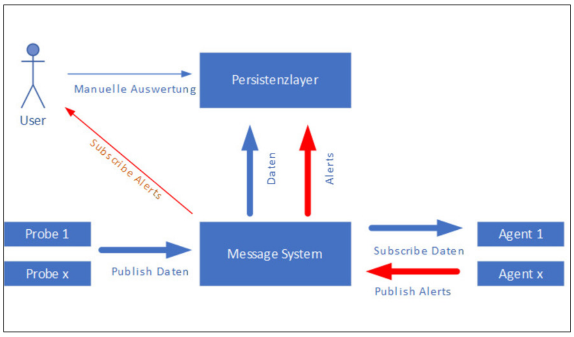
Janic
MIKES

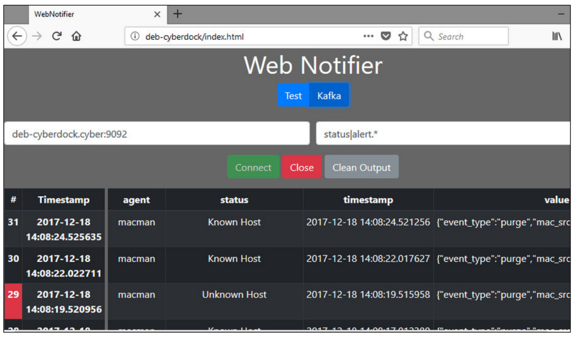
Marcel
Maeder

Students	Janic MIKES, Marcel Maeder
Examiner	Prof. Dr. Andreas Steffen
Subject Area	Security
Project Partner	Blue Diamond Asset Management, Pfäffikon, Schwyz

Cyber Security Integration Engine



Architecture Diagram



deb-cyberdock.cyber:9092

status|alert.*

#	Timestamp	agent	status	timestamp	value
31	2017-12-18 14:08:24.525635	macman	Known Host	2017-12-18 14:08:24.521256	{"event_type":"purge","mac_src
30	2017-12-18 14:08:22.022711	macman	Known Host	2017-12-18 14:08:22.017627	{"event_type":"purge","mac_src
29	2017-12-18 14:08:19.520956	macman	Unknown Host	2017-12-18 14:08:19.515958	{"event_type":"purge","mac_src

Screenshot WebNotifier

Introduction: Every company that is working with confidential data needs to fulfill certain regulations. Especially in the financial sector these requirements are crucial to a company's success. For small businesses this can become a severe problem. To help those small companies to fulfill these requirements we want to provide a prototype of an extensible software that will take care of such tasks.

Objective: The goal is to get a zero-configuration security box that is easily extensible and able to scale. It should collect necessary data and be able to determine a baseline on what is normal behavior on a client's network. To get started we want to be able to keep a list of machines communicating on the network. We will split the topic into three separate concerns. For the communication between the subsystems we will use a messaging system. Every information exchange goes through this system using messages. The probes are responsible for collecting potentially interesting information about a its environment. This could be network metadata or other kinds of information. The probe then publishes the gathered information into the messaging system. Agents subscribe to messages they are capable of analyzing. Based on these messages they investigate and publish their acquired information back to the messaging system so any other agent can reuse this information.

Result: In our lab environment we were able to collect and pass network activity data between multiple participants within our framework. We implemented a network probe and an agent that could detect an unknown device based on its mac address. We implemented this using two different messaging systems and compared these two in terms of implementation complexity and message throughput performance.

Test

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz