BHARATHIDASAN UNIVERSITY

Tiruchirappalli- 620024

Tamil Nadu, India.

Programme: M.Sc. Statistics

Course Title: Introduction to Big Data Analytics

Course Code: 23ST02VAC

Unit-IV

SECURITY ANALYTICS

Dr. T. Jai Sankar
Associate Professor and Head
Department of Statistics

Ms. S. Soundarya
Guest Faculty
Department of Statistics

Unit-IV

Introduction to Security Analytics

Security analytics is a cyber security approach that involves the collection, aggregation, and analysis of data to augment an organization's ability to detect, analyze, manage, and mitigate threats. It is a proactive means of making sense of high volumes of security data flowing in and out of the organization. Security analytics solutions are usually deployed in organizations to provide rapid threat-hunting capabilities, accelerate incident response, and prevent potentially costly data breaches. They are also used to conduct real-time risk assessments and to enhance an organization's overall cyber security posture.

Important of Security Analytics

Security analytics is important for organizations because it makes it easier to collect large volumes of security data, process, and transform it. In today's competitive landscape, it is crucial to analyze diverse datasets from multiple sources and identify correlations and anomalies in data. Security analysis allows experts to conduct root cause investigations and pinpoint various attack patterns. It enables them to generate comprehensive reports and save their findings for future use. Attackers are always on the constant lookout to locate vulnerabilities and exploit them. Security analytics helps disrupt their movement by prioritizing risks and keeping pace with their growing efforts.

Uses Security Analytics

Almost every modern organization with a digital architecture or presence uses security analytics. Security Operations Centers (SOCs) consist of teams that have analysts, engineers, and other frontline members who use security analytics. CISOs in companies use security analytics solutions to make sure that sensitive data gets adequate protection. Security analytics is needed by companies because it allows them to detect threats before they escalate, become major issues, and cause data breaches. It is a preventive measure that adds an extra layer of protection, thus ensuring robust cyber security. Below are the distinct differences between security analytics vs SIEM:

Security Analytics	SIEM
Designed for modern business architectures, dynamic, microservices, and DevOps-friendly; is elastic, multi-tenant, and secure	Designed for monolithic business applications, static, and has long development and release cycles
For cloud-based infrastructure;	For on-premises infrastructure
Solutions can be deployed instantly and in near real-time	Takes 15 months on average to deploy
Uses continuous monitoring methodologies and behavioral-based modeling to protect against unknown and hidden threats. Identifies abstract threat patterns, anomalies, trends, and fraudulent activities in networks.	Delivers perimeter-based security by analyzing attack signatures; has fixed rule sets when it comes to threat detection
Holistic and enterprise-wide visibility with APIs, integrations, and cloud-native services	Limited visibility with port mirroring and security islands

Security Analytics Components

There are various components to security analytics and they are as follows:

- Threat detection and incident response
- Compliance management
- Reports and dashboards
- Correlations and security events monitoring
- Identity and access management
- Anomaly detection
- Endpoint data security
- Data collection and user behavior analytics
- Cloud security and threat intelligence
- Enhanced incident investigation
- Cyber forensic analysis

Benefits of Security Analytics

- One of the biggest benefits of security analytics is how it can analyze high volumes of security data coming from different sources. It flawlessly connects the dots between security events and alerts. Security analytics enables proactive threat discovery, response, and incident risk management.
- Good security analytics will limit the scope for data breaches by identifying and reducing attack surfaces. It will analyze threats from the attacker's perspective and give users insights into where the next attack is targeting them. Businesses will be able to predict the frequency of attacks and better prepare for them.
- Security analytics can analyze a broad range of data such as endpoint and user behavior data, network traffic, cloud traffic, business applications, non-IT contextual data, external threat intelligence sources, third-party security data, and identity and access management information. It even provides proof of compliance during an audit and discovers hidden issues that may lead to policy violations, allowing organizations to effectively address them.

