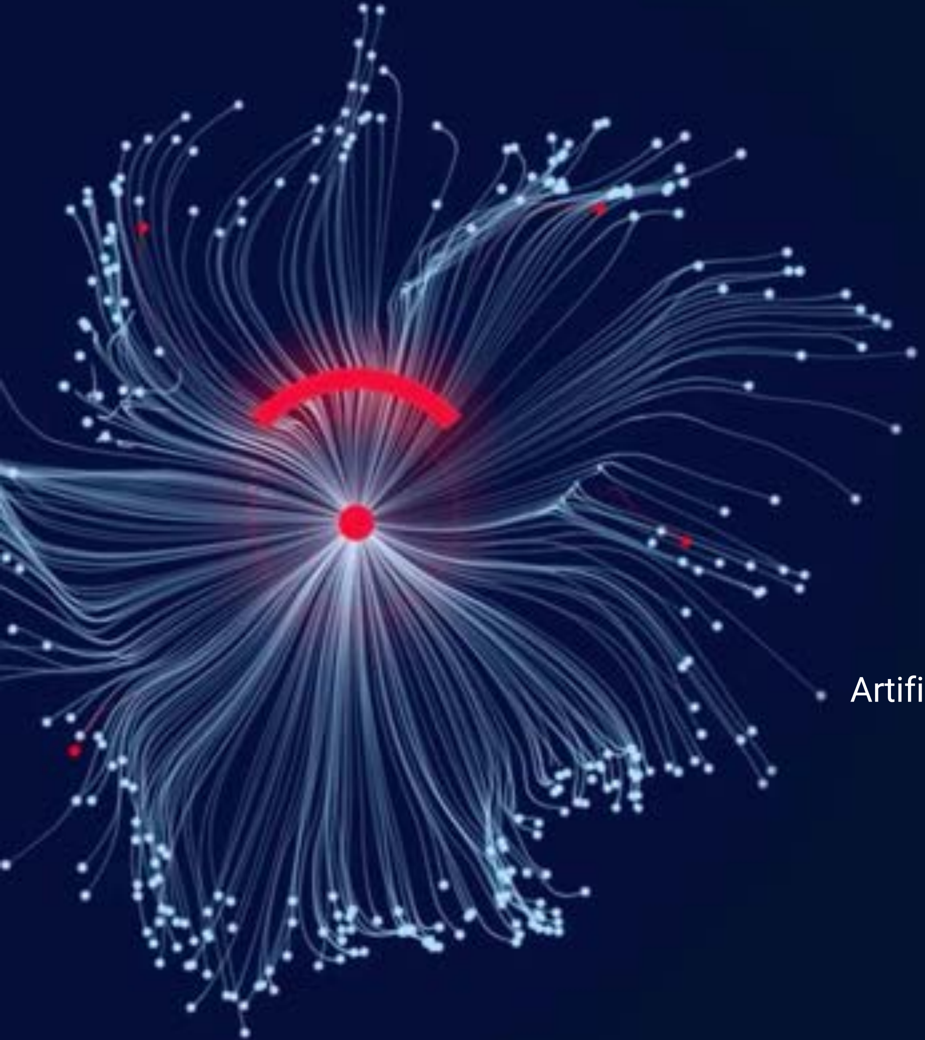


aramis®

by aizoOn

Know, protect, empower
Managed detection and response

React sooner, recognize, not just identify

Artificial and human intelligence, competence and passion for the early detection of advanced cyber threats

aramis by aizoOn | 2024

aramis overview

Artificial Intelligence applied to the field of Cyber Security **[2013]**

Independent platform totally financed by **aizoOn**

Algorithms, architecture, functionalities and dashboards are **proprietary**

A collaborative platform, designed to be integrated into complex scenarios

Continuous research and comparison with the scientific community**: patent applications and scientific papers**

Integration of multiple sources of cyber and intelligence

Traffic acquisition and processing **in the cloud, on-premises, and in virtual machines**

Modular and scalable architecture for networks of any size.

Customizable and extendable detection capabilities.

Data fusion
For automatic and adaptive learning with unified visibility across different attack vectors

aramis
by aizoOn

Patent

Method of detecting anomalies in SSL and/or TLS communications, respective device and computer-program product

Method for detecting anomalies in a monitored network regarding encrypted communications which use either SSL or TLS protocol. The proposed method analyzes SSL/TLS handshakes between network clients and external servers. Then, it combines machine learning techniques with the usage of parametrized cost functions to, respectively, classify suspicious communications and attribute them an anomaly score.

patent: IT102021000015782

Patent application countries:
IT, EU, US, CA, AU

Method of detecting systematic communications in a communication network, respective device and computer-program product

Method for detecting systematic communications in a monitored network that could be indicators of a malware infection. The method analyzes specific network protocols and, for each observed packet, extracts packet metadata to measure the systematicity of transmissions between a source and a destination machine, using incremental variance to guarantee the best performance.

patent: IT102021000011267

Patent application countries:
IT, EU, US, CA, AU

Method of detecting anomalies in communications, respective device and computer-program product

Method of detecting anomalies in unencrypted communications of a monitored network, through the analysis of communication metadata. Metadata characterize each network devises and helps building Bayesian network models able to detect possible behavioral anomalies.

Patent pending: IT102021000033203

Countries:
IT, EU, US, CA, AU

Method of detecting phishing attacks, respective device and computer-program product

Method of detecting phishing attacks through the analysis of screenshots of suspicious URLs.
The approach relies on recognizing logos belonging to reputable brands, with the aim of identifying the attempts of an attacker to spoof a website.

Patent pending: IT102023000019872

Countries:
IT,EU

Scientific Papers 2017-2023

A selection

ICCST 2017 (Spain) - Real-time behavioral DGA detection through machine learning

In this paper, we report on an effective DGA-detection algorithm based on network monitoring analysis. The proposed method first detects bots looking for the C&C and, then, analyzes resolved DNS requests in the same time interval. The linguistic and semantic features of the collected unresolved and resolved domains are then extracted in order to cluster them and identify specific bots. Finally, clusters are analyzed in order to reduce false positives.

ISC 2018 (UK) - Fast Flux Service Network Detection via Data Mining on Passive DNS Traffic

In this paper, we report on an effective fast flux detection algorithm based on the passive analysis of the DNS traffic of a corporate network. The proposed method is based on the near-real-time identification of different metrics that measure a wide range of fast flux key features; the metrics are combined via a simple but effective mathematical and data mining approach.

MALCON 2019 (USA) - DNS Covert Channel Detection via Behavioral Analysis: a Machine Learning Approach

This paper proposes an effective covert channel detection method, based on the analysis of DNS network data passively extracted from a network, employing a machine learning module and the extraction of specific anomaly indicators able to describe the problem at hand.

