GROUP-IB

WHITE PAPER

GROUP-IB UNIQUE FRAMEWORK

THE ART OF SOC

Ultimate guide to establishing and evolving Intelligence-Driven Security Operations with Group-IB SOC Framework

GROUP-IB.COM

SOC-CONSULTING@GROUP-IB.COM

TABLE OF CONTENTS

INTRODUCTION

Today's threat landscape is a fast-paced realm. Security Operations Centers (SOCs) face a wide array of challenges that must be addressed using modern methodologies and dynamic approaches to cybersecurity. The days when SOCs focused on incident monitoring and response are long gone. Today, to stay ahead of ever-emerging threats, SOCs should apply a broader range of advanced solutions – such as threat intelligence, Threat Hunting, and attack surface management.

This ebook presents Group-IB's brand-new Security Operations Center framework, designed to provide measurable, granular, and understandable services to help organizations build and maintain an effective Security Operations Center. It also explores some key concepts related to threat intelligence and the ever-evolving threat landscape. In addition, this guide explains in detail how to embed threat intelligence into every SOC service and how to create an intelligence-driven SOC.

As a bonus, we outline the key challenges that SOCs faced in 2023, and how to overcome them. We provide tips on how to build a comprehensive threat intelligence program for your own SOC or organization, regardless of its size and maturity.

Vladimir Goliashev
Director, MSSP & SOC Consulting

Alexander Asmolov
SOC Consultant

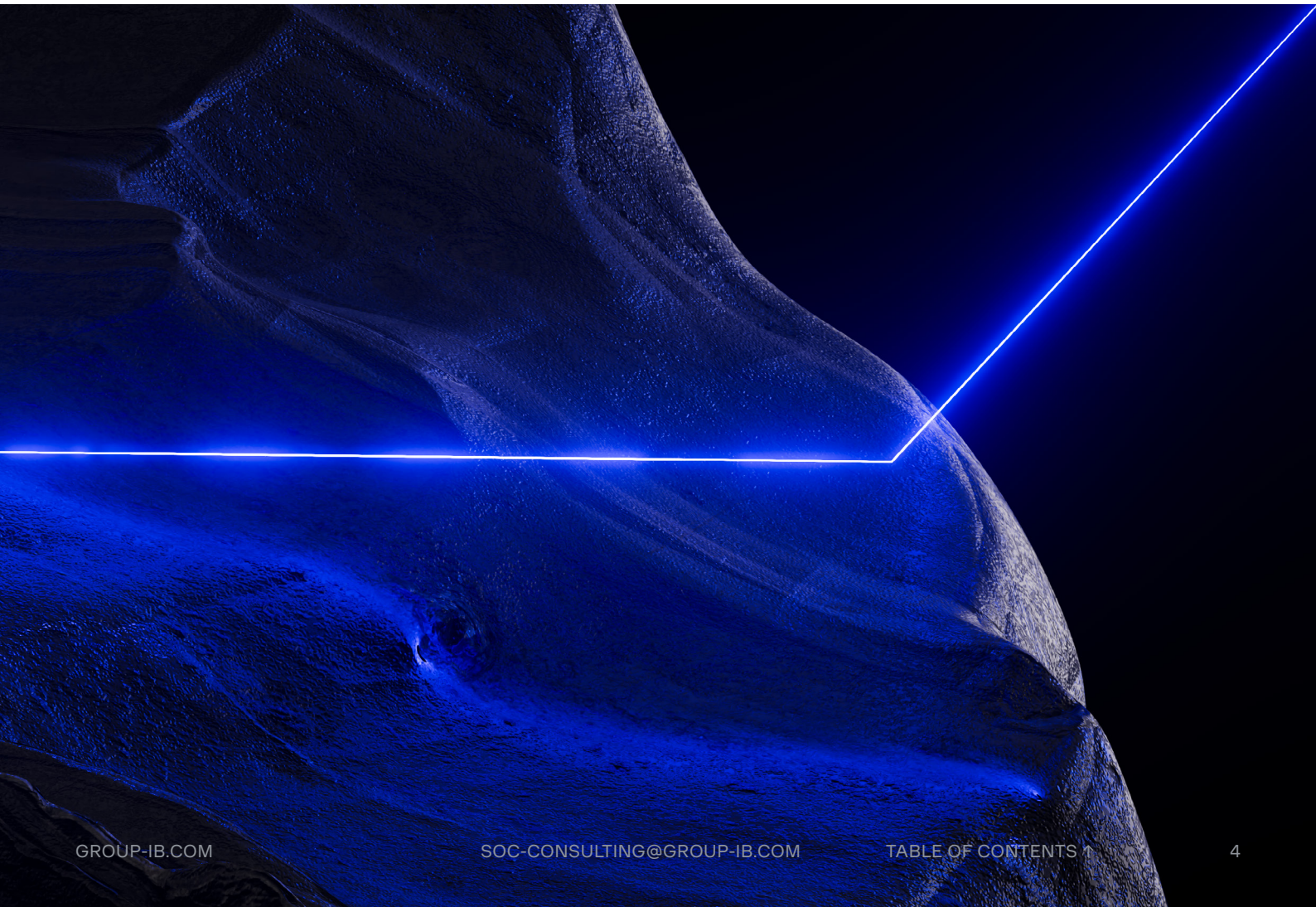
Anatoly Tykushin
Director, Cybersecurity Services, META

01

GROUP-IB SOC FRAMEWORK

Group-IB's expertise comes 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 work combined with CERT GIB's collaboration with CERTs worldwide. In addition, working with law enforcement agencies has for years been supporting and contributing to Group-IB's incident response skills and threat intelligence expertise.

We have developed our own service-based Security Operation Center framework consisting of ten cornerstone services:



GROUP-IB SOC FRAMEWORK

Process People Technology

SOC CORE

Threat Intelligence

- Threat intelligence process
- Threat intelligence analyst
- TIP
- TI feeds
- STIX/YARA/SIGMA tools
- OSINT tools

Architecture & Engineering

- Change Management Process
- Asset Management Process
- SOC Architect, SOC Engineer
- Security Controls
- Self-monitoring systems
- Backup-systems

Log Management

- Log Management Process
- SOC Architect
- SOC Engineer and relevant teams
- SIEM
- Central Log Management systems

Incident Monitoring

- Incident Monitoring Process
- L1/L2 Analyst
- Lead Analyst
- SIEM
- XDR
- IDS
- NGFW
- Other security controls
- Ticketing system

SOC Management

- SOC Charter
- SOC Roadmap
- SOC Operational model
- Service Catalogue
- SOC Manager
- Ticketing system
- Knowledge base
- Communication platforms

Incident Response

- Incident Response Process
- L1/L2 Analyst
- Lead Analyst
- SOC Engineer and relevant teams
- SIEM
- SOAR
- XDR
- WAF
- VPN
- Firewalls
- Anti-DDoS
- Host triage
- Packet analysis
- Sandboxes
- Ticketing system

SOC Advanced

Threat Hunting

- Threat Hunting Process
- Threat Hunter
- SIEM
- XDR

Vulnerability Management

- Vulnerability management process
- Vulnerability management analyst
- Vulnerability scanners
- Attack surface management tools

Self Assessment

- Pentesting
- Red teaming
- Table-top exercises
- Security control gap assessment
- SOC maturity assessment
- SOC MITRE ATT&CK assessment
- Penetration specialist
- Auditor
- Pentesting tools

Digital Forensics

- Malware analysis
- Reverse engineering
- eDiscovery process
- Digital forensics analyst
- Write blockers
- Memory collection tools
- Environment for MA & RE
- Sandboxes
- eDiscovery tools

There are many reasons to make a SOC service-based:

1. Each service is measurable and has its own SLA and metrics. This makes it easy to measure success and efficiency and to justify a service-based SOC in the eyes of senior management.
2. Each service is granular. This means it can be broken down into people, processes, and technologies.
3. Services are understandable by the business. It is easy for the business to understand the objective of each SOC component and define SLAs for each SOC service.

Each service includes three sections: Process, People, and Technology. The framework is also divided into two levels: **SOC CORE** and **SOC ADVANCED**. Based on our many years of experience, we 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. As for **ADVANCED**, we would include services such as Threat Hunting, Vulnerability Management, Self Assessment, and Digital Forensics.

When considering how to apply this framework to real-world scenarios, it is vital to bear in mind that it is almost impossible to have dedicated personnel for every service due to constraints such as a limited budget or a shortage of skilled staff. Some roles in the SOC will therefore cover several services at the same time.

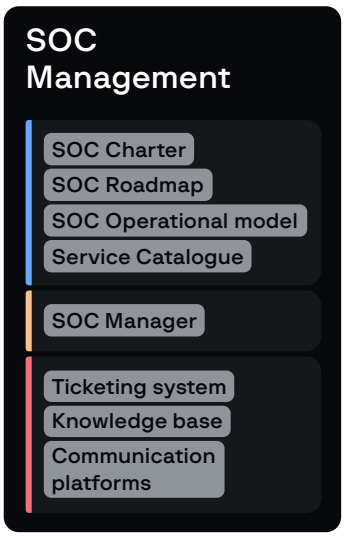
Here is an example of how services, roles, and operating modes could be divided:

Role	FTE*	OPERATING MODE	SOC SERVICE
SOC Manager	1	8x5	SOC Management
L1/L2/Lead Analyst	6	24x7	Incident Monitoring, Incident Response
SOC Engineer	1	8x5	SOC Architecture & Engineering, Log Management
SOC Architect	1	8x5	SOC Architecture & Engineering, Log Management
Threat Intelligence Analyst/Threat Hunter	1	8x5	Threat Intelligence, Threat Hunting
Vulnerability Analyst	1	8x5	Vulnerability Management

Figure 1. Roles mapped to services

In the example above, Self Assessment services and Digital Forensics are not presented or outsourced.

*FTE = Full-Time Equivalent



SOC Management

SOC Management

The SOC Management service plays a crucial role in defending against cybersecurity threats. It encompasses and defines all other SOC services involved in protecting the company. This service is the one ultimately accountable to senior management in terms of protecting the organization and it serves as the entry point to the SOC for internal and external stakeholders.

