SECURITY 2013

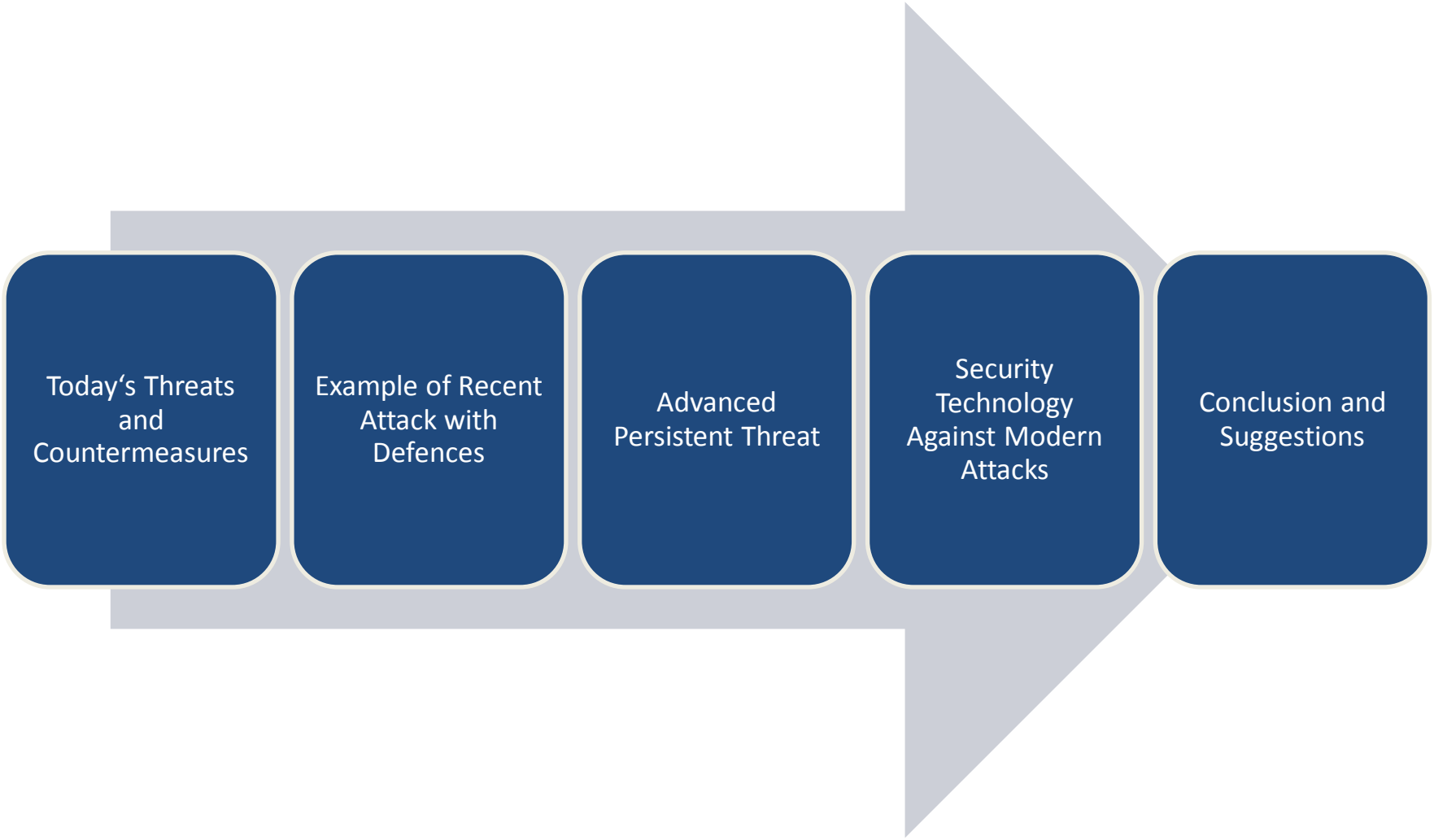
21. ročník konference o bezpečnosti v ICT

