GROUP-IB

CYBERSECURITY ULTIMATE ASSESSMENT GUIDE

PART 1. ASSESSMENT COMPASS

Table of contents

Introduction

“There is nothing more constant than change" – Heraclitus, 535 BC

The above timeless truth attributed to Heraclitus is especially relevant in the realm of cybersecurity, where the threat landscape keeps evolving at an alarming pace. Vendors introduce new technologies, cybercriminals refine their tactics, and regulators impose new compliance requirements. In this dynamic environment, your cybersecurity posture is in a perpetual state of flux and must keep being evaluated and adapted.
For cybersecurity teams, this relentless cycle often feels like a race against time, with limited resources and ever-growing responsibilities.

When it’s impossible to address every single issue, it is critical to identify and prioritize the most impactful tasks to strengthen your security posture. Regular security assessments play a vital role in this process, providing a clear picture of where to focus your efforts.

But how can you effectively measure your current security level?

For senior executives and board members, the question is often a direct one: “How secure are we?” While it may seem straightforward, the reality is far more complex. There is no simple response like “good” or “90% safe”. Instead, such inquiries spark deeper discussions. Are we protected across all critical domains? Can we withstand advanced persistent threats? How effectively can we detect and respond to incidents? Does our security posture align with compliance requirements and industry standards? Without clear insights, answers to these questions remain elusive. And yet many organizations fail to conduct proper assessments or adopt insights gained to strengthen their defenses.

The critical role of cybersecurity assessments

Security assessments are much more than formal checklists. They are cornerstones for evaluating an organization’s security maturity. They provide the clarity needed to address the gaps and answer the challenging questions mentioned above. However, with a plethora of assessments available — from penetration tests and vulnerability scans to red teaming and compliance audits — choosing the right one can feel overwhelming. Without a clear strategy, companies risk wasting budgets, overloading teams, and overlooking critical vulnerabilities.

This e-guide, crafted by Group-IB’s seasoned assessment practitioners, equips **SOC managers, CISOs, and other security experts and leaders** with the knowledge required to navigate the complexities of modern assessments. It delves into the various types of assessments, their use cases, key advantages and disadvantages, optimal cadence, and practical strategies to evaluate one’s security posture.

Written by Group-IB specialists

Alexander Asmolov
Head of Cyber Defence Consulting

A roadmap for resilience

Security leaders often grapple with budget limitations and resource shortages, which hinder their ability to assess risks in a comprehensive way. This guide helps to overcome such challenges by providing a clear roadmap for selecting the right assessments to optimize resources and strengthen outcomes.

Whether your goal is to validate defenses against targeted attacks, prepare for compliance audits, or benchmark your security posture against peers, our guide offers actionable insights tailored to your organization's needs.

We are releasing this guide as a series of e-books that will cover key cybersecurity assessments in detail. This first chapter serves as a starting point, offering an overview of assessment types and including **a practical matrix titled Cybersecurity Assessment Compass to help you identify the most suitable one for your organization.**

> As the saying goes, "If you don't know where you are, you don't know where to go." Let this e-guide be your trusted roadmap to a stronger, more resilient security posture.

Assessments as part of SOC and cybersecurity management

Group-IB's expertise stems from not only our experience in creating cutting-edge cybersecurity, brand protection, and anti-fraud technologies, but also from practical know-how. Group-IB's consulting services have been developed based on many years of consulting and security assessment work combined with CERT-GIB's collaboration with CERTs worldwide. In addition, working with law enforcement agencies such as INTERPOL, Europol and AFRIPOL has been fueling Group-IB's investigation strategies, incident response skills and threat intelligence expertise for over twenty years.

These skills and experience have fused into our own service-based Security Operations Center framework, which we shared in our whitepaper The Art of SOC. The framework includes ten cornerstone services:

