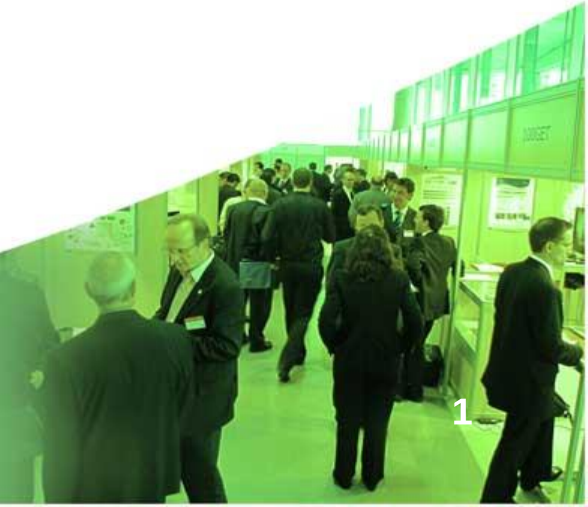
Celtic-Plus Proposers Day
21st February 2017, Berlin

New Generation Network Security System (ENTRUST)

Dr. Barış Bulut, Enforma Bilişim A.Ş.
baris@enforma-tr.com



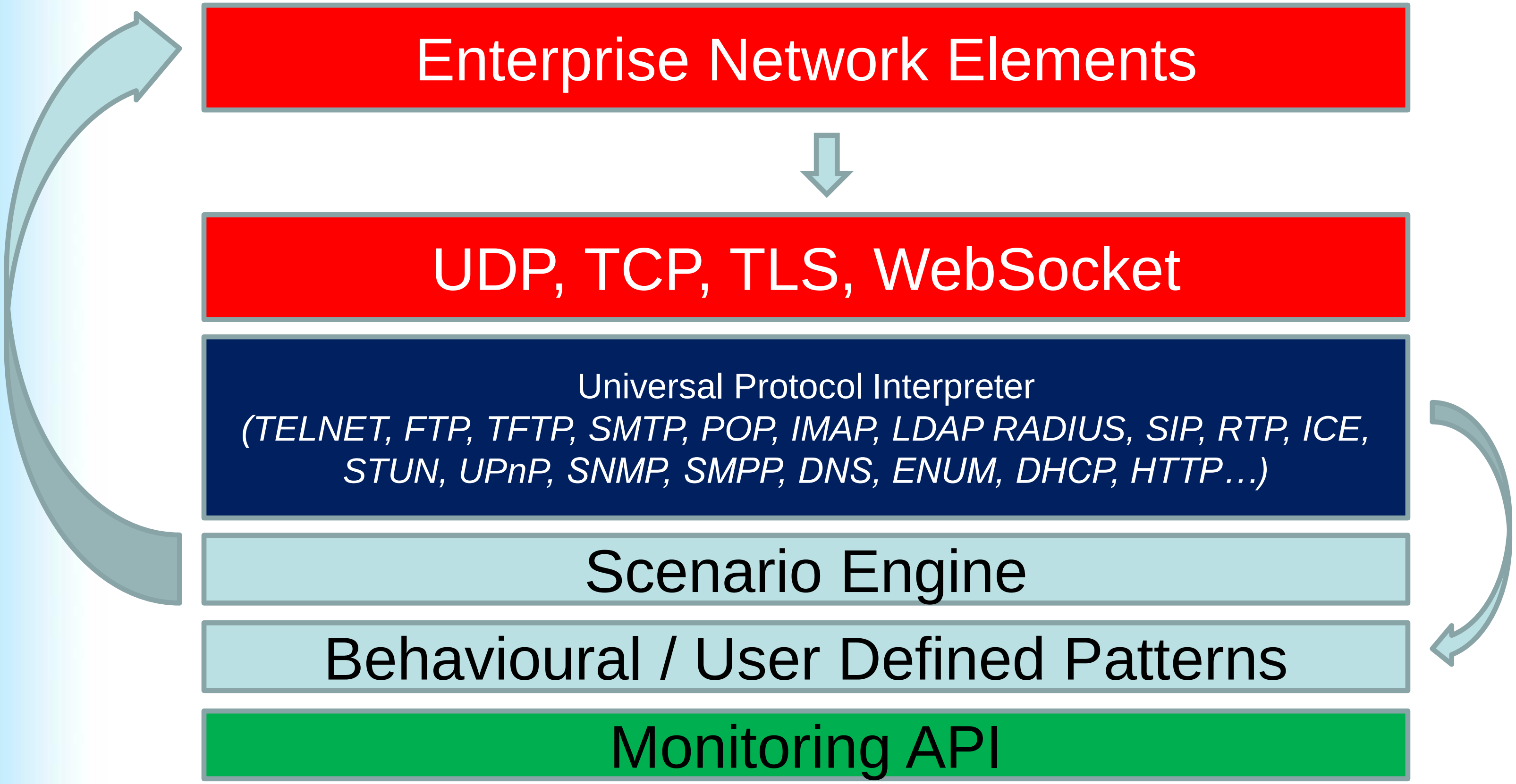
What we do

- **Our ongoing work is based around *ICT, telecommunications, data processing, telecoms regulations, product management & go-to-market, research and development consultancy, state funding and academia.***
- We perform **data analysis** in various areas such as telecommunications, opinion polling and vehicle tracking, all of which lead to better business intelligence, higher customer retention, lower customer churn.
- We develop **telecommunications systems software** used within a number of nodes of such as RADIUS, telecommunications billing, SIP proxy, WebRTC server, telecomunications middleware software.
- We have been successfully receiving R&D grants at national level.
- We are in the look-out for **partners we can work with in a cooperative and conducive successful collaboration**.

New generation network security system

- Network security evolved from access lists to firewalls to intrusion detection systems (IDS)
- Disadvantages:
  - Threat assumed to be from outside, rather than inside.
    - Ineffective against a Trojan horse or an infected user from inside
  - SSL-encrypted malicious activity raises no direct alarm in IDS
  - Also, known backdoors in leading non-EU manufacturers
- Need to:
  - Establish baseline for traffic flow (both the load and to/from)
    - Central or distributed probes
    - Expert knowledge also accommodated
  - Handle traffic in SSL-encrypted tunnel
  - Detect anomaly in the pattern in real time
  - Conform with EU information security standards

Basic schematics



Enterprise Network Elements

UDP, TCP, TLS, WebSocket

Universal Protocol Interpreter
(TELNET, FTP, TFTP, SMTP, POP, IMAP, LDAP RADIUS, SIP, RTP, ICE, STUN, UPnP, SNMP, SMPP, DNS, ENUM, DHCP, HTTP…)

