Group-IB

THREAT DETECTION SYSTEM

Adversary-centric detection and proactive threat hunting.

- Full visibility over attack chain
- Automated & streamlined response
- Unparalleled detection of advanced threats
• Evolution of advanced threat defense

1990 → 2010 → 2015 → 2020

Detection of known threats
- AV
- IDS/IPS

Detection of unknown threats
- Sandbox
- Advanced AV

Intelligence-based detection
- Threat Intelligence
- Internal threat hunting

Attribution-based detection
- Global threat hunting
- Attribution & hunting automation

• Start the hunt with Threat Detection System

Threat Detection System is a solution for creating local centers to detect, research and response to complex and unknown threats.

Maximum convenience with flexible options

Stand-alone solution
On-prem to keep all data inside the perimeter for absolute confidentiality

Cloud delivery
Flexible integration with cloud in your country

Hybrid
Mixed type of installation to fit your requirements
Wide functionality and unique advantages

- Threat hunting on hosts and in network traffic using correlated data
- Threat hunting both within and outside protected perimeters
- Analysis of attackers’ external infrastructure
- In-depth malware analysis in isolated environments
- Analysis of anomalies and covert channels in network traffic
- Detection of user and program behaviour anomalies on hosts
- Playbooks testing of attributed threats
- Remote incident response and digital forensics

Key differences of the system

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat hunting within and outside the organization</td>
<td>Handling of complex incidents rather than raw alerts</td>
</tr>
<tr>
<td>All necessary tools are connected to the system</td>
<td>Integrated Threat Intelligence data</td>
</tr>
<tr>
<td>Collaboration with the best experts in one environment</td>
<td>Adaptive automation of threat hunting, analysis, and response</td>
</tr>
</tbody>
</table>

Only correlation of internal and external telemetry data ensures effective threat hunting and analysis and helps detect skillfully prepared attacks.

How Threat Detection System works

- **Research**
  - Traffic
  - Files
  - Behaviour
  - Assets

- **Hunt**
  - Malware
  - Techniques
  - Adversary
  - Infrastructure

- **Detect**
  - Anomalies
  - Unknown threats
  - Lateral movement
  - Fileless attacks

- **Respond**
  - Isolation
  - Collaboration
  - Playbooks
  - Group–IB IR

By purchasing Threat Detection System, a policy will be automatically taken out with one of the largest insurance companies in the world, AIG. The policy covers risks of corporate or personal data leaks and computer system security breaches caused by infected or lost data.
Group-IB is a leading provider of advanced Threat Intelligence, best-in-class anti-APT and anti-fraud solutions.

Group-IB is ranked among the best threat intelligence vendors in the world by Gartner, IDC, Forrester, Cyber Defense Magazine and SC Media.

We have provided professional development training to Europol, INTERPOL, law enforcement agencies and corporate security teams on four continents.

Intelligence-Driven Services

Strengthen your cybersecurity posture with services and advice from experienced specialists with 'boots on the ground' and access to one of the most advanced threat intelligence gathering infrastructures in the world.

Security & Risk Assessment

- Penetration Testing
- Vulnerability Assessment
- Source Code Analysis
- Compromise Assessment
- Red Teaming
- Pre-IR Assessment
- Compliance Audit

Threat Hunting & Response

- 24/7 CERT-GIB
- External and Internal Threat Hunting
- Onsite Incident Response
- Incident Response Retainer

Digital Forensics

- Digital Forensics
- Investigations of hi-tech financial & corporate crimes, critical infrastructure attacks

Cyber Education

- Digital Forensics
- Incident Response
- Malware Analysis