DATASHEET

Group-IB Threat Hunting Framework / Decryptor

Group-IB Threat Hunting Framework / Decryptor

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.

Decryptor

Decryptor is an optional Group-IB Threat Hunting Framework module. It is a software and hardware complex designed to access and analyze* the content of encrypted sessions, thereby increasing visibility, improving control over the protected infrastructure, and making targeted attack detection more effective.

Technical approach

1 **SSL/TLS session decryption in any application on the go thanks to inline deployment**

2 **Automatic detection of encrypted traffic regardless of the services used**

3 **Transfer of decrypted session copies to external analyzing systems, including Sensor**

4 **Supported operating modes:**

- The bridge mode, as part of which Decryptor operates at the L2 level of the OSI network model
- The gateway mode, as part of which Decryptor operates at the L3 level of the OSI network model and is the gateway to the user's network
- Creation of automatic exceptions when the solution is running
- Operation in reverse proxy mode to control encrypted traffic when accessing corporate resources
- Support of modern encryption protocols, including:
- All modern Cipher Suites (RSA, DHE, ECDHE, ChaCha, Camilla, etc.)
- TLS 1.1 - 1.3 (including RFC 8446) and SSL handshake

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:

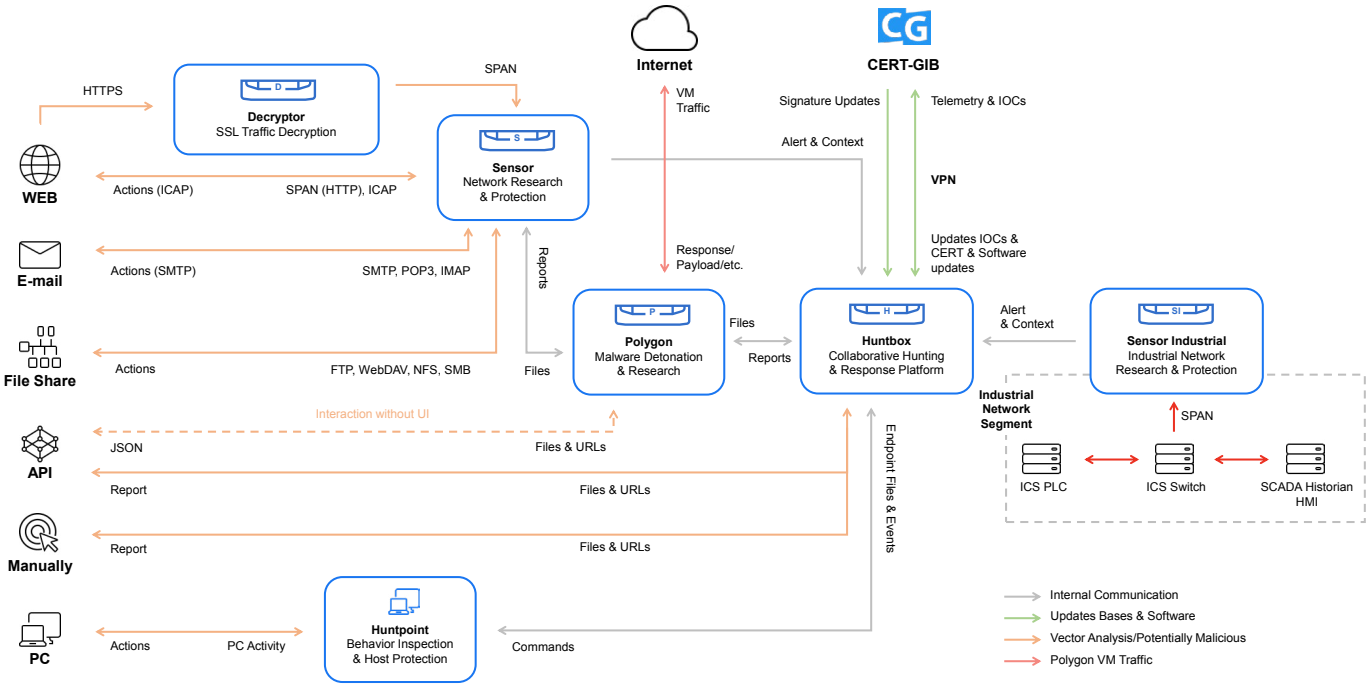
1. Threat Hunting
2. Incident response
3. Event correlation
4. Remote forensics

Deployment options:

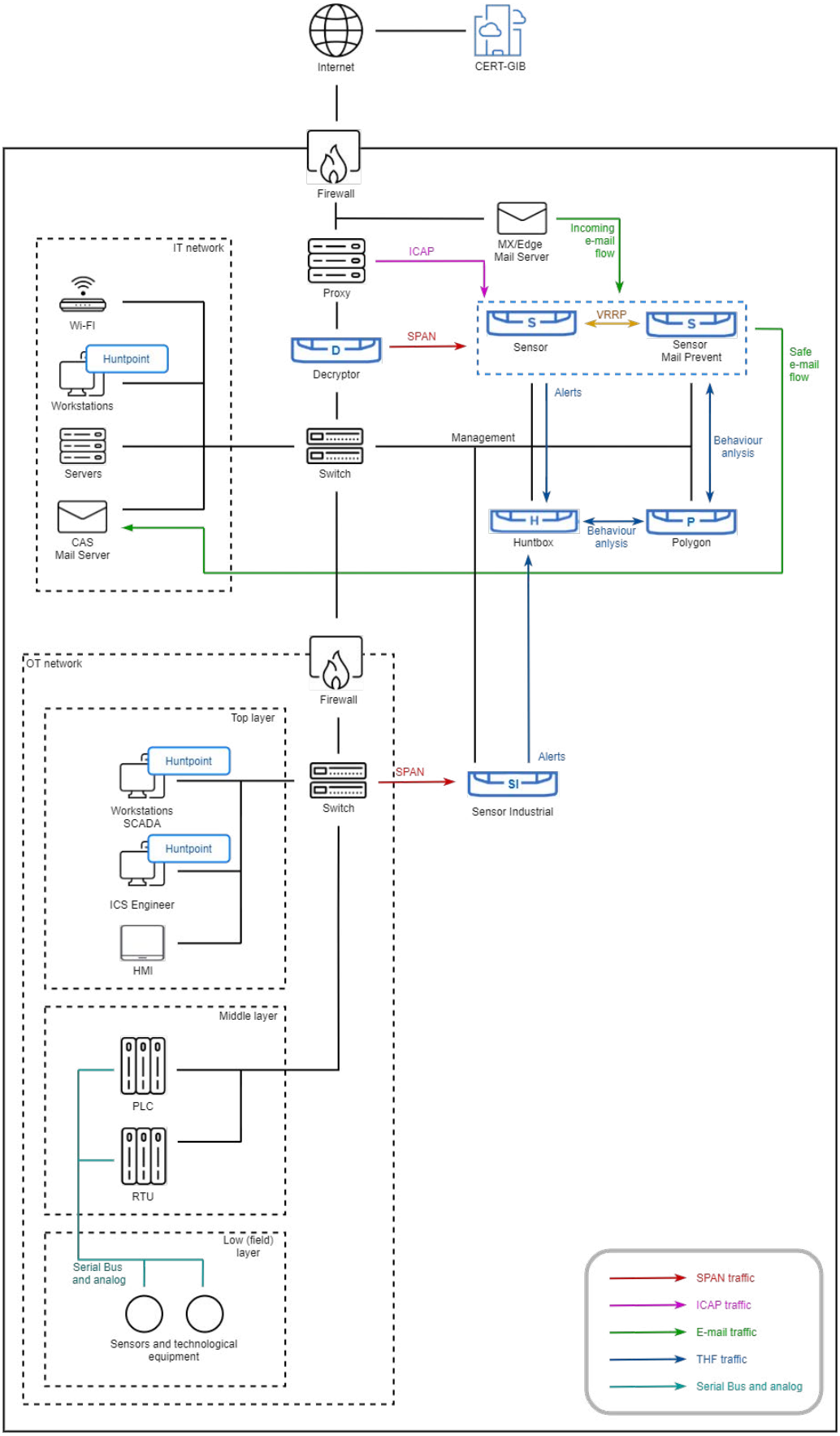
There are three supply options:

- Software
- Hardware
- Virtual

Architecture of Threat Hunting Framework



Integration scheme



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