

Monitor Unusual Behavior on Networked Machines

GREYCORTEX

***e*FOCUS**

Who? Why?

- Company: GREYCORTX s.r.o., Brno, Czech Republic
- Founded: 2016, with origins from 2013 and 2009
- A group of hackers, computer geeks, security experts, computer malware researchers, data mining experts, artificial intelligence nerds, and a manager
- To help protecting your business and critical infrastructure in most domains
 - Yes, this is not about physical security and fixing faulty code 😊

What?

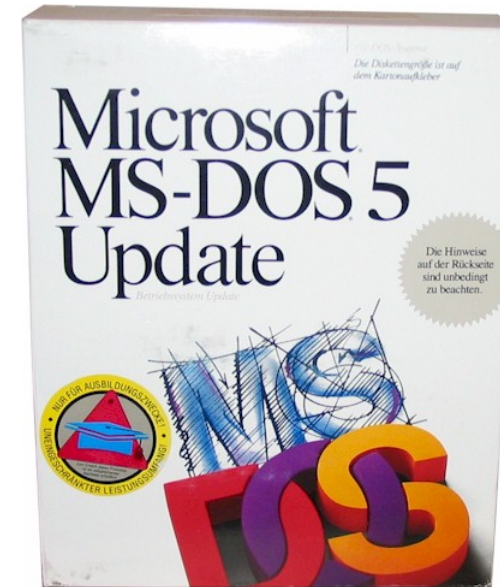
- Product: GREYCORTX MENDEL
- Network Traffic Analysis with Big Data and Artificial Intelligence
 - Detecting the most Advanced Persistent Threats
 - Detecting traditional malware in transit
 - Detecting miscompliance
 - Measuring what is „normal“ and promoting the „excursive“ to your attention
 - Analyzing performance issues
 - Storing evidence and visualizing network traffic (N.R.T. & historic)
 - Correlating detailed metadata to investigate incidents with ease

Network Security Evolution

Network and data security before and now

Network and data security before: OS

- Proprietary systems, limited tools
 - Only few really understood, fewer considered
- No Access Control
- Common Transport media up to 1,6MB
- Limited security awareness
 - Users, programmers, admins
 - Access control only in applications
- Attack surface
 - Boot worms to spread (stealth)
 - Program viruses to annoy or destroy (visible)
 - Physical stealing of media or copying content



MS-DOS Box - Image Copyright @ 2004-2011 Wolfgang Kainz-Huber
[2016-09-16 13:13] <http://www.computermuseum-muenchen.de/dictionary/history/dos.html>

Network and data security before: Network

1/2

- Proprietary systems, limited tools
 - Very few really understood
- Island networks
 - Low count of computers
 - Almost no computers at home
 - Low speeds (1-10/100Mbps)
- Weak links between networks
 - DialUp 56k, Leased 64k
 - Limited protocol routability
 - IPX was routable but rarely routed...
 - IP (SLIP) for Telnet and FTP

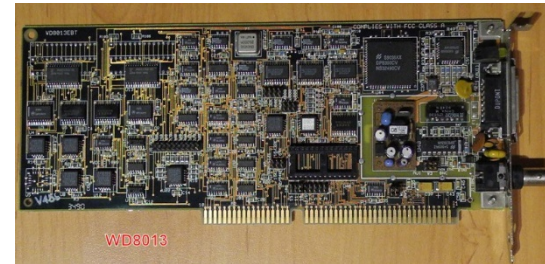


NetWare Box - Image © Mark Richards [2016-09-16 12:15]
<http://www.computerhistory.org/revolution/networking/19/382/2134>

Network and data security before: Network

2/2

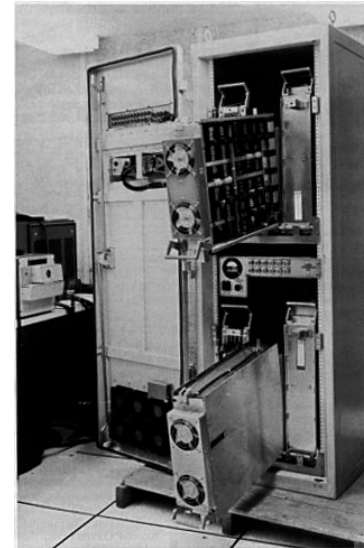
- Just a few apps in use
 - File access and sharing (FTP, NFS, NW, BBS)
 - Remote control (Telnet, xmodem)
- Attack surface
 - Disconnecting Ethernet terminator ☺
 - Stealing plaintext passwords via tap
 - Evading access controls
 - Copying data over network
- You had to come close and tap the wire!
Or dial-in.



WD8013 NIC - Image © Administrator [2016-09-16 14:01]
<http://www.z80.eu/blog/index.php?m=07&y=14&d=12&entry=entry140712-185307>

Only five decades ago in this galaxy

- Early 1960's - packet switching network concepts (aka „hot potato routing“ by Paul Baran)*
- ARPANet project started in 1967*
 - 1969 – AlohaNet, later Ethernet
 - 1972 – radio network
 - 1973 – TCP protocol
- Late 1970's computers started growing personal
 - (8008, 8080, Z80, 6502)
- Late 1980's personal computers (PC) standardized
- Early 1990's - privatization of NSFNet
- April 1991 - open source operating system for everybody (GNU/Linux)
- 13.2.1992 Internet in ČSFR, 1995 commercial



Interface Message Processor - Image © Randy H. Katz [2016-09-16 12:15]
<http://bnrg.cs.berkeley.edu/~randy/Courses/CS39C.S97/Internet/Internet.html>

* In [2017-09-19 15:37] <http://bnrg.cs.berkeley.edu/~randy/Courses/CS39C.S97/Internet/Internet.html>

Network and data security today: Factors

1/4

- Computers everywhere
 - CPUs are powerfull and cheap
 - Cheap MCUs win over traditional hardware design
 - Mostly for entertainment purposes
- Networks everywhere
 - Wired (copper, fibre), wireless (433 MHz, 2.45, 5.2/5.6/5.8, 66 GHz)
 - From ultra low power (8 bytes a day) to ultra fast (n x 100Gbps)
 - Making everything online (from mainframes to „not-so-“smart meters)
- One network to rule them all
 - Pretty everything is transported over Internetwork Protocol (v4, v6)
 - Networks are interconnected in real time, Skynet does exist 😊

Network and data security today: Factors

2/4

- Almost everything moved to cyberspace
 - „Computer aided everything“
 - Although we consume much more paper than before
- Content has gone online
 - News, media, entertainment
 - Sharing (spending) life on social networks
 - Government registers, reports, and submissions
- Cloud (serverless) computing paradigm
 - Still it is someone else's computer
 - Is there a real privacy?

Network and data security today: Factors

3/4

- No simple and closed technology anymore
 - Standards and research published online (paid, free, or „free“)
 - Everybody depends on other's brainwork, understanding and implementation
- Community-driven development
 - Open software and open hardware
 - Anybody can contribute (code, ammend, modify, repair)
 - Easy to inject fake, insecure code, or a bug, that can hide for ages (e.g. Heartbleed)
- Things are growing complex
 - Linux kernel: from 10,239 lines (ver. 0.01) to 19.5 million lines (ver. 4.1)*, 14,000 contributors
 - Always a work in progress – 13914 todos, hacks, workarounds, and fixmes (4.13-rc7)*

Network and data security today: Factors

4/4

- A lot of communication flows
 - Data and service communications may flow different paths
 - Some network and application protocols generate a lot of network traffic even in idle state
- Experts shortage
 - Only a few can really understand
 - Demands are massive
 - Anybody can fit
 - Real knowledge is hard to judge or measure
 - Expertise can be neither taught nor read from textbooks
 - and it evolves over time in both directions

Are Best Current Practices really the best?

- Do you change your password every 6 months?
 - How big is your change? 1p@ssword1 to 2p4ssw0rd2? Really THAT big?
- Is your password complex enough?
 - Or is it your mother's maiden name?
- Have you created different password for each service you use?
- Honestly, can you remember it, or did you write it on a yellow sticky paper and stuck on lower frame of your LCD? Do you use a password vallet app?
- Why would you need to change password if it is really strong and it has not been compromised yet?
 - But, how do you know it is really strong?
 - And once you know it has been compromised, how late is it?

How to eliminate possible attack?



Silo the systems! Make them isolated again!

- No way. There is no such thing as completely isolated one.
- There are various surfaces to attack.
- You can increase the cost of an attack by limiting the attack surfaces.
- Security is not convenient.
- You can't reach security by obscuring things. The only security is the one facing towards incoming threats.

Where is the actual perimeter?

1/3

- Network
 - The most used attack medium, usually combined with other vectors
 - Attacks may come from the outside and also from inside
 - Has to be hardened layer by layer, various approaches exist for each layer
 - Monitoring nodes behavior is highly desired
- Operating System
 - Usually a victim, can be used as attack tool both inside and outside
 - Can be attacked from network and software, a vulnerability always exists
 - Removing unused components, patching, updating, hiding versions
 - Monitoring of activities and behavior and scanning for signatures desired

Where is the actual perimeter?

2/3

- Software and services
 - A vulnerability always exists
 - Can be used as attack tool both inside and outside
 - Removing unused features, patching, updating, hiding implementation details
 - Monitoring of activities and behavior is desired, scanning as well
- Data (documents)
 - A software vulnerability is used to subvert content for execution
 - Users are mostly involved in gathering (viewing or downloading) such content
 - Documents have to come from known-to-be-safe sources
 - Documents have to be scanned for known malware signatures at least

Where is the actual perimeter?

3/3

- Peripherals and removable media, mobile and BYOD devices
 - Some peripherals may contain drivers or other executable code
 - May come infected from „outside“ world
 - Can be used as infiltration attack or data leakage tool
 - Execution may be suppressed by policies
 - Must be considered potentially harmful and separated from secure „internal“
 - Activities must be monitored, devices regularly scanned and verified
- People (users, programmers, administrators, consultants, etc.)
 - The weakest link, everybody has a price
 - Users have to be educated, motivated, and appropriately monitored

What does it mean?

- You can't make an attack impossible.
- It's your cost of attack mitigation controls related to value of protected assets to you versus attacker's cost of weaponry related to value of the same assets to the attacker.
 - You have to know whether an attack is in progress.
 - You have to know whether an attack was successful.
 - You have to know the details of an attack to find the broken link in your security chain.

How do I learn about an attack?

