DATA-THEFT Incident Response Playbook

Redback Operations

Version	Modified By	Approver	Date	Changes made
0.1	Devika Sivakumar		13 April 2024	First draft
1.0	Devika Sivakumar	Joel Daniel	29 April 2024	Approved for publishing.
2.0	Devika Sivakumar		02 August 2024	Key changes made in Introduction, expanded descriptions of attack types, expanded description of stakeholders, RACI chart is added, added more detailed activities in incident response stage, included comprehensive definitions for key terms in terminology and added the steps for monitoring threats.

Contents

1. Introduction

An organization's reputation may be harmed, confidential data may be compromised, and financial losses may ensue from data theft occurrences. To minimise the effects of data theft events and protect organisational assets, this playbook offers methods and principles for doing so.

1.1 Overview

Identification, containment, mitigation, and recovery from data theft events may be done in an organised manner with the help of the Data Theft Incident Response Playbook. It does this by defining roles, responsibilities, and procedures that facilitate an effective reaction to reduce the negative effects on Redback Operations' operations, reputation, and stakeholders.

1.2 Purpose

This playbook's goals are to:

- Provide a standardised framework for handling instances of data theft.
- Make sure that data breaches are quickly discovered and contained.
- Reduce the negative impact that data theft has on operations, stakeholders, and reputation.
- Encourage coordination, cooperation, and dialogue amongst stakeholders and reaction teams.

1.3 Attack Definition

The act of gaining unauthorised access to, leaking, or disclosing private firm information—such as financial records, intellectual property, and personally identifiable information (PII)—is known as data theft. Numerous strategies, such as malware, social engineering, phishing, external attacks, and insider threats, might cause this.

1.4 Scope

This playbook includes all instances of data theft that impact the networks, systems, applications, and data assets of the organisation. It covers incidents that affect partners, consumers, staff members, and outside vendors, among other internal and external stakeholders. Both deliberate and unintentional instances of data theft are included in the scope.

2. Attack Types

The different types of Data-Theft attacks include:

2.1 Insider Threat

An insider threat is when someone who works for the company—a contractor, business partner, or employee, for example—misuses their access to steal information.

<u>Signs of Insider Threat:</u>

- Abnormal access patterns: Workers accessing private data after hours or on the weekends, in addition to their regular duties.
- Illegal data access: Workers gaining access to systems or files for which they are not normally authorised.
- Unauthorised information sharing: Workers disclosing private information to outside parties or persons they are not authorised to.
- Behavioural or performance changes: Workers displaying abrupt behavioural shifts, such heightened confidentiality or attempts to avoid discovery.
- Employee discontent or unhappiness: When staff members voice their unhappiness with their jobs or the company, it may spark aggressive behaviour.

2.2 External Attack

Data theft carried out by external parties, such as nation-state enemies, hackers, or cybercriminals, is referred to as an external attack.

<u>Signs of External Attack:</u>

- Illegal entry attempts: Brute force attacks or suspicious login attempts directed at the networks or systems of the company.
- Unusual patterns of network traffic: Distinctive communication patterns or massive amounts of data being moved to other sites are examples of anomalies in network traffic.
- Malicious software or malware presence: Finding malware problems, including ransomware, trojans, or keyloggers, on the company's networks or systems.
- Phishing attempts: Getting shady emails or communications that try to fool staff members into disclosing private information or installing malicious software.
- Exploitation of applications or system vulnerabilities: Identification of attempted or accomplished exploitation of known weaknesses in the infrastructure of the company, such as improperly configured systems or unpatched software.

2.3 Data Breaches

Data breaches happen when unapproved parties obtain entry to confidential data that is kept on file by a company.

Signs of Data Breaches:

- Unexpected modifications to a user's rights or access authorisation.
- Unauthorised access attempts indicated by anomalies in system logs.
- Abnormal network activity patterns, such massive data transfers to other addresses.
- Conditions in user behaviour, including accessing private information after hours.

2.4 Phishing Attacks

Phishing attacks include sending people false emails or messages with the intention of fooling them into disclosing private information, including login passwords or bank account information.

Signs of Phishing Attacks:

- Getting faked or unknown sender emails that raise red flags.
- Email or message requests for private information, including account numbers or passwords.
- Links in emails that take recipients to phoney websites intended to steal login information.
- Sent with bad grammar or poor writing quality.