Key Challenges of Security Analytics

Some of the key challenges faced in security analytics are:

- **Shortage of Skilled Security Professionals**: Although security analytics technologies are evolving, there is a shortage of skilled security professionals who can use them. In today's digital threat landscape, the role of a threat hunter has become indispensable. A lack of skilled data scientists in the network security industry is a big problem.
- **Extrapolating Actionable Intelligence:** Sometimes security analytics solutions don't give the best security recommendations. Many services fall short and fail to deliver actionable insights via reporting. Simply handling and categorizing big data isn't enough.

Many businesses are overwhelmed with the high volumes of data and need to analyze it in ways that benefit their business revenue growth and performance. Without reliable security analytics solutions, organizations will stay open to malicious threats. Security analytics platforms need to be managed properly so that companies know where to invest additional cyber security efforts or scale their resources accordingly.

Intrusion detection system

An IDS is a type of software or application that monitors a network to detect suspicious activity and generate immediate alerts if and when it is detected. These alerts are recorded centrally via a security information and event management (SIEM) system or reported to an administrator. They provide key insights to enable incident response specialists or security operations centre (SOC) analysts to investigate issues and take appropriate action. An IDS can monitor for internal as well as external threats, in the form of a network intrusion detection system (NID). NIDS are commonly used in conjunction with host-based intrusion detection systems (HIDS) and SIEM solutions, which aggregate and analyse security events from multiple sources.

Intrusion detection changes

The emergence of more sophisticated security solutions means that the market is moving away from the use of IDS. Approaches to network security have evolved to become more holistic, drawing in information from multiple sources and providing a broader overview.

One notable change was the use of this type of technology in conjunction with SIEM, as mentioned, which provides a more comprehensive overview to utilise information from IDS, intrusion prevention systems (IPS), logs, and firewalls in order to build a more comprehensive picture of network security to advance measures beyond simply screening hostile traffic.

However, SIEMs only analyse and categorise log data from different IT systems to search for security issues and alert engineers, meaning the investigation itself must be undertaken manually. In contrast, SOAR (Security Orchestration, Automation and Response) security technologies allow organisations to collect and aggregate vast amounts of security data and alerts from a multitude of sources, enabling businesses to significantly improve their ability to swiftly detect and respond to attacks.

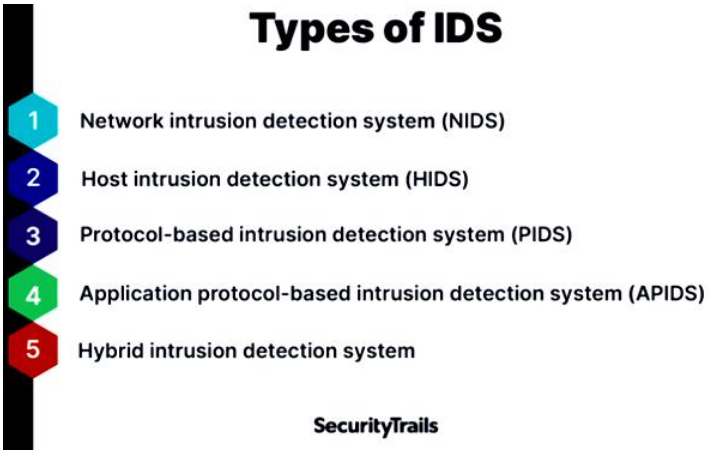
Changes in threat actor behaviour meant that breaches increasingly posed a threat at endpoint level, with traditional endpoint solutions limited in their ability to detect or address known file-based, or signature-based endpoint threats. This gave rise to endpoint detection and response (EDR) which is able to identify and contain potential threats at network perimeter level, as well as enabling security teams to uncover and mitigate emerging threats.
SOAR gathers alert data from a range of platforms, including SIEM, as well as EDR, extended detection and response (XDR), and threat intelligence platforms (TIP), enabling automated and adaptive incident response workflows. Although this evolution has made intrusion detection a much more sophisticated and effective element of cyber security, a number of issues continue to impact organisations.