The main objective of SOC Management is to ensure that the SOC operates effectively and efficiently and that it is able to detect, respond to, and mitigate cybersecurity threats and incidents.

The focus of the management service is on defining the SOC's mission, vision, and business drivers. It also decides on the organizational structure and operating model, communication methods between teams, onboarding procedures, skills assessment, staff training, and reporting to Senior Management and other external to the SOC stakeholders. In addition, the management service determines how to organize shifts, which SOC services will be in-house and which will be outsourced, reporting formats and methods, technologies in general, as well as the manager's role, responsibilities, and required skills. It also establishes how all other SOC services are connected so that the SOC can operate as one entity. Last but not least, it handles the use of technologies such as ticketing systems, knowledge bases, and communication platforms.

We have the following approach to building a reliable SOC Management service for our customers:

People	Process	Technologies
• Building the ultimate SOC course • C-level workshop	Consulting service that covers SOC Service Catalog development, defining priority SOC requirements, operating model, SOC Charter, Roles & Responsibilities, and more.	Consulting service that includes recommendations on developing a knowledge base (based on commercial or open-source tools), recommendations for ticketing, and defining reporting templates.

SOC Management service options

SOC Architecture & Engineering Service

Architecture & Engineering

Architecture & Engineering is a support service that helps ensure the proper design and configuration of a SOC in the face of modern threats and attack methods.

The main objective of Architecture & Engineering is to choose, design, document, and manage appropriate security controls in the SOC.

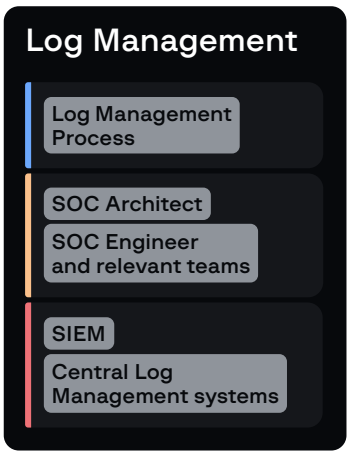
The SOC security Architecture & Engineering service includes:

- identifying which assets should be protected and why
- defining the security architecture and engineering practices related to security controls
- keeping the SOC system inventory
- handling the change management process during day-to-day operations with security controls
- preparing SOC architecture diagrams. It also defines the roles and responsibilities of the SOC architect and SOC engineer, as well as the skills they must have. Additionally, it covers self-monitoring systems (such as Zabbix and Nagios) for SOC operations, as well as backup systems for internal purposes.

We have the following approach to building an efficient and effective SOC Architecture & Engineering service for our customers:

People	Process	Technologies
• Cybersecurity specialist training • Team workshop	Consulting service that covers the change management and asset management processes, as well as defines a self-inventory	Our consulting service provides comprehensive recommendations for choosing security controls, building a reliable architecture and setting clear configuration guidelines.

SOC Architecture & Engineering service options



Log Management service

Log Management

Log Management is a crucial support service given that log data provides meaningful insights into the operations and efficiency of systems, networks, and applications. Log data can be used to pinpoint and resolve issues, enhance security, and meet regulatory requirements.

The main objective of Log Management is to collect and store log data from various systems and applications within an organization's IT infrastructure in order to be able to properly meet the needs of other SOC services.

The main technology used as part of the Log Management service is SIEM.

We have the following approach to building a trustworthy Log Management service for our clients:

People	Process	Technologies
• Team workshop	Consulting service based on choosing the most appropriate log sources, retaining and maintaining them, and setting the baseline requirements for logging and monitoring security events.	Consulting services including recommendations for configuring log sources and monitoring log availability

Log Management service options

Incident Monitoring service

Incident Monitoring

Detecting incidents in a timely manner is at the core of any Security Operations Center, and arguably its most important function. Prioritizing Incident Monitoring activities is crucial for ensuring that the SOC is prepared and adequately staffed. Cyber incidents have been occurring as long as there have been computers and networks.

Incident Monitoring analysts are on the front line when it comes to determining current events, their locations, and how they unfold. They are responsible for taking the most appropriate actions to counter any such incidents.

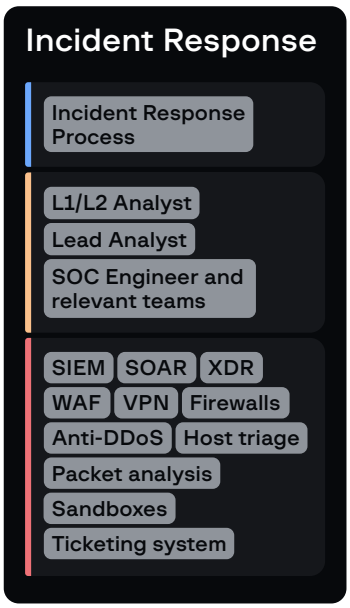
The main objective of Incident Monitoring is to detect security incidents as soon as possible and escalate them to the Incident Response team.

The Incident Monitoring service describes an approach to identifying, triaging, categorizing, classifying, prioritizing, analyzing, escalating, and notifying incidents. It also covers topics such as detection logic and use cases, detection tools, the roles and responsibilities of the L1/ L2 analyst teams, and the skills required in all these areas. The main security controls included in the technology section are SIEM, XDR, IDS, and NGFW.

We have the following approach to building an invaluable Incident Monitoring service for our clients:

People	Process	Technologies
• Blue team analyst training • Team workshop	Consulting service that covers Incident Monitoring process design and implementation, including detailed recommendations on detection use-cases	Group-IB XDR implementation

Incident Monitoring service options



Incident Response service

Incident Response

Much like the previous service, Incident Response is another essential SOC component because without a proper response to detected incidents, all other efforts become meaningless.

The main objective of Incident Response is to minimize the impact of security incidents on the business and IT environment and to restore the operation of any affected systems as quickly as possible.

The Incident Response service encompasses methods for managing and responding to incidents after they are detected by the Incident Monitoring team. This service explains how to contain, eradicate, and recover from incidents. It defines playbooks, incident reports, tools, roles, and the responsibilities of the parties involved, as well as the skills required for performing all Incident Response-related activities. The Technology section of this service covers a broad set of security controls and tools, such as host triage tools, packet analysis, sandboxes, XDR, SOAR, IRP, and more.

We have the following approach to building an effective Incident Response service for our clients:

People	Process	Technologies
• Incident responder training • Team workshop	Consulting service that covers Incident Response process design and implementation, including the development of detailed playbooks	Group-IB XDR implementation

Incident Response service options

Threat Hunting service

Threat Hunting

Between 80 and 90% of threats can be detected using classic detection methods. However, classic methods are powerless against the remaining 10–20% of threats (caused by lack of enterprise-wide visibility, detection coverage gaps, missing or ineffective security controls, misconfigurations, insider threats, advanced tactics, and unknown threats) . This is where Threat Hunting comes into play.

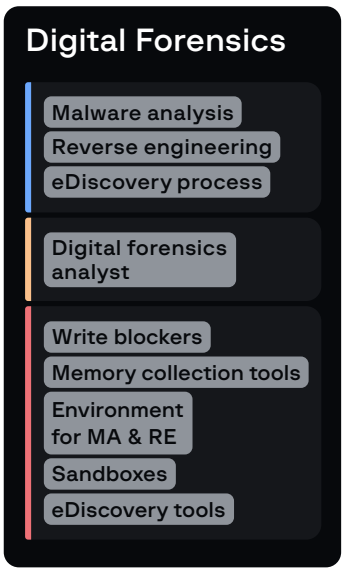
The main objective of Threat Hunting is to proactively search for signs of malicious activity within an organization's systems and networks and to identify patterns and anomalies that could indicate the presence of a threat. Threat Hunting involves data analysis and visualization to help identify new and unknown threats and to stay ahead of attackers.

This service involves identifying threat-hunting triggers, generating hypotheses, collecting and analyzing data, and sharing findings and recommendations with the client's SOC team. In the early stages of the service, Threat Hunting teams create a Threat Hunting template, specify key indicators of compromise, and establish the main techniques and tools used. Additionally, the service describes the roles and responsibilities of threat hunters, as well as the skills required for a hunt to be successful.

We have the following approach to building a reliable Threat Hunting Service for our clients:

People	Process	Technologies
• Threat hunter course • Team workshop	Developing a Threat Hunting program including a) recommendations for hypothesis generation based on previously constructed or current threat landscape, b) event analysis methods, c) writing Threat Hunting reports and any other relevant documentation (e.g., Threat Hunting process, hunting templates), performance of preliminary incident response	Conducting threat hunts using the customer's security controls (host-based security controls, network-based security controls, CTI, data analysis tools, etc.)

Threat Hunting service options



Digital Forensics service

Digital Forensics

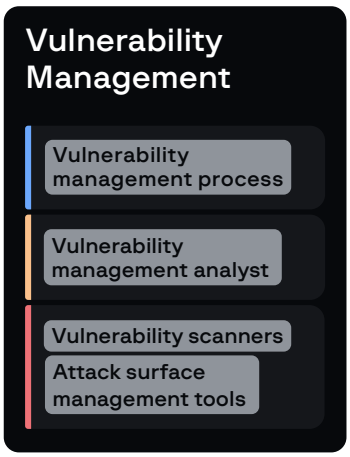
The main tasks during incident response are conducting an in-depth analysis of digital artifacts, performing malware analysis, and preserving evidence. This is where a Digital Forensics service will boost and enhance incident response.

The main objective of Digital Forensics is to investigate and analyze digital evidence in the event of a security incident. This involves implementing a forensic evidence lifecycle including tools and techniques in order to gather, preserve, analyze, document, retain, and review, and create a chain-of-custody.

The Digital Forensics service involves identifying, acquiring, processing, and analyzing digital evidence of a crime or attack. This includes malware analysis, reverse engineering, and analyzing other digital artifacts. The service covers the forensics process and toolset, the responsibilities of a forensics analyst, and the skills required to perform this role. There are many different tools involved in Digital Forensics, such as write blockers, environments for malware analysis and reverse engineering, and tools for memory and disk collection and analysis. As a result, the service reveals and produces new IOCs as well as other digital artifacts that can be presented in court. Recommendations for further action are also given.

