Choosing the right IDS for OT networks

Saber Mhiri [1]

[1]InprOTech, saber.mhiri@inprosec.com

Abstract. For an effective protection of all the elements of an industrial ecosystem against threats, it is necessary to understand the true scope of existing mechanisms capable of detecting potential anomalies and intrusions. It is the aim of this article to review the state of IDSs (Intrusion Detection Systems) functionalities as well as presenting the existing solutions available in the market.

Keywords: Industries 4.0, Cyber security, Intrusion Detection Systems IDS, Artificial Intelligence AI, Big Data.

1 INTRODUCTION

Control of industrial environments through systems such as SCADA (Supervisory Control and Data Acquisition) is now present in most critical infrastructures (e.g, power grids, nuclear plants or transport systems). These control systems allow remote and real-time access to devices that govern the production cycle, whether they are controllers such as PLC (Field Programmable Logic Controllers), or RTU (Remote Terminal Units). Traditionally, SCADA systems and industrial networks had to be isolated from other environments.
However, at present, we are dealing with the interconnection of SCADA systems for the storage of data or the outsourcing of services, as well as a standardization of the software and hardware used in control systems. Consequently, there has been a substantial increase in security risks based on new specific threats operating under different threat modes . A solution to mitigate these effects is the provision of awareness-based approaches (e.g. situational awareness), which help to provide the necessary tools to favor the detection and response to attacks and/or anomalies . Many of these anomalies arise from conflicts or security breaches due to interoperability issues, probably caused by multiple communication and control protocols.
In this paper we present the main functionalities offered by IDSs currently existing in the market as well as providing a detailed list of existing solutions in the market.
In this work we focus on the advanced capacities of IDS solutions, mainly the use of AI and Big data technologies. Through this work we also introduce the SANTI IA solution as a competing solution in the IDS market with OT specific capacities.

2 IDS functionalities

2.1 Basic functionalities

- **Network mapping**:
  Network mapping is **the process of visualizing all the devices on your network**, how they are connected, and how the overall network is structured. The network map generally equips you with information about whether the network is functioning properly or whether any particular device has a problem.
  Mapping your network is vitally important for keeping on top of how its performing, as well as for pinpointing bottlenecks or network issues, and troubleshooting problems. But approaching this process manually with a large or complex network can quickly become overwhelming.
  Through SANTI mapping capacity, you can have a complete and detailed view of your network communications and assets. SANTI provides an interactive map that helps you explore your network's hidden devices and communications.
- **Asset management**:
  Device management is the process of managing the implementation, operation and maintenance of a physical and/or virtual device. It is a broad term that includes various administrative tools and processes for the maintenance and upkeep of a computing, network, mobile and/or virtual device.
  Device management generally performs the following:

  - Installing device and component-level drivers and related software.
  - Configuring a device so it performs as expected using the bundled operating system, business/workflow software and/or with other hardware devices.
  - Implementing security measures and processes.

  When it comes to IDS systems, this functionality usually refers to applying segregation and device protection procedures to keep the network secure. Devices usually refer to physical/hardware devices such as computers, laptops, servers, mobile phones and more.But in the case of OT networks, the devices are usually:

  - PLC
  - RTU
  - MTU
  - SCADA
  - workstation PCs
  - IED.
  - CS PBX
  - CS Modem
  - Server: Data aquisition server, Application server, Historian, Database server, Configuration server, HMI computer
  - Ethernet I/O module
  - managed switch
  - protocol converter

SANTI provides the tools needed to manage the network assets as needed for security measurements. Starting from identifying and tagging devices till blacklisting devices depending on its critical level. With its extended list of device tags and icons, you can have a more comprehensive view of your assets.

- **Alert management**:
  Event Alert Management deals with any kind of Event Alert in the OT infrastructure and OT services. A well-defined and controlled process leads to the effective handling of these events and alerts. Event Alert Management is triggered by occurrence of noticeable signals or messages which has significance for the services of infrastructure. Typically these events and alerts are generated by monitoring tools, configuration items (CI) or OT services. Each Event Alert is classified by determining its significance, analysed and handled reflecting a handling rule. Handling is done by human or automated operations and might be followed up by a set of actions. Events and alerts which are critical for the delivery of defined class of services are forwarded to Incident, Problem or Change Management.
  SANTI clearly notify users of the threats in the network through its alerts categories depending on the risk level. These alerts are color coded and detailed with dynamic information (no generic alerts). SANTI also helps security officers mitigate and silence these alerts through the adequate procedures.
- **Rules engines**:
  rule engine is a piece of software that executes rules according to some algorithm. A rule engine combines a set of facts that are inserted into the system with its own Rule Set to reach a conclusion of triggering one or several actions. These rules typically describe in a declarative manner the business logic which needs to be implemented in our environment (which we assume rarely changes). The facts, on the other had, describe the conditions of the system that is to be operated on; they may change frequently. Logic, or rules in our case, are pieces of knowledge often expressed as, "When some conditions are evaluated to be true, then do some tasks".
  A system with a large number of rules and facts may result in many rules being true for the same facts; in this case, we say that rules are said to be in conflict. A rule engine can use different conflict resolver strategies to determine the order of execution of the conflict rules. In a rule engine, there are two execution methods:

  - **Forward chaining**: is a "data-driven" method. Upon facts being inserted or updated, the rule engine uses available facts and inference rules to extract more facts until a goal is reached, where one or more matching rules will be concurrently true and scheduled for execution. Hence the rule engine starts with facts and ends with conclusion.

  - **Backward chaining:** is a "goal-driven" or inference method, which is reversed with forward chaining. Backward chaining starts with a conclusion or a list of goals that the engine tries to satisfy. If it cannot satisfy these goals, then it searches for sub-goals that it can satisfy that will help satisfy some part of the current goals. The engine continues this process until either the initial conclusion is proven or there are no more sub-goal.

  Rules in IDS systems are defined to detect abnormalities and unauthorized communi-

cations in the network.
Through its advanced rule engine dedicated to cybersecurity threat detections in OT networks, SANTI detects patterns of unauthorized connections and unusual behaviors in the network. These capacities help security officers identify and eliminate threats in the network safely and fast.

- **Logs collections**:
  In the computing world, a log is a file that is produced automatically every time certain events occur in your system. Log files are usually time-stamped, and may record practically anything that is happening behind the scenes in operating systems or software applications - in a nutshell, they record everything that the server, network, OS, or application thinks is important to keep track of. Logs can document all kinds of events ranging from messages and transactions occurring between different users, what happened during a backup, the errors that stopped an application from running, or the files that have been requested by users from a website.
  There are several types of log: some can be opened and read by humans, while others are kept for auditing purposes and are not human-readable. Audit logs, transaction logs, event logs, error logs, message logs are just some examples of different log files - each one serving a different purpose. They come in a broad variety of extensions, such as .log, .txt, or different proprietary extensions.
  The first step in log management is to determine how to collect log data and where to store it. Your logs are aggregating data from different parts of the IT environment: operating system, firewalls, servers, switches, routers, etc. When it comes to storage, security systems such as firewalls are the most demanding in terms of data volume they produce. Those systems typically generate dozens of EPS (events per second), which calls for a log collector that can handle the corresponding amount of logs.
  Although an OT network may be static, it generates a big amount of data and the repetitiveness of communications between machines (request data, change state,...) can generate a huge amount of traffic that results in an important amount of security logs in the network.
  SANTI collects all the traffic logs in the network for future analysis and verifications. This functionality helps deep inspection of the network traffic. The centralization of the logs helps the security analysts protect the network without the need of manually collecting the logs from the different historians and equipment in the network.

- **Intuitive interfaces**:
  Although a lot of IDS providers have a simple to understand main interface where you can see the global state of the network. When it comes to displaying details of the vulnerabilities and networks state, most of the IDS interfaces are designed for advanced security expert users. These interfaces require the hiring of security experts from the client part to analyze the data displayed.
  SANTI interface is developed using the web framework Angular following the security best practices and methodologies to assure a safe and secure information display. The SANTI interface is highly interactive and easy to understand and handle. The use of simple and indicative colors helps the user understand and manage the security information displayed. SANTI is a bilingual system with English and Spanish interfaces capabilities.

