GROUP-IB

WHITE PAPER

THE 5 STEP GUIDE TO MAKING YOUR MDR MORE EFFICIENT

GROUP-IB.COM

Introduction

45%

of breaches start from simple perimeter-based vulnerabilities

Nearly 50%

of SOCs don't have dedicated IR or CTI specialists on staff

Let's face it: The threat landscape is evolving faster than cybersecurity can adapt. Regardless of how mature your company is or how well trained your information security personnel are, you should always assume that threat actors are several steps ahead.

Those on the front lines of the endless battle against cybercrime have it the hardest. Security operations centers (SOCs), the first line of defense in the event of a cyberattack, are not equipped to handle modern threats. This is in part due to the fact that SOCs run on outdated protocols and lack the resources to effectively prioritize and manage alerts — nearly half of SOCs do not have a dedicated incident response specialist or Cyber Threat Intelligence (CTI) analyst on staff.[1]

Moreover, modern SOCs lack the tools to give them adequate visibility of the threat landscape and of their own perimeter. In fact, 45% of breaches in 2020 were due to simple perimeter-based vulnerabilities and insecure infrastructure.[2]

Effective detection and response capabilities can mean the difference between your company losing millions and maintaining business operations as usual. To ensure the latter outcome, SOCs and MDR providers must think outside the box and proactively adopt new policies and solutions.

"MDR done right gives you contextual understanding of your environment and digs deeper into the nuanced details that make your environment vulnerable to threats. Managed detection and response helps you monitor and understand your overall security posture while also improving compliance and reducing your risks." Joeseph Shenouda, Cyber Consult

One factor holding SOCs back, however, is misconceptions about certain cybersecurity approaches — that they are complicated, require too many resources, or are not worth the trouble. This white paper will break down these myths and propose five easy steps you can take to ensure the efficiency of your SOC and the quality of your MDR offering:

1. Leverage the power of CTI
2. Conduct regular third-party audits
3. Measure your team's efficiency with KPIs
4. Build a service management practice
5. Consolidate your stack with XDR technology

[1] 2020 SOC-Survey: A Tale of Two SOCs – Christopher Crowley (2021)
[2] Hi-Tech Crime Trends 2020-2021, Group-IB (2020)

Tip #1

Leverage the power of CTI

Cyber threat intelligence (CTI) has become a staple in the cybersecurity community, as it empowers companies and individuals with information that can be attributed to threat actors. However, not all MSSPs realize CTI's full potential and the opportunities it can create.

Below are four examples of how being an intelligence driven provider can propel your business and boost your brand in the eyes of your customers.

A. Expand the personalization and targeting of your offerings

CTI has changed significantly over time. What once was based on pure IoC feeds has transformed into adversary-centric, expertisedriven solutions.

