# “Cyber kill chain”

Vladimir Vučinić

# Današnje pretnje

## Malware

**92%**
Increase in new downloader variants

**80%**
Increase in new malware on Macs


## Web Threats

More than
**1 Billion**
Web requests analyzed each day
Up 5% from 2016

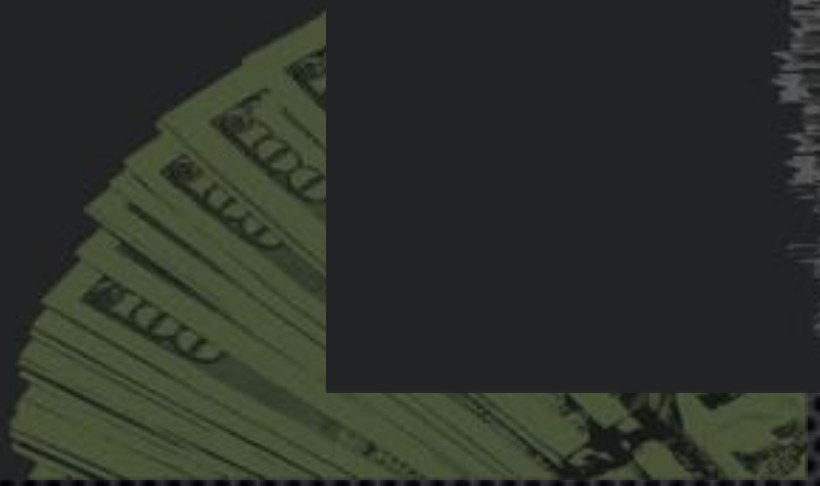
**1 in 13**
Web requests lead to malware
Up 3% from 2016