2.2 Advanced functionalities

- **AI traffic analysis capacity**:
  Analyzing and improving cybersecurity posture is not a human-scale problem anymore. In response to this unprecedented challenge, Artificial Intelligence (AI) based tools for cybersecurity have emerged to help information security teams reduce breach risk and improve their security posture efficiently and effectively.
  For an IDS, the capacity of analyzing complicated data and detecting new threats and patterns in the network is an essential attribute. Due to the rise of number of devices connected in the OT networks as well as the diversity of devices in these networks, the state of the art IDS systems have been increasingly failing to detect advanced patterns and threats, due to either the complication of the network or the size of the data treated.
  SANTI IA is an IA empowered technology that takes advantage of the AI advanced data analysis capacity in order to detect security threats and traffic patterns in the network that otherwise would not be detected through simple analysis or through traditional methods.

- **Big Data capacities**:
  Big Data is a collection of data that is huge in volume, yet growing exponentially with time. It is a data with so large size and complexity that none of traditional data management tools can store it or process it efficiently. Big Data is also data but with huge size.
  With the increase in the number of devices connected in the OT environment, specially with the introduction of concepts such as IoT devices and Industry 4.0.
  The size of data generated from OT networks is increasingly growing complicated. These data size and complications need to be dealt with through Big Data technologies.

  SANTI IA with its Big Data module will be able to manage all the data generated from big size industrial networks with efficiency and robustness. Although the OT network data may be static, it carry big amount of data due to the nature of protocols and servers in the network (repetitive data collection from sensors in the network may not carry a big amount of data, but the repetitiveness of these requests generate a data that need big data technologies to efficiently analyze)

- **Vulnerability scanner**:
  A vulnerability scanner is a software designed to assess computers, networks or applications for known weaknesses. In plain words, these scanners are used to discover the weaknesses of a given system.
  Although multiple vulnerability scanner solutions exist in the market, few have NOT scanning capabilities. OT devices as critical infrastructures need dedicated scanners that can identify the vulnerabilities as well as assuring the functioning of these devices specially that some OT machine can easily shutdown when receiving unidentified traffic or when it finds itself subject to malicious or intrusive scripts.
  SANTI uses OpenVAS as a vulnerability scanner. Its capabilities include unauthenticated testing, authenticated testing, various high level and low level Internet and industrial protocols, performance tuning for large-scale scans and a

powerful internal programming language to implement any type of vulnerability test.
The scanner is accompanied by a vulnerability tests feed with a long history and daily updates. This Greenbone Community Feed includes more than 50,000 vulnerability tests. The scanner has been developed and maintained by Greenbone Networks since 2009. The works are contributed as Open Source to the community under the GNU General Public License (GNU GPL).
Greenbone develops OpenVAS as part of their commercial vulnerability management product family "Greenbone Security Manager" (GSM). OpenVAS is one element in a larger architecture. In combination with additional Open Source modules, it forms the Greenbone Vulnerability Management solution. Based on this, the GSM appliances use a more extensive feed covering enterprise needs, a GVM with additional features, appliance management and a service level agreement.

3 IDS choices in the Market

In this chapter we will present the most innovative and used IDS solutions in the market. Within this presentation we will present the companies involved in the development of these solutions, the IDS product developed, the solutions advantages and disadvantages. For each solution we will also present the advantages of using SANTI IA.
SANTI IA is a solution currently being developed by a team of industrial security experts from InprOTech collaborating with the center of research and development Gradiant. The project is funded through the NEOTEC initiative dedicated to support advanced research and product development.
SANTI IA would be an IA empowered OT solution with cloud and big data capacities. The solutions would support a variety of industrial protocols and will help identify multiple advanced threats through the technologies implemented. SANTI IA would incorporate basic and advanced functionalities.

