



HAL
open science

Cybersecurity of Urban Critical Infrastructure by Intelligent Big Data Analytics...

Konstantinos Demertzis

► **To cite this version:**

Konstantinos Demertzis. Cybersecurity of Urban Critical Infrastructure by Intelligent Big Data Analytics.... Doctoral. Greece. 2020. hal-03066965

HAL Id: hal-03066965

<https://hal.science/hal-03066965>

Submitted on 15 Dec 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

[~] Cybersecurity of Urban Critical Infrastructure by Intelligent Big Data Analytics...

Dr Konstantinos Demertzis

Orestiada, Evros, Greece

Postdoctoral Researcher: School of Civil Engineering, DUTH



- postdoc...
- brainchip
- prospects
- in progress

#postdoc



1010000111101101001001111011010
00100110010 10001001100100111000
0100011100 00110101000101001010
0101010 1010000111010100100100
001001001110001001
11000001110101000

Stuxnet

infected







ΔΗΜΟΚΡΙΤΕΙΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΡΑΚΗΣ

DEMOCRITUS
UNIVERSITY
OF THRACE

postdoc



Cyber Security of Critical Infrastructures, “Development of intelligent models and respective big data analytics platform for cyberdefense of urban critical infrastructure”
Supervisor Professor Lazaros Iliadis

postdoc...

Α Φάση

Εναρμονισμός με τα θεσμικά κείμενα για την ψηφιακή ασφάλεια των κρίσιμων υποδομών

Τομέας
Ενέργειας

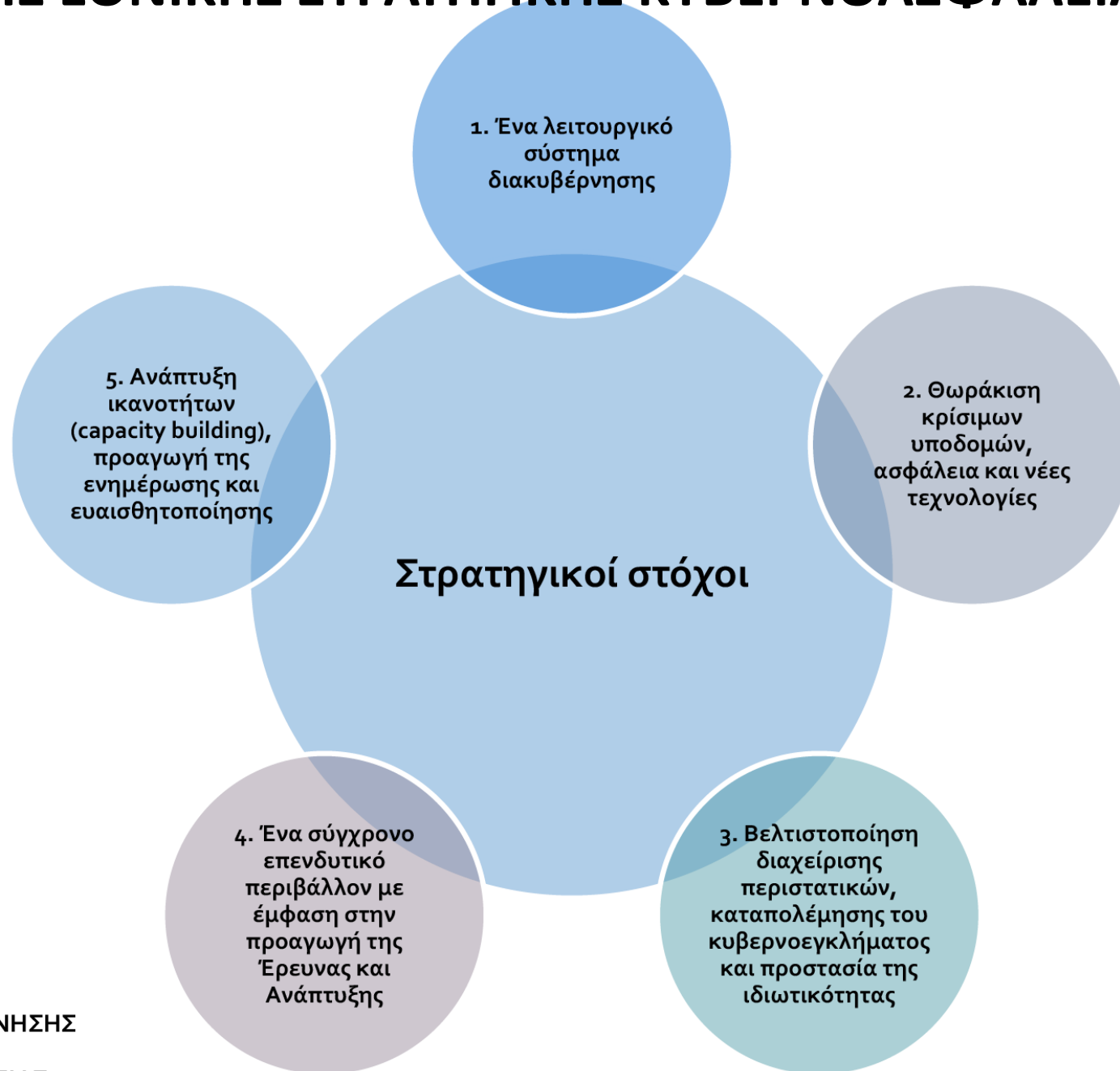
Τομέας ΤΠΕ

Τομέας
Μεταφορών

Τομέας
Εθνικής
Άμυνας

Βιομηχανικός
Τομέας

ΣΤΟΧΟΙ ΤΗΣ ΕΘΝΙΚΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020-2025



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ



enisa



THE EU
CYBERSECURITY
AGENCY



Critical Infrastructures and Services

- > Critical Information Infrastructures
- > Internet Infrastructure
- > ICS SCADA
- > Smart Grids
- > Finance
- > Health
- > Maritime
- > Railway



Recent deliberate disruptions of critical automation systems prove that cyber-attacks have a significant impact on critical infrastructures and services. Disruption of these ICT capabilities may have disastrous consequences for the EU Member States' governments and social wellbeing. The need to ensure ICT robustness against cyber-attacks is thus a key challenge at national and pan-European level.

Critical infrastructures, such as electricity generation plants, transportation systems, manufacturing facilities are controlled and monitored by Industrial Control Systems (ICS), including SCADA (Supervisory Control and Data Acquisition) systems. Today ICS products are mostly based on standard embedded systems platforms and they often use commercial off-the-shelf software. This results in the reduction of costs and improved ease of use but at the same time increases the exposure to computer network-based attacks.

Smart Grids will substantially improve control over electricity consumption and distribution to the benefit of consumers, electricity suppliers and grid operators. Nevertheless, improved operations and services will come at the cost of exposing the entire electricity network to new challenges, in particular in the field of security of communication networks and information systems. Vulnerabilities of communication networks and information systems may be exploited for financial or political motivation to shut off power to large areas or directing cyber-attacks against power generation plants.

The maritime sector is critical for the European society. Statistics show the augmenting trend of maritime transport share in the overall goods traffic, which in 2010 reached 52%. This continuous increase in dependency upon the maritime transport underlines its vital importance to our society

Recommended publications

Railway Cybersecurity

This ENISA study regards the level of implementation of cybersecurity measures in the railway sector, within the context of the enforcement of the...

Published on November 13, 2020



Power Sector Dependency on Time Service: attacks against...

Published on May 12, 2020

Encrypted Traffic Analysis

Published on April 23, 2020

Procurement Guidelines for Cybersecurity in Hospitals

Published on February 24, 2020

Recommended news

Healthcare's Cybersecurity Incident Response Spotlighted...

The EU Agency for Cybersecurity and the Danish Health Data Authority are joining forces again this



Communication network interdependencies in smart grids





73%





PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS

Good practices for the security of Healthcare services

FEBRUARY 2020





EUROPEAN UNION AGENCY
FOR CYBERSECURITY



RAILWAY CYBERSECURITY

Security measures in the Railway Transport Sector

NOVEMBER 2020





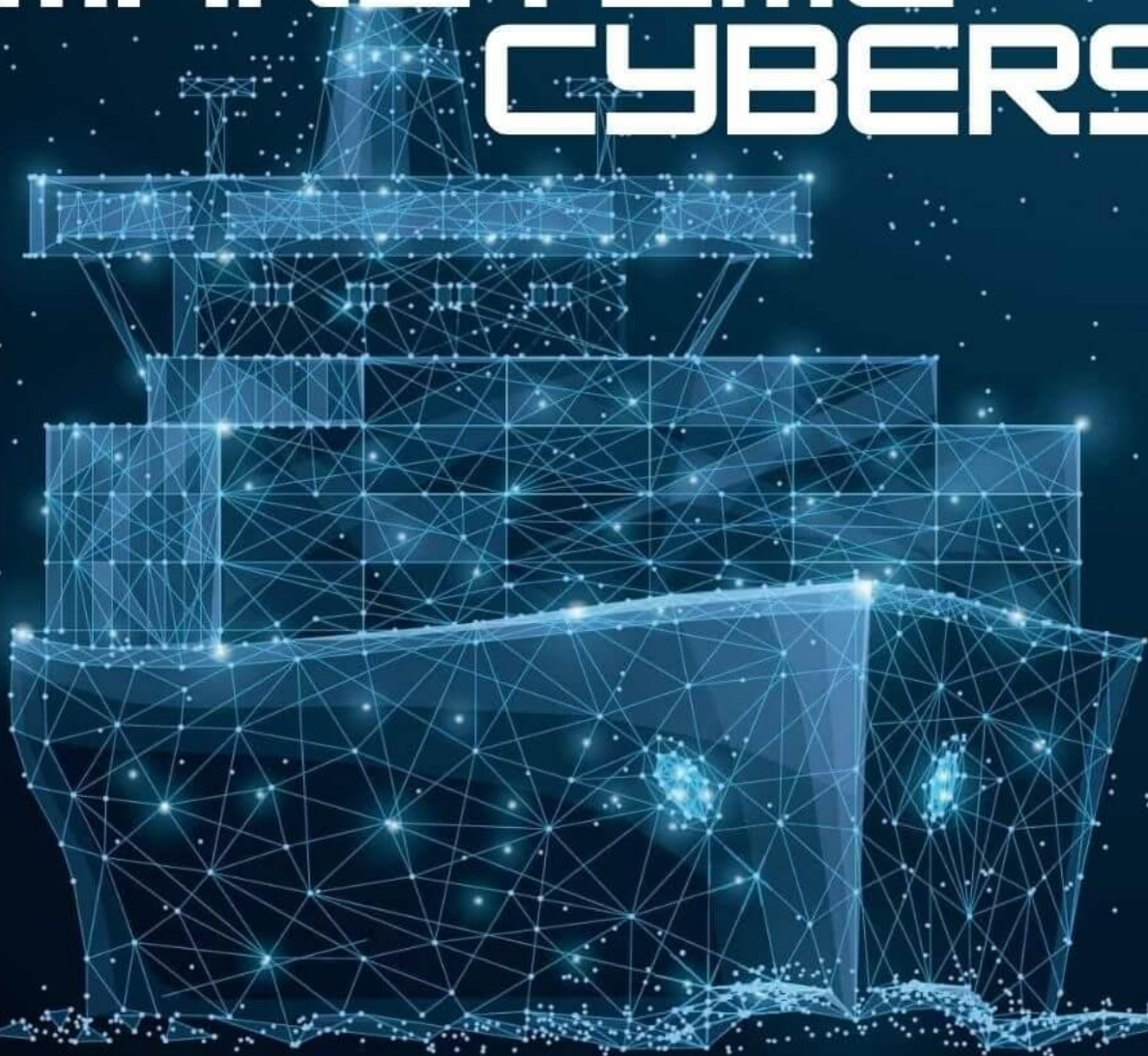
PORT CYBERSECURITY

Good practices for cybersecurity in the maritime
sector

NOVEMBER 2019

MARITIME CYBERSECURITY

CHALLENGES
AND BEST
PRACTICES

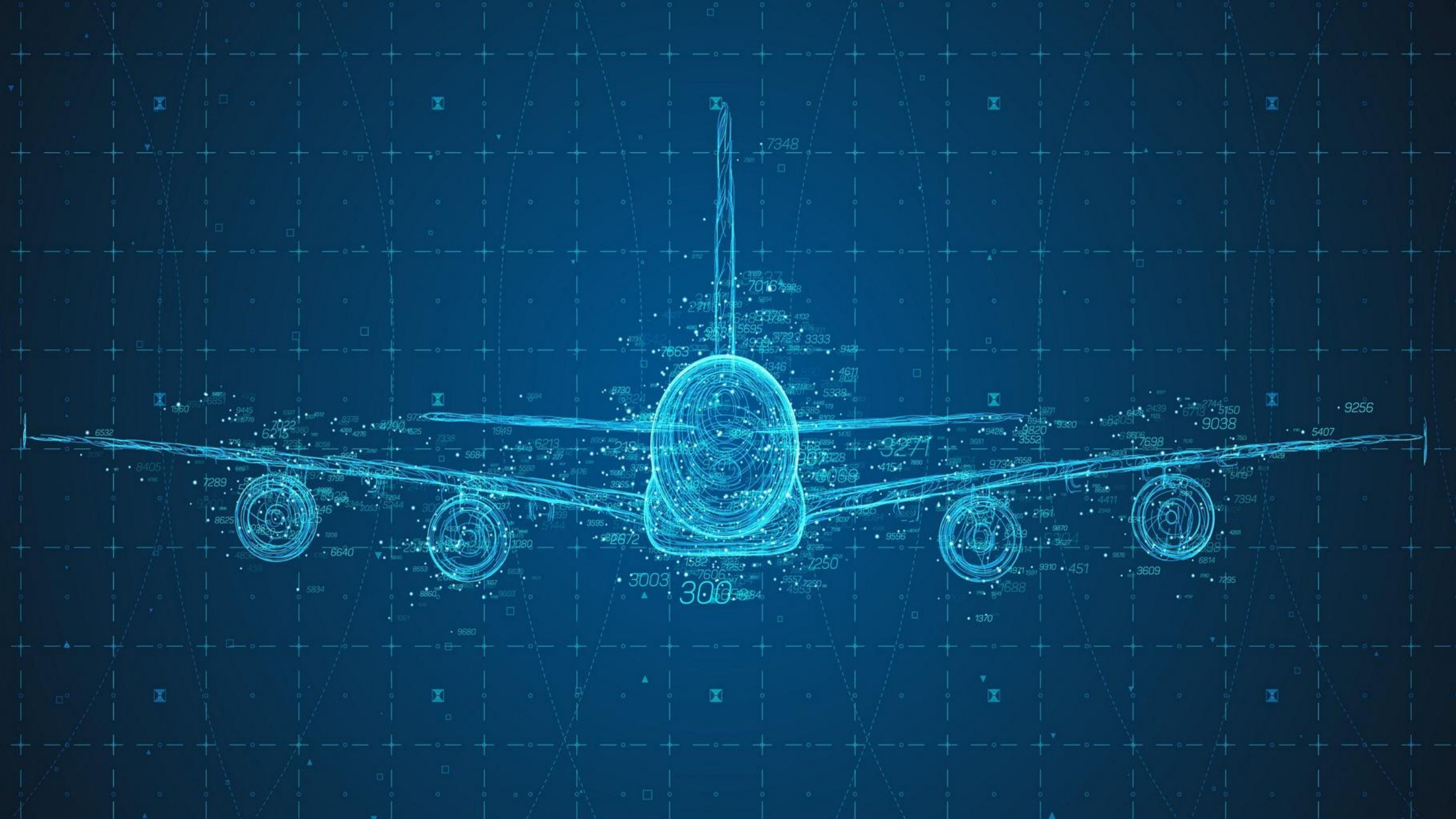




Securing Smart Airports

DECEMBER 2016





7348

7016

7663

9256

5407

9038

7698

3271

4154

1250

3003

3003

451

1370

3609

6688

6532

8405

7289

7022

6215

8625

6640

5834

4790

2075

9680

1949

5684

8860

1080

6213

3595

219

1582

7606

9073

2705

3189

5695

3333

4671

5328

5572

9731

9596

3691

9820

9731

2658

1827

5439

1114

4411

38

7394

4238

5479

2744

5150

9038

750

7029

2439

6719

1827

16409

58705

4226

2893

4628

4627

9731

9870

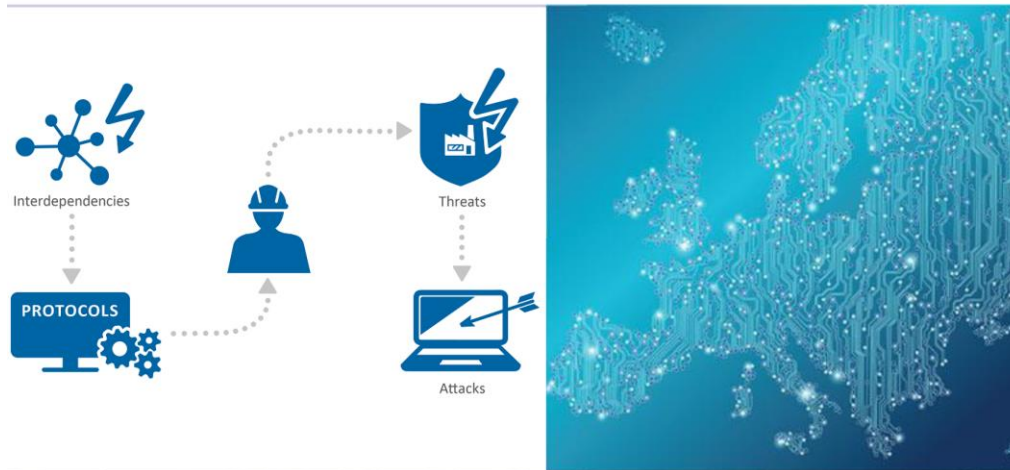
5174

9310

5814

7495

5407



Communication network dependencies for ICS/SCADA Systems

DECEMBER 2016



InduSoft SCADA Software



Host PC

Ethernet



NS-205
Ethernet Switch

Ethernet / Modbus TCP

Ethernet / Modbus TCP



TPD-433
4.3" Touch Screen PLC



tGW-715
Modbus TCP to RTU Gateway

PM-3112 Smart Power Meter



RS-485 / Modbus RTU







EUROPEAN UNION AGENCY
FOR CYBERSECURITY



ENCRYPTED TRAFFIC ANALYSIS

Use Cases & Security Challenges

NOVEMBER 2019

postdoc...

Β Φάση

Μελέτη του τρόπου ανάλυσης της δικτυακής κίνησης ως μέθοδο εντοπισμού σύγχρονων ψηφιακών απειλών

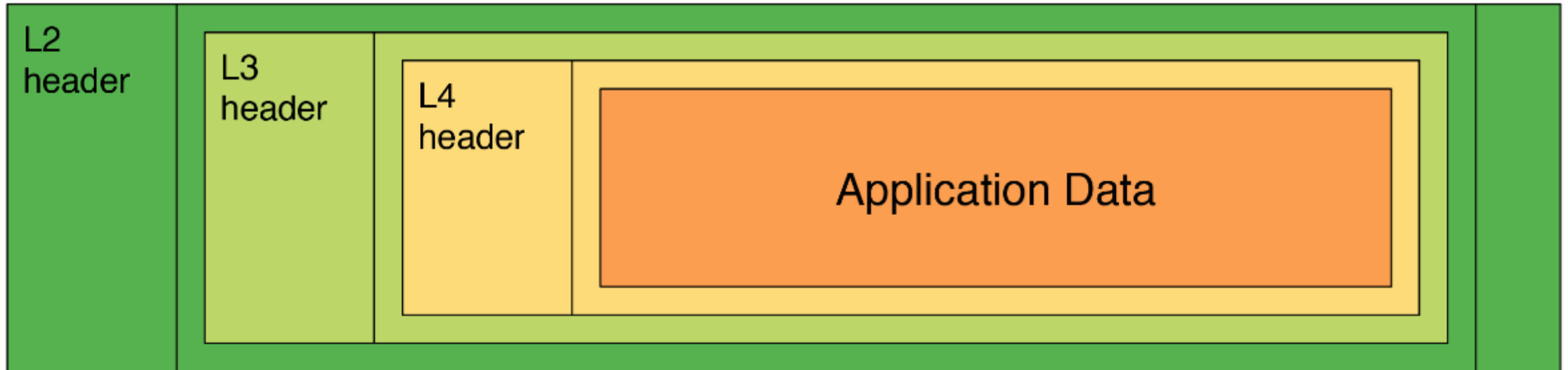
Network Traffic
Analysis

IDS/IPS

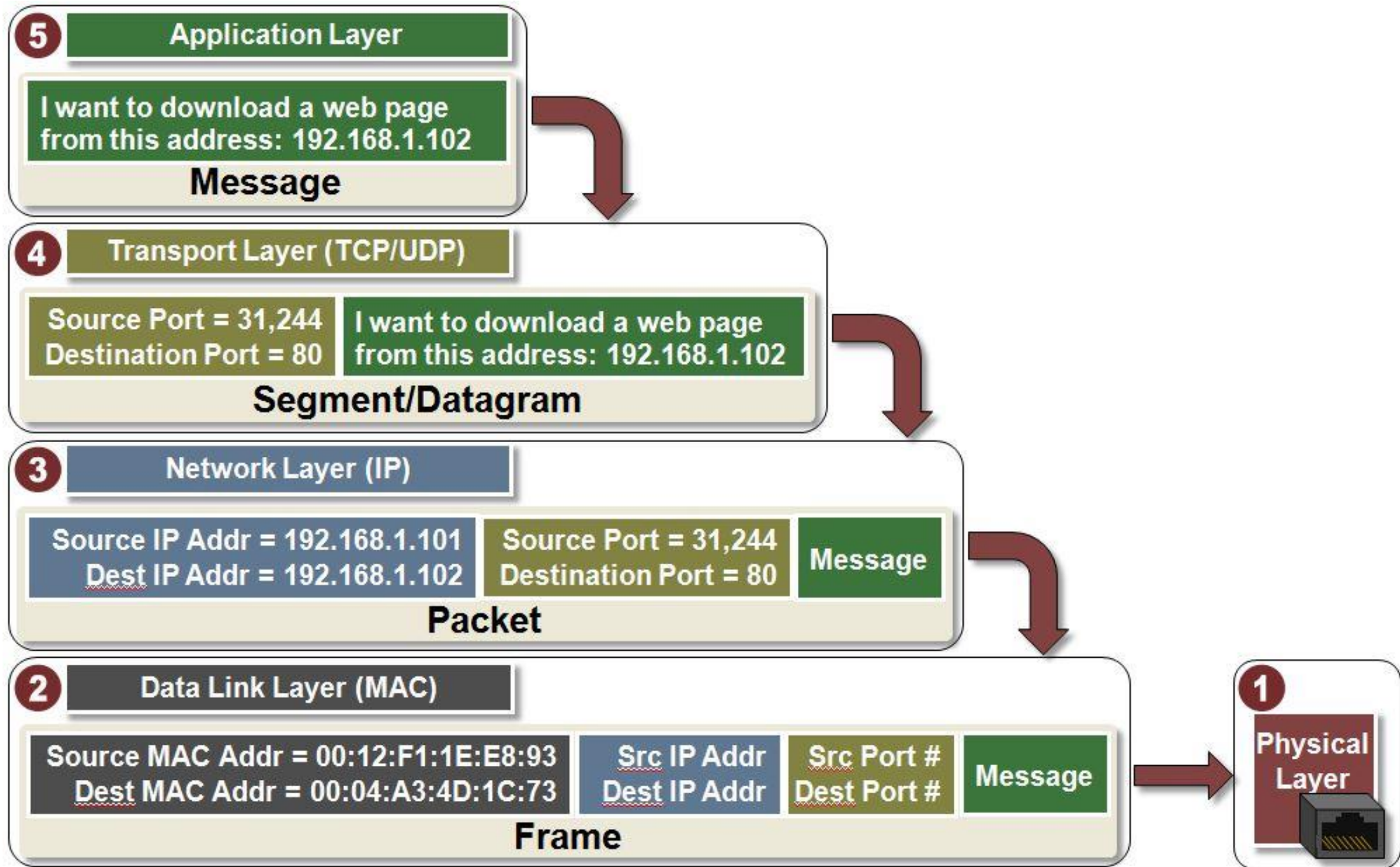
Demystification
Malware Traffic

Encrypted Traffic
Identification

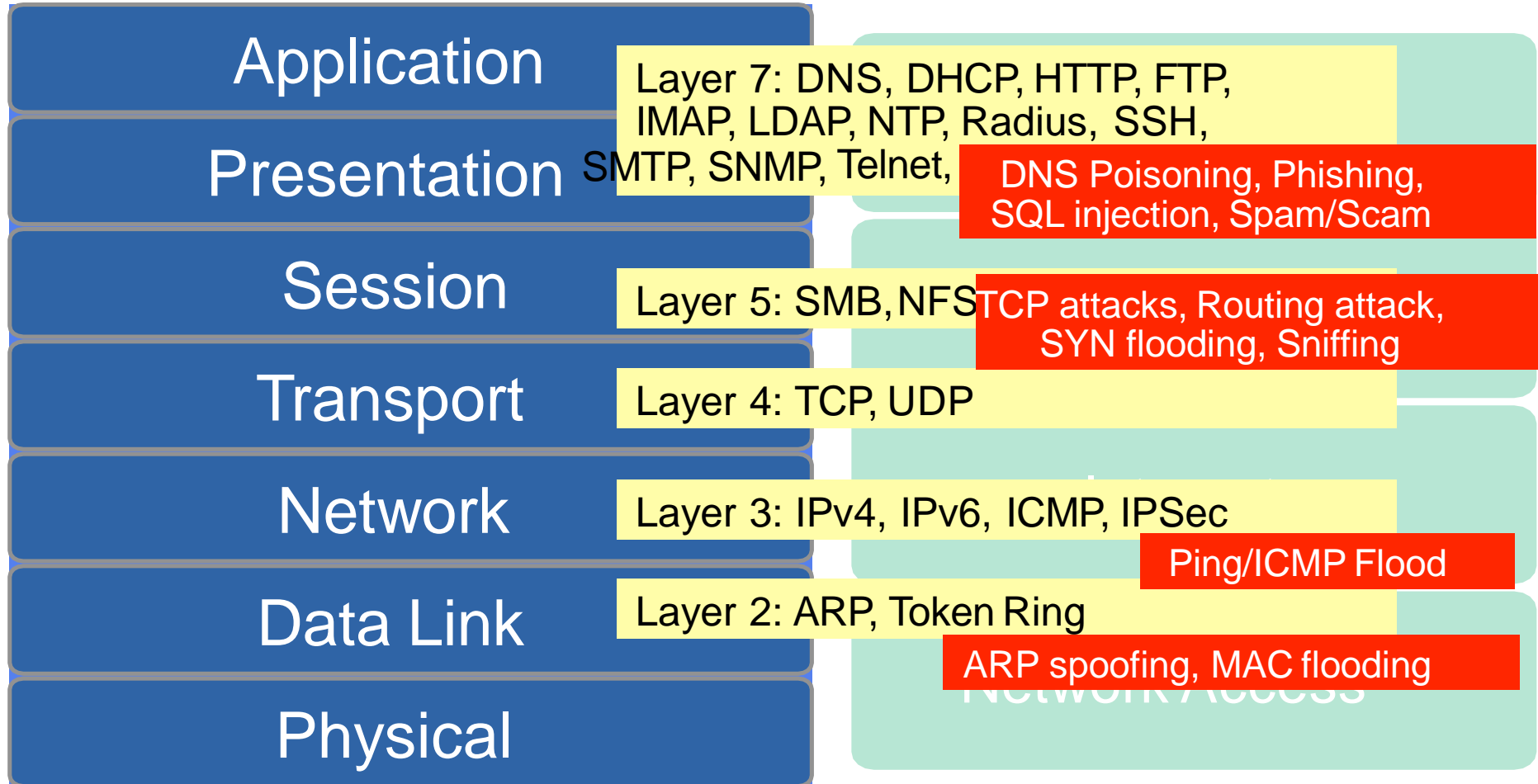
Encapsulation in Action



- L4 segment contains part of stream of application protocol
- L3 datagram contains L4 segment
- L2 frame has L3 datagram in data portion