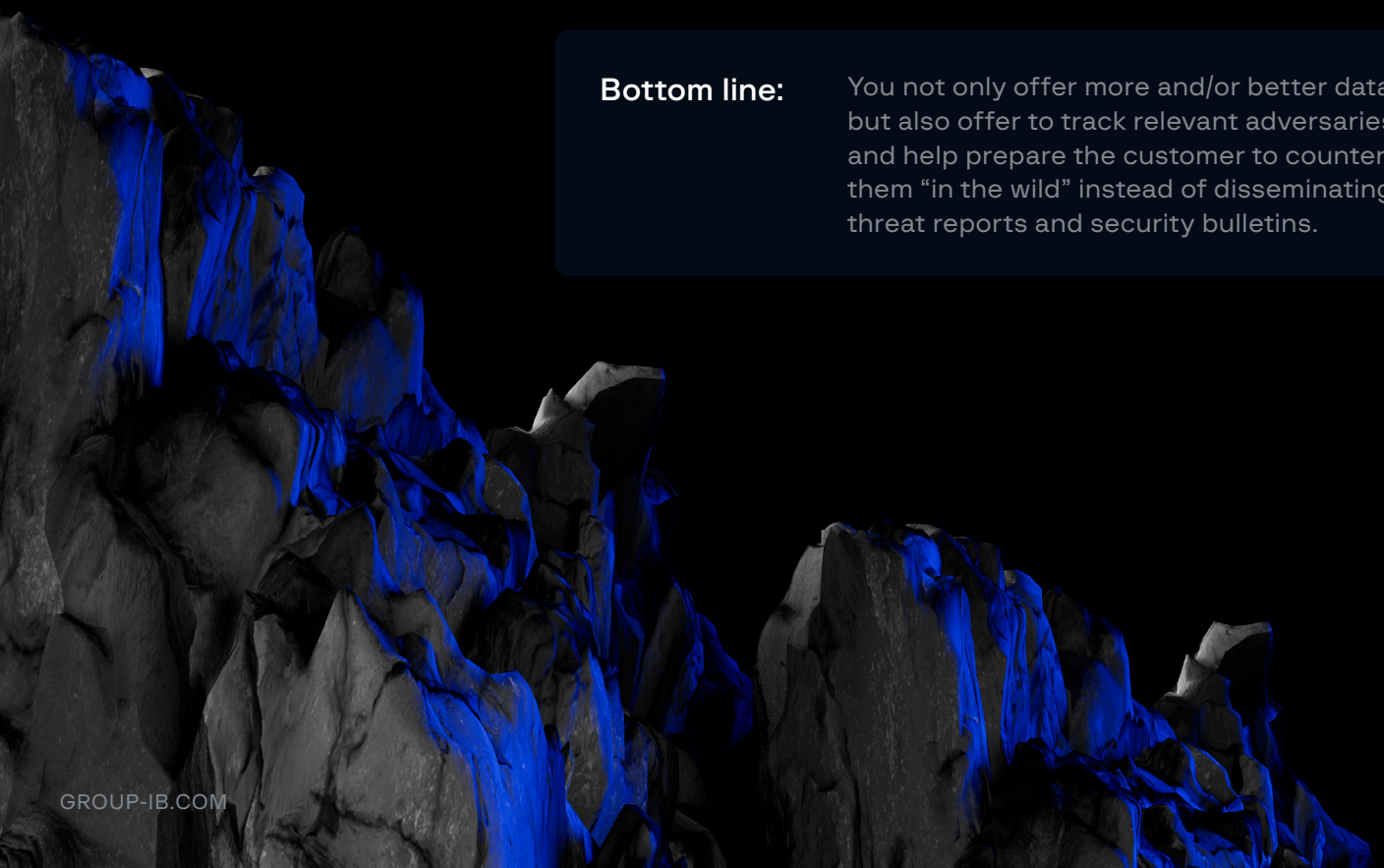
Despite the evolution, the core idea behind CTI has not changed: to provide a company with actionable data that will help in strategic and operational decision-making.

Including CTI into your MSS offering means two main improvements:

1. You can potentially gain access to unique and closed sources that contain information about cyberattacks before they actually happen.
2. You can tailor your proposal to a specific organization by completing intelligence requirements.

CTI allows you to offer managed security services based on which adversaries are most likely to be interested in the specific company/ industry. At the same time, you provide tailored and actionable data, no matter how mature a company's cybersecurity is.

Bottom line: You not only offer more and/or better data but also offer to track relevant adversaries and help prepare the customer to counter them "in the wild" instead of disseminating threat reports and security bulletins.



B. Be one step ahead of the market

Quality cyber threat intelligence is no longer about the response stage. Gathering information and understanding adversaries allows you to predict how the market will change so that you can act accordingly.

In the short term, discovering a new instrument or zero-day vulnerability months before anyone else is a crutial advantage. Leveragethis to craft a detection strategy and bring value to your customers via intelligence-driven consulting.

There are long-term benefits as well. In cybersecurity, one year is already a substantial time frame for forecasts. Leverage your access to unique data and the expert CTI community to gain an edge in prioritizing defensive tools, security controls, and skillsets.

Bottom line: You get a peek at the ever-changing future. Keep your services portfolio updated and on par with the latest trends. Gain customers' trust and worldwide recognition when your forecasts as a provider come to life.

C. Improve your services with global context

While closely related to the previous point, here we refer to day-today operations rather than long-term strategies.
There are ways CTI can enrich your overall portfolio as an MSSP.

Data sources are the key here. Imagine that attribution for every detection in a customer's network was almost fully automated and enriched by additional information such as the key tactics, techniques, and procedures (TTPs) of a specific threat actor, insights into attack stages, and probable next steps.

Intelligence-driven indicator enrichment and threat attribution are great practical steps for improving your services.

Including the promise of access to first-hand intelligence data straight from response and investigation activities (like attackers' C2 servers and machines) can also increase your offering's real and perceived value.

Bottom line: You help your customers focus their defensive efforts and empower your service portfolio with cyber threat intelligence on all levels.

D. Substantiate ROI in cybersecurity

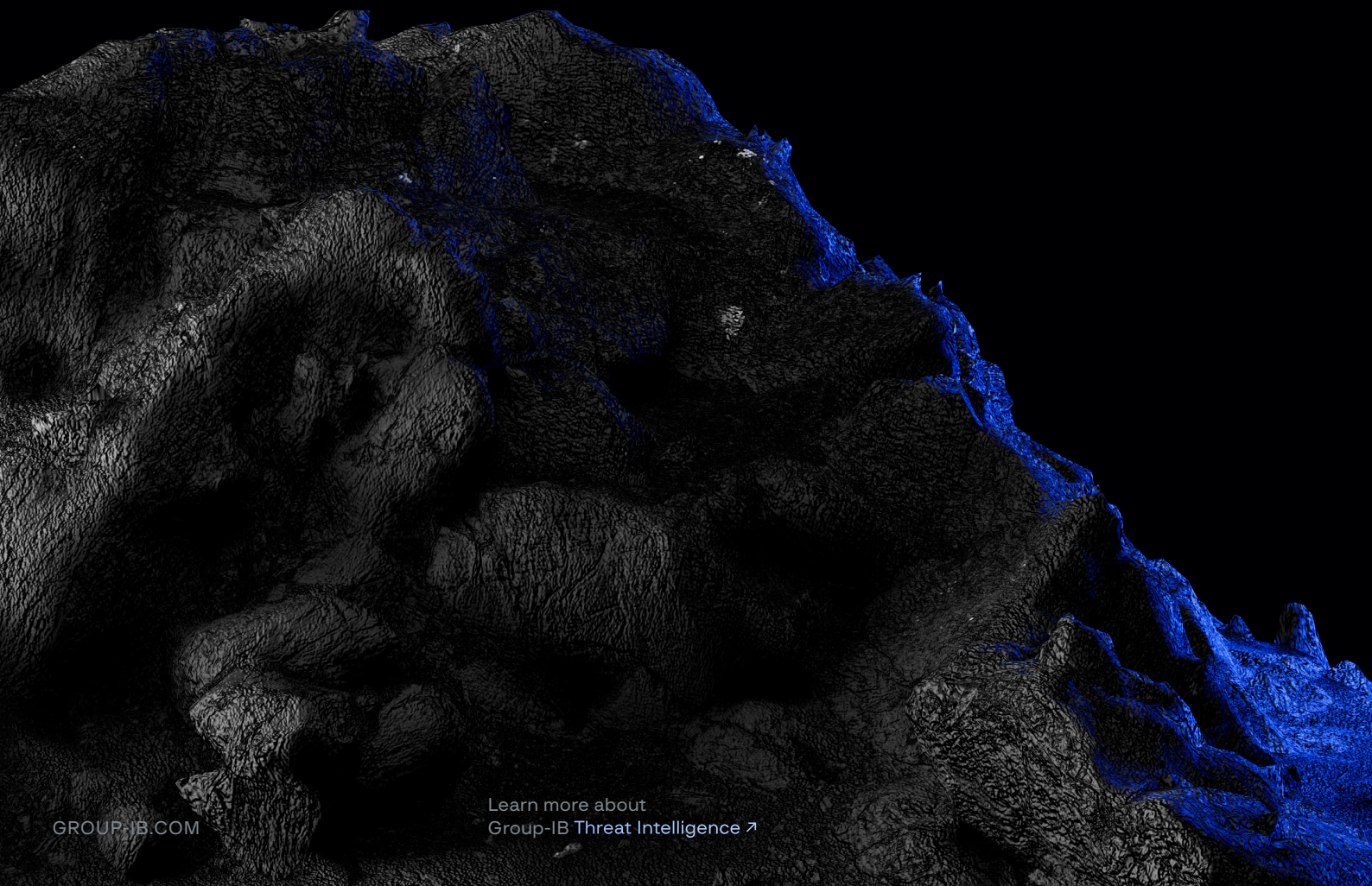
There is almost always miscommunication between technical and security experts, and top-level business executives and decisionmakers. The importance and validity of investments in cybersecurity on such a scale (e.g. when choosing an MSS provider) have to be conveyed properly.

CTI can facilitate this process. Apart from technical terms, IoCs, and TTPs, threat intelligence provides easy-to-understand business-related data for any level.

Threat intelligence can help answer the following questions:

- How much is an attack going to cost us?
- How many companies like ours went out of business last year after a successful cyberattack?
- How many critical vulnerabilities do we have in our infrastructure?
- How many threat actors target similar enterprises in our region and how hard are they hit?

Bottom line: By having these answers not only do you substantiate ROI but also show your customers' C-level executives numerous ways how to maximize ROI on cybersecurity by going back over previous points discussed above.



Learn more about Group-IB Threat Intelligence ↗

Tip #2

Conduct regular third-party audits

Whether in medicine or cybersecurity, it never hurts to get a second opinion. The value of an unbiased assessment of your policies, assets, infrastructure, and personnel cannot be overstated, with benefits including:

- Finding vulnerabilities that would have otherwise been overlooked
- Figuring out your true security posture
- Getting actionable recommendations tailored to your business needs
- Preparing your team to deal with real-life attacks

Therefore, SOCs and MDR providers should focus on conducting regular third-party audits.

Although there are many cybersecurity audits — each just as important as the next — your staples should be Red Teaming engagements and the Compromise Assessment. Both evaluations involve the vendor taking an attacker-centric approach, using its indepth understanding of attacker TTPs and behavior to detect deeply embedded vulnerabilities and traces of malicious activity.

Both should be performed at least one a year and by different vendors each time to ensure a truly objective assessment.

Red Teaming	Compromise Assessment
Red Teaming is the ultimate security test for organizations. In it, the Red Team (third-party auditor) performs an attack simulation based on real-life TTPs and cyber incidents. Conclusions of the engagement are drawn based on how well the Blue Team (SOC or MDR) responds to the simulation. Such engagements prepare the Blue Team to respond to real security incidents through the practical application of dormant skills and tools. Red Teaming engagements are strongly recommended for enterprises and larger companies, but they can also bring value for smaller companies in the form of actionable recommendations.	The core motivation for a compromise assessment is the realization that you may already be breached. While many companies believe that their security controls are air tight, they forget that threat actors are adept to finding new ways of bypassing detection logic. That is why attacker dwell time can be up to several months, if not years. During a compromise assessment, the auditor examines a company's infrastructure and network for traces of past or ongoing cyberattacks. The vendor then gives the company a detailed report on security breaches as well as tailored mitigation recommendations.

Bottom line: Red Teaming and Compromise Assessments give SOCs the wakeup call they need to bolster their protocols and staff training and provide better MDR capabilities.

Learn more about Red Teaming ↗ and Compromise Assessment ↗ by Group-IB.

Tip #3

Measure your team's efficiency

Having a clear picture of what success looks like for MDR is critical. Aligning the objectives and expectations of the MDR provider and the client is vital because any disconnect will destroy the MDR-client relationship and waste valuable resources.

There are two areas on which you should focus: timebased and quality-based metrics. Finding a balance is key because, otherwise, you could inadvertently encourage fast results over quality performance, which will hurt overall efficiency.

Examples of time-based metrics:

Threat Intelligence	Incident monitoring	Incident monitoring
Threat actor attribution rate	Time from detection to elimination	• Time to detection • The rate of incidents escalated • False positive incident rate

Examples of a quality metric:

One way of using a quality-based approach is to do regular reviews of incident analysis. This works especially well with Tier 1 analysts. The review can be done by the Tier 1 team supervisor or a Tier 2-3 analyst at regular intervals (e.g. five alerts per month).

Following the evaluation, you will understand what knowledge is lacking within your team, the common mistakes made during triage, and whether there is room for additional auto-enrichment.

Supervisors can also use the results to develop internal workshops to improve employees' knowledge about specific threats and teach them how to avoid human error. To encourage the learning process, you can include case reviews as part of the Tier 1 analyst's KPIs.

Separating the metrics reported to the client and internal performance metrics is crucial. The MDR provider must show the client their capabilities. The business components may see that the performance offered is sufficient for its purpose. For example, measuring the capacity and utilization of your analysts can help you calculate the ratio between the number of incidents and the number of analysts. With this information, you can determine when to look for additional resources

As for internal performance, maximizing coverage and visibility is the goal.

More often, SOCs rely on telemetry from:

- Endpoints (process and event data)
- Networks (NetFlow, metadata records, full packet captures [e.g. PCAP])
- Assets and vulnerability data (exposed common vulnerabilities and exposures, ports, etc.)

So you can avoid the risk of missing malicious activity in some areas that are not covered by monitoring, such as new network segments.

With regard to coverage, you can utilize the MITRE ATT&CK® framework for gap analysis.

Bottom line: Measuring the efficiency of MDR processes can provide muchneeded transparency between internal teams and clients and drive change and facilitate constructive partnerships.

Tip #4

Properly Manage The Attack Surface

Cloud migrations and digital transformations are causing a rapid expansion of the security perimeter for businesses across all industries. This can potentially lead to high-risk exposures like shadow IT, forgotten infrastructure, and misconfigurations.Attack surface management solutions address this challenge by continuously discovering and inventorying all of an organization's Internet-facing IT assets, including the unknown unknowns.

Back in 2016, Gartner estimated that "by 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources. "Recent research from IBM confirms these predictions. In 2021, the IBM X-Force Threat Intelligence Index report found that "Scan-and-exploit was #1 initial attack vector," representing the primary vector in 35% of attacks.

These numbers are also supported by data collected by the Group-IB Computer Emergency Response Team (CERT-GIB). In 2021, over 45% of DFIR cases stemmed from a preventable, perimeter-based security error.

So, while zero-day exploits and sophisticated supply chain attacks dominate headlines, a significant plurality of corporate breaches are the result of ordinary security errors, oversights, and misconfigurations.

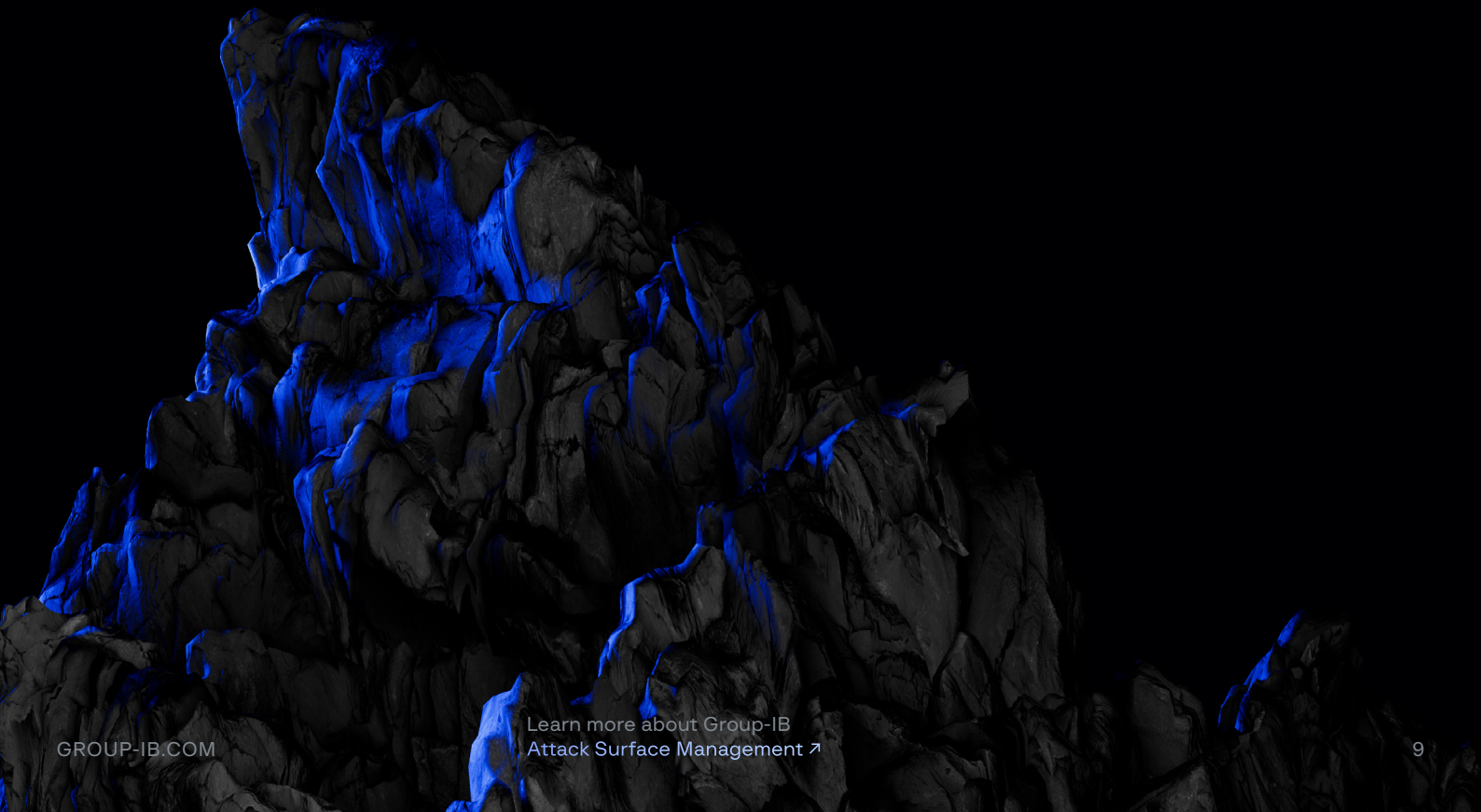
Attack Surface Management solutions help to overcome all of these challenges. The idea is to map out an organization's entire external attack surface from the attacker's point of view– that is, from the public Internet, using only publicly available records and data. This process helps to identify all external IT assets that belong to a particular business, rather than simply relying on an internal IT asset inventory, which is likely to be incomplete.

Most organizations know that their IT asset inventory will not be perfect– after all, infrastructure is constantly evolving and expanding, with new cloud instances being deployed and decommissioned by automated tools all the time. However, most corporate asset inventories are far worse than is commonly understood. In a report published in January 2022, Forrester wrote that "on average, attack surface management tools initially discover about 30% more cloud assets than security and IT teams even knew they have."

After discovering and inventorying all external IT assets, Attack Surface Management solutions take additional steps to help businesses improve security posture:

- check each external asset for potential vulnerabilities
- assess risk and assign a risk score to each asset
- prioritize issues for remediation to enable high-impact improvements
- track remediation efforts and issue resolution to gather data and show results.

Bottom line: Attack Surface Management is becoming an essential component of corporate cybersecurity programs. These tools automate the process of external IT asset discovery, which improves visibility, identifies previously hidden risks, and helps businesses to make major improvements to security posture with a minimal allocation of resources.



Learn more about Group-IB Attack Surface Management ↗

Tip #5

Consolidate your stack with help of XDR technology

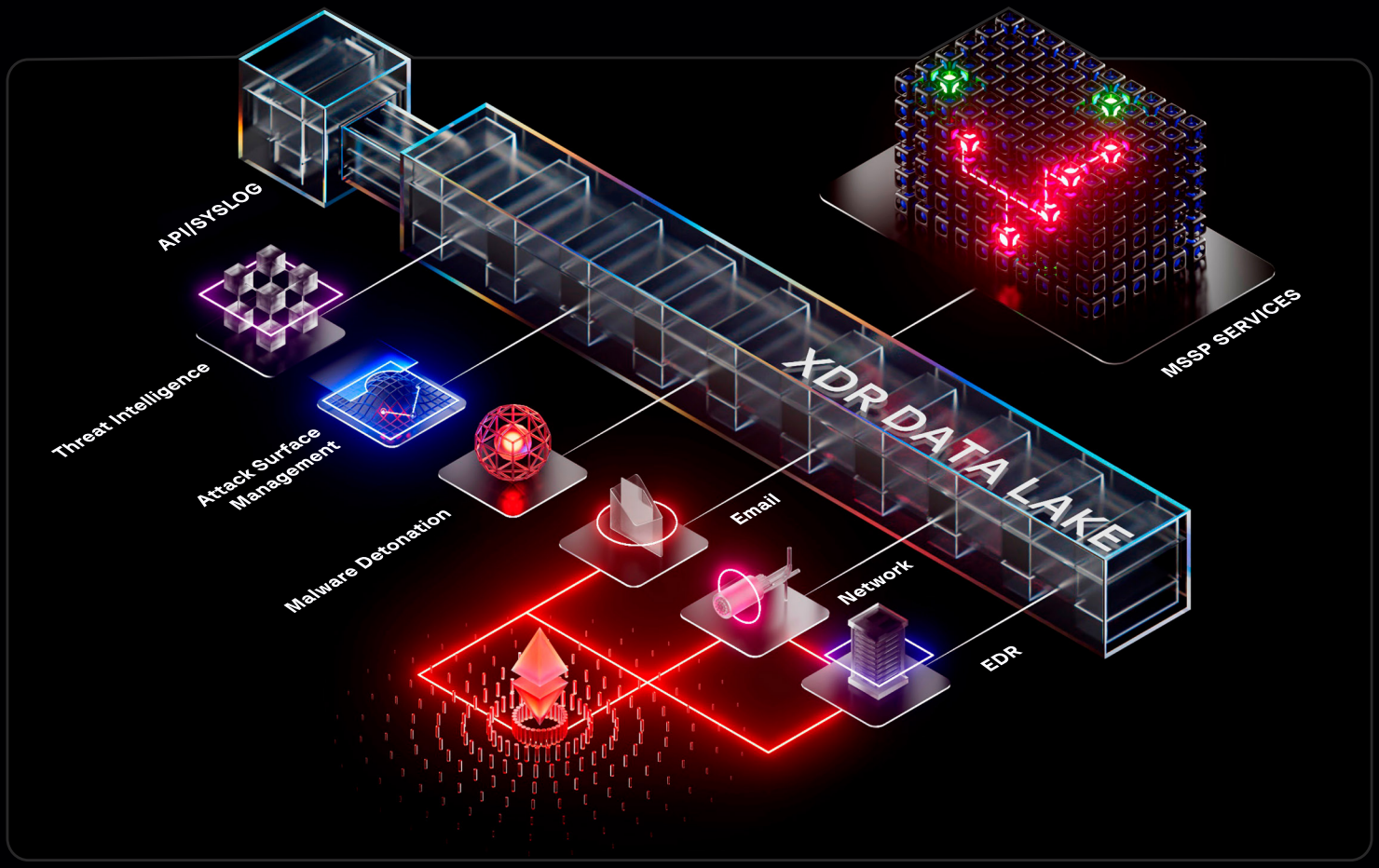
Every year, MDR providers face new challenges and search for ways to overcome them while increasing profitability and growing their businesses. The desire for a single, simplified end-to-end SOC platform among MDRs had been rising steadily until 2020, when the demand spiked due to the global pandemic and subsequent mass migration to remote work.

One of the most powerful ways MDRs can expand profitability and business growth is to use XDR technology to simplify SecOps, analyst training, and solution administration.

> **"Security teams need a simpler, more effective way to approach the breach problem, and that is what XDR aims to achieve"**
>
> Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR, Forrester (2021)

Example of XDR architecture:

Image 1: Group-IB Managed XDR

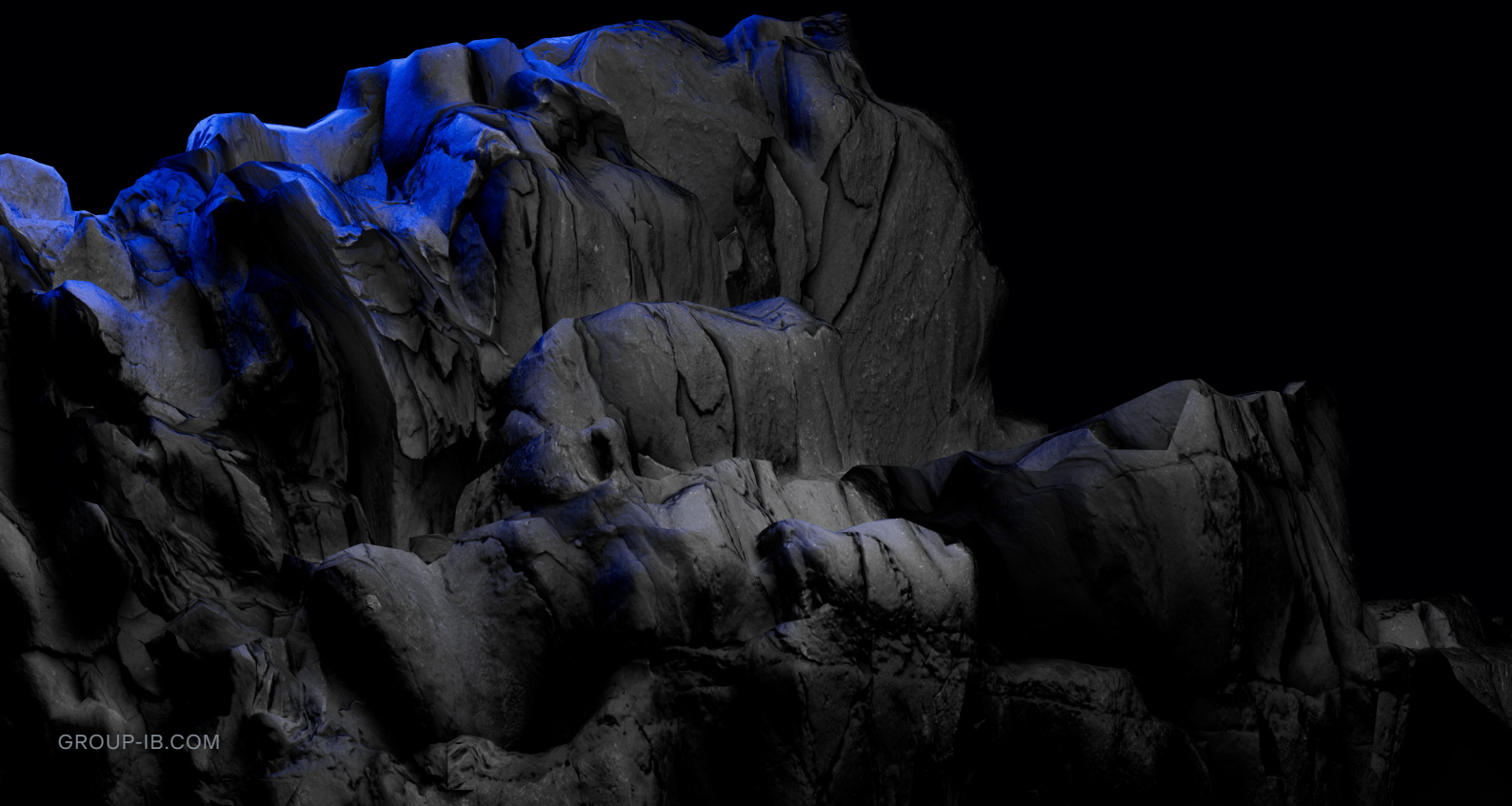


Having XDR at the core of your MDR offering will help you correlate attack telemetry across the network and endpoints via automated root-cause analysis that turns into a single incident alert that higher tier analysts can then inspect. The goal is a faster detection and response cycle that prevents burnout, lowers the barrier to threat hunting, and reduces attacker dwell time and SOC analysts' alert fatigue.

Modern attacks are complex and multi-staged, and traditional SOC tools such EDR and SIEM are limited in their prevention capabilities. EDR solutions lack the necessary telemetry that security teams need to stop sophisticated threats that focus on the attack surface beyond the endpoint. And while traditional SIEMs may be flexible and customizable, they are difficult to operationalize and tune due to the number of variables and available features. Moreover, deploying a traditional SIEM solution over the course of months or longer to keep tuning and adding new rules is no longer a viable option.

XDR extends visibility and detection capabilities across the larger enterprise IT environment and streamlines correlation, threat hunting, and response more holistically. It also breaks down data silos and unifies incident context for faster, more effective threat detection and response.

Bottom line: XDR can be an extremely effective technology that enables MSSPs to eliminate threats by extending detection and response capabilities across the entire enterprise environment. And for MDRs, this means a reduction in costs to support its SOC stack and, therefore, better service margin. Moreover, it is becoming increasingly vital to work with technology partners that can help you not only maintain and grow your client base but also contribute to cost-saving and higher margins.



Group-IB MSSP & MDR Partner Program

Group-IB strives to accommodate all potential partners, no matter where they are in their MSSP/MDR journey. We offer several paths for cooperation alongside flexible terms that seek to meet your business' needs. If your goals are to:

- Bring new value-added services to your end clients
- Enrich your portfolio with high-quality response services
- Give your business the knowledge base needed to enter a new class of MDR services
- Get automated attribution benefits and the best threat hunting practices

Then our program is the one for you.

Program details

Take MSSP to new heights

Go deeper into the MSSP market by expanding your portfolio.

What you get:

A scalable all-in-one product for Threat Hunting and Response that will help your business.

What you'll achieve:

Expaned market share by acquiring new customers and reducing capital expenses.

Learn more ↗

Begin your MDR journey

Join the MDR market with a single provider and no hassle.

What you get:

The full toolkit needed to enter a new class of MDR market plus the needed knowledge base.

What you'll achieve:

New levels of revenue growth by providing a modern, high-quality service.

Learn more ↗

Become the ulitamte MDR Provider

Get the missing piece to complete your MDR offering.

What you get:

Portfolio enriched with high-performance services that perfect end customers' experiences.

What you'll achieve:

A new revenue flow based on expanding portfolios and geographic scope of IR services.

Learn more ↗

Ready to grow your business together? Join Group-IB MSSP & MDR partner program today →

mssp@group-ib.com ↗

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®
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

Ready to grow your business together? Join Group-IB MSSP & MDR partner program today →

mssp@group-ib.com ↗

Preventing and investigating cybercrime since 2003