Scenario Engine

Behavioural / User Defined Patterns

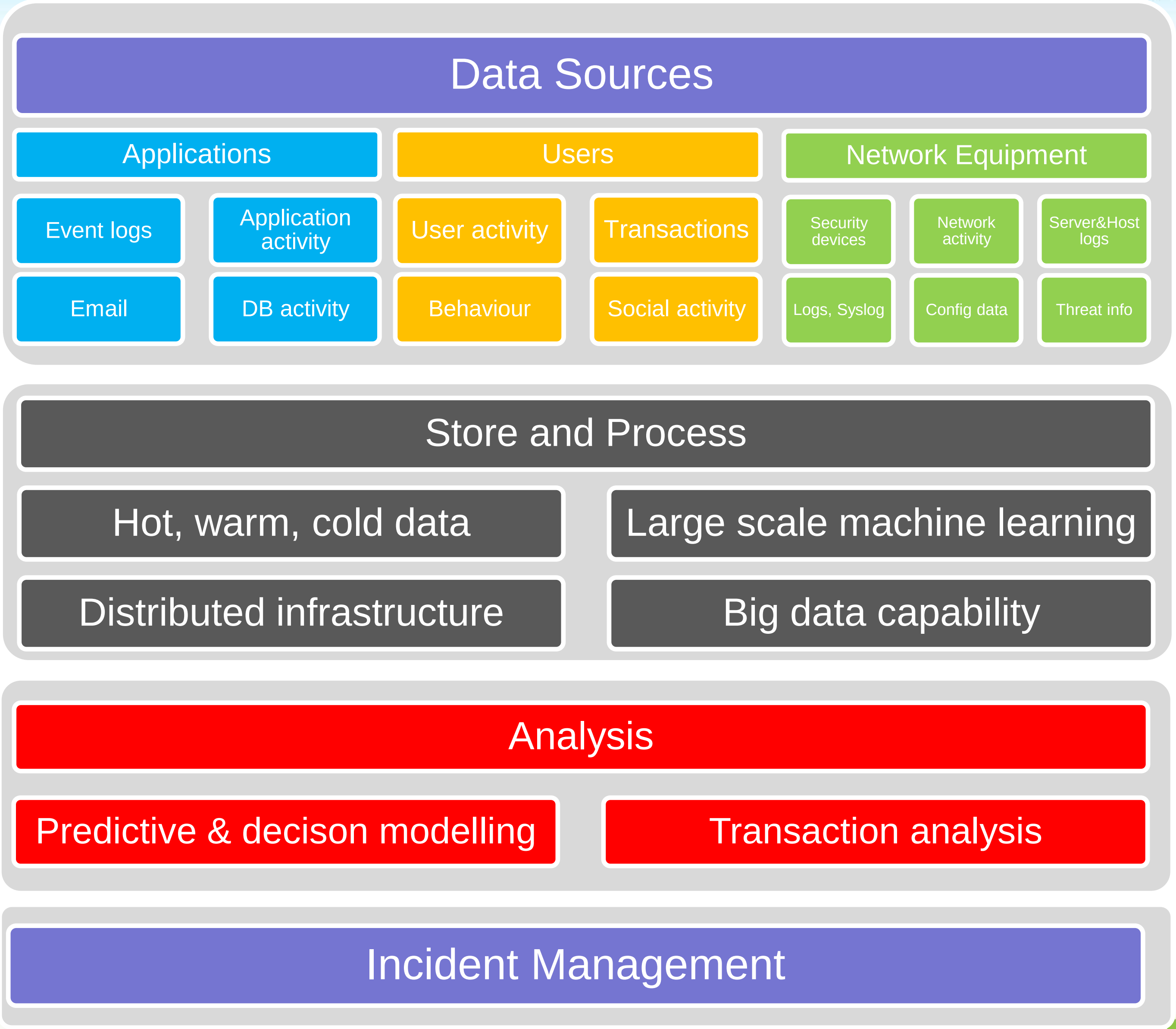
Monitoring API

Network Activity Abstraction Active Policy Enforcer (NACAPE) Functional Blocks

Evolution

Source considered	Stateless firewall: Packet Filters	Stateful firewall	Application Layer Firewall	Application Layer Firewall with DPI	Next Gen firewall, IDS
Layer 7: The application layer			+	+	+
Layer 4: The transport layer		+	+	+	+
Layers 3 & 2: The network & data link layers	+	+	+	+	+
Packet content				+	
Layer 3, 4, 7 Logs, incl. syslogs, event logs					+

Standardisation



Data Sources

Applications

- Event logs
- Application activity
- Email
- DB activity

Users

- User activity
- Transactions
- Behaviour
- Social activity

Network Equipment

- Security devices
- Network activity
- Server&Host logs
- Logs, Syslog
- Config data
- Threat info

Store and Process

- Hot, warm, cold data
- Large scale machine learning
- Distributed infrastructure
- Big data capability

Analysis

- Predictive & decison modelling
- Transaction analysis

Incident Management

Detection based on analysis of log and traffic data.

No common log format across the industry

Key selling points

- Proposed solution provides:
  - An evolved security system that can address ‘evolved risks’ currently undetectable by the IDS systems
    - Machine learning ideas incorporated
    - Kills threats from outside and inside
    - Detects extended list of network activities such as an abnormally high number of MX lookup local email addresses, or DDOS
  - A common log format for use in network equipment
  - A European security system with zero backdoors
    - Higher security of systems and personal information
  - Worldwide network security and information security markets nearing $10b and $100b in size, respectively
    - With 2-digit year-on-year growth
    - Governments, datacentres, corporates, SMEs

Partners & expertise

- **Partners currently interested**
  - Enforma
  - Grid Telekom
  - University of Amsterdam

- **Missing partners / expertise**
  - Vendor
  - Network traffic analysis experience,
  - Testing capability or a friendly customer status

Contact info

If interested please contact:

Dr. Barış Bulut, Enforma Bilişim A.Ş.
baris@enforma-tr.com
+90 212 932 7950
www.enforma-tr.com