aramis

Gabriele Liverziani

Roberto Obialero

Approccio Continuous Monitoring, Servizi SOC ed Intelligenza Artificiale, UN TRIO VINCENTE

ECS EUROPEAN CYBER SECURITY ORGANISATION

Gartner Cool Vendor 2016

aizoon® TECHNOLOGY CONSULTING

AUSTRALIA
EUROPE
USA

Verona 4/10/2018 | Security Summit CLUSIT

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

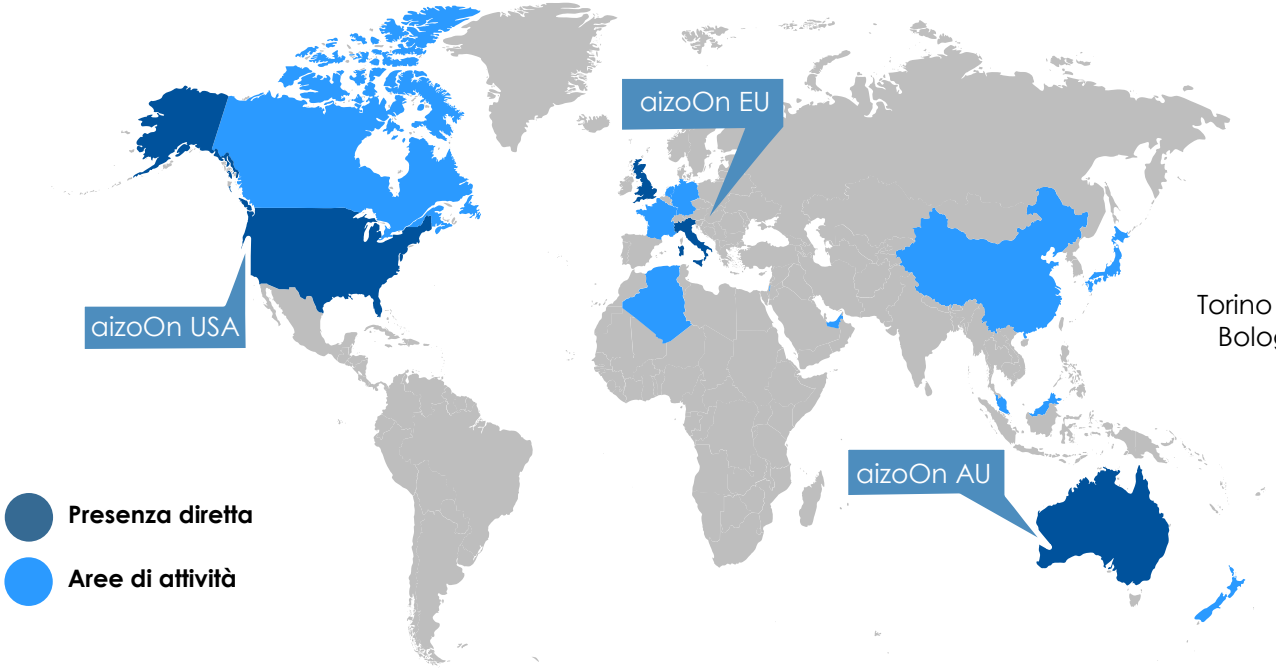
integriamo sinergicamente componenti di **tecnologia**, di **business** e di **innovazione** in grado di canalizzare le diverse dimensioni digitali in soluzioni innovative dedicate

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

Roberto Obialero

Cybersecurity & Data Protection Advisor
Delivery Unit Manager Risk & Compliance

Agenda dell'intervento

- Continuous Monitoring: analisi del contesto e delle minacce
- Continuous Monitoring benefits
- Le nuove frontiere
- Conclusioni

Prerequisiti organizzativi e tecnologici del Continuous Monitoring, ovvero …

Politica di Log Management

Sinergia tra diverse funzioni interne

Maturità Cybersecurity

Gestione delle vulnerabilità

Analisi dei rischi

Approccio orientato alla difes

Team dedicato alla gestione c

Commitment aziendale

SOC e Continuous Monitoring faccia a faccia con la Cybersecurity

Perchè questo titolo?

A chi si rivolge

Perché adottare processi e soluzioni di Continuous Monitoring?

Autori

Download

Altri lavori disponibili

https://iscmsoc.clusit.it/#/

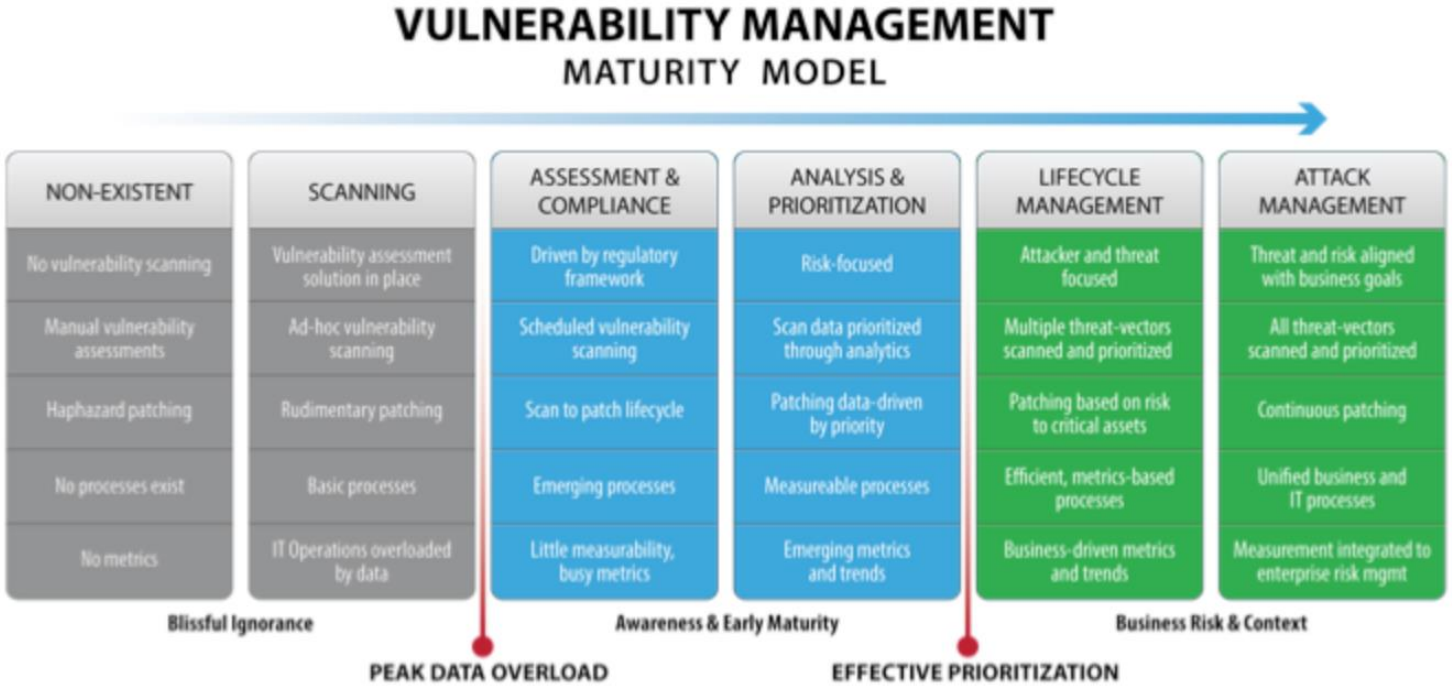
Minacce da cui difendersi: ENISA Top Threats

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	→	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	→	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	→	8. Botnets	↑	↓
9. Insider threat	→	9. Insider threat	→	→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	→	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

CM Benefit#1: Riduzione del livello di rischio

Dominio	Controllo
Security operations	A.12.04.01 Raccolta di log degli eventi (e monitoraggio)
	A.12.04.02 Protezione delle informazioni di log
	A.12.04.03 Log di amministratori e operatori
	A.12.05.01 Installazione del software sui sistemi di produzione
	A.12.06.01 Gestione delle vulnerabilità tecniche
	A.12.07.01 Controlli per l'audit dei sistemi informativi
Gestione degli incidenti di sicurezza	A.16.01.01 Gestione degli incidenti: Responsabilità e procedure
	A.16.01.02 Segnalazione degli eventi relativi alla sicurezza delle informazioni
	A.16.01.03 Segnalazione dei punti di debolezza relativi alla sicurezza delle informazioni
	A.16.01.04 Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni
	A.16.01.05 Risposta agli incidenti relativi alla sicurezza delle informazioni
	A.16.01.06 Apprendimento dagli incidenti relativi alla sicurezza delle informazioni
	A.16.01.07 Raccolta di evidenze
Conformità normativa	A.18.01.02 Diritti di proprietà intellettuale
	A.18.01.04 Privacy e protezione dei dati personali
	A.18.02.03 Verifica tecnica della conformità

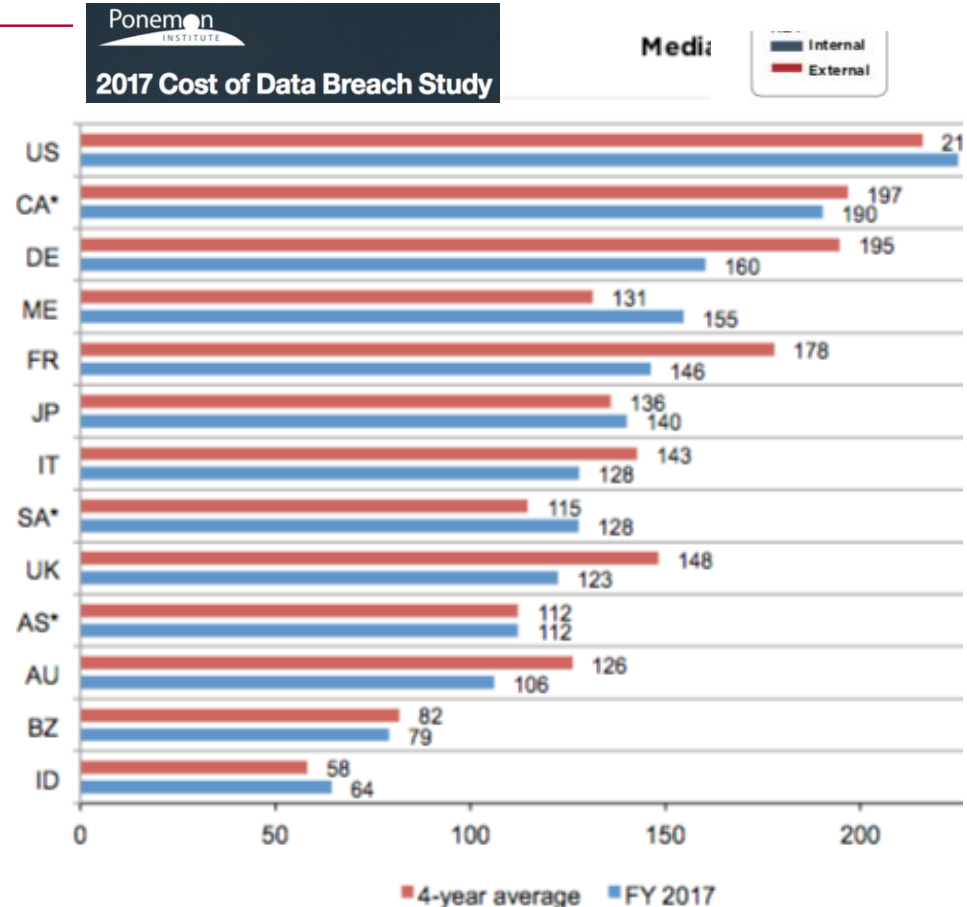
CM Benefit#2:
attivazione processo vulnerability management

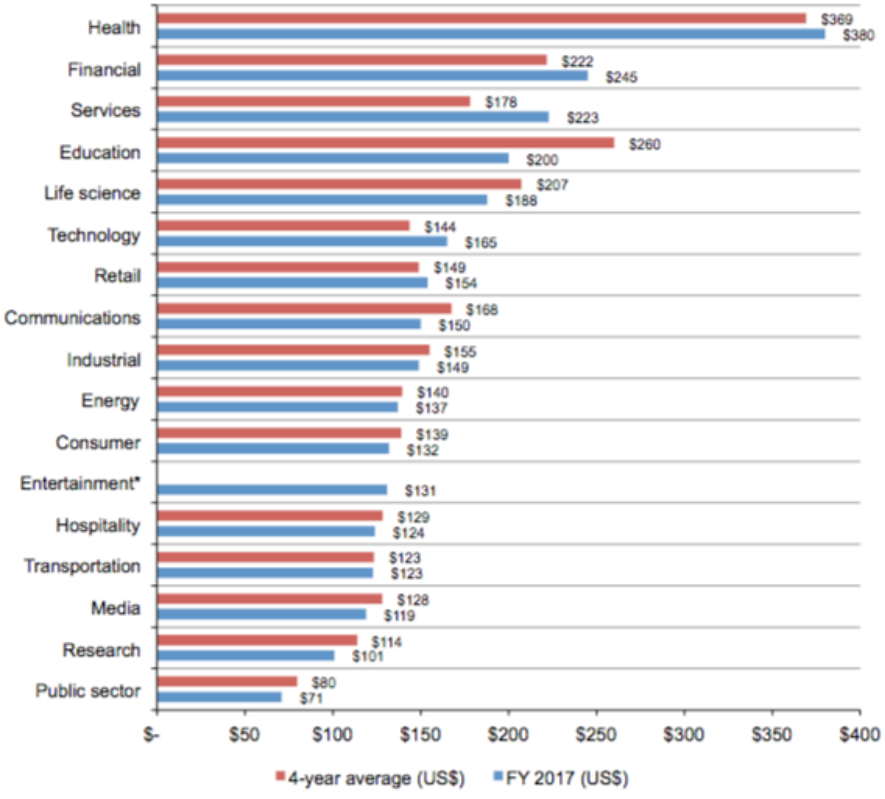


http://securitycigarsfud.com/wp-content/uploads/2014/08/MaturityModel.png

CM Benefit#3: Gestione eventi di sicurezza

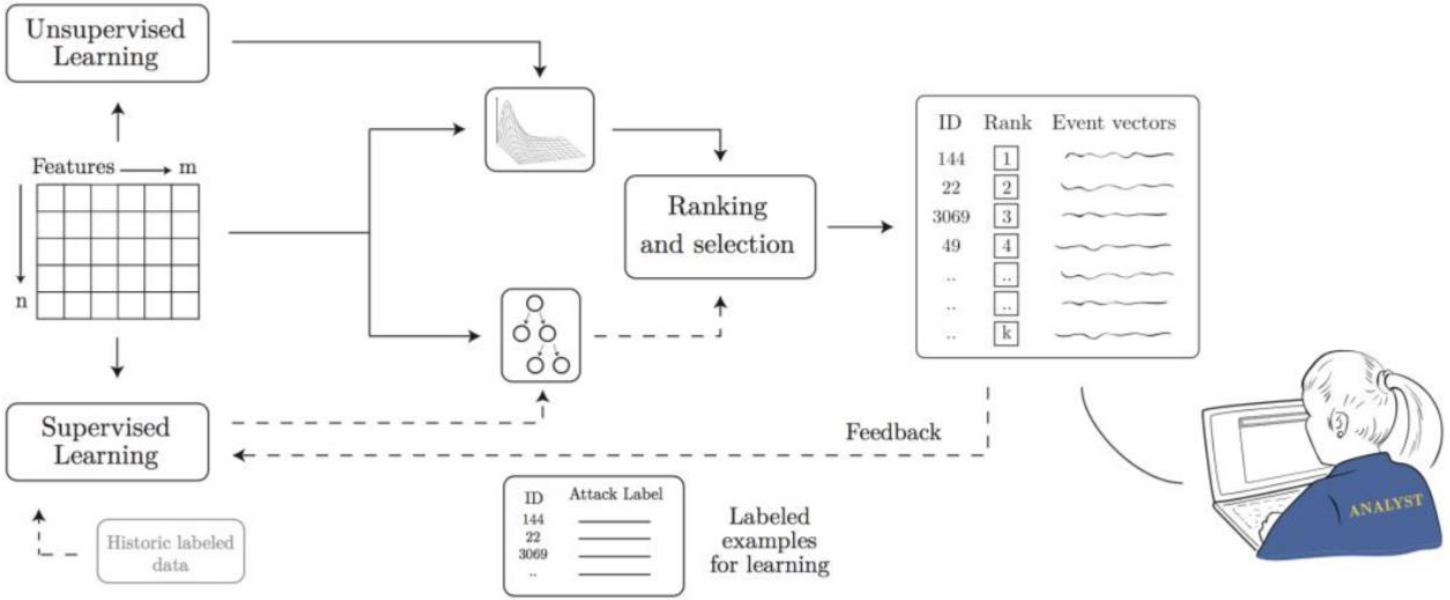
CM Benefit#4: riduzione dei tempi di reazione alle compromissioni e dei costi associati





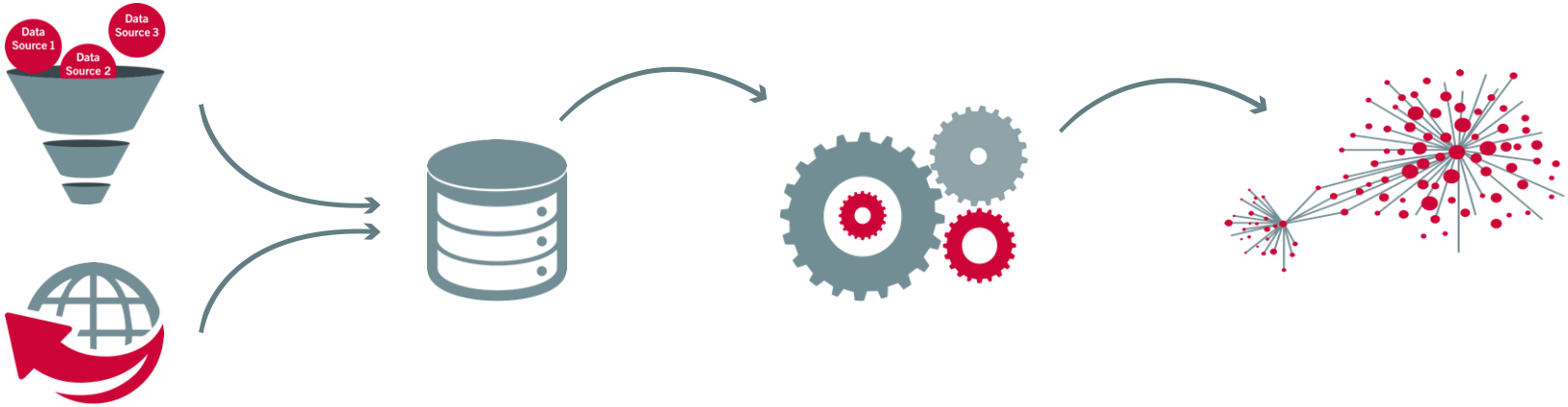
Data breach: dimensioni del fenomeno

Nuove frontiere: Machine Learning & Servizi SOC



https://people.csail.mit.edu/kalyan/AI2/

NBA workflow: collezione e trattamento dei dati
Rilevazione immediata dei pattern di attacco



COLLEZIONE

I sensori sono strategicamente posizionati nei diversi nodi all'interno della rete, a seconda della dimensione dei flussi e della quantità dei dati trasferiti. Ogni sensore raccoglie informazioni dal segmento di rete in cui è installato, le analizza in tempo reale e invia i risultati al server locale.

