

Dovinci – Cyber Threat Intelligence Platform

Gianni Amato

GARR Conference 2019

Politecnico di Torino, 4 giugno 2019



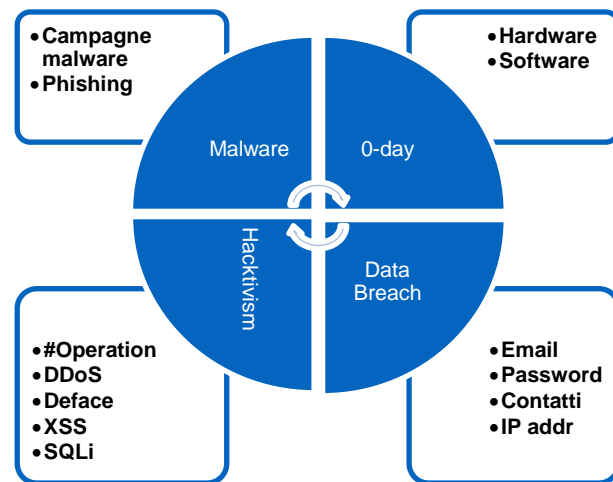
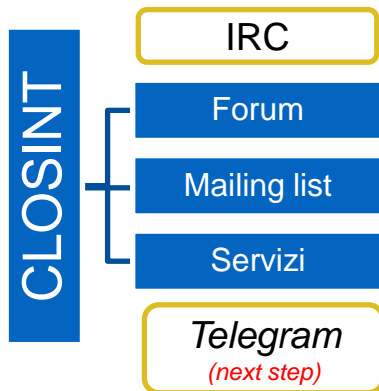
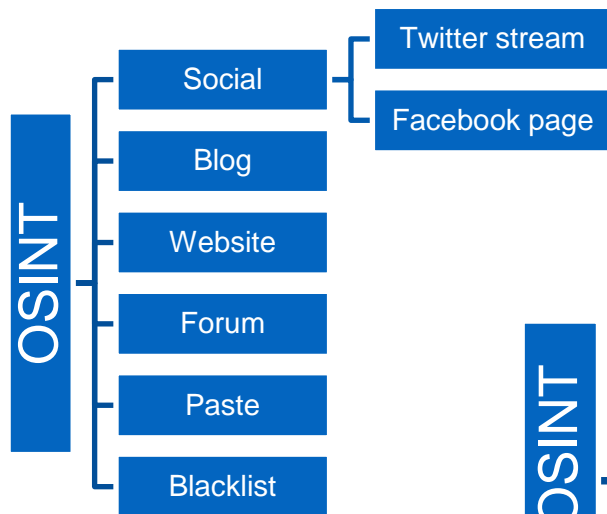
AGID | Agenzia per
l'Italia Digitale



Computer Emergency Response Team
Pubblica Amministrazione

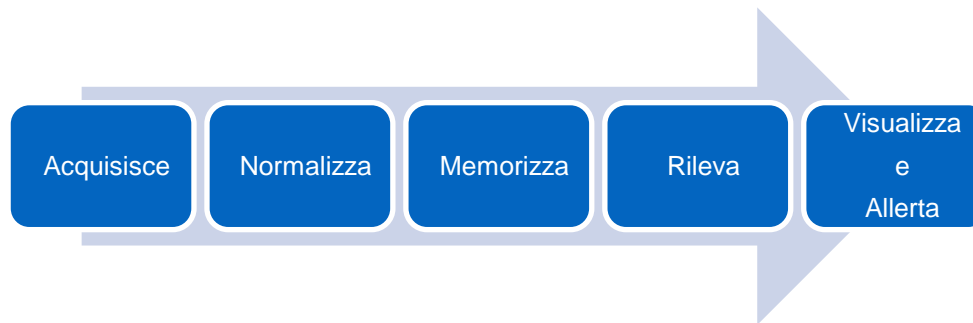
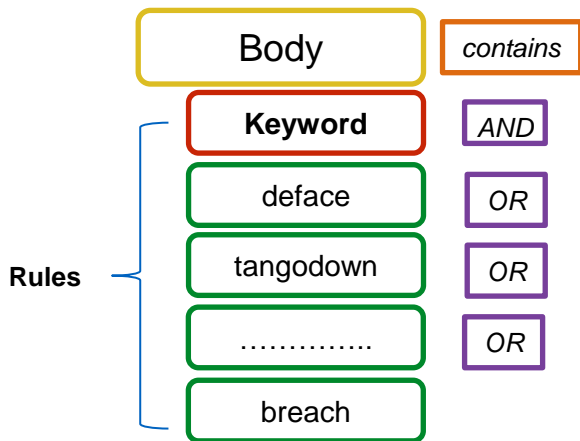
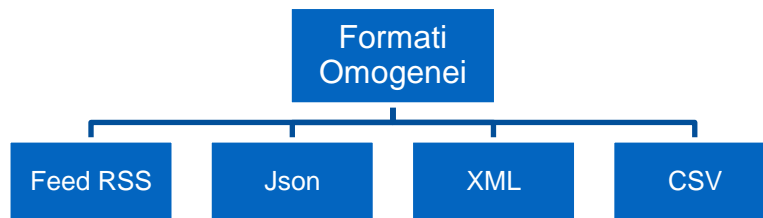
CERT-PA

Sorgenti di Informazione



Formati Eterogenei e Processo di Normalizzazione

Formati Eterogenei
«Testi e Liste non strutturate»
(es. le blacklist)



{ Kp AND [k1 OR (K2 AND K3) OR Kn] }

Dovinci dashboard

The dashboard displays a total count of 4,938 alerts. It features several widgets:

- Count:** A large number '4,938' with a 'Count' label below it.
- Community:** A donut chart showing the distribution of alerts across different communities.
- Alerts by Status:** A grid of circular progress indicators for categories like 'Alert CMS', 'Alert Structure Accreditate', and 'Alert Structure NON Accreditate'.
- Tagcloud News:** A word cloud containing terms like 'targets', 'opisrael', 'vulnerabilities', and 'business'.
- Table:** A table with columns for 'Time', 'source_name', 'title', 'description', 'permalink', 'date', 'tag', 'target', and 'category'. It lists several security-related alerts from March 2019.

This interface allows users to manage and filter alerts. It includes:

- Search Bar:** A search field with the text 'Cerca' and a dropdown menu.
- Alert List:** A table with columns: DATE/TIME ACQUISITION, TARGET, ALERT NAME, MATCHED, SOURCE NAME, EMAIL NOTIFY, and THREAT. It lists various alerts from different sources like 'Camera', 'Reg. VDA', and 'Reg. Marche'.
- Filters:** A 'Per Threat' dropdown menu with options 'TUT', 'SI', and 'NO'.

A zoomed-in view of a tag cloud showing terms such as 'datbreach', 'cybercrime', 'hacker', 'vulnerability', 'remote', 'wormable', 'flaw', 'execution', 'medical', 'update', 'patch', 'windows', 'desktop', '0708', 'scams', 'worm', 'analysis', 'vulnerable', 'million', 'systems', 'nearly', 'still', 'coming', 'facing', 'services', 'vulnerability', 'remote', 'wormable', 'flaw', 'execution', 'medical', 'update', 'patch', 'windows', 'desktop', '0708', 'scams', 'worm', 'analysis', 'vulnerable', 'million', 'systems', 'nearly', 'still', 'coming', 'facing'.

A zoomed-in view of another tag cloud showing terms such as 'vulnerability', 'remote', 'wormable', 'flaw', 'execution', 'medical', 'update', 'patch', 'windows', 'desktop', '0708', 'scams', 'worm', 'analysis', 'vulnerable', 'million', 'systems', 'nearly', 'still', 'coming', 'facing', 'services', 'vulnerability', 'remote', 'wormable', 'flaw', 'execution', 'medical', 'update', 'patch', 'windows', 'desktop', '0708', 'scams', 'worm', 'analysis', 'vulnerable', 'million', 'systems', 'nearly', 'still', 'coming', 'facing'.

The 'Modifica Twitter query' form includes:

- Source name:** A text input field containing 'PaperstormTA'.
- Username or Keyword:** A text input field containing 'oppaperstormita'.
- Category:** A dropdown menu set to 'Hackivism'.
- Target:** A dropdown menu set to 'Customers'.
- Tag:** A dropdown menu set to 'Twitter'.
- Buttons:** 'Controls' and 'Modifica' buttons.





AGID | Agenzia per
l'Italia Digitale

Il Paese che cambia passa da qui.

Gianni Amato

agid.gov.it | cert-pa.it



AGID | Agenzia per
l'Italia Digitale



Computer Emergency Response Team
Pubblica Amministrazione

CERT-PA