Secure and PrivaTE smArt gRid

(Grant Agreement No 787011)

D3.4 – Node-centric Reputation Models and Algorithms

2020-05-29

Version 1.0

Published by the SPEAR Consortium

Dissemination Level: Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787011

Document Control Page

Document Details

Document Version	**1.0**
Document Owner	CERTH
Contributors	UoWM
Work Package	WP 3 - Cyber Attack Detection in Smart Grid
Deliverable Type	Other (Software)
Task	Task 3.4 - Node-centric Reputation Models and Algorithms
Document Status	Ready for Submission
Dissemination Level	Public

Document History

Version	Author(s)	Date	Summary of changes
0.1	Odysseas Nikolis (CERTH)	2019-12-20	Definition of Table of Content
0.2	Thanasis Kotsiopoulos (CERTH)	2020-02-17	Update Table of content
0.3	Nikos Vakakis, Thanasis Kotsiopoulos (CERTH)	2020-02-25	Section 1 and Section 2 input
0.4	Panagiotis Radoglou (UOWM), Panagiotis Sarigiannidis (UOWM), Dimitris Pliatsios (UOWM), Stamatia Bibi (UOWM), Pantelis Angelidis (UOWM), Maria Diamantaki(CERTH)	2020-02-27	Contribution to Section 2
0.5	Thanasis Kotsiopoulos (CERTH)	2020-03-20	Section 3 and Section 4 input

0.6	Thanasis Kotsiopoulos (CERTH)	2020-04-27	Section 5 and Section 6 input
0.7	Dimos Ioannidis (CERTH)	2020-05-20	Comments and Technical Quality Improvement
0.9	Thanasis Kotsiopoulos (CERTH), Odysseas Nikolis (CERTH)	2020-05-22	Preparing the Document for peer review
1.0	Thanasis Kotsiopoulos (CERTH)	2020-05-29	Final version

Internal Review History

Reviewed By	Date	Summary of Comments
Vasilis Machamint - Eight Bells LTD (8BELLS)	2020-05-27	The quality deliverable is acceptable. A few sections of the document need to be modified.
Georgios Efstathopoulos and Vasilis Argyriou - 0 Infinity Limited (0INF)	2020-05-27	The quality of the deliverables is good. However, some comments attached inside the deliverable should be taken into account.

Legal Notice

Contents

Acronyms

Acronym	Explanation
AGVs	Automated Guided Vehicles
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
AUC	Area Under Curve
BDAC	Big Data Analytics Component
CAPEX	Capital Expenditure
C&C	Command-and-Control
CCS	Centralized Control System
CIA	Central Intelligence Agency
CSC	Collaborative Sensor-Cloud
DCS	Distributed Control System
DDoS	Distributed DoS
DF	Digital Forensic
DHS	Department of Homeland Security
DNS	Domain Name System
DoS	Denial of Service
DT	Decision Tree
FIFO	First In First Out
FP	False Positive
GLR	Generalized Likelihood Ratio
GOF	Grid OpenFlow Firewall
GTM	Grid Trusted Module
HAN	Home Area Network
HIDS	Host-based Intrusion Detection System
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
IAN	Industry Area Network

IFRA	Interactive Fuzzy Recommendation Aggregation
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information and Communications Technology
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
ISC	Independent Sensor-Cloud
IPS	Intrusion Prevention System
KNN	K-Nearest Neighbors
LOED	Locally Optimum Estimated Direction
LOUD	Locally Optimum Unknown Direction
MBR	Master Boot Record
MOA	Massive Online Analysis
MSC	Mutual Sensor-Cloud
MTU	Master Terminal Unit
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
OKB	Ontology Knowledge Base
One Time Signature	OTS
OPEX	Operational Expenditure
OSI	Open Systems Interconnection
PC	Personal Computer
PLC	Programmable Logic Controller
PPC	Public Power Corporation
QoS	Quality of Service
R2L	Remote to Local
RAM	Random Access Memory
REST	REpresentational State Transfer
RFC	the Request for Comment

Role Based Access Control	RBAC
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SIEM	Security Information and Event Management
Smart grid RbAC	SRAC
SMTP	Simple Mail Transfer Protocol
SPEAR-CHF	SPEAR Cyber Hygiene Framework
SPEAR-FRF	SPEAR Forensic Readiness Framework
SPEAR-RI	SPEAR Repository of Incidents
SPEAR-SIEM	SPEAR Security Information and Event Management
SVM	Support Vector Machine
TNR	True Negative Rate
TPR	True Positive Rate
TRSC	Testing, Research and Standards Centre
U2R	User to Root
V-IDS	Visual - Intrusion Detection System

List of Figures

List of Tables

Executive Summary

This document is a deliverable of the SPEAR project, funded by the European Commission (EC) under its Horizon 2020 Research and Innovation Programme (H2020).

It describes the intended achievement of the T3.4 Task, Trusted Platform Module. Grid Trusted Module (GTM) is a component of the SPEAR SIEM system that utilizes trust evaluation and management algorithms by applying node-centric reputation computation to all assets connected to the Smart Grid (SG) ecosystem. The task receives as an input the SPEAR SIEM system requirements from Task 2.2 and the user and security requirements from Task 2.1, while the output is the fourth layer of the SPEAR SIEM component. To this end, the system, user and security requirements of the GTM module are identified and a State-of-the-Art analysis is conducted on recent trust management and evaluation techniques. Based on the requirement identification and on the State-of the-Art analysis, the functionality, the inputs and the outputs of the GTM component are derived and documented.

The work done in this task mainly affects WP3 components such as SPEAR V-IDS. Concretely, the GTM component receives its input from the SPEAR Message Bus. The Message Bus contains anomalous events as they are detected by the SPEAR SIEM Basis, the SPEAR SIEM V-IDS and the SPEAR BDAC components. The GTM processes each anomalous event and produce a trust value for the affected assets of the SPEAR system. The trust management is node-centric and the trust is evaluated for all the assets of the system, by utilizing Fuzzy Logic. Different decision criteria for the trust evaluation are considered (e.g. the severity of the event, the time window between two consecutive anomalous events of an asset, the event priority, and the event reliability). The output of the GTM component is send to the SPEAR V-IDS via RESTful services. The output of the GTM is also stored in the GTM Database in order to store historic data about the trust evaluation of the system nodes. The communication with GTM Database is achieved through RESTful services.

In a nutshell, in Task 3.4 Fuzzy Logic is encapsulated in the GTM functionality for trust evaluation purposes. In comparison with existing frameworks which are not completely related to SG domain, the SPEAR GTM component takes into consideration multiple different criteria for evaluating trust and can sufficiently deliver a trust evaluation scheme in an efficient and accurate way.

1. Introduction

1.1 Purpose of this Document

The scope of this deliverable is to describe the work done and the research conducted in Task 3.4 Trusted Platform Module. The work has been carried out in Work Package 3 (WP3), "SPEAR Secure & PrivatE smArt gRid". Grid Trusted Module (GTM) is a component of the SPEAR SIEM system that utilizes trust evaluation and management algorithms by applying node-centric reputation computation to all assets (interfaces, devices, meters and gateways) connected to the SG ecosystem. This report will include at first an overview of the GTM functionality as well as an overview of the integration with the other SPEAR SIEM components.

1.2 Structure of this Document

The report provides an overview of the role of the GTM component in the SPEAR system, a description of the design and interfaces of the GTM and its dependencies on other components, specifically the SPEAR Message Bus and V-IDS. The document is structured as follows:

- Section 2 describes the State of the Art in trust management and trust evaluation.
- Section 3 presents the major inputs and outputs of the GTM module, as well as the functional and non-functional requirements used to develop the GTM component.
- Section 4 illustrates the architecture of the GTM component in details. At first, the functional process unit is described. At second, the integration with the SPEAR Message Bus and SPEAR V-IDS is presented.
- Section 5 provides the hardware and software prerequisites for the GTM deployment.
- Section 6 presents the unit testing of the GTM component while, section 7 concludes the deliverable and describes the future work.
- Section 7 illustrated the innovation summary of the work done in task 3.4/
- Section 8 concludes the Deliverable.

1.3 Relation to other Tasks and Deliverables

Task 3.4 receives the SPEAR SIEM system requirements from Task 2.2 and the user and security requirements from Task 2.1, in order to provide the fourth layer of the SPEAR SIEM component, the Grid Trusted Module. In all, deliverable 3.4 outputs the fourth layer of the SPEAR SIEM component. Analytically, the following deliverables support this deliverable and are referred to in this document:

- D2.1 User, Security and Privacy Requirements [1]: This deliverable is the output of Task 2.1 and defines the user, security and privacy requirements of the whole SPEAR Platform, including the SPEAR V-IDS related components (i.e. outcome of this deliverable) from the user needs and regulatory framework upon which the platform will operate.

- D2.2 System Specifications and Architecture [2]: This deliverable is the output of Task 2.2 and defines the functional and non-functional system requirements of the whole SPEAR Platform, including the SPEAR V-IDS related components, using as basis the user, security and privacy requirements of D2.1. It also describes the SPEAR Platform architecture; hence it explains how the SPEAR V-IDS related components fit in the complete SPEAR Platform architecture and how it relates to other SPEAR components.
- D3.1 Initial SIEM System [3]: This deliverable is the output of Task 3.1 and describes the architecture and the implementation of the SPEAR SIEM Basis. The SPEAR V-IDS receives data from SPEAR SIEM Basis through the Smart grid pre-processed data ingestion sub-component and illustrated with the use of visualization algorithms.
- D3.2 Multi-factor and Open Analytics Engine for Smart Grid Ecosystem [4]: This deliverable is the output of Task 3.2 and describes the functionalities and the algorithms deployed for the BDAC deployment which forwards data to the SPEAR V-IDS.
- D3.3 Open Visual-aided Intrusion Detection System [5]: This deliverable is the output of Task 3.3 and presents the final version of the visualization techniques that have been applied for network analysis and have been integrated in the IDS in the context of the SPEAR project.

2. State of the Art in Trust Management and Trust Evaluation

Academia has investigated many solutions aiming to analyze the trust level of various assets as well as their relationships. Below several research efforts dealing with trust and reputation calculation mechanisms are analyzed. Each paragraph describes a different case. These papers were used as initial thoughts for the development of GTM.

The authors in [6] presented a fuzzy logic trust model to detect untrusted nodes in smart grid networks and compared it with weighted-sum trust model. The trust evaluation is implemented in four categories. The first category is Direct Trust where, Node i computes absolute trust by observing its one-hop neighbors directly (node n, node m). The second category is Recommendation Trust where, node i calculates trust value for neighboring two-hops (node j) using the common neighbors 'recommendations (node m, node n). The fourth category is Indirect Trust where, node i calculates trust value for non-neighboring nodes (node k) using recommendations of other nodes.

James et al in [7] collected a dataset containing system logs from a Smart Grid. They used a set of machine learning and statistical methods and proved that the establishment of trust levels between substations using behavioral pattern analysis is possible. For the preprocessing of the dataset the Principal Component Analysis is implemented while, the machine learning techniques Block Entropy Analysis and Feature Centric Entropy Analysis are utilized to extract the probability of an event captured in syslog files, to contain threat about the SG security.

Aref et al in [8] developed a trust-building model that uses a multi-criteria (multidimensional) approach to help trustees in the IoA environment change their behaviors to improve their perceived trustworthiness, and gain more trusted interactions. The model calculates the requisite improvement per criterion when there is only one aggregated satisfaction value per interaction, where the model tries to predict both the correct value per criterion and its significance.

In [9], the authors developed a system encapsulating the Bayesian theory with Dempster–Shafer theory (BDST), to handle physical layer (transmission rate of the node) and medium access control (MAC) layer (buffering capacity of the node) metrics in order to calculate trust at node level for packet delivery. Each node calculates its neighbors trust and routes the data packet in a trustworthy route. When a node detects another node as faulty / malicious, it selects an alternative, trustworthy path to route data packets during the routing process. The proposed model considers malicious attacks such as packet dropping, bad-mouthing and on-off attacks affecting both data integrity and network availability

The authors in [10] proposed three types of trust-based communication mechanisms for sensor-cloud. The three types of trust-based communication mechanisms are independent sensor-cloud (ISC) mechanism, collaborative sensor-cloud (CSC) mechanism, and mutual sensor-cloud (MSC) mechanism. The reputation value thresholds of the system's nodes are defined by the Wireless Sensor Network and the cloud independently. The communication mechanisms are validated with the tool NetTopo.

Mendoza and Kleinschmidt in [11] developed a trust management system based on the computation of service quality and on recommendations from neighbors. The nodes locally compute the trust of their

neighbors, without the need of a central entity. The system is validated in the Cooja simulator of the Contiki operating system.

Selvaraj et al in [12] proposed an evidence-based trust model to determine contextual trustworthiness on cloud environment services. The trust model uses fuzzy logic to derive trust value to manage uncertainty and uses induced ordered weight averaging operator to aggregate the trust values, allowing this way real-time efficiency to be achieved.

Naderan et al in [13] proposed a trust management system for the social networks. At first, for every pair of social network users the feature vector is determined. Fuzzy logic is then implemented to assign trust membership to a particular class, according to classification of two, three and five classes. Eventually, three machine-learning methods, namely Support Vector Machine (SVM), Decision Tree (DT), and k-Nearest Neighbors (kNN), are used to identify user confidence values.