Advanced Forms of Attacks and Their Detection

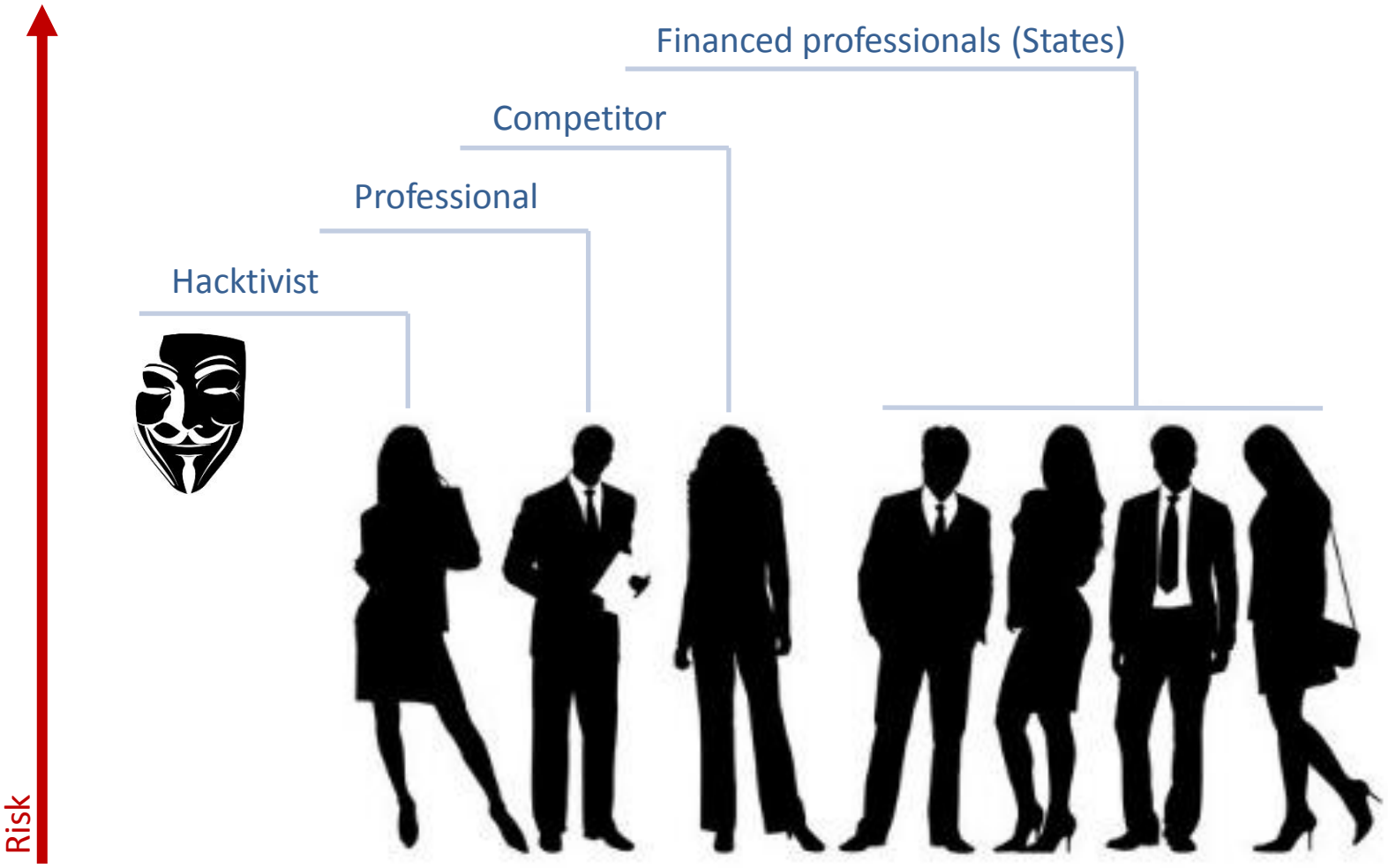
Maroš Barabas

AEC, spol. s r.o.

