aramis

Gabriele Liverziani
Pre-Sales Eng. - aizoOn

Matteo Herin
RSO – Leroy Merlin

aramis

Intelligenza artificiale e umana, competenza e passione per la gestione del rischio digitale

Gartner Cool Vendor 2016

ECS

aizoOn AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

Know, protect, empower. Don't learn malware.

aizoOn è una società di consulenza tecnologica di innovazione, indipendente, che opera a livello globale

la nostra visione: applicare diffusamente l'approccio scientifico e quantitativo, per una società più responsabile e sostenibile

la nostra missione: sostenere il futuro dei nostri clienti nell'era digitale, apportando competenza di tecnologia e di innovazione

Gartner Cool Vendor 2016

aizOon Cool Vendor 2016
Operational Technology in a Digital Business

> ***aizoOn*** *is cool in the context of managing OT in a digital business because of its ability to deliver holistic digital technology solutions, drawing from many diverse practices in IT; engineering; business innovation and process design; information management; and strategy and organization in an interdisciplinary way.*
>
> **GARTNER 2016**

APPROACH

adottiamo un modello operativo *digital oriented*, basato su logiche trans-disciplinari, agili ed iterative, collaborative ed aperte, abilitanti l'innovazione applicata

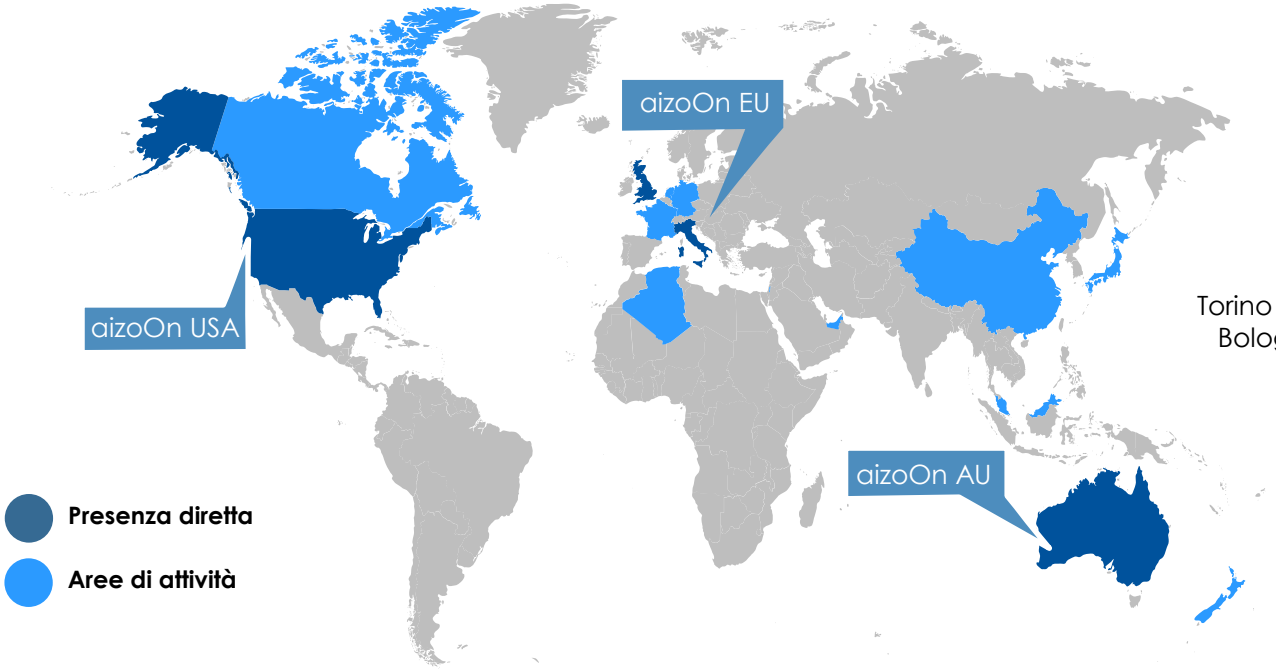
integriamo sinergicamente componenti di **tecnologia**, di **business** e di **innovazione** in grado di canalizzare le diverse dimensioni digitali in soluzioni innovative dedicate

ha **un approccio a rete** e si avvale della collaborazione di partner tecnologici e di ricerca

ECS EUROPEAN CYBER SECURITY ORGANISATION

Membro fondatore di ECSO (European Cyber Security Organisation), organizzazione firmataria del cPPP indetto dalla Commissione Europea sul tema della Cyber Security nel luglio 2016.

aizoOn Group Profile



AUSTRALIA
Sydney NSW

EUROPE
Torino ITA | Cuneo ITA | Milano ITA | Genova ITA
Bologna ITA | Roma ITA | Bari ITA | Sheffield UK

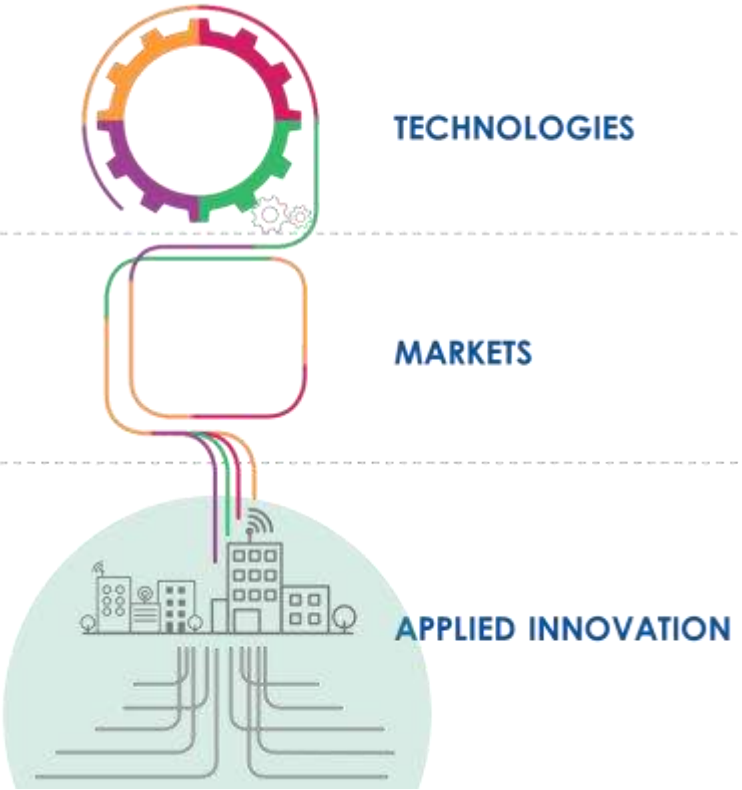
USA
New York NY | Troy MI
Cambridge MA | Lewiston ME

GLOBAL FOOTPRINT

Seguiamo i nostri Clienti in tutti i continenti: Africa, America, Asia, Europa, Oceania

aizoOn AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

aizoOn Approach



aizoOn

è pronta **a sostenere i suoi clienti nella transizione** all'era digitale, dove i confini tra settori ed aziende tradizionali tenderanno a sfumarsi ed i modelli di business a cambiare sempre più rapidamente

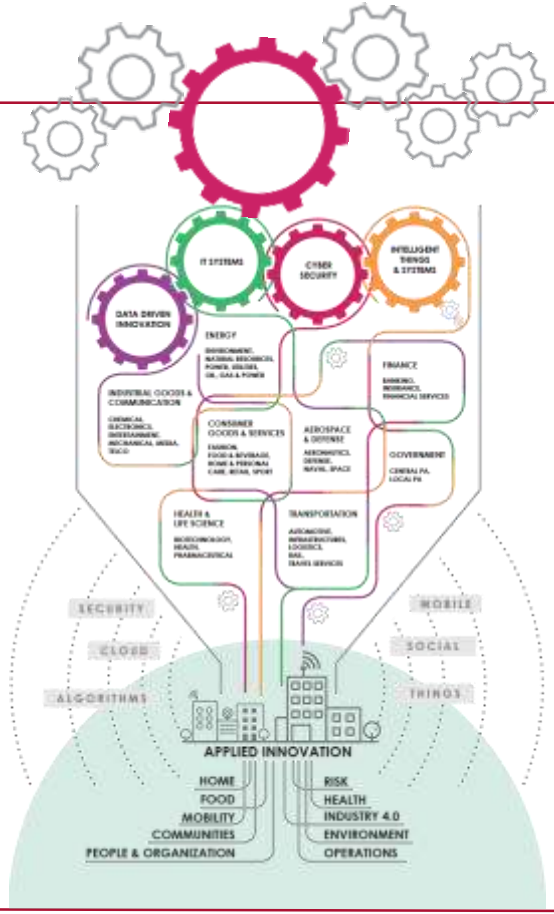
adotta un modello operativo *digital oriented*, basato su logiche trans-disciplinari, agili ed iterative, collaborative ed aperte, abilitanti l'innovazione applicata

integra sinergicamente componenti di **tecnologia**, di **business** e di **innovazione** in grado di canalizzare le diverse dimensioni digitali in soluzioni innovative dedicate (innovation stream)

ha **un approccio a rete** e si avvale della collaborazione di partner tecnologici e di ricerca

aizoOn AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

aizoOn e la Cyber Security



aramis

è una piattaforma di network security monitoring concepita per ridurre il "dwell time" di identificazione degli attacchi.