In [14], broker-based trust evaluation framework that focuses on identifying a trustworthy fog to fulfill the user requests is utilized. Fuzzy logic is used as the basis for the evaluation while considering the availability and cost of fog. The Request Matching algorithm is also proposed to identify a user request, and the Fuzzy based Filtering algorithm is implemented to match the request with one of the predefined sets created and managed by the broker.

The authors in [15] presented a robust and configurable trust management toolkit that facilitates the operation of SG systems in the presence of malfunctioning components. The toolkit utilizes reputation-based trust over network-flow algorithms to identify and mitigate untrusted communication components. To achieve this, the toolkit assigns trust values to all protection nodes. Faulty nodes, that correspond to a malfunctioning component or communication system, are assigned a lower trust value that indicates a higher risk of failure to mitigate detected faults. To demonstrate and evaluate the proposed toolkit, the authors carried out a series of simulations, comparing enhanced backup and special protection systems to unenhanced systems via an analysis of variance analysis. The simulation results indicate the efficiency of the proposed trust management toolkit in protecting SG systems.

In order to minimize the Capital Expenditure (CAPEX) and the Operational Expenditure (OPEX), only a limited number of nodes, called trust nodes, are equipped with trust functionalities. Hasan and Mouftah [16] proposed a trust system placement scheme that aims to defend SG networks by deploying the minimal required number of trust nodes. The scheme utilizes a heuristic algorithm based on the Minimum Spanning Tree (MST) partitioning problem to segment SG networks. The numerical results indicate that the proposed scheme ensures SG protection by leveraging topology-aware trust node selection. In addition, the proposed scheme is compatible with both types of cybersecurity planning approaches, e.g., a) optimal placement for a given number of trust systems, while the number of segments is unknown, and b) optimal location for a given number of segments, while the number of trust systems is unknown.

The authors in [17] designed a generic security architecture for ecosystems where heavily interconnected distributed devices collect, exchange, and process sensitive data. In addition, the authors identified the representative security requirements for such distributed systems and incorporated a trust factor for the devices, as well as the communication and data exchange. lifecycle. On the device-level, a trusted connector is proposed that isolates sensitive execution environments in order to protect the integrity of

the software stack, securing the sensitive data from malicious third parties. Finally, for demonstration purposes, the authors implemented a full-fledged prototype of the proposed secure architecture.

Allahbakhsh et al. [18] proposed a trust-based experience-aware method for the aggregation of fuzzy recommendations. The proposed approach utilizes an iterative technique, called Interactive Fuzzy Recommendation Aggregation (IFRA), for computing rating scores for online services based on fuzzy recommendations. The approach also takes into account trustworthiness and experience level of raters for calculating rating scores and employs an iterative technique for combining recommendations, so that the obtained rating scores are robust against manipulations, due to the global nature of iterative algorithms. The authors assessed the performance of IFRA using a real-world dataset and compared it to well-known alternatives. The evaluation results indicate the promise of IFRA and its capabilities in dealing with fuzzy recommendations.

The work in [19] investigates the optimal security deployment problem in resource-constrained industrial networks. Two schemes are proposed for the inline deployment of security devices, namely link coverage maximization and minimal path tolerance. The first scheme focuses on the overall monitoring coverage and is formulated as a quadratic assignment problem, while the second scheme focuses on the hop distance between consecutive trust nodes and uses a heuristic approach that deploys trust nodes in a distributive manner. Both of the proposed schemes are evaluated considering an IEEE testbed under various scenarios, while the numerical results demonstrate that the proposed schemes are capable of achieving their goals. Additionally, the results reveal a performance tradeoff between the proposed schemes in highly resource-constrained scenarios, where the second scheme provides better distributiveness.

The authors in [20] presented a unified trustworthy environment based on edge computing that can timely detect malicious service providers and service consumers, filter unreal information and recommend credible service providers. Edge computing is introduced as an effective service access point since it supports collecting service records to perform trust evaluations. Moreover, a service selection method is designed to choose the corresponding trustworthy and reliable service providers based on the trust evaluation and the recording criterion, which has distinct advantages in the succinct trust management, convenient searching service, and accurate service matching. The experimental results validated the feasibility of the proposed trustworthy environment.

Liu et al. [21] studied the network security and data redundancy of industrial environments and proposed a trust-based active detection (TBAD) scheme for improving the reliability of collecting data packets and reducing the data redundancy data collection security protocol. In the proposed scheme, each node's trust is evaluated by neighbor nodes, and the evaluation is added into data packets. A node is considered suspicious if the trust evaluated by its neighbors is unreliable. The authors compared the proposed scheme with conventional protection schemes in order to evaluate its performance. The results indicate that the proposed scheme features higher security and energy efficiency, and lower data redundancy.

Velusamy et al. in [22], studied the network security and data redundancy of industrial environments and proposed a trust-based active detection (TBAD) scheme for improving the reliability of collecting data packets and reducing the data redundancy data collection security protocol. In the proposed scheme, each node's trust is evaluated by neighbor nodes, and the evaluation is added into data packets. A node

is considered suspicious if the trust evaluated by its neighbors is unreliable. The authors compared the proposed scheme with conventional protection schemes in order to evaluate its performance. The results indicate that the proposed scheme features higher security and energy efficiency and lower data redundancy.

Wang et al. [23] presented a mobile edge computing-based intelligent trust evaluation scheme to comprehensively evaluate the trustworthiness of sensor nodes using a probabilistic graphical model. The proposed approach evaluates the trustworthiness of sensor nodes from the data collection and communication behavior. Moreover, the moving path for the edge nodes is scheduled to improve the probability of direct trust evaluation and decrease the moving distance. The experimental results indicate that the proposed intelligent trust evaluation approach can effectively distinguish compromised and malicious nodes, while also decreasing the energy consumption of the entire network. In addition, compared to traditional moving schemes, the proposed moving algorithm can effectively reduce the moving distance, thus further decreasing the energy consumption.

A trust-based team formation framework for mobile intelligence in industrial environments that utilize Automated Guided Vehicles (AGVs) is presented in [24] The authors defined a trust measure based on the reliability and reputation of AGVs, that are computed based on the feedbacks released for the AVG activities in a factory. Furthermore, the authors designed a trust framework exploiting the defined measures to support the formation of virtual, temporary, and trust-based teams of mobile intelligent devices. Finally, the authors carried out experimental evaluations using an industrial scenario in order to highlight the feasibility of the proposed framework.

Table 1 presents the strengths and the reported challenges for every solution. In a nutshell, the SPEAR GTM is developed to assess the reputation of each asset of the SG network based on Fuzzy Logic. Fuzzy theory has a special advantage from the classical theories. In classical theories, every variable is defined in a strictly manner, but in fuzzy logic each variable has a membership level. In GTM, the Fuzzy Logic is utilized to quantify the anomalous events and produce a dynamic reputation value for every asset of the system based on the received anomalous event and on the time difference between two consecutive anomalous events. The time difference is taken into consideration because a node with fewer anomalous events than a node which receives consecutive anomalous events, cannot have the same reputation degradation. In contrast with the analysed methodologies in Section 2, our solution is the only one which process time in order to produce reputation and it is asset agnostic. One important difference with the other developed solutions is also that our engine generates alerts about the condition of each asset and about the reputation of the system in general. More information about the GTM alerts are given in Section 4.2.2.

Reference No	Strengths	Reported Challenges
[6]	• A novel trust model based on fuzzy logic is proposed • An adaptive strategy for trust evaluation is developed	• Traditional security schemes are inadequate in detecting internal attacks • The weighted-sum methodology cannot be adopted by the smart grid as it is too complex and requires high processing capabilities

[7]	• The proposed approach does not rely solely on qualitative values for trust level assignment • Each node's trust level is based on statistical anomaly detection of local data • A real-world grid substation is utilized for the evaluation of the approach	• Fuzzy logic approaches assume that evidence supporting trust decisions is fuzzy in nature • Approaches based on the statistical reputation of nodes is centralized, therefore the system resilience is not guaranteed
[8]	• A multi-criteria model, that leads to more accurate trust evaluation, is proposed • The proposed model uses the provided feedback from trustors regarding how satisfied they were with recent transactions to predict the importance of different service dimensions for trustors, and adjust the trustee behavior accordingly	• Most trust establishment models are numerical models that use deterministic approaches to calculate trust levels • Models based on multiple trust criteria are more complicated and require higher computational capabilities • Centralized trust models may experience scalability and performance issues
[9]	• The authors combined Bayesian, Dempster-Shafer, and Fuzzy theories for establishing secure routing in SG • The proposed approach can evaluate the trustworthiness of both nodes and links • The use of simple mathematical equation makes the proposed approach suitable for implementing in real-time communications	• Internal attacks cannot be prevented by cryptographic authentication mechanisms • Authentication mechanisms have high complexity and cannot be realized in smart grid devices with limited resource • The existing identity-based security approaches are incompatible and inadequate to address the security challenges of the smart grid
[10]	• Three types of trust-based communication mechanisms for the sensor-cloud are proposed • The authors show that trust-based communications can greatly enhance the performance of sensor-cloud	• Trust evaluation for nodes that feature high-mobility is challenging

[11]	• The proposed model utilizes QoS for trust composition, weighted sum with direct and indirect observations for trust aggregation, and event-driven trust updates • In this model, the nodes are able to manage the trust values with respect to the services provided by the other nodes • A distributed approach is adopted, where each node has an autonomous and independent behavior in the trust evaluation	• Novel trust management mechanisms have to be designed, as IoT devices have limited processing, storage, and power resources • The trust model has to consider the heterogeneity of the network
[12]	• The authors proposed a dynamic evidence-based trust model that evaluates the trustworthiness of cloud services • The proposed trust model has high flexibility and can be used for existing, as well as upcoming services, making it suitable for dynamic cloud environments	• The rapidly growing trend of a dynamic cloud as the front runner introduces the need for an efficient trust management • Existing trust management systems are inadequate for cloud environments, as these environments consist of diverse applications • The existing tools and mechanisms have contributed a partial view of cloud trust but still lack knowledge on how the entities work together to form a trusted system
[13]	• The authors utilized a feature vector that combines both the structural and network properties • The proposed approach also includes a preprocessing stage, where the raw information is converted into a feature vector	• The optimal determination of each factor's weight, in order for the model to provide accurate evaluation, is challenging
[14]	• A novel fuzzy-based broker trust evaluation framework is proposed, that is able to optimally assign user requests to trustworthy fog devices	• Fog computing has low redundancy and vulnerable to certain cyberattacks • Trust management in computing of distributive and ubiquitous nature can be complicated especially without a central entity • The use of brokers in the trust evaluation process for fog computing is limited

[15]	• The proposed toolkit is based entirely software-based and can be easily deployed in smart grid environments • The toolkit can also augment existing protection schemes in order for them to more robust against failures and malfunction • The identification of malfunctioning nodes can be integrated into the protection schemes to allow them to operate through such failures	• The trust management toolkit requires an existing communication infrastructure and high computational resources
[16]	• The proposed approach is computationally lightweight • The proposed scheme can also be used to estimate the minimum number of trust nodes required to protect SCADA networks • The proposed scheme offers better quality of protection using topology-aware trust node selection	• Only a selected number of nodes can host trust systems due to budgetary constraints • The trust system can be unavailable for some reasons such as capacity outage, system failure, and link failure
[17]	• The solution is a generic security architecture for ecosystems where heavily interconnected devices in distributed networks exchange, gather and process sensitive data • The proposed approach includes a holistic security architecture, the trust ecosystem, for the system's identity and trust management, its data, application and device lifecycle, as well as secure device-to-device communication	• Creating trust management in decentralized IDS ecosystems requires a concept for the root of trust and a clear definition of trust boundaries, as well as the definition of secure gateways, the IDS connectors, between those trust boundaries

[18]	• The proposed approach provides a method for converting fuzzy recommendations to crisp values based on the membership function of the fuzzy variable as well as the trust and experience of the rater • The proposed scheme introduces a new algo n iterative algorithm, called IFRA	• Due to the large number of recommendations, it is not possible to rely on solutions such as defuzzification. • Several pieces of evidence show that credibility of a recommendation also depends on a lot of factors, which must be considered while converting a fuzzy recommendation to a number
[19]	• The proposed schemes utilize trust systems' active/router mode of operation, whereas the existing schemes in the literature are most likely appropriate for the tunnel/gateway mode • A constrained quadratic assignment problem (QAP) formulation is introduced to maximize the security monitoring coverage of SCADA backbone networks. • A new metric named path tolerance is introduced to evaluate the security of routes in a communication network	• Due to budgetary constraints, only a selected number of trust nodes are deployed in a large-scale SCADA network • An optimal deployment strategy is required to enhance quality of security service (QoSS) in a resource-constrained network.
[20]	• The proposed scheme provides a fine-grained recording criterion based on the services of service providers and the requirements of service consumers are designed • The proposed scheme provides a platform which provides a trust evaluation and service selection mechanism for service selection with a lot of storage and computing resources	• There is no unified and fine-grained trust evaluation mechanism to deal with the threats of internal attack and improve QoS of IIoT

[21]	• In the proposed approach, the trust of sensor nodes not only is evaluated by neighbor nodes, but also is evaluated by the UAV according to the reliable of collecting information • The proposed approach has lower data redundancy and network security	• Most trust management techniques process a lot of redundancy data which affects the determination of malicious nodes
[22]	• The proposed trusted model evaluates the stability of the link by calculating the trust of the link to carry the data using fuzzy theory • The proposed trusted routing algorithm enriches trust evaluation with a logarithmic punishment factor	• Evaluating trust by different adversarial attacks on wireless network is promising • The method is applicable for application scenarios like vehicle to grid (V2G) and grid to vehicle (G2V) communication
[23]	• The proposed approach introduces mobile elements in SCS-enabled industrial IoT to conduct trust evaluation • The new architecture connects underlying network and cloud, and provide more find-grained management for underlying sensor nodes	• Existing cloud computing models cannot provide direct and effective management for the sensor nodes. • The centralized trust management increases the energy consumption of the network • Decentralized trust management systems which are based on AI cannot be implemented on the sensor nodes due to their limited computing and storage capabilities
[24]	• The authors present a trust model for the Automated Guided Vehicles in Smart Factories that defines the devices' reliability, reputation and trust measures with respect to the activities they perform on the production-line.	• The proposed scheme is not evaluated in a real-world situation

Table 1 Strengths and reported challenges of the SoTA methodologies

3. Requirement Analysis of GTM

Section 3 analyses the GTM requirements and the inputs-outputs of this SPEAR component. First, the major inputs and outputs of the GTM module are presented. Afterwards, the functional requirements and non-functional requirements token under consideration for the GTM implementation are described. The design and the implementation of the SPEAR GTM were driven by the project's requirements. The main requirements - categorized as functional and non-functional – are listed below.