- At endpoints
 - By monitoring, scanning, and analyzing software behavior
 - Easy to install and use software available
- At network
 - By monitoring, scanning, and analyzing network traffic
 - Advanced, easy to deploy and use tool exists
- GREYCORTX MENDEL
 - Based on Artificial Intelligence, GMM, and Assisted Learning
 - Provides intelligent network traffic analysis

GREYCORTEX MENDEL

Advanced Network Traffic Analysis Tool

Seeing through your network

- We monitor
 - Network nodes
 - Network segments
 - Autonomous systems
 - Services
 - And all data flows between them
 - We do Deep Packet Inspection
 - We unpack tunneled data
 - We decrypt communication we have keys to
- To provide logically aggregated insights on your traffic
- To discover any new items in your internal network infrastructure
- To enable application and content analysis
- To give you true picture of your traffic

Advanced traffic indicators

- We measure
 - Volumes, throughputs, and delays
 - Perturbances and deviations
 - Application performance
- We collect
 - Our advanced security network metrics
 - Application layer data
 - Identities

To capture important data about your network, applications, services, and performance anomalies affecting user experience

To provide intelligent traffic analysis

To bind applications and users together

Artificial Intelligence verdict

- We check and detect
 - Reputations
 - Known attack signatures
 - Algorithmic repetitiveness
- We compute behavioral model
- We provide
 - Status dashboard
 - Correlated overview and details
 - Traffic records (packet capture)

