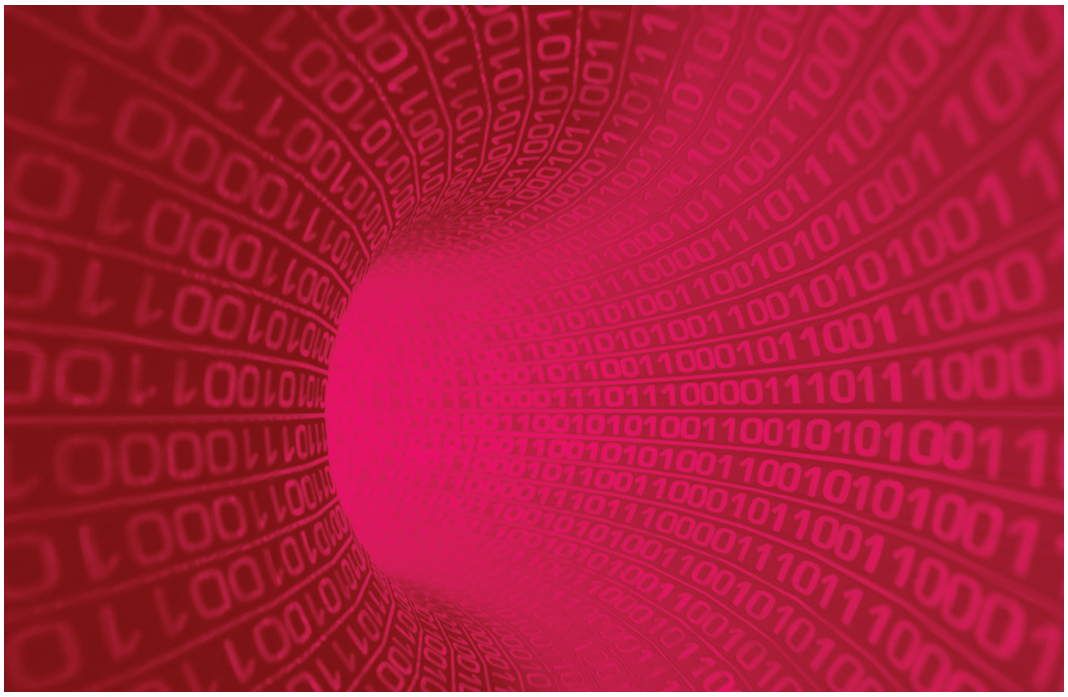
Ambience

Monitoring and detection of security and business events in the network traffic



Passus Ambience is a network based, real time solution designed for network data streams analyze, irrespective of data type and source or communication protocols. Modification, filtration and aggregation tools give a possibility to process large amounts of data and transform them into valuable security or business events described by metadata. The events can be complited with external information and delivered in real time to both business intelligence and security systems. All metadata can be also recorded to a build-in collector for further forensic analyses.

Passus Ambience is the flexible solution that can parse any type of input data or protocols including industrial, medical or individually tailored protocols or standards.

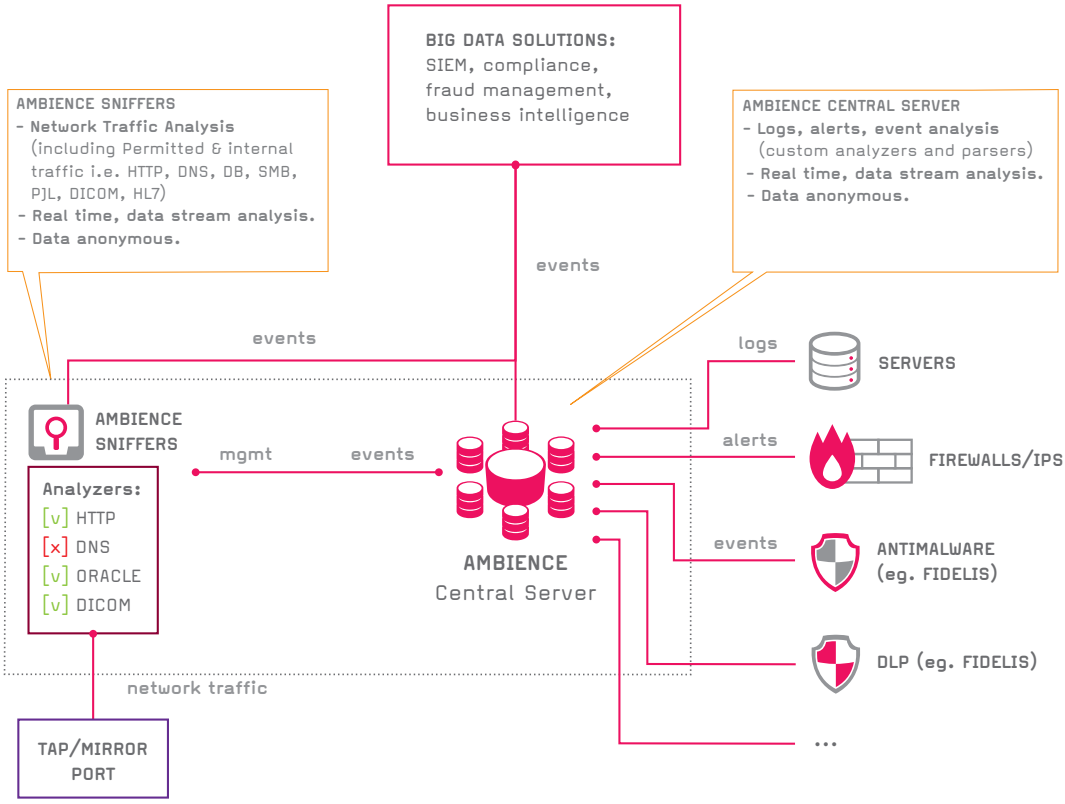
Key features of the solution

- Captures network traffic, logs, alerts and any events generated by 3rd part solutions.
- Collects either single event or a sequence of events related to IP Address, MAC, User,
- Delivers in real time user-defined events to any analytic system (SIEM, BI, AntyFraud, GRC etc.) in the tailored /suitable formats.
- Build-in analyzers i.e. HTTP, SMB, DNS, Kerberos, SSL and data base traffic Oracle, MS SQL).
- Out of the path solution, both agents and application modification are not required.
- Granular permissions system and anonymization allow to protect sensitive data.

Passus SA | ul. Bzowa 21, 02-708 Warsaw | phone (+48) 695 444 794 | e-mail: passus@passus.com.pl | www.passus.com.pl

PASSUS AMBIENCE

Passus Ambience detects a number of events and behaviors often overlooked by signature or behavior based solutions focused on perimeter security. Extracted, valuable data written as events contained metadata {key:value} allow to analyze both raw traffic data and alerts generated by 3rd part solutions. They can be used to find potential harmless incident in the activities which have not been assinged as treats or abuses. Moreover, metadata utilization enables to bring the correct order into a massive set of various network traffic data.



AREAS OF USE

Forensic, fraud management, IT security

Passus Ambience can detect and document anomalies and their circumstances to enrich process of indication breaches or frauds.

- Monitoring access to sensitive data to detect increase in the number of database queries, reading or copying files, printouts etc.
- Descrying nonstandard activities during log-in on to the network or web applications i.e.:
  - ✓ Attempts to guess login /password;
  - ✓ Untypical authentications to the network like strange location of employee who is on the sick leave, unauthorized devices;
  - ✓ One and the same login is used on many devices at the same time.
- Investigating of suspected activities on files, for example copying whole directories by employees during the termination period.
- Using of administrative privileges to access confidential data, such as the contents of employees electronic mail, healthcare electronic data (DICOM, HL7).
- A sudden increase in the number of database queries involving access to sensitive information within a specified time or by a given person.
- Detecting the unauthorized tunneled communication – transferring data using modified URL, diagnostic packages, DNS or HTTP services.
- Using of external forms and web applications to transfer data outside the organization.

