genua.

A new approach for IT security in production networks

There is an urgent need for action for the IT security in production networks due to the fact that the continued networking of machines and plants through Industry 4.0 and IoT significantly increases security risks. Cyber attacks on the information technology in production environments (operational technology, OT) often succeed because the existing IT security solutions do not offer sufficient protection. This white paper explains how the security in OT networks can be increased with the new security solution, the cognitix Threat Defender.

SecurITy made in Germany

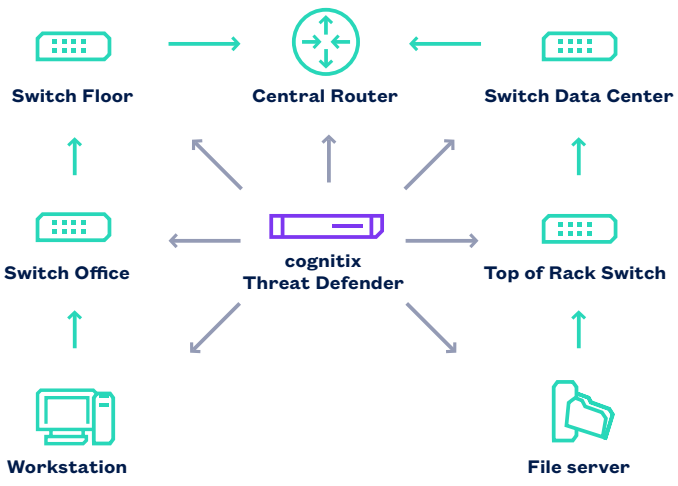
Contents.

1. Current threats for production networks

With Industry 4.0, production networks and services become “smart”: machines and plants, industrial control systems (ICS) and automation solutions are networked online and production networks are made more flexible and more efficient. For data transfer or for remote maintenance access, the previous physical separation of the OT from other IT systems and office networks is eliminated. OT networks, logistics processes or building control systems thereby become more susceptible to attacks from the outside.

The challenge: classic IT security concepts cannot generally be used for OT networks. Many systems run on outdated operating systems. It is frequently not possible to implement security updates or retrofitted hardening measures. Maximum availability and integrity requirements often make it impossible to intervene in running systems. Moreover, the plants – with life cycles of 30 or more years – usually have a low security level. Risks arise not only through the online connections, however. Infected USB sticks, mobile end devices such as the service technician’s laptop or a missing segmentation of the OT network can also result in the infection of plants operated offline through malicious software.

The German Federal Office for Information Security (BSI) warns of a highly dynamic nature in the further development of malicious software and avenues of attack. Nearly 70 percent of businesses and institutions in Germany have already fallen victim to cyber attacks. Yet successful cyber attacks often remain undetected. The attacks are concealed, manipulations are inconspicuous and changes made gradually. The consequences are often dramatic, however. The manipulations destroy plants, and sensitive safety systems are switched off. Every second successful attack has, in the past, resulted in an interruption in production or operation according to the BSI.



The innovative cognitix Threat Defender goes beyond intrusion prevention. With AI, data analytics and threat intelligence capabilities, it builds a second line of defense in the network to complement firewall solutions that control and secure data traffic at the interfaces.

2. How can OT networks be protected?

Effective protection for the confidentiality, integrity and availability of OT networks is achieved from the interplay of rules, processes, measures and tools as defined in, among other places, an information security management system (ISMS acc. to ISO/IEC 27000) and the standard for "Industrial communication networks – IT security for networks and systems" (IEC 62443).

2.1 Defense-in-depth principle (IEC 62443)

A defense-in-depth principle is anchored in standard IEC 62443. It defines the protection against cyber attacks in multiple layers (as with an onion). Even if one layer of security is defeated, only part of the network is affected. The complete system is further protected by additional layers of security. It is therefore useful to divide the network areas into different security zones and to assign tiered levels of protection.

2.2 Security zones, zone transitions and protection level

A necessary measure, therefore, is that different security zones be defined and that these zones be partitioned from one another. The zone transitions and the communication between the zones can be restrictively regulated through firewalls and appropriate filter rules. It is thereby possible to set up secured "air-locked" PCs, e.g., to enable the use of USB sticks.

Data diodes can be used for zones with an especially high protection level. A data diode only permits one-way data transfer. The flow of information is blocked in the opposite direction. Behind these data diodes, machines, plants and IT systems can be protected so that data can be set from the plant to the control station or via public networks to the manufacturer's service center without endangering its integrity.

2.3 Safeguarding remote maintenance

Secure remote maintenance solutions permit access to only one security zone. This can be implemented with a so-called rendezvous server that is installed in the demilitarized zone (DMZ) in addition to the firewall. Through this neutral intermediate layer, a direct connection to the Internet is rendered impossible. Both the maintenance service as well as the machine operator establish encrypted connections at the agreed-upon time here. Only once the rendezvous has been established on the server in the DMZ is the direct maintenance connection made to the machine that requires support.

2.4 Monitoring network communication (IDS/IPS)

As attack scenarios and techniques become more and more refined, cyber attacks are being more effectively concealed in the data stream of, e.g., HTTP, HTTPS, POP3 or IMAP. The communication is largely encrypted and difficult to check. An attack and the activity of malicious software are, therefore, not always easy to recognize at first glance. Harmful programs are thereby able to find a path into the OT network in spite of firewall and virus scanner.

The monitoring of OT networks is an additional protective measure here for keeping an eye on plant communication and checking for vulnerabilities. Intrusion detection systems (IDS) and intrusion

prevention systems (IPS) have become established for this purpose. They have been used in office networks for many years already.

IDS systems analyze the data stream in the OT network and alarm the administrator in the event of suspicious behavior. The IDS searches for patterns in the data stream of a communication connection here. Any possible malicious software is detected with the help of signatures that must, however, be continuously updated in order to detect new types of attack.

IPS systems analyze the data stream and also protect against attack by immediately interrupting communication in the event of suspicious behavior. IPS systems were unable to become established in OT networks, however. They have a relatively high risk of failure if the signatures result in, e.g., false positives and the IPS system then interrupts the plant communication. What can, under certain circumstances, be tolerated in office networks, is, on the other hand, not acceptable in OT systems.den kann, ist bei OT-Anlagen dagegen inakzeptabel.

2.5 New requirements on security technology

The cyber security recommendation of the BSI (BSI-CS 134) places special emphasis on anomaly detection as a means for protecting networks: “It enables the detection of atypical behavior and, thus, in addition to technical error states and incorrect configuration, the detection of previously unknown forms of attack on such networks. This distinguishes anomaly detection from other measures that are based on the detection of already-known attacks.”

The requirement for anomaly detection is also included in the draft for “IT Security Act 2.0” (IT-SiG 2.0). Based on this, the operators of critical infrastructures will, for the first time, be required to use systems for “attack detection.” “These systems represent an effective measure for countering cyber attacks.” (IT-SiG 2.0 from March 27, 2019).

3. Security holes in OT networks

A key disadvantage of IDS and IPS systems is that they are limited to anomalies in the data stream. If, for example, a given network component sends a control signal to a centrifuge, this is nothing unusual in the data stream itself and is, therefore, not detected. The IDS system does not check whether this network component is authorized to send such a signal. It also does not check whether this behavior is unusual for this network component. As a result, attackers can take over devices and plant components in the network without it being immediately noticed.

4. Monitoring the behavior of the network components

The cognitix Threat Defender closes the security gap of IDS and IPS systems. It monitors all network traffic and also analyzes the behavior of the network components (assets). The cognitix Threat Defender sets up a monitored, secure network by recognizing the behavior patterns of the network devices and assigning defined rules. Functions that were previously separate, such as network analysis, intrusion detection, asset tracking and a dynamic policy engine, are merged into a single system here.

4.1 Passive monitoring

The cognitix Threat Defender supports passive monitoring of the network communication so as not to interfere with OT networks. The data stream is monitored and analyzed. Focus here is not on an individual device or an individual network connection but rather on the communication in the entire network and the behavior of all network participants.

4.2 Asset tracking with real-time analysis

Through asset tracking with real-time analysis, an asset database of all devices in the network is created and a network status in the “base state” established. This serves to determine which devices are in the network and what network traffic takes place in this base state. This is performed by recording the network traffic. By establishing the initial condition of the network, general vulnerabilities and security holes are also identified that are caused by, e.g., configuration errors, network problems, unknown or unauthorized network elements, intentional or unintentional misbehavior, other “black marks” or even attacks in the network.

4.3 Threat intelligence database

The cognitix Threat Defender also uses the international MISP database for the automatic exchange of threat information (Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing). Stored in the database are technical and non-technical information on examples of malicious software, incidents, attackers, dangerous websites, known command and control servers (C&C) and other information. MISP is used worldwide by more than 6000 organizations. This information is utilized in the cognitix Threat Defender as additional context and helps in assessing the risk in the network.

4.4 Automated anomaly detection

The cognitix Threat Defender analyzes the network traffic according to IP and MAC addresses, ports, protocols and applications of OSI layers 2 to 7. The traffic is checked here for problematic addresses, domains or file signatures. Based on the asset database, the communication relationships of the devices are also examined. Behavior rules are assigned to the devices and these rules monitored.

With the automatic detection of the network traffic, patterns that are unusual and that deviate from the typical standard behavior (anomalies) in the data stream are identified, thereby allowing attacks on the security to be averted early on.

Examples for anomalies in the network:

A workstation that previously only had connections with the login server and file server suddenly begins to communicate with other computers within the network. In this case, undesired file sharing by the work station is detected (shadow IT).

During monitoring, a physical device is detected in the network that should not be present. This may be, e.g., a service technician who is communicating across security zones without permission. A printer contacts other devices in the network and attempts to download code from the network, an indication of malicious software.

There are other examples that also correspond to the behavior of malicious software. For example, if a work station establishes connections to many ports in a short amount of time (network scan) or if a pump control suddenly behaves like a human machine interface (HMI) and sends control signals to other components in the plant.

Such a changed communication behavior of the network components is detected neither by a firewall nor by an IDS system. Here, the cognitix Threat Defender closes a security hole.

4.5 Real-time reporting with alarm messages

The cognitix Threat Defender provides the administrator with real-time reporting using a traffic-light system. It provides messages about possible dangers and attacks. Here, the admin can set the minimum alarm message level he would like to be informed of (1 High, 2 Medium, 3 Low, 4 Notice). Alarms can be sent via e-mail, desktop notification or web systems or integrated in an existing alarm system (SIEM).

5. Best practice: anomaly detection in five steps

For the safeguarding of large OT networks, genua recommends taking an incremental approach. Five phases have proven effective in practice.

Phase 1 – Catalog assets

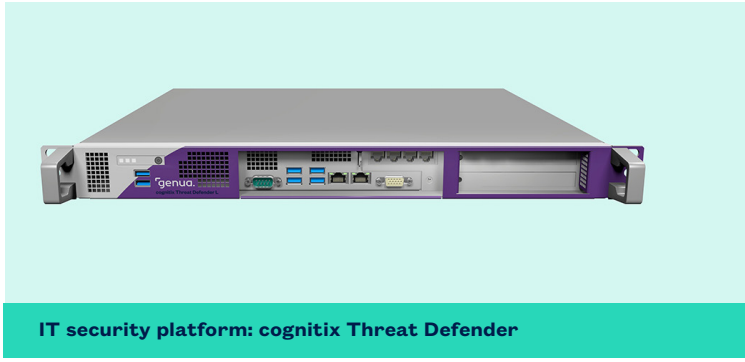
In the first phase, the communication partners within the OT network are determined. The network traffic is mirrored in the cognitix Threat Defender and all active devices in the observed network area recorded in an asset database. During this process, metadata, such as the used operating system, is identified for the devices. Recording is strictly passive based on the observed network traffic.

During this phase, misconfigurations, network problems, outdated device software or forbidden devices are detected after just a few hours. A faulty configuration of an active directory synchronization, for example, can thereby be detected. This can produce constant background traffic that results in no noticeable restriction. Nevertheless, it may indicate an error because the correct configuration of an AD only requires synchronization of changes if changes are made to the data and thus produces significantly less network traffic.

5.2 Phase 2 – Identify assets

In the next step, the structure of the network is examined to detect previously unknown devices in the network and to deactivate them if necessary. The security is thereby increased and the awareness for the network improved.

For this purpose, the asset database is manually consolidated. The administrator of the OT network assigns the automatically recorded assets to individual devices or device classes. He uses expressive names here and organizes the assets into domain-specific groups using tags. This manual effort allows communication structures to be simplified and makes it easier to perform the subsequent work for analyzing and monitoring the network.



IT security platform: cognitix Threat Defender

5.3 Phase 3 – Map communication paths

The communication between the devices is then analyzed in order to model the permissible communication in network policy. Undesired communication paths, unnecessary services or undesired protocols, such as multicast, are deactivated.

For this permissible communication, rules are created progressively. This is an iterative process in which more and more new tags and rules are created until a fine-grained network-policy is achieved.

5.4 Phase 4 – Stabilization

The created policy is validated and the network passively monitored. For this purpose, the created model is run passively in the OT network for several weeks. The administrator is informed via e-mail, slack or syslog if a logging rule engages and thereby results in new, as of yet unmapped communication being recorded. It may then be necessary to readjust the policy. It is more likely, however, that the new type of network traffic represents an anomaly that indicates a problem or even a malfunction or an intruder.

5.5 Phase 5 – Active blocking (optional)

The first four phases occur only with the mirrored network traffic. There is, thus, no danger posed by latencies or data loss. Only in the optional fifth phase does active intervention in the network traffic take place in order to prevent undesired communication. Here, the Threat Defender is removed from the mirror port and connected directly to the network switch.

For the active blocking, the rules created in phases 3 and 4 for the explicitly permitted communication are supplemented with rules that block explicitly forbidden and, if necessary, all unknown communication. As the security increases, so too does the risk of interruptions in the OT network, as no unexpected events are now permitted and will be blocked by the Threat Defender.

To reduce this risk, it is also possible to set up cognitix Threat Defender so that it dynamically responds to threats and anomalies with a graduated behavior (“adaptive behavior-based graylisting”). Here, the network traffic defined in phases 3 and 4 is permitted unconditionally. New traffic is permitted and taught-in for 24 hours as “known.” If IDS, threat intelligence or explicit rules for suspicious cases then indicate an event, the network communication taught-in as known can continue to pass through. The new communication is, however, suppressed for a couple hours, a warning output and the communication is not taught-in as being “known.” If other events now occur in this second section or the administrator identifies a problem in the network or in the devices during his analysis, an appropriate response can be taken. Otherwise, after the time has elapsed, the normal mode is restored and new behavior is again taught-in as “known.” It is thereby possible to respond to new and potentially dangerous communication without impeding the existing communication and, thus, the running processes.

“A very important benefit of the cognitix Threat Defender is the gain in transparency of one’s own network. The ability to then respond appropriately to visible threats is the big bonus after having acquired an overview of the network.”