To automatically hunt down cases of suspicious network traffic

Unusual or risky communication

Data leakage

Attack and breach

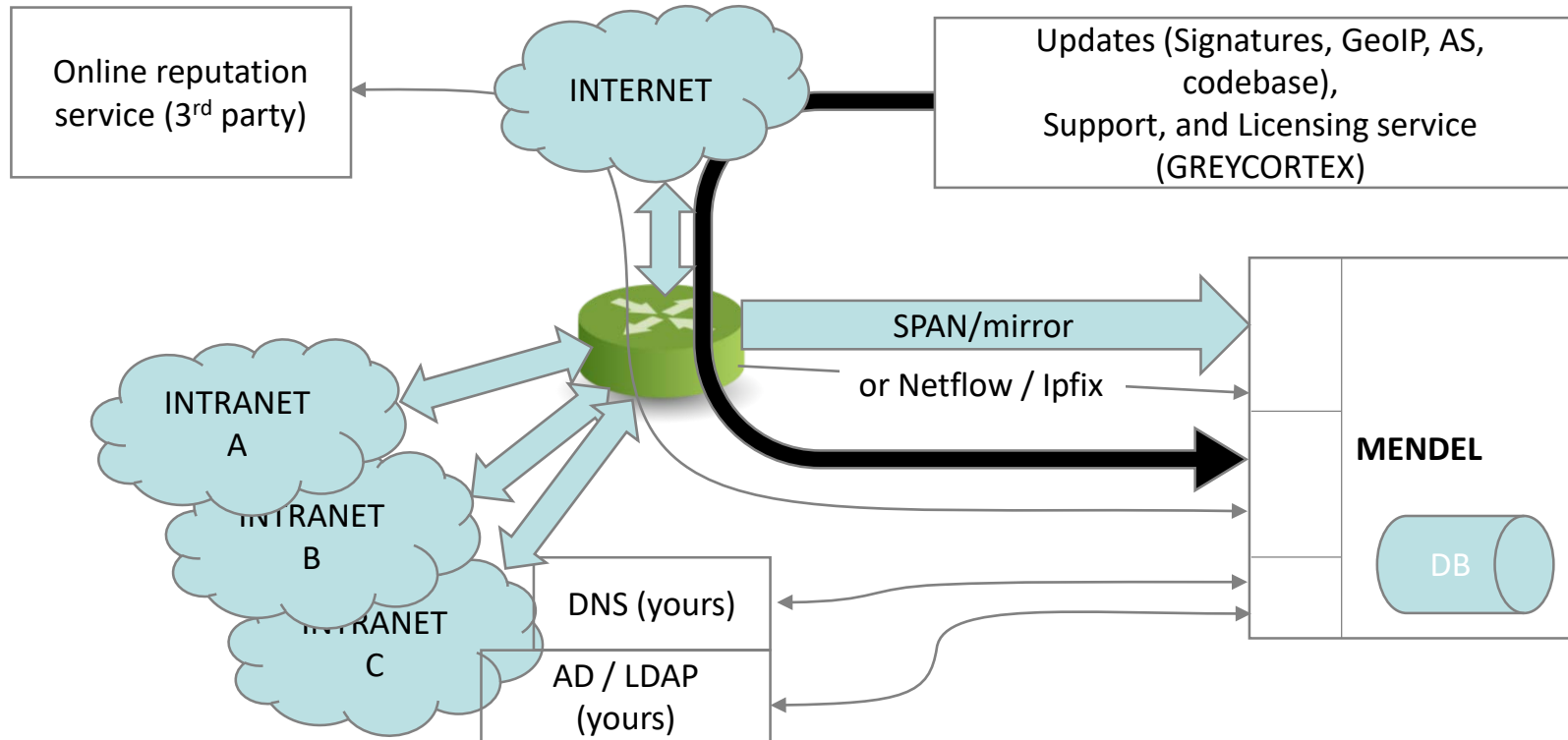
To prediction future traffic

To present collected findings

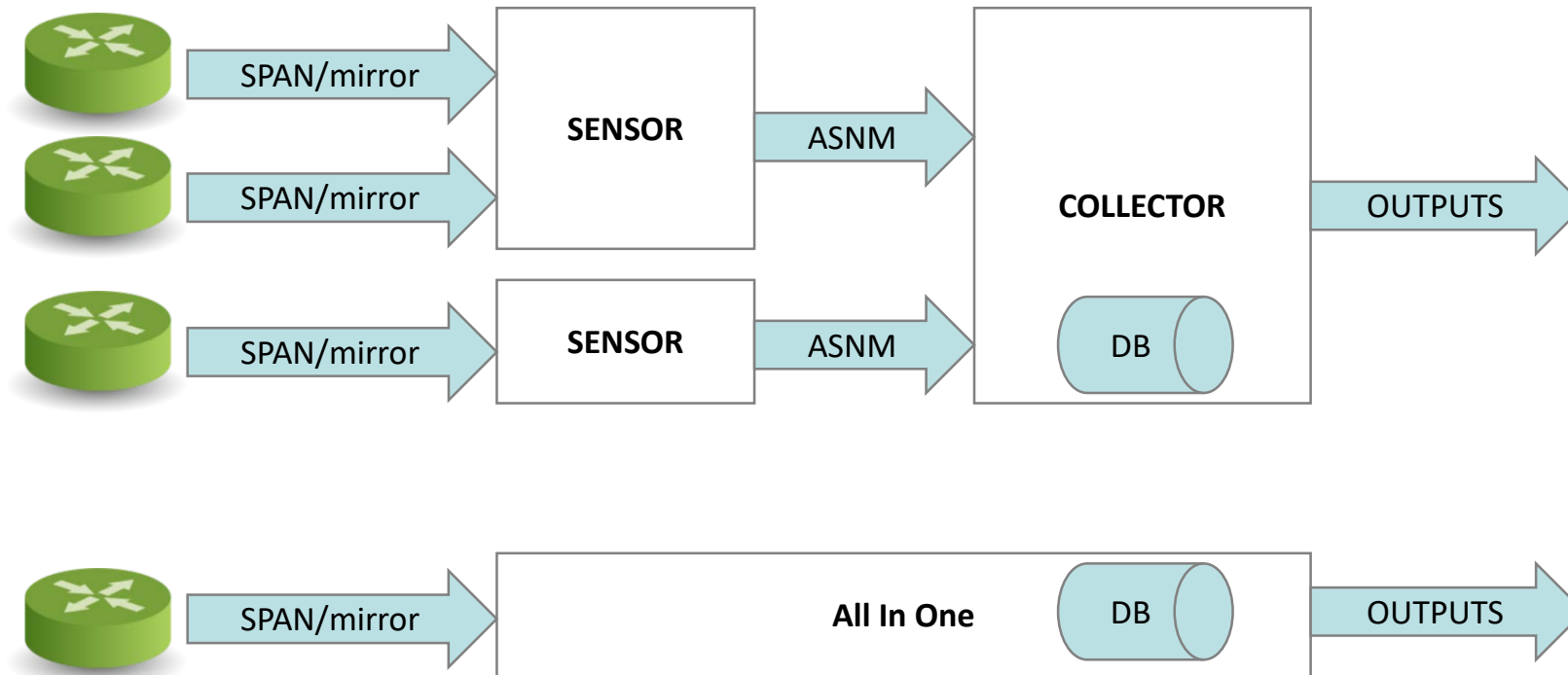
To teach the system

To ammend forensic data

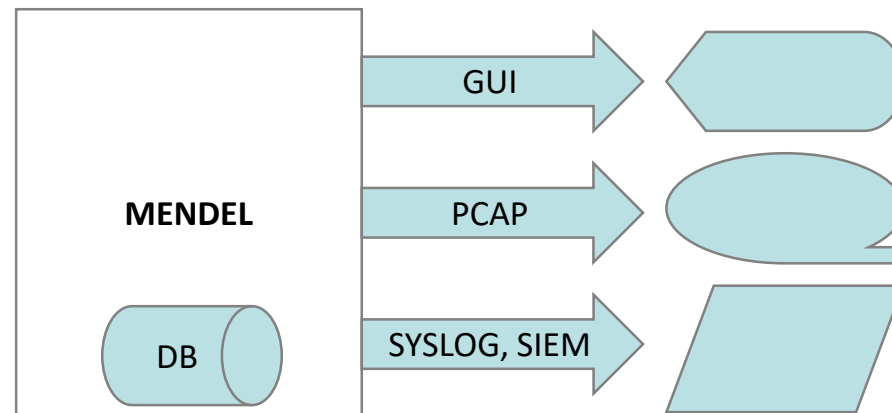
System Integration - inputs



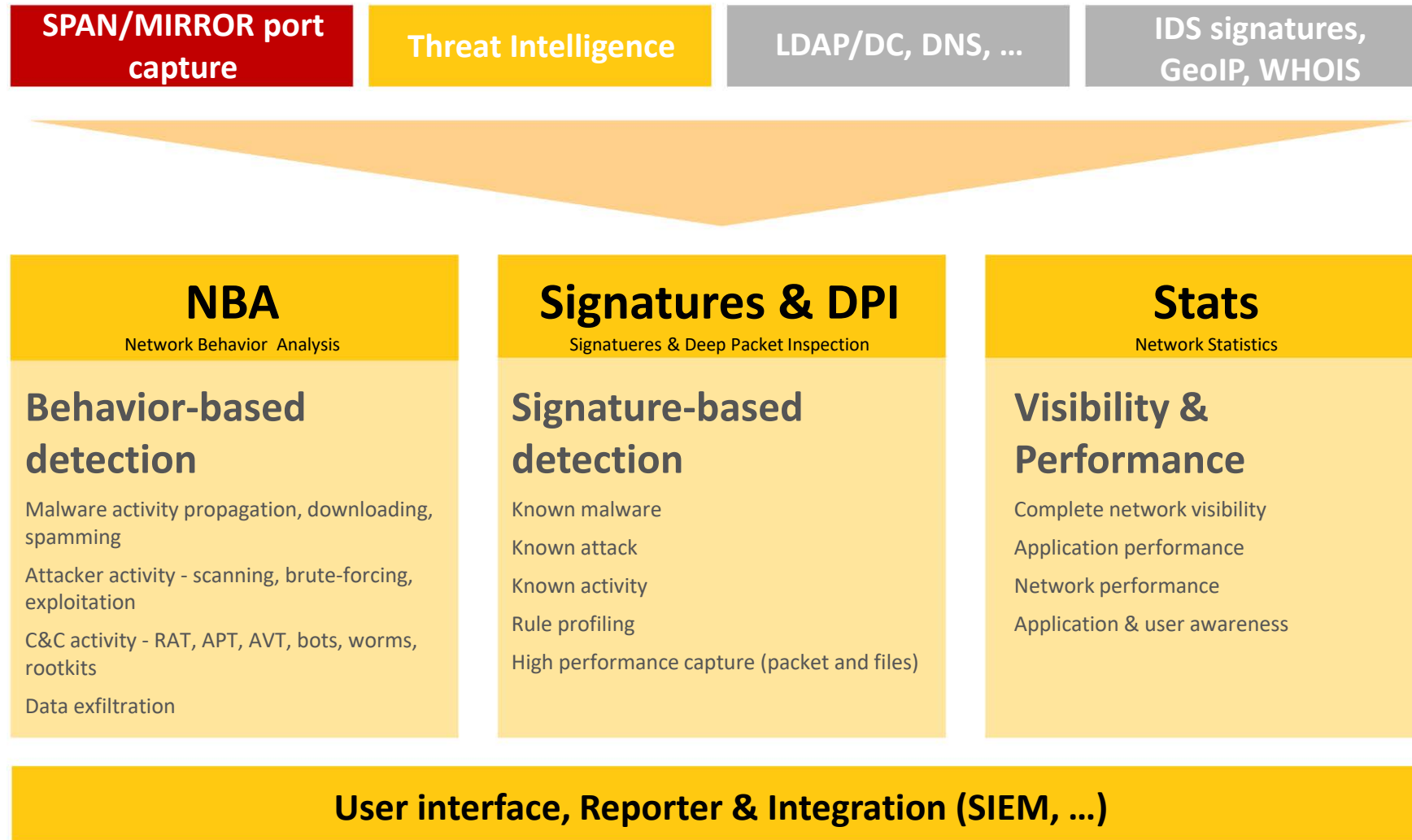
Processing paths



System Integration - outputs



Components



ASNM (Advanced Security Network Metrics)

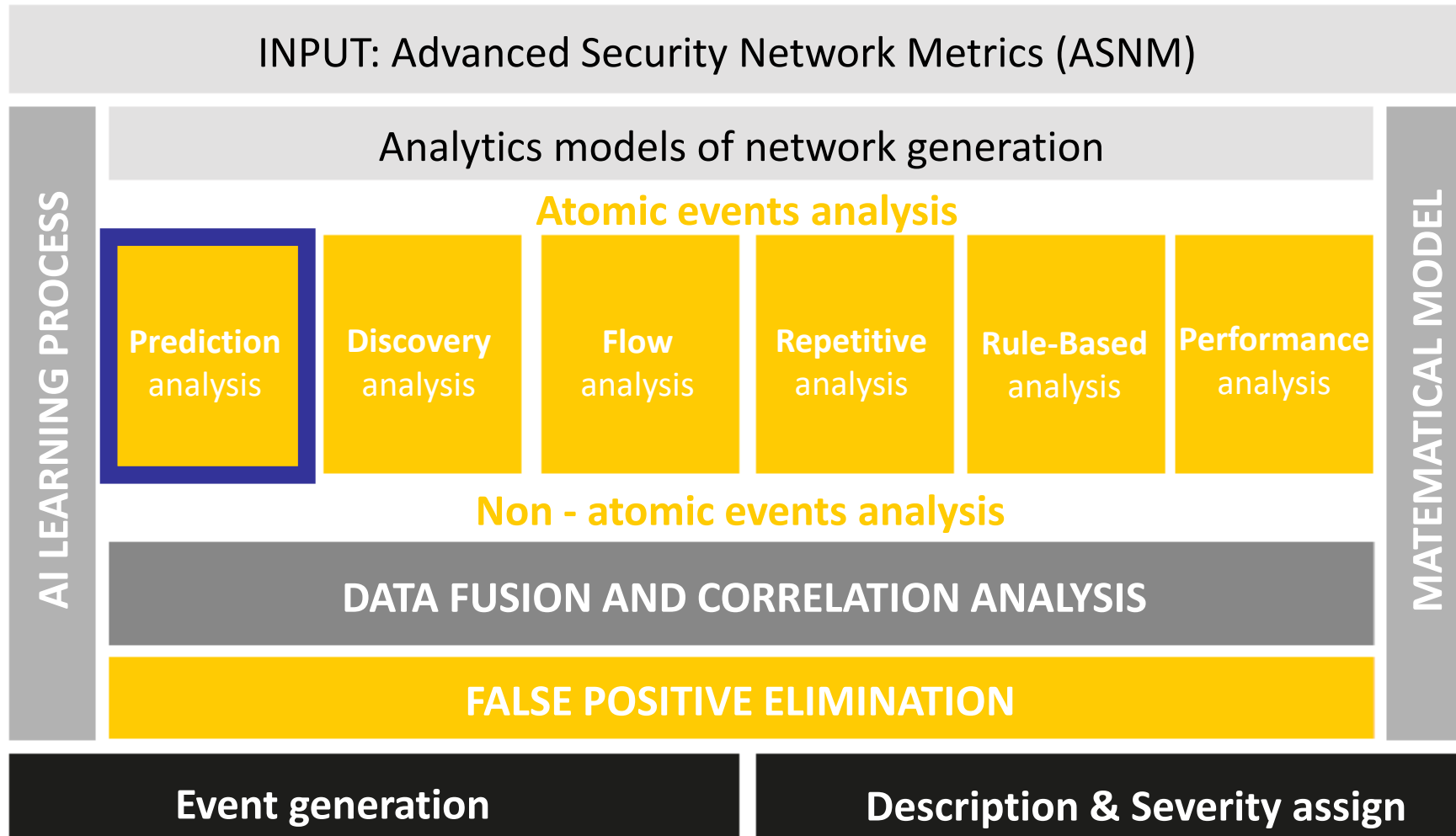
<i>sensor</i>	<i>dst_sn_addr</i>	-User-Agent	<i>-src_pktcnt</i>	dst_DCT
<i>timestamp</i>	<i>src_domain</i>	-X-Forwarded-	<i>-src_pktlen</i>	<i>src_trans</i>
<i>start_time</i>	<i>dst_domain</i>	For	<i>-src_strlen</i>	<i>-src_flags</i>
<i>end_time</i>	<i>ip_proto</i>	-Referer	<i>dst_cnt</i>	-src_err
output_type	<i>src_port</i>	-Method	<i>-dst_pktcnt</i>	<i>-src_qos</i>
<i>interface</i>	<i>dst_port</i>	-Protocol, ...	<i>-dst_pktlen</i>	<i>dst_trans</i>
<i>src_mac_addr</i>	<i>service (NBAR -</i>	dst_reply	<i>-dst_strlen</i>	<i>-dst_flags</i>
<i>dst_mac_addr</i>	<i>960 protocols)</i>	(http/s, DNS,	avg_rtt	-src_err
<i>ip_family</i>	src_request	smtp, ftp, sip,	avg_art	<i>-dst_qos</i>
<i>vlan_id</i>	(http/s, DNS,	...)	avg_dtt	sids
tunneled	smtp, ftp, sip,	-Status	avg_dlay	...
<i>src_ip_addr</i>	...)	-Content-Type	avg_jttr	(912
<i>dst_ip_addr</i>	-Host	-Location, ...	max_dlay	parameters in
<i>src_sn_addr</i>	-Uri	<i>src_cnt</i>	src_DCT	total)

Bidirectional (a flow represents both request and response)

Consistent (a flow for whole communication, no 1- or 5-minute splits)

MetaData: NetFlow/IPFIX **+Security** **+Performance** intelligence

Detection core - prediction



Prediction analysis

- Anomalies in data, flows, packets, peers, hosts, ports, performance
- Based on historical behavior (models)
 - Network & Subnets & Devices & Services
- Detected threats
 - Botnet communication, password guessing, data breaches, data enumeration, other attack preparation, scans, SPAM, ...
 - Unknown threats

EXCESSIVE COMMUNICATION THREAT

- The user normally communicates via 1 to 8 network services. The device tried to communicate via 39 services, and to 120 devices around the world including Brazil, Serbia, Bosnia and Herzegovina, the United States, Singapore, and Japan.