3.1 Major Inputs and Outputs

Section 3.1 is denoted in presenting the major inputs and outputs of the GTM component. Concretely, information about the GTM inputs about the anomalous event parsing as well as the major outputs of the GTM component are described.

3.1.1 Major Inputs

The GTM inputs are categorized into three main classes. The input of anomalous events as generated by the SPEAR OSSIM, BDAC and VIDS and the REST API to discover the assets of the SPEAR system and the reputation values per asset given as threshold by the security engineer, in order to raise alerts about the reputation of a node. Figure 1 presents the schematic diagram of the GTM inputs.

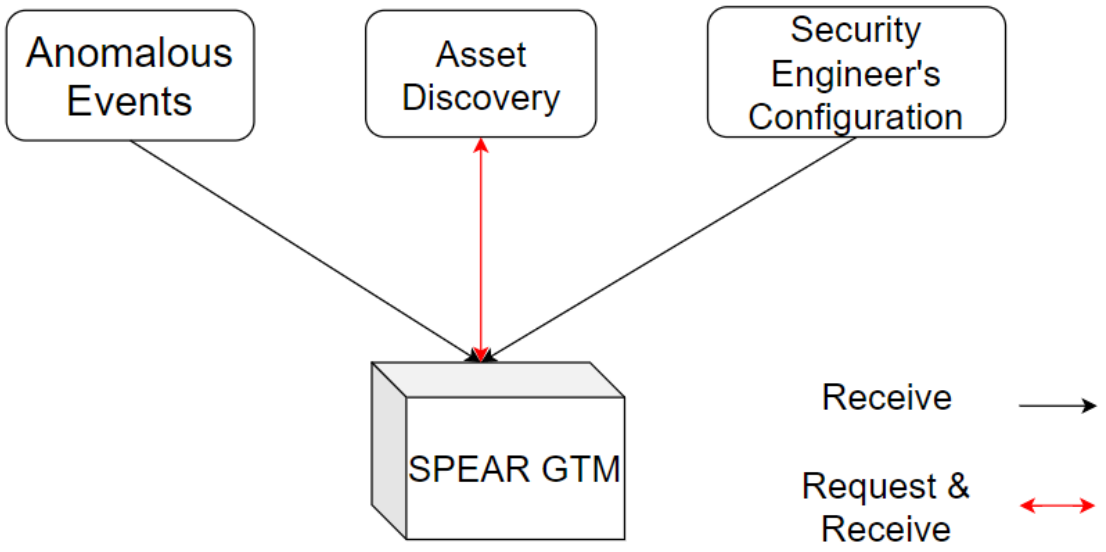


Figure 1 The inputs of the SPEAR GTM

The GTM receives the anomalous events, processes them and produces the output as it is defined in section 3.1.2. Periodically it requests to the asset discovery REST API the identity of the SPEAR assets, because the GTM must take under consideration if the corresponding anomalous incident belongs to a registered asset or not. Last but not least, the engine receives the security engineer's configuration containing the security threshold for raising an alert if the reputation value exceeds it.

3.1.2 Major Outputs

The outputs of the GTM component are presented in Table 2.

Fields	Origin	State	Description
Reputation Value	Generated in GTM	Necessary	Reputation Value of the node.
Node ID	Obtained from Asset List from SPEAR SIEM Basis	Necessary	Node Unique Identifier acquired from the Asset List provided by OSSIM Alien Vault with a REST API.
Node IP	Obtained from Asset List from SPEAR SIEM Basis	Necessary	Node IP acquired from the Asset List provided by OSSIM Alien Vault with a REST API.
Asset Location	Obtained from OSSIM Alien Vault Event format	Necessary	The location of the asset. This field is exactly the same with the field in OSSIM Alien Vault Event format.
Reputation Change Speed	Generated in GTM	Necessary	How much the reputation value of the node decreases or increase compared to the last reputation value.
Timestamp	Generated in GTM	Necessary	Timestamp generated after the calculation of the new reputation value.
Asset Value	Obtained from OSSIM Alien Vault Event format.	Necessary	Asset Value is the value (0 to 5) that each SG organization assigns to a specific asset that is connected to an event. This field is exactly the same with the field in OSSIM Alien Vault Event format.
Alerts	Generated in GTM	Optional	Alert is generated if the reputation value drops under the threshold defined by the End User

Table 2 The output of the GTM

3.2 Functional Requirements

In Table 3 are presented the Functional requirements token under consideration for the development of the GTM as they are addressed in the Deliverable 2.2.

Requirement	Short Description	Coverage
F01- Assets Protection	The SPEAR platform must be able to collect and analyse information for each asset of an	The fields Node_ID, Node_IP, priority, reliability, risk and asset value from each security

	environment, thus being able to detect possible security events.	event are used to collect and analyse information for each asset of the environment.
F03 - Data Transmission	The SPEAR Platform should support high-throughput data transmission between the data sources and the SPEAR SIEM components.	The GTM receives and transmits high-throughput data successfully.
F08 - Encrypted communications	In order to protect communications, SPEAR components should communicate with each other using encryption methods. The utilization of strong cryptographic protocols and algorithms will support end-to-end encryption, which will ensure that only the communicating components can have access to the content of the communication.	The REST APIs are transmitting data through SSL. The authorization of the communication is implemented with JSON Web Tokens. All passwords are encrypted with the SHA2 protocol.
F33 - VIDS Visual Analytics interconnection with GTM	The VIDS Visual Analytics back-end services should interconnect with GTM	The GTM is able to interconnect with the V-IDS via RESTful APIs. GTM can publish reputation values and alerts to the V-IDS and the V-IDS can obtain historic data.
F34 - Asset Reputation	A reputation score that characterises the behaviour (malicious or legitimate) of this asset.	The GTM processes the incoming anomalous event and produces the reputation value of an asset based on three different systems inside the GTM component. More information about the functional process of the GTM is given in section 4.2.1.
F35 - Trust Asset Alerts	Two different alert types that indicate that 1) the node reputation goes below a predefined threshold, 2) the rate of decrease of the node reputation exceeds a predefined threshold.	The GTM through a RESTful API informs the end user with alert messages if the node reputation goes below a predefined threshold and/or if the rate of decrease of the node reputation exceeds a predefined threshold.

F36 - Trust System Alert	A system-wide alert that informs the administrators about the number of assets that have been compromised, aiming to accelerate the investigation of an incident before it compromises the entire system.	The GTM through a RESTful API informs the end user about the number of assets that have been compromised. The compromised nodes are the ones whose reputation goes below a predefined threshold and/or if the rate of decrease of the node reputation exceeds a predefined threshold.

Table 3 Functional Requirements of GTM

3.3 Non-Functional Requirements

In Table 4 are presented the non-Functional Requirements of GTM token under consideration for the development of the GTM as they are addressed in the Deliverable 2.2.

Requirement Number	Short Description	Coverage
NF01 - Optionality	The SPEAR platform should be able to operate under as many OSes as possibly	The GTM module is written in the open source Python Language version 3.7. All the libraries used to create the module are also open-source. The module can be installed in all OSes able to run Python.
NF02 - Scalability	The SPEAR platform must be expandable by adding assets	The GTM dynamically retrieves the asset list of the SPEAR system through a REST API, in order to be aware about the assets of the system and any changes that may occur.
NF04 - Password Encryption	The SPEAR solution should make use of encryption to ensure that data is stored securely. The system should not store user passwords in plain-text.	Sensitive data such as passwords and authentication tokens are encrypted with SHA2 hash.
NF05 - Data Encryption	The SPEAR solution should not allow, when possible, any data transmission of sensitive information without encryption	The data that is transferred from/to the FTM to/from the other SPEAR components are transmitted over SSL.
NF08 - Bandwidth	Communication among the SPEAR components should not	The connections between GTM and the rest SPEAR components are deployed by using best

	impose a significant load on the LAN or WAN bandwidth.	practices and mature methodologies. However, the status of the network in the pilot/user premises might negatively affect the communications between the SPEAR components.

Table 4 Non-Functional Requirements of GTM

4. GTM Design & Architecture implementation

Section 4 describes the architecture and the design of the SPEAR GTM and it is the most extensive section of the deliverable, as it contains detailed description of the developed component.

4.1 Objective and overview

Grid Trusted Module is the fourth component of the SPEAR SIEM. Its main purpose is to assist the SIEM in analysing security threats, providing reputation value - derived from the security threat analysis - for every asset of the SPEAR system.

GTM component is designed after an extensive research on well-known reputation algorithms and schemes. Together with the GTM component, the trust management database is developed, containing historic data about the reputation values of each asset.

4.2 GTM Architecture

Section 4.2 describes in extent the architecture of the GTM component. At first, the process to extract reputation values is described. At second, the GTM interfaces with the other components are presented. Finally, the GTM Database is presented and analyzed.

Figure 2 illustrates the components of the GTM architecture. The GTM integrates with the Message Bus in order to receive the anomalous events. The engine receives the identity and the security thresholds for raising alerts for each asset of the system by V-IDS, via the REST API deployed by CERTH and stores them in the database. The anomalous events are getting processed by the GTM Functional Process Unit and the GTM output, as defined in section 3.1.2, is sent to the V-IDS. Then, the reputation values are registered into the GTM Database in order to acquire historic data about the trust evaluation of an asset. To sum up, the V-IDS can also obtain historic data about the reputation values of each asset by the provided REST API from the GTM side.

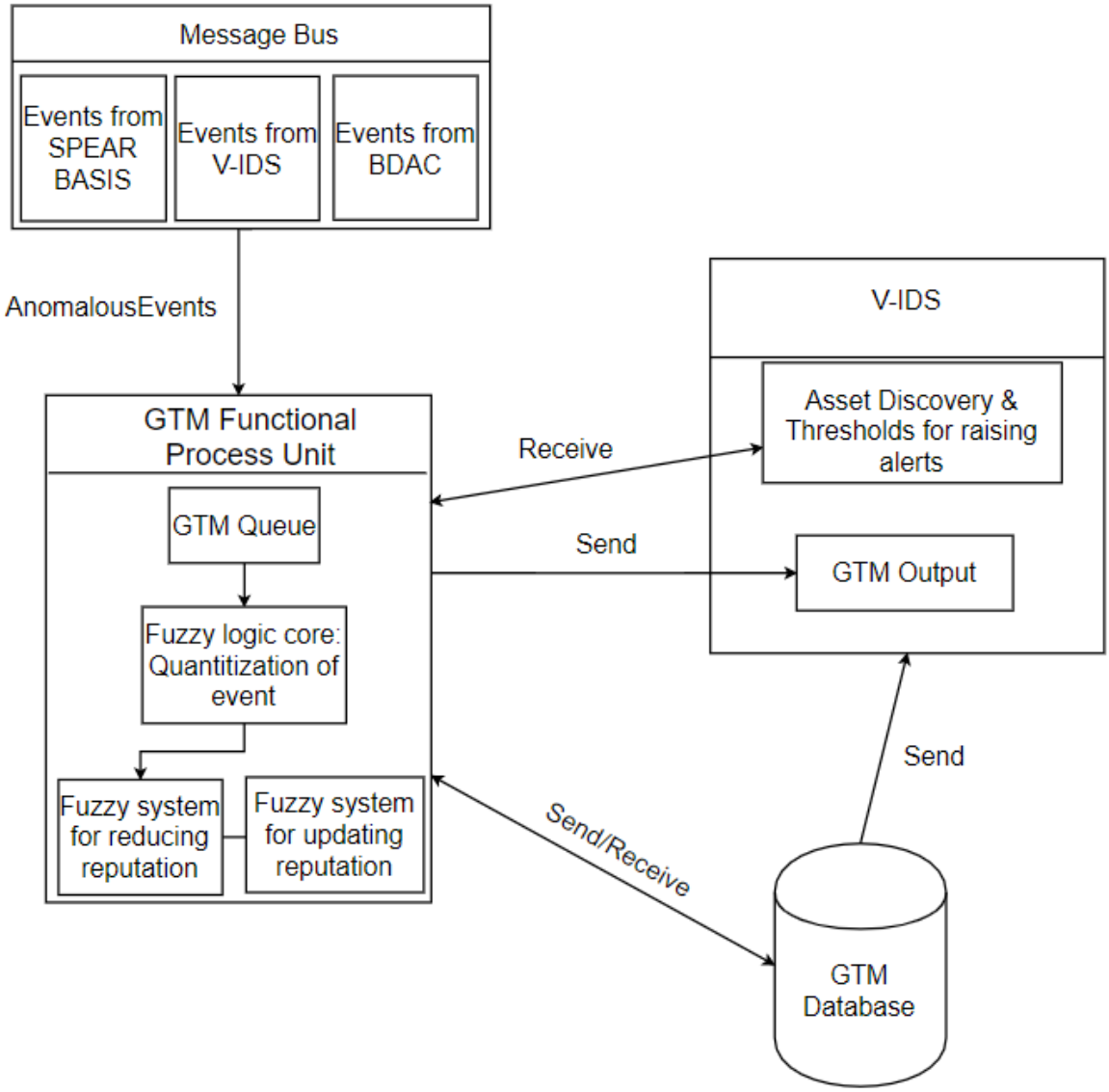


Figure 2 Components of GTM Architecture

4.2.1 Functional Process Logic

Section 4.2.1 provides the description of the Functional Process Logic of the GTM engine. Initially, the GTM receives the alert configuration for each asset, as well as its identity and its name from the V-IDS REST API. The above information is saved into the database. Each time there is a change in the configuration of an asset, the corresponding data are updated in the database. If there is no record matching the saved configuration of an asset in the database, then a new record is created. Initially, all the reputation values of the system are set with a trust value equal to 100. The GTM engine consists of four individual systems:

- The GTM queue, which implements a FIFO prioritization to the incoming events.

- The fuzzy logic core, which quantifies the detected anomalous incident.
- The fuzzy reputation reduction system, which delivers the reputation value of the asset based on the time window between the former event and the quantified value.
- The fuzzy reputation recovery system, which works in parallel with the other two systems and is responsible for recovering the reputation of the nodes.

The GTM is continuously listening to the Message Bus for anomalous events. The anomalous event is entered in the GTM queue which implements a FIFO prioritization. Next, the event exits the GTM queue and gets processed by the fuzzy logic core to quantify the incoming event. The time difference from the previous reputation reduction until the present time for the specific node is retrieved from the GTM database and the final reputation value is derived by the fuzzy logic system for reputation reduction. In parallel, the GTM system for reputation recovery is working to update the trust value of the system nodes, which are not affected by an anomalous incident. Extensive information about the operation of each system is given in the following sections.

4.2.1.1 Fuzzy Logic Core

The Fuzzy Logic Core quantifies the incoming anomalous incidents using Fuzzy Logic and by taking into consideration the OSSIM fields: asset value, the subcategory (Brute Force, Data injection etc) of the event, the event risk, the priority and the reliability. Table 5 illustrates an example of an anomalous event referring to a detected cyberattack. In this purpose, the Fuzzy Theory is utilized by GTM in order to map the value of each independent variable into a quantified value without specifying rules in a strict manner.

Fields	Value	Quantified value
Asset Value	5	15.42
Priority	5	
Reliability	9	
Risk	2	
SubCategory	Brute Force	

Table 5 The Fuzzy Logic Core application in GTM

Indicative examples of the fuzzy logic rules are illustrated in Table 6. All the rules of the fuzzy logic core are presented in the Appendix section. The Fuzzy Logic Core rules are asset agnostic and general for every system. Their main purpose is to quantify the severity of the detected anomalous event from 0 (low) to 100 (high).

Rule #No	Input[1]	Output: Quantified Value
Rule1	asset_value: high & priority: high & event_risk: high & subcategory: high & reliability: high	quantified_value: low
Rule2	asset_value: low & priority: low & event_risk: low & subcategory: low & reliability: low	quantified_value: high
Rule3	asset_value: high & priority: high & event_risk: high & subcategory: high & reliability: medium	quantified_value: low

[1] This input vector follows the schema described in Table 5.

Rule20	asset_value: high & priority: medium & event_risk: high & subcategory: high & reliability: high	quantified_value: low
Rule21	asset_value: high & priority: medium & reliability: high & subcategory: high & event_risk: medium	quantified_value: low
Rule 22	asset_value: high & priority: medium & reliability: high & subcategory: high & event_risk: low	quantified_value: medium

Table 6 Indicative rules of Fuzzy System 1

The rules are derived by forming the fuzzy universe. The fuzzy universe is unique and mandatory for every variable used to calculate the quantified value of the anomalous event. The fuzzy universe is also mandatory for the quantified value. In order to form the universe of each variable, the limitations about the minimum values and maximum values are considered. For example, the variable "reliability" can only take values from zero to ten, as it is defined by SPEAR OSSIM. Indicative examples of the reliability's universe-a variable used to compute the quantified value- and the quantified value's universe are shown in Figure 3.

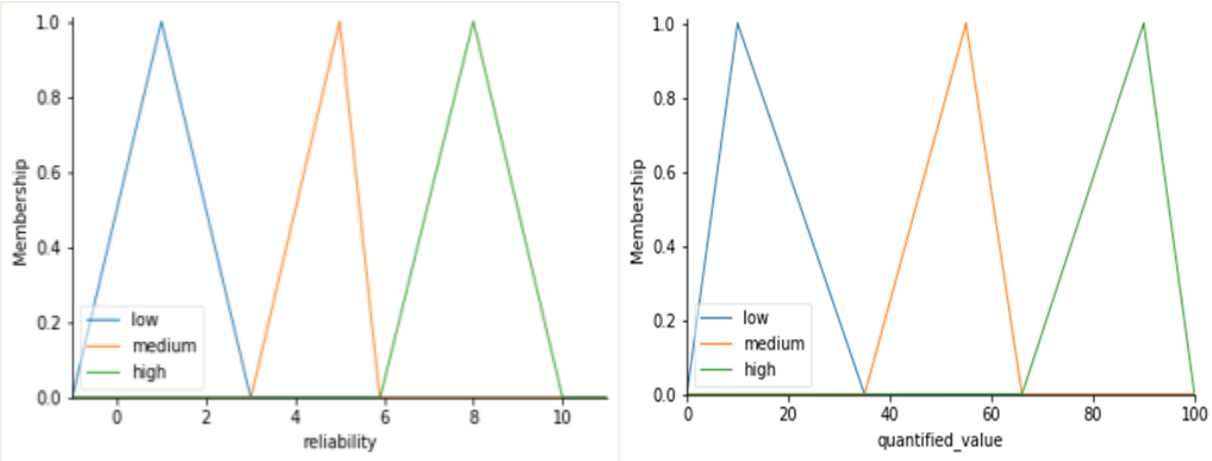


Figure 3 Example of fuzzy logic universes

4.2.1.2 Fuzzy System for reputation reduction

The main objective of this system is to produce the reputation value of any node to whom the event is referring to. For that purpose, after the quantification of the anomalous event, the latest reputation value and timestamp are retrieved from the corresponding asset table, from the GTM database. To this end, the Fuzzy System for reputation reduction examines the time difference between the previous reputation value of the system and the one from the quantified value, as well as the quantified value of the fuzzy logic core system to produce the final reputation value of each asset. The reputation reduction is applied in this way, since a node that receives malicious events spatially and not continuously does not have the same reputation as a node that receives malicious events simultaneously. The Fuzzy System for reputation

reduction is implemented with Fuzzy Logic. Table 7 depicts the rules of the Fuzzy System for reputation reduction.

Rule #No	Input	Output
Rule1	time: low & quantified_value: low	reputation_value: low
Rule2	time: low & quantified_value: medium	reputation_value: low
Rule3	time: low & quantified_value: high	reputation_value: medium
Rule4	time: medium & quantified_value: low	reputation_value: low
Rule5	time: medium & quantified_value: medium	reputation_value: medium
Rule 6	time: medium & quantified_value: high	reputation_value: high
Rule 7	time: high & quantified_value: low	reputation_value: low
Rule 8	time: medium & quantified_value: medium	reputation_value: high
Rule 9	time: medium & quantified_value: high	reputation_value: high

Table 7 The fuzzy rules of system 2

Figure 4 illustrates the fuzzy universes of the time difference and the qualified value, variables used to calculate the reputation score of a node. The categorization on low, medium and high time difference of the fuzzy universe can be derived by the functionality of the network. In private networks, the incoming events will be few compared to a public network, so the time difference universe will need to be adjusted accordingly. For the SPEAR system the categorization on low, medium and high of the time difference universe is based upon the testing of the component. The categorization will be further fine-tuned during the testing of the GTM component during the pilot phase/stage. The time difference is expressed in minutes. If a time difference exceeds the maximum value of the universe, it is mapped as equal with the maximum value of the universe.

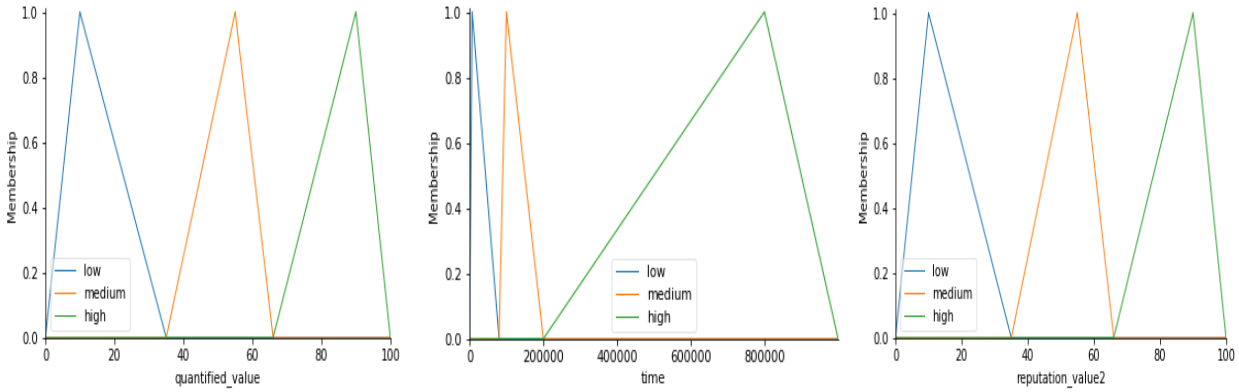


Figure 4 The fuzzy logic universes of the Fuzzy System for reputation reduction

4.2.1.3 Fuzzy System for reputation recovery

GTM dynamically handles the evaluation of trust for the system nodes. In this way, GTM not only reduces the reputation of the nodes based on the detected anomalies, but also increases the reputation based on the time difference between the last decrease in the reputation of the node and the time when a reputation is about to increase. The Fuzzy System for reputation recovery works in parallel with the Fuzzy

Logic Core and the Fuzzy System for reputation reduction. Initially, two variables are taken into account to calculate the reputation upgrade of a node. The first parameter is the time interval between the last stored reputation value - which came from the reputation reduction system- and the time the reputation update takes place. The second parameter is the previous reputation value of the asset. A time interval threshold is also applied in order to start calculating reputation update for each node. This threshold is the same for all the nodes. The threshold is used because it is not desirable to start upgrading the reputation immediately after an existence of an anomalous event. For the development and testing of the GTM component individually, this threshold was set equal to 30 minutes. This threshold will be further updated and fine-tuned during the pilot testing.

Fuzzy logic is also used as the implementation tool of this system. Table 8 summarizes the Fuzzy Logic rules implemented to recover the reputation. The fuzzy universe of the time interval is categorized as low and high. The minimum value of the universe is equal to the time interval threshold.

Rule #No	Input	Output
Rule 1	time: low & reputation_value: low	reputation_value: medium
Rule 2	time: high & reputation_value: low	reputation_value: medium
Rule 3	time: low & reputation_value: medium	reputation_value: medium
Rule 4	time: high & quantified_value: medium	reputation_value: high
Rule 5	time: low & quantified_value: high	reputation_value: high
Rule 6	time: high & quantified_value: high	reputation_value: high

Table 8 The fuzzy rules of the reputation recovery system

Figure 5 illustrates the fuzzy universes of the reputation recovery system. The time interval universe is selected based on the component testing. The universe will be further tuned during the pilot testing. If the time difference exceeds the maximum value of the universe, it is set equal to the maximum universe value.

