BUSINESS EMAIL PROTECTION

Secure corporate email in the cloud and on-premises from even the most sophisticated attacks

Block all email- borne attacks with one intelligent solution

Email is often the initial point of c ompromise in major security incidents. Threat actors effectively have unlimited attempts to succeed and only need to trick one unsuspecting user to gain a foothold in the corporate network.

Business Email Protection detects and blocks all email attacks, including sophisticated attacks that legacy solutions and third-party email providers often miss. Business Email Protection defends against every email-borne t hreat, from spam and phishing to malware delivery and business email compromise.

Business Email Protection

Detect and disrupt cyber threats with unprecedented speed and accuracy to reduce your cyber risk

Email Protection

EMAILS ANALYZ

MALICIOUS EMA

Endpoint protection

ENDPOINT DETECTION AND RESPONSE

Detect attacks on the host level, leveraging intelligence data, signature and behavioral analysis, and malware detonation capabilities. Prevent and respond to threats.

Emails Processing Time Statistics

Most attacke

Updated · 19:15

KEY FEATURES & BENEFITS

Attachment & Link Analysis

Inspect over 290 different file formats to ensure all attachments are safe. Check all links, including obfuscated and redirected links.

ANTI SPAM & ANTI PHISHING

Block spam and phishing attacks to prevent credential theft, malware infection on end-user workstations, and other potential risks

PAYLOAD DETONATION

Detonate and analyze suspicious attachments and links in isolated environments, stopping attacks at their roots

FLEXIBLE DEPLOYMENT

Get to full deployment quickly with a flexible solution that can be SaaS, self- hosted in the cloud, or hosted in a fully isolated on-prem installation

ANTI-EVASION TECHNIQUES

Utilize advanced detonation technologies to stay one step ahead of cybercriminals in their attempts to evade detection.

ATTACKER ATTRIBUTION

Cross-check detonation reports with Group-IB's Threat Intelligence to attribute attacks to specific threat actors or malware families

Business Email Protection

Detect and disrupt cyber threats with unprecedented speed and accuracy to reduce your cyber risk

Email Protection

Endpoint protection

ENDPOINT DETECTION AND RESPONSE

Detect attacks on the host level, leveraging intelligence data, signature and behavioral analysis, and malware detonation capabilities. Prevent and respond to threats.

Emails Processing Time Statistics

Most attacke

Updated · 19:15

DIGITAL RISK PROTECTION

Attachment & Link Analysis

The Digital Risk Protection platform leverages advanced technologies to detect the illegitimate use of logos, trademarks, content, and design layouts across the digital surface.

Automatic identification

The Digital Risk Protection platform leverages advanced technologies to detect the illegitimate use of logos, trademarks, content, and design layouts across the digital surface.

Machine learning that detects violations at earliest stages

- Identifies fraud and scam before the traffic attraction stage
- Continuously enriches detection algorithms across industries
- Utilizes Graph module to map and takedown entire fraud networks

HOW DIGITAL RISK PROTECTION WORKS

Step 1

RESOURCE
MONITORING

- Domain names
- Databases of phishing resources
- Search engines• Social media
- Mobile app stores
- Online classifieds and marketplaces
- Advertising•
  Instant messengers
- Deep/dark web
- Public databases and code repositories
- Breached databases

Step 2

VIOLATION D
ETERMINATION

- Phishing• Scam
- Trademark violation
- Counterfeit
- Piracy
- Partner policy compliance
- Data leakage
- VIP impersonations

Step 3

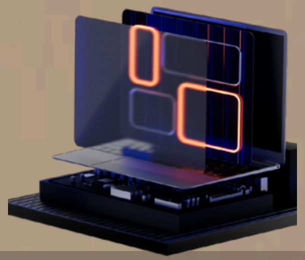
RESPONSE

- Comprehensive takedown procedure reaching an 85% pre- trial takedown rate on average

FRAUD PROTECTION

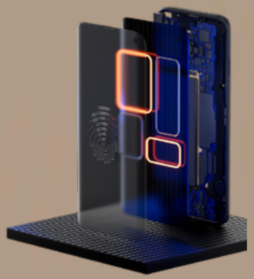
Eliminate fraud across all digital channels in real time

- Credit card fraud
- Social engineering attacks
- Malicious bot activity
- E-commerce fraud
- Attacks on gaming/betting sector
- Malware-related fraud
- Money laundering
- Payment fraud



Web Channel Protection

- Anonymized user mouse/trackpad/ keyboard behavioral analysis
- Malware, bot and RAT detection
- Device technical specifications
- Device graphic and display configuration
- Browser configuration



Mobile Channel Protection

- Android or iOS operating system configuration monitoring
- Device sensor monitoring
- Mobile operator characteristics monitoring
- Malware, bot and RAT detection
- Anonymized user behaviour monitoring
- Device technical specifications

No crime unpunished

Entrust your case to Group-IB's Investigation Team

- Proprietary technologies for crime detection

- Global collaboration with law enforcement agencies

- Deep knowledge of criminal schemes

- Individual approach and special project teams

More than detection

Integration with Threat Intelligence receives the following data:

- IP Intelligence data: TOR, proxy, hosting

- Phishing and malicious domains
- Malicious software behaviors and signatures

- Compromised user accounts

- Compromised payment cards

No bad bots allowed

Preventive Proxy protects web and mobile applications from various types of bot activity, including:

- Mobile API attacks

- Unauthorized use of API

- Automation framework detection

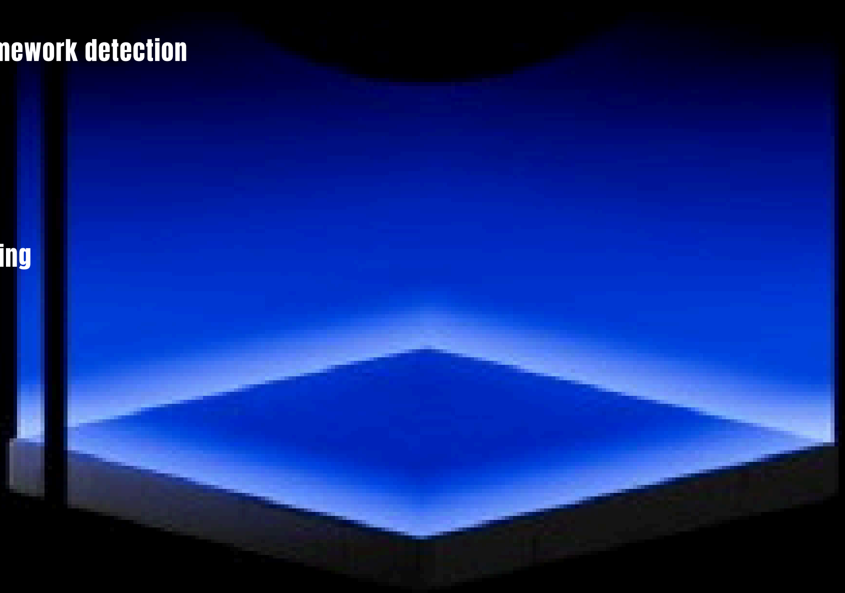
- Scraping

- Brute force

- Credential stuffing

- Layer 7 DDoS

- Cookie theft



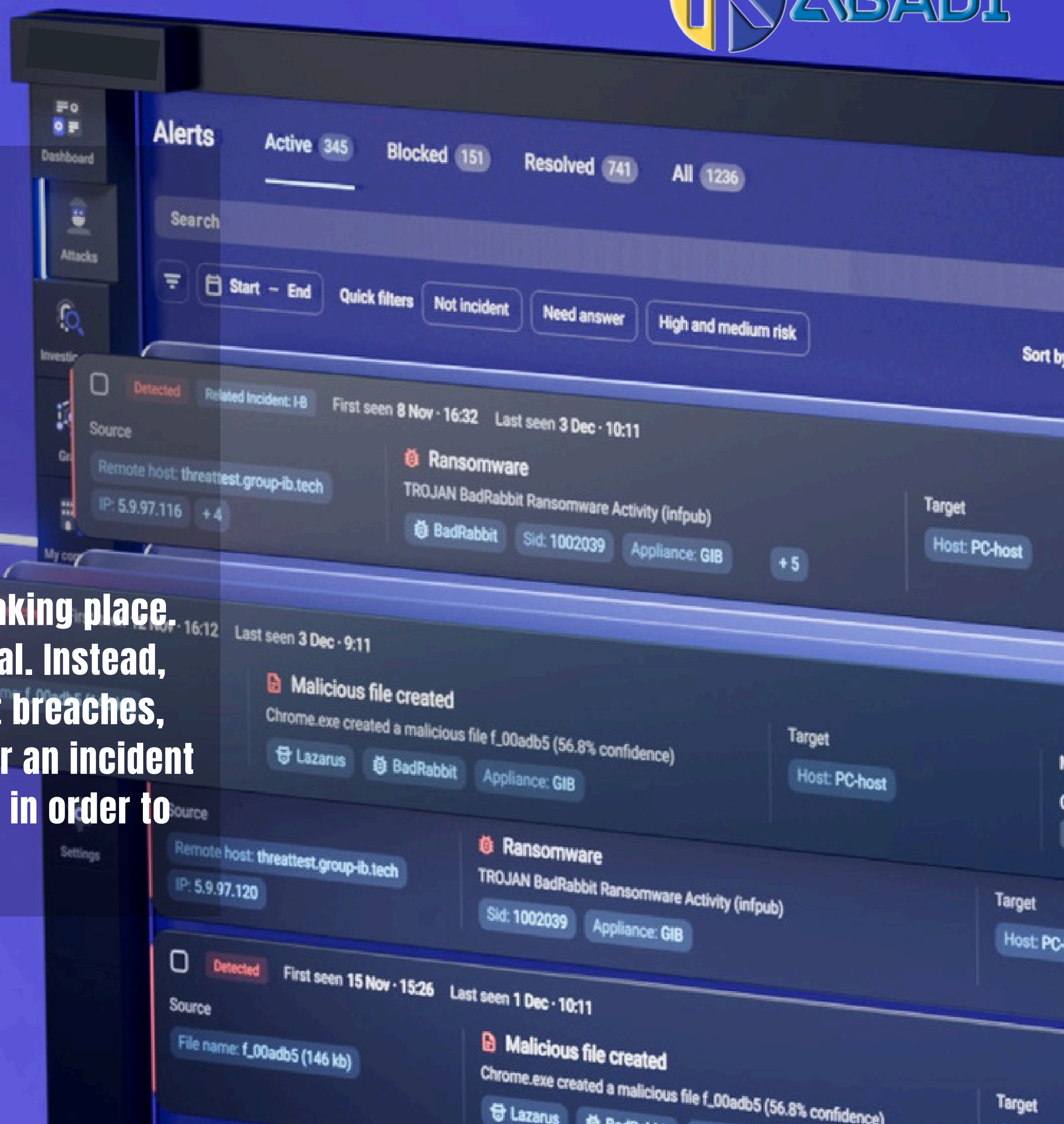
MANAGED XDR

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:

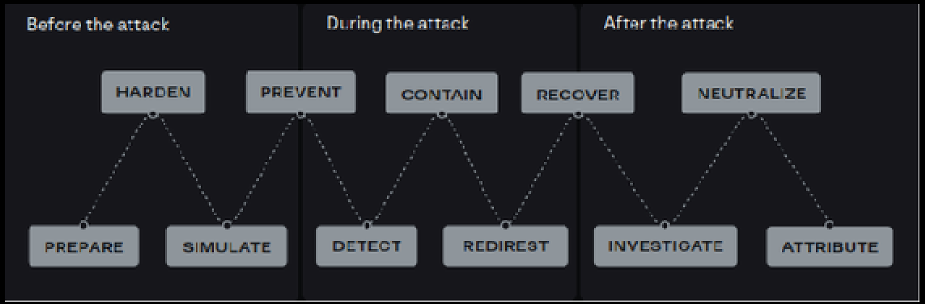


Detected · Related Incident: I-B · First seen 8 Nov · 16:32 · Last seen 3 Dec · 10:11
Source: Remote host: threattest.group-ib.tech · IP: 5.9.97.116 · +4
Ransomware
TROJAN BadRabbit Ransomware Activity (infpub)
BadRabbit · Sid: 1002039 · Appliance: GIB · +5
Target: Host: PC-host

