Customer Case: OpenPMF™ 4.0 protects criminal intel analytics

Big data and visual analytics brought groundbreaking new capabilities to intelligence systems, allowing improved analytics and sense making on large amounts of data from many sources – especially when coupled with support for data integration between different databases, collaboration between analysts and information exchange between organizations.

A globally unique project.
ObjectSecurity is part of the unique multi-year project "VALCRI", which is concerned with visual analytics for police intelligence. As part of the project, ObjectSecurity has developed an innovative security architecture for such demanding tasks based on its innovative **OpenPMF 4.0 security policy automation platform.**

Access to data is a risky business.
Access to data and processed intelligence also brings risks, in some cases so many risks that they prohibit the full use of the new systems. Access to information has to be contextually restricted to the minimum necessary for analysts to do their current tasks. Not all users, including analysts, are authorized to access all data in the systems – they may not have sufficient clearance, or there is no need to know, or because data has to be specifically protected.

Data protection regulations
Other data may only be obtained under specific conditions and is bound to a specific purpose. In some countries and domains, for example in **police intelligence**, strict data protection regulations have to be met. Meeting those using conventional security technologies is not only challenging, it is almost impossible, as history has shown.

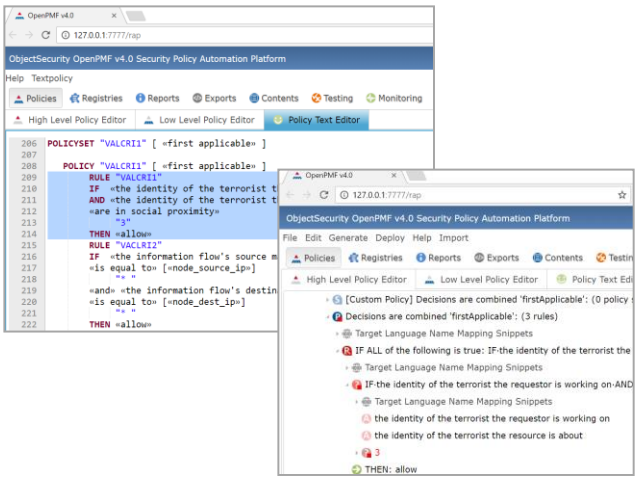
Security and audit requirements.
In addition, the usage of the system has to be strictly audited, including system administrators – to detect misuse by insiders and attacks from the outside.

ObjectSecurity OpenPMF 4.0 in VALCRI

Human-understandable policies.
OpenPMF allows the i**ntuitive authoring of rich, but human-understandable policies** driven by operational and regulatory security and data protection requirements.

Defense in depth.
From these policies, OpenPMF automatically **generates the matching technical security enforcement** for "defense in depth" across many systems and layers – including network layer filtering at domain boundaries and hosts, but also fine grained access control at middleware, database and application layers.

Testing and auditing.
OpenPMF also supports advanced policy testing, for example to verify that the policies meet the desired requirements. And it automatically produces human-readable documentation that can be audited by the appropriate authorities.



objectsecurity.com
@objectsecurity
info@objectsecurity.com