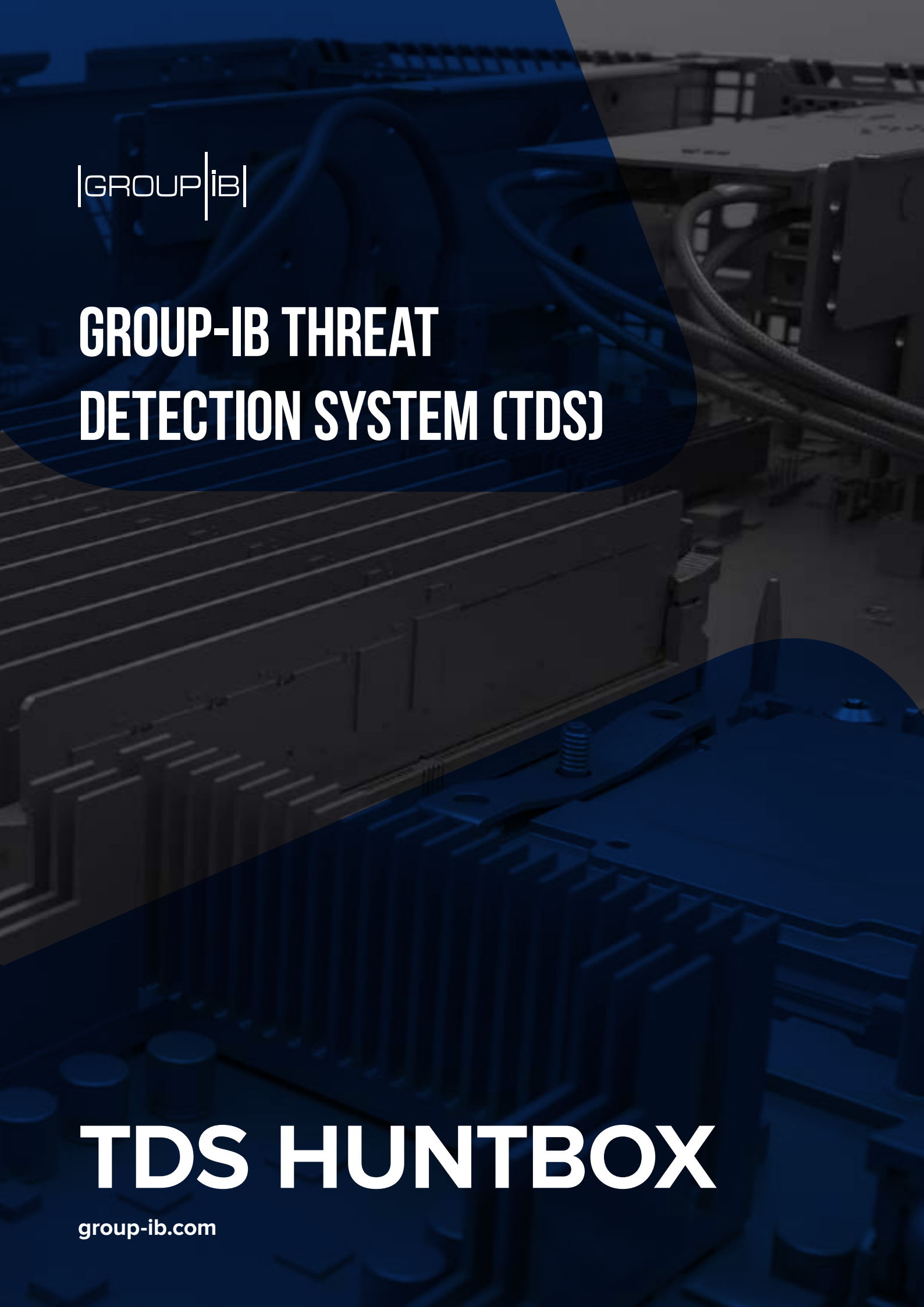

GROUP-IB THREAT DETECTION SYSTEM (TDS)

TDS HUNTBOX

group-ib.com

GROUP-IB THREAT DETECTION SYSTEM (TDS)

TDS is a comprehensive solution designed to detect unknown threats and targeted attacks, hunt for threats both within and beyond the protected perimeter, and help investigate and respond to cybersecurity incidents.

TDS detects infections overlooked by traditional security tools such as antivirus software, firewalls, and intrusion prevention systems.

KEY ADVANTAGES:

- More accurate detection of unknown threats and self-learning through feedback from each individual module
- Automated Threat Hunting
- Comprehensive solution that functions as a single unit and does not require any integration steps or correlation of events between different detection components
- Data integrated from Group-IB Threat Intelligence
- Includes 24/7 Threat Hunting; event monitoring; notifications via a ticket system, email and phone calls; and incident investigation and response services from CERT-GIB experts with years of experience
- Flexible deployment and user friendly
- Includes incident insurance from international insurers

TECHNICAL APPROACHES:

- In-depth analysis of network traffic to detect anomalies and malicious traffic
- Behavioral analysis of files and links in isolated sandboxes
- Detection of anomalies in user and computer program behavior
- Automated hunting for unknown threats
- Examination of indicators provided by Threat Intelligence
- Correlation of events collected by TDS as a whole

DETECTION OF THREATS AT VARIOUS ATT&CK MATRIX STAGES:

- Zero-day threats
- Exploits, Trojans, backdoors, and malicious scripts for desktop, server, and mobile platforms
- Covert channels
- Fileless threats
- Living off the land (LotL) attacks

THE COMPLETE THREAT DETECTION SYSTEM (TDS) SOLUTION INCLUDES FOUR MAIN MODULES

TDS Huntbox

Unified system for managing detection infrastructure, automated analysis, event correlation, and Threat Hunting.

TDS Sensor

Module for in-depth network traffic analysis and threat detection at network level.

TDS Polygon

Module for launching files and links and their dynamic analysis to detect both known and unknown threats in isolated environments.

TDS Huntpoint

Agent for detecting threats on hosts, recording the full timeline of system events, blocking anomalous behavior, isolating hosts, and collecting forensically relevant data.

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.

TDS HUNTBOX

TDS Huntbox is a set of tools that are indispensable for monitoring, incident response, and Threat Hunting in the protected environment. It can be used as either an additional SOC tool or its core.

MAIN FEATURES OF TDS HUNTBOX:

Management of detection infrastructure

TDS Huntbox is a single management tool for all of the system's modules (Sensor, Polygon, and Huntpoint) and a single storage location for all events, alerts, and incidents. The solution performs advanced searches in the entire database of past events and establishes correlations between them.

Attack detection, data correlation, and enrichment

Attacks are detected in trusted environments only, which helps exclude the possibility of an attacker's intrusion in the detection process.

Regardless of how an incident was detected, the process of correlating events from all TDS modules is launched. Once all correlated events have been found, their indicators are enriched in internal sources and threat intelligence data before the correlation and enrichment processes are launched again. This helps immediately obtain the whole picture of an attack in graph and table form.

Incident visualization

Clear visualization of links between processes, files, mutexes, and registry keys involved in an incident, i.e. the information required to promptly investigate any cybersecurity incident.

Threat Hunting

Threat Hunting in internal infrastructures involves advanced searches by all events and logs recorded in network traffic, on hosts, and in email headers, as well as reports with file behavior analysis and the fullest possible context from processes and their launch parameters.

Graph analysis

For Threat Hunting outside the customer's infrastructure, a separate graph tool is provided. Group-IB takes snapshots of the Internet, builds links between them, keeps historical data, and correlates all this information. We also perform analysis of malicious files and known TTPs (Tactics, Techniques and Procedures), which provides attribution to cybercriminal groups. The graph makes it possible to search manually by IP address, domain, email address, phone number, SSL certificate, SSH fingerprint, and hash. The tool can also automatically receive attackers' hidden infrastructure for further analysis.

Incident response

Collaboration between various experts during an incident response operation is ensured through a built-in messaging system.

With TDS Huntpoint implemented, the TDS Huntbox interface enables the following actions on hosts:

- Terminating malicious processes
- Blocking the launching of files involved in the incident
- Isolating the computer from the network
- Collecting forensic data such as memory dumps, list of installed updates, registry files and OS logs

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 SOC 24/7; the Intelligence feed works two-ways

	TDS Huntbox Enterprise	TDS Huntbox Performance	TDS Huntbox Storage
Number of Huntpoint solutions connected, units	<1000	1000-2000	*
Storage capacity	2x 960 GB(SSD) + 4x 1,2 TB(HDD)	2x 960 GB(SSD) + 4x 1,2 TB(HDD)	2x 960 GB(SSD) + 2x 1,2 TB(HDD)
Network interfaces	4x 1000 BASE-T	4x 1000 BASE-T	4x 1000 BASE-T
Form factor	1U	1U	1U
IPMI port (rear panel)	1	1	1
USB ports (rear panel)	2	2	2
Serial ports (rear panel)	1	1	1
VGA ports	1	1	1
AC power supply in Watts	2 x 550	2 x 550	2 x 550
Maximum power consumption in Watts	517	517	517
Dimensions in mm	43 x 434 x 755	43 x 434 x 755	43 x 434 x 755
Appliance weight in kg	22	24	19,9
Heat dissipation (max)	2x 2891 BTU/h	2x 2891 BTU/h	2x 2107 BTU/h
Certificates of conformity	TP TC 004/2011; TP TC 020/2011	TP TC 004/2011; TP TC 020/2011	TP TC 004/2011; TP TC 020/2011
Compliance with standards	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE
Operating temperature	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment
Operating relative humidity	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point

* HB Storage is used when the data volume and storage duration increase. HB Storage is used in conjunction with HB Standard/Enterprise.

Deployment options:

There are three TDS Huntbox supply options: SW/HW/Cloud. Depending on requirements, TDS 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** – TDS Huntbox deployment in Group-IB's infrastructure, which helps promptly increase capacity levels and carry out monitoring, investigation, and response