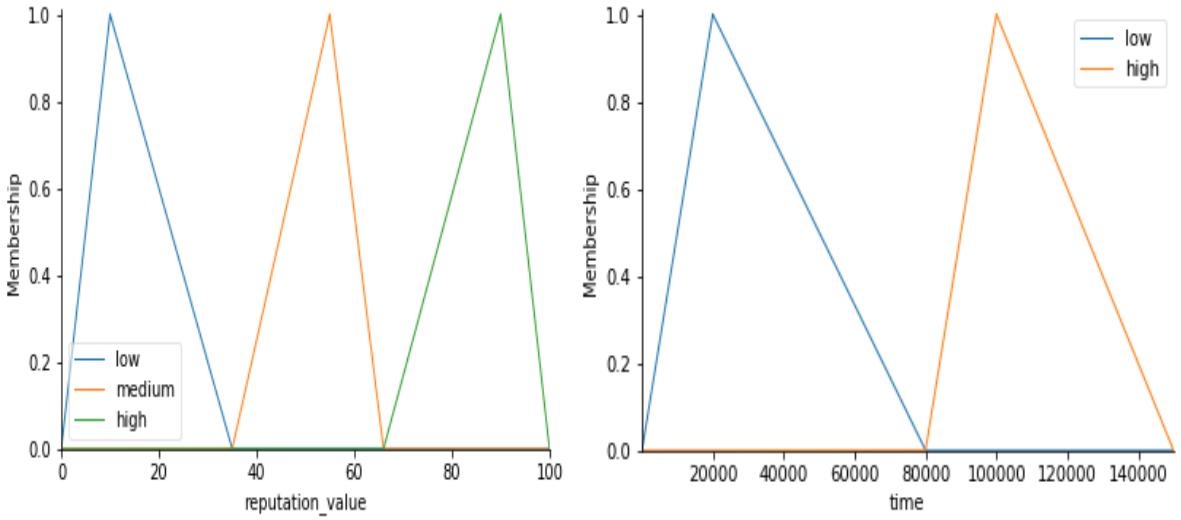


Figure 5 The fuzzy logic universes of the Fuzzy System for reputation recovery

4.2.2 GTM Alerts

GTM activates three different types of alarms. The first type of alarm concerns the reputation score, if it has crossed the threshold set by the user. This type of alarm is sent to V-IDS for each asset of the system that exceeds the security threshold. The alarm contains the message: “Asset: {asset_name}. The reputation value exceeded the defined threshold”.

The second type of alarm concerns the reputation change speed, if it has crossed the threshold set by the user. This type of alarm is sent to V-IDS for every node of the system that exceeds the threshold. The alarm contains the message: “Asset: {asset_name}. The reputation change speed exceeded the defined threshold”. In case where both the alarms are going to be triggered the following message is sent to the V-IDS: “Asset: {asset_name}”. The reputation value and the reputation threshold exceeded the defined thresholds”.

The third type is a general alarm about the devices that exceeded the reputation value threshold and/or the reputation change speed. The GTM sends or updates through a REST API the list of the devices raised an alarm.

4.2.3 GTM Database

The GTM Database is implemented in SQLite. Inside the GTM database, there is a table for every asset of the SPEAR system. The name of each table in the database is the name of the asset. The format of every table is shown in Table 9.

Table Name : Asset Name								
Node ID	Node IP	Asset Location	Reputation value	Reputation change speed	timestamp	Asset value	Alert	System Flag

Table 9 The database's table format for storing historic data

The fields Node ID and Node IP correspond to the ID of the asset and the IP of the asset respectively. The field Asset Location provides the location of the asset, while the reputation value of the asset is given by the field reputation value. The reputation change speed field provides the difference between the former reputation value and the existing one. The timestamp field provides the time of the new calculated reputation value, while the asset value field and the alert field inform about how valuable the asset is to the end user and whether an alert is triggered. The field system flag informs the user if the current reputation value is produced by the Fuzzy System for reputation reduction or by the Fuzzy System for reputation recovery.

There is also a table in which are stored the alert configuration, the asset name and the asset id of every asset of the system. Table 10 presents the format of the aforementioned table.

Table Name: Asset Name				
Node Name	Node ID	Reputation value threshold	Reputation change speed threshold	timestamp

Table 10 The database's table format for storing alert configuration

4.3 GTM Interfaces

The subsection 4.3 describes the interfaces the SPEAR GTM offers and how it communicates with the other components of the SPEAR.

4.3.1 Connection with SPEAR Message Bus

The connection with the SPEAR Message Bus is achieved through the subscription to the topic security_events of the Kafka client. The security events detected by BDAC, V-IDS and OSSIM components are forwarded in Message Bus. In order to establish communication, the following credentials were obtained from TECNALIA:

- The CA certificate
- The consumer/producer key
- The consumer/producer certificate
- The password of the certificate

An indicative example of the format of the asset related data is illustrated in Table 11.

Event field name	Event field description
Spear component	Identifier of the SPEAR component that generates the security event. Three options are available: ossim, bdac and vids.
Date	Date and time of the event.
AlienVaultSensor	Sensor that processed the event.
Device IP	IP address of the Sensor that processed the event.
Event Type ID	ID assigned by the component that generates the event to identify the event type.
Unique Event ID#	Unique ID number assigned to the event by the component that generates the event.
Protocol	Protocol used for the source/destination of the event, for example, TCP IP.
Category	Event taxonomy for the event, for example, Authentication or Exploit.
Sub-Category	Subcategory of the event taxonomy type listed under Category. For example, this would be Denial of Service, if the category were Exploit.

Data Source Name	Name of the external application or device that produced the event.
Data Source ID	ID associated with the external application or device that produced the event.
Product Type	Product type of the event taxonomy, for example, Operating System or Server.
Additional Info	If the event were generated by a suspicious URL, for example, this field would state URL. When present, these URLs provide additional background information and references about the components associated with the event. Usually filled by OSSIM.
Priority	Priority ranking, based on value of the event type. Each event type has a priority value, used in risk calculation.
Reliability	Reliability ranking, based on the reliability value of the event type. Each event type has a reliability value, which is used in risk calculation.
Risk	Risk level of the event: Low = 0, Medium = 1, High > 1 Note: Risk calculation is based on this formula: Asset Value * Event Reliability * Event Priority / 25 = Risk If Asset Value = 3, Reliability = 2 and Priority = 2, the risk would be 3 * 2 * 2 / 25 = 0.48 (rounded down to 0) Therefore, Risk is Low
OTX Indicators	Number of indicators associated with an IP Reputation or OTX pulse event. Filled by OSSIM.
Source/Destination ID	Identifier of the source/destination asset of the event.
Source/Destination IP	IP addresses of the source and destination assets, respectively, of the event.
Source/Destination Hostname	Hostname of the event source/destination.
Source/Destination MAC Address	Media Access Control (MAC) of the asset of the event, if known.

Source/Destination Port	External or internal asset source/destination port for the event.
Source/Destination Latest Update	The last time the component that generates the event updated the asset properties.
Source/Destination Username & Domain	Username and domain associated with the asset that generated the event.
Source/Destination Asset Value	Asset value of the asset source/destination if within the asset inventory.
Source/Destination Location	If the host country of origin is known, displays the national flag of the event source or destination.
Source/Destination Context	If the asset belongs to a user-defined group of entities, OSSIM displays the contexts.
Source/Destination Asset Groups	When the host for the event source/destination is an asset belonging to one or more of your asset groups, this field lists the asset group name or names.
Source/Destination Networks	When the host for the event source/destination is an asset belonging to one or more of your networks, this field lists the networks.
Source/Destination Logged Users	A list of any users who have been active on the asset, as detected by the asset scan, for example, with the username and user privilege (such as admin).
Source/Destination OTX IP Reputation	(Yes/No) Whether or not IP Reputation identifies the IP address as suspicious. Filled by OSSIM.
Source/Destination Service	List of services or applications detected on the source/destination port.
Service Port	Port used by the service or application.
Service Protocol	Protocol used by the service or application.
Raw Log	Raw log details of the event.
Filename	Name of file associated with the event.
Username	The username associated with the event.

Password	The password associated with the event.
Userdata1-9	User-created log fields.
Rule detection	AlienVault OSSIM NIDS rule used to detect the event.

Table 11 Format of events in Message Bus

4.3.2 Connection with SPEAR V-IDS

The connection with the SPEAR V-IDS is achieved by three APIs:

- REST API for receiving asset information (asset name, asset id) and thresholds for raising alerts, denoted hereafter as "**Asset Inventory"**
- REST API for obtaining historic data about the reputation values and the reputation change speed given as an input the asset id, denoted hereafter as "**Historic Data by Asset**"
- REST API for obtaining historic data about the reputation values and the reputation change speed given as an input the asset id and a specific time window to obtain values corresponding only to this time window, denoted hereafter as "**Historic Data by Time"**

Table 12 presents the URL and the request format for the available APIs implemented by CERTH.

Friendly Name	URL	Request Type	Input
Asset Inventory	**https://spear-certh.iti.gr/asset_alert_inventory**	POST	1. AUTH Credentials obtained from CERTH in the format: {"username":"**","password":"***"}
			2. Payload in the format: [{"node_id": "717fbb2841e769e55a6681cd6f82d15b", "node_name": "Just a node name", "reputation_value_threshold": 44, "reputation_value_change_threshold": 55}, {"node_id": "717fbb2841e769e55a6681cd6f82d15b", "node_name": "Just a node name 2", "reputation_value_threshold": 46, "reputation_value_change_threshold": 15}]

Historic Data by Asset	**https://spear-certh.iti.gr/historic_data**	POST	1. Credentials obtained from CERTH in the format: {"username":"**","password":"***"} 2. Payload in the format: {"name":"node_id_obtained_by_asset_discovery_api" }
Historic Data by Time	**https://spear-certh.iti.gr/historic_data_by_timestamp**	POST	1. Credentials obtained from CERTH in the format: {"username":"**","password":"***"} 2. Payload in the format: {"name":"717fbb2841e769e55a6681cd6f82d15b", "time1":"2020-03-01 08:58:03.020820", "time2": "2020-03-24 11:58:03.020820"}

Table 12 REST APIs implemented by CERTH

In Table 13 are presented the available APIs for the connection between SPEAR GTM and SPEAR V-IDS implemented by SIDROCO. The first API is used from V-IDS in order to post information about the asset identity and the security thresholds. The second is used to POST the output of the GTM as it is defined in section 3.1.2.

URL	Type of Request	Description
http://snf-3269.ok-kno.grnetcloud.net:8080/devices/gtmalerts-api/	POST	The API used from V-IDS in order to post information about the asset identity and the security thresholds
http://snf-3269.ok-kno.grnetcloud.net:8080/devices/device-api	POST	The API used to POST the output of the GTM as it is defined in section 3.1.2

Table 13 REST APIs implemented by SIDROCO

5. GTM Prototype deployment

This section comments on the hardware and software requirements for the deployment of the GTM component.

5.1.1 Prerequisites and installation

Table 14 presents the hardware and base operating system prerequisites of the GTM component.

Hardware	Software
At least a 3-core processor	Linux OS/MAC OS/Windows OS
RAM: 4GB or more memory	
40 GB of free disk space	

Table 14 Requirements

The GTM SPEAR component requires a Python installation with version >=3.6. Although it is not required, an installation of the software components into a virtual environment is proposed. The GTM component requires the following python libraries:

- Scikit-Fuzzy
- Numpy
- Sqlite3
- Pandas

The installation of the Scikit-Fuzzy library could be achieved via:

```
pip install scikit-fuzzy
```

The installation of the NumPy library can be made by:

```
pip install NumPy
```

The sqlite3 library, can be used with:

```
pip install db-sqlite3
```

To sum up, the pandas library can be installed with:

```
pip install pandas
```

After the installation, the user has only to execute the gtm_reputation_reduction service and the gtm_update_reputation service on a Linux environment using the commands:

```
sudo systemctl enable gtm_reputation_reduction

sudo systemctl start gtm_reputation_reduction

sudo systemctl enable gtm_update_reputation

sudo systemctl start gtm_update_reputation
```

On a Windows OS, the user has to execute the following commands via the cmd:

```
net start gtm_reputation_reduction
```

```
net start gtm_update_reputation
```

On MacOS, the user has to execute the following commands via the terminal:

```
sudo launchctl load [path_to_service]/gtm_reputation_reduction

sudo launchctl load [path_to_service]/gtm_update_reputation
```

No further actions are needed to be performed. The GTM is configured through the V-IDS platform. More information regarding the execution of the GTM engine will be given on the Deliverable 5.2.

5.1.2 Source code Repository

The code repository of the GTM component in hosted in GitLab by CERTH. GTM is a closed source software project. The use of the code is allowed after a license agreement obtained by CERTH.

6. Testing GTM component

Based on the assessment methodology defined in D2.3, "*Unit test plans will be developed during the implementation phase of the project. All individual units of the SPEAR solution will be tested to determine if they are operational and if they meet their specifications.*"

Therefore, in this deliverable unit test cases have been defined and implemented for the components developed within D3.4, namely the GTM component. The unit test cases are referencing system functional and non-functional requirements defined in D2.2; those system requirements have been previously elicited from the user, security and privacy requirements defined in D2.1. Table 15 illustrates the implemented unit tests of the SPEAR GTM. A detailed explanation of the unit tests is given in the Unit Tests section on Appendix.

Test Case ID – Description	Requirement	Results
TC-GTM-01 - Integration with SPEAR SIEM basis	F01- Assets Protection F03 - Data Transmission	Achieved, to be enhanced and tested in the pilot.
TC-GTM-02 - Fuzzy logic core functionality of GTM	F01- Assets Protection F34 - Asset Reputation	Achieved, to be enhanced and tested in the pilot.
TC-GTM-03 - Fuzzy System for reputation reduction functionality of GTM	F01- Assets Protection F34 - Asset Reputation	Achieved, to be enhanced and tested in the pilot.
TC-GTM-04 - Fuzzy System for reputation recovery functionality of GTM	F01- Assets Protection F34 - Asset Reputation	Achieved, to be enhanced and tested in the pilot.
TC-GTM-05 - Retrieval of historic data	F01- Assets Protection F03 - Data Transmission F33 - VIDS Visual Analytics interconnection with GTM	Achieved, to be enhanced and tested in the pilot.
TC-GTM-06 - Retrieval of the asset list and the end user configuration	F01- Assets Protection F03 - Data Transmission F33 - VIDS Visual Analytics interconnection with GTM F35 - Trust Asset Alerts F36 - Trust System Alert	Achieved, to be enhanced and tested in the pilot.

	NF02 - Scalability	
TC-GTM-07 - Deployment to different OSes	NF01 - Optionality	Achieved, to be enhanced and tested in the pilot.
TC-GTM-08 - Reputation and Alert Transmission to V-IDS	F01- Assets Protection F34 - Asset Reputation F35 - Trust Asset Alerts F03 - Data Transmission	Achieved, to be enhanced and tested in the pilot.
TC-GTM-09 - Encryption and authentication of the GTM communications	F08 - Encrypted communication NF04 - Password Encryption NF05 - Data Encryption	Achieved, to be enhanced and tested in the pilot.
TC-GTM-11 - Test the GTM response time for producing reputation.	NF02 - Scalability	Achieved, to be enhanced and tested in the pilot.

Table 15 Unit tests of the SPEAR-GTM Component

7. Innovation Summary

The novelty provided by GTM can be organized in four main pillars:

- **Evaluating Trust using Fuzzy Logic**: SPEAR GTM is developed to assess the reputation of each asset of the Smart Grid network based on Fuzzy Logic. Fuzzy theory has a special advantage from the classical theories. In classical theories, every variable is defined in a strictly manner, but in fuzzy logic each variable has a membership level.
- **Calculating the severity of an anomalous event based on multiple variables**: GTM quantifies the incoming anomalous incidents using Fuzzy Logic and by taking into consideration five different variables: the asset value, the subcategory (Brute Force, Data injection etc.) of the event, the event risk, the priority and the reliability.
- **Calculating reputation values not only by the severity of an event but also on time intervals:** Both the GTM system for reputation reduction and the system for reputation recovery do not only take in mind the former reputation value but also the time interval between the previous reputation value. In this way, it is ensured that an asset, which continuously receives an event, will not have the same reputation reduction as an asset, which receives events occasionally.
- **Raising alerts in three different domains**: SPEAR GTM raises three different type of alerts. First of all, an alert is raised if the reputation value exceeds a defined threshold. Second, an alert is raised if the difference between the previous reputation value with the new one also exceeds a defined threshold. Third, a general alert is also raised, informing the user about the number of the assets, which have a reputation value or a reputation change speed below the defined threshold. All the thresholds are configured by the user through the SPEAR V-IDS.

Based on the aforementioned remarks, Table 16 illustrates the possible GTM-related research papers that will disseminate the functionality of the GTM engine.

Journal	Link	Description
IEEE Transactions on Industrial Informatics for Special Section on Industrial Internet of Things (IIoT): Where we are and What's next?	http://www.ieee-ies.org/pubs/transactions-on-industrial-informatics	The paper will describe the architecture and functionality of the GTM engine
Special Issue on Novel Cyber-Security Paradigms for Software-defined and Virtualized Systems	https://www.journals.elsevier.com/computer-networks/call-for-papers/special-issue-on-novel-cyber-security-paradigms-for-software	The paper will describe the overall SPEAR SIEM

Table 16 Dissemination plans for the SPEAR GTM

8. Conclusions

In conclusion, this deliverable describes the final outcome of Task 3.4 - Trusted Platform Module of WP3. Some minor updates are possible as part of the continuous evaluation of the complete system by the end of the project (M36) and they can be related with the fine tuning of the Fuzzy System for reputation reduction and reputation recovery.

The SPEAR GTM has been implemented and presented after an analysis of related works and available tools and technologies. Moreover, the implemented version of the GTM was presented in this report with emphasis on Fuzzy Logic as it is a Fuzzy Logic rule-based trust manager which infers new reputation values to the assets of the system by applying Fuzzy Logic rules.

After consideration of the project's requirements and architecture, and after an analysis of available technologies and tools, a Grid Trust Module is developed in Python. It provides to SPEAR system a trust evaluation for every asset of the system and an assessment of a cyber attack's severity. The last working version of the GTM component contains the Fuzzy Logic Core for the quantification of the detected anomalous event, the Fuzzy System for reputation reduction, the Fuzzy System for reputation recovery and its corresponding APIs for the interconnection with the SPEAR V-IDS component.

The outcome of this deliverable mainly affects the WP3 and its components, the SPEAR BASIS, BDAC and the V-IDS. By using the GTM services the SPEAR system is able to perform a trust evaluation for every asset of the system and to raise alerts about the condition of each asset -and for the whole system- after a detected cyber-attack.

Finally, as it is perceived, the GTM component is a system that can support cyber-attack detection and prevention systems, by applying a node centric trust evaluation using Fuzzy Logic. The novelty of this work is the reputation assessment of each node by utilizing Fuzzy Logic. The reputation assessment is based on the multiple anomalous incident features (reliability, priority, risk, asset value, category of the anomaly, time intervals) which are taken into consideration for the production of a reputation value and are extensively discussed in Section 4. Further research and development will be conducted for this component during the evaluation on the SPEAR Pilots in order to fine tune the GTM component. As a future work, the usage of fuzzy deep learning techniques, which are going to upgrade the component's intelligence, will be investigated.

References

[1]. SPEAR Deliverable: D2.1 – User, Security and Privacy Requirements

[2]. SPEAR Deliverable: D2.2 – System Specifications and Architecture

[3]. SPEAR Deliverable: D3.1 – Initial SIEM System

[4]. SPEAR Deliverable: D3.2 – Multi-factor and Open Analytics Engine for Smart Grid Ecosystem

[5]. SPEAR Deliverable: D3.3 – Open Visual-aided Intrusion Detection System

[6]. Alnasser, Aljawharah, and Hongjian Sun. "A fuzzy logic trust model for secure routing in smart grid networks." IEEE access 5 (2017): 17896-17903

[7]. Obert, James, Adrian Chavez, and Jay Johnson. "Behavioral Based Trust Metrics and the Smart Grid." 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018

[8]. Aref, Abdullah, and Thomas Tran. "Multi-criteria trust establishment for Internet of Agents in smart grids." Multiagent and Grid Systems 13.3 (2017): 287-309.

[9]. Velusamy, Durgadevi, and Ganesh Kumar Pugalendhi. "Fuzzy integrated Bayesian Dempster–Shafer theory to defend cross-layer heterogeneity attacks in communication network of Smart Grid." Information Sciences 479 (2019): 542-566

[10]. Zhu, Chunsheng, et al. "Trust-based communication for the industrial Internet of Things." IEEE Communications Magazine 56.2 (2018): 16-22

[11]. C. V. L. Mendoza and J. H. Kleinschmidt, “A Distributed Trust Management Mechanism for the Internet of Things Using a Multi-Service Approach,” Wireless Personal Communications, vol. 103, no. 3, pp. 2501–2513, Sep. 2018.

[12]. Selvaraj, Alagumani, and Subashini Sundararajan. "Evidence-based trust evaluation system for cloud services using fuzzy logic." International Journal of Fuzzy Systems 19.2 (2017): 329-337.

[13]. Naderan, Marjan, Ehsan Namjoo, and Somayeh Mohammadi. "Trust Classification in Social Networks Using Combined Machine Learning Algorithms and Fuzzy Logic." Iranian Journal of Electrical and Electronic Engineering 15.3 (2019): 294-309.

[14]. Rahman, Fatin Hamadah, et al. "Find my trustworthy fogs: A fuzzy-based trust evaluation framework." Future Generation Computer Systems (2018).

[15]. J. E. Fadul, K. M. Hopkinson, T. R. Andel, and C. A. Sheffield, “A Trust-Management Toolkit for Smart-Grid Protection Systems,” IEEE Trans. Power Delivery, vol. 29, no. 4, pp. 1768–1779, Aug. 2014

[16]. Md. M. Hasan and H. T. Mouftah, “Optimal Trust System Placement in Smart Grid SCADA Networks,” IEEE Access, vol. 4, pp. 2907–2919, 2016

[17]. G. S. Brost, M. Huber, M. Weiß, M. Protsenko, J. Schütte, and S. Wessel, “An Ecosystem and IoT Device Architecture for Building Trust in the Industrial Data Space,” in Proceedings of the 4th ACM Workshop on Cyber-Physical System Security - CPSS ’18, Incheon, Republic of Korea, 2018, pp. 39–50,

[18]. M. Allahbakhsh, H. Amintoosi, A. Ignjatovic, and E. Bertino, “A Trust-Based Experience-Aware Framework for Integrating Fuzzy Recommendations,” IEEE Trans. Serv. Comput., pp. 1–1, 2019

[19]. Md. M. Hasan and H. T. Mouftah, “Optimization of Trust Node Assignment for Securing Routes in Smart Grid SCADA Networks,” IEEE Systems Journal, vol. 13, no. 2, pp. 1505–1513, Jun. 2019

[20]. T. Wang, P. Wang, S. Cai, Y. Ma, A. Liu, and M. Xie, “A Unified Trustworthy Environment Establishment based on Edge Computing in Industrial IoT,” IEEE Trans. Ind. Inf., pp. 1–1, 2019,

[21]. Y. Liu, A. Liu, X. Liu, and M. Ma, “A Trust-Based Active Detection for Cyber-Physical Security in Industrial Environments,” IEEE Trans. Ind. Inf., vol. 15, no. 12, pp. 6593–6603, Dec. 2019

[22]. D. Velusamy, G. Pugalendhi, and K. Ramasamy, “A Cross-Layer Trust Evaluation Protocol for Secured Routing in Communication Network of Smart Grid,” IEEE J. Select. Areas Commun., vol. 38, no. 1, pp. 193–204, Jan. 2020

[23]. T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, “MTES: An Intelligent Trust Evaluation Scheme in Sensor-Cloud-Enabled Industrial Internet of Things,” IEEE Trans. Ind. Inf., vol. 16, no. 3, pp. 2054–2062, Mar. 2020

[24]. G. Fortino, F. Messina, D. Rosaci, G. M. Sarne, and C. Savaglio, “A Trust-based Team Formation Framework for Mobile Intelligence in Smart Factories,” IEEE Trans. Ind. Inf., pp. 1–1, 2020

Appendix

The Appendix contains the set of the fuzzy logic core rules and GTM unit testing in details.

Fuzzy Logic Core rules:

In this section the fuzzy logic rules of the fuzzy logic core system are presented. The output of the Fuzzy Logic Core rule is the quantified value, which express the severity of the detected anomalous event. Table 17 depicts the entire set of the fuzzy rules.