Governance, risk, compliance and business continuity

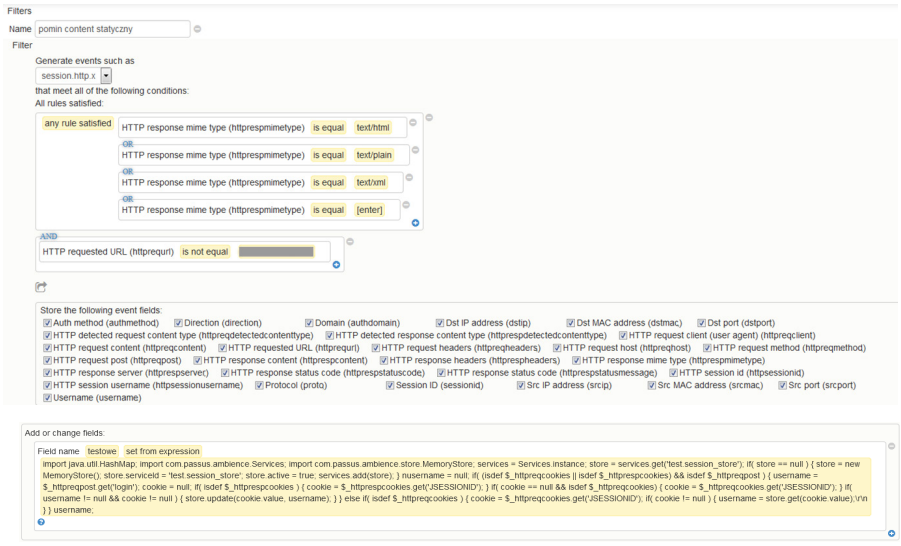
Passus Ambience allows to verify whether a company is following the security rules and regulations and gives visibility into the effectiveness of defense systems.

- Detection of new hosts, services and applications, including mobile devices to identify those which are not in accordance with compliance.
- Identifying topological changes like host addressing, new gates or DHCP servers, proxy servers.
- Verification of whether the traffic is encrypted according to the company standards.
- Detection of weak authentication methods, incorrect protected protocols or wrong configured services.
- Detection of unlocked accounts of ex-employees due to errors in procedures or malfunction failure.
- Notify a large number of very long or very short VoIP connection as well as connections to suspected numbers.

Business inteligence & web analytics

Passus Ambience enable to convert network traffic, logs and alerts into business events described by user defined qualitative and quantitative metadata. Build-in analyzers (i.e. HTTP, databases traffic, DNS, VoIP, Kerberos or FTP) deliver real time intelligence for analytic systems including big data based solutions.

- Individual queries or responses can be combined into a single business event that contains valuable information: a kind of activity, values of form fields as well as such information as “who” and “when” sent the information using standard forms or other formats like JSON, XML.
- Sequential activities can be enriched by information from previous steps and additional information from 3rd part systems LDAP, AD, HR and CRM systems etc.
- Extraction only important events or conversion of sequence of defined events into single event allows to reduce data transfer to analytic systems and decrease cost of their licenses.
- Access requirements, number of opened downloaded or modified documents, files or folders give valuable information about resources’ utilization.
- The amount of connection attempts, calls on hold, forward, call recording etc. empower knowledge about service level and employees or infrastructure efficiency.



Defining conditions that certain fields must meet, that an event in general would be reported by the analyzer. In this case, two filters established: delivering only events, where answer was a particular type: html, plain, xml, or empty and called address was different than / domain/testr5.html. Additional filters can be defined at the stage of creating the rules

Specifying the fields that will describe the event through their selection from a predefined list.

Defining new custom fields by using the built-in scripting language, in this case MVEL.

Fig. 2 Filters at the input of the analyzer

MAIN FEATURES

Data processing and transformation

Passus Ambience can process and transform data captured from network traffic. It enables to pars data, filter aggregate and combine specific information as well as anonymize or encrypt sensitive data.

