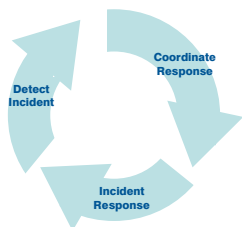


Secure Information Sharing for Homeland Security & Counter-Terrorism

Secure Information Sharing, Collaborative Decision Making, Situational Awareness for Homeland Security, Counter-Terrorism & Border Security

Detect-Coordinate-Respond

Border security organizations need to detect security relevant incidents and carry out a coordinated and effective response. The response needs to be as fast as possible to contain the damage. The success of homeland security operations is heavily impacted by better, faster, and more responsive information exchange, enabled by superior information technology integration. This is because all stakeholders need to have a high degree of situational awareness and accommodate for distributed collaborative decision making in order improve effectiveness and to carry out large-scale operations. This involves the rapid collection, processing, and dissemination of information across many different stakeholders (emergency services, fire services, police services, military, government) and systems. Networked, integrated IT systems have the power to make information available timely and reliably, and thus improve responsive coordination and command & control. Agencies across the globe are now working on improving the fast exchange of useful information via networks. There are many benefits, including faster reaction time, improved shared understanding and situational awareness, faster / more coherent / efficient / precise / timely / concurrent / responsive actions, improved force protection, and higher degree of task automation. To achieve the fast detect-coordinate-response loop, IT systems need to be integrated well.



Secure Information Exchange is Critical

Robustness of the mission-critical IT infrastructure used to coordinate responses is vital. Information security plays a critical part, both to achieve robustness against terror

attacks and to ensure that intruders are unaware of the response strategy. The complexity of IT security in such complex, interconnected environments is a major challenge. Many efforts are currently undertaken to design and build a common architectural standard for a joint-up, agile business-driven technology architecture. Service Oriented Architectures (SOAs), process-centric architectures (BPM), as well as data-centric architectures (e.g. DDS) are all being deployed alongside more traditional application integration platforms such as JavaEE, JMS, CORBA/CCM. This complex environment makes it hard to enforce and administer a uniform, coherent, organization-wide security policy across the many different systems used today by many agencies. ObjectSecurity OpenPMF can help:



ObjectSecurity OpenPMF lets you intuitively select business-centric security & compliance policies, which are then automatically enforced across your IT landscape (using a "model-driven security" approach). You can conveniently manage your policies at run-time, and even change your software applications and workflows without extra administration. OpenPMF reduces costs, improves security, and enables agility. Available as a packaged product and as an integrated turn-key solution.

Products & Services

- OpenPMF (packaged product & turn-key solution)
- SimulateWorld 4D synthetic environment toolkit
- SecureMiddleware: secure open source middleware
- Services: security policy management, Web 2.0 / SOA / Cloud / SaaS Security, middleware security, training workshop, tech. support, R&D
- Studies: in-depth documents about hot topics in security, e.g. model-driven security & SOA

www.objectsecurity.com