DATASHEET

Group-IB Threat Hunting Framework / Sensor Industrial

Group-IB Threat Hunting Framework / Sensor Industrial

Threat Hunting Framework — adversary-centric detection of targeted attacks and unknown threats. Proactive local and global threat hunting. Proprietary patented technologies.

Information security functions covered by THF

- Protects corporate emails from targeted phishing and letters containing malware
- Protects the network perimeter, services, and user workstations from ransomware, Trojans, viruses, keyloggers, and spyware, including those distributed outside of controlled network streams
- Protects infrastructure from being controlled by external attackers
- Secures the transfer of files from untrusted to trusted file storages
- Performs malware analysis
- Uses API to protect the customer's system against malware
- Protects workstations and servers from potentially unwanted apps and untrustworthy devices
- Collects forensic data for investigations
- Preforms threat hunting
- Performs remote incident response
- Identifies and investigates attacker infrastructure in anticipation of new attacks
- Recreates the full attack timeline
- Controls artifacts transferred through encrypted traffic
- Controls encrypted network traffic
- Protects technological networks from illegitimate devices for data transfers
- Protects technological networks from PLC modifications
- Protects technological networks from manipulations of the technical functions of network protocols
- Protects technological networks from the destruction of equipment

The complete Threat Hunting Framework includes follow modules

Huntbox

Manages detection infrastructure; performs automated analysis, event correlation, and threat hunting.

Sensor

Analyzes network traffic and detects threats on the network level. Integrations with the company's subsystems.

Sensor Industrial

Analyzes industrial network protocols to ensure protection against targeted attacks on technological networks and monitors the integrity of the industrial control system.

Polygon

Detonates malware (in the form of email attachments, files, and content links) in an isolated environment to perform behavioral analysis

Huntpoint

Protects workstations by checking for and collecting forensically relevant data.

Decryptor

Decrypts TLS/SSL traffic in the protected infrastructure.

CERT-GIB

Managed security service for Group-IB solutions by cybersecurity and malware analysts. CERT-GIB is authorized by Carnegie Mellon University and is a member of FIRST, Trusted Introducer, and IMPACT.

Sensor Industrial

Sensor Industrial is a Group-IB Threat Hunting Framework module designed to detect attacks on a company's technological segment at an early stage. By analyzing data packages of the technological traffic with its own signatures and behavioral rules, Sensor Industrial detects transfers of adversary control commands between the ICS levels. As such, it detects the use of ICS service commands for the purposes of modifying PLC firmware, substituting control programs, and interrupting technological processes.

Technical approach

1	**Machine learning to detect:**	• Lateral movement from the corporate network • Anomalies in application protocols	• Changes in the ICS network equipment • Changes in the ICS network sessions
2	**Passive control of technological equipment software integrity**		
3	**Control of commands sent to technological equipment:**	• Connection to technological equipment • Modification/downloading/ loading of control programs • Halting technological processes	
4	**Preventing attacks from the corporate segment:**	• Blocking targeted email campaigns* (Sensor + Polygon required for inline mode) • Blocking malware downloads from the Internet* (Requires ICAP integration with web proxy)	• Removing malware from file storage* (requires Polygon) • Blocking attacks at end host level* (requires Huntpoint)
5	**Support of open and proprietary equipment manufacturer protocol analysis**		
6	**Integration with analytical systems:**	• SysLog integration with SIEM systems • SNMP integration with status monitoring systems	
7	**Supported analysis protocols**	• Network protocols: (DNS, FTP, HTTP, RDP, SMB, SMTP, SSH, POP3, etc.) • Open (documented) industrial protocols: CIP, DNP3, IEC 60870-5-104, IEC 61850-MMS, Modbus TCP, OPC-DA, OPC-UA, MQTT	• Proprietary protocols of ICS equipment manufacturers: Siemens, Schneider Electric, Rockwell Automation, Emerson

Centralized management

Huntbox provides a graphical interface to manage THF modules installed in the protected infrastructure. It also provides a single storage location for data relating to all incidents. The solution performs advanced searches in the entire database of past events and alerts and provides the following functions:

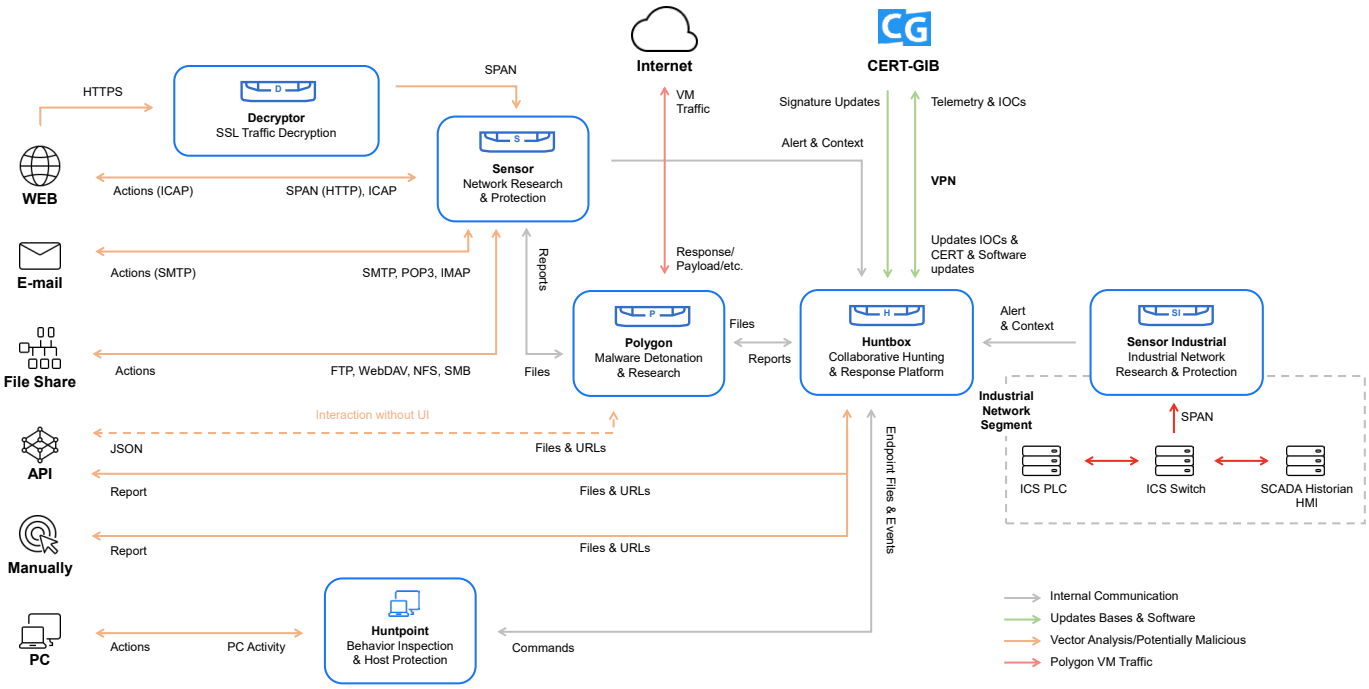
1. Threat Hunting
2. Incident response
3. Event correlation
4. Remote forensics

Deployment options:

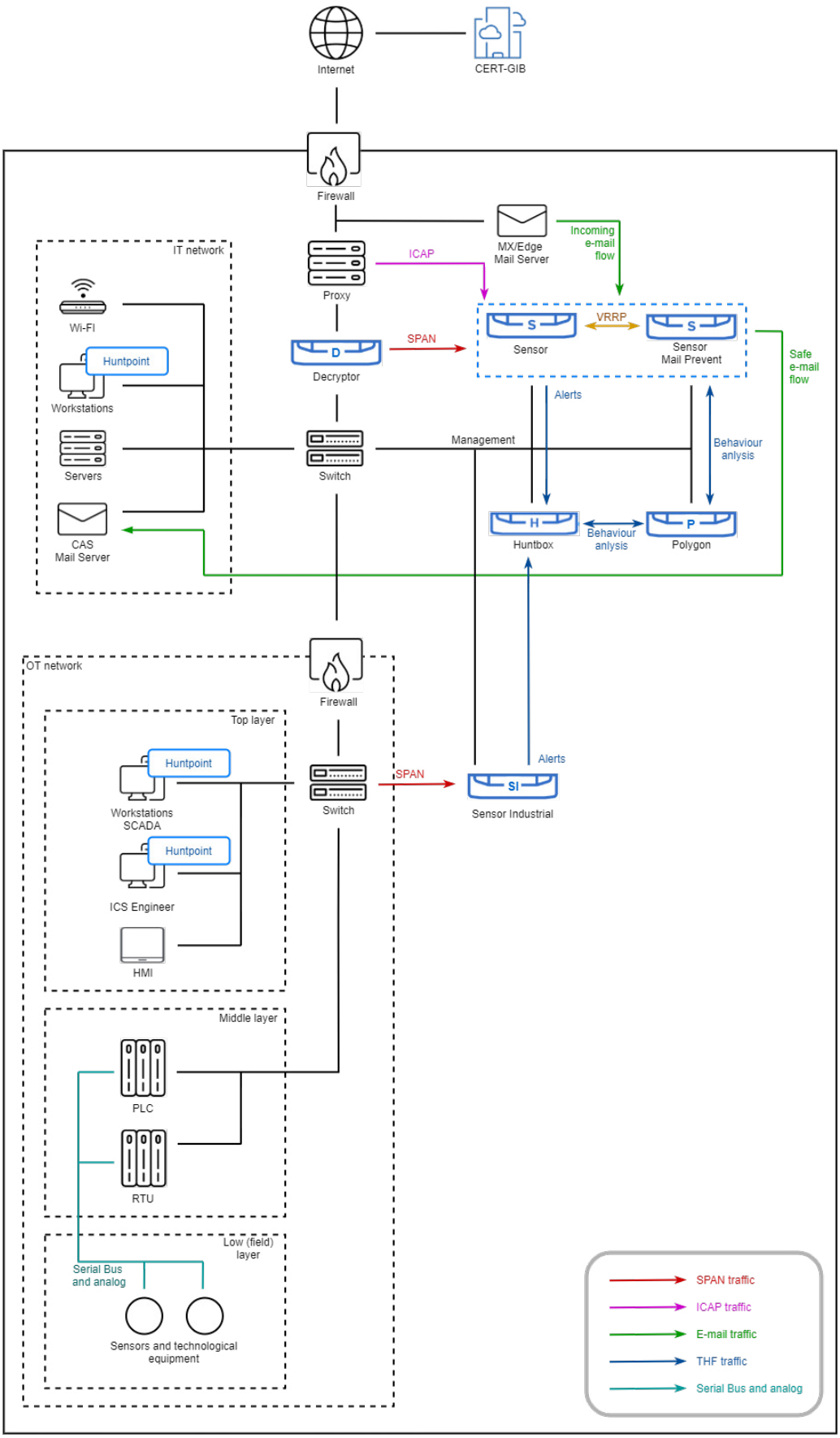
There are three supply options:

- Software
- Hardware
- Virtual

Architecture of Threat Hunting Framework



Integration scheme



	Sensor Industrial-1000		Sensor Industrial-5000	Sensor Industrial-10000
	1GbE RJ45	10GbE SFP+ & 1GbE RJ45		
Peak network loading for analyzed mirrored traffic (SPAN), Mbit/s	1000		5000	10000
Network interfaces for mirrored traffic (SPAN) monitoring	4x 1000BASE-T	2x 10GBASE-SR/LR 4x 1000BASE-T	2x 10GBASE-SR/LR 4x 10GBASE-T	4x 10GBASE-SR/LR 3x 10GBASE-T
Network interfaces for management (LAN)	2x 1000BASE-T	2x 1000BASE-T	2x 1000BASE-T	1x 10GBASE-T
IPMI (back panel)	1x 1000BASE-T			
Form factor	1U			
AC power supply, Watts	1x 450	2x 550	2x 750	2x 750
Maximum power consumption, Watts	400	450	705	705
Maximum heat dissipation, BTU/h	1x 1500	2x 2000	2x 2500	2x 2500
Approximate weight of an appliance, kg	13	14	22	22
Standard operating temperature	0° C to +35° C (+50° F to +95° F) with no direct sunlight on the equipment			
Operating relative humidity	0% to 80% relative humidity with +29°C (+84.2°F) maximum dew point			
Compliance with standards	• ISO 14001, • RoHS, • REACH 1907/2006, • ErP Directive 2009/125/EC			

Minimum technical requirements for THF Sensor Virtual (Sensor-250):

calculated for peak network loading of 250 Mbit/s on interfaces for mirrored traffic (SPAN) monitoring

CPU	1 unit with 16 cores	**Storage subsystem**	480GB
RAM	32GB	**Network interfaces**	at least 2: one for management (LAN) and, at least, one for capturing mirrored (SPAN) traffic

Contact us to test Threat Hunting Framework

thf@group-ib.com

Get to know us

group-ib.com
info@group-ib.com
twitter.com/GroupIB_GIB

Learn more about Threat Hunting Framework