ITASEC 2020 (Italy) - DNS Covert Channel Detection via Behavioral Analysis: a Machine Learning Approach

The paper proposes a technique for covert channel detection, based on the analysis of DNS data: the approach is based on a machine learning module and on specific anomaly indicators able to describe the problem at hand.

ITASEC 2021 (Italy) - Fast Flux Service Network Detection via Data Mining on Passive DNS Traffic

The paper proposes an effective method for detection of fast flux attacks, based on the analysis of DNS traffic: the technique is based on the identification of different metrics able to describe the characteristics of this type of attack through the use of a data mining approach and statistics.

aramis
by aizoOn

Scientific Papers 2017-2023

A selection

ITASEC 2021 (Italy) - Towards an Automated Pipeline for Detecting and Classifying Malware through Machine Learning

The paper proposes an approach for classifying Windows Portable Executables (PEs); in particular, given a PE sample the proposed method involves first a classification phase between good and malicious and then it identifies the type of threat, the family and malware beheviour.

MOLECON 2021 (Italy) - Attackers vs AI: how AI detects cyber threats

In this talk, we present how AI-powered solutions can help in amplifying the subtle signals of sophisticated attacks and allow security analysts to take immediate actions. After a brief introduction on defensive artificial intelligence, we will dive into the aspects of defensive machine learning and show how advanced techniques can be used to detect real-world cyber attacks performed by famous threat actors. The last part of the presentation will explore how AI can be also used to enhance attackers' capabilities.

CISDA 2021 (USA) & ITASEC 2022 (Italy) - Near-real-time Anomaly Detection in Encrypted Traffic using Machine Learning Techniques

The paper proposes an analytics monitoring encrypted traffic flows and extracting meaningful characteristics in order to identify possible attacks and anomalies, combining the use of machine learning with a statistical approach.

OL2A 2023 - PhishVision: a Deep Learning based Visual Brand Impersona-tion Detector for Identify-ing Phishing Attacks

The paper proposes a framework to visually identify phishing sites, through the accurate identification of the main logo of the page under analysis. PhishVision was designed and implemented to provide Security Operation Center analysts with a near-real-time detection service for phishing attempts.

JCP 2023 - Towards a Near-real-time Protocol Tunneling Detector based on Machine Learning Techniques

This paper proposes a prototype that detects, in near real time, protocol tunneling techniques observed within network traffic. The prototype monitors unencrypted traffic, extracting features that enable the detection of potential ongoing attacks and/or anomalies, combining both machine learning and deep learning techniques.

aramis
by aizoOn

“Cognitive” approach to the problem

Thanks to a combination of **Machine learning, advanced analytics and threat intelligence**, aramis allows to:

- automatically learn network behavior
- identify malicious and anomalous activities,
- detecti patterns and relationships autonomously
- analyze data without prior information or human input

Machine Learning

- Learn and highlight any anomalies compared to the normal behavior of the infrastructure through unsupervised algorithms

Advanced Cyber Analytics

- Advanced analysis aimed at identifying **specific anomalous behaviors,** particular malware, or attacks using data mining and machine learning techniques.

Threat Intelligence

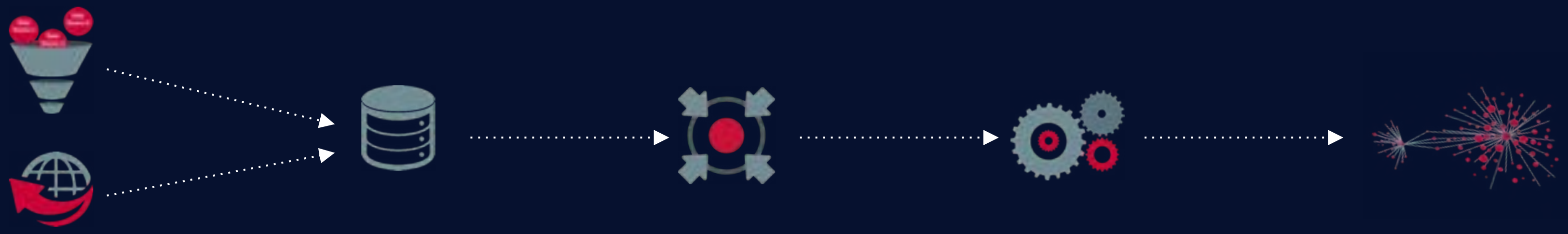
- We integrate sources of cyber intelligence, TTPs (Tactics, Techniques, and Procedures - MITRE -), IOCs (Indicators of Compromise) from Malware Labs, reputational databases of IPs, malicious domains, and TOR nodes.

Data Fusion

- We provide an integrated view by collecting all available data within the organization, including those typically not analyzed for security purposes.

Workflow: Data Collection and Processing

Immediate Detection of Attack Patterns



COLLECTION

The sensors are strategically positioned at different nodes within the network, based on the flow size and data quantity.

Each sensor gathers information from the network segment where it's installed, analyzes it in real-time, and sends the results to the processing server.

ENRICHMENT

On the processing server, the data received from the probes is enriched with information from all internal sources within the organization's architecture, cyber and threat intelligence sources, as well as using specific customer-specific information

FUSION

Merge data originating from various and heterogeneous systems, applications, and services to generate higher-quality information and enable more accurate detection and forensic analysis..

ANALYSIS

aramis constantly performs two kind of analysis on the collected data:

- Continuous Modulation of its analytics based on the dynamic variation of the measured risks.
- Analysis through the AI Engine of the behavior of each single network node, in order to detect any possible anomaly.

VISUALIZATION

The information is represented in the dashboards with an effective "cognitive visualization" approach allowing to promptly highlight any minimum deviations from repetitive patterns. These graphics, thanks to their zoom and drill down capabilities provide the analysts with a powerful tool for the identification and analysis of alarms.

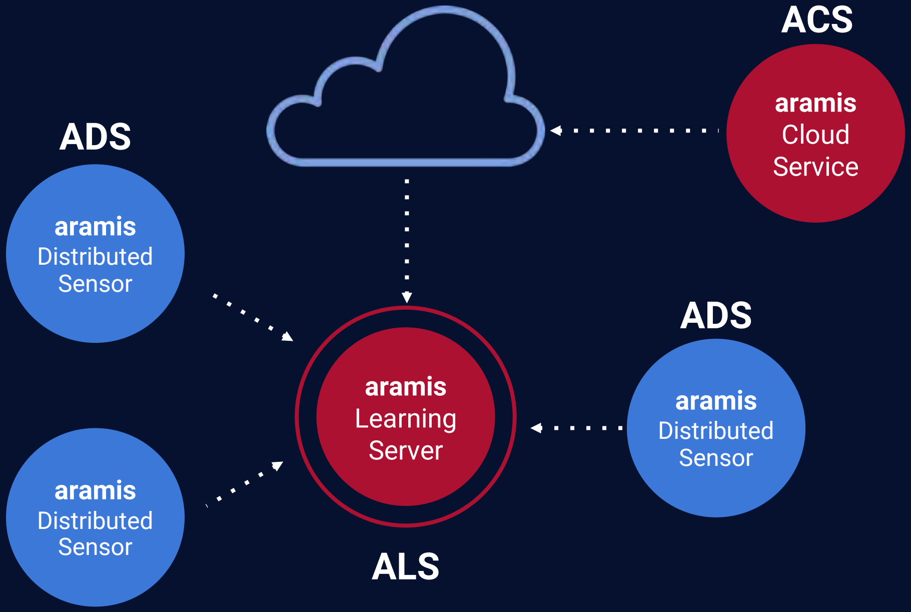
Architecture

Aramis platform is based on a modular and scalable architecture

The central element consists of an ALS (Aramis Learning Server) - the information processing server - which houses both advanced analytics and systems with machine learning algorithms. The ALS can be either on-premises or in the cloud.

Data collected by the ADS (Aramis Distributed Sensor), which acquire network traffic for monitoring, **are directed towards the ALS**. **The ADS can be physical, virtual, or in the cloud.**

The system for collecting and classifying cyber and threat intelligence sources accessible in a private cloud, called **ACS** (Aramis Cloud Service), ensures continuous updating.


ACS
aramis Cloud Service
ADS
aramis Distributed Sensor
ADS
aramis Distributed Sensor
aramis Learning Server
aramis Distributed Sensor
ALS

5 pillars

Artificial intelligence

is globally recognized as a powerful ally in early detection of advanced cyber threats;

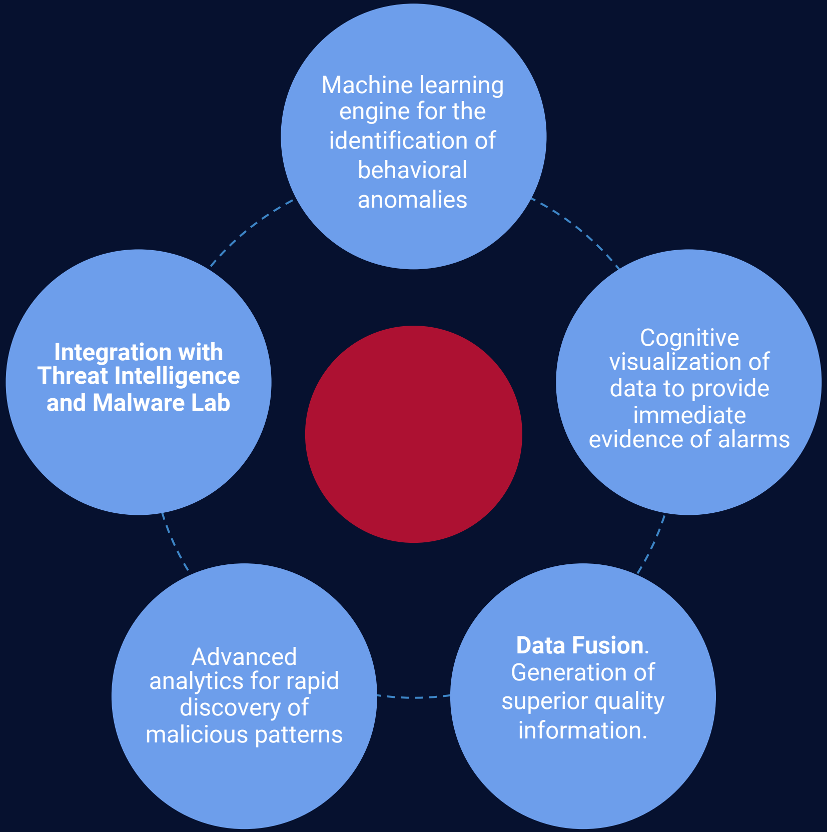
is capable of analyzing large amounts of data in real-time, and the algorithms can be trained to recognize typical patterns of behavior and traffic. Consequently, they can identify any anomalies or suspicious activities.

The value of information

It is the result of the acquisition, enrichment, integration, fusion, and advanced analysis of large amounts of data (Big Data)

It is accessible if appropriately represented through cognitive visualizations.

aramis is the platform aimed at enhancing prevention, detection, and response to cyber threats, reducing response times, and improving the accuracy of analyses.



Machine learning engine for the identification of behavioral anomalies

Cognitive visualization of data to provide immediate evidence of alarms

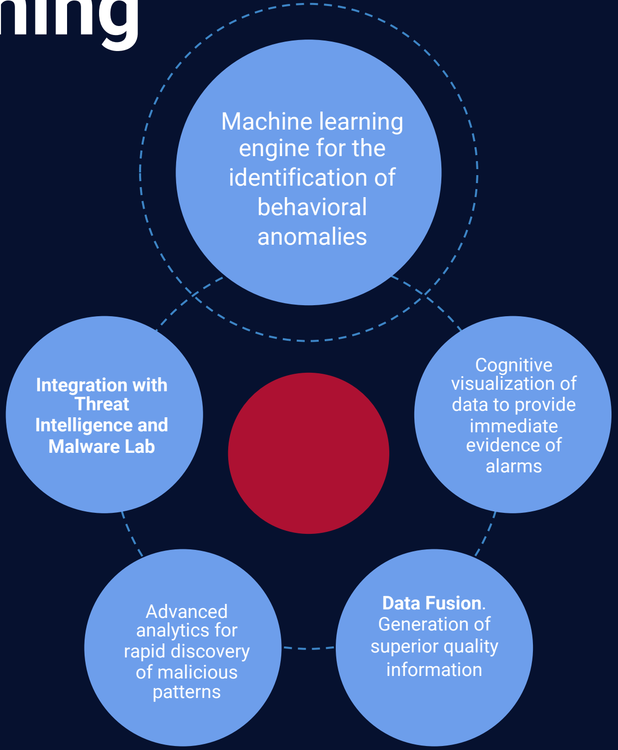
Data Fusion. Generation of superior quality information.

Advanced analytics for rapid discovery of malicious patterns

Integration with Threat Intelligence and Malware Lab

5 pillars / 1. Machine Learning

- Analysis of large amounts of data in short time;
- Definition of efficient mathematical models;
- Continuous improvement of the algorithms


Machine learning engine for the identification of behavioral anomalies
Integration with Threat Intelligence and Malware Lab
Cognitive visualization of data to provide immediate evidence of alarms
Advanced analytics for rapid discovery of malicious patterns
Data Fusion. Generation of superior quality information

5 pillars / 1. Machine Learning

ABE | Advanced Behavioural Engine

ABE analyzes the typical behavior of the machines within the network under scrutiny. Its purpose is to model the regular behavior of a machine using machine learning techniques to recognize and report behaviors that differ from this normality to the extent that they could potentially be classified as anomalous.

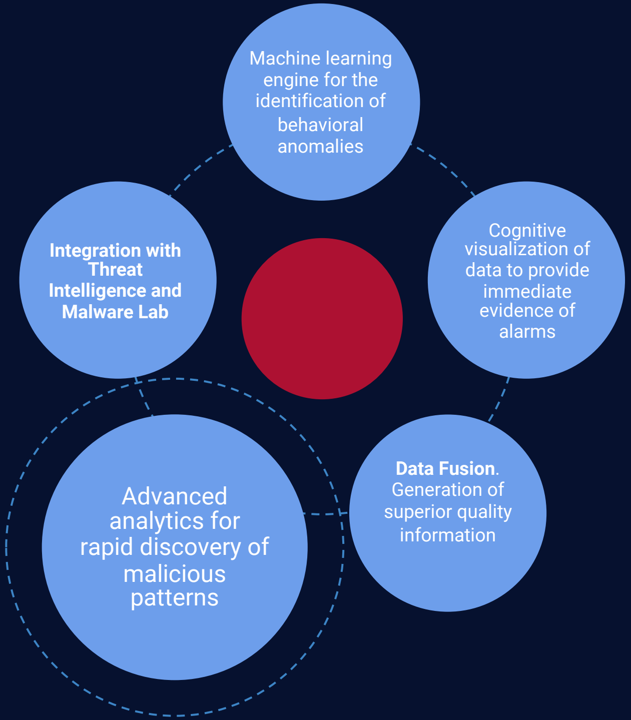
Some of the features extracted and analyzed include:

- Amount of data sent/received
- Amount of data sent from internal to external networks
- Percentage of outbound traffic
- Percentage of local traffic
- Activity times (morning, afternoon, evening)
- Location of contacted servers
- Contacted ports
- Contacted machines/IP addresses
- Contacted ASNs

The Compass functionality, integrated into the ABE user interface, assists the analyst in understanding the anomaly detected by the Machine Learning algorithms by highlighting how the features deviate from the expected baseline.

5 pillars / 2. Advanced Analytics

- Capability to evolve with the evolution of malware;
- Historical data analysis;
- Support in the identification and prevention of cybersecurity incidents and threats



Machine learning engine for the identification of behavioral anomalies

Cognitive visualization of data to provide immediate evidence of alarms

Data Fusion. Generation of superior quality information

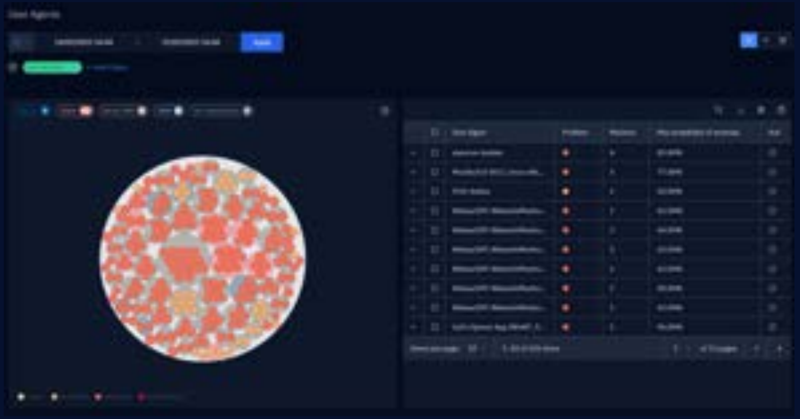
Advanced analytics for rapid discovery of malicious patterns

Integration with Threat Intelligence and Malware Lab

5 pillars / 2. Advanced Analytics

ACA | Advanced Cyber Analytics

Advanced analytics are data mining algorithms designed to analyze data traffic and detect specific classes of malicious or anomalous activities



User Agents

IP GEOLOCATION
Classifies the origin and destination of communications

INTRANET NETWORK
Analyzes the flow of local communications

OUTLIER DETECTION
Identifies anomalous amounts of traffic

PROTOCOL ANALYSIS
Identifies anomalous amounts of traffic categorized by protocol

SCHEDULED OPERATIONS
Identifies scheduled operations

CONSTANT DATA TRANSMISSION
Identifies constant data transmission

USER AGENT
Identifies anomalies in the user agent field

IOC
Deterministic identification based on IP, host, and URL

IPFLUX
Detects Fast Flux attacks

DRIVE BY DOWNLOAD
Identifies the download of files associated with exploits and malware.

SMB ANALYSIS
Analyzes and identifies activities typical of ransomware.

COVERT CHANNEL
Identifies unauthorized communications usage through DNS or HTTP.

SCAN DETECTION
Identifies NMAP-type scans.

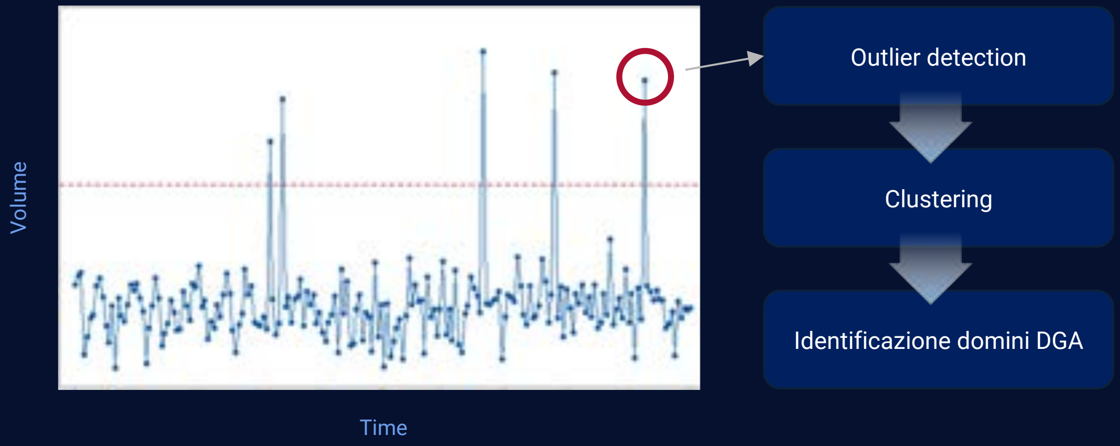
TLS/SSL ANALYSIS
Identifies anomalies in encrypted traffic metadata.

PHISHING
Identifies contacts with potential phishing domains.

DGA
Identifies the presence of Domain Generation Algorithms used by various malware.