CORRELAZIONE

Sul server locale i dati ricevuti dalle sonde sono arricchiti con le informazioni provenienti da fonti OSINT e dalla threat intelligence generata dalle sorgenti proprietarie, utilizzando informazioni specifiche del Cliente.

ANALISI

Il sistema esegue costantemente due tipi di analisi sui dati raccolti:
Modulazione continua delle analitiche sulla base dell'evoluzione del rischio dinamicamente rilevato.
Analisi, tramite il motore di intelligenza artificiale, del comportamento di ogni singolo nodo della rete per evidenziare anomalie comportamentali.

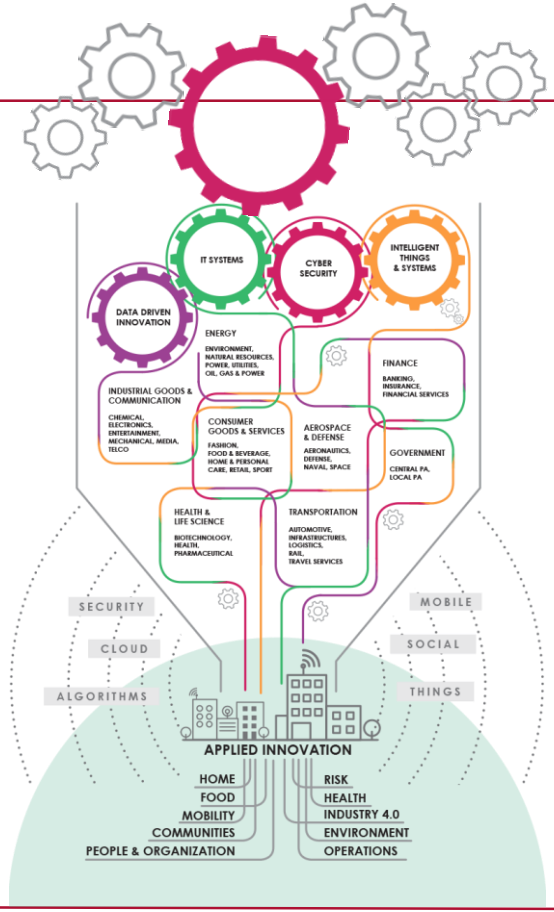
VISUALIZZAZIONE

Le informazioni sono rappresentate nella dashboard con grafiche di «cognitive visualisation», molto efficaci per evidenziare minimi scostamenti da schemi ripetitivi. Tali grafiche, grazie a funzionalità di zoom e drill-down sui dati, sono un potente strumento nelle mani degli l'analisti per l'identificazione e l'analisi degli allarmi.

la nostra soluzione: aramis

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.

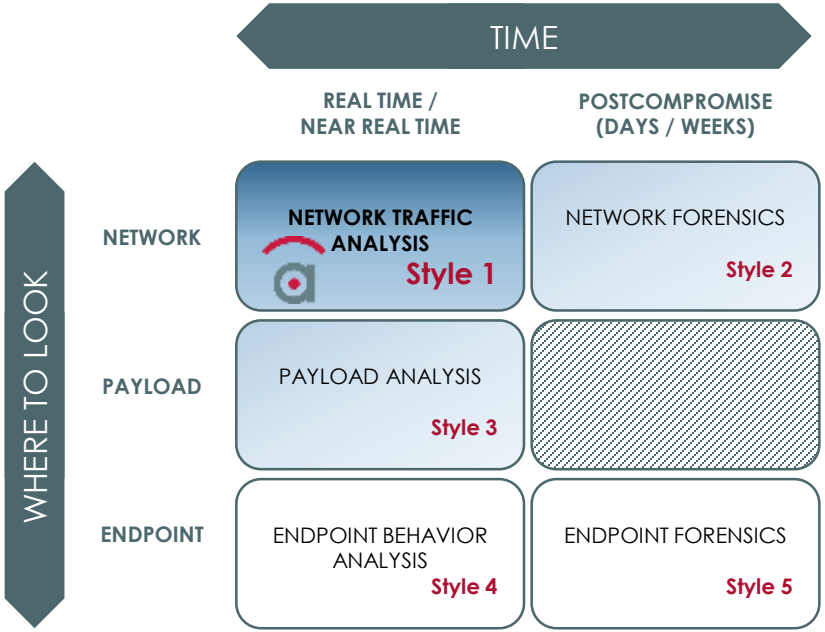
aramis, network security monitoring

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.

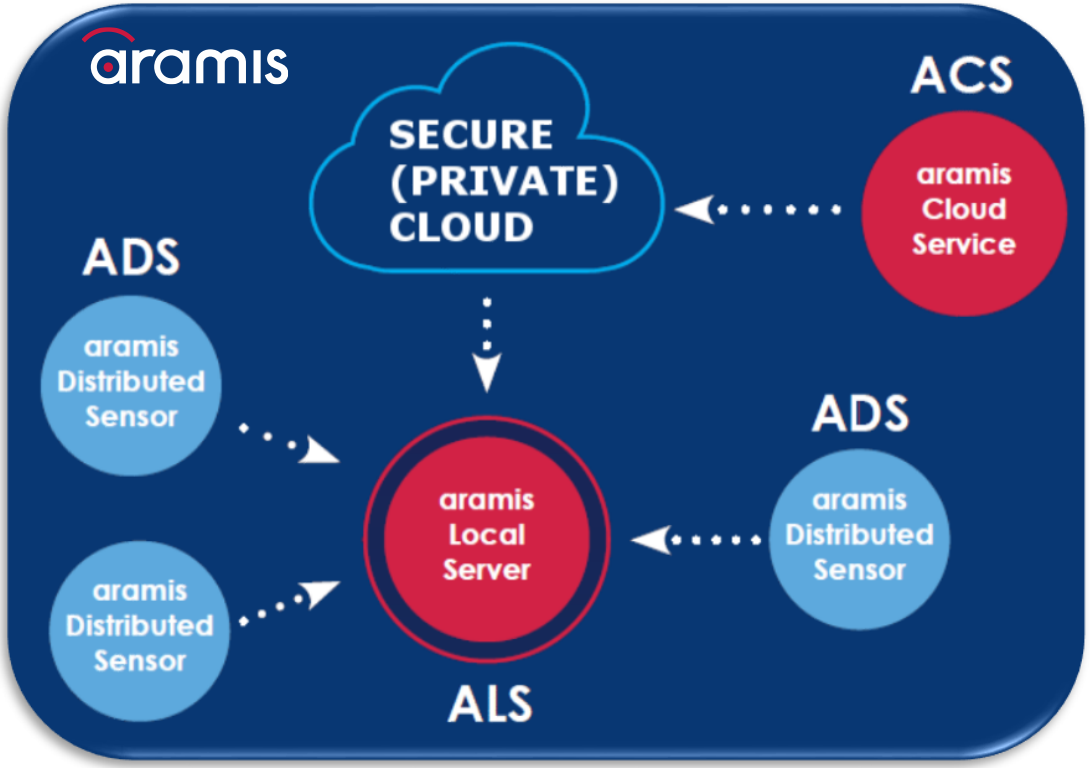
Il **posizionamento di aramis** trova riscontro nell'analisi di **Gartner "Five Styles of Advanced Threat Defense"** [L. Orans, J. D'Hoinne – 2013, 2016] **nello style 1**.

