DATASHEET

Group-IB Threat Hunting Framework / Polygon

Group-IB Threat Hunting Framework / Polygon

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.

Polygon

Polygon is a Group-IB Threat Hunting Framework module that carries out behavioral analysis of files extracted from emails, network traffic, file storage systems, PCs, and automated systems via API or downloaded manually. Polygon complements product functionality by more effectively detecting malicious files targeting the protected infrastructure.

Technical approach

1 **Malware detonation automatically detects the need to use additional OS images or parameters and functions in order to identify all the malicious capabilities of the object analyzed**

2 **Analysis of file objects from the following streams:**

- Mail traffic
- Web traffic* (ICAP integration with proxying solutions)
- SPAN traffic
- Local file storage
- Legitimate public file storage
- End host users* (requires Huntpoint)
- SSL traffic* (Decryptor or ICAP)

3 **Supports 294 formats of analyzed objects**

4 **Content analysis of links in email messages or files**

5 **Retrospective analysis of files and links to identify delayed attacks**

6 **Accessing password-protected archives taking the following contexts into account:**

- Message content
- Email headers
- Attachments
- Email chains (related emails)
- Link content
- Internal dictionary

7 **Protection agains behavioral analy countermeasures:**

- WinAPI monitoring
- Restart using necessary time parameters for malware taking timeframes into account (high CPU load, long pauses, etc.)
- Using and emulating realistic system parameters of the environment analyzed
- Use of the latest office software in the environment analyzed
- Retrospective analysis of link information
- Identification of additional conditions for malware detonation (OS reboot, macros for terminating/running applications, scheduled launches, etc.)
- Accessing multivolume containers with branches
- User activity emulation system (clicks on certain screen points, document closing, etc.)
- Computer vision
- Extraction and execution of additional commands from the registry (not executed by default)

8 **Multiversion analysis**

Windows XP, Windows 7 - x86/x64,
Windows 10 - x86/x64, ENG/RUS

9 **YARA rules for a more thorough customization of file and link analysis**

10 **API integration with incident control and file analysis systems to receive malware detonation verdicts* (requires Huntbox)**

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:

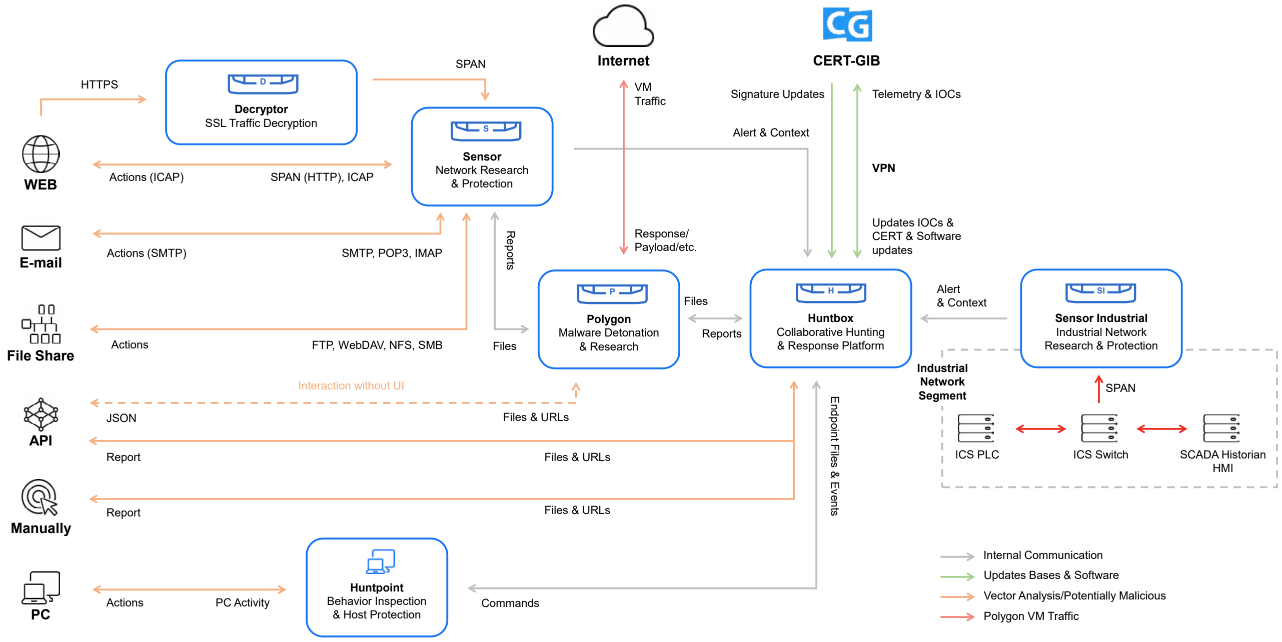
1. Threat Hunting
2. Incident response
3. Event correlation
4. Remote forensics

Deployment options:

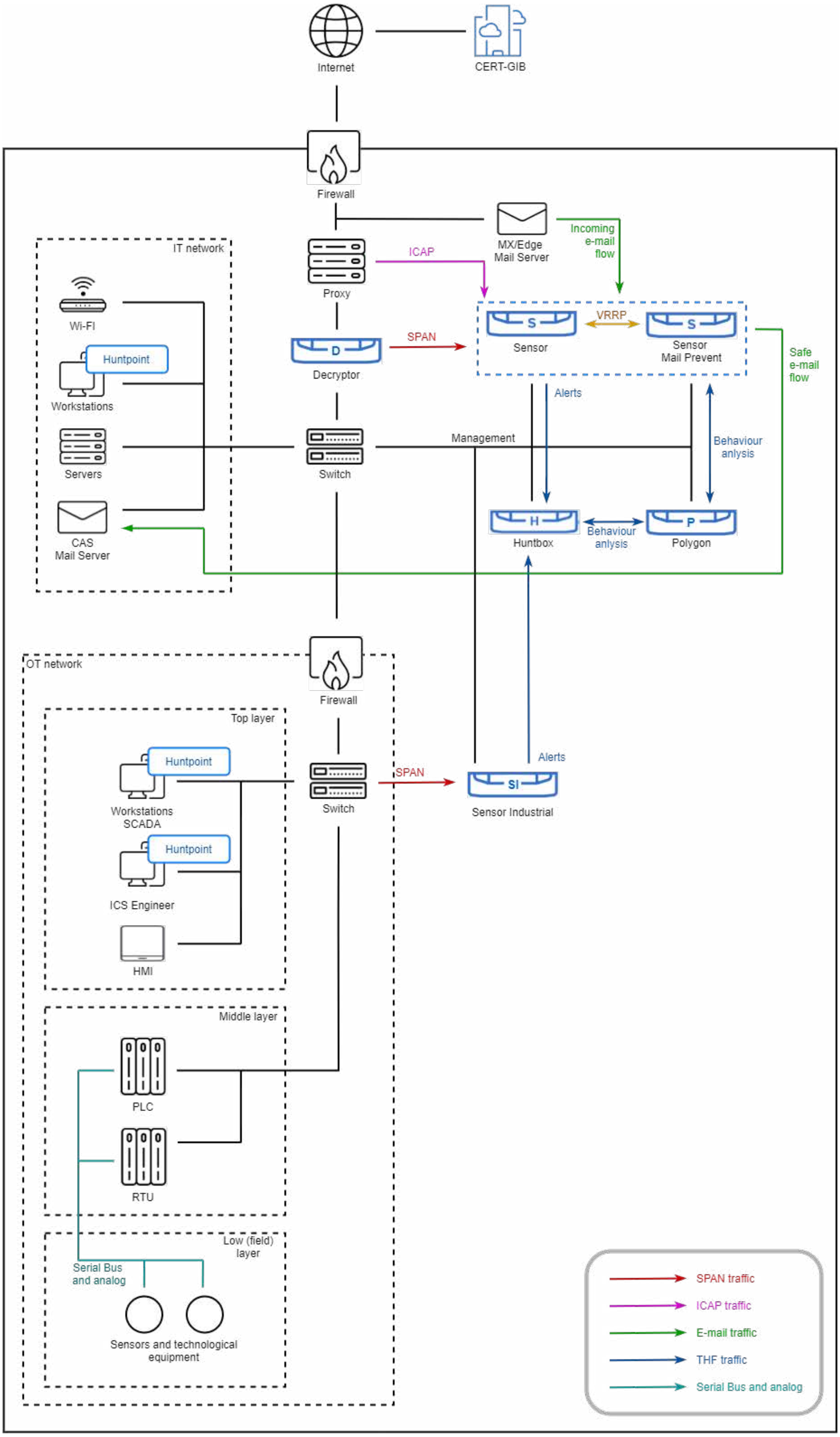
There are four supply options:

- Software
- Hardware
- Cloud
- Virtual

Architecture of Threat Hunting Framework



Integration scheme



	Polygon Standard	Polygon Enterprise
Peak performance, unique files per day	~9000	~19000
Network interfaces for management (LAN)	4x 1000BASE-T	
IPMI (back panel)	1x 1000BASE-T	
Form factor	1U	
Storage subsystem	2x 480GB SATA SSD (RAID-1)	
AC power supply, Watts	2x 750	
Maximum power consumption, Watts	705	
Maximum heat dissipation, BTU/h	2x 2500	
Approximate weight of an appliance, kg	22	24
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