5 outlier: Entropy (ports) at Host									
Src IP			Dst IP			Src Subnet		Dst Subnet	
10.0.0.1			10.0.0.2			10.0.0.0/24		10.0.0.0/24	
Flows Peers									
	Src Host	Dst Host	Protocol	Src Port	Dst Port	Service	Src Packet Count	Src Packet Length	Src Data Length
+	10.0.0.1	10.0.0.2	UDP (17)	54281	45430		10	640	10240
+	10.0.0.1	10.0.0.3	UDP (17)	54281	60574		10	640	10240
+	10.0.0.1	10.0.0.4	UDP (17)	54281	43910		2	128	2048
+	10.0.0.1	10.0.0.5	TCP (6)	49913	389		6	396	6144
+	10.0.0.1	10.0.0.6	TCP (6)	49909	12350		22	2.74 k	1.37 M
+	10.0.0.1	10.0.0.7	UDP (17)	54281	443		2	128	2048
+	10.0.0.1	10.0.0.8	UDP (17)	54281	443		2	128	2048

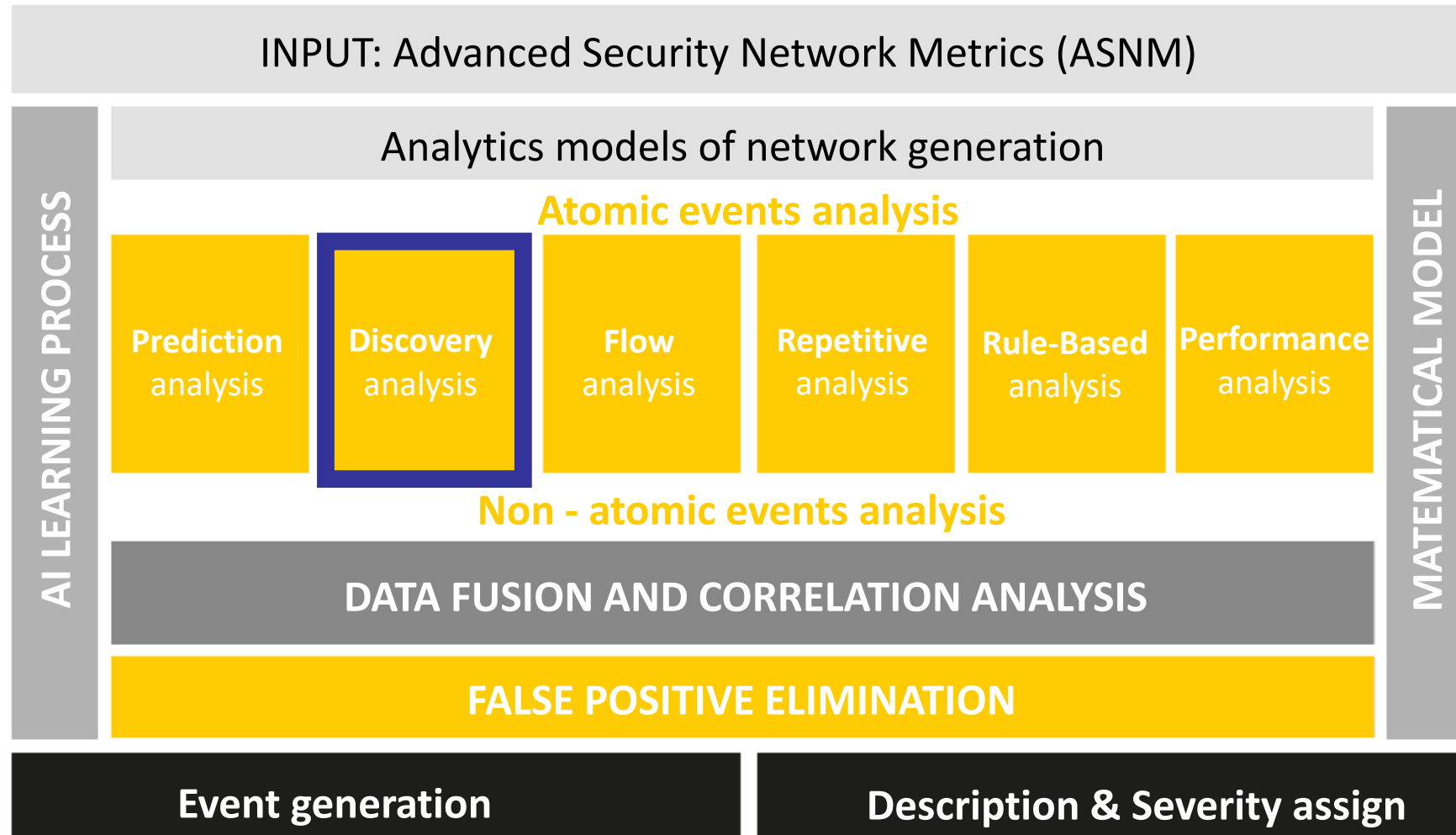
SMB ANOMALY

- 14 000 identical requests in an hour

Src MAC:	
Dst Name:	
Dst MAC:	
IP Family:	1
Src VLAN ID:	1101
Dst VLAN ID:	103
Interface:	em2
Tunneled:	0
Start Time:	
Duration:	3ms
Reported Timestamp:	
Output Type:	0

Request	Response
StructureSize: 64	StructureSize: 64
CreditCharge: 1	CreditCharge: 1
Status: 0	Status: 5
Command: NEGOTIATE	Command: NEGOTIATE
CreditRequest: 31	CreditRequest: 31
Flags: 0	Flags: 1
NextCommand: 0	NextCommand: 0
MessageId: 0	MessageId: 0
ProcessId: 65279	ProcessId: 65279
TreeId: 0	TreeId: 0
SessionId: 0	SessionId: 0
Signature: 0x00000000000000000000000000000000	Signature: 0x00000000000000000000000000000000
StructureSizeRaw: 16	StructureSizeRaw: 16

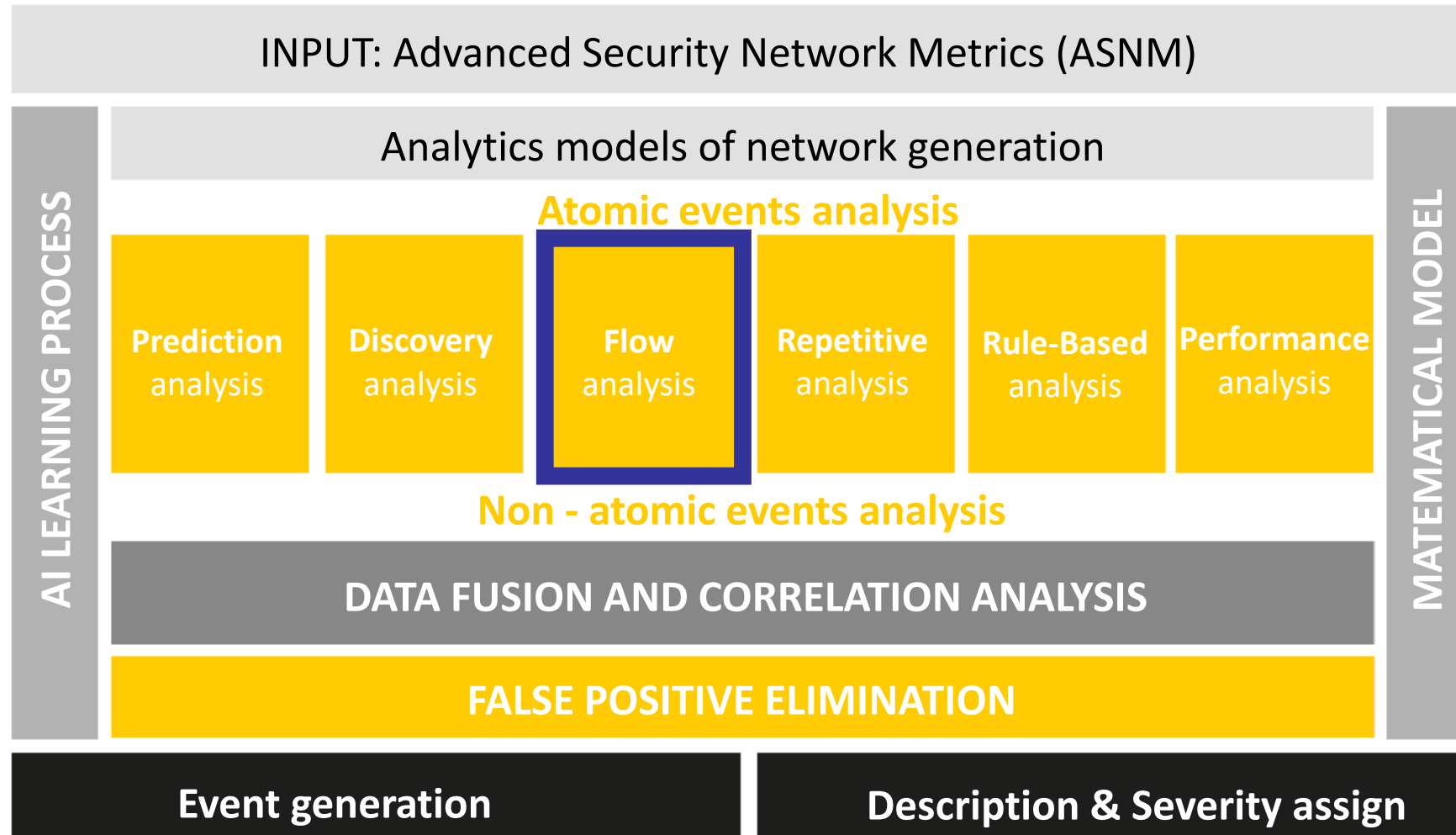
Detection core - discovery



Discovery analysis

- Communication matrices
 - Who communicates with whom
 - Detailed policies could be defined
- Detection of new or lost...
 - ...services, devices (IP, MAC, hostname), gateways, subnets.
- Focus on problems of availability of services and devices
- Detected events:
 - New forbidden service, Unreachable service/host, Duplicate/changed Hostname/MAC/IP, Change VLAN,
...

Detection core - flows



Flow analysis

- Detection of threats described by rules
 - Port scan (horizontal, vertical)
 - Brute-force and dictionary attacks
 - Data enumeration
 - DoS, DDoS

