aramis

Pierangelo Lombardo
Gabriele Liverziani

Dalla Threat Intelligence alla Threat Hunting…
la naturale evoluzione della specie

aizoon® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

CLUSIT Security Summit | Roma 7 giugno 2017

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**

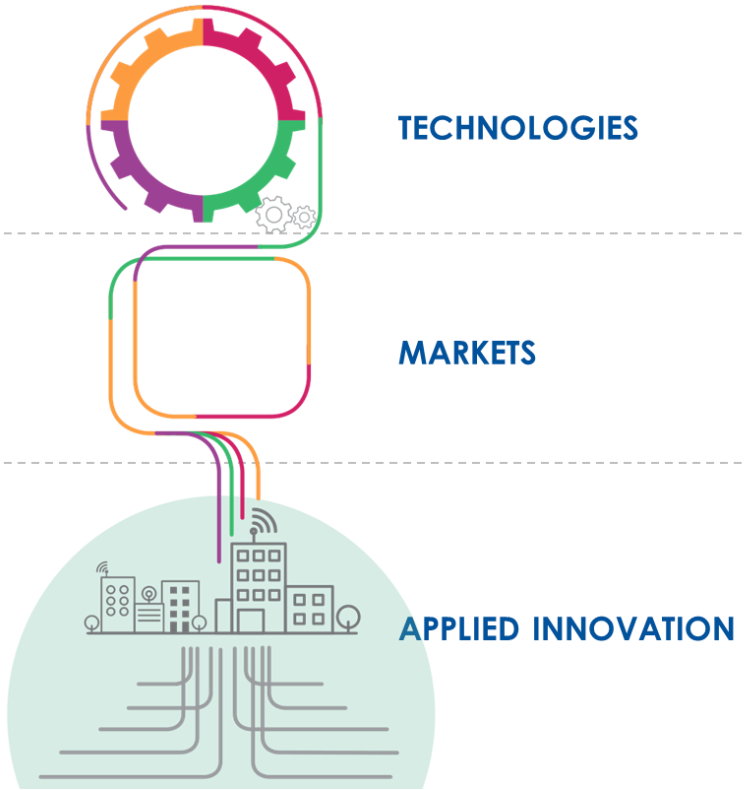
La sicurezza è una sfida continua

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.

aizOn 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

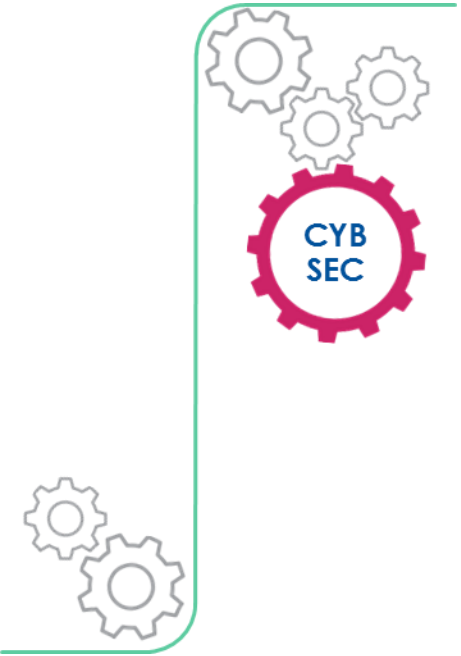
adotta un modello operativo *digital oriented*, basato su logiche trans-disciplinari, agili ed iterative, collaborative ed aperte, abilitanti l'innovazione applicata

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 – Cyber Security



IOT & EMBEDDED SECURITY

Verifica e messa in sicurezza di sistemi automotive, di dispositivi indossabili, di sistemi IoT e sensori di diversa natura

MOBILE SECURITY

La proliferazione di apparati mobile a cui abbiamo assistito nell'ultimo decennio richiede nuove metodologie e processi, non solo per la messa in sicurezza delle applicazioni, ma anche del dispositivo stesso, sia esso un dispositivo aziendale o personale (BYOD). Integriamo i sistemi mobile nelle infrastrutture cliente in modo sicuro ed efficiente

CYBERSEC ASSESSMENT

Attività di verifica tecnica quali vulnerability assessment e penetration test per poter valutare la reale esposizione dei sistemi e delle applicazioni aziendali. Eroghiamo queste attività fornendo sempre al cliente una visione completa di quanto rilevato e suggerendo le necessarie operazioni correttive

CRITICAL INFRASTRUCTURE SECURITY

L'identificazione di strategie e best practices più adatte a prevenire o mitigare il rischio, per garantire la sicurezza di servizi e sistemi. Adottando i migliori standard di sicurezza possibili e definendo le corrette procedure siamo in grado di supportare la messa in sicurezza delle infrastrutture critiche

RISK AND COMPLIANCE

L'analisi, la definizione e l'implementazione di processi e procedure riguardanti la sicurezza dei sistemi informatici. Supportiamo i nostri clienti adattando le loro procedure a normative, leggi o policy di sicurezza (siano esse governative o di mercato, contratti in essere con altre aziende o standard internazionali)

FORENSIC ANALYSIS AND INCIDENT RESPONSE

Supportiamo i clienti nelle operazioni di gestione degli incidenti. Eseguiamo perizie tecniche di parte in ambito civile e penale ed operazioni di eDiscovery

MALWARE LAB

I Malware Lab, utilizzato dai nostri servizi e applicazioni è un ambiente specificamente progettato per lo studio dei malware più avanzati. I nostri analisti sono in grado di analizzare e classificare le minacce più recenti e ancora sconosciute

Dalla Threat Intelligence alla Threat Hunting…

la naturale evoluzione della specie

Cosa succede quando ci si rende conto che la Threat Intelligence non basta a risolvere il problema?

Eppure eravamo tutti convinti di aver imboccato la giusta strada…

Adesso che la consapevolezza della consistenza e della pericolosità delle minacce cyber è stata raggiunta non solo dagli esperti di sicurezza, ma anche (finalmente) dai vertici delle organizzazioni, ci si sta rapidamente accorgendo che non ci può essere alcun meccanismo, per quanto avanzato, che possa sostituire l'intuito e la capacità di reazione dell'analista umano.

Dalla Threat Intelligence alla Threat Hunting…

la naturale evoluzione della specie

Il nuovo paradigma è la **«Threat Hunting»,** la caccia alle minacce.