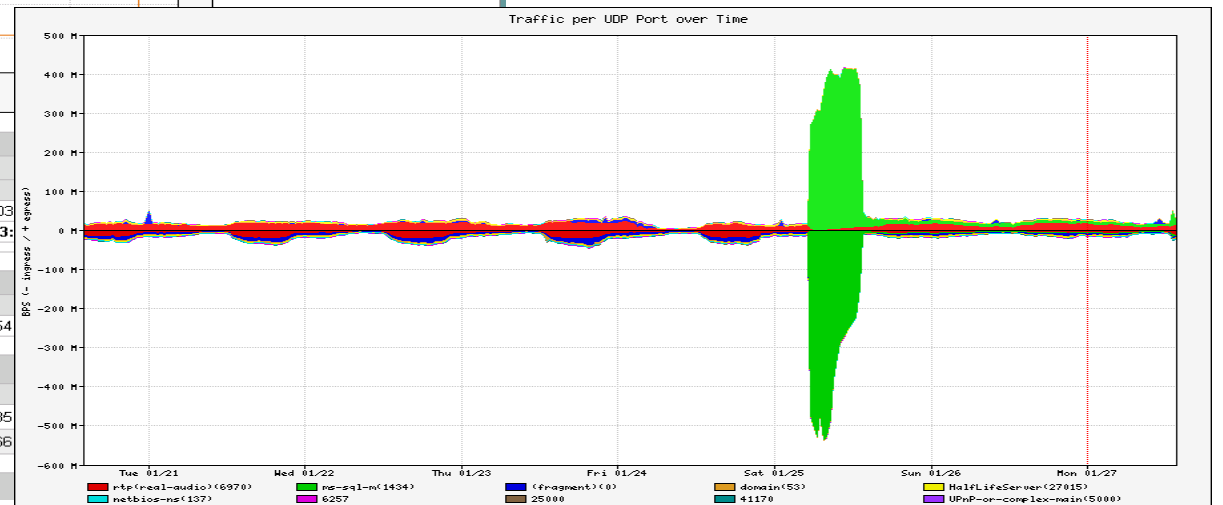
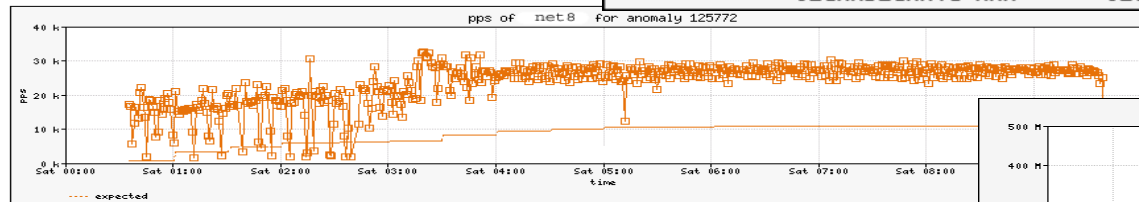
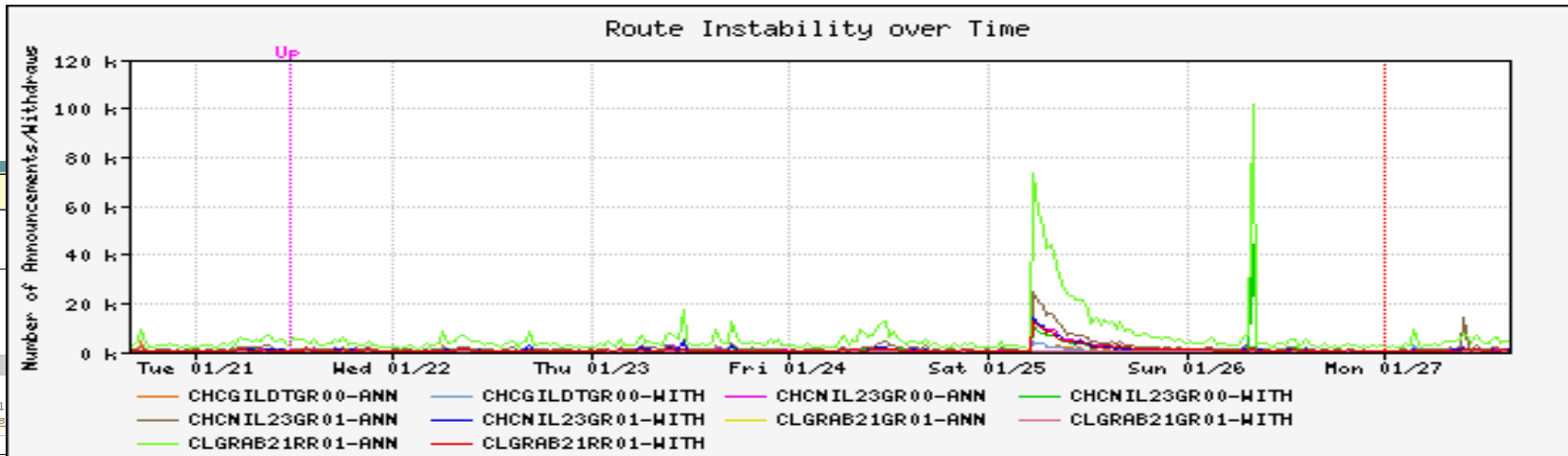
Attacks on Different Layers



Flow-based Detection

- **Once baselines are built anomalous activity can be detected**
 - Pure **rate-based** (pps or bps) anomalies may be legitimate or malicious
 - Many **misuse** attacks can be immediately recognized, even **without** baselines (e.g., TCP SYN or RST floods)
 - **Signatures** can also be defined to identify “interesting” transactional data (e.g., proto udp and port 1434 and 404 octets (376 payload) == slammer!)
 - Temporal compound signatures can be defined to detect with higher precision

Detect Anomalous Events: SQL "Slammer" Worm*



peakflow | DoS

Recent Anomalies : Anomaly 125772 : Detailed 11:51:49 EST 27 Jan 2003

Statistics

Status Topology Ongoing Recent Dark IP Admin About

Anomaly 125772 Detailed Statistics

ID	Importance	Severity	Duration	Direction
125772	High	958.2% of 3.40 Kpps	09h 06m 47s	Outgoing

Affected Network Elements

Router	Triggering	Expected	Difference	Maximum
net8 1.2.3.4	71.69 Mbps	2.34 Mbps	69.35 Mbps	105.26 Mbps @ 03:00
	22.20 Kpps	712 pps	21.49 Kpps	32.58 Kpps @ 03:00

Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Summary of all Data Snapshots Collected:

	Bytes	Packets	Bytes/Pkt	bps
	308.01 GB	762,849,500	404 B	76.05 Mbps
				23.54

Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Source Addresses

Network / Mask	Bytes	Packets	Bytes/Pkt	bps
192.168.20.217/32	168.22 GB	416,436,800	404 B	41.54 Mbps
192.168.18.187/32	139.53 GB	345,372,800	404 B	34.45 Mbps

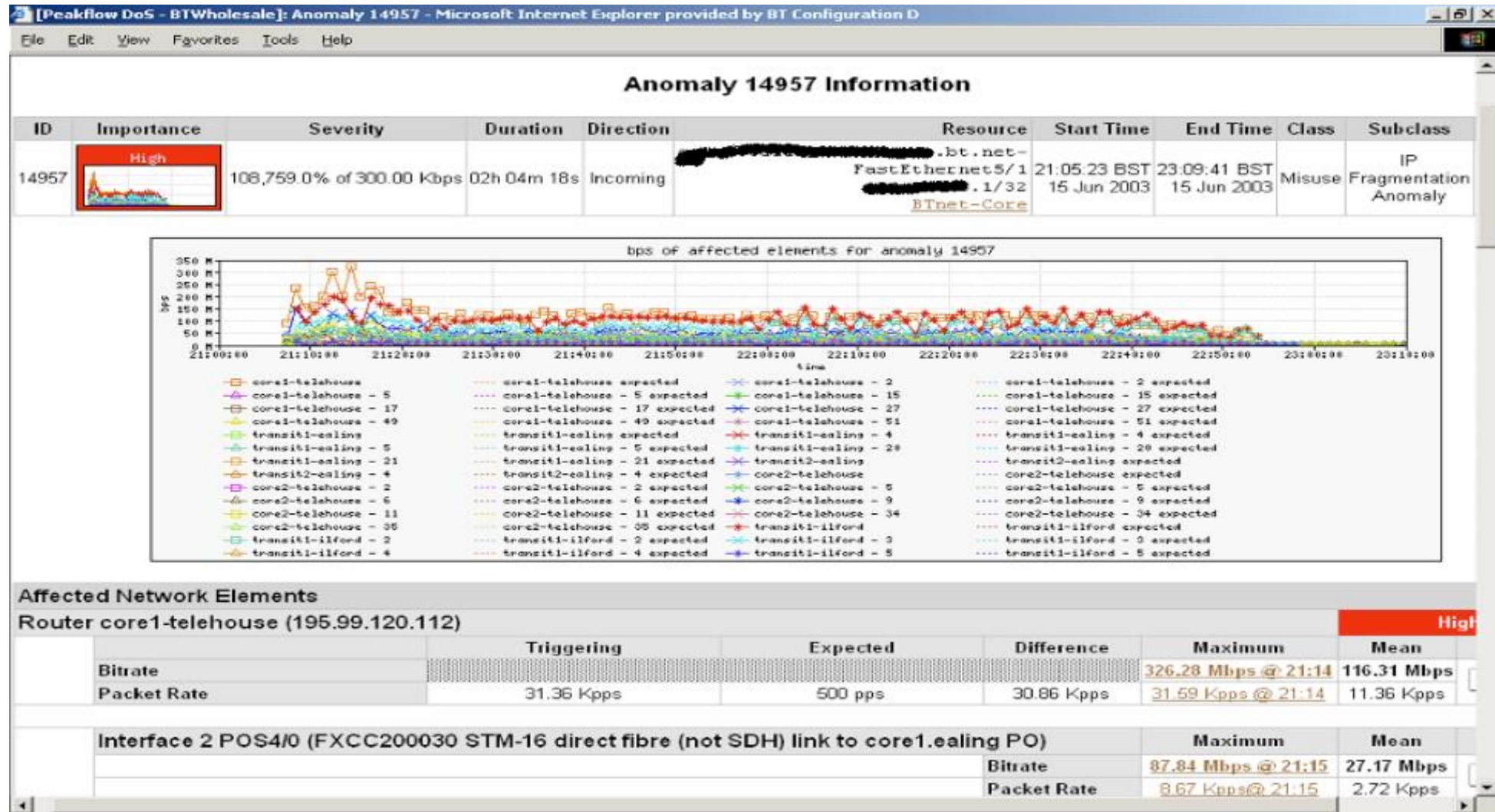
Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Destination Addresses

How to Identify a Security Attack?

- Suddenly highly-increased overall traffic in the network
- Higher CPU and memory utilization of network devices
- Unexpectedly large amount of traffic generated by individual hosts
- Increased number of accounting records generated
- Multiple accounting records with abnormal content, like one packet per flow record (e.g. TCP SYN flood)
- A changed mix of traffic applications, e.g. a sudden increase of "unknown" applications
- An increase of certain traffic types and messages, e.g. TCP resets or ICMP messages
- An increasing number of ACL violations

A Large Scale DOS attack



What Does a DOS Attack Look Like?

Potential DoS Attack on Router

Estimated: 660 pkt/s 0.2112 Mbps

```
Router# show ip cache flow
```

SrcIf	SrcIPAddress	SrcP	SrcAS	DstIf	DstIPAddress	DstP	DstAS	Pr	Pkts	B/Pk
29	192.1.6.69	77	aaa	49	194.20.2.2	1308	bbb	6	1	40
29	192.1.6.222	1243	aaa	49	194.20.2.2	1774	bbb	6	1	40
29	192.1.6.108	1076	aaa	49	194.20.2.2	1869	bbb	6	1	40
29	192.1.6.159	903	aaa	49	194.20.2.2	1050	bbb	6	1	40
29	192.1.6.54	730	aaa	49	194.20.2.2	2018	bbb	6	1	40
29	192.1.6.136	559	aaa	49	194.20.2.2	1821	bbb	6	1	40
29	192.1.6.216	383	aaa	49	194.20.2.2	1516	bbb	6	1	40
29	192.1.6.111	45	aaa	49	194.20.2.2	1894	bbb	6	1	40
29	192.1.6.29	1209	aaa	49	194.20.2.2	1600	bbb	6	1	40
...

Typical DoS Attacks Have the Same (or Similar) Flow Entries:

- Input Interface (SrcIf)
- Destination IP (DstIf)
- 1 Packet per flow (Pkts)
- Bytes per packet (B/Pk)

Trends in Malware Evolution

- Botnets:
 - Distributed Management (C&C Servers/anti-network forensics techniques, such as randomized and encrypted packets that made traffic filtering difficult.
 - Full-Featured Control (remote access trojans (RATs), designed to facilitate remote control of individual compromised endpoints.
 - Sophisticated endpoint control with automated propagation techniques, automated self-update mechanisms, and multilayer, hierarchical, and/or peer-to-peer C&C channels.
 - Also legitimate enterprise networks, including internal DNS, web, email, and software update mechanisms.

Encryption and Obfuscation

- Hiding C&C Channels
- Maintaining Control
- Hiding and encrypted IRC
- Peer-to-Peer C&C
- Pool Ips
- Blind Redirection
- Fast-Flux DNS
- DGA domains
- Tor-based C&C

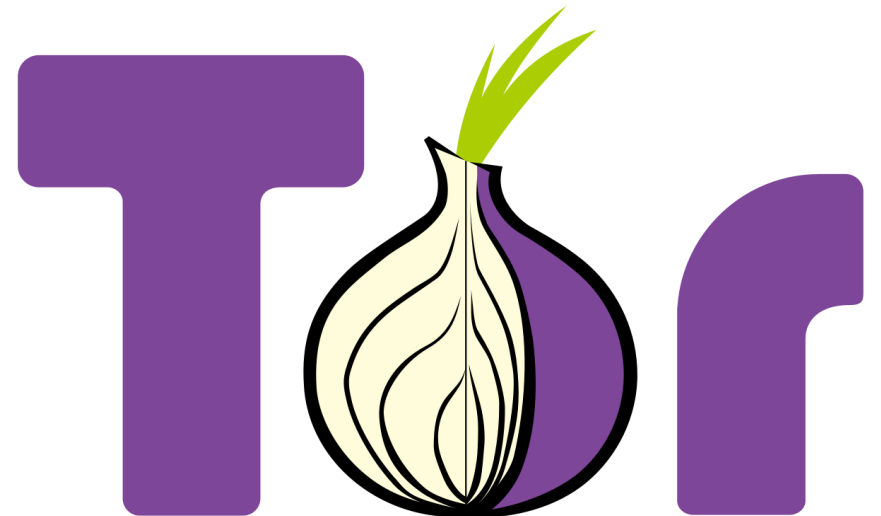
Code: 0: getstatic #2; //Field java/lang/System.out:Ljava/i-
o/PrintStream; 3: ldc #3;; invokevirtual #4; //Method ja-
va/io/PrintStream.println:(Ljava/lang/String;)V okestatic #5;



//Method 1000 6: System.out: **#PART-1**
sipush 1000 6: ldc #3;; if_icmpge 44 9: iconst_2 10: isto-
re_2 11: iload_2 12: iload_1 13: if_icmpge 31 16: cp 34

Tor-based Botnets and Tor Traffic Analysis

- The Tor network is operating in the Transport layer of the OSI, the onion proxy software shows customers the Secure Socket interface (SOCKS) which operates in the session layer.
- The Tor network can use the TCP port 443, which is used by the HTTPS, so that the supervision and interpretation of a session exclusively with the determination of the door cannot constitute a reliable method.



Tor Traffic Analysis

The screenshot shows the Wireshark network protocol analyzer interface. The filter bar is set to `x509sat.DirectoryString`. The packet list pane shows several TLSv1 records, with packet 206 selected. The packet details pane shows the structure of the selected certificate, with the issuer and subject fields highlighted in red boxes. The issuer is `rdnSequence (0)` with one item: `id-at-commonName=www.s5rc22gpzrwt4e.com`. The subject is `rdnSequence (0)` with one item: `id-at-commonName=www.qzsg2ioaoplbs2gaha5.net`. The packet bytes pane shows the raw data of the TLSv1 record, with the first few bytes highlighted in orange.

Filter: `x509sat.DirectoryString` Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
107	2.267706	198.27.97.223	10.0.0.126	TLSv1	803	Server Hello, Certificate, Server Key Exchange, Server Hello Done
125	2.281025	66.18.12.197	10.0.0.126	TLSv1	994	Server Hello, Certificate, Server Key Exchange, Server Hello Done
141	2.320225	212.83.140.45	10.0.0.126	TLSv1	801	Server Hello, Certificate, Server Key Exchange, Server Hello Done
143	2.320285	64.62.249.222	10.0.0.126	TLSv1	788	Server Hello, Certificate, Server Key Exchange, Server Hello Done
175	2.349662	31.7.186.228	10.0.0.126	TLSv1	809	Server Hello, Certificate, Server Key Exchange, Server Hello Done
184	2.366189	82.96.35.8	10.0.0.126	TLSv1	802	Server Hello, Certificate, Server Key Exchange, Server Hello Done
186	2.366273	95.211.225.167	10.0.0.126	TLSv1	815	Server Hello, Certificate, Server Key Exchange, Server Hello Done
202	2.384445	88.159.20.120	10.0.0.126	TLSv1	1001	Server Hello, Certificate, Server Key Exchange, Server Hello Done
204	2.384602	212.83.158.5	10.0.0.126	TLSv1	807	Server Hello, Certificate, Server Key Exchange, Server Hello Done
206	2.385513	80.100.45.156	10.0.0.126	TLSv1	996	Server Hello, Certificate, Server Key Exchange, Server Hello Done

▼ Certificate (id-at-commonName=www.qzsg2ioaoplbs2gaha5.net)

- ▼ signedCertificate
 - version: v3 (2)
 - serialNumber : 0x00a0d20578a2e6562e
 - ▶ signature (shaWithRSAEncryption)
 - 7 issuer: rdnSequence (0)
 - ▶ rdnSequence: 1 item (id-at-commonName=www.s5rc22gpzrwt4e.com)
 - ▶ validity
 - ▼ subject: rdnSequence (0)
 - ▶ rdnSequence: 1 item (id-at-commonName=www.qzsg2ioaoplbs2gaha5.net)
 - ▶ subjectPublicKeyInfo
 - ▶ algorithmIdentifier (shaWithRSAEncryption)
 - Padding: 0
 - encrypted: 9d9e02d11df69e3a5342fdc03383bbf462c582ee8abd3392...
 - ▶ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange

```
3080 cd 00 01 ca 00 01 c7 30 82 01 c3 30 82 01 2c a0 .....0 ...0...
3090 03 02 01 02 02 09 00 a0 d2 05 78 a2 e6 56 2e 30 .....x.V.0
30a0 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00 30 21 ...*.H. ....!
30b0 31 1f 30 1d 06 03 55 04 03 13 16 77 77 77 2e 73 1.0...U. ...www.s
30c0 35 72 63 32 32 67 70 7a 72 77 74 34 65 2e 63 6f 5rc22gpz rwt4e.co
30d0 6d 30 1e 17 0d 31 33 31 32 33 30 31 39 35 34 30 m0...131 23019540
```

How can an organization detect an attacker who has already entered the network with legitimate credentials?



**WOLF IN SHEEP'S
CLOTHING**

Detecting Algorithmically Generated Malicious Domains

DGA Algorithm: Generates a domain by the current date

```
1. defgenerate_domain(year, month, day):
2.     """Generates a domain by the current date"""
3.     domain = ""
4.     for i in range(32):
5.         year = ((year ^ 8 * year) >> 11) ^ ((year & 0xFFFFFFFF) << 17)
6.         month = ((month ^ 4 * month) >> 25) ^ 9 * (month & 0xFFFFFFFF8)
7.         day = ((day ^ (day << 13)) >> 19) ^ ((day & 0xFFFFF0FE) << 12)
8.         domain += chr(((year ^ month ^ day) % 25) + 97)
9.     domain += '.com'
10. return domain
```

E.g., on June 18th, 2014, this method would generate the following domain names:

k.com	kafph.com	kafphogvi.com	kafphogvifahu.com
ka.com	kafpho.com	kafphogvif.com	kafphogvifahut.com
kaf.com	kafphog.com	kafphogvifa.com	kafphogvifahutb.com
kafp.com	kafphogv.com	kafphogvifah.com	kafphogvifahutbl.com

WCry Ransomware Analysis

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	57	41	4E	41	43	52	59	21	00	01	00	00	54	54	15	97	WANACRY!....TT.-
00000010	2D	1F	9A	10	07	4C	33	8A	BB	38	2F	33	AA	74	7C	96	-.š..L3Š»8/3^t -
00000020	16	C4	01	FB	6A	F9	E5	42	6E	83	53	CA	EA	6A	20	B7	.Ä.ûjùâBnfSÊêj -
00000030	D2	88	07	21	16	70	80	C1	7D	A0	A5	28	8E	39	D7	4E	Ò^.! .p€Á) ¥(Ž9×N
00000040	CA	A0	34	90	80	FC	FB	03	09	0B	FD	BB	86	78	1B	E4	Ê 4.€üû...ý»+x.ä
00000050	5B	AB	F0	A1	35	A2	A5	33	A9	A1	F6	EE	47	B8	8F	2E	[«š;5¢¥3€;öîG,..
00000060	4C	53	FC	D3	4C	1E	16	DF	89	F9	35	2F	63	F6	E0	FB	LSüÓL..B%ù5/cöàû
00000070	A8	25	1D	96	11	A6	0A	2A	D9	94	B6	71	C7	09	2F	8B	~%.-.!.*Û"ŕqÇ./<
00000080	D6	D8	22	FD	C0	A4	12	53	9E	DD	FB	DA	65	9B	03	89	Öø"ýÀ¤.SžÝûÚe>.%
00000090	A8	8B	37	84	06	84	F8	EF	8B	A0	B4	87	82	57	06	EA	~<7...øi< '†,W.ê
000000A0	82	7D	49	01	64	61	5E	50	37	47	0E	7A	51	00	CE	A5	,)I.da^P7G.zQ.Î¥
000000B0	E2	AE	E7	5E	4F	60	1B	C2	04	4E	EA	D9	59	FA	45	68	â@ç^O`.Ä.NèÛYúEh
000000C0	98	5A	BD	56	BC	A6	68	7F	C4	87	69	96	84	89	00	03	~Z%V%¡h.Ä+i-...%
000000D0	47	6A	2B	7C	96	4D	D9	42	57	05	0C	1F	02	16	FB	64	Gj+ -MÜBW.....ûd
000000E0	DE	F0	39	7D	52	83	FA	FF	19	49	5E	6C	99	5E	E2	14	Bš9)Rfúÿ.I^l™^â.
000000F0	92	D4	66	57	16	98	F0	B0	84	A8	FD	4E	E5	BC	70	3D	'ÔfW.~š°...ýNâ%p=
00000100	CE	25	4B	1C	8B	14	DA	48	7B	86	4C	51	04	00	00	00	Î%K.<.ÚH{†LQ}....
00000110	8B	6E	03	00	00	00	00	00	D9	0A	05	5F	4A	E4	E0	E6	<n.....Û.._Jääæ
00000120	35	5E	44	7A	DD	DE	3E	4D	DA	6D	8C	EE	FB	FD	5A	AE	5^DzÝB>MÚmEiûÿZ@
00000130	47	80	D3	CC	F8	6F	6F	72	2D	01	1B	C7	D4	9B	ED	A3	GEÓÏøoor-..ÇÔ>if
00000140	12	A9	1C	DE	A1	A4	BB	6D	39	28	47	9D	E8	FA	53	EE	.@.P;¤»m9(G.èúSi
00000150	1A	8D	56	B6	B5	6D	E6	2A	E5	51	A7	DF	C7	90	3D	CD	..Vŕumæ*âQ\$BÇ.=Í
00000160	69	09	53	DF	BC	78	BC	A4	B1	C3	DC	56	8B	A1	AE	9A	i.SB%¤%±ÄÛV<;@š
00000170	C0	E0	F3	C7	1F	EA	A4	6B	BF	DB	DC	E5	A6	FC	C9	72	ÀàóÇ.ê¤k;ÛÛâ;úÉr

What Is PCAP?

- PCAP == **P**acket **C**apture
- PCAP is a straight copy of ALL* network traffic that flows through the pipe for as long as you keep recording. That can be a LOT of data!
- Complete record of network activity
 - Layers 2 – 7
- Most common format is `libpcap`
- Things to think about
 - How long do you need to listen?
 - Can your NIC capture it fast enough?
 - Can your hard drive store it fast enough?
 - How long can you listen before you have to free up space?

PCAP data

What does it look like?



mytrace.pcapng — Locked

Position: ISO_8859-1:1987 Grammar: PCAPNG Parse File: <none>

Position	Offset	Length	Index	Element	Value
0x00	0	12847128	0	PCAPNG file [0]	
0x00	0	12847128	0	Blocks [0]	
0x00	0	148	0	Section Header Block [0]	
0x00	0	4	0	BlockType	SectionHeader: 0xA0D0D0A
0x04	+4	4	1	TotalLength	0x94
0x08	+8	136	2	Body [0]	
0x08	0	4	0	Byte-OrderMagic	0x1A2B3C4D
0x0C	+4	2	1	MajorVersion	1
0x0E	+6	2	2	MinorVersion	0
0x10	+8	8	3	SectionLength	-1
0x18	+16	120	4	Options [0]	
0x18	0	28	0	Comment Option [0]	section header block
0x34	+28	12	1	Hardware Option [0]	x86_64
0x40	+40	20	2	OS Option [0]	Darwin 15.5.0
0x54	+60	56	3	User Application Opti...	tcpdump (libpcap version 1.5...
0x8C	+116	4	4	End of Options [0]	
0x90	+144	4	3	TotalLength2	0x94
0x94	+148	32	1	Interface Description Block [0]	
0x94	0	4	0	BlockType	0x00000001: 0x1
0x98	+4	4	1	TotalLength	0x20
0x9C	+8	20	2	Body [0]	
0x9C	0	2	0	LinkType	LINKTYPE_ETHERNET: 1
0x9E	+2	2	1	Reserved	0
0xA0	+4	4	2	SnapLen	262144
0xA4	+8	12	3	Options [0]	
0xA4	0	8	0	Interface Name Optio...	en0
0xAC	+8	4	1	End of Options [0]	
0xB0	+28	4	3	TotalLength2	0x20
0xB4	+180	96	2	Enhanced Packet Block [0]	FF FF FF FF FF FF BC 16 65 C...
0xB4	0	4	0	BlockType	0x00000006: 0x6
0xB8	+4	4	1	TotalLength	0x60
0xBC	+8	84	2	Body [0]	FF FF FF FF FF FF BC 16 65 C...
0xBC	0	4	0	InterfaceID	0
0xC0	+4	4	1	Timestamp (High)	341749
0xC4	+8	4	2	Timestamp (Low)	610728766
0xC8	+12	4	3	CapturedLength	42
0xCC	+16	4	4	PacketLength	42

Start End Length Content
0x144 0x75F 0x61C ø6...g\$ê...ê...M^ç ©RT.øÑ6..E..ÛÝ|@.3.k?*Q~.tn.»Bø.....<ø...BÅ....

PCAPNG file[0] > Blocks[0] > Enhanced Packet Block[0] > Body[0] > InterfaceID[0]

Position Module Number Severity Message
Empty Hide if successful

No Debug Messages

postdoc...

Γ Φάση

Ανάπτυξη ευφυούς πληροφοριακού συστήματος διαχείρισης και ανάλυσης δεδομένων μεγάλης κλίμακας

Big Data
Tools

ML Tools

Cloud IaaS

Crypto
Blockchain

Visual
Analytics



All data originates in real-time!

SLURRY A TRANSFER SECTION







30 Billion

Connected Devices



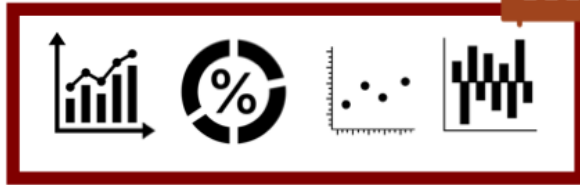
Generates



500 Zettabytes

Data/Year

Data Processing at Edge



Real-Time Data Analytics at Edge

Assists

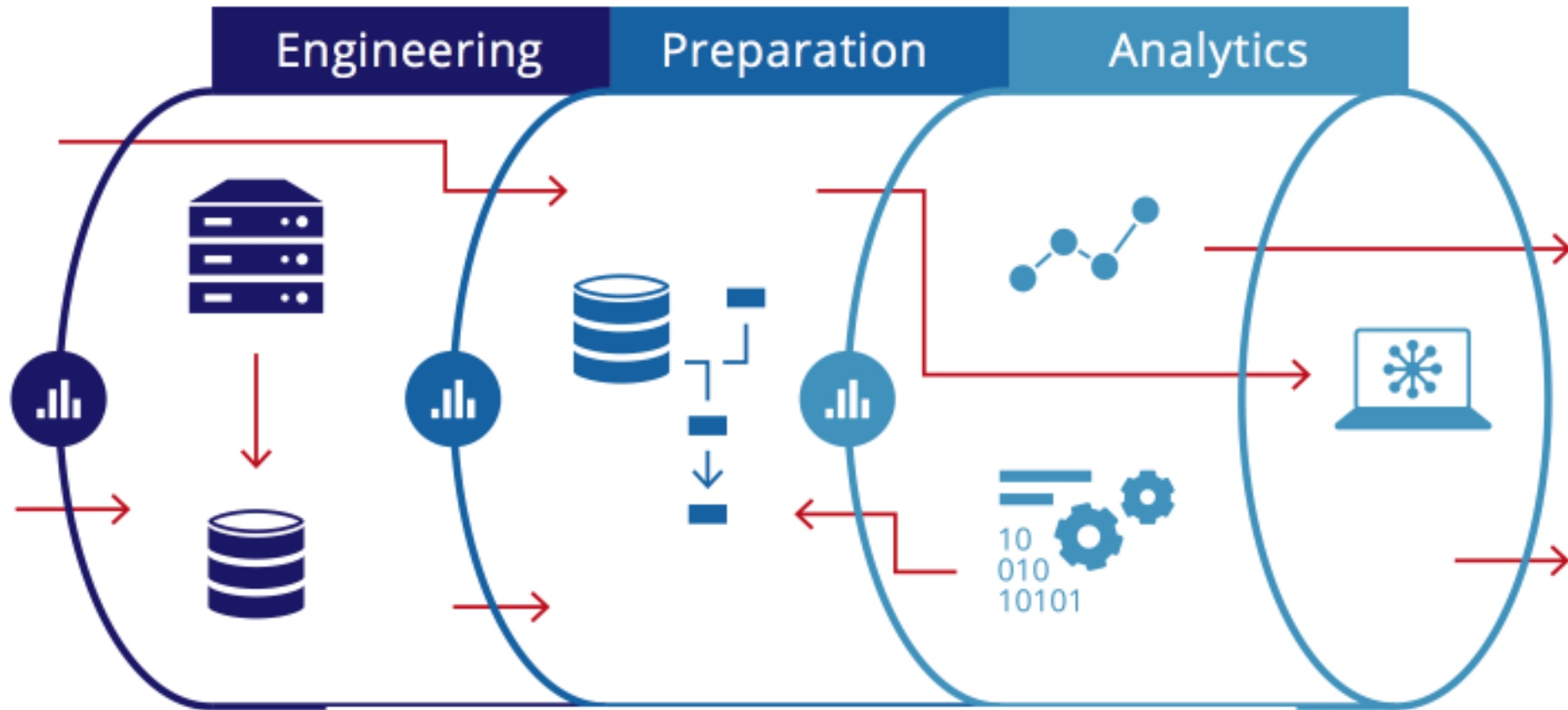


Quick Business Decisions

Data Processing in Cloud



Data Analytics in Cloud



- Administration
- Security
- Lifecycle Management
- Data Provenance
- Dynamic Data Pipeline
- Monitoring
- Automation

okeanos

CREATE



Create a new Project. Name it, describe its purpose, choose virtual resources to be granted to members, and submit. Your application will be reviewed, and if

JOIN



Request to be a member of an existing Project and instantly gain access to the resources it has to offer you. Search for public Projects, or submit a join

MY PROJECTS

Search:

Name	Status ▼	Application	Expiration	Members	Action
System project	Accepted member	17/11/2014	17/11/2114	1	
biosecurity.fmenr.duth.gr	Denied	23/04/2014	31/12/2016	0	
biosecurity.filab.duth.gr	Denied	16/03/2015	31/03/2017	0	
biosecurity.filab.duth.gr	Denied	23/03/2015	31/01/2016	0	
tartarus.duth.gr	Pending	06/08/2018	31/12/2020	0	

Showing 1 to 5 of 5 entries

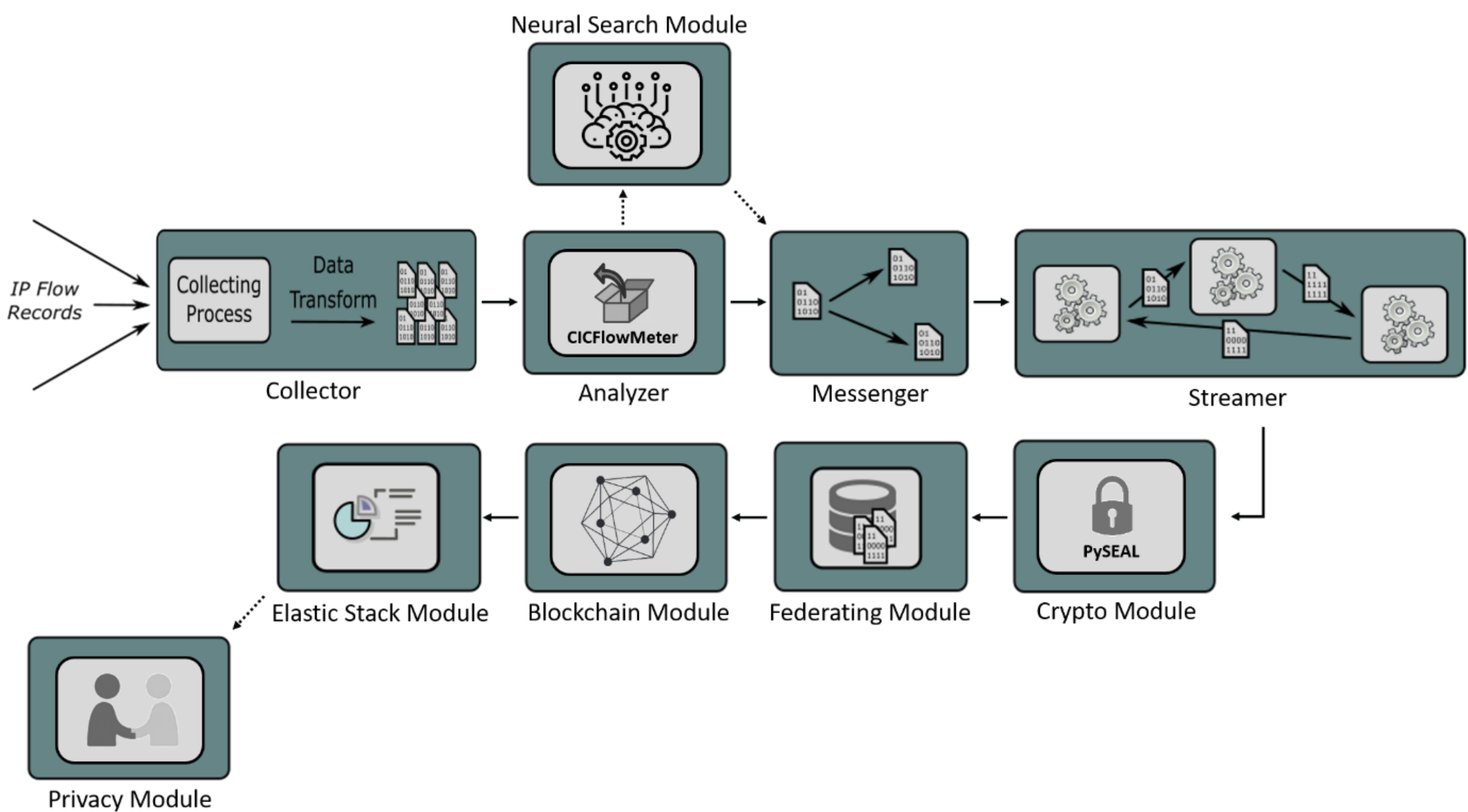
Pagination ▼

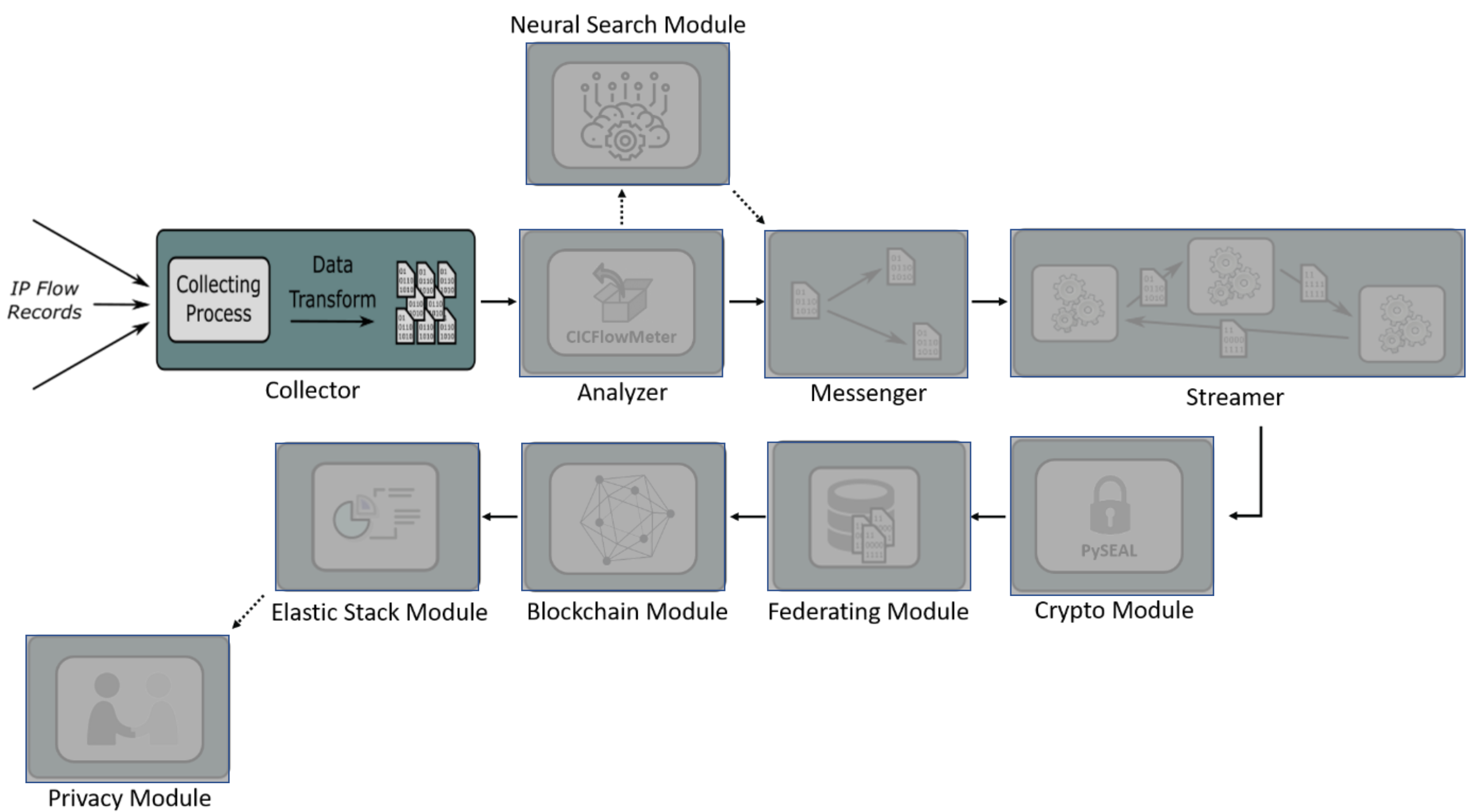
< Previous Next >

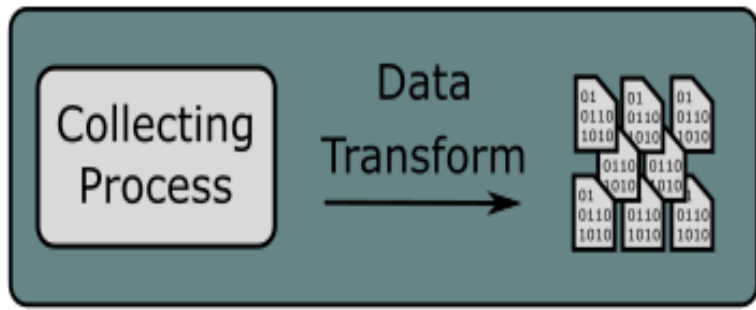
real-time anomaly detection over big data streams

- AutoAI
- Adaptive
- Scalable
- Portable
- Lightweight
- Secure
- Privacy
- Visual

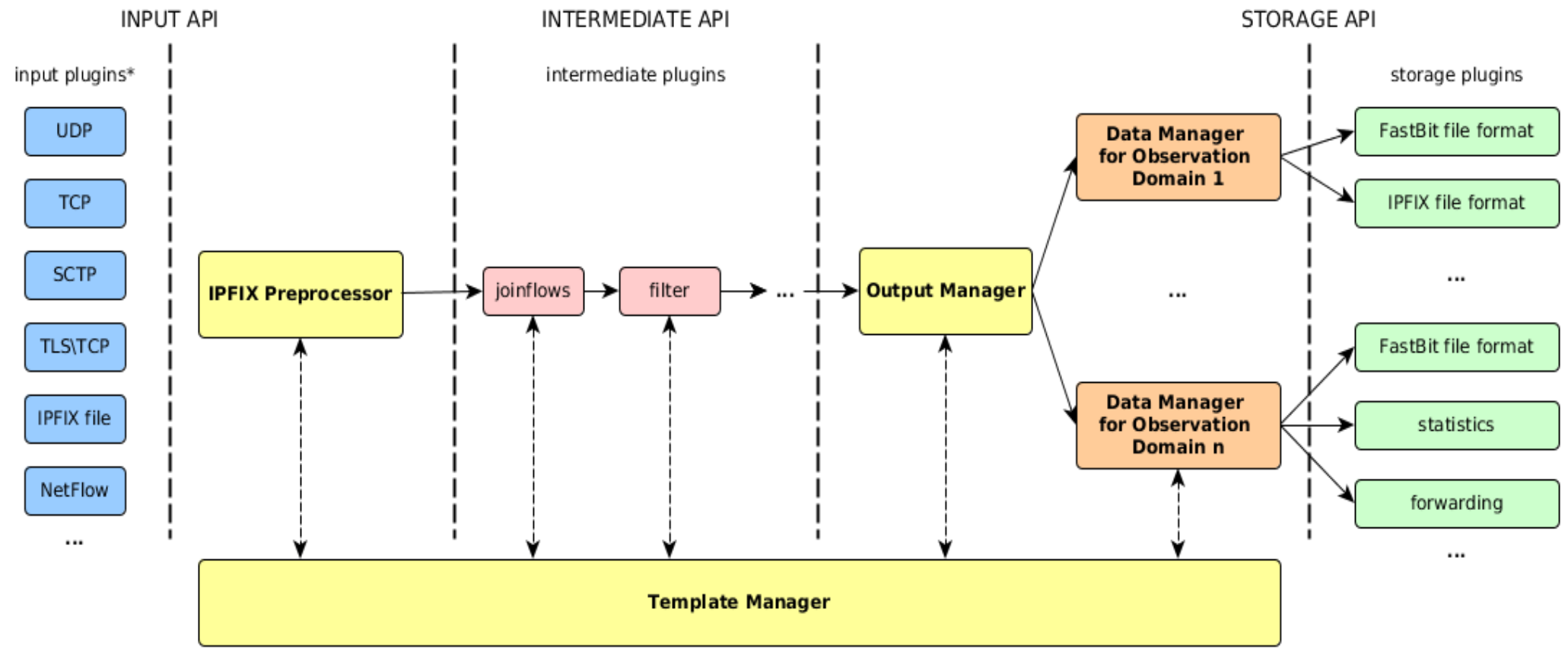




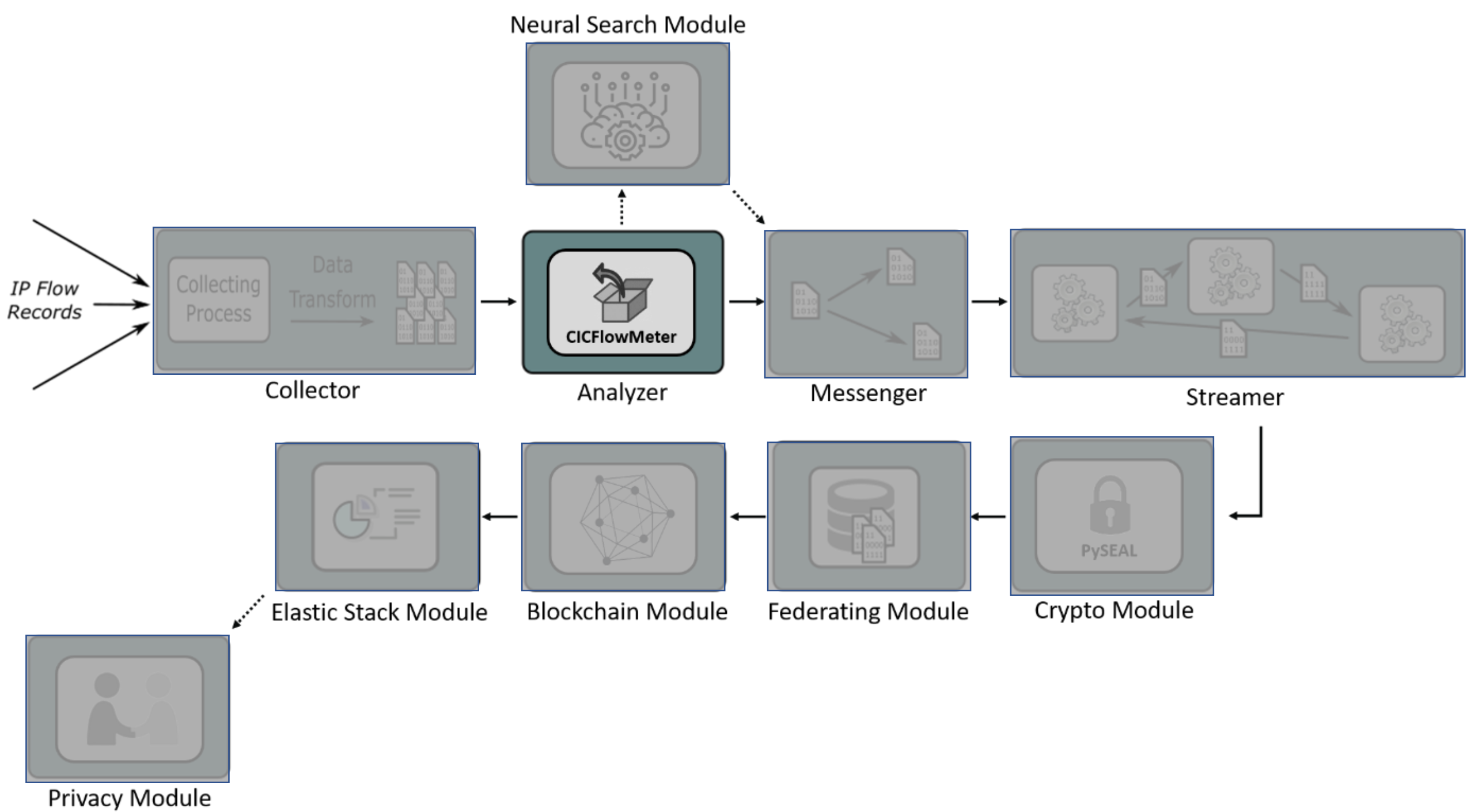


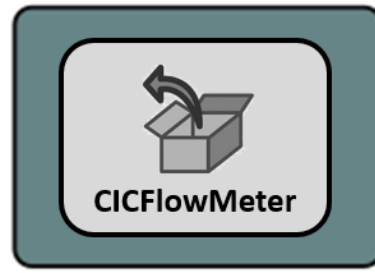


Collector

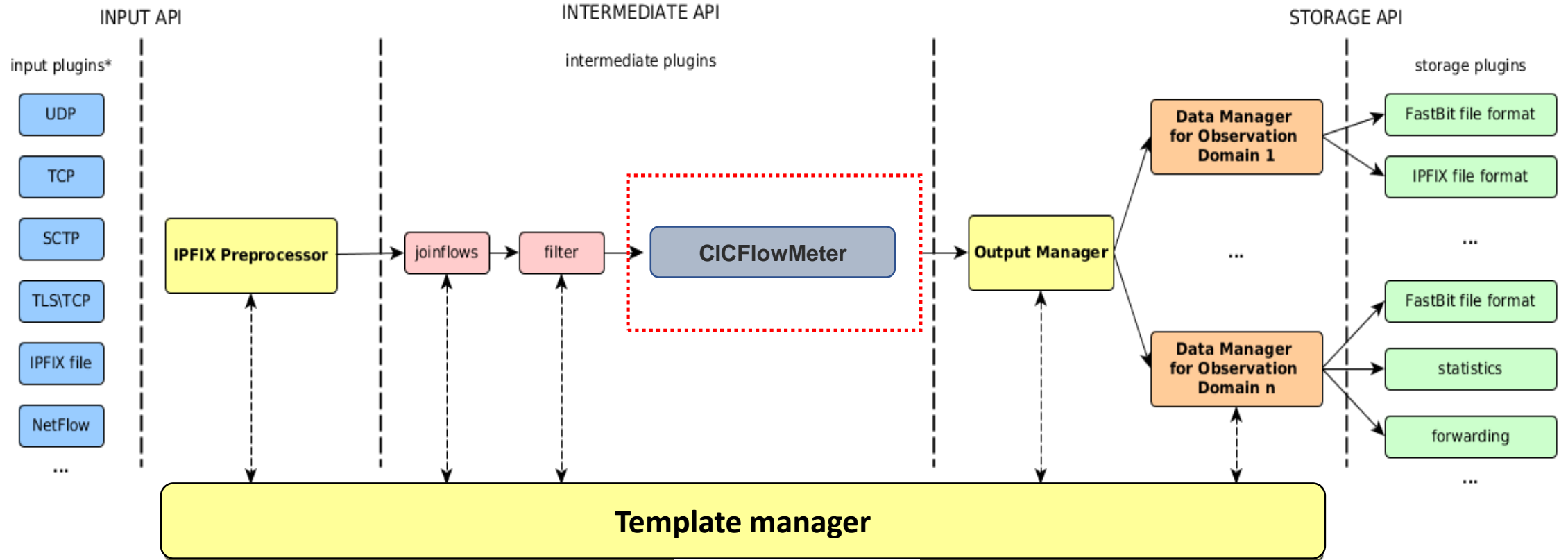


IPFIXcol

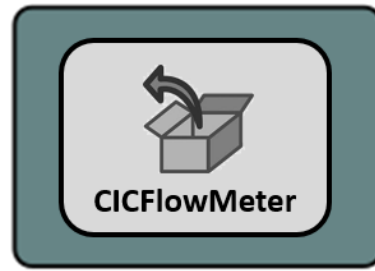




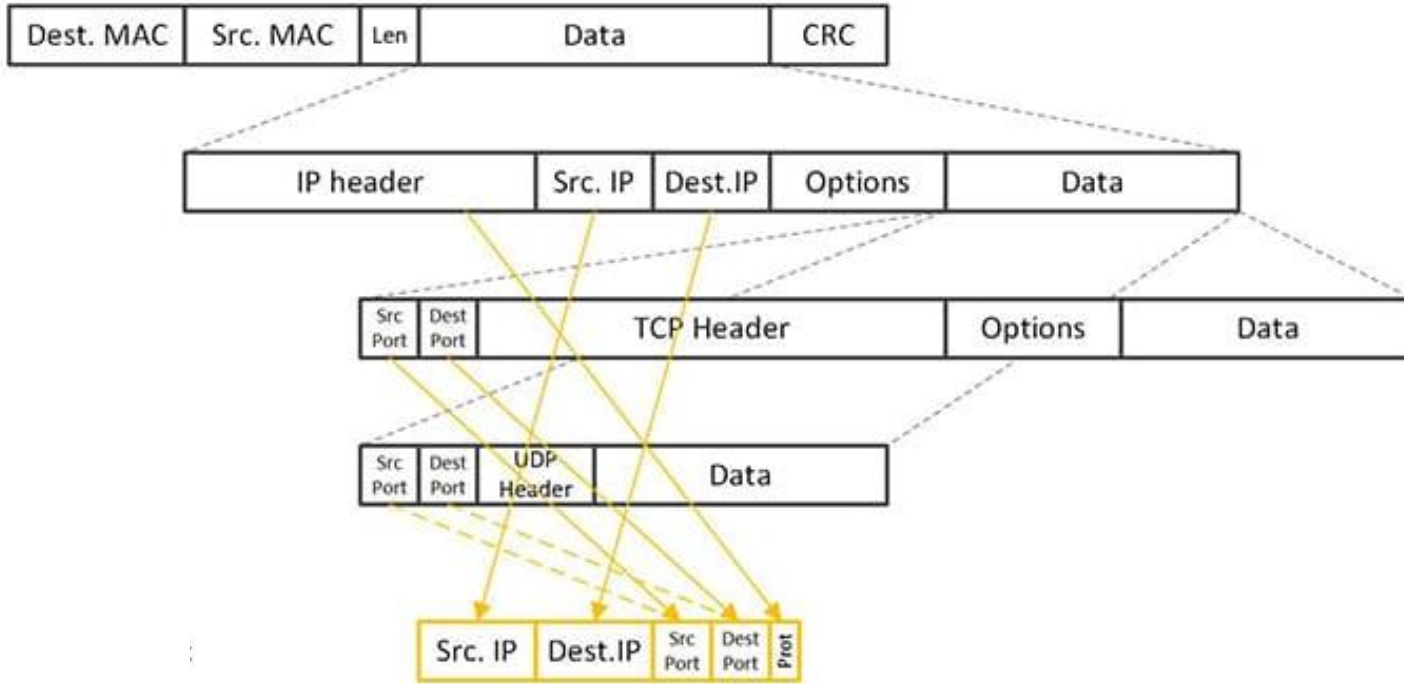
Analyzer



IPFIXcol

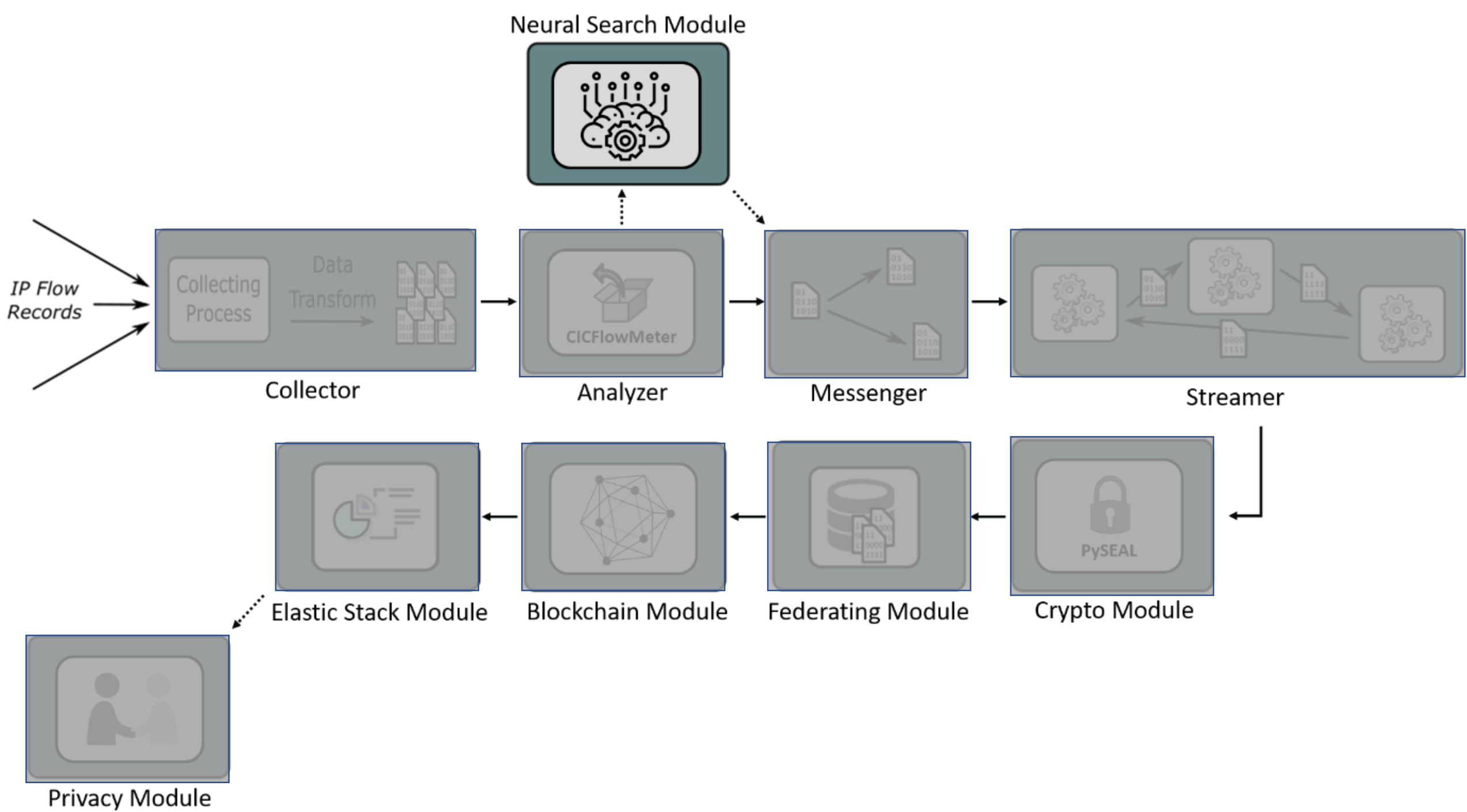


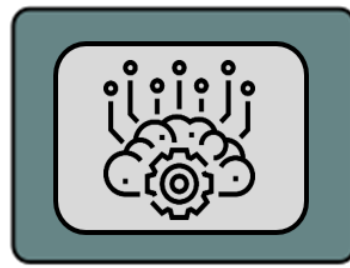
Analyzer



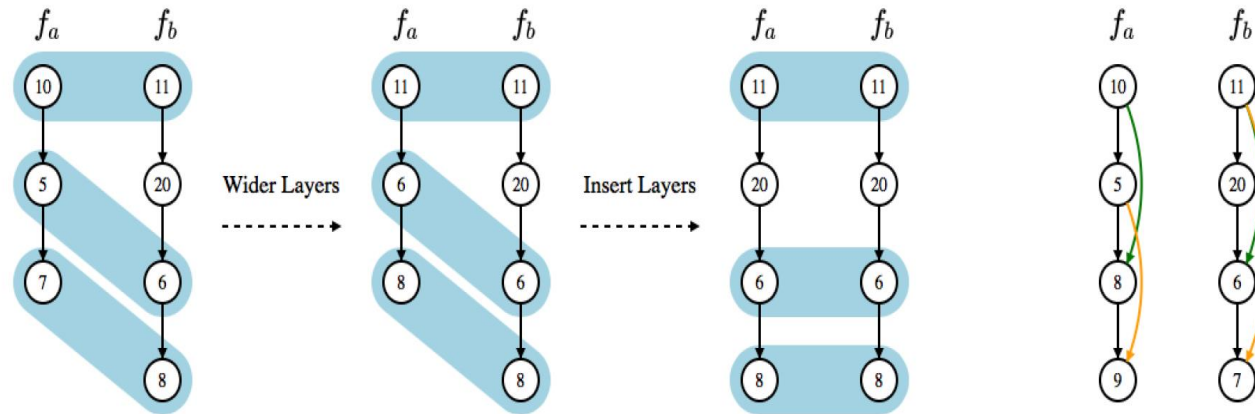
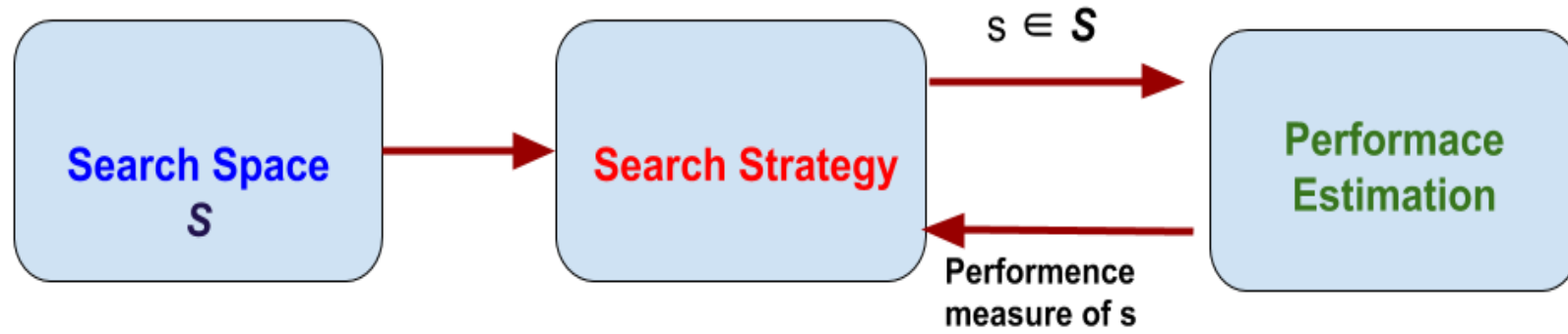
CICFlowMeter