Rule	Asset_Value	Priority	Reliability	Subcategory	Risk	Quantified_value
1	high	high	high	high	high	**low**
2	low	low	low	low	low	**high**
3	high	high	high	high	medium	**low**
4	high	high	high	high	low	**medium**
5	high	high	high	low	high	**low**
6	high	high	high	low	medium	**medium**
7	high	high	high	low	low	**medium**
8	high	high	medium	high	high	**low**
9	high	high	medium	high	medium	**low**
10	high	high	medium	high	low	**medium**
11	high	high	medium	low	high	**medium**
12	high	high	medium	low	medium	**medium**
13	high	high	high	low	low	**high**
14	high	high	low	high	high	**low**
15	high	high	low	high	medium	**medium**
16	high	high	low	high	low	**medium**
17	high	high	low	low	high	**medium**
18	high	high	low	low	medium	**medium**
19	high	high	low	low	low	**high**
20	high	medium	high	high	high	**low**
21	high	medium	high	high	medium	**low**
22	high	medium	high	high	low	**medium**
23	high	medium	high	low	high	**low**
24	high	medium	high	low	medium	**medium**
25	high	medium	high	low	low	**high**
26	high	medium	medium	high	high	**medium**
27	high	medium	medium	high	medium	**medium**
28	high	medium	medium	high	low	**high**
29	high	medium	medium	low	high	**medium**
30	high	medium	medium	low	medium	**high**

31	high	medium	medium	low	low	**high**
32	high	medium	low	high	high	**low**
33	high	medium	low	high	medium	**medium**
34	high	medium	low	high	low	**high**
35	high	medium	low	low	high	**medium**
36	high	medium	low	low	medium	**medium**
37	high	medium	low	low	low	**high**
38	high	low	high	high	high	**low**
39	high	low	high	high	medium	**medium**
40	high	low	high	high	low	**high**
41	high	low	high	low	high	**low**
42	high	low	high	low	medium	**medium**
43	high	low	high	low	low	**high**
44	high	low	medium	high	high	**low**
45	high	low	medium	high	medium	**medium**
46	high	low	medium	high	low	**medium**
47	high	low	medium	low	high	**low**
48	high	low	medium	low	medium	**medium**
49	high	low	medium	low	low	**high**
50	high	low	low	high	high	**medium**
51	high	low	low	high	medium	**medium**
52	high	low	low	high	low	**high**
53	high	low	low	low	high	**medium**
54	high	low	low	low	medium	**medium**
55	high	low	low	low	low	**high**
56	medium	high	high	high	high	**low**
57	medium	high	high	high	medium	**medium**
58	medium	high	high	high	low	**medium**
59	medium	high	high	low	high	**low**
60	medium	high	high	low	medium	**medium**
61	medium	high	high	low	low	**medium**
62	medium	high	medium	high	high	**low**
63	medium	high	medium	high	medium	**medium**
64	medium	high	medium	high	low	**high**
65	medium	high	medium	low	high	**low**
66	medium	high	medium	low	medium	**medium**
67	medium	high	medium	low	low	**high**
68	medium	high	low	high	high	**medium**
69	medium	high	low	high	medium	**medium**
70	medium	high	low	high	low	**high**
71	medium	high	low	low	high	**medium**

72	medium	high	low	low	medium	**medium**
73	medium	high	low	low	low	**high**
74	medium	medium	high	high	high	**low**
75	medium	medium	high	high	medium	**medium**
76	medium	medium	high	high	low	**high**
77	medium	medium	high	low	high	**low**
78	medium	medium	high	low	medium	**medium**
79	medium	medium	high	low	low	**high**
80	medium	medium	medium	high	high	**medium**
81	medium	medium	medium	high	medium	**high**
82	medium	medium	medium	high	low	**high**
83	medium	medium	medium	low	high	**medium**
84	medium	medium	medium	low	medium	**high**
85	medium	medium	medium	low	low	**high**
86	medium	medium	low	high	high	**medium**
87	medium	medium	low	high	medium	**high**
88	medium	medium	low	high	low	**high**
89	medium	medium	low	low	high	**medium**
90	medium	medium	low	low	medium	**high**
91	medium	medium	low	low	low	**high**
92	medium	low	high	high	high	**low**
93	medium	low	high	high	medium	**medium**
94	medium	low	high	high	low	**high**
95	medium	low	high	low	high	**medium**
96	medium	low	high	low	medium	**high**
97	medium	low	high	low	low	**high**
98	medium	low	medium	high	high	**medium**
99	medium	low	medium	high	medium	**medium**
100	medium	low	medium	high	low	**high**
101	medium	low	medium	low	high	**medium**
102	medium	low	medium	low	medium	**high**
103	medium	low	medium	low	low	**high**
104	medium	low	low	high	high	**medium**
105	medium	low	low	high	medium	**medium**
106	medium	low	low	high	low	**high**
107	medium	low	low	low	high	**high**
108	medium	low	low	low	medium	**high**
109	medium	low	low	low	low	**high**
110	low	high	high	high	high	**low**
111	low	high	high	high	medium	**medium**
112	low	high	high	high	low	**medium**

113	low	high	high	low	high	**low**
114	low	high	high	low	medium	**medium**
115	low	high	high	low	low	**high**
116	low	high	medium	high	high	**low**
117	low	high	medium	high	medium	**medium**
118	low	high	medium	high	low	**medium**
119	low	high	medium	low	high	**medium**
120	low	high	medium	low	medium	**medium**
121	low	high	medium	low	low	**high**
122	low	high	low	high	high	**low**
123	low	high	low	high	medium	**medium**
124	low	high	low	high	low	**medium**
125	low	high	low	low	high	**medium**
126	low	high	low	low	medium	**medium**
127	low	high	low	low	low	**high**
128	low	medium	high	high	high	**low**
129	low	medium	high	high	medium	**medium**
130	low	medium	high	high	low	**high**
131	low	medium	high	low	high	**low**
132	low	medium	high	low	medium	**medium**
133	low	medium	high	low	low	**high**
134	low	medium	medium	high	high	**medium**
135	low	medium	medium	high	medium	**high**
136	low	medium	medium	high	low	**high**
137	low	medium	medium	low	high	**medium**
138	low	medium	medium	low	medium	**high**
139	low	medium	medium	low	low	**high**
140	low	medium	low	high	high	**medium**
141	low	medium	low	high	medium	**high**
142	low	medium	low	high	low	**high**
143	low	medium	low	low	high	**medium**
144	low	medium	low	low	medium	**high**
145	low	medium	low	low	low	**high**
146	low	low	high	high	high	**low**
147	low	low	high	high	medium	**medium**
148	low	low	high	high	low	**high**
149	low	low	high	low	high	**medium**
150	low	low	high	low	medium	**high**
151	low	low	high	low	low	**high**
152	low	low	medium	high	high	**medium**
153	low	low	medium	high	medium	**high**

154	low	low	medium	high	low	**high**
155	low	low	medium	low	high	**high**
156	low	low	medium	low	medium	**high**
157	low	low	medium	low	low	**high**
158	low	low	low	high	high	**medium**
159	low	low	low	high	medium	**high**
160	low	low	low	high	low	**high**
161	low	low	low	low	high	**high**
162	low	low	low	low	medium	**high**
163	low	low	low	low	low	**high**

Table 17 Fuzzy Logic Core Rules

Unit Tests

This section illustrates in details the conducted unit tests of the SPEAR GTM component.

Test Case ID	TC-GTM-01 - Integration with SPEAR SIEM basis	Component	GTM
Description	The GTM receives and processes every anomalous event coming from Message Bus.		
Req ID	F01, F03	Priority	High
Prepared by	CERTH	Tested by	CERTH
Pre-condition(s)	None		
Test steps			
1	Initialize a connection to the Message Bus		
2	Listen for incoming anomalous events		
3	Receive all the incoming events		
Input data	Events in the OSSIM Alien Vault format		
Result	The GTM is able to receive the anomalous events generated by the SPEAR OSSIM, SPEAR BDAC and SPEAR V-IDS.		

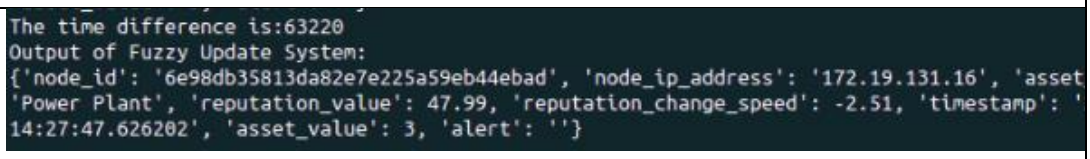
	 b'{"spear_component": "ossim", "date": "2020-04-24 17:14:12.969780", "alienvault_sensor": "Sensor_51JXY9", "device i "160.40.48.16", "event type id": "EventType_BFPBXU", "unique event id": "UniqueEvent_LSUGA6", "protocol": "Radius", "category": "Authentication", "subcategory": "Logout", "data source name": "BDAC_mqtt", "data source id": "BDAC_mqtt_QCEA7I", "product type": "", "Additional Info": "anyadditionalinfo", "otx_indicators": "", "Asset value": "Event Priority": 2, "Event Reliability": 10, "Risk": 3.2, "source": {"id": "", "ip": "160.40.48.112", "hostname": " "mac": "00:50:56:ce:d9:83", "port": 247, "latest update": "", "username domain": "", "asset_value": 4, "location": "Substation", "context": "", "asset_groups": [], "networks": ["Local_172_26_40_0_23"], "logged_users": [], "otx_ip_reputation": "", "services": {"service": "", "port": "", "protocol": ""}}, "destination": {"id": "Device8", "212.174.15.8", "hostname": "", "mac": "00:50:56:03:9d:f3", "port": 2226, "latest_update": "", "username_domain": "" "asset_value": "", "location": "Germany", "context": "", "asset_groups": [], "networks": [], "logged_users": [], "otx_ip_reputation": "", "services": {"service": "", "port": "", "protocol": ""}}, "raw_log": " GET /alienvault5/ alienvault/binary/en.gz HTTP/1.1\\r\\nHost: data.alienvault.com\\r\\nCache-Control: max-age=0\\r\\nUser-Agent: Debia HTTP/1.3 (1.0.9.8.5)\\r\\n\\r\\n ", "filename": "", "username": "", "password": "", "userdata1": "", "userdata2": "" "userdata3": "", "userdata4": "", "userdata5": "", "userdata6": "", "userdata7": "", "userdata8": "", "rule_detectio "File: emerging-policy.rules\\r\\nRule: alert http $HOME_NET any -> $EXTERNAL_NET any\\r\\nmsg:\\"ET POLICY GNU/Linu User-Agent Outbound likely related to package management\\"\\r\\nflow: established,to_server\\r\\ncontent: \\"APT-HT \\"\\r\\nhttp_user_agent:reference: url,help.ubuntu.com/community/AptGet/Howto\\r\\nclasstype: not-suspicious\\r\\ns 2013504\\r\\nrev: 5\\r\\nmetadata: created_at 2011_08_31, updated_at 2011_08_31"}' Sending to SPEAR SIEM Basis - Kafka Topic: [security_events]

b'{"spear_component": "ossim", "date": "2020-04-24 17:14:43.501899", "alienvault_sensor": "Sensor_RGK0TB", "device i "160.40.48.172", "event type id": "EventType_WBXOWY", "unique event id": "UniqueEvent_XWBS6K", "protocol": "UDP", "category": "Alarm", "subcategory": "DoS", "data source name": "Burp", "data source id": "Burp_PE3JJF", "product typ "", "Additional Info": "anyadditionalinfo", "otx_indicators": "", "Asset value": 5, "Event Priority": 3, "Event Reliability": 10, "Risk": 6.0, "source": {"id": "", "ip": "160.40.48.191", "hostname": "", "mac": "00:50:56:ef:27:71 "port": 414, "latest update": "", "username domain": "", "asset_value": 5, "location": "Substation", "context": "", "asset_groups": [], "networks": ["Local_172_26_40_0_23"], "logged_users": [], "otx_ip_reputation": "", "services": {"service": "", "port": "", "protocol": ""}}, "destination": {"id": "Device14", "ip": "42.34.134.56", "hostname": "" |
| Test Case Result | Achieved, to be enhanced and tested in the pilot. |

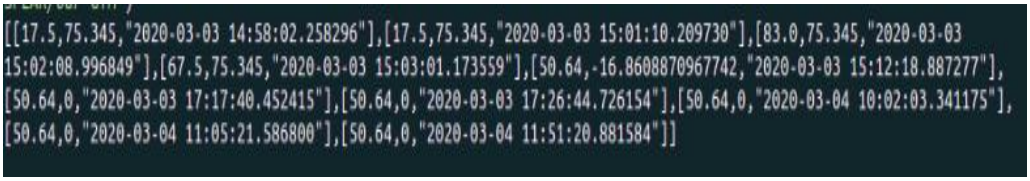
Test Case ID	TC-GTM-02 - Fuzzy logic core functionality of GTM	Component	GTM
Description	The GTM receives an anomalous event and produce a quantified value based on the fuzzy logic core		
Req ID	F01, F34	Priority	High
Prepared by	CERTH	Tested by	CERTH
Pre-condition(s)	None		
Test steps			
1	Initialize GTM		
2	Receive an Anomalous Event, which is categorized as a cyberattack with high risk, priority and reliability.		
3	Quantify the anomalous event of the affected asset(s)		

Input data	Event in the OSSIM Alien Vault format
Result	The quantified values is:17.5 Output of Fuzzy Logic Core: {'node_id': 'Device9', 'node_ip_address': '172.19.130.11', 'asset_location': 'Power Plant' 'reputation_value': 17.5, 'reputation_change_speed': 75.345, 'timestamp': '2020-05-30 14:2 'asset_value': 4, 'alert': ''}
Test Case Result	Achieved, to be enhanced and tested in the pilot.