Adotta tecniche di Machine Learning, Advanced Cyber Analytics e Threat Intelligence per consentire ai cybersecurity analyst di prendere le migliori decisioni in tempi rapidi e proteggere le infrastrutture dai cyber threats.

la nostra soluzione: aramis

aizon® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

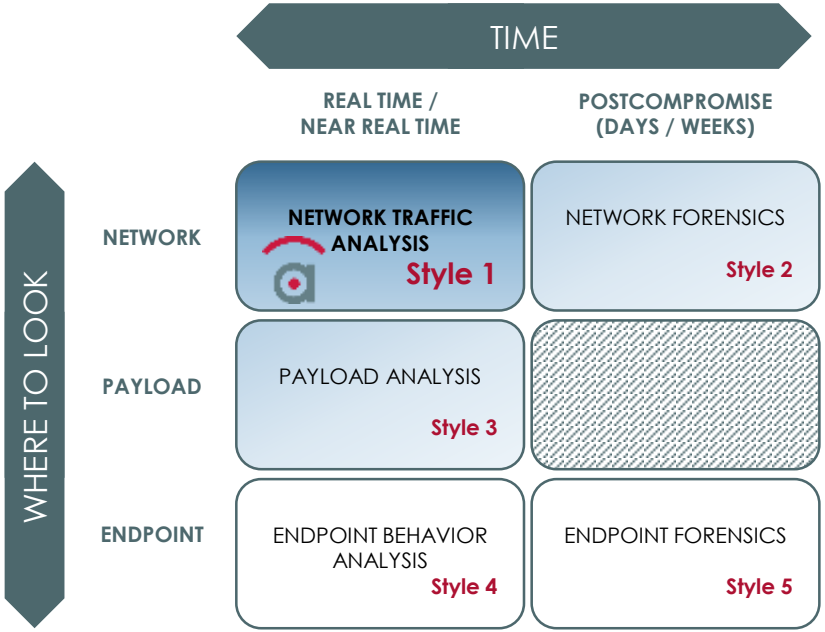
aramis, network security monitoring

Approccio innovativo al problema

aramis è la piattaforma di network security monitoring interamente progettata e realizzata da **aizoOn** grazie all'utilizzo convergente di algoritmi avanzati Machine Learning e Advanced Cyber Analytics.

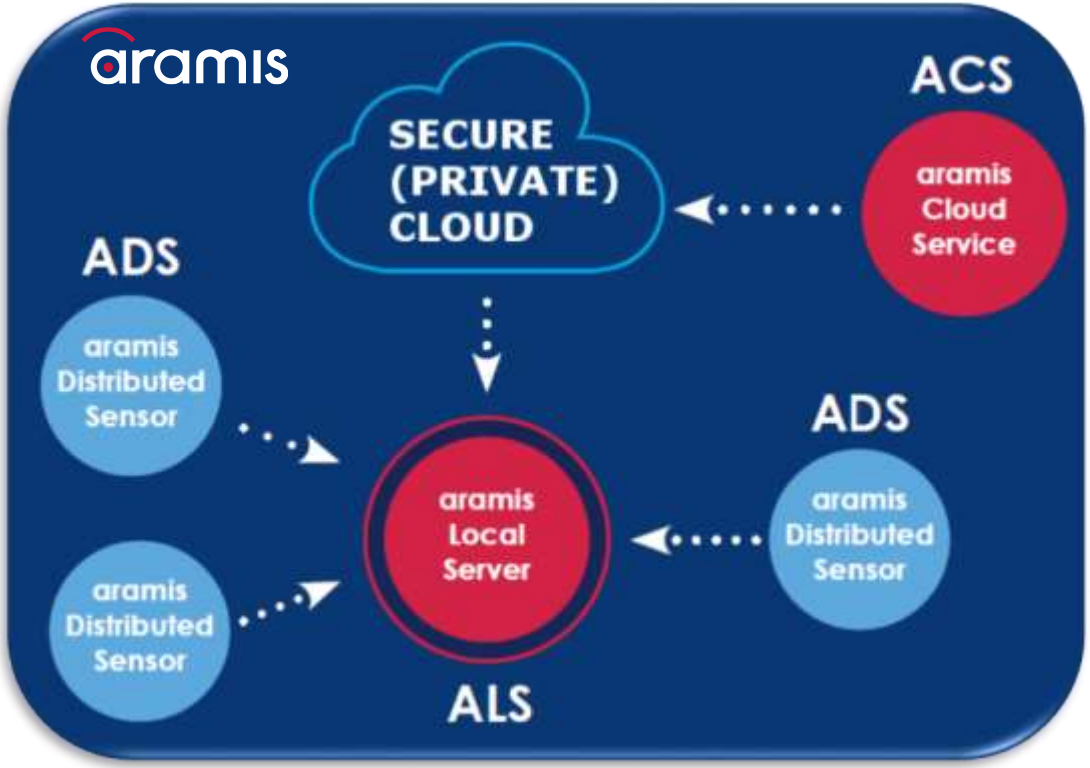
Il **posizionamento di aramis** trova riscontro nell'analisi di **Gartner "Five Styles of Advanced Threat Defense"** [L. Orans, J. D'Hoinne – 2013, 2016] **nello style 1**.

Tuttavia le caratteristiche avanzate della piattaforma consentono ad aramis® di **agire efficacemente a supporto degli style 2 e 3**.



GARTNER (August 2013, June 2016) - Five Styles of Advanced Threat Defense - "Lawrence Orans, Jeremy D'Hoinne"