Last seen 3 Dec · 9:11
Malicious file created
Chrome.exe created a malicious file f_00adb5 (56.8% confidence)
Lazarus · BadRabbit · Appliance: GIB
Target: Host: PC-host

Source: Remote host: threattest.group-ib.tech · IP: 5.9.97.120
Ransomware
TROJAN BadRabbit Ransomware Activity (infpub)
Sid: 1002039 · Appliance: GIB
Target: Host: PC-

Detected · First seen 15 Nov · 15:26 · Last seen 1 Dec · 10:11
Source: File name: f_00adb5 (146 kb)
Malicious file created
Chrome.exe created a malicious file f_00adb5 (56.8% confidence)
Lazarus
Target



Before the attack

During the attack

After the attack

HARDEN

PREVENT

CONTAIN

RECOVER

NEUTRALIZE

PREPARE

SIMULATE

DETECT

REDIRECT

INVESTIGATE

ATTRIBUTE

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.

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 everevolving 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 placeevery hour. Group-IB XDR correlates data and identifies the issues that require action.

Connects siloed solutions

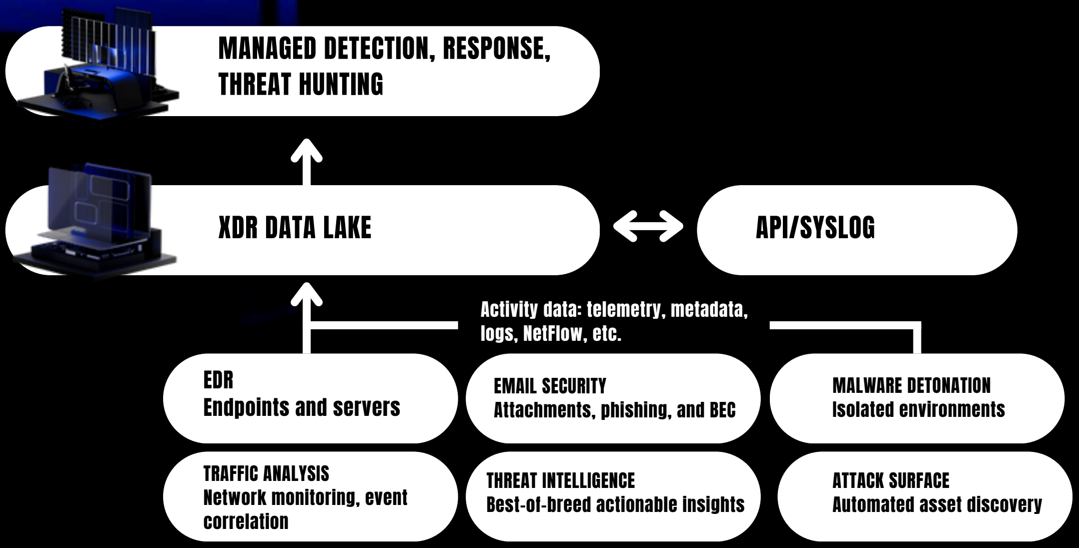
Managing a portfolio of security solutions is difficult and time-consuming. Every component of Group-IB XDR works in unison to increase ROI.

Extends limited resources

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

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 DETECTION, RESPONSE, THREAT HUNTING

XDR DATA LAKE

API/SYSLOG

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

EDR
Endpoints and servers

EMAIL SECURITY
Attachments, phishing, and BEC

MALWARE DETONATION
Isolated environments

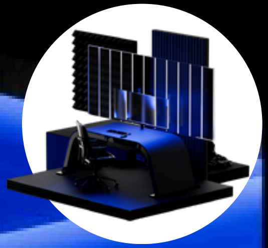
TRAFFIC ANALYSIS
Network monitoring, event correlation

THREAT INTELLIGENCE
Best-of-breed actionable insights

ATTACK SURFACE
Automated asset discovery

Extend your security team

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

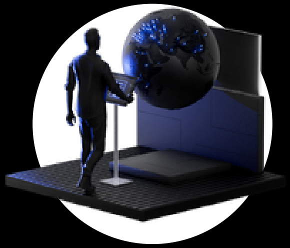


Managed detection

Offload internal teams with 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 DFIR experts leveraging XDR capabilities to collect forensic data and implement remote response actions

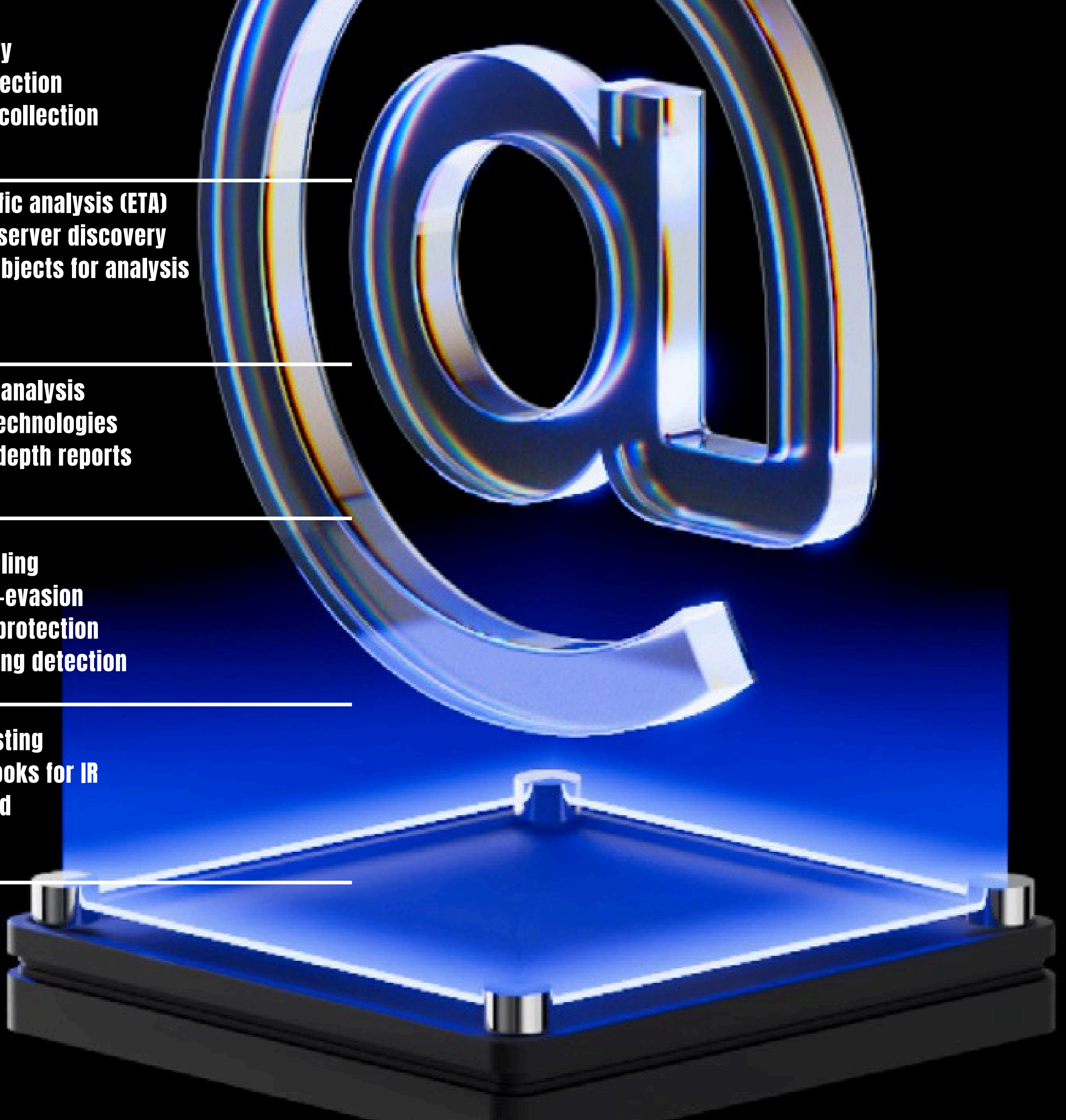


Managed threat hunting

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 postur

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
Malware Detonation 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



THREAT INTELLIGENCE

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

Threat Intelligence provides unparalleled insight into your adversaries. Integrate the intelligence to maximize the performance of every component of your security ecosystem. Equipping your team with Group-IB's strategic, operational, and tactical intelligence streamlines security workflows and increases efficiency.

