Share experience. Build resilience

Welcome to SECCON NL 2022

digital trust center.

Connect2Trust

HSD securitydelta.nl

CYBERVEILIG NEDERLAND

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

telindus a Proximus company

avit

cisco SECURE

NORTHWAVE

UNIVERSITY OF TWENTE.

Anomaly based

Improving Intrusion detection Using ~~Machine Learning~~ For Practical Use

Auto Encoders

Unsupervised

Share experience. Build resilience.

Agenda

1. Background
2. The goal
3. How to use Anomaly Detection
4. Lessons learned

Background

Network Intrusion Detection

Signature-based

SNORT®

SURICATA

EMERGING THREATS

Signature-based

If an email contains the word ”Corona”
delete email

Signature-based

If an email contains something I do not want to read,

delete email

Signature-based

How do we know what that something is?

Anomaly-based

Email title
A
B
C
4

Anomaly-based

Statistics

PCA
K-Nearest Neighbors
Clustering

Machine Learning

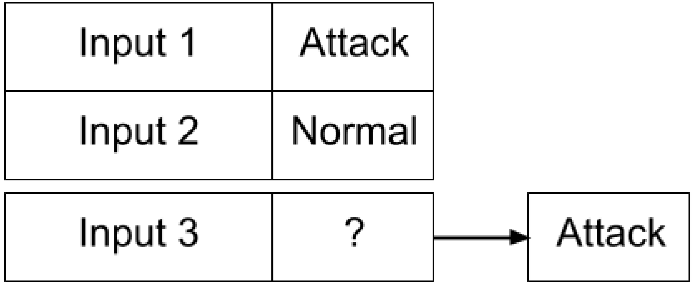
Decision Trees
Support Vector Machines
Auto Encoders

The goal

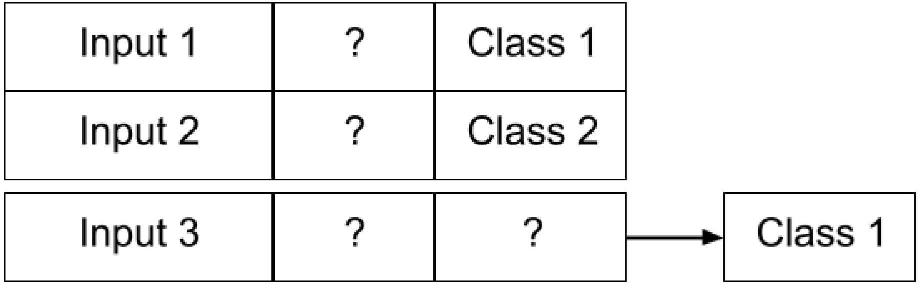
Can we achieve anomaly-based detection for practical commercial use?

If so, how?

What data can we use?



Labeled



Unlabeled

Unsupervised Anomaly-based

Statistics

K-~~Nearest~~ Neighbors
PCA
Clustering

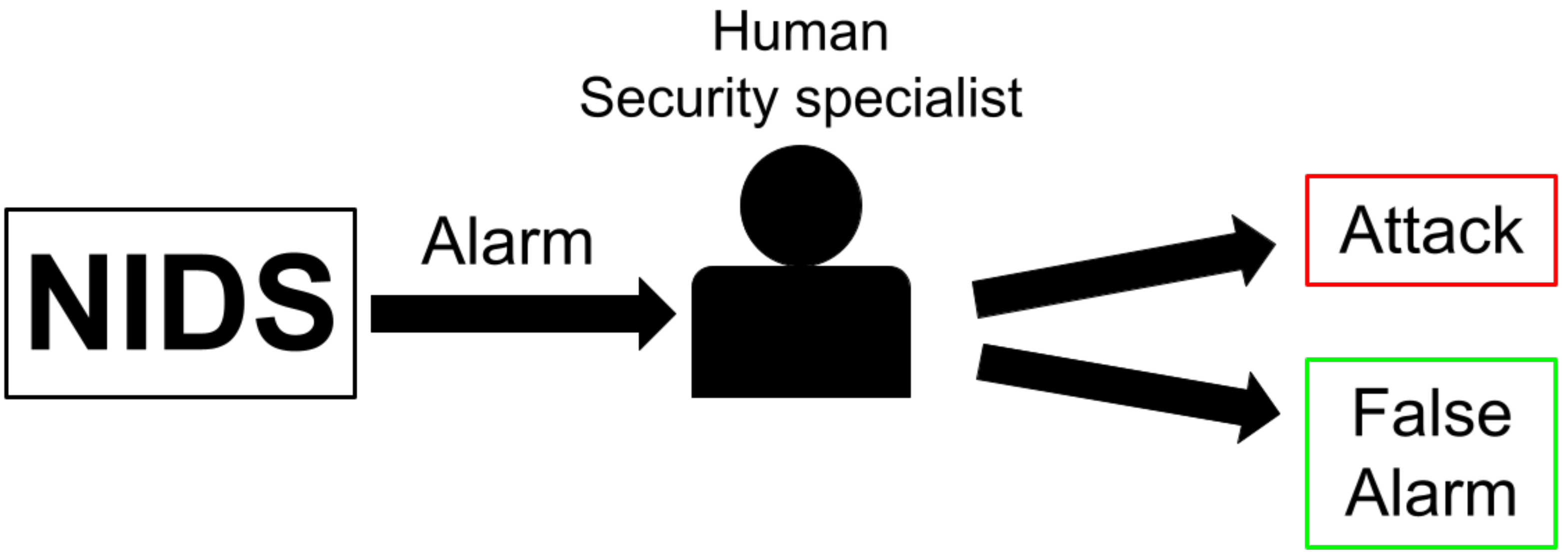
Machine Learning

~~Decision Trees~~
~~Support Vector Machines~~
Auto Encoders

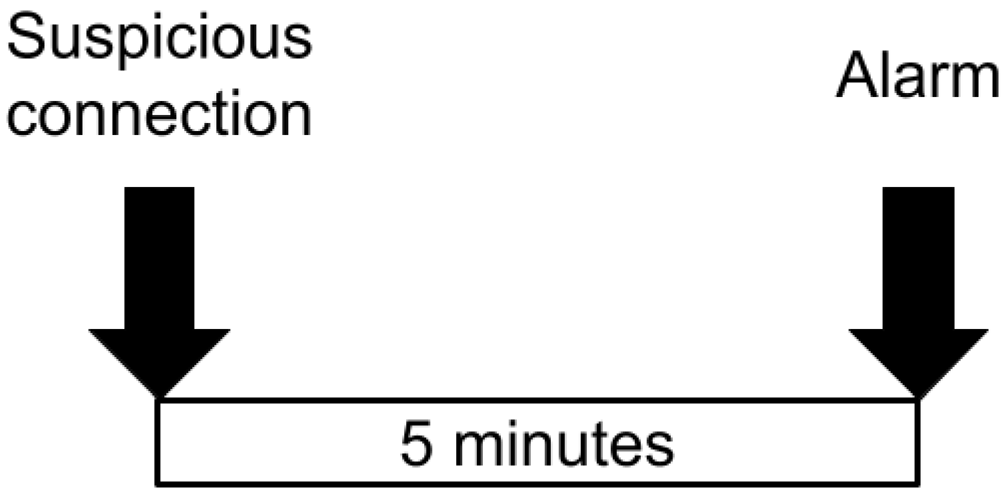
What is practical?