Ma come si possono combinare in un giusto mix la Threat Intelligence, attuata con soluzioni automatizzate quali «advanced analytics» e tecniche di «machine learning», con l'analisi dei dati realizzata da «cacciatori» umani di IoC (Indicators of Compromise)?

La risposta sta nel considerare la Threat Intelligence **l'inizio - e non la fine - del processo**, come in una **«naturale» evoluzione della specie** in cui il fattore abilitante rimane sempre la valutazione dinamica del rischio.

- aramis, network security monitoring
- aramis heading Threat Hunting
- Focus sulle nuove Advanced Cyber Analytics e Tecniche di Machine Learning

aramis: intelligenza artificiale e umana

competenza e passione per la gestione del rischio digitale

L'intelligenza artificiale è globalmente riconosciuta quale potente alleato nella **rilevazione anticipata delle minacce informatiche avanzate**.

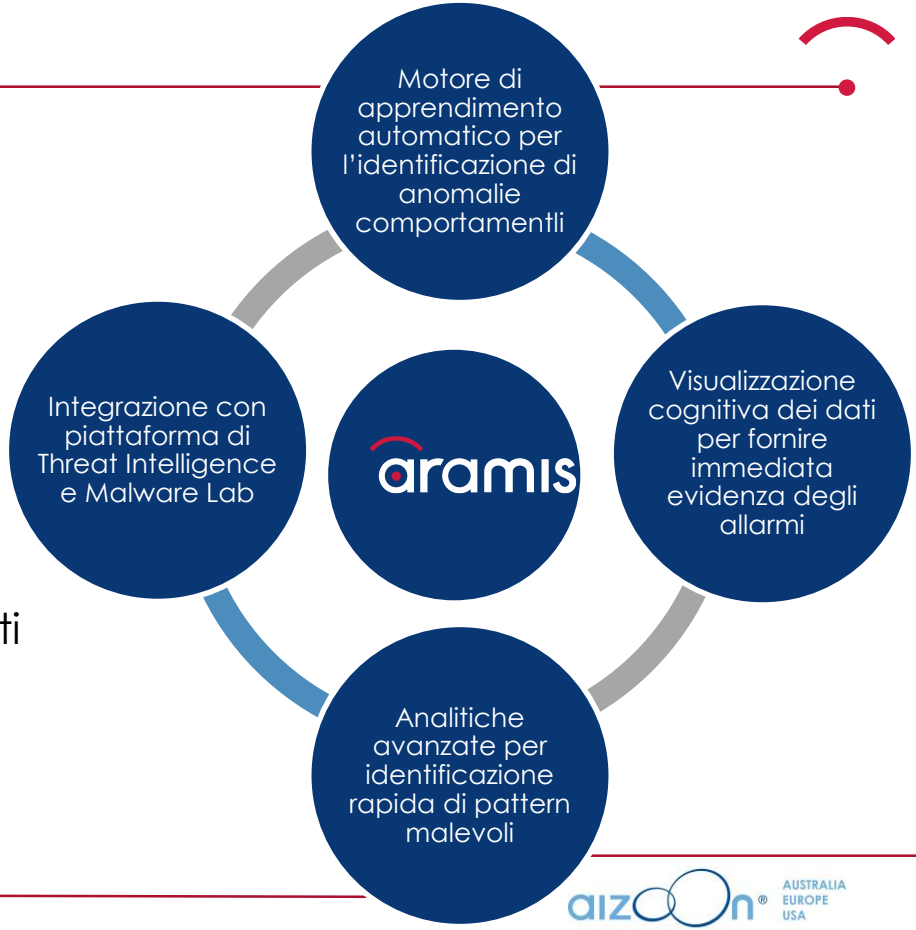
L'efficacia di questi strumenti matematici applicati alla cyber security dipende dalla capacità degli algoritmi di eliminare il rumore di fondo, di «leggere i dati come farebbe un esperto analista» e di fornire al Security Operation Center strumenti di monitoraggio e informazioni utili ad una rapida identificazione delle reali minacce.

aramis è la soluzione di network security monitoring ideata da aizoOn che fa uso di algoritmi proprietari di machine learning e data mining.

I 4 pilasti di aramis

Le nostre sfide:

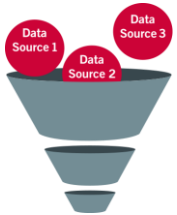
- identificazione dei **segnali deboli;**
- utilizzo di **threat intelligence**;
- dashboard per la **rapida identificazione** degli eventi rilevanti;
- **valorizzazione** del ruolo degli analisti attraverso la **focalizzazione** sugli elementi più critici.



- aramis, network security monitoring
- aramis heading Threat Hunting
- Focus sulle nuove Advanced Cyber Analytics e Tecniche di Machine Learning

aramis 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.

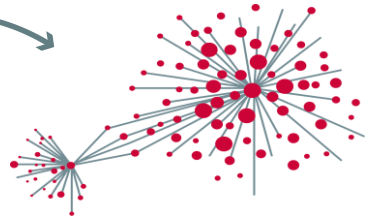
CORRELAZIONE

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 di aizoOn, nonché utilizzando informazioni specifiche del Cliente.

ANALISI

aramis 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.

Threat Hunting

Alcune definizioni

- **Threat** = Intent + Capability + Opportunity**;**
- **Hunting =** *"the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions" (*);*

