Vulnerability Management in SCADA and ICS Environments

How to do it with Greenbone Networks Appliances

White Paper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

2018-08-21

Contents

Introduction

Vulnerability Management

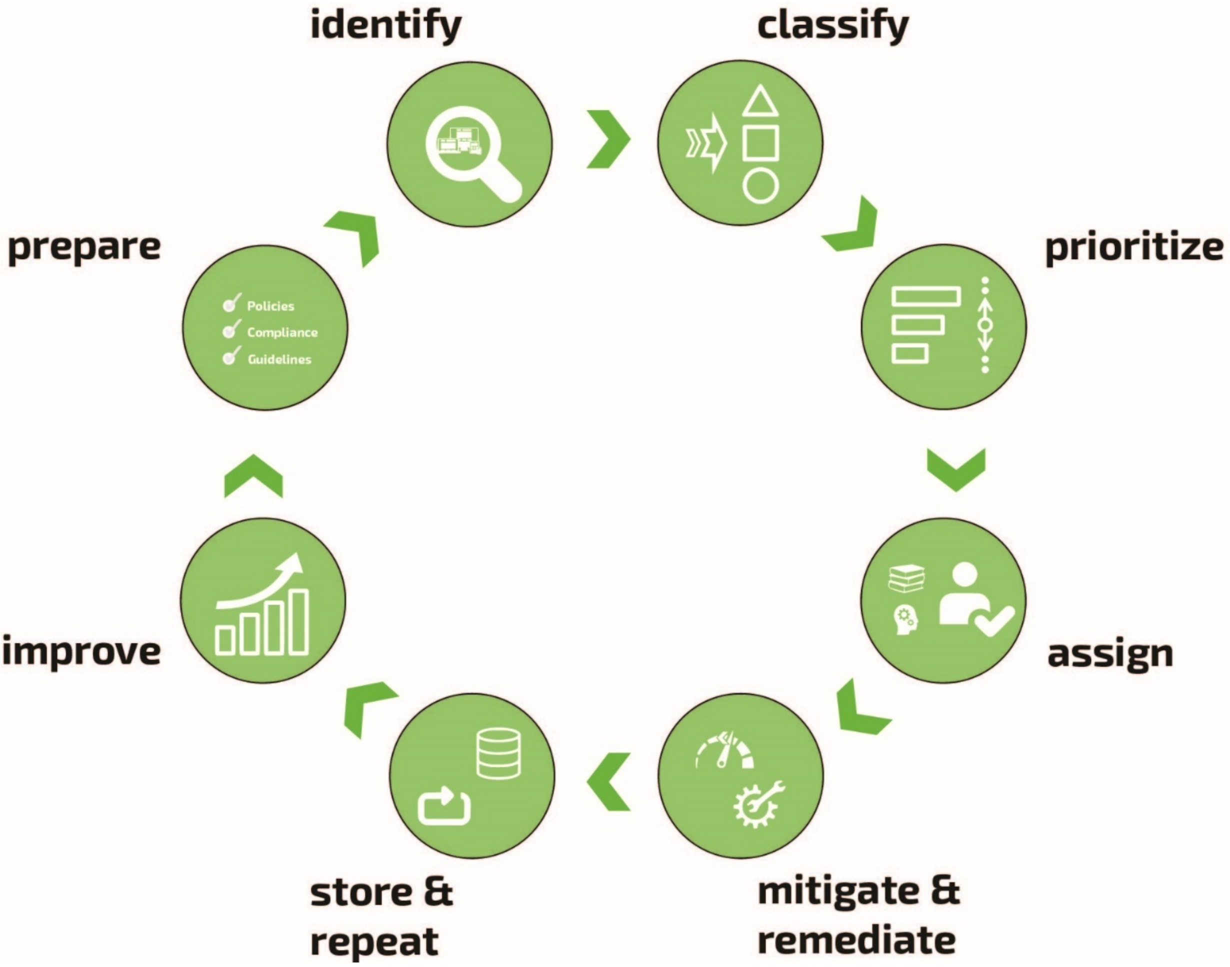
Vulnerability Management is a vital element of your IT compliance: within IT security, technical security must be ensured by an ongoing management process; the aim of which is to protect the system from dangers and threats, avoid damage and minimize risks. Managing Directors and Information (IT) Directors must ensure the complete protection of corporate data. In its simplest form, the continuing process consists of three steps:

Assessment -> Measures -> Controls

The security measures taken must be adapted continuously to changing basic conditions. It is best to prepare the necessary regulatory and control measures using an automated, integrated system.

Vulnerability Management Process

Greenbone's Vulnerability Management Process is designed to provide for this in an orchestrated, effective and adaptive way.



The process reflects the business needs of an organization to efficiently and effectively address its vulnerabilities. At the same time the protection levels for an individual asset (i.e. high, medium, low) can be adjusted to update the overall internal security guidelines due to regulatory changes or internal security policy enhancements.

The steps can be outlined as follows:

- Prepare:
    - Define the goals of IT security within your organization
    - What is allowed / What is not
    - Tie that to technical controls
- Identify, Classify, Prioritize:
    - What to address first?
    - Which one has the greatest impact?
- Assign, Mitigate & Remediate:
    - The right person makes the necessary changes, having all vital information at hand
- Store & Repeat, Improve:
    - Automated, scheduled processes
    - Improvement of IT Sec documented with KPIs
    - Adding to and enhancing the goals set for IT Sec

For more information about Greenbone's Vulnerability Management Process, please refer to our website (www.greenbone.net).

SCADA and ICS is not ITS

What is SCADA?

It stands for **S**upervisory **C**ontrol and **D**ata **A**cquisition and it represents a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management but uses other peripheral devices such as programmable logic controllers and discrete PID controllers to interface to the process plant or machinery.

The complete automation and actors are called **I**ndustrial **C**ontrol **S**ystem (ICS)

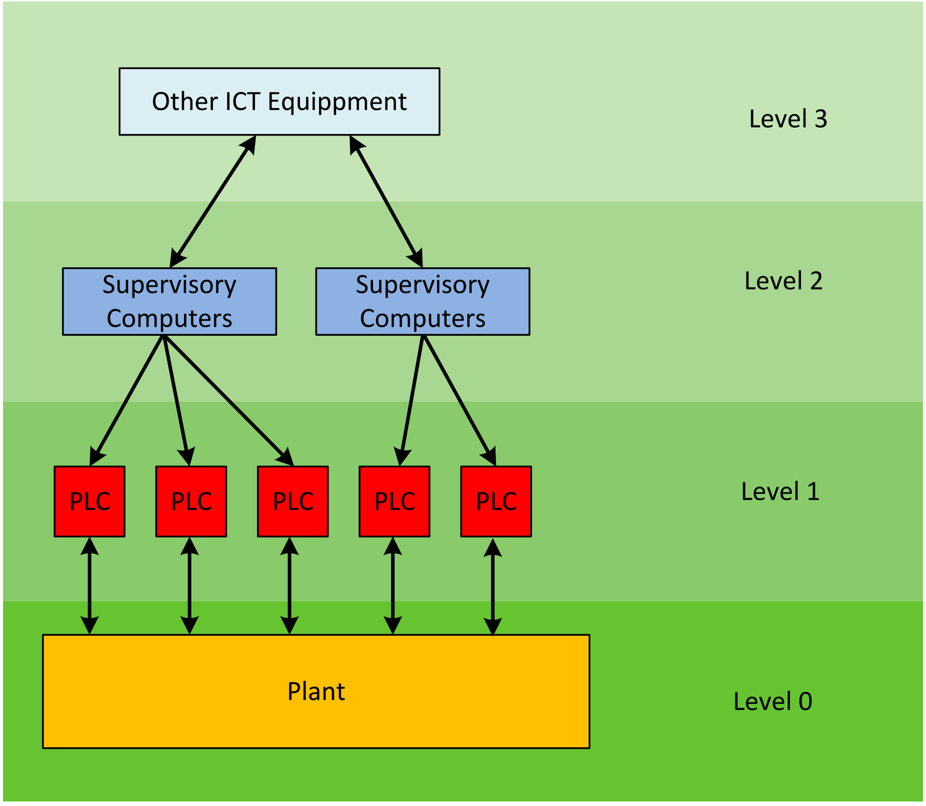
The operator interfaces which enable monitoring and the issuing of process commands, such as controller set point changes, are handled through the SCADA computer system.

However, the real-time control logic or controller calculations are performed by networked modules that are connect to the field sensors and actuators.

The SCADA concept was developed as a universal means of remote access to a variety of local control modules, which could be from different manufacturers, allowing access through standard automation protocols.

In practice, large SCADA systems have grown to become very similar to distributed control systems in function, but using multiple means of interfacing with the plant. They can control large-scale processes that can include multiple sites, and work over large distances as well as locally. It is one of the most commonly-used types of industrial control systems; however there are concerns about SCADA systems being vulnerable to cyberwarfare/cyberterrorism attacks.

SCADA structures and concepts of Industrial Control Systems



Area	Function
Level 0	Contains the field devices such as flow and temperature sensors, and final control elements, such as control valves.
Level 1	Contains the industrialized input/output (I/O) modules, and their associated distributed electronic processors.
Level 2	Contains the supervisory computers, which collate information from processor nodes on the system, and provide the operator control screens.
Level 3	Contains other ICT components already handed by IT security products

Need for Action

While all SCADA Systems of the 3rd generation are networked and use TCP/IP, it will bring a lot of additional risks and attack vectors for cyber-attacks and needs vulnerability management.

The 4th generation also known as “Internet of things” will bring a new dimension of risks and security requirements as well.

Vulnerability Management is well known in the ICT world (Level 3), but due to the wide spread use of TCP/IP on the Levels 0-3, and that this protocol can be accessed on a global scale; it should be integrated into your vulnerability management process as well.

Common pitfalls and reasons for ICS fails

If you try to use off the shelf security components, you will fail; there are several reasons why it´s not a good idea to use ICT security products without awareness of the special needs of ICS vulnerability scans.

Fragile TCP/IP Stack

While your computer is constantly attacked and Operating-Systems from Linux and Microsoft have been under constant attack since 1994, ICS components have just recently been connected to the IT world. That means you are running the equivalent of a vintage car from 1900 on the information super highway.

Such a combination results into a very fragile TCP/IP stack, without the needed resilience. An off the shelf vulnerability scanner or even an NMAP might crash your ICS components.

Same device different animal

Often the same device comes with the identical technical function, but it has different hardware and firmware revisions that act in the defined operating state identically, but during a vulnerability scan or if some abnormal IP-Packets are sent, it reacts totally differently.

If one device fails during the scan, a complete other set of otherwise identical device might survive without any issues.

Can´t update firmware

If a device runs in a productive state, it´s often impossible to run a firmware upgrade without stopping the complete production of the entire plant.

Sometimes a hardware exchange is needed to run fixed firmware.

Best practice: how to scan a ICS

Step by Step

It is not recommended to run a pre-configured “Full&Fast” scan like, Greenbone is shipping it with its turnkey appliances, as you would with your normal office environment.

Greenbone provides a “Discovery Scan” this is helpful and prevents crashish any ICS components during the first discovery of TCP/IP devices on the industrial level network.

- If you don´t have emergency plans or cannot run it in a safe mode, or high value products are at risk, you must build a Laboratory with spare parts of your factory to scan here.
- Don not scan everything at once, start with a small part
- Build a special scan configuration
- Depending of the local situation, it might be necessary to build an extended scan configuration

A scan configuration defines the amount and order of network vulnerability tests (NVTs) that the Greenbone Security Manager runs against the scan targets.

Step-1

Start with a “Discovery” Scan, use only “Host Discovery”. At this stage Greenbone is not sending any TCP or UDP packets, just ICMP, but it helps you to get an overview of your environment.

Step-2

Generate a new Scan-Configuration that includes only the following NVTs:

Family: Port scanners

Nmap (NASL wrapper), OID: 1.3.6.1.4.1.25623.1.0.14259

Ping Host, OID: 1.3.6.1.4.1.25623.1.0.100315

Family: Service detection

Host Details, OID: 1.3.6.1.4.1.25623.1.0.103997

Additionally you should change the “timing policy” to “polite”, deactivate parallel requests per host and add 0.4 seconds between every single request.

With these changes, you can run a 2nd scan after your first discovery scan.

This special ICS Scan-Configuration can be requested from the Greenbone Support without any additional costs.

Step-3

Repeat Steap-2 but change the “timing policy” to “normal”

Step-4

Repeat Steap-2 but change the “timing policy” to “aggressive”

Step-5

If your ICS still runs stable, you can now try to run a “Full&Fast” Scan against it.

For this you can create a new Task and change the “maximum concurrently executed NVTs per host” to one. You can change the timing policy and “time_between_requests” to act more politely with the fragile TCP/IP stacks and old devices in your plant.

What does Greenbone cover in the ICS environment

Here is a small excerpt what Greenbone covers, when it comes to ICS scans.

Vendor specific tests:

- Siemens SIMATIC S7 (e.g. CPU 1200, CPU 300)
- Siemens SIMATIC CP (e.g. CP 343-1, CP 443-1)
- Siemens SIMATIC SCALANCE (e.g. XB-200, XC-200, XP-200, XR300-WG, XR-500,XM-400, M876)
- Siemens Desigo PXC
- SpiderControl SCADA Web Server
- Rittal Smart Monitoring System
- Rockwell Automation MicroLogix (e.g. 1100, 1400)
- PHOENIX CONTACT FL COMSERVER
- Schneider Electric StruxureOn
- Emerson ControlWave
- Belden / Hirschmann (e.g. MACH, MICE, EAGLE)
- Saia Burgess Controls PCD
- Moxa (Mgate, EDR, EDR G903, EDS-40x/50x, ioLogik, MiiNePort, MXview, NPort, AWK)

Generic Industrial tests:

Apart from certain products, our solution also supports common Industrial protocols, frameworks and platforms such as:

- Modbus
- Moxa Management Protocol
- EtherNet/IP
- Distributed Network Protocol (DNP3)
- AB Ethernet Protocol (CSP)
- Factory Interface Network Service (FINS)
- ProConOS
- CODESYS
- Geovap Reliance SCADA
- PCWorx
- ECAVA IntegraXor

Additional coverage is always possible with a feature request via Greenbone Support.

What´s next?

Greenbone Networks is integrating an “Achilles” mode into its appliance.

What is Achilles?

The Achilles Certificates defines what type of requests and malicious packets an industrial device must withstand without malfunction. It will define a resilience level for the device, to prevent major faults during a vulnerability scan.

What is Greenbone implementing an Achilles mode?

If a device is certified, it is must still be vulnerability managed, Greenbone provides a daily updated security feed, so an Achilles mode will limit our powerful scanner to just running certain Achilles compliant requests, where it is known that the target device will not malfunction in the ICS environment. This will bring a lot of additional stability to a rock solid vulnerability management process within the ICS world.

The Solution

The Greenbone technology architecture consists of two main components (Greenbone OS and Greenbone Feed) and is available in two different versions.

The Greenbone Security Manager (GSM) is a feature-rich enterprise solution providing the needed capabilities for its integration into an overall security architecture, even for high-security networks requiring an air-gap approach. It is built for professional use in enterprises and administrations. It is delivered as a turn-key appliance that delivers the full capabilities and features to our enterprise customers in a hassle-free way, the only Vulnerability Management Solution you need – Greenbone Networks.

Greenbone Networks GmbH

Greenbone Networks delivers a vulnerability management solution for enterprise IT which includes reporting and security change management.

The company was founded in 2008 by leading experts in the fields of network security and Free Software with the goal to engineer products and concepts able to cope with the present and future challenges of next generation Open Source vulnerability assessment and management. Greenbone especially focuses on a transparent, white-box solution that provides a customer-provable level of security, designed to operate in most critical Fortune-500 environments, as well providing a comprehensive, cost-conscious turn-key solution for small and medium sized customers.

At Greenbone we take a holistic approach to minimize and manage risks originating from system vulnerabilities. Greenbone is the first in this market providing a 100% Open Source solution. The full white-box approach enables our customers to eliminate the risks that a proprietary vulnerability assessment management solution draws into critical IT infrastructure. Greenbone works with the global, multi-cultural security and Open Source communities in a cooperative manner. We understand the concept of give and take as well as the joint development and community processes around Free Software.