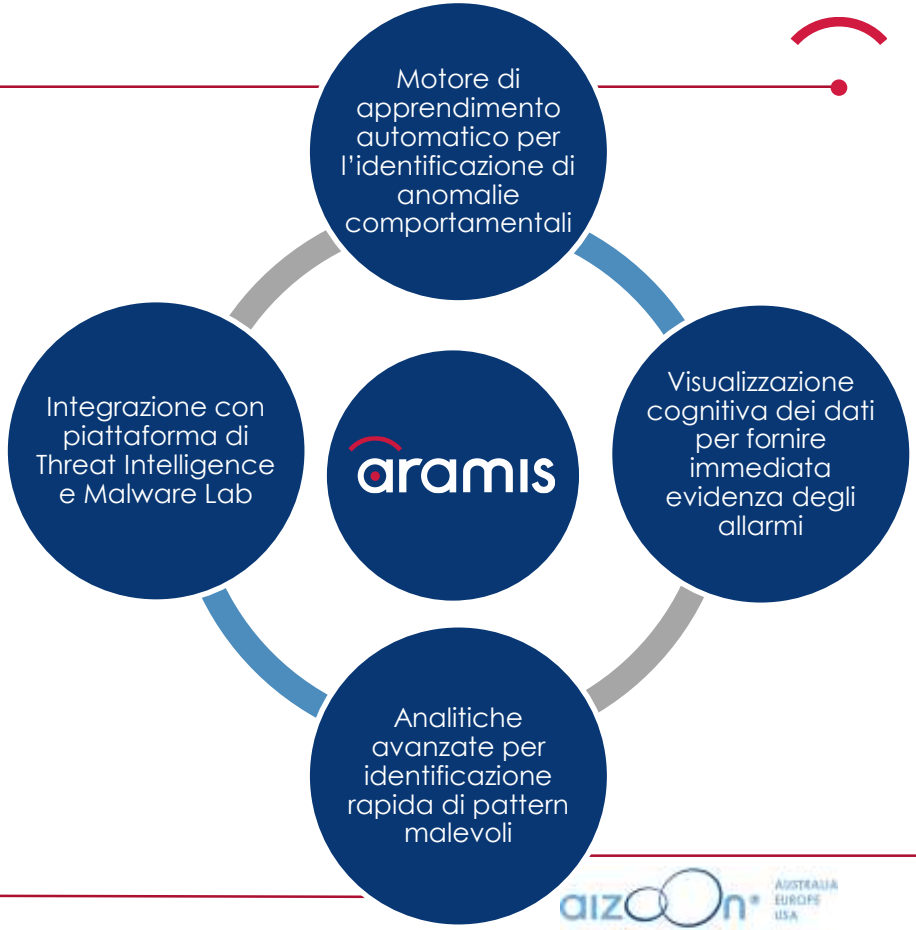
aramis architecture



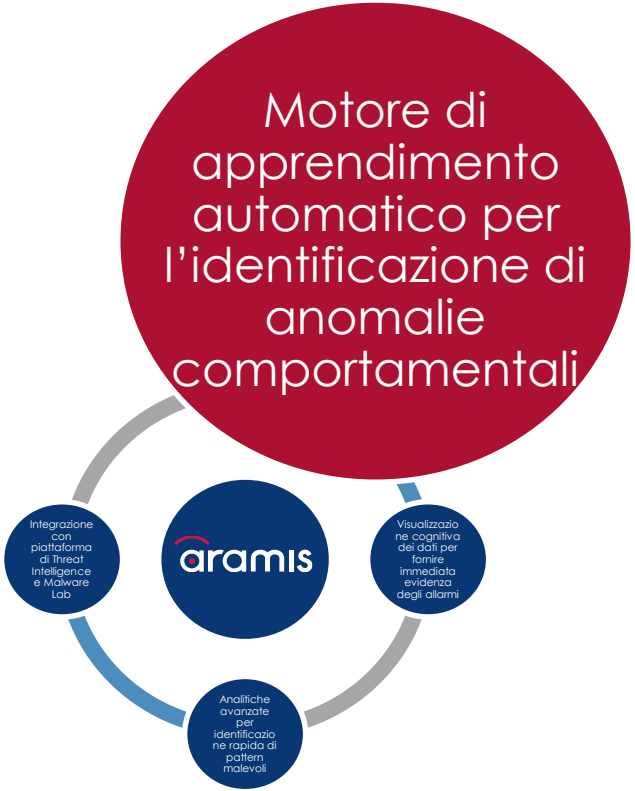
aramis: i 4 pilastri

L'intelligenza artificiale è globalmente riconosciuta quale potente alleato nella **rilevazione anticipata delle minacce informatiche avanzate**.
L'efficacia di questi strumenti matematici applicati alla cyber security dipende dalla capacità degli algoritmi di eliminare il rumore di fondo, di «**leggere i dati come farebbe un esperto analista**» e di fornire al Security Operation Center strumenti di monitoraggio e informazioni utili ad una rapida identificazione delle reali minacce.

aramis è una soluzione scalabile di Network Monitoring progettata per essere facilmente e organicamente integrata nel processo di ICT Risk Management.



1° Pilastro: machine learning



- analisi di grandi quantità di dati in «near real-time»;
- modelli matematici efficaci;
- rimozione del rumore di fondo;
- evoluzione continua degli algoritmi.

aramis: machine learning

Un approccio non supervisionato

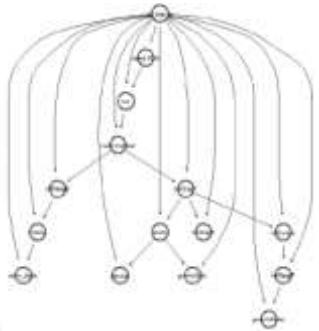
L'approccio non supervisionato permette ad aramis di:

- **Apprendere autonomamente** il comportamento del network
- Identificare le **attività anomale**
- Rilevare **automaticamente** pattern e relazioni
- Lavorare senza **informazioni a priori**
- **Non necessita di input umani**

aramis: machine learning

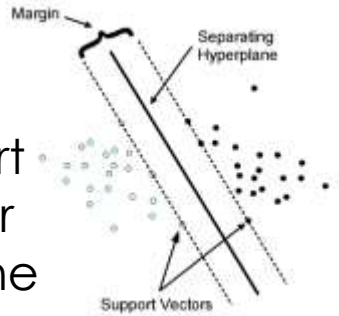
Riduzione del rumore di fondo

Prefilter



Bayesian Network

Support Vector Machine



Aggregation & postfilter

Anomaly detection

aramis: machine learning

Bayesian Networks (BNs)

Primo layer

pc1_model

pc2_model

pc3_model

srv1_model

srv2_model

Secondo Layer

Global_pc_model

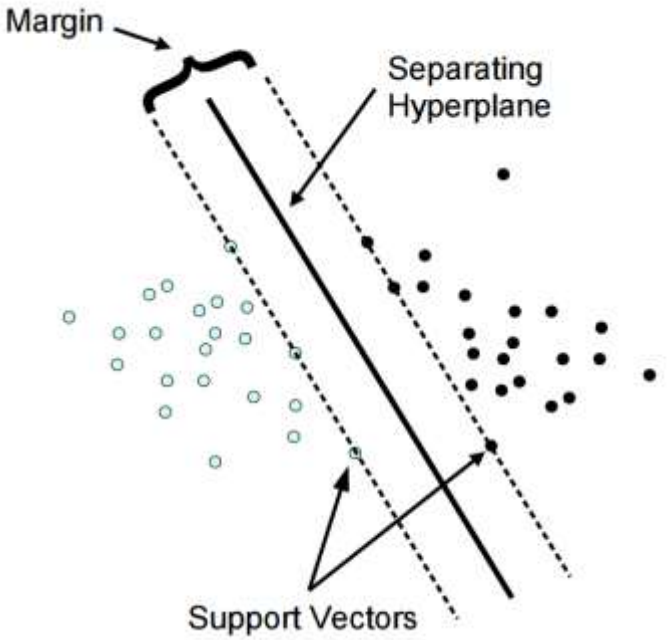
Global_srv_model

Outcome

Valutazione del **singolo evento**
Valutazione della **singola macchina**
Valutazione della **classe di macchine**
Valutazione dell'**intero network**

aramis: machine learning

Support Vector Machine (SVM)



Iperpiano a massimo margine:

$$f(\boldsymbol{x}) = \boldsymbol{w} \cdot \boldsymbol{x} + b$$

$$\begin{cases} \mathcal{H}_1 : & \boldsymbol{w} \cdot \boldsymbol{x} + b = 1 \\ \mathcal{H}_2 : & \boldsymbol{w} \cdot \boldsymbol{x} + b = -1 \end{cases}$$

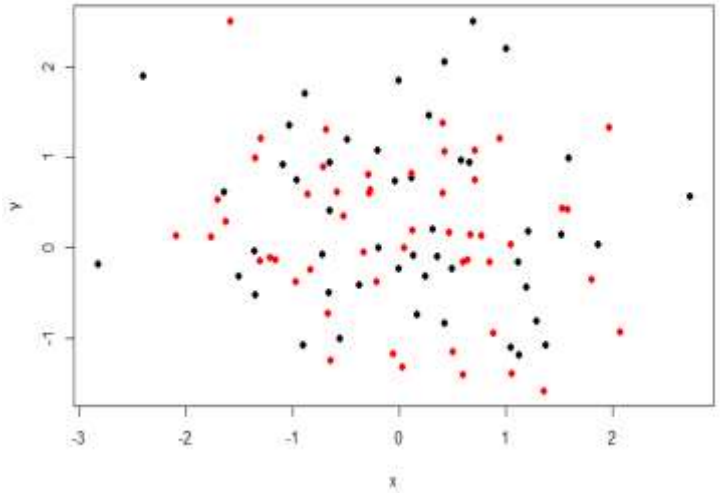
Minimizzazione:

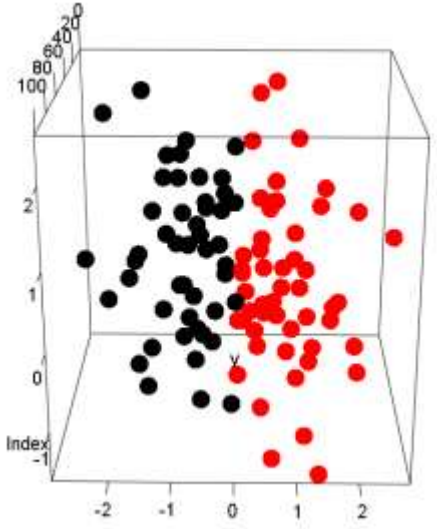
$$\min_{\boldsymbol{w},b} \quad \frac{\|\boldsymbol{w}\|^2}{2}$$

$$y_i (\boldsymbol{w} \cdot \boldsymbol{x}_i + b) \geq 1, \quad \forall i = 1, \ldots, l$$

aramis: machine learning

Support Vector Machine (SVM)





Mapping in uno spazio dove le classi sono linearmente separabili

aramis: machine learning

Dimensioni di Analisi

- Richieste HTTP
- Attività FTP
- Sessioni SSL
- Certificati usati in sessioni SSL
- Traffico SMTP sul network
- Attività DNS sul network
- Connessioni
- Attività su porte non standard
- File trasmessi
- Protocolli e servizi

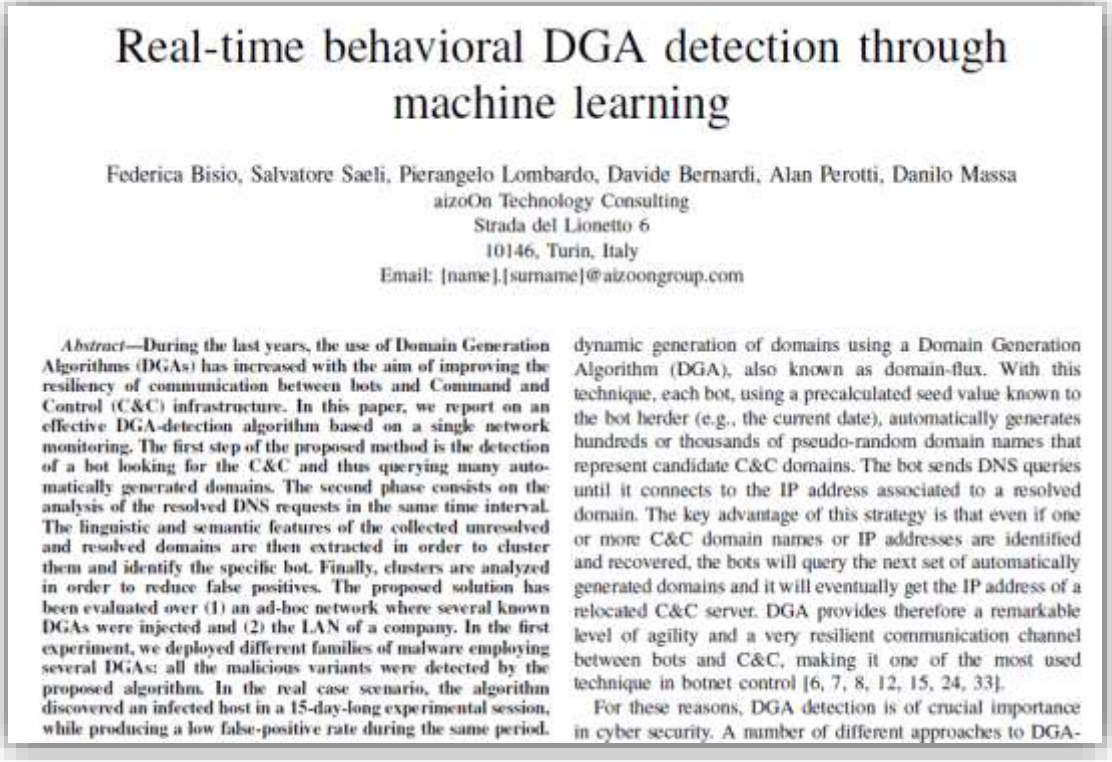
2° Pilastro: analitiche avanzate

Algoritmi di Data Mining

- Adattamento continuo in funzione dell'evoluzione del malware;
- analisi su dati storici;
- arricchimento della conoscenza degli esperti di cyber security del **Malware Lab** di aizoOn;
- arricchimento dei risultati dell'analisi degli incident eseguita dagli analisti del **I_SOC di aramis**;

aramis: analitiche avanzate

aizoOn at ICCST 2017



Real-time behavioral DGA detection through machine learning

Federica Bisio, Salvatore Saeli, Pierangelo Lombardo, Davide Bernardi, Alan Perotti, Danilo Massa
aizoOn Technology Consulting
Strada del Lionetto 6
10146, Turin, Italy
Email: [name].[surname]@aizoongroup.com

Abstract—During the last years, the use of Domain Generation Algorithms (DGAs) has increased with the aim of improving the resiliency of communication between bots and Command and Control (C&C) infrastructure. In this paper, we report on an effective DGA-detection algorithm based on a single network monitoring. The first step of the proposed method is the detection of a bot looking for the C&C and thus querying many automatically generated domains. The second phase consists on the analysis of the 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 the specific bot. Finally, clusters are analyzed in order to reduce false positives. The proposed solution has been evaluated over (1) an ad-hoc network where several known DGAs were injected and (2) the LAN of a company. In the first experiment, we deployed different families of malware employing several DGAs: all the malicious variants were detected by the proposed algorithm. In the real case scenario, the algorithm discovered an infected host in a 15-day-long experimental session, while producing a low false-positive rate during the same period.

dynamic generation of domains using a Domain Generation Algorithm (DGA), also known as domain-flux. With this technique, each bot, using a precalculated seed value known to the bot herder (e.g., the current date), automatically generates hundreds or thousands of pseudo-random domain names that represent candidate C&C domains. The bot sends DNS queries until it connects to the IP address associated to a resolved domain. The key advantage of this strategy is that even if one or more C&C domain names or IP addresses are identified and recovered, the bots will query the next set of automatically generated domains and it will eventually get the IP address of a relocated C&C server. DGA provides therefore a remarkable level of agility and a very resilient communication channel between bots and C&C, making it one of the most used technique in botnet control [6, 7, 8, 12, 15, 24, 33].

For these reasons, DGA detection is of crucial importance in cyber security. A number of different approaches to DGA-

MADRID ICCST2017 CARNAHAN

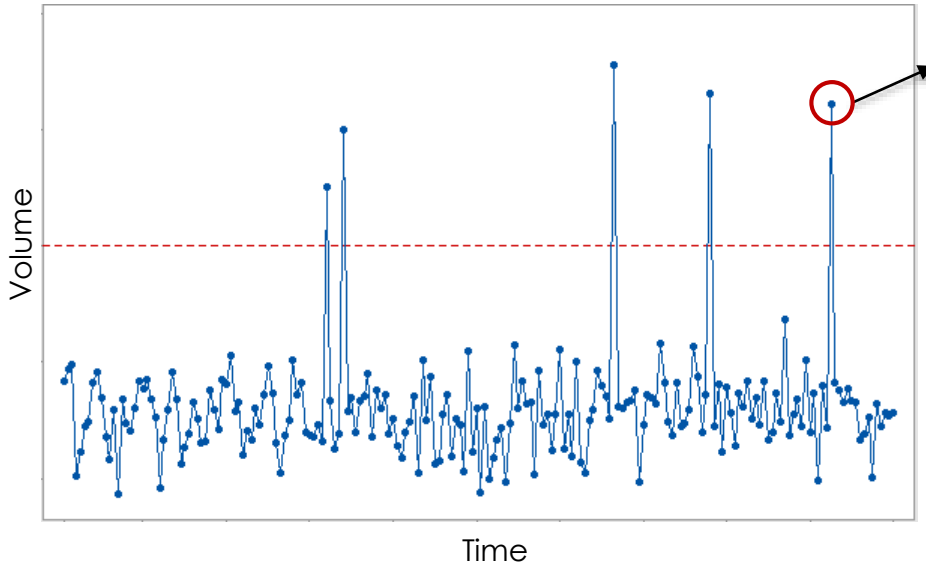
The 51st International Carnahan Conference on Security Technology
Madrid, Spain
October 23-26, 2017

IEEE

http://ieeexplore.ieee.org/document/8167790/

aramis: analitiche avanzate

Identificazione Domain Generation Algorithms (DGA)



Outlier detection

Clustering

Identificazione domini DGA

Malware **keylogger**
Rilevato il 19/01/2017

116 richieste non risolte
54 richieste risolte

Domini malevoli identificati

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

PROBABILITA' DI ANOMALIA
90,4%

3° Pilastro: fonti di Threat Intelligence

- Honeypot distribuite;
- intelligence sharing (**I_SOC di aramis**);
- iniezione di fonti OSINT;
- integrazione di nuovi schemi di attacco (**Malware Lab di aizoOn**);

aramis: fonti di Threat Intelligence

Malware Lab

Honeypot

aramis

OSINT

Dati della propria rete

Rilevazione automatica di **malware, attacchi, scansioni**

Identificazione di schemi, **correlazioni** e **pattern di attacco**

Clustering per evidenziare **variazioni di comportamento** dei dispositivi in rete

Analisi per identificare **attacchi e malware e comportamenti anomali**

Ranking e prioritizzazione

Tag e collection di **eventi correlati**

Feedback al sistema

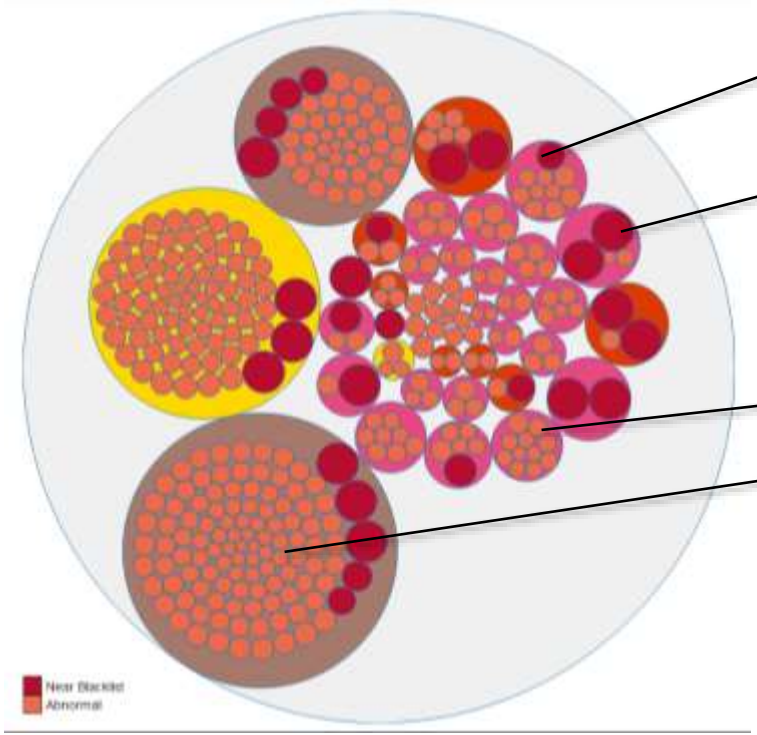
Miglioramento continuo

4° Pilastro: dashboard e visualizzazione cognitiva

- diagrammi **intuitivi**;
- disponibilità e navigazione semplificata dei dati a **supporto dell'analisi investigativa**;
- possibilità di definizione di eventi;
- invio **eventi verso SIEM** e **dashboard** esterne;
- **dashboard a più livelli** per organizzazioni complesse

aramis: dashboard e visualizzazione cognitiva

Analisi delle stringhe dei domini DNS



faceb000k.7host08.com

googlle.in

Simili ma non uguali agli originali

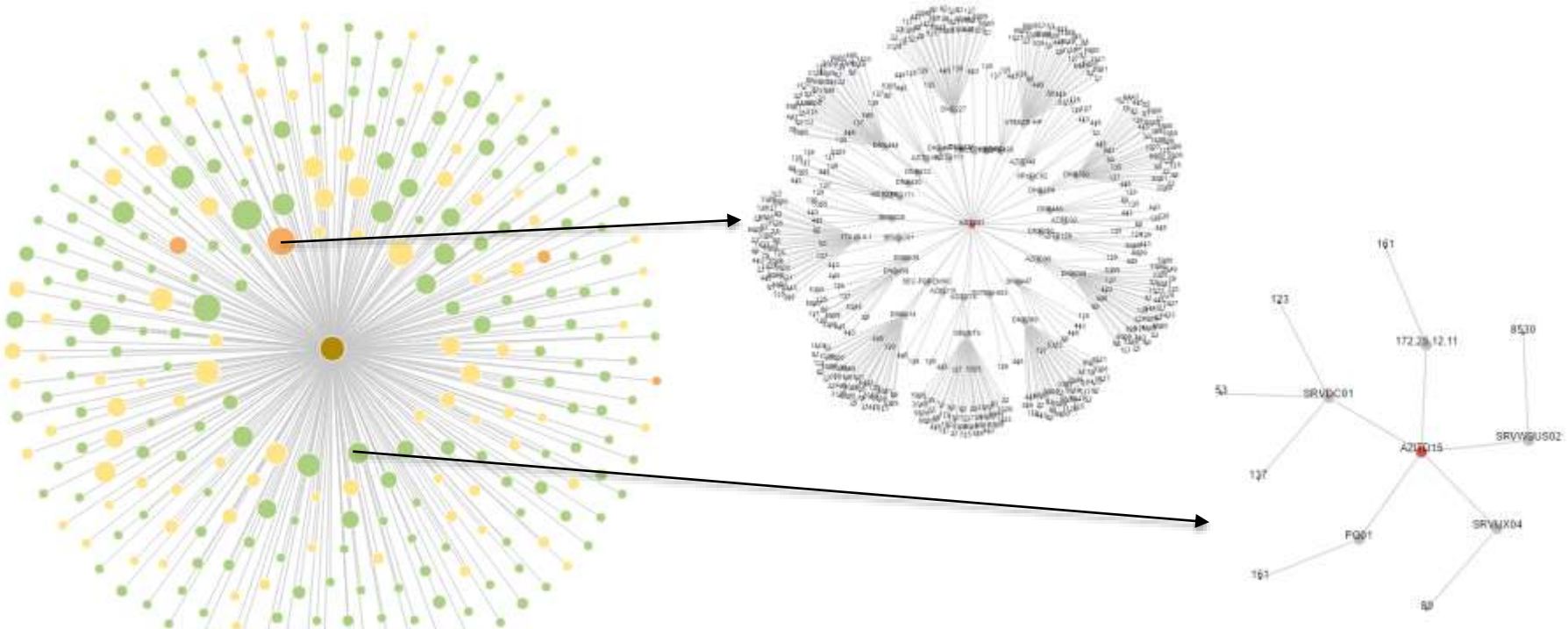
zn_1i8wqguxh5uzvbz.interceptics.com

5fe8a3d39a5226a54c2.activitylt.com

Domini random & pseudorandom

aramis: dashboard e visualizzazione cognitiva

Network analysis



aramis: la gestione della Sicurezza IT

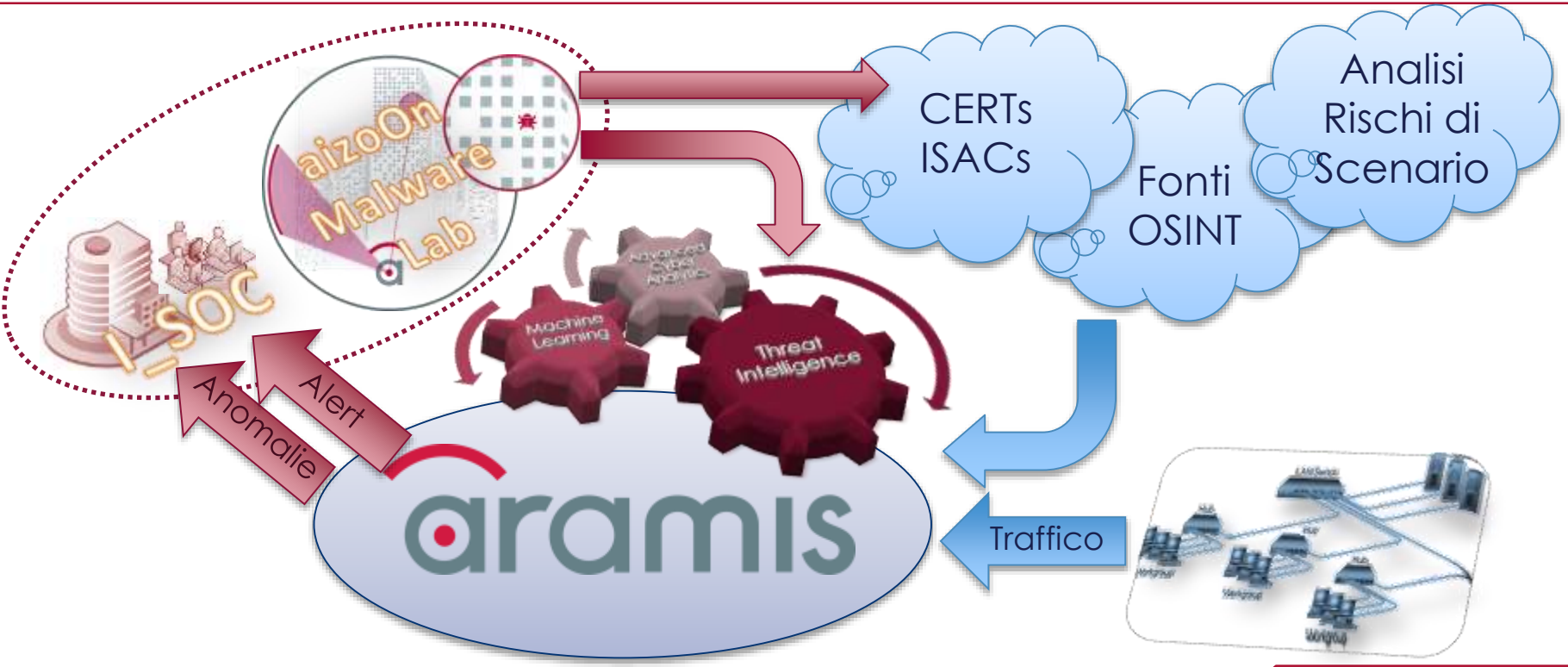
alcuni Processi e alcuni contesti

aizoon® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

aramis: Threat Hunting process

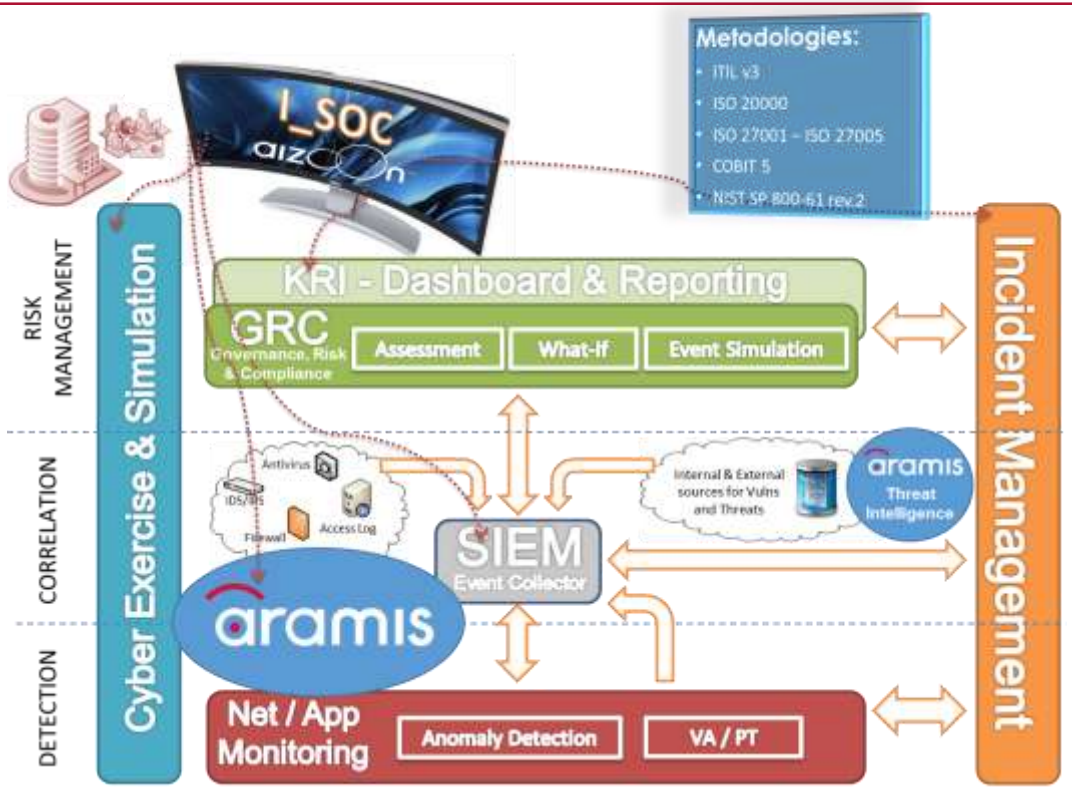
aramis: InfoSharing

Evoluzione del processo



Processi di Sicurezza IT

Il posizionamento di aramis



aramis, si colloca perfettamente all'interno di una visione globale della Sicurezza IT**.**
Si tratta di uno **strumento di detection avanzato** che si integra e **valorizza** gli altri strumenti «tradizionali» normalmente disponibili in ambienti complessi, quali **IPS/IDS e SIEM**.
Inoltre, la componente di **Threat Intelligence** di aramis fornisce un determinante **miglioramento qualitativo e quantitativo** alle altre sorgenti informative relativa a vulnerabilità e minacce note.

La dashboard di aramis

aizon® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

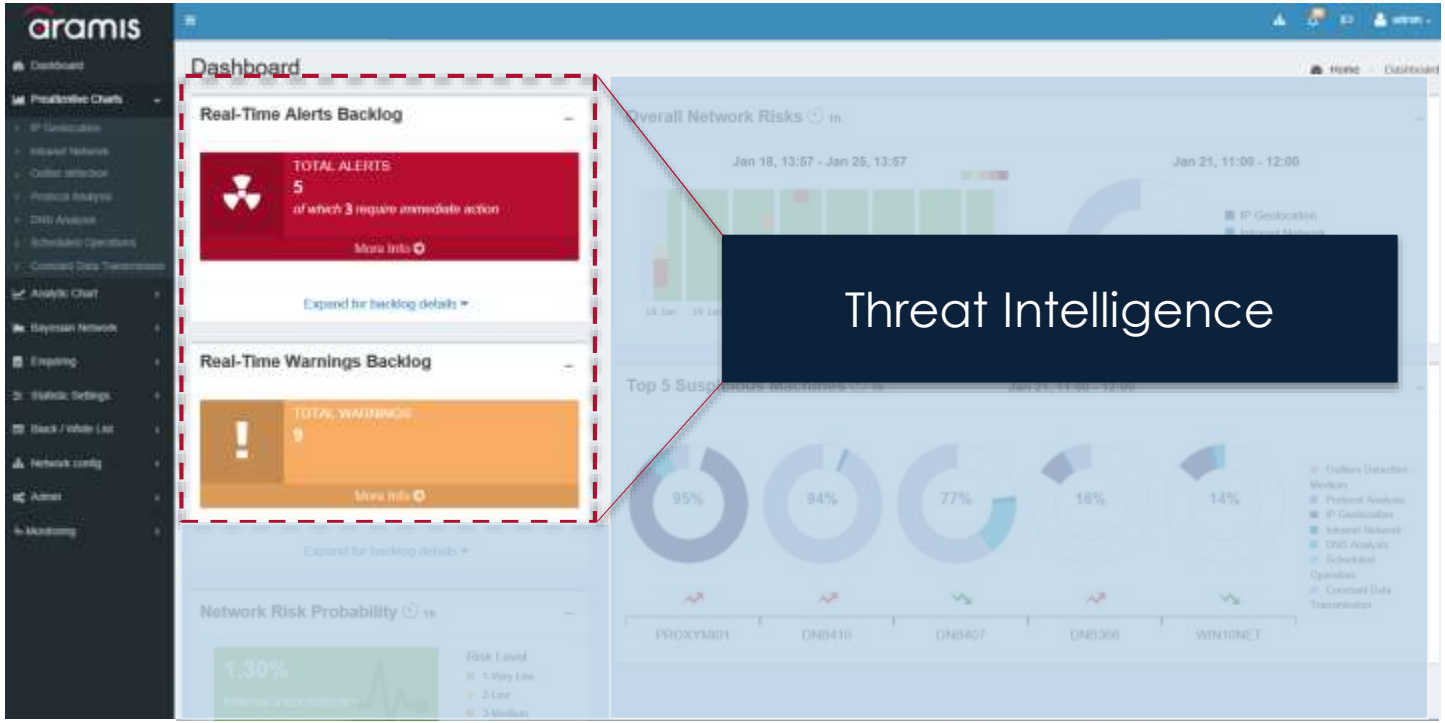
aramis: highlights

Dashboard

Cognitive Visualisation: «Visualizzazione multidimensionale dei dati in una singola immagine che consente di individuare la fonte di un problema in un tempo minore e di contribuire alla creazione di nuova conoscenza».

aramis: highlights

Dashboard – threat intelligence



Uso di fonti OSINT e threat intelligence proveniente dal **Malware Lab di aizoOn** per l'identificazione di IP e DNS malevoli,exit node TOR e signature di malware all'interno del traffico collezionato dalle sonde.