People	Process	Technologies
• Windows DFIR Analyst Course • Linux DFIR Analyst Course • Network Forensics Analyst Course • Team workshop	Consulting service that includes designing Digital Forensics process (collecting evidence sources , gathering and recovering evidence, analyzing evidence, translating findings into the language of the governing law, reporting and handover, expert witnessing)	Recommendations for Digital Forensics toolsets and the best practices for their use

Digital Forensics service options



Vulnerability Management service

Vulnerability Management

There are billions of vulnerabilities — flaws or weaknesses, in assets, that could potentially result in a security breach or event. Vulnerabilities can originate from various sources, including the way that assets are designed and implemented, as well as the procedures and controls aimed at securing them. While all bugs have unintended effects on assets, vulnerabilities are bugs that have the potential to be maliciously exploited. To address vulnerabilities effectively, it is essential to design a Vulnerability Management service.

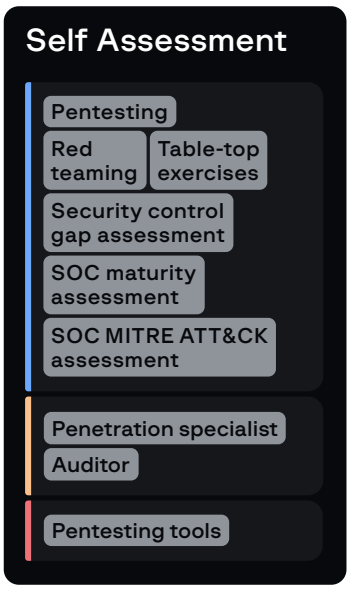
The main objective of Vulnerability Management is to identify, assess, prioritize, and remediate security vulnerabilities in an organization's IT infrastructure to prevent adversaries from exploiting them.

The Vulnerability Management service focuses on identifying vulnerabilities and associated risks. It defines the assets and infrastructure elements involved in vulnerability scans, the scoring of discovered vulnerabilities, mitigation methods, and the types of vulnerability scanning. It also defines the Vulnerability Management team and its roles and responsibilities, as well as the skills required for vulnerability analysts and the requirements of vulnerability reports. The main technologies used are vulnerability scanners and attack surface management tools.

We have the following approach to building a stellar Vulnerability Management service for our clients:

People	Process	Technologies
• Vulnerability Management Analyst Course • Team workshop	Consulting service that includes designing a Vulnerability Management process (assessment, prioritization, remediation, verification, management reporting)	• Recommendations for Vulnerability Management toolsets and the best practices for their use • Group-IB Attack Surface Management

Vulnerability Management service options



Self Assessment set of services

Self Assessment

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

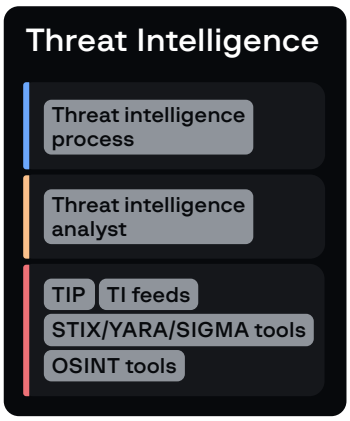
Sun Tzu, The Art of War

Self Assessment addresses the first piece of advice for success from Sun Tzu: **"know yourself"**. In other words, a Self Assessment allows customers to understand their weaknesses and gaps so that they can defend themselves against threats more effectively.

The Self Assessment service includes several different sub-services such as penetration testing, red teaming, security controls gap assessment, compromise assessment, security awareness, SOC/SOC maturity assessment, and MITRE ATT&CK assessment (coverage assessment).

To conduct a comprehensive Self Assessment, we offer our customers the following options:

1. SOC coverage assessment (MITRE ATT&CK SOC Assessment)
2. SOC capability and maturity assessment (SOC-CMM)
3. Penetration testing
4. Red teaming
5. Purple teaming
6. Security controls gap assessment
7. Compliance audits according to local regulatory requirements (MEA, APAC, Europe)
8. Compromise assessment
9. Threat intelligence assessment
10. Table-top exercises



Threat Intelligence service

Threat Intelligence

Threat intelligence addresses the second piece of advice for success from Sun Tzu: **"know your enemy"**, which means understanding the tactics, techniques, and motives of threat actors.

The main objective of threat intelligence is to proactively identify and understand potential cyber threats and risks to an organization's assets, systems, and network infrastructure and provide the best course of action to address these threats and risks.

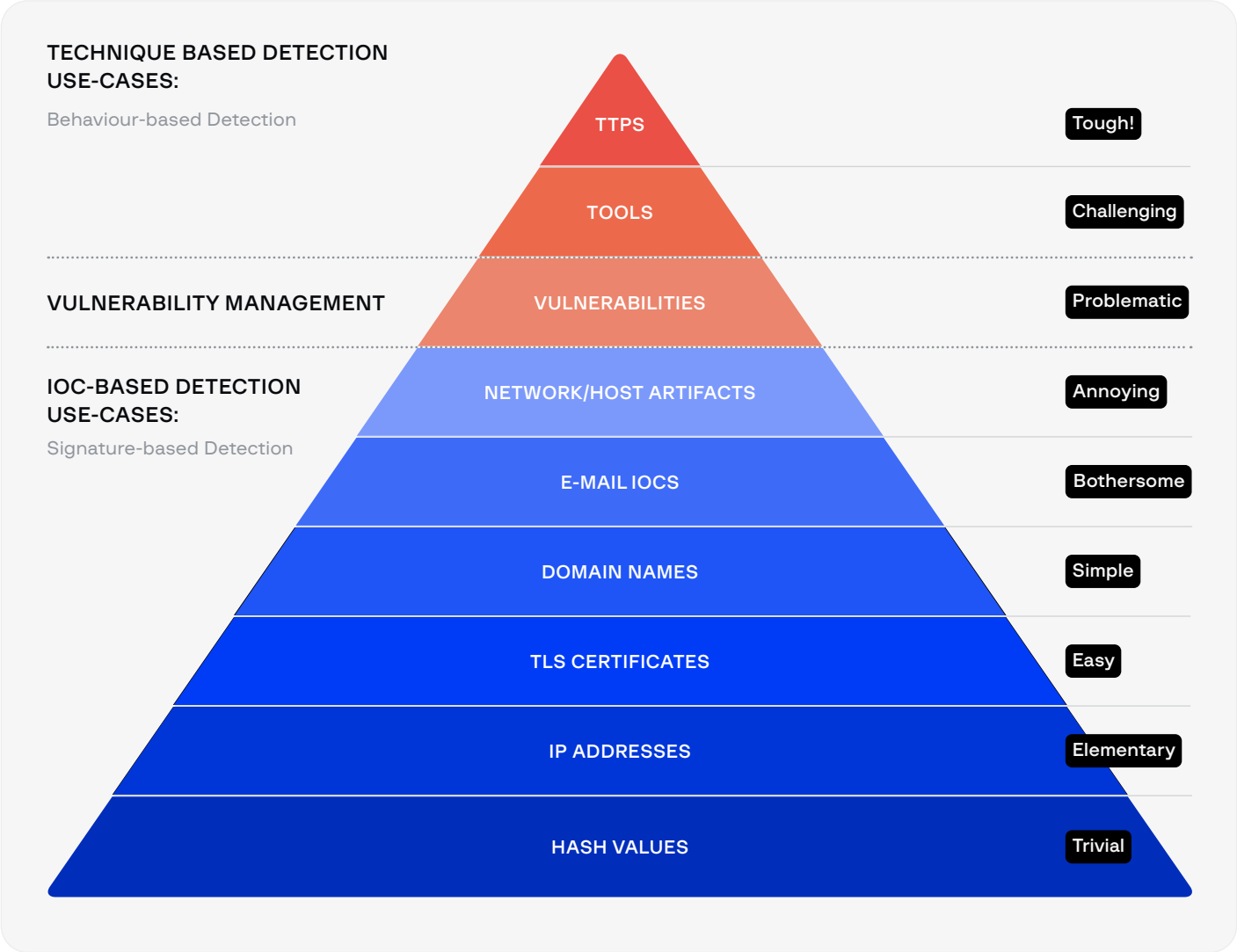
Threat intelligence is the complex service of planning, collecting, processing, analyzing, and disseminating information about potential threats to an organization. This service defines the main stakeholders, the priority intelligence requirements, the collection sources, the methods for collection, processing, and analysis, the intelligence delivery methods and formats, and the threat landscape. It also covers the tools, roles and responsibilities of the threat intelligence team and the skills required for performing day-to-day intelligence operations.

Since the main idea behind this white paper is an intelligence-driven SOC, let's dive into some threat intelligence concepts that will help us understand the value of threat intelligence for SOCs.

Enhanced Pyramid of Pain

The **Pyramid of Pain by David Bianco** is a CTI concept that describes a hierarchical approach based on the various attacker attributes that are used during an intrusion. The pyramid is made up of several layers, each of which represents a different level of how easily the adversary could change anything they use. The idea is that by focusing on the layers at the top of the pyramid, organizations can more effectively disrupt and deter cybercriminals while also making it more costly and difficult for them to carry out attacks.

As part of our consulting and training services, we have taken inspiration from Bianco and developed the **Group-IB Enhanced Pyramid of Pain:**



Enhanced Pyramid of Pain by Group-IB

We introduced three new layers:

1. **Vulnerabilities.**
   In our opinion, in Bianco's pyramid vulnerabilities are undeservedly not presented as a separate level, although vulnerability exploitation is an inherent part of almost every intrusion. Often threat actors can be attributed based on their use of vulnerabilities alone. Exploring 0-day vulnerabilities and developing exploits for them is quite **Problematic.**
2. **Email IOCs.**
   Things such as phishing email addresses, email content, and headers are considered email IOCs. For adversaries, building new email infrastructure can be **Bothersome.**
3. **TLS certificates.**
   Adversaries apply TLS certificates to their infrastructure, for example to place them on C2 servers and thereby ensure an encrypted connection. For adversaries, generating new certificates is an **Easy** task. Threat intelligence analysts are able to identify adversary infrastructure by searching for TLS certificate fingerprints:

Explore the solution ↗

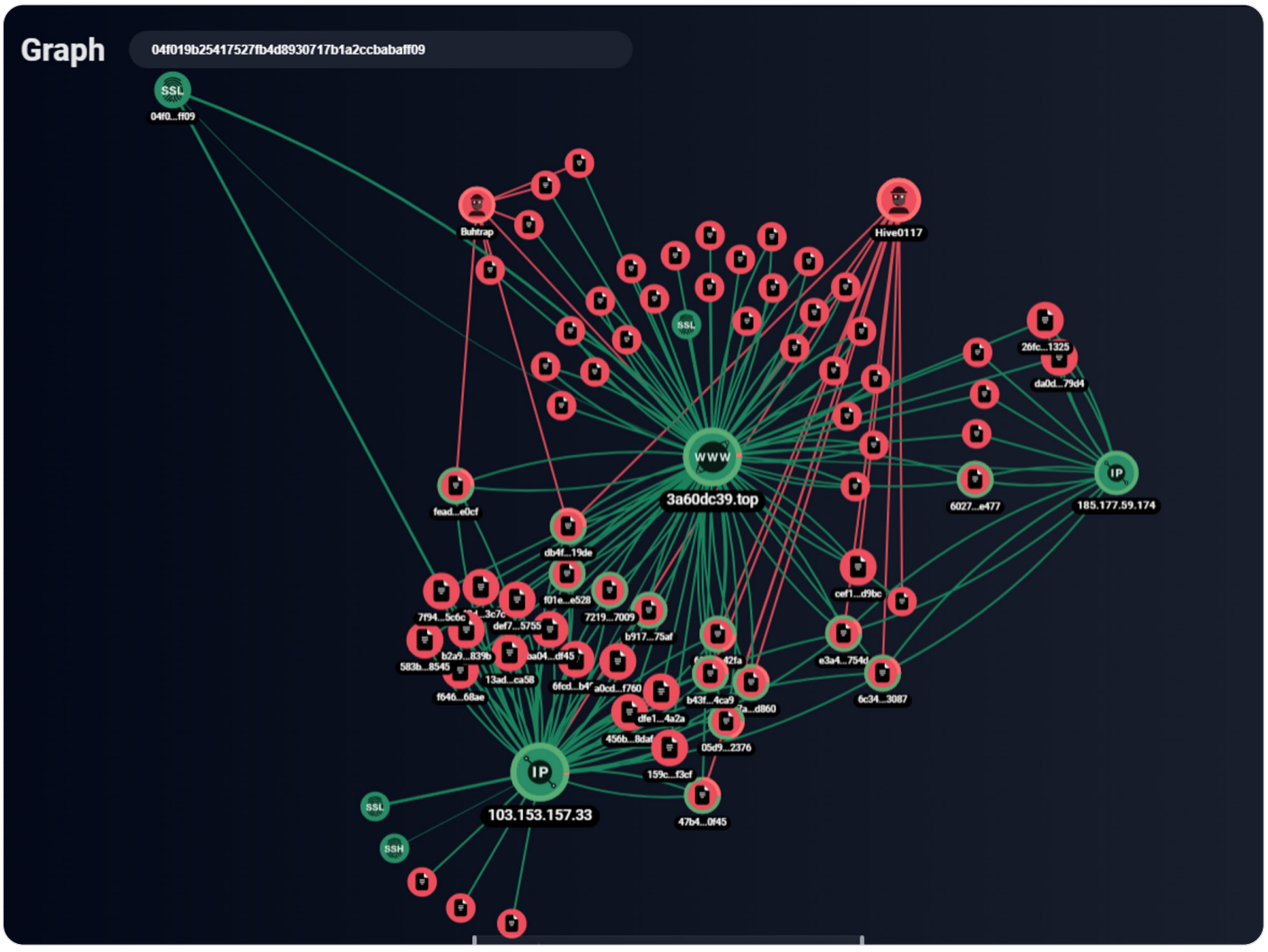


Figure 2. Example of graph analysis using a TLS certificate fingerprint search from Group-IB Threat Intelligence

To combat adversaries on every layer of the pyramid shown above, we can use the following approaches:

1. **TTPs and tools layers.**
   We create technique-based detection use cases that mean we can implement behavior-based detection. For example, based on this approach, we will monitor PowerShell execution, Windows Registry Keys modification, etc.

Here is an example of such a technique-based detection use case:

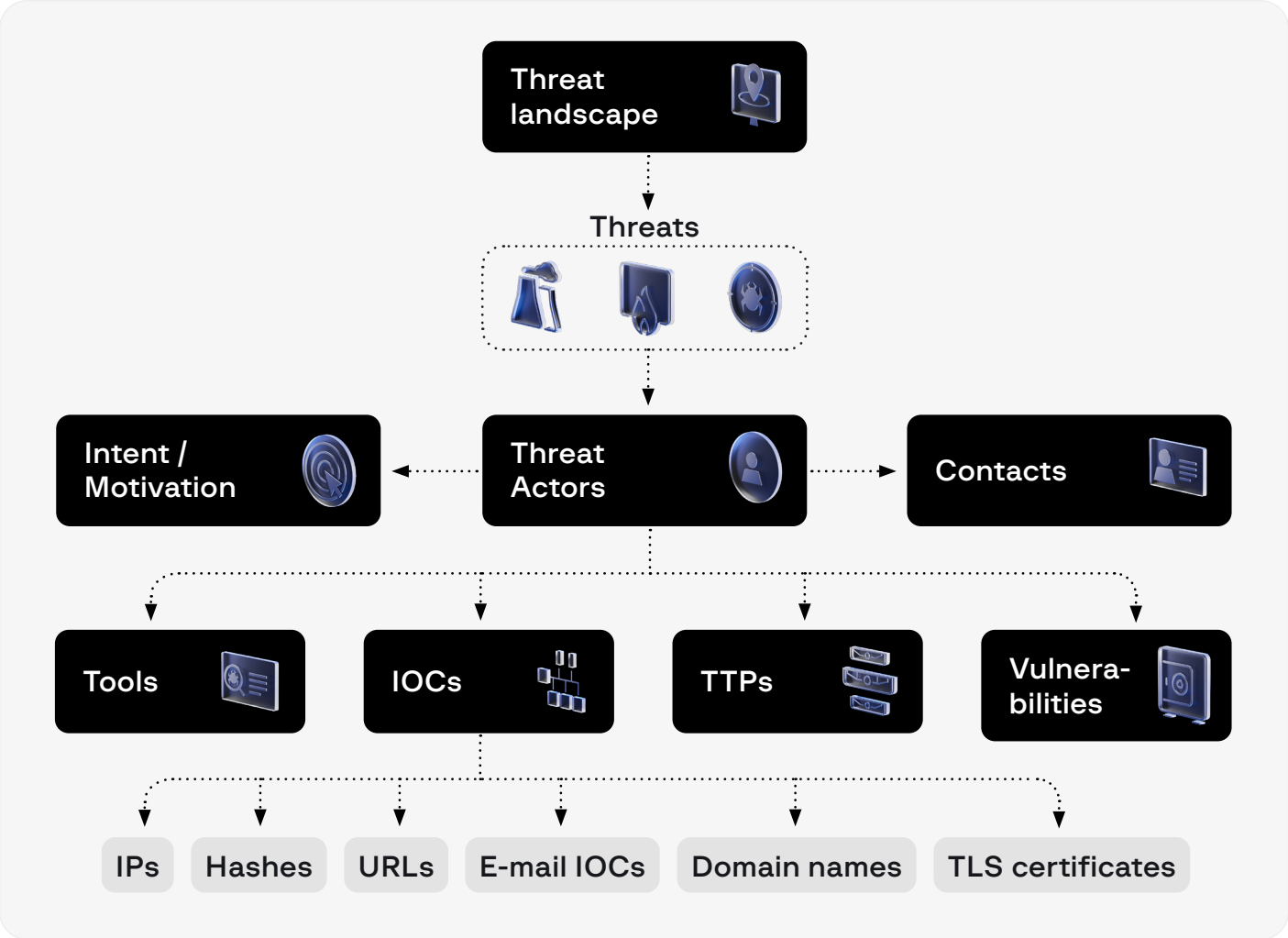
Incident Category	Use-case ID	MITRE Att&ck ID	Technique	Tactic	Priority	Items to monitor	Log source	SIEM Rule
Intrusion/ Malware	55	T1053	Scheduled Task/Job	Execution, Persistence, Privilege Escalation	Medium	Processess: at.exe, schtasks.exe	MS Windows Event Logging - PowerShell MS Windows Event Logging XML - Security MS Windows Event Logging XML Sysmon 8/9/10	97

Example of a technique-based detection use case

2. **Vulnerabilities layer.**
   We must properly implement a Vulnerability Management service with the relevant tools (vulnerability scanners, attack surface management tools, etc.) and related people and processes.
3. **From the "Network host/artifacts" to the "Hash values" layers.**
   We create IOC-based detection use cases for SIEM enriched with TI feeds – for example, "TOR nodes" and "C2 domains,". Signature-based detection (such as IDS, AV, and email security gateways) perfectly covers these layers for both detection and mitigation capabilities.

Threat landscape

The threat landscape is a combination of relevant threats and threat actors (based on industry, region, and partners), which is then divided into TTPs (Tactics, Techniques, and Procedures), the tools used by the threat actors (such as malware and living-off-the-land tools), IOCs, intent and motivation, and contact details for the threat actors (such as crypto wallet addresses, usernames on forums, and email addresses), as well as the vulnerabilities used in their intrusions.



Architecture of the threat landscape

The Threat Landscape is specific to the platform (Windows, Linux, Android, etc.) and infrastructure type (Enterprise/ICS/Mobile, in line with the terminology of MITRE ATT&CK).

By combining all tactics, techniques, and procedures relevant to your company, you can build a **Threat Landscape Techniques Heat map.** This allows different SOC teams (such as Incident Monitoring, SOC Architecture & Engineering, and SOC Management) to make informed and prioritized decisions about detection and mitigation strategies.

To build the heat map, we need to extract techniques from all related threat actors in the region/country (for example, MEA, KSA), industry-related techniques (for example, finance), and techniques from previous incident reports (successful intrusions or penetration/red teaming reports), then add the Top 10 techniques worldwide and exclude any irrelevant techniques (for example, Linux, Office 365, etc.).

Techniques based on Region/Country threats + Techniques based on Industry Threats + Techniques from previous incidents + Top-10 techniques - Irrelevant techniques (OS, Software) = Threat Landscape Techniques Heat-map

Threat Landscape Techniques Heat map

According to our own research, the latest Top 10 Techniques worldwide for Enterprise and Windows OS are:

1. PowerShell
2. Scheduled Task
3. Service Execution
4. Registry Run Keys
5. Disable or Modify Tools
6. Rundll32
7. OS Credential Dumping
8. Remote System Discovery
9. Remote Desktop Protocol
10. SMB/Windows Admin Shares

The well-known tool **MITRE ATT&CK Navigator** can be used to obtain the final summarized heat map.

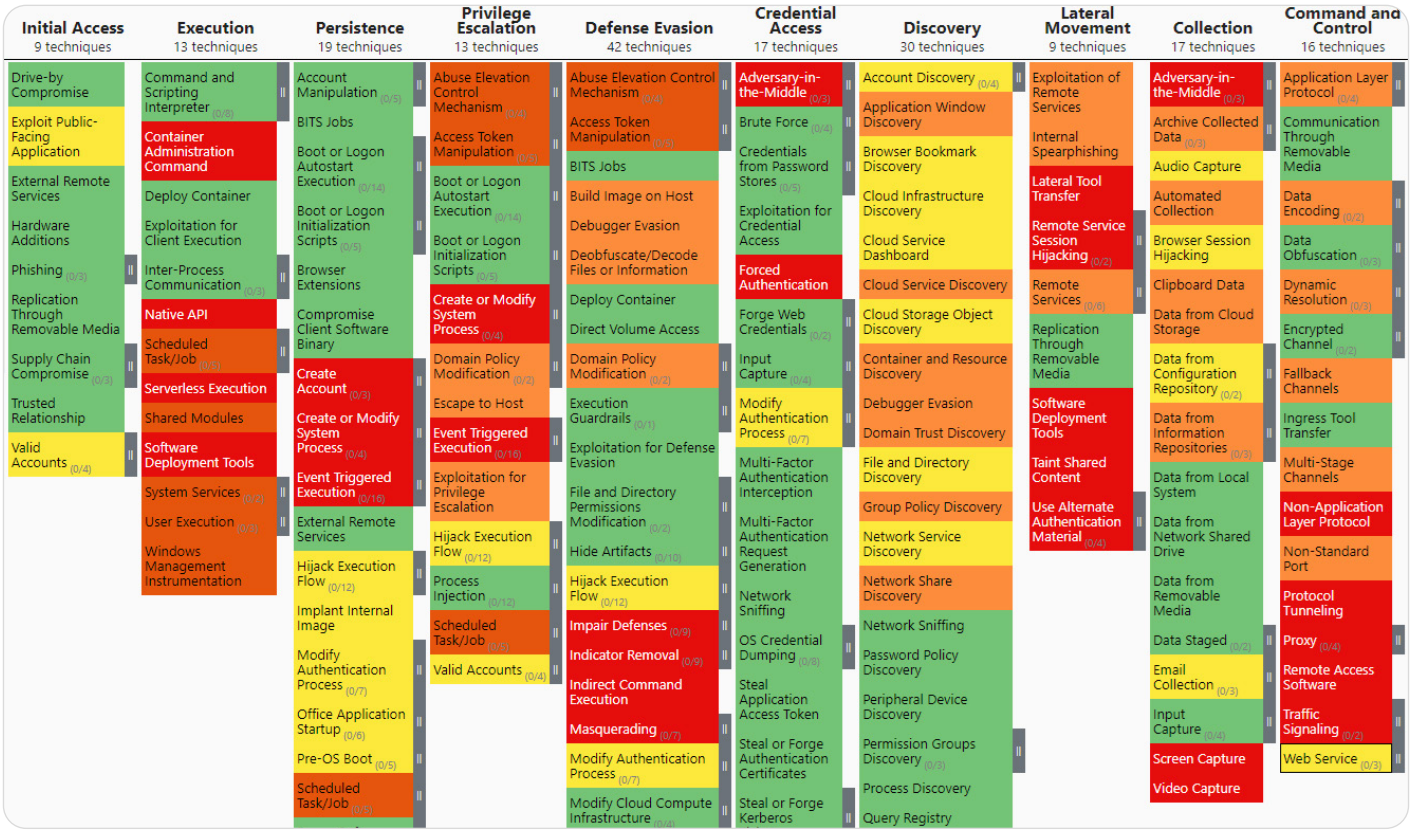


Figure 3. Threat Landscape Techniques Heat Map

It is essential to highlight that constructing such a heat map (and other components of the threat landscape) is not a one-off task; it is a regular process. This is because new threat actors appear, old threat actors change their techniques and tools, and new threats emerge in industries and countries. All of this in combination creates an **evolving threat landscape.**

Later we will show how heat maps can enhance MITRE ATT&CK SOC Assessments.

When building a foolproof threat intelligence service for our clients, we use the following approach:

People	Process	Technologies
• Threat Intelligence Analyst Course • Team workshop	Consulting service that includes developing a threat intelligence program, including developing priority intelligence requirements, developing a threat landscape, threat modeling, and more.	Implementing Group-IB Threat Intelligence

Threat intelligence service options

02

ADDRESSING TODAY'S SOC KEY CHALLENGES

According to the **latest SANS SOC Survey 2023**, most SOCs face several key challenges. We will focus on the top three and show how we help our customers to address them.

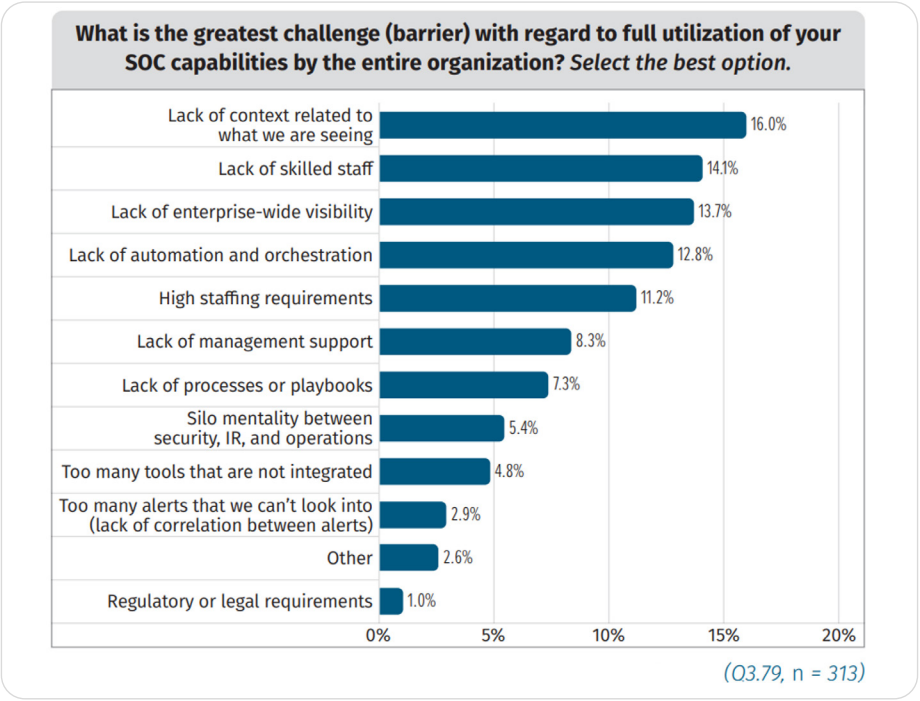


Figure 4. SANS SOC Survey 2023 Key Challenges

1. **"Lack of context related to what we are seeing".** Typical questions in every SOC/SOC's routine include: "What do we know about this IP address?", "Which malware family is this file hash related to?", and "Who is the system owner of that internal IP?" The simplest way to tackle issues related to external artifacts is to establish a threat intelligence program, that will be described at the end of this ebook. For internal artifacts, determine all your assets by using asset management solutions, conducting interviews with system owners, and choosing effective vulnerability management and attack surface management solution.
2. **"Lack of skilled staff".** To address this challenge, we offer our customers regular training and help them sharpen every role, whether it's a SOC Manager, Incident Responder, Blue Team Analyst, or other. We also have the resources needed to organize any additional technical training upon request. Moreover, as part of our consulting services, we help our clients build their SOC services from scratch, with a focus on coaching personnel, and help them to understand their daily tasks and job routing, relying on supporting documentation (Processes, Standard Operating Procedures, etc.). The idea behind our consulting services is to ensure that all teams know exactly what to do. We achieve this through interactive workshops — supporting documentation is only a part of the process.

Discover Group-IB Training Programs ↗

Explore the solution ↗

3. **“Lack of enterprise-wide visibility”.** In recent years, the attack surface has been expanding to include cloud infrastructure, VPN users, B2B/3rd parties, OT/ICS, and more. One of the cornerstones of cybersecurity is to know what you are protecting and why.
In the case of external assets (such as IP addresses, domains, subdomains, SSL certificates, services, ports, software, and storage systems), we can leverage attack surface management solutions.
For internal assets, we can build a Vulnerability Management service alongside any asset management solution. We also recommend performing regular OSINT drills against your company to be aware of your public profile, i.e., events, procurements, public relations, media activities, exposed data, job announcements, requests for proposals for specific vendors and equipment in your supply chain, and more. Adversaries will be looking into these so that they can target you more easily. By seeing what threat actors see, you will be able to **deter them in the reconnaissance phase.**

Figure 5. Group-IB Attack Surface Management dashboard

03

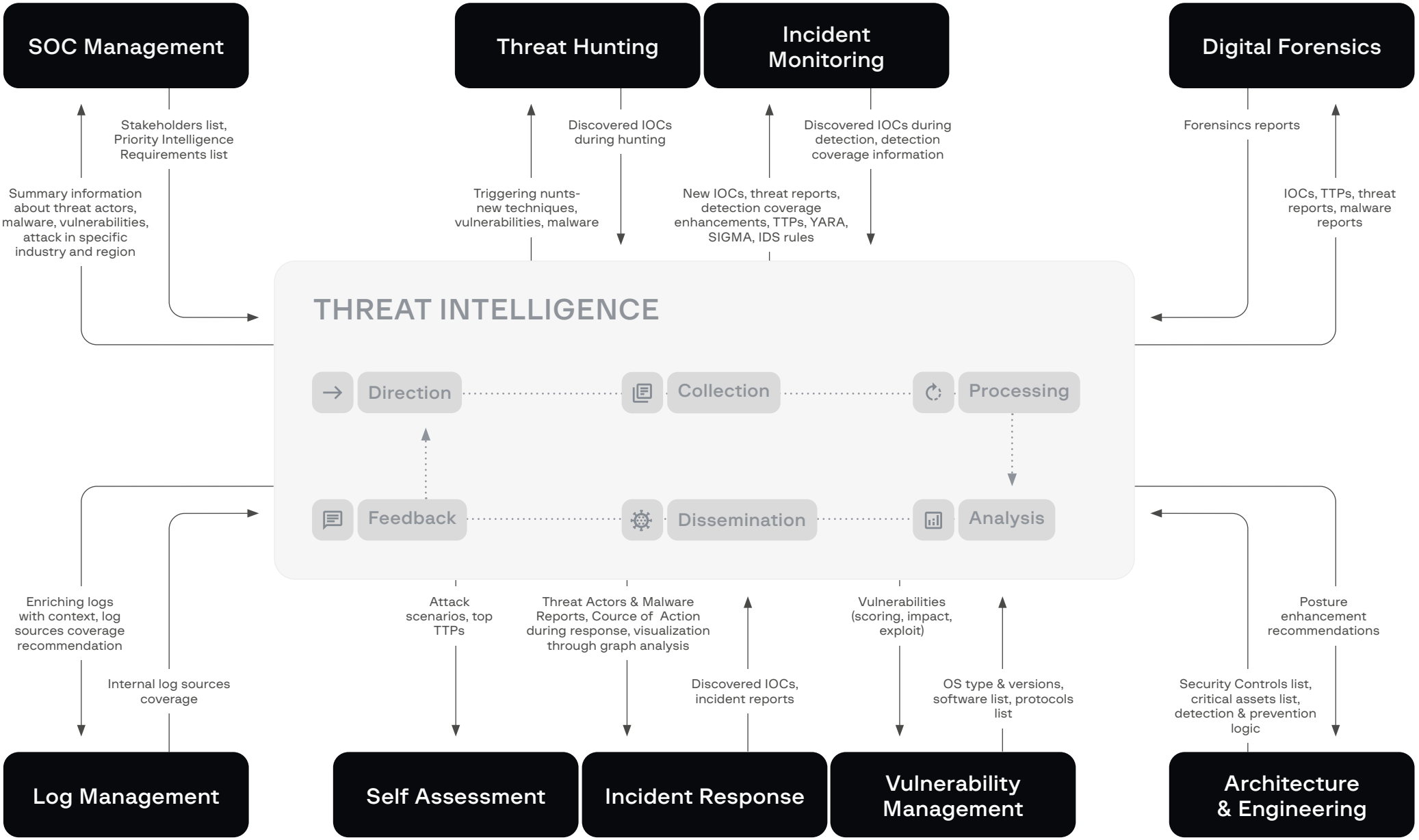
BOOSTING SOC SERVICES WITH THREAT INTELLIGENCE

Implementing threat intelligence in your company might be a challenging task without a clear vision and understanding of who will benefit from it and how.

Threat intelligence can be a valuable tool for businesses. Here's why:

1. **Improved security posture.**
   By regularly collecting and analyzing data on potential threats, businesses can improve their overall security posture and better protect themselves from cyber attacks. This may involve identifying and mitigating vulnerabilities, improving incident response processes, and implementing stronger security controls.
2. **Reduced risk of data breaches.**
   By using threat intelligence to identify and respond to potential threats, businesses can reduce the risk of experiencing a data breach. This helps protect sensitive data and prevent the financial and reputational damage that can result from such a breach.
3. **Enhanced compliance.**
   Most businesses must comply with various regulations and standards that require them to maintain a certain level of security. By using threat intelligence to identify and respond to potential threats, businesses can better meet these requirements and enhance their overall compliance posture.
4. **Increased efficiency.**
   Threat intelligence helps businesses prioritize their efforts and allocate resources, leading to increased efficiency. By identifying and responding to the most critical threats first, businesses can protect themselves better without overburdening their security and IT teams.
5. **Competitive advantage.**
   By using threat intelligence to identify and respond to potential threats, businesses stand out from their competitors and demonstrate their commitment to security. This can be a key factor in attracting and retaining customers and partners.

Let's explore in detail how various teams within a SOC can reap the benefits of integrating threat intelligence into their workflows.



Interactions between threat intelligence and other SOC services

SOC Management

A SOC manager is responsible for the security operations team and reports to the CISO (Chief Information Security Officer), who is the main person responsible for information security in a company.

Both SOC Managers and CISOs must be capable of making strategic data-driven decisions, and threat intelligence can help them in many ways.

Here is an overview of the challenges they face and potential solutions:

Challenge	Solution
Identifying the attacker's profile, intentions and tools	Obtain information about various threat actors and their tools, methods, and intentions by leveraging TI and illustrating your own threat landscape.
Choosing which security controls to invest in first	Based on the threat landscape (and corresponding technique heat map) and existing security controls, it is easy to outline gaps in your security environment and make a weighted decision about implementing new security controls. Some vendors also provide the MITRE ATT&CK coverage map to help customers better understand their own capabilities.
Summing up what we know about a threat actor	Generate a summary of the threat actor's intent, TTPs, tools, and contacts.
Summing up what we know about the malware	Generate a summary of malware's capabilities, impact, distribution methods, and behavior.
Ascertaining exposure to a new zero-day vulnerability.	Get all the relevant information about scoring, impact, OS, exploit availability aligned with your own infrastructure (OS, software).

Architecture & Engineering

As mentioned above, SOC architecture and engineering focuses on the proper design and configuration of all related security controls. The table below shows some challenges that can be solved with the help of threat intelligence.

Challenge	Solution
Defining which SIEM rules to enable	Drawing on the concept of the Enhanced Pyramid of Pain, a SOC Engineer — with the support of a SOC Architect — can design and configure IOC-based detection use-cases and technique-based detection use-cases.
Identifying which security features on security controls to configure	Based on techniques and sub-techniques from the Threat Landscape, specific detection and mitigation recommendations aligned with security controls in your infrastructure can be easily extracted.

Log Management

Log Management can be improved by threat intelligence in many ways. By integrating SIEM with IOCs provided by threat intelligence, Log Management can help with incident monitoring and finding information about specific artifacts. It also speeds up incident triage.

Moreover, based on techniques used by threat actors these days, threat intelligence can help in choosing and prioritizing relevant log sources. The table below describes some typical Log Management challenges and solutions to give an idea of the measures that can be taken:

Challenge	Solution
Being overwhelmed with logs or not knowing which logs need to be collected first	Based on the Threat Landscape heat map, you can identify prioritized techniques, which in turn helps to understand which log sources are needed to cover these techniques. For example, to properly detect the PowerShell technique, logs are required from endpoints, not from WAF or NGFW.
Not knowing which types of logs need to be monitored	Security logs, application logs, system logs, authentication logs, traffic logs... There could be many different types of logs on the selected log source. Again, based on prioritized techniques from the threat landscape, you can dive into the description of each technique and determine which log types need to be monitored. Following the example with PowerShell execution, you might consider collecting Windows Security Log, Sysmon Logs, etc. If you already have EDR/XDR on your endpoints, it is likely that they cover this specific technique, and all you need to do is connect your EDR/XDR to the SIEM and configure the relevant rules. One more piece of advice: when choosing an EDR/XDR solution, ask the vendor for the MITRE ATT&CK Coverage Map so that you are aware of all its capabilities.
Defining what specific events should be monitored in the collected logs	Each log contains different types of events, and not every event will be useful. On example of PowerShell: Event ID 4688 from Windows Security Logs and EventID 1 (ProcessCreate) from Sysmon (searching for powershell.exe) can be options.

Incident Monitoring

Incident Monitoring involves day-to-day monitoring of incidents, detecting suspicious activity, triaging incidents, categorizing and prioritizing incidents, analyzing incidents, escalating incidents, and notifying any relevant parties. While investigating incidents, security specialists may encounter various challenges:

Challenge	Solution
No information about the specific IP address, domain name, or URL. Searching for this information in several threat data sources can be very time-consuming.	Enrich your SIEM with the IOCs provided by threat intelligence to easily find information about specific artifacts and make incident triage faster.
A new threat has emerged, but you are not sure whether you are protected against it.	Integrate your security controls with threat intelligence and enrich them with the following: 1. IDS/IPS → IDS rules (Snort/Suricata signatures) 2. AV/EDR/XDR → YARA rules 3. SIEM → IOCs, SIGMA rules 4. Firewalls/Proxy → IOCs (text, CSV) 5. SOAR → IOCs (text, STIX, CSV) Get detailed information about new attacks and threat actors specific to your company.
Putting together information about specific malware and how to detect it	Get IDS/IPS/YARA rules and other observables related to the malware.
Boosting triage speed	Intelligence provides Security Operations Center (SOC) analysts with the context they need to classify and prioritize all generated alerts using risk scoring in detected observables.

Incident Response

Incident Response is about managing and responding to security incidents. The main goal is to minimize the impact of a security incident and restore normal operations as quickly as possible. This may involve identifying and containing the incident, gathering information to understand its scope and cause, and implementing measures to prevent it recurring. The Incident Response team is also responsible for communicating with stakeholders and providing regular updates about the incident and its resolution. The main benefit of implementing TI for Incident Response is reducing the time it takes to investigate and respond to threats. Let's take a look at the key challenges incident responders face and how they can be solved by applying the power of threat intelligence:

Challenge	Solution
No information about the specific IP address, domain name, or URL. Searching for such information in several threat data sources can be very time-consuming.	Enrich SIEM/SOAR/IRP with the IOCs provided by threat intelligence to easily find out information about specific artifacts and make incident triage faster.
Ascertaining what the malware discovered actually does.	Obtain information from TI about the malware in question (type, impact, configurations, detection, behavior, etc.)
Forecasting the adversary's next steps and deciding how to prevent them.	Based on MITRE ATT&CK or Kill Chain identify the current phase of adversary actions, TTPs, and then you will find out what he is able to do next, and how to mitigate their actions.
Containing the adversary	Based on the adversary techniques discovered, identify a possible course of action (for example, disable a compromised account, terminate a session, stop a process, etc.).

Threat Hunting

Threat Hunting involves proactively searching for signs of malicious activity within an organization's systems and networks. Threat hunters use a variety of tools and techniques, including data analysis and visualization, to identify patterns and anomalies that could point to a threat. The challenges they encounter include sifting through large amounts of data to find relevant information, identifying new and unknown threats, and keeping up-to-date with the latest attack techniques and tactics. Threat intelligence can help a Threat Hunting team by providing information about the latest threats, including how they are being used in attacks and what indicators of compromise (IOCs) to look for. This information helps the team be more effective in their work and stay ahead of attackers.

Challenge	Solution
Having the latest information about new threats in order to conduct threat hunts based on them.	The initial stage of Threat Hunting is when a trigger event is identified that suggests the possibility of a security threat. This event could be a security incident, a change in the security landscape, or the identification of a new threat. Threat intelligence keeps the Threat Hunting service up-to-date about recently emerged threats.
A new threat has emerged, but you are not sure how relevant it is to your company.	One of the cornerstone principles of threat intelligence is that any information should be relevant — to your organization, industry, region, or country. A bank in the US will not be interested in ICS attacks directed at MEA industrial companies. Sticking to relevant intelligence enables organizations to focus on the important things and not waste time on details that don't affect them. A well-built threat intelligence program highlights only the relevant threats (actors, malware, attacks, etc.).
Preparing correct specific hunting queries while conducting threat hunts can take up a lot of time	Threat intelligence provides detailed information about the procedures used by adversaries. For example, imagine that you are notified that the APT called Conti Group, which is relevant to your organization, recently started using the Windows Management Instrumentation technique. After searching for a relevant threat intelligence report, you come across a useful report titled "CONTI ARMADA: THE ARMATTACK CAMPAIGN." The report contains an example of using this technique: "wmic /node:%local_ip% process call create "cmd /c rundll32.exe C:\ windows\System32\comsvcs.dll, MiniDump 508 C:\ProgramData\lsass.dmp full"", which in turn can be used in your hunt.

Digital Forensics

Digital Forensics involves investigating and analyzing digital evidence when a security incident occurs. Specialists use various tools and techniques (such as data recovery, disk imaging, and network analysis) to gather and analyze evidence. The challenges they encounter include identifying and storing evidence, reconstructing incident timelines, and dealing with large volumes of data. Threat intelligence can help Digital Forensics teams by providing information about the latest attack methods and tactics, including what indicators of compromise (IOCs) to look for. Such information helps the team more effectively identify and store evidence, reconstruct incident timelines, and identify the attackers responsible for the incident.

Challenge	Solution
Identifying the attackers and learning about them	Identifying the attackers is a common task for CISOs, CEOs, and SOC managers after an intrusion. Threat intelligence can help answer this question by making it possible to search through any collected big data and to attribute — with a high degree of probability — the threat actor responsible for the intrusion. Examples of such assistance include specific filenames, extensions, contacts in ransomware notes, and the techniques used by the perpetrators.
Establishing what data was stolen	Another frequently asked question that arises after an intrusion is: What data was stolen? Threat intelligence helps Digital Forensics by monitoring DLS sites, dark web channels in messengers, and hacker forums. It also provides details about the stolen information (account names and passwords, PII, credit card numbers, etc.).
Outlining how attacks can be prevented in the future	Each report prepared by the DFIR team should contain recommendations on how to enhance the organization's security posture. Threat intelligence can provide detailed information on Digital Forensics for possible detection and mitigation capabilities mapped to each type of artifact discovered during the intrusion (IOCs, techniques, vulnerabilities).

Vulnerability Management

Vulnerability Management involves identifying, evaluating, and mitigating security vulnerabilities in an organization's systems and networks. Specialists use tools and techniques to scan for known vulnerabilities and assess their potential impact. They may also work with developers and other teams to implement patches and other solutions.

The challenges they encounter include keeping up-to-date regarding new vulnerabilities, deciding which vulnerabilities to prioritize and address first, and ensuring that vulnerabilities are mitigated effectively. Threat intelligence helps Vulnerability Management teams by providing information about the latest vulnerabilities, including information on who is exploiting them in the wild and how. Such information can be extremely beneficial, especially in situations when vulnerability scanners don’t cover some systems or don’t scan them due to the risk of disruption.

In general, Threat Intelligence can provide Vulnerability Management teams with information about the following:

1. Operating system (OS) vulnerabilities
2. Software and web application vulnerabilities
3. Protocol vulnerabilities
4. Database servers vulnerabilities
5. Vulnerability prioritization based on specific vulnerabilities and exploits being mentioned on hacker forums and the dark web

In short, threat intelligence can help Vulnerability Management teams prioritize vulnerabilities and develop more effective mitigation strategies.

Self Assessment

Two main sub-services in Self Assessment greatly benefit from threat intelligence: MITRE ATT&CK SOC assessment and red teaming.

MITRE ATT&CK SOC assessment

The idea of a **MITRE ATT&CK SOC Assessment** is simple – it involves gathering information about all your data sources (log sources), security control configurations, and SIEM rules followed by generating MITRE techniques coverage heat maps and summarizing them. One summary heat map is created for each platform (Windows, macOS, Linux, etc.). Based on this assessment, you can make quick adjustments to your detection and mitigation measures.

We believe that the only component missing from this great approach is a Threat Landscape Techniques Heat Map — which shows prioritized threats relevant to your organization. The total number of techniques to consider will be reduced and you will be able to focus on the relevant ones.

This means that the resulting formula for each platform (Windows, Linux, etc.) might be as follows:

> “Threat Landscape Techniques Heat Map” + “Data sources map” + “SIEM rules map” + “Security controls maps (many)” = Final heat map

Red teaming

Red teaming can be significantly enhanced with threat intelligence in several ways. Threat Intelligence can be used to identify and understand potential cyber threats and risks to an organization's assets, systems, and network infrastructure. Combined with TI insights, red teaming can be used to simulate more realistic attack scenarios and identify weaknesses in an organization's security posture. Red teaming can also be improved with threat intelligence to keep up-to-date regarding the latest attack techniques and tactics, which helps red teams to create more effective attack scenarios. Additionally, TI can help red teaming to identify and prioritize the most critical vulnerabilities and attack vectors. Furthermore, many BAS (breach attack simulation) products can be integrated with MITRE Techniques to emulate them in your infrastructure by deploying agents on test workstations monitored using your in-house detection tools.

04

BUILDING A THREAT INTELLIGENCE PROGRAM

In their latest report titled **Hype Cycle for Security Operations, 2023,** Gartner highlights the following obstacles regarding threat intelligence:

- "Many organizations have no formal TI program or dedicated analysts to use TI solutions, like a TIP, or interpret the value from bespoke TI reports. They rather focus on indicators like IP addresses, domains and hash values, and allocate too few resources to human-readable or advanced TI solutions."
- "Organizations struggle to measure and justify the value of TI solutions. Lack of TI performance reporting will increase the likelihood of TI budget cuts or prohibition of program maturation"
- "Many organizations lack well-defined priority intelligence requirements (PIRs), which can lead to overinvestment in or underutilization of TI solutions."

Having discussed the importance of threat intelligence within a modern SOC and its main obstacles, let's elaborate on the key steps that should be taken to build your own threat intelligence program, regardless of the size or maturity of your SOC or organization.

1. **Define the stakeholders.**
   Stakeholders are the individuals, departments, and other interested parties who receive the threat intelligence. This could include all the aforementioned SOC teams and other teams such as the Anti-Fraud Team, the Legal Team, the Risk Management Team, and so on.
2. **Define the Priority Intelligence Requirements (PIR).**
   Priority Intelligence Requirements are the pieces of threat intelligence that help stakeholders close the knowledge gap and perform their mission. They might include "Adversaries impacting the telecom industry," "Ransomware," or simply "Malicious Domains."

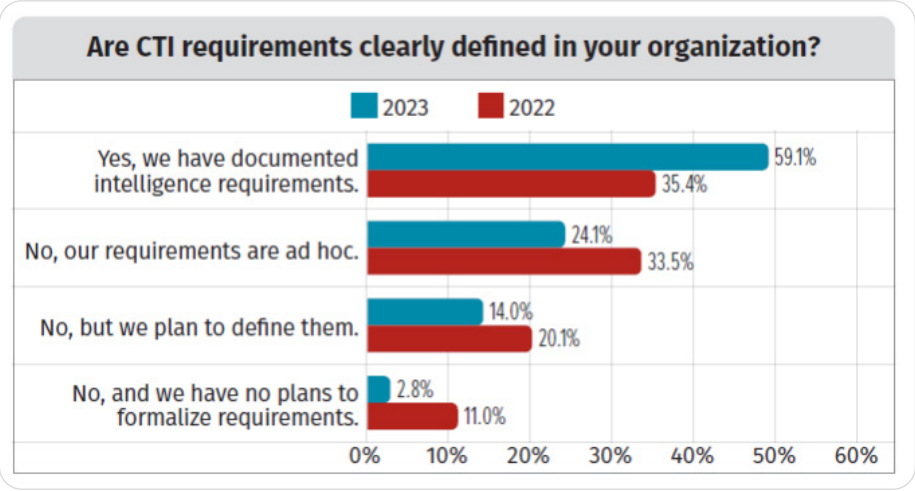


Figure 6. SANS 2023 CTI Survey: Trends in CTI requirements

3. **Collect information about critical assets.**
   Without a clear understanding of your critical business systems and assets (including the information stored on them, the operating systems, the software installed, and the access methods), it is almost impossible to properly align the threat landscape with your own infrastructure.

4. **Hire or train a threat intelligence analyst.**
   Cyber threat intelligence analysts collect and analyze multi-source information about cybersecurity threats as a way of developing an in-depth understanding and awareness of cyber threats and the Tactics, Techniques, and Procedures (TTPs) used by threat actors. They derive and report indicators that help organizations detect and predict cyber incidents and protect systems and networks from cyber threats. They also conduct extensive research and analyses for internal and external threat data and develop or contribute to courses of action based on their understanding of the threat.

5. **Identify and choose internal and external collection sources.**
   To satisfy every priority intelligence requirement, you should determine the available internal collection sources (endpoint protection, network security controls, SIEM, etc.) and external collection sources (open-source TI feeds, commercial threat intelligence providers, ISAC feeds, government agency feeds). Examples of open-source TI feeds include URLHaus, SSLBL, and FeodoTracker.

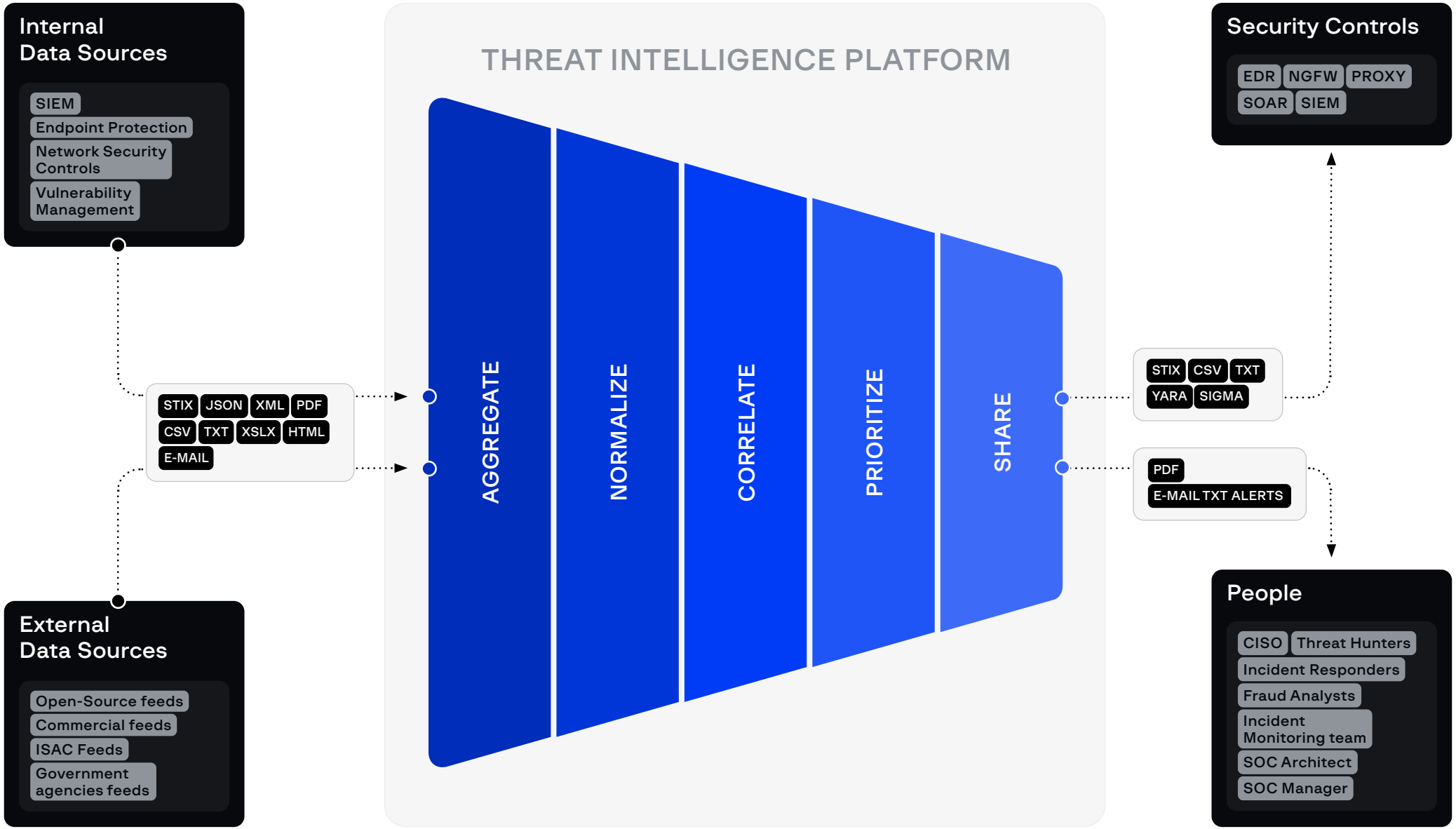
6. **Define collection methods and formats and collection frequency.**
   After identifying collection sources, you should ask yourself: how will I obtain this information, in what format, and how often? Gathering might involve manual extraction (simple copy-pasting) or automated methods (API, TAXII). The format might be STIX, JSON, XML, CSV, TXT, PDV, XLS, and more. Frequency-wise, it might be in real time, daily, weekly, monthly, etc.

7. **Classify collected information.**
   To determine the rules for potentially re-sharing threat intelligence, stakeholders should follow the **Traffic Light Protocol (TLP) classification scheme.**

8. **Consider implementing a threat intelligence platform.**
   A threat intelligence platform aggregates, normalizes, correlates, prioritizes, and shares threat intelligence in your organization. There are plenty of open-source platforms (such as MISP, OpenCTI, etc.) as well as commercial ones.

   As a rule of thumb, consider implementing a threat intelligence platform in the following cases:

   - You have multiple threat intelligence collection sources.
   - You want to not only consume but also produce your own threat intelligence.
   - You need to integrate threat intelligence with various security controls.
   - Due to in-house policies, internet access is restricted so you must manually extract information from external collection sources and import it into the TIP.



Architecture of a threat intelligence platform

9. **Identify the most appropriate analysis methods.**
   Every priority requirement as regards threat intelligence calls for a different analysis method. For example, in the case of domains, it might be as simple as a checklist: WHOIS information, passive DNS records, and graph analysis. In the case of threat actors, trend analysis might be necessary – identifying and recording their last seen activities and determining their current status (active or inactive).

10. **Draft relevant documentation.**
    To support threat analysts in their daily work, draft a set of relevant documentation (policies, processes, standard operating procedures, RFI templates, etc.).

11. **Build and regularly track the threat landscape.**
    As previously described, the threat landscape is a cornerstone artifact in threat intelligence that should be created and updated regularly to identify new threats and threat actors. Irrelevant and outdated information should be removed from it.

12. **Identify attack scenarios.**
    The threat landscape provides an overview of all threats and threat actors, while attack scenarios provide specific information about how threat actors execute their intrusions step by step (based on either the Cyber Kill Chain or the MITRE ATT&CK Framework). This information can be easily found in threat intelligence reports.

13. **Define the best delivery methods, delivery formats, and delivery frequency.**
    For each PIR, you should define the best delivery method or methods (email, API, secure TI online portals, TIP GUI, TAXI, etc.), delivery formats (PDF, CSV, TXT, STIX, etc.), and delivery frequency (near real-time, daily, weekly, monthly).

14. **Start sharing your threat intelligence.**
    Implement sharing rules (TIP or TI portal) and start sharing threat intelligence with people and security controls.

15. **Gather feedback from stakeholders**
    To ensure that all stakeholders are satisfied, you should ask for feedback regularly. Here are some examples of questions you could ask: "How relevant was the content to your requirements?", "How actionable was the content to your requirements?", "Did you receive the information you needed on time?".

16. **Measure the efficiency of the threat intelligence program.**
    Measuring metrics is the perfect way to establish whether your TI program is efficient. Consider measuring the following metrics: MTTD and MTTR before and after TI implementation, number of new external campaign/threat groups tracked, number of actions taken using intelligence, number of incident response tickets directly attributable to intelligence, and more.

17. **Remove obsolete IOCs and inactive threat actors.**
    Each type of threat intelligence has its own TTL. For example, a malicious IP address could become benign within a few months after being released back to the ISP and reassigned to a new customer.

GROUP-IB SOC CONSULTING SERVICES PORTFOLIO

I. BUILDING

- SOC Program Development
- Cyber Threat Intelligence Program Development
- Cyber Fraud Program Development

II. ASSESSMENT, REVIEW & IMPROVEMENT

- SOC Maturity Assessment, Review & Improvement
- Threat Intelligence Program Assessment
- Cyber Fraud Program Assessment
- Security Controls Gaps Assessment
- MITRE ATT&CK Enterprise Assessment

III. TRAINING

- SOC Basics training
- SOC Advanced training
- Tabletop Exercise

About Group-IB

Group-IB is a leading provider of innovations and solutions for detecting and preventing cyberattacks, eliminating fraud, and protecting brands from digital risks worldwide.

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

250+
employees

650+
enterprise customers

60
countries

$1 bln
saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

120+
patents and applications

17
inventors in our team

4
Digital Crime Resistance Centers (Singapore, Dubai, Amsterdam, Phuket)

* According to Cybersecurity Excellence Awards

Global partnerships

INTERPOL

Europol

Recognized by top industry experts

FORRESTER®

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN

Preventing and investigating cybercrime since 2003

FIGHT AGAINST CYBERCRIME

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

APAC
+65 3159 3798

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785