2.5 Ransomware Attacks

Ransomware attacks entail the introduction of software into a victim's computer or network, encrypting files and requesting payment for the key to unlock them.

Signs of Ransomware Attacks:

- Unable to access folders or files because they are encrypted.
- The appearance of messages requesting money in order to unlock the ransom.
- Abnormal network behaviour as the malware propagates.
- The existence of files or processes connected to ransomware on compromised computers.

2.6 Credential Theft

Theft of login credentials, which include usernames and passwords, from people or organisations is known as credential theft. The goal is to obtain unauthorised access to accounts or systems.

Signs of Credential Theft:

- Notifications of illegal access to systems or user accounts.
- Unusual locations or a pattern of unsuccessful login attempts are examples of anomalies in login behaviour.
- Malware that is intended to intercept keystrokes or steal passwords that have been stored.
- Using credentials that have been stolen to gain access to private data or carry out unauthorised activities.

3. Stakeholders

3.1 IT Security Team
Lead: Daniel McAulay (Senior Project Leader)
The IT security team oversees overseeing and maintaining the company's security infrastructure, keeping an eye out for any security risks, and handling instances of data theft.

Roles and Responsibilities:

- Examine and evaluate security events to ascertain the extent of identity theft.
- Put controls and security measures in place to stop more illegal access.
- Work together with the incident response team to handle and lessen the effects of occurrences involving data theft.
- To find the source of security breaches and stop such situations in the future, do forensic analysis.
- Advise appropriate stakeholders and senior management on security enhancements and incident response protocols.

3.2 Incident Response Team
Lead: Devika Sivakumar (Blue Team Leader)
The incident response team oversees overseeing the incident response procedure and organising the organization's reaction to occurrences involving data theft.

Roles and Responsibilities:

- Determine the scope and consequences of data theft occurrences, then take the necessary corrective action.
- Organise staff and resources to control and lessen the effects of instances involving data theft.
- Gather information for a possible legal action by conducting forensic investigations to ascertain the source and extent of data theft.
- Inform all relevant parties about incident reaction and recovery efforts, including customers, third-party vendors, senior management, and the IT security team.
- To improve the organization's incident response skills, capture best practices and lessons gained from data theft events in documentation.
- To find the source of security breaches and stop such situations in the future, do forensic analysis.
- Advise appropriate stakeholders and senior management on security enhancements and incident response protocols.

3.3 Communication Team
Lead: Kaleb Bowen (Company Lead)

The communication team oversees overseeing both internal and outside communications about cases of data theft and making sure that messages are clear and consistent.

Roles and Responsibilities:

- Create and implement communication plans to notify relevant parties—such as staff members, clients, and outside suppliers—about instances of data theft.
- To respond to questions and concerns from stakeholders, create and disseminate communication pieces including news releases, statements, and FAQs.
- Oversee media and public relations initiatives to safeguard the company's image and lessen the damaging effects of data theft occurrences.
- Give the incident response team and senior leadership regular reports on the state of stakeholder engagement and communication initiatives.

3.4 Customers

Customers are people or organisations that may be impacted by instances of data theft and have a stake in the goods or services offered by the company.

Roles and Responsibilities:

- Report any unauthorised or questionable behaviour pertaining to their transactions or accounts.
- Contribute to the data theft incident investigation by giving the incident response team pertinent data or supporting documentation.
- Observe the advice and guidelines provided by the organisation to safeguard personal information and lessen the effects of data theft events.

3.5 Third-Party Vendors

Third-party vendors are outside companies that supply the company with goods, services, or support; they may also have access to its networks, systems, or data.

Roles and Responsibilities:

- Work together with the incident response team to find and fix security flaws in their services or products.
- When managing and investigating data theft situations that affect the organization's networks or systems, offer support and help.
- Respect the terms of the contract and any legal requirements pertaining to data security and privacy. This includes reporting security breaches and helping with incident response.

RACI Chart:

- **R:** Responsible (who does the work)
- **A:** Accountable (ultimate ownership)
- **C:** Consulted (provides input)
- **I:** Informed (kept up to date)

Key Definitions:

- **Responsible (R):** The individual(s) who perform the work to achieve the task.
- **Accountable (A):** The individual who is ultimately answerable for the correct and thorough completion of the task.
- **Consulted (C):** The individual(s) whose opinions are sought.
- **Informed (I):** The individual(s) who are kept up-to-date on progress and outcomes.

