DATASHEET

Group-IB Threat Hunting Framework / Huntpoint

Group-IB Threat Hunting Framework / Huntpoint

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, iles, 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.

Huntpoint

Huntpoint is a Group-IB Threat Hunting Framework module that provides end host control and protection against targeted attacks. It is also used to collect additional contextual information and detect malicious activity on the host.

Technical approach

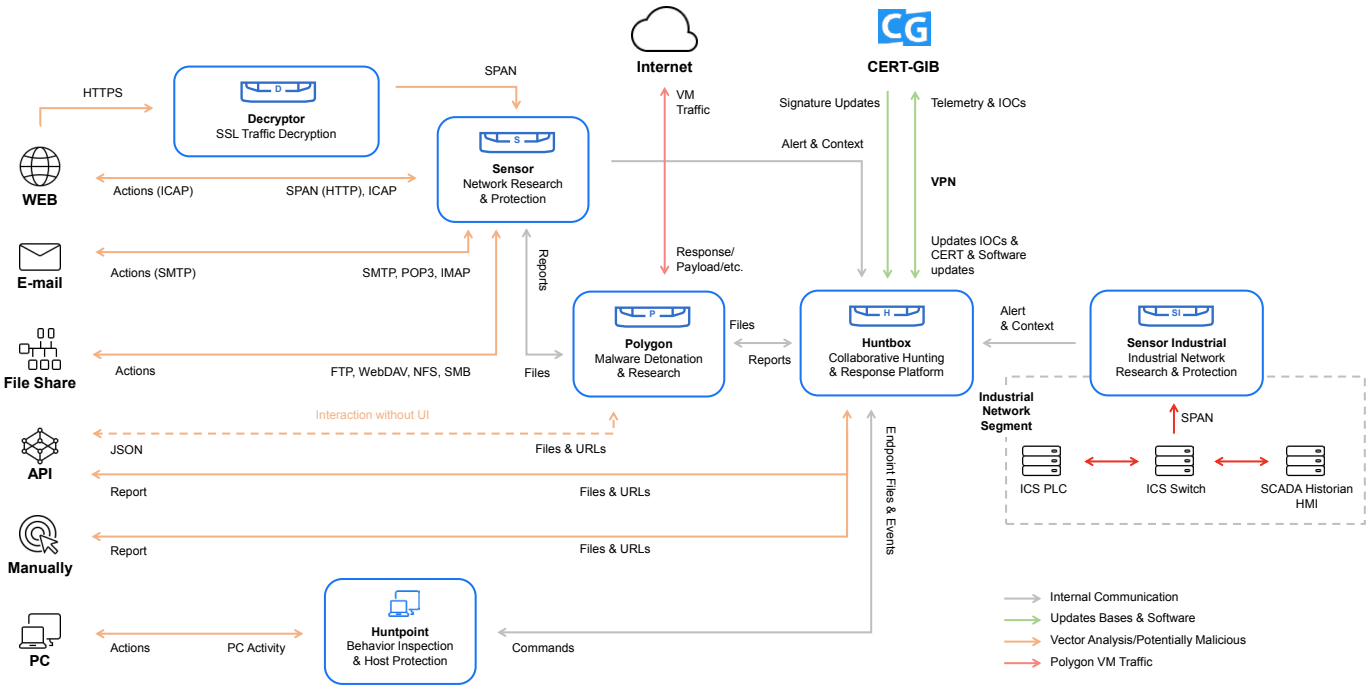
1. Continuous forensic data collection from end hosts
2. Automatic file object transfer for behavioral analysis* (requires Polygon)
3. YARA rules for additional fine-tuning of file and link analysis* (using Polygon)
4. Automatic blocking of malware launches
5. Automatic qurantine implementation for malware for further analysis
6. Automatic blocking of malicious processes
7. Access to Group-IB's malicious objects database for reputation checks when behavioral analysis is not needed
8. Blocking of possible end host interaction when requested by the analyst
9. Threat hunting by data collected
10. Supported OS:
    - Windows 7, 8/8.1, 10
    - Windows server 2008
    - Windows server 2012 R2
    - Windows server 2016
    - Windows server 2019
11. Collected data is stored locally in case connection with Huntbox is lost
12. Centralized management from Huntbox with on-premise/on-cloud deployment options