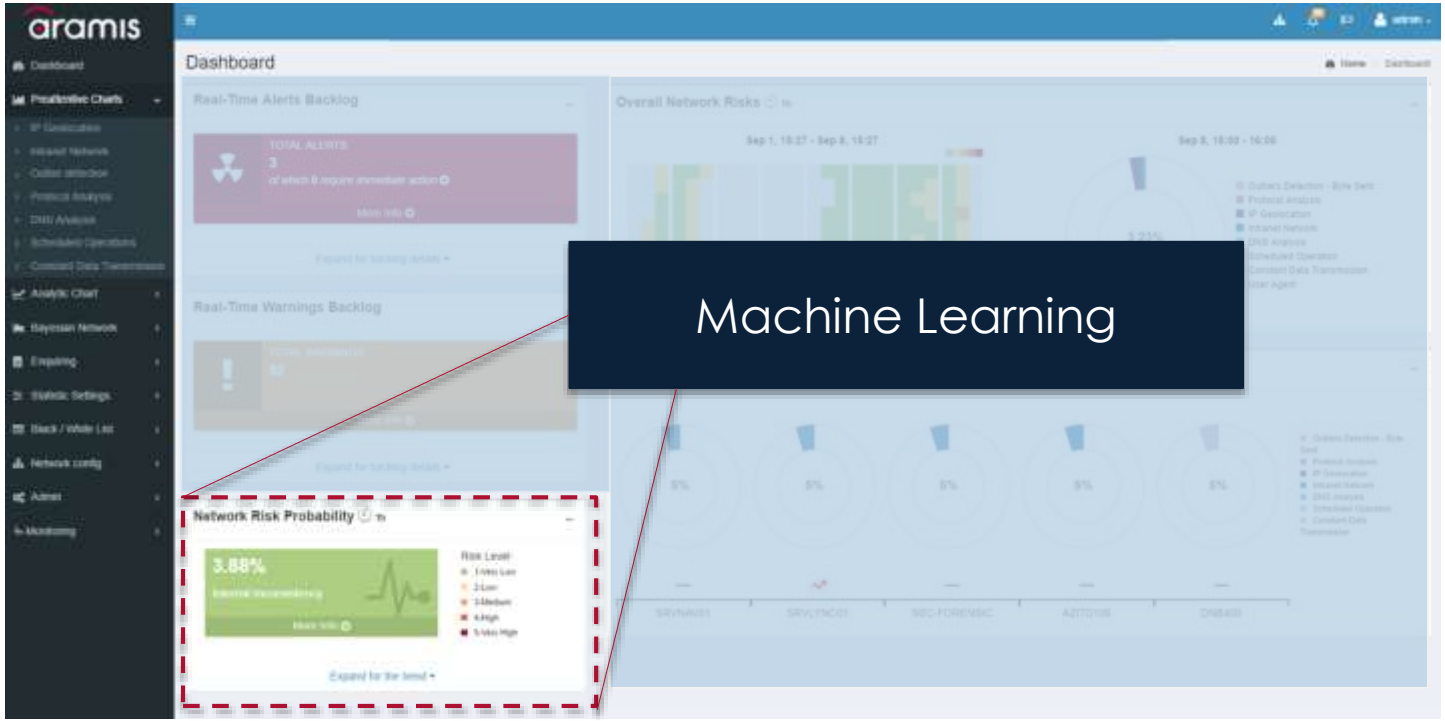
aramis: highlights

Dashboard – data mining

Allarmi generati dalle analitiche avanzate sviluppate dal team dei Data Scientists sulla base dell'esperienza degli esperti di security di aizoOn.

aramis: highlights

Dashboard – machine learning



Indice di inconsistenza, inteso come deviazione dal comportamento normale della rete, generato dagli algoritmi di analisi bayesiana nati dalla sinergia fra i team di Data Scientists e di Cyber Security di aizoOn.

aramis: highlights

Dashboard – Vista Multi-Site

Un caso di Successo

LEROY MERLIN
Voglia di Fare casa

aizoon® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

Leroy Merlin Italia

Leroy Merlin è leader in Italia e in Europa nella vendita di soluzioni per la casa presente con **48 grandi punti vendita** distribuiti su tutto il territorio nazionale.

Sulla base della strategia globale del Gruppo in ambito ICT Security, **Leroy Merlin Italia** ha stabilito di **adottare una soluzione di Network Security Monitoring** basata su algoritmi matematici innovativi e supportata da un **servizio gestito di monitoraggio**.
Per questo motivo **aizoOn**, dopo aver svolto un periodo di sperimentazione attiva della piattaforma **aramis** e dei servizi dell'**I_SOC di aizoOn** (Proof-of-Value – PoV), ha concordato la fornitura di una soluzione così strutturata:

- **Monitoraggio** attivo 8hx5gg con **security analyst dedicato** dell'HQ del Cliente, erogato dall'I_SOC tramite aramis
- Utilizzo di **sonde ADS** (aramis Distributed Sensor) in forma di **Virtual Appliance**, installate presso il Deposito e i Punti Vendita in Italia, attivabili «a rotazione» con finalità di detection e «cleansing» delle anomalie e degli eventuali malware presenti.
- **Raccolta** delle informazioni **statistiche** e di «healtiness» della rete distribuita WAN per finalità di **gestione e ottimizzazione** della stessa.

Leroy Merlin Italia

Risultati del servizio aramis di monitoraggio (circa 5.000 nodi-3 mesi)

- **5.108 diversi modelli matematici generati dal motore di machine learning** per il monitoraggio di:
  - **utenti e server della rete della sede principale**
  - **nodi di rete del magazzino principale**
  - **IP device distribuite in 4 negozi della catena**

- **2.260.000 indicatori di compromissione utilizzati** provenienti da 33 diverse fonti OSINT e dal Malware Lab di aizoOn

- **33 report/comunicazioni inviati al cliente**

connessioni raccolte
ed analizzate da aramis
Oltre 650 milioni

eventi generati dalle analitiche di aramis
40 milioni

~120 comportamenti sospetti analizzati dal team I_SOC

minacce comunicate al cliente

33

- 3 address scans
- 1 port scan
- 18 suspicious activities
- 2 misconfigurations
- 1 well-known IoC
- 1 unwanted application
- 3 black list domain
- 3 network hygene warning
- 1 scheduled operation

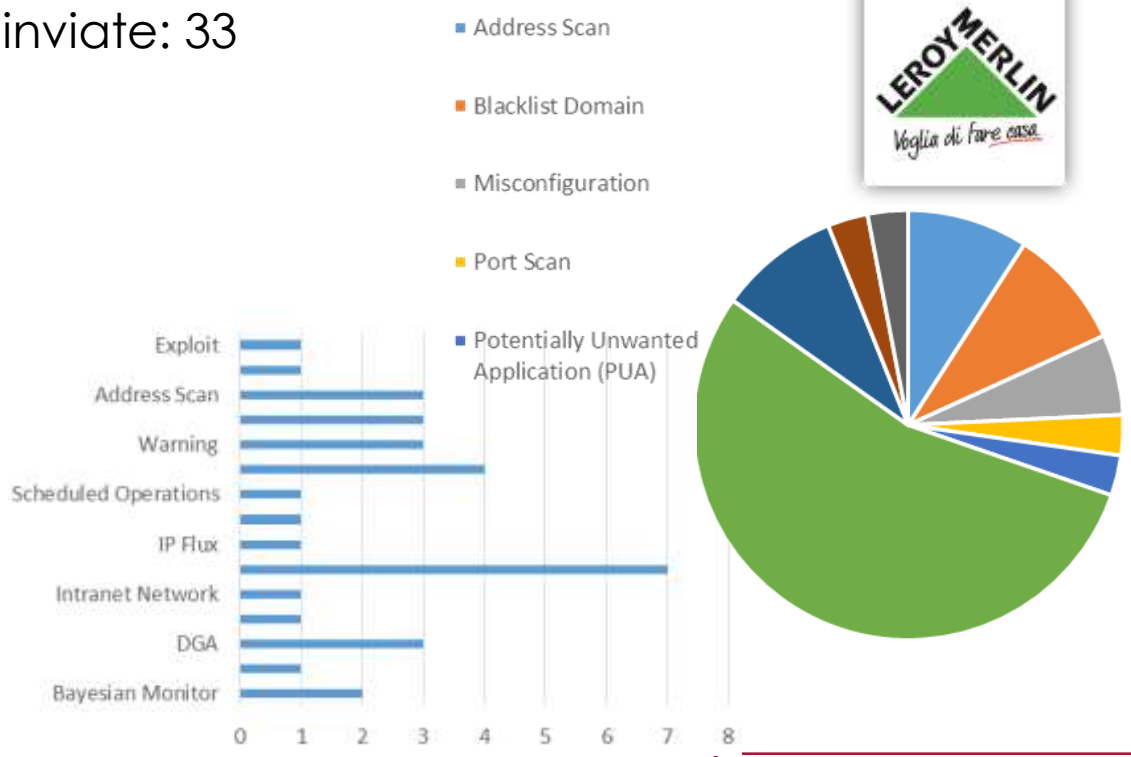
aizoOn AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

Leroy Merlin Italia

Risultati del servizio aramis di monitoraggio della rete

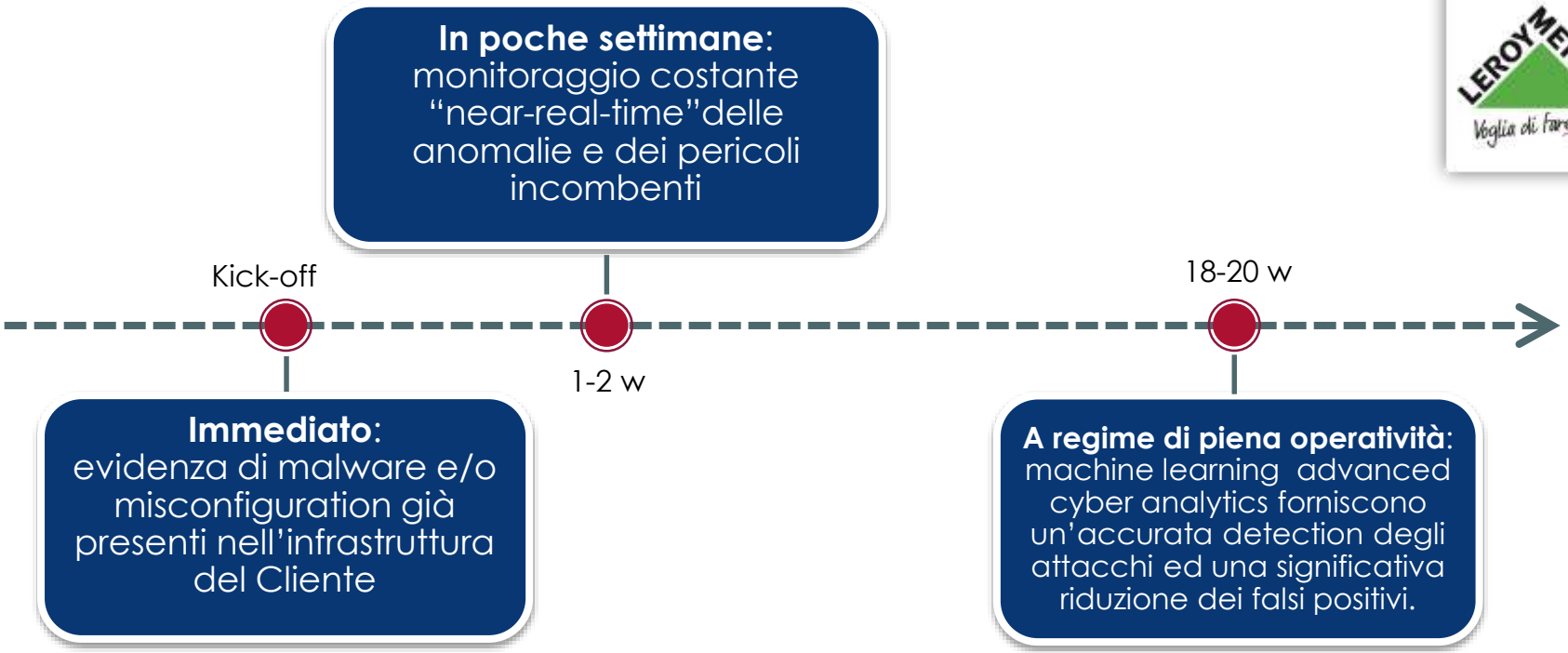
Totale report/comunicazioni inviate: 33

Mese	Nome Report	Categoria	Tipologia
Dicembre	Technical Summary	DGA	Suspicious Activity
Dicembre	Technical Summary	DGA	Suspicious Activity
Dicembre	Technical Summary	DGA	Suspicious Activity
Dicembre	Technical Summary	IP Geolocation	Suspicious Activity
Dicembre	Technical Summary	User Agent	Suspicious Activity
Dicembre	Technical Summary	User Agent	Suspicious Activity
Dicembre	Technical Summary	IoC	Blacklist Domain
Dicembre	Technical Summary	DNS Not Resolved	Suspicious Activity
Dicembre	Technical Summary	User Agent	Suspicious Activity
Dicembre	Technical Summary	User Agent	Suspicious Activity
Dicembre	Technical Summary	Warning	Address Scan
Dicembre	Technical Summary	IoC	Suspicious Activity
Dicembre	Technical Summary	IoC	Blacklist Domain
Dicembre	Technical Summary	IoC	Blacklist Domain
Dicembre	Technical Summary	IoC	Suspicious Activity
Dicembre	Technical Summary	Warning	Address Scan
Dicembre	Technical Summary	Intranet Network	Port Scan
Dicembre	Technical Summary	Constant Data Transmissio	Misconfiguration
Dicembre	Technical Summary	Scheduled Operations	Misconfiguration
Dicembre	Technical Summary	Bayesian Monitor	Suspicious Activity
Dicembre	Technical Summary	Bayesian Monitor	Suspicious Activity
Gennaio	email mercoledì 10/01/2018 11:43	Warning	Address Scan
Gennaio	Aramis_ _AnomalyReport_12012018	IP Flux	Potentially Unwanted Ap
Gennaio	email lu 08/01/2018 20:13	IoC	Suspicious Activity
Gennaio	email lu 22/01/2018 17:37	IoC	Suspicious Activity
Gennaio	Aramis_ _AnomalyReport_12012018	Potentially Unwanted App	Suspicious Activity
Gennaio	Aramis_ _AnomalyReport_25012018	Potentially Unwanted App	Suspicious Activity
Gennaio	Aramis_ _AnomalyReport_25012018	Potentially Unwanted App	Suspicious Activity
Gennaio	Aramis_ _AnomalyReport_29012019	Address Scan	Warning
Gennaio	Aramis_ _AnomalyReport_30012019	Address Scan	Warning
Febbraio	Aramis_ _AnomalyReport_30012029_2	Recurrent Connections	Scheduled Operations
Febbraio	Aramis_ tZN_AnomalyReport_07022018	Address Scan	Warning
Febbraio	email Venerdì 09/02/2018 10:07	Exploit	IOC



Leroy Merlin Italia

Benefit Delivery Timeline



Risultati percepiti dai Clienti di aramis

Miglioramento dell'awareness rispetto ai fenomeni ed agli eventi rilevanti che si verificano correntemente nell'infrastruttura di rete a causa di:

- configurazioni errate o variazioni inattese della topografia;
- azioni malevole deliberate da parte degli utenti (dipendenti o altri soggetti connessi in rete);
- azioni involontarie dei medesimi soggetti;
- violazioni di disposizioni regolamentari, policy e protocolli riferibili a standard o best practice di sicurezza.

Semplificazione e miglioramento nella detection delle anomalie, nonché riduzione dei falsi positivi.

Automatizzazione del processo di selezione degli eventi rilevanti e significativi rispetto al rumore di fondo.

Integrazione e miglioramento del servizio gestito di monitoraggio dello stato di sicurezza della rete IT.

Valorizzazione degli strumenti di IT Network Security già nella disponibilità degli utenti finali della piattaforma (SIEM, IPS/IDS, NGFW…)

Supporto alla revisione ed al miglioramento del processo di ICT Security.

Grazie!

Contatti:
www.aramisec.com
www.aizoongroup.com

aizoon® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING