GROUP-IB

PRODUCT OVERVIEW

MANAGED XDR

Supercharge security and defeat attacks before they begin with knowledge of how and when you will be attacked

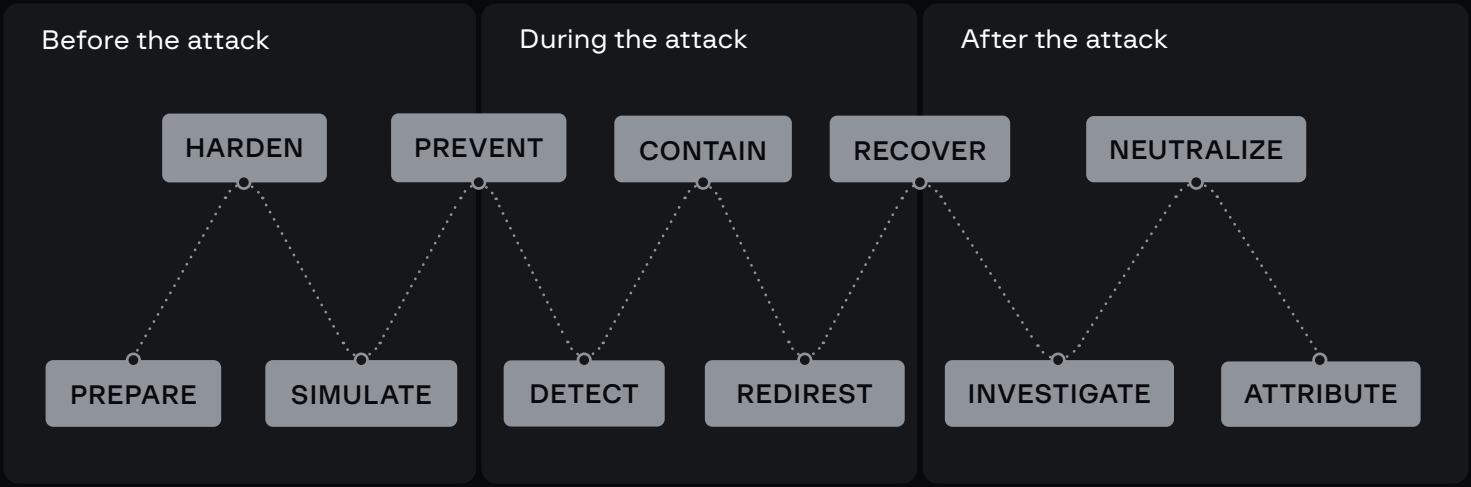
A new set of security objectives

Cyber response chain

Security teams are no longer expected to prevent breaches from taking place. In today's threat landscape, prevention simply is not a realistic goal.

Instead, security teams today are assessed by how quickly they can detect breaches, limit the blast radius, and minimize the mean time to recovery after an incident occurs.

Security teams must manage the following chain of events in order to apply these new metrics:



Time is of the essence

Breaches are unavoidable, so a fast response is imperative. The longer it takes to discover and respond to an incident, the more expensive it is to fully recover from it.

13 days

the average dwell time that passes between threat actors gaining initial access to a victim's network and deploying ransomware

$1,25 mln

average cost of a breach when discovered after 200 days or more (with an average discovery time of 287 days), according to IBM

Managed Extended Detection and Response (XDR)

A faster and more efficient product class

XDR solutions were designed to leverage both the increasing number of telemetry sources and the ever-evolving ML algorithms, providing superior detection and response capabilities.

Empowered with malware detonation, threat intelligence, and ML models for event correlation, Group-IB Managed XDR works seamlessly across networks, endpoints, and clouds in order to make the effectiveness of your security operations greater than the sum of their parts.

Managed XDR overcomes the most pressing security challenges in today's world

Eases alert fatigue

Thousands of security events take place every hour. Group-IB XDR correlates data and identifies the issues that require action.

Extends limited resources

Security teams are often overtasked and under-resourced. Use Group-IB XDR to ease workflows by streamlining detection and response.

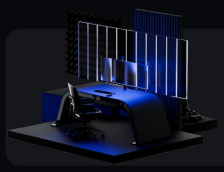
Connects siloed solutions

Managing a portfolio of security solutions is difficult and time-consuming. Every component of Group-IB XDR works in unison to increase ROI.

Keeps up with evolving threats

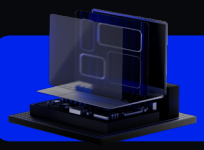
Cyberattacks are constantly evolving and becoming more sophisticated. To keep up with them, leverage intelligence insights and advanced tech.

Managed XDR powered by Group-IB



MANAGED DETECTION, RESPONSE, THREAT HUNTING

GROUP-IB SERVICES



XDR DATA LAKE

GROUP-IB XDR

API/SYSLOG

SIEM/SOAR

Activity data: telemetry, metadata, logs, NetFlow, etc.

EDR
Endpoints and servers

EMAIL SECURITY
Attachments, phishing, and BEC

MALWARE DETONATION
Isolated environments

TRAFFIC ANALYSIS
Network monitoring, event correlation

THREAT INTELLIGENCE
Best-of-breed actionable insights

ATTACK SURFACE
Automated asset discovery

Group-IB Managed XDR covers most parts of the cyber response chain

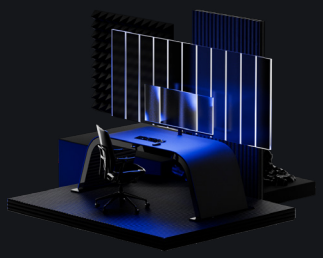
GROUP-IB MANAGED XDR — Additional services

Before the attack	During the attack	After the attack
HARDEN	CONTAIN	NEUTRALIZE
PREVENT	RECOVER	
PREPARE	DETECT	INVESTIGATE
SIMULATE	REDIREST	ATTRIBUTE

GROUP-IB XDR
Additional services

Extend your security team

Strengthen your security posture with Managed Detection, Managed Incident Response, and Managed Threat Hunting capabilities

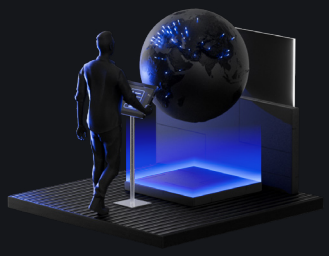


Managed detection

Offload internal teams with Group-IB's 24/7 CERT. Our team will analyze alerts and provide you with actionable recommendations on relevant threats

Managed incident response

Mitigate threats and get a faster response with Group-IB DFIR experts leveraging XDR capabilities to collect forensic data and implement remote response actions



Managed threat hunting

Detect yet undiscovered threats and APTs and let expert threat hunters test hypotheses based on XDR data to give you full visibility over your security posture

Group-IB Managed XDR: quantifiable agility and superior speed

Unprecedented product synergy

Group-IB's point solutions are designed to work together to provide better security across attack vectors and infrastructure segments, on-premises or in the cloud

Innovative timesaving automation

Let the system handle complex incident management instead of digging through hundreds of scattered alerts and have the best experts at hand

Intelligent prioritization and recommendations

Leverage region and industry-specific knowledge about relevant threats accumulated in local intelligence centers and over 18 years of DFIR activities, research and development

Detection and response in real time

Receive immediate response when threats are detected on protected infrastructure, including real-time host isolation, forensic data collection, file quarantine, and more

The solution in numbers

272% ROI

According to a study by Forrester

20% faster

First-tier incident response activities

20% increase

In measurable efficiency of security teams using Managed XDR toolset

Managed XDR Features

Endpoint Detection and Response

Endpoints

- Host-level detection
- Behavioral ML-classifiers
- Streamlined response
- Application control
- Asset inventory
- UEFI threat detection
- Forensic data collection

Network Traffic Analysis

Network

- L2-L7 protocol support
- Network logging and metadata collection
- Custom rules
- Detection of covert channels (DNS-, ICMP-tunneling, DGA)
- Encrypted traffic analysis (ETA)
- C2 traffic and server discovery
- Extraction of objects for analysis

Malware Detonation

Files and links

- Automatic VM customization
- Object analysis across infrastructure
- 290+ supported object formats
- Link analysis
- Retrospective analysis
- Anti-evasion technologies
- Actionable in-depth reports

Email Protection

Malware, spam, and BEC attacks

- On-prem or fully cloud deployment
- Anti-spam filtering
- AV analysis
- Realistic VMs (image morphing)
- Network tunneling
- Advanced anti-evasion
- Post-delivery protection
- BEC and phishing detection

Managed Services

Detection, response, and threat hunting

- 24/7 alert monitoring
- False positives triage
- Direct connection with analysts
- Personalized threat landscape
- Hypothesis testing
- Custom playbooks for IR
- Experts at hand

About Group-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,400+
Successful investigations of high-tech cybercrime cases

300+
employees

600+
enterprise customers

60
countries

$1 bln
saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

120+
patents and applications

7
Unique Digital Crime Resistance Centers

* According to Cybersecurity Excellence Awards

Global partnerships

INTERPOL
EUROPOL
AFRIPOL

Recognized by top industry experts

FORRESTER®
Aité Novarica
kuppingercole ANALYSTS
Gartner
IDC
FROST & SULLIVAN

Technologies and innovations

Cybersecurity

- Threat intelligence
- Attack surface management
- Email protection
- Network traffic analysis
- Malware detonation
- EDR
- XDR

Anti-fraud

- Client-side anti-fraud
- Adaptive authentication
- Bot prevention
- Fraud intelligence
- User and entity behavior analysis

Brand protection

- Anti-phishing
- Anti-piracy
- Anti-scam
- Anti-counterfeit
- Protection from data leaks
- VIP protection

Intelligence-driven services

Audit & Consulting		• Security Assessment • Penetration Testing	• Red Teaming • Compliance & Consulting
Education & Training		• For technical specialists • For wider audiences	
DFIR	• Incident Response • Incident Response Retainer	• Incident Response Readiness Assessment • Compromise Assessment	• Digital Forensics • eDiscovery
Managed Services		• Managed Detection • Managed Threat Hunting	• Managed Response
High-Tech Crime Investigation		• Cyber Investigation • Investigation Subscription	

GROUP-IB

Fight against cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785