INTERNAL SCAN

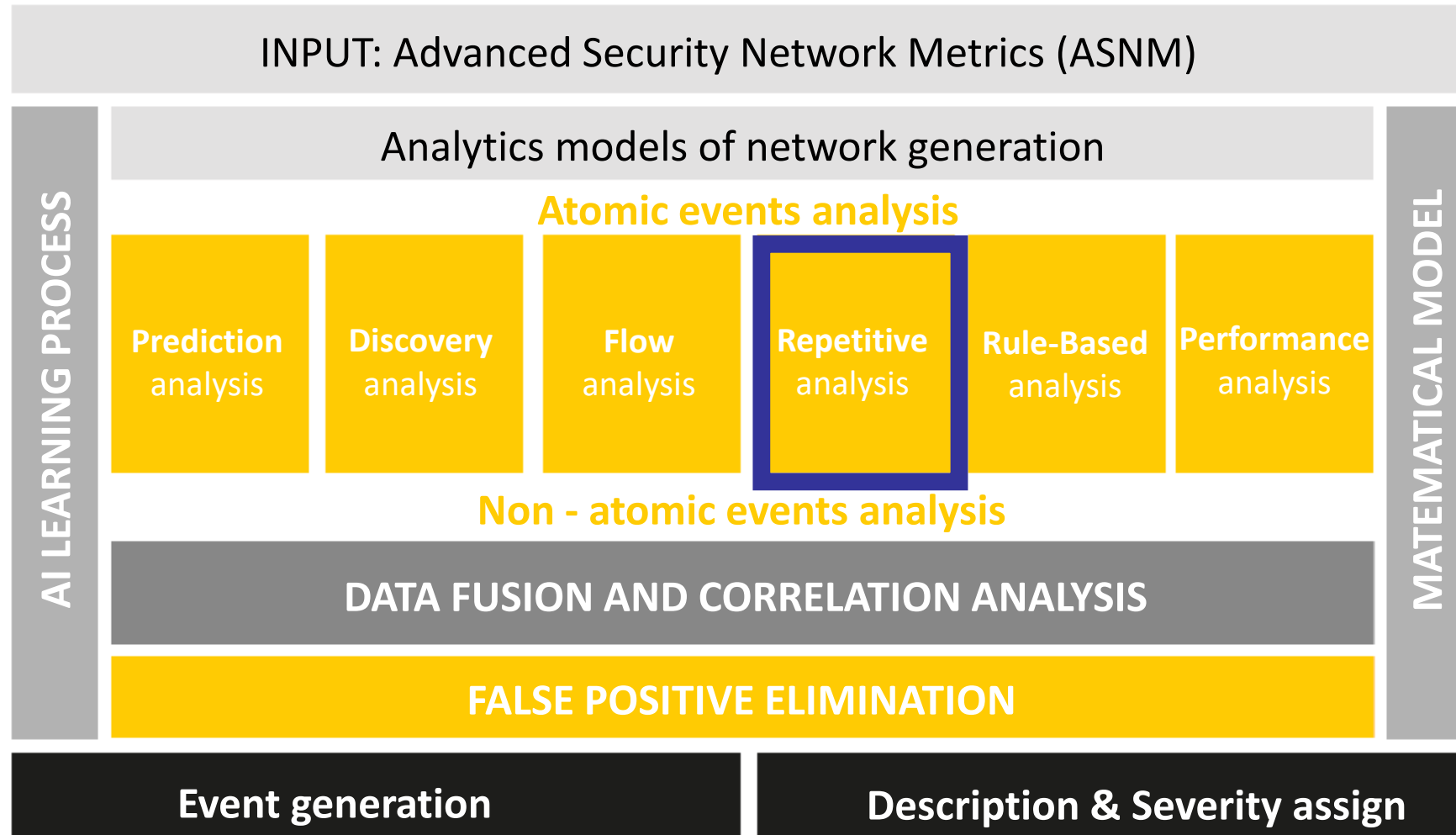
- Port sweep signifying malware reconnaissance, internal audit etc.

8 scan: Internal scan-like behavior

Src IP	Dst IP	Src Sub
 10.0.0.1	 10.0.0.1	 10.0.0.1

Flows		Peers				
	Src Host	Dst Host	Protocol	Src Port	Dst Port	Service
+	 10.0.0.1	 10.0.0.1	TCP (6)	62848	20	
+	 10.0.0.1	 10.0.0.1	TCP (6)	64672	20	
+	 10.0.0.1	 10.0.0.1	TCP (6)	65393	20	
+	 10.0.0.1	 10.0.0.1	TCP (6)	62884	20	
+	 10.0.0.1	 10.0.0.1	TCP (6)	63318	20	
+	 10.0.0.1	 10.0.0.1	TCP (6)	63263	20	
+	 10.0.0.1	 10.0.0.1	TCP (6)	65186	20	
-	 10.0.0.1	 10.0.0.1	TCP (6)	65360	20	

Detection core - repetitiveness



Repetitive analysis

- Recognition of periodical behavior
 - Focused on communication vector used by advanced malware
- Difference between machine and human behavior
 - Machine behavior – predictable
 - Human behavior – unpredictable
- Communication of infected devices with an attacker
 - Malware types like Sality, Conficker, Duqu 2, Hesperbot, ...

PERIODIC COMMUNICATION

- Periodic communication with a supposedly legitimate IP-address. The network metadata were classified as anomalous. The user installed software with unknown malware.

Src Name:
Src MAC:
Dst Name:
Dst MAC:
IP Family:
Src VLAN ID:
Dst VLAN ID:
Interface:
Tunneled:
Start Time:
Duration:
Reported Timestamp:
Output Type:

Request

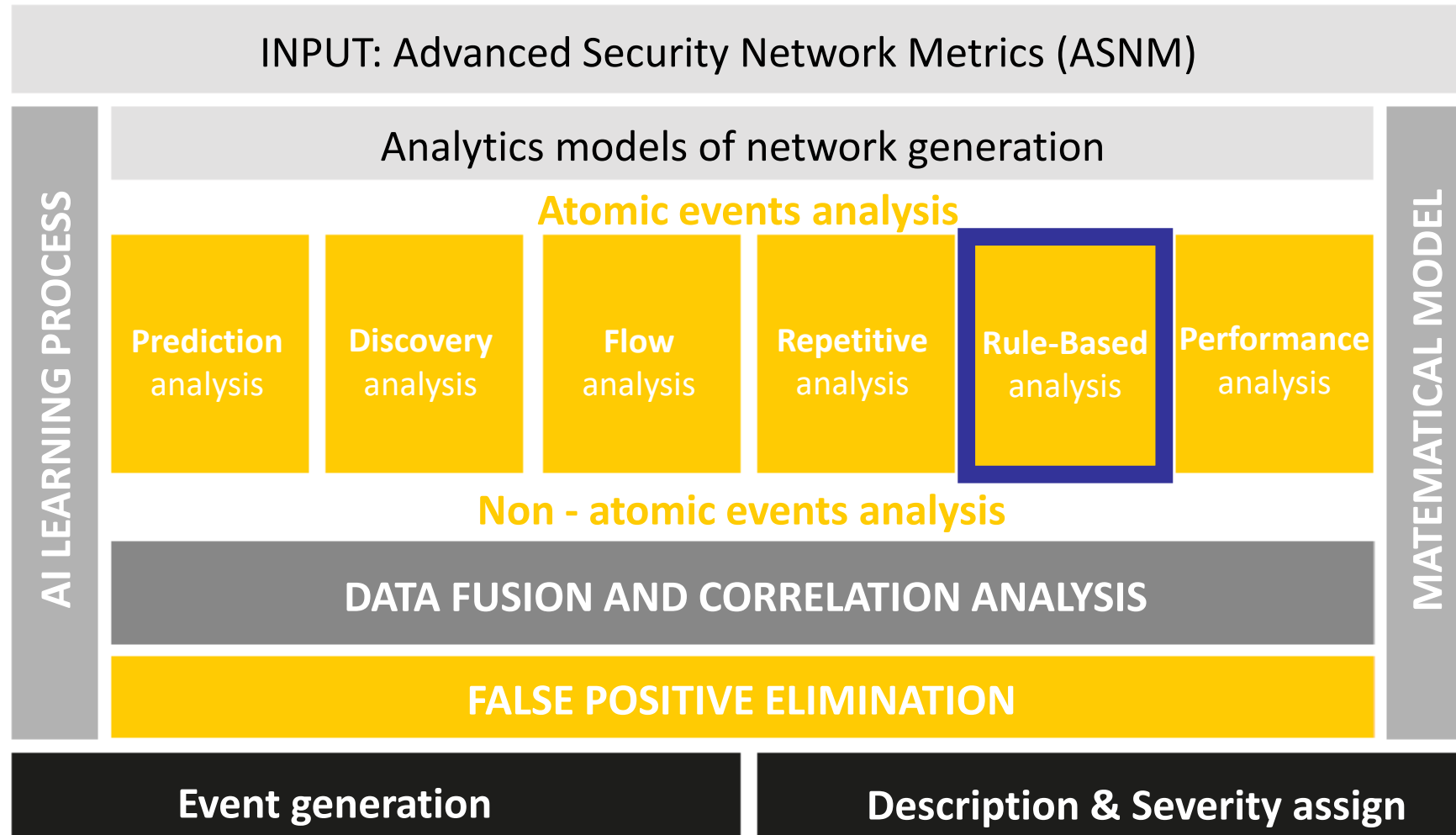
Host:

Uri:

Method: GET

Protocol: HTTP/1.1

Detection core - rules



Rule-based analysis

- User defined rules
 - Limits per devices, services, subnets ...
 - Services permeability
 - NBA algorithms coloring per protocol
- Blacklists
 - About 60.000 to 100.000 blacklisted IPs addresses daily updated
- Signature-based detection
 - Over 40.000 detection signatures of known threats with daily updates
 - Over 40 categories of network behaviors...

*Attack Response
Botcc | Chat
Current Events |
DNS | DOS | Exploit
| File | FTP |
Games | ICMP | IMAP
| Malware
Mobile Malware
Netbios | POP3 |
P2P Policy | RPC |
SCADA | Scan |
Shellcode SMTP |
SNMP | SQL TELNET |
TFTP
TLS-Events | TOR
Trojans | User
Agents | VOIP | Web
Client Web Server |
Worms*

POLICY BREACH

- An exposed network device administration with an unencrypted HTTP service with an illegitimate access attempts from China.

Flows Peers

	Src Host	Dst Host	Protocol	Src Port	Dst Port	Service
-	[Redacted]	[Redacted]	TCP (6)	59842	8888	HTTP

Flow Informations

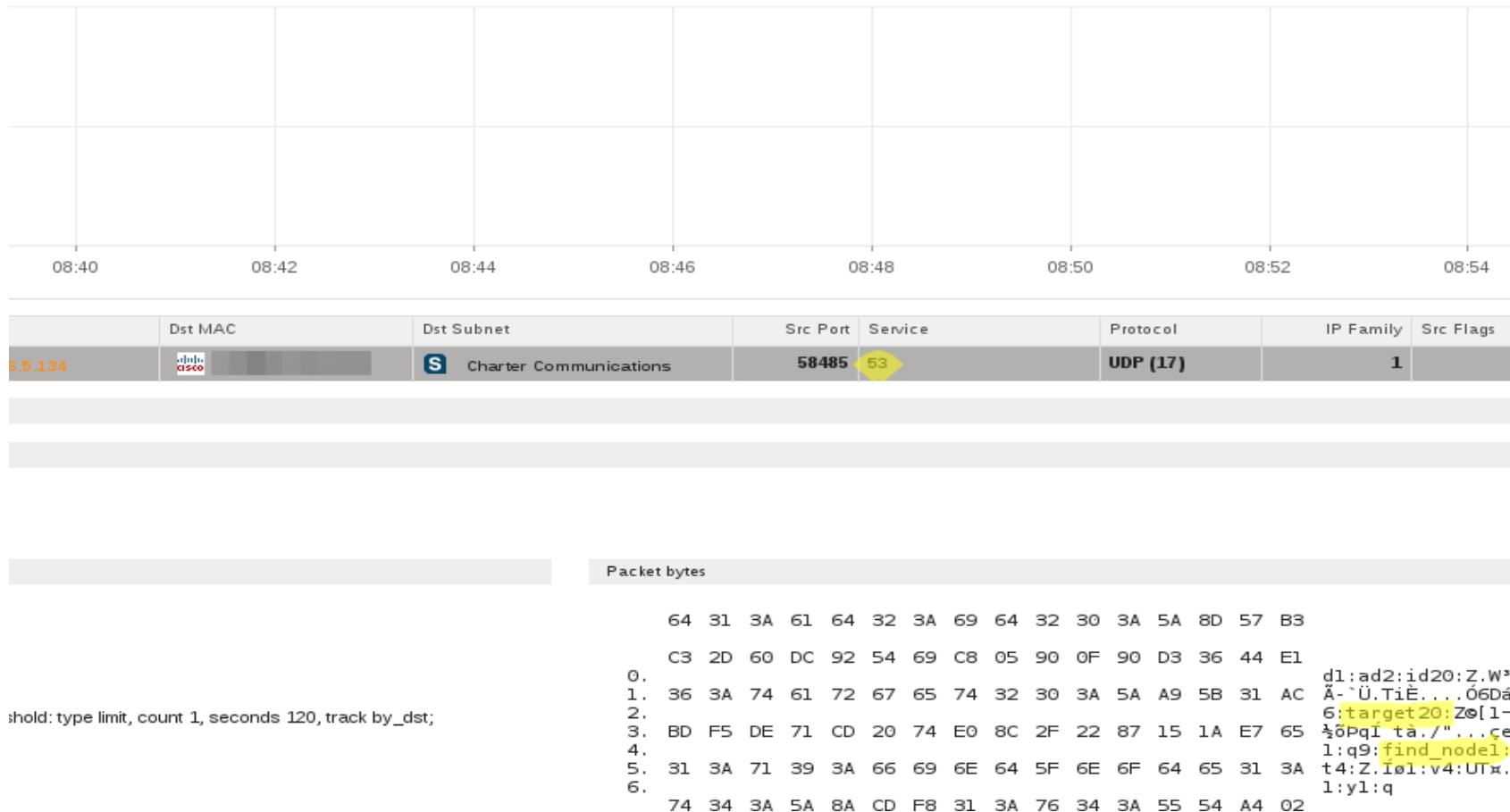
Src Name: [Redacted]
Src MAC: [Redacted]
Dst Name: [Redacted]
Dst MAC: [Redacted]
IP Family: 1
Src VLAN ID: 1
Dst VLAN ID: 1
Interface: em2
Tunneled: 0
Start Time: [Redacted]
Duration: 1s 320ms
Reported Timestamp: [Redacted]
Output Type: 0

Request

Host: [Redacted]
Uri: [Redacted]
User-Agent: Mozilla/3.0 (compatible; Indy Library)
Method: GET
Protocol: HTTP/1.1

DNS TUNNEL

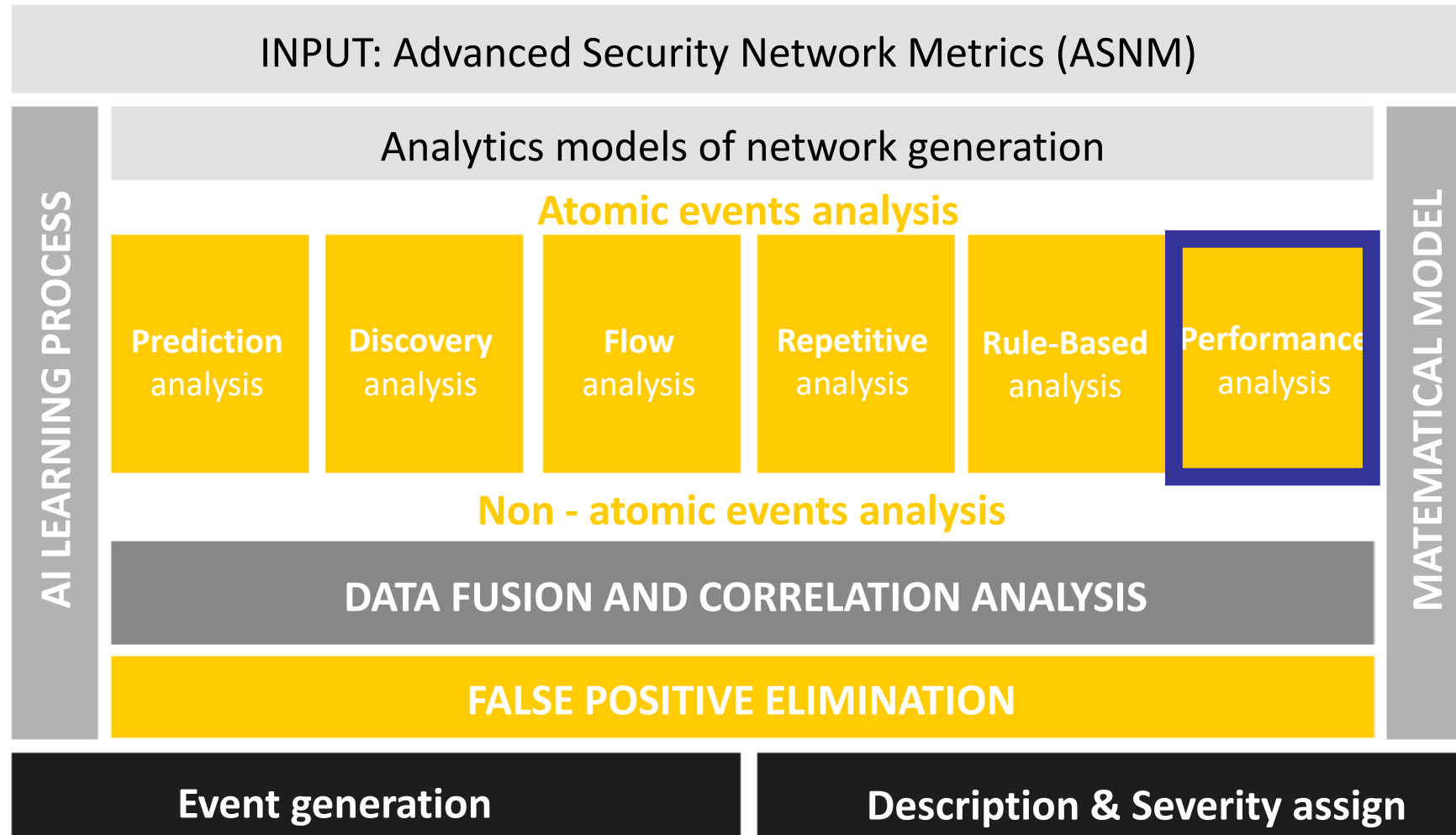
- Communication with a blacklisted IP address on standard port 53 (DNS) from an infected torrent client.



OTHER ADVANCED THREATS

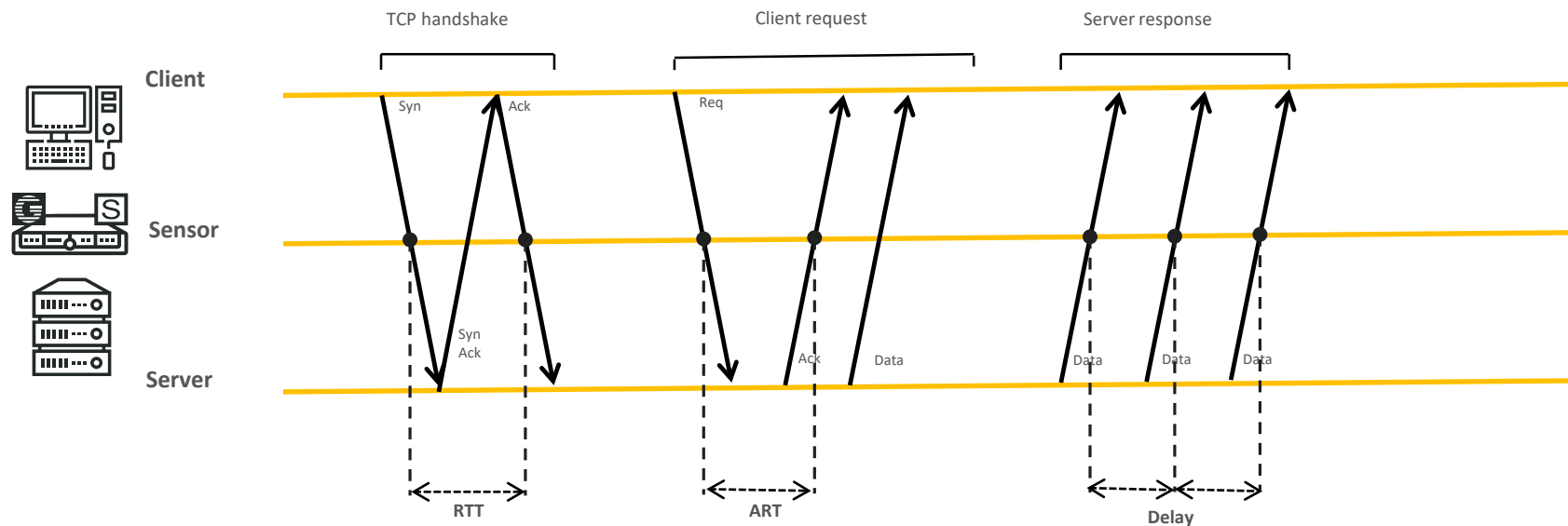
- + Data leaks with DNS, SSH, HTTP(S), etc.
- + Tunneled traffic
- + Protocol anomalies
- + Masquerade attacks
- + Spam detection
- + Malware on mobile and IoT devices
- + Preparation for data theft & exfiltration
- + Automated data harvesting
- + Data theft
- + Phishing attacks