High performance and high efficiency

Practical situation

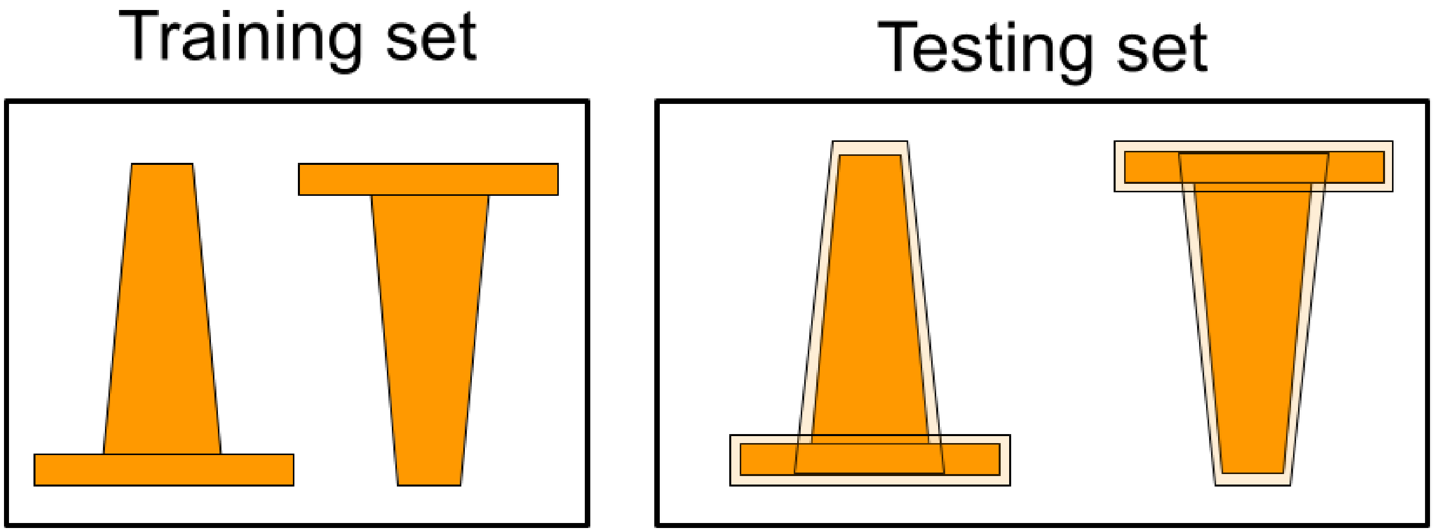


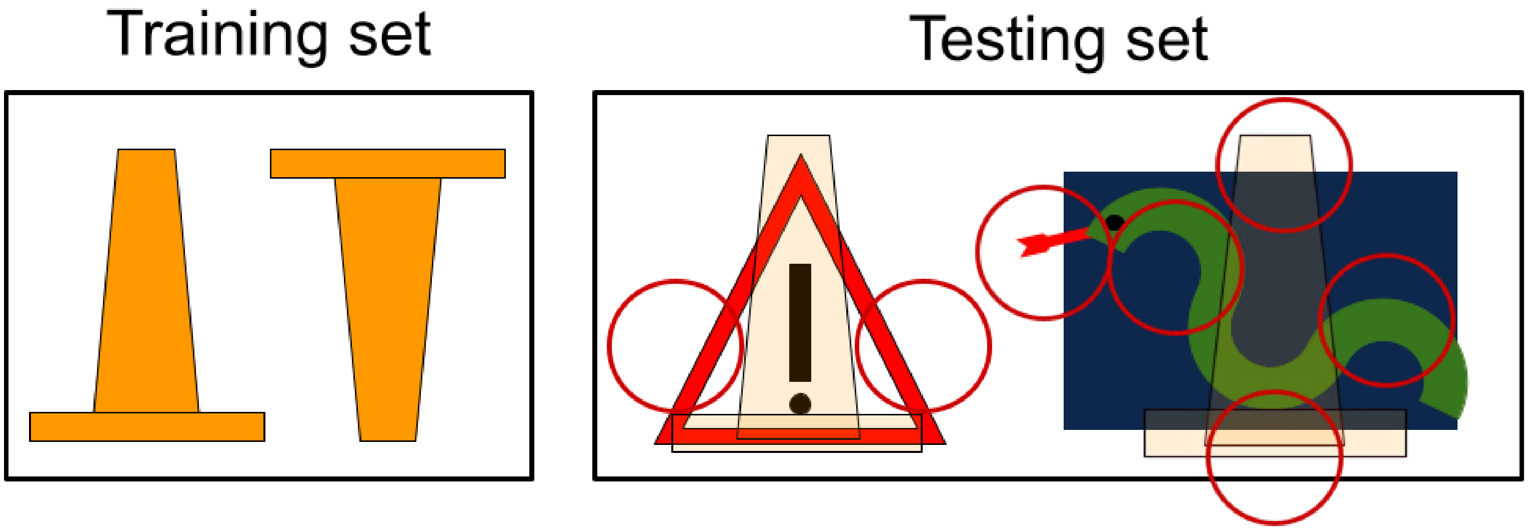
Efficiency



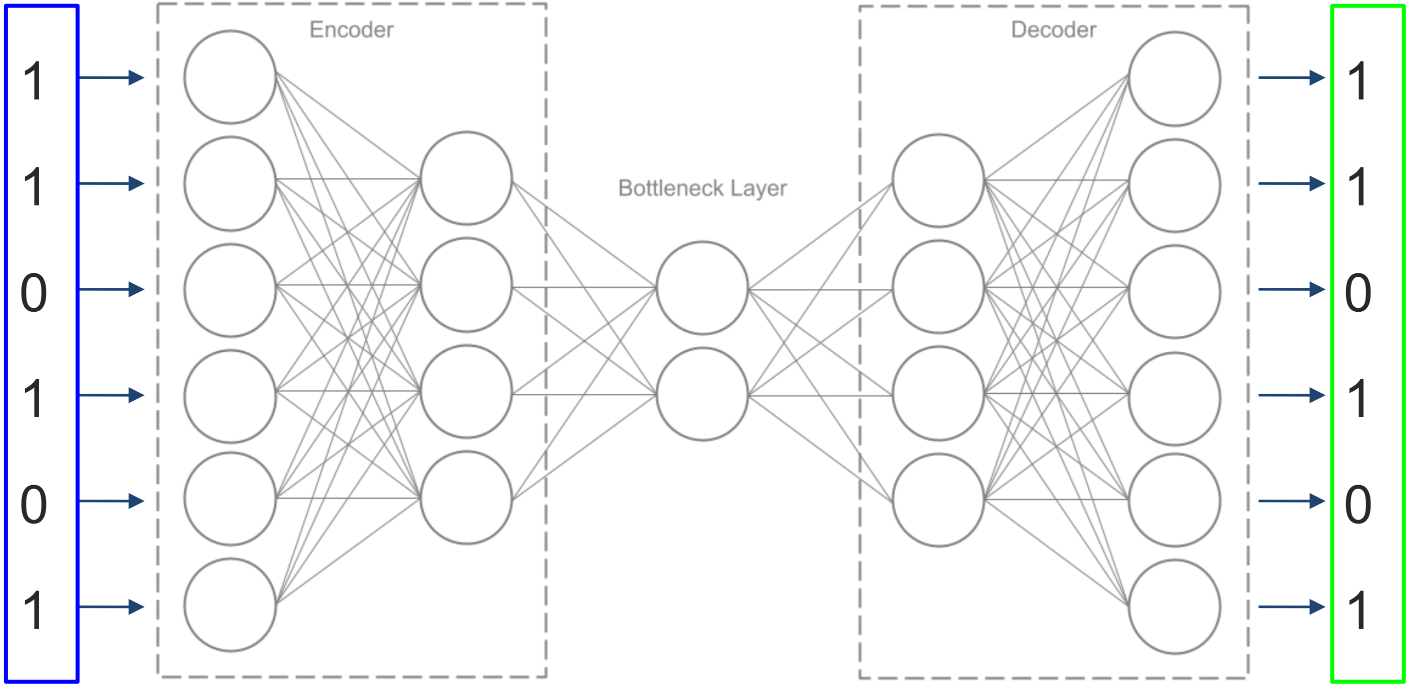
Auto Encoders

Deep learning method

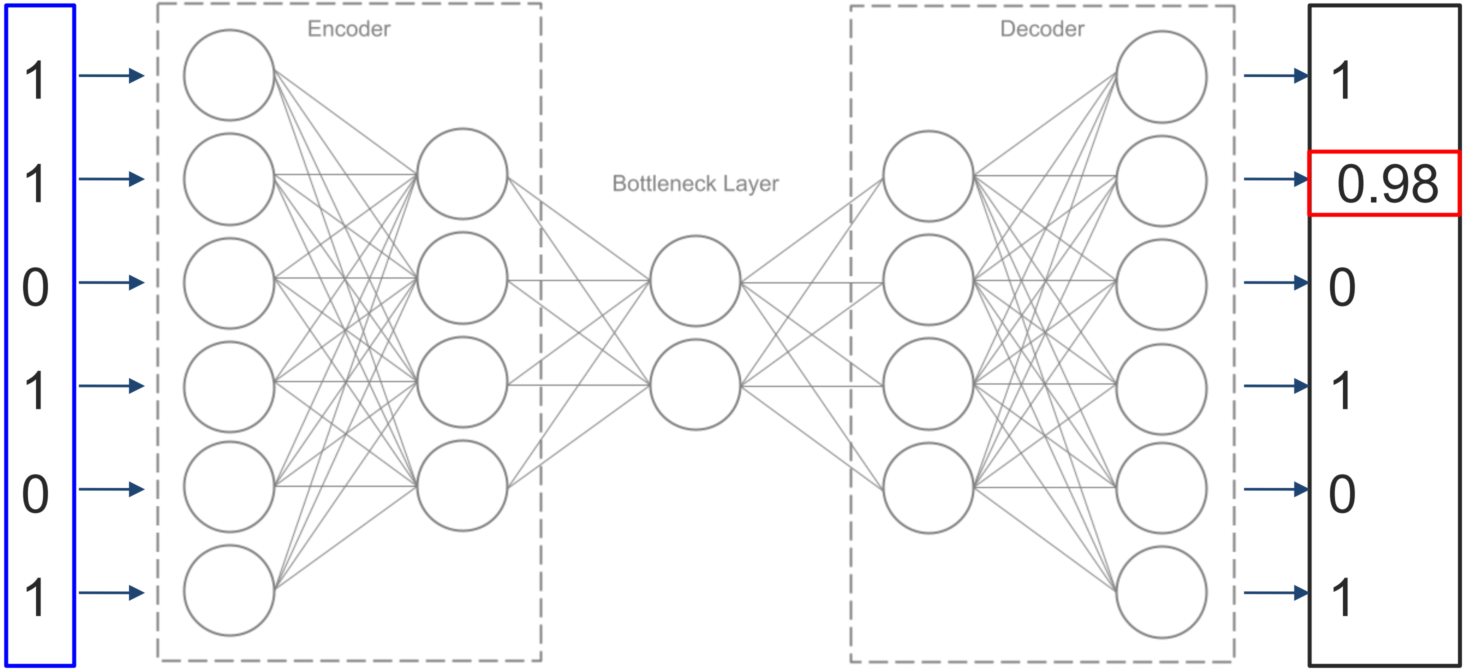

Training set
Testing set


Training set
Testing set

Correctly reconstructed

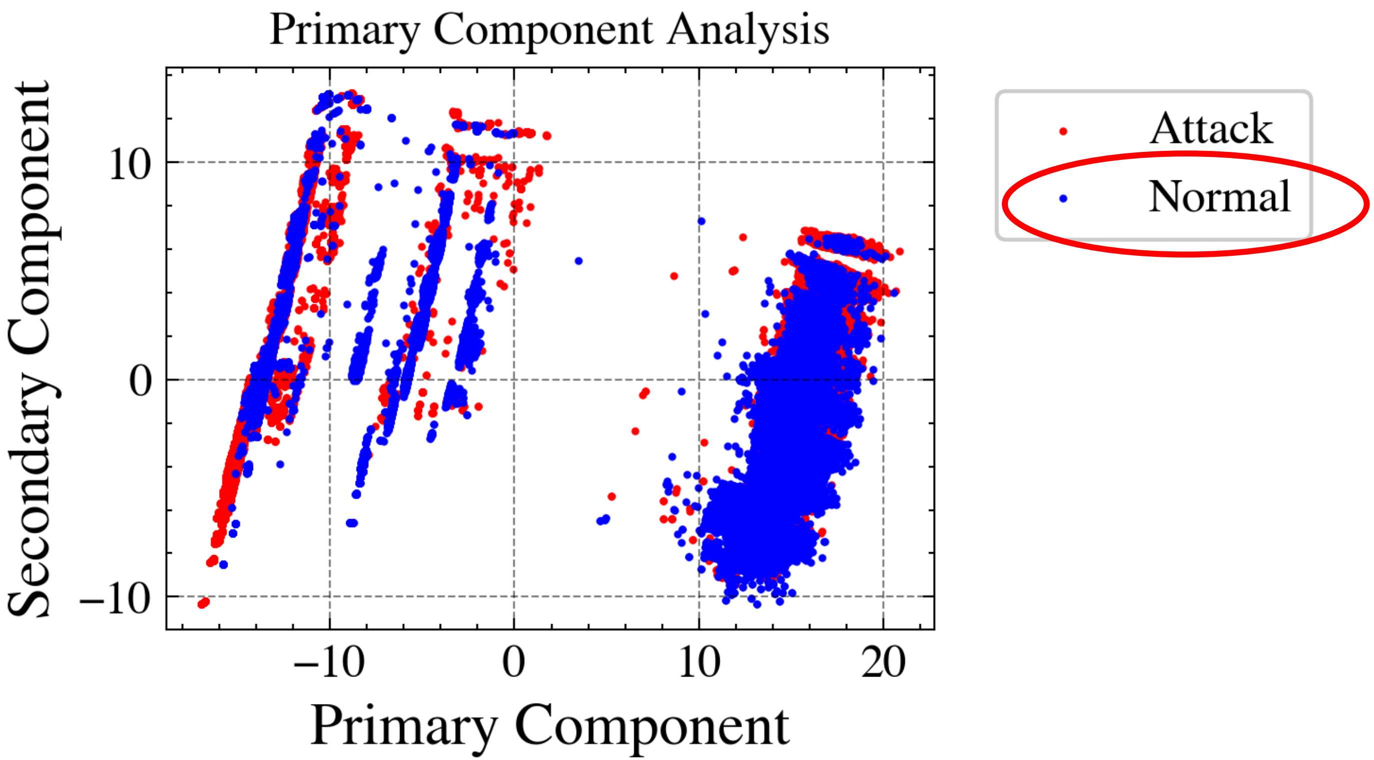


Reconstructed with error

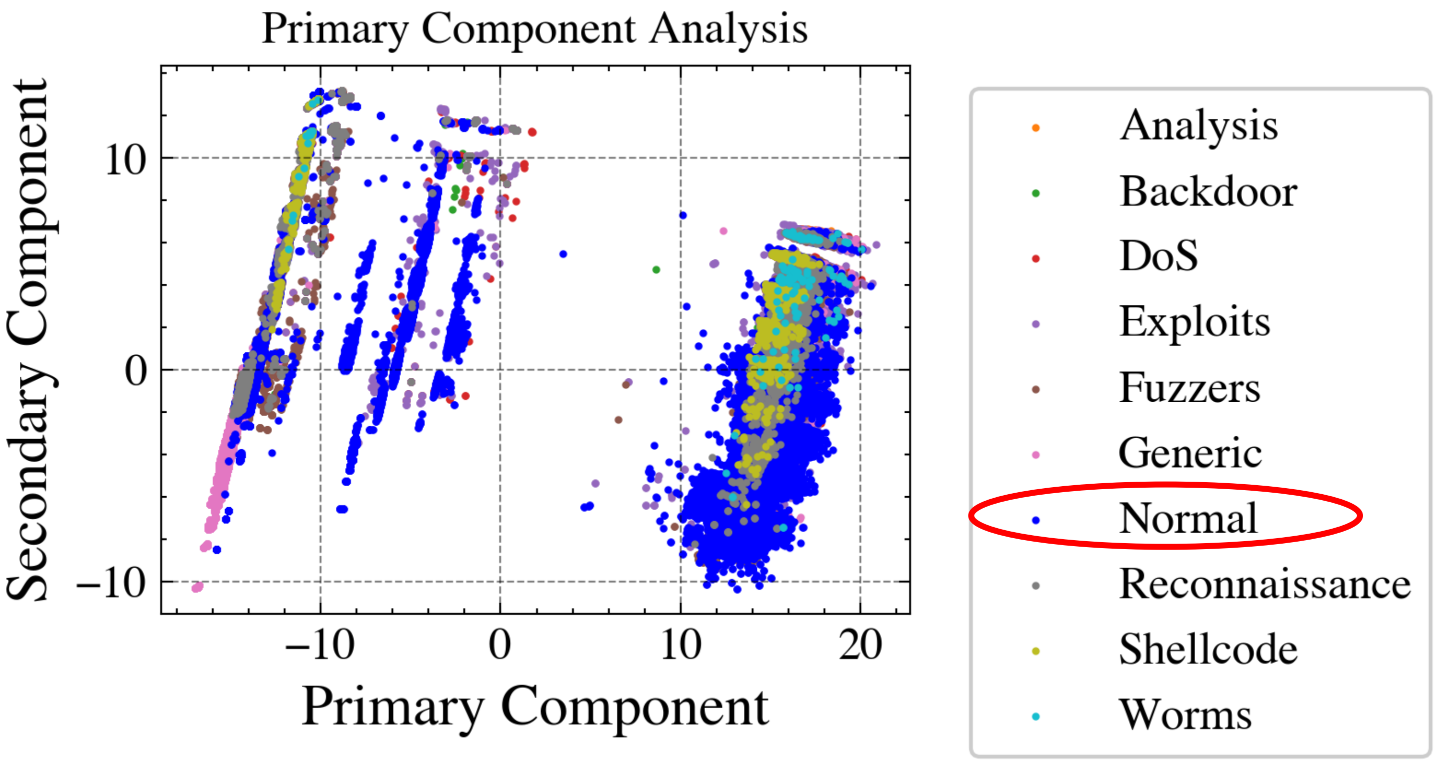


How can we use this for network data?

UNSW NB15 - All data

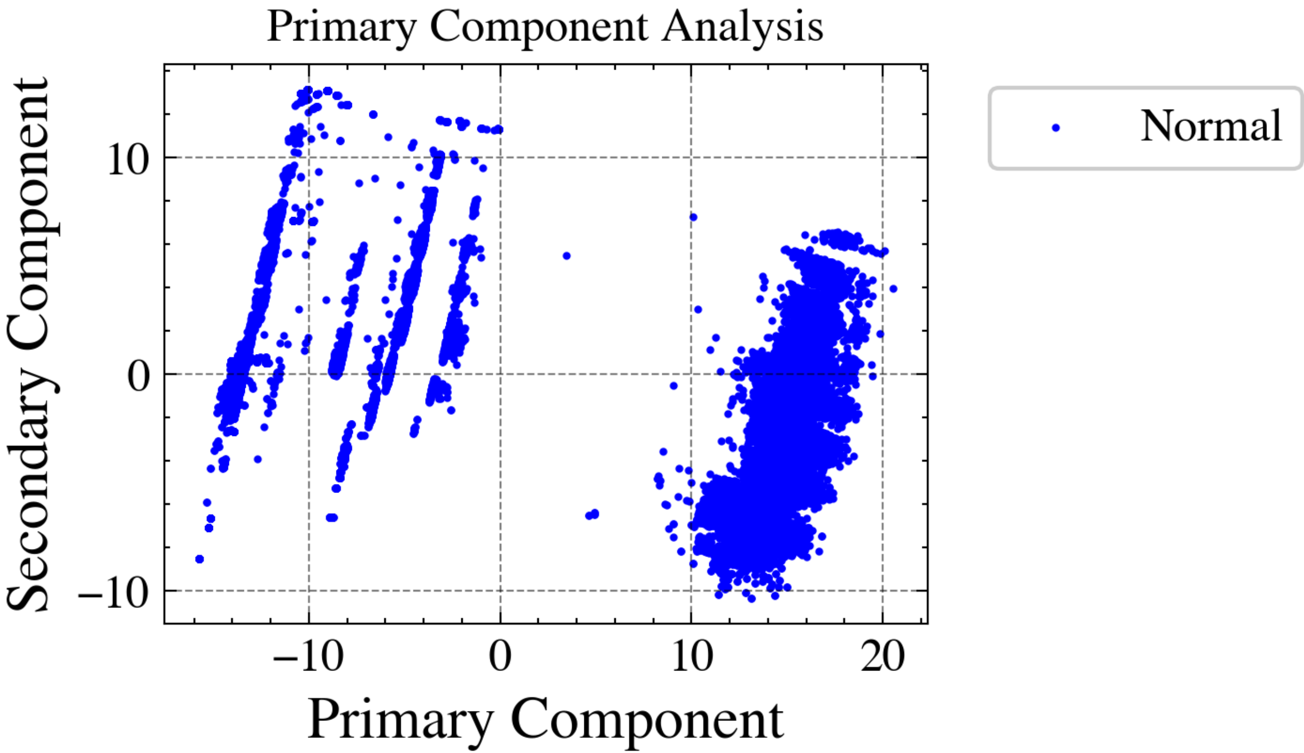


UNSW NB15 - All data



How does ML find the Attacks?

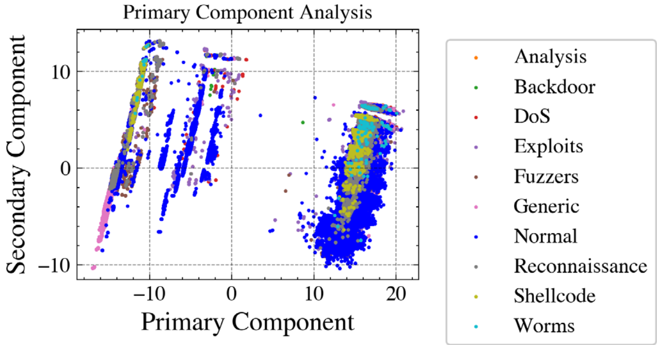
UNSW NB15 - All data

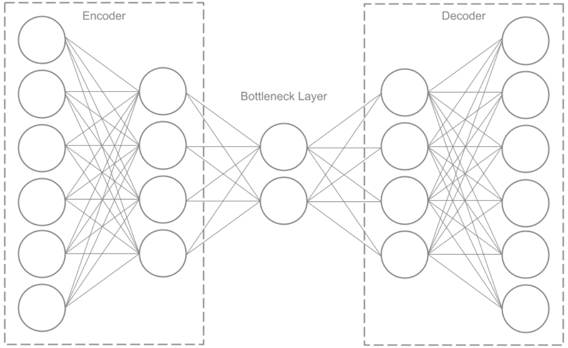


Training

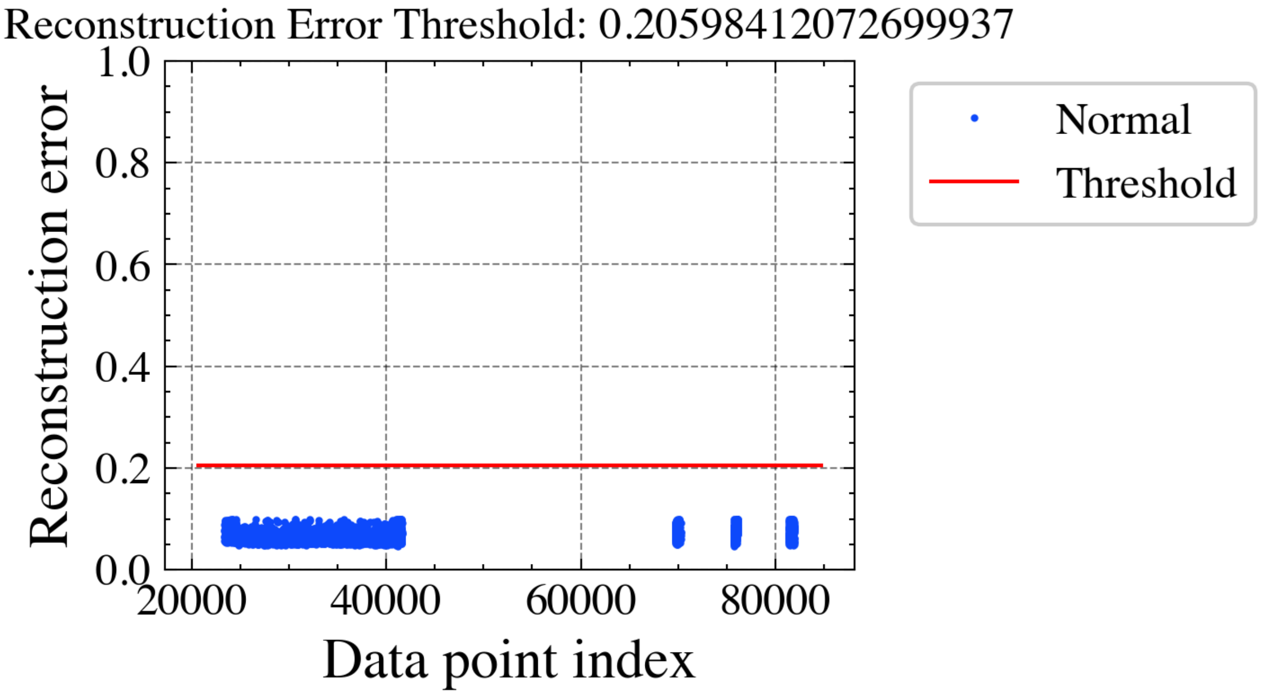

Primary Component Analysis
Secondary Component
Primary Component
10
0
−10
−10
0
10
20
Normal
Encoder
Bottleneck Layer
Decoder

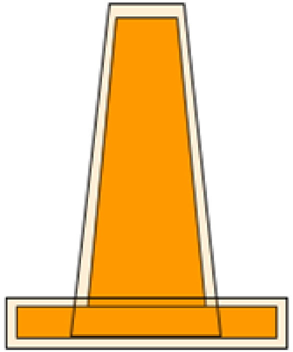
Training


Primary Component Analysis
Secondary Component
Primary Component
10
0
−10
−10
0
10
20
Analysis
Backdoor
DoS
Exploits
Fuzzers
Generic
Normal
Reconnaissance
Shellcode
Worms

