Office of the Government Chief Information Officer

INFORMATION SECURITY

Practice Guide

for

IT Security Threat Management

Version 1.0

April 2024

COPYRIGHT NOTICE

Amendment History				
Change Number	Revision Description	Pages Affected	Revision Number	Date

Table of Contents

1 Introduction

In today's interconnected and digital landscape, B/Ds face an ever-increasing range of threats to their information systems, networks, and sensitive data. To help bureaux and departments (B/Ds) navigate this complex landscape, this guideline provides a comprehensive IT security threat management framework with the knowledge and strategies necessary to establish robust threat monitoring capabilities, proactively detect potential security breaches, and respond swiftly and effectively to mitigate the impact of IT security threats. With this framework, managerial users, IT managers, system administrators and other technical and operational staff can better understand the IT security threat management process to safeguard their digital assets in the increasingly challenging threat landscape.

1.1 Purpose

This document shows a general framework for IT security threat management. It should be used in conjunction with other security documents such as the Baseline IT Security Policy [S17], IT Security Guidelines [G3] and relevant procedures, where applicable.

This practice guide is intended for all staff who are involved in IT security threat management as well as for the external IT security consultants or suppliers who support the IT security threat management process for the Government.

1.2 Normative References

The following referenced documents are indispensable for the application of this document.

- Baseline IT Security Policy [S17], the Government of the Hong Kong Special Administrative Region
- IT Security Guidelines [G3], the Government of the Hong Kong Special Administrative Region
- Information technology - Security techniques - Information security management systems - Requirements (third edition), ISO/IEC 27001:2022
- Information technology - Security techniques - Code of practice for information security controls (third edition), ISO/IEC 27002:2022
- NIST SP 800-92 – Guide to Computer Security Log Management
- NIST SP 800-150 - Guide to Cyber Threat Information Sharing
- NIST SP 800-137 – Information Security Continuous Monitoring for Federal Information Systems and Organizations
- Guide to Cyber Threat Modelling, Cyber Security Agency of Singapore
- Cyber-threat intelligence information sharing guide, GOV.UK

- Practice Guide for Security Risk Assessment and Audit
- Practice Guide for Information Security Incident Handling
- Endpoint Detection & Response: A Malware Identification Solution ,IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/9703010
- Best endpoint detection and response solutions reviews 2024: Gartner Peer insights, Gartner. Available at: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

1.3 Definitions and Conventions

For the purposes of this document, the definitions and conventions given in S17, G3, and the following shall apply.

Abbreviation and Terms	
ACL	Access Control List
APT	Advanced Persistent Threat
CRM	Customer Relationship Management
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DNS	Domain Name System
EDR	Endpoint Detection and Response
EPP	Endpoint Protection Platforms
ERP	Enterprise Resource Planning
ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IOA	Indicators Of Attack
IoC	Indicators of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
ITSM	IT Service Management

KPI	Key Performance Indicators
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond
NAC	Network Access Control
NDR	Network Detection and Response
PAM	Privileged Access Management
PoC	Proof of Concept
POS	Point-Of-Sale
ROI	Return On Investment
SEM	Security Event Management
SIEM	Security Information and Event Management
SIM	Security Information Management
SOAR	Security orchestration, automation, and response
SOC	Security Operations Center
TCO	Total Cost of Ownership
TIP	Threat Intelligence Platform
TTP	Tactics, Techniques, and Procedures
UEBA	User and Entity Behaviour Analytics
URL	Uniform Resource Locator
VM	Virtual Machines
VPN	Virtual Private Network
WAF	Web Application Firewall
XDR	Extended detection and response

1.4 Contact

This document is produced and maintained by the Office of the Government Chief Information Officer (OGCIO). For comments or suggestions, please send to:

Email:	it_security@ogcio.gov.hk
Lotus Notes mail:	IT Security Team/OGCIO/HKSARG@OGCIO
CMMP mail:	IT Security Team/OGCIO

2 Information Security Management

Information security is about the planning, implementation and continuous enhancement of security controls and measures to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission and its associated information systems. Information security management is a set of principles relating to the functions of planning, organising, directing, controlling, and the application of these principles in harnessing physical, financial, human and informational resources efficiently and effectively to assure the safety of information assets and information systems.

Information security management involves a series of activities that require continuous monitoring and control. These activities include, but are not limited to, the following functional areas:

- Security Management Framework and the Organisation;
- Governance, Risk Management, and Compliance;
- Security Operations;
- Security Event and Incident Management;
- Awareness Training and Capability Building; and
- Situational Awareness and Information Sharing.

Security Management Framework and Organisation

B/Ds shall establish and enforce departmental information security policies, standards, guidelines and procedures in accordance with the business needs and the government security requirements.

B/Ds shall also define the organisation structure on information security and provide clear definitions and proper assignment of security accountability and responsibility to involved parties.

Governance, Risk Management and Compliance

B/Ds shall adopt a risk based approach to identify, prioritise and address the security risks of information systems in a consistent and effective manner.

B/Ds shall perform security risk assessments for information systems and production applications periodically and when necessary so as to identify risks and consequences associated with vulnerabilities, and to provide a basis to establish a cost-effective security program and implement appropriate security protection and safeguards.

B/Ds shall also perform security audits on information systems regularly to ensure that current security measures comply with departmental information security policies, standards, and other contractual or legal requirements.

Security Operations

To protect information assets and information systems, B/Ds should implement comprehensive security measures based on their business needs, covering different technological areas in their business, and adopt the principle of "Prevent, Detect, Respond and Recover" in their daily operations.

- Preventive measures avoid or deter the occurrence of an undesirable event;
- Detective measures identify the occurrence of an undesirable event;
- Response measures refer to coordinated actions to contain damage when an undesirable event or incident occurs; and
- Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

Security Event and Incident Management

In reality, security incidents might still occur due to unforeseeable, disruptive events. In cases where security events compromise business continuity or give rise to the risk of data security, B/Ds shall activate their standing incident management plan to identify, manage, record, and analyse security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response to security risks to subdue distrust or unnecessary speculation. When developing an incident management plan, B/Ds should plan and prepare the right resources as well as develop the procedures to address necessary follow-up investigations.

Awareness Training and Capability Building

As information security is everyone's business, B/Ds should continuously promote information security awareness throughout the organisations and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

Situational Awareness and Information Sharing

As the cyber threat landscape is constantly changing, B/Ds should also constantly attend to current vulnerabilities information, threat alerts, and important notices disseminated by the security industry and the GovCERT.HK. The security alerts on impending and actual threats should be disseminated to and shared with those responsible colleagues within B/Ds so that timely mitigation measures could be taken.

B/Ds could make use of the cyber risk information sharing platform to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

Staff may also raise their security awareness by participating in security drills, attending seminars, showcases or visiting theme pages containing security intelligence information (e.g. Cyber Risk Information Sharing Platform) and general security information (e.g. Cyber Security Information Portal, InfoSec website).

3 IT security Threat Management

3.1 Introduction of IT security Threat Management and its Importance

IT security threats refer to any circumstances or events that have the potential to negatively impact the operations, assets, reputation, or individuals of an organisation through unauthorised access, destruction, disclosure, modification of information, or denial of service. These threats have become increasingly prevalent in the digital landscape, posing significant risks to governments and organisations worldwide.

To effectively address these threats, B/Ds need to understand the various elements associated with IT security threat management. Threat actors, individuals or groups posing threats, play a vital role in this context. Additionally, B/Ds require access to threat information, which includes indicators, tactics, techniques, and procedures (TTPs), security alerts, threat intelligence reports, and tool configurations. This information helps B/Ds protect themselves and detect the activities of threat actors.

Threats are closely related to risk, vulnerability, and impact in the context of IT security.

Figure 2.1 Risk is Defined as a Combination of Threat, Vulnerability and Impact

They exploit vulnerabilities within an B/D's systems or networks, which can lead to various negative consequences. B/Ds need to identify and assess threats, vulnerabilities, and potential impacts to effectively manage and mitigate risks, safeguarding the confidentiality, integrity, and availability of their digital assets. Please refer to **Practice Guide for IT Security Risk Management** and **Practice Guide for Security Risk Assessment & Audit** for more details.

In other words, managing threats sets the foundation for managing risks. IT security threat management encompasses a comprehensive approach to mitigate and respond

to IT security threats in the digital landscape. By adopting a robust IT security threat management capability, B/Ds can continuously monitor the threat landscape, swiftly identify potential attacks, implement controls to reduce vulnerabilities, and promptly contain threats. This enhances situational awareness, reduces risk exposure, and enables agile responses to potential IT security incidents.

Effective IT security threat management is important for building resilience against IT security attacks, protecting sensitive data, and maintaining public trust. To achieve an intelligence-driven and risk-based approach to IT security threat management, B/Ds need to have a solid understanding of the threats they face. This understanding allows B/Ds to assess the maturity of their defences and determine the likelihood of a security incident occurring. It also enables them to evaluate and prioritise risks effectively, allocating their security resources accordingly.

IT security threat analysis can be classified into three levels: departmental, system, and equipment or application. Each level provides insights into different aspects of threat analysis, contributing to a B/D's overall threat management direction.

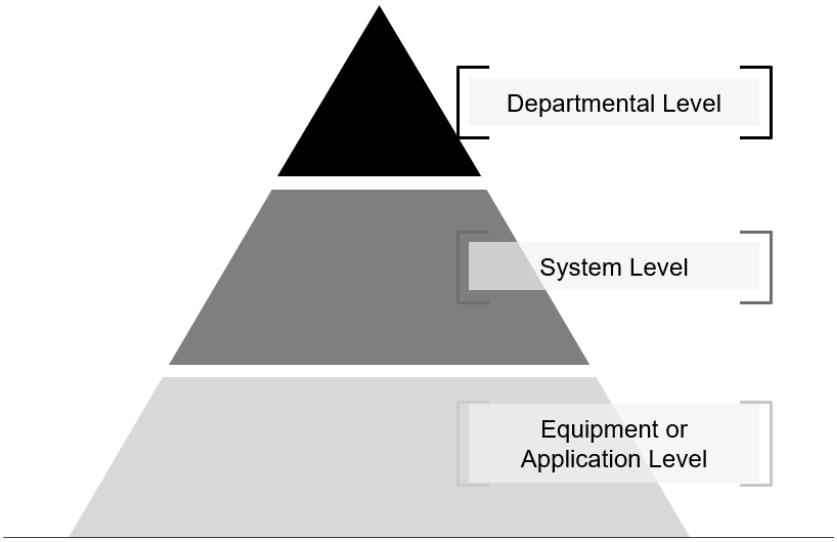

Figure 2.2 Hierarchy of Threat Analysis

Departmental Level

The departmental level involves analysing intelligence feeds and trends at the departmental level, focusing on external factors such as geopolitics. B/Ds profile adversaries based on their motives and actions before and after intrusions. This level of analysis is typically done from a high level perspective for management's consumption.

System Level

The system level considers the system's constructs, relationships, and behaviours. It involves modelling assets, data flows, and boundaries within the environment to determine relevant threat events to the system. More details on this level of analysis

can be found in the Security Risk Assessment, as described in the **Practice Guide for Security Risk Assessment & Audit**.

Equipment or Application Level

The equipment or application level is the most granular level of threat analysis. It involves activities such as threat hunting, log correlation, detailed data triaging, advanced analytics, and heuristic techniques. This level of analysis aims to identify and address detailed evasion and exploitation of published vulnerabilities.

By implementing IT security threat management, B/Ds are able to better understand threats and proactively implement measures to prevent, detect, and respond effectively through a structured framework. There are several key benefits associated with implementing IT security threat management:

- ***Protection of sensitive government information.*** B/Ds often need to process sensitive information, including citizen records, financial information, and classified documents. Safeguarding those information is crucial to maintain the trust and confidence of the public. By implementing effective threat management practices, B/Ds can establish robust security measures, such as access controls, encryption, and secure data storage, to prevent unauthorised access, data breaches, and leaks.

- ***Ensuring the continuity of essential services.*** Any disruption or compromise of critical systems can have severe consequences, hindering the delivery of vital services to the public. By proactively managing IT security threats, B/Ds can identify potential vulnerabilities, implement mitigating measures, and establish incident response plans. This enables B/Ds to quickly detect and respond to security incidents, minimising the impact on essential services and ensuring the uninterrupted provision of services to citizens.

- ***Commitment to upholding regulatory requirements and international standards.*** Regulatory frameworks are in place to protect personal data, ensure privacy, and maintain IT security. Adhering to these regulations and standards is vital for B/Ds to comply with legal obligations and maintain public trust. By implementing IT security threat management practices, B/Ds can demonstrate their dedication to protecting sensitive information, complying with data protection laws, and maintaining high IT security.

3.2 IT Security Threat Management Framework

To establish a consistent and effective approach to IT security threat management, B/Ds should adopt a standardised IT security threat management framework. This framework aligns with international best practices and industry standards, providing a structured methodology for managing IT security threats and ensuring comprehensive IT security.

Adopting a standardised framework provides a common ground for B/Ds to communicate and collaborate on managing IT security threats, enhancing coordination and information sharing among B/Ds and OGCIO.

There are six major stages in IT security threat management. An overview of these stages is provided below. The activities in each stage are described in more detail in the corresponding sections.

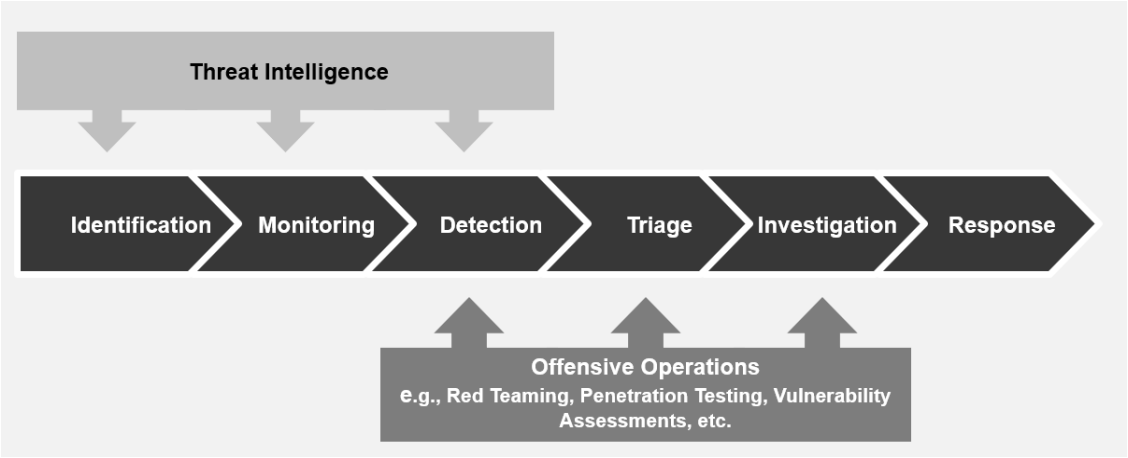

Figure 2.3 Major Stages in IT Security Threat Management Framework

A. Identification (Departmental and System Level) (Section 4)

In this stage, B/Ds should identify potential threats that can harm information systems, data, operations, or reputation. The major activities involved in this stage are listed below:

- Identifying and Categorising Relevant IT Security Threats
- Utilising Threat Intelligence Sources and Sharing Platforms

B. Monitoring (Equipment or Application Level) (Section 5)

In this stage, B/Ds should continuously monitor network traffic, system logs, and security events. The major activities involved in this stage are listed below:

- Designing and Implementing a Comprehensive Monitoring Strategy

C. Detection (Equipment or Application Level) (Section 5)

In this stage, B/Ds should analyse collected data, such as log files and network traffic, to identify patterns or anomalies that may indicate a security breach or malicious activity. The major activities involved in this stage are listed below:

- Data Collection, Log Analysis, and Threat Intelligence Integration
- Behaviour Analysis, Anomaly Detection, and Threat Intelligence Application

D. Triage (Equipment or Application Level) (Section 6)

Once the detection stage generates alerts for potential threats, B/Ds need to prioritise and categorise these alerts based on their severity and potential impact. This triage process can facilitate the efficient allocation of resources to address critical threats promptly. An overview of the triage stage is as follows:

- Alert Collection and Analysis
- Alert Validation
- Severity Classification
- Continuous Monitoring and Iterative Triage

E. Investigation (Equipment or Application Level) (Section 6)

After selecting an alert from the triage queue, B/Ds should conduct a thorough investigation to determine the validity and nature of the potential threat. The investigation stage plays an essential role in accurately assessing the presence of an actual attack. The major activities involved in this stage are listed below:

- Evidence Gathering
- Threat Analysis

F. Response (Equipment or Application Level) (Section 7)

In this stage, B/Ds should formulate and perform actions and measures to respond to potential threats or alerts before they materialise into actual incidents, or lead to damages after confirming as actual incidents in the investigation stage. The major activities may involve:

- Containment
- Blocking
- Patching
- Training

Listed below are examples of IT security threat management mechanisms for different information system tiers. The security requirements are **cumulative** across the different tiers of information systems (i.e. security requirements mandated for Tier 1 Information Systems shall also be extended to Tier 2 and Tier 3 Information Systems).

Stage	Tier 3 Information Systems	Tier 2 Information Systems	Tier 1 Information Systems
Identification	Establish a mechanism to prioritise and monitor threat intelligence sources covering all threat components.	The threat intelligence and analysis processes are assigned to a specific group or individual.	Processes are in place to monitor threat intelligence to identify emerging threats.

	Analyse threat intelligence to generate comprehensive threat summary reports with cyber risk details and recommended actions. Utilise threat intelligence to inform the B/D's risk profile, prioritise mitigation actions, and update IT security architecture and configuration standards. Employ multiple intelligence sources and analytical techniques to predict future attacks and identify trends.		
Monitoring	Establish a centralised security monitoring process with a dedicated 24/7 surveillance team. A system is in place to monitor and analyse user behaviour (e.g. IP addresses, network use patterns, work hours, and known devices) and provide alerts for anomalous activities.	Audit logs are backed up to a centralised log server or media to prevent unauthorised changes to the logs. Tools actively monitor security logs for anomalous behaviour and provide alerts within established parameters.	Regularly review system logs for unusual or suspicious activities. A process is in place to detect anomalous activities through environmental monitoring.
Detection	Automated tools are installed to detect unauthorised changes to critical system files, firewalls, IPS, IDS, or other security devices. Real-time network monitoring and detection tools have been implemented. Tools exist to actively correlate event information from multiple sources and send alerts based on	A process is in place to discover infiltration before an attacker can traverse systems, establish a foothold, steal information, or cause damage to data and systems. Endpoint behavioural detection capabilities (e.g. EDR solutions) should be available on endpoints (i.e. user workstations, laptops and servers).	Mechanisms (e.g. antivirus alerts, log event alerts, etc.) are in place to alert the security monitoring function and management to potential attacks.

	established parameters.		
Triage	Prioritise threats based on severity and potential impact.		
Investigation	Investigate the characteristics, motivations, and potential impact of the threats.		
Response	Develop and implement measures to respond to the threat.		

Table 2.1 Examples of IT Security Threat Management Mechanisms for Different System Criticality

At different stages of the IT security threat management process, there may be different outputs or deliverables, shown below in Table 2.2.

Stages	**Outputs/Deliverables Examples**
Identification	• Threat intelligence reports provide up-to-date information on emerging threats, attack trends, and relevant security news. • Threat taxonomy, a comprehensive list of identified threats.
Monitoring	• Threat monitoring objectives, tools, and techniques adopted.
Detection	• Defined rules and thresholds for generating alerts and events based on suspicious activities, anomalous behaviour, or known threat patterns.
Triage	• Defined mechanism, classification criteria, process and workflow for prioritising security alerts based on severity and potential impact.
Investigation	• Documented steps, tools, and techniques for the investigation process on potential threats, including data collection, analysis, and evidence preservation.
Response	• Defined actions and measures to respond to threats before they materialise into actual incidents.

Table 2.2 Outputs/Deliverables Examples of IT Security Threat Management Framework

4 Departmental Context Establishment

4.1 Understanding the Threat Landscape and Emerging Trends

Understanding the threat landscape and emerging trends is important for B/Ds to manage and mitigate IT security risks effectively. Here are some activities to gain insights into the threat landscape and emerging trends:

- ***Stay Informed.*** Regularly monitor and gather information from reliable sources such as IT security news websites, industry reports, and government advisories. Subscribe to relevant mailing lists, follow security blogs, and join professional networks to stay updated on the latest threats and trends.

- ***Engage in Threat Intelligence.*** Leverage threat intelligence services or platforms that provide real-time information about IT security threats, vulnerabilities, and emerging trends. These services aggregate data from various sources and provide actionable insights.

- ***Perform Regular Risk Assessments***. Identify potential threats and vulnerabilities through regular threat modelling and risk assessments. This includes analysing network infrastructure, systems, applications, and data assets.

- ***Participate in Information Sharing Initiatives***. Engage in information sharing initiatives and government-sponsored programs. These platforms facilitate the exchange of threat intelligence among B/Ds and OGCIO, enabling B/Ds and OGCIO to gain insights into the threats faced by others.

- ***Analyse Incident Data.*** Regularly review and analyse security incident data. Look for patterns, trends, and common attack vectors. This analysis can help B/Ds understand the evolving TTPs employed by threat actors.

- ***Continuous Learning and Training***. B/Ds should continuously promote IT security threat management awareness and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

Given the evolving nature of IT security threats, B/Ds should actively participate in the above activities to collect and exchange insights, threat indicators, and best practices. This collaborative approach strengthens the collective defence against attacks, and enables timely identification and response to emerging threats with the following benefits:

- ***Shared Situational Awareness.*** Information sharing enhances the defensive capabilities of B/Ds by leveraging the collective knowledge and experience of sharing partners, increasing the security of the entire community.

- ***Improved Security Posture.*** Sharing threat information allows B/Ds to understand the threat environment better, leading to informed IT security

practices, identification of affected systems, implementation of protective measures, and more effective incident response and recovery.

- ***Knowledge Maturation.*** Sharing and analysing seemingly unrelated observations leads to enriched information, enhanced indicators, and knowledge of threat actors' tactics, techniques, and procedures (TTPs), improving overall understanding and response capabilities.

- ***Greater Defensive Agility.*** Sharing information informs B/Ds about evolving threat actor TTPs, enabling rapid detection and response. This increases the operational tempo, reduces the probability of successful attacks, and creates cost disadvantages for threat actors as they are forced to develop new TTPs.

B/Ds may face various IT security threats that can significantly affect national security, public safety, and government operations. Listed below are several major types of threat actors:

- ***Cybercriminals.*** These individuals or groups commit cyber crimes, mostly for financial gain. Common crimes cybercriminals commit include ransomware attacks and phishing scams that trick people into making money transfers or divulging credit card information, login credentials, intellectual property or other private or sensitive information.

- ***Nation-state actors.*** Nation-states and governments frequently fund threat actors to steal sensitive data, gather confidential information, or disrupt another government's critical infrastructure. These malicious activities often include espionage or cyberwarfare and are highly funded, making the threats complex and challenging to detect.

- ***Hacktivists.*** Hacktivists use hacking techniques to promote political or social agendas, such as spreading free speech or uncovering human rights violations. Hacktivists believe they are affecting positive social change and feel justified in targeting individuals, organisations, or B/Ds to expose secrets or other sensitive information.

- ***Thrill seekers.*** Thrill seekers attack computers and information systems primarily for fun. Some want to see how much sensitive information or data they can steal; others want to use hacking to understand better how networks and computer systems work. Though they do not always seek to cause harm, thrill seekers can still cause unintended damage by interfering with a network's security and opening the door to future attacks.

- ***Insider threats.*** Insider threat actors do not always have malicious intent. Some hurt their companies through human error, e.g. by unwittingly installing malware or losing a company-issued device that a cybercriminal finds and uses to access the network. Nevertheless, malicious insiders exist—for example, a disgruntled employee who abuses access privilege to steal data for monetary gain or causes damage to data or applications in retaliation for being passed over for promotion or unfairly treated by his/her superior.

- ***Cyberterrorists.*** Cyberterrorists launch politically or ideologically motivated cyberattacks that threaten or result in violence. These cyberterrorists may include nation-state actors and individuals acting independently or on behalf of a non-government group. Threat actors deploy a mixture of tactics when executing an attack, which include but not be limited to the following:

- ***Advanced Persistent Threats (APTs).*** APTs are sophisticated and targeted security attacks typically carried out by state-sponsored actors or highly skilled hacking groups. These threats involve long-term, stealthy infiltration of government networks to gather sensitive information, disrupt operations, or conduct espionage.

- ***Ransomware Attacks.*** Ransomware attacks have become increasingly prevalent and pose a significant threat to B/Ds. Attackers encrypt critical data and demand ransom payments in exchange for restoring access. Such attacks can paralyse government systems, disrupt public services, and compromise sensitive information.

- ***Distributed Denial of Service (DDoS) Attacks.*** DDoS attacks overwhelm government websites or networks with a flood of traffic, rendering them inaccessible to users. These attacks can disrupt public services, compromise citizen trust, and serve as a distraction from other intrusions.

- ***Social Engineering and Phishing.*** Social engineering techniques, such as phishing emails and fraudulent phone calls, are commonly used to deceive government employees into revealing sensitive information or providing unauthorised access to systems. This can lead to data breaches, unauthorised access, or the installation of malware.

- ***Supply Chain Attacks.*** B/Ds rely on a vast network of suppliers and contractors, making them vulnerable to supply chain attacks. Malicious actors can compromise the software or hardware these vendors provide, infecting government systems with malware or backdoors.

- ***Critical Infrastructure Attacks.*** B/Ds often operate and oversee critical infrastructure, such as power grids, transportation systems, and water treatment plants. IT security attacks targeting these systems can have severe consequences, including disruption of essential services, economic damage, or even loss of life.

- ***Zero-Day Exploits.*** Zero-day exploits target previously unknown vulnerabilities in software or systems that have not yet been patched. B/Ds are attractive targets for hackers who discover or purchase these exploits on the black market, as they can be used to gain unauthorised access or conduct targeted attacks.

- ***Information Warfare and Disinformation.*** B/Ds are also susceptible to information warfare campaigns and disinformation campaigns. These involve

spreading false information, manipulating public opinion, or conducting IT security operations to influence political processes or undermine public trust.

4.2 Defining Scope

Defining the scope is critical for B/Ds to effectively allocate resources, establish controls, and prioritise security measures in IT security threat management tailored to their specific needs.

At the departmental level, clearly defining the scope allows B/Ds to identify the specific departments or divisions within their B/Ds that require protection from potential threats. For example, this may include the finance department, human resources department, or research and development division. By defining the scope at this level, B/Ds can allocate resources and implement security measures that address the unique vulnerabilities and risks associated with each department or divisions.