Strategic intelligence

- Revolutionize risk management with bespoke on-demand, and regular monthly and quarterly threat reports written by analysts specifically for the board and executive business cases
- Enable growth with actionable threat intelligence before expanding into a new region / business line, and get industry-specific threats before digital transformation
- Lower the cost of cyber security by avoiding unnecessary purchases and postponing upgrades by maximizing the efficacy of your existing security investment

Operational intelligence

- Transform security and adapt instantly, use the insights to block malicious network and endpoint activity the moment it is first observed anywhere in the world
- Identify and remove weaknesses before they are exploited by conducting Red Teaming with detailed knowledge of threat actor's tools, tactics and processes
- Automate workflows and improve team efficiency by enriching your SIEM, SOAR, EDR and vulnerability management platforms with outof-the-box integrations for Group-IB threat intelligence

Tactical intelligence

- Prioritize vulnerability patching for your technology stack with automated alerts that inform you the moment vulnerabilities are discovered or begin being exploited by threat actors targeting your industry
- Eliminate false positives and focus on legitimately risky events with a continuously updated database of system and network indicators of compromise for cybercriminals in your threat landscape
- Reduce response time with complete information about the cyber kill chain in the MITRE ATT&CK® matrix format, use the information to quickly remove them from your network

KEY FEATURES

Graph interface

Investigate and research threats with an intuitive graphical interface. Use the Graph to easily explore the relationship between threat actors, their infrastructure and the tools they use at a glance and drill into the details with just a click.

Compromised data detection

Discover compromised credentials, including VIP's personal accounts, payment card information and breach databases before they are used to launch attacks or cause financial damage. Alerts within can be created to inform you whenever a compromise for your organization is discovered.

Dark web insights

Group-IB's Unified Risk Platform has the industry's largest dark web database, access into intelligence with Threat Intelligence to discover illegal activities and monitor whether your organization is mentioned on the dark web. Create rules to inform you when a topic of interest is discussed.

Phishing detection and response

Configure the Unified Risk Platform with Group-IB Threat Intelligence to automatically detect and takedown malicious websites automatically to protect your brand and customers. Mitigate damage caused by phishing in record time thanks

Threat actor attribution

Easily understand threat actors' behaviors, preferred methods and infrastructure with insight into their activity in the MITRE ATT&CK format. The Unified Risk Platform tracks and logs their attacks in real-time; review these insights within Group-IB Threat Intelligence.

Malware and vulnerability investigation

Use Group-IB Threat Intelligence to detonate suspicious files on the Unified Risk Platform or submit them to our reverse engineering team. Review in-depth analysis of the weaknesses targeted by malware and threat actors from the dashboard to prioritize patching.

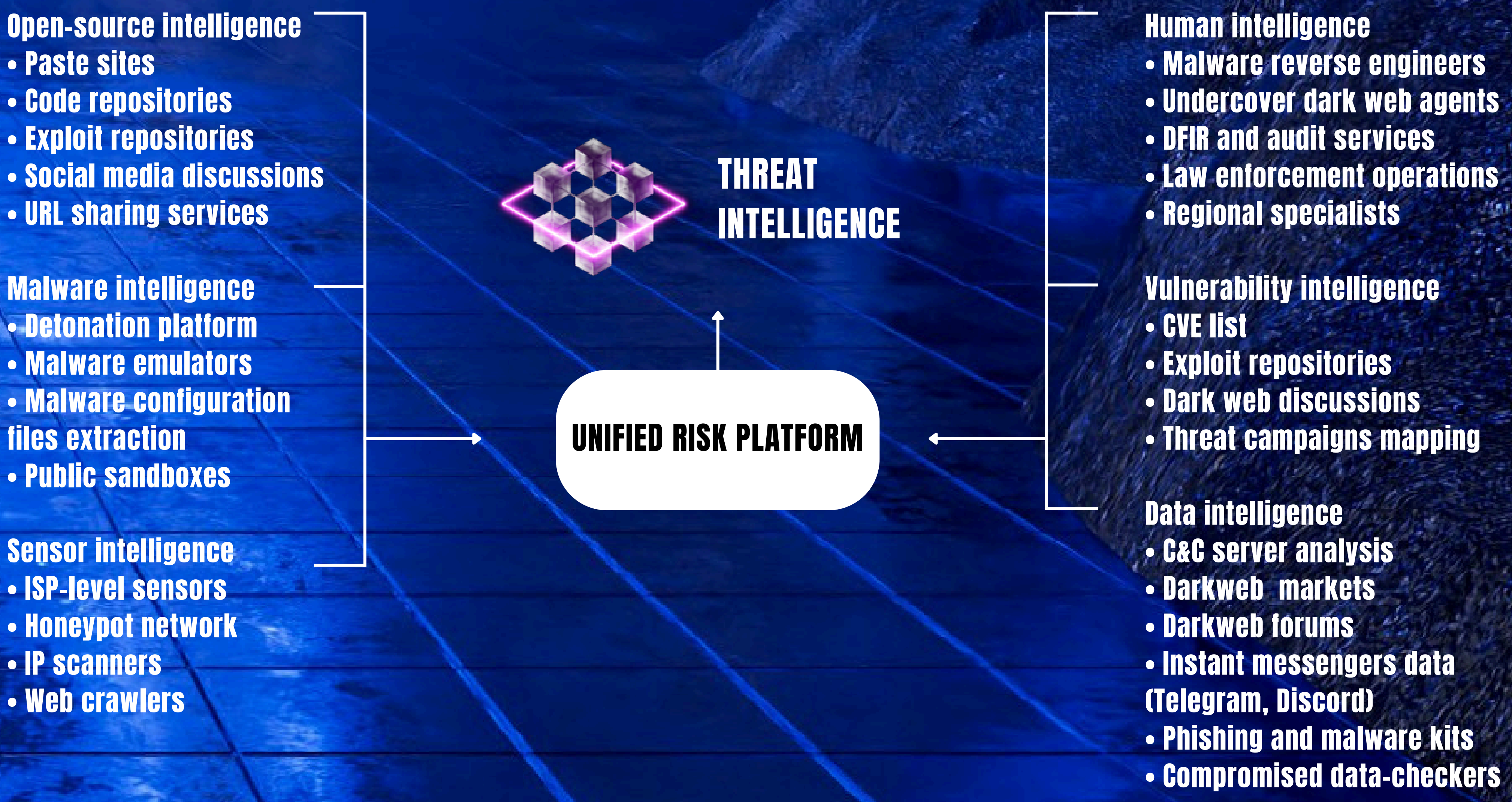
Tailored threat landscape

Track threat actors easily with a customized threat landscape dashboard, giving you a single pane of glass to monitor their attacks. Use the landscape to track actors that target you, your industry, partners, clients and those of interest.

Comprehensive integrations

Enhance your existing security ecosystem easily with out-of-the-box integrations for the Unified Risk Platform with popular SIEM, SOAR, and TIP solutions, or via API and STIX/TAXII data transfer to any tool in your security ecosystem.

Comprehensive intelligence powered by the Unified Risk Platform



Open-source intelligence
- Paste sites
- Code repositories
- Exploit repositories
- Social media discussions
- URL sharing services

Malware intelligence
- Detonation platform
- Malware emulators
- Malware configuration files extraction
- Public sandboxes

Sensor intelligence
- ISP-level sensors
- Honeypot network
- IP scanners
- Web crawlers

THREAT INTELLIGENCE

UNIFIED RISK PLATFORM

Human intelligence
- Malware reverse engineers
- Undercover dark web agents
- DFIR and audit services
- Law enforcement operations
- Regional specialists

Vulnerability intelligence
- CVE list
- Exploit repositories
- Dark web discussions
- Threat campaigns mapping

Data intelligence
- C&C server analysis
- Darkweb markets
- Darkweb forums
- Instant messengers data (Telegram, Discord)
- Phishing and malware kits
- Compromised data-checkers