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



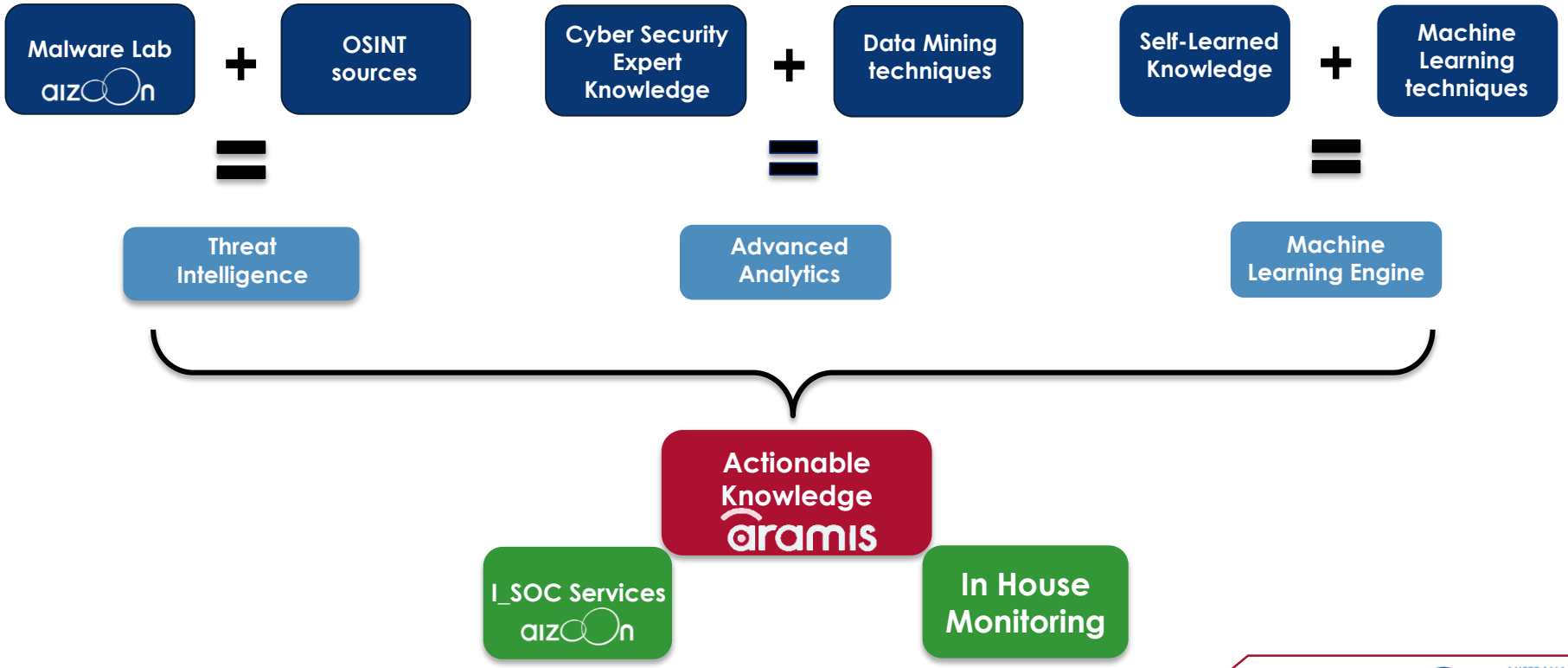
GARTNER (August 2013, June 2016) - Five Styles of Advanced Threat Defense - "Lawrence Orans, Jeremy D'Hoinne"

aramis architecture



The aramis approach to security monitoring

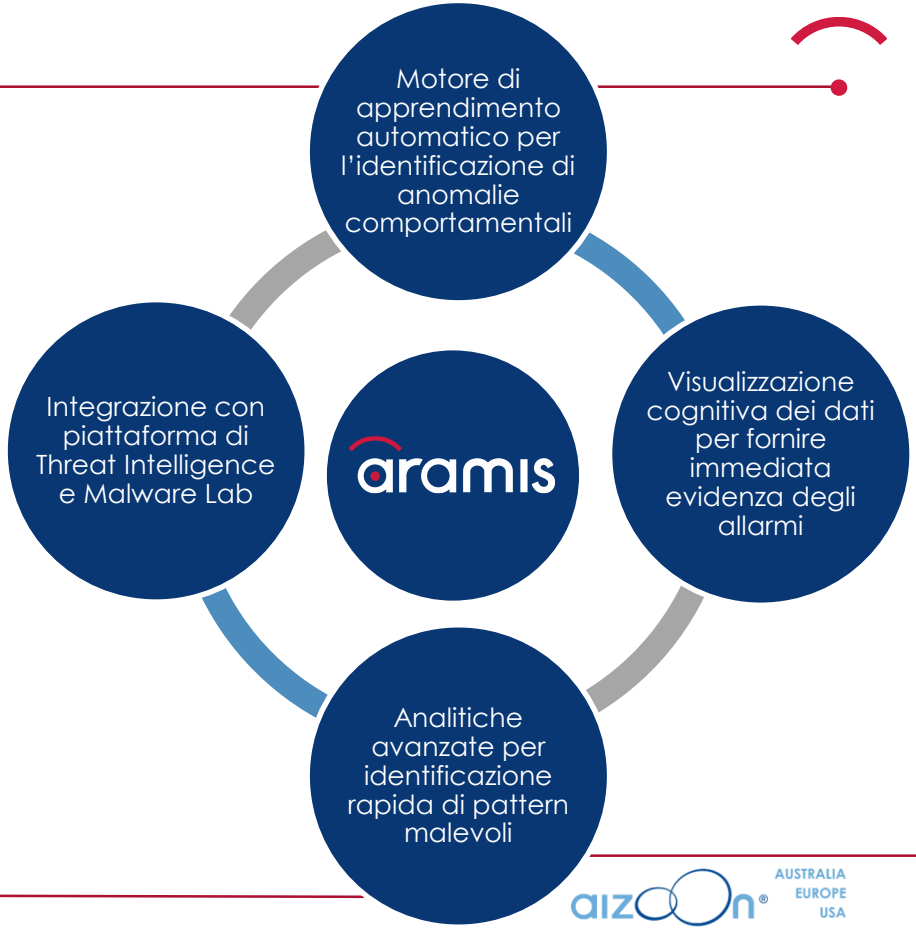
Machine learning, advanced analytics and threat intelligence



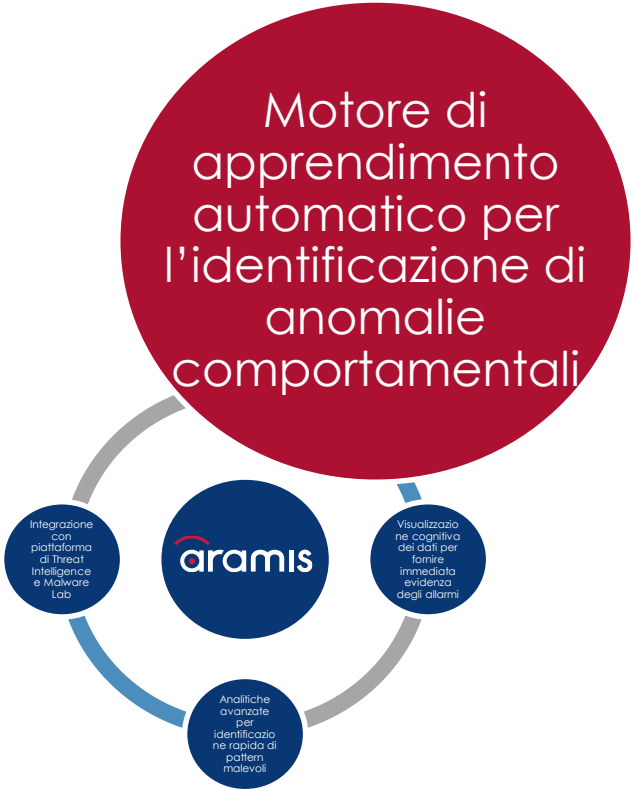
aramis: i 4 pilastri

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

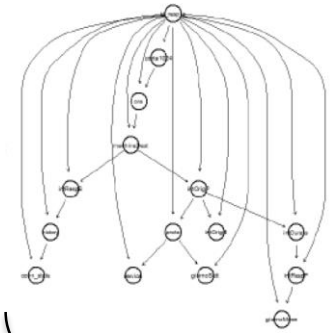


- analisi di grandi quantità di dati in «near real-time»;
- modelli matematici efficaci;
- rimozione del rumore di fondo;
- evoluzione continua degli algoritmi.

aramis: machine learning

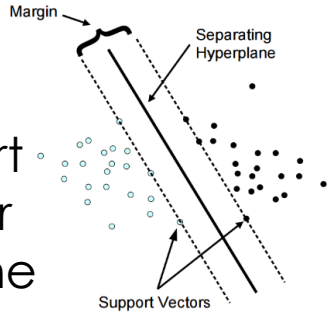
Riduzione del rumore di fondo

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

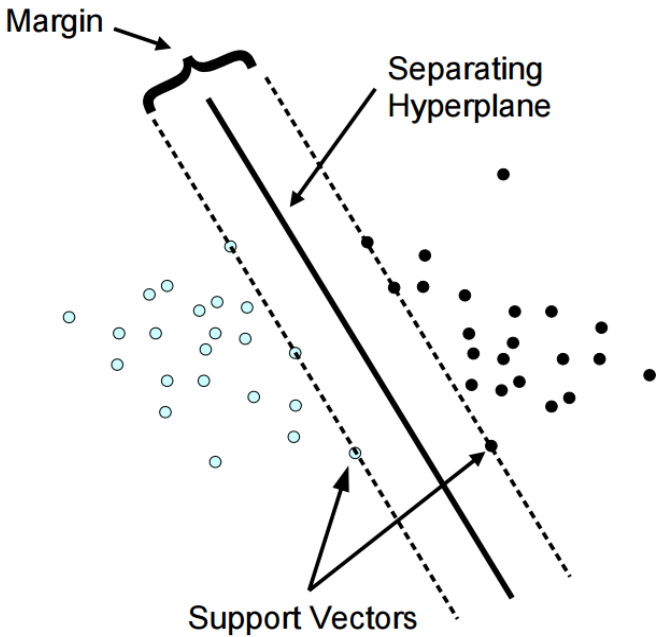
Global_srv_model

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:

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

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

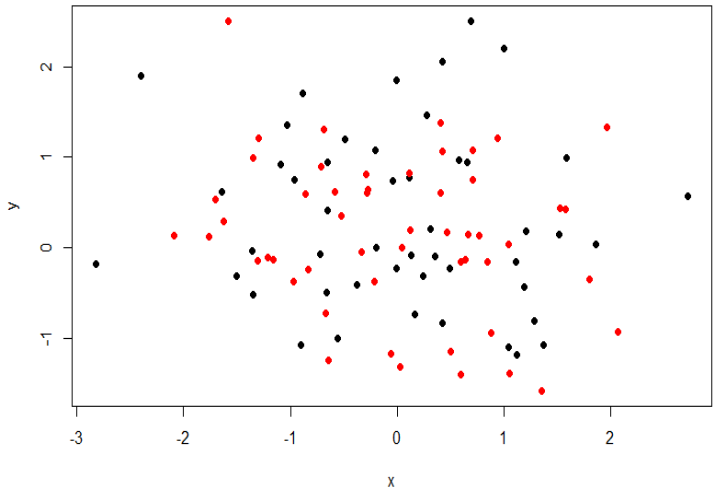
Minimizzazione:

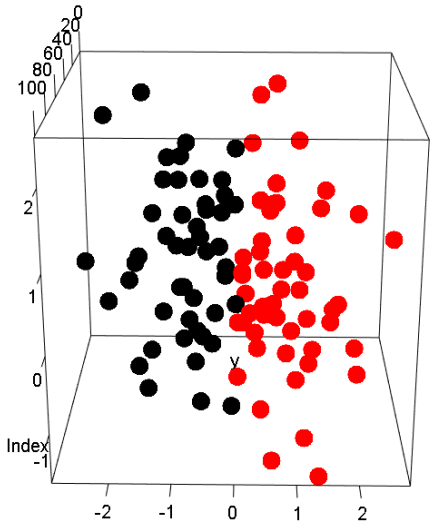
$$\min_{\boldsymbol{w},b} \quad \frac{\|\boldsymbol{w}\|^2}{2}$$

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

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

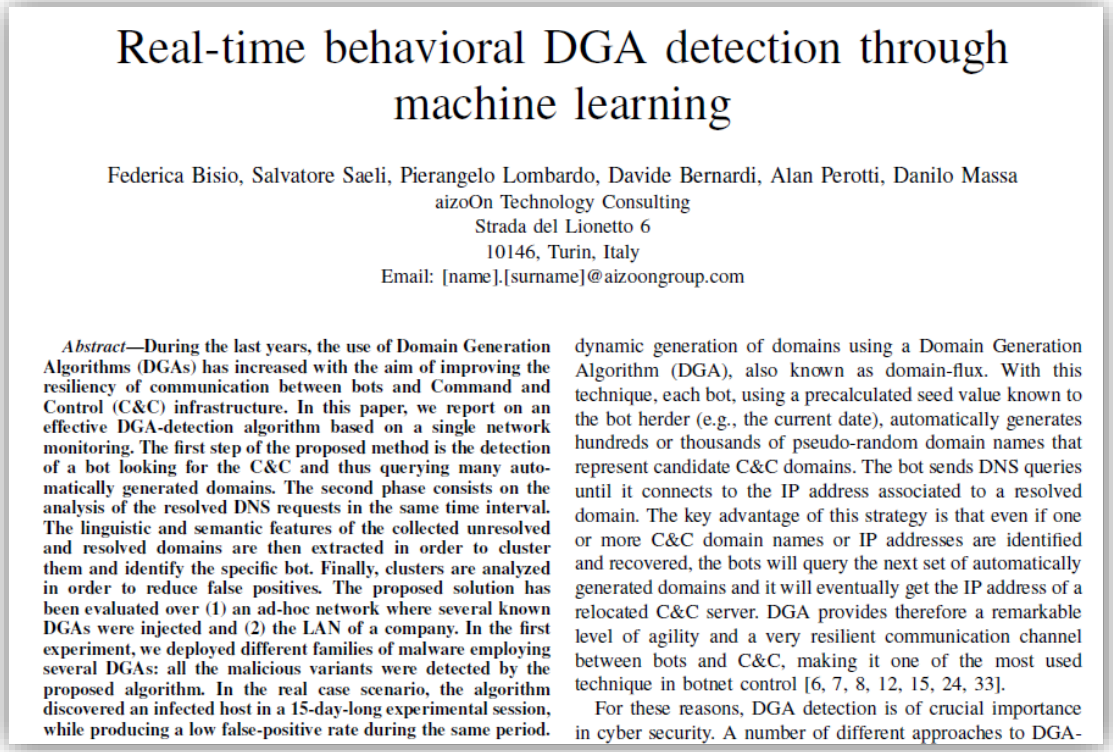
2° Pilastro: analitiche avanzate

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

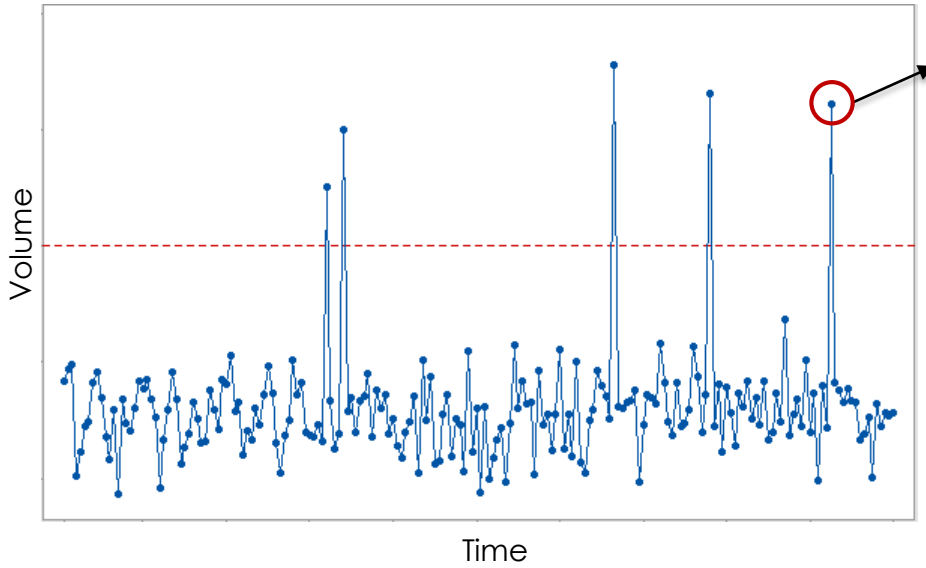
The 51st International Carnahan Conference on Security Technology
Madrid, Spain
October 23-26, 2017

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

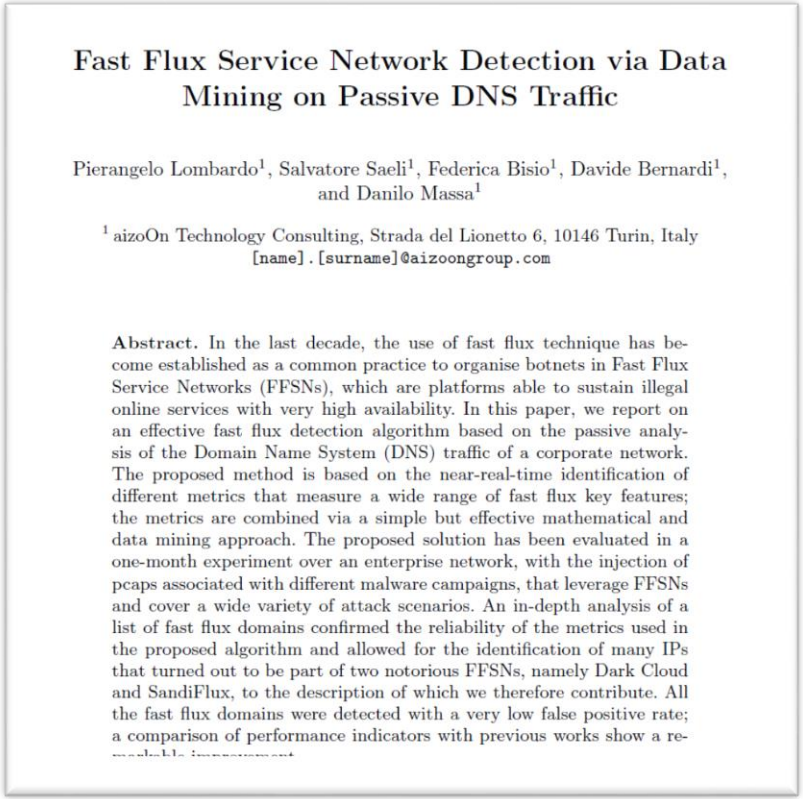
Domini malevoli identificati

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

PROBABILITA' DI ANOMALIA
90,4%

IP-Flux research

aizoOn at ISC 2018



Fast Flux Service Network Detection via Data Mining on Passive DNS Traffic

Pierangelo Lombardo[1], Salvatore Saeli[1], Federica Bisio[1], Davide Bernardi[1], and Danilo Massa[1]

[1] aizoOn Technology Consulting, Strada del Lionetto 6, 10146 Turin, Italy
[name].[surname]@aizoongroup.com

Abstract. In the last decade, the use of fast flux technique has become established as a common practice to organise botnets in Fast Flux Service Networks (FFSNs), which are platforms able to sustain illegal online services with very high availability. In this paper, we report on an effective fast flux detection algorithm based on the passive analysis of the Domain Name System (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. The proposed solution has been evaluated in a one-month experiment over an enterprise network, with the injection of pcaps associated with different malware campaigns, that leverage FFSNs and cover a wide variety of attack scenarios. An in-depth analysis of a list of fast flux domains confirmed the reliability of the metrics used in the proposed algorithm and allowed for the identification of many IPs that turned out to be part of two notorious FFSNs, namely Dark Cloud and SandiFlux, to the description of which we therefore contribute. All the fast flux domains were detected with a very low false positive rate; a comparison of performance indicators with previous works show a re-

21st Information Security Conference

ISC 2018

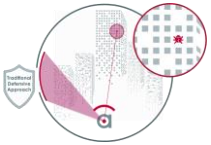
The 21st Information Security Conference
Guildford, UK
September 9-12, 2018

Springer

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

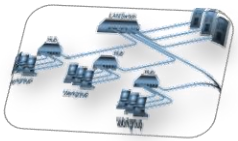


Malware Lab

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

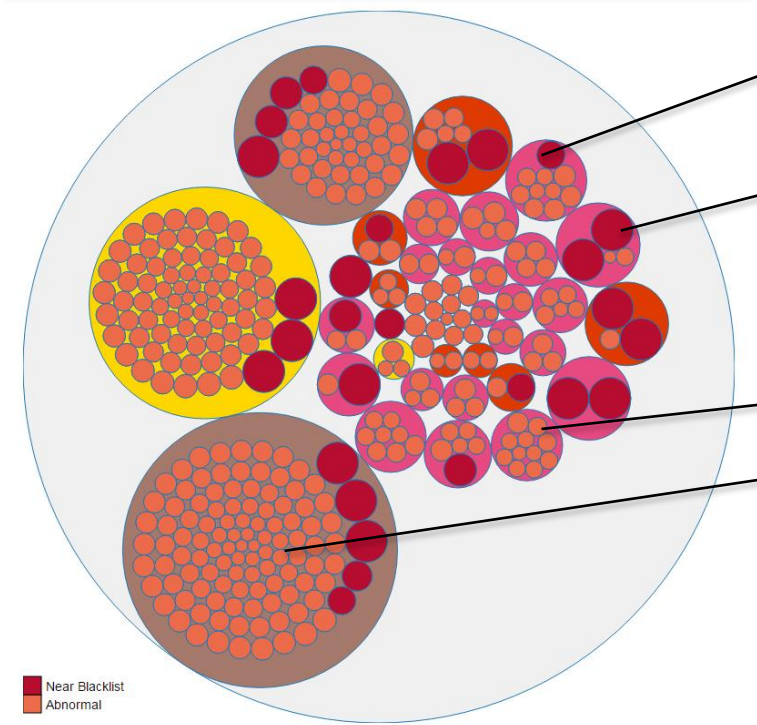
Miglioramento continuo

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

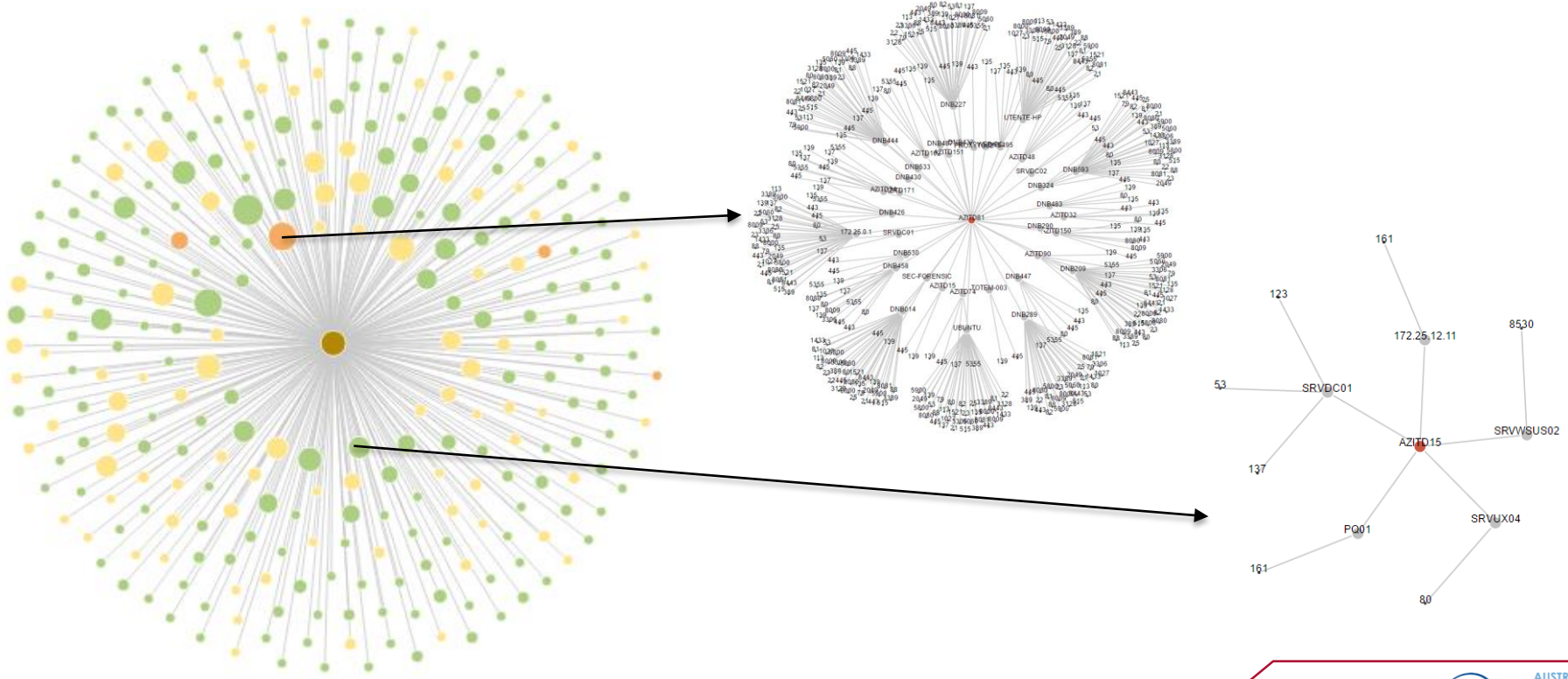
zn_1i8wqguxh5uzvbz.interceptics.com

5fe8a3d39a5226a54c2.activitylt.com

Domini random & pseudorandom

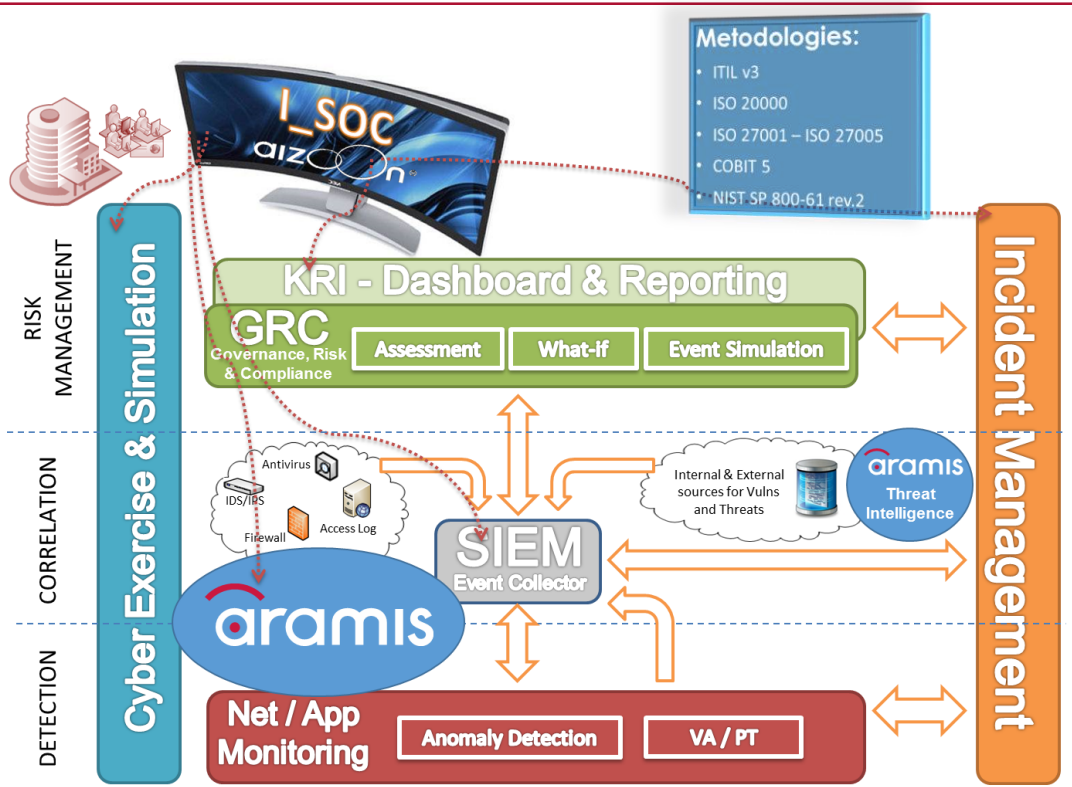
aramis: dashboard e visualizzazione cognitiva

Network analysis



Processi di Sicurezza IT

Il posizionamento di aramis

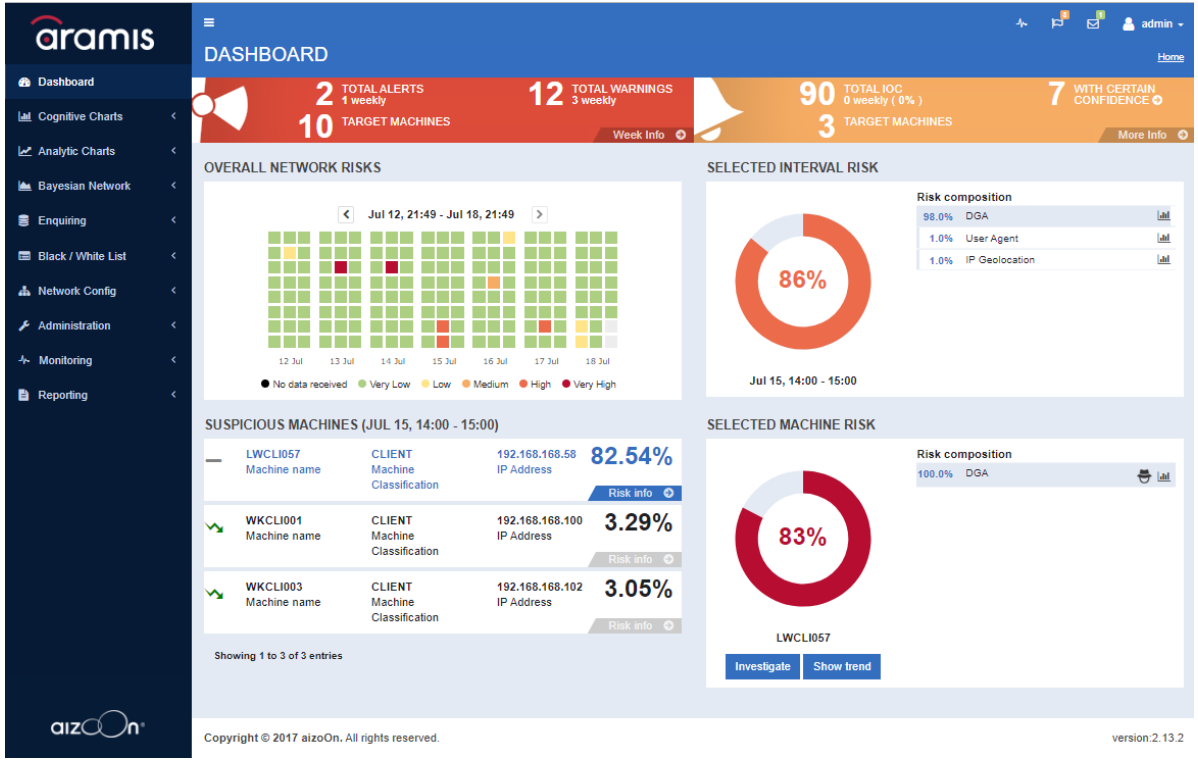


aramis, si colloca perfettamente all'interno di una visione globale della Sicurezza IT.
Si tratta di uno **strumento di detection avanzato** che si integra e **valorizza** gli altri strumenti «tradizionali» normalmente disponibili in ambienti complessi, quali **IPS/IDS e SIEM**.
Inoltre, la componente 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

aramis: highlights

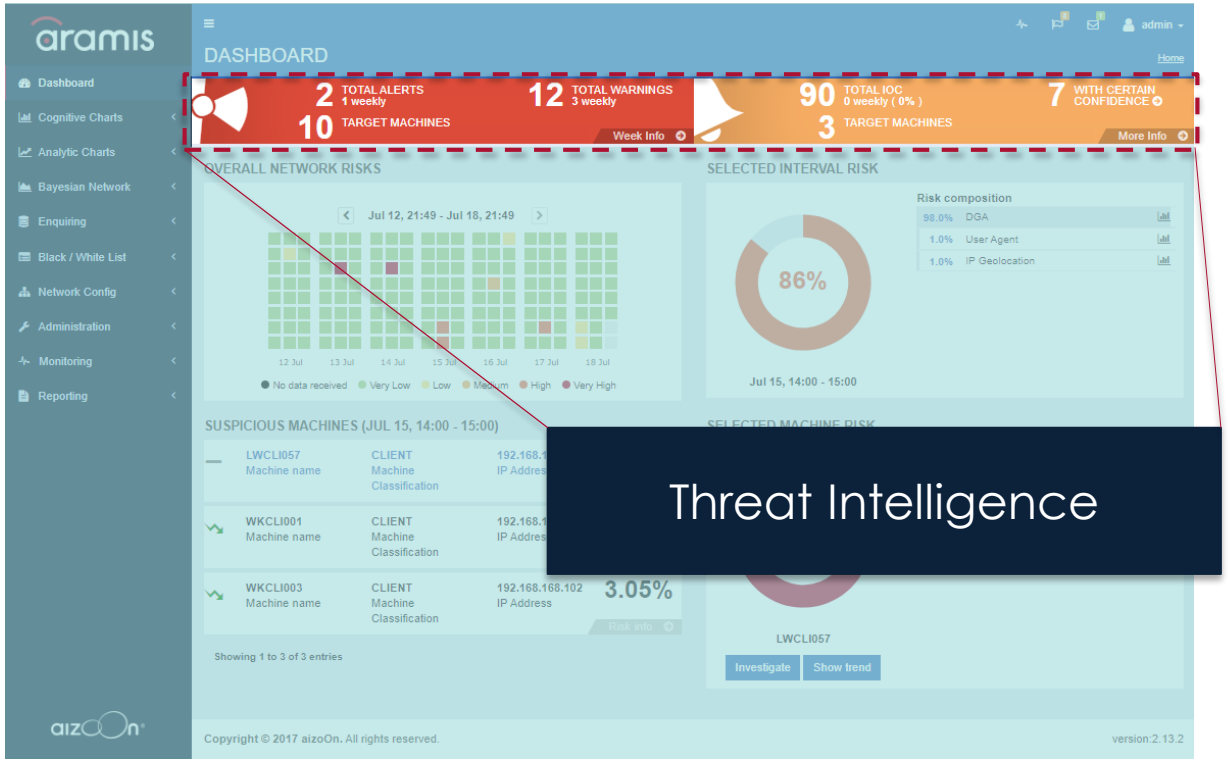
Dashboard



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

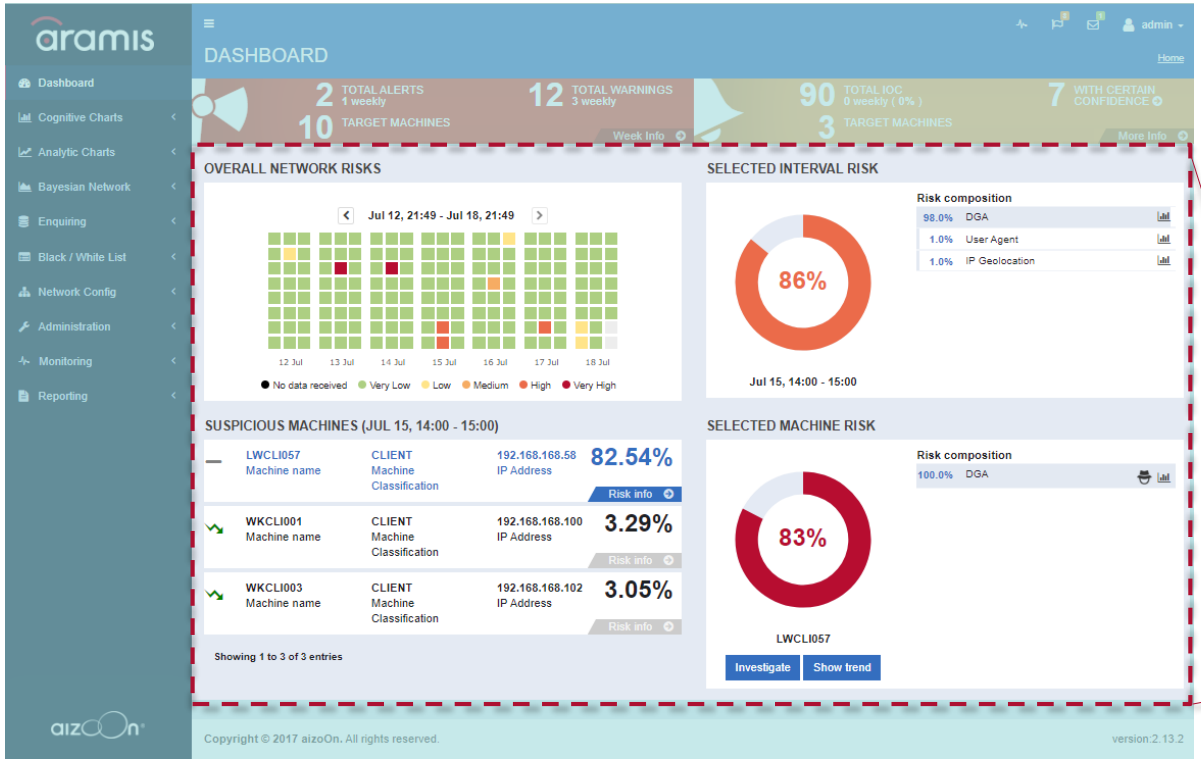
Dashboard – threat intelligence



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

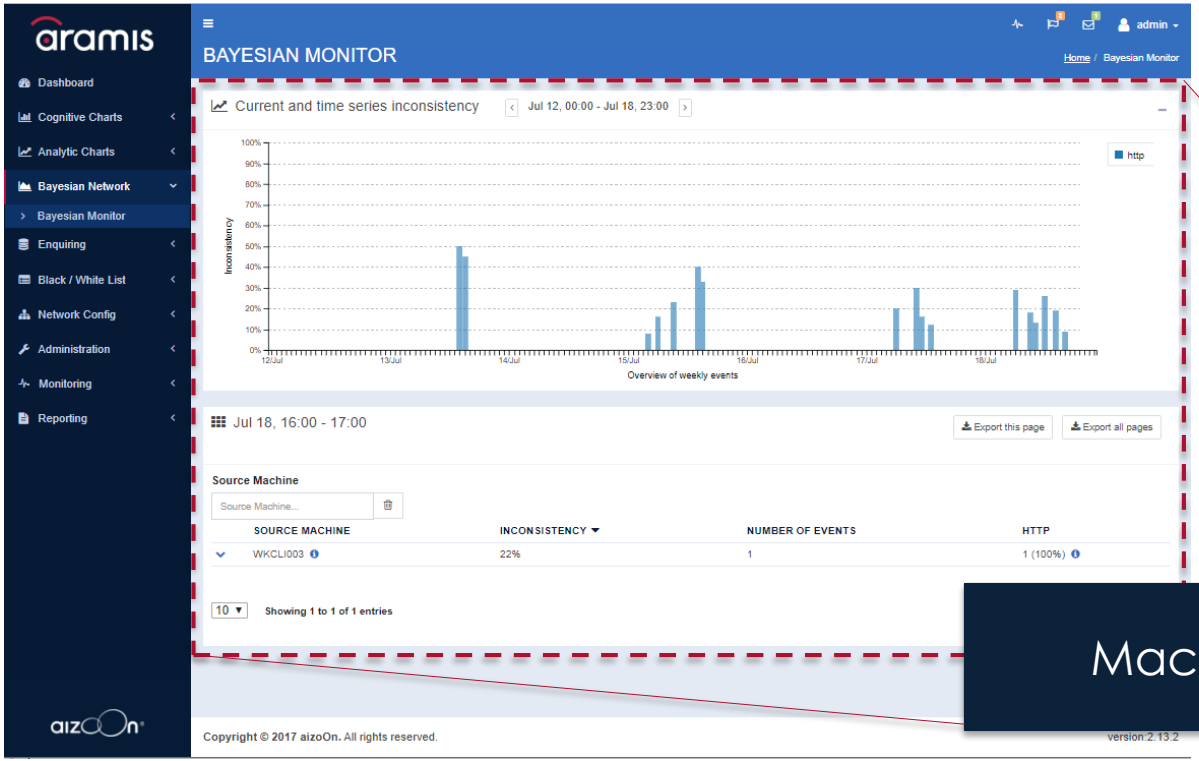


Allarmi generati dalle **analitiche avanzate** sviluppate dal team dei Data Scientists sulla base dell'esperienza degli esperti di security di aizoOn.

Data mining

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.

Machine Learning

aramis: highlights

Dashboard – Vista Multi-Site

Alcuni casi di Successo

AUSTRALIA
EUROPE
USA

aizon®
TECHNOLOGY CONSULTING

USE CASE 1 - Multinazionale ambito automotive

Risultati del servizio aramis di monitoraggio (circa 2.000 nodi-6 mesi)

- **719 diversi modelli matematici generati dal motore di machine learning** per il monitoraggio di:
  - **utenti e server della rete di una porzione della sede principale**
- **2.260.000 indicatori di compromissione utilizzati** provenienti da 33 diverse fonti OSINT e dal Malware Lab di aizoOn
- **11 report/comunicazioni inviati al cliente**

connessioni raccolte ed analizzate da aramis
Oltre 3,5 miliardi di connessioni

eventi generati dalle analitiche di aramis
17 milioni

95 comportamenti sospetti analizzati dal personale I_SOC

minacce comunicate al cliente

11

- 2 port scan
- 5 suspicious activity
- 1 malware
- 1 black list IP
- 1 network hygene warning
- 1 address scan

USE CASE 2 - Multinazionale della Grande Distribuzione

Azienda leader in Italia e in Europa nella vendita retail di soluzioni per la casa presente con oltre **50 grandi punti vendita** distribuiti su tutto il territorio nazionale.

Sulla base della strategia globale del Gruppo in ambito ICT Security, l'Azienda 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 Magazzino Principale 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.

USE CASE 2

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 di connessioni

eventi generati dalle analitiche di aramis
40 milioni

~100 comportamenti sospetti analizzati dal team I_SOC

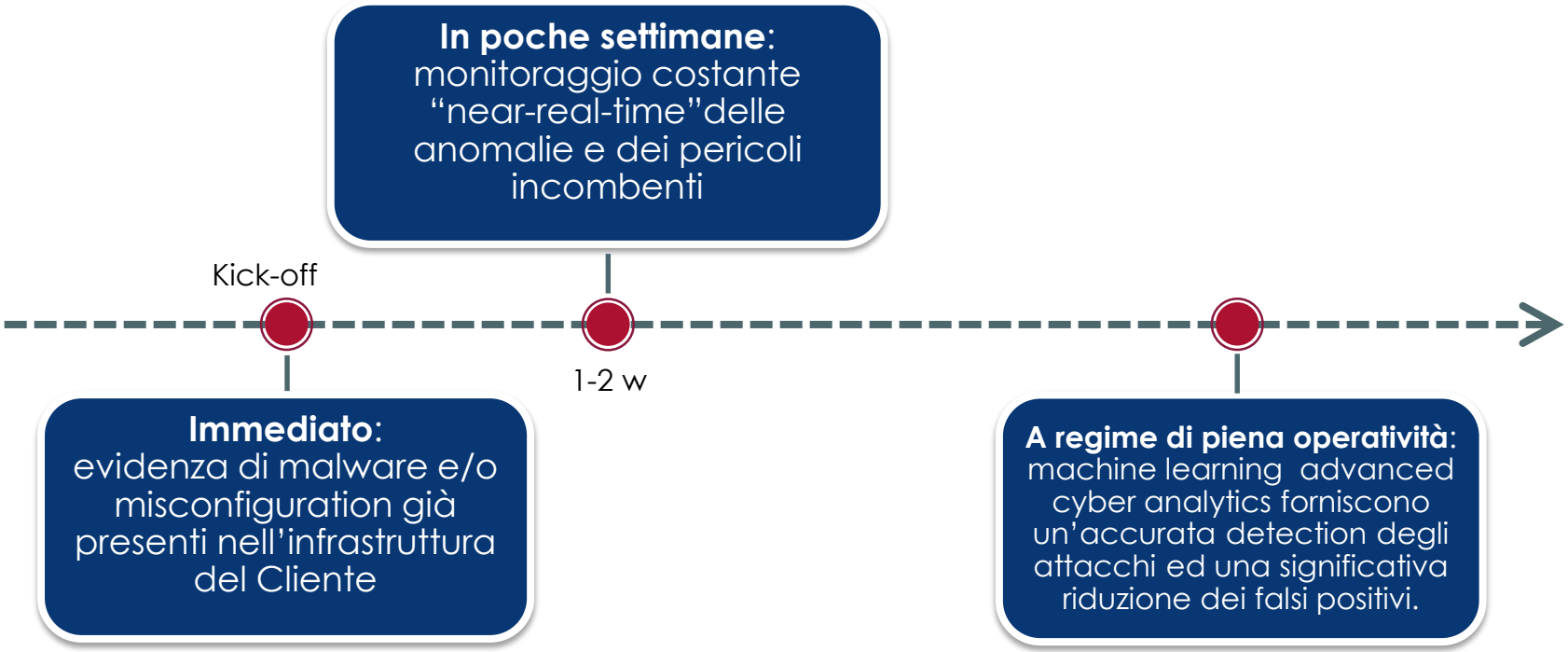
minacce comunicate al cliente

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

USE CASE 2

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 per l'attenzione …

aizoon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

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

www.aizoongroup.com
aizoon@aizoongroup.com
aizoon Technology Consulting
@aizoongroup

roberto.obialero@aizoongroup.com

RobyObialero

Grazie!

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

AUSTRALIA
EUROPE
USA
TECHNOLOGY CONSULTING