5 pillars / 2. Advanced Analytics

Domain Generation Algorithms (DGA) detection



Outlier detection

Clustering

Identificazione domini DGA

Malware **keylogger**

116 not resolved reqs
54 resolved reqs

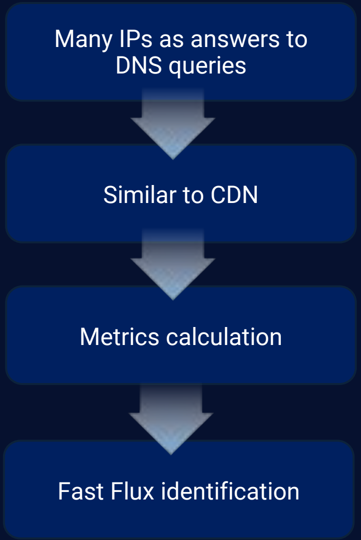
Malicious domains identified
"cogefdi.top" [NOT RESOLVED]
"agifdoc.top" [NOT RESOLVED]
"agifdocg.top" [NOT RESOLVED]
"ogemdacw.top" [**RESOLVED**]

Anomaly probability
90,4%

aramis
by aizoOn

5 pillars / 2. Advanced Analytics

Fast flux identification



Many IPs as answers to DNS queries

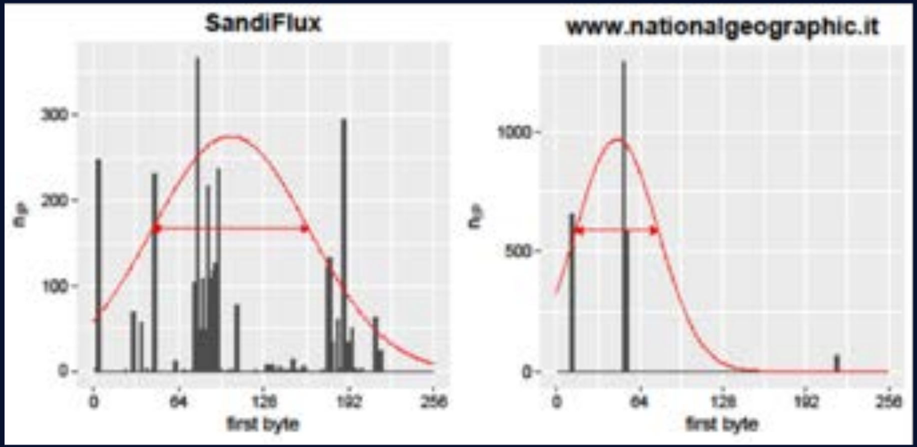
Similar to CDN

Metrics calculation

Fast Flux identification

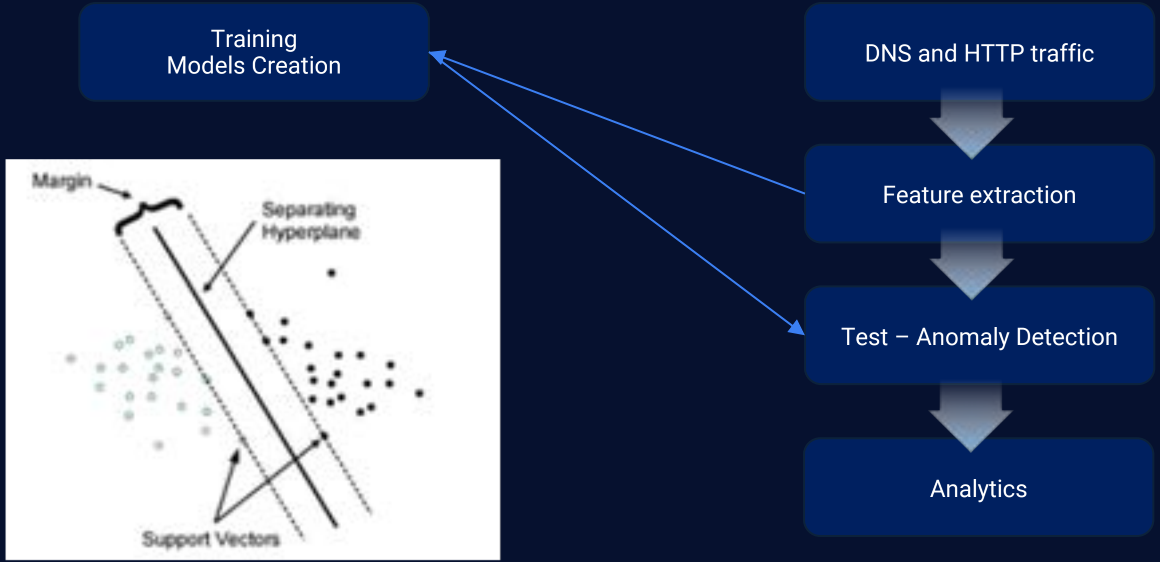
scottfranch.org
62.100.255.25
155.133.93.30
109.121.206.4
85.105.136.98
82.114.68.102
109.172.179.12
82.114.65.50

IP-dispersion



5 pillars / 2. Advanced Analytics

Covert Channel



Training
Models Creation

DNS and HTTP traffic

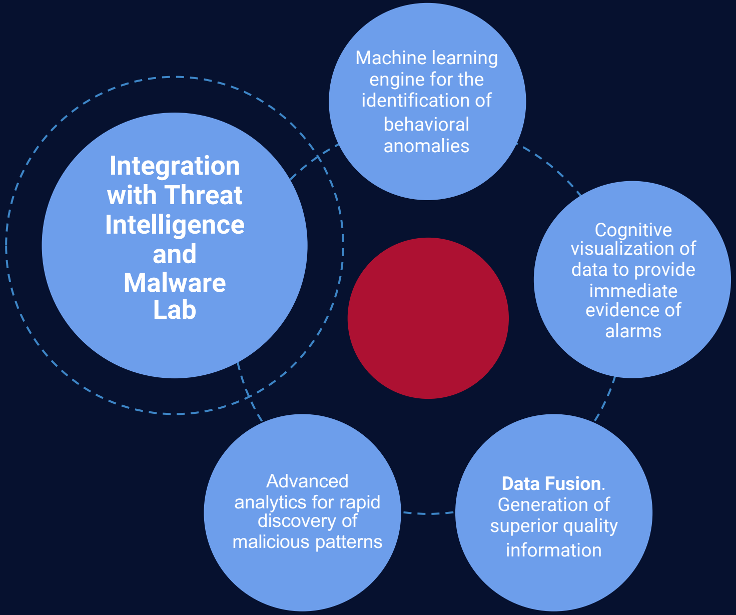
Feature extraction

Test – Anomaly Detection

Analytics

5 pillars / 3. Cyber and Threat Intelligence Sources

- Honeypot distribuite
- Intelligence sharing
- Cyber Intelligence
- Integration of new attack patterns (Malware Lab)
- MITRE ATT&CK
- Integration with Risk Management & Governance Platform



Integration with Threat Intelligence and Malware Lab

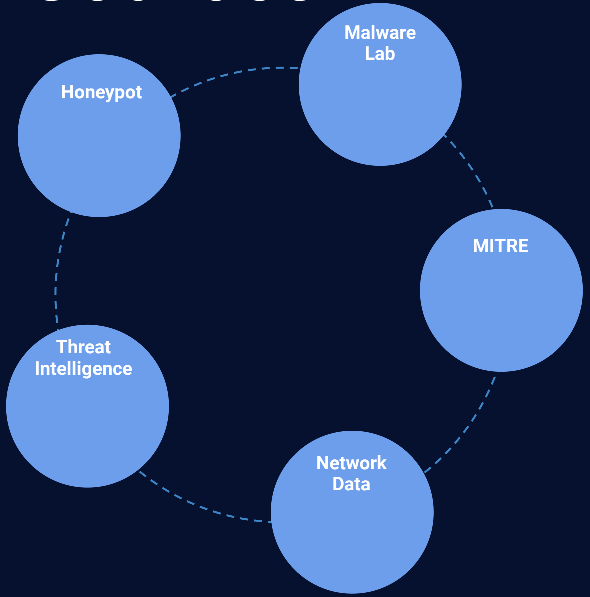
Machine learning engine for the identification of behavioral anomalies

Cognitive visualization of data to provide immediate evidence of alarms

Data Fusion. Generation of superior quality information

Advanced analytics for rapid discovery of malicious patterns

5 pillars / 3. Cyber and Threat Intelligence Sources



Automatic detection of **malware, attacks, scans**

Identification of schemas, **correlations** and **patterns of the attacks**

Clustering to highlight **behavioral variations** of the network nodes

Analysis to detect **threats**

Ranking and prioritization

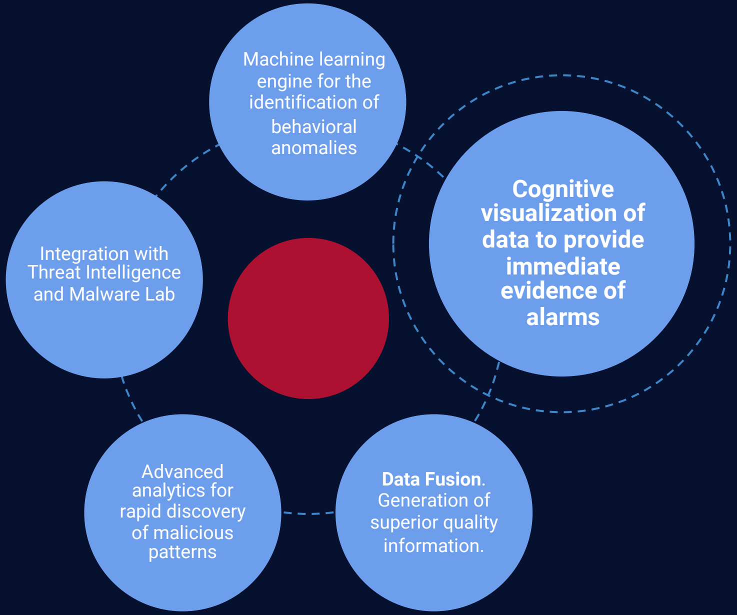
Tagging and collection of **correlated events**

Feedback to the platform

Continuous Improvement

5 pillars / 4. Dashboard and Cognitive Visualization

- **A synthetic and multidimensional representation of information that allows the analyst to easily visualize anomalies and threats**
- **Multi-level dashboards** for complex organizations
- Simplified data availability and navigation supporting investigative analysis
- Customizable dashboards in color schemes



Machine learning engine for the identification of behavioral anomalies

Cognitive visualization of data to provide immediate evidence of alarms

Data Fusion. Generation of superior quality information.

Advanced analytics for rapid discovery of malicious patterns

Integration with Threat Intelligence and Malware Lab

5 pillars / 4. Dashboard and Cognitive Visualization

Dashboard aramis

The aramis Dashboard synthetically represents the security level of the monitored network.

Real-time Parameters

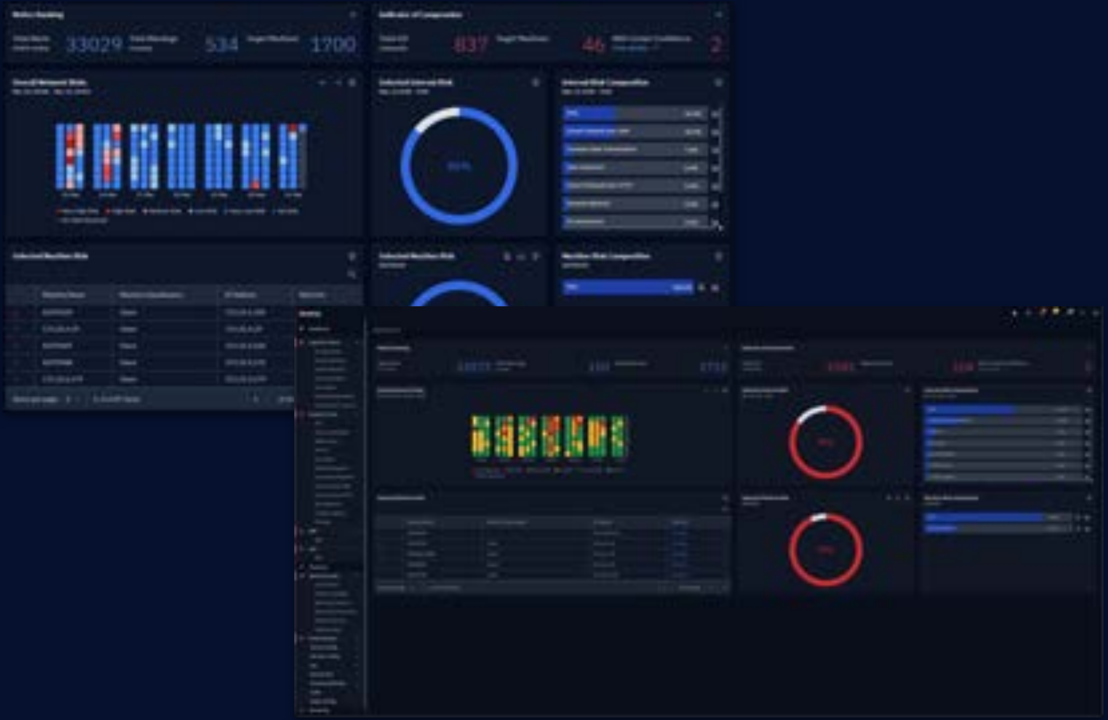
- IOCs and Alerts are displayed at the top of the window, allowing easy access to the chronological list.

Overall Network Risk

- Represents the risk level in hourly time intervals.
- By selecting an interval, it's possible to view the detection details and at-risk machines.

Display Modes

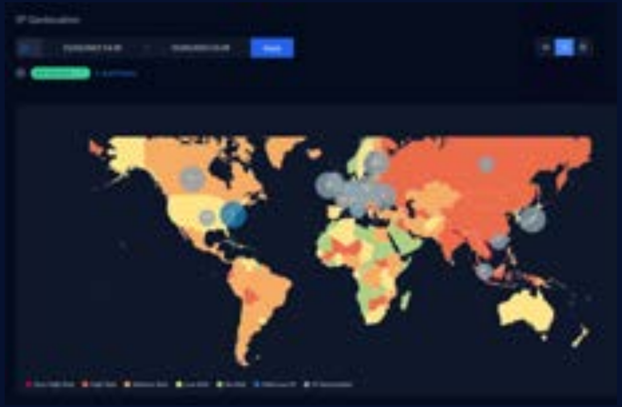
- Thanks to the dark or light themes and the two-color palette, a more accessible or traffic light mode, it's possible to adapt to the analyst's preferences.



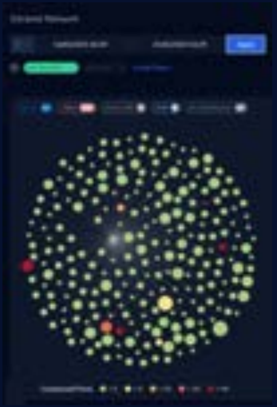
5 pillars/ 4. Dashboard and Cognitive visualization

Cognitive Visualization

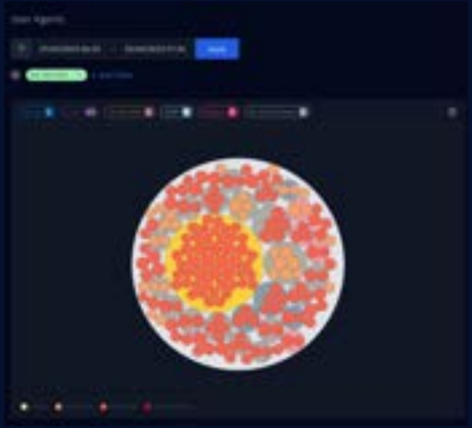
IP Geolocation.
This analytics displays the destinations of connections indicating the associated risk



Intranet Network.
Represents the quantity of connections present and the diversity of ports used



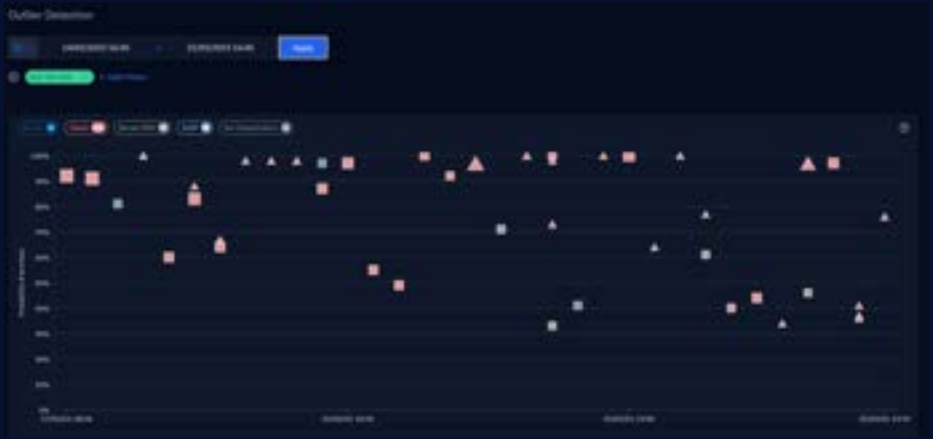
User Agent.
Summarizes which User Agents are present on the network and their distribution



5 pillars/ 4. Dashboard and Cognitive visualization

Cognitive visualization

Outlier detection.
Detects the amount of bytes sent that deviate from the usual behavior of a specific machine-



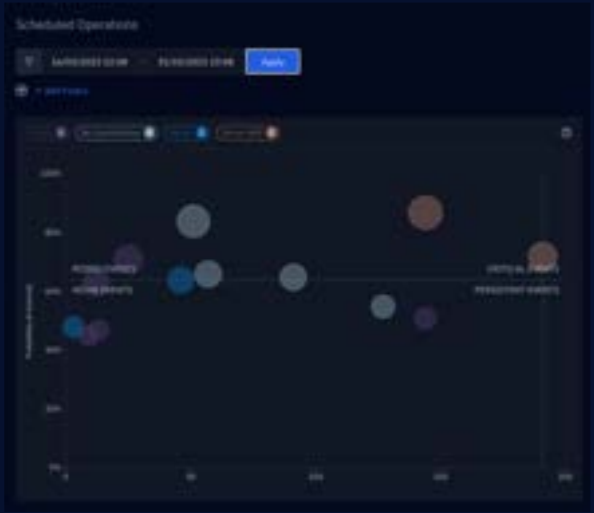
Protocol Analysis.
It consolidates various information including:

- Communication direction
- Protocols
- Services

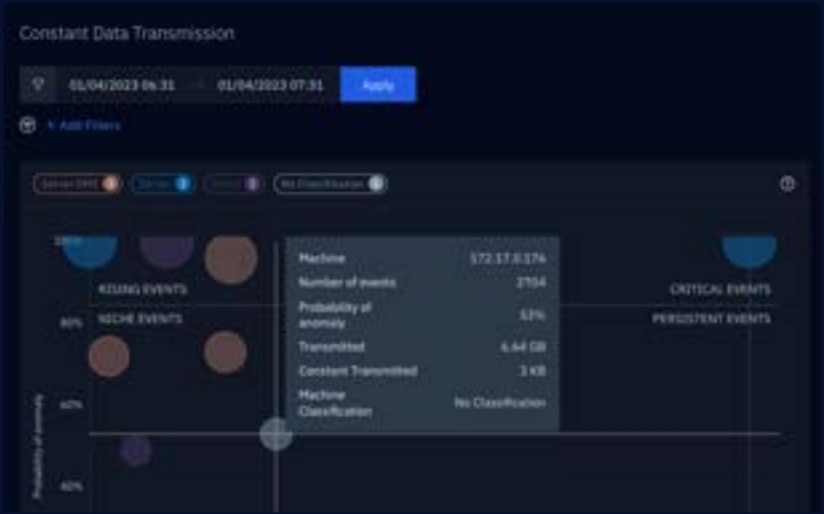
5 pilastri / 4. Dashboard and Cognitive Visualization

Cognitive Visualization

Scheduled Operations.
This analytics recognizes scheduled operations, which repeat at constant time intervals, occurring between a source, destination, and port.



