Greinfort Technical Data Sheet.

Greinfort

OBSERVE | UNDERSTAND | PREDICT



Date: 02/2025
Document reference: Greinfort Technical Data Sheet
Version: 1.0

This document has been prepared by **Greinfort** for the exclusive use of **Greinfort.** Its contents are confidential and may not be disclosed to third parties or used for any purpose other than that for which it was provided without the prior written consent of **Greinfort.** If this document is delivered under a contract, its use and distribution shall be limited to the terms and conditions expressly authorized therein. **Greinfort** shall not be held liable for any errors or omissions that may exist in this document.

Contents

1. Document content. 4
1.1. Content scope. 4
1.2. Greinfort service. 4
2. Product description. 4
2.1. Introduction. 4
2.2. Benefits. 5
2.3. Use cases. 6
2.4. Differentiators. 7

1. Document content.

1.1. Content scope.

This document is a product description that contains the main features, use cases, benefits, and differentiators of the Greinfort service for monitoring OT infrastructure.

1.2. Greinfort service.

Greinfort is a technology focused on providing real-time monitoring for organizations with OT infrastructure.

It uses advanced technologies based on in-house R&D to perform, among other functions, asset inventory, anomaly detection through various strategies, vulnerability management, and traffic analysis.

This helps prevent and mitigate cybersecurity threats, securing digital infrastructure, sensitive data, and communications. It also plays a key role in compliance with certain security standards and regulations (ISO 27001, NIS2, etc.).

2. Product description.

2.1. Introduction.

In today's industrial sector, cybersecurity is a crucial issue. Threats are increasingly sophisticated, and classic perimeter monitoring is no longer sufficient. Due to the paradigm shift toward hyperconnectivity brought by Industry 4.0 and beyond, the boundaries between the internet, IT zone, and OT zone blur, creating new risks.
This, combined with the demand for production protection and regulatory pressure from public administrations and regulators, makes it increasingly necessary to have OT cybersecurity solutions that provide comprehensive responses, such as Greinfort.

Greinfort technology enables visibility of network assets, detects anomalies based on network traffic, checks statistics or behavioral patterns, discovers vulnerabilities to mitigate, and blocks malicious connections.
The deployment is fully flexible, and it can be installed on-premises or in the cloud, using hardware sensors owned by the client or provider, or even fully virtualized.
All this ensures plant managers can rest easy.

2.2. Benefits.

The benefits of the Greinfort service are based on the following features and capabilities:

- Monitoring and reporting service: real-time monitoring of cybersecurity status in the factory, with periodic reports on risks, alerts, and detected vulnerabilities.
- Focus: specialized in OT, not an adapted IT solution. It becomes the “logical Greinfort” of factories, complementing physical surveillance already in place.
- Market: aimed at both large companies and SMEs, democratizing its use, as well as any sector with industrialized processes. Thus, it is a highly scalable solution.
- Price and customization: aware that security investments are costly, as commercial solutions are usually expensive, and open-source ones often require specialized technical staff and carry risks like vulnerabilities due to lack of maintenance or project abandonment. The offering is modular, based on additional service bundles contracted with Greinfort and/or subcomponents of the monitoring solution, providing great flexibility.
- Ease of use: simple interface (desktop and mobile versions) adapted to non-technical factory personnel, avoiding complex consoles overloaded with information.
- Role-based permissions: defines capabilities assigned to each company operator interacting with Greinfort.
- Multi-probe/multi-site: natively aggregates traffic sources from different probes, whether at the same plant or geographically dispersed, so all can be monitored and managed from the same user interface.
- Non-intrusiveness: non-intrusive solution that offers security without interfering with plant operation. Most detection capabilities are passive inference techniques, with very low-impact active scanning, which is optional.
- Standardization: supports widely used OT communication protocols, including Modbus TCP/IP, BACnet, Profinet, Siemens communication, OPC UA, Ethernet/IP, DNP3, Ethernet POWERLINK, EtherCAT, and Ether-S-Bus.
- Technology: integration with AI module for cyberattack prevention.
- Alerts: vulnerability analysis linked to NIST’s NVD, threat detection through known signatures or patterns, IDS, AI/ML algorithms analyzing session summaries or packet payloads, honeypots or decoys.
- Proactive communications: alerts can be scheduled to be sent to operators based on specific configurations.
- Remote analysis: capability to analyze the state of an industrial plant remotely through lab analysis of traffic provided by the client in a pcap file, without deploying the solution onsite.
- Integration: supports third-party vulnerability databases and high event volumes.
- Third-party integration: Greinfort can send active alerts to third-party systems such as SIEMs (Security Information and Event Management) for ingestion and correlation with other log sources using the syslog protocol.

- Scalability: service can grow easily by adding more probes to the monitoring solution.
- API interaction: allows simple customization of integrations for special client needs.

2.3. Use cases.

Some use cases related to the solution's capabilities include:

- Asset inventory: fully automatic detection of devices on the network and their communications, both internally and externally. Often discovers devices or routes unknown to the client. Lists all assets, allows tagging and property assignment, and enables custom columns for an online, tailored inventory.
- Wireless device detection: especially useful in critical infrastructures or environments where mobile terminals are banned by security policy. Inventories and controls all WiFi and Bluetooth devices near the probe.
- Network map: draws a real-time network diagram of the industrial plant (or subnets), showing topology and regulatory compliance. Helps visually detect segmentation problems violating best practices of PURDUE and ISA/IEC 62443 models to properly segregate zones and conduits.
- Anomaly detection: generates real-time, fully automated anomalies based on different protection strategies:
    - Static rules (new connections, devices, port or protocol changes, fingerprinting, man-in-the-middle...).
    - Intrusion detection system.
    - AI/Machine learning algorithms analyzing network traffic.

These anomalies generate alerts that can be managed throughout their lifecycle via the interface, proactive notifications, or third-party systems like SIEM.

- Vulnerabilities: identifies vulnerabilities associated with services deployed on network devices for proper management (patching, physical or virtual) to prevent exploitation.
- UEBA (User and Entity Behavior Analytics): special anomaly use case based on process variables. Process mining techniques detect irregularities affecting cybersecurity or even physical safety of employees or customers (due to manipulation of production processes).
- Honeypot: special anomaly detection case via decoy systems. Detects threats and provides detailed information on attacker techniques.
- Traffic blocking: ability to block malicious connections from the industrial network to the outside via integration with the client's firewall. Fully optional and policy-configurable (informative, semi-supervised, or automatic). Automatically mitigates external threats.

- Traffic analysis: traceability of communications between internal network devices or with external IPs, useful for forensic analysis and proper network segmentation.
- Service reports: automated periodic reports with relevant service information to facilitate information processing. Reports include vulnerabilities, unauthorized devices, scoring levels, connections to external IPs, etc.
- Regulatory compliance: all previously described identification, protection, detection, and response capabilities support the implementation of security measures imposed by national and international security standards and regulations, such as ISO27001, ENS, ISA/IEC 62443, NIST CSF, NIS2, etc..

2.4. Differentiators.

There are other solutions on the market with capabilities similar to Greinfort. The differentiating aspects are:

- Simplicity: Greinfort is a simple, intuitive, and easy-to-use tool. Years of cybersecurity product experience show that this is key to success, as users don’t need to be experts to manage factory security, and no payment is required for superfluous features.
- No need for outsourcing: the technology is so easy to handle that outsourcing management is a business decision, not a technical competence requirement.
- Flexibility: offered in different modalities to adapt to client needs.
- Affordable: aims to democratize access to this technology, originally only affordable by large companies or multinationals due to high cost, so it can be contracted even by SMEs with high-value industrial production processes.
- Customizable: customer feedback drives many capabilities and service improvements.
- National sovereignty: due to the current turbulent geopolitical landscape, many organizations and public administrations discourage the use of foreign solutions (USA, Israel, Russia, etc.). Our solution is 100% made in the EU (Galicia, Spain), both in R&D and manufacturer support.

Greinfort

Greinfort Solutions S.L
Maria Berdiales 20, 4th fl.
36203 | Vigo | Spain
(+34) 886 251 058
info@greinfort.com
greinfort.com