Detection core - performance



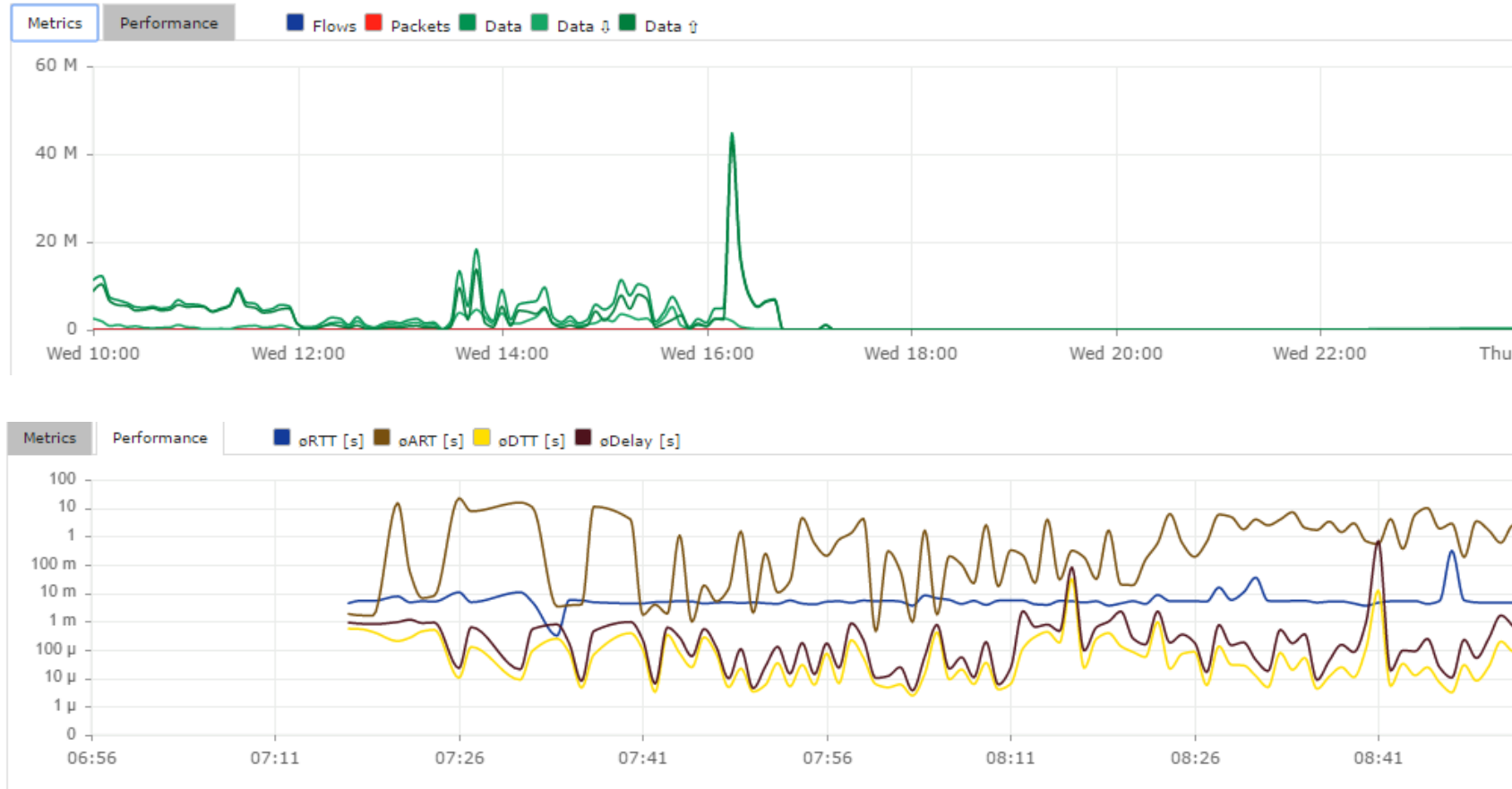
PERFORMANCE ANALYSIS

- Performance of the network and applications (full spectrum of system ports 0 - 65535)
- Recognition of applications
- Monitoring current and average bandwidth, response times, transit times, delay, jitter, ports in use, connection peers, etc.

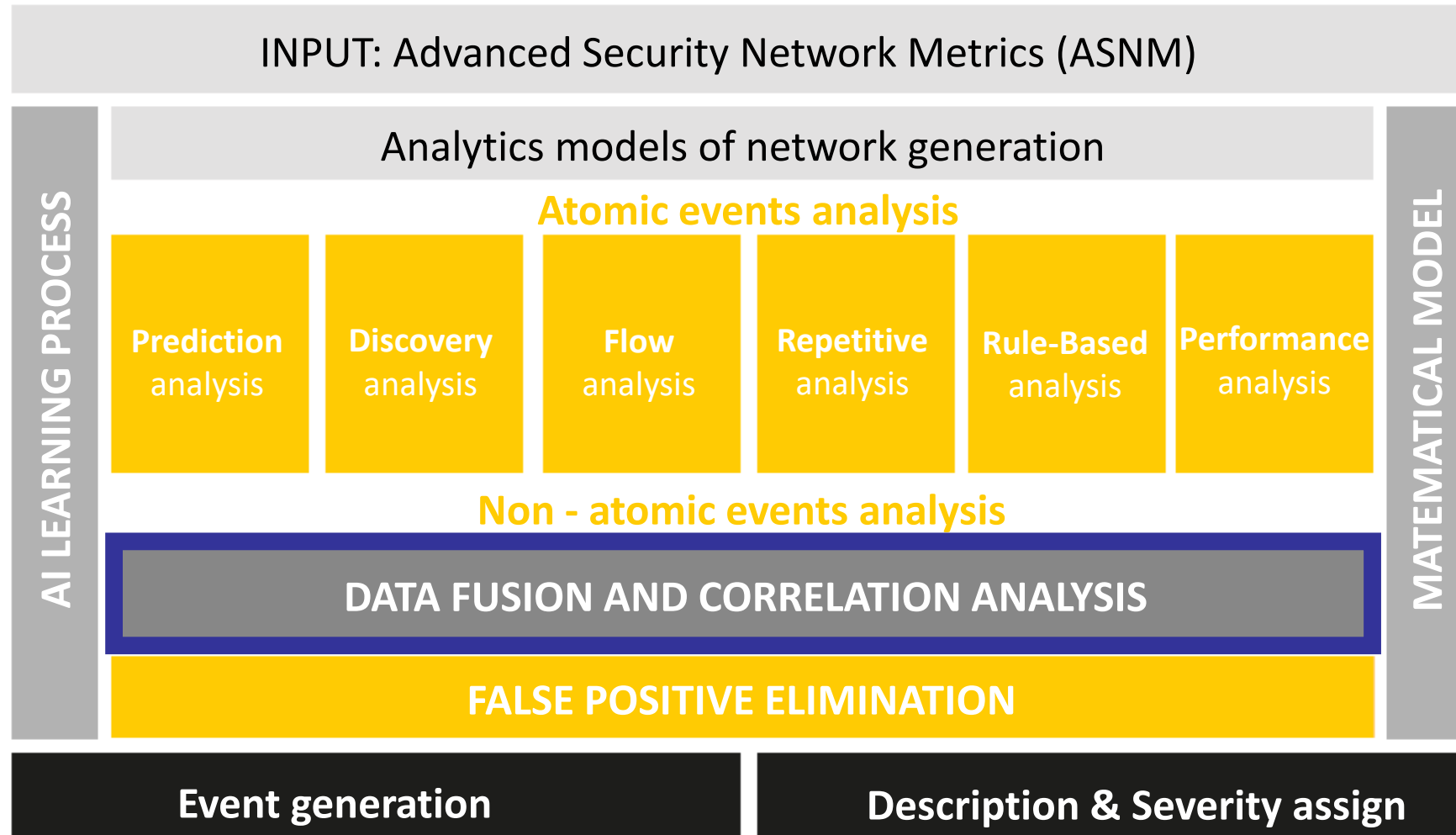


MS-SQL PERFORMANCE ANOMALY

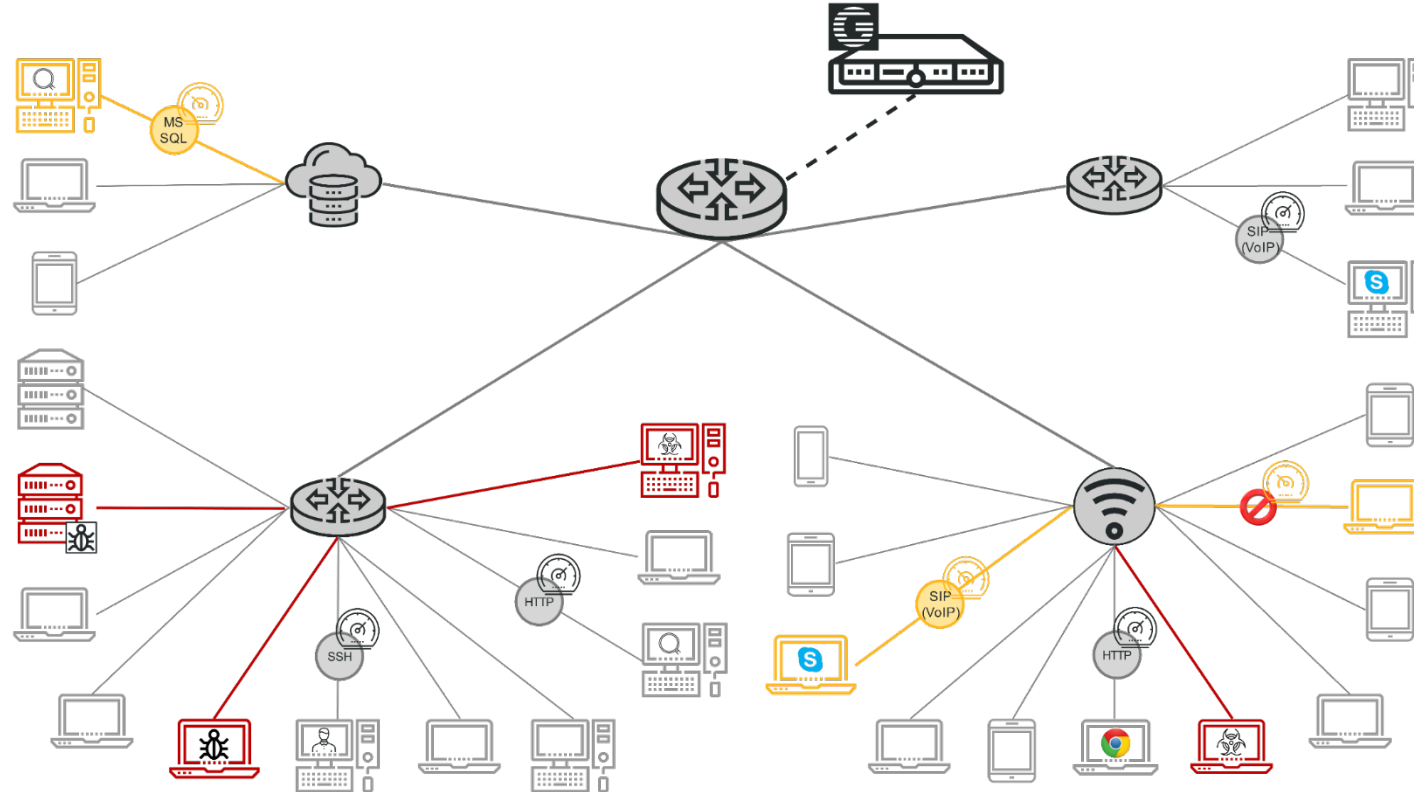
- Anomalous excessive response time at MS-SQL of 30s



Detection core - correlation



DETAILED NETWORK VISIBILITY



NETWORK SEARCH

- Full DB approach
 - No profiling
 - Visualization of any and all data
- Filtering options
 - All application tabs
 - All dashboards
 - Content search
 - Analytics overview
- High granularity of search options

*IP address | Host
name | MAC
address
Subnet | User
name
Domain string
Service location
Traffic
direction
Port | Protocol
Tunneled traffic
VLAN ID | Event
Event category
Incident status*

NETWORK VISIBILITY

- Data decryption (SSL)
 - HTTPS, FTPS, ... ***S
 - Full data inspection
- Conditional data recording
 - PCAP files
- Data encapsulation
 - IP-IP, IPv4-IPv6, IPv6-IPv4, MPLS, Teredo, GRE
 - L7 application protocols parsers

*DNS | HTTP |
HTTPS
TLS | MODBUS |
SMB
SMB2 | SSH | SSL
SMTP | FTP |
DCERPC IRC | VNC
| POP3
Oscar | SIP |
MS-SQL DHCP*

QUICK OVERVIEW

- We have fancy dashboard too. It is user configurable.