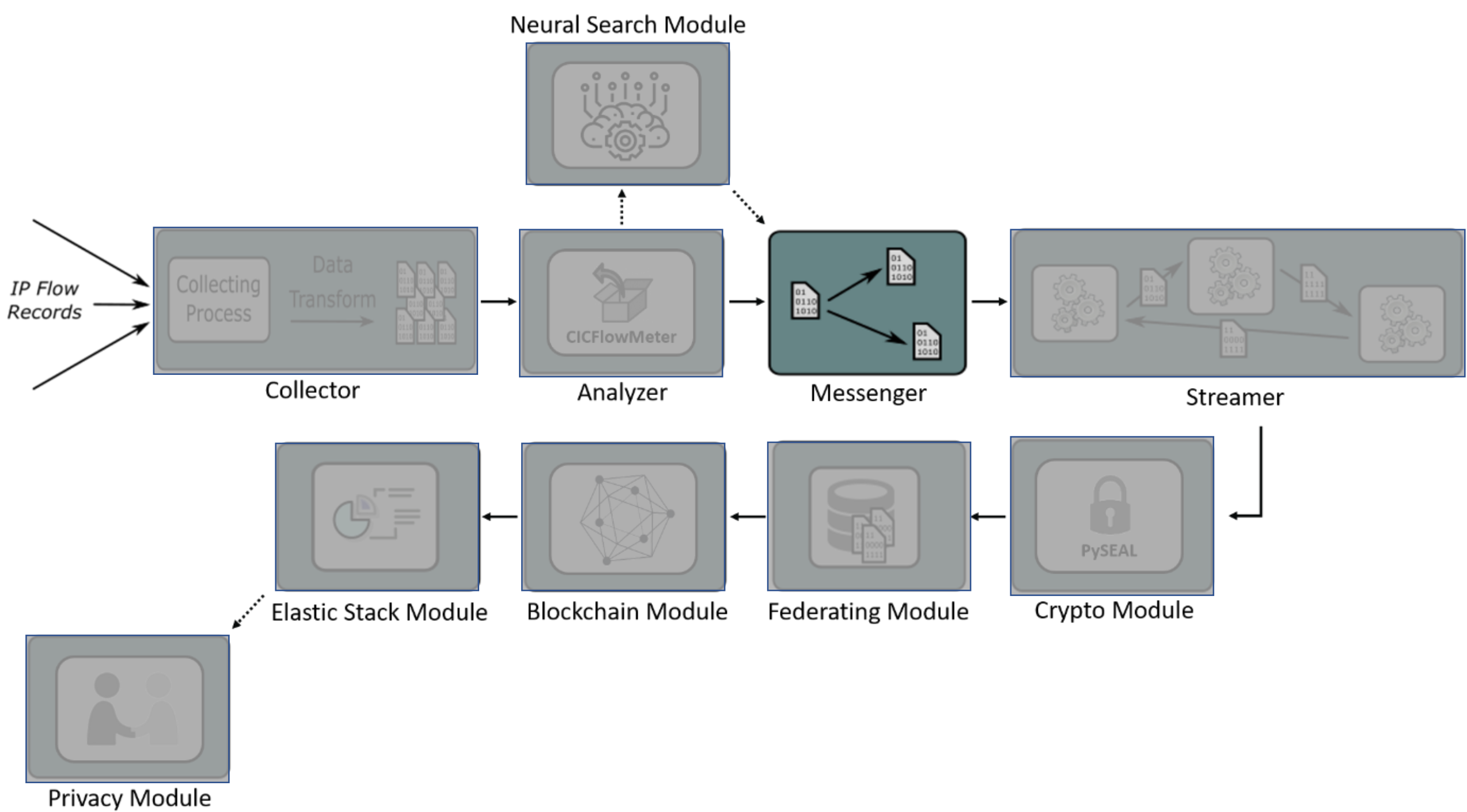
Feature Name	Feature Name	Feature Name
fl_dur	fl_byt_s	ece_cnt
tot_fw_pk	fl_pkt_s	down_up_ratio
tot_bw_pk	fl_iat_avg	pkt_size_avg
tot_l_fw_pkt	fl_iat_std	fw_seg_avg
fw_pkt_l_max	fl_iat_max	bw_seg_avg
fw_pkt_l_min	fl_iat_min	fw_byt_blk_avg
fw_pkt_l_avg	fw_iat_tot	fw_pkt_blk_avg
fw_pkt_l_std	fw_iat_avg	fw_blk_rate_avg
Bw_pkt_l_max	fw_iat_std	bw_byt_blk_avg
Bw_pkt_l_min	fw_iat_max	bw_pkt_blk_avg
Bw_pkt_l_avg	fw_iat_min	bw_blk_rate_avg
Bw_pkt_l_std	bw_iat_tot	subfl_fw_pk
fw_urg_flag	bw_iat_avg	subfl_fw_byt
bw_urg_flag	bw_iat_std	subfl_bw_pkt
fw_hdr_len	bw_iat_max	subfl_bw_byt
bw_hdr_len	bw_iat_min	fw_win_byt
fw_pkt_s	fw_psh_flag	bw_win_byt
bw_pkt_s	bw_psh_flag	fw_act_pkt
pkt_len_min	urg_cnt	fin_cnt
pkt_len_max	cwe_cnt	syn_cnt
pkt_len_avg	atv_avg	rst_cnt
pkt_len_std	atv_std	pst_cnt
pkt_len_va	atv_max	ack_cnt
idl_avg	atv_min	idl_max
idl_std	fw_seg_min	idl_min

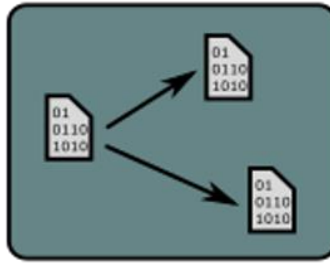




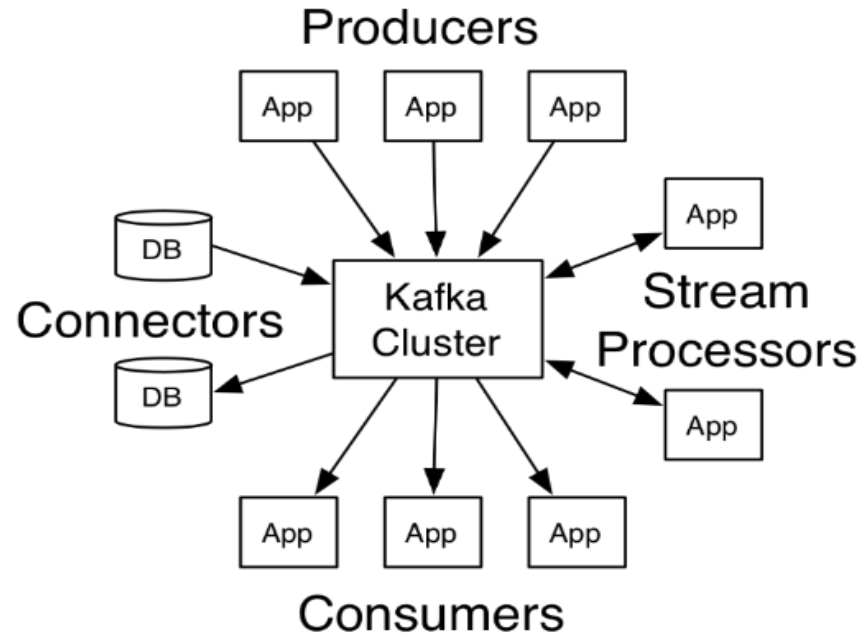
Neural Search Module

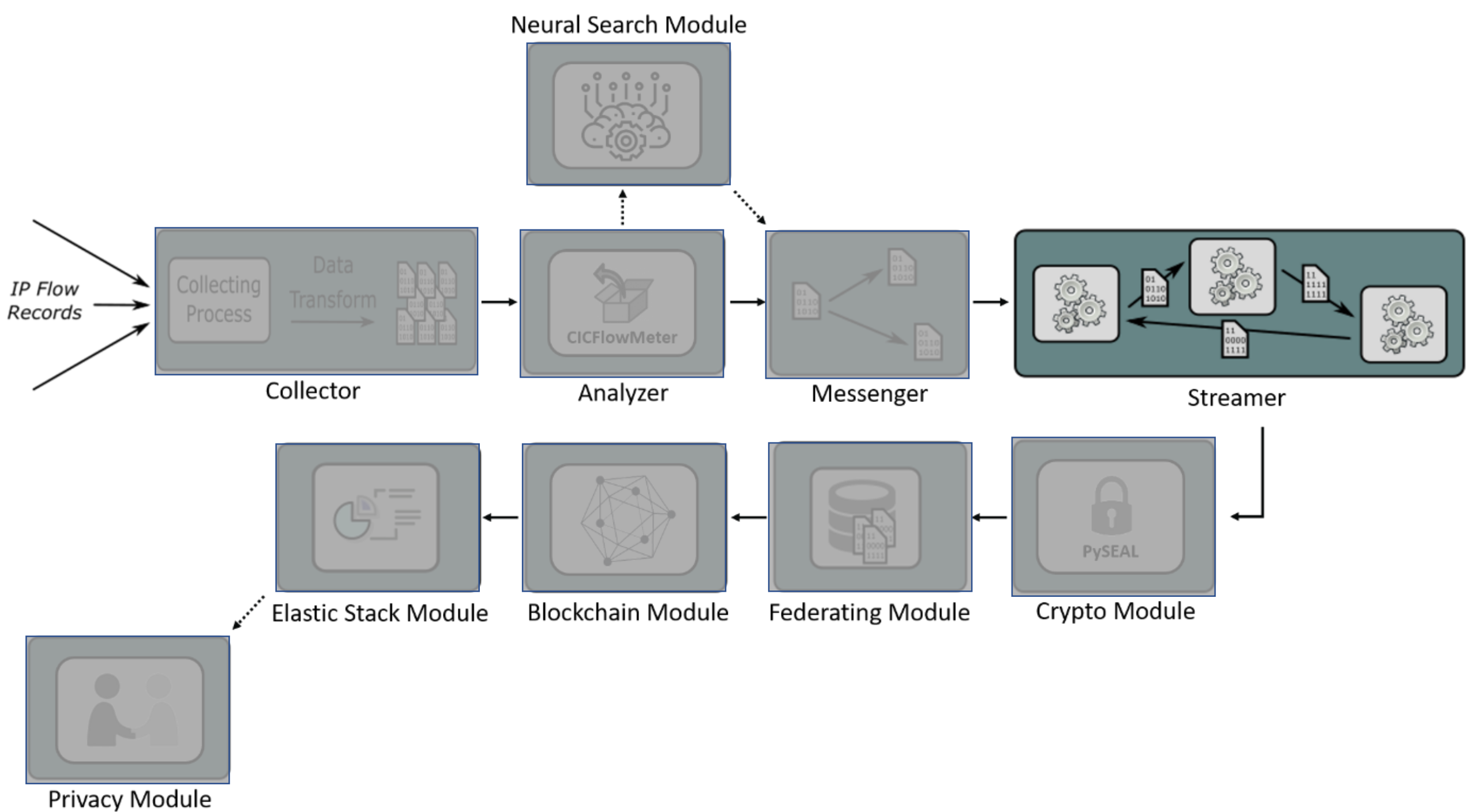


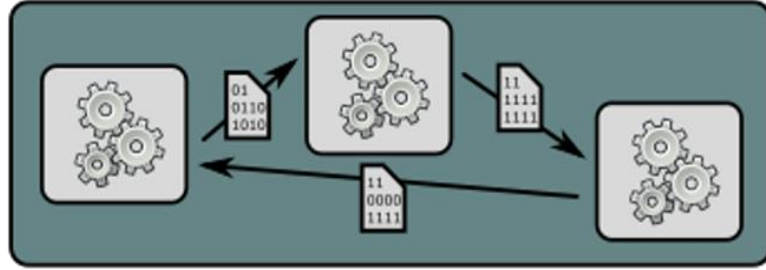




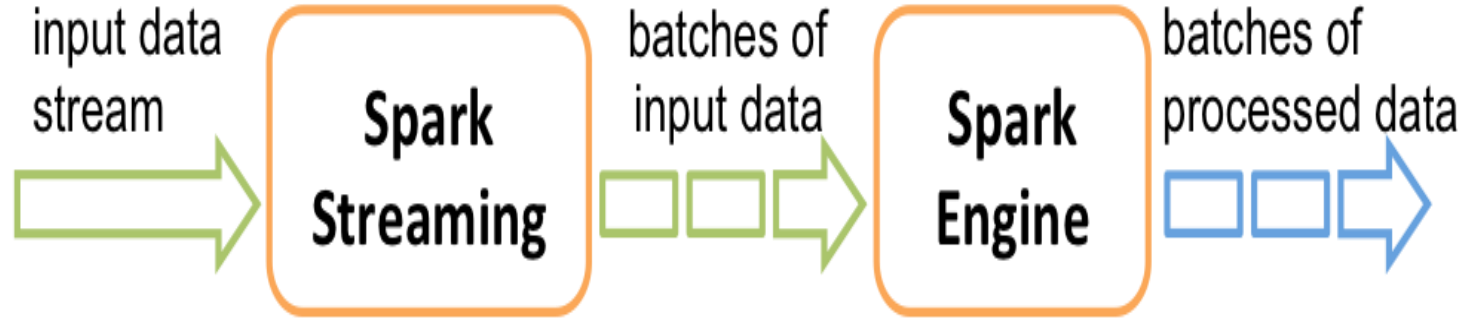
Messenger



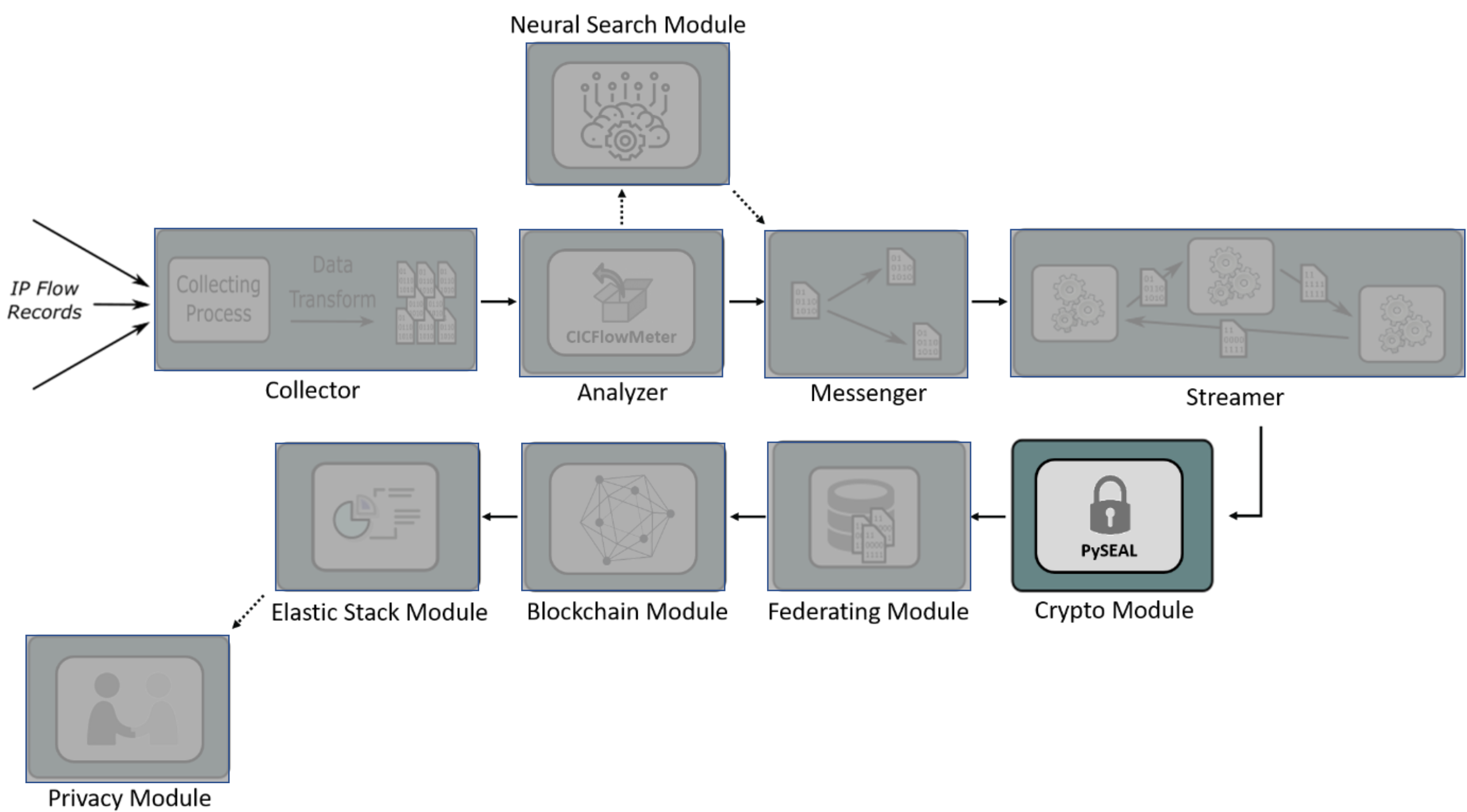




Streamer

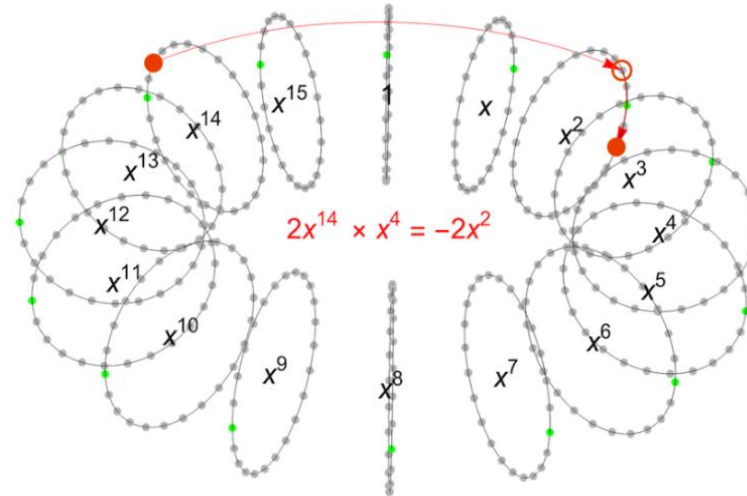


Spark
Streaming

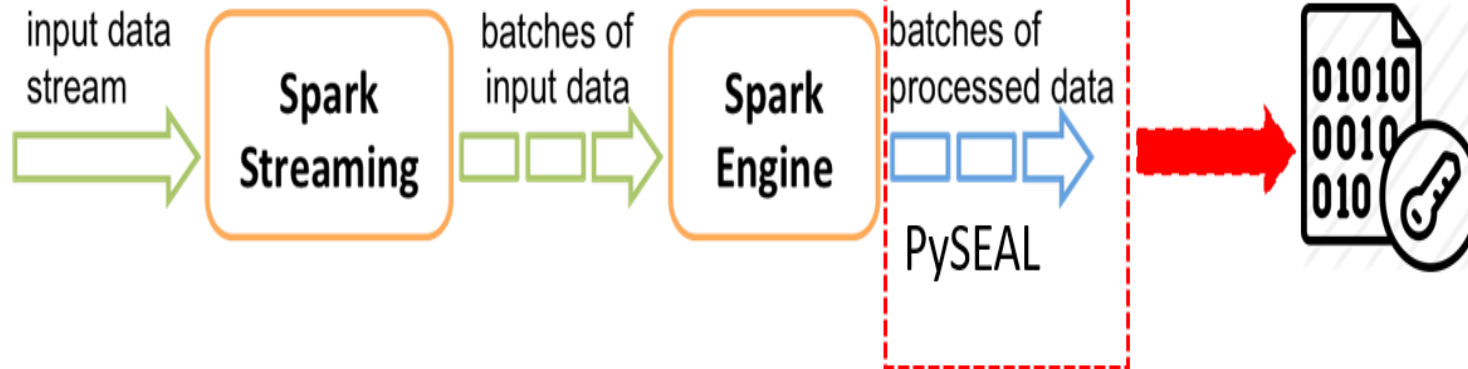


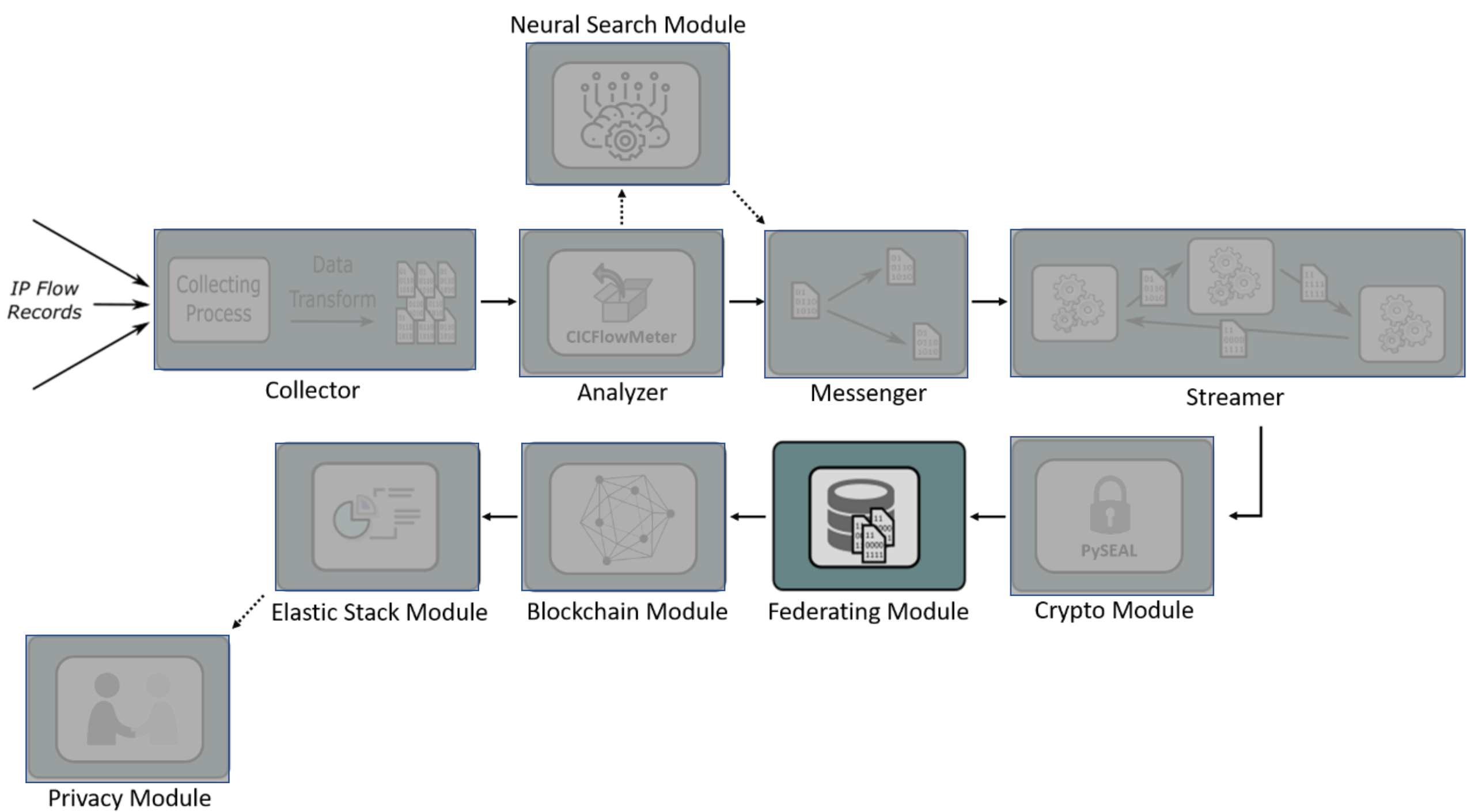


Crypto Module



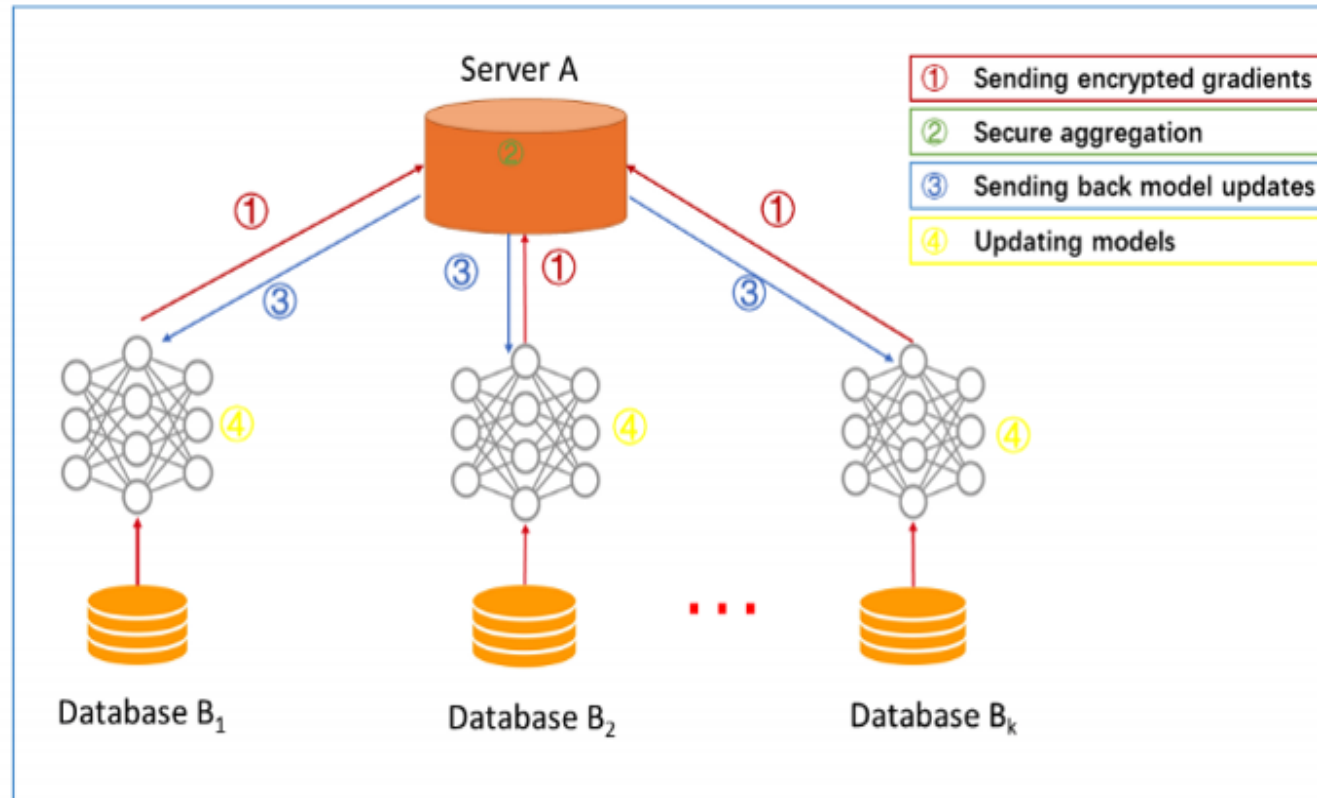
Secure Multi Party Computation
Homomorphic encryption