- **Choice 1**:
  - **Company**:its-security
  - **Product**: CID360
  - **Advantages**:
    - Detect threats, correlate and analyze indicators between files, users, networks, devices, digital identities and workstation.
    - It integrates easily into existing security infrastructure, allowing organizations rapid capacity and flexibility to respond, neutralizing unknown threats, anomalies, and unsigned malware that have been bypassed by existing detection solutions.
    - Control from a single platform the state of cybersecurity of the company
  - **Disadvantages**:
    - An IT product being used for OT
  - **How SANTI stands out**:
    - SANTI IA is a dedicated AI-capable OT solution that uses advanced mapping capabilities to identify threads.

- **Choice 2**:
  - **Company**: Nozomi
  - **Product**: SCADAGuardian
  - **Advantages**:
    * Support for a large number of OT protocols
    * Asset inventory and vulnerability analysis
  - **Disadvantages**:
    * Limited number of nodes supported per machine.
  - **How SANTI stands out**:
    * SANTI IA has an active vulnerability analysis.
- **Choice 3**:
  - **Company**:S2Grupo
  - **Product**: Platforma de S2GRUPO-CERT (GLORIA ICS)
  - **Advantages**:
    * Alert management, event correlation, surveillance.
  - **Disadvantages**:
    * No use of AI capability.
  - **How SANTI stands out**:
    * Easy to use (compared to multiple modules and platforms).
    * AI capability.
- **Choice 4**:
  - **Company**: Fortinet
  - **Product**: Fortisiem from Fortinet
  - **Advantages**:
    * Security with asset analysis and user behavior through IA (UEBA) capability.
  - **Disadvantages**:
    * Non-OT specific.
    * Complicated to install.
    * High price ranges.
  - **How SANTI stands out**:
    * OT-specific IA capability.
- **Choice 5**:
  - **Company**: Splunk
  - **Product**: Splunk enterprise security
  - **Advantages**:
    * Using machine learning for behavior analysis.
  - **Disadvantages**:

    * No dedicated OT vulnerability scanning solution.
  - **How SANTI stands out**:
    * Easy to implement.
    * Economic.
    * Advanced log and alert management.

- **Choice 6**:
  - **Company**:Checkpoint
  - **Product**: 1570R
  - **Advantages**:
    * Protects all types of OT assets.
    * Non-disruptive for critical industrial processes.
    * Complete segmentation between IT and OT networks.
    * Granular control through OT environment.
    * Zero-day attack prevention.
    * Scalable.
  - **Disadvantages**:
    * Initially IT solution that has been customized for OT, its previous version was not so personalized.
  - **How SANTI stands out**:
    * Specific solution for OT.
    * Smart Scoring.

- **Choice 7**:
  - **Company**: IBM.
  - **Product**: IBM Security QRadar.
  - **Advantages**:
    * Support of multiple industrial protocols with specialized module.
    * IBM's own AI module: Watson.
  - **Disadvantages**:
    * Automatic responses only available through IBM add-on products.
    * User interface not consistent in the various components of the platform.
    * User experience (UX) in Qradar is less than modern.
  - **How SANTI stands out**:
    * Consistent user interface.
    * Simple and current user experience.

- **Choice 8**:
  - **Company**: LogRhythm
  - **Product**: LogRhythm
  - **Advantages**:
    * Different types of analytic on machines.

    * Wide range of modules to expand functionalities.
  - **Disadvantages**:
    * They do not support third party vulnerability databases.
    * Low capacity to support large volume of events.
  - **How SANTI stands out**:
    * A complete vulnerability scanner with OT capabilities.
    * An event and log manager.
    * Specific for OT.

4 CONCLUSIONS

There are multiple IDS products in the market with a high variety of providers as well as functionalities. We hope that this guide helps you choose the right IDS system for your industrial infrastructure taking into account the advantages as well as the risk. Here in InprOTech, we re developing a state of the art IDS system with advanced capability that would helps you monitor and protect your facilities. Although we have our own solution, we also offer a variety of consulting services that can help you improve your security.