Arnold Krille, Head of department
Product Development coginitx Threat Defender

6. Summary: anomaly detection in an OT network

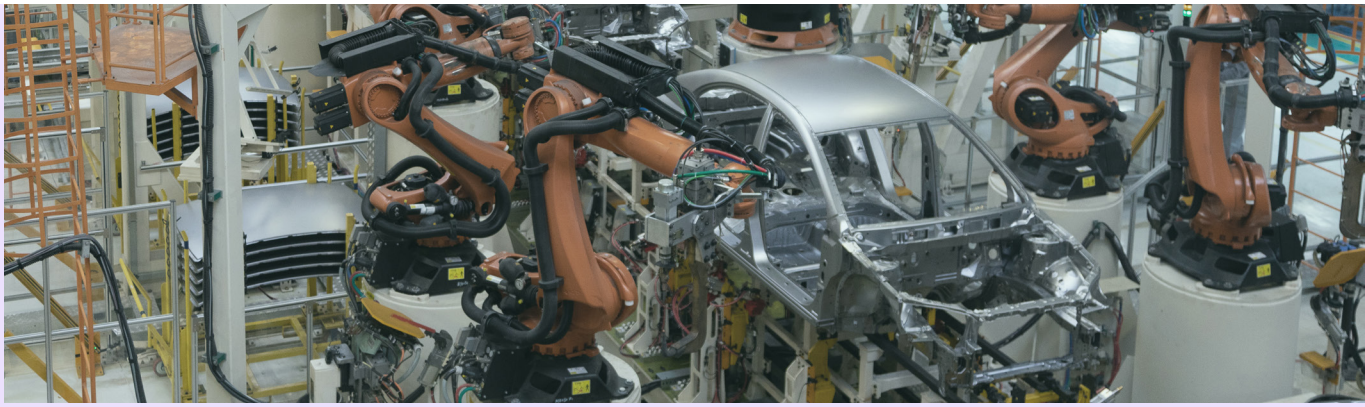
With Industry 4.0, the previous physical separation of the OT from other IT systems and office networks is eliminated. OT networks, logistics processes or other building control systems are thereby more susceptible to attacks from the outside. At the same time, cyber attacks are becoming more effective and more difficult to identify due to the increasingly refined attack scenarios and attack techniques. As a result, malicious software can find a way into the OT network in spite of firewall and virus scanner.

Effective protection for the confidentiality, integrity and availability of OT networks is achieved through the interplay of rules, processes, measures and tools (cf. ISMS acc. to ISO/IEC 27000 and IEC 62443). The cyber security recommendation of the BSI (BSI-CS 134) and the draft of “IT Security Act 2.0” (IT-SiG 2.0) emphasize anomaly detection as a means for protecting networks. The intrusion detection systems (IDS) and intrusion prevention systems (IPS) used for this purpose are, however, limited to the detection of anomalies in the data stream. The systems do not check whether a network component is authorized to send signals. Nor do they check whether this behavior is unusual for this network component. As a result, attackers can take over devices and plant components in the network without it being immediately noticed.

The cognitix Threat Defender closes the security gap of IDS and IPS systems. It monitors all network traffic and also analyzes the behavior of the network components (assets). It sets up a monitored, secure network by recognizing the behavior patterns of the network devices and assigning defined rules. It supports passive monitoring of the network communication so as not to disturb OT networks.

When safeguarding large OT networks, genua recommends taking an incremental approach. Five phases have proven effective in practice (1 – Categorize assets, 2 – Identify assets, 3 – Map communication paths, 4 – Stabilization and (optional) 5 – Active blocking).

The cognitix Threat Defender monitors and analyzes the data stream in an automated process. Focus here is not on an individual device or an individual network connection, but rather on the communication in the entire network and the behavior of all network participants. The previously separated functions such as network analysis, intrusion detection, asset tracking and a dynamic policy engine are merged into a single system.



Further information:

www.genua.eu/threat-defender

https://youtu.be/RA9BVAUwM7s

About genua

genua is a German specialist for IT security with many years of experience in the industrial sector. Our range of services spans from the safeguarding of sensitive interfaces and networks to the connection of highly critical infrastructures, encrypted data communication via the internet, remote maintenance systems as well as remote access solutions for mobile employees. Our solutions are developed and produced in Germany. Many mediumsized and large enterprises rely on our solutions to protect their IT. genua is a company of the Bundesdruckerei Group.

genua GmbH, Domagkstrasse 7, 85551 Kirchheim, Germany
T +49 89 991950-0, info@genua.eu, www.genua.eu