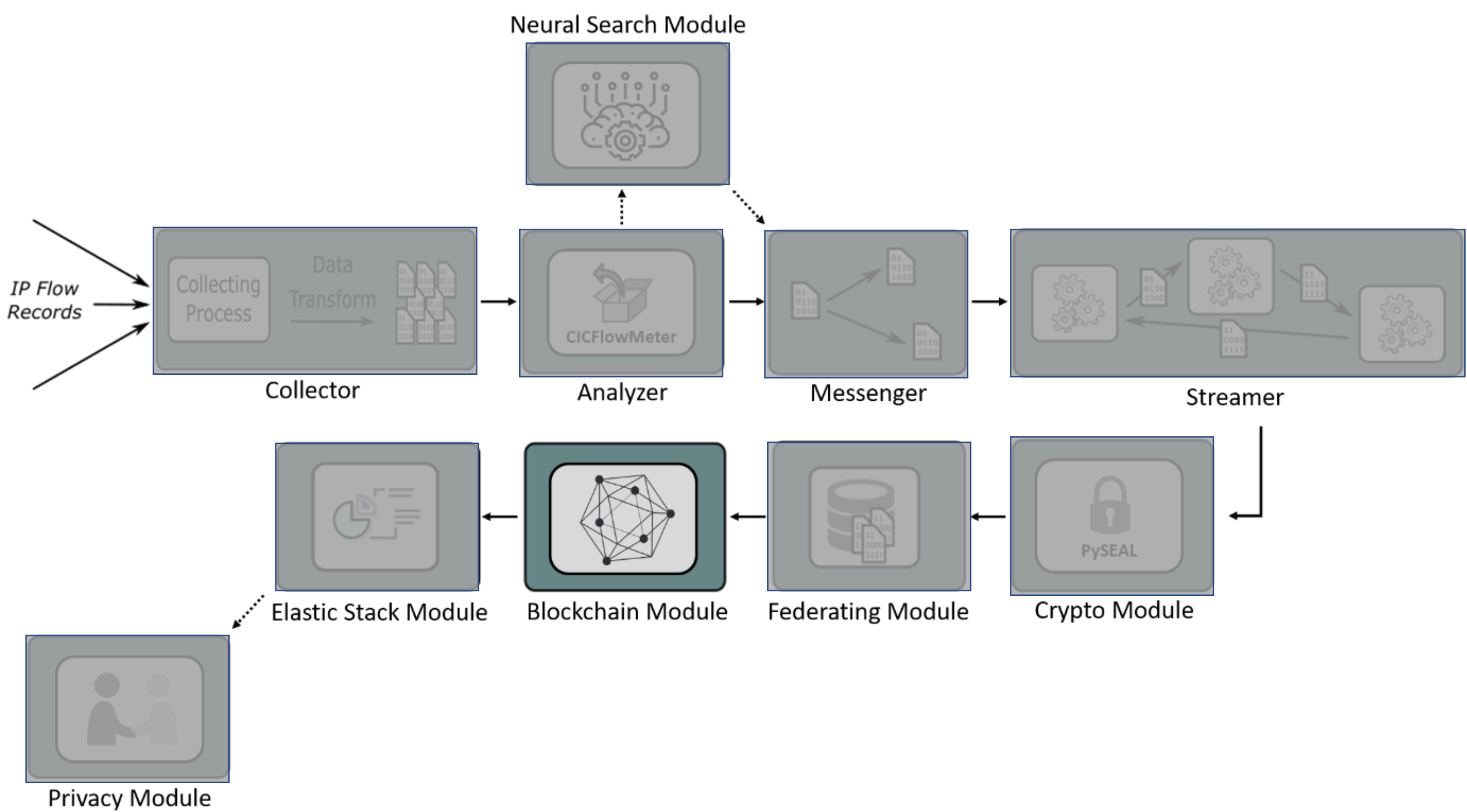


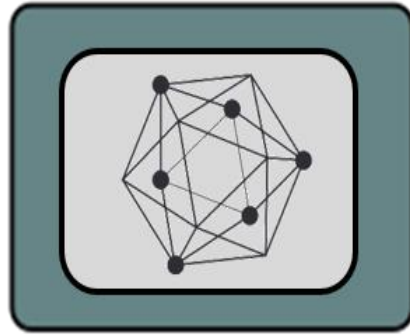




Federating Module



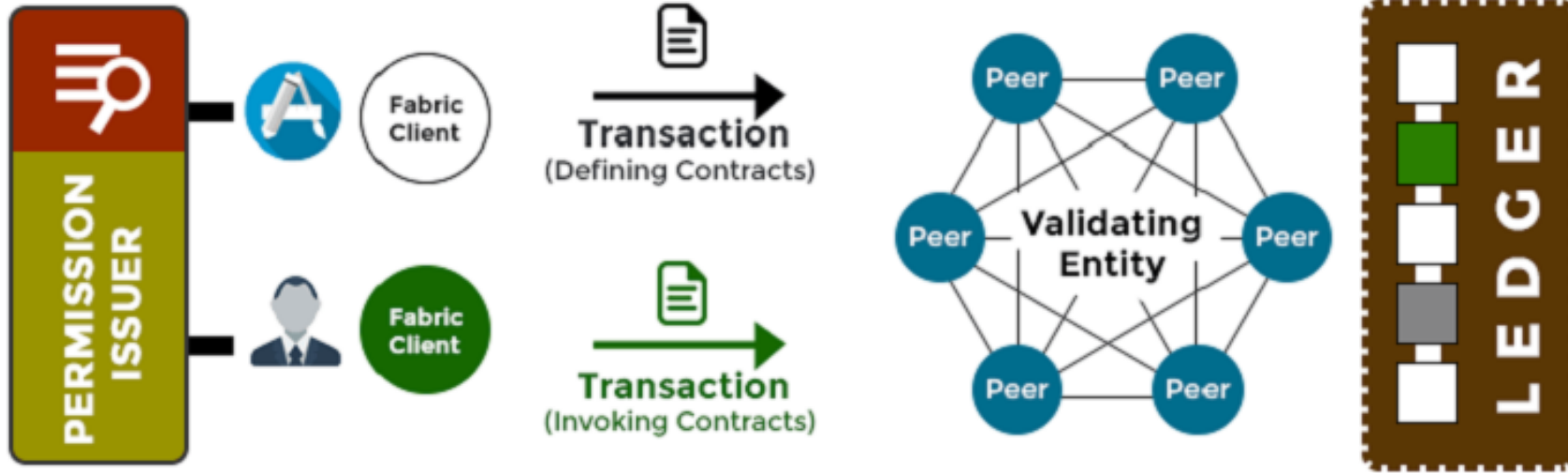


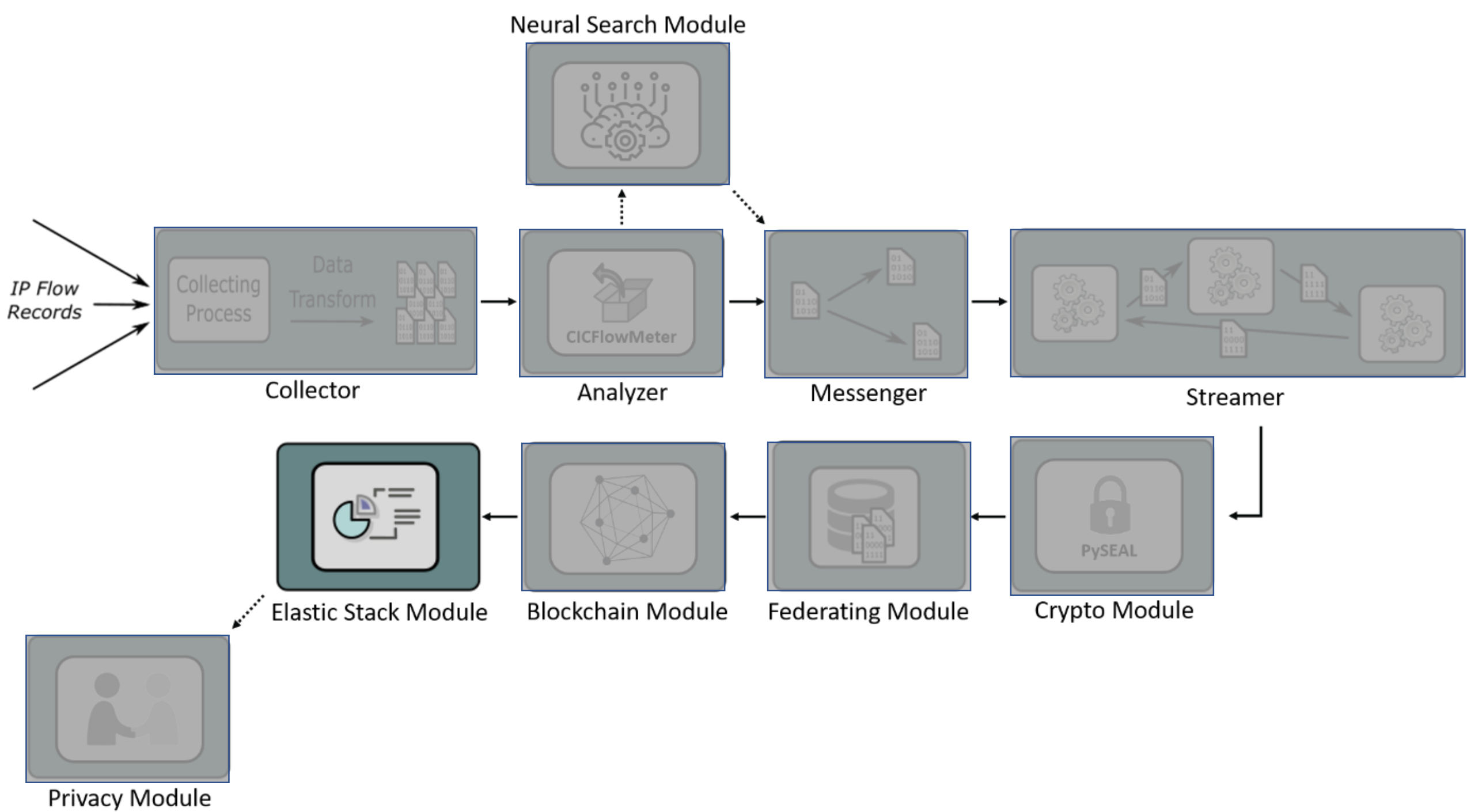


Blockchain Module



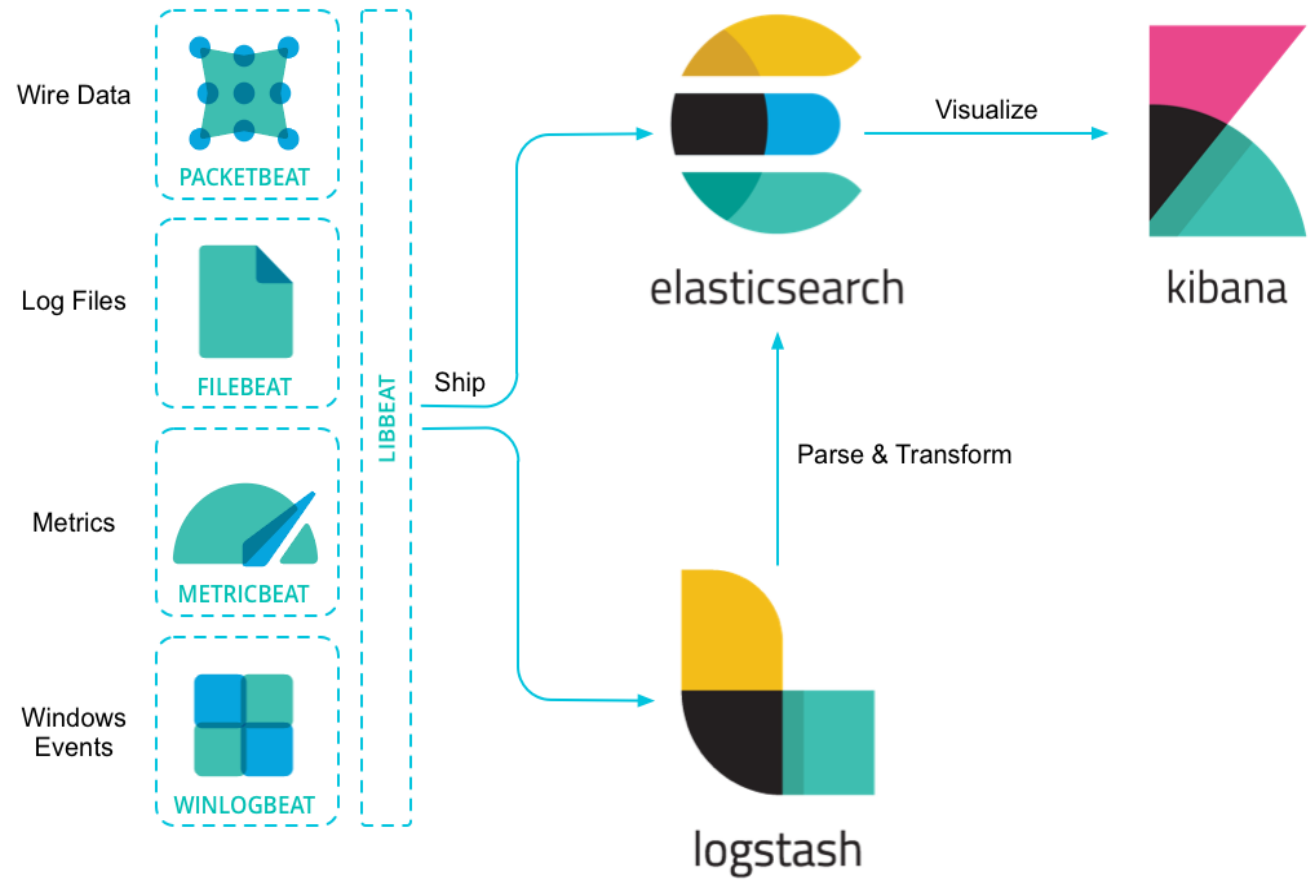
HYPERLEDGER FABRIC

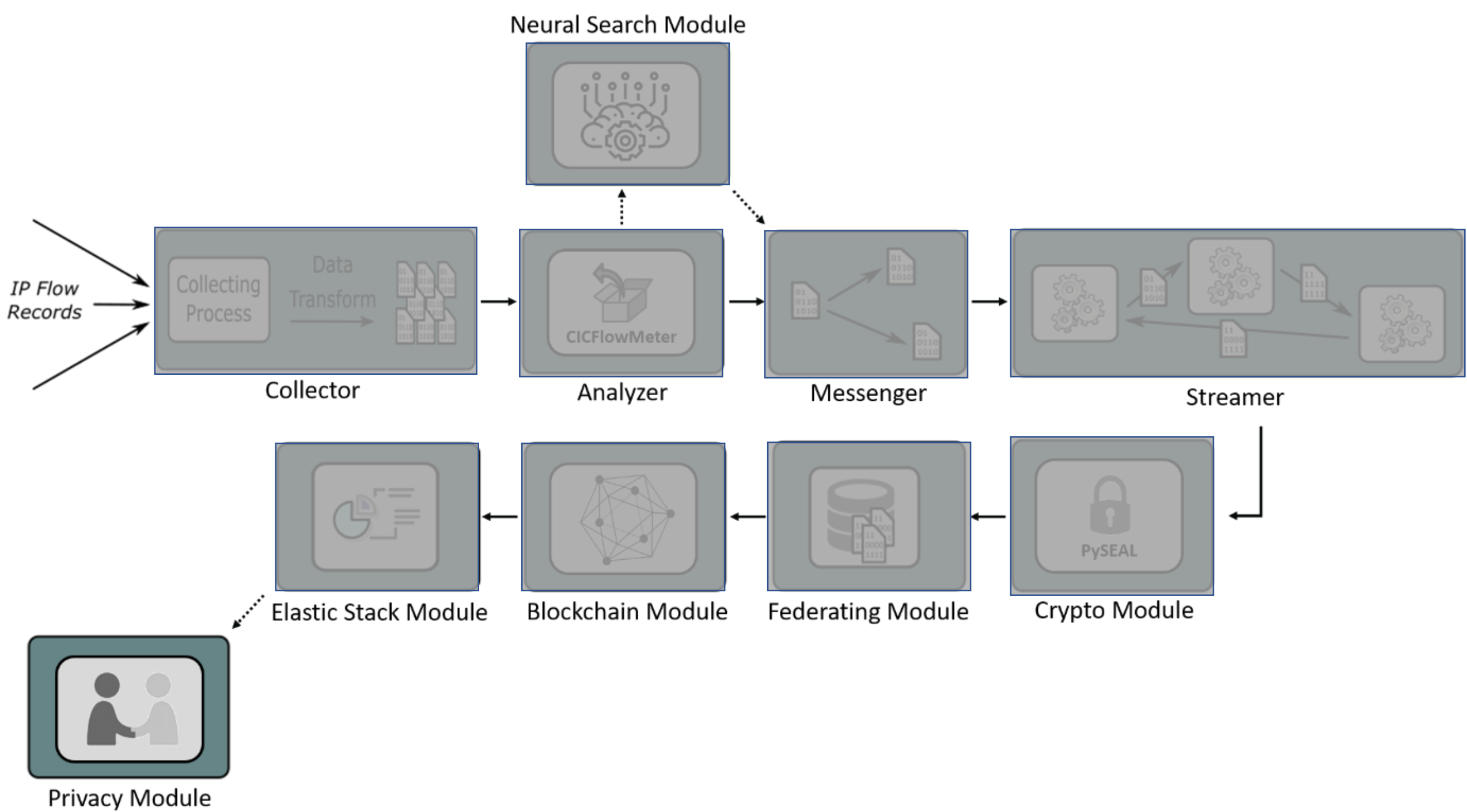






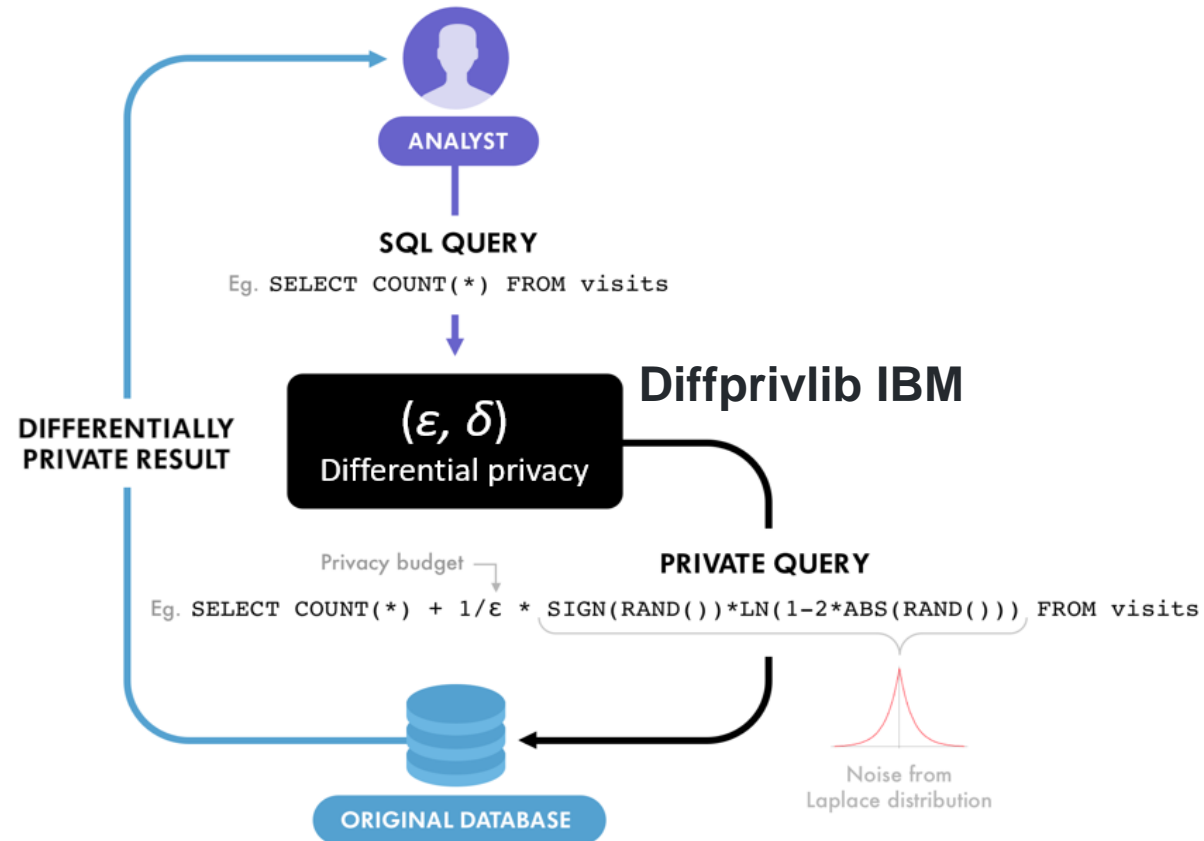
Elastic Stack Module

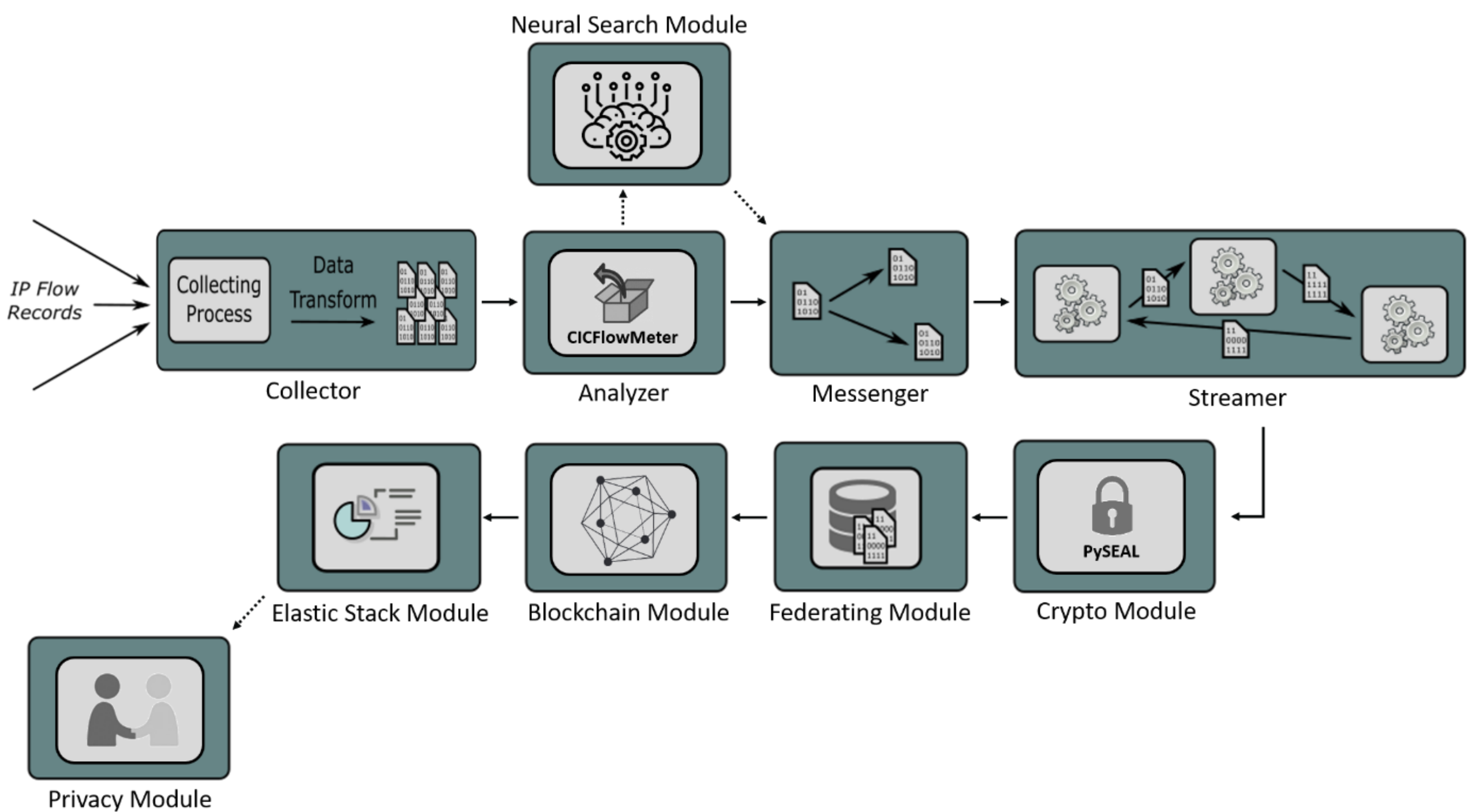


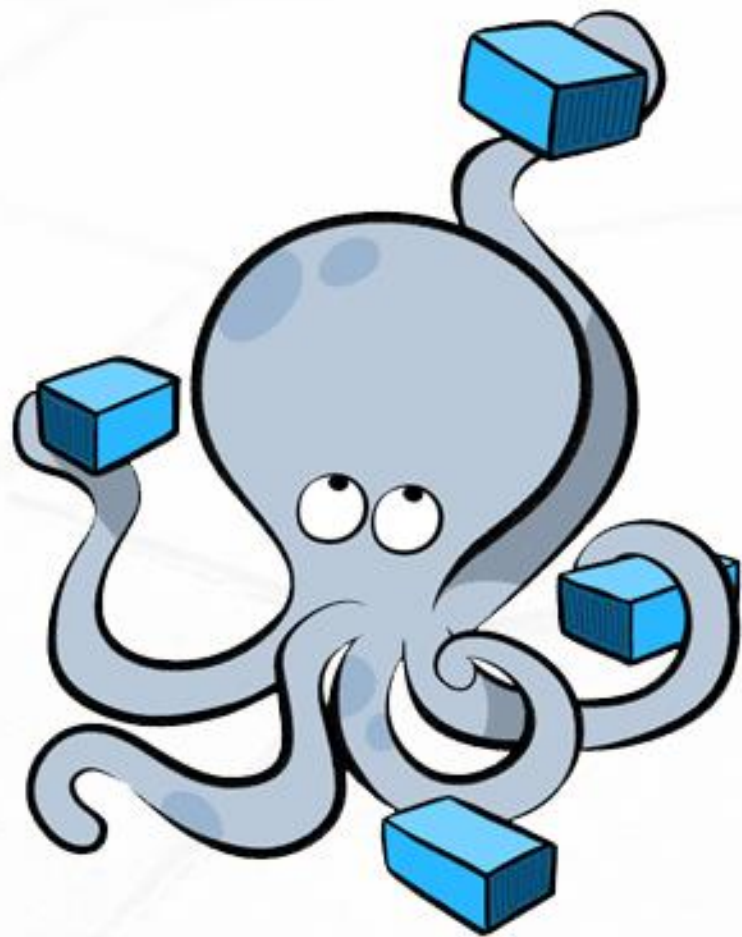




Privacy Module







```
php:  
  build: php  
  ports:  
    - "80:80"  
    - "443:443"  
  volumes:  
    - ./php/www:/var/www/html  
  links:  
    - db
```

```
$ docker-compose up
```

EDGE COMPUTING





postdoc...

Δ Φάση

Διάχυση των αποτελεσμάτων της έρευνας

Journals

Conferences

Collaborations

Research Projects

publications...



publications..International Scientific Journals

1. Demertzis, K., Iliadis, L., Tziritas, N., Kikiras, P., 2020, *Anomaly detection via blockchained deep learning smart contracts in industry 4.0*. Neural Comput & Applic (2020), **(Impact Factor 4.774)**
2. Demertzis, K., Iliadis, L. & Bougoudis, I., 2019, *Gryphon: a semi-supervised anomaly detection system based on one-class evolving spiking neural network*. Neural Comput & Applic (2019), **(Impact Factor 4.774)**
3. Xing, L., Demertzis, K. & Yang, J., 2019, *Identifying data streams anomalies by evolving spiking restricted Boltzmann machines*. Neural Comput & Applic (2019), **(Impact Factor 4.774)**
4. Demertzis, K.; Iliadis, L.; Pimenidis, I., **Geo-AI to Aid Disaster Response: Domain Adaptation with Memory-Augmented Deep Convolutional Reservoir Computing**, Integrated Computer-Aided Engineering, IOS Press **(Impact Factor 4.904)** (in press).
5. Demertzis, K.; Kikiras, P.; Tziritas, N.; Sanchez, S.L.; Iliadis, L., 2018, *The Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cybersecurity Intelligence*. Big Data Cogn. Comput. 2, 35, MDPI.
6. Demertzis, K.; Tziritas, N.; Kikiras, P.; Sanchez, S.L.; Iliadis, L., 2019, *The Next Generation Cognitive Security Operations Center: Adaptive Analytic Lambda Architecture for Efficient Defense against Adversarial Attacks*. Big Data Cogn. Comput. 2019, 3, 6.
7. Demertzis K., Iliadis L., Anezakis V. D., 2018, *An innovative soft computing system for smart energy grids cybersecurity*, Advances in Building Energy Research, 12:1, 3-24, DOI: 10.1080/17512549.2017.1325401, Taylor & Francis.
8. Demertzis, K.; Iliadis, L., 2019, *Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks*, Journal of Computations & Modelling, vol.9, no.2, 2019, 1-26, ISSN: 1792-7625, Scienpress Ltd.
9. Demertzis, K.; Iliadis, L., 2020, *GeoAI: A Model-Agnostic Meta-Ensemble Zero-Shot Learning Method for Hyperspectral Image Analysis and Classification*. Algorithms 2020, 13, 61.

publications..International Conferences Proceedings

1. **Demertzis K.**, Iliadis L., Anezakis VD., 2018, *A Dynamic Ensemble Learning Framework for Data Stream Analysis and Real-Time Threat Detection*. In: Kůrková V., Manolopoulos Y., Hammer B., Iliadis L., Maglogiannis I. (eds) Artificial Neural Networks and Machine Learning – ICANN 2018. ICANN 2018. Lecture Notes in Computer Science, vol 11139. Springer, Cham,
2. **Demertzis, K.**, Iliadis, L., Anezakis, V., 2018. *MOLESTRA: A Multi-Task Learning Approach for Real-Time Big Data Analytics*, in: 2018 Innovations in Intelligent Systems and Applications (INISTA). Presented at the 2018 Innovations in Intelligent Systems and Applications (INISTA), pp. 1–8. <https://doi.org/10.1109/INISTA.2018.8466306>
3. **Demertzis K.**, Iliadis L., Kikiras P., Tziritas N., 2019, *Cyber-Typhon: An Online Multi-task Anomaly Detection Framework*. In: MacIntyre J., Maglogiannis I., Iliadis L., Pimenidis E. (eds) Artificial Intelligence Applications and Innovations. AIAI 2019. IFIP Advances in Information and Communication Technology, vol 559. Springer, Cham.
4. **Demertzis K.**, Iliadis L., Pimenidis E., 2020, *Large-Scale Geospatial Data Analysis: Geographic Object-Based Scene Classification in Remote Sensing Images by GIS and Deep Residual Learning*. In: Iliadis L., Angelov P., Jayne C., Pimenidis E. (eds) Proceedings of the 21st EANN (Engineering Applications of Neural Networks) 2020 Conference. EANN 2020. Proceedings of the International Neural Networks Society, vol 2. Springer, Cham.
5. **Demertzis, K.**, Iliadis, L., 2018, **A Computational Intelligence System Identifying Cyber-Attacks on Smart Energy Grids**, in: Daras, N.J., Rassias, T.M. (Eds.), Modern Discrete Mathematics and Analysis: With Applications in Cryptography, Information Systems and Modeling, Springer Optimization and Its Applications. Springer International Publishing, Cham, pp. 97–116. https://doi.org/10.1007/978-3-319-74325-7_5.
6. **Demertzis, Konstantinos**, Iliadis, L.S., 2018. **Real-time Computational Intelligence Protection Framework Against Advanced Persistent Threats**. Book entitled "Cyber-Security and Information Warfare", Series: Cybercrime and Cybersecurity Research, NOVA science publishers, ISBN: 978-1-53614-385-0, Chapter 5.

editorial...

editor

- Special Issue "**Advances in Machine Learning**" *Processes*— Open Access Journal, MDPI – IF 2.753

editor

- Special Issue "**Bio-inspired Hybrid Artificial Intelligence Framework for Cyber Security**" *Applied Sciences* — Open Access Journal, MDPI – IF 2.474

editor

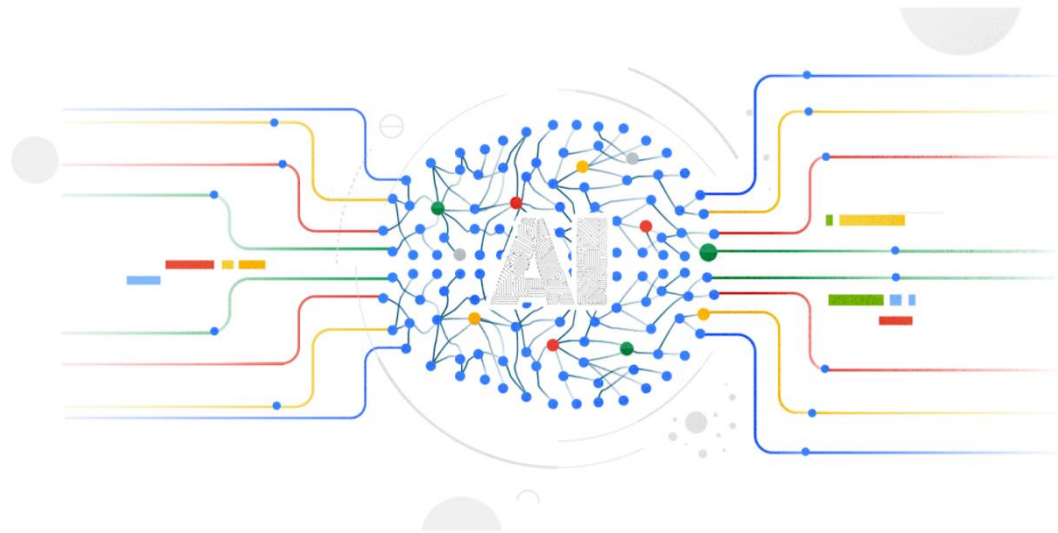
- Special Issue "**Sustainability Science and Technology**" *Sustainability* — Open Access Journal, MDPI – IF 2.576

lecturer...



ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
DEMOCRITUS UNIVERSITY OF THRACE

School of Civil Engineering, Democritus University of Thrace,
Postgraduate Program “Applied Mathematics”, “Intelligent Models and Hybrid Soft Computing Information Systems”



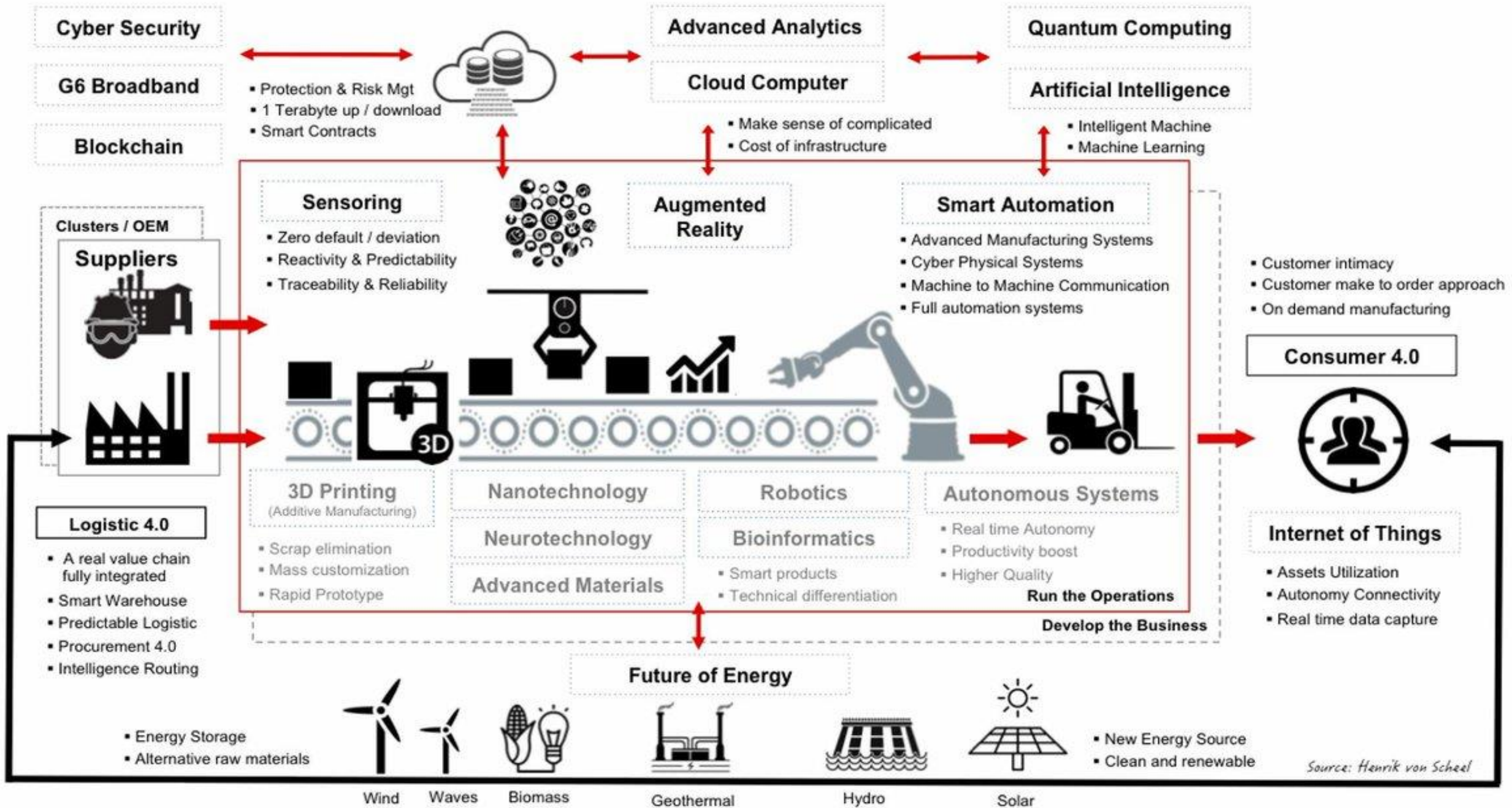


universidad
de león



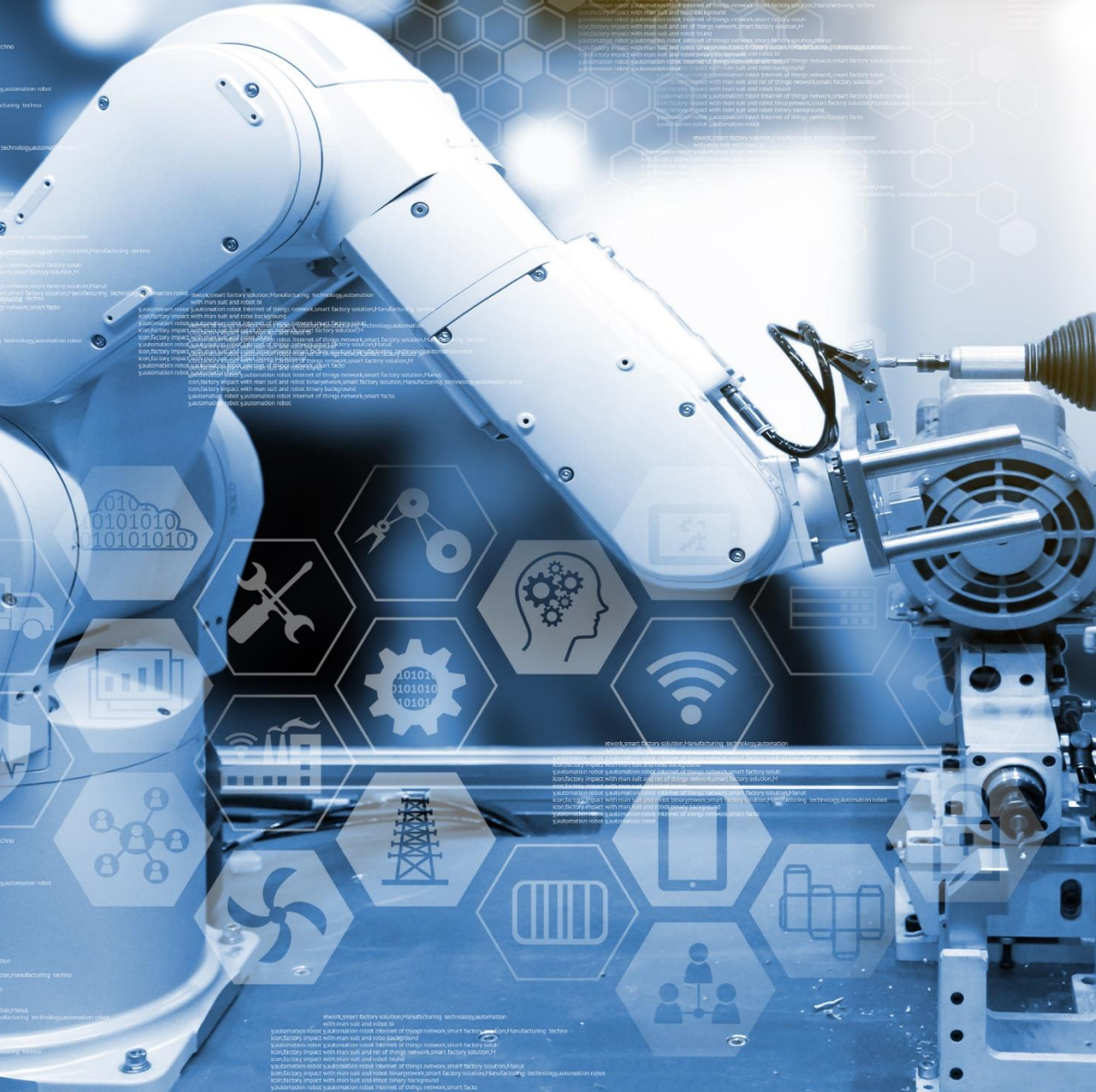


Industry 4.0 ecosystem



Industrial 4.0 Cyber Physical Systems

Internet of things network smart factory solution/Manufacturing technology/automation robot
Industrial 4.0 Cyber Physical Systems
Automation machine
Product



01016565659
56513174
25413
8231151
1548412215
1843748
81982
3465186451



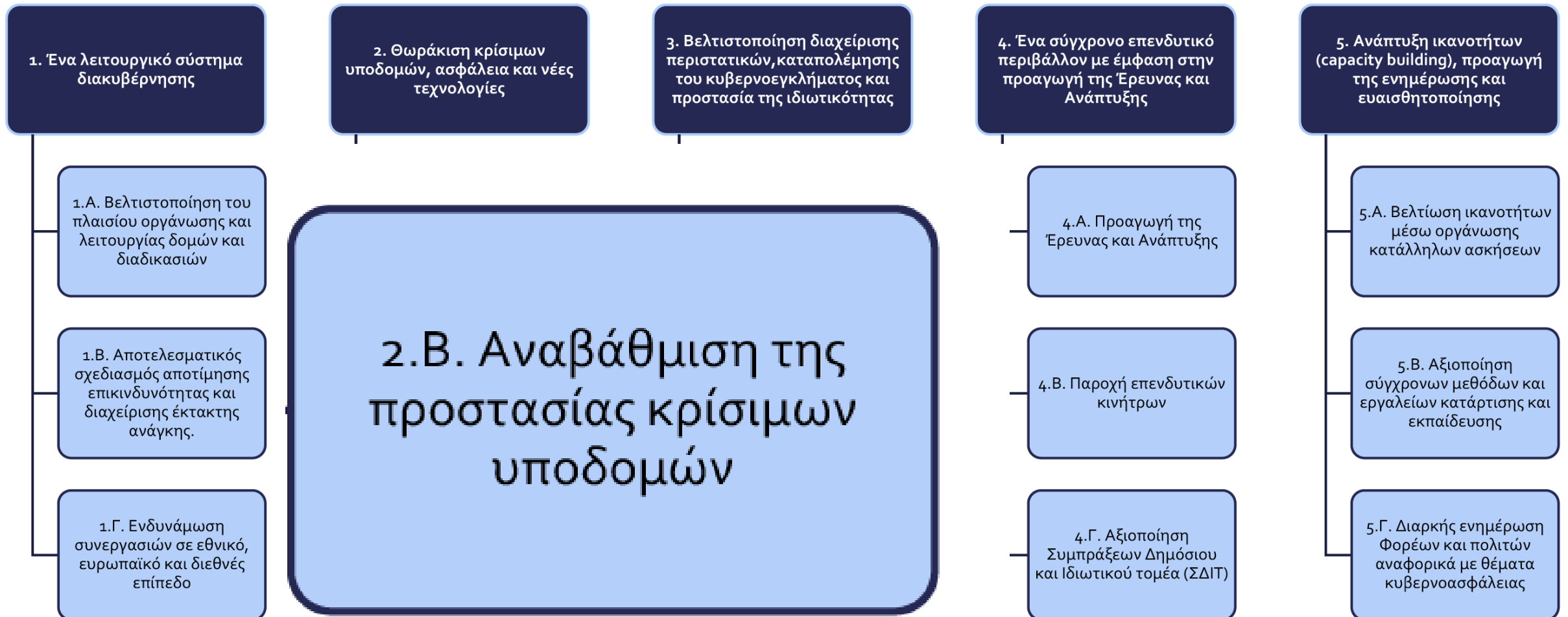


ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Δεκαπέντε ειδικοί στόχοι στο πλαίσιο στοχοθεσίας της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025



9.1.1 Σύσταση Κέντρου Παρακολούθησης Κρίσιμων Υποδομών Security Operations Center – SOC)

Κρίνεται απαραίτητη η ανάπτυξη δυνατότητας παρακολούθησης και απόκρισης σε συμβάντα ασφάλειας και η ανταλλαγή στοιχείων με τους αρμόδιους Φορείς. Η εν λόγω δυνατότητα παρέχεται μέσω υποδομής Κέντρου Παρακολούθησης Κρίσιμων Υποδομών (Security Operations Center – SOC) και σύστασης Ομάδας Απόκρισης Κυβερνοπεριστατικών (CSIRT).

Η λειτουργία Κέντρου Παρακολούθησης Κρίσιμων Υποδομών (SOC), απαιτεί, κατ' ελάχιστον, τα ακόλουθα:



Εικόνα 14 Λειτουργία SOC

Σκοπός του Κέντρου αποτελεί η διαρκής παρακολούθηση των κρίσιμων υποδομών Φορέων και η έγκαιρη αναγνώριση και αντιμετώπιση των περιστατικών ασφάλειας.

**ΣΤΡΑΤΗΓΙΚΟΙ ΣΤΟΧΟΙ ΤΗΣ
ΕΘΝΙΚΗΣ ΣΤΡΑΤΗΓΙΚΗΣ
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020-2025**



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Νοέμβριος 2020



The Next Generation Cognitive Security Operations Center

- Network Flow Forensics Using Cybersecurity Intelligence
- Adaptive Analytic Lambda Architecture Framework for Efficient Defense Against Adversarial Attacks



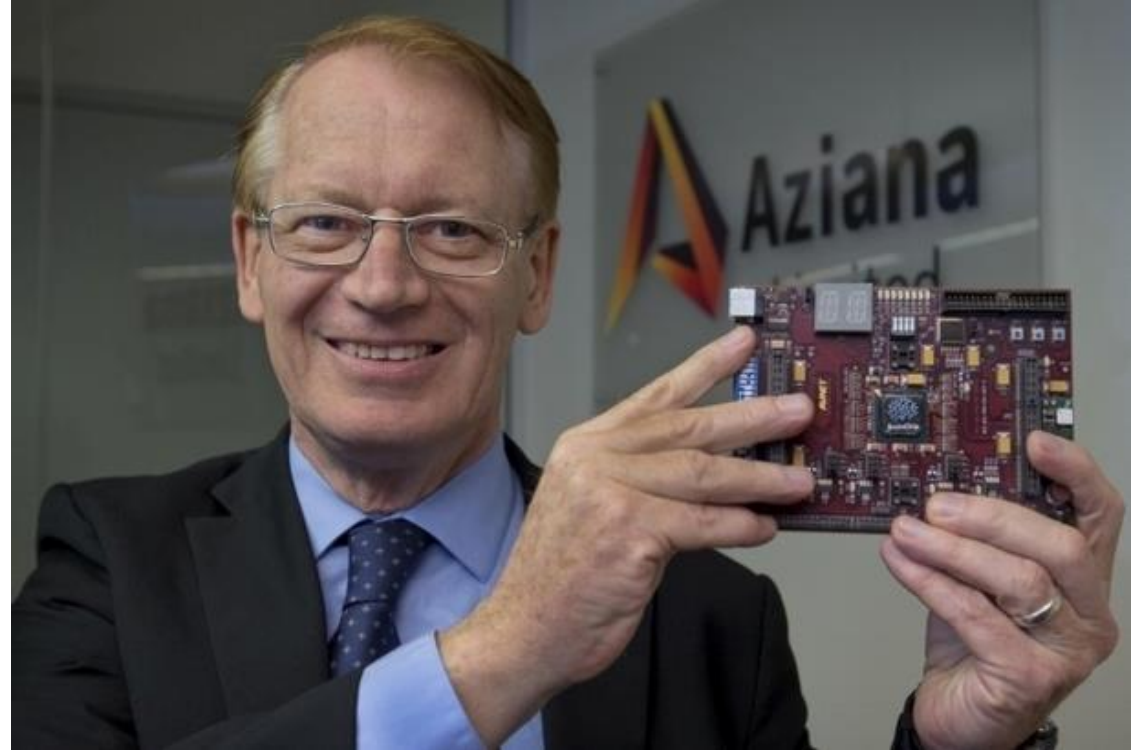
#brainchip

research projects...

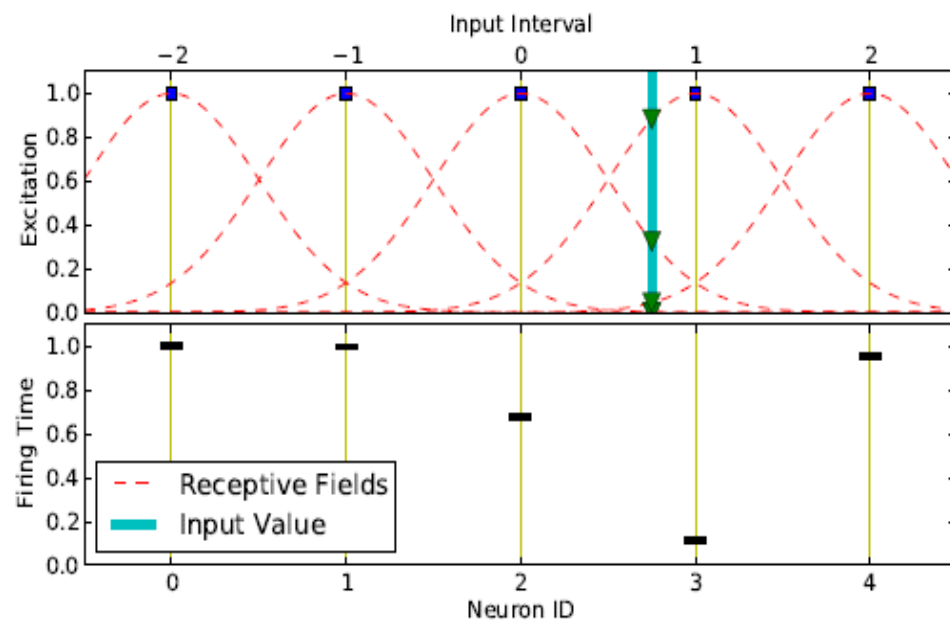
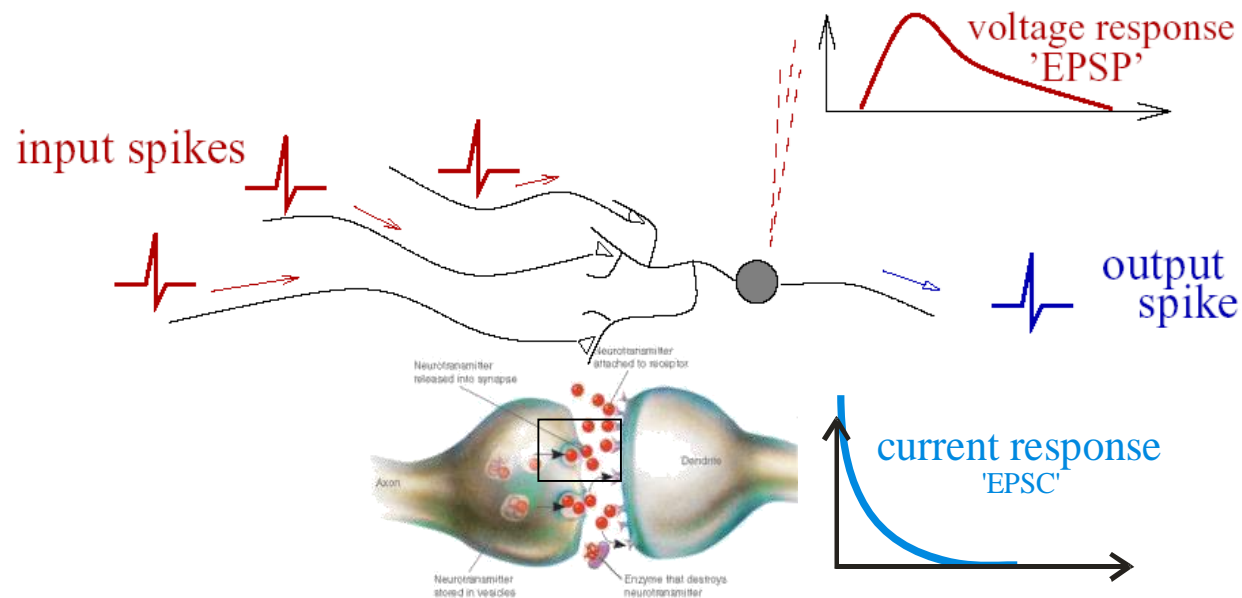
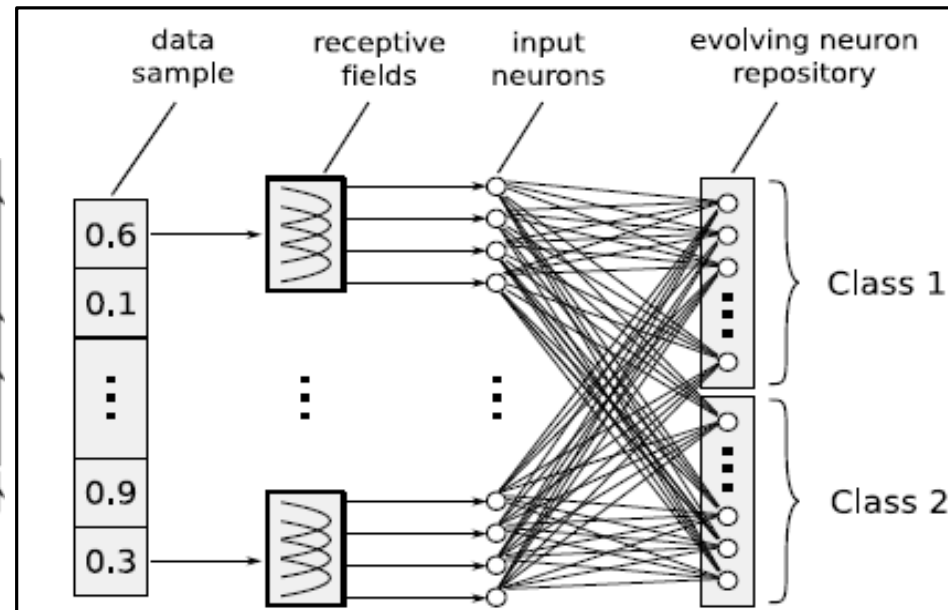
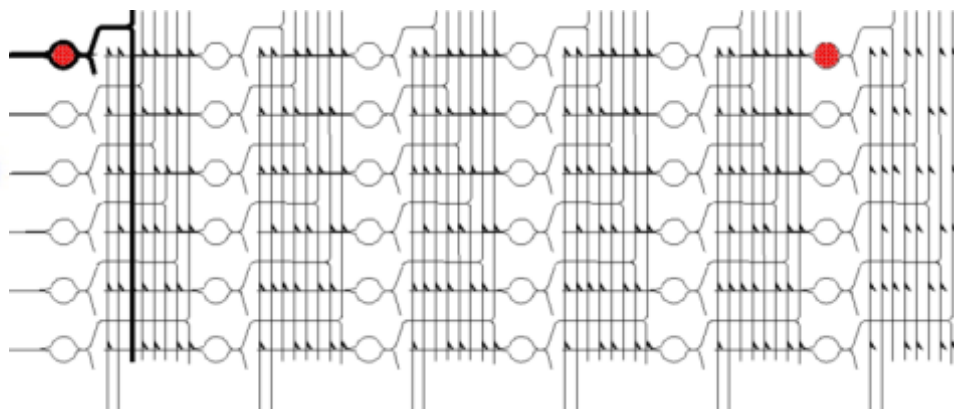
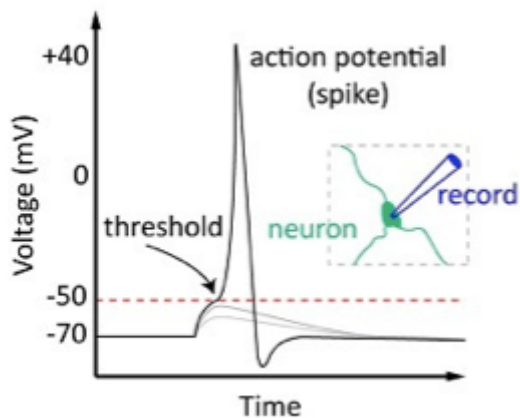


2018 – 2019, “Cybersecurity Algorithms for Spiking Neural Networks”, BrainChip - DUTh

brainchip*



Spiking Neural Network





ακίδα^{*} NSoC

Biologically Inspired, Digitally Engineered

Neural Network Comparison



	Convolutional Neural Networks		Spiking Neural Networks	
	Characteristic	Result	Characteristic	Result
Computational functions	Matrix Multiplication, ReLU, Pooling, FC layers	Math intensive, high power, custom acceleration blocks	Threshold logic, connection reinforcement	Math-light, low power, standard logic
Training	Backpropagation off-chip	Requires large pre-labeled datasets, long and expensive training periods	Feed-Forward, on or off-chip	Short training cycles, continuous learning

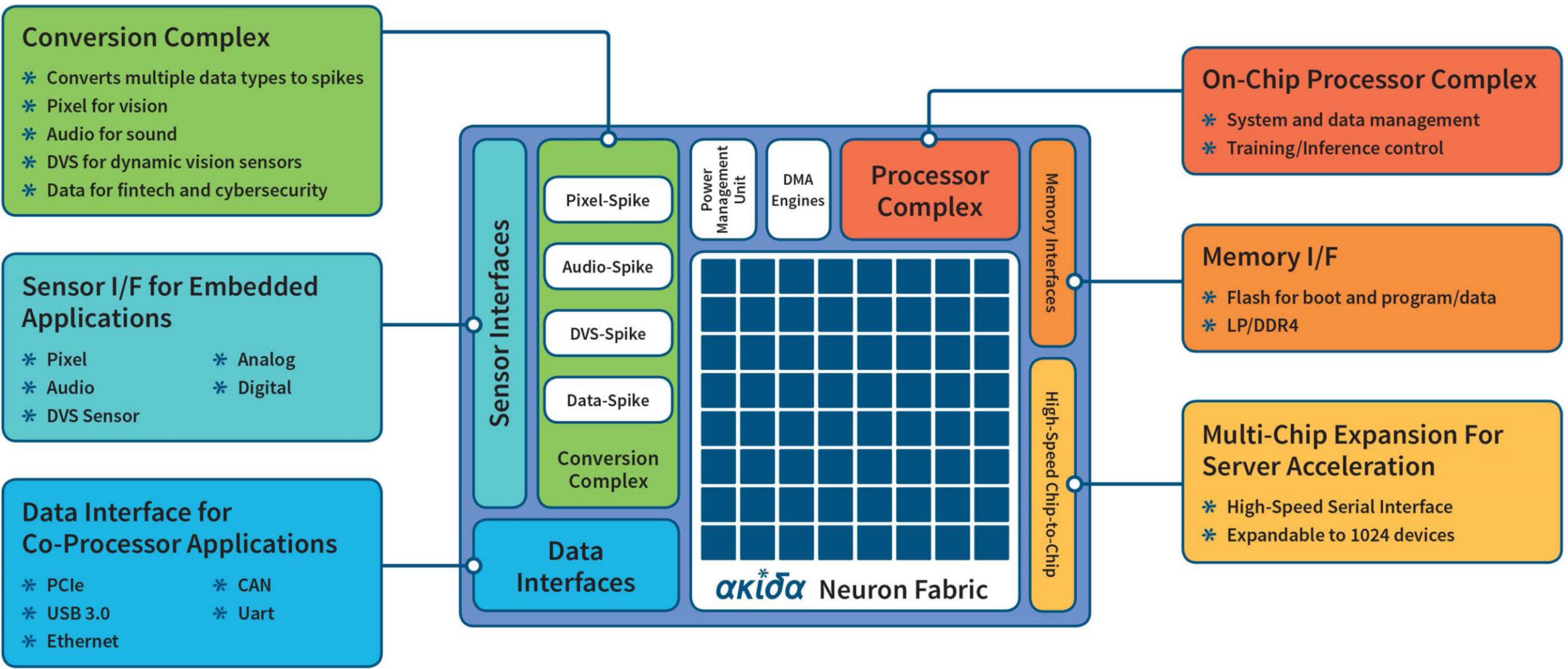
* **Math intensive cloud compute**

* **Low power edge deployments**



- * World's first Neuromorphic System on Chip (NSoC)
 - * Efficient neuron model
 - * Innovative training methodologies
- * Everything required for embedded/edge applications
 - * On-chip processor
 - * Data->spike conversion
- * Scalable for Server/Cloud
- * Neuromorphic computing for multiple markets
 - * Vision systems
 - * Cyber security
 - * Financial tech

Akida NSoC Architecture



Akida Neuron Fabric

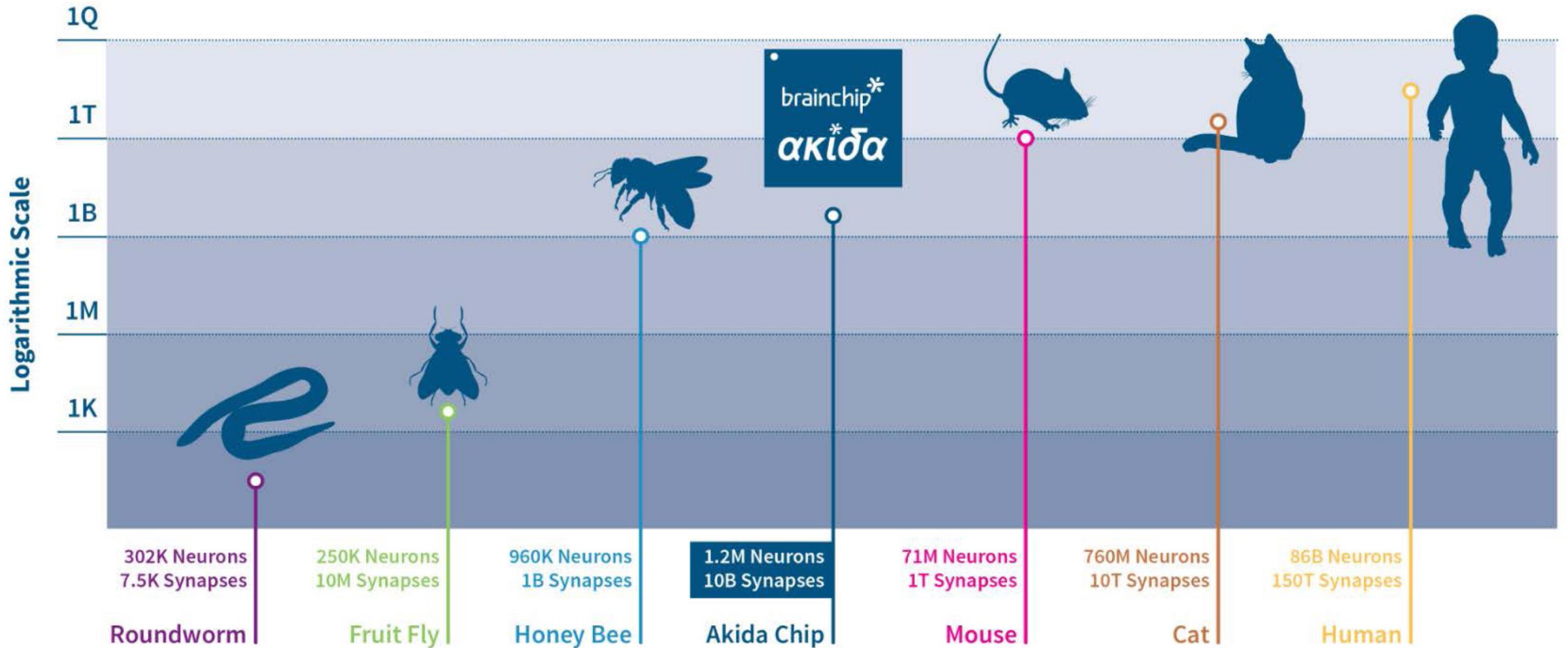
- * Most efficient spiking neural network implementation
 - * 1.2M Neurons
 - * 10B Synapses
- * Able to replicate most CNN functionality
 - * Convolution
 - * Pooling
 - * Fully connected



- * Meets demanding performance criteria
 - * 1,100 fps CIFAR-10
 - * 82% accuracy

- * Right-Sized for embedded applications
- * 10 classifiers (CIFAR 10)
 - * 11 Layers
 - * 517K Neurons
 - * 616M Synapses

Neuron and Synapse Counts in the Animal Kingdom



The Most Efficient Neuromorphic Computing Fabric

Relative Implementation Efficiency
(Neurons and Synapses)

IBM



intel



3X

300X

brainchip*
ακiδa*

Keys to efficiency

- * Fixed neuron model
 - * Right-sized Synapses minimized on-chip RAM
 - * 6MB compared to 30-50MB
 - * Programmable training and firing thresholds
- * Flexible neural processor cores
 - * Highly optimized to perform convolutions
 - * Also fully connected, pooling
- * Efficient connectivity
 - * Global spike bus connects all neural processors
 - * Multi-chip expandable to 1.2 Billion neurons

Akida NSoC Applications



Embedded vision

- * Object classification
- * ADAS/AV
- * Surveillance
- * Vision guided robotics

Supervised



Cybersecurity

- * Packet inspection
- * File property classification
- * Anomaly detection

Supervised



Financial Technology

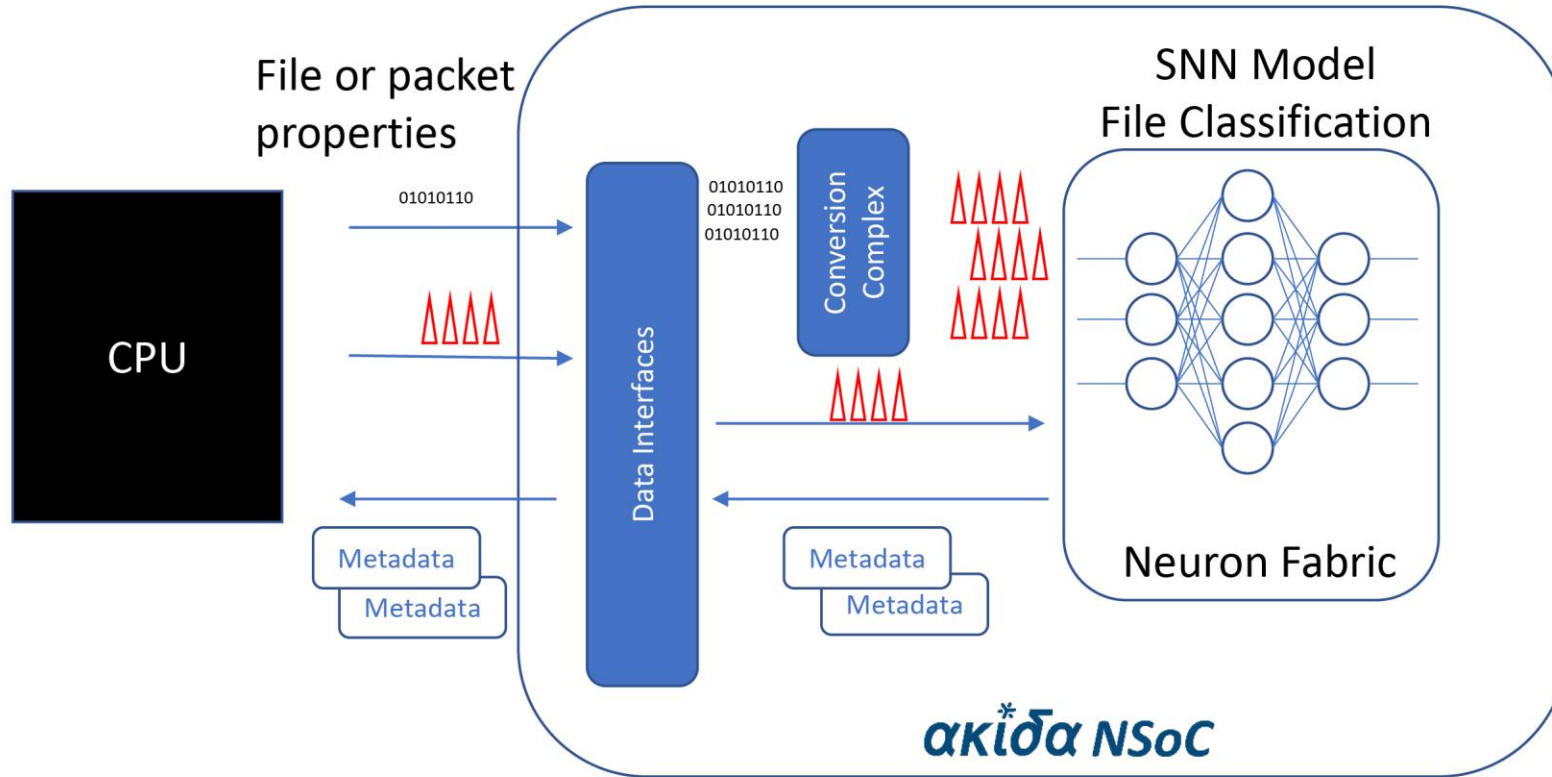
- * Trading pattern detection
- * Price prediction

Unsupervised

MARKET

TRAINING METHOD

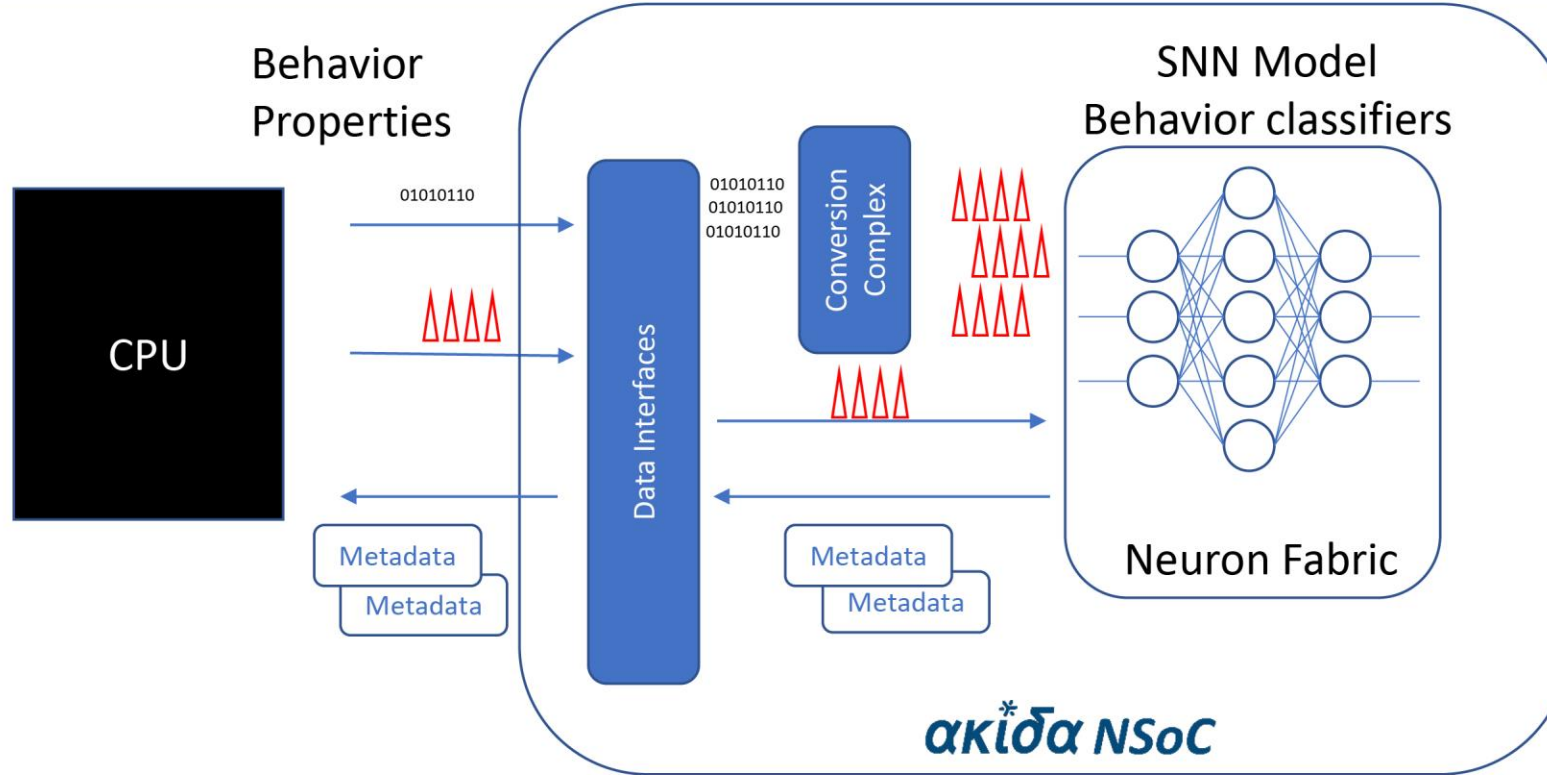
Cybersecurity Applications: Malware Detection



- * Supervised learning for file classification based on file properties

File or packet properties – distinguishing parameters for files/network traffic, can be converted to spikes in SW on CPU or by Akida NSoC

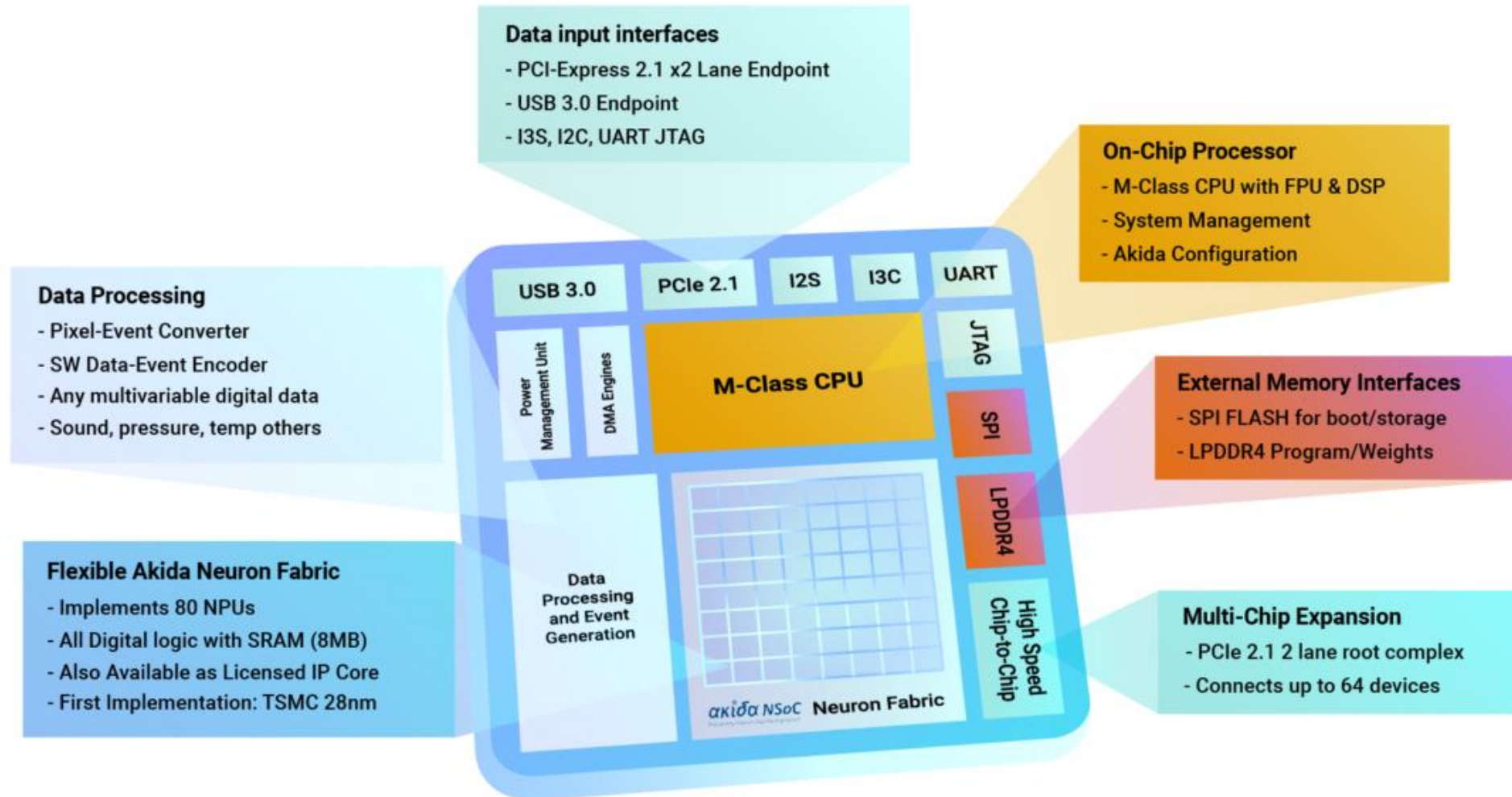
Cybersecurity Applications: Anomaly Detection



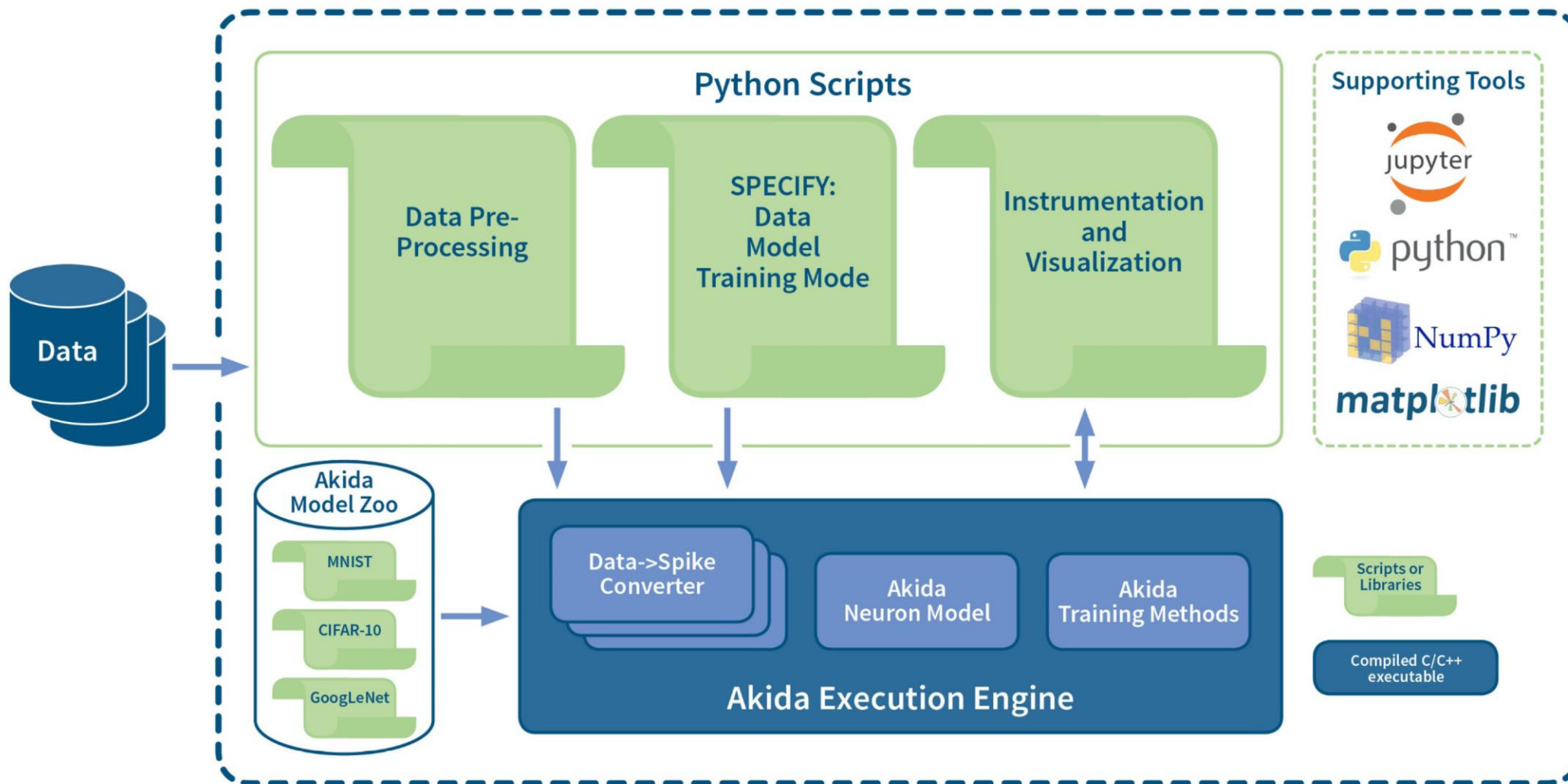
* Supervised learning on known good behavior and anomalous behavior

Behavior properties can be CPU loads for common applications, network packets, power consumption, fan speed, etc..

Features of Akida NSoC



Creating SNNs: The Akida Development Environment



AKIDA Training Methods



- * Unsupervised learning from unlabeled data
 - * Detection of unknown patterns in data
 - * On-chip or off-chip
- * Unsupervised learning with label classification
 - * First layers learns unlabeled features, labeled in fully connected layer
 - * On-chip or off-chip



* World's first NSoC

- * Low power and footprint of neuromorphic computing
 - * Highest performance /w/\$
 - * Estimated tape-out 1H2019, samples 2H2019
- ## * Complete solution for embedded/edge applications – but scalable for cloud/server usage

brainchip



News

Like 0 Tweet LinkedIn +

BrainChip acquires licence to university's cybersecurity technology

04 OCTOBER 2018



Neuromorphic computing firm BrainChip Holdings have entered into a cybersecurity implementation agreement with Greece's Democritus University of Thrace (DUTH) – using the former's neuromorphic SoC for system acceleration.

The agreement consists of a licence to DUTH's cybersecurity technology and their researcher's support in porting the technology to the Akida Development Environment. Such cybersecurity technology includes data-to-spike converters, and it is specifically designed for network intrusion and anomaly detection: this is through a spiking neural network (SNN) that can be accelerated by the **Akida Neuromorphic system-on-chip (NSoC)**.

As Lazaros Iliadis, a professor of the DUTH's School of Engineering, is responsible for the program, commented: "We have been working with spiking neural networks for several years and our cybersecurity technology has proven highly accurate in detecting threats. The Akida NSoC is an ideal platform to accelerate our SNNs."

To quote Robert Beachler, BrainChip senior VP of Marketing and Business Development, moreover: "As the Akida NSoC design progresses, it is important that we have proven examples of SNN models and data to spike converters for our target markets."

"According to **MarketsandMarkets**, the artificial intelligence cybersecurity market is estimated to be \$35B by 2025 and this technology acquisition will jump-start our solutions in this lucrative application space."

Peter van der Made, BrainChip founder and CTO added: "Working with the exceptional team at the Democritus University of Thrace will serve to increase our expertise and knowledge in the area of cybersecurity – and widen the reach of our low-power and low-latency Akida NSoC device."

Related Articles

Register



Digital Rail to take centre stage at Railtex 2019...

Amplicon's Impact-E 150AL series

New from RDS - Jaguar - MINI STX PC

Popular articles



British engineering celebrated with Royal Mail stamps

On World Password Day: Are passwords becoming obsolete?...

EPDT magazine May 2019 issue (inc. PXI supplement) now available online

Recent Videos



Tiny needles give defibrillators a big boost

Configuring your Vicor Brick converter

Introduction to Vicor's AC Front End Module

brainchip*



ακίδα NSoC

Biologically Inspired, Digitally Engineered

ΕΤΑΙΡΕΙΑ ΑΡΧΕΙΟ ΠΡΟΓΡΑΜΜΑ WEBTV ΣΕΙΡΕΣ ΤΑΙΝΙΕΣ WEBRADIO HYBRID ΠΕΡΙΣΣΟΤΕΡΑ

EPT

ΕΙΔΗΣΕΙΣ ▾

ΑΘΛΗΤΙΣΜΟΣ

ΡΑΔΙΟΤΗΛΕΟΡΑΣΗ ▾

ΠΕΡΙΦΕΡΕΙΑ ▾

LIVE ▾

INTERNATIONAL ▾



Καινοτόμο Λογισμικό Τεχνητής Νοημοσύνης από ομάδα του ΔΠΘ

10 ΟΚΤΩΒΡΙΟΥ 2019

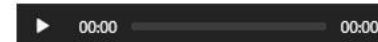
Mri Diagnostics Magnetic Resonance Imaging Hospital

Καινοτόμο Λογισμικό Τεχνητής Νοημοσύνης με τεχνολογία Spiking Νευρωνικών Δικτύων, ανέπτυξε η ερευνητική ομάδα του Εργαστηρίου

Μαθηματικών και Πληροφορικής του Τμήματος Πολιτικών Μηχανικών του Δ.Π.Θ., αποτελούμενη από τον Καθηγητή κ. Λάζαρο Ηλιάδη και τον Μεταδιδακτορικό Ερευνητή Δρ. Κωνσταντίνο Δεμερτζή.

Το λογισμικό ανιχνεύει μεγάλο αριθμό Κυβερνοεπιθέσεων, σε χρόνο που τείνει στο μηδέν. Με βάση το εν λόγω Λογισμικό, αναπτύχθηκε στις Η.Π.Α. από την εταιρεία Hardware Brainchip, το Νευρομορφικό Ολοκληρωμένο Κύκλωμα – NSoC (Neuromorphic System-on-Chip) με την Ελληνική επωνυμία

ακούστε live



LiveRadio σε νέο παράθυρο

brainchip*

BrainChip Holdings Limited
2,615 followers
1d • 🌐

ICYMI - NASA, in collaboration with Brainchip Inc and Vorago, uses Akida to control space flight. For example, it tries to detect and deal with possible problems in space flight <https://lnkd.in/g3DJpCR> #neuromorphic #nasa #ai #edge #cybersecurity



Greek cybersecurity software in space flight control ATHENS 9,84

athina984.gr • 3 min read

🌐 63 • 7 Comments

Thank you for... I wonder... I think... Thanks for posting... (>

👍 Like 💬 Comment ➔ Share ↗ Send

ακίδα NSoC

Biologically Inspired, Digitally Engineered

Νέα Ελλάδα Πολιτική Οικονομία Κόσμος Ομάδα Γνώμες Περισσότερα ▾ **TA NEA**

🏠 > Επιστήμη & Τεχνολογία
Ευφύες λογισμικό

Τι είναι το τσιπ Ακίδα που αγόρασε η NASA από το Πανεπιστήμιο Θράκης

Ως ασπίδα προστασίας από κάθε είδους παρέκκλιση από τη φυσιολογική λειτουργία και γενικότερα ως σύστημα ελέγχου διαστημικών πτήσεων της NASA, χρησιμοποιείται πλέον, πειραματικά, το νευρομορφικό ολοκληρωμένο κύκλωμα Neuromorphic System on Chip (nsoc) Ακίδα που δημιουργήθηκε και με το ευφύες λογισμικό που ανέπτυξε ερευνητική ομάδα του Δημοκρίτειου Πανεπιστημίου Θράκης».