# Današnje pretnje

## Ransomware

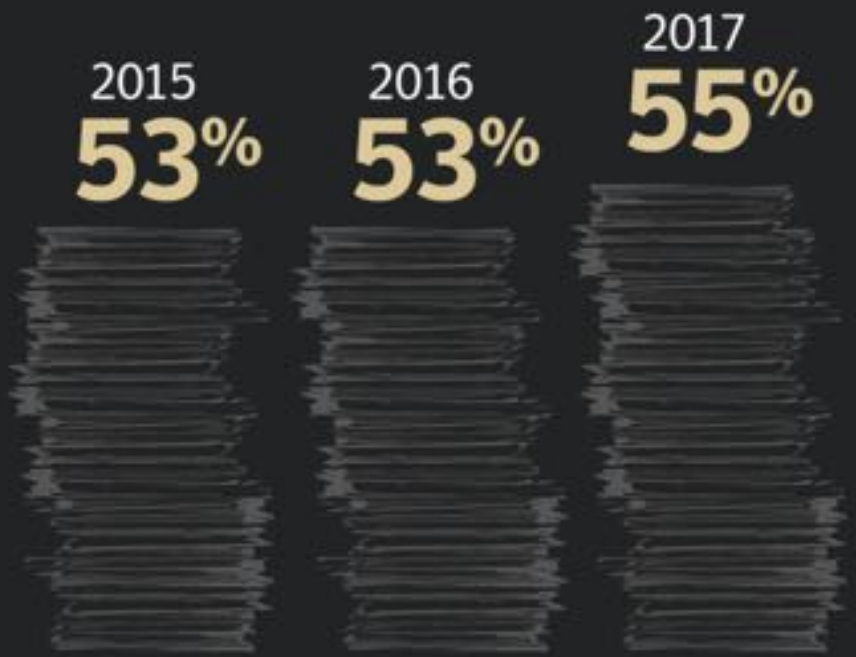
**5.4B**
WannaCry
attacks blocked

**46%**
Increase in new
ransomware
variants

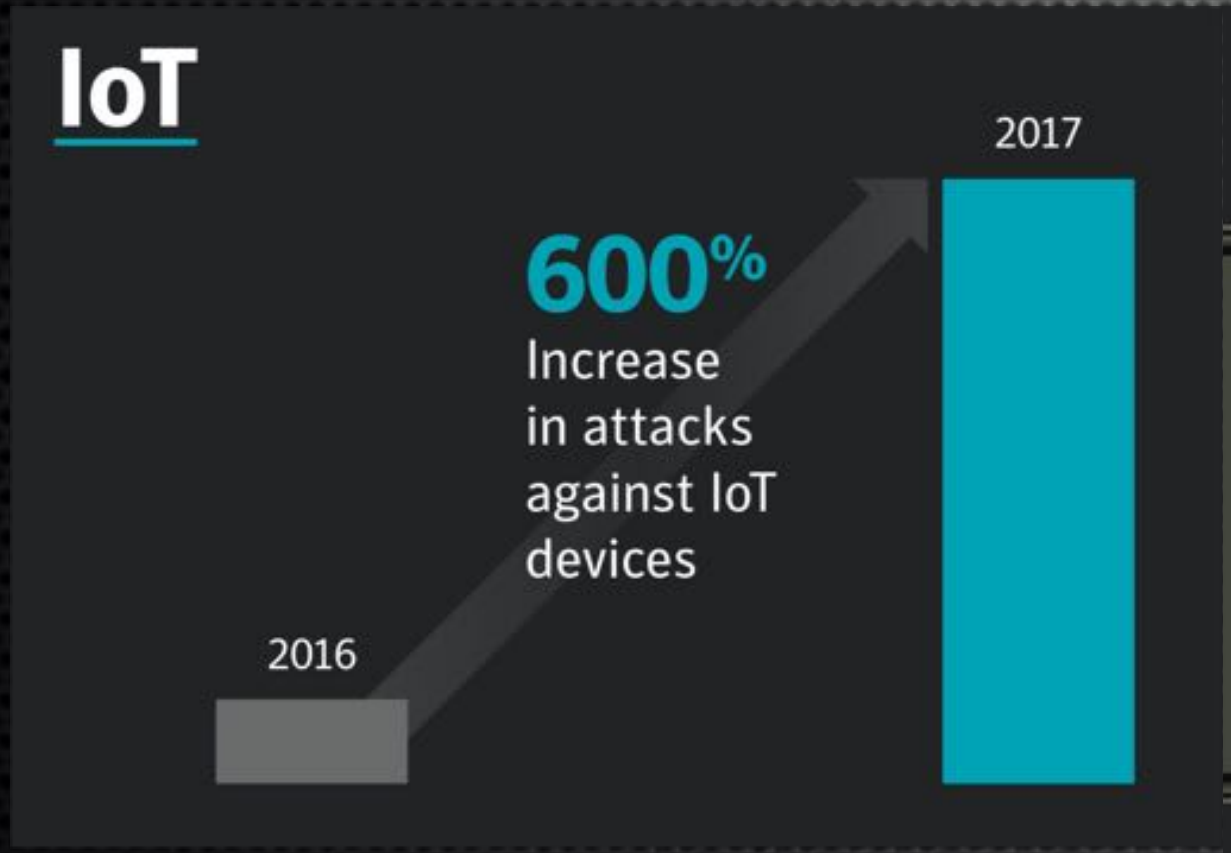


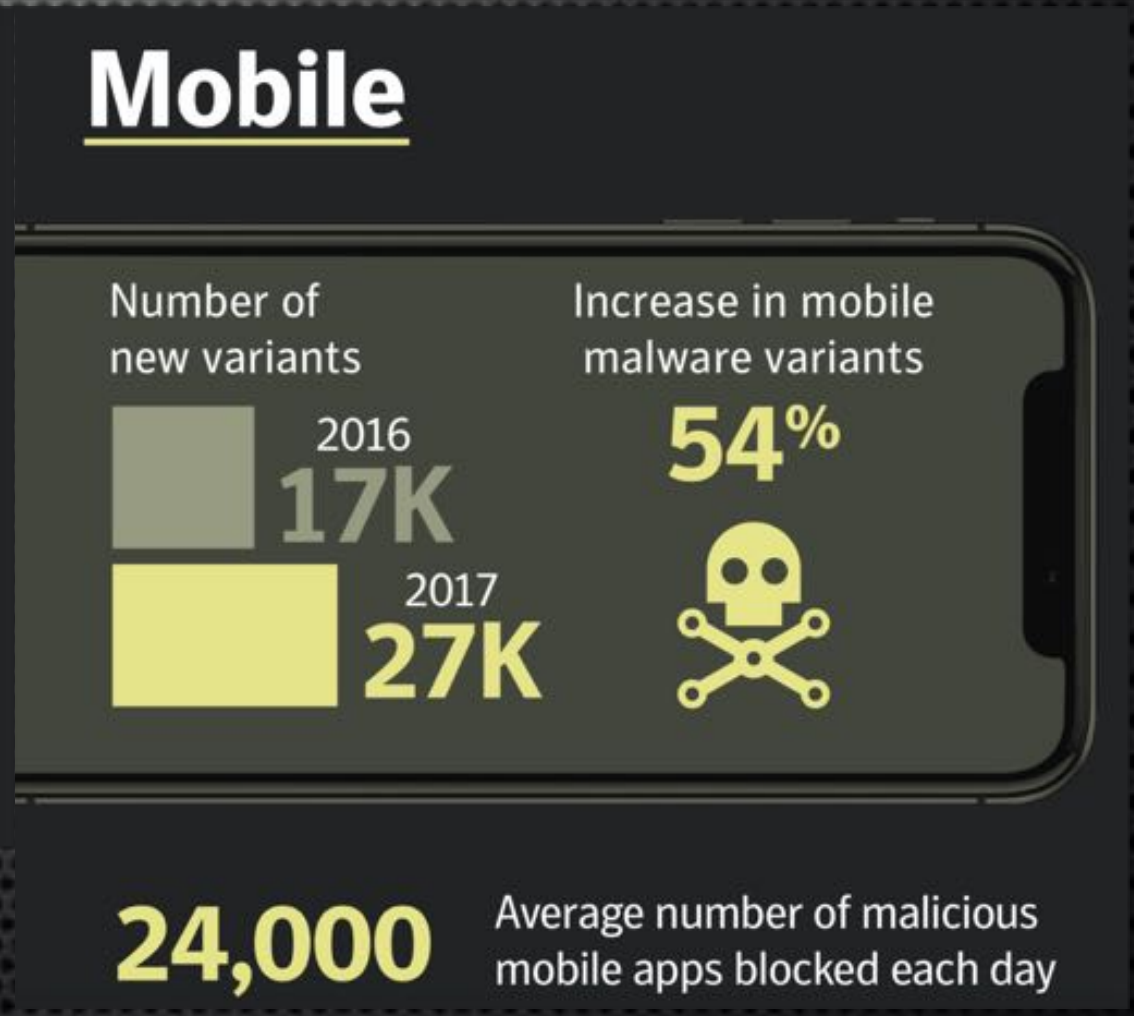
## Email

Percentage
spam rate



# Današnje pretnje



# Današnja preduzeća


Mobilni, tableti, IoT


Nestaje granica odbrane


Prihvatanje cloud-a


Smanjen budžet, nedostatak kadrova


Nove regulative, kontrole


Security as a Service

# Kako da se onda odbranimo?

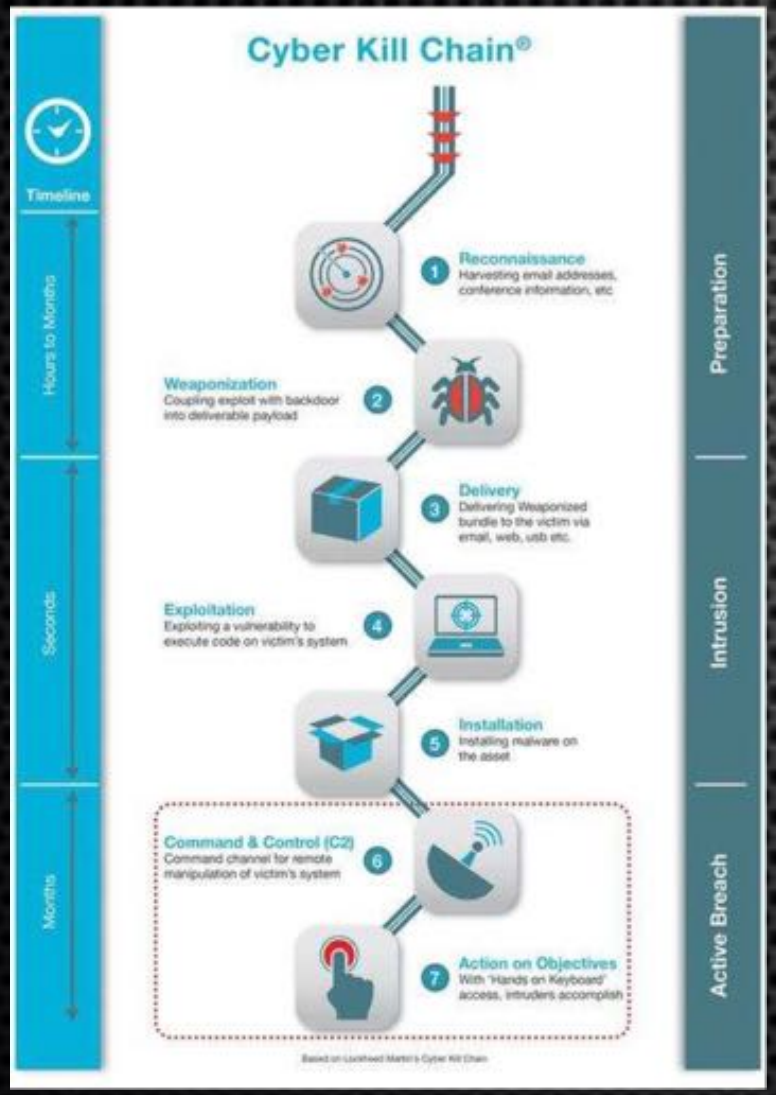
1. Sistematično

   **Cyber Kill Chain**

   +

2. Security Framework