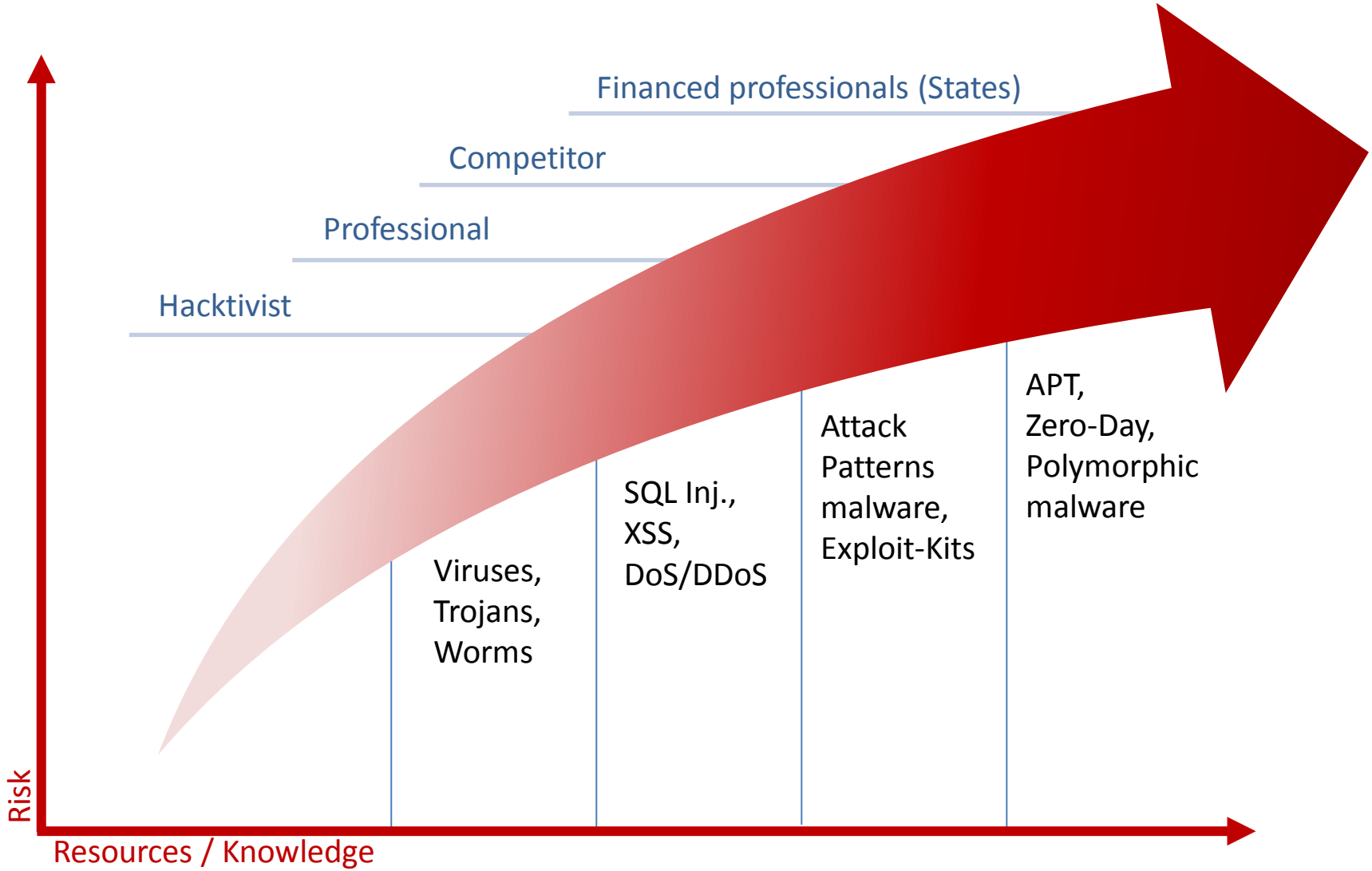
Agenda


Today‘s Threats and Countermeasures
Example of Recent Attack with Defences
Advanced Persistent Threat
Security Technology Against Modern Attacks
Conclusion and Suggestions

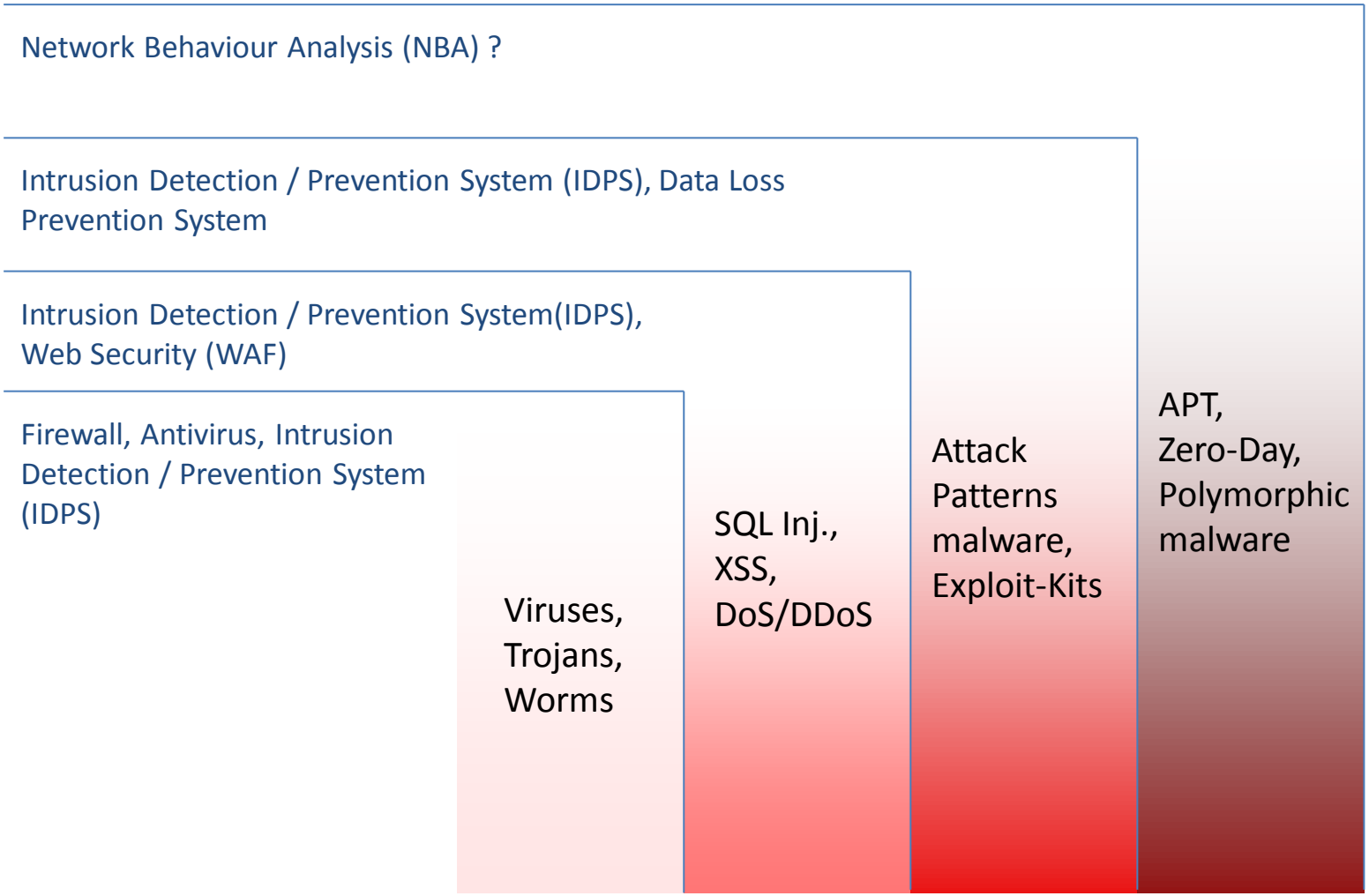
Threats


Financed professionals (States)
Competitor
Professional
Hacktivist
Risk

Threats and Resources



Attacks vs. Defence mechanisms



Today‘s Threats

Advanced Persistent Threat

[02.02.2013] *After **New York Times**, **Wall Street Journal** report suspected Chinese hacks on their systems, **The Washington Post** says its computers were hit too.*

[04.02.2013] ***The Department of Energy**[1] has just confirmed a recent cyber incident that occurred in mid-January which targeted the Headquarters' network and resulted in the unauthorized disclosure of employee and contractor Personally Identifiable Information.*

[05.02.2013] *The wave of high-level cyberattacks continues as the **Federal Reserve** confirmed that one of its internal Web sites was hacked into today, according to Reuters.*

[07.02.2013] *More recently, on 31 January 2013, **Amazon**’s homepage was briefly taken offline.*

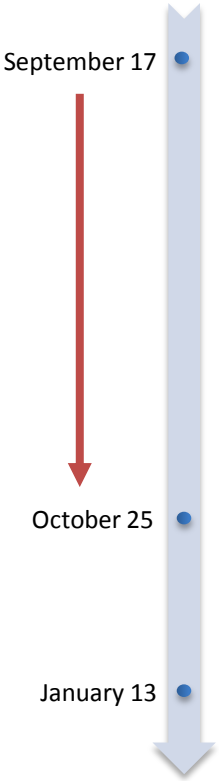
[19.02.2013] ***Apple** has identified malware which infected a limited number of Mac systems through a vulnerability in the Java plug-in for browsers. The malware was employed in an attack against Apple and other companies, and was spread through a website for software developers*

[1]The DOE/NNSA has federal responsibility for the design, testing and production of all nuclear weapons.

Attack Vector

[02.02.2013] *After **New York Times**, **Wall Street Journal** report suspected Chinese hacks on their systems, **The Washington Post** says its computers were hit too.*

New York Times Hack



1. Botnet compromised US Universities used to obscure source of attack.
2. 45 pieces of malware code gives attackers run of Times‘ network (likely spear phishing).
3. Windows network domain controller found.
4. User directory & password tables obtained.
5. Passwords cracked.
6. Systems accessed, custom program built, Times‘ email server breached, information stolen.
7. Suspicious activity over network detected.
8. Remediation.
9. General public informed of attack.

Attack Vector & Defences

[02.02.2013] *After **New York Times**, **Wall Street Journal** report suspected Chinese hacks on their systems, **The Washington Post** says its computers were hit too.*

New York Times Security Defences

1. **Traditional Anti-virus system** – *of the 45 pieces of malware that were used in the attack, **only one** was reportedly detected*

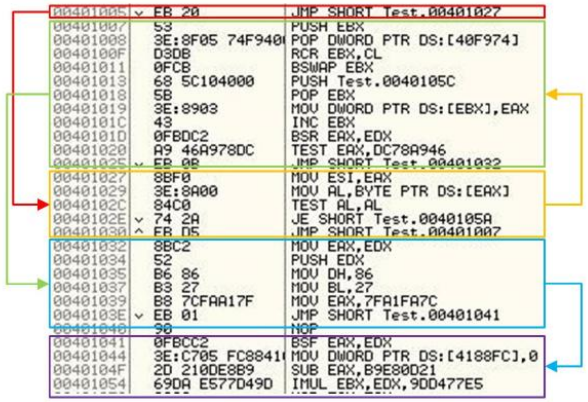
2. **Security solution to address suspicious activity** – *In this particular case, adversaries used valid credentials of New York Times' employees to pose as authenticated users and move beyond the perimeter to the internal network*

3. **Data Loss Prevention System** – *The Times attack not only involved the exfiltration of user logins and passwords, but also other information the attackers were stealing off of computer systems on the Times network*

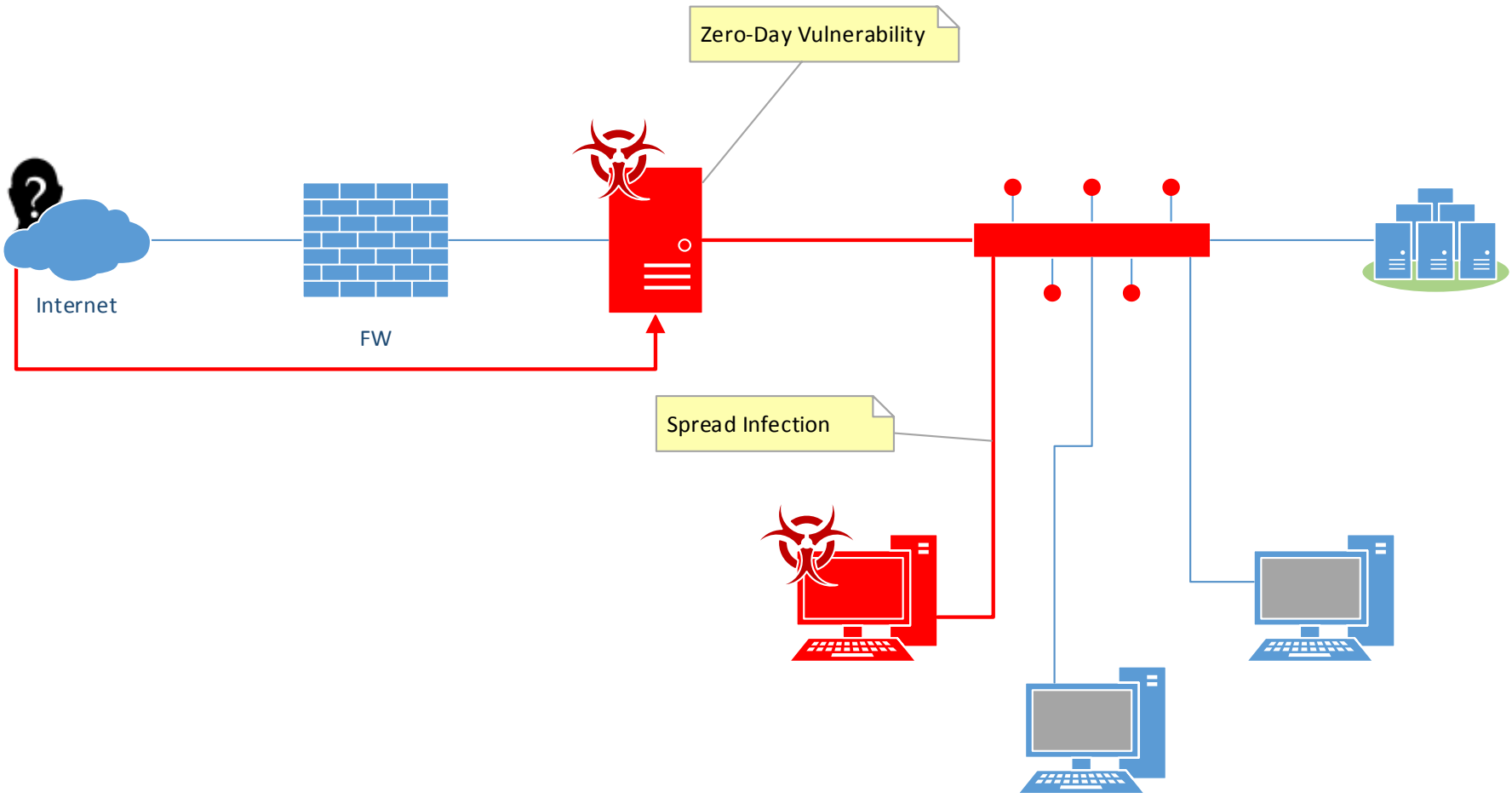
4. **Network Anomaly Detection** – *… it's unlikely that this traffic represented normal network traffic patterns at the Times.*

Advanced Persistent Threat

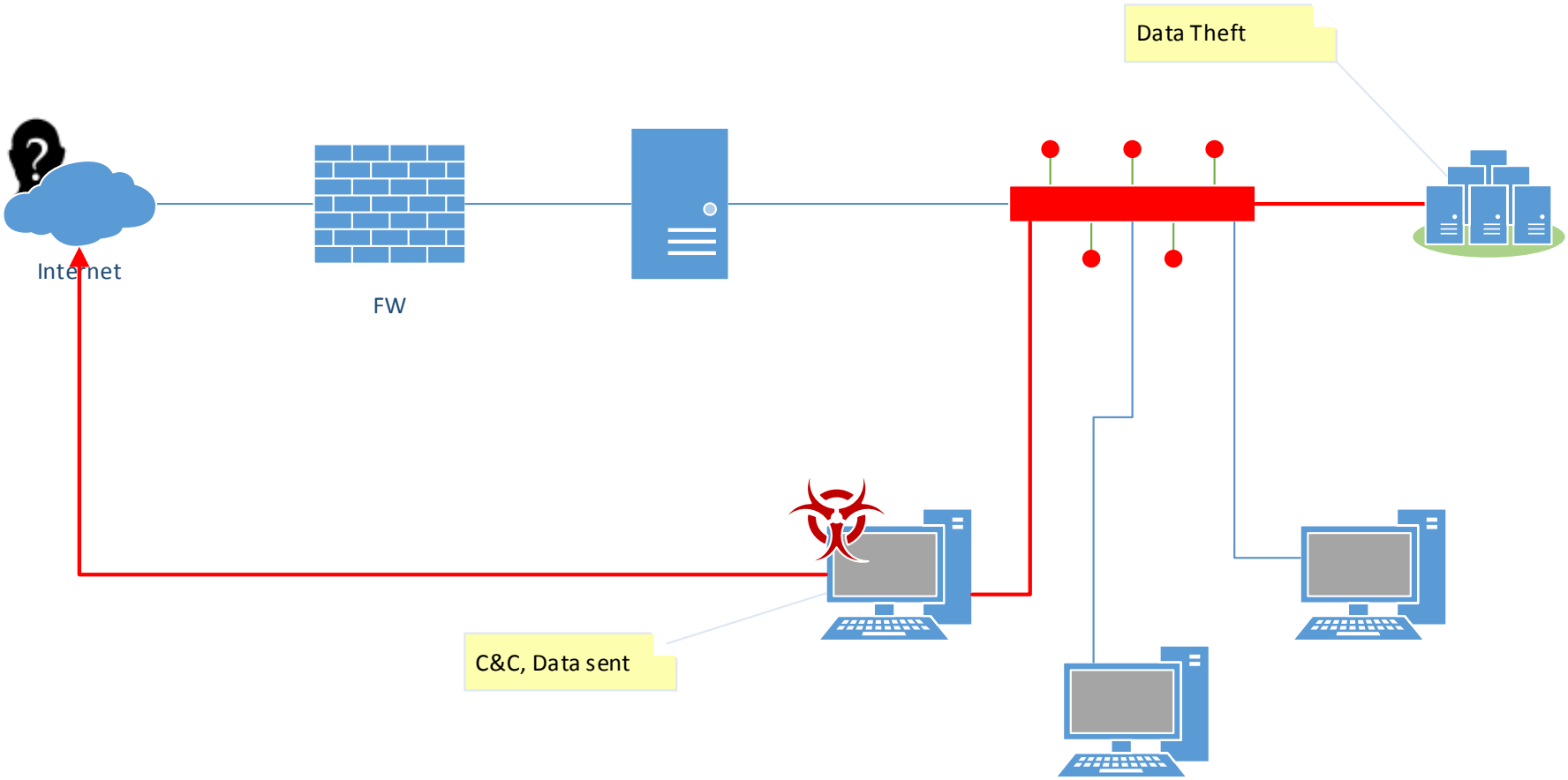
- Zero-Day Exploits
  - Exploit previously unknown vulnerabilities
  - Traditional security technologies such as Anti-virus, Intrusion Detection Systems, Firewalls etc. fail to detect.
- Remote Access Trojans
  - Trojan horses and generally malware used to remotely control infected computers
  - Capable of monitor user behavior, log user activity (key-loggers), distribute malware, infect other computers, etc.
  - A small part infecting target system can download additional modules on request
- Polymorphic / Metamorphic Malware
  - Various mutations, evading signatures
  - Metamorphic – matter of time?
- Other
  - DoS / DDoS Attacks
    - Attempt to make a service or resource unavailable
    - Wide area of possible attacks
  - Social engineering
    - (Spear) phishing



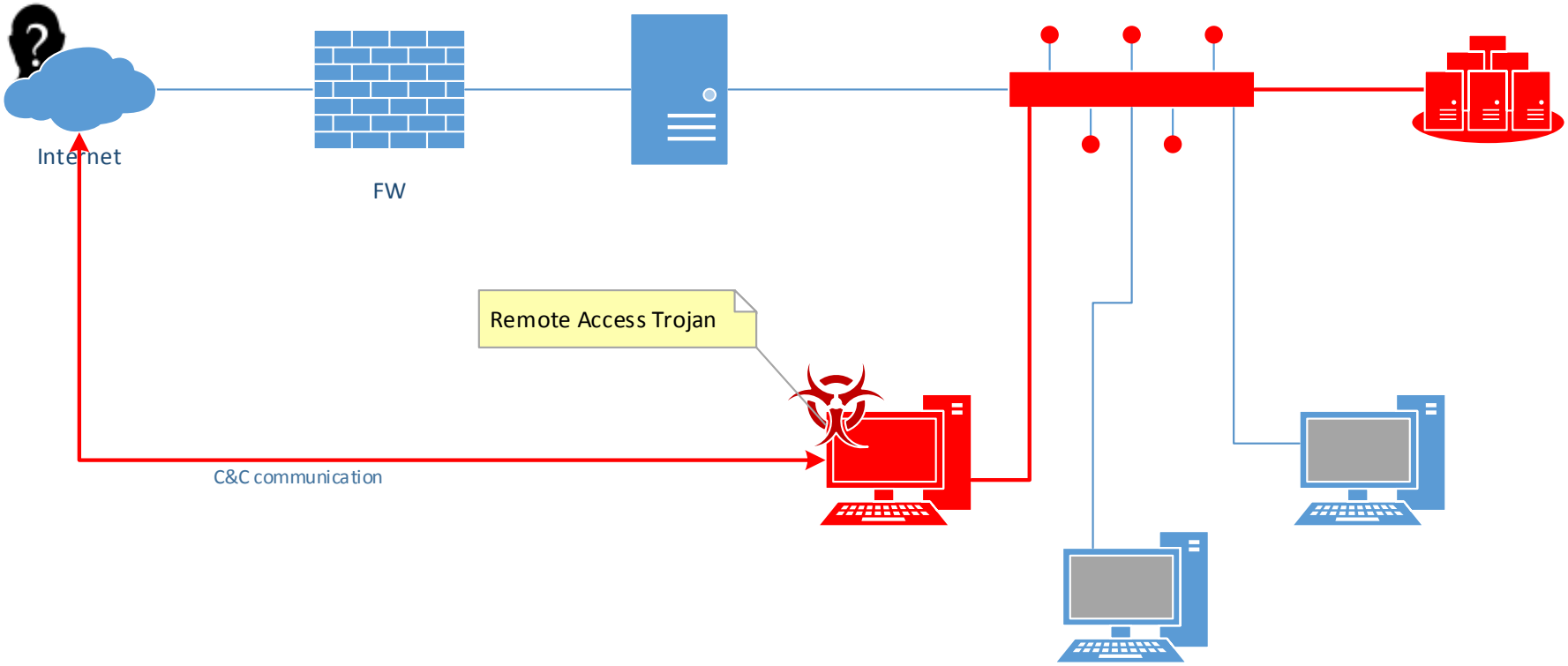
APT Schema



APT Schema



APT Schema



Traditional Detection

- Firewall
  - Can be easily avoided by using common protocols such HTTP, HTTPS or DNS.
  - Next generation
    - User authentication
    - Deep Packet Inspection (shall we?)

- Anti-virus
  - Heavily signature-based with anomaly detection
  - Can‘t protect against zero-day exploits
  - Should protect against malware, but 1 of 45??
  - Statistic vs. Dynamic analysis
  - Transparent *micro-virtualization* of untrustworthy tasks

Advanced Detection

Intrusion Detection/Prevention Systems - IDPS

- Signature-based = no zero-day prevention
  - Easy to evade
- Doesn't address suspicious activity, user behavior
- New generation
  - User management - user behavior, controlling access to applications
  - Including Firewall, Application Control, DLP, Antivirus

GET /stun.png HTTP/1.1
Host: victim.com
Range: bytes=0-,2-10,2-11,2-12,2-13,2-14,2-15,… (0- means 0 to EOF)

Content:"Range:bytes=**0**-";
threshold:type threshold, track by_src,
count 5, seconds 20;

GET /stun.png HTTP/1.1
Host: victim.com
Range: bytes=**1**-,0-,2-10,2-11,2-12,2-13,2-14…

Signature: content:"Range|3a|"; nocase; http_header;
content:"bytes="; http_header; nocase; distance:0;
isdataat:10,relative; content:","; http_header; within:11;
isdataat:10,relative; content:","; http_header; within:11;
isdataat:10,relative; content:","; http_header; within:11;
isdataat:70,relative; content:!"|0d 0a|"; within:12;
pcre:"/Range\x3a\s?bytes=[-0-9,\x20]{100,}/iH";

Advanced Detection

Network Behavioral Anomaly Detection System – NBA

NBA Detection Systems are capable of detecting advanced persistent threats, sophisticated malware, information exfiltration, hidden channels, trojans, C&C communication and anomalous user activity.

- Based on network flow analysis to avoid signatures
- Focused on description of users' behavior

- Based on statistical analysis – statistic model of subject behaviour within network traffic.
- Based on Artificial Intelligence:
  - Basic approach – using AI for classification of malicious/benign flows, searching for known typical anomalies
  - Advanced AI – classification all flows together with minimalizing false positivies based on various approaches (reputation systems, agent systems, ..)

Advanced Detection

Network Behavioral Anomaly Detection System – NBA

+ Detection of APT, RAT, C&C
+ Presence of Artificial Intelligence engine (self-adaptation)
+ Independent from signature based detection techniques
+ Ability to detect low-profiled malware
+ Usually supports integration with SIEM
+ Added value of behaviour analysis of entire network
+ Easy deployment (requires only NetFlow probe)
+ DNS, Geoloc.
+ Bad configuration, network optimization

- Human analysts with regular inspections necessary
- Adding delay between infection and detection -> can‘t be used for automated prevention
- Higher false-positive ratio
- Could be potentially avoided by hiding malicious activity to a regular behaviour

Advanced Detection

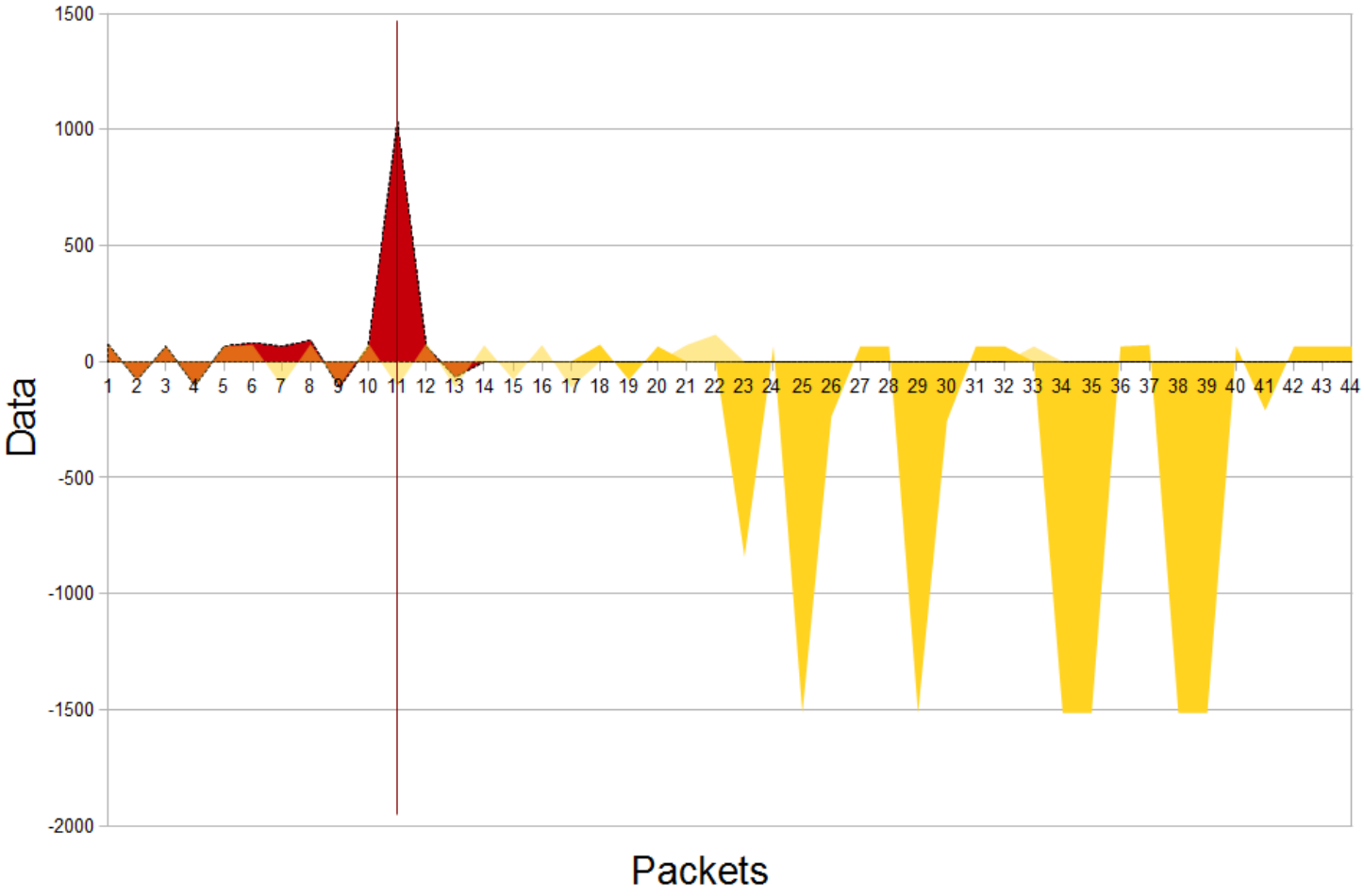
Automated Intrusion Prevention System – AIPS

Automated Intrusion Prevention System technology is designed to automatically detect and stop advanced and unknown attacks. It uses around 170 metrics extracted from network traffic to higher the describtion capability of malicious activity in the network.

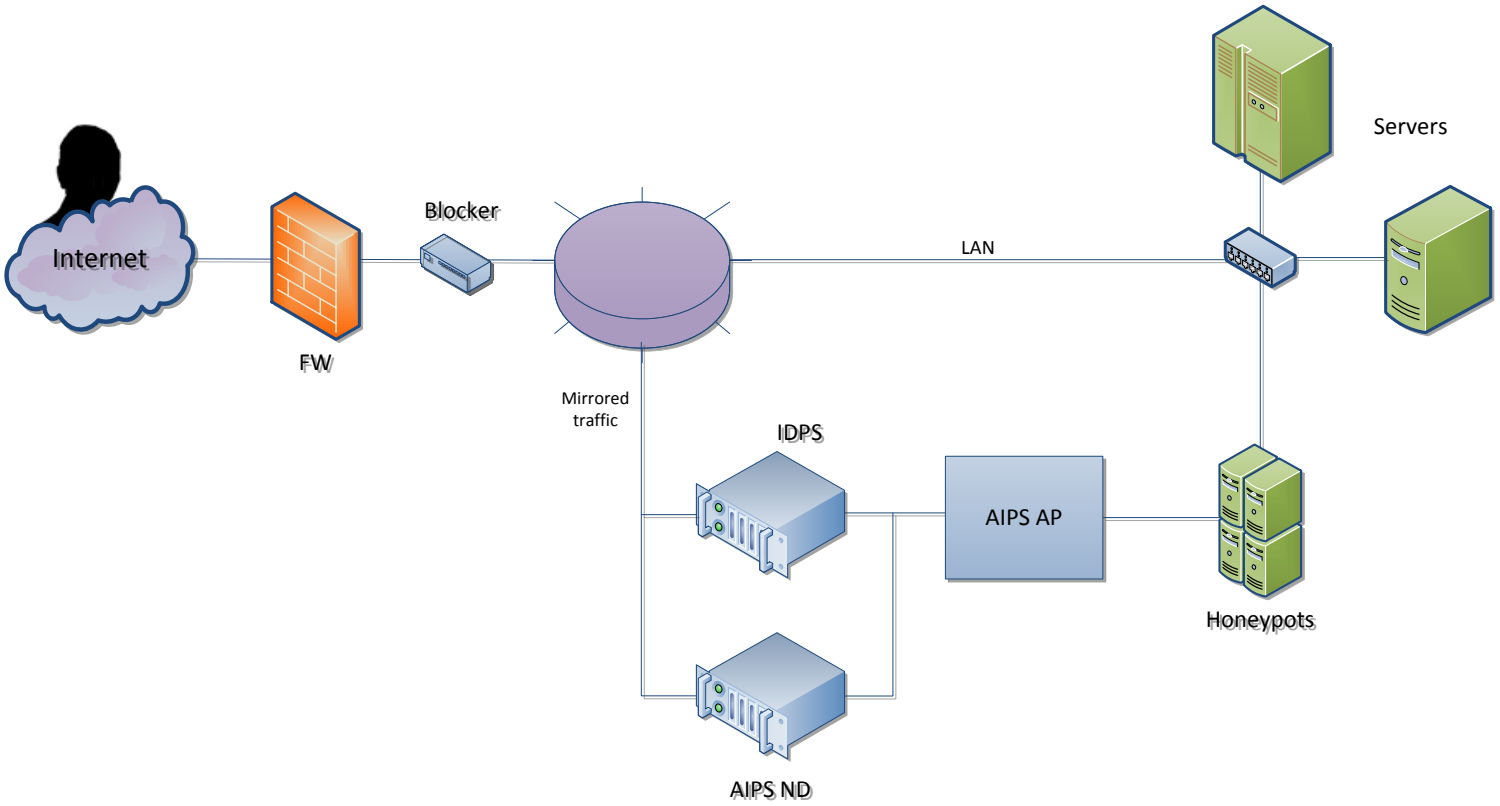
+ Detection of APT, Zero-Day buffer-overflow exploits, (D)DoS, RAT
+ Presence of Artificial Intelligence engine (self-adaptation)
+ Independent from signature based detection techniques
+ Using Advanced Security Network Metrics (ASNM) to create unique behavioral representation
+ Adoption of Honeypots‘ expert knowledge for zero-day attacks detection
+ No Human intervention is required

- Not yet ready for deployment (University research, under heavy development)

AIPS - Detection



AIPS - Deployment



Conclusion

BRUSSELS - *Large EU-based companies will have to disclose major cyber-attacks to designated national authorities, under new legislative rules proposed by the European Commission on Thursday* (7th February)

- Threat management – real-time monitoring, reporting and early responding. Monitoring of user activity, correlate network flow, log-event and vulnerability data to early breach detection
- Forensics and mitigation plan
- To think about security:
  - Address suspicious activity on your network – use NBA, AIPS and similar systems
  - Deploy Anti-viruses, Firewalls, Data Loss Prevention systems
- Security as Service

- **No ultimate weapon against APT**

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

"We shouldn't wait until there is a 9/11 in the cyber world,"

US Homeland Security Secretary, Janet Napolitano

Thank you.

Maroš Barabas

AEC, spol. s r.o.

maros.barabas@aec.cz