Master Thesis / HiWi
Correlation Graph-based Intrusion Detection using Zeek event logs

Background: The most dangerous attackers for critical infrastructures are the so-called Advanced Persistent Threat (APT) actors who often employ low and slow strategies with many system built-in tools. Zeek, as a popular network analysis tool, provides semantic-rich network event logs. Host event logs can be collected by additionally installing Zeek-agent on target devices. Zeek event logs have proven to be useful for threat hunting / detection of APT actors. Though, in reality, a vast amount of event logs / alarms which do not necessarily represent malicious behaviors are generated in a monitored system. A security analyst needs to sift through these logs manually to spot possible attack traces, which often leads to alarm fatigue problem and ultimately missing of important attack traces. Hence, with this proposed master thesis, we aim to develop an approach to automatically “connect the dots” across Zeek event logs in the form of a correlation graph. The attack traces will be automatically identified in a context-rich correlation graph. The experimental devices are provided in our security lab (see the figure above).

Tasks:
- Literature review of major cyber-attacks, and common intrusion detection methods
- Get familiar with Zeek, and tools/frameworks for processing Zeek event logs and constructing correlation graphs
- Come up with some new ideas about how to automate/optimize the entire workflow or a specific building block of correlation graph-based intrusion detection
- Implement and evaluate those new ideas

Benefits: Given the complexity of the problem, the student can first work as a HiWi for up to 6 months, if desired, and then continue the work as a master thesis. Throughout the work, the supervisor will work very closely with the student, to ensure that the student can deliver a thesis with good quality at the end. At the beginning (1-2 months), the supervisor will spend a reasonable amount of time to teach, guide and support the student with the appropriate materials. At the end, the student should have a solid understanding of cyber-attacks and common detection methods, and practical experience in researching on intrusion detection systems etc., which are a competence strongly desired by both security industry and academia.

Requirements: Highly motivated; knowledge and experience of data analysis; basic programming skills; adequate understanding of operating systems and network communication.