Moving to the system level, defining the scope involves identifying the various systems within the B/D that need protection. This may include enterprise resource planning (ERP) systems, customer relationship management (CRM) systems, or internal communication systems. By defining the scope at the system level, B/Ds can focus their efforts on securing these critical systems and ensuring their resilience against potential threats.

At the equipment or application level, defining the scope involves identifying specific equipment or applications that require protection. This may include servers, routers, firewalls, or key business applications. By defining the scope at this level, B/Ds can implement targeted security controls and measures to safeguard these critical components from potential threats.

Moreover, when defining the scope of IT security threat management, it is essential to recognise dependencies. For instance, B/Ds should consider dependencies on external stakeholders, such as vendors or service providers. This could include third-party software providers, cloud service providers, or suppliers of critical components. By identifying these dependencies, B/Ds can assess associated risks and implement appropriate security measures to ensure the security of their systems and data.

5 Threat Identification and Intelligence Gathering

5.1 Identifying and Categorising Relevant IT Security Threats

Threats can be categorised into three main types:

- ***Social Threats***. Directly related to human factors can be intentional or unintentional, such as human errors, results of omission or negligence, theft, fraud, misuse, damage, destruction, disclosure and modification of data.
- ***Technical Threats.*** Caused by technical problems such as wrong processes, design flaws, and breakage of communication paths like cabling.
- ***Environmental Threats.*** Caused by environmental disasters such as fire, water damage, power supply, and earthquake.

Identifying and categorising relevant IT security threats is fundamental for effective risk mitigation. Developing a comprehensive and accurate threat taxonomy is essential for this purpose. A threat taxonomy organises and classifies different types of IT security threats for clearly understanding the threat landscape and enabling B/Ds to allocate resources and efforts accordingly.

To identify and categorise IT security threats, B/Ds should follow these suggested steps:

1. ***Conduct a Threat Assessment:*** Conduct a comprehensive assessment of potential threats to the B/D's IT security. This can involve analysing historical data, studying industry trends, consulting security experts, and considering the specific characteristics of the B/D's IT infrastructure.
2. ***Identify Threat Categories:*** Based on the assessment, categorise the threats into relevant categories. The three types mentioned above—social threats, technical threats, and environmental threats—can serve as a starting point. It is important to ensure that the categories cover the breadth of threats specific to the B/D.
3. ***Define Threat Types:*** Within each category, define specific threat types relevant to the B/D. For example, under social threats, it might include malware, phishing attacks, insider threats, social engineering, etc. It is recommended to be as comprehensive as possible to capture the various threats the B/D may encounter.
4. ***Regularly Update and Refine:*** The threat landscape is dynamic, with new and existing threats evolving. Reviewing and updating the threat taxonomy to stay current regularly is vital. B/Ds should stay informed about emerging threats, attack techniques, vulnerabilities, and industry best practices, and incorporate this knowledge into the threat taxonomy to ensure its relevance and effectiveness.
5. ***Document and Communicate:*** B/Ds should document the threat taxonomy in a clear and accessible format, create a repository or knowledge base where

relevant stakeholders can access and understand the categorised threats, and communicate the threat taxonomy to related stakeholders to increase awareness and ensure a collective understanding of the risks.

The threat taxonomy should adapt to suit the B/D's needs and evolve as the threat landscape changes. It is a living document that requires regular updates and refinement to guide the B/D's IT security efforts effectively. See also **Annex A** for a sample threat taxonomy and an illustrative example showing how a threat taxonomy can be used to assist a B/D in identifying and prioritising specific threats.

The threat taxonomy and security risk assessment are interconnected and mutually reinforcing elements in IT security. The threat taxonomy provides a structured framework for organising and classifying different IT security threats, allowing B/Ds to understand the threat landscape they face. The taxonomy forms the foundation for conducting a comprehensive security risk assessment by categorising threats into specific types.

The security risk assessment uses the threat taxonomy to identify and evaluate vulnerabilities and potential consequences of each threat. It considers the B/D's assets, their value, existing control measures, and the likelihood of exploitation to determine the level of risk posed by each threat. The threat taxonomy informs and guides the risk assessment process, ensuring that all relevant threats are considered and prioritised based on their potential impact.

Conversely, the risk assessment outcomes, such as identified risks and their associated likelihood and severity, provide valuable insights for refining and updating the threat taxonomy. This iterative process ensures the threat taxonomy remains current and aligned with the evolving risk landscape.

Therefore, the threat taxonomy and security risk assessment should be used to systematically identify, prioritise, and mitigate IT security risks. For more details, please refer to the **Practice Guide for IT Security Risk Management** and the **Practice Guide for Security Risk Assessment & Audit**.

5.2 Utilising Threat Intelligence Sources and Sharing Platforms

Threat information refers to any information that can help an organisation protect itself or detect threat actors' activities, such as the following:

- **Indicators of compromise (IoCs)** are technical artefacts or observables suggesting an attack is imminent or underway or a compromise may have already occurred. These indicators serve as clues that can be used to detect and defend against potential threats. Examples of indicators include the Internet Protocol (IP) address of a suspected command and control server, a suspicious Domain Name System (DNS) domain name, a Uniform Resource Locator (URL)

that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message.

- **Tactics, techniques, and procedures (TTPs)** describe an actor's behaviour. Tactics are high-level descriptions of behaviour, techniques are detailed descriptions of behaviour in the context of a tactic, and procedures are even lower-level, highly detailed descriptions of a technique. TTPs could describe an actor's tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism (e.g., phishing or watering hole attack), or exploit.
- **Security alerts**, also known as advisories, bulletins, and vulnerability notes, are brief, usually human-readable, technical notifications regarding current vulnerabilities, exploits, and other security issues.
- **Threat intelligence reports** are generally prose documents that describe TTPs, actors, types of systems and information being targeted, and other threat-related information that provides greater situational awareness to an organisation. Threat intelligence is threat information aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes.
- **Tool configurations** are recommendations for setting up and using tools (mechanisms) that support the automated collection, exchange, processing, analysis, and use of threat information. For example, tool configuration information could consist of instructions on installing and using a rootkit detection and removal utility or creating and customising intrusion detection signatures, router access control lists (ACLs), firewall rules, or web filter configuration files.

Threat intelligence refers to the information and insights about potential IT security threats, including emerging attack techniques, vulnerabilities, and indicators of compromise. Using threat intelligence, B/Ds can enhance their IT security capabilities and proactively defend against evolving threats.

Threat intelligence is a critical component in understanding and addressing IT security threats. It involves gathering and analysing information about potential threats, including their tactics, techniques, and indicators. Different types of threat intelligence provide valuable insights to B/Ds:

- ***Strategic Intelligence.*** Strategic intelligence focuses on long-term trends, geopolitical factors, and the capabilities and motivations of threat actors. It helps B/Ds anticipate risks and adjust their security strategies accordingly. Strategic intelligence assists in formulating longer-term strategies by providing plain language reports on business risks.

- ***Tactical Intelligence.*** Tactical intelligence provides specific and actionable information about immediate threats, such as new malware or vulnerabilities. It enables B/Ds to respond promptly and effectively to these threats. Tactical intelligence includes TTPs used by threat actors and delivers IoCs that can be used to update defence systems.

- ***Operational Intelligence.*** Operational intelligence focuses on threat actor tactics, infrastructure, and campaigns. It provides insights into the strategies and methods used by threat actors. Operational threat intelligence often relates to details of potential impending operations against an organisation. It helps B/Ds anticipate and prepare for specific threat activities.

Threat intelligence should be:

- relevant (i.e., related to the protection of the B/D);
- insightful (i.e., providing the B/D with an accurate and detailed understanding of the threat landscape);
- contextual, to provide situational awareness (i.e., adding context to the information based on the time of events, where they occur, previous experiences and prevalence in similar organisations); and
- actionable (i.e., the B/D can act on information quickly and effectively).

Threat intelligence suppliers gather information from various sources, such as indicators of compromise, client-derived data, the deep web, the dark web, messaging platforms, social media, human intelligence, malware analysis, geopolitical developments, code repositories, and paste sites. This diverse range of sources provides comprehensive insights into threats, including tactics, techniques, and procedures used by threat actors, vulnerabilities to be patched, and potential indicators of breaches or attacks. Effective threat intelligence suppliers corroborate and fuse information from different sources to provide a comprehensive understanding of threats. Multi-sourced intelligence reports, combining information from at least two source types, are ideal. Please refer to **Annex B** for a sample list of questions for assessing suppliers of IT security threat intelligence.

Threat intelligence is delivered through various methods, including subscriptions, threat intelligence platforms (TIPs), and data feeds. Subscriptions provide access to current and historical intelligence, interactive investigation capabilities, and integration with existing processes. TIPs aggregate and correlate different feeds, allowing users to pivot from various threat intelligence sources and conduct investigations. Data feeds provide a continuous stream of threat intelligence updates that can be integrated into security systems and processes for real-time protection.

B/Ds are encouraged to adopt threat intelligence platforms to effectively leverage threat intelligence proactively. These platforms are centralised repositories that collect, analyse, and disseminate threat intelligence from various sources. By utilising such platforms, B/Ds can streamline the collection and analysis of threat intelligence, enabling them to identify relevant threats and take timely proactive measures to mitigate risks. Threat intelligence platforms also promote collaboration and information sharing among different B/Ds, fostering a collective and collaborative approach to IT security.

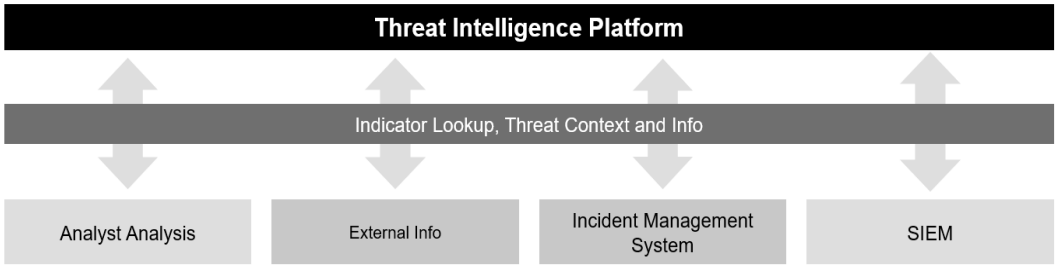

Figure 4.1 Utilisation of Threat Intelligence Platforms

Furthermore, B/Ds may establish strategic partnerships with trusted IT security organisations, such as industry associations, research institutions, and private-sector security companies. These partnerships can provide B/Ds with access to specialised expertise, research findings, and additional threat intelligence feeds that complement their existing capabilities.

To effectively utilise threat intelligence sources and sharing platforms, the following steps are suggested:

1. ***Establish Objectives:*** Define the goals and objectives for threat intelligence production within the B/D, considering the specific needs and priorities of the B/D's operation.

2. ***Identify and Select Information Sources:*** Identify and vet internal and external information sources that provide relevant and reliable threat intelligence. These sources can include government sources (e.g. GovCERT.HK, Cyber Risk Information Sharing Platform (CRisP)), industry-specific organisations, IT security vendors, and international information-sharing platforms. These sources provide timely and credible information about emerging threat trends, known vulnerabilities, and the tactics employed by cybercriminals.

3. ***Collect Information:*** Gather information from the selected sources, both internal and external, to build a comprehensive dataset for analysis. This can involve collecting indicators of compromise, client-derived data, deep web and dark web sources, messaging platforms, social media, human intelligence, malware analysis, geopolitical developments, code repositories, and paste sites.

4. ***Process and Prepare Information:*** Process the collected information to make it suitable for analysis. This may involve translating, formatting, or corroborating the data to ensure its accuracy and consistency.

5. ***Analyse Information:*** Conduct a thorough analysis of the collected information to understand its relevance and significance to the B/D. Identify patterns, trends,

and potential risks associated with threat actors, tactics, techniques, and procedures (TTPs), vulnerabilities, and indicators of compromise (IoCs).

6. ***Communicate and Share:*** Effectively communicate and share the analysed threat intelligence with relevant individuals and departments within the B/D. Present the information in a format that is easily understandable and actionable.

7. ***Incorporate into IT Security Processes:*** Integrate the threat intelligence gathered from various sources into the B/D's IT security threat management processes. This can involve updating technical preventive and detective controls such as firewalls, intrusion detection systems, anti-malware solutions, etc. with the relevant IoCs and TTPs.

8. ***Enhance Information Security Testing:*** Utilise threat intelligence as an input for information security test processes and techniques. This can help identify vulnerabilities and weaknesses within the B/D's systems and infrastructure.

Here is an illustrative example of how a B/D can effectively process threat intelligence:

A B/D receives a threat intelligence report indicating that a specific type of malware is being used in increasing frequency across their industry. The report includes technical details such as the file hash for the malware executable, a crucial Indicator of Compromise (IoC).

Upon receiving this intelligence, the B/D springs into action. The B/D's IT security management unit initiates a process to understand the context of the threat. They examine the Tactics, Techniques, and Procedures (TTPs) associated with the reported malware. These include the infection method (e.g., email attachments, compromised software downloads), the behaviour of the malware once installed (e.g., data exfiltration, system damage), and any known defences.

IT security management unit communicates these insights to key stakeholders, including senior management, DITSO and the relevant IT teams. This ensures that everyone understands the threat's nature and the steps required to mitigate it.

The team then uses the IoC (the file hash for the malware executable) to update their defensive measures. They configure their anti-malware systems to identify and isolate any files with the reported hash. They also adjust their intrusion detection systems to look for network traffic patterns associated with the malware.

Finally, the team reviews the threat intelligence report for any information about software vulnerabilities that can be exploited by the malware. If their systems use any of the vulnerable software or hardware, it should be patched as soon as possible to further protect against the malware.

6 Threat Monitoring and Detection with Threat Intelligence Integration and Application

6.1 Define Monitoring Objectives, Techniques and Tools

B/Ds should clearly define the monitoring objectives, including identifying critical assets, systems, and networks that require protection and comprehending the potential threats and risks. By gaining a thorough understanding of these factors, B/Ds should then align the monitoring efforts with their overarching IT security goals. After establishing the objectives, B/Ds can select the appropriate monitoring techniques and tools. B/Ds should evaluate and deploy tools that align with their monitoring objectives, offer adequate coverage, and integrate well with other security solutions.

B/Ds should select suitable security monitoring tools based on their objectives and specific requirements. The following tools are illustrative examples and should be selected considering specific departmental requirements, budget considerations, and existing infrastructure:

- ***Intrusion Prevention System (IPS).*** It is a system that can detect and attempt to stop an intrusive activity, ideally before it reaches its targets.

- ***Network Detection and Response (NDR) Solution***. NDR solution focuses on real-time monitoring of network traffic, analysing behaviour, and detecting potential threats. It provides network communications visibility, identifies anomalies, and helps uncover hidden threats.

- ***Endpoint Detection and Response (EDR) Solution***. EDR solution focuses on monitoring and protecting individual endpoints and collecting and analysing endpoint data to detect and respond to advanced threats. For more details about EDR, please refer to Annex D.

- ***Endpoint Protection Platform (EPP).*** EPP combines antivirus, anti-malware, and host-based intrusion prevention capabilities to secure endpoints against various threats.

- ***TIPs.*** TIPs aggregate, analyse, and disseminate threat intelligence data from various sources, aiding in identifying emerging threats and IoCs.

- ***User and entity behaviour analytics (UEBA).*** UEBA is a type of security software that uses behavioral analytics, machine learning algorithms, and automation to identify abnormal and potentially dangerous user and device behavior.

- ***Extended detection and response (XDR) Solution.*** XDR collects threat data from previously siloed security tools across an organisation's technology stack for easier and faster investigation, threat hunting, and response. An XDR

platform can collect security telemetry from endpoints, cloud workloads, network email, and more.

- ***SIEM Systems.*** SIEM systems collect and analyse security event logs from diverse sources, correlating events and generating alerts based on predefined rules and patterns.

- ***Security orchestration, automation, and response (SOAR) Solution.*** SOAR platforms monitor threat intelligence feeds and trigger automated responses to security issues, which can help quickly and efficiently mitigate threats across numerous complex systems.

A diagram provides an illustration of a comprehensive threat monitoring architecture, showcasing the interconnected monitoring tools that work together for IT security threat monitoring is in Annex E for reference.

When selecting appropriate solutions for IT security threat monitoring, B/Ds should consider the following factors, among others:

- ***Scalability:*** Ensure the solutions can handle increasing data volumes as the B/D grows.
- ***Compatibility:*** Make sure the solutions work well with existing systems and technologies.
- ***Real-time Monitoring Capabilities:*** The solutions should be able to monitor and detect threats in real-time.
- ***Threat Intelligence Integration:*** The ability to integrate with external threat intelligence sources is important.
- ***Customisation and Flexibility:*** The solutions should be customizable to fit the B/D's specific needs.
- ***Reporting and Analysis Capabilities***: Look for solutions that provide comprehensive reporting and analysis features.
- ***Vendor Reputation and Support:*** Consider the reputation and support provided by the solution vendor.
- ***Cost-effectiveness:*** Evaluate the cost of the solutions and ensure they provide value for money.

In addition, B/Ds should strategically deploy sensors throughout the network infrastructure to capture pertinent data and detect potential threats. The placement decisions should consider the following:

- ***Network Topology:*** Consider the layout and structure of the network.
- ***Critical Assets:*** Identify and prioritise the protection of important assets.
- ***Entry and Exit Points:*** Focus on areas where network traffic enters or leaves.
- ***Network Segments:*** Look at different sections or divisions within the network.
- ***Network Intersections:*** Pay attention to points where different network segments intersect.
- ***Known Attack Vectors:*** Consider common methods used by attackers.

- ***Vulnerable Services and Protocols:*** Identify weaknesses in services and protocols.
- ***Historical Attacks:*** Learn from past attacks and vulnerabilities.
- ***Threat Intelligence:*** Stay informed about current and emerging threats.

It is important to adopt a risk-based approach to sensor placement, prioritising critical assets, high-risk areas, and those with historical vulnerabilities. Regular review and assessment of network topology, attack vectors, and evolving threats should be performed for sustained effectiveness.

Here are examples of monitoring objectives, techniques and tools for IT security threats that can be implemented to identify and respond to IT security threats promptly:

Objective	**Techniques and tools**
To minimise their impact, detect and respond to malware infections as early as possible.	Implement real-time malware scanning on endpoints and network traffic to identify and block malicious files or activities. Unauthorised Access Detection:
Identify and respond to unauthorised access attempts to protect sensitive data and systems.	Implement user activity monitoring and anomaly detection to detect suspicious login attempts, privilege escalation, or unauthorised changes to user permissions.
Monitor data exfiltration attempts and prevent sensitive data from being leaked outside the B/D.	Deploy data loss prevention (DLP) solutions to monitor and block unauthorised transfers of sensitive data through email, web uploads, or removable devices.
Monitor user behaviour and detect potential insider threats or malicious activities by employees or contractors.	Implement user behaviour analytics and monitor for unusual data access patterns, excessive file downloads, or unauthorised attempts to access confidential information.
Detect and respond to network intrusions or unauthorised access attempts.	Deploy intrusion detection systems (IDS) or intrusion prevention systems (IPS) to monitor network traffic for known attack signatures or suspicious activities. Web Application Security:
Monitor web applications for security vulnerabilities and protect against web-based attacks.	Implement web application firewalls (WAFs) to monitor and filter incoming web traffic, blocking malicious requests or attempts to exploit application vulnerabilities.
Monitor cloud infrastructure and services to detect and respond to security incidents or misconfigurations.	Utilise cloud-specific monitoring tools and services the cloud provider provides to track and analyse security events, such as unauthorised access attempts or suspicious API calls.

Table 5.1 Examples of monitoring objectives, techniques and tools for IT security threats

B/Ds may face significant challenges in achieving effective monitoring and detection capabilities for cybersecurity. These capabilities often rely on specialised tools and technologies that require substantial financial investments. Unfortunately, limited budgets can obstruct the acquisition and implementation of these tools, leaving B/Ds struggling to monitor their systems and detect potential security incidents adequately.

However, despite these constraints, B/Ds with budget limitations can still take steps to enhance their monitoring and detection capabilities. Adopting a resourceful and strategic approach that maximises the available resources and leverages alternative methods is crucial. Here are some recommendations:

- ***Prioritise Monitoring Objectives and Areas:*** Identify the most critical assets, systems, and networks that require protection. Allocate resources based on risk assessments and the potential impact of a security breach. Focus on protecting high-value targets and sensitive information by prioritizing monitoring efforts in these areas.

- ***Utilise Built-in Security Features:*** Leverage the built-in security features available in existing infrastructure and systems. Modern operating systems, network devices, and cloud platforms often have native security monitoring capabilities, such as log aggregation, auditing, and basic threat detection. Ensure these features are enabled and appropriately configured.

- ***Focus on Endpoint Protection:*** Prioritise endpoint protection by implementing robust antivirus/anti-malware solutions on all B/D devices. Configure these tools to provide real-time monitoring, threat detection, and incident response capabilities. Regularly update antivirus or malware's signatures to protect against the latest threats.

- ***Focus on User Awareness and Training:*** Invest in user awareness and training programs to educate employees about common security threats, phishing attacks, and best practices for secure computing. Well-informed users can serve as the first line of defence against security risks, reducing reliance on monitoring tools.

- ***Implement Network Segmentation:*** Utilise network segmentation to isolate critical systems and sensitive data from the rest of the network. This allows for more focused monitoring efforts and reduces the attack surface. Implement network segmentation through VLANs or firewalls without significant monetary investments.

6.2 Data Collection, Log Analysis, and Threat Intelligence Integration

To effectively monitor and detect IT security threats, it is essential to enable logging and data collection mechanisms. Security logs may originate from various sources,

such as hardware appliances, software systems and applications. For security log management and related security considerations, please refer to the Practice Guide for Security Log Management.

Centralised log aggregation and analysis solutions, such as SIEM systems, provide comprehensive visibility into security events and factilitate correlation analysis of logs from various sources within the IT infrastructure. SIEM is a security software product and service that combines security information management (SIM) and security event management (SEM) functions. Apart from SIM and SEM functionalities, some SIEM products offer additional functionalities such as real-time security alert analysis, threat verification and incident workflow automation.

SIM automates collecting event log data from network and security devices/endpoints such as firewalls, proxy servers, intrusion detection systems and antivirus software. The collected data and the threat intelligence log would be correlated and simplified for long-term storage, analysis and reporting.

SEM provides event management and can import security events for analysis and visual presentation (such as charting and dashboard) for incident response and security operations. It focuses on real-time monitoring, event aggregation, correlation and notification of events from operating systems, antivirus, firewalls and IDS, and events reported directly by authentication systems, servers and databases.

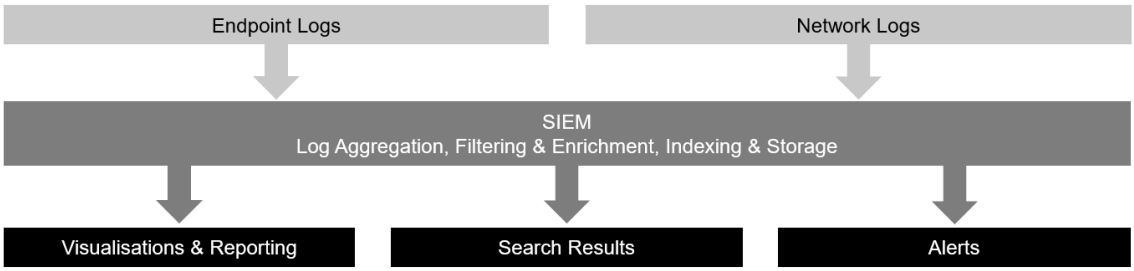

Figure 5.2 SIEM Functions

There are alternative solutions to SIEM for log aggregation and analysis that can be more cost-effective: log management tools focus on collecting, storing, and analysing logs from various sources. These tools provide centralised log aggregation and analysis capabilities without the advanced security features of SIEM. However, while these alternative solutions may be more cost-effective, they may not offer the same level of advanced security features and threat detection capabilities as a full SIEM solution. B/Ds should carefully evaluate their requirements and budget constraints before choosing an alternative solution.

The success of the detection stage relies heavily on the availability of data obtained during the previous collection stage. The more efficient the collection function operates, the greater the effectiveness of the detection function.

The quality of the tools influences the effectiveness of the detection stage utilised. This includes the strength of threat hunting capabilities, the availability of threat

intelligence information from external feeds and internally generated intelligence, and the efficacy of the detection engineering functions.

Furthermore, for effective threat detection and analysis, B/Ds should integrate threat intelligence into the monitoring and analysis processes. Threat intelligence encompasses information about known IoCs, emerging threats, attacker methods, and vulnerabilities.

- ***Leveraging External Threat Intelligence.*** Integrate threat intelligence feeds, databases, or platforms into the monitoring infrastructure to enhance the ability to identify and respond to specific threats. By leveraging threat intelligence, B/Ds can proactively defend against known threats and stay ahead of evolving attack techniques.

- ***Correlation and Alert Generation.*** Use threat intelligence integration to compare incoming logs, network traffic, and endpoint activities against known threat indicators. This correlation enhances the accuracy and effectiveness of threat detection, enabling the system to generate alerts or notifications when potential threats are identified.

Threat intelligence feeds offer data on the latest attack campaigns, malware variants, vulnerabilities, and exploit techniques. By carefully analysing this information, B/Ds can uncover patterns and trends in cybercriminal activities, identify their motivations, and understand the tools and methodologies deployed.

The following are some suggested steps to be taken for data collection, log analysis, and threat intelligence integration:

1. ***Identify log sources:*** Determine which ones should be monitored based on their importance to the business, governance, and compliance requirements. These may include network switches, routers, firewalls, host OS, security software, web applications, email applications, etc.

2. ***Define logging policies:*** Evaluate the importance of the components to the business and operations and decide what information should be logged. Establish logging policies that specify what events/activities should be recorded. For example, B/Ds may log all login attempts, access control changes, and critical system events.

3. ***Conduct load testing:*** Prior to implementing logging policies in the production environment, perform load testing on logging in a testing environment. This will help ensure that the planned log configuration can handle the expected load and not adversely affect system performance. For example, B/Ds can simulate a high volume of log events to ensure the configuration can handle the expected load without impacting system performance.

4. ***Implement centralised log aggregation and analysis:*** Consider implementing a centralised log aggregation and analysis solution, such as a Security Information and Event Management (SIEM) system. SIEM systems provide comprehensive

visibility into security events and allow for effective analysis of logs from various sources within the IT infrastructure.

5. ***Evaluate SIEM functionalities:*** Assess SIEM products based on their capabilities, such as security information management (SIM), security event management (SEM), real-time security alert analysis, threat verification, and incident workflow automation. Choose a SIEM solution that best meets the B/D's needs.

6. ***Integrate threat intelligence:*** Incorporate threat intelligence into the monitoring and analysis processes. This can involve leveraging external threat intelligence feeds, databases, or platforms to enhance the ability to identify and respond to specific threats.

7. ***Correlation and alert generation:*** Use threat intelligence integration to compare incoming logs, network traffic, and endpoint activities against known threat indicators. This correlation enhances the accuracy and effectiveness of threat detection, enabling the system to generate alerts or notifications when potential threats are identified.

8. ***Analyse threat intelligence:*** Carefully analyse threat intelligence information to uncover patterns and trends in cybercriminal activities, identify motivations, and understand the tools and methodologies deployed by attackers. This analysis can help strengthen the B/D's defences and stay ahead of evolving attack techniques.

9. ***Assess detection tools:*** Evaluate the quality of the detection tools available, including the strength of threat hunting capabilities and the availability of threat intelligence information from external feeds and internally generated intelligence. Ensure the effectiveness of the detection engineering functions.

10. ***Ensure efficient data collection:*** The effectiveness of the detection function relies on the availability of data obtained during the data collection stage. Ensure the collection function operates efficiently, collecting the necessary data for effective threat detection.

11. ***Stay updated:*** Continuously monitor and update the logging and threat intelligence integration processes based on evolving security threats and new technologies.

6.3 Behaviour Analysis, Anomaly Detection, and Threat Intelligence Application

To effectively monitor and detect IT security threats, B/Ds should establish baseline behaviour patterns for their network, systems, and users. By understanding what constitutes normal behaviour within the environment, B/Ds can identify deviations or anomalies that may indicate potential threats or malicious activities. After establishing the baseline behaviour patterns, B/Ds should leverage behaviour analysis techniques to identify anomalies or deviations. Behaviour analysis involves

monitoring and analysing ongoing activities to detect deviations from the established norms. This can be achieved using advanced analytical tools and techniques that compare current behaviour against the established baseline.

Here are some suggested steps:

1. ***Deployment of Data Analysis Tools:*** Deploy appropriate data analysis tools or platforms, such as SIEM systems, log management solutions, or other data analytics tools, to process and analyse historical data.

2. ***Data Preparation and Analysis:*** Analyse historical data on network traffic, system activities, and user behaviour to gain insights into typical patterns and activities within the B/D's infrastructure. Normalise the collected data by standardizing formats, converting timestamps to a common time zone, and addressing variations or inconsistencies in the data sources.

3. ***Identification of Relevant Data Parameters:*** Identify key parameters or attributes within the data that are relevant to establishing baseline behaviour patterns, such as network traffic flows, system resource utilisation, user login activities, and application usage.

4. ***Statistical Analysis and User/System Profiling:*** Apply statistical analysis techniques, such as mean, median, standard deviation, or clustering algorithms, to the historical data to identify trends, patterns, and distributions. Perform user and system profiling based on historical data analysis to create profiles or personas for typical user behaviour, system activities, and network traffic patterns.

5. ***Review, Update, and Documentation:*** Establish a process for continuous monitoring of ongoing data to update the baseline behaviour patterns over time as the B/D's infrastructure and user behaviour evolve. Document establishing baseline behaviour patterns, including the data collection plan, analysis techniques, and the identified normal behaviour parameters. Create documentation summarizing the baseline behaviour patterns and guide ongoing monitoring and detection efforts.

The application of threat intelligence in behaviour analysis enables B/Ds to correlate observed anomalies with known attack techniques or indicators. This correlation helps prioritise and validate potential threats, reduce false positives, and focus resources on the most critical risks. By studying threat intelligence, B/Ds can identify common attack vectors, such as phishing emails, social engineering techniques, or malicious software distribution methods. This allows B/Ds to proactively implement preventive measures and educate their staff about potential risks, reducing the likelihood of successful attacks.

To apply threat intelligence feeds and data into the monitoring and detection process, B/Ds can refer to the following steps:

1. ***Selecting relevant threat intelligence sources:*** B/Ds can choose from a variety of threat intelligence sources, such as commercial providers, open-source feeds, and industry-specific information sharing platforms. These sources provide information on emerging threats and known attack techniques.

2. ***Defining indicators of compromise (IoCs):*** Based on the identified threats and attack vectors, B/Ds can define IoCs. These IoCs are specific pieces of information that indicate a potential security incident, such as IP addresses, domain names, file hashes, or patterns of behaviour associated with known threats.

3. ***Collecting and aggregating threat intelligence data:*** B/Ds gather threat intelligence data from various sources and aggregate it into a central repository. This comprehensive collection of data provides a broader understanding of the threat landscape.

4. ***Normalising and enriching threat intelligence data:*** B/Ds normalise and enrich the collected threat intelligence data to ensure consistency and enhance analysis effectiveness. This process involves standardising formats, adding contextual information, and correlating data from different sources.

5. ***Integrating threat intelligence feeds into monitoring and detection processes:*** Threat intelligence feeds are integrated into the B/D's monitoring and detection systems. This integration allows for correlating observed anomalies with known attack techniques or indicators, enabling faster and more accurate threat detection.

6. ***Matching and correlating IoCs with collected data:*** The defined IoCs are matched and correlated with the collected data to prioritise and validate potential threats. This process helps identify and focus on the most relevant and high risk security incidents.

7. ***Continuously updating and refreshing threat intelligence data:*** Threat intelligence data is not static, and new threats and vulnerabilities emerge regularly. B/Ds need to continuously update and refresh their threat intelligence data to stay informed about emerging threats and adapt their security measures accordingly.

8. ***Monitoring and evaluating effectiveness:*** B/Ds monitor and evaluate the effectiveness of integrating threat intelligence feeds and data into their monitoring and detection processes. This evaluation helps identify areas for improvement and ensures that the threat intelligence program provides value in enhancing cybersecurity.

7 Threat Triage and Investigation

7.1 Prioritising Threats through a Triage Process

Triage refers to the initial assessment and classification of security alerts to determine their priority and appropriate response. Triage aims to perform rapid remediation or escalation to cater to a high volume of security alerts. Similar to the triage process in an emergency room of a hospital, B/Ds aim to prioritise the investigation queue based on the available data logically. Leveraging their previous defence experience, B/Ds make informed decisions to ensure efficient resource allocation.

To facilitate the triage process, the following prerequisites should be met:

1. ***Establish predefined criteria:*** B/Ds should develop clear criteria to guide the decision-making process during triage. More illustrative examples are shown in Table 6.1. These criteria should be regularly reviewed and updated to adapt to changes in the threat landscape and emerging technologies.

2. ***Leverage threat frameworks:*** B/Ds should utilise frameworks such as the Lockheed Martin Cyber Kill Chain and the MITRE ATT&CK framework to gain insights into the lifecycle and different stages of an attack and common techniques used by adversaries. These frameworks can aid in understanding and categorizing security alerts.

Here is an overview of the triage process:

1. ***Alert Collection and Analysis:*** Alerts are collected and analysed by security analysts or automated tools. Analysts review the details provided by each alert, including relevant logs, network traffic data, and any associated indicators of compromise (IoCs).

2. ***Alert Validation:*** The next step is to validate the alerts to confirm their accuracy and relevance. This involves examining the supporting evidence, such as network logs, system logs, or intrusion detection system data, to determine if the alert indicates a genuine security incident or a false positive. Misconfigurations, software glitches, or benign user behaviour can cause false positives. False positives should be identified and feedback provided to the detection engineering team for rule refinement.

3. ***Severity Determination:*** Alerts are categorised and assigned a severity level based on their potential impact and urgency per the predefined criteria. This lets the security team focus on addressing the most severe threats first. Common categories may include attack steps/ stages or techniques. Common severity levels may include high, medium, and low or a similar determination scheme tailored to the B/D's needs. This step helps in prioritising the alerts for further investigation.

4. ***Continuous Monitoring and Iterative Triage:*** Throughout the response process, continuous monitoring and further triage are conducted to identify any new alerts or changes in the threat landscape. This ensures that emerging threats or evolving incidents are promptly detected and addressed.

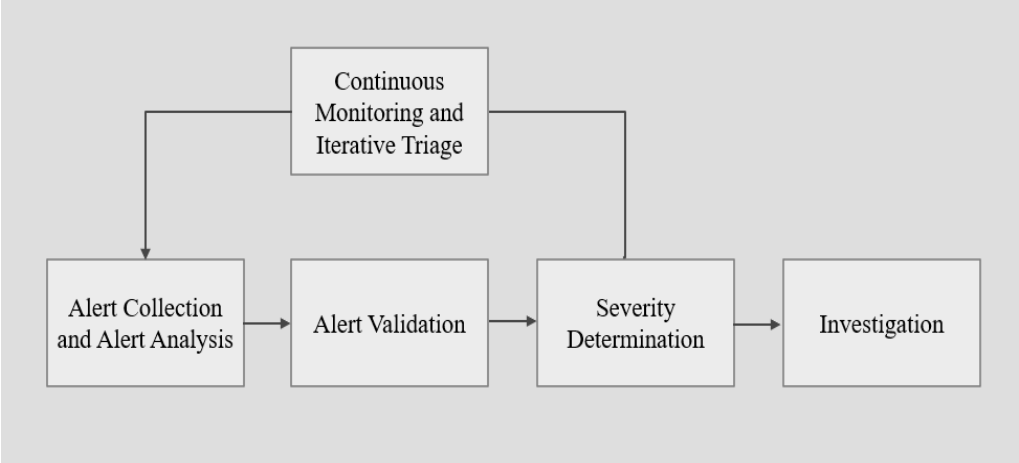

Figure 6.1 Overview of the Triage Process

The effectiveness of the triage process is driven mainly by the level of detail and additional context provided by security tools and techniques when B/Ds triage alerts. Security tools, such as ticketing systems and SIEMs (Security Information and Event Management), can offer features that enhance decision-making, automate workflows, and contribute to a more efficient and effective triage process. Triage tools provide dedicated platforms for security teams to intake, assess, and manage security incidents quickly and consistently.

It is important to note that the triage process is dynamic and may require ongoing reassessment with contextual understanding gathered from threat intelligence. Threat intelligence provides valuable context about threat actors' nature, capabilities, motivations, and targets. This contextual understanding helps B/Ds assess the potential impact of threats on their systems, data, and business operations. As new information becomes available or the threat landscape evolves, the triage process may need to be adjusted to reflect the changing threat landscape.

Here is a sample to illustrate the predefined criteria for triage using the MITRE ATT&CK framework. Assume a B/D receives an alert about a suspicious outbound connection from an internal system to a known malicious IP address. They need to prioritise their response based on the following criteria:

Criteria	Description	Sample illustration
Severity of the Alert	Assess the severity level assigned to the alert, indicating the potential impact and urgency of the security alert. Higher severity alerts may require	The team assesses the severity level of the alert. If the connection indicates a high-risk incident or is associated with a known threat actor, they prioritise it over lower severity alerts.

Criteria	Description	Sample illustration
	immediate attention and prioritization.	
Potential Impact on Critical Systems or Functions	Consider the potential impact of the alert on critical systems or functions that are essential for the B/D's operations. Alerts that have the potential to disrupt or compromise critical systems should be given higher priority.	They consider the potential impact of the malicious IP connection on critical systems or essential functions of the B/D. If the connection poses a risk of unauthorised access, data exfiltration, or disruption to critical operations, they prioritise it accordingly.
Regulatory and Compliance Requirements	Consider any regulatory or compliance requirements that the detected technique may impact. Techniques that could result in non-compliance or regulatory violations should be prioritised.	The team considers any regulatory or compliance requirements the malicious IP connection may implicate. If non-compliance or regulatory violations can occur due to unauthorised communication with malicious entities, they prioritise it to ensure adherence to legal and industry standards.
Potential for Operational Disruption	Assess the potential for the alert to cause significant operational disruption or downtime. Alerts with a higher risk of disrupting business operations or services should be prioritised accordingly.	They evaluate the potential for the malicious IP connection to cause operational disruption. If there is a risk of system compromise, network-wide infection, or service disruption, they prioritise it to minimise the impact on business operations.
Number of Affected Systems	Consider the number of systems or assets affected by the alert. Alerts impacting a larger number of systems may require immediate attention and prioritization due to the potential for widespread impact.	The team considers the scope and scale in terms of the number of systems affected by the malicious IP connection. If multiple systems communicate with the same malicious IP address or critical systems are involved, they prioritise it due to the potential for widespread impact and increased risk.
Urgency of the Situation	Evaluate the urgency of the alert and the need for immediate action. Alerts that indicate an ongoing or active security incident or require immediate containment or remediation should be	They assess the urgency based on factors such as the nature of the connection, the level of threat associated with the IP address, or the potential for immediate data exfiltration. If swift action is required to block the connection or contain the

Criteria	Description	Sample illustration
	prioritised to minimise further damage or compromise.	threat, they prioritise it accordingly.
Technique Relevance	Assess the relevance of the detected technique in relation to the B/D's infrastructure and systems. Prioritise techniques that are known to be effective against the B/D's environment.	The team assesses the relevance of the malicious IP connection technique to their B/D's infrastructure. They consider whether similar incidents have occurred or if there is a history of similar attacks. If threat actors frequently employ the technique or pose a significant risk to their systems, they prioritise it accordingly.
Tactic Importance	Consider the importance of the tactic associated with the detected technique. Focus on techniques that align with high-priority tactics, such as initial access, execution, or exfiltration.	They evaluate the importance of the tactic associated with the malicious IP connection. If the connection is part of an initial access tactic or indicates an attempt to gain unauthorised entry into their systems, they prioritise it due to the criticality of preventing such unauthorised access.
Persistence Potential	Evaluate the potential for the detected technique to enable persistence within the B/D's systems. Give higher priority to techniques that are more likely to enable long-term access.	The team considers the potential for the malicious IP connection to enable persistence within their systems. If successful, could it allow the attacker to maintain long-term access or establish a foothold for future attacks? They prioritise addressing this technique if it has a high potential for persistence.
Exploit Maturity	Consider the maturity level of the exploit associated with the detected technique. Give higher priority to techniques that have known, effective exploits readily available.	They assess the exploit maturity associated with the malicious IP connection. If there are known, effective exploits associated with the IP address or if it is associated with sophisticated attack techniques, they prioritise addressing this technique promptly.
Known Adversary Usage	Determine if the detected technique has been observed in use by known	The team determines if the malicious IP address has been observed in use by known

Criteria	Description	Sample illustration
	threat actors or if it aligns with their typical tactics, techniques, and procedures (TTPs). Techniques used by sophisticated or targeted attackers may warrant higher priority.	threat actors. If the IP address is associated with advanced persistent threats or known malicious campaigns, they prioritise addressing this technique due to the potential implications of being targeted by these adversaries.
Potential for Lateral Movement	Techniques used by sophisticated or targeted attackers may warrant higher priority. Evaluate the potential for the detected technique to facilitate lateral movement within the B/D's network. Techniques that enable easy lateral movement should be prioritised.	They evaluate the potential for the malicious IP connection to facilitate lateral movement within their network. If successful, could it allow the attacker to move laterally and access additional systems? Techniques that enable easy lateral movement are prioritised as they can lead to further compromise and data exfiltration.
Visibility	Consider the visibility and detection capabilities for the detected technique within the B/D's security controls. Techniques that can bypass or evade existing security measures should be prioritised.	The team considers the level of visibility and detection capabilities they have for identifying and monitoring outbound connections. If the existing security measures can effectively detect and alert malicious IP connections, they may prioritise this technique lower compared to other techniques that are harder to detect.

Table 6.1 Sample to illustrate the predefined criteria for triage using the MITRE ATT&CK framework

7.2 Investigate Suspicious Activities and Indicators

After triaging an alert, B/Ds should follow a structured approach involving advanced analysis to investigate if the validated alerts constitute threats or actual attacks, such as alerts that indicate a more sophisticated attacker that triggers behavioural alerts and possible ongoing attack campaigns.

Here are the key steps involved in the investigation process:

1. ***Evidence Gathering:*** Once an alert is validated and triaged as a legitimate security alert, the analysts collect additional evidence to understand better the potential threat. This may involve capturing and preserving relevant logs,

network traffic data, system snapshots, or other artefacts that can provide insights into the nature and impact of the incident.

2. ***Threat Analysis:*** Investigation analysts comprehensively analyse the threat to determine its characteristics, motivations, and potential impact. This may involve leveraging threat intelligence feeds, analysing malware samples, or researching known attack techniques associated with the incident. Threat analysis helps identify the attacker's intent, the potential risks, and any indicators of compromise (IoCs) that can aid detection and prevention.

Below are two illustrative examples for B/Ds to understand the key tasks and flow of the investigation stage.

- A B/D has received a triaged alert of a malicious IP connection attempt; the team collects network logs, firewall logs, or any other relevant network data that captures the connection attempt. They consult threat intelligence feeds and databases to identify known malicious IPs, their associated activities, and potential threat actors. Then, they analyse the characteristics of the connection attempt, such as source IP, destination IP, and port numbers, to identify patterns or similarities with known malicious activities.

- A B/D has received a triaged alert regarding the detection of new administrator credentials on a client system. The team collects relevant logs, such as system event logs or authentication logs, to gather information about creating the new admin account. They consult threat intelligence feeds and databases to identify any known techniques or indicators of compromise (IoCs) associated with unauthorised account creation or privilege escalation. The team analyses the logged events, including timestamps, account names, and system activity, to identify any suspicious patterns or anomalies in creating the new admin credentials.

B/Ds should undergo rigorous training to perform systematic analyses to ensure effective investigation, avoiding cognitive biases and common errors. This training equips them with the necessary skills to conduct investigation thoroughly and unbiasedly.

The effectiveness of the investigation stage depends on several factors. The experience and analysis techniques of the personnel involved, the availability of relevant data, and the use of technology and automation tools that assist in generating and presenting evidence to B/Ds all contribute to the effectiveness of the investigation.

By conducting thorough investigation and leveraging their skills, knowledge, and available resources, B/Ds can accurately determine threats' nature, scope, and root cause. This enables the implementation of appropriate responses.

8 Threat Response

Threat response is a proactive approach to mitigating and preventing cyber threats before they escalate into incidents. It involves timely actions to neutralise threats and minimise their impact. Effective threat response relies on accurate threat intelligence and predefined measures to ensure swift and appropriate actions are taken. Accurate threat intelligence provides real-time information about emerging threats and vulnerabilities, enabling B/Ds to take timely actions to prevent attacks.

When security alerts have been confirmed as threats, appropriate responses should be made. To minimise the impact of threats and protect assets, systems, and data, B/Ds should develop predefined actions and measures that can be executed in response to potential threats or alerts. Severity classification guides the selection of appropriate response actions. Higher severity threats require immediate and focused response efforts, such as containment, investigation, and eradication. In comparison, lower severity threats can be more controlled based on resource availability and priority.

Here are some key actions and measures commonly employed in effective threat response:

1. ***Containment:*** This involves measures such as retracting delivered emails from users' mailboxes, adding users to low permission groups, updating block lists of firewalls and web filters, and implementing blocking mechanisms across various solutions like mail gateways, firewalls, EDR (Endpoint Detection and Response), web gateways, Active Directory, network access control (NAC), and others.

2. ***Blocking:*** Implementing measures to block malicious activities or unauthorised access to systems and networks.

3. ***Patching:*** Applying necessary software patches and updates to address vulnerabilities and strengthen the security posture.

4. ***Training:*** Conducting training programs to educate users and employees about potential threats, best practices, and security awareness.

After responding to the threats, B/Ds should enrich and group all these threats from various sources and determine if these should be escalated into incidents. The analysts should provide a context-rich view of threats based on the forensic analysis. This enables them to identify areas for additional investigations or trigger the required incident response. Please refer to the **Practice Guide for Information Security Incident Handling** for more details.

Here is an example of a threat response:

When the monitoring tools detect suspicious activity, immediate threat response actions are initiated. The analyst analyses the alert and confirms it as a potential threat to the B/D's security. Based on the severity classification, it is determined that the threat can be mitigated with predefined actions.

The affected systems are promptly isolated from the network as a containment measure, preventing the potential spread of the threat. Simultaneously, the analyst employs blocking mechanisms across various solutions, such as firewalls, web filters, and network access control, to block malicious activities and unauthorised access.

To address any vulnerabilities that may have been exploited, the analyst ensures that necessary software patches and updates are applied promptly, enhancing the overall security posture.

After the threat response, the analyst reviews and enriches the threat intelligence by grouping and analysing the collected data. This analysis provides a context-rich view of the threats. If needed, it helps identify areas of additional investigations or escalations to the incident response team.

To promote security awareness among employees, the B/D conducts regular training programs that educate users about potential threats, best practices, and security awareness. These training sessions build a culture of vigilance and proactive threat reporting.

In this case, the threat response successfully mitigates the potential incident.

B/Ds may also consider establishing playbooks to document defined actions and measures to respond to threats before they materialise into actual incidents. Examples of playbooks are available in **Annex C**.

9 Continuous Improvement and Adaptation

9.1 Regular Monitoring, Evaluation, and Security Posture Assessment

Regular monitoring, evaluation, and security posture assessments should be carried out to measure the effectiveness of threat monitoring and make informed decisions to enhance the overall security posture.

B/Ds should establish Key Performance Indicators (KPIs) to measure the effectiveness of threat monitoring. These measurable metrics provide insights into the performance and progress of B/Ds' IT security efforts. When determining KPIs, B/Ds should consider factors such as the volume and types of threats encountered, incident response time, detection accuracy, and the effectiveness of implemented security controls. These KPIs should align with the B/D's objectives and reflect its unique risk landscape.

Continuous monitoring of the threat landscape is essential to stay ahead of emerging risks and vulnerabilities. This includes monitoring external threat intelligence sources, security alerts, and incidents within the B/D. Regular evaluations of the effectiveness of threat monitoring processes and technologies should be performed to ensure they remain up-to-date and efficient. The evaluation may involve assessing the accuracy and timeliness of threat detection systems, the effectiveness of security controls, and the responsiveness of incident response procedures. Examples of specific KPIs for IT security threat management include:

- ***Mean Time to Detect (MTTD).*** This KPI measures the average time to detect an IT security threat or security incident. It provides insights into the efficiency and effectiveness of the B/D's monitoring capabilities. The lower the MTTD, the faster the B/D can respond to threats, minimising potential damage.

- ***Mean Time to Respond (MTTR).*** This KPI measures the average time to respond and resolve an IT security threat or security incident once detected. It reflects the B/D's incident response efficiency and ability to contain and mitigate the impact of threats. A lower MTTR indicates a faster and more effective response.

- ***False Positive Rate.*** This KPI measures the percentage of alerts generated by the monitoring system that are determined to be false positives, i.e., not actual security threats. A high false positive rate indicates more unnecessary investigations or resources for non-threatening events. Lowering the false positive rate helps improve the efficiency of threat monitoring and reduces the burden on incident response teams.

- ***Detection Accuracy.*** This KPI measures the percentage of actual security threats successfully detected by the monitoring system. It reflects the system's ability to identify and flag genuine threats accurately. A higher detection accuracy rate indicates a more robust and reliable monitoring capability.

- ***Incident Response Time.*** This KPI measures the time to initiate an appropriate response once a security incident has been detected. It includes the time required for incident triage, assessment, and activation of incident response processes. A shorter incident response time enables a more rapid containment and mitigation of threats.

- ***Threat Intelligence Utilisation.*** This KPI measures the extent to which the B/D effectively incorporates threat intelligence into its monitoring and response processes. It assesses the B/D's ability to proactively leverage external threat intelligence sources to identify and address emerging threats.

- ***Coverage of Monitored Assets.*** This KPI assesses the percentage of critical assets or systems actively monitored for potential threats. It ensures comprehensive coverage and identifies any gaps in monitoring, allowing B/Ds to prioritise resource allocation and enhance their overall monitoring capabilities.

- ***Compliance with Monitoring Policies and Procedures***. This KPI evaluates the adherence of the B/D to established monitoring policies and procedures. It measures compliance with regulatory requirements, internal policies, and industry best practices, ensuring that monitoring activities align with established standards.

Security posture assessments provide a comprehensive view of B/D's overall security readiness. It involves evaluating the effectiveness of security controls, identifying vulnerabilities, and assessing the B/D's ability to detect and respond to threats. Examples of security posture assessments include:

- ***Penetration Testing.*** Penetration testing involves simulating real-world attacks to identify system, network, or application vulnerabilities. By conducting controlled and authorised tests, B/Ds can effectively assess their ability to detect and respond to various attack scenarios. The results of penetration testing help pinpoint specific areas that require immediate attention and allow remediation actions to be prioritised based on their criticality.

- ***Vulnerability Assessments.*** Vulnerability assessments involve scanning systems and networks for known vulnerabilities and misconfigurations. By identifying these weaknesses, B/Ds can promptly patch or mitigate them, reducing the risk of exploitation by threat actors.

- ***Red Team Exercises.*** Red team exercises refer to a dedicated team emulating real-world adversaries' tactics and techniques to test defences' capability. This simulation provides a realistic assessment of the effectiveness of threat monitoring controls and practices. By challenging the security measures in place, red team exercises help uncover potential vulnerabilities and identify areas that need improvement.

- ***Purple Team Exercises.*** Purple team exercises refer to a team of experts taking on the role of both the red team and blue team, intending to provide a more

substantial, more profound assurance activity that delivers more tailored and realistic assurance. Through these exercises, the teams learn from each other to improve both offensive and defensive strategies, enhancing B/D's overall IT security posture.

B/Ds should engage qualified and reputable IT security professionals or external service providers with the necessary expertise, tools, and methodologies to perform security posture assessments.

9.2 Evaluating and Updating Threat Intelligence

Review and validation of the relevance and accuracy of threat intelligence sources should be conducted regularly. B/Ds should establish a process for continuous evaluation, which may include the following factors:

- Source Relevance;
- Source Accuracy;
- Timeliness; and
- Quality and Credibility.

Based on the evaluation outcomes, B/Ds should update their threat intelligence sources as necessary. This may involve adding new sources, removing irrelevant or non-credible ones, or adjusting the weighting and priority given to different sources based on their performance and relevance.

9.3 Evaluating and Updating Controls and Technologies

IT security controls and technologies should be evaluated and updated regularly to keep pace with the rapidly evolving nature of IT security threats. B/Ds should take the following considerations into account when evaluating and updating controls and technologies:

- ***Industry Trend Monitoring.*** Actively monitor industry trends and advancements in threat monitoring and detection. Stay informed about the latest technologies, tools, and methodologies in the IT security landscape. Stay updated through industry publications, relevant conferences, and seminars, and participate in industry forums and working groups.

- ***Threat Monitoring and Detection Technologies.*** Regularly assess the effectiveness of threat monitoring and detection technologies deployed within the B/D. Evaluate their ability to identify and respond to evolving threats, including APTs, zero-day vulnerabilities, and insider threats. Consider the availability of new technologies, such as machine learning, artificial intelligence, and behaviour analytics, which can enhance threat detection capabilities.

- ***Incident Response Plan Evaluation.*** Evaluate the efficacy of existing incident response plans and procedures. Review how effectively incidents are handled, including response times, containment measures, and recovery processes. Stay

informed about the latest incident response frameworks and methodologies to ensure alignment with industry best practices and evolving threat scenarios.

- ***Collaboration and Information Sharing.*** Foster collaboration and information sharing with other B/Ds and industry partners. Engage in knowledge exchange initiatives to learn about successful strategies and technologies others implement. Participate in information sharing platforms, such as threat intelligence-sharing communities, to gain insights into emerging threats and effective mitigation strategies.

B/Ds should update controls and technologies based on the evaluation result to align with the evolving threat landscape and industry advancements. This may involve implementing new technologies, adopting updated frameworks and methodologies, or revising incident response plans based on lessons learnt and emerging best practices.

*** ENDS ***

Annex A: Sample Threat Taxonomy

No.	Threat Types	Threats	Threat Details
1	Social Threats	Fraud	Fraud committed by humans.
2	Social Threats	Theft (devices, storage media, and documents)	Stealing information or IT assets. Robbery.
3	Social Threats	Information leak /sharing	Information leak / sharing information due to intentional or unintentional human actions or errors.
4	Social Threats	Unauthorised physical access / Unauthorised entry to premises	Unapproved access to facility.
5	Social Threats	Terrorist attack	Threats from terrorists.
6	Technical Threats	Using information from an unreliable source	Bad decisions based on unreliable sources of information or unchecked information.
7	Technical Threats	Inadequate design and planning or improper adaptation	Threats caused by improper IT assets or business process design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors).
8	Technical Threats	Failure or disruption of communication links (communication networks)	The threat of failure or malfunction of communications links.
9	Technical Threats	Denial of service	The threat of service unavailability due to massive requests for services.
10	Technical Threats	Malicious code/ software/ activity	The threat of malicious code or software execution.
11	Technical Threats	Unauthorised installation of software	Threat of unauthorised installation of software.
12	Environmental Threats	Fire	Threat of fire
13	Environmental Threats	Thunderstrike	The threat of damage to IT hardware caused by thunder strike (overvoltage).
14	Environmental Threats	Water	The threat of damage to IT hardware caused by water.

15	Environmental Threats	Explosion	The threat of damage to IT hardware caused by explosion
16	Environmental Threats	Unfavourable climatic conditions	The threat of disruption of work of IT systems due to climatic conditions negatively affecting hardware.
17	Environmental Threats	Wildlife	Threat of destruction of IT assets caused by animals: mice, rats, birds.

Here is an illustrative example that focuses on how a threat taxonomy assists the B/D in identifying and prioritising specific threats, enabling them to implement targeted security measures to protect taxpayer information and maintain the integrity of their operations:

This B/D is responsible for administering Hong Kong's tax laws and ensuring the collection of taxes to support government operations and public services. As part of their efforts to safeguard taxpayer information and maintain the integrity of their systems, the B/D conducts a threat assessment to identify potential IT security threats specific to their operations.

During the threat assessment, the B/D identifies various threats across different categories that could compromise taxpayer data and disrupt their operations.

In the social threats category, they recognise the risk of phishing attacks targeting taxpayers or B/D's employees. These attacks aim to deceive individuals into divulging sensitive information, such as tax identification numbers or login credentials, which could be exploited for fraud.

Within the technical threats category, the B/D acknowledges the potential for ransomware attacks that could encrypt their systems and render them inaccessible until a ransom is paid. They also consider the risk of unauthorised access to taxpayer databases, either through external hacking attempts or insider threats where employees abuse their access privileges.

In the environmental threats category, the B/D recognises the impact of power outages or other infrastructure failures that could disrupt their IT systems and compromise data availability. They also consider the risk of physical breaches, such as unauthorised entry into their data centres or offices, which could lead to theft or tampering with sensitive taxpayer information.

Based on these identified threats, the B/D develops a taxonomy tailored to their specific needs. They define specific threat types within each category, such as targeted tax phishing emails as social threat, ransomware attacks as a technical threat, and physical breaches as environmental threats.

By having a well-defined threat taxonomy, the B/D can implement targeted security measures to protect taxpayer data and maintain the continuity of its operations. They invest in robust email filtering and awareness programs to educate taxpayers and employees about the risks of phishing attacks. They also implement advanced endpoint protection, regular system backups, and incident response protocols to mitigate the impact of ransomware and unauthorised access attempts.

Additionally, the B/D establishes stringent physical security measures, including access controls, surveillance systems, and personnel vetting, to safeguard their premises and prevent unauthorised entry.

Regular security audits and penetration testing help identify vulnerabilities and ensure the effectiveness of implemented security controls. The B/D also maintains strong partnerships with law enforcement agencies, industry associations, and other government departments to share threat intelligence and collaborate on cybersecurity initiatives.

Annex B: Sample List of Questions for Suppliers of IT Security Threat Intelligence

1. How wide a range of sources do you use?
   Providers should collect from and fuse a broad range of original sources to provide intelligence, as per the intelligence cycle.

2. How do you collect from these sources?
   Providers should be able to deliver sufficient detail to reassure regarding their collection capabilities and ideally be able to collect the information independently without having to rely on third parties.

3. What types of threat actors does the intelligence cover?
   Providers should cover all types of actors from which the B/D faces a threat, which usually means collecting from diverse sources.

4. How timely is the intelligence you provide?
   This should be governed by the level of intelligence provided, i.e., strategic, tactical or operational.

5. What format is the intelligence provided in?
   This will vary according to the nature and level of the material. However, analyst access, in-person briefings, bespoke reports and intelligence reports relevant to the B/D are likely to be more useful than generic threat data.

6. How can the product integrate with my existing capabilities?
   The ability to integrate will be important if a B/D has existing providers and infrastructure.

7. How bespoke is the product to the B/D?
   Tailored products will invariably be more useful than generic outputs, and data is invariably less useful than fused intelligence assessed by skilled analysts for the B/D.

8. What evaluation process do you apply to the intelligence you produce?
   Mature providers will have established methodologies for assessing intelligence and ensuring it is bespoke to the B/D.

9. How do you remove false positives?
   Human vetting of material will result in less inaccurate reporting.

10. What are your team's backgrounds and language capabilities?
    Diverse and experienced analytical teams will invariably be able to provide the highest quality products, and the certifications of individuals may well be a useful guide.

11. Is your analysis predictive as well as reactive?
    Mature providers should be able to provide forward-looking assessments for the B/D.

12. Are your team individually certified as Threat Intelligence professionals?

Professional-level qualifications exist in the practice of threat intelligence, such as those provided by CREST and other organisations such as SANS.

13. Is your business accredited as a Threat Intelligence provider by recognised authorities?
    Accreditations, such as by CREST, show that the provider has proved its capabilities in addition to high legal and ethical standards.

14. Do you regularly provide services for these regulated frameworks?
    Mature suppliers will regularly support engagements for these frameworks.

15. How can you demonstrate knowledge of our (the buyer's) sector?
    The supplier may have experience in conducting bespoke research and have dedicated subject matter experts within the team.

16. What security measures does your company employ to keep our threat intelligence secure?
    Due to the potential sensitivity of the intelligence produced, suppliers should be able to reassure clients as to its security, for example, by sharing client information security policies.

17. How can you prove the quality of your products and services?
    Suppliers should be able to provide references following successful engagements.

Annex C: Example of playbooks for threat response

Please note that the below playbooks are illustrative examples for threat response, B/Ds should tailor for their specific needs instead of merely following the steps listed below.

1. New Vulnerability from Threat Intelligence

Stages	Description
Identification	• Identify and categorise relevant IT security threats, including the newly discovered vulnerability from threat intelligence.
Monitoring	• Continuously monitor network traffic, system logs, and security events for any indicators related to the identified vulnerability.
Detection	• Analyse collected data, such as log files and network traffic, to detect patterns or anomalies that may indicate exploitation of the identified vulnerability.
Triage	• Initiate triage based on available vulnerability and asset criticality information. • Check for any indications of attacks that have already occurred, analysing Indicators of Compromise (IoC) and Tactics, Techniques, and Procedures (TTP). • Verify if the assets are vulnerable by matching their version/configuration information with the vulnerable ones. • Escalate the situation as per the triage results.
Investigation	• Conduct a thorough investigation to assess the impact of the vulnerability, identify potential attack vectors, and gather additional intelligence for future prevention. • Review firewall rules and other security configurations to identify potential attack vectors. Automated tools can be utilised for this purpose.
Response	• Discuss mitigation measures with SOC, IT security management unit, and IT support teams. • Formulate and perform actions and measures to respond to the identified vulnerability, which may involve immediate shutdown, applying patches, implementing workarounds, or considering preventive measures for future asset builds. • Perform a vulnerability rescan to confirm closure.

2. Privileged Account Brute Force Authentication

Stages	Description
Identification	Not applicable.
Monitoring	• Utilise privileged access management (PAM) systems to monitor privileged access usage. • Monitor and log authentication activities from relevant endpoints.
Detection	• Correlate PAM logs with authentication logs from relevant endpoints to detect unauthorised use and identify potential stolen credentials. • Trigger alerts for any logon activity by privileged accounts without corresponding PAM approval.
Triage	• Initiate triage based on available vulnerability and asset criticality information. • Check for any indications of attacks that have already occurred by analysing Indicators of Compromise (IoC) and Tactics, Techniques, and Procedures (TTP). • Verify if the assets are vulnerable by matching their version/configuration information with the vulnerable ones. • Escalate the situation as per the triage results.
Investigation	• Conduct further investigation to determine the extent of the unauthorised access, assess potential security breaches, and gather additional information for future prevention. • Contact relevant system administrators to inquire if they have used the accounts during the specified time frame. • If no administrator claims responsibility for the usage, expand the collaboration to include related application support teams. • If no conclusion is reached, treat this as an incident and proceed to incident response.
Response	• Engage in incident response procedures to mitigate the impact of the successful attack. • Make updates to the correlation rules for risk-accepted exceptions to refine the detection process and accurately identify unauthorised privileged access incidents.

3. Virtual Private Network (VPN) abnormalities

Stages	Description
Identification	Not applicable.
Monitoring	• Continuously monitor for VPN abnormalities, as attackers often exploit VPNs to maintain persistent access to the organisation's environment.
Detection	• Receive alerts from the identity management system indicating the presence of VPN accounts without corresponding account creation approval records. • If an identity management system is unavailable, manually or through scripting, cross-check the exported VPN account list with the user account request ticketing system. • Users report unexpected VPN password resets or changes in registered mobile devices without their consent.
Triage	• Verify the legitimacy of the concerned VPN accounts and their activities. • Consult with the VPN administrator to confirm the account's legitimacy and activities. • Gather access logs for the identified VPN accounts and examine the source IPs of the connections. Confirm if they align with legitimate VPN users. • Exercise caution when relying solely on geo-IP information, as attackers may rent rack space near the B/D's user base (e.g., data centres in the same city) to bypass location-based filters. • Escalate the situation as per the triage results to relevant IT teams to identify the root cause, as the VPN system may not be the initial entry point for the attacker.
Investigation	• Perform in-depth forensic analysis to understand the root cause of the VPN abnormalities and identify any additional compromised systems.
Response	• Inform VPN account owners of the abnormalities discovered and recommend changing passwords on other systems, including personal devices. • If unauthorised accounts or activities are detected, consider the concerned accounts (and even the VPN system) compromised. Trigger the incident response.

4. DNS callback

Stages	Description
Identification	Not applicable.
Monitoring	• Continuously monitor DNS-related indicators of malicious activity. • Set up DNS monitoring to generate alerts for long domain name queries, known bad queries (IoC/TTP), and abnormal DNS traffic volume and frequency.
Detection	• Recognise using DNS as a callback mechanism by malware, which has evolved. • Network security devices like IPS/IDS may raise alerts for unusual DNS queries.
Triage	• Confirm the presence of malicious DNS activity and its extent. • Review DNS logs to determine the start date of similar DNS queries and identify similar behaviour from other endpoints. Include refused queries in the log review based on DNS server configurations. • Examine endpoint security event logs (e.g., XDR) for indications of malware on the relevant endpoints. • If necessary, conduct forensic analysis on the affected endpoints to identify the process responsible for sending out the suspicious DNS queries.
Investigation	• Perform detailed forensic analysis to uncover the root cause of the DNS callback and identify any additional possible compromised systems. • Analyse the gathered data and evidence to understand the entry point of the malware.
Response	• If a compromise is confirmed, trigger an incident response to investigate how the malware gained access. • Implement the appropriate response actions on the compromised hosts, which may involve isolating, quarantining, or removing the malware.

Annex D: Guidance on Endpoint Detection and Response Adoption and Architecture

In the ever-evolving landscape of cybersecurity threats, EDR solutions have emerged as a critical line of defence for B/Ds seeking to safeguard their digital assets. These guidelines aim to provide comprehensive guidance on EDR adoption and architecture to assist B/Ds in implementing these solutions effectively.

D.1. Introduction of EDR

EDR solutions act as vigilant sentinels, fortifying B/Ds against myriad threats lurking in the digital realm. By adopting EDR, B/Ds can elevate their threat detection capabilities, enhance incident response procedures, and bolster their security posture. Through real-time monitoring, behaviour analysis, and threat intelligence integration, EDR empowers B/Ds to proactively identify and neutralise advanced threats like malware, ransomware, and insider attacks.

D.1.1. EDR Core features

EDR solutions are distinguished by their essential features, which empower B/Ds to combat sophisticated threats. Real-time monitoring, behaviour analysis, threat intelligence integration, incident response automation, and forensic capabilities are among the core features that define EDR solutions. Below, delve into the significance of each feature, highlighting how they contribute to effective threat management and incident response within B/D environments. Here are some core features of EDR solutions:

- ***Endpoint Visibility:*** EDR solutions provide real-time visibility into all endpoints, including laptops, desktops, mobile devices, servers, and IoT devices. This visibility allows security teams to monitor and analyse endpoint activities to identify suspicious behaviour.

- ***Threat Detection:*** EDR solutions use advanced threat detection techniques, such as behavioural analytics and machine learning, to identify indicators of compromise (IOCs) and indicators of attack (IOAs). EDR solutions can detect and alert security teams about potential threats by analysing endpoint events and telemetry data.

- ***Incident Investigation:*** EDR solutions offer investigation capabilities to analyse and understand security incidents. They provide tools for searching and querying endpoint data, allowing security teams to investigate the root cause of an incident and gather evidence for further analysis.

- ***Threat Hunting:*** EDR solutions enable proactive threat hunting by allowing security teams to search for potential threats and indicators of compromise across endpoints. This capability helps identify hidden or advanced threats that may have evaded traditional security measures.

- ***Threat Intelligence Integration:*** EDR solutions integrate with threat intelligence sources to enhance threat detection and response capabilities. By leveraging up-to-date threat

intelligence, EDR solutions can identify known malicious activities and provide contextual information about the attack.

- ***Real-time and Historical Visibility:*** EDR solutions act as a DVR on endpoints, recording and providing comprehensive visibility into security-related activities in real-time. This includes monitoring network connections, user logins, process executions, and file creation. Historical visibility allows security teams to analyse past events and identify patterns or trends.

- ***Incident Response and Remediation:*** EDR solutions enable fast and decisive incident response by providing real-time response capabilities. This includes the ability to isolate compromised endpoints from the network, contain threats, and remediate incidents without impacting performance.

D.1.2. EDR's Distinction from Other Products

In several key ways, EDR solutions stand apart from traditional endpoint security products, such as antivirus software or intrusion detection systems. Here are the main differences:

1. ***Detection Approach:***
    - Traditional antivirus software primarily relies on signature-based detection, which involves comparing files against a database of known malware signatures. This approach is effective against known threats but may struggle with new or unknown malware.
    - EDR solutions, on the other hand, focus on behaviour-based detection. They monitor and analyse endpoint activities in real-time, looking for suspicious or anomalous behaviour that may indicate a potential threat. This approach allows EDR to detect known and unknown threats, including zero-day attacks.

2. ***Visibility and Response Capabilities:***
    - Antivirus software typically provides limited visibility into endpoint activities, often only alerting when a known threat is detected. It lacks the ability to provide detailed insights into the attack chain or the ability to respond effectively.
    - EDR solutions offer enhanced visibility and control over endpoints. They collect and analyse a wide range of endpoint data, including file modifications, process creations, network connections, and more. This comprehensive visibility enables security teams to quickly identify and respond to security incidents, minimising the impact of an attack.

3. ***Incident Response and Threat Hunting:***
    - Traditional antivirus software is primarily focused on detecting and blocking malware. It may not provide robust incident response capabilities or support for proactive threat hunting activities.
    - EDR solutions are designed to support incident response and threat hunting. They offer integrated incident response capabilities within the same console, allowing security analysts to investigate and respond to security incidents quickly. EDR also provides threat hunting support, enabling B/Ds to proactively search for indicators of compromise and identify potential threats that may have evaded other security measures.

4. Automation and Remediation:

- Antivirus software often relies on manual intervention for incident response and remediation. Security analysts need to analyse and address detected threats manually.
- EDR solutions automate certain incident response activities and provide multiple response options, such as quarantine or eradication, to address security incidents. This automation streamlines the incident response process and reduces the impact and cost of security incidents.

EDR solutions go beyond traditional antivirus software by providing behaviour-based detection, enhanced visibility, incident response capabilities, and support for proactive threat hunting. They offer a more comprehensive and proactive approach to endpoint security, enabling B/Ds to detect, respond to, and mitigate a wide range of threats. By understanding these distinctions, B/Ds can avoid confusion and select EDR solutions that offer the necessary depth and breadth of protection.

D.2. EDR Deployment and Implementation

Deploying and implementing an Endpoint Detection and Response (EDR) solution is a multi-step process that involves careful planning, technical configuration, and integration within a B/D's security infrastructure. Here are the key considerations for EDR deployment and implementation:

1. ***Define Objectives and Requirements:*** Start by defining the objectives and requirements of deploying an EDR solution. Identify the security challenges and risks the B/D aims to address with EDR. Consider factors such as the number and types of endpoints to be protected, regulatory compliance requirements, and the desired level of visibility and threat detection capabilities. This information will guide the selection of an appropriate EDR solution.

2. ***Evaluate and Select an EDR Solution:*** Conduct a thorough evaluation of available EDR solutions. Consider factors such as the solution's features, scalability, integration capabilities, performance impact on endpoints, and vendor reputation. Evaluate the solution's ability to detect and respond to advanced threats using behavioural analytics, machine learning, and threat intelligence integration. Select an EDR solution that aligns with the B/D's objectives, requirements, and budget.

3. ***Plan for Deployment:*** Develop a detailed deployment plan that outlines the necessary steps, resources, and timelines. Consider aspects such as endpoint coverage, agent deployment, network considerations, integration with existing security tools, and user and stakeholder communication.

4. ***Infrastructure Readiness:*** Ensure that the B/D's infrastructure meets the requirements of the EDR solution. Verify that the necessary hardware, network resources, and storage capacity are available. Identify any potential compatibility issues with existing systems or software.

5. ***Installation and Configuration:*** Install the EDR solution on the designated servers or appliances according to the vendor's guidelines. Configure the solution's settings,

policies, and rules based on the B/D's security objectives and operational requirements. This includes defining what events and data should be collected from endpoints, setting up detection rules, and configuring response actions.

6. ***Endpoint Agent Deployment:*** Deploy the EDR agents on the endpoints that will be protected. This may involve automated deployment methods, such as software distribution tools or group policies, to ensure consistent and efficient installation across all endpoints. Validate that the agents are successfully installed and operational on each endpoint.

7. ***Integration with Security Infrastructure:*** Integrate the EDR solution with other security tools and systems within the B/D's environment. This may involve configuring data feeds, integrating with a Security Information and Event Management (SIEM) system, or connecting to threat intelligence platforms. Ensure the integration is properly established and data flows seamlessly between the EDR solution and other security components.

8. ***Tuning and Customisation:*** Fine-tune the EDR solution to align with the B/D's specific needs and environment. Adjust detection rules, policies, and response actions based on the B/D's risk tolerance, compliance requirements, and operational considerations. Customise alerts and notifications to ensure relevant security events are appropriately prioritised and communicated to security analysts.

9. ***Testing and Validation:*** Conduct thorough testing and validation of the EDR solution to ensure its effectiveness and accuracy. Simulate various attack scenarios and evaluate the solution's ability to detect and respond to these threats. Verify that the solution generates accurate alerts, captures the desired level of endpoint telemetry, and performs as expected.

10. ***Monitoring and Maintenance:*** Establish ongoing monitoring and maintenance processes to ensure the continued effectiveness of the EDR solution. Regularly review and analyse EDR alerts and events to identify security incidents and potential threats. Keep the solution current by applying vendor-provided updates, patches, and threat intelligence feeds. Perform routine maintenance tasks like database optimization, log rotation, and system health checks.

11. ***Staff Training and Awareness:*** Provide training to security operations teams on the features, capabilities, and best practices of the EDR solution. Ensure they are well-equipped to effectively use the solution for threat detection, investigation, and response. Additionally, raise end-user awareness about the EDR solution, its purpose, and any security procedure or policy changes.

D.2.1. Scope of EDR Coverage

To ensure comprehensive coverage and effective threat management, EDR solutions must extend their protective reach beyond traditional endpoints. The scope of coverage typically includes a wide range of endpoint devices across the B/D's network. These devices can include:

- ***Desktops and Laptops:*** EDR solutions commonly cover desktop computers and laptops running various operating systems, such as Windows, macOS, and Linux. These endpoints are typically used by employees within the B/D.
- ***Servers:*** EDR solutions often extend their coverage to include physical and virtual servers that are critical to the B/D's infrastructure. This includes file servers, application servers, database servers, and cloud-based servers.
- ***Mobile Devices:*** With the growing use of mobile devices in the workplace, EDR solutions may also provide coverage for smartphones and tablets. This can include devices running Android or iOS operating systems, ensuring that mobile endpoints are protected against security threats.
- ***Virtual Machines:*** B/Ds that heavily utilise virtualization technologies may require EDR solutions capable of monitoring and protecting virtual machines (VMs). These VMs can be hosted on hypervisors such as VMware, Hyper-V, or KVM.
- ***IoT Devices:*** As the Internet of Things (IoT) becomes more prevalent in B/Ds, EDR solutions may offer coverage for IoT devices connected to the network. This can include devices such as IP cameras, smart thermostats, industrial sensors, and other IoT endpoints.
- ***Embedded Systems:*** In certain B/Ds, there may be a need for EDR coverage on specialised embedded systems or devices, such as point-of-sale (POS) systems, ATMs, industrial control systems (ICS), or medical devices. These devices may have unique requirements and constraints that need to be addressed.
- ***Kiosks:*** In certain B/Ds, there may be a need for EDR coverage on specialised kiosk systems. These kiosks can be found in public spaces, retail environments, or other locations where self-service interactions occur. EDR solutions may offer coverage for kiosks to ensure that these endpoints are protected against security threats and vulnerabilities.

Building a resilient security posture requires consistent coverage across all endpoint types. B/Ds should note the importance of a unified approach to EDR implementation. By integrating desktops, workstations, servers, mobile devices, etc., into a centralised monitoring and response system, B/Ds can effectively detect, investigate, and respond to threats. Strategies for managing heterogeneous endpoint environments, including policy enforcement and agent management, should be detailed to ensure a cohesive defence strategy.

Annex E: Threat Monitoring Architecture Illustration

The below diagram provides an illustration of a comprehensive threat monitoring architecture, showcasing the interconnected monitoring tools that work together for IT security threat monitoring:

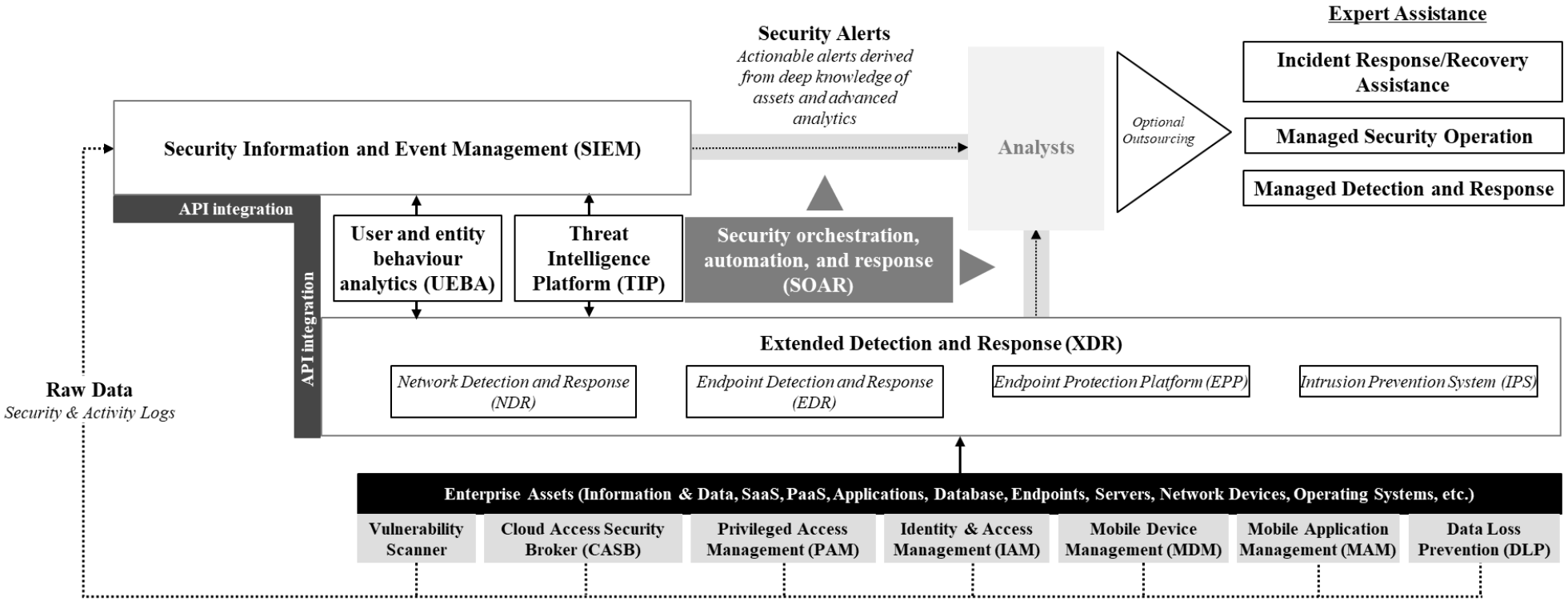

Figure E.1 Threat Monitoring Architecture Illustration