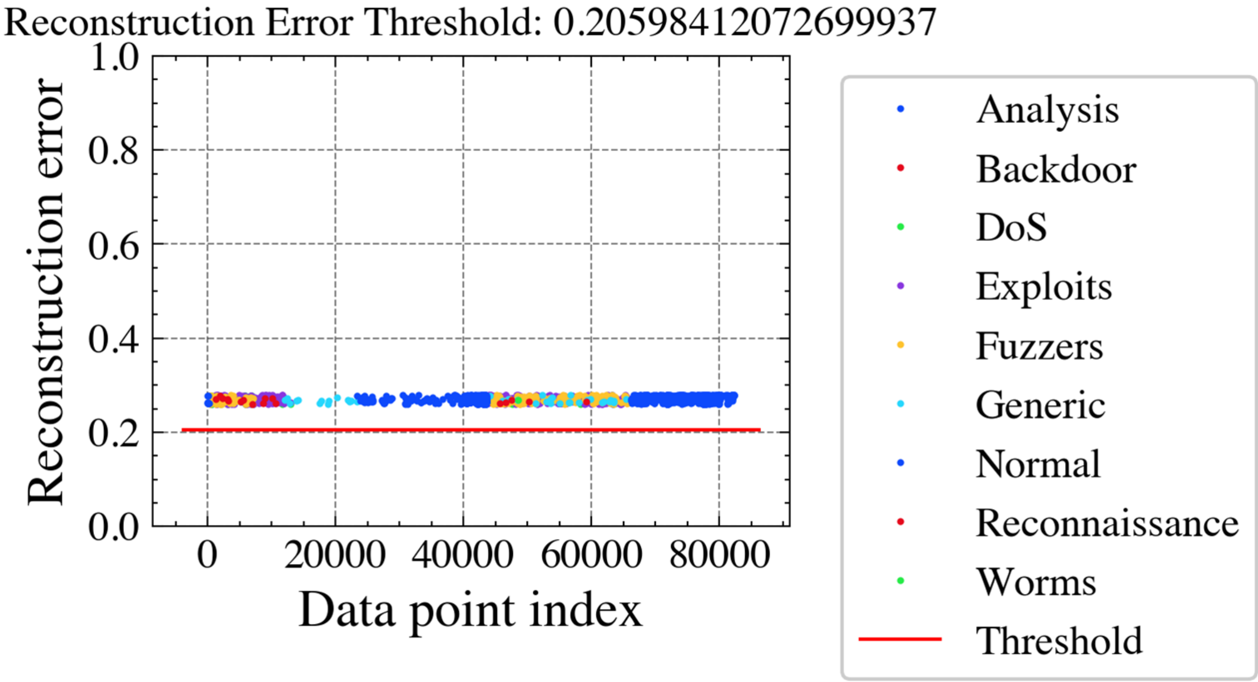

Encoder
Bottleneck Layer
Decoder

Low Reconstruction error

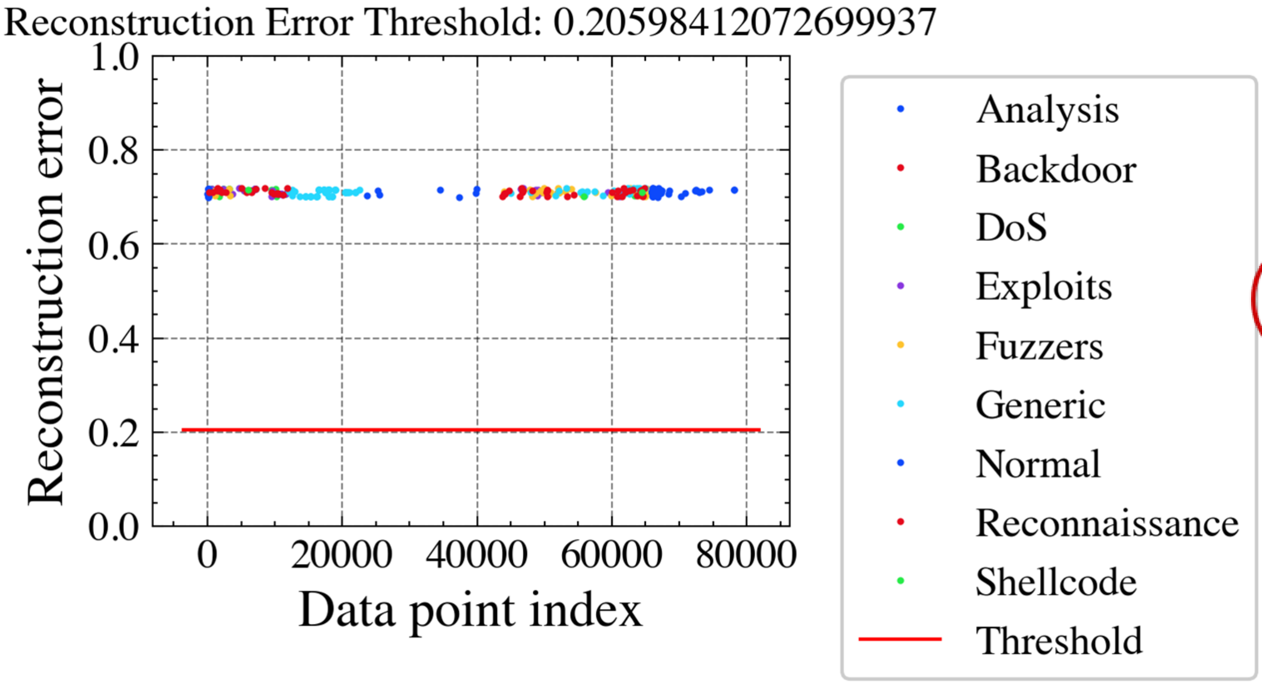


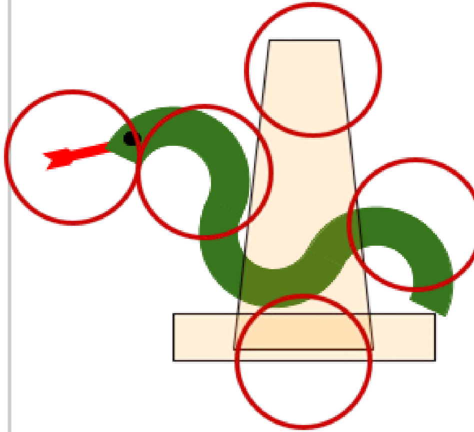


Medium Reconstruction Error

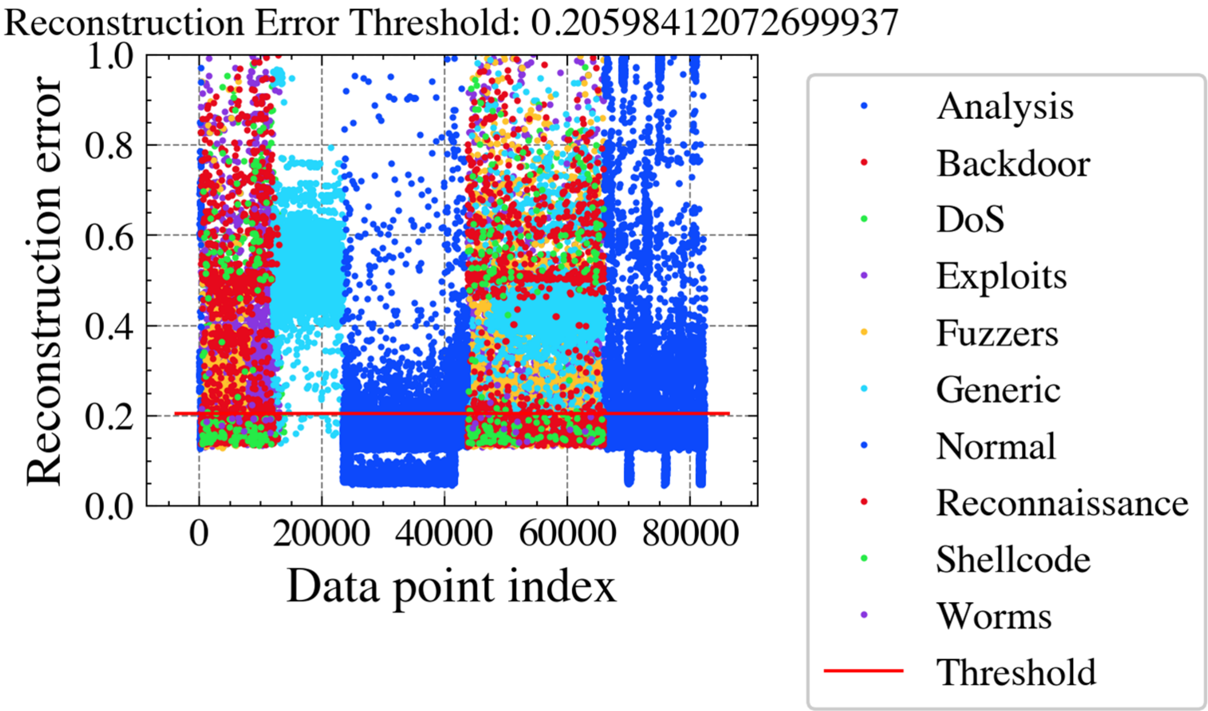


High reconstruction error





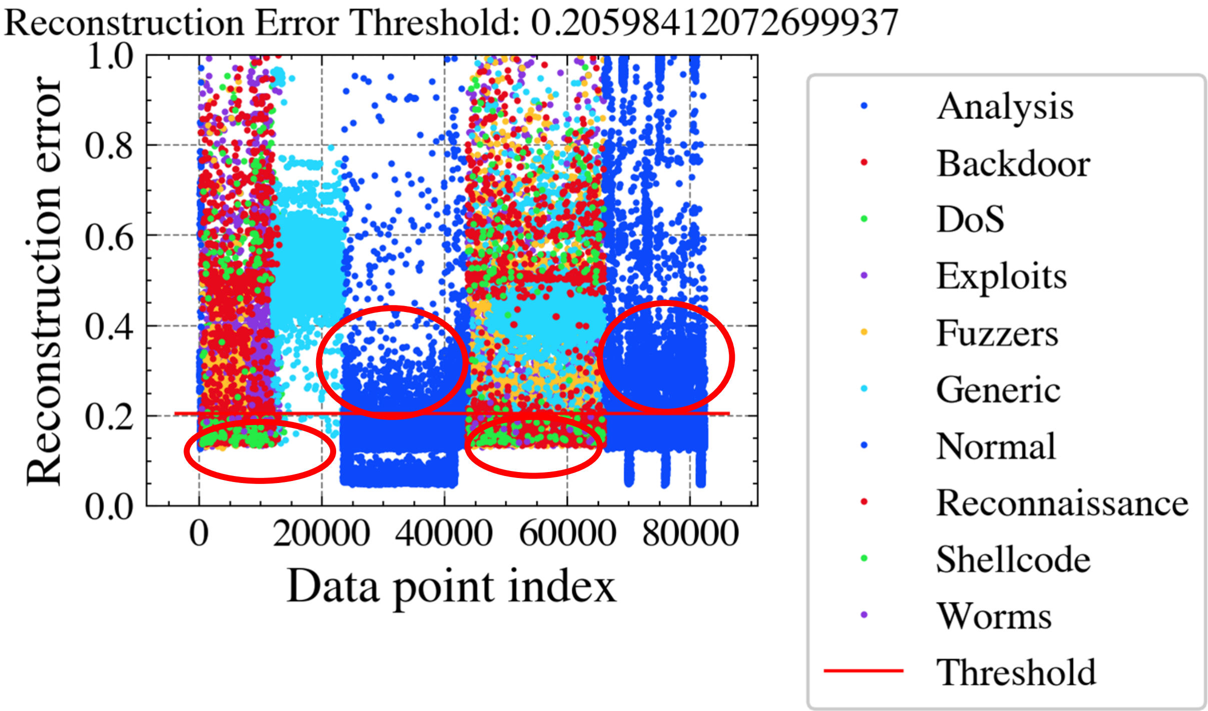
All reconstruction error



The problem of anomaly based detection

Large number of False Positives

All reconstruction error

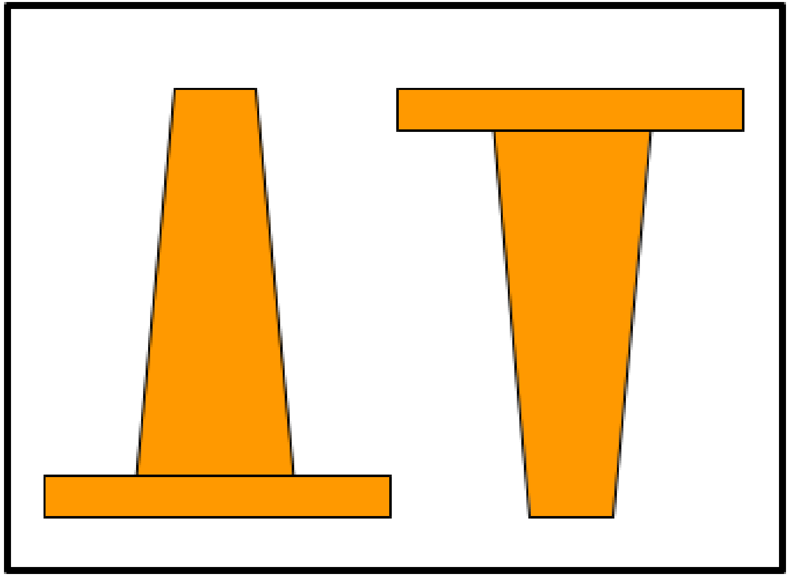


How can we Improve?

Split data on application level services

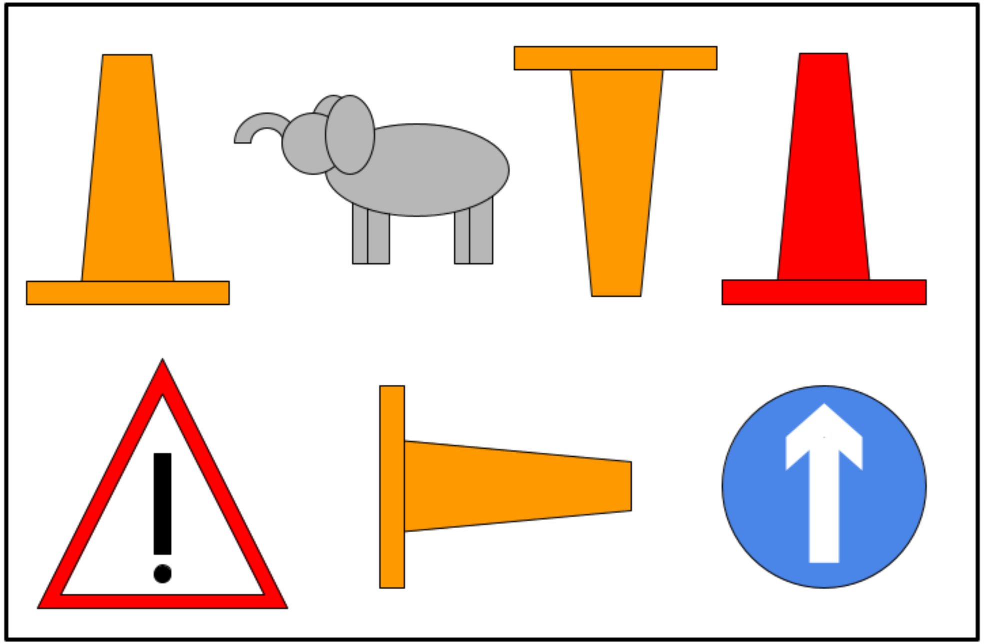
Ideal situation

Training set



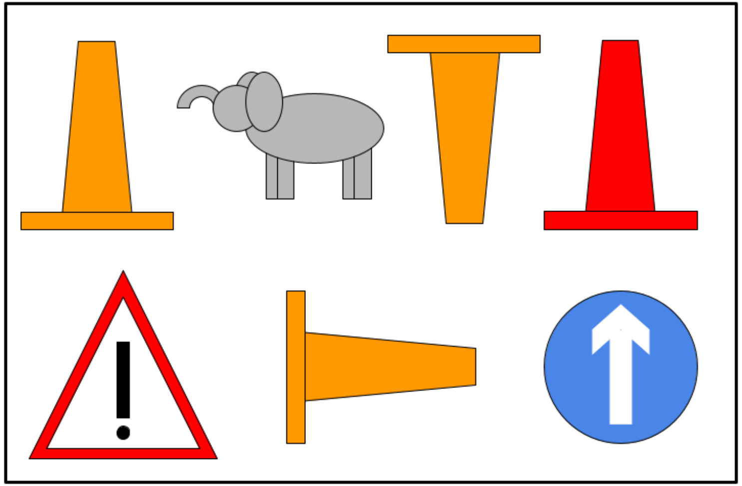
Actual situation

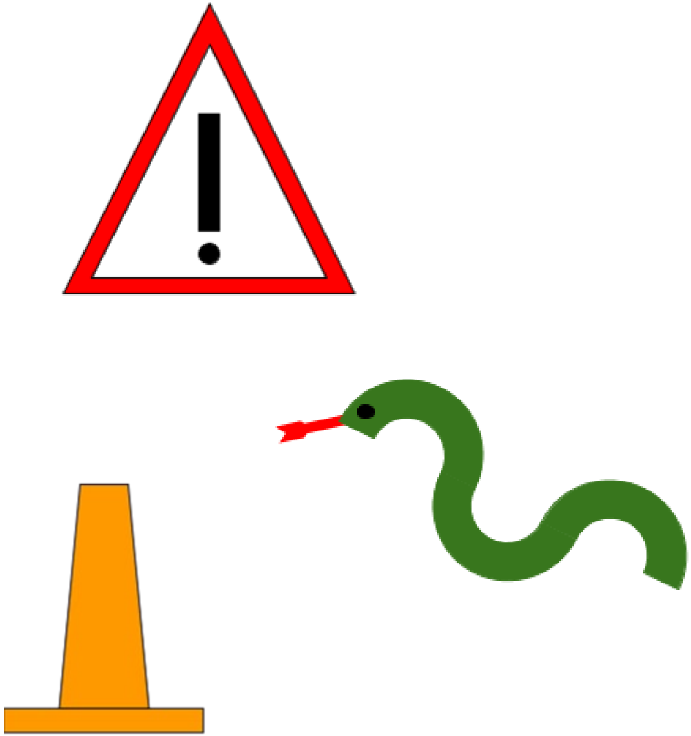
Training set



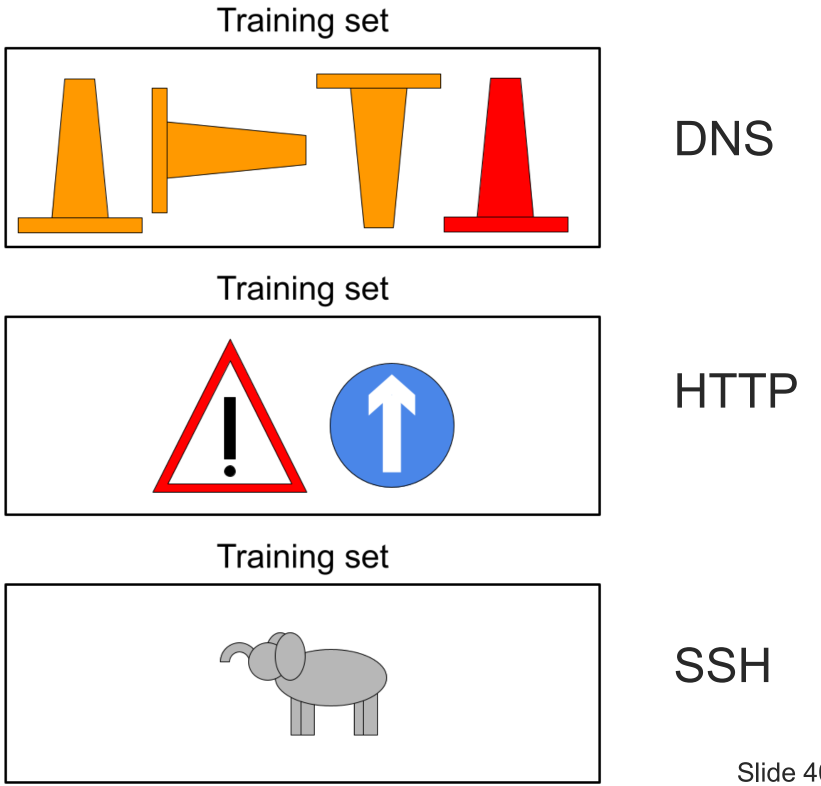
Actual situation

Training set

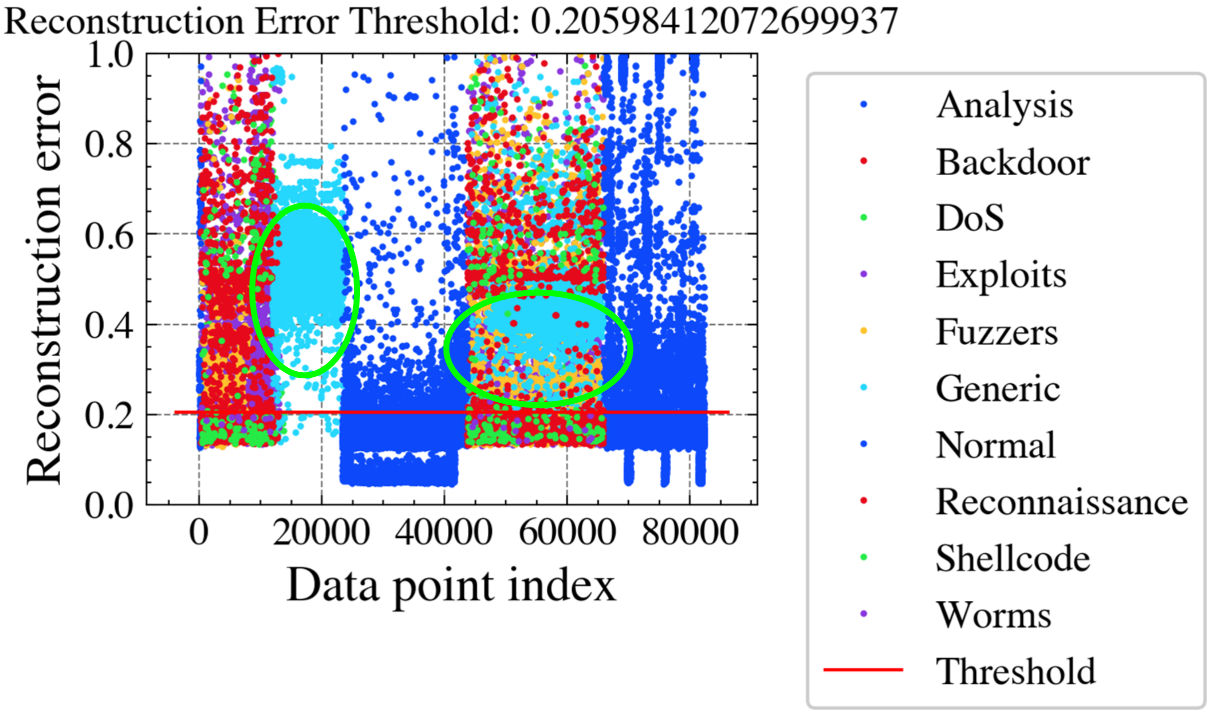




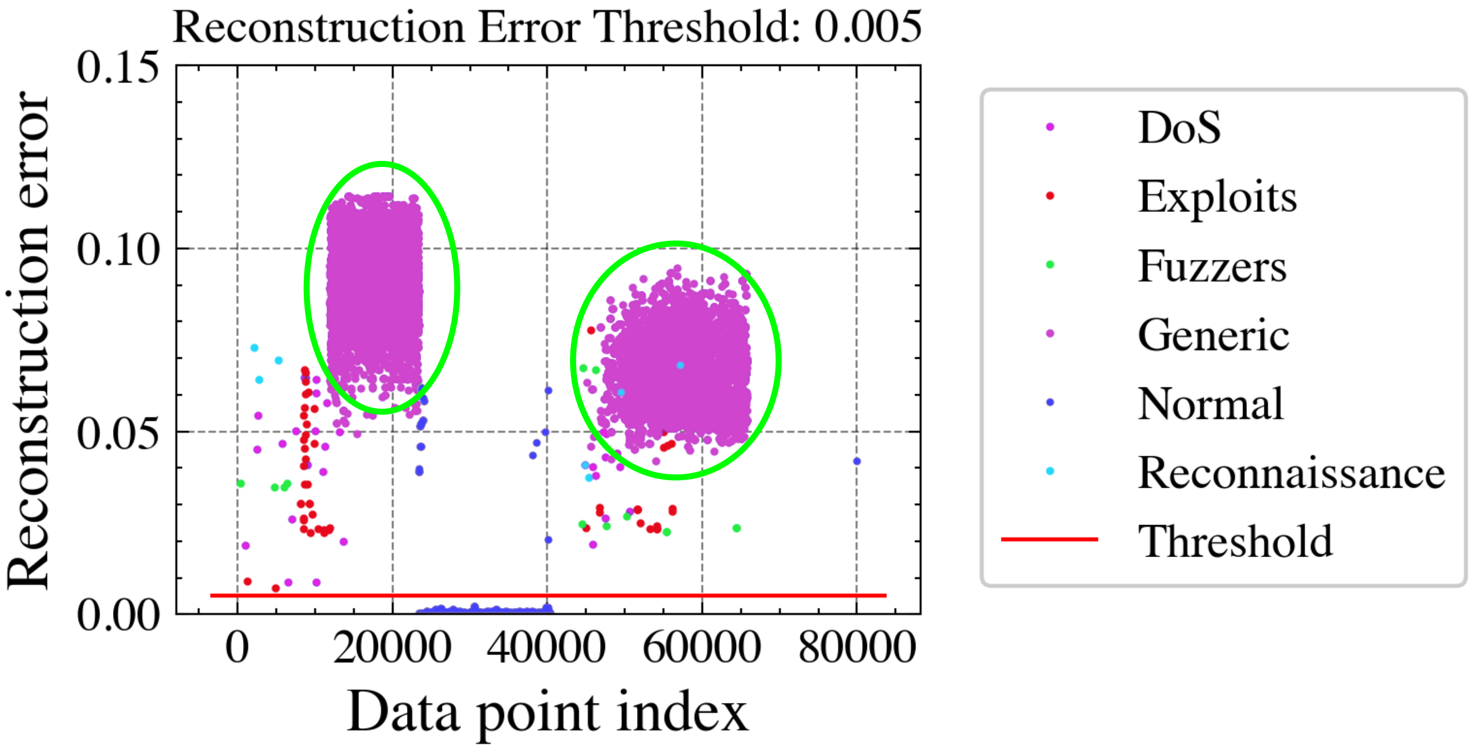
Proposed method



All reconstruction error

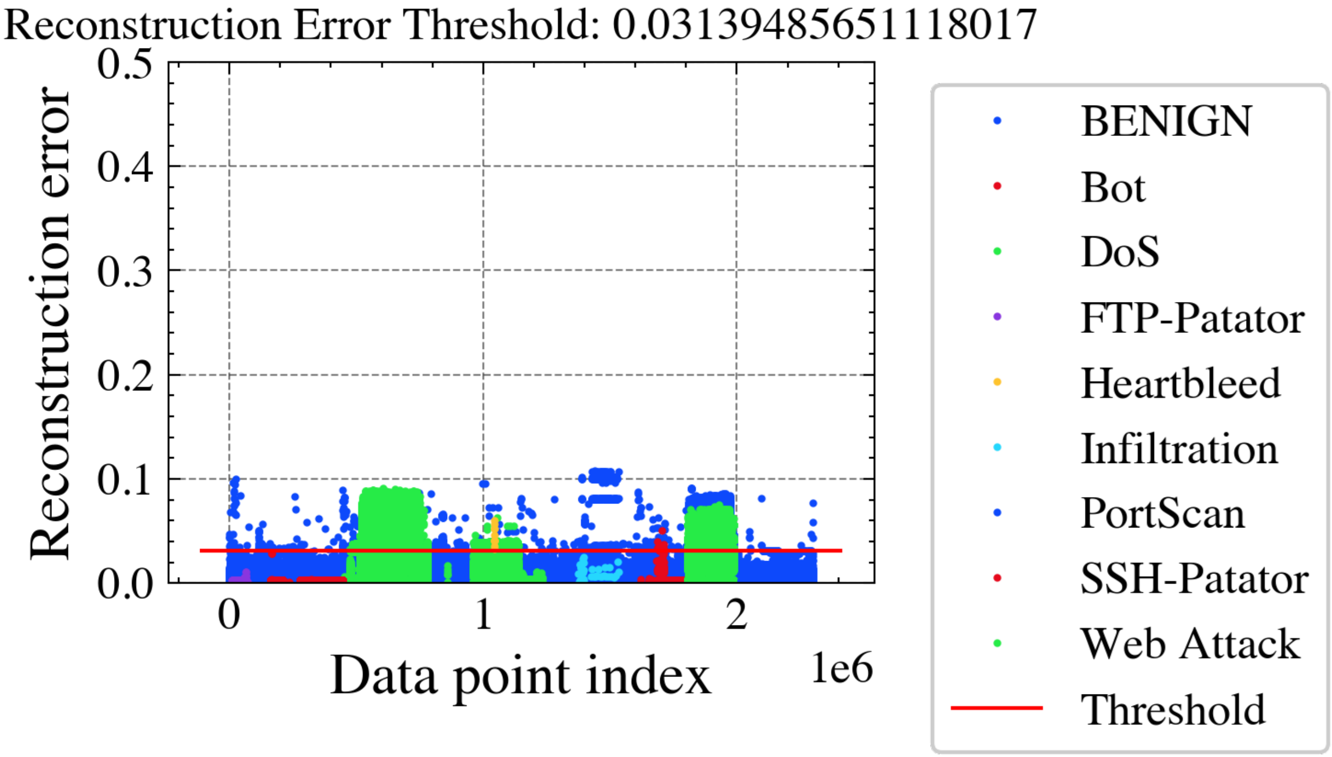


UNSW NB15 - DNS

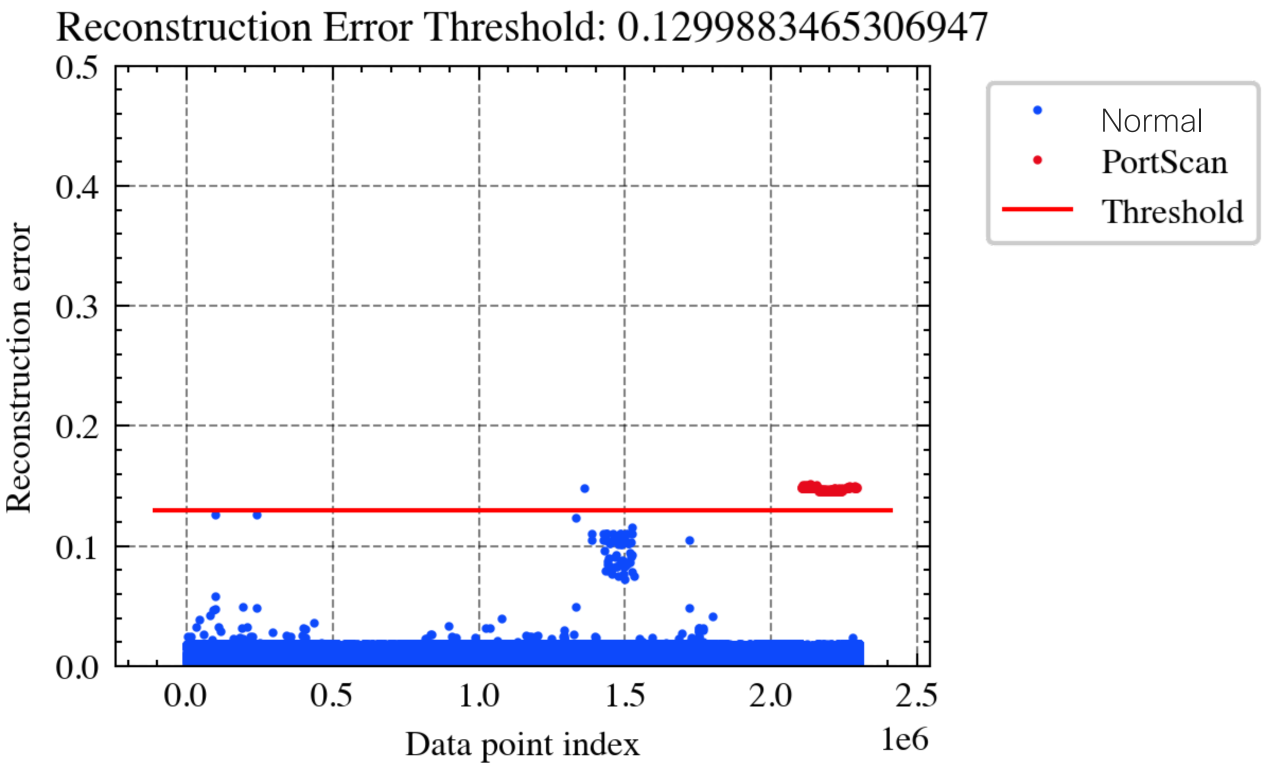


Does it work on every dataset?

CICIDS 2017 - All Data



CICDIDS 2017 – Port 53

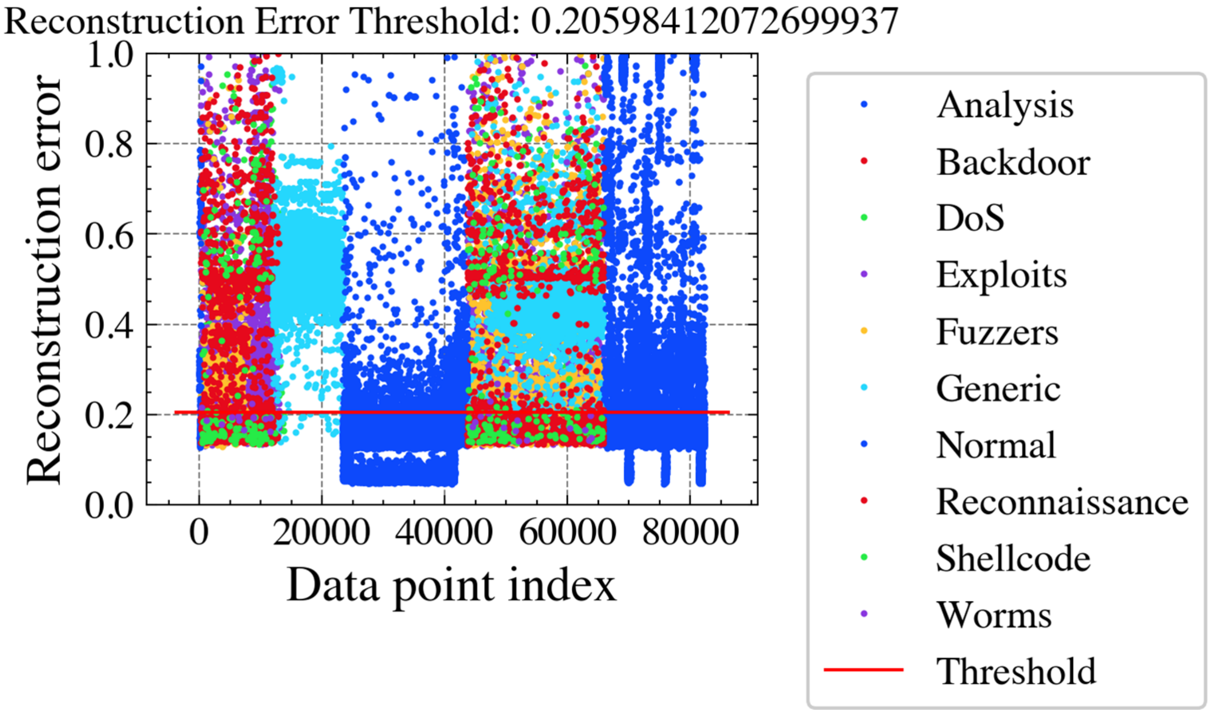


 Share experience. Build resilience.

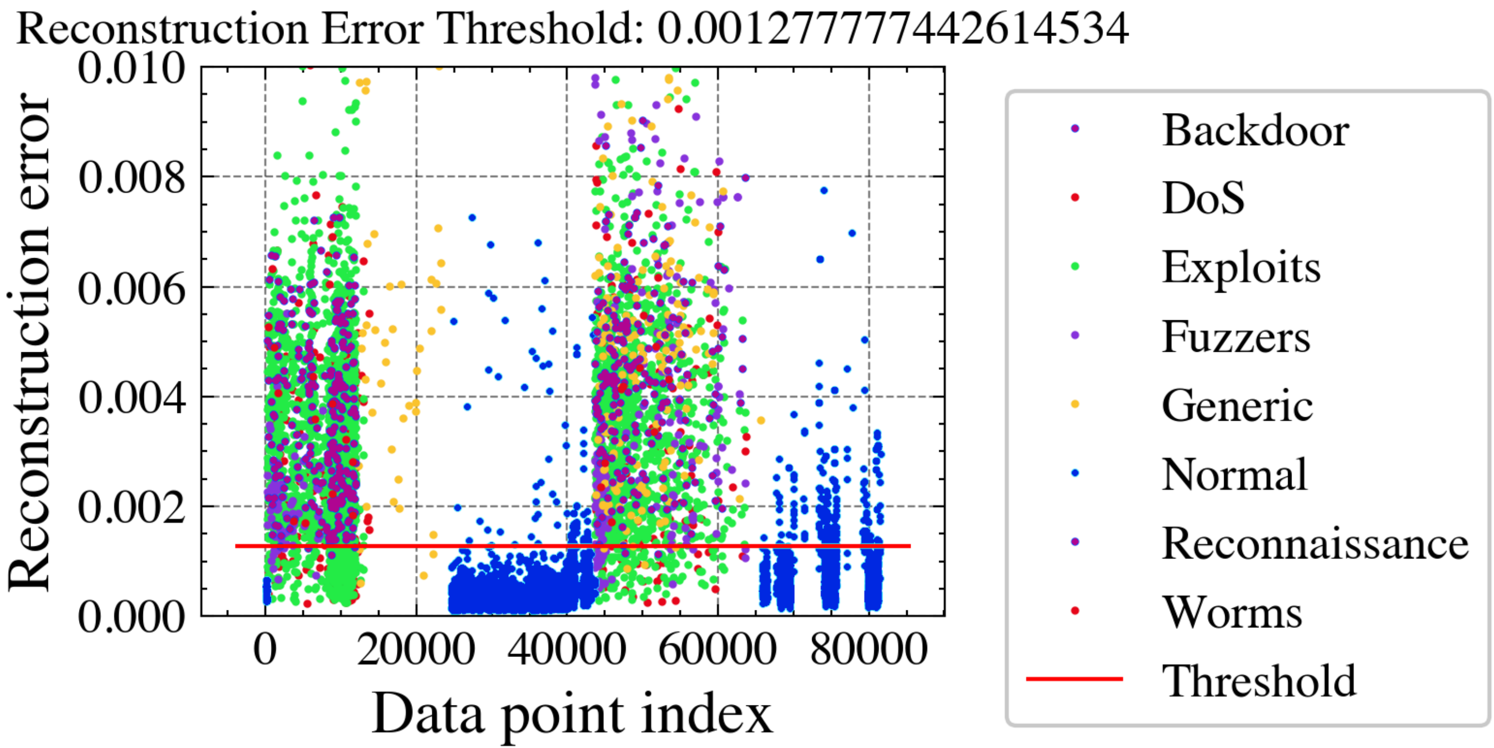
Class	Classified as Anomaly	Total	Percentage anomalies
Benign	1	743138	0.0001 %
Portscan	159	159	100 %

Does it work for every service split?

All reconstruction error

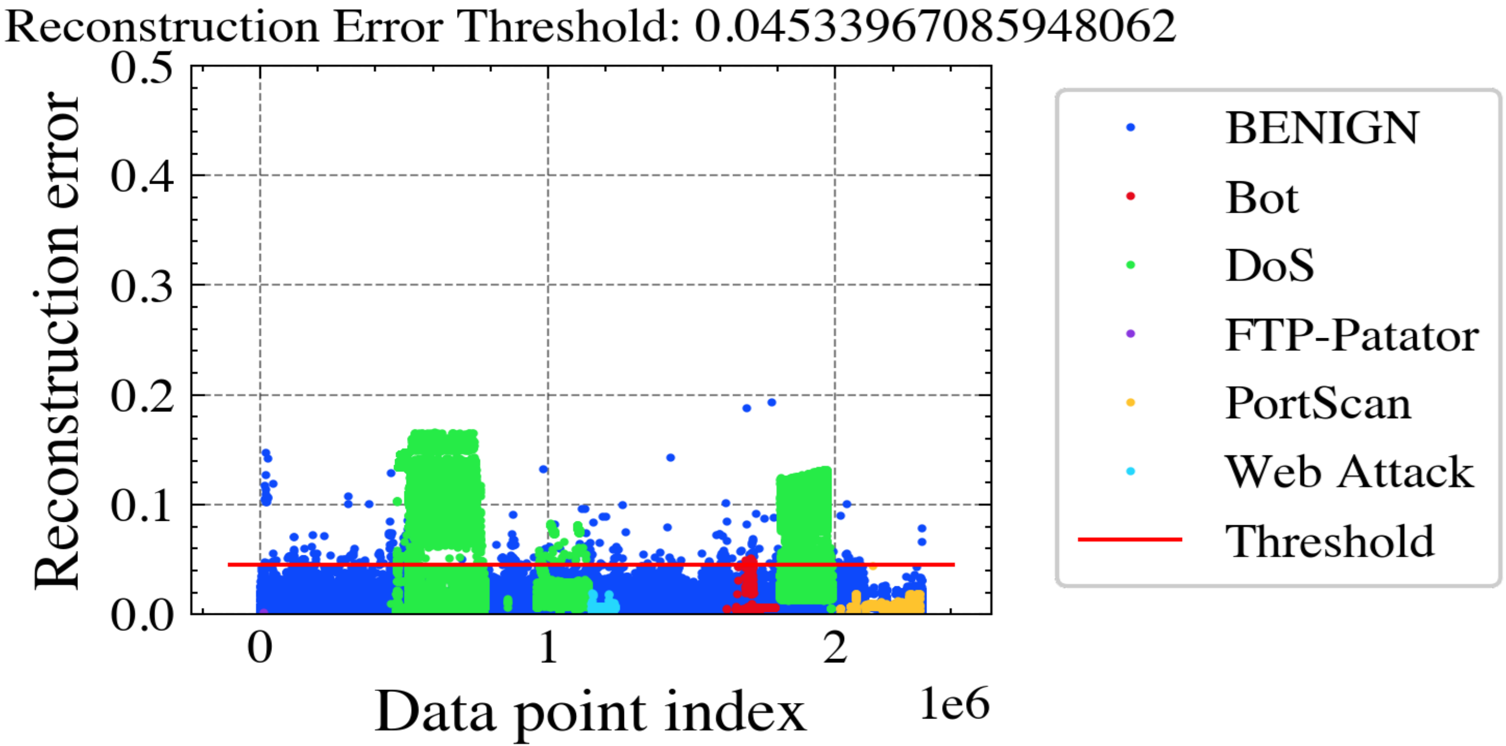


UNSW NB15 - HTTP



 Share experience. Build resilience.

CICIDS 2017 - HTTP



Improvements

	TPR	FPR
UNSW-NB15 All data	0.896	0.237
UNSW-NB15 Proposed Method	0.896	0.160
CICIDS 2017 All data	0.306	0.008
CICIDS 2017 Proposed Method	0.683	0.003

How can we create more representative results?

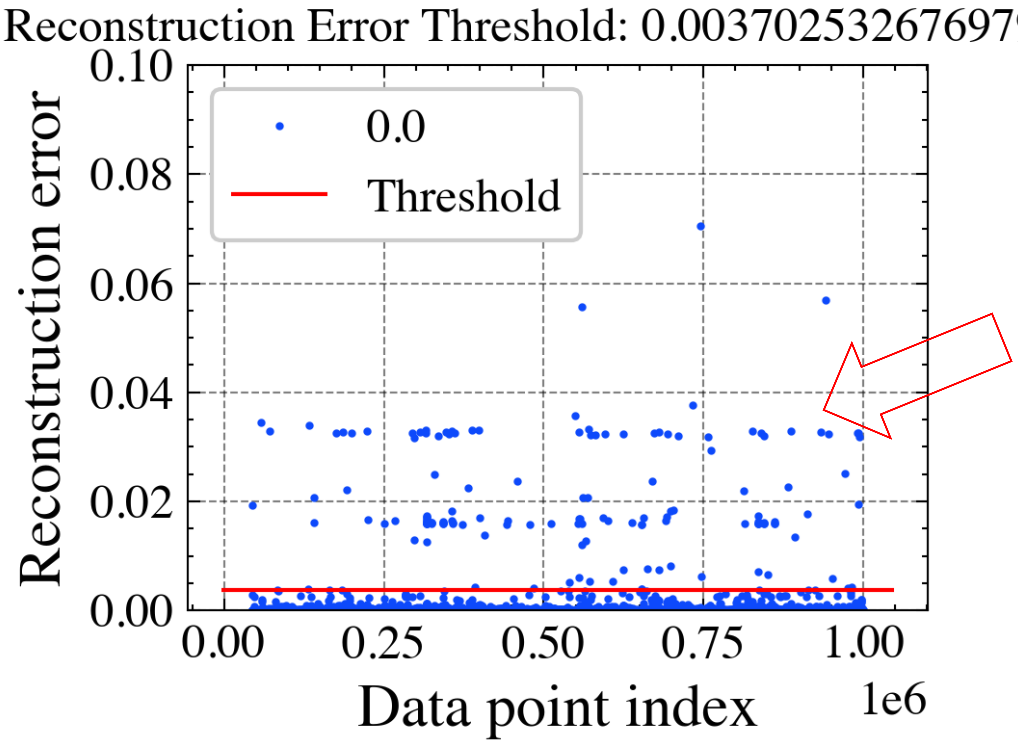
Real data

Captured in a commercial NIDS

Database sizes

	CICIDS 2017	UNSW NB15	Our dataset
Timespan	5 days	2 days	4 hours
Amount of connections	2.830.743	2.540.047	4.604.988

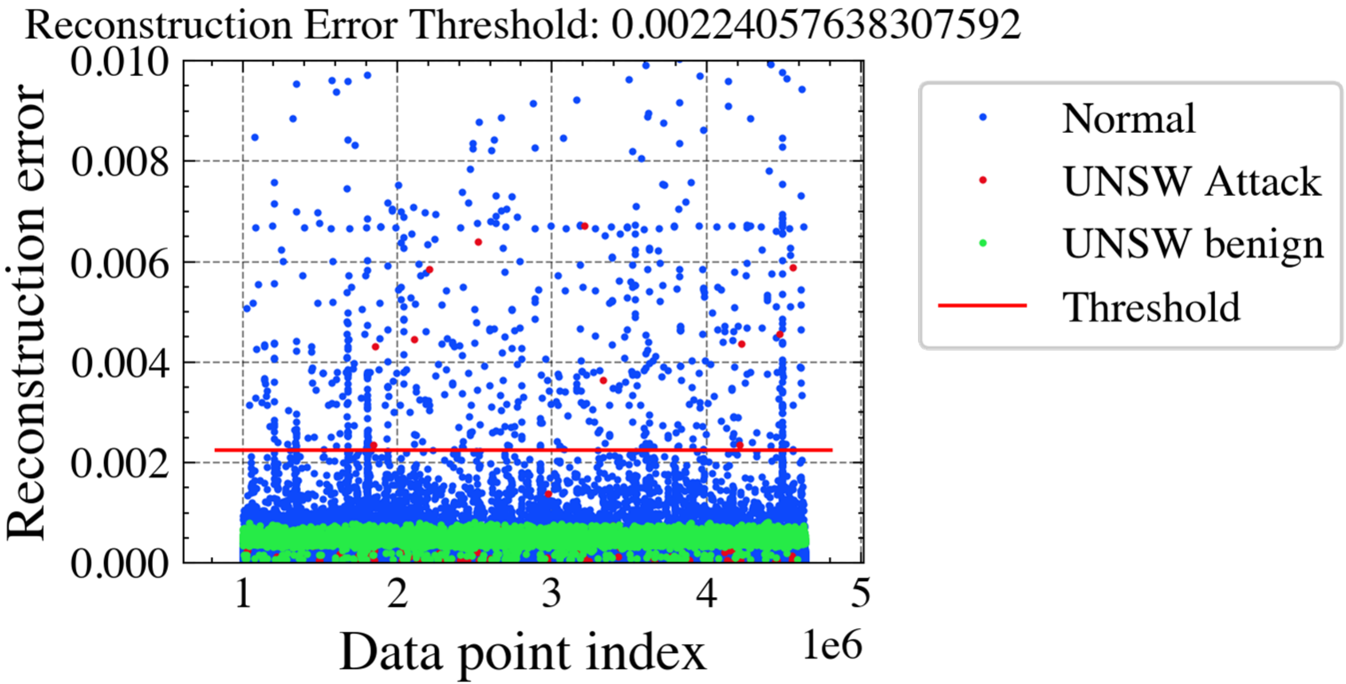
Real data - HTTP service - Only normal data



Attacks?

How can we verify the performance?

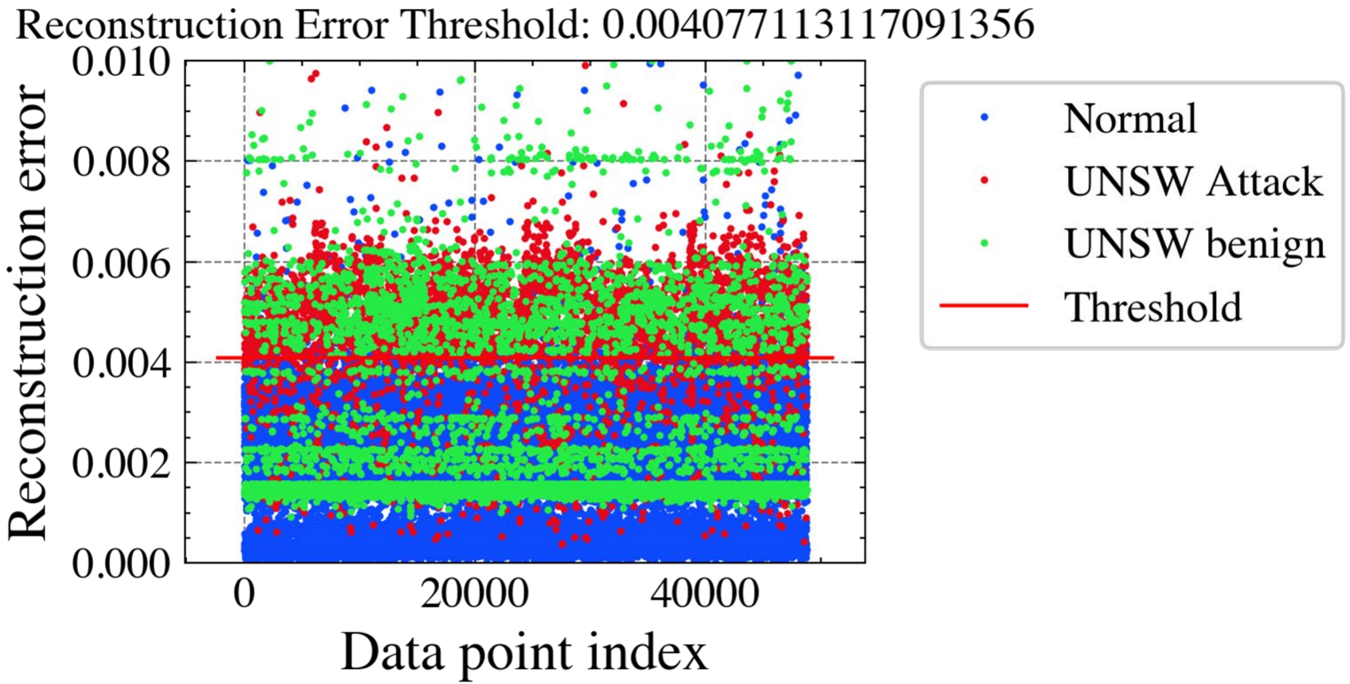
Real data - DNS with UNSW-NB15 attacks



Real data - DNS with UNSW-NB15 attacks

	Percentage detected as Anomaly
Real data	0.1 %
UNSW dataset Attack	54 %
UNSW dataset Normal	0 %

Real data - HTTP with UNSW NB15 attacks



Real data - HTTP with UNSW NB15 attacks

	Percentage detected as Anomaly
Real data	3 % Likely attacks
UNSW dataset Attack	81 %
UNSW dataset Normal	27 %

Is it for practical use?

Real data - HTTP with UNSW NB15 attacks

	Amount of Anomalies	Percentage detected as Anomaly
Real data	1000	3 %
UNSW dataset Attack		81 %
UNSW dataset Normal		27 %

Likely attacks

Ip addresses with more than 10 detections

ID	IP Address	Anomaly Count	Anonymized	Cause
1	175.45.176.2	1374	No	UNSW attack
2	175.45.176.3	1100	No	UNSW attack
3	175.45.176.0	839	No	UNSW attack
4	175.45.176.1	816	No	UNSW attack
5	59.166.0.5	723	No	UNSW benign
6	59.166.0.7	665	No	UNSW benign
7	59.166.0.8	648	No	UNSW benign
8	134.32.95.87	225	Yes	Known anomaly
9	134.32.95.115	130	Yes	Known anomaly
10	123.167.67.120	86	Yes	Known anomaly
11	123.167.67.222	30	Yes	No information
12	13.139.58.167	20	Yes	Known Malicious IP
13	247.209.145.27	11	Yes	No information

11
/ 85

Community Score

11 security vendors flagged this IP address as malicious

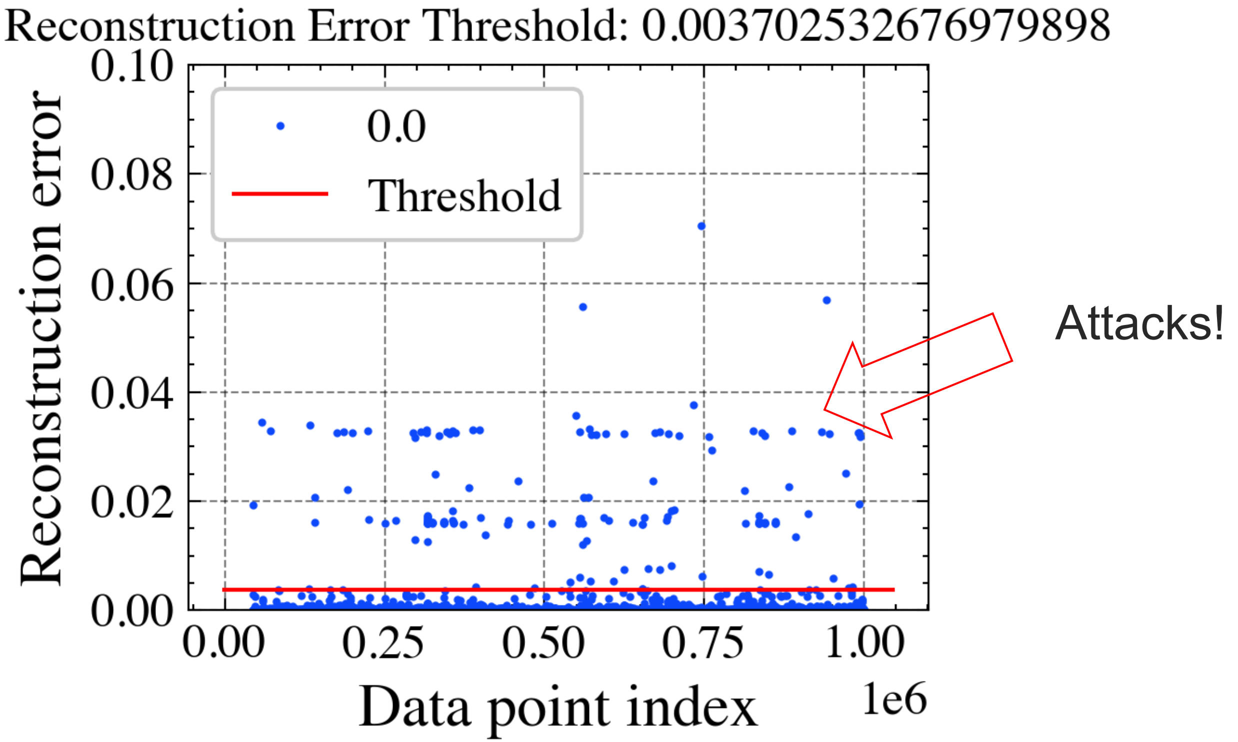
[redacted]

RU

DETECTION | DETAILS | RELATIONS | COMMUNITY 11

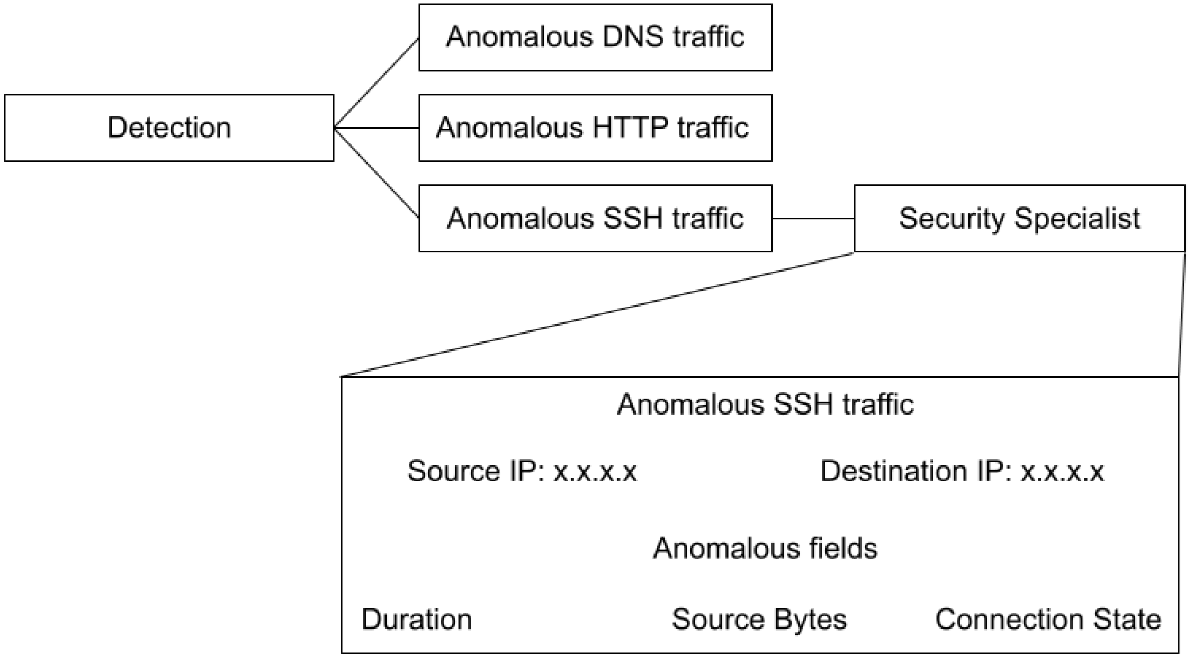
AlienVault	Malicious	Certego	Malicious
Comodo Valkyrie Verdict	Malicious	CRDF	Malicious
CyRadar	Malicious	EmergingThreats	Malicious
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
IPsum	Malicious	Kaspersky	Malware
Quttera	Malicious	Threatsourcing	Suspicious

Real data - HTTP service - Only normal data



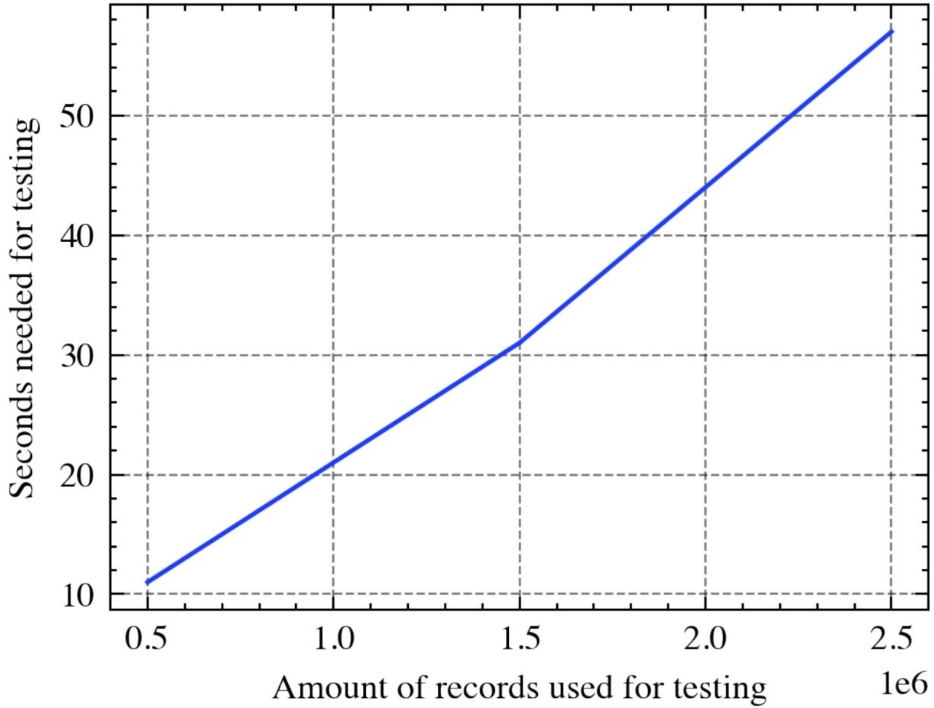
 Share experience. Build resilience.

Practical implementation



Is the efficiency high enough?

Testing times



Anomaly based

Improving Intrusion detection

Using ~~Machine Learning~~ For Practical Use

Auto Encoders

Unsupervised

Share experience. Build resilience.

Ask me anything

Share experience. Build resilience.

SECCON-NL 2022

Share experience. Build resilience

Time	Main stage (Zilversmederij 300 seats)	Breakout room 1 (Penningzaal 80 seats)	Breakout room 2 (Depot 80 seats)	Breakout room 3 (Stempelkamer 60 seats)	Breakout room 4 (Schatkamer 30 seats)
09:00 - 10:00	Opening Keynote Sadie Creese (Professor Cybersecurity @ Oxford University)				
10:00 - 10:15	Break - switch to main stream				
10:15 - 10:45	Threat Intell	Threat Intel	Post Quantum Security	Threat Intel	AI
	Threat Intel update from Talos - Martin Lee (Talos Threat intelligence organization)	No More Leaks Project - Felix Nijpels (Dutch Police)	The Impact of Quantum on security - a general outlook - Sam Samuel (Cisco)	Threat managemen at the Dutch Railway - Dimitri van Zantvliet Rozemeijer (Chief Cyber Dutch Railway)	Get ready for the AI attack bot - Richard de Vries (Tata Steel)
10:45 - 11:00	Break - switch to main stream				
11:00 - 11:30	Detection and Response	SOAR	Post Quantum Security	Detection and Response	Detection and Response / AI
	Day in life at the Dutch Tax Office SOC - Karl Lovink (Belastingdienst)	Stay Ahead of the Game: Automate your Threat Hunting Workflows - Christopher van der Made (Cisco)	Quantum hurdles: an optimistic view of post-quantum security - Sander Dorigo (Fox Crypto)	What Cyber can learn from Biology? - Koen Hokke (KPN)	Unsupervised Anomaly-Based Network Intrusion Detection Using Auto Encoders for Practical Use - Julik Keijer (Northwave)
11:30 - 11:45	Break - switch to main stream				
11:45 - 12:15	Detection and Response	Detection and Response	DevSecOps/ Detection and Response	DevSecOps	
	Compliancy vs security. Pentesting is dead - Edwin van Andel (ZeroCopter)	Incident Response without compromise. How to prepare for the worst day of your career with dice! - Wouter Hindriks (Avit)	Threat Modelling: it's not just for developers - Timothy Wadhwa-Brown (Cisco)	Changed responsibilities in modern software development environments - Martin Knobloch (Microfocus)	How to break a data center? Fred Streefland (Secior)
12:15 - 13:00	LUNCH				
13:00 - 13:45	Panel Discussion with Liesbeth Holterman (host CVNL) Koen Sandbrink (NCSC), Jochem Smit (Northwave), Oscar Koeroo (Min Ezk), Jan Heijdra (Cisco)				
13:45 - 14:00	Break - switch to main stream				
14:00 - 14:30	Threat intel / Detection and Response	Threat Intel	Detection and Response	DevSecOps	
	CERT in Ukraine exeperience sharing by Andrii Bezverkhyi (SOCPrime)	This is why you will fail: Most successful attack scenarios and their defenses - Tijme Gommers (Northwave)	Risk-based Auth & ZTA - Frank Michaud (Cisco)	Creating clarity and unity in security standards and guidelines - OpenCRE.org - Rob van der Veer (Software Improvement Group)	(Placeholder) WICCA Breakout (with Wendy joining)
14:30 - 14:45	Break - switch to main stream				
14:45 - 15:15	Detection and Response	Detection and Response	Detection and Response	Threat Intel	Detection and Response / AI
	Advanced Attacker Automation: Botnet capabilities and techniques used to evade your defences - David Warburton (F5)	Security Maturity: from XDR to SIEM - Gilles van Heijst (Orange Cyber Defense)	Improving Business Security by implementing Security.txt - Julius Offers (Digital Trust Center)	Tackling the challenge of translating threat intelligence into actual action - Raymond Bierens (Connect2Trust)	Fostering emerging technologies in cybersecurity, to reinforce our strategic autonomy.- Christian van der Woude (Dcypher)
15:15 - 16:00	Closing Keynote - Wendy Nather				

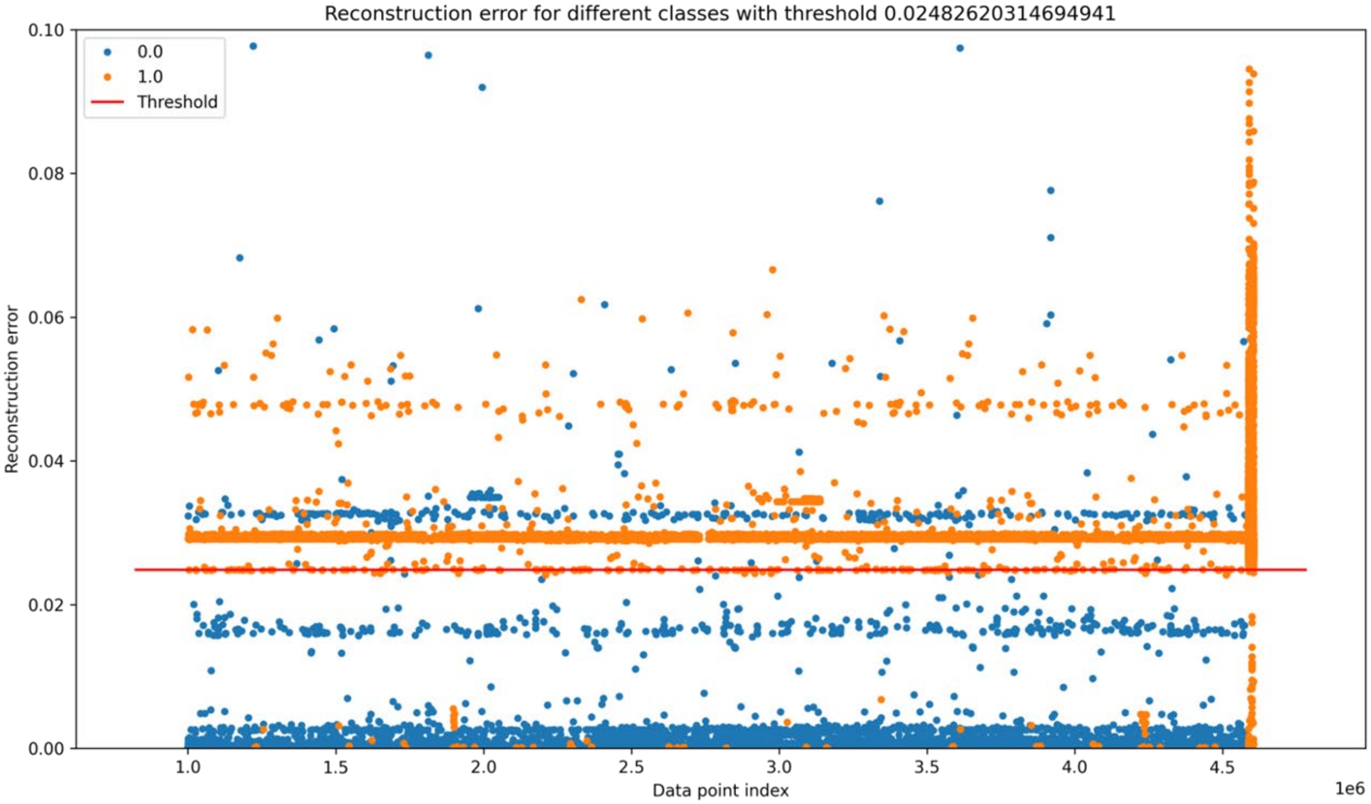
Confusion Matrix

		Actual	
		Attack	Normal
Predicted	Attack	True Positive (TP)	False Positive (FP)
	Normal	False Negative (FN)	True Negative (TN)

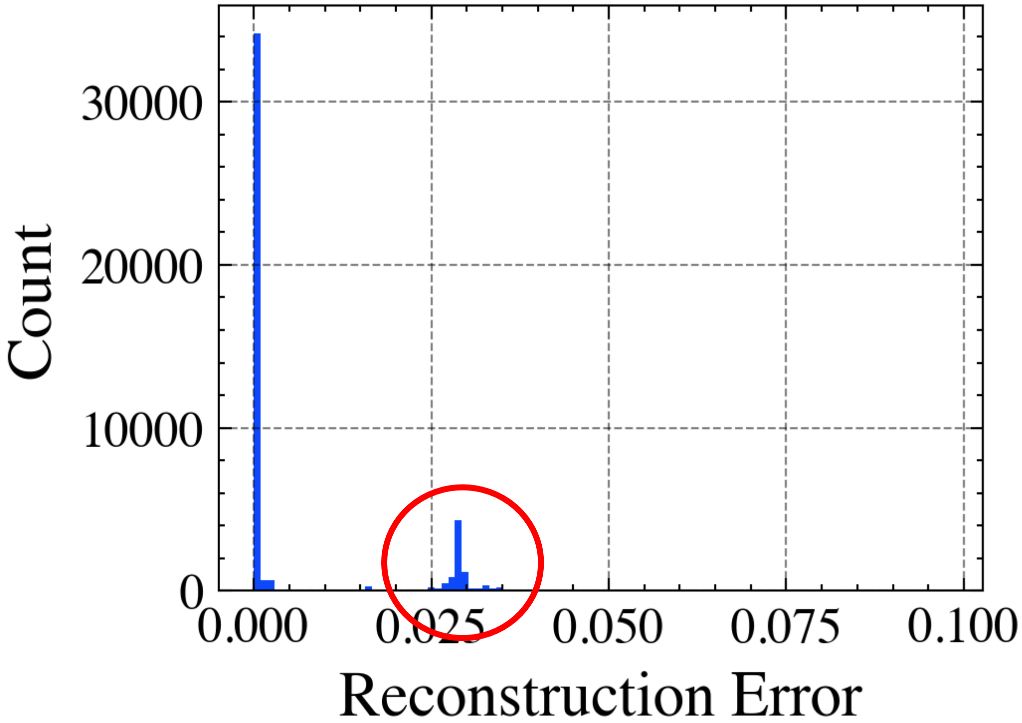
Future work

- Capture data over a longer time to collect real attacks
- Create better statistical features or connection correlations
- By using human security specialists, create a labeled dataset

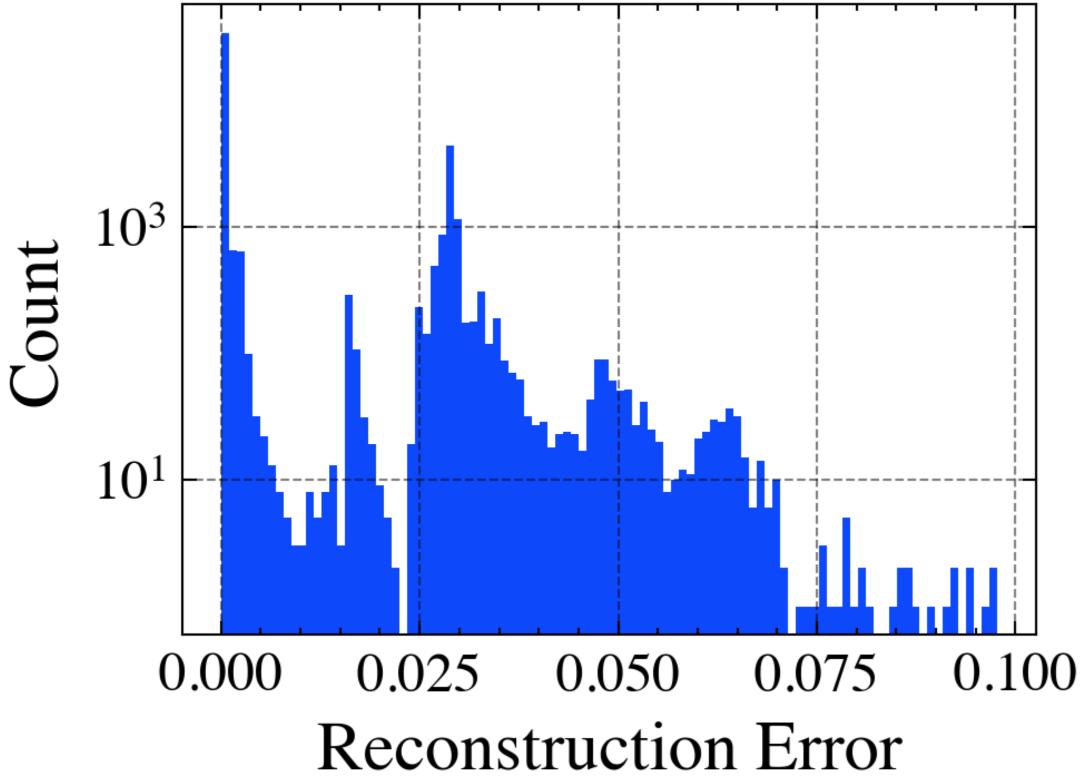
Our data - HTTP with UNSW NB15 attacks



Unsupervised thresholding



Unsupervised thresholding

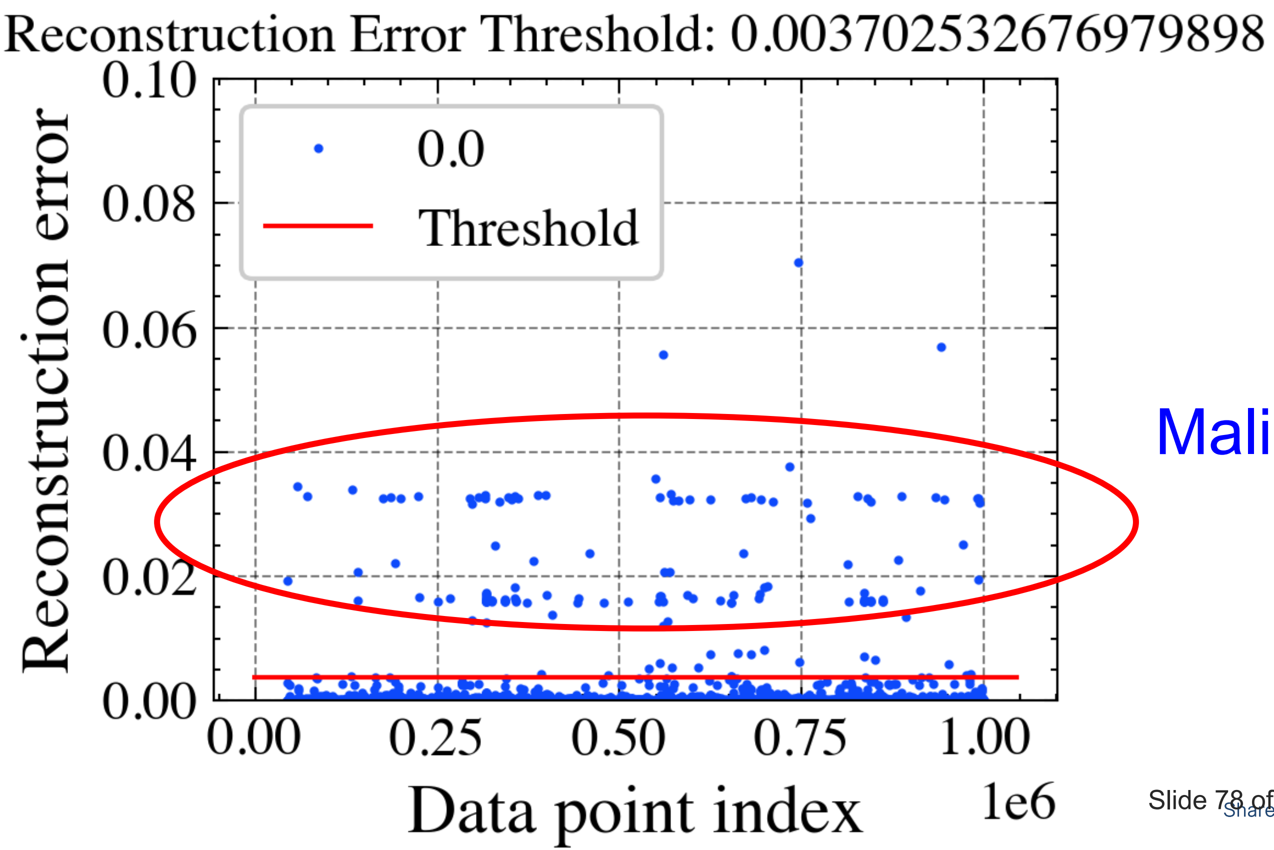


Classification results CICIDS 2017 dataset

TABLE V

True Class	Anomaly in All data	Total in All data	Anomaly in HTTP data	Total in HTTP data	Anomaly in SSH data	Total in SSH data	Anomaly in FTP data	Total in FTP data
BENIGN	13242	1743179	386	186133	242	8669	118	4381
Bot	11	1966	9	1261				
DoS	170802	380688	170843	380685				
FTP-Patator	0	7938	0	1			7920	7937
Heartbleed	11	11						
Infiltration	0	36						
PortScan	0	158930	0	533	243	243	140	244
SSH-Patator	0	5897			2921	5897		
Web Attack	0	2180	0	2180				

Our data - HTTP



Malicious?

TABLE IV
SERVICE DISTRIBUTION IN THE REAL DATASET.

Service	Amount
No Service	2397618
dns	1065914
ssl	713753
krb_tcp	82741
dce_rpc	66574
ntlm,dce_rpc	54712
http	45675
krb,smb,gssapi	18603
dce_rpc,ntlm	18253
gssapi,smb,krb	9351

TABLE V
PORT DISTRIBUTION OF THE "NO SERVICE" CATEGORY IN THE REAL DATASET.

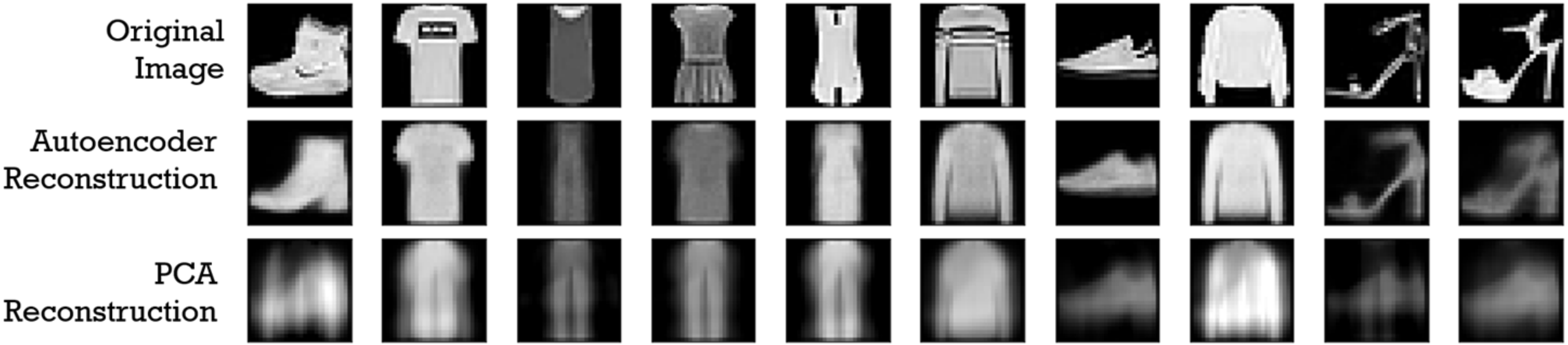
id.resp_p	amount
443.0 - ssl	1757725
389.0 - LDAP	152535
3389.0 - RDP	142428
5985.0 - WINRM	36175
1433.0 - ms-sql-s	26146
41121.0 - tentacle	24723
5246.0 - firewall	19212
80.0 - HTTP	16737
547.0 - DHCP	15086
135.0 - RPC	12435

TABLE I
UNSW-NB15 AND CICIDS 2017 DISTRIBUTION OF NORMAL AND ATTACK DATA PER SERVICE

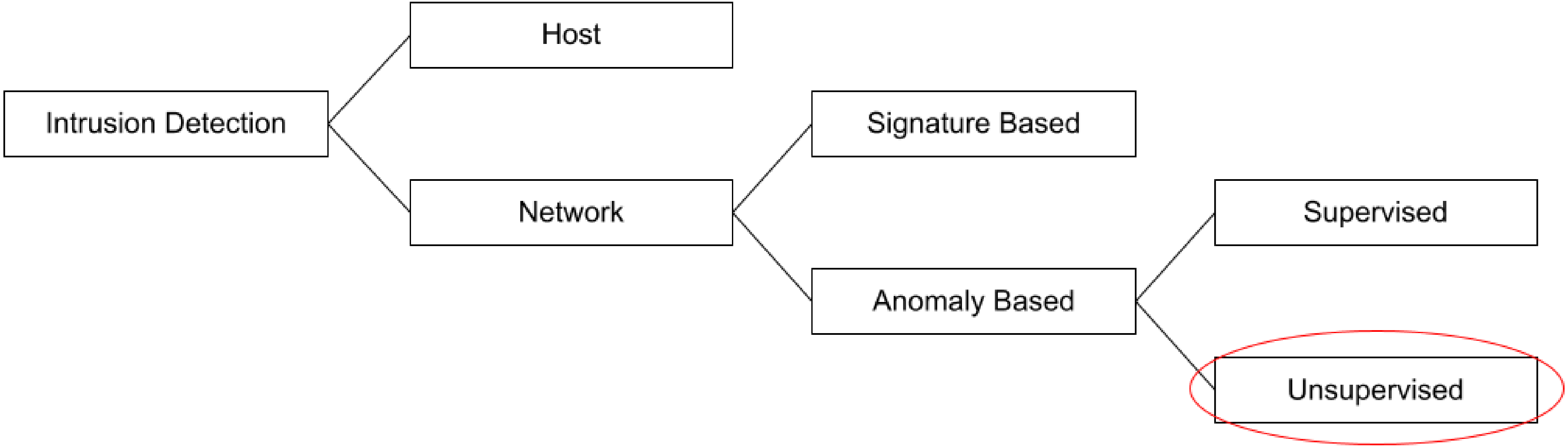
Service	Label	UNSW-NB15			CICIDS 2017
		Training set	Testing set	Entire dataset	Entire dataset
No service	Normal	36512	27375	1166520	530121
	Attack	57656	19778	79877	158731
dhcp	Attack	94	26	172	0
dns	Normal	7493	3068	571037	957812
	Attack	39801	18299	210631	159
ftp	Normal	1218	758	46075	5341
	Attack	2210	794	3015	8181
ftp-data	Normal	2552	949	123893	61
	Attack	1443	447	1890	158
http	Normal	5348	4013	187426	235695
	Attack	13376	4274	18847	383239
ntp	Normal	0	0	0	23879
	Attack	0	0	0	1
irc	Normal	0	0	1	66
	Attack	25	5	30	158
pop3	Normal	4	0	4	61
	Attack	1101	423	1529	160
radius	Normal	2	2	10	67
	Attack	10	7	30	160
smtp	Normal	1579	635	76656	3657
	Attack	3479	1216	4989	160
snmp	Normal	1	0	1	66
	Attack	79	29	112	159
ssh	Normal	1291	200	47141	10801
	Attack	11	4	19	6140
ssl	Normal	0	0	0	505470
	Attack	56	30	142	240

Research questions

- RQ 1: What is the best method in the state-of-the-art in anomaly-based NIDS?
- RQ 2: What improvements can be made on Auto Encoders for anomaly-based NIDS?
- RQ 3: Can we achieve unsupervised anomaly-based NIDS for practical use?


Original Image
Autoencoder Reconstruction
PCA Reconstruction

Unsupervised Anomaly-Based Network Intrusion Detection



Standard connection and statistical features

ID	Name	Type
7	Duration	Float
8	Source bytes	Integer
9	Destination bytes	Integer
10	State	String
11	Source is local origin	Bool
12	Destination is local origin	Bool
13	Missed bytes	Integer
14	Source packet count	Integer
15	Destination packet count	Integer
16	Source TTL	Integer
17	Destination TTL	Integer

ID	Name	Type
24	Source bytes per second	Float
25	Destination bytes per second	Float
26	Mean Source packet size	Integer
27	Mean Destination packet size	Integer
28	No. of connections that contain the same service (14) and source address (1) in 100 connections	Integer
29	No. of connections that contain the same service (14) and destination address (3) in 100 connections	Integer
30	No. of connections of the same destination address (3) in 100 connections	Integer
31	No. of connections of the same source address (1) in 100 connections	Integer
32	No of connections of the same source address (1) and the destination port (4) in 100 connections	Integer
33	No of connections of the same destination address (3) and the source port (2) in 100 connections	Integer
34	No of connections of the same source (1) and the destination (3) address in in 100 connections	Integer

Service specific features

ID	Name	Source log	Type
35	Query type	DNS	Integer
36	Return code	DNS	Integer
37	rtt	DNS	Integer
38	TTLs	DNS	Integer
39	dns_query_len	DNS	Integer
40	method	HTTP	String
41	trans_depth	HTTP	Integer
42	http_query_len	HTTP	Integer
43	status_code	HTTP	Integer
44	referrer_bool	HTTP	Binary

How can we implement this method?

Mean over absolute reconstruction error per features

True_class	Reconstruction_error	ct_dst_ltm	ct_dst_sport_ltm	ct_dst_src_ltm	ct_flw_http_mthd	ct_src_dport_ltm	ct_src_ltm	ct_srv_dst	ct_srv_src	ct_state_ttl	dinpkt	dload	dloss
DoS	0.023195	0.012326	0.004868	0.020292	0.013933	0.014114	0.002742	0.072739	0.021187	0.131657	0.009248	0.015556	0.012310
Exploits	0.006095	0.004968	0.003790	0.007841	0.013651	0.030341	0.001613	0.026839	0.026936	0.179090	0.013407	0.017660	0.012766
Fuzzers	0.029745	0.016044	0.009930	0.003975	0.015863	0.018178	0.027035	0.038416	0.016406	0.451187	0.107350	0.003535	0.020209
Generic	0.019101	0.132567	0.269077	0.182693	0.001234	0.138053	0.094871	0.194547	0.173181	0.241012	0.000802	0.033618	0.017531
Normal	0.000032	0.001182	0.000608	0.000129	0.000042	0.000629	0.001385	0.000957	0.000142	0.000262	0.000831	0.003104	0.000242
Reconnaissance	0.046770	0.018343	0.003067	0.040874	0.021585	0.017605	0.009287	0.100376	0.020816	0.108352	0.018820	0.016991	0.013673

Security Events

Windows Security Events

Machine Learning

Event at Time x is anomalous

What is anomalous?

Security Events

Windows Security Events TGT requests

Machine Learning

Event at time x has anomalous encryption level requests

Why is it anomalous?

Security Events

Windows Security Events TGT requests

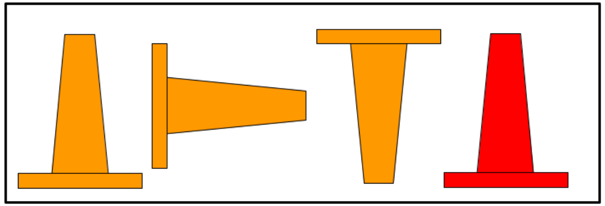
Machine Learning

Event at time X has unusual weak encryption level requests

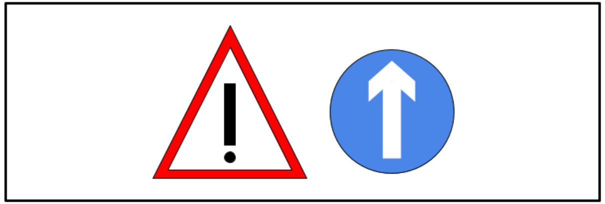
Possible Kerberoasting

Proposed method

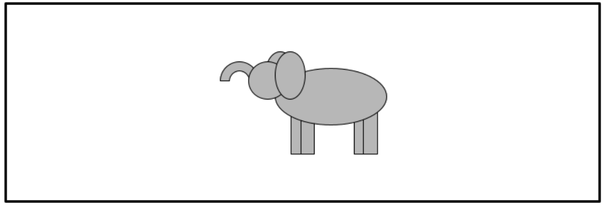
Training set



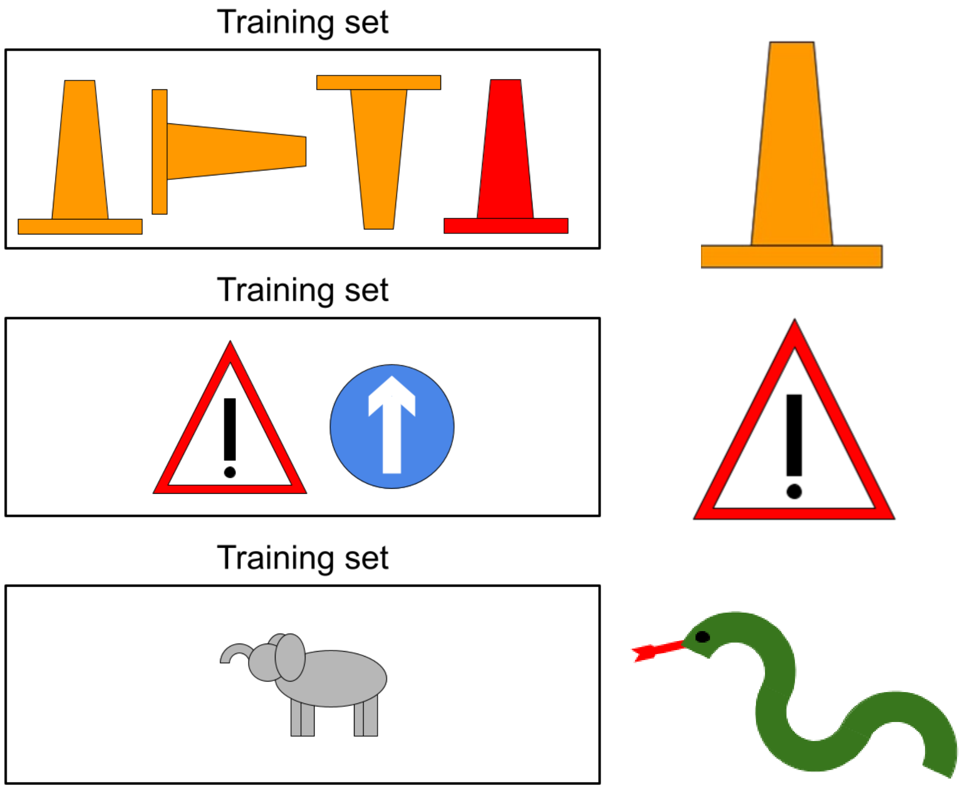
Training set



Training set



Proposed method



Mean over absolute normalised features

True_class	ackdat	ct_dst_ltm	ct_dst_sport_ltm	ct_dst_src_ltm	ct_src_dport_ltm	ct_src_ltm	ct_srv_dst	ct_srv_src	ct_state_ttl	dload	dmean	dtcpb	dttl
DoS	0.004618	0.015086	0.005405	0.005645	0.010776	0.019915	0.045492	0.026210	0.279167	0.000740	0.044667	0.096691	0.316601
Exploits	0.000561	0.017748	0.024642	0.024905	0.040314	0.045862	0.038573	0.095825	0.401961	0.001043	0.079843	0.009070	0.500814
Fuzzers	0.000000	0.004057	0.006359	0.005693	0.004057	0.013958	0.003857	0.003795	0.568627	0.000000	0.000000	0.000000	0.000000
Generic	0.000001	0.258485	0.292622	0.333444	0.256867	0.258447	0.375076	0.369398	0.333324	0.000000	0.000012	0.000021	0.000055
Normal	0.000000	0.038855	0.001656	0.006072	0.008132	0.053903	0.033156	0.033115	0.000109	0.030799	0.056988	0.000000	0.113542
Reconnaissance	0.006440	0.005747	0.000000	0.002688	0.000000	0.012712	0.015027	0.000000	0.263889	0.000082	0.012389	0.207475	0.415020

True_class	ackdat	ct_dst_ltm	ct_dst_sport_ltm	ct_dst_src_ltm	ct_src_dport_ltm	ct_src_ltm	ct_srv_dst	ct_srv_src	ct_state_ttl	dload	dmean	dtcpb	dttl	dur	dwin
DoS	0.004618	0.015086	0.005405	0.005645	0.010776	0.019915	0.045492	0.026210	0.279167	0.000740	0.044667	0.096691	0.316601	0.003035	0.175000
Exploits	0.000561	0.017748	0.024642	0.024905	0.040314	0.045862	0.038573	0.095825	0.401961	0.001043	0.079843	0.009070	0.500814	0.019691	0.029412
Fuzzers	0.000000	0.004057	0.006359	0.005693	0.004057	0.013958	0.003857	0.003795	0.568627	0.000000	0.000000	0.000000	0.000000	0.473338	0.000000
Generic	0.000001	0.258485	0.292622	0.333444	0.256867	0.258447	0.375076	0.369398	[illegible]	0.000000	0.000012	[illegible]	0.000055	0.000001	0.000055
Normal	0.000000	0.038855	0.001656	0.006072	0.008132	0.053903	0.033156	0.033115	0.000109	0.030799	0.056988	0.000000	0.113542	0.000020	0.000000
Reconnaissance	0.006440	0.005747	0.000000	0.002688	0.000000	0.012712	0.015027	0.000000	0.263889	[illegible]	[illegible]	0.207475	0.415020	0.004234	0.416667

True_class	is_ftp_login_0	rate	sinpkt	sload	smean	spkts	state_CON	state_FIN	state_INT	state_REQ	stcpb	sttl	swin	synack	tcprtt
DoS	1.000000	0.064841	0.000304	0.007317	0.031943	0.000218	0.200000	0.175000	0.625000	0.000000	0.056534	0.751765	0.175000	0.003582	0.006563
Exploits	1.000000	0.065957	0.000038	0.007064	0.030137	0.000392	0.529412	0.029412	0.441176	0.000000	0.015018	0.342791	0.029412	0.000468	0.000824
Fuzzers	1.000000	0.000009	0.006583	0.000002	0.107552	0.007808	0.000000	0.000000	0.647059	0.352941	0.000000	0.996078	0.000000	0.000000	0.000000
Generic	1.000000	0.201417	0.000000	0.017438	0.022309	[illegible]	0.000000	[illegible]	0.999945	0.000000	0.000034	0.996078	0.000055	0.000001	0.000002
Normal	1.000000	0.005333	0.000000	0.000591	0.031601	0.000094	0.990548	0.000000	0.009452	0.000000	0.000000	0.122745	0.000000	0.000000	0.000000
Reconnaissance	1.000000	0.139684	0.000456	0.014840	0.027759	[illegible]	0.000000	[illegible]	[illegible]	[illegible]	0.139019	0.996078	0.416667	0.006877	0.010743

Mean over absolute reconstruction error per features

True_class	Reconstruction_error	ct_dst_ltm	ct_dst_sport_ltm	ct_dst_src_ltm	ct_flw_http_mthd	ct_src_dport_ltm	ct_src_ltm	ct_srv_dst	ct_srv_src	ct_state_ttl	dinpkt	dload	dloss
DoS	0.023195	0.012326	0.004868	0.020292	0.013933	0.014114	0.002742	0.072739	0.021187	0.131657	0.009248	0.015556	0.012310
Exploits	0.006095	0.004968	0.003790	0.007841	0.013651	0.030341	0.001613	0.026839	0.026936	0.179090	0.013407	0.017660	0.012766
Fuzzers	0.029745	0.016044	0.009930	0.003975	0.015863	0.018178	0.027035	0.038416	0.016406	0.451187	0.107350	0.003535	0.020209
Generic	0.019101	0.132567	0.269077	0.182693	0.001234	0.138053	0.094871	0.194547	0.173181	0.241012	0.000802	0.033618	0.017531
Normal	0.000032	0.001182	0.000608	0.000129	0.000042	0.000629	0.001385	0.000957	0.000142	0.000262	0.000831	0.003104	0.000242
Reconnaissance	0.046770	0.018343	0.003067	0.040874	0.021585	0.017605	0.009287	0.100376	0.020816	0.108352	0.018820	0.016991	0.013673

True_class	Reconstruction_error	ct_dst_ltm	ct_dst_sport_ltm	ct_dst_src_ltm	ct_flw_http_mthd	ct_src_dport_ltm	ct_src_ltm	ct_srv_dst	ct_srv_src	ct_state_ttl	dinpkt	dload	dloss
DoS	0.023195	0.012326	0.004868	0.020292	0.013933	0.014114	0.002742	0.072739	0.021187	0.131657	0.009248	0.015556	0.012310
Exploits	0.006095	0.004968	0.003790	0.007841	0.013651	0.030341	0.001613	0.026839	0.026936	0.179090	0.013407	0.017660	0.012766
Fuzzers	0.029745	0.016044	0.009930	0.003975	0.015863	0.018178	0.027035	0.038416	0.016406	0.451187	0.107350	0.003535	0.020209
Generic	0.019101	0.132567	0.269077	0.182693	0.001234	0.138053	0.094871	0.194547	0.173181	0.241012	0.000802	0.033618	0.017531
Normal	0.000032	0.001182	0.000608	0.000129	0.000042	0.000629	0.001385	0.000957	0.000142	0.000262	0.000831	0.003104	0.000242
Reconnaissance	0.046770	0.018343	0.003067	0.040874	0.021585	0.017605	0.009287	0.100376	0.020816	0.108352	0.018820	0.016991	0.013673

True_class	dmean	dpkts	dtcpb	dttl	dur	dwin	rate	sbytes	sload	state_CON	state_FIN	state_INT	state_REQ	stcpb	sttl	swin	trans_depth
DoS	0.048608	0.015699	0.100908	0.031748	0.006182	0.186768	0.054090	0.011800	0.013831	0.099223	0.172118	0.092115	0.001629	0.055759	0.491183	0.176686	0.018103
Exploits	0.080175	0.010206	0.008994	0.038262	0.010461	0.043047	0.060825	0.013675	0.002882	0.014370	0.028699	0.037277	0.001537	0.007110	0.090120	0.026536	0.027669
Fuzzers	0.065920	0.005260	0.006865	0.230214	0.133693	0.010186	0.010112	0.018967	0.003150	0.229622	0.004536	0.142219	0.355999	0.007550	0.744051	0.012206	0.015346
Generic	0.037557	0.049761	0.002448	0.131975	0.000101	0.020505	0.195508	0.029062	0.060984	0.027445	0.005285	0.016823	0.000226	0.004779	0.704653	0.000828	0.002417
Normal	0.000376	0.000189	0.000048	0.001436	0.002518	0.000395	0.002225	0.000012	0.000219	0.000964	0.000135	0.000753	0.000128	0.000107	0.000072	0.000472	0.000094
Reconnaissance	0.076044	0.019111	0.214980	0.127102	0.034411	0.426153	0.128317	0.012622	0.011082	[illegible]	[illegible]	[illegible]	0.000924	0.142143	0.726642	0.421283	0.017104

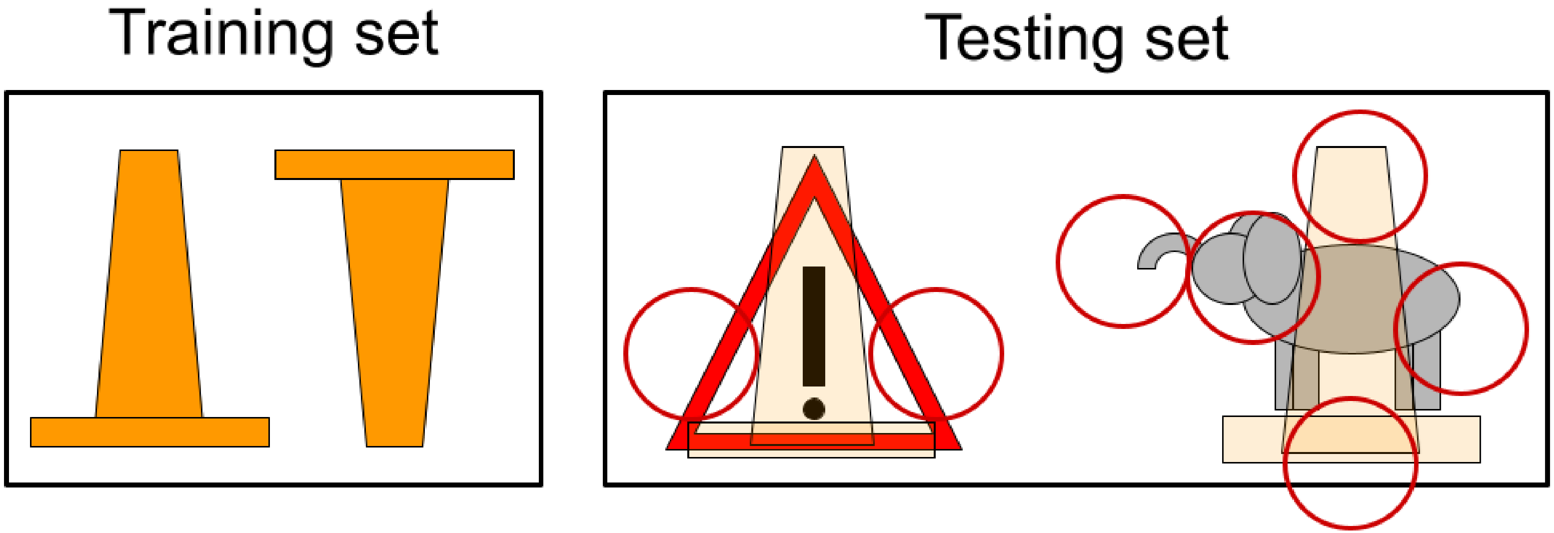
Signature-based

SNORT®

SURICATA

EMERGING THREATS

	Total amount of IP pairs	Amount of IP pairs above the threshold	IP pair Occurrence >10 times above threshold	Source IP Occurence >10 times above threshold
Total	4062	137	47	6
Attack	40	40	40	4


Training set
Testing set

Classification results CICIDS 2017 dataset

TABLE V

True Class	Anomaly in All data	Total in All data	Anomaly in HTTP data	Total in HTTP data	Anomaly in SSH data	Total in SSH data	Anomaly in FTP data	Total in FTP data
BENIGN	13242	1743179	386	186133	242	8669	118	4381
Bot	11	1966	9	1261				
DoS	170802	380688	170843	380685				
FTP-Patator	0	7938	0	1			7920	7937
Heartbleed	11	11						
Infiltration	0	36						
PortScan	0	158930	0	533	243	243	140	244
SSH-Patator	0	5897			2921	5897		
Web Attack	0	2180	0	2180				

Data distribution per service UNSW-NB15 and CICIDS 2017

Service	Label	UNSW-NB15			CICIDS 2017
		Training set	Testing set	Entire dataset	Entire dataset
No service	Normal	36512	27375	1166520	530121
	Attack	57656	19778	79877	158731
dhcp	Attack	94	26	172	0
dns	Normal	7493	3068	571037	957812
	Attack	39801	18299	210631	159
ftp	Normal	1218	758	46075	5341
	Attack	2210	794	3015	8181
ftp-data	Normal	2552	949	123893	61
	Attack	1443	447	1890	158
http	Normal	5348	4013	187426	235695
	Attack	13376	4274	18847	383239


Training set
Testing set

Training on 30 minutes of data

Type of Data	Action	Amount of connections	Time (with early stopping)
All Data	Training	776.371	0:05:50.982308
	Testing	3.636.051	0:00:44.226864
DNS	Training	184.424	0:01:29.271912
	Testing - Total	849.540	0:00:14.300020
	Testing - 5 minutes	24.317	0:00:00.452973

* 1/4

* 1/4

Our goal

Can we achieve anomaly based detection for practical commercial implementation?

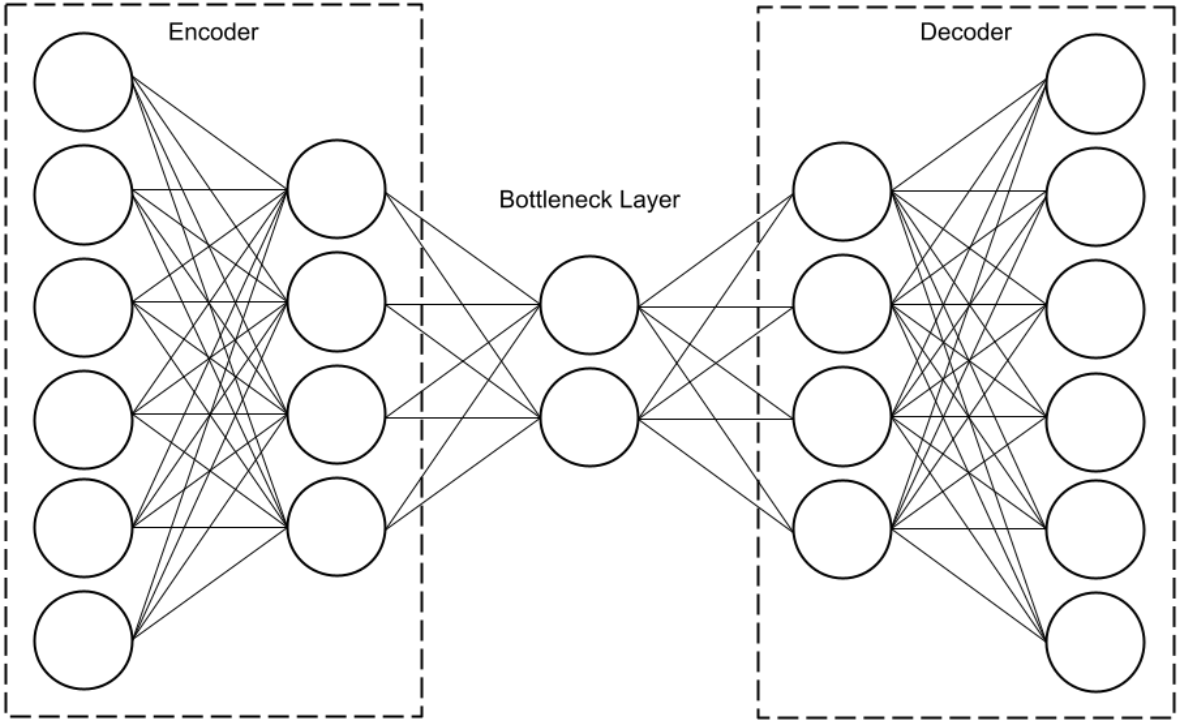
If so, how?

Using Auto Encoders on specific data

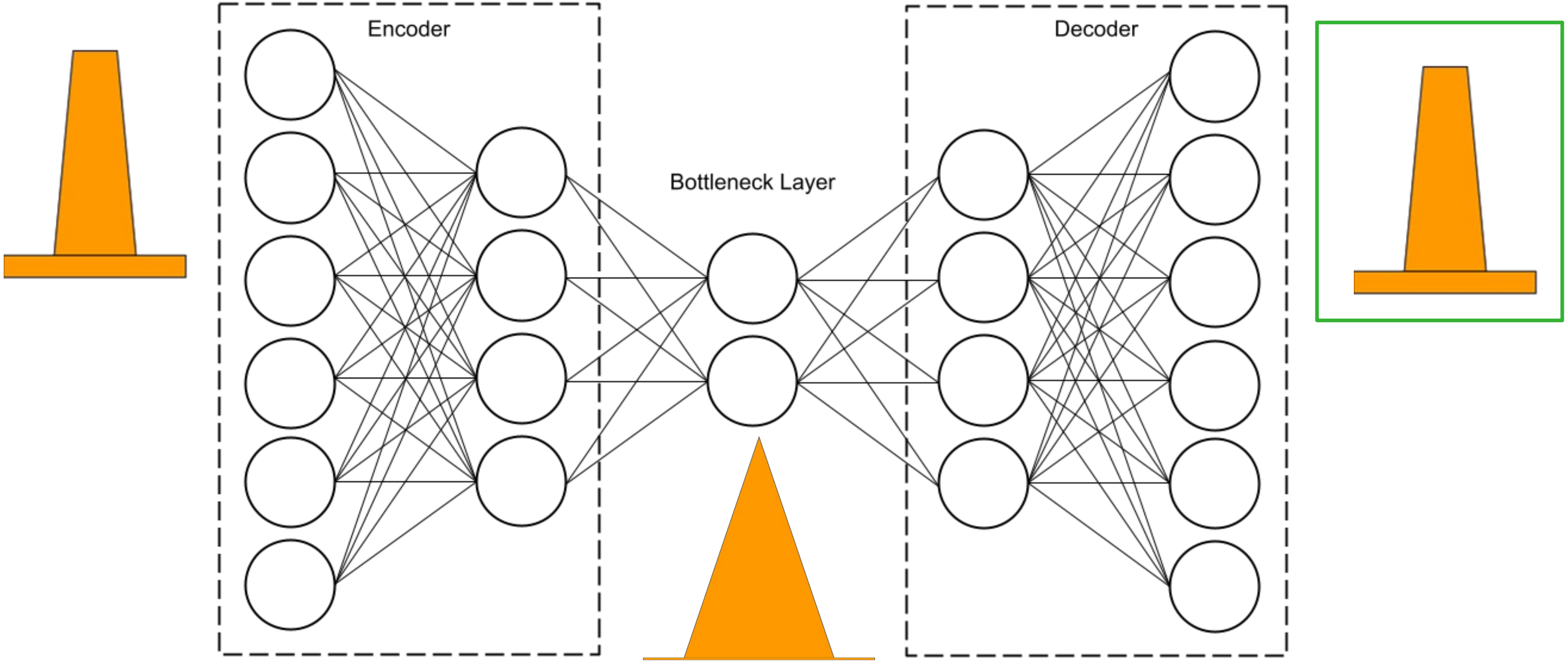
Concluding

- Improvement in performance for Auto Encoders
- Improvement in efficiency due to split data
- Alerts contain more information, reducing the “black box” nature of deep learning

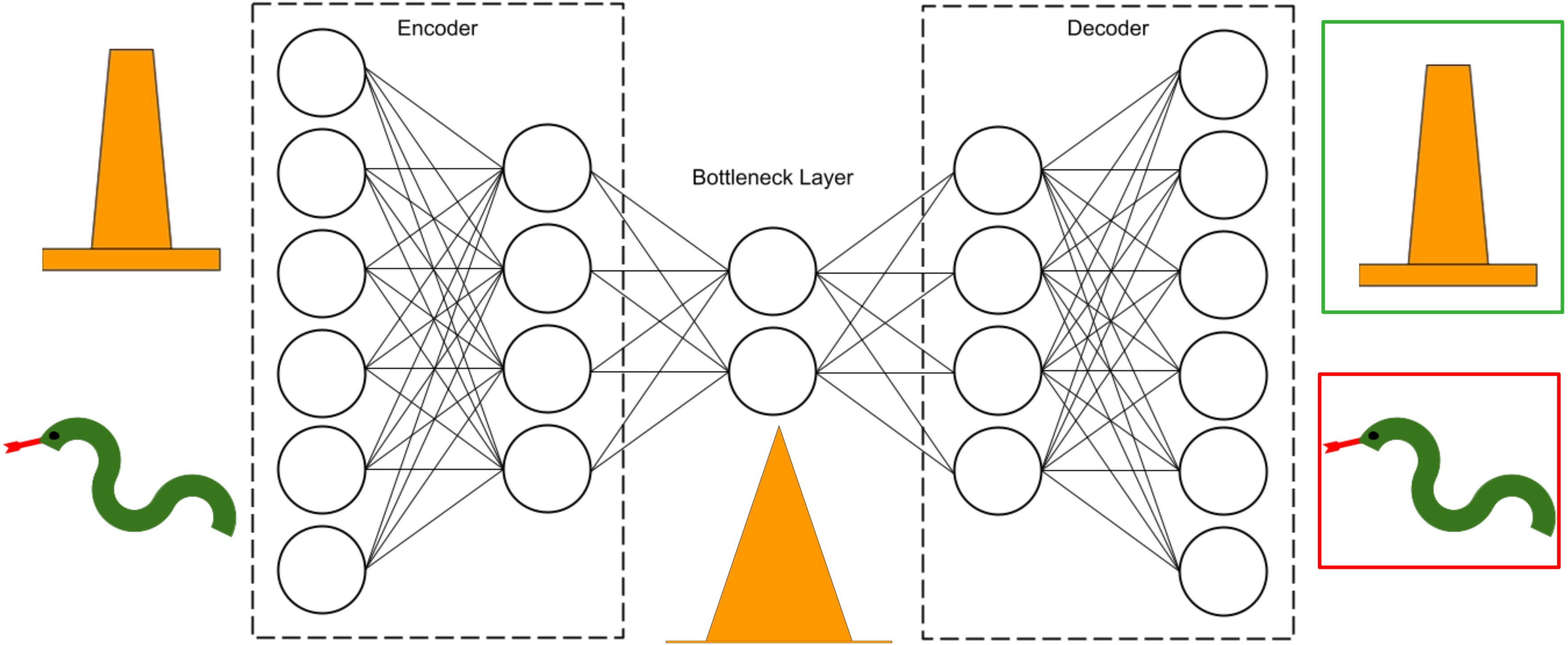
Auto Encoder model



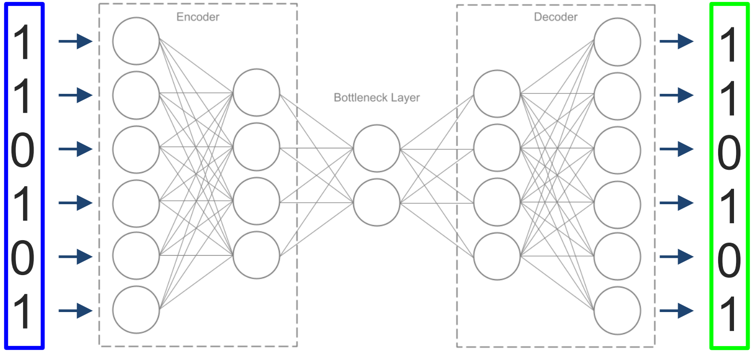
Auto Encoder model



Auto Encoder model



Correctly reconstructed

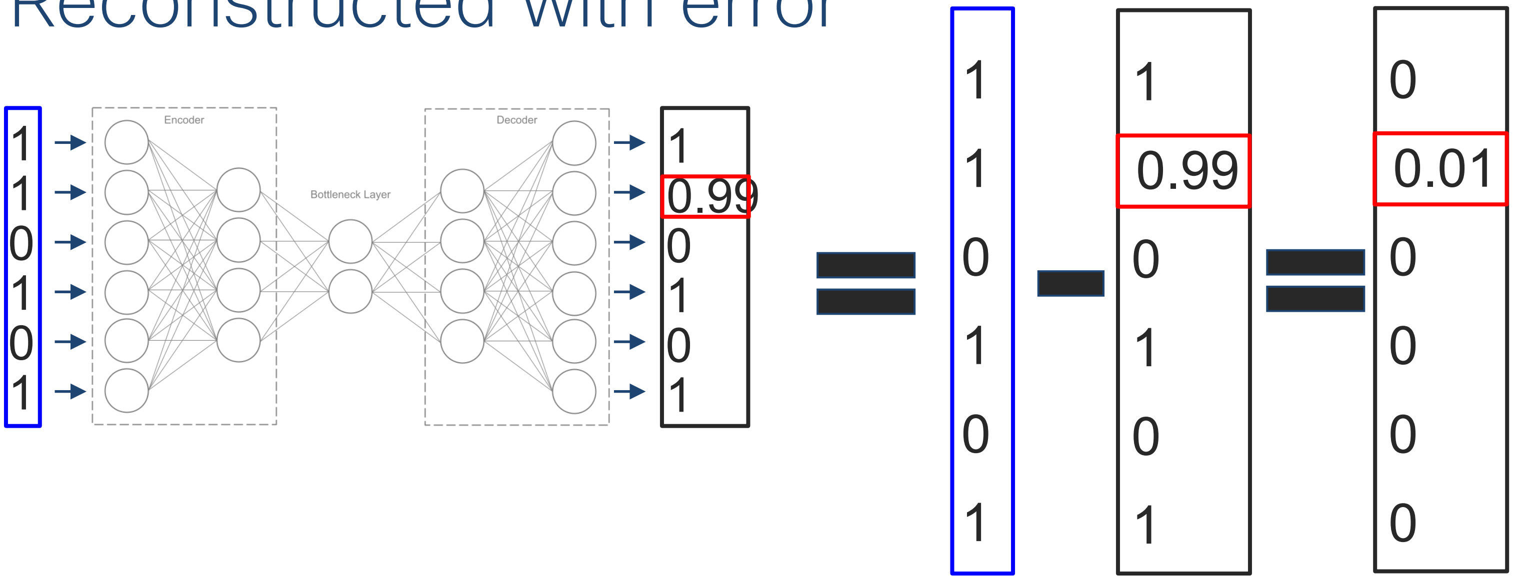


$$= \begin{bmatrix}1\\1\\0\\1\\0\\1\end{bmatrix} - \begin{bmatrix}1\\1\\0\\1\\0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\\0\\0\end{bmatrix}$$

Reconstruction

Error = 0

Reconstructed with error



Reconstruction
Error = 0.01

RQ3: How can we achieve unsupervised anomaly-based NIDS for practical use?

Experiments on real data