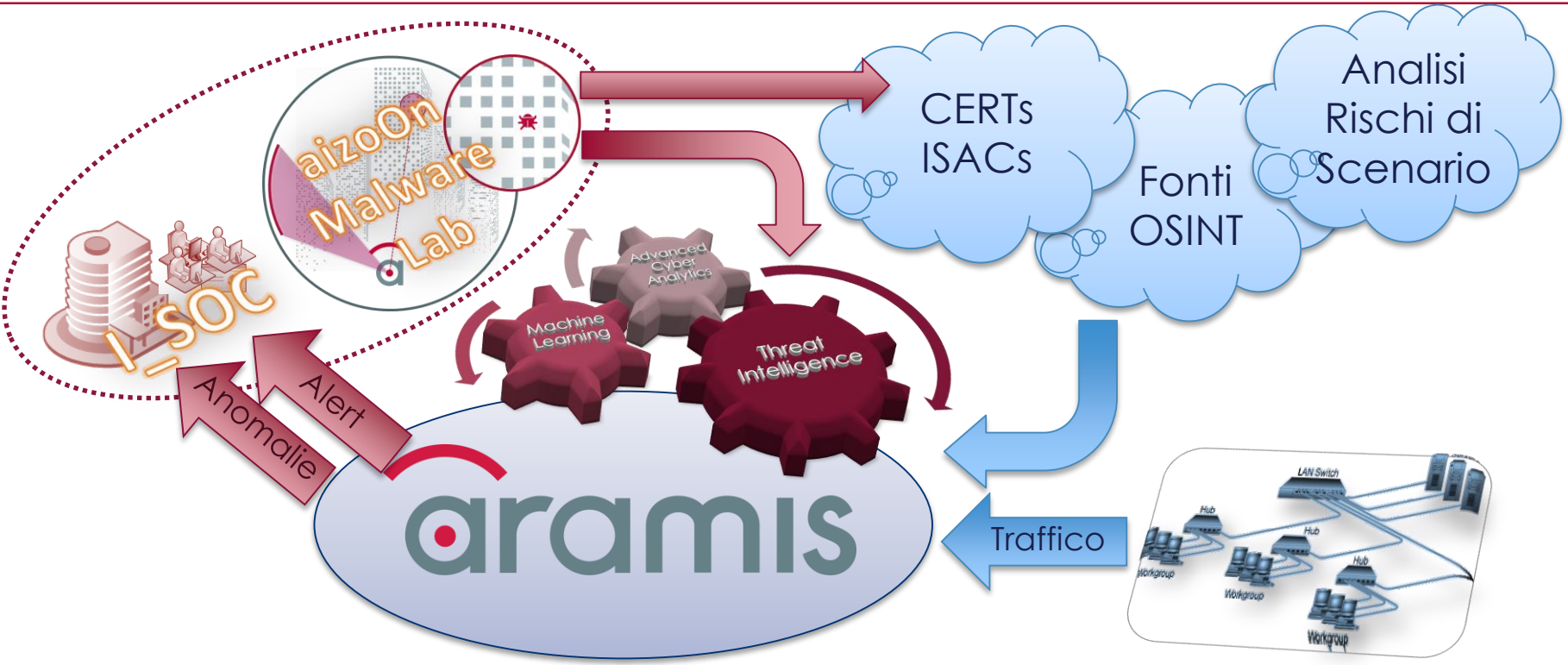
- Threat Hunting Loop (*): Step1 - Create **Hypotheses**… may be derived from:

  - Threat Intelligence
  - Situational awareness
  - Domain expertise

(*) from "A Framework for Cyber Threat Hunting" - Sqrrl Data, Inc. 2016

aramis heading Threat Hunting

evoluzione del processo



aramis heading Threat Hunting

evoluzione del processo

- Costruzione di nuove ACA (Advanced Cyber Analytics) e implementazione di nuovi algoritmi di Machine Learning per:
  - supportare la formulazione automatica delle ipotesi di partenza per il lavoro degli hunter, con un approccio «risk based»;
  - valorizzare ed incrementare le fonti di Threat Intelligence aggiungendo elementi anche eterogenei, ma sempre legati al concetto di rischio (non necessariamente tecnologico);
  - costruire una Situational Awareness che dia evidenza agli analisti della natura dinamica del contesto monitorato;
  - facilitare l'automazione e la prototipazione delle nuove modalità di detection individuate dagli hunter con le loro analisi.

aramis

aramis heading Threat Hunting

evoluzione del processo

- Valorizzare ed incrementare le fonti di Threat Intelligence:
  - l'approccio «risk based» rimane il riferimento, introducendo o rafforzando l'elemento dinamico;
  - in un modello collaborativo, le fonti di Threat Intelligence sono condivise ed alimentate da tutti gli attori, ciascuno secondo il proprio punto di vista;
  - il rischio di contesto, opportunamente valutato, produce un fondamentale valore aggiunto;
  - occorre meglio qualificare gli elementi di Threat Intelligence più «utili», costruendo un'efficace modalità di condivisione e utilizzo:
    - Indicators of compromise (IoCs)
    - Risultati della Threat Research and Analysis
    - Tactics, Techniques, and Procedures (TTPs)

aramis

aramis heading Threat Hunting

evoluzione del processo

- Automazione e prototipazione delle nuove modalità di detection individuate dagli hunter con le loro analisi:
  - le attività di Threat Hunting non possono essere completamente automatizzate;
  - vanno però automatizzati i processi ricorrenti, la ricerca di segnali e pattern noti, l'utilizzo di algoritmi ACA e ML sui dati relativi ai threat individuati;
  - gli hunter devono avere strumenti per supervisionare e convalidare con le proprie capacità investigative i modelli automatici;
  - la modellizzazione dei TTPs è particolarmente importante per poter associare una caratterizzazione - talvolta anche un autore – agli attacchi analizzati senza dover ripetere processi di detection già noti.