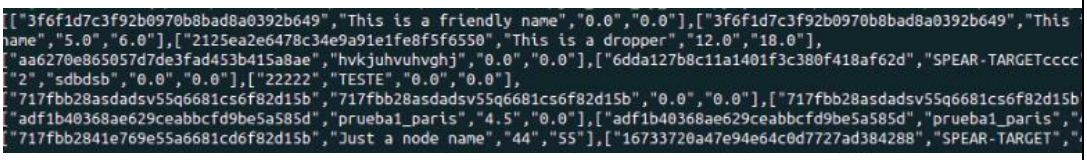
Test Case ID	TC-GTM-03 - Fuzzy System for reputation reduction functionality of GTM	Component	GTM
Description	The GTM receives an anomalous event and produce a reputation value based on the Fuzzy System for reputation reduction.		
Req ID	F01, F34	Priority	High
Prepared by	CERTH	Tested by	CERTH
Pre-condition(s)	Based on the previous quantified value of the TC-GTM-01 the Fuzzy System for reputation reduction produces the reputation value of the asset.		
Test steps			
1	Initialize GTM		
2	Receive an Anomalous Event		
3	Produce a reputation value based on the quantified value and the time difference.		
Input data	Event in the OSSIM Alien Vault format, time difference of the previous reputation degradiation		
Result	The time difference is:208 Output of Fuzzy Reduction System: {'node_id': '3f6f1d7c3f92b0970b8bad8a0392b649', 'node_ip_address': '172.19.130.11', 'asse 'Power Plant', 'reputation_value': 14.39, 'reputation_change_speed': -3.07, 'timestamp': 14:25:39.875347', 'asset_value': 4, 'alert': ''}		
Test Case Result	Achieved, to be enhanced and tested in the pilot		

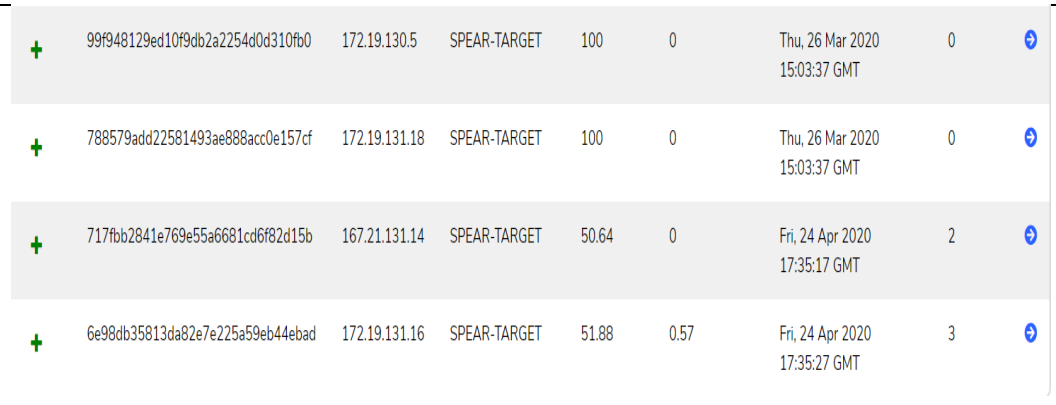
Test Case ID	TC-GTM-04 - Fuzzy System for reputation recovery functionality of GTM	Component	GTM
Description	The GTM updates the reputation of the node based on the time difference between the last reputation reduce and the last reputation value.		
Req ID	F01, F34	Priority	High
Prepared by	CERTH	Tested by	CERTH
Pre-condition(s)	None		
Test steps			
1	Initialize GTM		
2	Update the reputation value of the node based on the fuzzy logic rules of the reputation recovery system.		
Input data	Time Difference, Former Reputation value of a node		
Result			
Test Case Result	Achieved, to be enhanced and tested in the pilot		

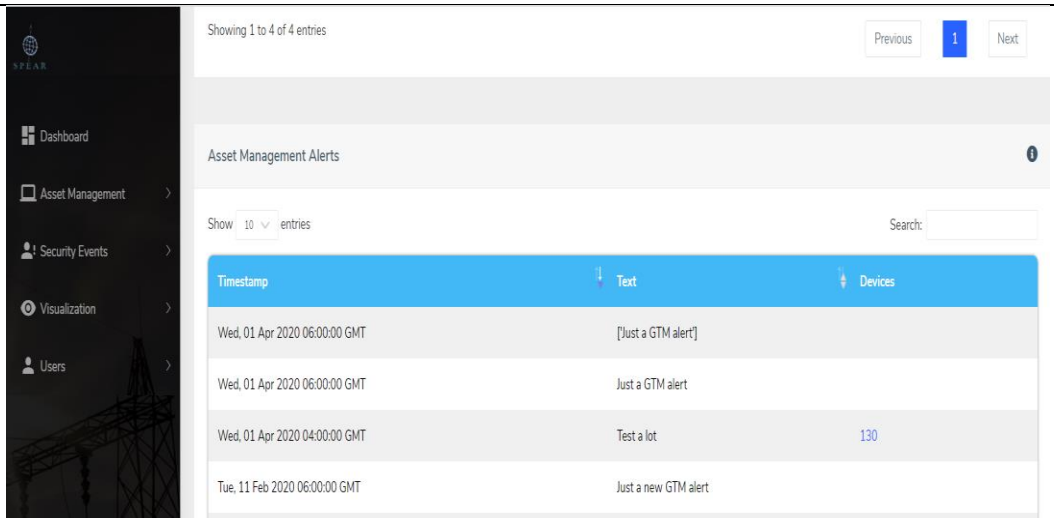
Test Case ID	TC-GTM-05 - retrieval of historic data	Component	GTM
Description	The V-IDS user obtains through the REST APIs the historic data of a node with two options. The user can obtain the historic data only by the name of the node or by the name and a timestamp.		
Req ID	F01, F03, F33	Priority	High
Prepared by	CERTH	Tested by	CERTH
Pre-condition(s)	None		

Test steps		
1	The end user creates a post request to the **https://spear-certh.iti.gr/historic_data_by_timestamp** or to the **https://spear-certh.iti.gr/historic_data.**	
2	The end user obtains the historic data of a specified node.	
Input data	A post request as it is defined in Table 15 , for the node 717fbb2841e769e55a6681cd6f82d15b	
Result	The reputation value, the reputation change speed and the time of the produced reputation value of the node. 	
Test Case Result	Achieved, to be enhanced and tested in the pilot	

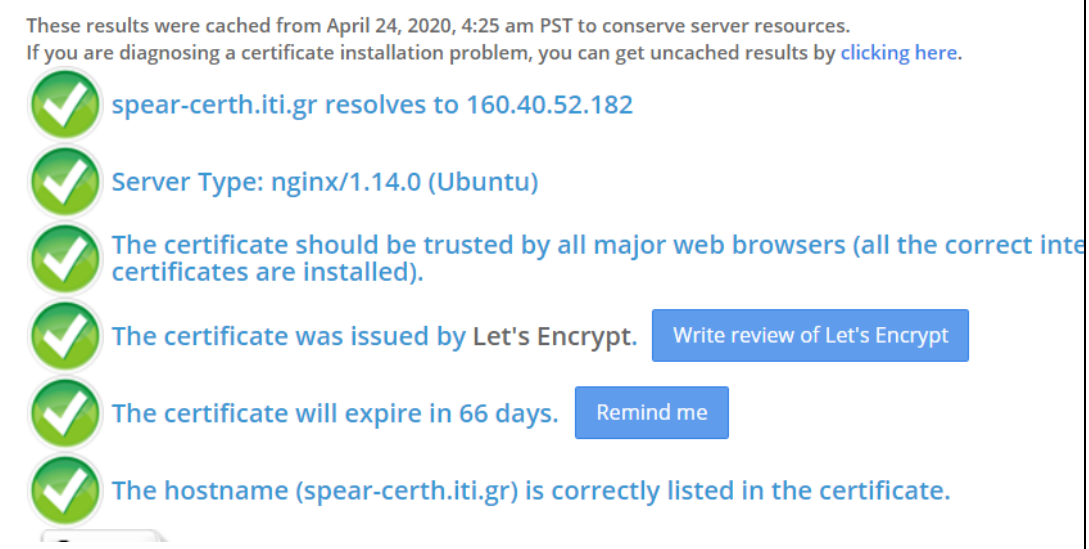
Test Case ID	TC-GTM-06 - Retrieval of the asset list and the end user configuration for raising alerts	Component	GTM
Description	The V-IDS user sends through a REST APIs the asset list of the system and the alert configuration, the GTM is able to handle the assets and the security thresholds for raising alerts		
Req ID	F33, F35, F36, NF02	Priority	High
Prepared by	CERTH	Tested by	CERTH
Pre-condition(s)	None		
Test steps			
1	The end user creates a post request to the **https://spear-certh.iti.gr/ asset_alert_inventory**		
2	The GTM receives the assets of the system and the security configuration for raising alerts		
Input data	-		

Result	The asset id, the asset name, the reputation value threshold and the reputation change speed threshold .  [["3f6f1d7c3f92b0970b8bad8a0392b649","This is a friendly name","0.0","0.0"],["3f6f1d7c3f92b0970b8bad8a0392b649","This name","5.0","6.0"],["2125ea2e6478c34e9a91e1fe8f5f6550","This is a dropper","12.0","18.0"], ["aa6270e865057d7de3fad453b415a8ae","hvkjuhvuhvghj","0.0","0.0"],["6dda127b8c11a1401f3c380f418af62d","SPEAR-TARGETcccc ["2","sdbdsb","0.0","0.0"],["22222","TESTE","0.0","0.0"], ["717fbb28asdadsv55q6681cs6f82d15b","717fbb28asdadsv55q6681cs6f82d15b","0.0","0.0"],["717fbb28asdadsv55q6681cs6f82d15b ["adf1b40368ae629ceabbcfd9be5a585d","prueba1_paris","4.5","0.0"],["adf1b40368ae629ceabbcfd9be5a585d","prueba1_paris"," ["717fbb2841e769e55a6681cd6f82d15b","Just a node name","44","55"],["16733720a47e94e64c0d7727ad384288","SPEAR-TARGET","
Test Case Result	Achieved, to be enhanced and tested in the pilot

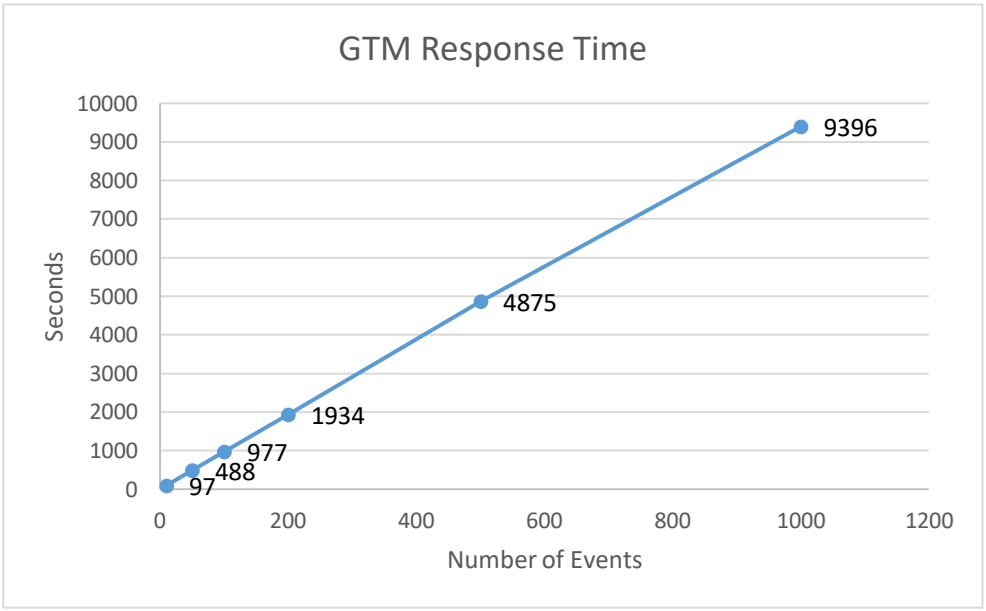
Test Case ID	TC-GTM-08 - Reputation and Alert Transmission to V-IDS	Component	GTM
Description	The GTM sends through a REST APIs the reputation value of a node and any alert message.		
Req ID	F01, F34, F35	Priority	High
Prepared by	CERTH	Tested by	CERTH
Pre-condition(s)	None		
Test steps			
1	The GTM produces a reputation value		
2	The GTM sends to the V-IDS the GTM output		
Input data	Incoming events from Message Bus		
Result			

	
Test Case Result	Achieved, to be enhanced and tested in the pilot

Test Case ID	TC-GTM-09 - encryption and authentication of the GTM communications	Component	GTM
Description	Test the SSL encryption and the authentication of the GTM Rest APIs for transmitting and receiving data.		
Req ID	F08, NF04, NF05	Priority	High
Prepared by	CERTH	Tested by	CERTH
Pre-condition(s)	None		
Test steps			
1	To test the SSL encryption the SSL Shopper checker is used (https://www.sslshopper.com/ssl-checker.html).		
2	In the SSL checker, type the spear-certh.iti.gr		
3	For the authentication, we are trying to obtain information via the REST APIs without providing password or by providing false passwords.		
Input data	-		

Result	For the SSL encryption:  For the authentication: 
Test Case Result	Achieved, to be enhanced and tested in the pilot

Test Case ID	TC-GTM-11 - Test the GTM response time for producing reputation.	Component	GTM
Description	Test the response time of the GTM reputation reduction system.		
Req ID	NF02	Priority	High
Prepared by	CERTH	Tested by	CERTH
Pre-condition(s)	None		
Test steps			
1	Test the response time for 10, 50, 100, 200, 500 and 1000 events respectively.		
Input data	Events in the SPEAR OSSIM format		

Result	The following diagram illustrates the time in seconds that takes for the GTM to produce a reputation value for 10, 50, 100, 200, 500 and 1000 events respectively. 
Test Case Result	Achieved, to be enhanced and tested in the pilot