SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Network Behavior Analysis
One Step Ahead of the Attackers

Michal Pechoucek and **Martin Rehak**,
Cognitive Security s.r.o.

Inside a modern NBA system…

…using advanced AI technologies to achieve high sensitivity, low error rate, high robustness and secure self-operation in distributed network intrusion detection


603
NAVY
603

Motivation

- **NASDAQ**: “Hackers have repeatedly penetrated the computer network of the company that runs the Nasdaq Stock Market during the past year, and federal investigators are trying to identify the perpetrators and their purpose […] range of possible motives, including unlawful financial gain, theft of trade secrets and a national-security threat designed to damage the exchange” WSJ, Feb 5, 2011

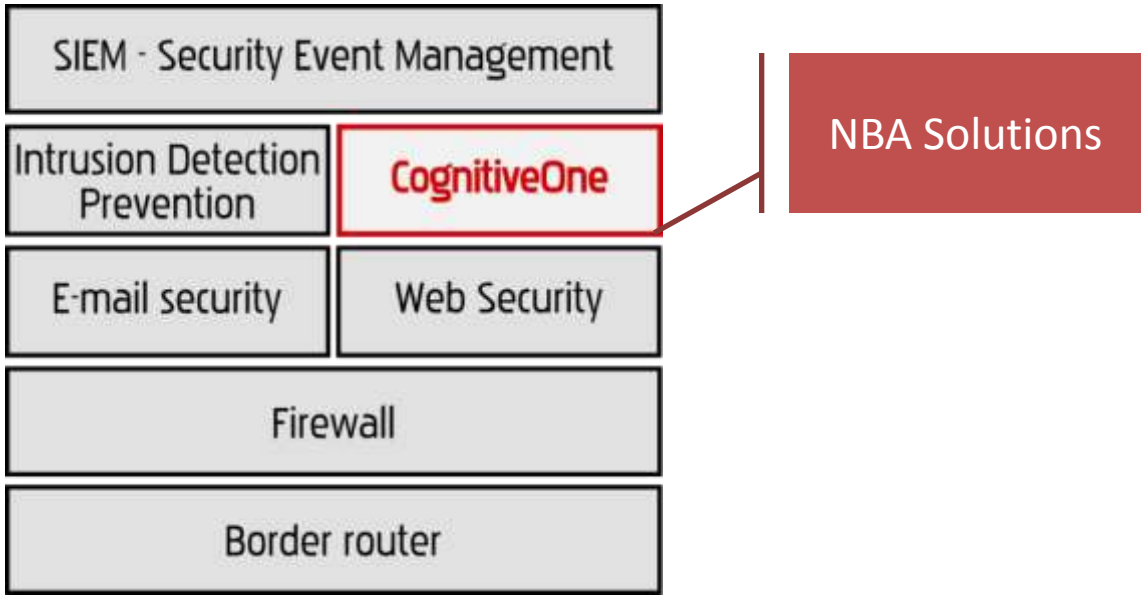
Motivation

- **OTE**: “Způsob provedení a rychlost problematických transakcí přes jednotlivé účty ukazují na promyšlené jednání, při kterém část převodů byla realizována přes účty různých evropských rejstříků během několika minut”
  ceskapozice.cz, Leden 2011

Threats

- Strategic, persistent approach to computer crime
  - *Previously government-level techniques in common use*
- Technological progress
  - Attackers getting increasingly **sophisticated**
  - **Custom-written** (customized) **attacks** are becoming a norm
- Conceptual progress
  - Old threats were IT oriented
  - New threats are **business-specific**
  - Non-trivial attack scenarios using financial markets (derivatives)
  - Difficult risk management/defense
- New targets: infrastructure, embedded control, automation, trading systems (with derivatives), ERP, CRM,…

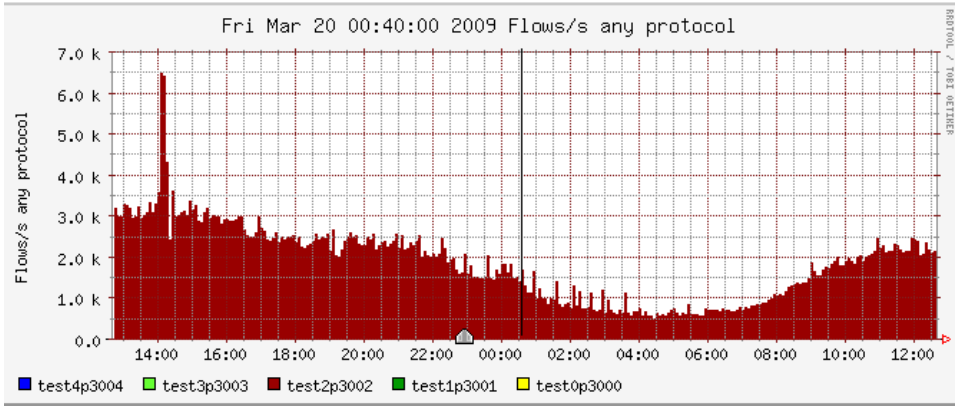
Positioning



Network Behavior Analysis

- Processes **NetFlow** data
  - **no content**
  - source, destination IP address/port + protocol
  - bytes, packets, (flows)
  - flags (TCP)
  - Aggregation 1-15 min. interval (typ. 5 min.)
  - widely available, quality varies, IETF standard

- Anomaly detection methods
- Broad decision rules
- Statistical traffic prediction and analysis



Anomaly Detection vs. Signatures

Signature matching

- Historically validated
- Widely deployed
- Verifiable & Stable
- Number of patterns
- Scaling
- Management
- New threats detection

Anomaly detection

- No patterns
- New threats detection
- Scaling
- **Error Rate/Sensitivity**
- **Verifiability**
- **Stability**
- **Management**

Why NBA ? Features ?

- *Near-instant detection of **simple problems** vs.*
- *Reliable long-term detection of **persistent advanced threats***

- **Large, Open Networks**
  - Infrastructure targets
  - Extrusion control
  - Traditional threats
  - Policy enforcement
- **Enterprise Networks**
  - Critical business processes
  - Customized attacks
  - Strategic attackers
  - Insider access

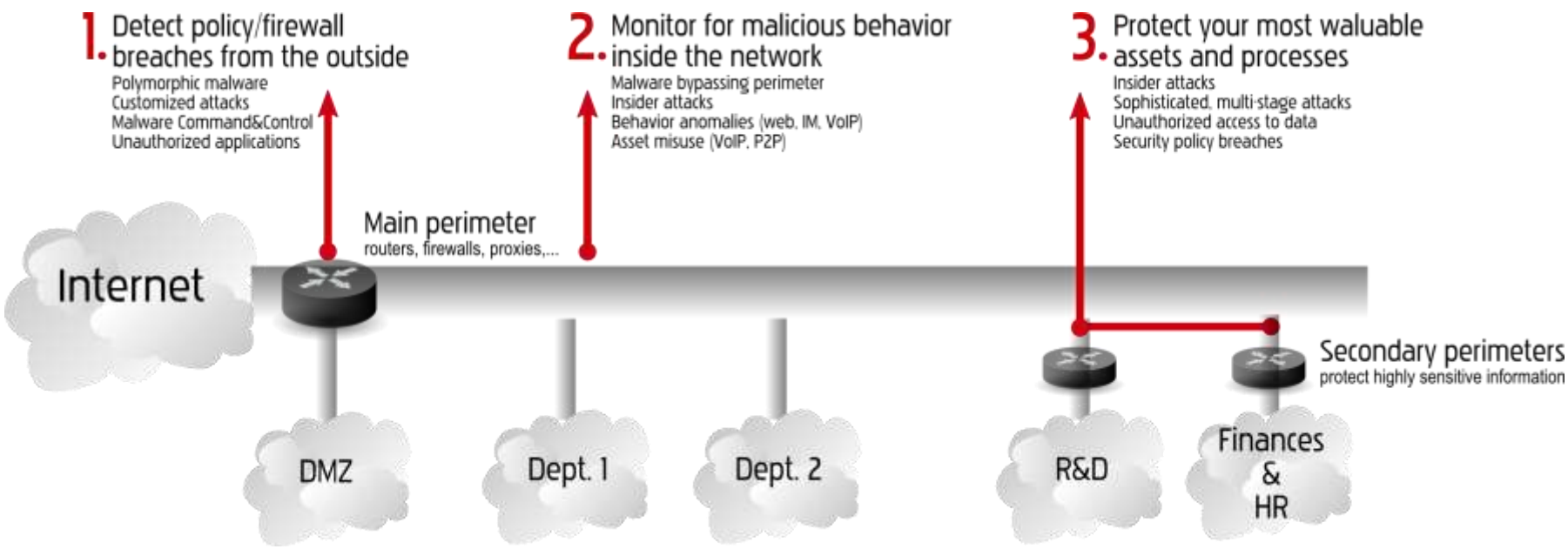
Why NBA ? Features ?

- *Near-instant detection of **simple problems** vs.*
- *Reliable long-term detection of **persistent advanced threats***

- **Large, Open Networks**
  - Infrastructure targets
  - Extrusion control
  - Traditional threats
  - Policy enforcement
- **Enterprise Networks**
  - Critical business processes
  - Customized attacks
  - Strategic attackers
  - Insider access

- *NBA regains the **initiative** if it provides:*
  - *Multiple detection algorithms (low false alerts, better detection)*
  - *Published, peer-reviewed algorithms (long-term effectiveness)*
  - *Strategically randomized detection (against strategic attackers)*
  - *Dynamic strategic adaptation (low management costs)*

NBA Deployment



Inside Modern NBA System

Stage 1

- **Anomaly Detection:** **Predicting current network behavior from the history and looking for deviations**

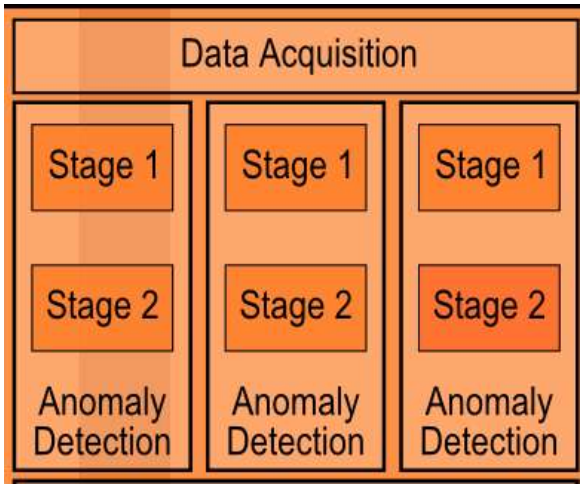
Inside Modern NBA System

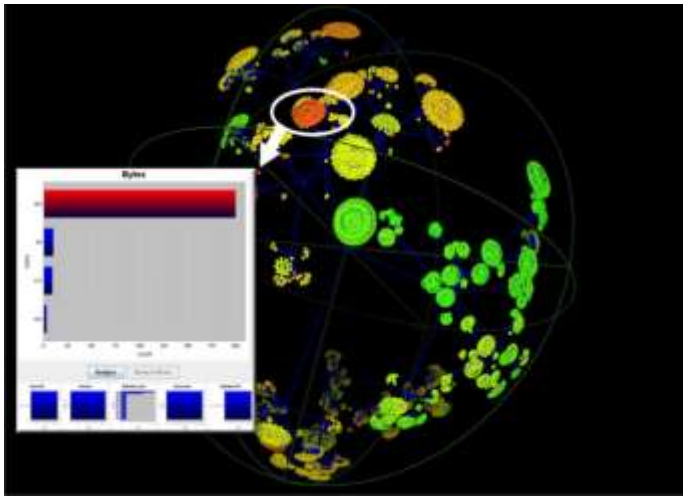
- **Multi-Algorithm Anomaly Detection:**
- **Entropy modeling**
- **Trend modeling**
- **Volume modeling**
- **Principal components analysis**
- **Information-theoretical measures**
- **…**

Anomaly Detection (Selection)

Method/Attack	Malware Brute force	Horizontal scanning	Vertical Sc. Fingerprint.	DoS/DDoS Flooding/Spoof.
MINDS	***	****	****	***
Xu	**	****	***	***
Xu-dst IP	*	*	**	*****
Lakhina - Volume	**	***	***	****
Lakhina - Entropy	***	****	**	***
TAPS	***	*****	*****	**

Inside Modern NBA System





- **Trust Modeling:** **Synthesizing the Anomaly detection data across the algorithms and over time**

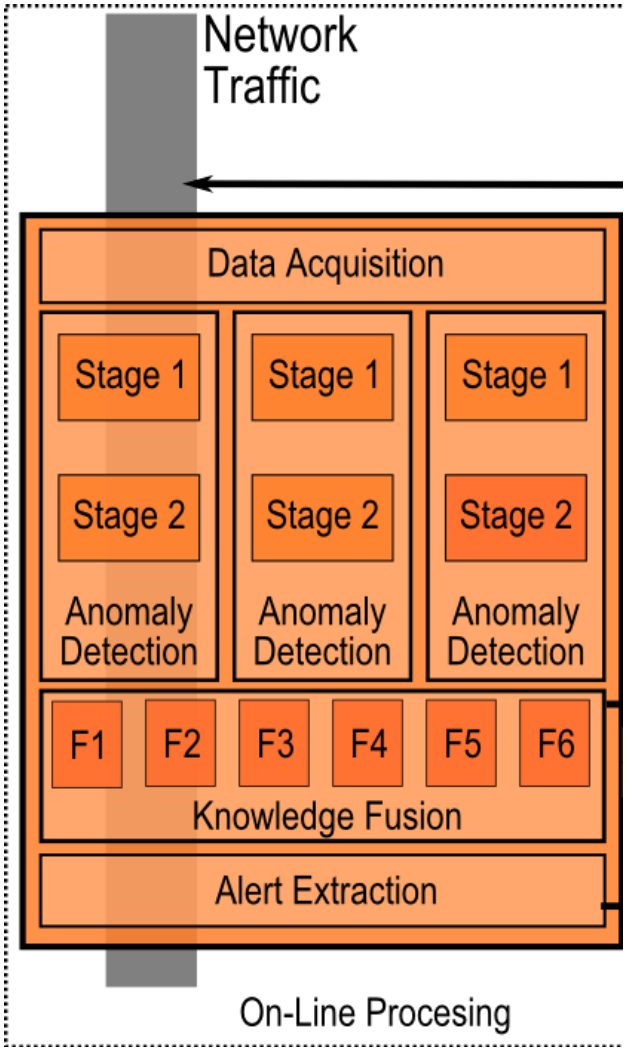
Identity and Context Example

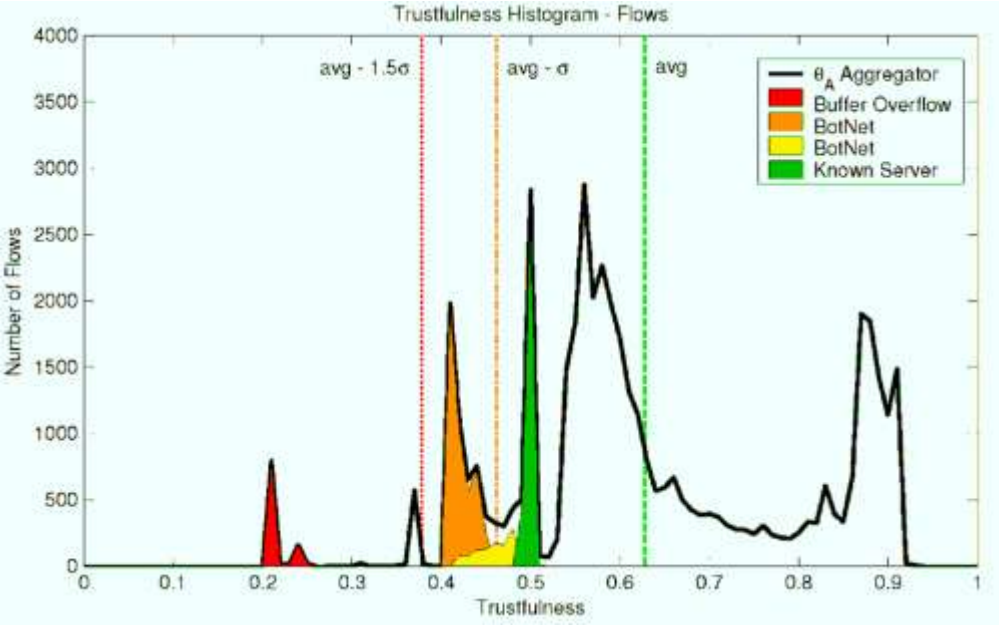
Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2009-03-20 01:11:12.923	364.932	TCP	147.251.198.84:2430	->	78.154.195.124:47575	8699	8.1 M	104
2009-03-20 01:12:38.215	276.256	UDP	92.240.244.30:27022	->	147.251.211.107:27005	19266	4.1 M	72
2009-03-20 01:11:51.690	308.352	TCP	62.67.50.133:80	->	147.251.68.5:3671	41696	53.3 M	55
2009-03-20 01:12:18.467	292.902	TCP	91.66.122.66:53858	->	147.251.215.168:23314	18189	1035699	51
2009-03-20 01:12:01.886	337.372	TCP	64.15.156.212:8000	->	147.251.146.27:1150	2028	2.0 M	47
2009-03-20 01:16:56.525	28.134	TCP	147.251.215.235:2517	->	213.134.25.222:27192	343	269375	45
2009-03-20 01:12:39.400	299.943	UDP	147.175.185.54:1693	->	147.251.206.207:29359	18214	2.4 M	44
2009-03-20 01:15:42.653	15.283	TCP	77.75.73.48:25	->	147.251.4.40:40166	186	16009	43
2009-03-20 01:13:46.343	213.639	TCP	147.251.210.122:55628	->	66.55.141.34:80	3864	155898	43
2009-03-20 01:08:00.699	578.690	TCP	147.251.211.172:64037	->	217.162.223.125:14817	4900	215352	41

- **Identity**
  - srcIP = 147.251.198.84
  - dstIP = 78.154.195.124
  - srcPrt = 2430
  - dstPrt = 47575
  - proto = TCP
  - packets = 8699
  - bytes = 8 ,100,000

