DATASHEET

Group-IB Threat Hunting Framework / Huntbox

Group-IB Threat Hunting Framework / Huntbox

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.

Huntbox

Huntbox is a platform that provides a set of tools for monitoring, incident response, and threat detection within protected infrastructure and on the Internet.

Technical approach

1 **Automatic event, alert and incident attribution to the adversary groups involved and the malware used in the attack**

2 **Graph analysis: technology for monitoring adversary infrastructure**

3 **Threat hunting: searching and checking for possible cases of network compromise based on raw traffic and end host data (requires Huntpoint and/or Sensor)**

4 **Management of the Threat Hunting Framework modules**

5 **Manual or automatic blocking of malware and end host activity* (requires Huntpoint)**

6 **Information security incident monitoring tools:**

- Accumulation and storage of all information security events detected by modules
- Correlation of multiple events into a single record according to the target
- Correlation of multipurpose and multi-vector attacks into a single incident

7 **Adjustable THF analyst notifications about the solution status**

8 **Integration with analytical systems:**

- SysLog integration with SIEM systems
- SNMP integration with status monitoring systems

9 **Integration with IS event orchestration systems and incident management platforms via API to provide malware detonation reports* (requires Polygon)**

10 **Integration with systems for IS event collection and correlation from various sources via API to obtain and share the full context relating to the incidents identified**

Centralized management

Different updates and Threat Intelligence feed options

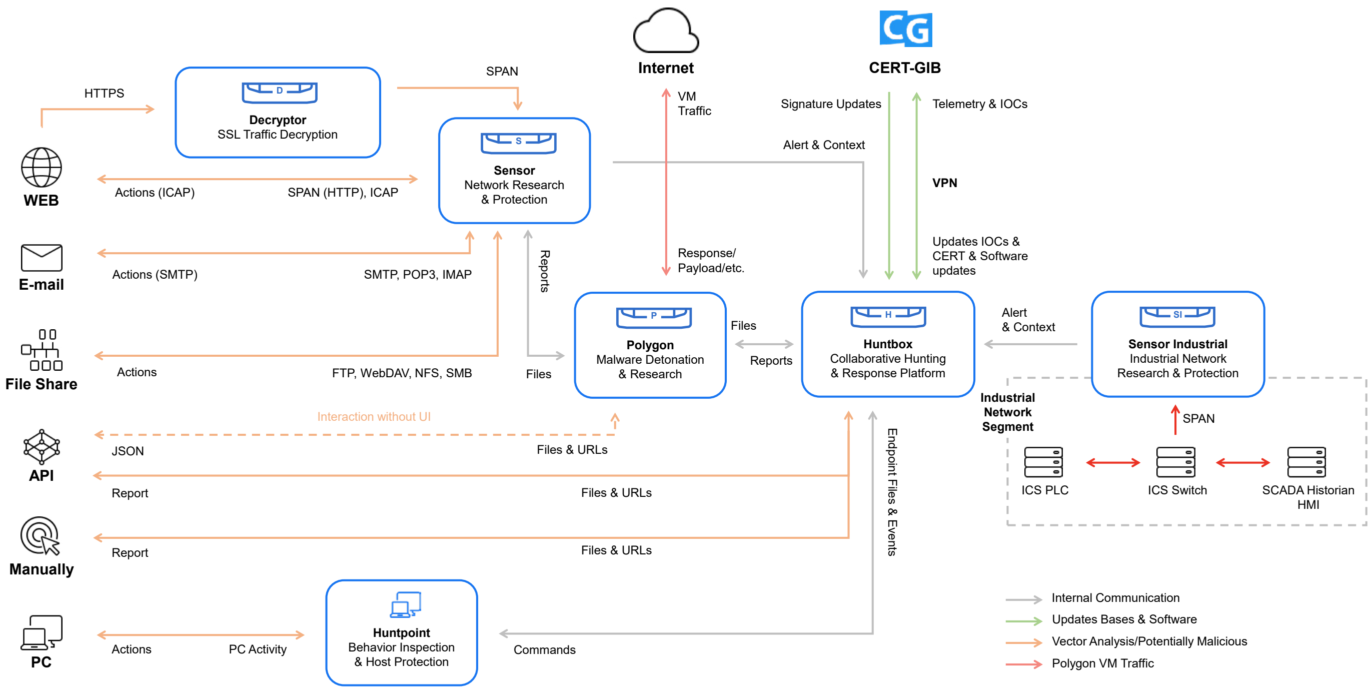
1. Full isolation without software and rule updates
2. One-way software, rule and IoC updates initiated by Huntbox
3. Updates initiated by Group-IB, heartbeats monitored by Group IB, and functionality to detect perpetrators' infrastructure
4. Monitoring and support services from CERT-GIB 24/7; the Intelligence feed works two-ways

Deployment options:

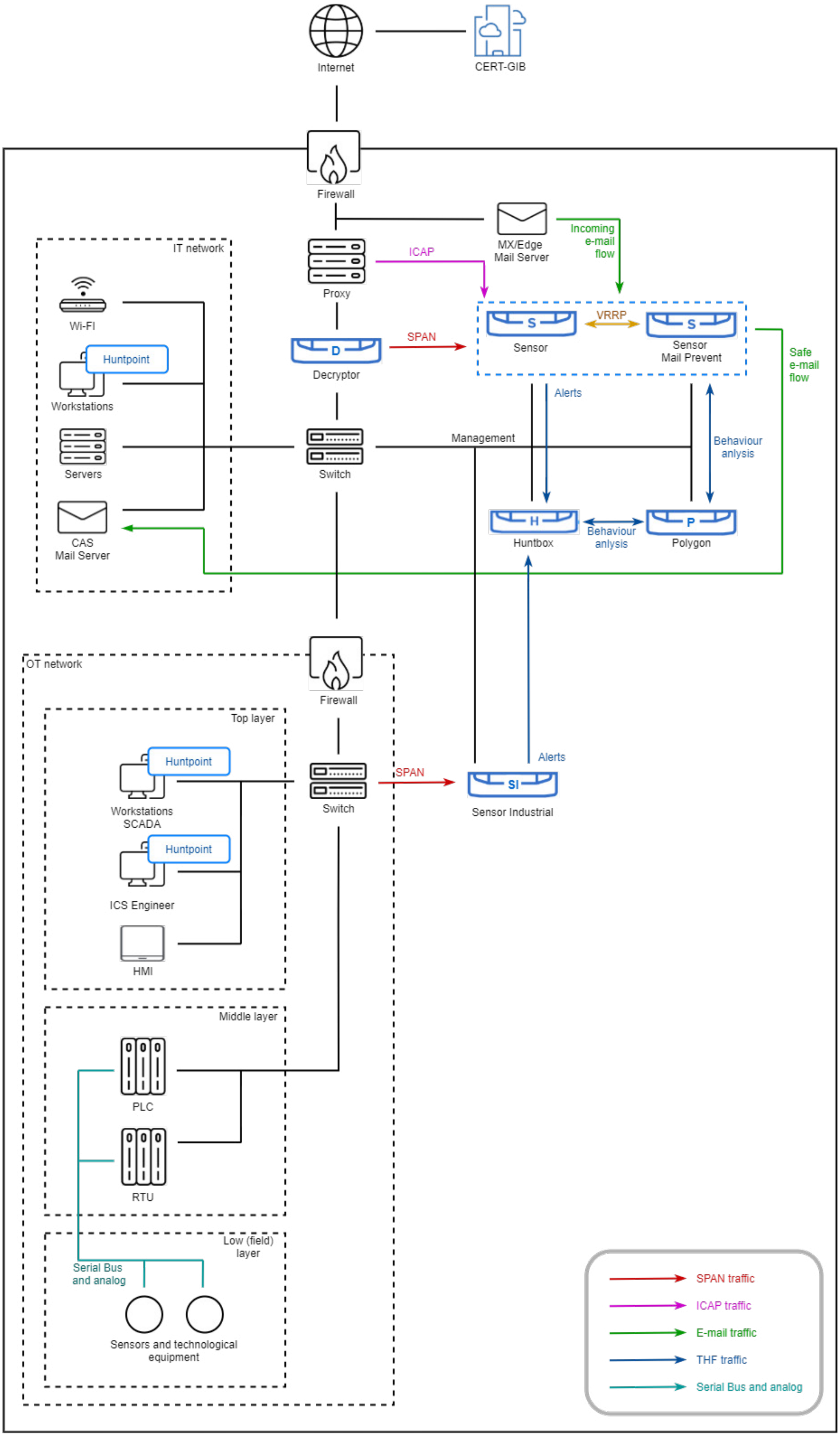
There are three Huntbox supply options: SW/HW/Cloud. Depending on requirements, Huntbox can be deployed in the following ways:

- **on-prem (SW/HW/Cloud)** – an isolated solution, in which all data are stored within the customer's perimeter
- **on-cloud** – Huntbox deployment in Group-IB's infrastructure, which helps promptly increase capacity levels and carry out monitoring, investigation, and response

Architecture of Threat Hunting Framework



Integration scheme



	Huntbox Standard	Huntbox Enterprise	Storage
Number of Huntpoint agents connected, units	up to 1000	up to 2000	up to 2000 (for 1 Storage appliance); larger installations with more than 2000 (custom configurations: in addition to main Huntbox Standard/ Enterprise appliances)
Network interfaces for management (LAN)	4x 1000BASE-T		
IPMI (back panel)	1x 1000BASE-T		
Form factor	1U		
AC power supply, Watts	2x 750	2x 750	2x 550
Maximum power consumption, Watts	705	705	450
Maximum heat dissipation, BTU/h	2x 2500	2x 2500	2x 2000
Approximate weight of an appliance, kg	22	24	14
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		

→

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