Constant Data Transmission.
This analytics detects operations associated with a constant data exchange.



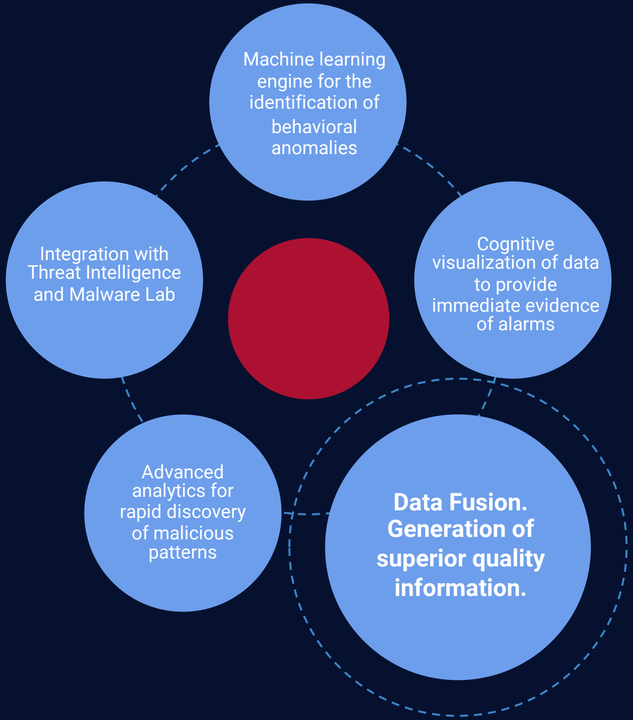
Machine 172.17.0.176
Number of events 2704
Probability of anomaly 63%
Transmitted 6.44 GB
Constant Transmitted 3 KB
Machine Classification No Classification

5 pillars / 5. Data Fusion

- Querying metadata is a fundamental process for analyzing network traffic and other sources - even those unrelated to security - in order to identify any anomalies or security issues.

- Metadata is collected and analyzed to identify patterns and anomalies. Metadata includes - for example - information such as source and destination IP addresses, the protocol used, destination port, connection duration, volume of exchanged data, firewall routes, user-associated permissions, running processes, etc.

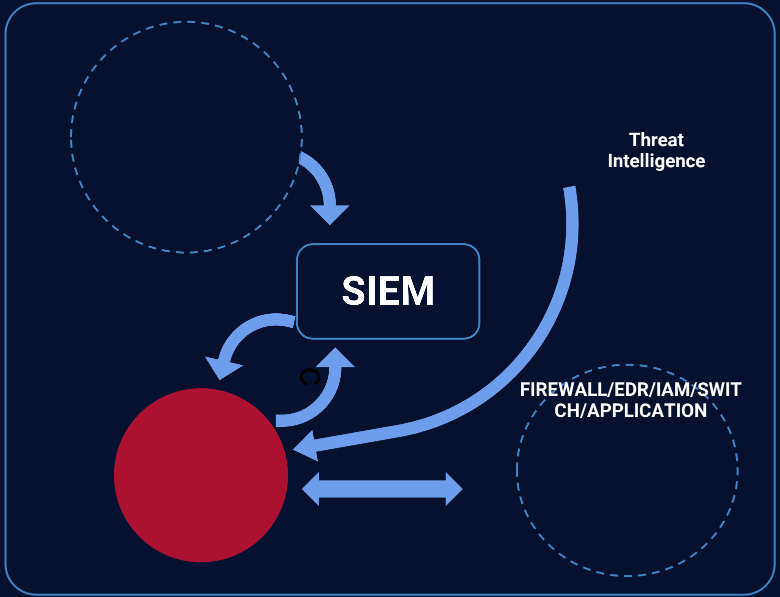
- The Enquiring interface facilitates forensic activities and event reconstruction, aiding in the detection of any suspicious activities that may indicate the presence of illegal or harmful activities to the infrastructure's security


Machine learning engine for the identification of behavioral anomalies
Integration with Threat Intelligence and Malware Lab
Cognitive visualization of data to provide immediate evidence of alarms
Advanced analytics for rapid discovery of malicious patterns
Data Fusion. Generation of superior quality information.

5.pillars / 5. Data Fusion

aramis has been designed to be an autonomous and **self-consistent platform**, but today it's even more **effective as it leverages all data** sources within the organizational architecture to better understand threat information **through automatic and adaptive learning.**

Moreover, **Aramis serves as a high-value information source for other systems,** such as SIEMs, by providing **pre-analyzed and aggregated** events ready to be **correlated** with other sources, both raw and «intelligence-based».



aramis
by aizoOn

5 pillars / 5. Data Fusion

ACE | Advanced Correlation Engine

aramis ACE, Advanced Correlation Engine, is a programmable engine that allows correlating:

- Detections from ACA Analysis algorithms
- Network traffic metadata captured by ADS (aramis Distributed Sensors)
- Information from other platforms, extending detection capabilities to include the local activity of individual machine

Thanks to integration with various sources, Aramis can provide information on the processes that generated specific events, allowing for a more in-depth analysis of anomalies or the elimination of false positives.

- Correlation simplifies and automates the detection of event chains occurring over time.
- Correlation rules are easily programmable

Example of a correlation rule between a DGA and traffic within a time frame.

```
rule "Dga and Traffic detection"
when
  $dga : DgaOutput(this.getExternalIpsInvolved() != null)
  $traffic : ProtocolData(hasMachine($dga.getMachine()), this after[0,2d] $dga )
  eval($traffic.existsDstIn($ips))
  not FactFlag(key == FactFlag.key($traffic.getTs(), 60, "dga-traffic", $dga.getMachine(),
$traffic.getDst()))
then
     insert(FactFlag.from($traffic.getTs(), 60, "dga-traffic", $dga.getMachine(),  $traffic.getDst()));

end
```

5 pillars / 5. Data Fusion

enquiring

This represents the ability to extract information from the historical acquired traffic, based on multiple parameters in different combinations.

Complex queries can be constructed as needed to properly isolate a single event or a set of events related to one or more hosts. It also allows retrospective querying of events.

aramis®

by aizoOn

aramisec.com
aizoongroup.com

AUSTRALIA
Sydney NSW | Adelaide SA

EUROPE
Aosta ITA | Bari ITA | Bologna ITA | Catania ITA | Cuneo ITA
Genova ITA | Milano ITA | Roma ITA | Terni ITA | Torino ITA
Sheffield UK | Zurigo CH

USA
New York NY | Cambridge MA

aizoOn® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING