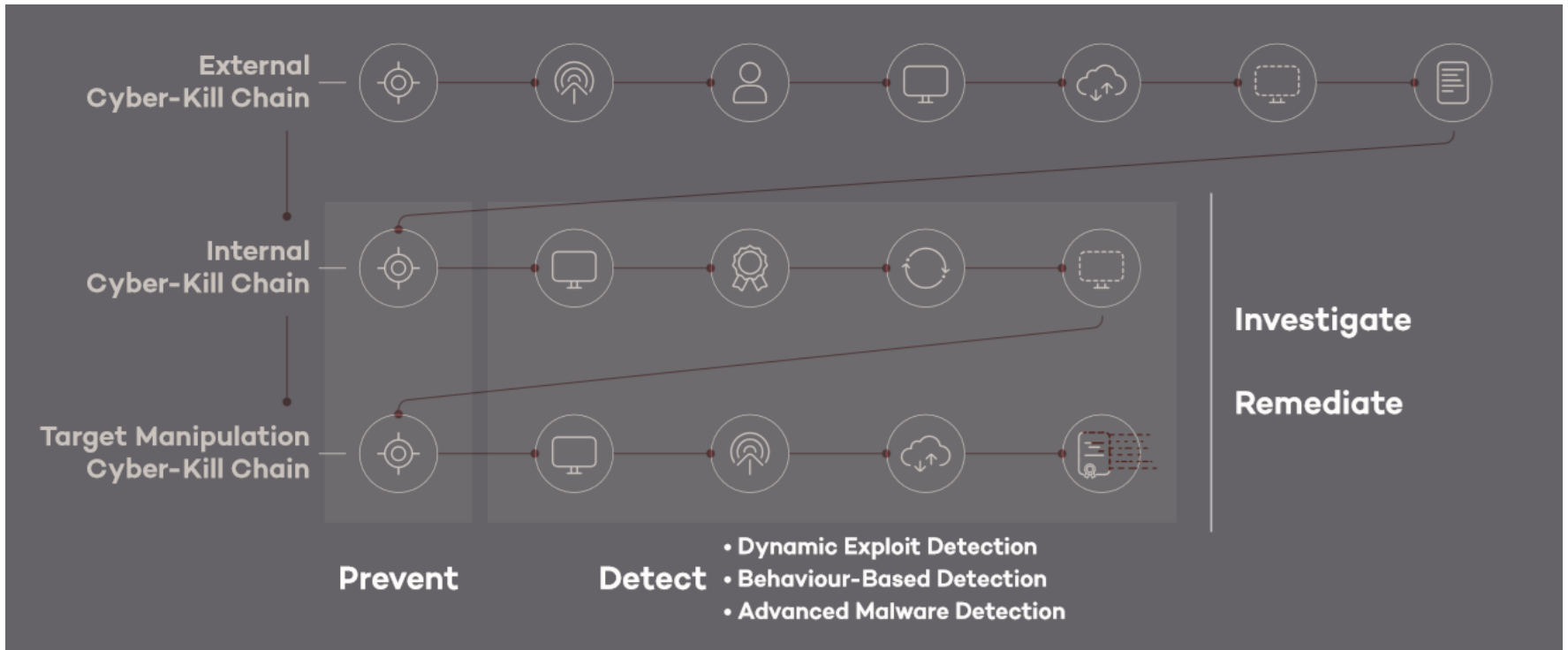


The screenshot displays the Panda Security Adaptive Defense interface. At the top, it shows 'Adaptive Defense Demo' with a user 'uk' and a status 'ACTIVE Since 04/09/2015'. Below this is an 'Alerts' section for 'MW:Malware (Malicious software) PUP:Potentially unwanted program'. A filter is set to 'All'. The main area shows a process flow diagram for 'tencentdl.exe' with nodes for 'Receives data', 'Creates PE file', 'Modifies PE file', 'Creates registry key', and 'Extracts data'. A timeline at the bottom shows the sequence of events from 20 to 28. On the right, a table shows the status of various alerts:

Status	Count
Executed	0
Executed	0
Executed	0
Executed	0
Executed	0
No Executed	0
Executed	0
No Executed	0

Below the table, it indicates 'Managed Service' and 'Active: 0 Risk'. At the bottom right, a note states 'Success is good or there is no suspicion.'

# Panda Adaptive Defense u Cyber-Kill lancu





# Hvala!



[pandasecurity.com](https://www.pandasecurity.com)