USER BEHAVIOR

- Easy filtering of anomalous events by an user. An anomalous periodic communication was followed by anomalous data transfer.

The screenshot displays a network security interface with a table of events and a detailed view of a specific host.

Event	Src Host	Dst Hosts
8 periodic: Repetitive connections (every 30 minutes in 6 hours)	dcrawford (10.22.6.224)	1
7 periodic: Repetitive connections (every 30 minutes in 6 hours)	dcrawford (10.22.6.224)	165
5 outlier: Data at Host	dcrawford (10.22.6.224)	1

Description:
Anomalies caused by excessive amounts of data to a specified IP address.
Check event details, please. In the case this is a legitimate communication, mark the event as False Positive.

Signature details:
Signature ID: 3103
Created: 2015-05-07
Class: Potentially bad traffic
[View Signature Details](#)

Top Src Hosts: dcrawford (10.22.6.224)

Top Src Subnets: Local net (10.22.0.0/16)

Top Users: David Crawford (dcrawford)

Buttons: To filter, False positive, Capture, Show more details

Event	Src Host	Dst Hosts
1 periodic: Repetitive connections (>> 1 every minute in an hour)	dcrawford (10.22.6.224)	1

Host Information:

IP: dcrawford (10.22.6.224)
Comment:
Sensor: demo
MAC: 00:04:96:1d:4e:30
Subnet: Local net (10.22.0.0/16)

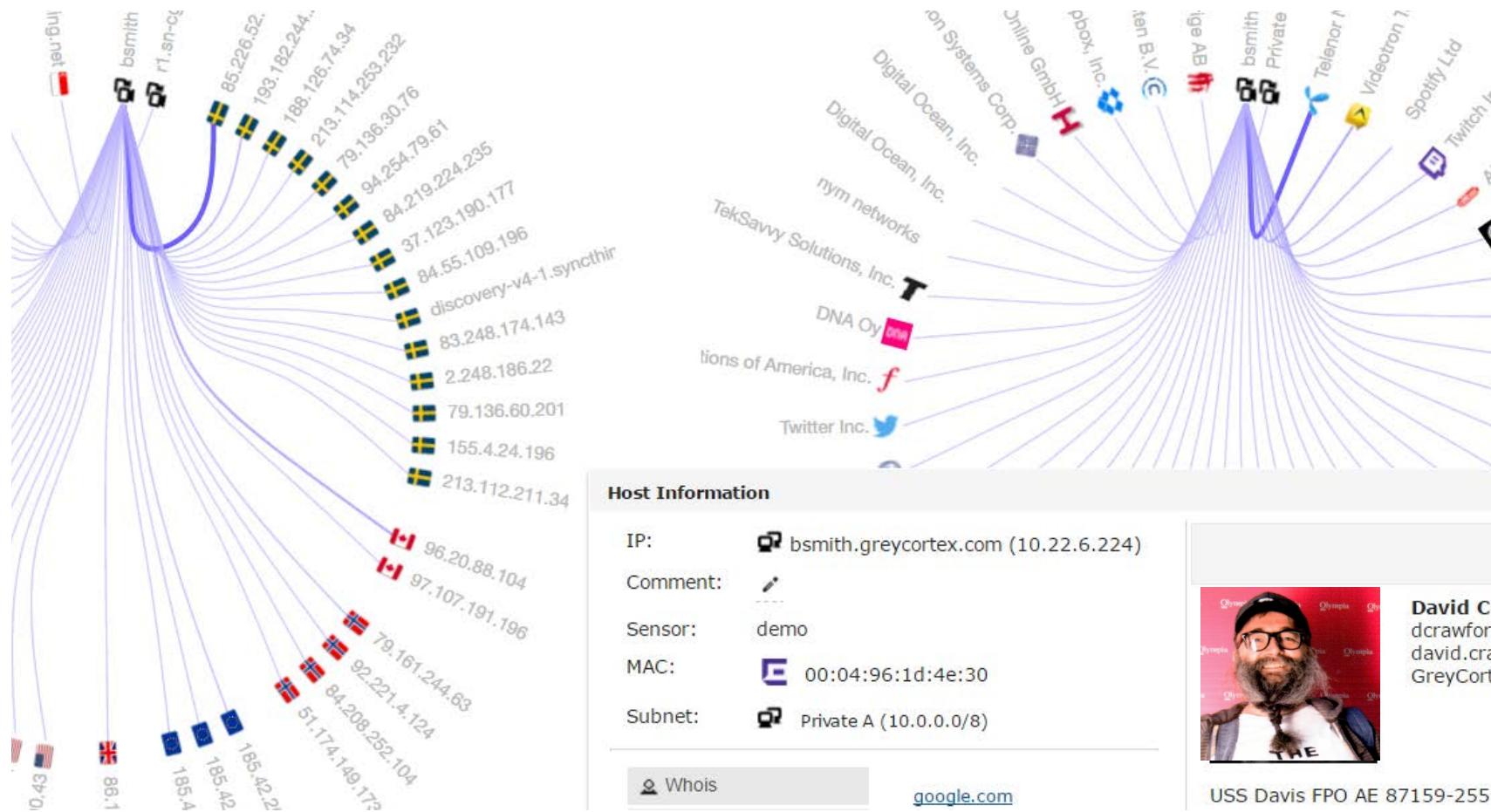
Whois: qoogle.com

User Profile: David Crawford (dcrawford)

Address: USS Davis FPO AE 87159-1

USER COMMUNICATION

- Communication of a user displayed by communication partners and subnetworks.



USER ACCESSED SERVICES

- Services accessed filtered by transferred data together with application and network performance

Service	Port	Service Type	Protocol	Flows	Packets	Data [B]	Data ↓ [B]	Data ↑ [B]
	40197	REMOTE	UDP (17)	264	87.38 k	88.16 M	2.04 M	86.12 M
HTTP	80	REMOTE	TCP (6)	1.54 k	168.57 k	25.93 M	14.06 M	11.87 M
HTTPS	443	REMOTE	TCP (6)	2.77 k	48.65 k	12.14 M	8.48 M	3.66 M
	60415	REMOTE	UDP (17)	51	4.25 k	5.55 M		5.55 M
IMAPS	993	REMOTE	TCP (6)	246	14.8 k	3.67 M	3.07 M	602.54 k
	60180	REMOTE	UDP (17)	1	26.5 k	1.84 M		1.84 M
Panagolin-ident	9021	REMOTE	TCP (6)	9	18.32 k	1.34 M	51.86 k	1.29 M
	11530	REMOTE	UDP (17)	1	19.02 k	1.33 M		1.33 M
	52072	REMOTE	UDP (17)	631	8.56 k	1.27 M		1.27 M
	51413	REMOTE	UDP (17)	1.24 k	8.89 k	1.26 M	107.71 k	1.15 M
	35001	REMOTE	UDP (17)	615	8.23 k	1.2 M		1.2 M
	53410	REMOTE	UDP (17)	349	6.92 k	1.12 M	530.23 k	593.31 k
Savant	3391	REMOTE	UDP (17)	320	6.71 k	1.1 M	529.28 k	572.45 k
	49180	REMOTE	UDP (17)	545	6.95 k	1.02 M		1.02 M
	11382	REMOTE	UDP (17)	538	6.98 k	1.0 M		1.0 M
	24513	REMOTE	UDP (17)	502	6.37 k	927.41 k		927.41 k
	30880	REMOTE	UDP (17)	476	5.81 k	854.32 k		854.32 k
	53298	REMOTE	UDP (17)	224	4.22 k	691.27 k	332.3 k	358.98 k
	30343	REMOTE	UDP (17)	392	4.67 k	681.92 k		681.92 k
	51413	REMOTE	TCP (6)	1.1 k	5.68 k	674.66 k	301.25 k	373.41 k

GREYCORTEX MENDEL

- Is Advanced machine learning, artificial intelligence, and big data combined
- Detects modern threats traditional security technologies miss
- Does Performance monitoring without slowing the network and devices
- Supports enterprise, SME, government, and critical infrastructure users
- In Network Traffic Analysis segment

by **Gartner**

BENEFITS OF MENDEL

- Deep network visibility
 - Full visibility into the internal network
 - Rich metadata describing past behavior
 - Recognition of applications and user identities
 - Full sorting and filtering capabilities
- Compliance
 - Proving compliance with industry standards and government regulation
 - Detection of policy breaches
 - Knowing that security infrastructure works well

Real-time & Detailed

Information up to single transactions of individual users

Automatic anomaly detection

Administrators identify problems before users are affected

Easy root-cause analysis

INCREASED SECURITY!!

Lower risk of serious security incidents

Alliances in Technology

- A part of Konica Minolta product range
 - Performance monitoring and advanced network traffic analysis to become an extension to the Konica Minolta Workplace Hub
- Proud member of Eset Technology Alliance
 - Complementing ESET's existing endpoint security solutions by addressing traffic within the network
 - GREYCORTX MENDEL is available through all ESET partners, worldwide.

Become a customer

- PoC programme
 - We offer a 30 day trial to prove our capabilities
 - Including hardware to try and buy (and keep your data confident)
 - With support of an analyst
 - Ask for more at info@greycortex.com
- Our partners
 - We partner with the best partners from around the world to provide excellent services and to comply with local regulations
 - Ask for contact at info@greycortex.com

Ďakujeme za pozornosť

- www.greycortex.com – whitepapers, use cases, and more
- info@greycortex.com – general inquiries
- vladimir.sedlacek@greycortex.com – technical questions
- www.youtube.com/greycortex – watch our videos and Tales from Malware Labs

The logo for GREYCORTEX, featuring the word "GREY" in a stylized font with horizontal lines through the letters, followed by "CORTEX" in a bold, sans-serif font.The logo for eFOCUS, featuring a stylized orange "e" followed by the word "FOCUS" in a bold, sans-serif font.