- The ability to filter traffic data by type (i.e. text, pictures, DICOM and SCADA formats) keywords, source addresses, destination IPs and any other custom field.
- Built-in graphical designer equipped with logical operators helps to build queries which filter and extrude valuable events or sequence of events.
- Any value of metadata field can be extracted, analyzed and modified, therefore they can be send to another event as a new value or dynamically changed logical parameter which can be used as trigger.
- Sensitive data can be anonymized or encrypted on event generation layer in different ways:
  - ✓ Sign substitution – changes are irreversible, data can't be analyze;
  - ✓ Symmetric encryption – adjustments are reversible, data can be analyzed;
  - ✓ Asymmetric encryption - changes are irreversible but data can be analyzed;
- Different methods of presentation of hiding information (changing all the characters to an asterisk, all characters into exactly 5 asterisks, leaving last 4 digits, etc.);
- Built-in algorithms to detect common types of sensitive files, contented metadata such as credit card numbers, social security number, identity card or medical data stored in DICOM format.

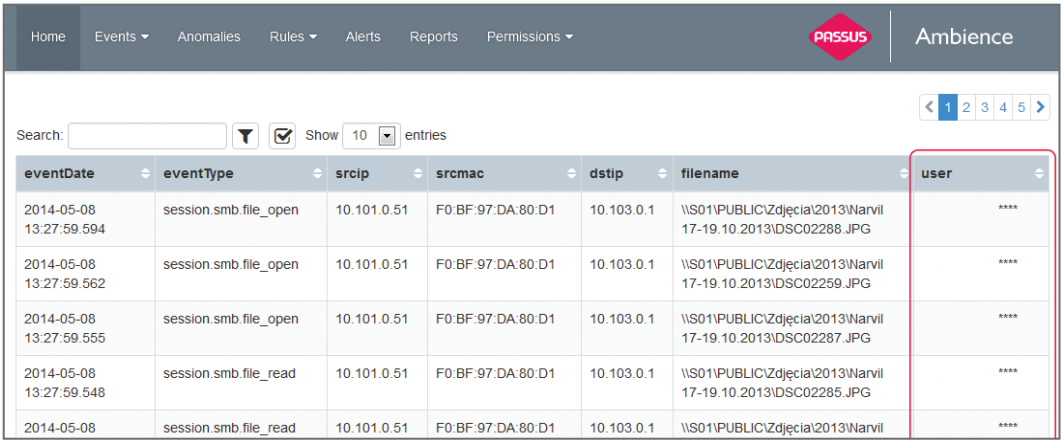
Single event basing on the sequence of events

- Requests and responses as a part of the common protocols can be joined and machined with advanced filters and aggregation functions.
- Possibility of defining event sequences in various protocols and connecting them into another single event using different parameters (MAC address, IP, login etc.).
- Defining the intervals at which the event should or should not take place.
- Access to detailed information bounded with a given sequence i.e. possibility to analyze detailed information concerning all events in the sequence.

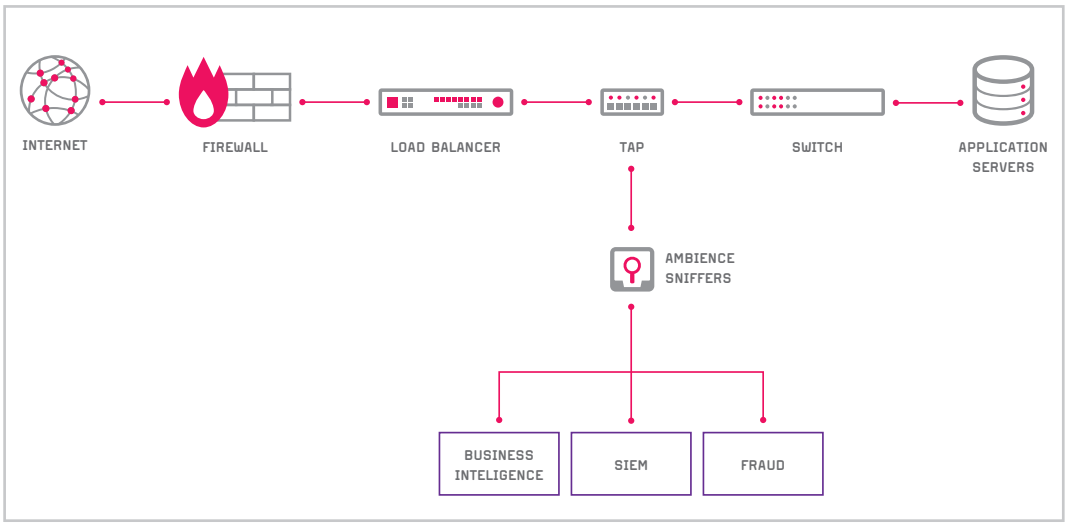
Enriching information using external data sources

Additional information from many sources can be modified or added directly to the event metadata, generated in the system.

- Geolocation;
- Active Directory;
- DNS;
- CSV files;
- Data base.



Anonymization of data can be used to hide user logins and any other sensitive information.



Passus Ambience as a HTTP Sniffer in Bank

USE CASES

Financial sector – business intelligence, antifraud

Passus Ambience provides real time web traffic monitoring focusing on both business events and fraud incidents. Among of others Ambience:

- Collects information concerning successful and failed log-ins, bank transfers or completing the personal data change form;
- Delivers details of the given operation. For example, in the case of remittances there are a kind of transfer, an authentication method, account numbers, a name and the state of a payee, amount, balance etc.;
- Real time monitoring the user behaviors like a session duration, pageviews, content drilldown, duration of the chosen activity for example a bank transfer;
- A geographical location of the user and kind of used device.

Healthcare sector - compliance

Passus Ambience provides real time internal traffic monitoring towards the needs of the compliance analysis. Among of others Ambience:

- Discovers network traffic and verifying whether there is a proper type of traffic in the monitored zones;
- Discovers DICOM files in the internal traffic (SMB) and external traffic (SMTP, FTP, HTTP) to support a compliance monitoring;
- Records and analyze healthcare databases queries;
- Monitor network activities of medical devices to give answers on such question as “who” “when”, “how” used medical equipment;
- Printout monitoring.

Telecommunication sector – IT security

Identifies unusual or dangerous behavior of users and devices. Detects abuse even in situations where users act within their normal access privileges. Among of others Ambience:

- Perpetual inventory of storage resources in the network and monitoring any activities, in particular file deletion, modification or transfer;
- Combines SMB protocols users with domain username;
- Records and analyze CRM databases queries;
- Monitors VoIP calls and compares outgoing connections to the black list;
- Monitors employees internet activities, file transfers, discovers risk of tunneling;

PASSUS AMBIENCE – THE EXAMPLE OF IMPLEMENTATION

Passus Ambience is operated from a central console, which allows to configure any probes located across infrastructure, define rules and policies, create of new search patterns and customize way of data presentation.

The basis of the system is a complex event processing. Security Anomaly Detector uses a probe (1U appliance or virtual machine - standard server architecture) placed inside the network, which collect data and send them to a central server. The central server is used for aggregation, analysis and presentation of collected data. The probes works passive. Probe is listening for redirected/mirrored traffic from the TAP devices or switch ports. All traffic passing through the switch can be sent to the probe.

On each probe works from several to a dozen specialized analyzers, which are processing data flow coming to them and log spotted events preprocessing them.

The central server is equipped with redundant disks arrays and systems for backup. Query on/receive from all configured sensors collected incremental logs and performs next layer of analysis on them (for example, to detect serious abuses, network worms, etc.) and then store information to highly efficient Splunk database engine.

Algorithms used in the analysis mostly do not rely on predefined signatures. Analysis is based on behavior patterns and changes in them. Thanks to that we get successful detections of P2P connections regardless of their type, hidden sessions (covert channels) of SSH or other cryptographic traffic in legit data flow etc.

Events can be processed further on central servers, resulting in the ability to rise alerts from network anomalies based on combination of several different events coming one after another or any other fully customizable sequence of information.