securiCAD Vulnerability Assessment

Whitepaper

2022

foreseeti

KTH VETENSKAP OCH KONST

Authored by:
Joar Jacobsson
Ismail Butun, Robert Lagerström, Jose Cabus

ENERGY SHIELD

securiCAD Vulnerability Assessment Tool

> ***Combining user information with a threat model is a very powerful combination since information on "soft" assets are usually more difficult to gather than information on networks, assets, communication and related security status.***
>
> *Joar Jacobsson,*
>
> *Cyber Security Expert, FORESEETI*

IN A NUTSHELL

The threat modelling and attack simulation approach makes use of a model of an environment which is used to run attack simulations on. In other words, a digital twin or offline copy of the environment is created, allowing for attack simulations using a virtual attacker, which means that the method is non-intrusive by nature.

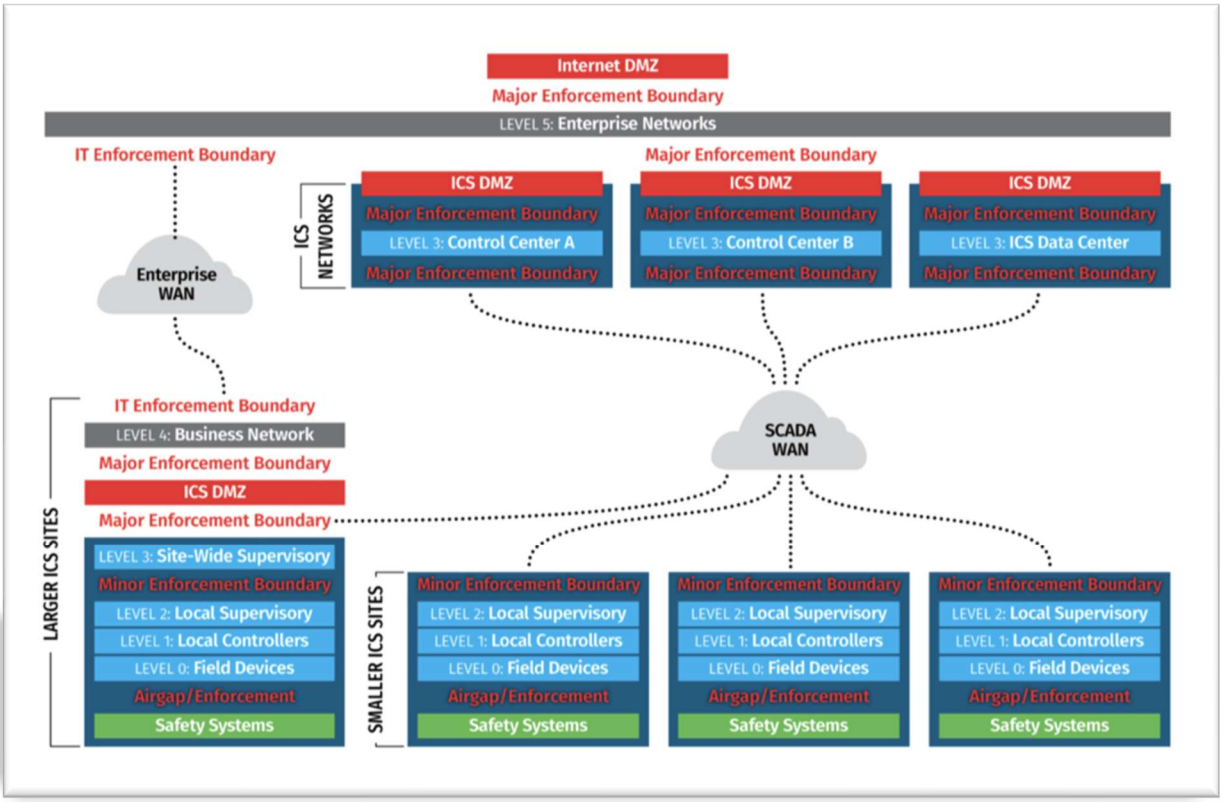
A model can be automatically generated using different suitable data sources, i.e., the "data-driven" approach, or it can be created manually if the availability of actual data is limited or if the architecture is not yet implemented.

The attack simulations will then show information about the security status of the architecture (existing or planned) in terms of an attacker's expected attack path or, from the architect's point of view, the environment's weakest links.

The effects of different attack vectors can be simulated and compared, and among other findings, the simulations can present suggested mitigations to improve the attack resilience of the architecture.

CONTEXT

IEC62443/ICS410. Within the energy sector, and other industries with solutions based on SCADA environments, a common approach to designing an architecture is to use the ICS410 reference model (https://www.sans.org/blog/introduction-to-ics-security-part-2/) or the IEC62443 Purdue model.



Zones and zone separation. The architectural structure described in the model above defines a separation of zones within the SCADA architecture. This separation is based on different tasks or categories of the systems within the architecture. Systems belonging to a certain category, or "SCADA level", are only intended to communicate with "neighboring" SCADA levels.

A "zone" is, according to the International Society of Automation , defined as "a grouping of logical or physical assets based upon risk or other criteria such as criticality of assets, operational function, physical or logical location, required access, or responsible organization."

Thus, to investigate to what extent an architecture is conforming with the ICS410 reference model or the IEC62443 Purdue model, not only the "technical" security aspects need to be considered but also the more administrative aspects like the purpose of different systems. Therefore, systems belonging to a SCADA architecture are usually assigned a "SCADA level".

Threat modeling is recommended. According to ISA, "One of the key processes in the product SDL (Security Development Lifecycle) is threat modelling which is a systematic process to identify data flows, trust boundaries, attack vectors, and potential threats to the control system. The security issues identified in the threat model must be addressed in the final release of the product and the threat model itself must be periodically updated during the product's lifecycle."

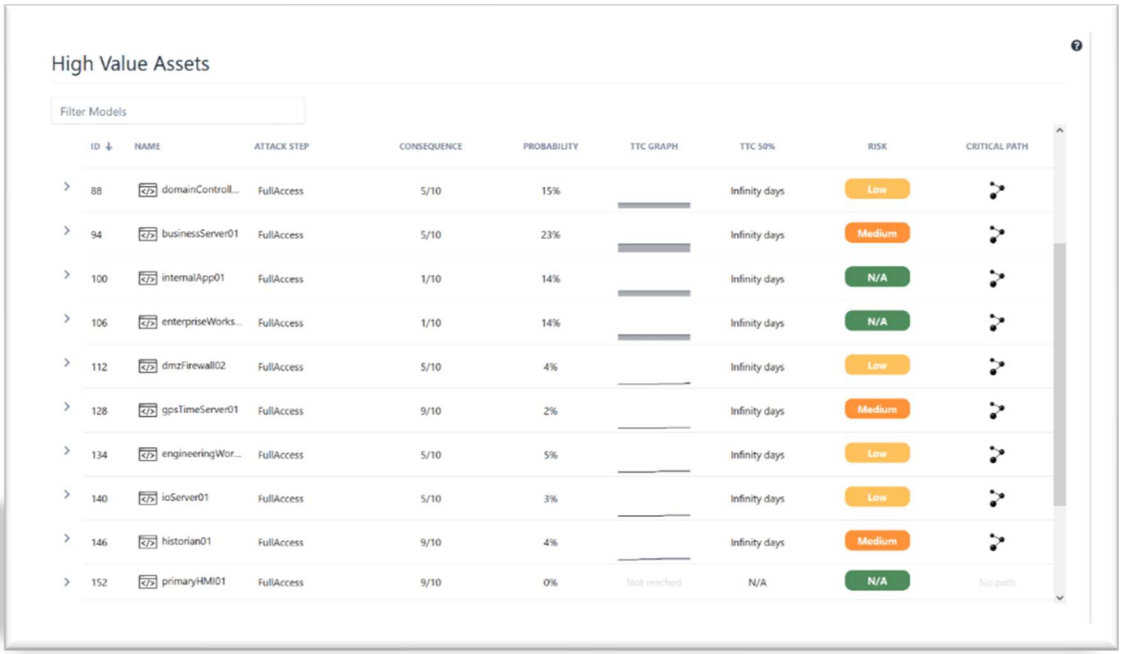
Continuous threat modelling can reveal changes to an environment when new information is made available. Such information can, like in the EnergyShield project, come from information about User

behaviour provided by the SBA tool. Taking such updated information into account and then running a second simulation will reveal the User behaviour's actual impact on the modelled architecture .

TECHNICAL DETAILS

The purpose of creating a model of an architecture or a live environment is to be able to run attack simulations on that model. The attacker is given a starting point, defining the initial attack vector, and the simulation engine then calculates and presents the expected path the attacker will follow within the model. This is possible since the modelling language/objects contain logic regarding which attacker operations are expected to lead to different achievements, which in turn make further operations possible. Some operations are a direct effect of previous achievements, while others require additional effort or are not guaranteed to be successful depending on the status of the objects in the model.

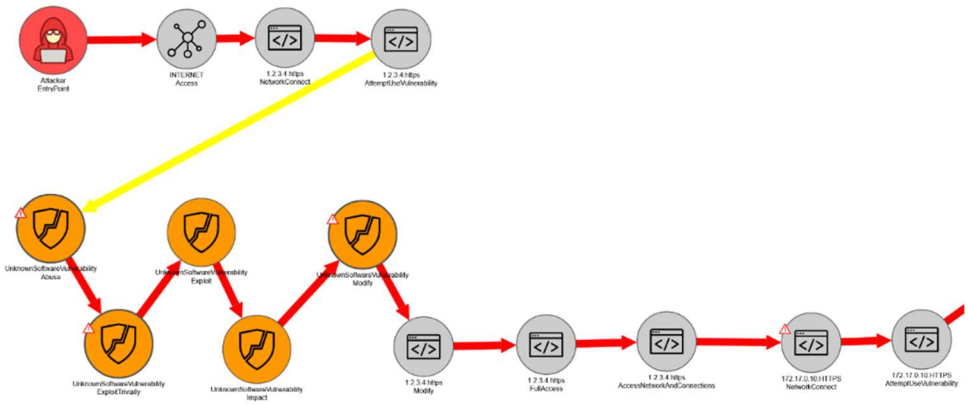
High value assets._When running an attack simulation on the example model, the results are presented in terms of the success rate and the expected path of least resistance for reaching and compromising selected "high value assets". These can be seen as attacker targets or golden eggs. The assignment of these objects in the model can either be done manually or be based on criticality information for different assets provided that such information is available in the asset/inventory input data.



As seen in the simulation results of the example model above, the listed high-value assets (based on the criticality level read from the inventory system information) are expected to be at different levels of risk when simulating an attack starting from the Internet.

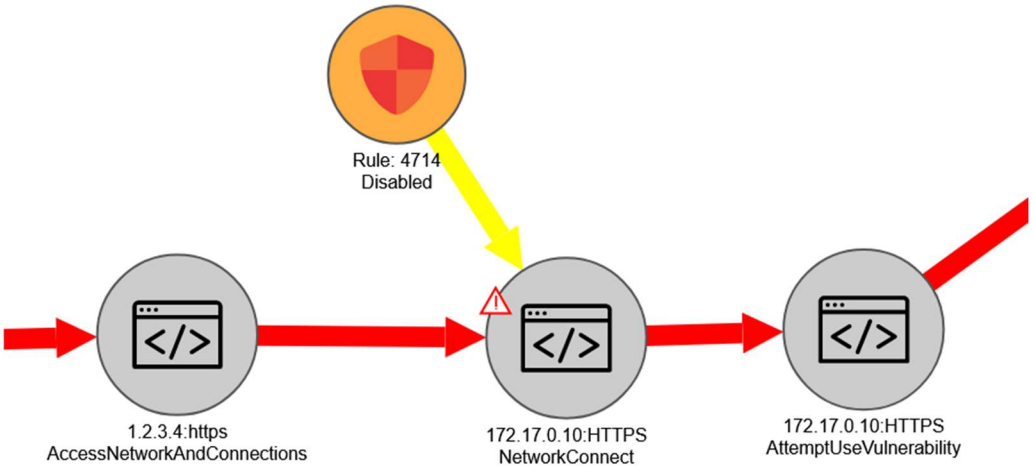
Attack paths. To get more insights of the expected weakest path from the Attacker's starting point to a selected high value asset, we can look at the "critical path" map.

The initial part of the corresponding attack path, i.e., expected path of least resistance, for "Historian01", is as follows.

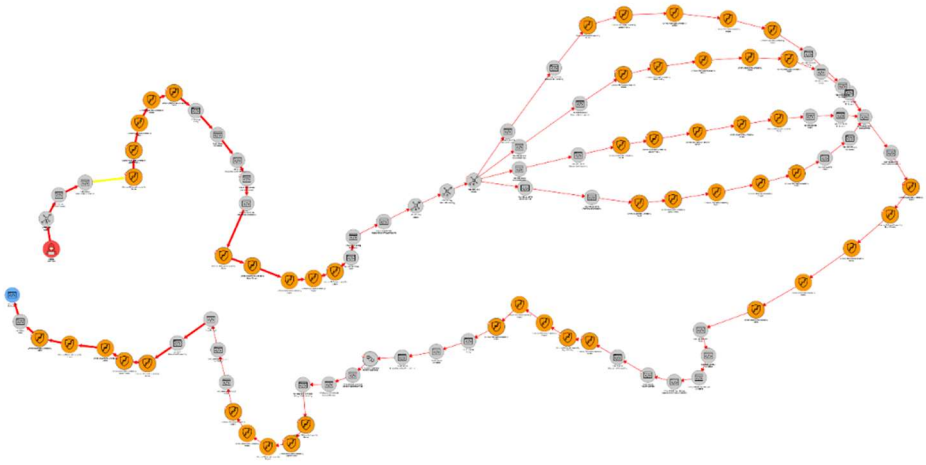


The attacker is connected to Internet where the application responding on the public IP address 1.2.3.4 is present. This application is related to an "UnknownSoftwareVulnerability" which, in lack of actual vulnerability scanner data, is representing the potential presence of a useful software vulnerability. If successfully exploited, it leads to the ability to connect to HTTPS application on the internal 172.17.0.10 host.

Selecting to "show defenses" in the critical/attack path map reveals that firewall rule number 4714 is allowing this connection.



This will in turn lead to additional attack steps (expected attacker achievements) that will with more or less effort in each step, eventually lead to the compromise of the Historian. However, it will require some extensive effort from the attacker to reach all the way to the Historian and thus has a low probability of success. Below is a picture of the complete attack path starting from the red attacker object and reaching to the blue Historian object.



In summary, the attacker would need to discover and make use of seven vulnerabilities, in addition to rule 4714 to reach and gain full access to Historian. Note that these vulnerabilities are “unknown” since we have no data on them (or their presence) collected, but vulnerabilities might be present in these positions in the architecture. (*This shall not be seen as the attacker requiring seven zero-day vulnerabilities, which is not the case.*)

For some areas in the architecture, vulnerability scanner data can be possible to gather and for other areas, it is out of the question (considering that this, in most cases, is a critical infrastructure environment). But for the areas (network zones) where vulnerability scanner data can be collected, such data should be used as an additional data source when generating this kind if models. In that case, that data will replace some of the unknown vulnerabilities with confirmed, actual, vulnerabilities while other systems will be regarded as less likely to have vulnerabilities.

ENERGYSHIELD DEMONSTRATOR

Setup and Configuration. The VA tool is installed alongside the other EnergyShield tools in a stand-alone fashion. In the demonstrator set-up the tools were installed within the same server.

Communication between the tools, like VA, SBA, SIEM and the Dashboard, is carried out via different message queues based on the Kafka application.

The approach is that once a tool has new information to share with other tools or publish on the Dashboard, it posts it in a related Kafka queue. The other tools, who will use the information will then listen to new messages being posted on the relevant queues.

One such example is that the SBA tool posts a message to a queue once a campaign is completed, the VA tool listens to that queue, fetch new campaign-information using the VA tool's APIs, updates the model in the VA tool, runs a simulation and posts the results to

a different Kafka-queue which the Dashboard, in turn, is listening to.

Early Results. The workflow described above has been confirmed to work as expected; A message on "New campaign data available" is posted by the SBA tool, the VA tool picks that notification up, connects to the SBA to fetch the actual findings/data (typically a new value for the SecurityAwareness parameter for the group of users participating in the campaign/survey), updates the information in the model, triggers a simulation and puts a notification message about the updated simulation results on a different queue where the Dashboard is picking it up.

Implementation Process. The implementation is based on using a wrapper application that is subscribing/listening to messages on Kafka-queues. When messages arrive, it uses the SBA APIs to fetch the new campaign data and then use the VA APIs to update a predefined model with the new campaign data and run a simulation. Ince the simulation is complete and new data is available, this information is published on a different queue where the Dashboard application can pick it up.

During the development of the wrapper, the essential sources of information were the API documentation of the SBA tool, the VA tool and the Kafka solution. All these pieces of documentation were found to be good which made the development of the wrapper managing the messages relatively smooth.

BEST PRACTICES & LESSONS LEARNED

Enriching a model with information on users which the SBA tool is providing and combining that information with a model is a very powerful combination since information on "soft" assets are usually more difficult to gather than information on networks, assets, communication, and related security status.

As mentioned briefly above, the simulations run by the VA tool are executed on a model that is representing the environment to be simulated. This model can be created in different ways from fully automated to fully manual. Early in the project the possibility to automatically gather information on a running environment was explored. However, due to confidentiality constraints this turned out not to be an option. Instead, a model based on a provided architecture diagram was created manually. This is also a quite common and realistic approach to modeling an environment, particularly when it comes to critical infrastructure.

In a more production-oriented deployment, however, there are multiple information-collection options available for generating and updating a model.

DISSEMINATION & COMMUNICATION

This whitepaper has previously been published on the foreseeti website (www.foreseeti.com). The paper was also disseminated among foreseeti customers within the energy sector.

ABOUT THE COMPANY

Foreseeti is a leading provider of Cyber Security Posture Management Solutions through Automated Threat Modeling and Attack Simulations. Our flagship products, the securiCAD solutions, empower IT decision makers with insight to the cyber risk exposure and resilience of their IT architectures, uncovering critical paths to high value assets and weak spots in the architecture so that proactive actions can be taken where they really matter. Our solutions are used around the globe by a broad audience, including national and multi-national companies and organizations, bank and finance companies, critical infrastructure operators, defence and military organizations, leading consulting firms, and other companies for whom cyber security is truly important.Contact: sales@foreseeti.com

This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907

Website: www.energy-shield.eu **Twitter**: @EnergyShield_
LinkedIn Group; https://www.linkedin.com/groups/8831159/
Youtube channel: https://www.youtube.com/channel/UCtNRIf0uXvDsxVCSo1NfF_Q
E-mail: EnergyShield@siveco.ro