

DON'T LEARN MALWARE



KNOW

The detection process does not require vendor-specific or malware knowledge. The key factor is the knowledge of your environment trends and behaviour.



PROTECT

aramis proprietary logic is designed to reduce the "dwell time" passing from the infection to the identification and eradication of malware to hours instead of days or weeks.



EMPOWER

aramis does not rely on signature triggering; it highlights the presence of malicious behaviour, enabling the analyst to immediately identify and classify threats by collating the data presented in the pre-attentive dashboard.



CYBER SECURITY

aizoOn's Cyber Security Technology Unit is specialized in Security Assessment, Mobile & Embedded Security, IoT & Wearable Devices Security, Incident Handling, Digital Forensics, Malware Reverse Engineering, Critical Infrastructure & Production Systems Security and Enterprise Cyber Risk

MALWARE LAB



The **aramis** Lab studies and classifies the behaviour of the most advanced malware. The Lab was built to constantly improve aramis' malware identification capabilities.

APAC

+61 02 8299 7302
aramis@aizoon.com.au
aizoon.com.au

EMEA

+39 011 2344611
aramis@aizoongroup.com
aizoongroup.com

NORTH AMERICA

+1 866 398 6567
aramis@aizoon.us
aizoon.us



ARAMISEC.COM

A DIFFERENT APPROACH

In a world where threats are evolving at an unprecedented pace, it is crucial to have a comprehensive view of your networks and systems.

aramis allows you to monitor your network accurately, promptly and smoothly no matter the complexity of your organisation.

aramis uses a specifically designed Machine Learning Engine and Deterministic Rules Advanced Cyber Analytics to enable organisations to identify unknown threats inside their perimeter by fostering human analysis through pre-attentive dashboards.

FOUR PILLARS

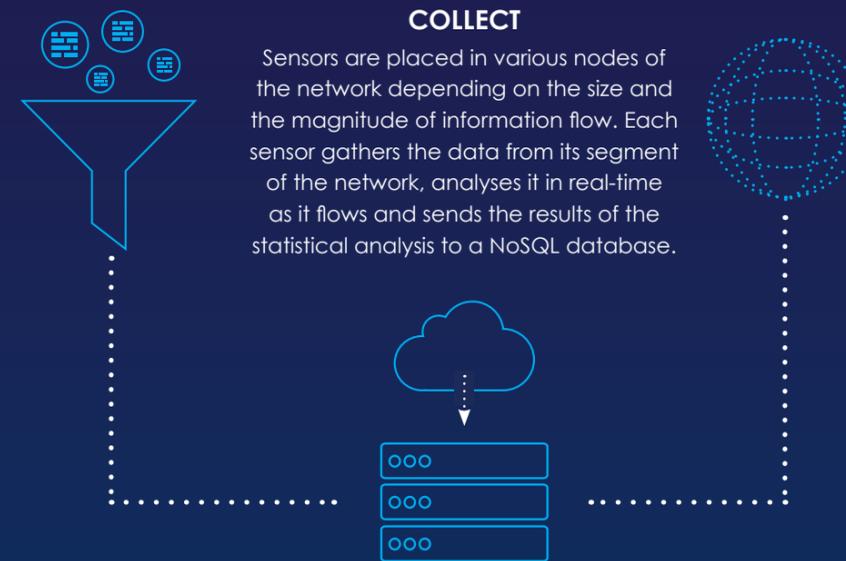
Identify threats inside a network by highlighting the deviations from the network's normal behaviour.

Foster human analysis using pre-attentive dashboards and graphics.

Take advantage of specifically designed **Bayesian Network Artificial Intelligence Engine Data Mining and Machine Learning Techniques**.

Collect data passively without altering the current network layout.

HOW ARAMIS WORKS



ENRICH

Inside the NoSQL database, data is enriched with information coming from the aramis Cloud Service. The Cloud Service collects intelligence from various OSINT sources and from internally managed sources.



VISUALIZE

Using pre-attentive graphs, humans can spot deviations from repetitive patterns much faster than computers, especially when there's a lot of data to visualise. This particular ability is called cognitive ability.



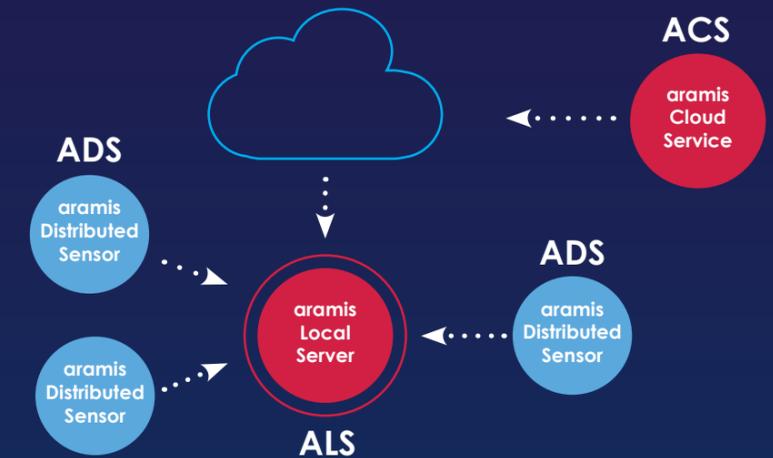
Our dashboards make use of pre-attentive processing to foster this kind of analysis, allowing at the same time in-depth analysis when needed, thanks to zooming, drill-down and filtering capabilities.

CORRELATE

aramis constantly runs two kinds of analyses on the stored data:

- **Deterministic Rules**
Advanced Cyber Analytics, tailored to the customer Risk perception, are able to spot and highlight risky conducts.
- **The Machine Learning Engine**
analyses the behaviour of each machine and correlates the current behaviour with its usual behaviour, highlighting even the slightest deviation.

ARAMIS AS A PRODUCT



ARAMIS AS A SERVICE

WEEKLY DIGEST + BRIEFING CALL	✓	✓	✓
INCIDENT HANDLING CONSULTANCY HOURS INCLUDED	✗	8 HR	40 HR
COVERAGE	8 / 5	12 / 5	24 / 7
REACTIVITY	4 HRS	2 HRS	1 HR
UP-TIME	96 % *	98 % *	99,9 %

* Calculated on service hours

PROOF OF VALUE

