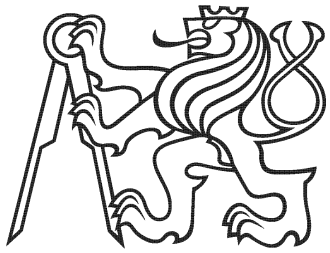


Monitoring sítí pomocí NetFlow dat – od paketů ke strategiím

Martin Rehák, Karel Bartoš , Martin Grill, Jan Stiborek a Michal Svoboda

ATG, České vysoké učení technické v Praze

Jiří Novotný, Pavel Čeleda a Vojtěch Krmíček

ÚVT, Masarykova Univerzita

cognitivesecurity

CAMNEP Project

- Network security monitoring
- Intrusion detection system
- Includes:
  - Anomaly detection techniques
  - Aggregation of more opinions
  - Fusion mechanism
  - Adaptation process
  - Game theory

CAMNEP Goals & Assumptions

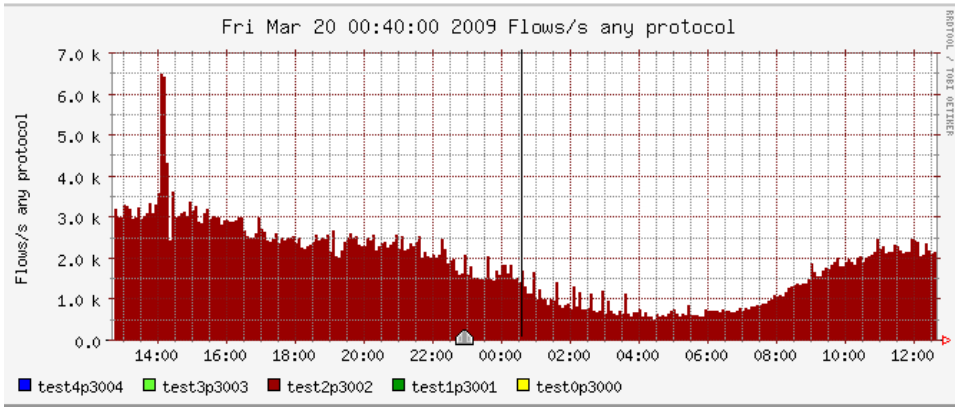
- Improve the **error rate**
  - lower false positives
  - same false negatives
- **Validation** & **Stability**
  - reliable response to typical threats
  - traffic-independent response
- **Management**
  - self-optimization and self-configuration

- Reasonable-sized traffic
- Reasonable attack types
- Not-real time (minimal response delay 40 sec.)
- Integrates with other defense techniques
- Low predictability by opponent
- Structured, actionable output

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



CAMNEP: System overview

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Tos	Packets	Bytes	pps	bps	Bpp	Flows
2007-02-12 10:00:43.839	0.001	TCP	147.251.192.4:524	->	147.251.192.86:1033	.AP...	0	2	187	1999	1.4 M	93	1
2007-02-12 10:00:43.845	0.000	UDP	147.251.192.1:53	->	147.251.192.153:1159	.....	0	1	133	0	0	133	1
2007-02-12 10:00:43.848	0.000	UDP	147.251.192.153:1159	->	147.251.192.1:53	.....	0	1	53	0	0	53	1
2007-02-12 10:00:43.848	0.000	TCP	147.251.193.76:1028	->	147.251.192.4:524	.AP...	0	2	284	0	0	142	1
2007-02-12 10:00:43.848	0.000	UDP	147.251.193.76:1529	->	147.251.192.1:53	.....	0	2	126	0	0	63	1
2007-02-12 10:00:43.848	0.000	UDP	147.251.192.1:53	->	147.251.193.76:1529	.....	0	2	224	0	0	112	1
2007-02-12 10:00:41.525	2.324	TCP	147.251.193.76:1026	->	147.251.192.4:524	.AP...	0	3	292	1	1005	97	1
2007-02-12 10:00:43.848	0.001	TCP	147.251.192.4:524	->	147.251.193.76:1028	.AP...	0	2	162	1999	1.2 M	81	1
2007-02-12 10:00:43.849	0.000	UDP	147.251.4.33:53	->	147.251.193.76:1529	.....	0	2	224	0	0	112	1
2007-02-12 10:00:41.552	2.298	TCP	147.251.192.4:524	->	147.251.193.76:1026	.AP...	0	2	116	0	403	58	1
2007-02-12 10:00:43.848	0.002	UDP	147.251.193.76:1529	->	147.251.4.33:53	.....	0	2	126	999	503999	63	1
2007-02-12 10:00:43.336	0.580	TCP	147.251.192.1:44254	->	70.42.39.14:2703	.AP.SF	0	6	510	10	7034	85	1
2007-02-12 10:00:43.421	0.497	TCP	147.251.192.1:44255	->	70.42.39.14:2703	.AP.SF	0	7	534	14	8595	76	1
2007-02-12 10:00:43.935	0.000	UDP	61.151.252.240:53	->	147.251.192.1:53859	.....	0	1	123	0	0	123	1
2007-02-12 10:00:42.632	1.307	TCP	84.60.32.153:24023	->	147.251.192.106:6881	.AP.SF	0	12	2194	9	13429	182	1
2007-02-12 10:00:43.624	0.318	TCP	194.79.52.10:80	->	147.251.192.153:1158	.AP.S.	0	5	3191	15	80276	638	1
2007-02-12 10:00:43.943	0.000	TCP	65.78.80.176:57889	->	147.251.192.106:3514	.A....	0	1	42	0	0	42	1
2007-02-12 10:00:43.943	0.034	TCP	129.12.31.4:14017	->	147.251.195.20:1077	.AP...	0	3	126	88	29647	42	1
2007-02-12 10:00:34.713	9.268	TCP	212.80.76.24:80	->	147.251.192.153:1108	.AP.SF	0	11	6797	1	5867	617	1
2007-02-12 10:00:43.251	0.748	TCP	147.251.192.1:25	->	147.251.4.36:33555	.AP.SF	0	21	1242	28	13283	59	1
2007-02-12 10:00:43.251	0.748	TCP	147.251.4.36:33555	->	147.251.192.1:25	.AP.SF	0	28	28556	37	305411	1019	1
2007-02-12 10:00:44.002	0.004	TCP	194.228.32.6:80	->	147.251.195.144:2887	.A...F	0	2	84	499	167999	42	1
2007-02-12 10:00:43.839	0.197	TCP	147.251.192.86:1033	->	147.251.192.4:524	.AP...	0	4	310	20	12588	77	1
2007-02-12 10:00:44.056	0.000	TCP	194.79.52.199:80	->	147.251.192.153:1160	.AP...	0	2	1150	0	0	575	1
2007-02-12 10:00:43.863	0.197	TCP	147.251.192.153:1160	->	194.79.52.199:80	.AP.S.	0	4	397	20	16121	99	1
2007-02-12 10:00:43.559	0.503	TCP	70.42.39.14:2703	->	147.251.192.1:44255	.APRS.	0	7	399	13	6345	57	1
2007-02-12 10:00:43.467	0.596	TCP	70.42.39.14:2703	->	147.251.192.1:44254	.APRS.	0	8	457	13	6134	57	1
2007-02-12 10:00:23.849	30.141	TCP	147.251.195.20:1077	->	129.12.31.4:14017	.AP...	0	18	780	0	207	43	1
2007-02-12 10:00:44.086	0.000	UDP	147.251.192.1:53859	->	192.42.93.30:53	.....	0	1	62	0	0	62	1
2007-02-12 10:00:40.249	3.839	UDP	147.251.192.146:137	->	147.251.193.255:137	.....	0	5	370	1	771	74	1
2007-02-12 10:00:43.767	0.000	UDP	82.208.50.129:6354	->	147.251.192.27:32225	.....	0	1	119	0	0	119	1
2007-02-12 10:00:43.773	0.000	UDP	82.208.50.129:21128	->	147.251.192.27:29123	.....	0	1	119	0	0	119	1
2007-02-12 10:00:43.294	0.486	TCP	147.251.192.153:1158	->	194.79.52.10:80	.AP.S.	0	5	459	10	7555	91	1
2007-02-12 10:00:43.151	0.656	TCP	147.251.192.5:80	->	147.251.193.59:1414	.AP.SF	0	58	71055	88	866524	1225	1
2007-02-12 10:00:43.149	0.658	TCP	147.251.193.59:1414	->	147.251.192.5:80	.AP.SF	0	32	2144	48	26066	67	1
2007-02-12 10:00:43.831	0.000	UDP	86.193.122.29:6881	->	147.251.192.170:61158	.....	0	1	66	0	0	66	1
2007-02-12 10:00:43.832	0.000	UDP	147.251.192.170:61158	->	86.193.122.29:6881	.....	0	1	104	0	0	104	1
2007-02-12 10:00:43.501	0.334	TCP	147.251.49.10:443	->	147.251.192.105:1404	.AP.SF	0	7	2551	20	61101	364	1
2007-02-12 10:00:43.499	0.343	TCP	147.251.192.105:1404	->	147.251.49.10:443	.AP.SF	0	7	1029	20	23999	147	1
2007-02-12 10:00:43.828	0.034	TCP	147.251.192.9:80	->	213.29.7.70:51071	.AP.SF	0	5	418	147	98352	83	1
2007-02-12 10:00:43.828	0.036	TCP	213.29.7.70:51071	->	147.251.192.9:80	.AP.SF	0	5	772	138	171555	154	1
2007-02-12 10:00:43.905	0.000	UDP	86.212.219.202:6881	->	147.251.192.170:61158	.....	0	1	89	0	0	89	1
2007-02-12 10:00:43.908	0.000	UDP	147.251.192.170:61158	->	86.212.219.202:6881	.....	0	1	234	0	0	234	1
2007-02-12 10:00:43.909	0.001	UDP	147.251.18.65:59861	->	147.251.195.131:137	.....	0	2	148	1999	1.1 M	74	1
2007-02-12 10:00:43.910	0.004	UDP	147.251.195.131:137	->	147.251.18.65:59861	.....	0	2	434	499	867999	217	1
2007-02-12 10:00:43.947	0.000	UDP	147.251.192.1:53859	->	85.17.42.212:53	.....	0	1	73	0	0	73	1
2007-02-12 10:00:43.950	0.000	UDP	10.192.192.25:123	->	10.192.192.1:123	.....	192	1	72	0	0	72	1
2007-02-12 10:00:43.951	0.000	UDP	192.42.93.30:53	->	147.251.192.1:53859	.....	0	1	300	0	0	300	1
2007-02-12 10:00:43.975	0.000	UDP	85.17.42.212:53	->	147.251.192.1:53859	.....	0	1	327	0	0	327	1
2007-02-12 10:00:43.969	0.006	UDP	147.251.18.65:59861	->	147.251.195.132:137	.....	0	2	148	333	197333	74	1
2007-02-12 10:00:43.975	0.000	UDP	147.251.195.132:137	->	147.251.18.65:59861	.....	0	2	470	0	0	235	1
2007-02-12 10:00:44.003	0.014	TCP	147.251.192.89:3059	->	81.95.96.121:80	.AP..F	0	5	484	357	276571	96	1
2007-02-12 10:00:44.003	0.018	TCP	81.95.96.121:80	->	147.251.192.89:3059	.AP.S.	0	5	2044	277	908444	408	1
2007-02-12 10:00:44.027	0.000	UDP	147.251.195.133:137	->	147.251.18.65:59861	.....	0	2	470	0	0	235	1
2007-02-12 10:00:44.027	0.001	UDP	147.251.18.65:59861	->	147.251.195.133:137	.....	0	2	148	1999	1.1 M	74	1
2007-02-12 10:00:44.026	0.010	TCP	147.251.192.89:3060	->	81.95.96.121:80	.AP.SF	0	5	595	499	475999	119	1
2007-02-12 10:00:44.026	0.021	TCP	81.95.96.121:80	->	147.251.192.89:3060	.AP.SF	0	5	338	238	128761	67	1
2007-02-12 10:00:39.140	4.942	TCP	86.41.152.176:49172	->	147.251.192.170:61158	.AP...	0	10	448	2	725	44	1
2007-02-12 10:00:44.087	0.000	UDP	147.251.18.65:59861	->	147.251.195.134:137	.....	0	2	148	0	0	74	1
2007-02-12 10:00:43.975	0.112	TCP	205.188.165.249:80	->	147.251.193.4:1954	.AP.S.	0	3	646	26	46142	215	1
2007-02-12 10:00:44.728	0.000	UDP	147.251.195.134:137	->	147.251.18.65:59861	.....	0	2	470	0	0	235	1

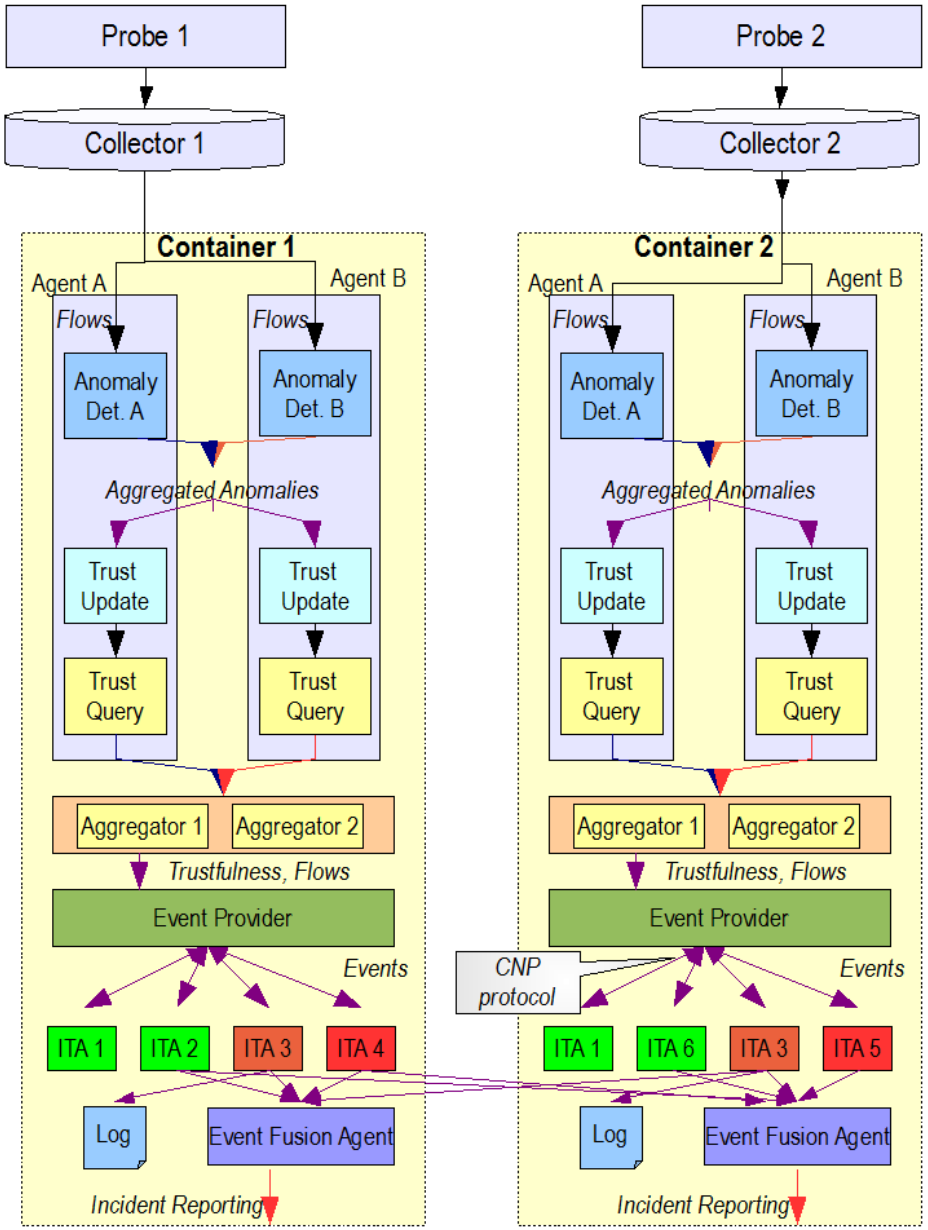
Architecture

- Levels by speed:

- **Up to 10 M packets ps**
- **Up to 10 K flows ps**

- **Detected flows (10K fps)**
- **Events (0-1000 per 5min)**

- **Plans/ Attack Trees**
- **Adaptation processes**



agent technology center

cognitivesecurity

Data Acquisition Layer

Network probe

- COMBO card
- High-performance hardware probes
- 10 Gbits/sec full volume
- NetFlow/IPFIX protocol

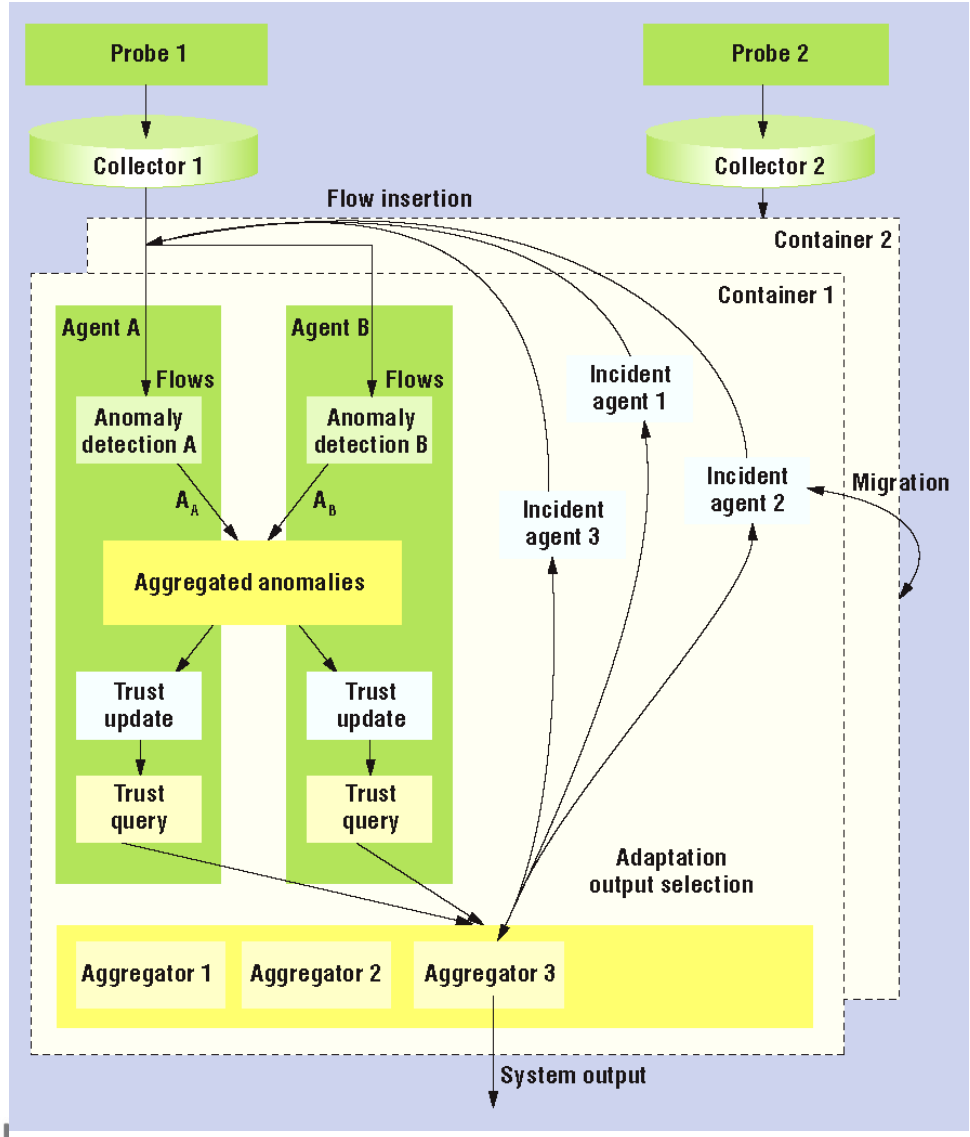
Collector + preprocessing

- nfdump/nfsen collector
  - Open-source
  - Swiss led effort
  - Actively maintained
- Customized plugin for:
  - Data preprocessing
  - Communication with CAMNEP engine

agent technology center cognitivesecurity

Detection Layer Overview

- **Flows** to **categories**
- **Multiple AD methods**
- Multiple trust models
- Multiple aggregation methods
- Agent-based
- Dynamic
- Several layers of learning



agent technology center

cognitivesecurity

Anomaly Detection Methods

MINDS

- number of connections
- Trends, aggregated by:
  - srcIP, dstIP, srcIP-dstPort, dstIP-srcPrt

TAPS

- Scan detection
- Dest. ports/dstIP, flow size entropy
- Aggregated by srcIP

Anomaly Detection Methods

- Principal Component Analysis used to generalize the traffic model by dimensionality reduction
- Aggregated by source IP
- Captures relationships between traffic sources

Lakhina Volume

- Models flows, packets, and bytes for larger traffic sources

Lakhina Entropy

- Models traffic characteristics – header value distributions

Anomaly Detection Methods

Xu

- Traffic characteristics
  - dstIP, srcPrt, dstPrt distribution entropies
- Aggregated by traffic source

Xu-dstIP

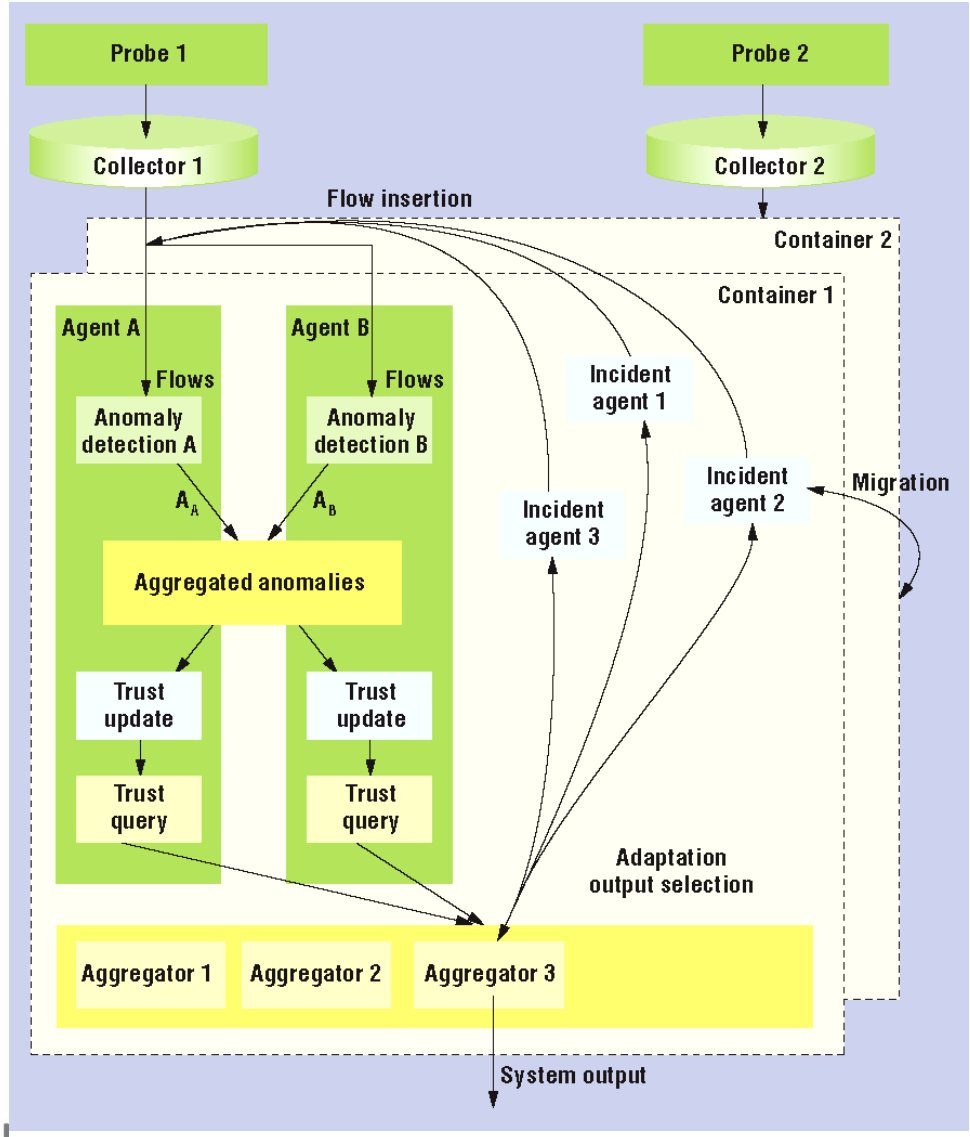
- Traffic characteristics
  - srcIP, srcPrt, dstPrt distribution entropies
- Aggregated by traffic destination

Anomaly Detection Methods

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

Detection Layer Overview

- **Flows** to **categories**
- Multiple AD methods
- **Multiple trust models**
- Multiple aggregation methods
- Agent-based
- Dynamic
- Several layers of learning



agent technology center

cognitivesecurity

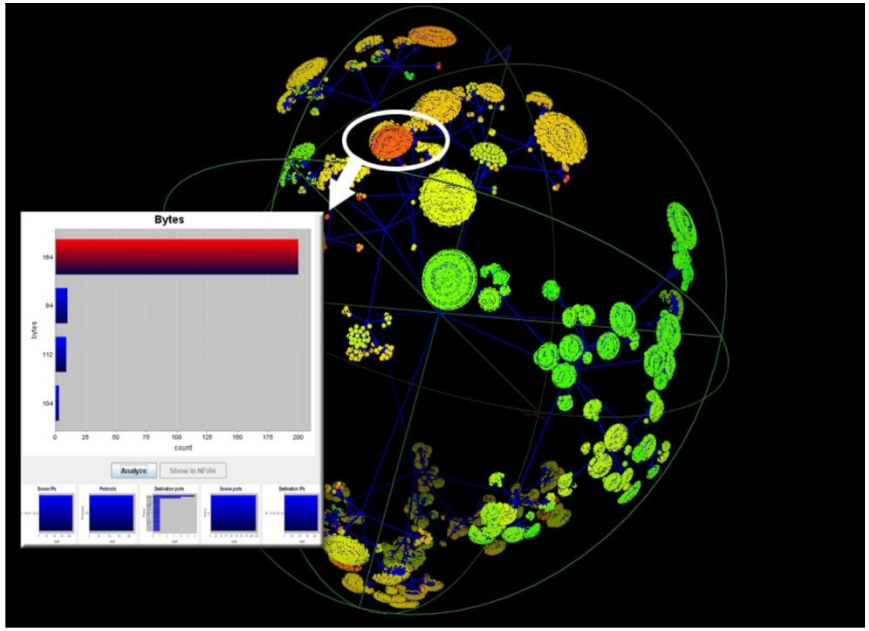
Identity and Context Example

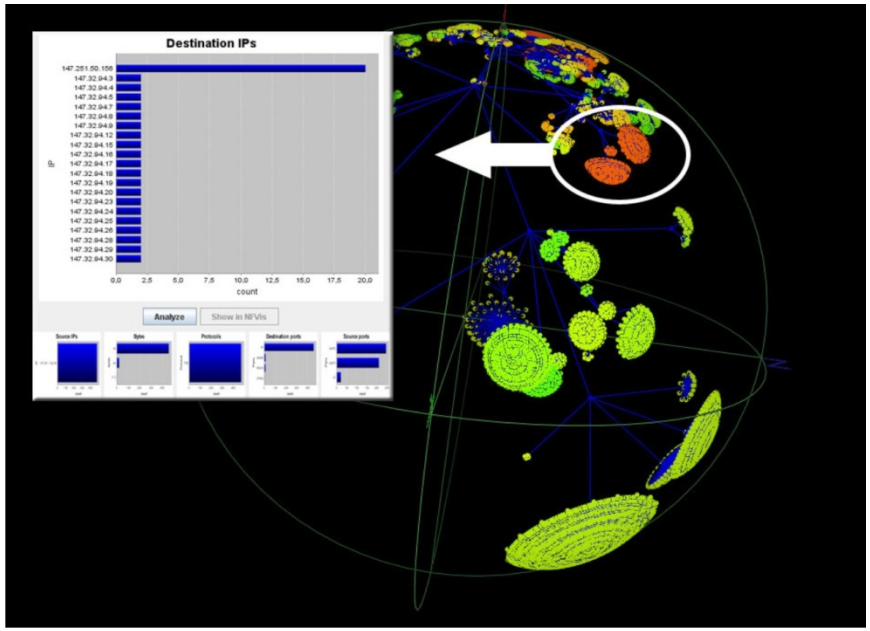
Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2009-03-20 01:11:12.923	364.932	TCP	147.251.198.84:2430	->	78.154.195.124:47575	8699	8.1 M	104
2009-03-20 01:12:38.215	276.256	UDP	92.240.244.30:27022	->	147.251.211.107:27005	19266	4.1 M	72
2009-03-20 01:11:51.690	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**

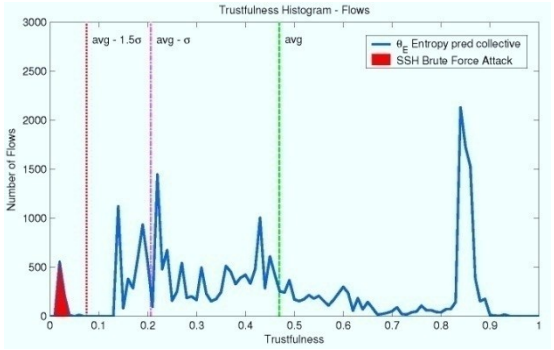
Trust Modeling

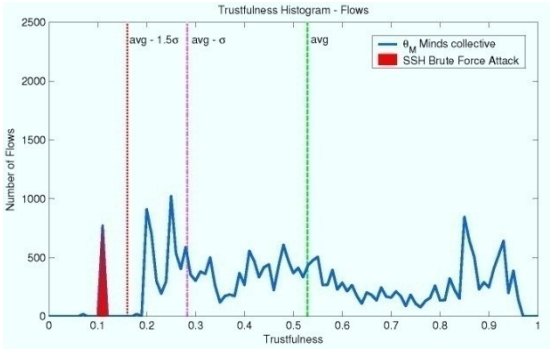
- Reduction of false positives by:
  - Multi-source aggregation
  - Historical experience aggregation
- Incremental, unsupervised learning
- Automatic identity-context construction
- Associated trust model

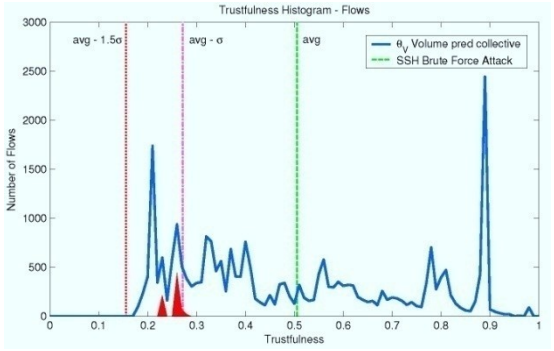


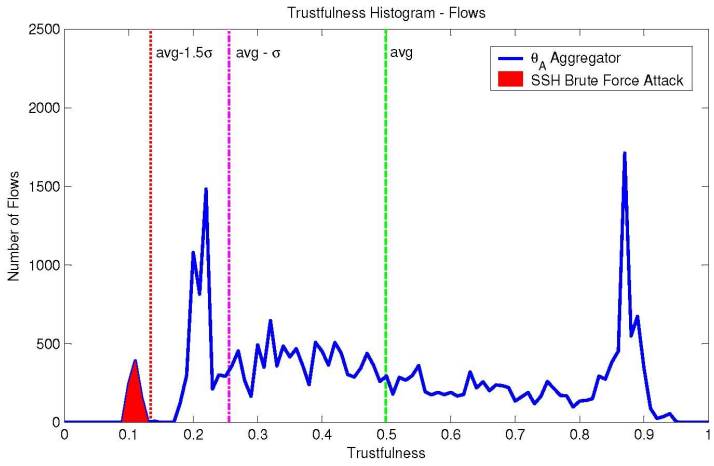


Trust Aggregation







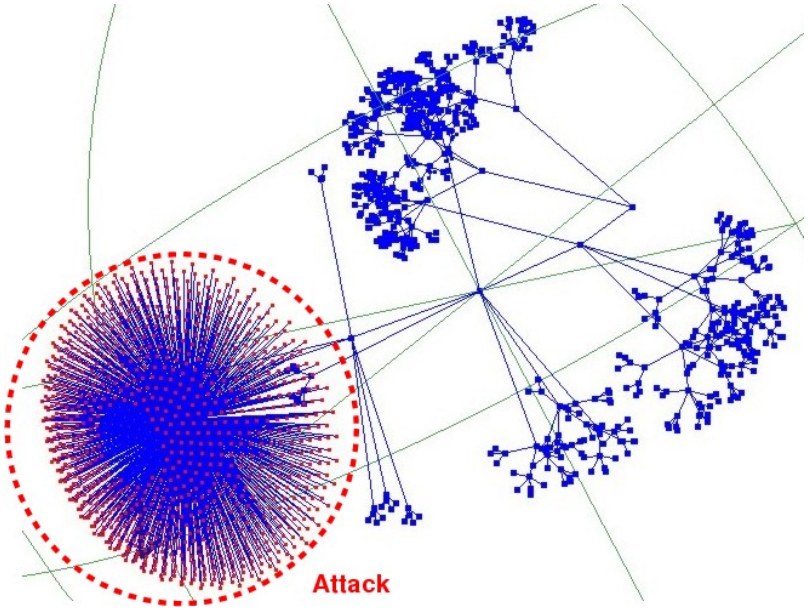


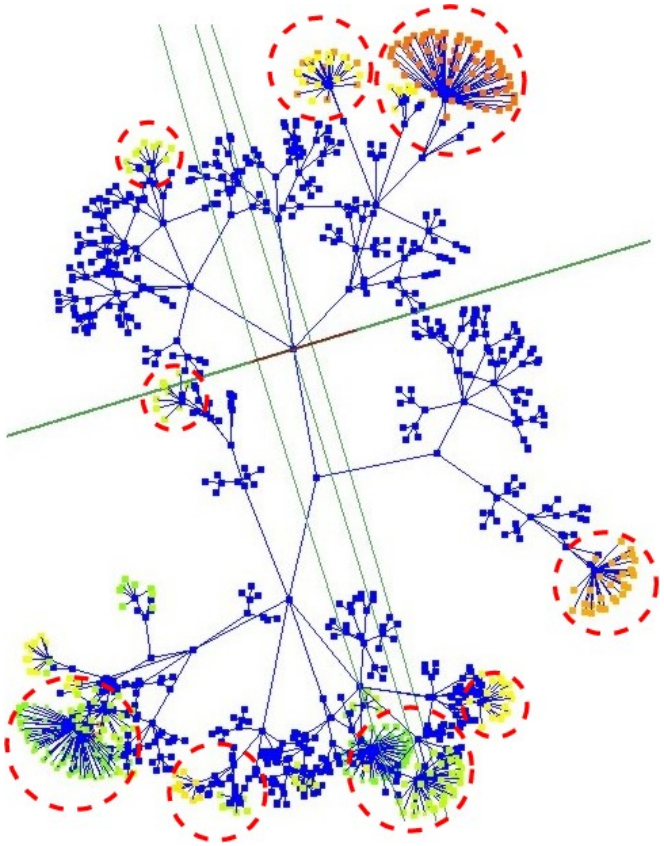
- Error reduction
  - Feature diversity
  - Algorithm diversity
  - Multistage error reduction:
    - AD
    - Trustfulness

agent technology center

cognitivesecurity

Trust Aggregation Importance



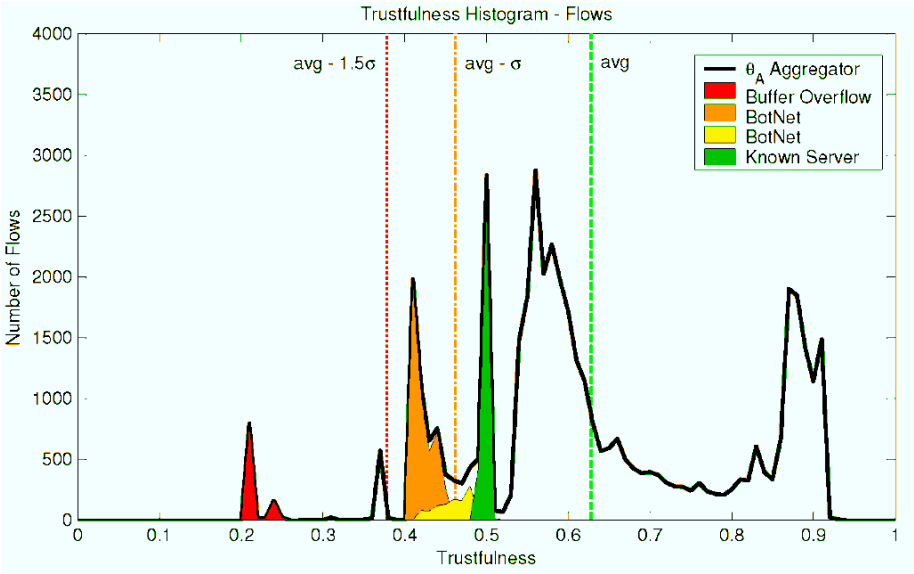


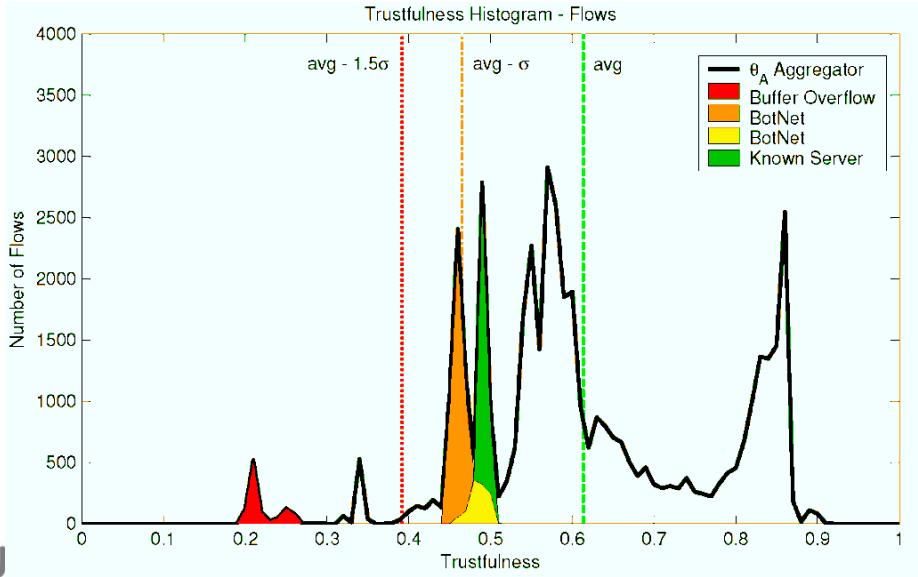
Self-Management and Adaptation

- Monitoring:
  - Self-monitoring
  - Self-evaluation
  - Defect detection
- Reflection:
  - Component generation
  - Component selection
  - Component combination
  - Component repair

Dynamic Classifier Selection

- Unsupervised
- Dynamic:
  - Background traffic
  - Model performance
  - Attacks
- Strategic behavior
  - Evasion
  - Attacks on learning



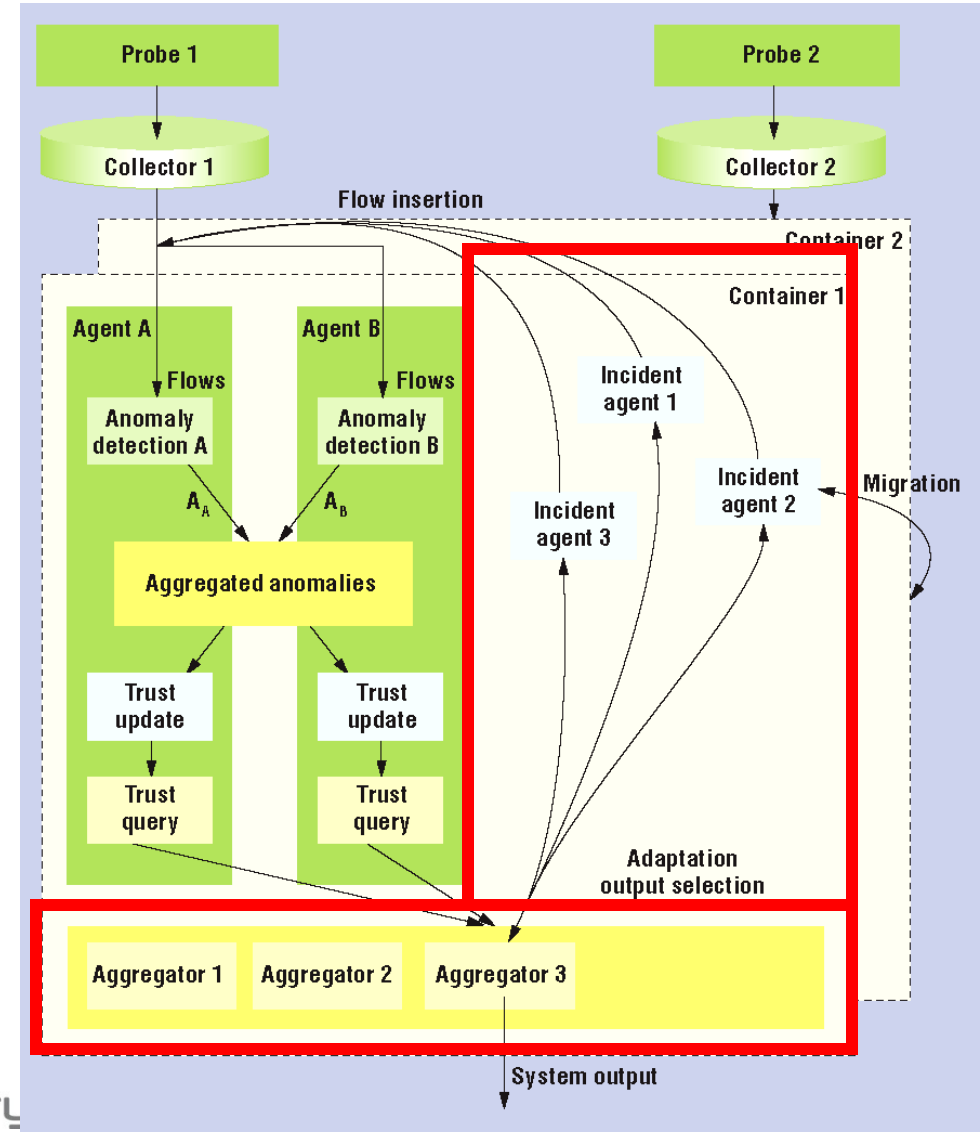


agent technology center

cognitivesecurity

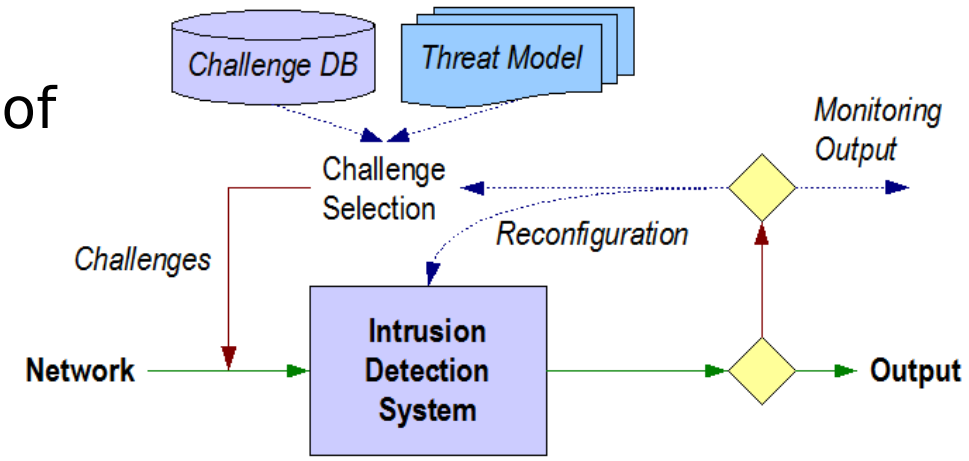
Adaptation Architecture

- Monitoring & evaluation
  - Challenge insertion
  - Challenge insertion control
  - Challenge selection strategy
- Adaptation
  - Aggregation function selection
  - Aggregation function creation

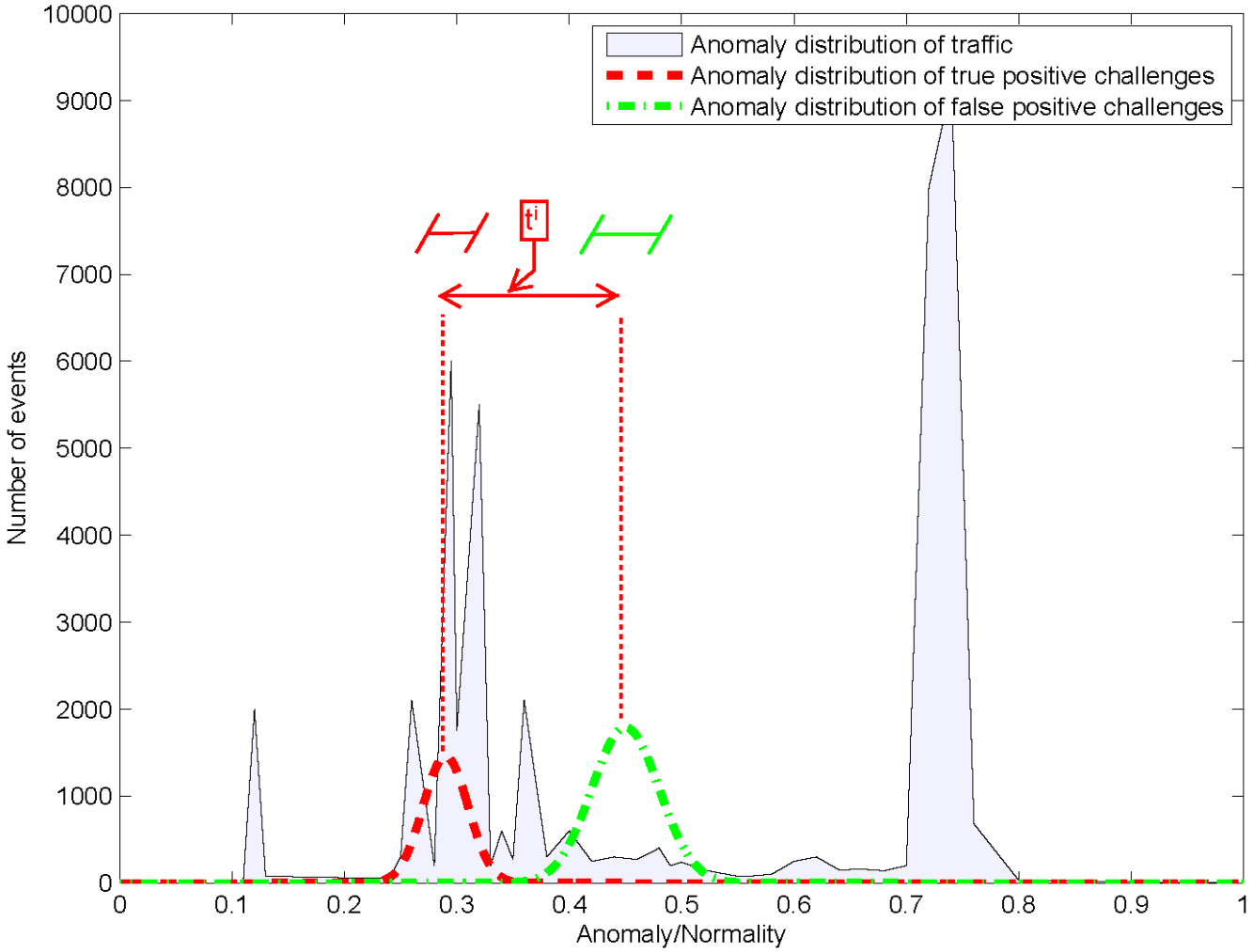


Monitoring: Challenge Insertion

- Unlabeled background input data
- Insertion of small set of challenges
  - Legitimate
  - Malicious
- Response evaluation
- Problems: Noise, challenge non-uniformity, distribution, system compromise



Challenge Insertion Control



Results

Processing level	FP	TP
Individual anomaly detection algorithm	**300**	**2**
Average of anomalies	**58**	**2**
Arithmetic average of trustworthiness	**15**	**2**
Adaptive aggregation of trustworthiness	**5**	**2**

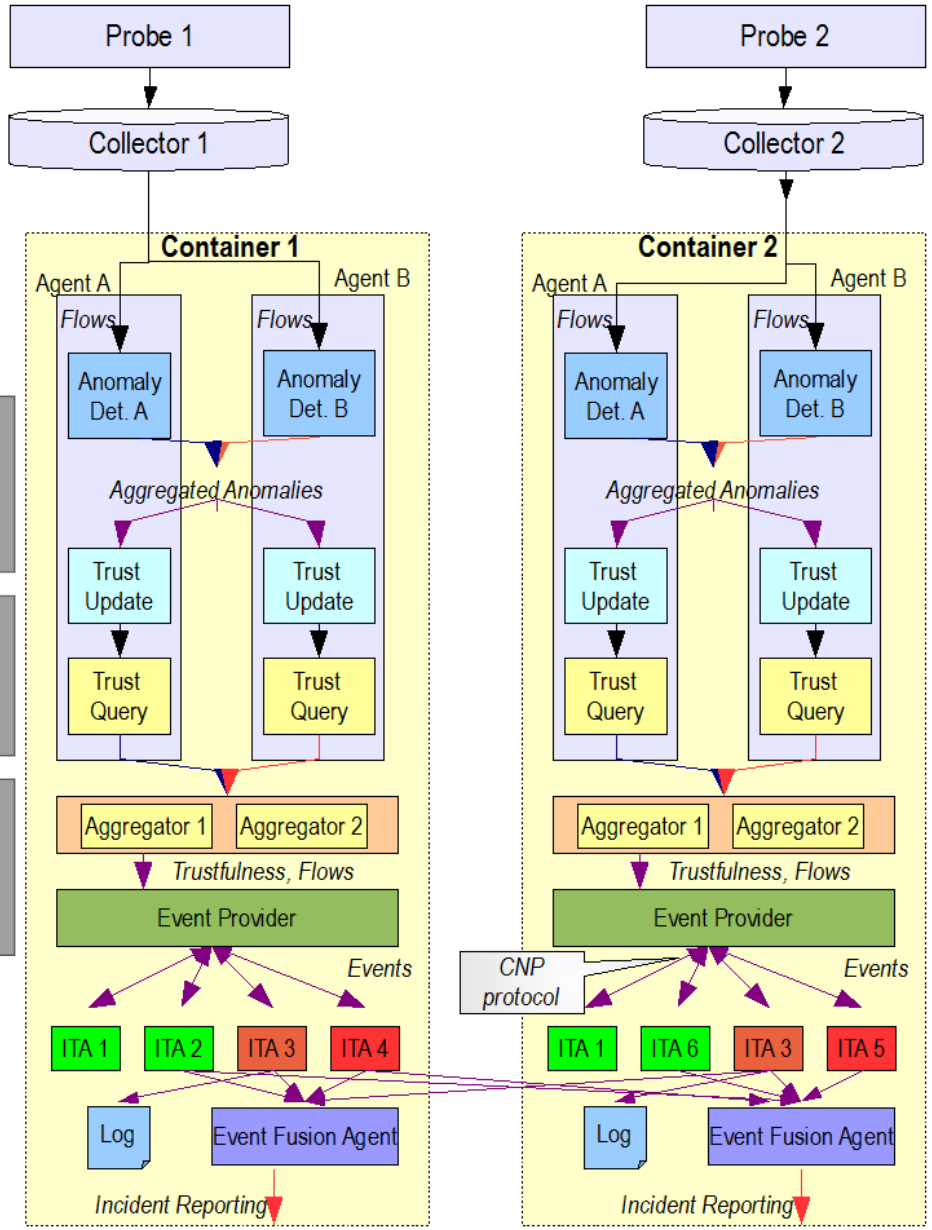
Architecture

- Levels by speed:

- **Up to 10 M packets ps**
- **Up to 10 K flows ps**

- **Detected flows (10K fps)**
- **Events (0-1000 per 5min)**

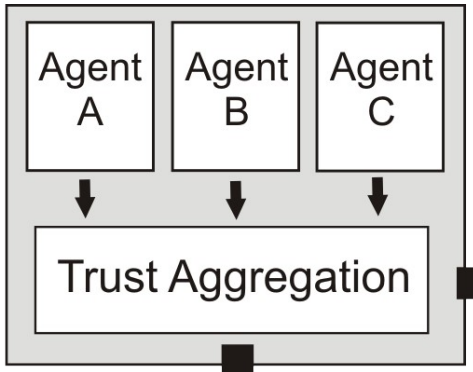
- **Plans/ Attack Trees**
- **Adaptation processes**



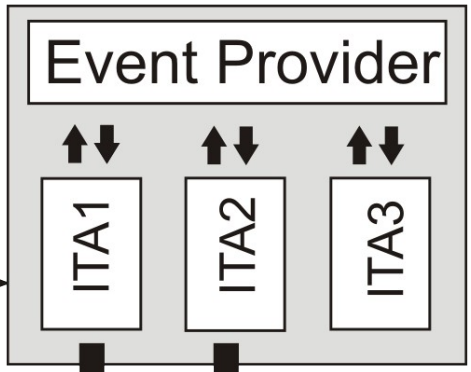
agent technology center

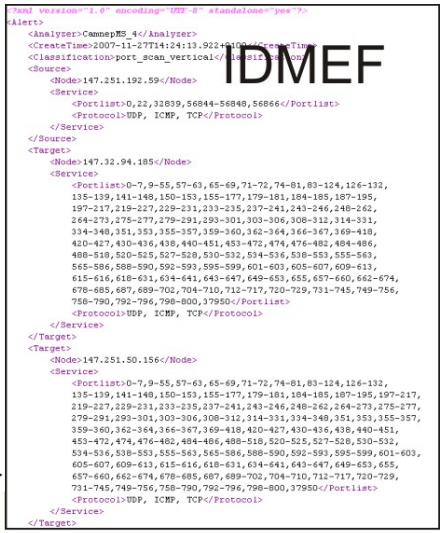
cognitivesecurity

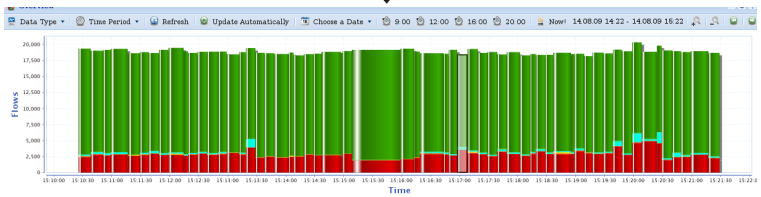
Incident Classification & Reporting



Events

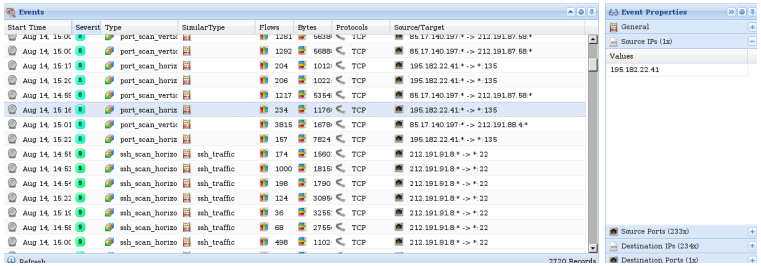






Classified incidents

Incident reporting



Text report

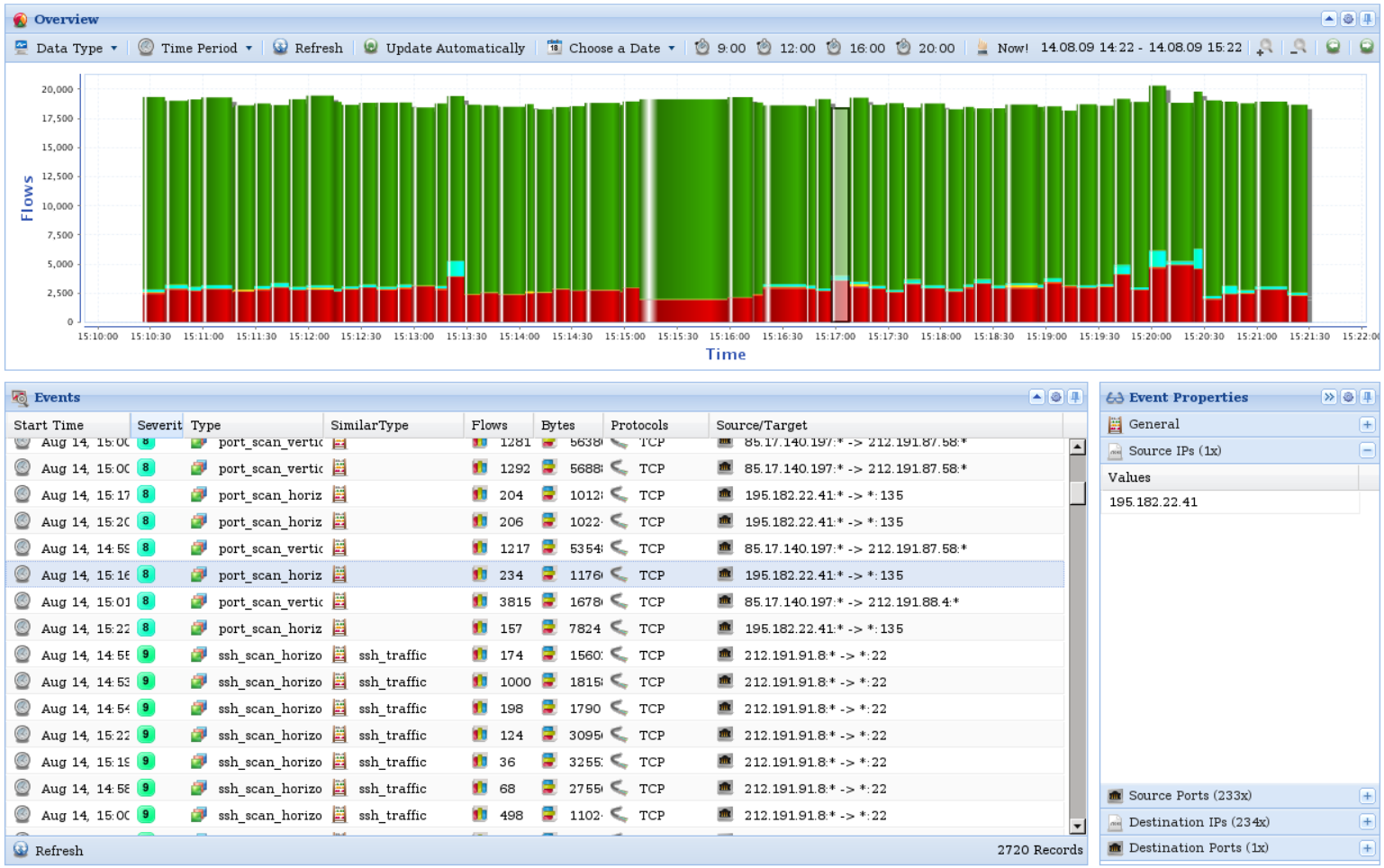
```
Analyzer:       CamnepMS_4
Create Time:    2007-11-27T14:24:13.922+0100
Classification: port_scan_vertical
Sources:
        Nodes:  147.251.192.59
        Ports:  0,22,32839,56844-56848,56866
        Protocol: UDP, ICMP, TCP
Targets:
        Nodes:  147.32.94.185           147.251.50.156          147.251.192.1

        Ports:  0-7,9-55,57-63,65-69,71-72,74-81,83-124,126-132,135-139,141-148,
                150-153,155-177,179-181,184-185,187-195,197-217,219-227,229-231,233-235,237-241,
                243-246,248-262,264-273,275-277,279-291,293-301,303-306,308-312,314-331,334-348,
                351,353,355-357,359-360,362-364,366-367,369-418,420-427,430-436,438,
                440-451,453-472,474,476-482,484-486,488-518,520-525,527-528,530-532,534-536,
                538-553,555-563,565-586,588-590,592-593,595-599,601-603,605-607,609-613,615-616,
                618-631,634-641,643-647,649-653,655,657-660,662-674,678-685,687,689-702,
                704-710,712-717,720-729,731-745,749-756,758-790,792-796,798-800,37950
        Protocol: UDP, ICMP, TCP
```

agent technology center

cognitivesecurity

From research to product

cognitivesecurity



agent technology center

cognitivesecurity

Conclusions

- CAMNEP uses **advanced AI** methods to tackle real business problems:
  - Automatically reduces and maintains the **error rate**
  - **Reduces downtime** and fault rate
  - Monitors system **performance**
  - **Optimizes** system performance
  - Resists **strategic behavior** of informed opponent

cognitivesecurity