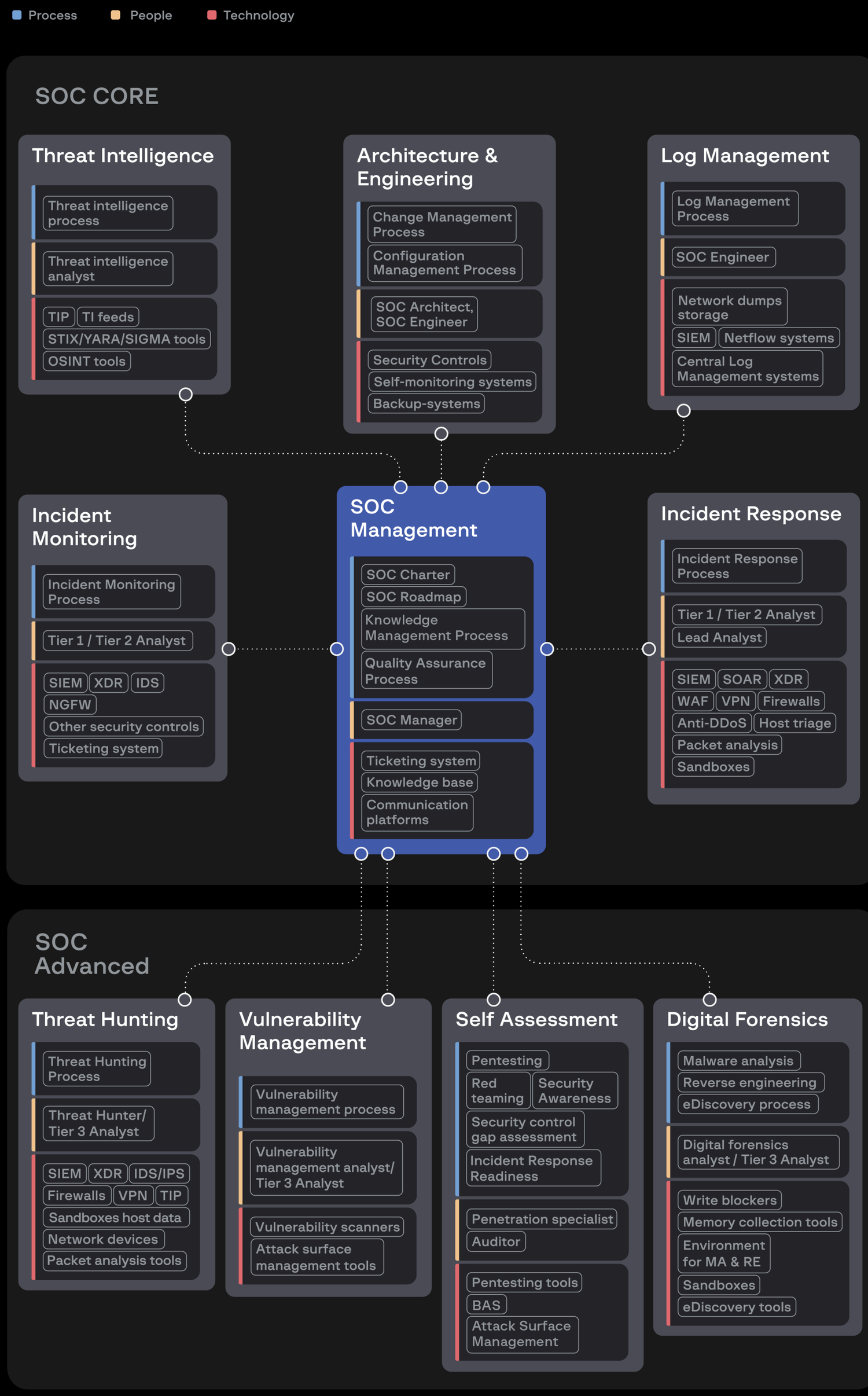

Figure 1.
GROUP-IB SOC Framework

Each service includes three sections: Process, People, and Technology. The framework is also divided into two levels: SOC CORE and SOC ADVANCED. Group-IB experts believe that CORE (or, in other words, the minimum set of services in every SOC) must include SOC Management, Architecture & Engineering, Log Management, Incident Monitoring, Incident Response, and Threat Intelligence. Meanwhile, SOC ADVANCED should include services such as Threat Hunting, Vulnerability Management, Self Assessment, and Digital Forensics.

In this e-book, we focus on all security assessments (the Self-Assessment) that are essential not only for advanced SOCs but for any cyber security strategy, as they are designed to help SOC Managers, CISOs and other security leaders evaluate their security posture and improve security operations.

General assessment process

While every cybersecurity assessment is unique, with its own methods, tools, and stakeholders, the overall process follows a structured approach that ensures consistency and effectiveness. Before proceeding to the Group-IB Assessment Compass, let’s look at the main components of any successful assessment. Below is a streamlined overview of the general process, applicable to most assessments, that will help you make your approach more streamlined:

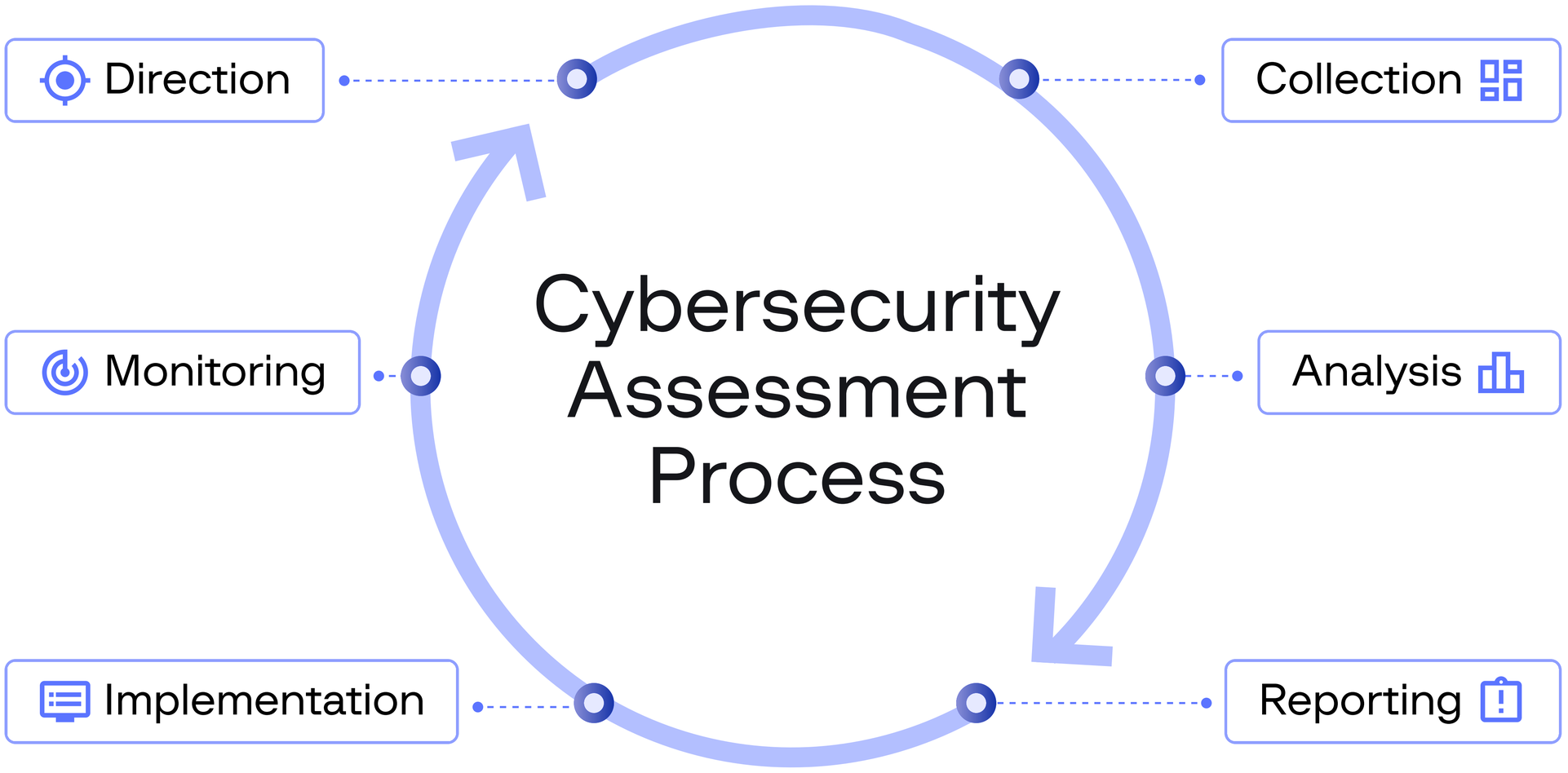

Figure 2. Cybersecurity assessment process

01 Direction

The foundation of any successful assessment begins with clear objectives and a defined scope:

Set the scope

Identify what areas will be assessed – this could include specific systems, networks, applications, data, processes, users, security domains, or the entire organization.

Clarify your goals

Determine the purpose of the assessment, such as achieving compliance, reducing risk, identifying relevant threats, enforcing best practices, or testing defenses.

Identify any pre-requisites

Specify any requirements or preparations needed before starting the assessment, such as setting up access permissions or gathering initial documentation.

This stage ensures that all stakeholders are aligned and sets the stage for actionable outcomes.

02 Collection

Data gathering is a crucial phase that combines various methods to ensure a comprehensive understanding of the security posture. The methods are:

Interviews

Talk to key stakeholders and system owners as well as SOC, IT and security staff to gain insights from those directly involved with the systems. Interviews are a way to clarify points raised in workshops or fill in gaps if some stakeholders were unable to attend. Begin with a standard set of questions and follow up with shorter, more focused questions to encourage people to expand on their responses.

Practical testing

Put systems, applications, users, and security controls through realistic tests to assess their performance under different scenarios. Such an approach can reveal vulnerabilities not apparent in routine operations. Ensure that the testing takes place in a controlled environment to avoid unintended disruptions.

Review of documentation

Review existing policies, procedures, compliance documents (e.g., GDPR, ISO 27001, NIST), and previous assessment results to identify any risks and areas for improvement. Doing so will help to ensure alignment with industry standards and highlight top remediation priorities.

Review of configurations

Gather the configuration details of operating systems, firewalls, databases, and applications to identify any security gaps. Collect information about access controls, gaps in detection and mitigation capabilities, logs, and so on.

The above methods help to ensure a well-rounded collection of data for analysis.

03 Analysis

Collected data is transformed into actionable insights, leveraging a combination of expertise, best practices, and intelligence:

Subject matter expertise

Leverage expert insights to interpret findings and understand their implications.

Best practices

Recommend best practices to enhance security and resilience.

Threat Intelligence

Use threat intelligence to correlate findings with your unique Threat Landscape, including known relevant tactics, techniques, and procedures (TTPs) used by attackers so that you can prioritize remediation efforts.

For instance, a weak password policy on a critical web-server might lead to the technique T1078: Valid Accounts being used by the threat actors.

Compliance requirements

Identify any gaps related to regulatory or industry compliance standards.

Configuration and hardening guides

Suggest adjustments aligned with configuration and hardening best practices to improve security posture.

04 Reporting

An effective assessment culminates in a comprehensive report that serves as both a roadmap to address identified risks and improve the organization's security posture and a communication tool for stakeholders:

Executive summary

Summarize the key findings, scoring, and overall security posture scoring.

Implementation timeline and resource planning

Outlines a timeline for each recommendation, identifying responsible individuals or teams. Consider defining the necessary resources, budget, and personnel for each action.

Visuals and data representation

Include diagrams, charts, and tables to clarify findings, actions, and priorities.

Detailed findings and recommendations

Provide information about quick wins (immediate, high-priority actions to mitigate critical risks) and long-term strategies (plans for implementing robust, sustainable security measures in the future). Prioritize findings by ranking issues so as to guide remediation efforts.

Compliance mapping

If applicable, map recommendations to relevant compliance and industry standards for reference.

Stakeholder workshops

Plan interactive workshops to review findings and recommendations and to refine and finalize the action plan based on stakeholder feedback.

05 Implementation

Turning insights into action is key. Follow the developed action plan to close security gaps and improve resilience. Ensure that teams are clear on their roles and timelines for putting each recommendation into practice.

06 Monitoring

After all recommendations have been implemented, continuous monitoring will ensure that any issues are addressed, improvements are sustained, and new gaps are identified promptly. Regular assessments should be scheduled to guarantee that the stated goals are achieved, to maintain a robust security posture and to adapt to evolving threats.

Understanding the Cybersecurity Assessment Compass

To make this e-guide practical and actionable, we have developed the Cybersecurity Assessment Compass — a comprehensive tool designed to help organizations navigate the often overwhelming world of cybersecurity evaluations. The Compass simplifies decision-making by organizing critical information about assessments in one place. Here's how to use the Compass effectively and understand each of its components:

How to use the Compass

The Assessment Compass serves as a structured framework to guide organizations in selecting the most relevant assessments based on their objectives, industry, and maturity level.
Begin by identifying where your organization fits within the Compass. The columns for industry and maturity level will help pinpoint assessments tailored to your unique needs.

Next, prioritize the assessments that align with your immediate and strategic goals. The Priority ranking in the Compass enables you to focus on high-value evaluations, while the Scope column clarifies the focus of each assessment.

Use the columns Cadence and Pre-requisites to plan the timing and resources for each assessment.

Review the column Intersections to identify related assessments that could complement or overlap with your chosen evaluation. This helps to create a streamlined assessment plan, maximizing efficiency and avoiding unnecessary duplication. Lastly, ensure that the necessary tools and expertise are in place.

Components of the Assessment Compass

“Scope”

defines what the assessment covers. It could be a targeted evaluation focusing on specific networks, applications, or systems, or it might encompass a broader, comprehensive analysis of the entire organization, including multi-vector attacks.

“Recommended Cadence”

suggests how often each assessment should be conducted. Depending on the type of assessment, it may need to be conducted annually, semiannually, or on-demand, ensuring that assessments are timed in a way that makes it possible to address evolving risks effectively.

“Average Duration”

estimates the time required to complete the assessment. Knowing this helps with planning and resource allocation.

“Pros and Cons”

summarizes the benefits and limitations of each assessment. This helps to weigh the value of a given evaluation against potential challenges or constraints.

“Industry”

specifies which sectors the assessment is particularly relevant for. While many assessments apply to “any” industry, certain evaluations may be more critical for highly regulated or high-risk sectors such finance, healthcare, or energy.

“Organization’s Maturity Level”

helps to select assessments that align with your organization’s security maturity. Maturity levels are defined using the Capability Maturity Model Integration (CMMI), a globally recognized framework developed by Carnegie Mellon University that assesses and improves organizational processes as follows:

Low maturity

corresponds to CMMI Level 0 (Incomplete) or Level 1 (Initial), where organizations have minimal or no formalized security processes, basic or non-existent controls, and no dedicated security teams.

Medium maturity

reflects CMMI Level 2 (Managed), where organizations have some foundational processes in place, such as a SOC with core services like incident monitoring and response, along with basic controls such as SIEM, NGFW, EDR/XDR, VPN, Mail Security Gateway, and Vulnerability Scanner.

High maturity

corresponds to CMMI Level 3 (Defined) or higher, where organizations have well-established and integrated security processes, multiple dedicated teams (e.g., SOC, GRC, Cybersecurity Architecture and Engineering, TI), and all key security controls and advanced controls like WAF, DLP, and anti-DDoS.

Assessments marked as “Any” are suitable for all levels of maturity.

“Priority”

ranks each assessment based on its relevance and impact, considering all the above factors. This subjective rating built by Group-IB experts helps to focus on what matters most for your specific context.

Cybersecurity Assessment Compass

Assessment	Description	Scope	Recommended Cadence	Average Duration	Pros	Cons	Industry	Organization's Cybersecurity Maturity Level	Priority
Risk Assessment	Evaluates the risks to information systems by identifying assets, vulnerabilities, threats, and the potential impact of security breaches	Comprehensive, entire organization	Annually	1–3 months	• Identifies main risks and guides mitigation, simple to understand for senior management and other non-security stakeholders • Business oriented and aligned approach • Gives a thorough understanding of the cybersecurity initiatives and projects to be implemented	• Can be too high-level and challenging to precisely quantify risks, very subjective • Qualitative risk matrices do not work well - there is no proof that they work and they oversimplify complex things by subjectively assigning High-Medium-Low labels and even multiplying non-uncountable values	Any	Any	1
Penetration Testing	Practical simulation of real-world attacks to identify exploitable gaps and weaknesses in systems, networks, or applications	Targeted (specific networks, apps, or systems)	Semiannually	2–4 weeks depending on the scope	• Easiest way to practically test technology defenses, wide coverage of attacks • Quickly reveals gaps and problems in the overall cybersecurity to senior management in companies without a cybersecurity strategy or one in its initial stages.	• Usually identifies only a few initial access vectors (for external penetration testing) • Not suitable for complex attacks • Limited defense evasion and bypassing • Social engineering is rarely used	Any	Any	1
Vulnerability Assessment	Identifies and prioritizes security vulnerabilities within the organization's network, systems, and applications with or without exploiting (validating) them	Targeted (specific networks, apps, or systems)	Near-real time, before implementing a new system, or on demand	Near real-time, depending on the number of assets	• Identifies known vulnerabilities in systems and applications • Quick to perform • Wide scope and functionality of coverage	• Finds only known vulnerabilities • Smaller depth of assessment (in terms of exploitation vulnerabilities)	Any	Any	1
Threat Landscape Assessment	Identifies and analyzes potential threats specific to the organization's industry, geography, and business model, including threat actors, their attack methods and their tools	External and Internal Threats	Semiannually/near-real time	2 weeks/near-real time if automated	• Identifies relevant threats and threat actors, malware and tools, TTPs based on real attacks • Helps to prioritize efforts in detection and mitigation	• Requires huge data sets of threat intelligence to construct it properly • Poor coverage of unclassified/ unattributed threat actors	Any	Medium - High	2
SOC Assessment	Reviews maturity and capability levels and the effectiveness of the Security Operations Center, including incident monitoring, incident response, log management and other SOC Services	Security Operations Center (SOC) / Cyber Defense Center (CDC)	Annually	4–6 weeks depending on SOC services/technologies in scope	• Reveals gaps in SOC people, processes and technologies • Increases maturity and capability levels • Provides a target operating model of the SOC and gives management recommendations to make data-driven decisions • Creates a SOC Roadmap	• May not cover security domains and services that are not under SOC governance (Prevention, Self Assessment, etc.) • Partially validates the real configuration of the security controls inside the SOC	Any, high-priority for MSSPs	Medium - High	2
Red Teaming	Emulates the tactics, techniques, and procedures (TTPs) used by high-skilled threat actors in the form of attack scenarios to test the organization's detection and response capabilities and its overall security posture	Comprehensive (multi-vector attacks), entire organization	Annually	6–12 weeks depending on the number of attack scenarios and their complexity	• Provides a realistic practical assessment of defense/ response capabilities and overall security posture and helps to identify resilience level to the specific APT groups and their methods without notifying the Blue Team (real-world emulation) • Mandatory defense evasion and bypassing, social engineering	• May be time-consuming to execute • Requires highly skilled staff to execute; scope coverage is less wide but much deeper • Requires a blue team in place	Any	Medium - High	2
Compliance and industry standards assessments	Verifies adherence to regulatory and industry standards (e.g., GDPR, PCI-DSS, ISO 27001, NIST) to ensure that the organization's cybersecurity practices comply with required norms	Comprehensive (all compliance/standard areas)	Annually or on demand (new framework enforced)	2–6 months depending on compliance framework or industry standard	• Ensures compliance with regulations and/or industry standards and ability to operate in a given industry • Prevents fines (if applicable) • Applying industry standards (NIST, ISO) is a good starting point for creating a baseline for an effective cybersecurity strategy • Demonstrates a company's adherence to cybersecurity standards and best practices	• Might be not very useful in achieving real security, may be considered as a "paper work" mostly • Often is not deep/covering enough, follows yes/no logic • Might not fit your business and security goals.	Any	Any	2
Compromise Assessment	Detects signs of past or ongoing compromise within the network, such as malware infections, unauthorized access, or data breaches	Targeted (specific networks and systems)	Annually or on demand (suspected compromise)	2–4 weeks	• Detects breaches and compromise within the network • Helps with incident response and can confirm suspected security incidents	• Time-consuming and resource-intensive • Requires access to all logs and systems in scope	Any	Medium - High	2
Purple Teaming	Combines the Red (offensive) and Blue (defensive) teams to enhance collaboration and improve the overall security posture, with coordination by a White team	Comprehensive (multi-vector attacks with Blue Team cooperation), entire organization	Annually	3–8 weeks depending on the number of detections/mitigations tested and the way of testing (BAS or dedicated Red Team)	• Provides instant feedback for the Blue Team on each step/phase of attack executed • Provides a realistic and practical assessment of defense capabilities and allows to identify resilience level to the specific APT groups and their methods • Mandatory defense evasion and bypassing, mandatory social engineering	• May be time-consuming to prepare and validate attack scenarios • Requires highly skilled staff to execute, requires engagement and collaboration of a seasoned Blue Team • Requires a detection engineering process in place	Any	Medium - High	3

Assessment	Description	Scope	Recommended Cadence	Average Duration	Pros	Cons	Industry	Organization's Cybersecurity Maturity Level	Priority
External Attack Surface Assessment	Identifies and assesses the organization's external-facing digital assets that could be targeted by attackers, including any vulnerabilities and gaps	External-facing assets	Semiannually/near-real time	Up to 1 month depending on the number of identified assets (manual engagement) or near real-time (fully automated using commercial tools)	• Fast and effective automated approach to identify external attack surface, including vulnerabilities, software, logon forms, open ports and more.	• Requires manual work and collaboration with system owners to validate assets and issues • Does not identify remote users and related third parties or partners	Any, except fully isolated environments	Medium - High	3
Infrastructure Security Assessment	Reviews the security posture relating to the configuration of critical infrastructure components, including servers, databases, and network equipment	IT infrastructure	Annually	1–6 months depending on infrastructure complexity and the number of assets	• Ensures that infrastructure components are hardened according to well-established standards like CIS, NIST, or DISA STIGs, providing a strong baseline of security across the environment • Following hardening guides reduces the attack surfaces by disabling unnecessary services, applying secure configurations, and enforcing least-privilege principles, which protects against common threats like brute-force attacks, privilege escalation, and lateral movements	• Blindly following hardening guides without considering the organization's unique operational needs can lead to overly restrictive configurations, impacting functionality • Applying security hardening recommendations may inadvertently cause issues with legacy applications or services that rely on less secure settings • It can be difficult to assess custom systems and niche infrastructure	Any	Any	3
Identity and Access Management (IAM) Assessment	Reviews the security of how Identity and Access Management solutions and systems (e.g., Active Directory) are configured to prevent unauthorized access, privilege escalation, and lateral movements	Active Directory (AD) or other IAM solutions	Annually	2–3 weeks depending on the complexity of IAM infrastructure	• Identifying misconfigurations, overprivileged accounts, and improper access controls can significantly reduce the risk of data breaches • When access pathways and vulnerabilities within the IAM system are known, incident response can be faster and more targeted • Proper IAM assessments identify and mitigate vulnerabilities that allow attackers to escalate privileges or move across the network	• Some tools (e.g., BloodHound, ADRecon) require an in-depth knowledge of AD and IAM systems • IAM systems like Active Directory are often subject to changes in user roles and permissions, which means that assessments must be conducted regularly to stay up to date • The output of such assessments can sometimes be overwhelming, especially if the IAM environment has a lot of legacy configurations and poorly managed permissions	Any	Any	3
Email Security Assessment	Reviews the organization's email security controls, including phishing defenses, spam filters, SPF/DKIM/DMARC and email system configurations	Email environment (email servers, mail security gateways)	Semiannually	2–4 weeks depending on the complexity of the email infrastructure	• Helps to evaluate how effective email protection is against phishing, email spoofing, insecure authentication mechanisms, malicious attachments, malicious links, and misconfigured protocols (SPF, DKIM, DMARC) before attackers can exploit them • Helps to prevent Business Email Compromise attacks	• Planning and executing phishing simulations often requires significant resources to design realistic scenarios and track responses • Assessing the email behavior of employees may conflict with privacy laws like GDPR (which requires careful consideration as to how data is collected, processed and stored), limited scope (only email initial access vector)	Any	Any	3
Cyber Range Exercises	Simulated environments where teams can practice responding to cyber incidents to enhance their skills in a controlled and realistic setting	People (Security/ SOC team)	Annually	1–2 weeks	• Tests the team's practical skills and its ability to use various tools and sources for effective incident detection, response and recovery • Helps to identify areas where the cybersecurity team's skills can be improved	• Assessment on a virtual environment cannot guarantee the same level of efficiency of the incident response and recovery because it is different to a real environment and due to the potential conflicts that might arise while completing specific activities. • Cyber Range Exercises often do not include specific incident monitoring and incident response tools installed in a company's unique infrastructure	Any	High	3
Security Controls Gaps Assessment	Identifies gaps in an organization's security controls by evaluating their effectiveness against modern threats and whether they align with configuration best practices	Security Controls, security Tools	Annually	1–3 months depending on the number and type of security controls	• Helps to identify vulnerabilities, misconfigurations, or missing controls before they can be exploited by malicious actors • Enhances cybersecurity architecture • Improves detection and mitigation capabilities	• A thorough security controls gaps assessment can take a long time, especially for large organizations with complex environments • Outcomes might be either biased (subject matter expert judgments) or limited by the specific methodology or framework used (hard to identify all the possible gaps in security controls)	Any	Any	3
Security Staff Skills Assessment	Identifies gaps and lack of skills and knowledge for each cybersecurity team member (in accordance with their role) as well as their understanding of the organization's policies, processes, and procedures	People (Security/SOC team)	Semiannually	1–2 days per team member depending on their role	• Helps to pinpoint specific areas where team members need additional training or support, in accordance with their role • Ensure that the security team adheres to the organization's policies, processes and procedures • Outcomes and findings can be used in Career Progression Paths/Training Plans/Certification Plans and help to define improvement goals for the team	• Requires good management skills to justify the need for such assessments (to avoid lowering the team's morale) • Preparing custom assessment materials can be time-consuming	Any	Any	3
Digital Fraud Assessment	Evaluates the organization's exposure and resistance to digital fraud schemes, including phishing, impersonation, and online scams	Financial transactions, digital footprints	Semiannually or on demand (if new fraud scheme revealed)	1–2 weeks per scheme	• Identifies gaps in technical capabilities to detect and prevent fraud schemes specific to an organization's industry and region	• By default, does not cover people, processes capabilities and compliance domains	Finance, Insurance, Online Gambling and Betting	Medium - High	3

Assessment	Description	Scope	Recommended Cadence	Average Duration	Pros	Cons	Industry	Organization's Cybersecurity Maturity Level	Priority
Security Awareness Assessment	Evaluates the organization's exposure and resistance to digital fraud schemes, including phishing, impersonation, and online scams	People (all employees)	Quarterly	1–4 weeks depending on the number of employees	• Identifies gaps in employee knowledge • Encourages security-focused behavior • Makes employees more prepared for social engineering attacks and improves compliance	• If not designed correctly, the assessment can lead to employee disengagement, a "check the box" mentality, or inaccurate results	Any	Any	3
Applications Security Assessment	Reviews software applications to identify security flaws, improper configurations, and vulnerabilities.	Application software	Before the implementation of a new system or before new major software update	from 3 days to 4 weeks per each application, overall duration depends on number of applications and their complexity and methodology used	• Can assess applications running on various platforms (mobile, desktop, cloud, web) • Identifies vulnerabilities across multiple layers, including the application itself, backend systems, APIs, and third-party services • Deep functionality coverage	• Requires good understanding from stakeholders of which applications and components (based on business criticality) need this type of assessment to not waste time and resources for not signficant applications and components	Any, high-priority for companies with internal software development	Any	3
Cloud Security Assessment	Assesses the security of cloud infrastructure, services, and configurations to ensure that data and applications in the cloud environment are protected	Cloud environment	Annually	2–4 weeks depending on the size of the cloud infrastructure and its complexity	• Regular assessments help to identify misconfigurations, vulnerabilities, and gaps in the cloud environment that could be exploited by attackers	• Cloud environments are dynamic and can be difficult to assess without the right knowledge and tools • Assessment might be limited due to the cloud model used (IaaS, PaaS, SaaS) because of the shared-responsibilities model	Any	Any	3
Tabletop Exercises	Facilitates simulated discussions of hypothetical security incidents to evaluate the organization's response plan and readiness as well as its crisis management capabilities	People (IT, Security, GRC, product teams, senior management)	Annually	3–4 weeks depending on the amount of documentation, the condition of internal processes and the customer team's collaboration	• Checks whether the coordination between technical teams is effective and verifies their knowledge and ability to properly implement incident response plans, playbooks, and escalation procedures, evaluates their awareness and analytical skills • Exercises for the management team make top managers more aware, highlight their role in managing a cybersecurity crisis, tests their decision-making skills and ensures that the strategies used are efficient — all in a safe environment	• Due to discussion-based nature of the exercise, it cannot fully guarantee that the organization will be able to implement all of the discussed decisions and hypothetical actions in the event of a real cybersecurity incident	Any	Medium - High	3
Incident Response Readiness Assessment	Evaluates the organization's preparedness to handle security incidents, focusing on the incident response six-phase process	Security Controls, People (Security/SOC team)	Annually or on demand (if poor incident response revealed)	1–2 weeks	• Improves the organization's ability to handle incidents • Identifies weaknesses in current IR capabilities • Makes the team more ready to handle cybersecurity incidents	• Requires a blue team and commitment from several departments • Limited impact without follow-up and if recommendations are not implemented	Any, low-priority for the companies with outsourced incident response service	Medium	4
Digital Footprint Evaluation	Assesses the organization's public-facing online presence, identifying potentially sensitive or exploitable information available on the internet	Brand presence, employees, external-facing assets	Semiannually/near-real time	Up to 1 month depending on the number of assets and people (manual engagement) or near real-time (fully automated by using commercial tools)	• Helps to identify publicly accessible information that could be exploited by attackers, such as exposed email addresses, leaked credentials, and sensitive business information • Helps individuals and organizations discover if their private data is exposed (such as personal addresses, phone numbers, or financial information) on social media, blogs, or other platforms • Helps to monitor public perceptions and mentions across social media and online platforms	• Potentially time-consuming and resource-intensive (especially for large organizations) • The digital landscape is changing all the time, with new data being created and deleted regularly (near real-time monitoring is required) • Data gathered during a digital footprint evaluation can be complex and may require expert analysis	Any	Medium - High	4
Crown Jewels Assessment	Identifies the organization's most critical assets ("crown jewels") and evaluates the security measures protecting them, using both Threat Modeling and Risk Assessment	Critical assets	Annually	2–4 weeks per crown jewel depending on the number of crown jewels and their complexity	• Helps to prioritize resources by focusing on the most critical asset(s) • Combines risk assessment and threat modeling to provide a comprehensive view of vulnerabilities and potential impacts on critical assets, aligned with business goals	• Risk that less critical assets will be overlooked • Challenges when it comes to identifying which assets are truly critical and why • Resource-intensive • Risk assessments can be biased (too subjective)	Any	Medium	4
Network Devices Security Assessment	Analyzes the security of network devices (e.g., routers, firewalls, switches) to identify misconfigurations, vulnerabilities, and outdated firmware	Network devices	Annually	1–3 months, depending on the number and type of network devices	• Helps to identify vulnerabilities and potential gaps in the configuration, software, or firmware of network devices (routers, switches, WLCs, etc.), such as outdated software, weak encryption protocols, and insecure management interfaces that can be exploited by attackers	• A comprehensive network device security assessment can take a long time, especially for organizations with large or complex networks • Effective assessment requires specialized skills in networking and security as well as configuration analysis tools	Any, high-priority for Telecom industry	Any	5
Threat Modeling	Analyzes potential threats and attack vectors against critical systems, identifying mitigations to reduce risks	One system/ application	Before a new system is introduced or before a new major software update	2–4 weeks per system/ application depending on the complexity of the application	• Helps to identify potential security threats and attack vectors early in the software development life cycle (SDLC) or system design phase • Increases awareness of specific threats that the organization or system may face, helping stakeholders (developers, IT, security teams) understand how attackers might compromise the system • Supports the shift-left security approach, where security is considered early in the development process	• Threat modeling can be a time-consuming process, especially for large and complex systems • Requires a detailed understanding of the system architecture and considerable effort to map out all potential threats • Requires specialized knowledge in both security and system architecture	Any	Medium - High	5

Use cases: Tailored security assessment bundles by industry and maturity

The following examples illustrate how security assessment needs vary based on organizational maturity and industry-specific challenges. Each case shows how companies in various industries can use a recommended assessment bundle and cadence to ensure optimal security outcomes.

01 Organization from any industry with low maturity (priorities 1-2)

A startup or small-to-medium business (SMB) with basic cybersecurity measures in place but limited resources for advanced strategies. Such organizations are often unaware of their own vulnerabilities, struggle with real-time incident detection, and find it challenging to meet compliance requirements.

Key threats and challenges

Such companies often have insufficient knowledge about vulnerabilities and risks, basic detection capabilities, and gaps in regulatory compliance readiness. Their limited resources require assessments that provide maximum impact with minimal complexity.

Recommended assessments and cadence

Assessment	Cadence
Risk Assessment	Annually
Penetration Testing	Semiannually
Vulnerability Assessment	Near-real time, before implementing a new system, or on demand
Compliance and industry standards assessments	Annually or on demand (new framework enforced)

02 Financial organization or bank with medium maturity (priorities 1, 2, and 3)

A financial institution operating in a highly regulated environment, with established cybersecurity measures in place but needing to improve its ability to detect and respond to advanced threats.

Key threats and challenges

Such organizations are prime targets for advanced persistent threats (APTs) due to the critical nature of their data and infrastructure. They must also navigate stringent regulatory requirements while managing a complex digital ecosystem that requires continuous monitoring and adaptation.

Recommended assessments and cadence

Assessment	Cadence
Risk Assessment	Annually
Penetration Testing	Semiannually
Vulnerability Assessment	Near-real time, before implementing a new system, or on demand
Threat Landscape Assessment	Semiannually/near-real time
SOC Assessment	Annually
Purple/Red Teaming	Annually
Compliance and industry standards assessments	Annually or on demand (new framework enforced)
Compromise Assessment	Annually or on demand (suspected compromise)
External Attack Surface Assessment	Semiannually/near-real time
Infrastructure Security Assessment	Annually
Identity and Access Management (IAM) Assessment	Annually
Email Security Assessment	Semiannually
Security Controls Gaps Assessment	Annually
Security Staff Skills Assessment	Semiannually
Digital Fraud Assessment	Semiannually or on demand (if new fraud scheme revealed)
Security Awareness Assessment	Quarterly
Applications Security Assessment	Before implementing a new system or before a new major software update
Cloud Security Assessment (if applicable)	Annually
Tabletop Exercises	Annually

03 MSSP with high maturity (priorities 1, 2, 3, and 4)

A Managed Security Service Provider (MSSP) delivering advanced cybersecurity services to clients and requiring the ability to stay ahead of evolving threats across various industries.

Key threats and challenges

MSSPs must ensure that they are ready for sophisticated, multi-vector attacks while maintaining compliance across various client industries. They must also demonstrate cutting-edge incident response capabilities and adapt their strategies to meet various client needs.

Recommended assessments and cadence priorities 1, 2, 3, and 4

Assessment	Cadence
Risk Assessment	Annually
Vulnerability Assessment	Near-real time, before implementing a new system, or on demand
Threat Landscape Assessment	Semiannually/near-real time
SOC Assessment	Annually
Purple/Red Teaming	Annually
Compliance and industry standards assessments	Annually or on demand (new framework enforced)
External Attack Surface Assessment	Semiannually/near-real time
Infrastructure Security Assessment	Annually
Identity and Access Management (IAM) Assessment	Annually
Email Security Assessment	Semiannually
Cyber Range Exercises	Annually
Security Controls Gaps Assessment	Annually
Security Staff Skills Assessment	Semiannually
Security Awareness Assessment	Quarterly
Cloud Security Assessment (if applicable)	Annually
Incident Response Readiness Assessment	Annually or on demand (if poor incident response revealed)
Digital Footprint Evaluation	Semiannually/near-real time
Tabletop Exercises	Annually

Get support in your assessment journey

Group-IB offers a comprehensive suite of services that support organizations in navigating the complex cybersecurity landscape. Each service is aligned with the assessment types outlined in this guide and ensures that your organization can achieve its goals effectively and efficiently. Whether you're addressing vulnerabilities, preparing for compliance checks, or strengthening your threat detection and response capabilities, Group-IB's expertise ensures actionable insights and practical solutions.

SOC Assessments: Enhancing your security operations

One of our cornerstone offerings is the SOC Assessment, designed to elevate your Security Operations Center's maturity and performance. Leveraging industry-leading methodologies like SOC-CMM, our service evaluates your SOC's capabilities in depth across five key domains: business, people, process, technology, and services.

Our SOC Assessment includes a detailed review of documentation, discussions with staff, evaluations of existing processes and technologies, and a thorough analysis of maturity levels. The process is collaborative, incorporating interactive workshops for both technical teams and senior management to help them review the findings and develop actionable recommendations.

Group-IB is an authorized SOC-CMM Silver Partner, uniquely positioned to provide expert advice. With Digital Crime Resistance Centers (DCRCs) strategically located in the Middle East, Europe, Central Asia, and the Asia-Pacific region, Group-IB offers global SOC-CMM assessments, consulting services, and targeted training. Partnering with us means that you receive comprehensive assessments, consulting services, and tailored SOC training no matter where you are located in the world.

Beyond SOC: A full spectrum of intelligence-powered assessments

Group-IB supports you no matter where you fit in the **Assessment Compass**. Our assessments are threat intelligence-driven — these are more than mere words. This is our core approach.

As part of Red Teaming, for example, we design attack scenarios using our extensive knowledge base of campaigns, incidents, and TTPs used by known APTs and other threat actors that could attack you. This means that we are able to emulate realistic, high-stakes scenarios that mirror the tactics used by real-life adversaries.

In Threat Modeling, we move beyond outdated methodologies such as STRIDE and PASTA. Instead, we use a dynamic Threat Landscape generated from our Threat Intelligence, focusing on the most relevant threats, actors, and TTPs. Our methodology aligns seamlessly with the MITRE ATT&CK® framework, which ensures precision and relevance.

In Digital Fraud Assessments, we leverage our uniquely designed Fraud Intelligence Matrix. Our proprietary approach is informed by existing fraud schemes, real-world incidents, and factors specific to your industry and region so that we can deliver unparalleled insights and actionable recommendations.

Our team is here to guide you through every step of your assessment journey and provide tailored solutions that will meet your unique needs.

Selecting the right assessment is just the beginning of your security journey. Learn how to execute them effectively with Group-IB.

Talk to our experts →

About Group-IB

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

1,550+
Successful investigations of high-tech cybercrime cases

400+
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

8
Unique Digital Crime Resistance Centers

* According to Cybersecurity Excellence Awards

Global partnerships

INTERPOL
EUROPOL
AFRIPOL

Recognized by top industry experts

Forrester®
Aite 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