GROUP-IB

WHITE PAPER

RANSOMWARE READINESS: FROM QUICK WINS TO LONG-TERM STRATEGIES

Complete guide to establishing effective security and defense strategies against ransomware with the Ransomware Readiness Framework

GROUP-IB.COM

01

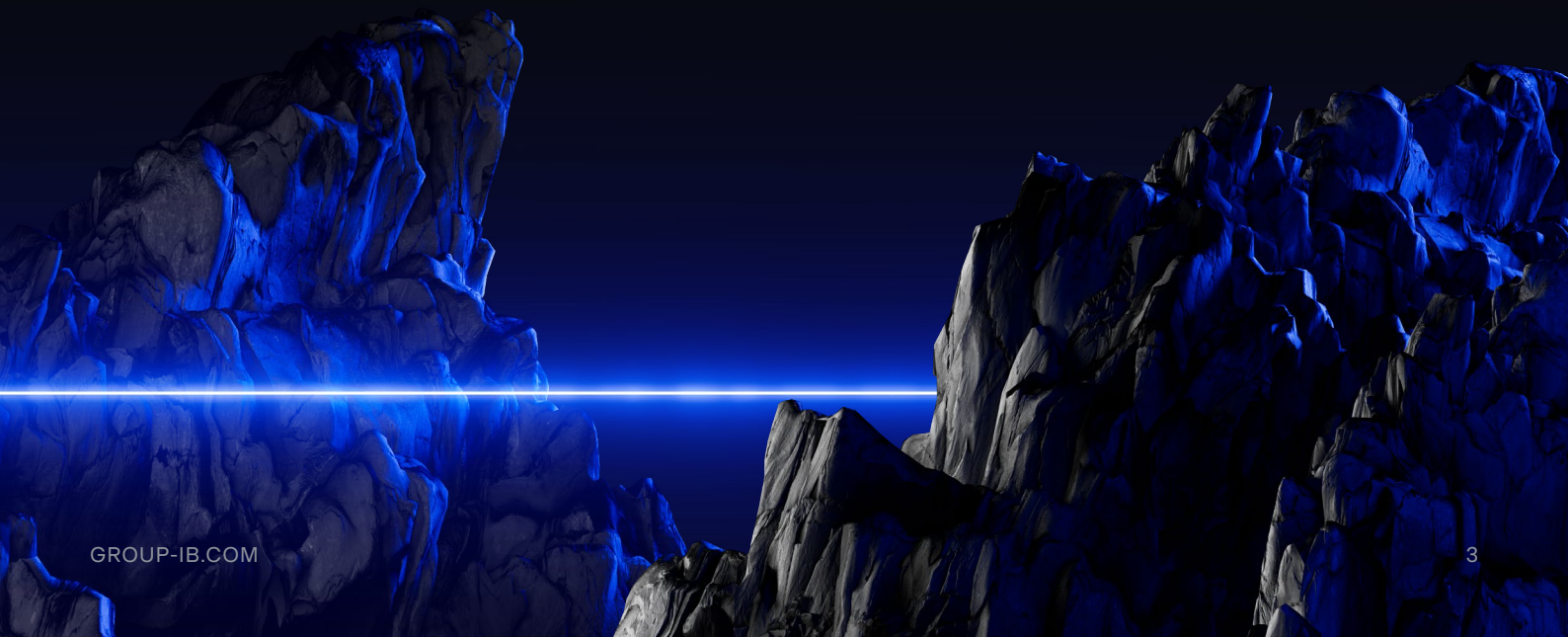
Table of contents

02 Disclaimer

Written by Group-IB specialists:

- → **Anatoly Tykushin**
  Director of Services
- → **Abdulmohsen Almuqati**
  Head of Digital Forensics and Incident Response Lab, META

1. The white paper was written by Group-IB experts without any third-party funding.
2. The white paper is for information purposes only and Group-IB is limiting its distribution. Readers are not authorized to use it for commercial purposes or any other purposes not related to training or personal non-commercial use. Group-IB grants readers the right to use the white paper worldwide by downloading, reviewing, and quoting it to the extent justified by legitimate citation, provided that the white paper itself (including a link to the copyright holder's website on which it is published) is given as the source of the quote.
3. The entire white paper is subject to copyright and protected by applicable intellectual property law. It is prohibited to copy, distribute (including by placing on websites), or use any of its content without the copyright holder's prior written consent.
4. In case of copyright infringement, Group-IB will have the right to approach a court or other state institution to protect its rights and interests and seek punishment for the offender as provided by law, including recovery of damages.



03 Introduction

"We see the threat actors evolving continuously every year. The number of cybercriminals who manage this ransomware activity and affiliate programmes continues to grow. That's why, because of high competition, they're always trying to learn new ways to earn money from new regions. The whole ecosystem of threat actors continues to develop. They don't rely on one single group, they attack simultaneously, on multiple companies."

Dmitry Volkov, Group-IB CEO

For many years, ransomware has been one of the most universal, pervasive and destructive cyberthreats targeting companies of all sizes and in all industries. Although every organization seems aware of this horribly common threat, routine incident response and investigation activities by Group-IB experts show that the situation is only getting worse. Being informed about a threat does not necessarily mean that the required steps to protect the company are being taken. While ransomware operators become increasingly devious and sophisticated, organizations continue to rely on obsolete or misconfigured security controls limited to network traffic filters, endpoint solutions, website blacklists, and attachment download restrictions. Moreover, businesses also often fall short when it comes to people, processes, and precise contingency playbooks.

Ransomware is a fast-growing cybercriminal business fueled by many factors. **The ransomware-as-a-service (RaaS)** model allows even low-skilled cybercriminals to join the industry, ultimately contributing to the surge in the number of victims. RaaS operators lease ransomware toolkits and other infrastructure (e.g., command-and-control servers, payment portals, and secure communication channels), and even technical support to hackers in exchange for splitting the proceeds from successful attacks. In 2023 the number of offers looking for partners to join RaaS programs was **1.5 times** higher than in 2022. Ransom payments made in cryptocurrency and then "cleaned" through so-called cryptomixers make it difficult to trace the perpetrators. The fact that many victims choose to pay the ransom encourages more cybercriminals to engage in this type of activity and demand increasingly higher ransoms. Another factor that will continue to bolster this market is leaks of ransomware source code, which threat actors can use to create their own malware.

Initial Access Brokers (IABs) are another threat closely related to the rising number of ransomware attacks. IABs are skilled hackers who gain access to computer systems and then sell that access on underground markets. Data sold includes access to VPN and RDP servers, corporate email accounts, remote management systems, and cloud solutions. In addition to dark web markets, threat actors can obtain compromised credentials with minimal effort on Underground Clouds of Logs. For a relatively low fee (or even no fee at all), cybercriminals can gain access to account credentials that are then leveraged as an entry point during major ransomware campaigns.

In the face of this relentless multi-vector onslaught, businesses must arm themselves with a proactive strategy that will make them capable of outmaneuvering all these threats. This guide is designed to help cybersecurity leaders (including CISOs, SOC managers, and decision-makers) equip themselves with the knowledge they need to effectively prevent and fight cybercrime and to facilitate "Lessons Learned" sessions after an incident. Our white paper is a practical step-by-step guide to both strategic and tactical planning for companies with various budgets and needs.

04

Shifts in the ransomware landscape: an escalating threat

74%

increase in ransomware attacks compared to 2022

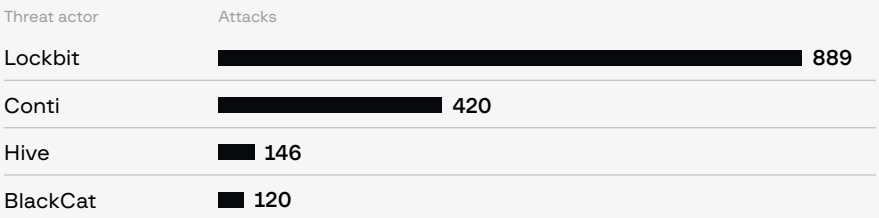
4,583

attacks published on DLSs in 2023

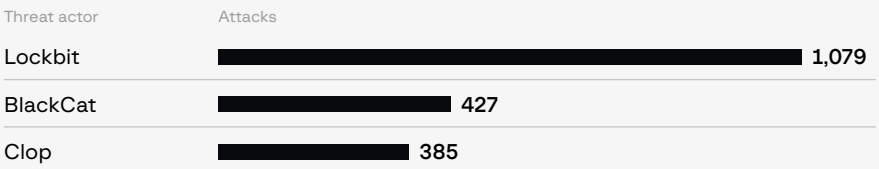
The ransomware threat continues to grow especially because ransomware attacks are so profitable, even if some players leave the market for various reasons. This section explains some elements of the ransomware landscape and discusses the top three ransomware groups.

To identify trends in ransomware attacks, Group-IB experts analyze Dedicated Leak Sites (DLSs) used by ransomware actors to publish stolen data in cases when the victim refuses to pay. Group-IB's analysis shows that in 2023 there was an overwhelming **74%** increase in ransomware attacks compared to 2022, totaling **4,583 attacks** published on DLSs. Based on data published on DLSs over the course of a year, we can see that the number of incidents in which LockBit, BackCat, and Cl0p have been involved has changed drastically. In 2023 BlackCat carried out significantly more attacks, as did LockBit, and Cl0p moved up from 9th to 3rd place in the list of most active ransomware groups, which shows that cyber threats do not stay the same for very long.

Active ransomware groups in H2 2021 - H1 2022



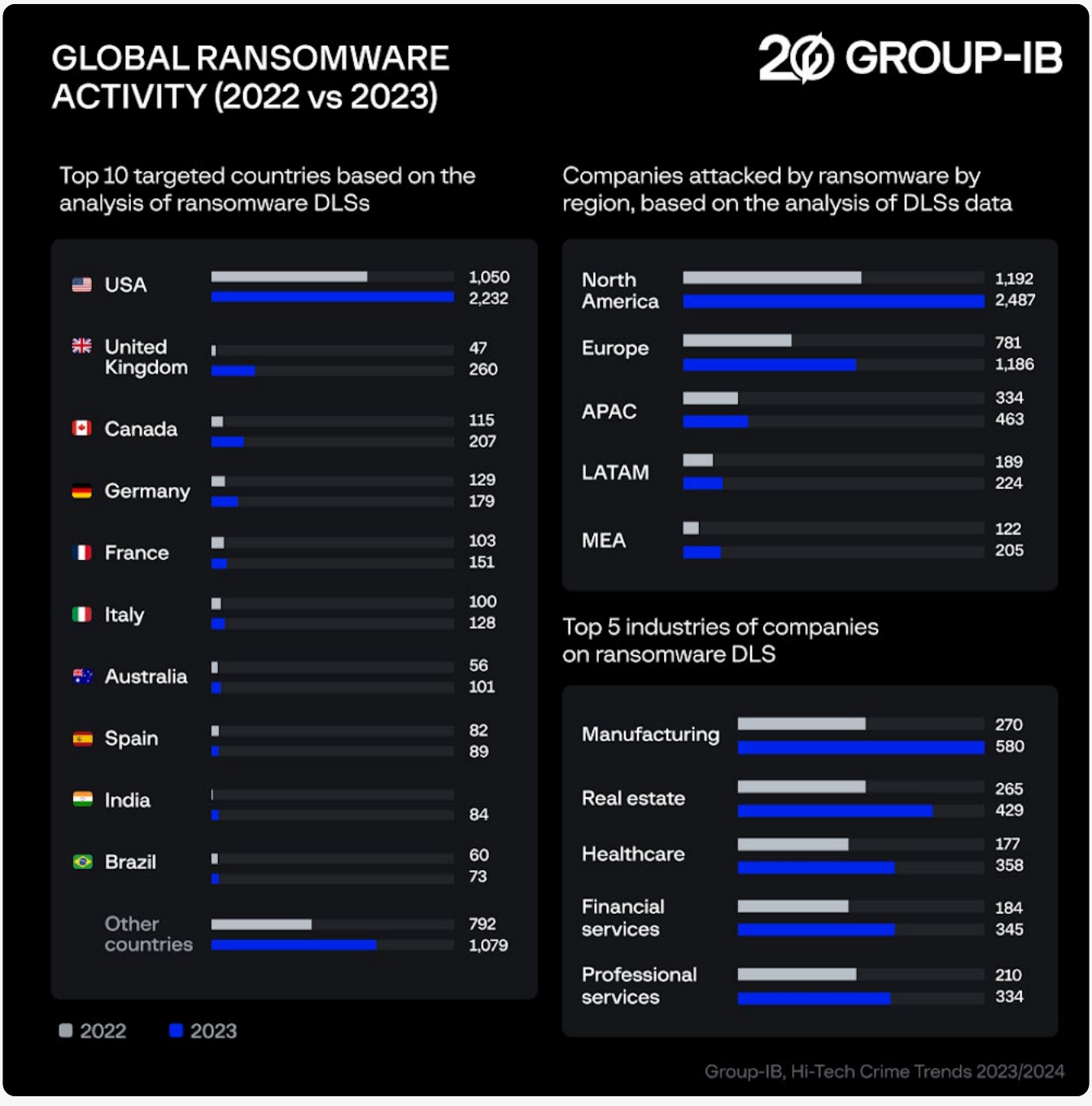
Active ransomware groups published data on DLSs in 2023



Conti stopped operating in 2022 after an internal conflict. In February 2024, the FBI reported that it had seized LockBit's infrastructure. Meanwhile, BlackCat pulled an exit scam — it tried to shut down its operations and run off with its affiliates' money, pretending that the FBI had seized its website and infrastructure. Despite all this, the affiliates of these big groups are most likely still engaged in ransomware attacks and have partnered up with other Ransomware-as-a-Service (RaaS) programs. The events highlight how quickly the threat landscape evolves and escalates, which emphasizes the critical need to take proactive action.

Get the full report →

Our **reports on the ransomware landscape** present alarming statistics that should not be underestimated. Ransomware attacks have increased in number significantly throughout the world. With an attack dwell time of less than two hours from initial access to impact, organizations must learn how to handle rapid and stealthy intrusions. Not far behind in terms of attack numbers are ransomware families with auto-spreading capabilities such as BlackCat, LockBit, Qilin, and BabLock. BlackCat and Qilin have built-in PsExec, while LockBit members have implemented the PsExec functionality themselves using Admin Shares. BabLock, meanwhile, uses PowerShell scripts or auto-deploys across virtual infrastructure via VMWare vCenter. Although deploying ransomware requires privileged access, threat actors do not struggle to compromise administrative credentials.



Group-IB strongly advises organizations that fall victim to ransomware against paying the ransom

Another challenge that companies face is restoring the affected data while recovery mechanisms are restricted. In most cases, data cannot be decrypted without the original encryption tool. While the most reliable way of securing your digital assets remains protecting your network, email and endpoints in a comprehensive way, combined with using practices that foster security incident preparedness, using backup copies is the most popular way of ensuring that data is restored if it is encrypted. Nevertheless, even backups do not provide a guarantee that data will be recovered after an attack.

Group-IB strongly advises organizations that fall victim to ransomware against paying the ransom, which aligns with global best practices. Alarmingly, **83% of ransomware cases involve data exfiltration**, further amplifying the multifaceted threats posed by these ransomware attacks. When an organization has their data exfiltrated, they find themselves under enormous pressure to pay the ransom. Even if they do, however, there is no guarantee that they will be able to recover their systems or have their data removed from DLSs. Paying the ransom also encourages cybercriminals further, as any victim who pays the ransom earns the reputation of an easy mark. If you fall victim to a ransomware attack, the only advisable course of action is to hire incident response professionals who will help contain and mitigate the incident. That said, preventing attacks and staying ahead of ransomware operators requires revisiting your security strategy entirely and taking proactive cybersecurity measures.

05

Overview of impact on businesses

42%+

of clients claimed Data Loss

40%

reported Business Downtime

30%+

reported Lost customers

Significant stress to the SOC team

24x7 work mode, managing management expectations, fighting against cybercrime and will to sleep

Negative public exposure

Hacktivists, Ransomware make some noise on social media claiming successful attacks against their victims

Confidential information disclosure

Ransomware affiliates will publish bulk data on their Data Leak Site. Nation-state groups will reuse the leaked data for their own needs.

Regulatory fines

Incident Response must be performed by a trusted third-party cybersecurity provider. The investigation results will discover any violation committed prior to the attack. This should be disclosed with Regulatory authorities and may lead to a fine.

Ransomware attacks can have a significant impact on businesses. They can damage a company's reputation as a result of negative public exposure or leaks of confidential information. Data leaks and infrastructure compromise mean that regulatory authorities become involved, and the situation can escalate. Compromise assessments may need to be conducted for all third parties whose infrastructure is integrated with that of the victim. Ransomware attacks also inflict considerable stress on SOCs (Security Operations Centers) due to potential operational disruptions and fines.

Furthermore, downtime caused by ransomware attacks can halt critical business operations, resulting in lost productivity and revenue. The costs associated with remediation efforts (including ransom payments, cybersecurity enhancements, and data recovery) can also put a huge strain on financial resources. Ransoms are based on the volume of encrypted and exfiltrated data, as well as on the size and annual revenue of the victim. Therefore, the larger the amount of data affected and the size of the business, the higher the ransom demanded. Many threat actors have adopted the approach to look up information available to the general public (i.e., ZoomInfo) and leaked documents to find out the company's annual revenue size. This is why one ransomware group demanded USD 50 million from an oil and gas company but only USD 100,000 from a telecom operator. A common strategy is not to exceed 5–10% of the victim's annual revenue.

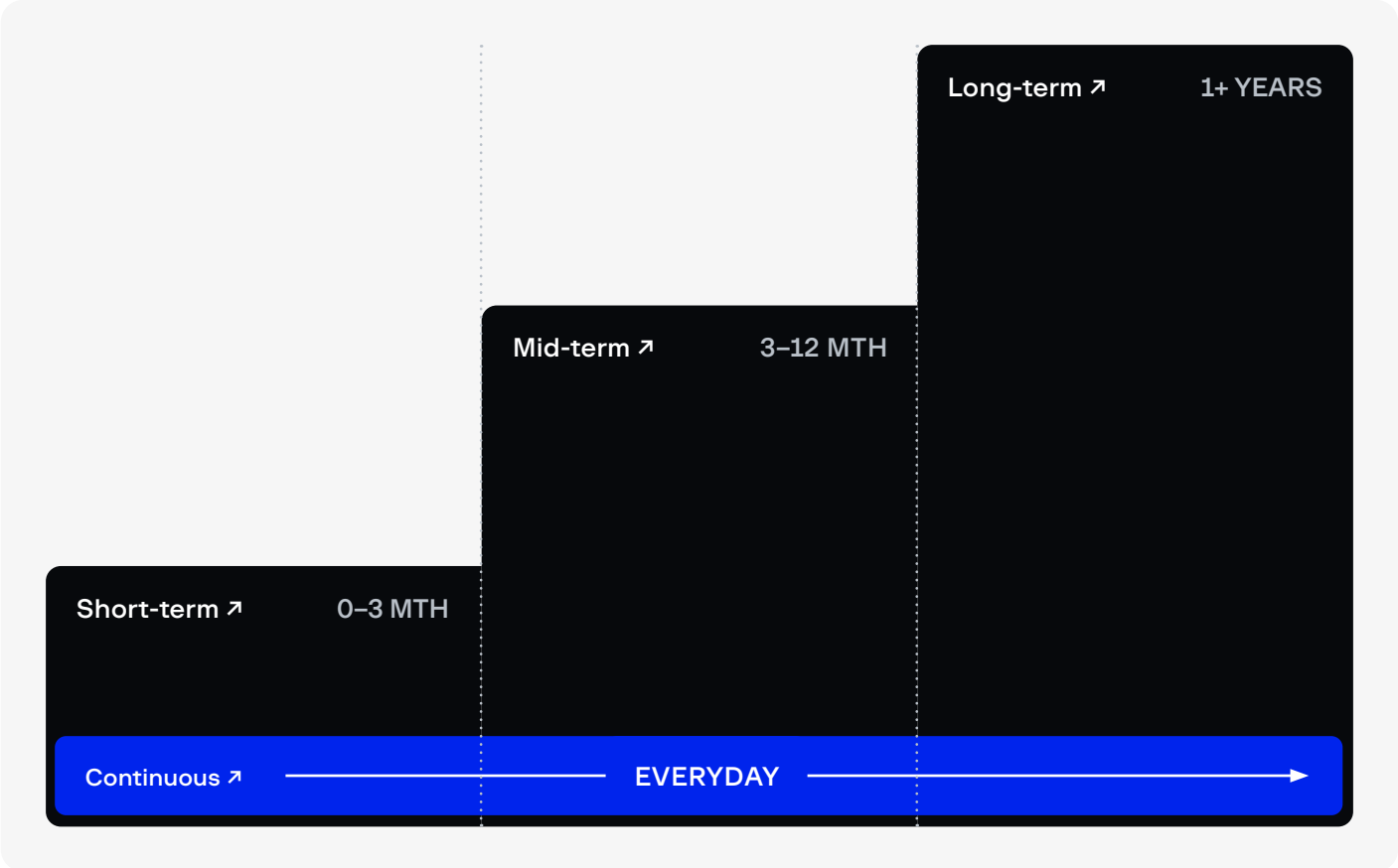
Organizations should assess and mitigate these impacts carefully to protect their operations and reputation.

06

Ransomware readiness framework. Key steps to building a resilient cybersecurity posture

Group-IB experts have developed a framework to help organizations prioritize investments in cybersecurity so that they can address the evolving threat landscape in a targeted manner and enhance their defenses. Our framework is grounded in industry best practices and powered by insights from **thousands of incident response cases** Group-IB experts have worked on. Ransomware attacks are complex threats that target organizations at several levels (including people, processes and architecture) at the same time and they cannot be countered through one-time efforts or technologies alone.

Group-IB offers a multi-stage framework with a practical and feasible action plan ready to be implemented. The strategies cover the entire ransomware kill chain and are broken down by implementation timeline into **short-term**, **mid-term**, **long-term**, and **continuous** strategies. They are also divided into three domains: **people**, **processes** and **technology**, and the technology domain is split into Endpoint protection, Data protection, Identity protection, and Network protection. Group-IB experts recommend choosing the appropriate strategy based on your organization's needs and objectives, available resources, and timeline requirements.



Short-term (0–3 months)

This strategy provides fast and efficient “wins” and quick gap assessments.

People

1. **Resource gaps**
    a. Define missing roles and full-time equivalents. Identify hiring needs and estimate budgets.
    b. Perform market research to find a representative vendor to delegate SOC services.
    c. **Define the model for SOC Core and SOC Advanced practices with the following guide** (in-house or delegated).

2. **Skills gaps**
    a. Assess the skills of the existing team (evaluation test) to highlight any missing domains.
    b. Develop a **training plan** for each role and prepare a budget proposal.
    c. Consider subscribing to an **Incident Response Retainer** from a trusted vendor (recommended by Gartner, Forrester, IDC, Frost & Sullivan, etc.).

Technology

Endpoint protection

Assess gaps in endpoint security controls. Evaluate Endpoint Detection & Response (EDRs) and Antivirus (AV) defenses to screen for:

- Lack of coverage
- Misconfigurations
- Outdated agent software versions
- Outdated detection logic (behavior analysis, heuristic detection or signature-based detection databases)
- Weak detection and prevention logic
- Architecture issues resulting in delayed incident detection

Data protection

- **Review and update access controls**. Ensure that employees have access only to the information and systems they need to perform their roles. This can often be refined through existing identity and access management systems.

- **Review backup architecture**. Implement or review your data backup strategy to ensure critical data is being backed up regularly. This includes backup policies, backup job monitoring routine, and backup protection mechanisms. Doing so can be a "quick win", especially with cloud-based backup solutions that offer rapid deployment. Any gaps found should be addressed and shared with senior management for budgetary approvals in case significant investments are needed.
- **Review Data Loss Prevention (DLP) security control (if used)**. The goal is to identify any gaps in detecting unauthorized or holistic access to key assets (confidential and/or classified data). In some cases, eliminating the gaps could require significant investments (in terms of both time and materials), which means that any decisions should be a subject to budgetary planning for the next fiscal year.

Identity protection

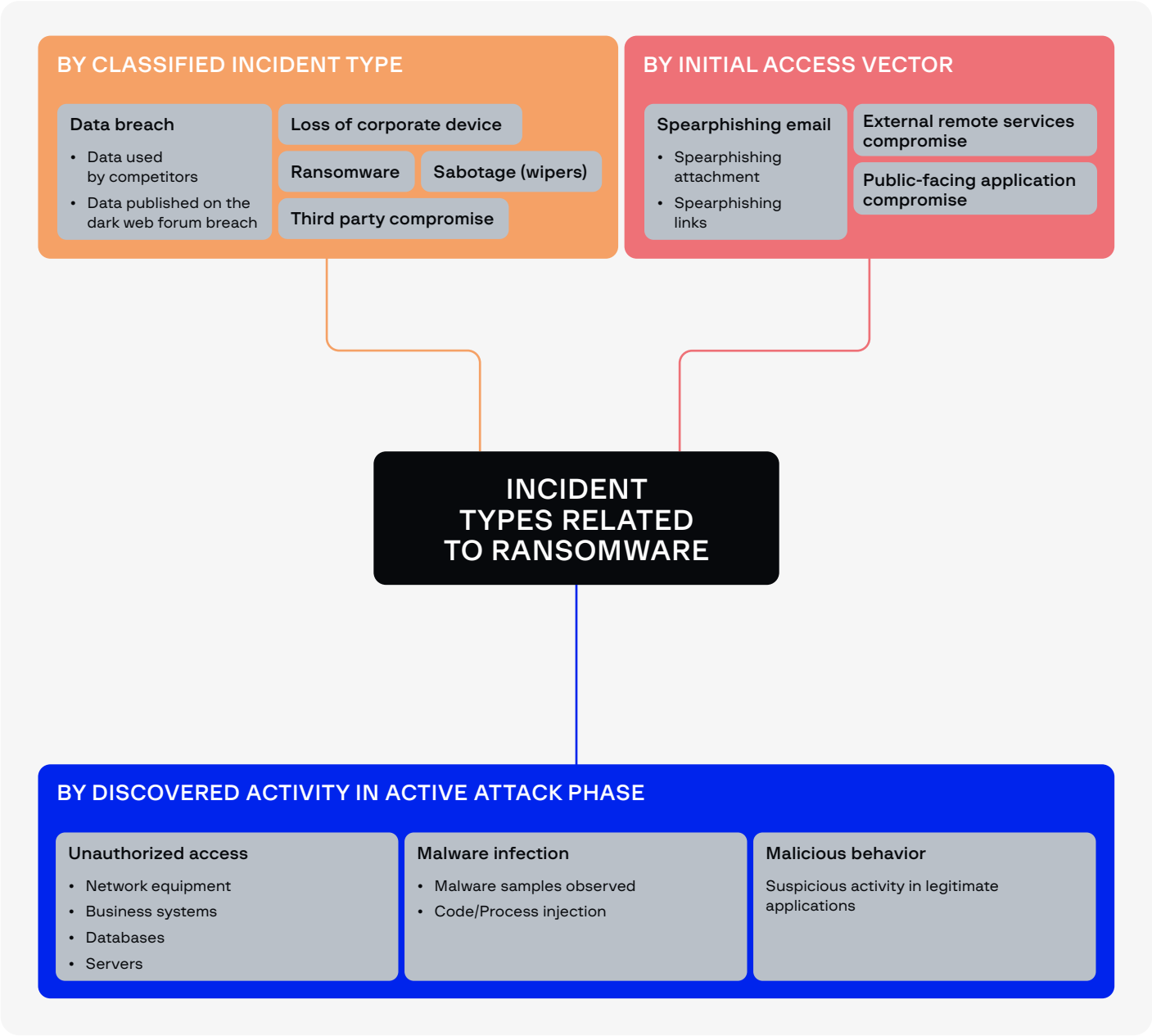
- **Enforce strong password policies and multi-factor authentication (MFA)** for uncovered segments, controls and user groups. If this step requires significant resources or long-term architecture changes, make it part of your long-term strategic goals.
- **Run a cyber threat exposure assessment** (encompassing compromises and leaks) to identify any compromised authentication details being sold on the dark web and to pull any information from initial access Trojans and infostealers. Doing so should reset all compromised user accounts and identities.

Network protection

- **Review your infrastructure architecture** (making sure to cover network segmentation) to ensure the proper visibility of Next-Generation Firewall (NGFW) and **Network Detection & Response (NDR) solutions** for east-west and north-south traffic.
- **Use an Attack Surface Management solution** (if you do not already) to identify any threats and vulnerabilities in the infrastructure, to prioritize issues that require remediation and to discover unmanaged assets and other hidden risks.
- **Perform an assessment of NGFW and NDR control gaps** in terms of routine detection, timely updates from **Cyber Threat Intelligence** sources and building the baseline for traffic, including peak usage.

Process

- **Assess your readiness to respond to ransomware incidents** to identify any gaps in the overall preparedness of your processes and playbooks relating to ransomware attacks and other related incidents such as spear-phishing attacks, exploitation of public-facing applications and external remote services, malware infections, and suspicious network/endpoint behavior (see figure below).



A readiness analysis should cover the following stages:

- **Detect and verify** (including escalations from Managed Detection & Response or Managed SOC vendors, external **Threat Intelligence vendors**)
- **Analyze and contain**
- **Escalate internally** (to business owner, crisis committee) **and externally** (to third-parties, regulatory authorities, media)
- Eradicate and recover (post-incident activities)

- **Perform tabletop exercises** with the technical leadership team and the senior management using ransomware scenarios to test the effectiveness of communication, escalation, crisis management, collaboration, and planning.
- **Perform drills** with technical teams to test their capabilities and skill set in case of a ransomware attack. The scope of cyber drills could also include testing the escalation process to third-party experts.

Mid-term (3–12 months)

During this stage, organizations can significantly step up their technical measures of resisting ransomware attacks, develop the necessary hard skills for cybersecurity and IT teams, raise awareness among employees about real-world ransomware attacks, and improve their incident response processes.

People

1. **Resource gaps**
    - Approve the hiring budget, prepare job descriptions, and initiate the hiring process.
    - Prepare the onboarding process and headcount planning.

2. **Skills gaps**
    - Approve the training plan for existing cybersecurity teams based on a hard skills assessment and allocate budgets and time slots for training to avoid disruptions in continuous cybersecurity operations.
    - Plan and attend training sessions based on real-life use cases instead of using a traditional academic approach for your existing team and new employees. **Break down the SOC services into Core and Advanced** and agree with a representative vendor on knowledge transfer sessions or a short-term internship program (up to 1 month, relating to threat intelligence consumption, incident response, Windows/Linux digital forensics, network forensics, malware analysis) and/or a SOC Tier 1–2 **training program**.
    - Attend workshops for SOC managers and team leads related to incident response preparedness.
    - Attend workshops relevant for CISOs on **incident response preparedness** and cybersecurity architecture.
    - Conduct Purple Teaming exercises using ransomware attack scenarios to verify your organization's ability to detect and respond to real-world attacks under the supervision of skilled and experienced incident response vendors. If your team has not yet experienced such type of engagements involving mature **Red Teaming** activities, Group-IB strongly recommends choosing a simplified approach to emulating TTPs in a test environment covered with existing security controls without defense evasion techniques and with strongly defined attack goals.
    - For organizations that have already conducted Red Teaming in the past, we recommend running another Red Teaming service involving the most sophisticated TTPs used by Big Game Hunting ransomware affiliates.
    - Plan an awareness session for employees with non-technical roles to boost your company's overall digital hygiene and to teach employees how to recognize social engineering attacks.

Technology

Endpoint protection

- **Assessment of gaps in business email protection** to test against a maximum number of potential scenarios used by Initial Access Brokers (IABs) and ransomware affiliates who want to infect end-user machines.
- **Breach and attack simulation exercise** to test your company's endpoint protection solution's ability to detect TTPs used by ransomware affiliates.

Data protection

- **Upgrade backup architecture**. Make the most of backup and recovery solutions to ensure that all critical information and systems are backed up securely and can be reverted to any point in time.
- **Organize workshops on data governance**. These will help your employees understand how to categorize data, how to identify where in the infrastructure it resides, and how to control the flow of sensitive information and personal data. This approach will provide a clear structure for data location, data usage policies, and defenses to prevent indiscriminate data access, collection and exfiltration outside the protected perimeter.
- **Update data classification policies** (if applicable). Establish clear data classification categories (e.g., public, internal, confidential) that dictate the level of protection required. This process helps to prioritize security measures based on how sensitive the data is.
- **Upgrade data leak prevention architecture**. Ensure that your DLP solution (if you have one) covers all the data points, monitors all possible data flows, and detects any deviations from data transmission and usage.
- **Improve visibility**. Enable the option that backup solution audit logs can be forwarded to SIEM for continuous monitoring by the SOC team.
- **Test the backup infrastructure**. Conduct **Red Teaming** exercises with the goal to inhibit recovery.

Identity protection

- **Introduce identity protection solutions** that help to detect and prevent identity-driven breaches.
- **Upgrade identity management**. Apply any necessary configuration changes to Privilege Access Management (PAM) solutions in line with the discovered gaps.
- **Improve visibility**. Forward PAM and Identity and Access Management (IAM) solution logs to SIEM for permanent monitoring by the SOC team.

Network protection

Upgrade network security. Implement network segmentation after the infrastructure architecture review to limit the threat actor's ability to move laterally within your network if a ransomware attack occurs.

Process

- **Increase your readiness to respond to ransomware incidents**. Improve or develop incident response playbooks for ransomware-related scenarios based on a previously conducted workshop on assessing ransomware readiness gaps. Develop a communication matrix and internal escalation plans to be used in case of cybersecurity incidents (e.g., involve business leaders, owners, senior management or trigger a crisis management committee). Improve or develop disaster recovery plans (DRP) and business continuity plans (BCP).
- **Test the Disaster Recovery and Business Continuity Plans**. Conduct cyber drills for selected business factions so that your entire team is prepared in case of ransomware attacks.
- **Enhance data privacy measures**. Review and strengthen policies related to data privacy to ensure compliance with relevant regulations (e.g., GDPR, CCPA). This may involve updating privacy notices, consent mechanisms, and data processing agreements.
- **Update data classification policies**. Establish clear data classification categories (e.g., public, internal, confidential, secret) that dictate the level of protection required for different types of data. This process helps to prioritize security measures based on how sensitive the data is.
- **Create a Data Governance Committee**. If not already in place, form a cross-functional team responsible for overseeing data governance policies, compliance, and strategy. The goal of this committee is to ensure that data governance is in line with business objectives and regulatory requirements.

Long-term (1+ years)

This strategy involves conducting advanced training, deploying state-of-the-art solutions and practices to ensure visibility into the infrastructure, identifying threats before they can cause any damage, and mitigating threats through effective network segmentation and vulnerability management programs.

People

- **Plan, organize and facilitate custom training programs** targeting all necessary **SOC Core and Advanced capabilities**, which require tailored education materials that cover all domains related to cybersecurity: secure software development lifecycle (SSDLC), DevOps, SecDevOps, and cyber threat intelligence programs.
- **Teach relevant threat hunting competencies** to SOC team members who have extensive experience in incident analysis.

- **Reach a milestone** where all employees and board members have completed cybersecurity awareness workshops and put the lessons learned into practice: they recognize and report phishing, use strong passwords, apply multi-factor authentication, update software regularly, and browse the web safely.
- **Conduct data governance training**. Organize training sessions for employees to help them understand the importance of data governance and their roles in maintaining data security and privacy. Such training helps to foster a culture of data responsibility throughout the organization.

Technology

Endpoint protection

- Choose, test and deploy (or replace) an **Endpoint Detection and Response** solution in line with best practices and that has all the detection, response and handling capabilities required for an efficient incident response process. Involve unbiased and trusted third-party consultants during the testing phase to verify whether the solution is suitable for solving critically important goals as regards securing your network environment.
- Achieve more than 95% coverage with endpoint security controls for critical infrastructure, servers and endpoints in your organization.
- Implement a SIEM solution (if you do not have one), ensure that it maintains 100% visibility across the infrastructure, forward all required data sources from endpoints and security controls, and enforce tried-and-tested log retention policies to create a unified ecosystem of security controls.
- Upgrade your infrastructure and decommission endpoints with unsupported OS versions.

Data protection

- Implement encryption-at-rest practices for confidential and other classified information.
- Finish implementing a DLP solution (if you did not have one before) to cover data points and data transfer and exchange channels.
- Implement robust backup for the organization's architecture, filling any identified gaps.

Identity protection

- Implement Privileged Access Management (PAM) solutions to restrict access to critical systems and data.
- Implement Identity and Access Management solutions to centralize controls of privileged and service accounts in case they are compromised.
- Forward PAM, IAM, and UEBA logs to the SIEM solution for monitoring by the SOC team.

Network protection

- **Achieve "zero-trust" security architecture**: Work towards implementing a zero-trust security model, where by default no entity from inside or outside the network is trusted, and the identity of anyone trying to access network resources must be verified. This involves a long-term strategy for deploying identity verification, microsegmentation, and least-privilege access controls across all endpoints.
- Finish network segmentation, which requires significant resources and cross-business unit efforts.
- Implement an **Attack Surface Management** solution capable of assessing third-party risks.
- Conduct an internal **Red Teaming** scenario in which the red team can move to critical isolated segments and bypass security controls, impair defenses, etc.

Process

- **Develop comprehensive endpoint security policies**: Create detailed policies that cover all aspects of endpoint security, including device management, access controls, encryption standards, and incident response. This involves continuous evaluation and updates to adapt to new threats and technologies.
- **Implement an incident response platform or SOAR systems**.
- **Create a knowledge base** to keep a record of all cybersecurity incidents that the organization has ever faced.
- **Develop ransomware-related playbooks and runbooks** to leverage automation and orchestration tools and to streamline security workflows (such as patch management, vulnerability scans, and incident response).
- **Create a vulnerability management program** bearing in mind the latest trends in evaluating the severity of vulnerabilities, based on a scoring system encompassing data analytics, threat intelligence, attack surface, and asset information.
- **Develop data classification policies**: Establish clear data classification categories (e.g., public, internal, confidential, secret) that dictate the level of protection required for different types of data. This process helps to prioritize security measures based on how sensitive the data is.
- **Carry out third-party risk assessments** based on the implemented Attack Surface Management solution.

Continuous

Given that ransomware keeps getting more and more sophisticated, your resilience strategy must also evolve. Only by committing to ongoing cybersecurity practices can organizations protect themselves against ransomware attacks and secure critical systems and data against potential harm.

People

- Cybersecurity teams should be current on the latest ransomware trends, tools, techniques, and procedures (TTPs) used by threat actors. Equally, they should be familiar with relevant mitigation strategies. Both can be achieved by reading public ransomware incident response reports, by following cybersecurity blogs, and by leveraging open-source threat intelligence and subscribing to commercial threat intelligence feeds.
- **Simulate phishing exercises**. Periodically run simulated phishing campaigns to test employees' awareness and preparedness against social engineering attacks, which are common vectors for ransomware.
- **Promote an effective security culture**. Encourage an effective culture of security within the organization so that employees feel responsible for maintaining a high level of cybersecurity and are comfortable reporting suspicious activities without fear of repercussion.
- **Conduct periodic Purple Teaming exercises** that enhance an organization's defense against ransomware and other cyber threats by blending offensive tactics used by red teams with defensive strategies used by blue teams. This collaborative approach aims to improve an organization's overall cybersecurity posture through a cycle of testing, feedback, and improvement.

Technology

- **Application whitelisting**. Implement and continuously review application whitelisting to ensure that only approved software can run on network devices, thereby reducing the risk of ransomware being executed within your network.
- **Cyber threat intelligence**: Use threat intelligence platforms to stay informed about emerging ransomware threats and tactics. With the knowledge gained, you will be able to adjust your defense mechanisms in a proactive way.
- **Develop use cases on threat detection**: continuously assess and test your security controls (defenses) to ensure that you are able to detect and prevent threats by applying customized payloads crafted by industry experts.

Process

- **Incident response planning**. Regularly update your incident response plan, including specific procedures for responding to ransomware attacks. This plan should be tested and refined through tabletop exercises and drills.
- **Conduct regular security audits and assessments**. Establish a schedule for regular **security audits and vulnerability assessments** on endpoint devices to identify and remediate any weaknesses. This should include penetration testing to evaluate the effectiveness of endpoint defenses.
- **Backup and recovery procedures**. Maintain robust backup and recovery procedures. Regularly test backups to ensure that they can be restored quickly and effectively if a ransomware attack happens.
- **Plan for secure endpoint lifecycle management**. Develop strategies for the entire lifecycle of endpoint devices, from secure deployment and regular maintenance to safe decommissioning. This includes ensuring that data is securely erased and devices are properly disposed of or recycled.
- **Regularly review and update ransomware prevention strategies** based on annual/half-year risk assessments. The review and updates should reflect changes in technology, regulations and the cyber threat landscape.
- **Conduct regular SOC team metrics and KPI reviews** to measure the effectiveness of security operations.
- **Conduct a regular retrospective review of alerts** (10–15% of the most serious alerts), hiring trusted third-party experts to verify that the actions taken by the SOC team were correct and appropriate.
- **Perform an annual compromise assessment** to uncover hidden or unresolved breaches and to identify any gaps in the people, processes and technology domains.
- **Run regular (monthly or quarterly) threat hunting operations** to ensure that no threats remain undetected.
- **Patch management**: Follow a systematic process for regularly updating and patching software and systems according to the Vulnerability Management program. This reduces the attack surface by eliminating known vulnerabilities that ransomware operators could exploit.

07

Put effective prevention strategies into action with Group-IB

Capture the full pack of ransomware prevention and mitigation solutions tailored to your needs and targeting all points of potential attack

Solutions for Ransomware Protection →

While companies may be prepared to mitigate numerous attack vectors, when ransomware actually strikes, organizations are often left perplexed. When faced with an unpredictable and devastating threat like ransomware, a trustworthy partner to rely on is worth its weight in gold. With a two-decade track record in combating cybercrime together with INTERPOL, Europol, AFRIPOL and other law enforcement agencies, we have tackled and defeated ransomware head-on. Group-IB has taken part in some notable anti-ransomware operations, including **Operation Cyclone** and **Operation Synergia** — which have led to ransomware criminals being arrested and their malicious infrastructure being taken down. With our experience and proven solutions by your side, you can face ransomware challenges with confidence. Below, we describe but a few essential tools that will help you build an effective defense posture:

Any bulletproof strategy starts with assessing what's already in place. Group-IB's **Incident Response Readiness Assessment** helps to thoroughly check whether you are prepared for ransomware attacks. As part of the service, we ensure that your infrastructure includes all the necessary and properly configured tools, that your processes are up-to-date and in line with current cybersecurity trends, and that your team is armed with all the skills and knowledge you could need. For in-depth infrastructure analysis and detection of existing compromises, you can count on Group-IB's **Compromise Assessment**. This service helps uncover and analyze advanced threats such as APTs, ransomware, espionage that often evade the detection radars of conventional security solutions.

For end-to-end risk management, our **Incident Response Retainer** will give you confidence from day one with world-renowned experts at your disposal — round the clock and ready to assist with any incidents. The major benefit is that you can repurpose the service for many other security services provided by Group-IB experts. Group-IB's Incident Response Retainer services have received a seal of approval from major analytical agencies, including Forrester and Gartner.

Group-IB's **Managed XDR (Extended Detection and Response)** is an essential part of our incident response activities. With its advanced threat monitoring capabilities, MXDR has proven effective in detecting and isolating ransomware threats and in minimizing their spread and impact. The solution provides 24/7 monitoring of all instances, helping to rapidly identifying and responding to ransomware indicators of compromise. It uses advanced analytics that could indicate a ransomware attack, thereby ensuring rapid mitigation.

The most effective shield against ransomware is to counter ransomware deployment in a proactive manner. Group-IB's **Threat Intelligence** provides visibility into the evolving ransomware landscape relevant to your organization and industry. It helps to track active ransomware groups and any changes to their tactics, tools, and procedures. Our intelligence will prepare your team to ward off ransomware attacks before they infiltrate your network and cause irreversible damage.

In most ransomware attacks, human error and lack of skills or expertise are key factors in determining whether the threat actors succeed or not. The most effective form of defense against them is training your cybersecurity teams and non-technical employees. **Group-IB's training courses** will empower your team with the skills to identify and mitigate ransomware threats proactively. Our courses enhance the ability to understand TTPs (tactics, techniques, and procedures) used by attackers and to raise overall awareness of cyberattacks, thereby improving the organization's resilience and significantly reducing the risk that an attack will be successful.

Ransomware attacks are usually insidious and multifaceted — why limit yourself to one approach? Group-IB offers a full pack of ransomware prevention and mitigation **solutions** tailored to your needs and targeting all points of attack. **Talk to our experts** and find the best option for your company.

08

Estimate your company's readiness to thwart ransomware campaigns with Group-IB

Take off where incident response readiness starts and make sure your business is ready to face the trickiest attacks and incidents.

Infrastructure is ready

Your company can be considered as safe if it disposes of all the necessary technical setup to defend against an extremely wide range of threats.

Processes are steady

Your level of security rises up if all Incident Response guidelines, instructions are available, up-to-date, and based on current information security trends.

Team is prepared to go

Your business security also depends on a proper structure and accountability among teams put in place: always ready to act and repel any attack.

What does our Readiness Ladder involve?

Group-IB experts assess how ready your organization is to respond to attacks of any level of complexity and defend against a wide range of threats. Our unique methodology is based on experience gained from handling thousands of incident response and investigation cases.

#	Readlines level	Percentage range %	Dangerous
1	Highly prepared	88 - 100+	
2	Well prepared	75 - 87	
3	Basic preparedness	60 - 75	
4	Less prepared	40 - 60	
5	Unprepared	< 40	

You will get not just a report but the readiness to repel cyber attack

Integrated assessment of key elements — technology, team, processes

Actionable and applicable response plan and understanding of procedures

Practical recommendations and roadmap to implement improvements

Clear scenarios to ensure effective teamwork between different departments if an incident occurs

Incident response training to arm your team with specialized skills and knowledge

Confident team that takes full advantage of company's own security systems and processes

---

From theory to practice: Secure your business with a full range of ransomware resilience solutions

Get in touch with Group-IB experts →

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