GROUP-IB THREAT DETECTION SYSTEM (TDS)

# TDS POLYGON

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 POLYGON

**TDS Polygon** is a Group-IB Threat Detection System (TDS) module designed to conduct behavior analysis of files extracted from emails, network traffic, file storage systems, personal computers, and automated systems, as well as manually uploaded files and those extracted through API integration. TDS Polygon complements TDS functionality by enhancing the detection of malicious files targeting the protected infrastructure.

## CHARACTERISTICS:

- **Coverage of the main threat distribution channels:** email, Internet, infections of official websites, insiders, and USB drives
- **Continuously updated classifier and IoC databases** powered by our threat intelligence system and forensic investigations
- **Effective threat detection** through a proprietary low-level monitor and a system designed to hide virtualization from malware
- **Detection of social engineering techniques** and of attempts by malicious files to bypass anti-APT solutions during behavioral analysis
- **Multiversion analysis:** Windows XP, Windows 7, and Windows 10 in both bitness versions (x32/x64) with two system languages (Russian/English)
- **Detection of delayed attacks** through retrospective analysis when integrated with various systems within the protected infrastructure
- **Detection of malware** in emails and file storage systems, as well as when files are downloaded from the Internet, with the possibility to block them*
- **Absolute confidentiality:** file processing and analysis is performed within the customer's security perimeter, directly on TDS Polygon
- **Interface with a ticket system** in Group-IB SOC (optional)
- **Internal threat classifier**
- **Various HW/Cloud deployment options**

* Requires interaction with TDS Sensor and its integration in relevant systems of the protected infrastructure.

## CENTRALIZED MANAGEMENT

TDS Huntbox provides a graphic interface for managing TDS modules installed in the protected infrastructure. It is a single storage location for incident data and allows for advanced searches by all indicators in all system events and alerts. The solution's functionality also includes:

1. **Threat Hunting**
2. **Incident response**
3. **Event correlation and remote forensics**

# TDS POLYGON

## MAIN FEATURES OF TDS POLYGON:

**File launch in an isolated environment**

This feature identifies file type and launch rules based on file headers. If for any reason the file is not launched in the environment selected, it will be relaunched in a new environment. Moreover, various methods of masking TDS Polygon virtualization are used.

**Activity log after file launch**

Complete log of all changes that have taken place in an isolated environment after a file has been launched, including screen recordings.

**User behavior emulation**

Once an object is placed in a selected virtual environment, several real OS user capabilities are simulated: from mouse movements and keystrokes to following links and downloading, opening, and launching files.

**Social engineering techniques**

Social engineering techniques used to bypass security systems and analyzed by Group-IB specialists are built into TDS Polygon. The system works with password-protected archives, analyzing the text in both the email body and any attachments. The solution makes it possible to work with file storage systems and has several modes for working with links, including intellectual analysis of link types and redirecting links.

**Retrospective analysis**

TDS uses Polygon's free capacities to additionally analyze objects whose initial examination did not reveal any malicious signs. This ensures that delayed attacks on the protected infrastructure are detected.

**Detailed reports**

The experience of our forensic specialists in collecting and structuring data about malware behavior powers the reporting subsystem of TDS Polygon. Reports include:

- risk assessment
- object attribution
- video of file execution
- file structure
- behavioral markers
- network activity
- process tree
- information about affected system data
- additional analysis artifacts

**More than 200 supported object formats.**

| | TDS Polygon Cloud | TDS Polygon Standard | TDS Polygon Enterprise |
|---|---|---|---|
| Peak performance (files per day) | Any | 9000 | 19000 |
| Network ports (LAN) | — | 4x 10/100/1000 BASE-T | 4x 10/100/1000 BASE-T |
| IPMI port (rear panel) | — | 1 | 1 |
| Form factor | Cloud | 1U | 1U |
| Storage capacity | — | 2x 480GB SSD | 2x 480GB SSD |
| USB ports (rear panel) | — | 2 | 2 |
| USB ports (front panel) | — | 2 | 2 |
| Serial ports (rear panel) | — | 1 | 1 |
| VGA ports | — | 1 | 1 |
| AC power supply in Watts — | — | 2 x 550 | 2 x 550 |
| Maximum power consumption in Watts | — | 517 | 517 |
| Dimensions in mm | — | 43 x 434 x 678 | 43 x 434 x 678 |
| Appliance weight in kg | — | 16 | 16 |
| Heat Dissipation (max | — | 2x 2107 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 |
| Compliance with standards | — | 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 |
| Operating relative humidity | — | 0% to 80% Relative Humidity with 29°C (84.2°F) maximum dew point | 0% to 80% Relative Humidity with 29°C (84.2°F) maximum dew point |