aramis

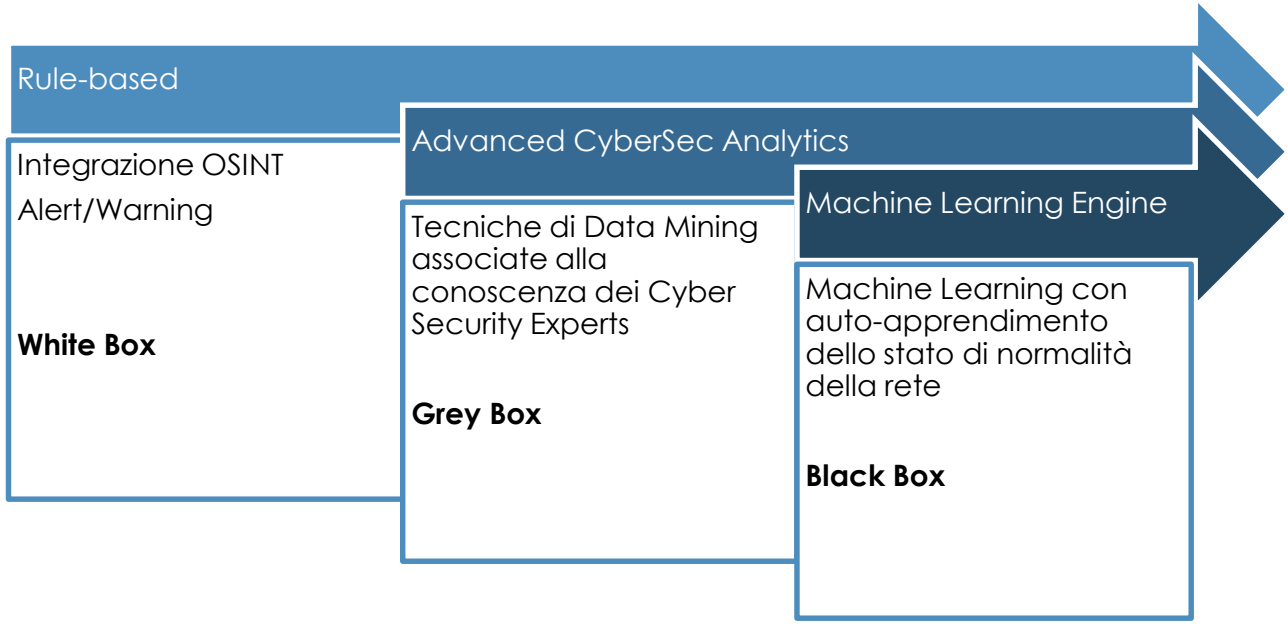
- aramis, network security monitoring
- aramis heading Threat Hunting
- Focus sulle nuove Advanced Cyber Analytics e Tecniche di Machine Learning

aramis: machine learning e analitiche avanzate

"Threat hunting is active search for threats, instead of waiting for an attack to occur and react after the fact. It means you need to tie together a number of activities, both automated scans, threat landscape intelligence and context development, and smart use of machine learning, data science and creative data exploration."

http://blog.sqrrl.com/what-is-threat-hunting-in-cybersecurity-defense

aramis: machine learning e analitiche avanzate



Statistics and Data Viz

you can't have one without the other

Un esempio:

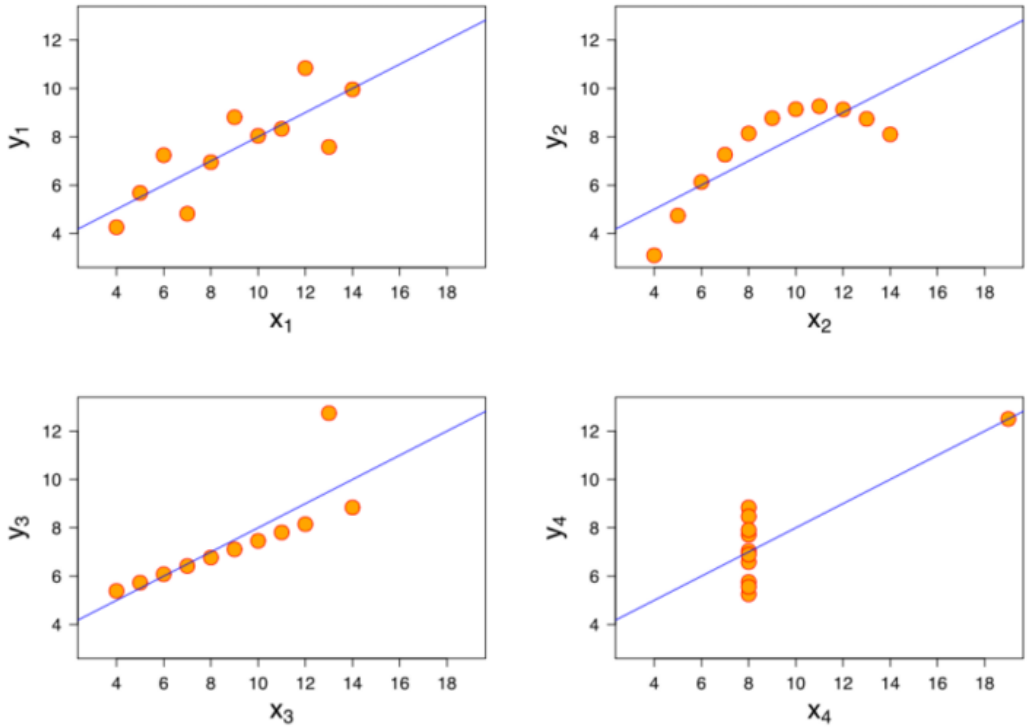
	I		II		III		IV	
	x	y	x	y	x	y	x	y
	10.0	8.04	10.0	9.14	10.0	7.46	8.0	6.58
	8.0	6.95	8.0	8.14	8.0	6.77	8.0	5.76
	13.0	7.58	13.0	8.74	13.0	12.74	8.0	7.71
	9.0	8.81	9.0	8.77	9.0	7.11	8.0	8.84
	11.0	8.33	11.0	9.26	11.0	7.81	8.0	8.47
	14.0	9.96	14.0	8.10	14.0	8.84	8.0	7.04
	6.0	7.24	6.0	6.13	6.0	6.08	8.0	5.25
	4.0	4.26	4.0	3.10	4.0	5.39	19.0	12.50
	12.0	10.84	12.0	9.13	12.0	8.15	8.0	5.56
	7.0	4.82	7.0	7.26	7.0	6.42	8.0	7.91
	5.0	5.68	5.0	4.74	5.0	5.73	8.0	6.89
Average	**9.0**	**7.5**	**9.0**	**7.5**	**9.0**	**7.5**	**9.0**	**7.5**
Variance	**11**	**4.12**	**11**	**4.12**	**11**	**4.12**	**11**	**4.12**
Correlation		**0.816**		**0.816**		**0.816**		**0.816**
Linear Regression Line	***y = 0.5x + 3***		***y = 0.5x + 3***		***y = 0.5x + 3***		***y = 0.5x + 3***	

http://www.datasciencecentral.com/profiles/blogs/when-data-viz-trumps-statistics

aizon AUSTRALIA EUROPE USA TECHNOLOGY CONSULTING

Statistics and Data Viz

you can't have one without the other

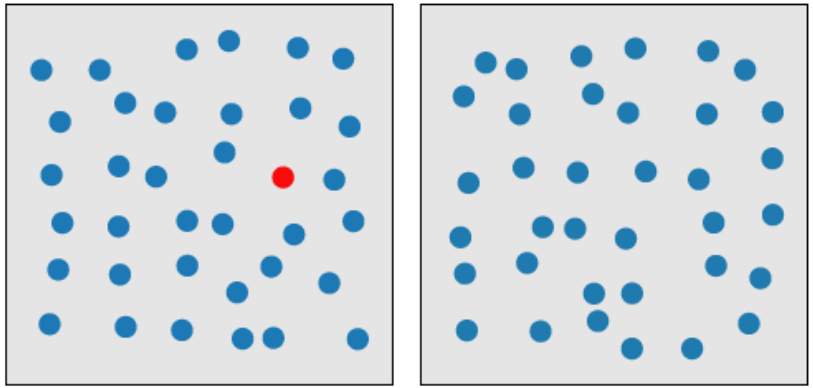


http://www.datasciencecentral.com/profiles/blogs/when-data-viz-trumps-statistics

aizon AUSTRALIA EUROPE USA TECHNOLOGY CONSULTING

Statistics and Data Viz: Cognitive Processing

"Human perception plays an important role in the area of visualization. An understanding of perception can significantly improve both the quality and the quantity of information being displayed"
- Ware -



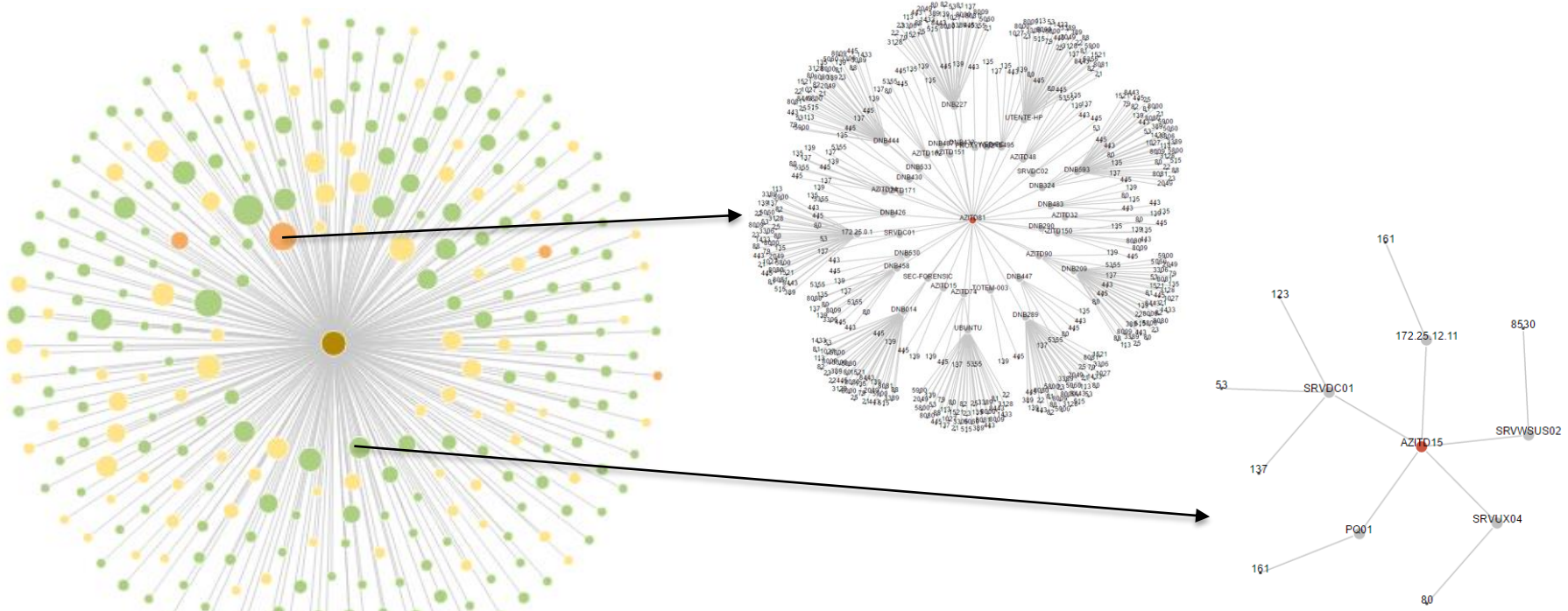
(a) (b)

Ware, C. *Information Visualization: Perception for Design*. Morgan Kaufmann Publishers, Inc., San Francisco, California, 2000.