RACI Chart

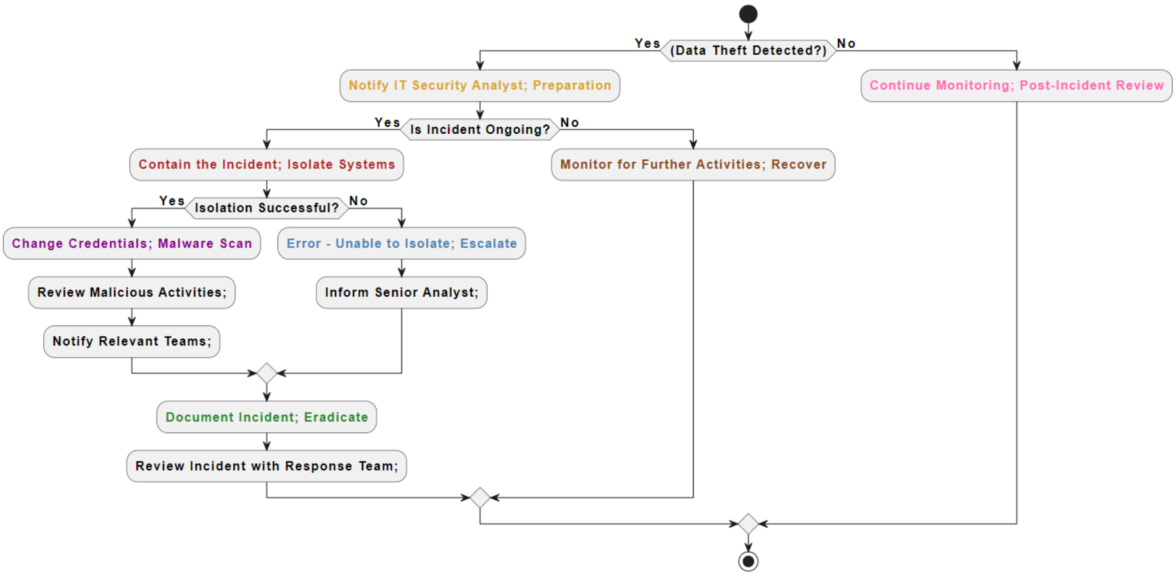
Task/Activity	**IT Security Team**	**Incident Response Team**	**Communication Team**	**Senior Management**	**Legal and Compliance**	**Customers**	**Third-Party Vendors**
Preparation	R, C	A, R	I	I	C	I	I
Establishing incident response team	A	R	I	I	C	I	I
Developing data theft response procedures	A, R	R, C	I	C	C	I	I

Conducting training and practice sessions	A, R	R	I	I	I	I	I
Implementing data protection systems	A, R	R	I	I	I	I	I
Detection	A, R	R	I	I	I	I	I
Monitoring system logs and network traffic	R	A, R	I	I	I	I	I
Using IDS and SIEM tools	A, R	R	I	I	I	I	I
Analyzing alerts	A, R	R	I	I	I	I	I
Analysis	A, R	R	I	I	I	I	I
Collecting data for forensic analysis	A, R	R	I	I	I	I	I
Identifying attack methods	A, R	R	I	I	I	I	I
Determining impact	A, R	R	I	I	I	I	I
Containment	A, R	R	I	I	I	I	I

Isolating compromised systems	A, R	R	I	I	I	I	I
Implementing safeguards	A, R	R	I	I	I	I	I
Blocking unauthorized access	A, R	R	I	I	I	I	I
Eradication	A, R	R	I	I	I	I	I
Removing compromised data	A, R	R	I	I	I	I	I
Patching vulnerabilities	A, R	R	I	I	I	I	I
Updating security policies	A, R	R	I	I	I	I	I
Recovery	A, R	R	I	I	I	I	I
Restoring backups	A, R	R	I	I	I	I	I
Rebuilding systems	A, R	R	I	I	I	I	I
Conducting user awareness training	A, R	R	I	I	I	I	I

Post-Incident Review	A, R	R	I	I	I	I	I
Reviewing incident response process	A, R	R	I	I	I	I	I
Documenting best practices	A, R	R	I	I	I	I	I
Updating response procedures	A, R	R	I	I	I	I	I
Communication Plan	C	C	A, R	I	C	I	I
Creating communication plans	C	C	A, R	I	C	I	I
Drafting communication materials	C	C	A, R	I	C	I	I
Managing media relations	C	C	A, R	I	C	I	I
Providing updates	C	C	A, R	I	C	I	I

4. Flow Diagram


Yes
(Data Theft Detected?)
No
Notify IT Security Analyst; Preparation
Continue Monitoring; Post-Incident Review
Yes
Is Incident Ongoing?
No
Contain the Incident; Isolate Systems
Monitor for Further Activities; Recover
Yes
Isolation Successful?
No
Change Credentials; Malware Scan
Error - Unable to Isolate; Escalate
Review Malicious Activities;
Inform Senior Analyst;
Notify Relevant Teams;
Document Incident; Eradicate
Review Incident with Response Team;

1. Preparation (Prep): Yellow

   - Notify IT Security Analyst and Threat Intelligence Team: The IT security analyst is instantly contacted to begin incident response preparations upon detection of data theft.

2. Identification (Identify): Red

   - Contain the Incident; Isolate Systems: Containment procedures, such as isolating impacted systems to prevent additional unauthorised access, are put in place if the issue is continuing.

3. Notification (Notif): Violet

   - Change Credentials; Malware Scan: Changing passwords and running malware scans are two urgent steps that should be taken after a successful isolation to lessen the effect of the occurrence.
   - Review Malicious Activities; Notify Relevant Teams: Malicious activity is found through additional analysis, and teams who need to respond are alerted so that they may plan accordingly.

4. Containment (Contain): Sky Blue
   - Error - Unable to Isolate; Escalate: Senior analysts are notified to resolve the issue and the incident is escalated if the impacted systems cannot be isolated.
5. Eradication (Erad): Light Green
   - Document Incident; Eradicate: To eliminate any last hazards and return to regular operations, the occurrence is recorded, and eradication procedures are put in place.
6. Recovery (Recover): Brown
   - Monitor for Further Activities; Recover: To guarantee the organization's resilience, recovery actions are started and ongoing monitoring for additional activities is carried out.
7. Post-Incident Actions (Post): Light pink
   - Continue Monitoring; Post-Incident Review: Continuous observation persists, and a post-event assessment is carried out to appraise the efficacy of the reaction and pinpoint opportunities for enhancement.

5. Incident Response Stages

5.1 Preparation

- **Objective:** Establishing the rules, processes, and resources required to properly handle cases of data theft is the main goal of the preparation phase.
- **Activities:**
  - Forming an incident response group with clearly defined duties.
  - Creating processes and strategies for incident response that include escalation routes and communication protocols.
  - Regularly providing incident responders with training and drills to guarantee preparedness.
  - Putting security measures and monitoring systems in place to identify and stop instances of data theft.
- **Outcome:** A well-equipped company capable of reacting to instances of data theft swiftly and efficiently.

5.2 Detection

- **Objective:** Finding signs of illegal access or data theft within the organization's networks and systems is the task of the detection stage.
- **Activities:**
  - Keeping an eye out for suspicious activities, such as strange access patterns or unauthorised file transfers, by monitoring system logs and network traffic.
  - Putting in place security information and event management (SIEM) and intrusion detection system (IDS) solutions to find any attacks.
  - Examining abnormalities and alarms to differentiate between harmful and legitimate activity.
- **Outcome:** Early data theft event identification allows for quick response and mitigation actions.

5.3 Analysis

- **Objective:** The investigation and comprehension of the type and extent of the data theft occurrence are the main objectives of the analysis stage.
- **Activities:**
  - Gathering information and determining the origin and scope of the data theft through forensic analysis.
  - Examining hacked networks and systems to ascertain the attack strategies and the effects on compromised data.
  - Recognising threat actors' tactics, methods, and procedures (TTPs) and indications of compromise (IOCs).

- **Outcome:** A thorough comprehension of the data theft occurrence, including the reasons, consequences, and attribution of the theft.

5.4 Containment

- **Objective:** To stop more unauthorised access or data exfiltration, the containment step entails reducing the incident's effect and spread.
- **Activities:**
  - Isolate hacked systems to stop attackers from moving widely.
  - Put access restrictions in place to prevent unwanted access to private information.
  - To stop more harm, quarantine or block rogue programmes, data, or network traffic.
- **Outcome:** Successful management of the data theft event, reducing the damage it caused to the systems and data of the company.

5.5 Eradication

- **Objective:** The goal of the eradication step is to eradicate any remaining risks or vulnerabilities as well as the attackers' presence from the company's IT infrastructure and networks.
- **Activities:**
  - Deleting harmful software and data from hacked computers and returning them to a safe condition.
  - Upgrading or patching susceptible systems and software to stop further exploitation.
  - Review and update security policies and practices to address any identified weaknesses or vulnerabilities.
- **Outcome:** Eradicating all evidence of the data theft event and reducing vulnerabilities to stop such ones in the future.

5.6 Recovery

- **Objective:** Restoring impacted systems and information to regular functioning and carrying on business as usual are the objectives of the recovery stage.
- **Activities:**
  - Restoring systems and data backups that were hacked to guarantee data availability and integrity.
  - Rebuild or reconfigure systems to enhance security and prevent similar incidents.
  - Conduct user education and awareness campaigns to prevent future data theft incidents.

- **Outcome:** Full restoration of operations and services with enhanced security measures to reduce the risk of future incidents.

5.7 Post- Incident Review

- **Objective:** Evaluate the organization’s response to the data theft incident and identify areas for improvement.
- **Activities:**
  - Conduct a thorough review of the incident response process, identifying strengths, weaknesses, and areas for improvement.
  - To improve incident response skills in the future, record best practices and lessons learned.
  - Revise security protocols, policies, and incident response plans in light of the review's conclusions.
- **Outcome:** Constant enhancement of incident response capacities and preparedness for upcoming data theft events.

6. Steps for Monitoring Threats

6.1 Establish a Monitoring Strategy

Objective: Establish and put into action a thorough plan for ongoing threat surveillance.

Activities:

- **Objectives:** Clearly state your objectives for using threat monitoring, such as finding malware, detecting unauthorised access, or keeping an eye out for unusual network traffic.
- **Tools:** Select the technology and security tools that will best support your monitoring goals. IDS/IPS (Intrusion Detection/Prevention Systems), SIEM (Security Information and Event Management) systems, and EDR (Endpoint Detection and Response) solutions are examples of common technologies.
- **Baselines:** Set baselines of usual activity for user activity, system behaviour, and network traffic. This makes it easier to spot variations that could point to possible dangers.
- **Outcome:** A clear monitoring plan that improves threat detection skills and is in line with company's objectives.

6.2 Deploy Monitoring Solutions

Objective: Install and set up the chosen monitoring tools throughout the infrastructure of the company.

Activities:

- **Install and Configure Tools:** Deploy the selected monitoring tools across your network, systems, and endpoints. Ensure they are properly configured to collect and analyze relevant data.
- **Integrate with Threat Intelligence:** To improve your monitoring systems' capacity to identify existing attacks and newly discovered vulnerabilities, integrate them with threat intelligence streams.
- **Enable Logging:** Make sure that the logging feature is enabled on all important networks, applications, and systems. Log collecting should be centralised for effective analysis and correlation.
- **Outcome:** Efficient implementation and assimilation of surveillance systems offering all-encompassing insight into any hazards.

6.3 Continuous Monitoring and Analysis

Objective: Maintain constant data monitoring and analysis to quickly identify any security risks.

Activities:

- **Real-Time Monitoring:** Use real-time monitoring to keep an eye on user activity, system behaviour, and network traffic all the time. This makes it easier to spot questionable activity as it happens.
- **Anomaly Detection:** Utilise behavioural analytics and machine learning to find anomalies that depart from predetermined baselines. This may aid in locating hazards that were previously unidentified.
- **Correlate Events:** Connect occurrences from many sources to find trends that could point to a well-planned assault or ongoing danger.
- **Outcome:** Improved capacity to identify hazards and take immediate action to prevent any harm.

6.4 Deploy Monitoring Solutions

Objective: By using a reliable alerting system, you can make sure that risks are addressed quickly and effectively.

Activities:

- **Set Alert Thresholds:** Set thresholds according to the seriousness and possible consequences of the identified danger for various kinds of alerts.
- **Automated Alerts:** Set up automated notifications to inform the security staff to any dangers. Make sure warnings have enough context to allow for prompt evaluation and action.
- **Prioritize Alerts:** Put in place a system that ranks warnings according to their importance and possible consequences. This makes it easier to concentrate on the biggest risks first.
- **Outcome:** Prompt and efficient handling of any hazards, lowering the possibility of serious harm.

6.5 Investigate and Respond

Objective: Undertake comprehensive enquiries and implement suitable measures to alleviate identified hazards.

Activities:

- **Initial Triage:** Sort the alerts initially to ascertain their veracity and possible significance. This entails determining the threat's seriousness and determining if the warning is a false positive.
- **Detailed Analysis:** Analyse genuine warnings in-depth to determine the kind and extent of the danger. To obtain information and track out the source of the danger, employ forensic instruments and methods.
- **Containment and Eradication:** Initiate containment actions to stop more harm if a threat is verified. To eliminate the hazard from the environment, carry out the necessary eradication operations.

- **Outcome:** Efficient examination and reduction of hazards, guaranteeing little influence on the establishment.

6.6 Post-Incident Review

Objective: Analyse the response's efficacy and pinpoint areas that need improvement.

Activities:

- **Document Findings:** Keep a record of all the incident's information, including how it was discovered, what analysis was done, and what steps were made to address it.
- **Review and Improve:** Review your monitoring and response procedures after the occurrence to find areas that need improvement and lessons learned.
- **Update Monitoring Tools:** Update your monitoring tools, setups, and thresholds considering the results to enhance threat detection and response in the future.
- **Outcome:** Constant enhancement of incident response and threat monitoring systems.

6.7 Continuous Improvement

Objective: Preserve and improve the tools and approach used by the organisation for threat monitoring.

Activities:

- **Regular Audits:** Make sure your tools and monitoring approach are up to date with the latest risks and operating as intended by conducting routine audits.
- **Training and Awareness:** To keep your security personnel informed about the newest dangers and best methods for monitoring and responding, provide them regular training.
- **Adapt to New Threats:** Make constant adjustments to your monitoring plan to handle emerging dangers. Keep up with the most recent threat intelligence and incorporate it into your processes for monitoring.
- **Outcome:** A proactive, flexible approach to threat monitoring that adjusts to the changing environment.

7. Terminology

- Data Theft: The illicit procurement, duplication, or elimination of private or sensitive information from a company's networks or systems.
- Insider Threat: A security risk brought on by employees of a company who may, whether on deliberately or accidentally, abuse or divulge sensitive information for nefarious or personal benefit.
- External Attack: An attempt to steal confidential information through a cyberattack carried out by people or organisations not connected to its internal network, such as hackers, cybercriminals, or nation-state enemies.
- Incident Response: A methodical strategy for dealing with and handling security events, such as data theft incidents, with the objectives of minimising harm, restarting operations, and averting such occurrences.
- Indicators of Compromise (IOCs): Observable indicators, such as strange network traffic patterns, unauthorised access attempts, or questionable file alterations, that point to the existence of malicious activity or a security breach.
- Security Controls: Procedures put in place to guard against security risks, such as instances of data theft, and to safeguard networks, systems, and data. Intrusion detection systems (IDS), encryption, access restrictions, and security awareness training are a few examples of security controls.
- Forensic Analysis: The methodical inspection of digital evidence connected to a security event, such data theft, to collect and examine data for legal or investigative needs, including figuring out the incident's cause and consequences.
- Vulnerability: Vulnerabilities or weaknesses in networks, apps, or systems that an attacker may use to get unauthorised access, steal information, or interfere with normal operations. Inadequate security measures, incorrect setups, and software defects can all lead to vulnerabilities.
- Threat Intelligence: Organisations can predict, detect, and respond to cybersecurity risks with the use of information on current and upcoming threats gathered from a variety of sources.
- Security Information and Event Management (SIEM): A system that analyses security alarms produced by network hardware and applications in real time. SIEM systems compile and examine activities from many IT infrastructure resources.
- Intrusion Detection System (IDS): A hardware or software programme that monitors a network or systems for malicious activity or policy breaches.

- Endpoint Detection and Response (EDR**):** A security solution that provides real-time monitoring and detection of endpoint threats, enabling rapid response to security incidents.
- Triage: The process of prioritizing incidents and alerts based on their severity and impact, ensuring that the most critical threats are addressed first.
- Baseline: A set of data points or metrics that represent normal behavior, used as a reference to identify deviations that could indicate potential security threats.