Dr. L. Allodi (TU/e), SeReNity

English scientific summary

Prompt and timely response to incoming cyber-attacks and incidents is a core requirement for business continuity and safe operations for organizations operating at all levels (commercial, governmental, military). The effectiveness of these measures is significantly limited (and oftentimes defeated altogether) by the inefficiency of the attack identification and response process which is, effectively, a show-stopper for all attack prevention and reaction activities. The cognitive-intensive, human-driven alarm analysis procedures currently employed by Security Operation Centres are made ineffective (as opposed to only inefficient) by the sheer amount of alarm data produced, and the lack of mechanisms to automatically and soundly evaluate the arriving evidence to build operable risk-based metrics for incident response.

This project will build foundational technologies to achieve Security Response Centres (SRC) based on three key components: (1) risk-based systems for alarm prioritization, (2) real-time, human-centric procedures for alarm operationalization, and (3) technology integration in response operations.

In doing so, SeReNity will develop new techniques, methods, and systems at the intersection of the Design and Defence domains to deliver operable and accurate procedures for efficient incident response. To achieve this, this project will develop semantically and contextually rich alarm data to inform risk-based metrics on the mounting evidence of incoming cyber-attacks (as opposed to firing an alarm for each match of an IDS signature). SeReNity will achieve this by means of advanced techniques from machine learning and information mining and extraction, to identify attack patterns in the network traffic, and automatically identify threat types.

Importantly, SeReNity will develop new mechanisms and interfaces to present the gathered evidence to SRC operators dynamically, and based on the specific threat (type) identified by the underlying technology. To achieve this, this project unifies Dutch excellence in intrusion detection, threat intelligence, and human computer interaction with an industry-leading partner operating in the market of tailored solutions for Security Monitoring.

English public summary

Cybersecurity Operation Centres monitor incoming threats, but are only useful for incident investigation (as opposed to prevention) because of the vast amount of generated incoming alerts. SeReNity will develop new technologies accounting for alarm prioritization that integrates with human expertise to enable Security Response Centres and stop attacks before it’s too late.

Dutch public summary

Cybersecurity operation centres controleren binnenkomende dreigingen, maar zijn enkel inzetbaar voor onderzoek van incidenten achteraf (in tegenstelling tot voorkoming) vanwege de overdaad aan gegenereerde meldingen. SeReNity zal nieuwe technologieën ontwikkelen voor het prioriteren van meldingen die de expertise van gebruikers ondersteunen, waardoor Security Response Centres aanvallen in de kiem kunnen smoren.