- **Context (Xu)**
  - H(dstIP)= 0.2
  - H(srcPrt)= 0.3
  - H(dstPrt)= 0.3

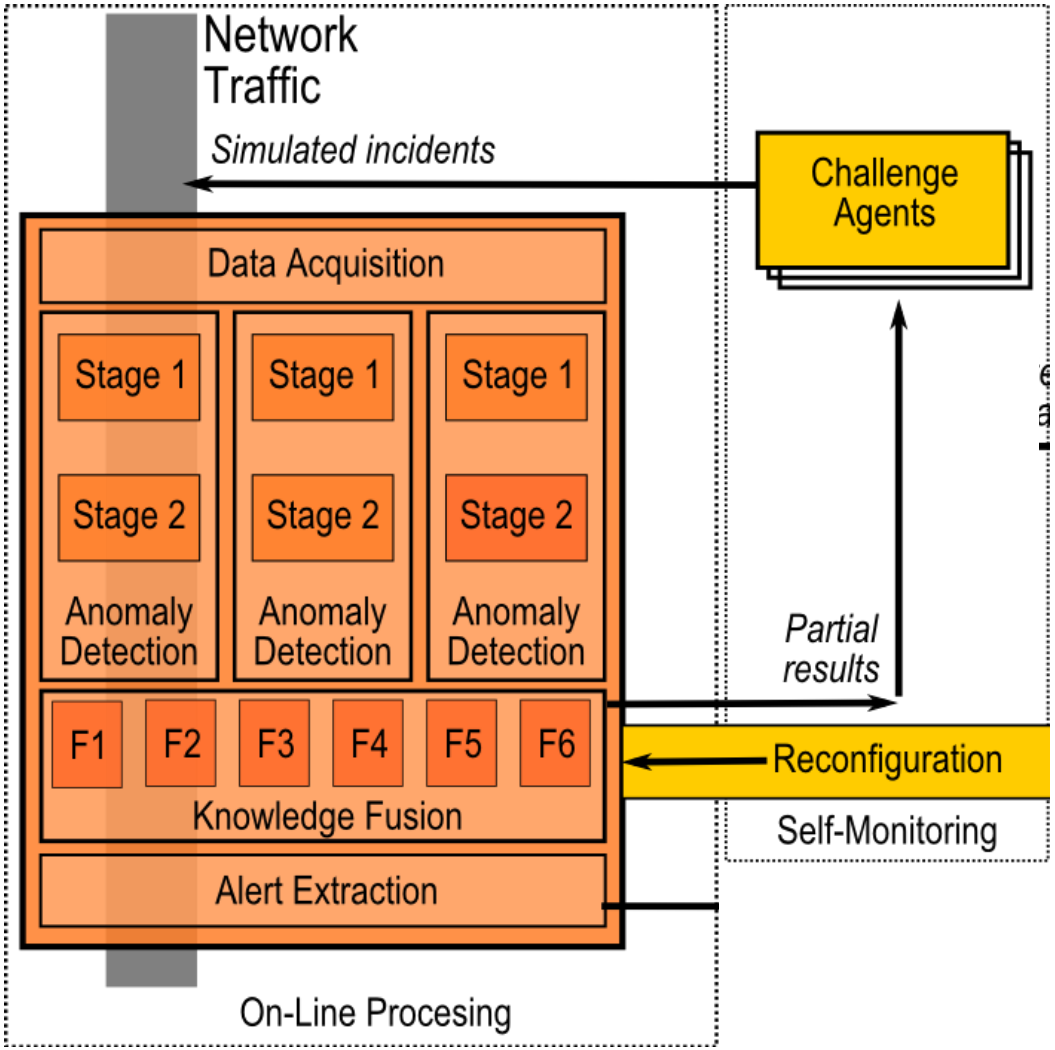
Inside Modern NBA System





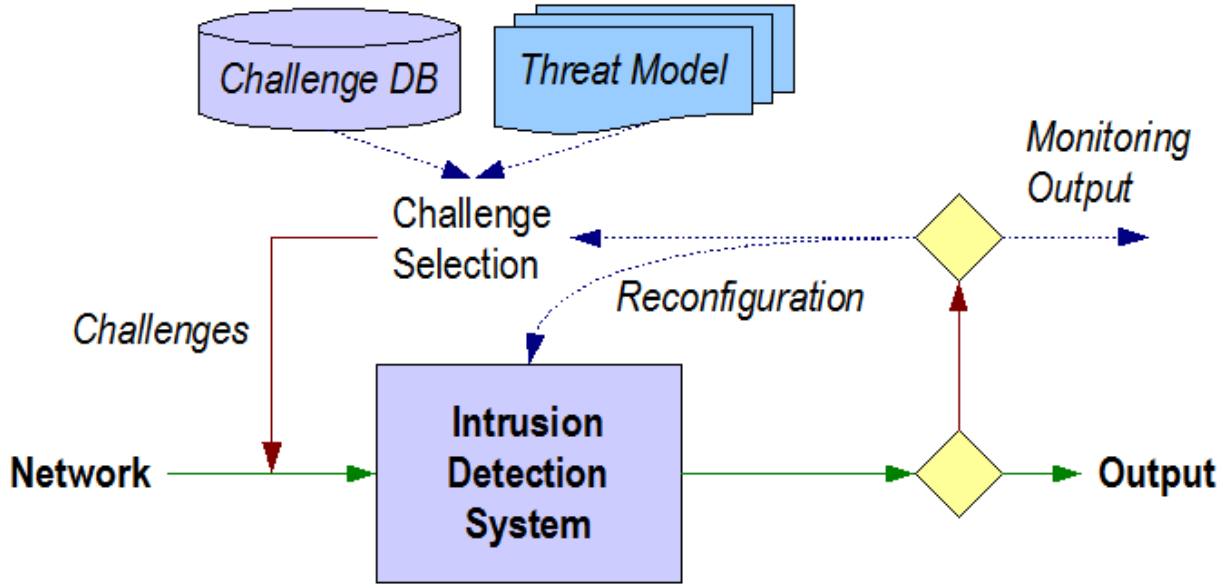
– **Event Extraction:** **Converts the statistics into actionable output**

Inside Modern NBA System



- **Self-Monitoring:** **Real-time assessment of system effectiveness in unknown environment**

Monitoring: Challenge Insertion



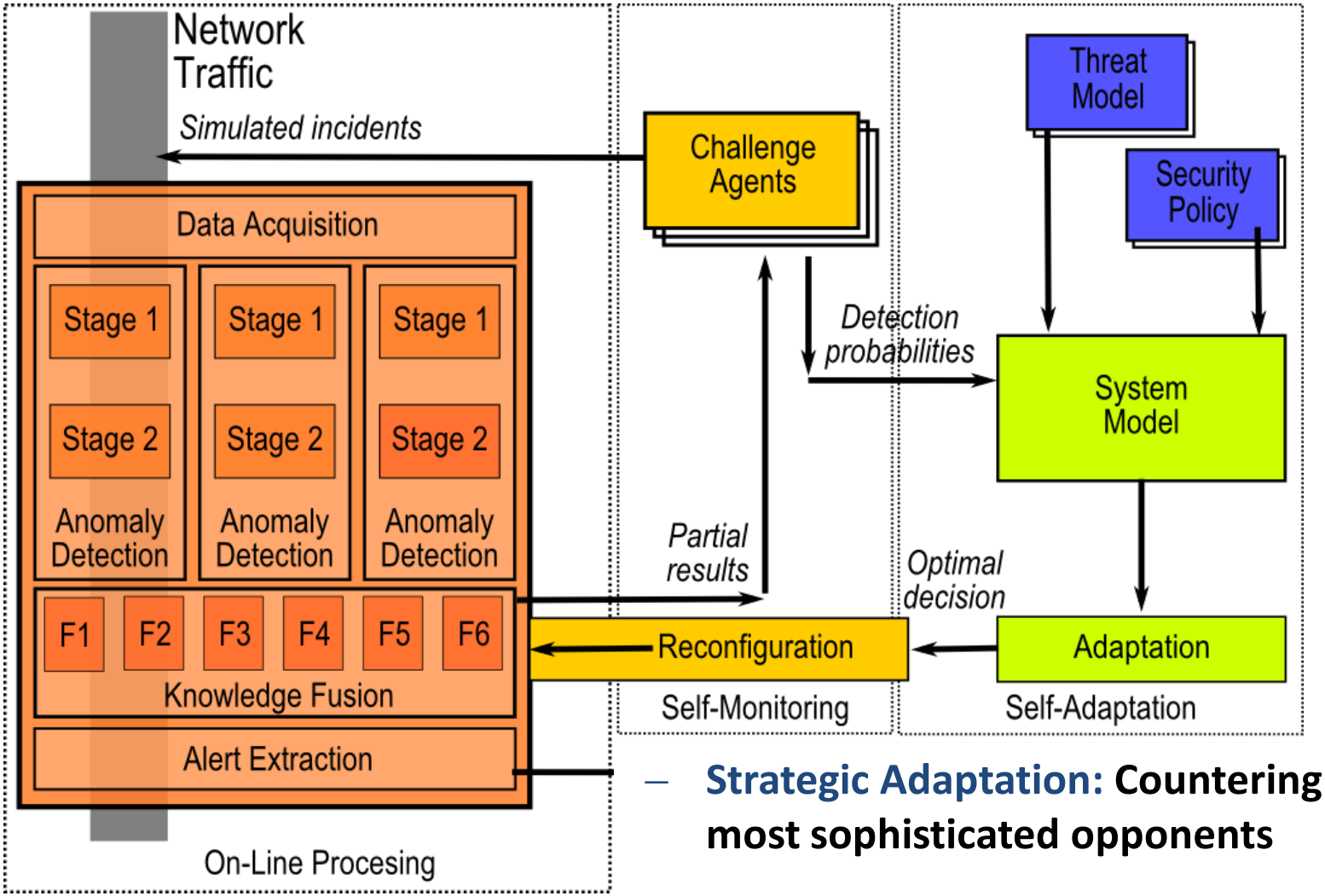
- Unlabeled background input data
- Insertion of small set of challenges
  - Legitimate vs Malicious

(1) Response evaluation

(2) What challenges ?

