**Cyber Security Defence Agent with Reinforcement Learning**

*Supervisors TNO: Frank Fransen, Sebastiaan Tesink*

In this MSc thesis project experiments and a test environment will be developed to do research on using Reinforcement Learning (and other AI techniques) for automated security. The idea is to train Cyber Security Defence Agent on how to best respond to attacks. The test environment will consist of an automated attack system (e.g. Infection Monkey) and defence agent that can interact with the system under attack to respond to the action by the automated attack system.

**Security events correlation**

*Supervisors TNO: Eric Meeuwissen, Irina Chiscop, Yoram Meijaard*

In this project we are interested in combining security events and alerts from different intrusion detectors (by means of Bayesian Networks, Belief Networks, Deep Neural Networks, Semantic Learning etc.). We want to model causal relationships between these events and investigate different correlations in order to filter, prioritize and better explain the alerts that go to the (Security Operations Center) SOC analyst. We are particularly interested in building a fusion/correlation engine that can process DNS, Netflow and network logs anomalies.

**Threat landscape methodology improvement and tool implementation**

*Supervisors TNO: Frank Fransen, Sebastiaan Tesink*

In corporation with several Dutch banks, TNO has developed a CTI based threat landscaping methodology. This methodology can be used to prioritise emerging threats for a specific organisation. Based on collected CTI data, the tool quantifies different aspects of threats and maps specific attacks techniques used. By means of a Bayesian networks the different metrics and organisation specific information a priority score can be calculated. The internship will focus on improving the metrics, automating CTI collection and quantification, Bayesian networks calculations, organisation specific impact assessment and implementing the threat landscaping tool.

**Business Impact Quantification for Automated Security**

*Supervisors TNO: Frank Fransen, Sebastiaan Tesink*

Currently SOCs use pre-assign criticality information per asset to determine potential impact of security incidents. We want to provide SOCs with more accurate and actual business impact information. The internship is focussing on developing technologies to automatically create models (i.e. Bayesian networks) to produce business impact quantification for different type of security breaches: i.e. confidentiality, integrity, availability, and privacy. The MSc thesis work builds on results of a previous student and H2020 project SOCCRATES, and uses among other Business Process Modelling, IT infrastructure modelling and Bayesian Networks.