# Cyber Kill Chain




- Vojni concept, primenjen na Cyber Security
- Razvijen u Lockheed Martin –u tokom 2011.g.
- Opisuje 7 faza koje će protivnik primeniti u napadu na organizaciju
- Napad se smatra uspešnim kada i ako se izvrše sve faze napada

# Cyber kill chain - faze


## 1. Reconnaissance - izviđanje

Traženje informacija o cilju, pretraga email adresa, LinkedIn i Facebook profila tj. socijalnih mreža, informacija sa konferencija,sa fakulteta, raznih foruma, igrica i sl.

# Cyber kill chain - faze


## 2. Weaponization – naoružavanje

Spremanje malvera, spajanje “payload”-a sa ranjivostima. Kreiranje alata za udaljeni pristup, kao što su virusi ili crvi krojeni po meri, posebno ako se zna vrsta ranjivosti koje se može iskoristiti.

# Cyber kill chain - faze


## 3. Delivery – isporuka

**Isporuka spremljenog oružija – malvera cilju - žrtvi, putem emaila, web-a, USB-a ili na drugi raspoloživ način.**

# Cyber kill chain - faze


## 4. Exploitation – esploatacija

Pokreće se malver koji cilja mrežu, računare i servere, mrežne uređaje i sl. da bi pronašao i iskoristio eventualne ranjivosti unutar sistema.

# Cyber kill chain - faze


## 5. Installation – instalacija

**Malware instalira pristupnu tačku na sistem, (na pr., "backdoor") koji će napadač koristiti u sledećim fazama napada/upada.**

