ITS INVENTORY

Product description

ITS Inventory application helps companies to instantly access disparate inventory information about computer network assets. This access allows IT professionals, information security officers and Security Operation Center analysts to quickly receive up-to-date information about servers, computer workstations, network and other devices.

This speeds up the analysis of any incident, increases the staff efficiency, helps to identify failures, configuration errors and problem areas in the network.

Hardware and software inventory are the most important IT management tasks that nowadays has become a «classic» problem. Its solution in any organization is complicated by the fact that static information in CMDB databases, multiple XLS tables and online directories (such as, for example, a corporate directory service) becomes outdated very quickly, has consistency issues, has many disconnected owners in various departments, have a different form, structure and purpose. As a result, straightforward identification of information, which system owns which IP address, where the server is located, or who is responsible for operating the switch, becomes as difficult as putting together a jigsaw puzzle from several thousand pieces.
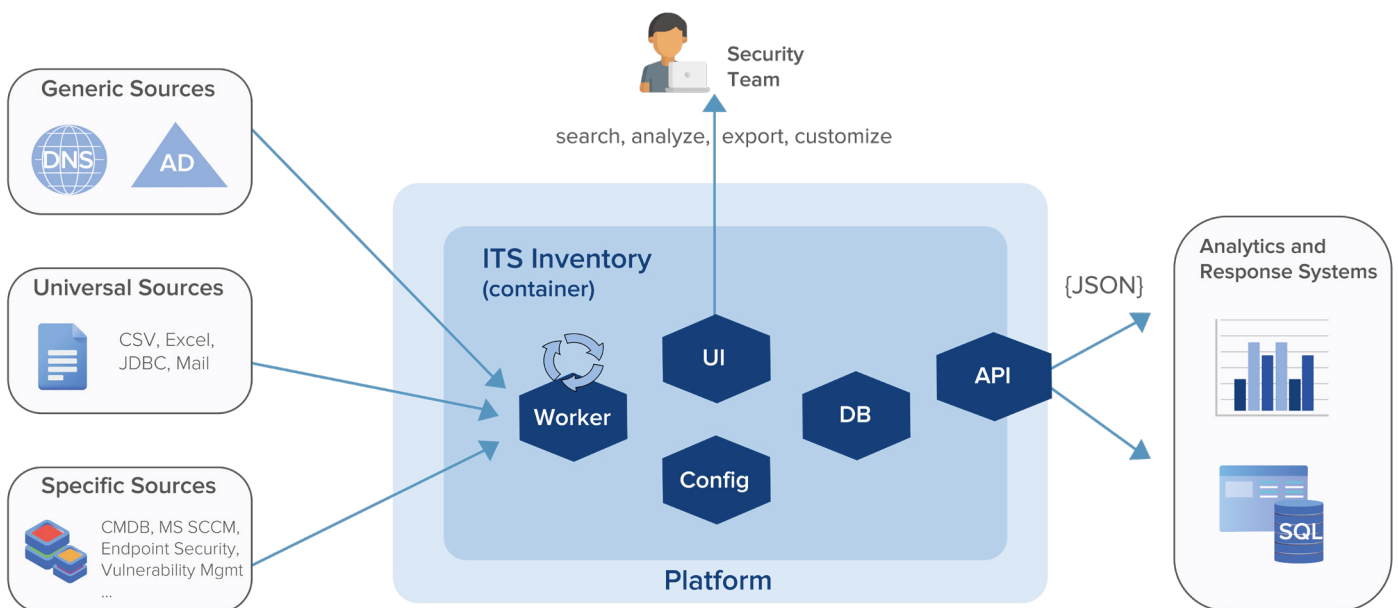
It is no coincidence that the American Center of Internet Security placed the inventory of hardware and software in the first two positions in its famous list of TOP 20 Security Controls. Without a clear understanding of what and where operates in the network, what it consists of, how these components are used and who is responsible for them, it is almost impossible to efficiently manage the IT infrastructure and ensure its protection against modern threats. ITS Inventory allows you to solve the following tasks:

- Collect all valuable data related to assets and endpoints in one place;
- Quickly switch between tabular and detail views;
- Perform a quick search on any field;
- Select important records for analysis and hide unimportant ones;
- Compare different records with each other according to various parameters;
- Interactively select fields with valuable data to display as a table;
- Save table view as a template for future use;
- Share view templates between users;
- Highlight date fields in different colors for quick identification of problems;
- Export collected data in JSON or CSV format;
- Generate events when data changes to trigger correlation rules and implement complex monitoring scenarios;
- Access inventory data directly from the system's SIEM interface via the context menu;
- Use built-in API for data enrichment in CMDB, external BI, SOAR systems and reporting systems.

The ITS Inventory software was initially developed as a software module for the IBM QRadar SIEM system. Its interface is embedded in the IBM QRadar web console and uses this system as one of the infrastructure data providers. At the same time, it is possible to use the application independently on a standalone server to integrate it with other SIEM systems, i.e. Splunk, ArcSight, McAfee, LogPoint, ELK etc.
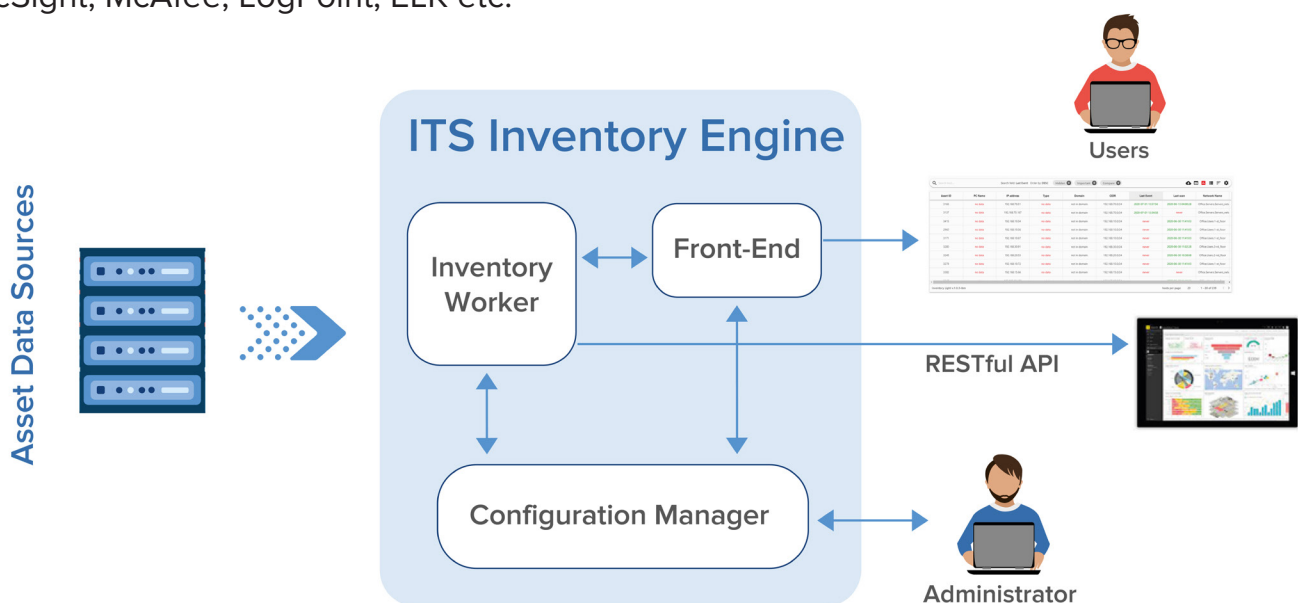
ITS Inventory consists of two parts - front-end GUI interface and back-end service (Worker). The GUI is developed in Angular, which makes it very fast, ergonomic, convenient and functional. The system interface displays information about the components on the network in a simple tabular form. A component can be any physical or virtual device that has an IP address or a name. For each component, the interface can display the values of several thousand data fields. Data fields are formed individually for each customer based on the sources used in the company.

Each user of ITS Inventory has the opportunity to create his own list of information fields and apply his own filters to the table to create a visual representation that is convenient for his work. Such visual representations can be stored in the system, reused or exported as a configuration file and shared with other users. Also, each user can view all the fields available for a specific device.

Such fields may include, for instance:

- name;
- network address;
- location;
- type;
- subnet;

- responsible administrator;
- installed software;
- list of open ports;
- reboot and shutdown history;
- status of backup tasks;

- runtime environment;
- presence of critical vulnerabilities;
- parent business process etc.

The list of fields is limited only by the desire of the Customer and the availability of relevant information anywhere in the IT infrastructure.

The interface also allows you to perform a quick search in any field, identify devices using any portion of available data, compare information between different systems, identify value conflicts between different data sources, and set tasks for IT specialists to update data. Through integration with a SIEM system, the application can monitor changes in the source data and notify responsible personnel about them, or use this information to identify and escalate more complex incidents related to the IT infrastructure or information security.

The internal Worker process constantly analyzes data sources and extracts up-to-date information about network components. This information is stored in internal storage (database cache), which allows you to always have fresh data at hand.

Information received from various sources is combined according to a certain attribute, compared, analyzed and prepared for display in the GUI. Depending on the size of the infrastructure and the response speed of sources, the frequency of data updates can vary from 15 minutes to 2 hours. The number and types of sources, as a rule, are individual for each company. Most often, companies connect ITS Inventory to the corporate directory services, cloud services, virtualization systems, infrastructure monitoring systems, network management, SOC.

Standard ITS Inventory connectors support data retrieval using various protocols such as:
- JDBC;
- LDAP;
- HTTP(S) RESTful API;
- SOAP/XML API;
- syslog;
- SSH;
- FTP/SFTP;
- CIFS;
- NFS;
- HTTP GET/POST.

The analysis of text files and Microsoft Office files is also supported. Additionally, we constantly extend the connectors library by developing them for systems that are used by current Inventory customers.

ITS Inventory collects, aggregates and enriches infrastructure data almost bit by bit in order to provide the valuable information to those who need it to perform their tasks - analysts, administrators, business process owners, developers, top management.

As well, ITS Inventory can be used as a source of information for external systems. With its built-in and well-documented HTTPS RESTful API, ITS Inventory becomes a provider for Business Intelligence (BI), Business Process Automation, IT Accounting (CMDB), IT Process Management and Change Control systems. So, for example, on the basis of ITS Inventory, many companies implement interactive analytical dashboards to control the backup system, the health of business processes and network monitoring.

IT Specialist team is ready to conduct an extended demonstration of the product (Proof-of-Value) in your company's infrastructure, to show the ease of implementation, integration and use to solve daily SOC and IT problems. Our developers will, if necessary, provide new connectors to the unique IT systems that are used in your infrastructure and implement your wishes for an interface or automation of inventory, change management and monitoring processes.