Ξεφυλλίστε την έντυπη έκδοση

Τελευταία Νέα

🕒 5 λεπτά
Κοροναϊός: Αυξημένη η κίνηση στους δρόμους παρά το lockdown

🕒 14 λεπτά
Live: Ολυμπιακός - Άλμπα Βερολίνου

🕒 33 λεπτά
Εκλογές ΗΠΑ: Οι Δημοκρατικοί του Κογκρέσου ξεκαθαρίζουν

🕒 38 λεπτά
Δημοσκόπηση: Τι λένε οι πολίτες για τα νέα μέτρα - Η διαφορά ανάμεσα σε ΝΔ και ΣΥΡΙΖΑ

🕒 45 λεπτά
Κοροναϊός: Η Βρετανία βάζει σε καραντίνα όσους ταξιδεύουν από την Ελλάδα

🕒 57 λεπτά
Η Πάνα Αγγελούπουλου - Δασκαλάκη στο MEGA για τις δράσεις της Επιτροπής «Ελλάδα 2021»

🕒 1 ώρα

#prospects

prospects...School of Civil Engineering

Η μεταδιδακτορική έρευνα αποτελεί για το Τμήμα, πηγή συλλογικής αριστείας, επιστημονικής συνεργασίας υψηλού επιπέδου και διεθνούς διάκρισης. Με αυτούς τους τρόπους, συμβάλλει στην ποσοτική και ποιοτική αναβάθμιση της ερευνητικής δραστηριότητας και στη μεταφορά τεχνογνωσίας σε νέα και δυναμικά ερευνητικά πεδία προς όφελος της κοινωνίας και της εθνικής οικονομίας.

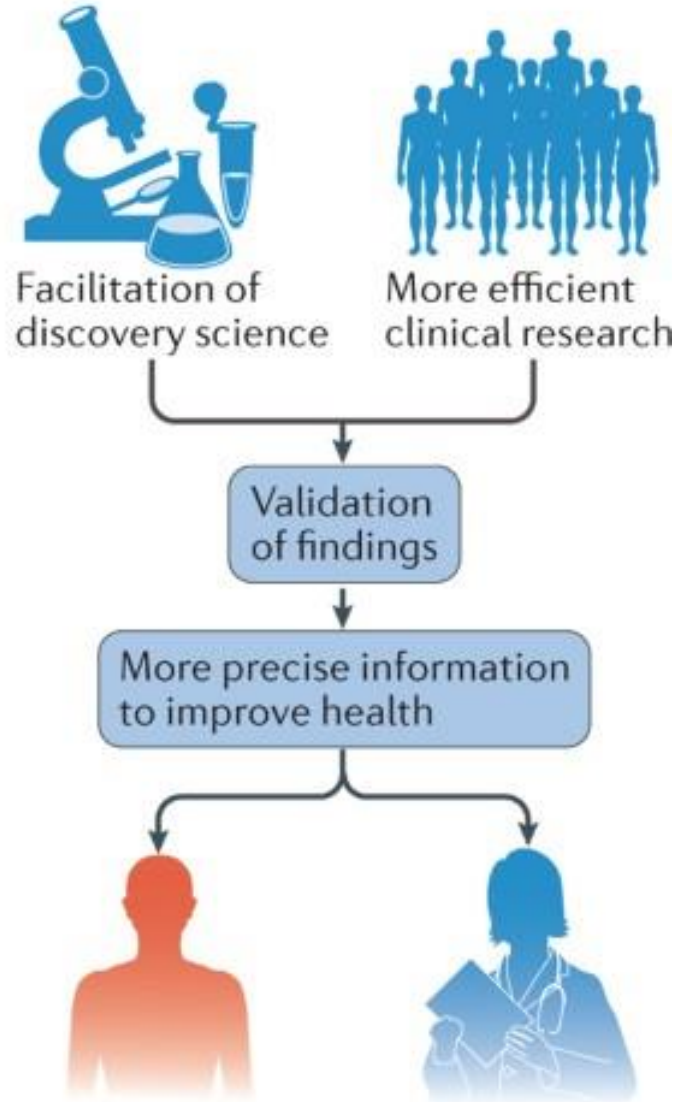
1. Ενίσχυση της γνωστικής περιοχής της ασφάλειας κρίσιμων υποδομών
2. Ενίσχυση της γνωστικής περιοχής της ψηφιακής ασφάλειας
3. **Συνεργασία με το University of León** (Erasmus, επίβλεψη διατριβών, ερευνητικές συνεργασίες, κτλ)
4. Περαιτέρω συνεργασίες με αντίστοιχα πανεπιστημιακά ιδρύματα ή ερευνητικούς φορείς
5. **ΜΠΣ στην ανάλυση δεδομένων** μεγάλης κλίμακας με μεθόδους τεχνητής νοημοσύνης στο γνωστικό αντικείμενο του Πολιτικού Μηχανικού
6. **Ακίδα** στο Τμήμα Πολιτικών Μηχανικών

#in progress

a Precision medicine system



b Precision medicine goals



#whole-heartedness

respect...



Lazaros Iliadis

Professor of Applied Informatics, Democritus University of Thrace, School of Engineering, Department of Civil Engineering, Faculty of Mathematics, Programming and general courses, Lab of Mathematics and Informatics (ISCE)

thank you

Complete List of my Publications

Journals

1. Bougoudis, I., **K. Demertzis**, and L. Iliadis. **Fast and low cost prediction of extreme air pollution values with hybrid unsupervised learning**. *Integrated Computer-Aided Engineering* 23, no. 2 (2016): 115–27. <https://doi.org/10/f8dt4t> doi:10.3233/ICA-150505. **(Impact Factor 4.904)**
2. **K. Demertzis**, L. Iliadis, N. Tziritas, and P. Kikiras, “**Anomaly detection via blockchained deep learning smart contracts in industry 4.0**”, *Neural Comput & Applic*, vol. 32, no. 23, pp. 17361–17378, Dec. 2020, doi: 10.1007/s00521-020-05189-8. **(Impact Factor 4.774)**
3. Xing, L., **K. Demertzis**, and J. Yang. **Identify Data Streams Anomalies by Evolving Spiking Restricted Boltzmann Machines**. *Neural Computing & Application*, Springer, 2019. doi:10.1007/s00521-019-04288-5. **(Impact Factor 4.774)**
4. **Demertzis, K.**, L. Iliadis, and I. Bougoudis. **Gryphon: A semi-supervised anomaly detection system based on one-class evolving spiking neural network**. *Neural Computing & Application*, Springer, 2019. doi:10.1007/s00521-019-04363-x. **(Impact Factor 4.774)**
5. **Demertzis, K.**, and L. Iliadis. 2017. **Detecting invasive species with a bio-inspired semi-supervised neurocomputing approach: the case of Lagocephalus sceleratus**. *Neural Computing & Application*, Springer, vol. 28 pp. 1225–1234. <https://doi.org/10/gbkgb7> doi:10.1007/s00521-016-2591-2. **(Impact Factor 4.774)**
6. **Demertzis, K.**, L. Iliadis, S. Avramidis, and Y. A. El-Kassaby. 2017. **Machine learning use in predicting interior spruce wood density utilizing progeny test information**. *Neural Computing & Application*, Springer, vol. 28, 505–519. <https://doi.org/10/gdp86z> doi:10.1007/s00521-015-2075-9. **(Impact Factor 4.774)**
7. Bougoudis, I., **K. Demertzis**, and L. Iliadis. 2016. **HISYCOL a hybrid computational intelligence system for combined machine learning: the case of air pollution modeling in Athens**. *Neural Computing & Application*, Springer, vol. 27, 1191–1206. <https://doi.org/10/f8r7vf> doi:10.1007/s00521-015-1927-7. **(Impact Factor 4.774)**
8. Bougoudis, I., **K. Demertzis**, L. Iliadis, V.-D. Anezakis, and A. Papaleonidas. 2018. **FuSSFFra, a fuzzy semi-supervised forecasting framework: the case of the air pollution in Athens**. *Neural Computing & Application*, Springer, vol. 29, 375–388. <https://doi.org/10/gc9bbf> doi:10.1007/s00521-017-3125-2. **(Impact Factor 4.774)**
9. **Demertzis, K.**; Tsiotas, D.; Magafas, L. **Modeling and Forecasting the COVID-19 Temporal Spread in Greece: An Exploratory Approach Based on Complex Network Defined Splines**. *Int. J. Environ. Res. Public Health* 2020, 17, 4693. **(Impact Factor 2.849)**
10. Dimou, V., V.-D. Anezakis, **K. Demertzis**, and L. Iliadis. **Comparative analysis of exhaust emissions caused by chainsaws with soft computing and statistical approaches**. *International Journal of Environmental Science and Technology* 15, no. 7

- (2018): 1597–608. <https://doi.org/10/gdp864> doi:10.1007/s13762-017-1555-0. **(Impact Factor 2.540)**
11. Demertzis, Konstantinos. Iliadis, L., Anezakis, V.-D., 2017. **Commentary: Aedes albopictus and Aedes japonicus—two invasive mosquito species with different temperature niches in Europe.** *Frontiers Environmental Science* 5. <https://doi.org/10/gdp865> **(Impact Factor 1.841)**
 12. Anezakis, V.-D., K. Demertzis, L. Iliadis, and S. Spartalis. **Hybrid intelligent modeling of wild fires risk.** *Evolving Systems*, no. 4 (2018): 267–83. <https://doi.org/10/gdp863> doi:10.1007/s12530-017-9196-6. **(Impact Factor 1.170)**
 13. Demertzis, K., and L. Iliadis. **Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks,** *Journal of Computations & Modelling*, vol.9, no.2, 2019, 1-26, ISSN: 1792-7625 (print), 1792-8850 (online), Scienpress Ltd, 2019.
 14. Demertzis, K., and L. Iliadis. 2017. **Computational intelligence anti-malware framework for android OS.** *Vietnam Journal of Computer Science* vol. 4, 245–259. <https://doi.org/10/gdp86x> doi:10.1007/s40595-017-0095-3.
 15. Demertzis, Konstantinos. Iliadis, L.S., Anezakis, V.-D., 2018. **An innovative soft computing system for smart energy grids cybersecurity.** *Advances in Building Energy Research* 12, 3–24. <https://doi.org/10/gdp862>
 16. Demertzis, Konstantinos. Kikiras, P., Tziritas, N., Sanchez, S.L., Iliadis, L., 2018. **The Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cybersecurity Intelligence.** *Big Data and Cognitive Computing* 2, 35. <https://doi.org/10/gfkhpp>
 17. Demertzis, Konstantinos. Iliadis, L.S., 2016. **Ladon: A Cyber Threat Bio-Inspired Intelligence Management System.** *Journal of Applied Mathematics & Bioinformatics*, vol.6, no.3, 2016, 45-64, ISSN: 1792-6602 (print), 1792-6939 (online), Scienpress Ltd, 2016.
 18. Demertzis, K., N. Tziritas, P. Kikiras, S. L. Sanchez, and L. Iliadis. **The Next Generation Cognitive Security Operations Center: Adaptive Analytic Lambda Architecture for Efficient Defense against Adversarial Attacks.** *Big Data Cognitive Computing* 3, no. 1 (2019): 6. doi:10.3390/bdcc3010006.
 19. Demertzis, K.; Rantos, K.; Drosatos, G. **A Dynamic Intelligent Policies Analysis Mechanism for Personal Data Processing in the IoT Ecosystem.** *Big Data Cogn. Comput.* 2020, 4, 9.
 20. Demertzis, K.; Iliadis, L. **GeoAI: A Model-Agnostic Meta-Ensemble Zero-Shot Learning Method for Hyperspectral Image Analysis and Classification.** *Algorithms* 2020, 13, 61
 21. Anezakis, V.-D., L. Iliadis, K. Demertzis, and G. Mallinis. **Hybrid Soft Computing Analytics of Cardiorespiratory Morbidity and Mortality Risk Due to Air Pollution.** In *Information Systems for Crisis Response and Management in Mediterranean Countries, Lecture Notes in Business Information Processing.* Edited by I. M. Dokas, N. Bellamine-Ben Saoud, J. Dugdale, and P. Díaz, 87–105. Springer International Publishing, 2017. doi:10.1007/978-3-319-67633-3_8.
 22. Demertzis, Konstantinos. Iliadis, L.S., Anezakis, V.-D., 2018. **Extreme deep learning in biosecurity: the case of machine hearing for marine species identification.** *Journal of Information and Telecommunication* 2, 492–510. <https://doi.org/10/gdwszn>

23. Iliadis, L., V.-D. Anezakis, **K. Demertzis**, and G. Mallinis. 2017. **Hybrid Unsupervised Modeling of Air Pollution Impact to Cardiovascular and Respiratory Diseases**. *IJISCRAM* 9, 13–35. <https://doi.org/10/gfkhpm> doi:10.4018/IJISCRAM.2017070102.

arxiv

24. V. Demertzi and **K. Demertzis**, **A Hybrid Adaptive Educational eLearning Project based on Ontologies Matching and Recommendation System**, arXiv:2007.14771 [cs], Jul. 2020, Accessed: Jul. 31, 2020. [Online]. Available: <https://arxiv.org/abs/2007.14771>
25. **K. Demertzis**, L. Magafas, and D. Tsiotas, “**Flattening the COVID-19 Curve: The ‘Greek’ case in the Global Pandemic,**” arXiv:2010.12040 [stat], Oct. 2020, Accessed: Oct. 26, 2020. [Online]. Available: <http://arxiv.org/abs/2010.12040>.
26. **Demertzis K**, Tsiotas D, Magafas L. **Modeling and forecasting the COVID-19 temporal spread in Greece: an exploratory approach based on complex network defined splines**. arXiv:200501163 [physics] [Internet]. 2020 May 3 [cited 2020 May 5]; Available from: <http://arxiv.org/abs/2005.01163>

In press

27. V. Demertzi and **K. Demertzis**, **A Hybrid Adaptive Educational eLearning Project based on Ontologies Matching and Recommendation System** Learning, Media and Technology, Taylor & Francis Group, (**Impact Factor 2.547**) *in press*
28. **Konstantinos Demertzis**, Lazaros Iliadis, Ilias Pimenidis **Geo-AI to Aid Disaster Response: Domain Adaptation with Memory-Augmented Deep Convolutional Reservoir Computing**, Integrated Computer-Aided Engineering, IOS Press, (**Impact Factor 4.904**), *in press*

Conferences

29. **Demertzis K.**, Iliadis L., Pimenidis E. (2020) **Large-Scale Geospatial Data Analysis: Geographic Object-Based Scene Classification in Remote Sensing Images by GIS and Deep Residual Learning**. In: Iliadis L., Angelov P., Jayne C., Pimenidis E. (eds) Proceedings of the 21st EANN (Engineering Applications of Neural Networks) 2020 Conference. EANN 2020. Proceedings of the International Neural Networks Society, vol 2. Springer, Cham.
30. Demertzis, K., L. Iliadis, P. Kikiras, and N. Tziritas. **Cyber-Typhon: An Online Multi-task Anomaly Detection Framework**. In Artificial Intelligence Applications and Innovations. AIAI 2019. IFIP Advances in Information and Communication Technology, Vol. 559. Edited by J. MacIntyre, I. Maglogiannis, L. Iliadis, and E. Pimenidis. Cham: Springer, 2019. doi:10.1007/978-3-030-19823-7_2.
31. Demertzis, K., and L. Iliadis. **Bio-inspired Hybrid Intelligent Method for Detecting Android Malware**. In Knowledge, Information and Creativity Support Systems, Advances in Intelligent Systems and Computing. Edited by S. Kunifuji, G. A. Papadopoulos, A. M. J. Skulimowski, and J. Kacprzyk, 289–304. Springer International Publishing, 2016. doi:10.1007/978-3-319-27478-2_20.
32. Demertzis, K., and L. Iliadis. **Evolving Smart URL Filter in a Zone-Based Policy Firewall for Detecting Algorithmically Generated Malicious Domains**. In Statistical Learning and Data Sciences. Edited by A. Gammerman, V. Vovk, and H. Papadopoulos, 223–33.

- Lecture Notes in Computer Science. Springer International Publishing, 2015. doi:10.1007/978-3-319-17091-6_17.
33. Demertzis, K., and L. Iliadis. **SAME: An Intelligent Anti-malware Extension for Android ART Virtual Machine**. In Computational Collective Intelligence. Edited by M. Núñez, N. T. Nguyen, D. Camacho, and B. Trawiński, 235–45. Lecture Notes in Computer Science. Springer International Publishing, 2015. doi:10.1007/978-3-319-24306-1_23.
 34. Demertzis, K., and L. Iliadis. **A Hybrid Network Anomaly and Intrusion Detection Approach Based on Evolving Spiking Neural Network Classification**. In E-Democracy, Security, Privacy and Trust in a Digital World, Communications in Computer and Information Science. Edited by A. B. Sideridis, Z. Kardasiadou, C. P. Yialouris, and V. Zorkadis, 11–23. Springer International Publishing, 2014. doi:10.1007/978-3-319-11710-2_2.
 35. Demertzis, K., and L. Iliadis. **Evolving Computational Intelligence System for Malware Detection**. In Advanced Information Systems Engineering Workshops, Lecture Notes in Business Information Processing. Edited by L. Iliadis, M. Papazoglou, and K. Pohl, 322–34. Springer International Publishing, 2014. doi:10.1007/978-3-319-07869-4_30.
 36. Demertzis, K., L. Iliadis, and V. Anezakis. 2018. **MOLESTRA: A Multi-Task Learning Approach for Real-Time Big Data Analytics**, in: 2018 Innovations in Intelligent Systems and Applications (INISTA). Presented at the 2018 Innovations in Intelligent Systems and Applications (INISTA), pp. 1–8. doi:10.1109/INISTA.2018.8466306.
 37. Demertzis, Konstantinos. Iliadis, L., Anezakis, V.-D., 2018. **A Dynamic Ensemble Learning Framework for Data Stream Analysis and Real-Time Threat Detection**, in: Kůrková, V., Manolopoulos, Y., Hammer, B., Iliadis, L., Maglogiannis, I. (Eds.), Artificial Neural Networks and Machine Learning – ICANN 2018, Lecture Notes in Computer Science. Springer International Publishing, pp. 669–681.
 38. Demertzis, Konstantinos. Iliadis, L., Spartalis, S., 2017. **A Spiking One-Class Anomaly Detection Framework for Cyber-Security on Industrial Control Systems**, in: Boracchi, G., Iliadis, L., Jayne, C., Likas, A. (Eds.), Engineering Applications of Neural Networks, Communications in Computer and Information Science. Springer International Publishing, pp. 122–134.
 39. Rantos, K., G. Drosatos, K. Demertzis, C. Ilioudis, and A. Papanikolaou. 2018. **Blockchain-based Consents Management for Personal Data Processing in the IoT Ecosystem**. Presented at the International Conference on Security and Cryptography, pp. 572–577. doi:10.5220/0006911005720577.
 40. Rantos, K., G. Drosatos, K. Demertzis, C. Ilioudis, A. Papanikolaou, and A. Kritsas. **ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT Using Blockchain Technology**. In Innovative Security Solutions for Information Technology and Communications. SECITC 2018, Vol. 11359. Edited by J. L. Lanet and C. Toma. Lecture Notes in Computer Science. Cham: Springer, 2019. doi:10.1007/978-3-030-12942-2_23.
 41. Demertzis, K.; Rantos, K.; Drosatos, G. **A Dynamic Intelligent Policies Analysis Mechanism for Personal Data Processing in the IoT Ecosystem**. Big Data Cogn. Comput. 2020, 4, 9.
 42. Demertzis, K., L. Iliadis, and V. D. Anezakis. **A Machine Hearing Framework for Real-Time Streaming Analytics Using Lambda Architecture**. In Engineering Applications of Neural Networks. EANN 2019. Communications in Computer and Information Science, Vol. 1000. Edited by J. Macintyre, L. Iliadis, I. Maglogiannis, and C. Jayne. Cham: Springer, 2019. doi:10.1007/978-3-030-20257-6_21.

43. Anezakis, V., G. Mallinis, L. Iliadis, and K. Demertzis. 2018. **Soft computing forecasting of cardiovascular and respiratory incidents based on climate change scenarios**, in: 2018 IEEE Conference on Evolving and Adaptive Intelligent Systems (EAIS). Presented at the 2018 IEEE Conference on Evolving and Adaptive Intelligent Systems (EAIS), pp. 1–8doi:10.1109/EAIS.2018.8397174.
44. Anezakis, V.-D., K. Demertzis, and L. Iliadis. 2018. **Classifying with fuzzy chi-square test: The case of invasive species**. AIP Conference Proceedings 1978, 290003. <https://doi.org/10/gdtm5q>
45. Anezakis, V.-D., K. Demertzis, L. Iliadis, and S. Spartalis. **A Hybrid Soft Computing Approach Producing Robust Forest Fire Risk Indices**. In Artificial Intelligence Applications and Innovations, IFIP Advances in Information and Communication Technology. Edited by L. Iliadis and I. Maglogiannis, 191–203. Springer International Publishing, 2016. doi:10.1007/978-3-319-44944-9_17.
46. Anezakis, V.-D., K. Demertzis, L. Iliadis, and S. Spartalis. **Fuzzy Cognitive Maps for Long-Term Prognosis of the Evolution of Atmospheric Pollution, Based on Climate Change Scenarios: The Case of Athens**. In Computational Collective Intelligence. Edited by N.-T. Nguyen, L. Iliadis, Y. Manolopoulos, and B. Trawiński, 175–86. Lecture Notes in Computer Science. Springer International Publishing, 2016. doi:10.1007/978-3-319-45243-2_16.
47. Bougoudis, I., K. Demertzis, L. Iliadis, V.-D. Anezakis, and A. Papaleonidas. **Semi-supervised Hybrid Modeling of Atmospheric Pollution in Urban Centers**. In Engineering Applications of Neural Networks, Communications in Computer and Information Science. Edited by C. Jayne and L. Iliadis, 51–63. Springer International Publishing, 2016. doi:10.1007/978-3-319-44188-7_4.
48. Demertzis, Konstantinos. Anezakis, V.-D., Iliadis, L., Spartalis, S., 2018. **Temporal Modeling of Invasive Species' Migration in Greece from Neighboring Countries Using Fuzzy Cognitive Maps**, in: Iliadis, L., Maglogiannis, I., Plagianakos, V. (Eds.), Artificial Intelligence Applications and Innovations, IFIP Advances in Information and Communication Technology. Springer International Publishing, pp. 592–605.
49. Demertzis, K., and L. Iliadis. **Adaptive Elitist Differential Evolution Extreme Learning Machines on Big Data: Intelligent Recognition of Invasive Species**. In Advances in Big Data, Advances in Intelligent Systems and Computing. Edited by P. Angelov, Y. Manolopoulos, L. Iliadis, A. Roy, and M. Vellasco, 333–45. Springer International Publishing, 2017. doi:10.1007/978-3-319-47898-2_34.
50. Demertzis, K., and L. Iliadis. **Intelligent Bio-Inspired Detection of Food Borne Pathogen by DNA Barcodes: The Case of Invasive Fish Species Lagocephalus Sceleratus**. In Engineering Applications of Neural Networks, Communications in Computer and Information Science. Edited by L. Iliadis and C. Jayne, 89–99. Springer International Publishing, 2015. doi:10.1007/978-3-319-23983-5_9.
51. Demertzis, K., L. Iliadis, and V. Anezakis. 2017. **A deep spiking machine-hearing system for the case of invasive fish species**, in: 2017 IEEE International Conference on INnovations in Intelligent SysTems and Applications (INISTA). Presented at the 2017 IEEE International Conference on INnovations in Intelligent SysTems and Applications (INISTA), pp. 23–28doi:10.1109/INISTA.2017.8001126.
52. Iliadis, L., V.-D. Anezakis, K. Demertzis, and S. Spartalis. **Hybrid Soft Computing for Atmospheric Pollution-Climate Change Data Mining**. In Transactions on Computational Collective Intelligence XXX. Edited by N. Thanh Nguyen and R.

Kowalczyk, 152–77. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018. doi:10.1007/978-3-319-99810-7_8.

In press

53. Lykourgos Magafas, **Konstantinos Demertzis**, Dimitrios Tsiotas, **COVID-19 Pandemic Analytics: Greece Case Study**, Proceedings of the FEBA Jubilee Conference "Just and SMART Transitions" 2020 Conference. 23-24 November 2020, FEBA, Sofia

Book Chapters

54. Demertzis, K., and L. Iliadis. **A Bio-Inspired Hybrid Artificial Intelligence Framework for Cyber Security**. In Computation, Cryptography, and Network Security. Edited by N. J. Daras and M. T. Rassias, 161–93. Cham: Springer International Publishing, 2015. doi:10.1007/978-3-319-18275-9_7.
55. Demertzis, Konstantinos. Iliadis, L.S., 2018. **Real-time Computational Intelligence Protection Framework Against Advanced Persistent Threats**. Book entitled Cyber-Security and Information Warfare, Series: Cybercrime and Cybersecurity Research, NOVA science publishers, ISBN: 978-1-53614-385-0, Chapter 5.
56. Demertzis, K., and L. Iliadis. **A Computational Intelligence System Identifying Cyber-Attacks on Smart Energy Grids**. In Modern Discrete Mathematics and Analysis: With Applications in Cryptography, Information Systems and Modeling, Springer Optimization and Its Applications. Edited by N. J. Daras and T. M. Rassias, 97–116. Cham: Springer International Publishing, 2018. doi:10.1007/978-3-319-74325-7_5.
57. Demertzis, K., and L. Iliadis. 2018. **The Impact of Climate Change on Biodiversity: The Ecological Consequences of Invasive Species in Greece**, in: Leal Filho, W., Manolas, E., Azul, A.M., Azeiteiro, U.M., McGhie, H. (Eds.), Handbook of Climate Change Communication: Vol. 1: Theory of Climate Change Communication, Climate Change Management. Springer International Publishing, Cham, pp. 15–38. https://doi.org/doi:10.1007/978-3-319-69838-0_2.

In press

58. **K. Demertzis**, Bougoudis, I., L. Iliadis, **Geospatial Big Data Analytics: Air Quality and Pollution Forecasting Using AI and GIS**, Machine Learning Paradigms – Advances in Data Analytics, Springer, Intelligent Systems Reference Library bookseries

Greek Books Chapters

59. Κωνσταντίνος Δεμερτζής, 2018, **Ενίσχυση της Διοικητικής Ικανότητας των Δήμων Μέσω της Ηλεκτρονικής Διακυβέρνησης: Η Στρατηγική των Έξυπνων Πόλεων με Σκοπό την Αειφόρο Ανάπτυξη**, Θέματα Δασολογίας και Διαχείρισης Περιβάλλοντος και Φυσικών Πόρων, 10ος Τόμος: Περιβαλλοντική Πολιτική: Καλές Πρακτικές, Προβλήματα και Προοπτικές, σελ. 84 - 100, ISSN: 1791-7824, ISBN: 978-960-9698-14-6, Νοέμβριος 2018, Εκδοτικός Οίκος: Δημοκρίτειο Πανεπιστήμιο Θράκης.

60. Κωνσταντίνος Δεμερτζής, Λάζαρος Ηλιάδης, 2015, **Γενετική Ταυτοποίηση Χωροκατακτητικών Ειδών με Εξελιγμένες Μεθόδους Τεχνητής Νοημοσύνης: Η Περίπτωση του Ασιατικού Κουνουπιού Τίγρης (Aedes Albopictus)**. Θέματα Δασολογίας & Διαχείρισης Περιβάλλοντος & Φυσικών Πόρων, 7ος τόμος, Κλιματική Αλλαγή: Διεπιστημονικές Προσεγγίσεις, ISSN: 1791-7824, ISBN: 978-960-9698-11-5, Εκδοτικός Οίκος: Δημοκρίτειο Πανεπιστήμιο Θράκης.

Panhellenic Conferences

61. Ανεζάκης, Βαρδής-Δημήτριος, Κωνσταντίνος Δεμερτζής, Λάζαρος Ηλιάδης, (2017) **Πρόβλεψη Χαλαζοπτώσεων Μέσω Μηχανικής Μάθησης**. 3ο Πανελλήνιο Συνέδριο Πολιτικής Προστασίας SafeEnros 2016: Οι νέες τεχνολογίες στην υπηρεσία της Πολιτικής Προστασίας, Proceedings, ISBN : 978-960-89345-7-3, Ιούνιος 2017, Εκδοτικός Οίκος: Δημοκρίτειο Πανεπιστήμιο Θράκης.
62. Κωνσταντίνος Δεμερτζής, Λάζαρος Ηλιάδης, 2019, **Η Αξιοποίηση των Συγχρόνων Τεχνολογιών Πληροφορικής και Επικοινωνιών στην Μουσειοπαιδαγωγική: Η Περίπτωση του Λαογραφικού Μουσείου Νέας Ορεστιάδας και Περιφέρειας**, Πρακτικά 2ου Πανελληνίου Συνεδρίου Ιστορίας και Πολιτισμού της Ορεστιάδας Πολιτιστική Κληρονομιά και Τοπική Ανάπτυξη, Έκδοση Σχολής Επιστημών Γεωπονίας και Δασολογίας Δημοκρίτειου Πανεπιστημίου Θράκης και Δήμου Ορεστιάδας, ISBN: 978-618-00-1152-4, Απρίλιος 2019, Επιμέλεια: Ευάγγελος Μανωλάς.

Articles

63. Κωνσταντίνος Δεμερτζής, **Open Source Intelligence**, (2014), Available from: http://army.gr/sites/default/files/mag_20140301.pdf
64. Κωνσταντίνος Δεμερτζής, Αν. Καθηγητής Χαράλαμπος Σκιάνης, (2011), **Smart Energy Grids, Ο ηλεκτρισμός αποκτά ευφυΐα**, Available from: http://army.gr/sites/default/files/mag_20111001.pdf
65. Κωνσταντίνος Δεμερτζής, (2009), Ασύρματη Επανάσταση στα 2,4 GHz, Available from: http://army.gr/sites/default/files/mag_20090601.pdf