# Cyber kill chain - faze


## 6. Command & Control – upravljanje i kontrola

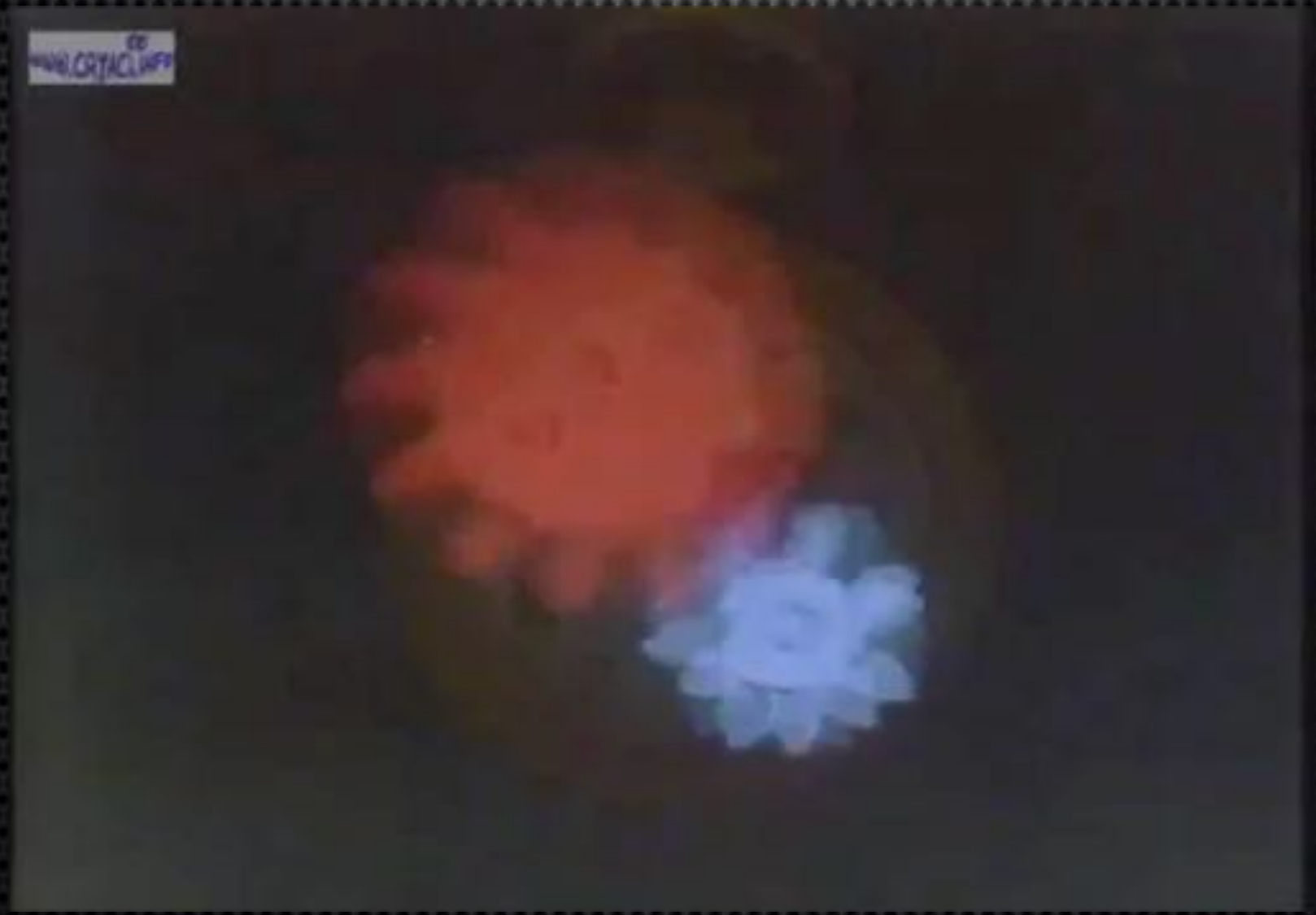
**Malver pruža napadaču priliku da preuzme kontrolu i upravljanje unutar sistema – da ima “ruke na tastaturi” i praktično stalan pristup mreži.**

# Cyber kill chain - faze


## 7. Actions on Objectives – akcije nad ciljem

Sa “sekirom u medu”, napadač izvršava željene ciljeve - akcije, kao što je izvlačenje podataka, uništavanje podataka ili kriptovanje dokumenata i ucena (ransomware).

# Cyber kill chain – čemu ovo služi?



# Cyber kill chain - odbrana

1. Detekcija
2. Zabrana/sprečavanje pristupa
3. Ometanje, iskorenjivanje ili obmana
4. Oporavak

# Cyber kill chain - odbrana


## 1. Reconnaissance - izviđanje

**Detektovati da li napadač njuška oko nas i sprečiti takve aktivnosti!**

paloalto NETWORKS

Symantec + BLUE COAT

# Cyber kill chain - odbrana


## 2. Weaponization – naoružavanje

**Procena i testiranje ranjivosti, PEN testovi, configuration hardening, application remediation i izolacija.**

paloalto NETWORKS®

Symantec. + BLUE COAT®

# Cyber kill chain - odbrana


## 3. Delivery – isporuka

**Obuka korisnika, security analitika, network behavior analitika (IPS/IDS), threat intelligence, NGFW, WAF, DDoS, SSL inspekcija, enpoint zaštita, izolacija.**

paloalto NETWORKS®

Symantec. + BLUE COAT®

# Cyber kill chain - odbrana


## 4. Exploitation – esploatacija

Next gen. endpoint protection (na pr. SEP), SIEM, WAF, Advanced Threat Protection, EDR.

Symantec + BLUE COAT

# Cyber kill chain - odbrana


## 5. Installation – instalacija

**EPP (endpoint protection), endpoint forenzika – (SEP flight recorder – EDR 2.0), sandboxing, ATP.**

Symantec + BLUE COAT

# Cyber kill chain - odbrana


## 6. Command & Control – upravljanje i kontrola

Mrežna forenzika, SIEM, DNS security, proxy, DLP.

paloalto NETWORKS®

Symantec. + BLUE COAT®

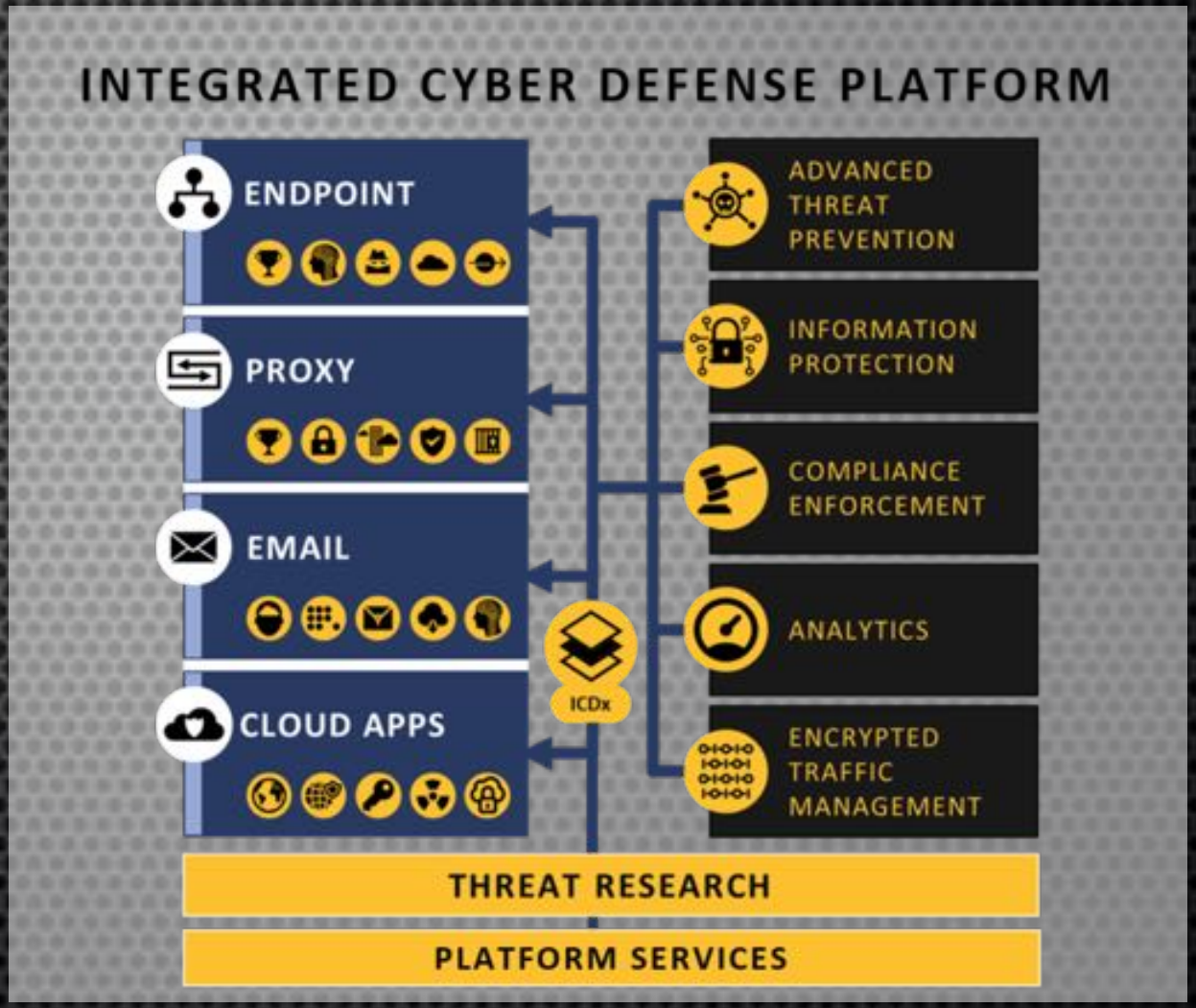
# Cyber kill chain - odbrana


## 7. Actions on Objectives – akcije nad ciljem

**Logging, SIEM, DLP, ATP, proxy, honeypot.**

# Cyber kill chain - odbrana

- Sistematična
- Na više nivoa
- Koordinisana
- Integrisana

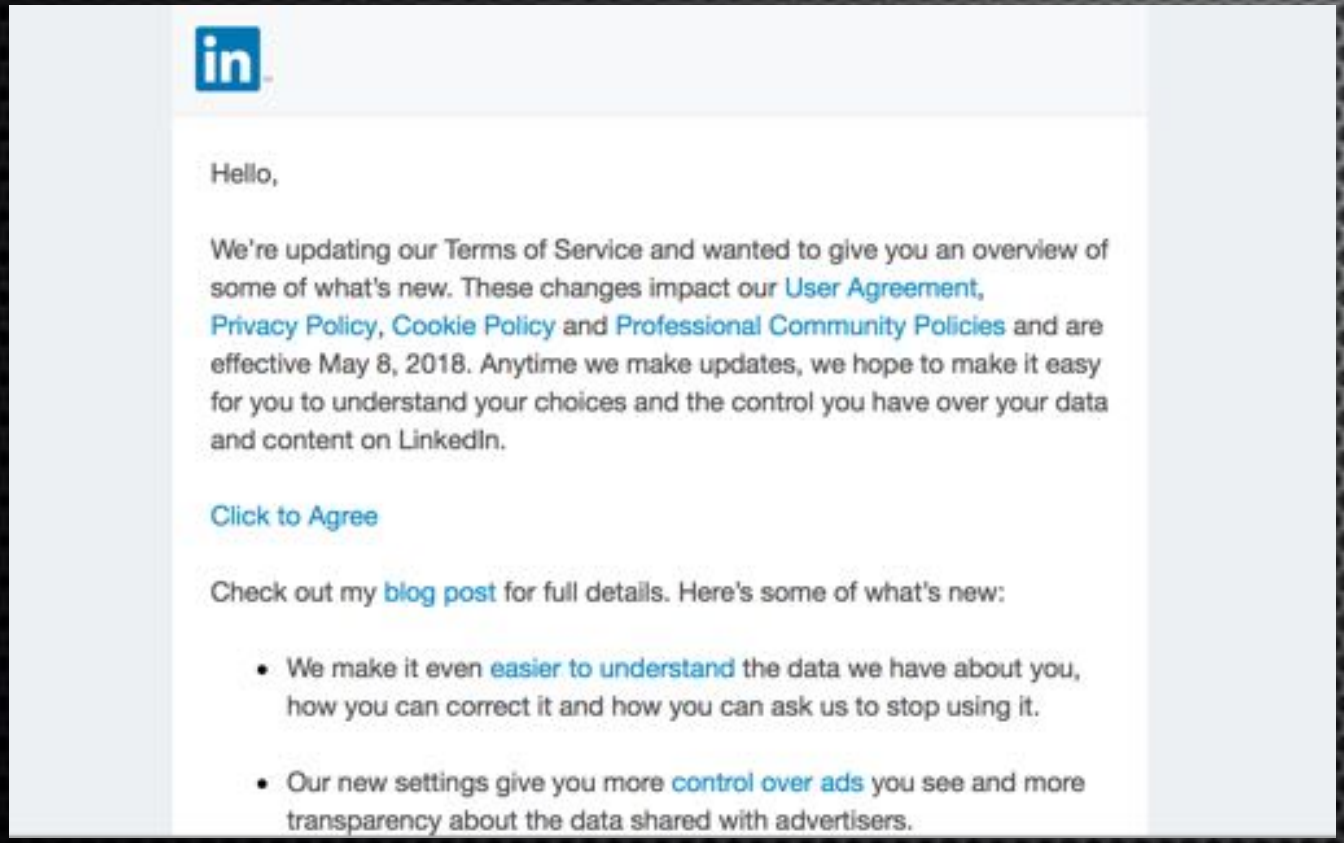


# Cyber kill chain

**Vladimir Vučinić**
**vladimir@netpp.rs**
**tel. (011) 36-999-67, mob. (063) 245-250**

# Cyber kill chain - primer

## Kako počinje napad...



Hello,

We're updating our Terms of Service and wanted to give you an overview of some of what's new. These changes impact our User Agreement, Privacy Policy, Cookie Policy and Professional Community Policies and are effective May 8, 2018. Anytime we make updates, we hope to make it easy for you to understand your choices and the control you have over your data and content on LinkedIn.

Click to Agree

Check out my blog post for full details. Here's some of what's new:

- We make it even easier to understand the data we have about you, how you can correct it and how you can ask us to stop using it.
- Our new settings give you more control over ads you see and more transparency about the data shared with advertisers.

**Emailovi (100%)**

**Potvrđeno otvorenih (27%)**

**Klikova (15%)**

**Gubitka kredencijala (5%)**