Cyber Deception Technology

Subject areas:	Cyber Security, Managed Security Service Provider
Student:	Raluca Schibli
Supervisor:	Dieter Arnold
Expert:	Christoph Marbach
Client:	Natalya Arbuzova, Swisscom (Schweiz) AG
Keywords:	Deception technology, Managed Security Service Provider, Security Operation Center

1. Problem Statement

Together with information technology, cybercrime is evolving, malicious users are becoming more dexterous. Phishing and social engineering attacks, threats of malware and ransomware, the fast spread of fake news and misinformation, security, and data breaches, renders the necessity of developing new methods of defense.

Swisscom (Schweiz) AG regularly evaluates technologies in the cyber security detection area to define the next steps for the expansion of the Threat Detection and Response portfolio, in accordance with its strategy. Thus, of interest is the relatively new and fast evolving technology of deception.

2. Solution Concept

The first goal of the project was an extensive literature survey to better understand how the deception technology works, how is it applied, what are the advantages and challenges. To implement the deception technology in a Managed Security System Provider (MSSP), the vendors of such technology are important. Establishing the requirements and selection criteria allows narrowing down the vast number of deception technology vendors, to choose the best one regarding the current needs. The challenges of implementing a new technology in an existing MSSP can only be appreciated when implementing a Proof of Concept (PoC) and studying the behavior of the solution for at least 30 days. Ideally, a penetration test should also be performed.

3. Specific Challenges

Deception technology is not a defense mechanism and cannot be used without other complementary security measures. Generally, deception technology assumes that the attacker has already penetrated the enterprise's environment. The biggest challenge remains the complete coverage of important assets and the creation of believable credentials. Decoys can be detected or hacked, thus losing their efficiency.
Regarding the present work, the literature survey did not provide any challenges, but the implementation of a PoC was unfortunately impossible due to delays, technical difficulties, or low priority to support academy research from commercial deception technology vendors.

4. Results

Introducing deceptive elements within an enterprise can delay the malicious user and prevent an attack, by deflecting them from the real assets of a company. Automated deception technology can interact with the attacker and gives valuable information about their tactics and techniques when moving along an enterprise's infrastructure. This knowledge can be further used to improve the cyber defense methodology.
To gain a glance in the deception technology practical aspects, a commercial solution was pursued. Several types of tokens have been created and deployed on the local computer. The technology could be proved: when the deceptive assets are accessed, an alert with useful information for the defender, such as IP address, geolocation, timestamp, sometimes user name, is triggered. How to deploy deception technology in a larger environment remains an open question.

5. Outlook

As a complementary method, deception technology can bring significant improvements in understanding the cyber attacker and in the preparation of security strategies. In a Managed Security Service Provider deception technology can bring the advantage of detecting more advanced threats, while providing a small number of false positive alerts and can respond to the attacker's actions. Deception technology can be applied for IoT, SCADA and other environments where the use of other security controls is not possible or difficult.
The first step in implementing the technology in an MSSP remains the creation of a PoC, preferably from two vendors, to ensure that the defined objectives are achieved.