Report on Existing CS Patents

Method and system for cyber security management of industrial control systems

The Cybersecurity Management and Data Acquisition Systems (SCADA) are provided to increase situational awareness and cyber security management in industrial control systems. Centralized Security Management (SSM) is integrated with SCADA to collect security-related data for the industrial control system, and the integrated user interface for commands and controllers display security-related data, system security level and user interfaces, allowing you to change the system security settings for an industrial control system based on aggregated safety data. It manages SCADA operating state changes based on security level to limit the use of system interface and access.

The invention relates to a method and a system for computer security management in industrial control systems, in particular for computer security management in monitoring and data collection systems (SCADA). In general, the present invention provides a method and system for managing network security in a Data Acquisition Monitoring and Control System (SCADA). The present invention is a method and system for integrating network security, training, engineering, command and control into a comprehensive solution using a SCADA system.

The present invention provides a solution for an integrated engineering system in which configuration data is defined only once. It provides a complete user interface for direct connection to internal SCADA functions, data, alarms and controls. In addition, the Operator Training Simulator will be extended to train users to properly use network security features. The present invention is supported by organizing all security related information (data monitoring, alerting, security settings) into a series of presentations.

Adaptive cyber-security analytics

Perform an adaptive network security analysis, including computer-implemented methods, to obtain an online report. The computer network response and scoring model is calculated on the computer. The result is a potential security breach. The result is validated and the result model is automatically updated based on the validation results. Network activity has been reported as suspicious if the result is a security breach. This invention is typically applied to IT security monitoring, especially in the monitoring of inbound security events to determine the existence of security breaches.

Examples of target approaches are anti-virus-based anti-virus and intrusion detection systems into the network. Discovering behavior behavior provides alerts that are based on behavior behavior or deviations from the normal behavior of users and / or entities on the network. Many threats to security such as malware (malware) are automatically developed and the existing detection mechanisms (e.g. B. Polymorphism, snapshot, sand, reverse engineering, attacks, etc.). The network activity is reported as suspicious in response to the score being within a threshold of a security violation value.

In the current invention of inventions, other functions and benefits have been implemented. The other characteristics and characteristics of the invention are described in detail and are considered to be a part of the invention. There is a description of the benefits and capabilities of this invention by referring to the description and drawing. The purpose of the current invention is to create and develop automatically targeted detectors (commonly used for the general use of undetectable or clear-cut), behavioural deviations and other scoring methods and combinations thereof for the purpose of monitoring cyber security. Free assistive tool for the monitoring of cybersecurity by monitoring future security events and determining whether future safety incidents constitute a security breach.

Control system cyber security

The systems, methods and systems of the cyber security monitoring system are described below. A method comprises the receipt of a plurality of measurements by a number of devices for the detection and training of a control system, a determined part of the measurements obtained being determined, the suspect part of the measurements obtained during a certain period of time being monitored, and determine whether the suspect part of the measurements obtained is related to a computer attack. Many processes can depend on the control systems to increase efficiency and/or automation, or to optimise a set of functions on a physical system.

For various reasons, someone can launch a cyber attack on a control system. Such reasons include cybercrime, blackmail and/or war. For example, the possible cost of an attack on processes such as the refining of gas, chemical production and electrical current may be large. Traditional techniques receive measurements from various aspects of the control system (e.g., sensors), which may destroy the data of suspect (such as noise). In the previous approach, the previous approach may be vulnerable to cyber attacks, since it may not be able to recognize that an attack is occurring.

The control systems can be regarded as unique in different ways on the basis of other systems. A user (e.g. An administrator) that monitors the monitoring system, for example, has a physical system on which the user can create simulation data and/or pointers. The simulator (e.g. B. executable statements) can show the different values that must exist throughout the process (e.g. For example, the expected values). For example, if the measurements are influenced by a cyber attack, the installation of the current information can reveal changes in the measurements by observing the physical movement of the process itself. In the event of a cyber attack, the procedures for the implementation of these advertisements may take several measures.

Cyber security in an automotive network

The prevention of spooning in the car network includes monitoring, electronic control unit, data packets on the bus network on the car network. If it is established that the data package is not an electronic control unit, which is not an electronic control unit, which is not an electronic control unit, it shall include the creation and transmission of diagnostic messages on a car network via a bus, a diagnostic message indicating at least one module that does not take the data package, to prevent the use of the car network. The spooling of messages in a vehicle bus includes the location of the messages on the bus from a form that outputs a different mask to ensure that the vehicle is not determined by an operator of the vehicle.

This disruptive module can send messages to the bus, and the target modules send messages without knowing where they are located and where they are. The consequences of a vehicle that deals with fake embassies can be serious. It is better to provide the means to detect the messages used in the automobile network and to avoid the unintended consequences of these messages. The method comprises the monitoring, the electronic control unit, the database in the network. If you specify whether a data packet with an identifier is a source that is not an electronic control device, the diagnostic message is converted at least once into the production and allocation of the diagnostic message when a network module is present on the bus.

The system includes an electronic control control, an edb processor. The system also includes a program file, where the program processor of the computerprocessor is edb registry driver. The review of the application of the application of the Acadian is the configurable of the implementation of a method. The method includes monitoring the monitoring of monitor data packets on a bus in the automobile web. Af frakly for af, that a data package is from a country's source, ophes the electronic control, includes the method, that there are opes and transcends an indensnared message to the mindset module in the automotive web in connection with the bus. The co-share announcement instructs the modular to, that there is no gene action on the data packet. In another mode of exemplary embodification, a method of prevention of misfit is put in place in a network of cars.

Cyber security adaptive analytics threat monitoring system and method

Systems and methods are disclosed to detect malware commands and control behaviors on client computers. One or more DNS messages are monitored by one or more client computers to the DNS server to determine the risk that one or more client computers are communicating with Botnet. A real-time profile is generated for at least one client computer based on at least one DNS message for one or more client computers, DNS query names, domain names, IP domain names, client language domain names, domain names, and corresponding allowed IP addresses, or domain name IP addresses, respectively, based on at least one DNS message. Real-time profiles define the risk of one or more client computers being infected with malware using DNS messages for management and control, and a nonregular data transmission is defined.

The dangerous threats made available to the Internet cannot be completely blocked by network administrators, without strictly limiting the access of subscribers to the Internet for legitimate purposes. In any important organization, it is inevitable that a user of an internal computer will capture malware and mine the security of your computer with malicious software, which can only be included on other computers in the organization's computer network. Some malicious software attempts to extract valuable information from the computer computer and use a message (a collection of zombie computers controlled by aggressive aggressors) by exploiting the computer to exploit the Botnet infrastructure connected to the malicious software.

As malware and its delivery mechanisms are changing, it is necessary to view the networks that already compromised and invest resources in the detection of malware on the network and on target destination for malware. Once the C&C channel is identified between compromised internal computers and external suspicious hosts, the outbound communication can be reduced, thereby protecting sensitive information and preventing botnet from being added to additional resources. The details of all the tracked C&C information can also be logged by the responsible network administrators in the security organization, so that other networks may, before emptying are the same person. The assertions resulting from this publication are intended to define the scope of the protected subject.