**Proposition de recherche doctorale**

**Development of new techniques for Security Information Management (SIM) based on service dependencies and attack impact models**

**Mots clés**:
- Directeur de thèse : Hervé Debar
- Co-encadrant(s) :
- Unité de recherche : Services répartis, Architectures, MOdélisation, Validation, Administration des Réseaux
- Ecole doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal : Divers

**Résumé du projet de recherche (Langue 1)**

This PhD proposal addresses the domain of information systems and networks security, and more specifically operational network security. The objective of operational network and system security is to monitor information systems and networks, looking for evidence of attacks. More specifically, intrusion detection systems have been designed to analyze traces generated by the system under monitoring, such as logs, network packets or operating system calls, and seek evidence of malicious activity in these traces. Security information and/or event management systems (SIEM) are tasked with receiving, correlating and analyzing the alerts generated by intrusion detection sensors and other log producers, to make available a global view of the security status of the monitored system, and support the system administrator in making the right decisions for the continuous operation of his system. The main goal of the PhD thesis is the research and development of novel techniques for intrusion detection and alert correlation, addressing cross-layer detection, quantitative risk analysis, decision support and threat remediation.

**Informations complémentaires (Langue 1)**

This PhD is executed in the context of the FP7 "MASSIF" project.