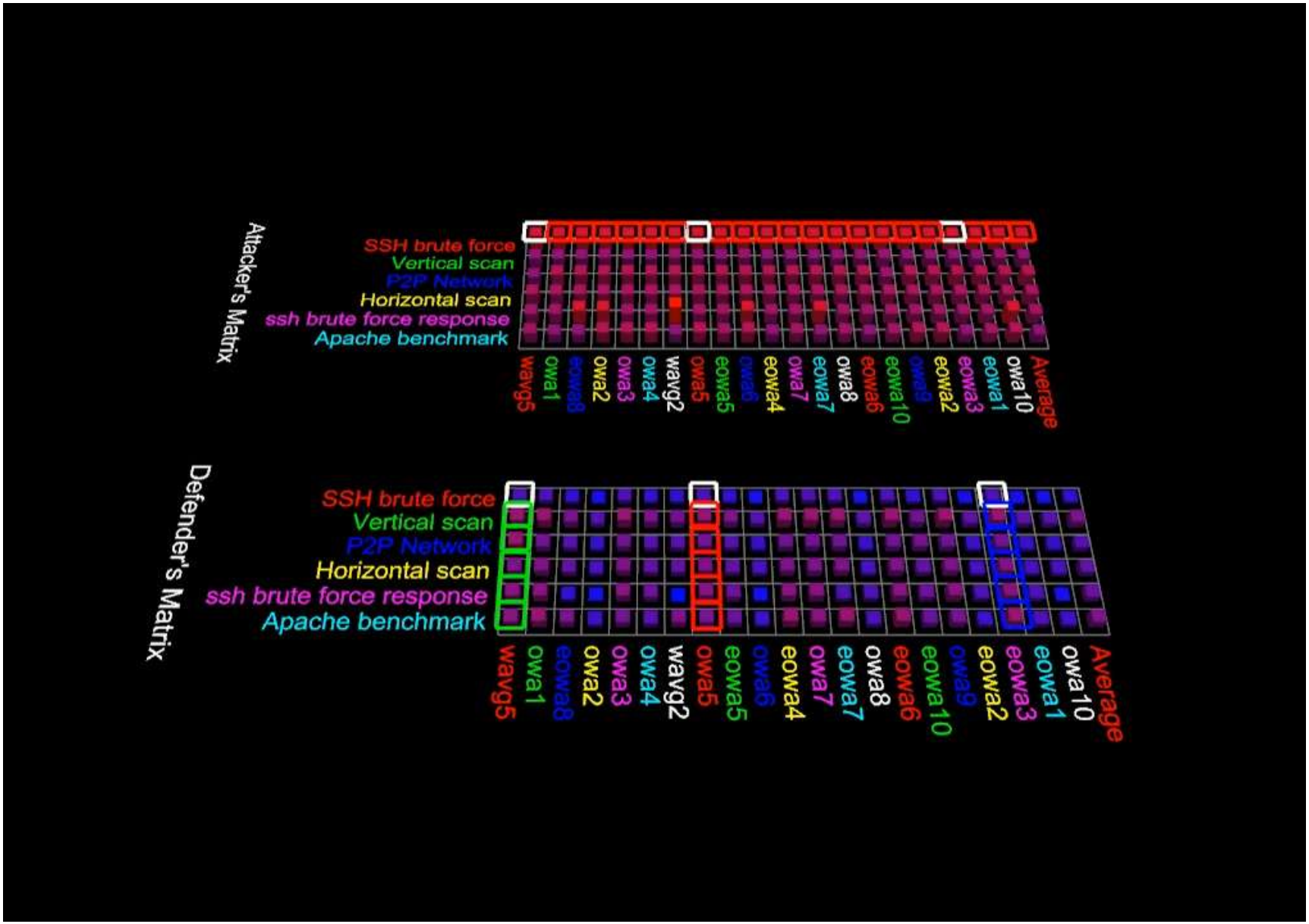
(3) How many ?

Inside Modern NBA System

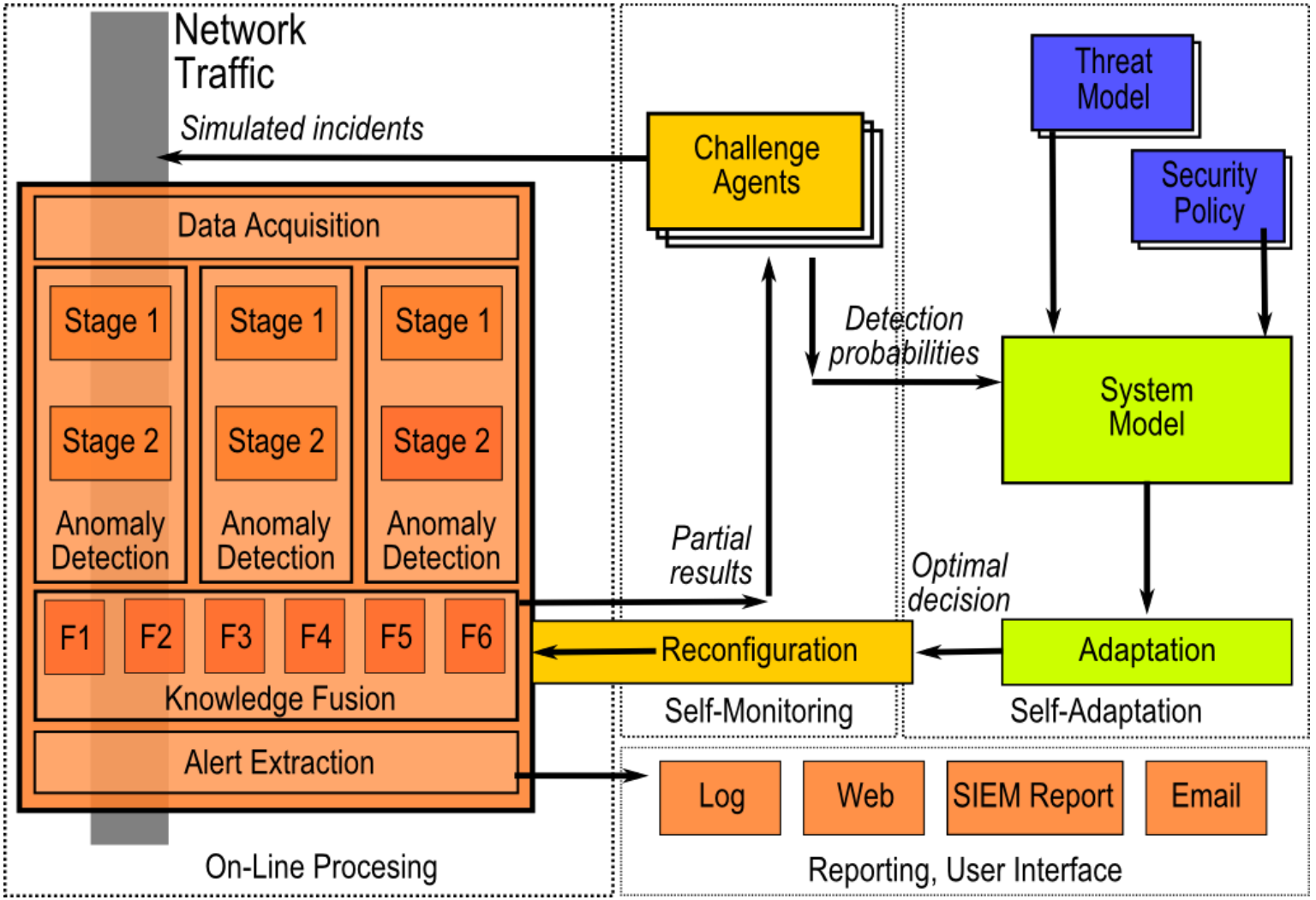


- **Strategic Adaptation:** **Countering the most sophisticated opponents**

Game-Theoretic Security

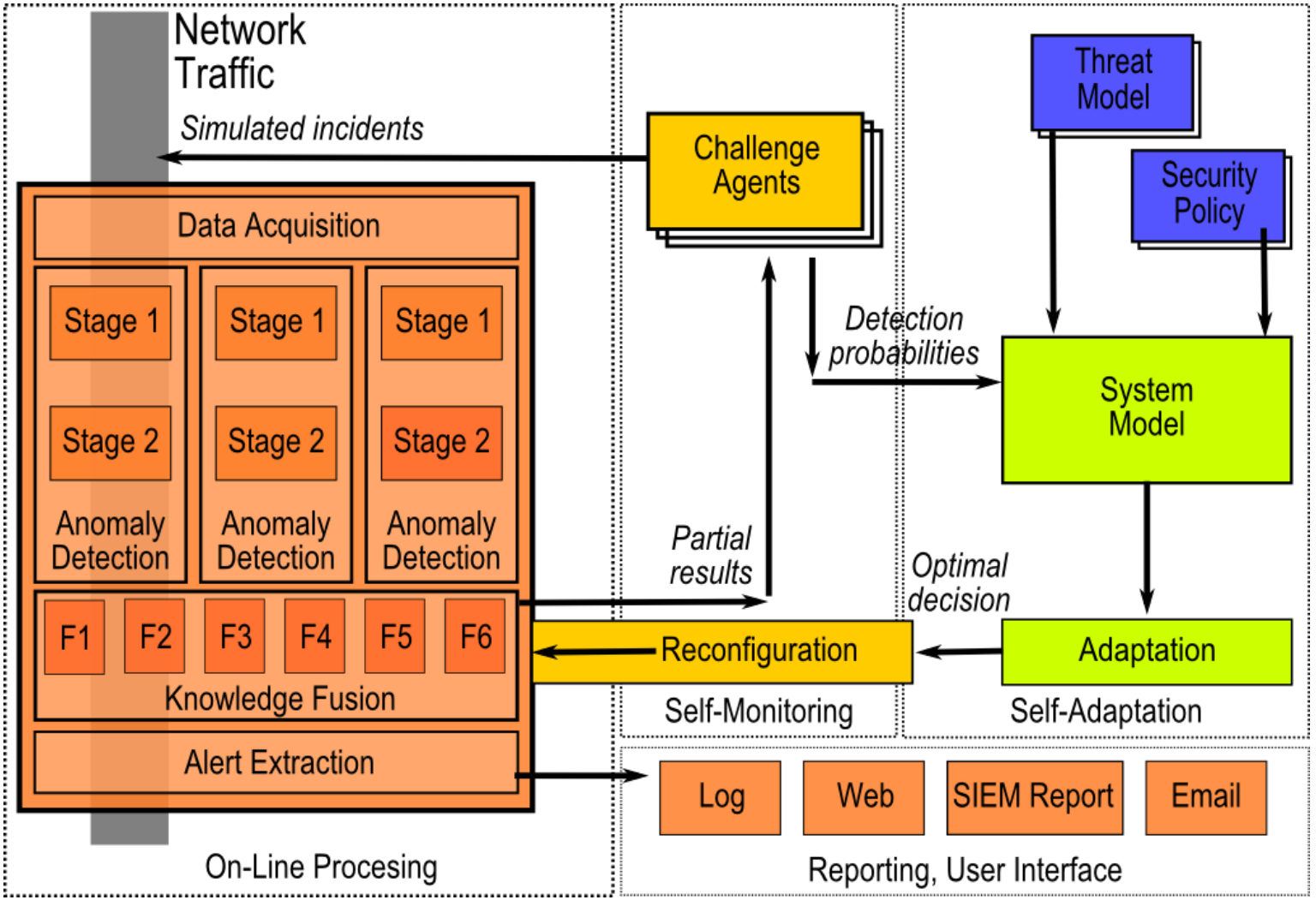


Inside Modern NBA System



Inside Modern NBA System

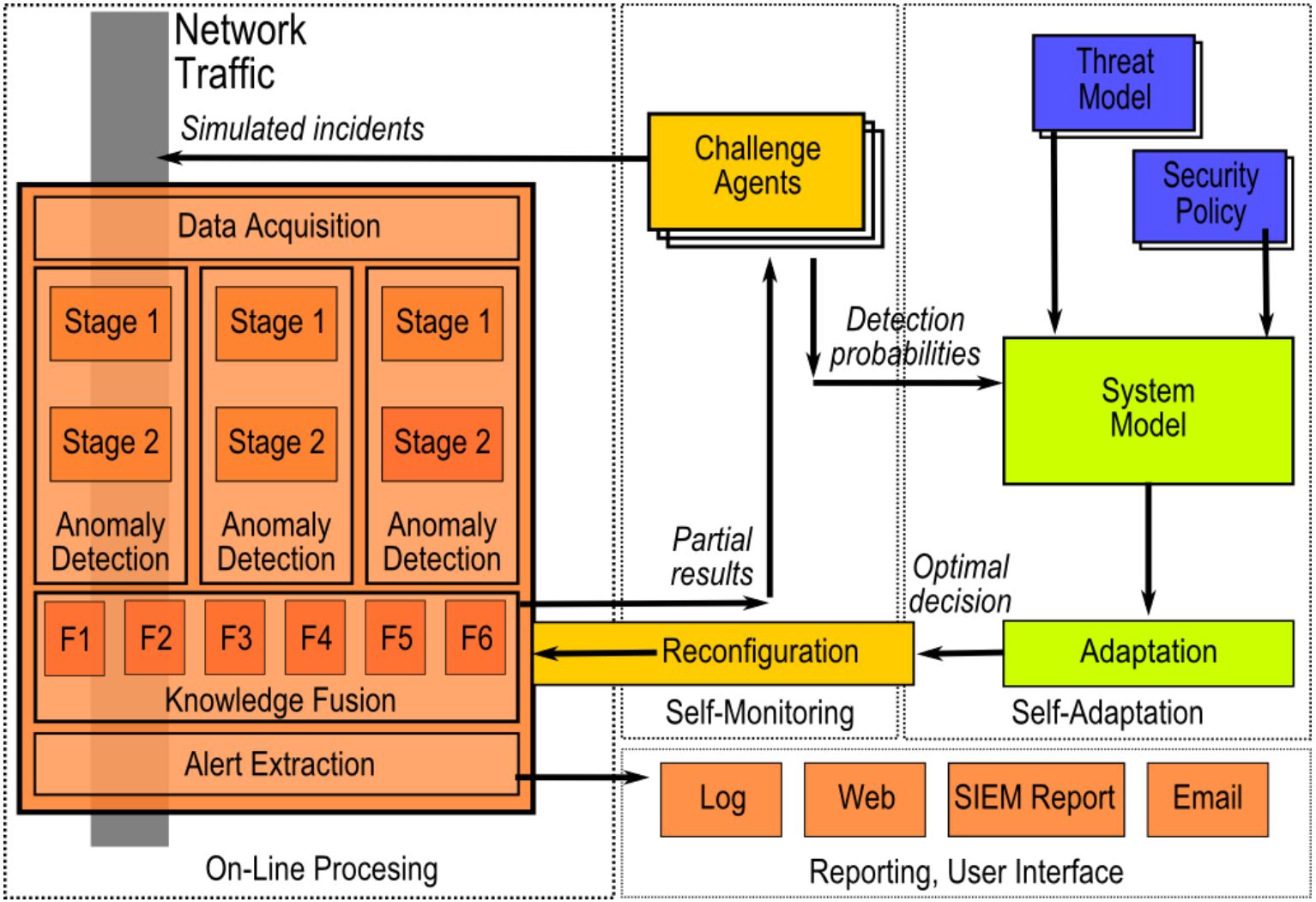
300:2



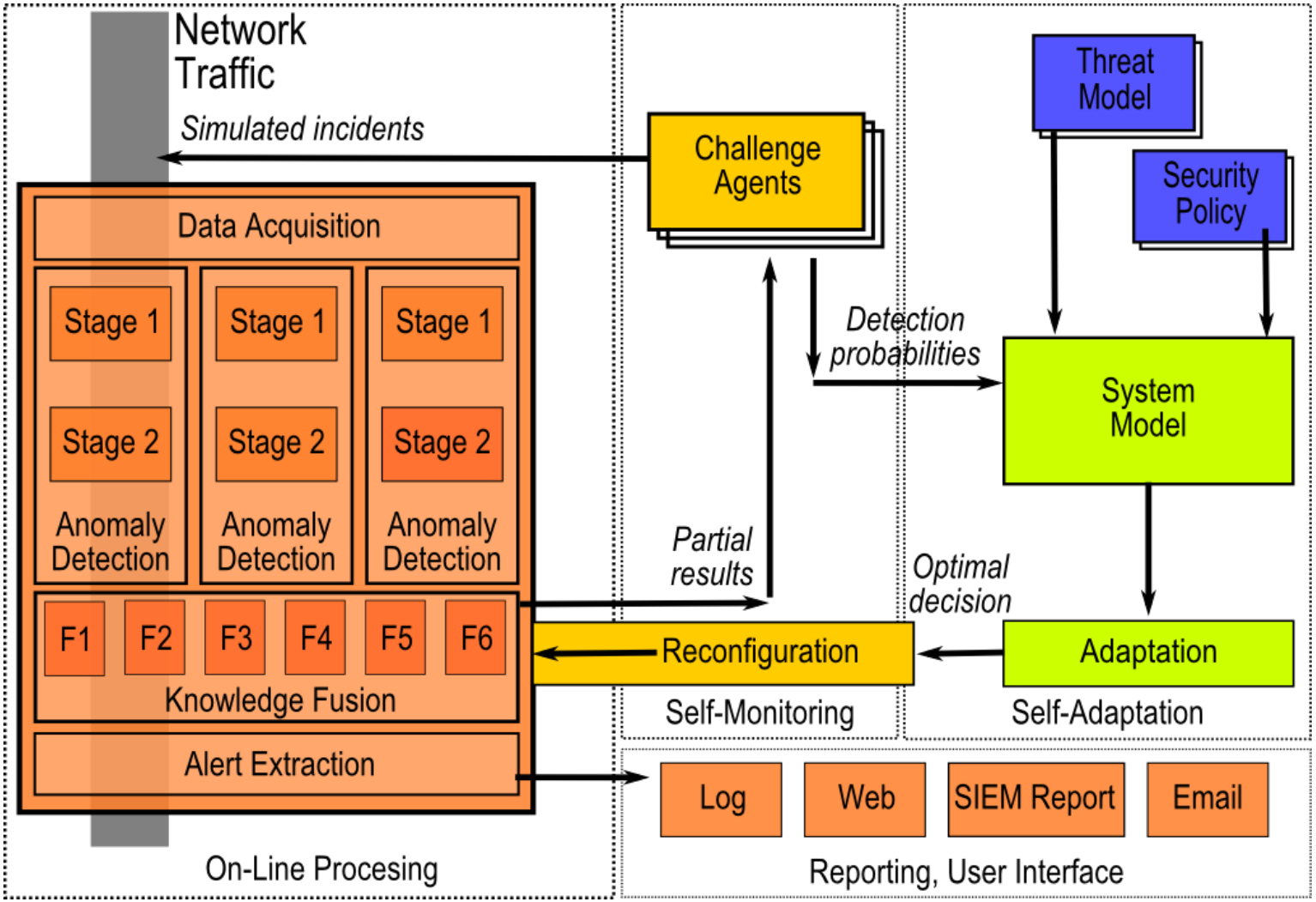
Inside Modern NBA System

300:2

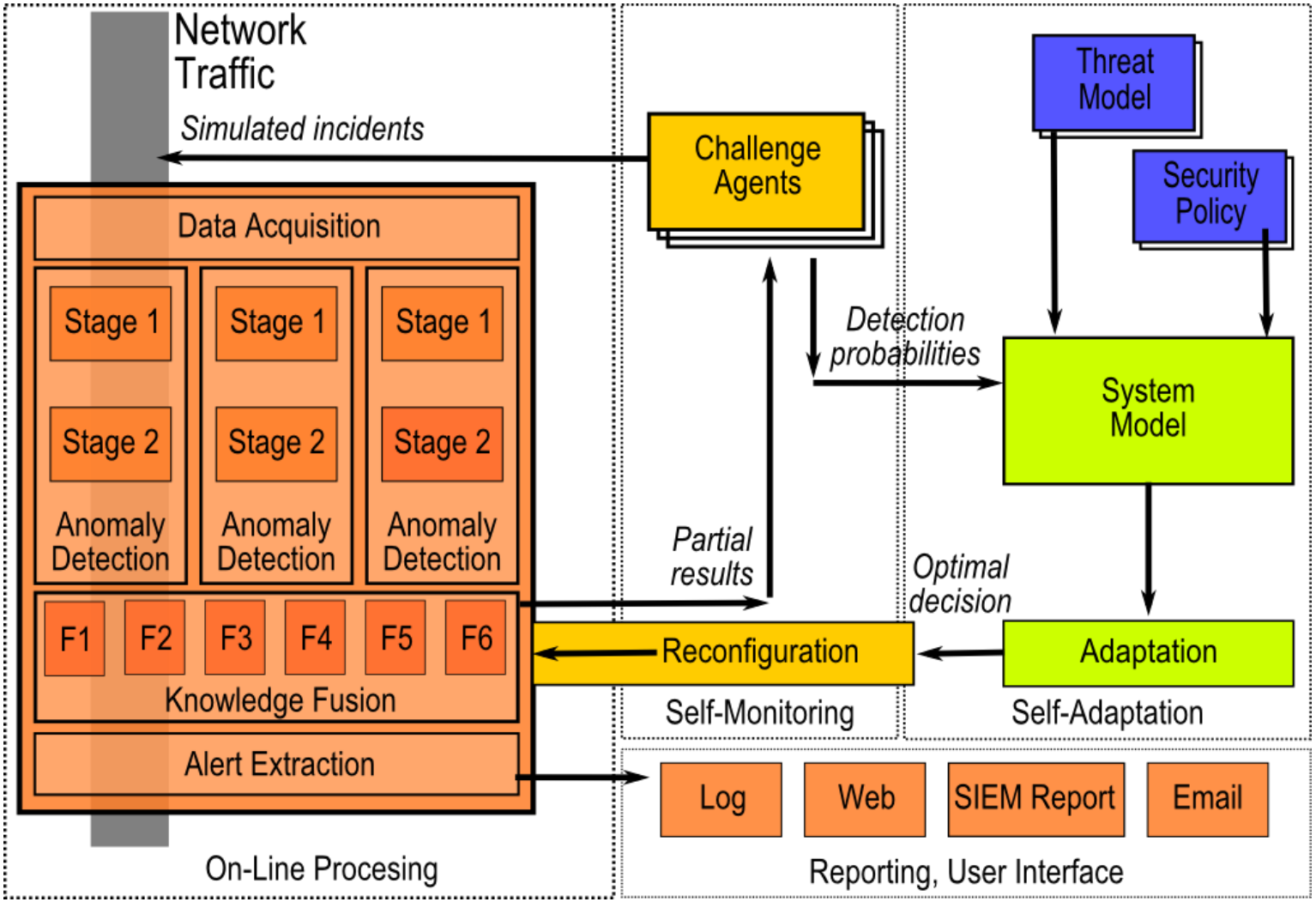
58:2



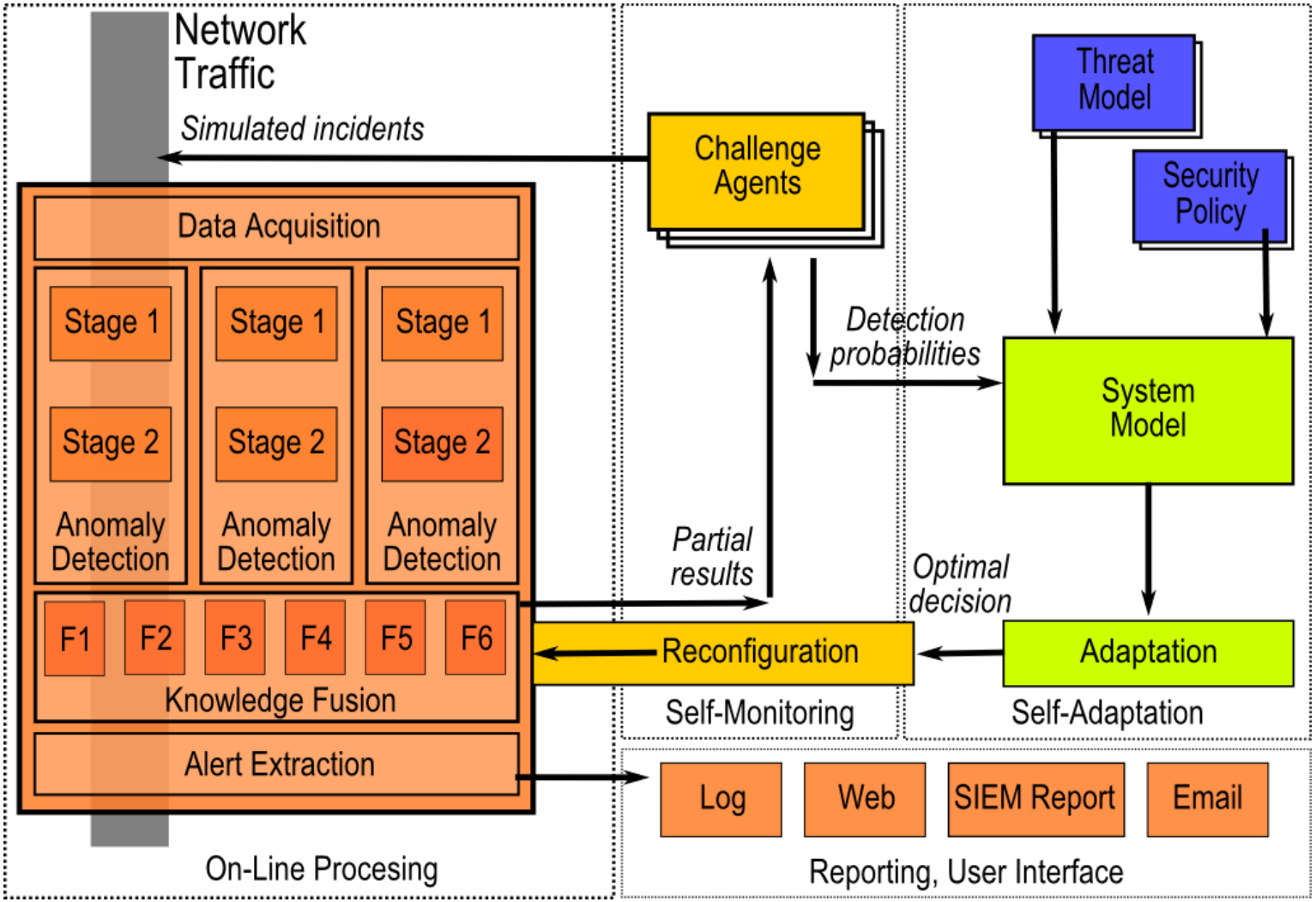
Inside Modern NBA System



Inside Modern NBA System



Inside Modern NBA System



Prioritized (10:1) 1:1 (1:10)

Conclusions

- NBA allows you to:
  - Assess the security of large (open) networks (ISP, universities, corporations)
  - Detect the actions of strategic, persistent attackers in enterprise/high-value networks
  - Cost-effectively cover the network together with SIEM
- NBA is the ultimate black-box solution
  - Confidence, verifiability and state-of-the-art methods are essential
  - Multiple algorithms, strategic reconfiguration and self-management

NBA will not make you secure against advanced persistent threats …

…but will make the attackers insecure.

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

cognitivesecurity

Questions ?
Demo available !
…with pilot competition…

pechoucek@cognitive-security.com
rehak@cognitive-security.com