

IBM Security

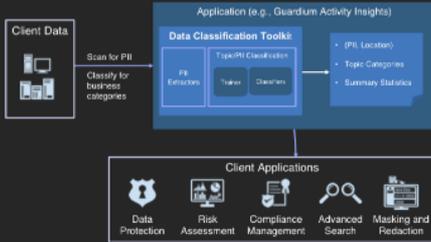
Intelligenza Artificiale per la Cybersecurity: un contributo essenziale per una protezione efficace

Giulia Caliarì
Security Architect, Italy

Alcuni esempi di ML/AI per proteggere utenti, dati e dispositivi

Protect

Data classification



Continuously access risk

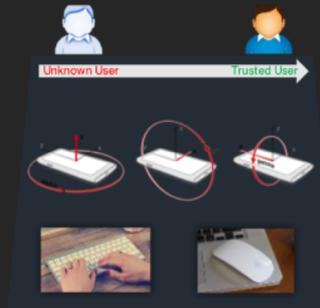
This block shows a 'Passcode' recommendations interface with 'Cognitive Recommendations'. It lists: 65% of organizations within the community have passcode policy set, Alphabetic is the most common Passcode Quality set, Minimum passcode length set is 6, and Maximum passcode age (in days) is 90. Below this is a dashboard with a donut chart showing 'Continuously access risk' and a bar chart showing 'Risk scores assigned'.

Detect

Predictive Analytics / Outlier Detection

This block contains two screenshots. The left one is a 'Data Extraction' alert from 'IBM Security Guardium Insights' dated 2019-10-08 11:00:00. The right one is a 'Predictive Analytics / Outlier Detection' dashboard showing a line graph of activity over time and a table of detected anomalies.

Behavior biometrics-based verification

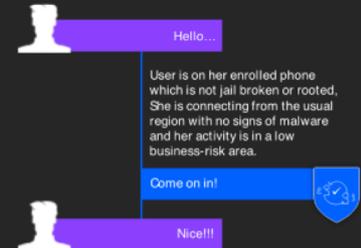


Respond

Risk based Certification

This is a 'Risk based Certification' dashboard showing various metrics: 110, 264, 15, and 76. It includes a 'Quick insights' section with a donut chart and a table of 'Top risky applications' with columns for Name, Risk, and Status.

User / Data Access Enforcement



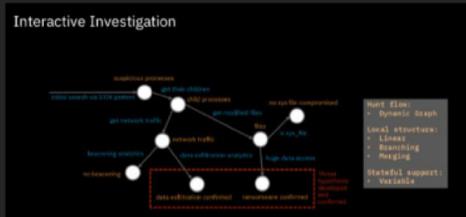
Alcuni esempi di ML/AI nel Threat e Risk Management

Protect

Risk analysis based on multiple Vectors and Asset Criticality

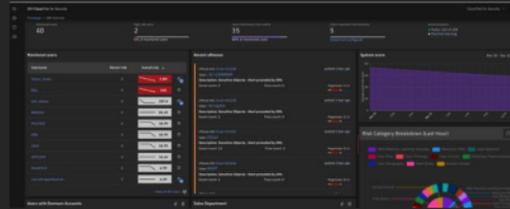


Open Threat Hunting Language and Analytics



Detect

Rapid Identification of Risky Users and Insider Threats

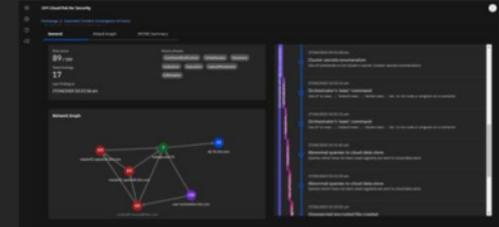


Identify beaconing with network analytics and entity behavior



Respond

Automatic, accurate, consistent case investigations



Automating repetitive tasks with composable playbooks