Centralized management

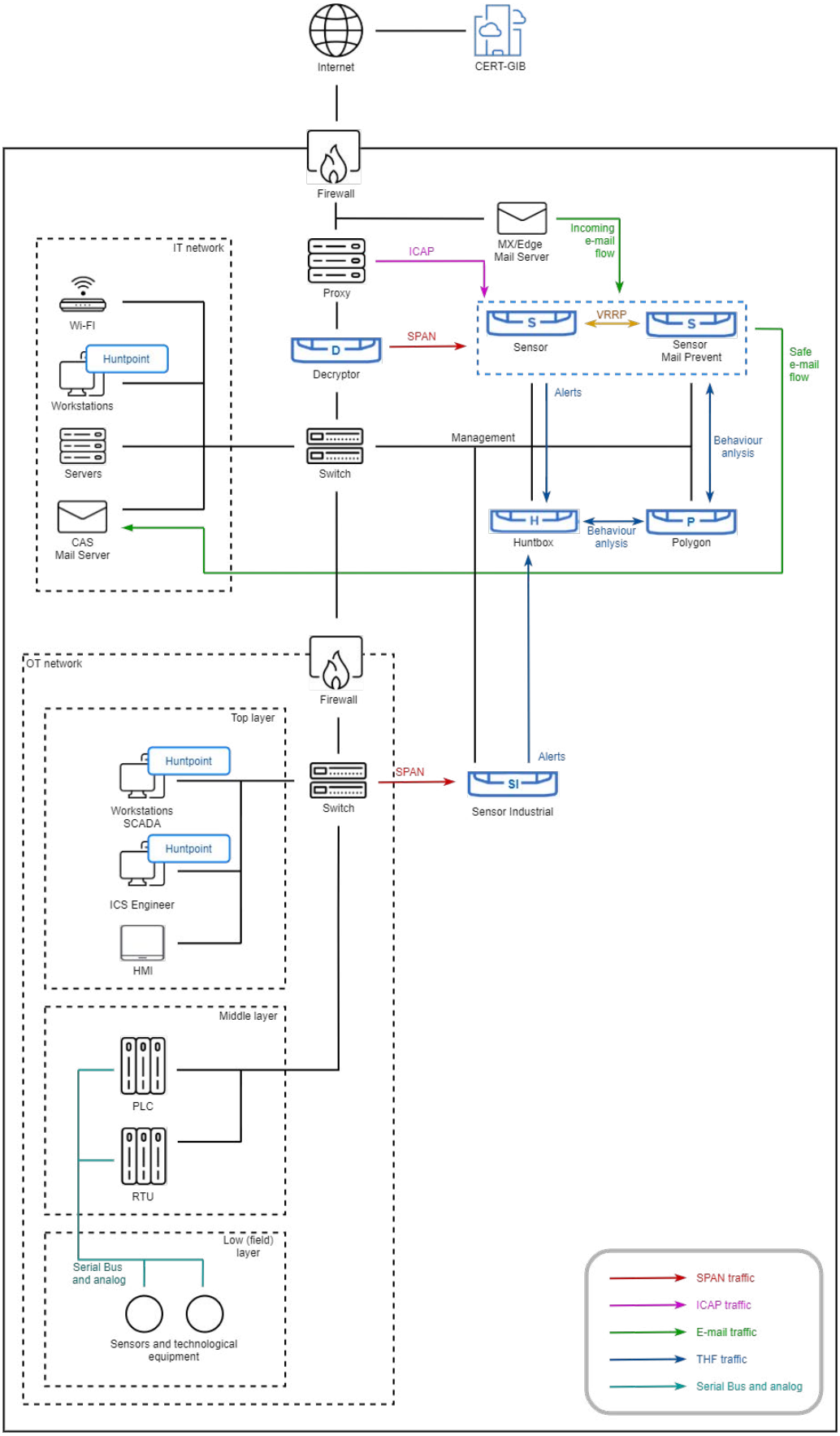
Huntbox provides a graphical interface to manage THF modules installed in the protected infrastructure. It also provides a single storage location for data relating to all incidents. The solution performs advanced searches in the entire database of past events and alerts and provides the following functions:

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

Architecture of Threat Hunting Framework



Integration scheme



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