aizon AUSTRALIA EUROPE USA TECHNOLOGY CONSULTING

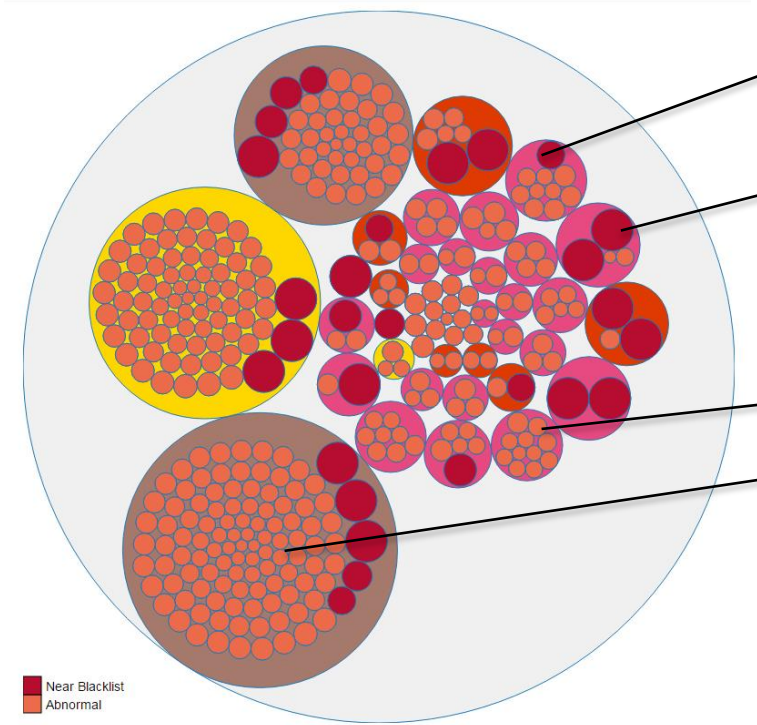
aramis: analitiche avanzate

Network analysis



aramis: analitiche avanzate

Analisi delle stringhe dei domini DNS



faceb000k.7host08.com

googlle.in

Simili ma non uguali agli originali

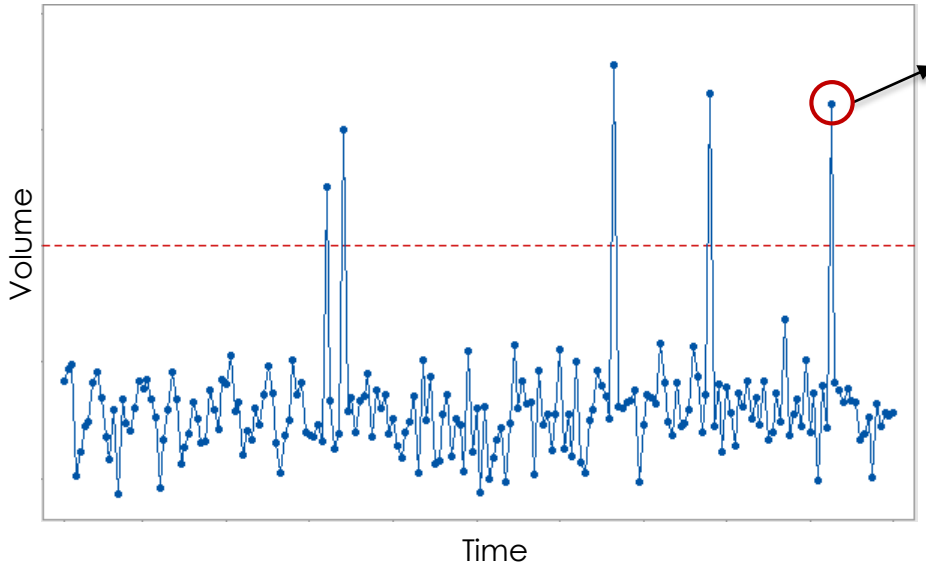
zn_1i8wqguxh5uzvbz.interceptics.com

5fe8a3d39a5226a54c2.activitylt.com

Domini random & pseudorandom

aramis: analitiche avanzate

Identificazione Domain Generation Algorithms (DGA)



Outlier detection

Clustering

Identificazione domini DGA

Malware **keylogger**
Rilevato il 13/03/2017

116 richieste non risolte
54 richieste risolte

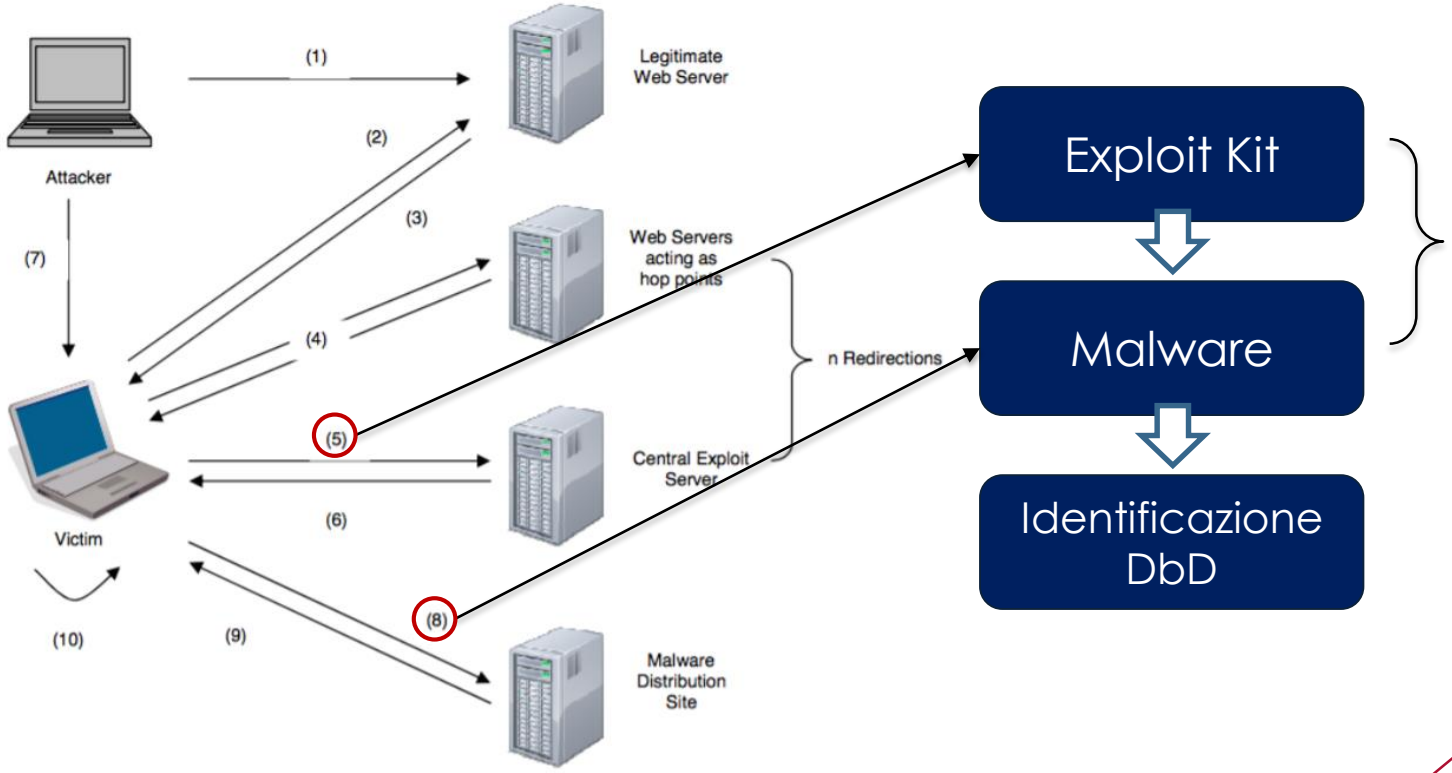
Domini malevoli identificati

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

PROBABILITA' DI ANOMALIA
98,93%

aramis: analitiche avanzate

Identificazione Drive by Download (DbD)



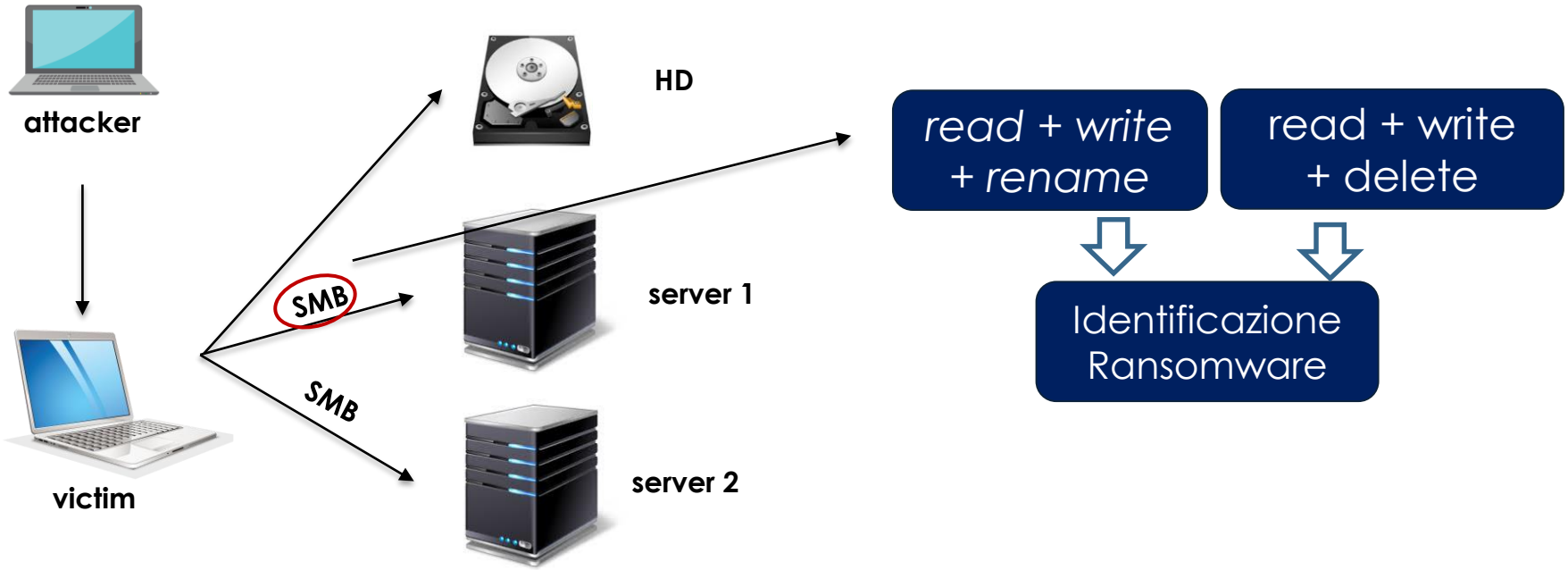
Analisi dei mime type

application/jar
application/pdf
application/vnd.adobe.flash-movie
application/vnd.osgi.bundle
application/x-java-applet
application/x-java-archive
application/x-shockwave-flash
application/x-silverlight-app

Livello di entropia sui file

aramis: analitiche avanzate

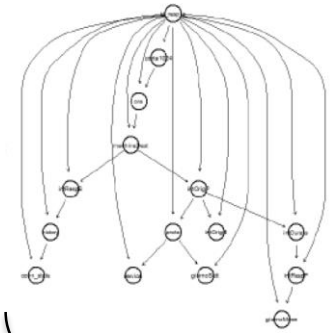
Identificazione Ransomware



aramis: machine learning

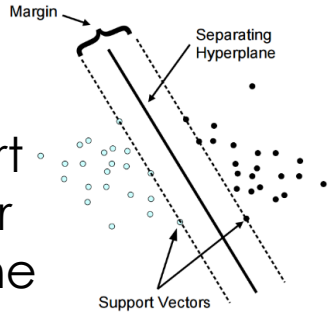
Riduzione del rumore di fondo

Prefilter



Bayesian Network

Support Vector Machine



Aggregation & postfilter

Anomaly detection

aramis: machine learning

Un approccio non supervisionato

L'approccio non supervisionato permette ad aramis di:

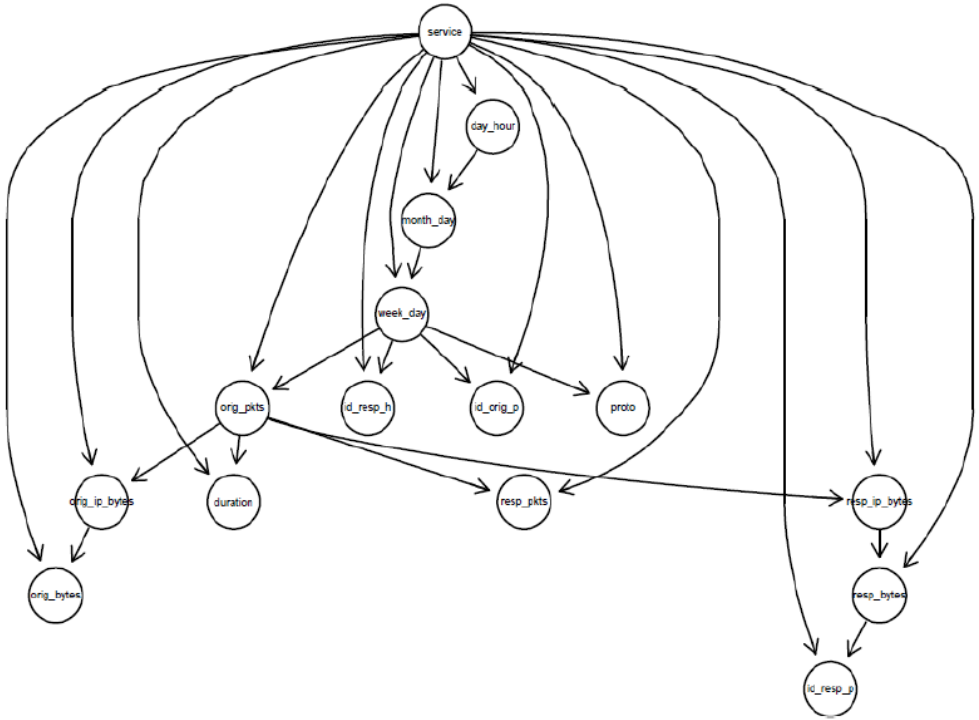
- **Apprendere autonomamente** il comportamento del network
- Identificare le **attività anomale**
- Rilevare **automaticamente** pattern e relazioni
- Lavorare senza **informazioni a priori**
- **Non necessita di input umani**

aramis: machine learning

Bayesian Networks (BNs)

La relazione tra le variabili è espresso mediante un **Direct Acyclic Graph** (DAG).

Ogni nodo all'interno del network viene mappato mediante un DAG che descrive le sue modalità usuali di comunicazione.



aizon AUSTRALIA EUROPE USA TECHNOLOGY CONSULTING

aramis: machine learning

Bayesian Networks (BNs)

Primo layer

pc1_model

pc2_model

pc3_model

srv1_model

srv2_model

Secondo Layer

Global_pc_model

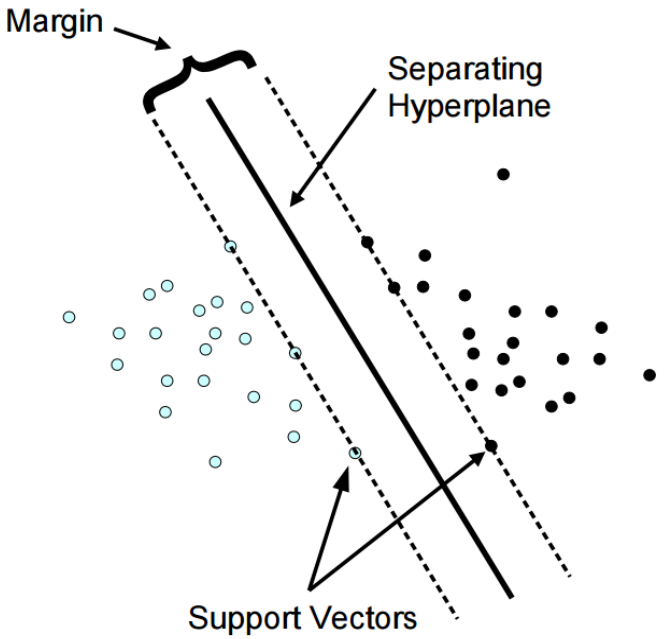
Global_srv_model

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:

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

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

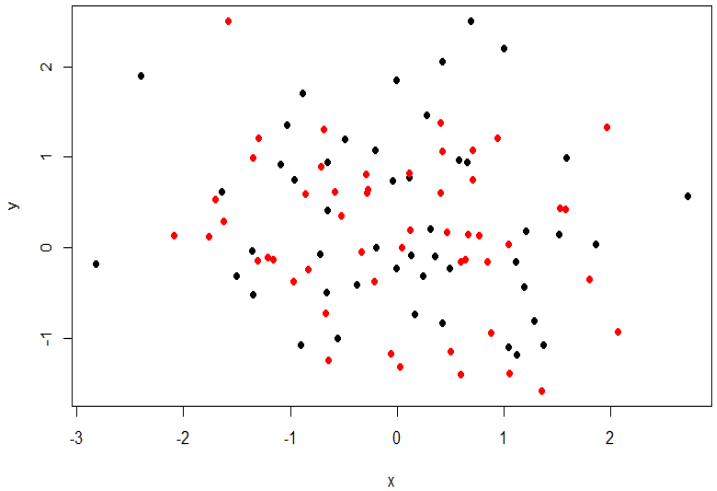
Minimizzazione:

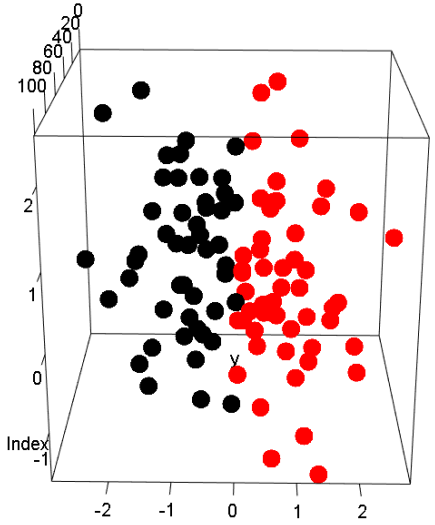
$$\min_{\boldsymbol{w},b} \quad \frac{\|\boldsymbol{w}\|^2}{2}$$

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

aramis: machine learning

Support Vector Machine (SVM)



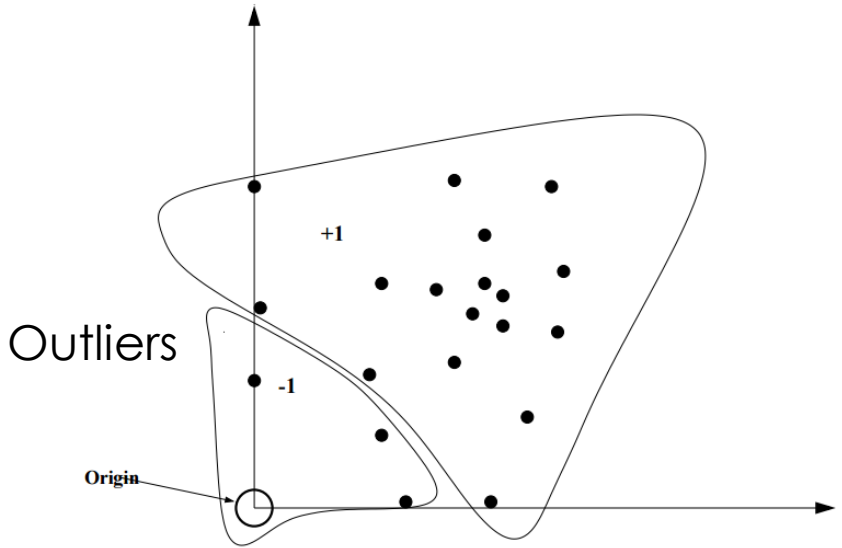


Mapping in uno spazio dove le classi sono linearmente separabili

aizon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

Machine Learning Engine: Support Vector Machine (SVM)

Identificazione degli eventi utilizzando la distanza dalla distribuzione originale



aizon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

Threat Hunting process

Grazie!

aizoOn® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING