Title: Protecting Communications in SIEM Systems

Description

SIEM systems offer various capabilities for the collection and analysis of security events and information in networked infrastructures. A SIEM system integrates a number of components that can be organized (see Figure 1) as:

- Sensors: generate events and information about the target system and sends it to the collectors
- Collectors: collect, aggregate and normalize information in a standard format; this information is then send to the correlation engine
- SIEM correlation engine: aggregates and correlates the data to provide reporting and operational control
- Logger: digitally signs and forensically stores data

The goal of this project is to design a solution for the protection of the communication between the collectors and the correlation engine.

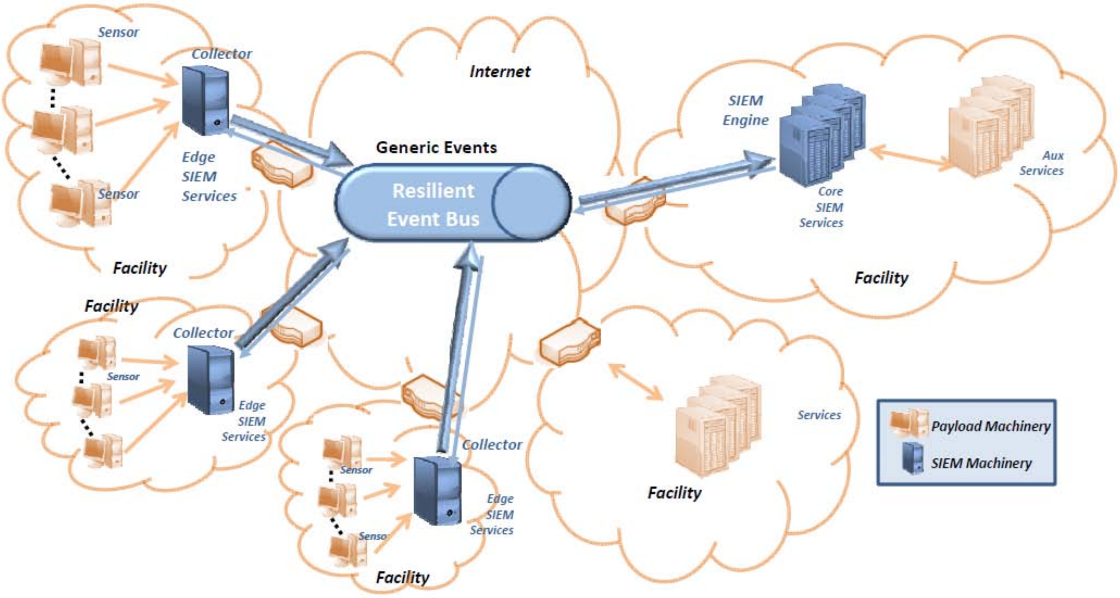

Figure 1: Architecture of a SIEM system.

Objectives

State of the art

Provide a (small) overview of the main SIEM products currently available on the market, with a special emphasis on the topic of the project. Potential examples are: AlientVault OSSIM, Cisco MARS, Q1 Labs QRadar, ArcSight EMS, RSA envision, Novell Sentinel.

Gap analysis

Identify limitations on the way communication is performed in these systems with respect to different kinds of failures.

Design a Solution

Provide an **initial** design for a Resilient Event Bus (REB), responsible for the communication among the collectors and the correlation engine. This feature is responsible for delivering events from the edge nodes (i.e., the collectors) to the core correlation engine despite the threats affecting the underlying communication network. Even though most of the traffic will be from the edge nodes to the core, in some cases, it might be necessary to send a few commands to the collectors (e.g., start to collect more data about some feature of the network). Therefore, the bus is bidirectional but asymmetric because most messages travel in one direction.

There are two main requirements on the resilient event bus should attempt to fulfill: 1) the bus should tolerate a large range of accidental and malicious failures; 2) messages should be transmitted respecting some delivery deadline. The objective is to make the events be processed at the correlation engine while they are (temporally) valid, which requires the communication subsystem to enforce (probabilistic) timeliness properties of the communication.

References

Use you favorite search engine and look for SIEM Systems.

http://en.wikipedia.org/wiki/Security_information_and_event_management

https://mosaicsecurity.com/categories/85-log-management-security-information-and-event-management