The challenges of intrusion detection

- **Ensuring an effective deployment:** To attain a high level of threat visibility, organisations must ensure that their choice of intrusion detection solution is correctly installed and optimised. Budgetary and monitoring constraints mean that it may not be practical to integrate certain types of intrusion detection technology throughout an IT environment. With many organisations lacking a complete overview of their IT network however, deploying these types of solutions effectively can be tricky and if not done well may leave critical assets exposed.
- **Managing the high volume of alerts:** The vast quantity of alerts generated by intrusion detection solutions can be a significant burden for internal teams. Many system alerts are false positives but organisations rarely have the time and resources to screen every alert, meaning that suspicious activity can often slip under the radar.
  Most intrusion detection systems come loaded with a set of pre-defined alert signatures but for most organisations these are insufficient, with additional work needed to baseline behaviours specific to each environment.
- **Understanding and investigating alerts:** Investigating alerts detected by intrusion detection systems can be very time– and resource-intensive, requiring supplementary information from other systems to help determine whether an alarm is serious. Specialist skills are essential to interpret system outputs and many organisations lack the support of dedicated security experts capable of performing this crucial function.
- **Knowing how to respond to threats:** A common problem for organisations attempting to implement intrusion detection systems is that they lack an appropriate incident response capability. Identifying a problem is half the battle, while knowing how to respond appropriately and having the resources in place to do so is equally important.
  Effective incident response requires skilled security personnel with the knowledge of how to swiftly remediate threats, as well as robust procedures to address issues without impacting day-to-day operations. In many organisations there is a big disconnect between the people charged with monitoring alerts and those managing infrastructure, meaning that swift remediation can be difficult to achieve.
  To highlight the importance of having an appropriate incident response plan in place, the General Data Protection Regulation (GDPR) requires organisations that process any type of personal data to have appropriate controls in place to report breaches to a relevant authority within 72 hours, or risk a large fine.

Types of intrusion detection systems

Intrusion detection systems come in different variations and can detect suspicious activity using different methods and capabilities. Usually, the different flavors of IDSs can be classified by five types:



- **Network intrusion detection system (NIDS):** A network intrusion detection system (NIDS) is set up across the network, on tactical points, where it monitors inbound and outbound traffic to and from all devices on a network. It examines traffic and matches it with indicators of known attacks. When anomalous activity is detected, an alert is generated for the incident to be examined further.
- **Host intrusion detection system (HIDS):** A host intrusion detection system (HIDS) runs on all of a network's hosts and devices that have access to the internet as well as the internal network. It monitors the operations of individual hosts and tracks the status of all files on an endpoint and detects any activity, such as deletion or modification of system files. An HIDS also scans all data packets that are sent to or from an endpoint, meaning it can detect suspicious activity that originates inside an organization, an important capability to aid in the prevention of insider threats.
- **Protocol-based intrusion detection system (PIDS):** A protocol-based intrusion detection system (PIDS) is typically deployed on a web server and is used to monitor and analyze communication between devices on a network and online resources, as it scans data transmitted over HTTP/HTTPS.
- **Application protocol-based intrusion detection system (APIDS):** An application protocol-based intrusion detection system (APIDS) monitors the communication between users and applications. It monitors the packets transmitted over application-specific protocols and identifies instructions, tracing it to individual users.
- **Hybrid intrusion detection system:** A hybrid intrusion detection system is defined exactly as its name implies: It's a combination of two or more types of IDSs. In the hybrid type, the capabilities of two systems—host- and network-based IDSs for example—are combined, rendering it more effective than any single type of IDS.

Intrusion detection systems are also categorized as active or passive:

- An active IDS is also known as an intrusion detection and prevention system (IDPS). Not only is it configured to monitor traffic and detect anomalous behavior, it is also automated to block any suspected attacks with blocking IPs or by restricting access to sensitive resources without any need for admin involvement.
- A passive IDS only monitors and analyzes network traffic and alerts an admin to a potential attack. It doesn't have the ability to perform any blocking or preventative activity on its own.

Malware Analysis

Malware analysis is the study of the unique features, objectives, sources, and potential effects of harmful software and code, such as spyware, viruses, malvertising, and ransomware. It analyzes malware code to understand how it varies from other kinds.

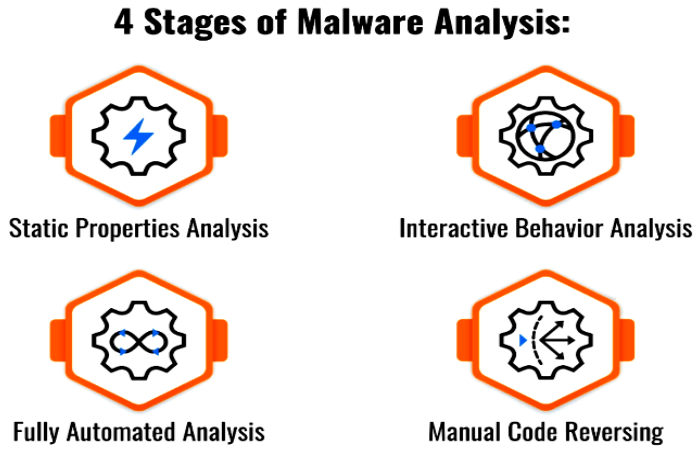
Benefits Of Malware Analysis

Malware analysis provides several significant benefits. For example, it enables organizations to perform the following malware analysis steps:

- Figure out how much damage an intrusion caused
- Identify who may have installed malware inside the system
- Determine the attack's level of sophistication
- Pinpoint the exact vulnerability the malware exploited to access your system

Stages of Malware Analysis

You can break down the malware analysis process into four stages:



- **Static properties analysis:** Static properties refer to strings of code embedded inside the malware file, hashes, header details, and metadata. Static properties analysis provides a quick and easy way to gather helpful information about malware because the malware does not have to be executed for you to study it.
- **Interactive behavior analysis:** Interactive behavior analysis involves a security analyst interacting with malware running in a lab, making observations regarding its behavior. In this way, you can better understand how malware uses different elements of a computer system, such as its memory.
- **Fully automated analysis:** Fully automated analysis scans suspected malware files using automated tools, focusing on what the malware can do once inside your system. After the analysis, you get a report outlining the potential damage to assets connected to your network.
- **Manual code reversing:** Manual code reversing breaks down the code used to build the malware to learn how it works and what it is capable of doing. This is a time-consuming process that requires significant skill. However, when used correctly, manual code reversing can reveal valuable information about the malware.

Types of Malware Analysis

There are several types of malware analysis. You can use one or a combination before or after an attack, depending on the situation your organization faces.

- **Static malware analysis:** Static malware analysis looks for files that may harm your system without actively running the malware code, making it a safe tool for exposing malicious libraries or packaged files. Static malware analysis can uncover clues regarding the nature of the malware, such as filenames, hashes, IP addresses, domains, and file header data. The malware can be observed using a variety of tools, such as network analyzers.
- **Dynamic malware analysis:** Dynamic malware analysis uses a sandbox, which is a secure, isolated, virtual environment where you can run suspected dangerous code. Security professionals can closely monitor the malware in the sandbox without worrying about infecting the rest of the system or network, allowing them to gather more information about the malware.
- **Hybrid malware analysis:** Hybrid malware analysis combines both static and dynamic techniques. For example, if malicious code makes changes to a computer's memory, dynamic analysis can detect that activity. Then, static analysis can determine exactly what changes were made.

Tools For Malware Analysis

Several malware analysis tools are available on the market, and here are some of the most well-known:

- **Process hacker:** Process Hacker enables analysts to understand the processes that are running on any given device on the network. This can be very useful as you allow malware to execute because you can watch the processes it impacts. With this information, you can determine how different computers react when malware is introduced to your system.
- **Fiddler:** Fiddler can observe and study malicious traffic because it serves as a proxy, accepting and managing network traffic. Running Fiddler enables malware analysts to study the code and locate the hardcoded malicious sites that will be used to download the malware.
- **Limon:** Limon is a controlled sandbox environment for studying malware that attacks Linux systems, enabling IT teams to monitor how the malware behaves and determine what it was designed to do.
- **PeStudio:** PeStudio identifies potentially suspicious files by analyzing what is happening on your system. After it identifies malicious files, it quarantines them and assigns each a hash. You can then use each hash to access the malware and run it in a safe environment to learn how it behaves.
- **Ghidra:** Ghidra disassembles malware instead of merely identifying it. It then takes whatever it finds in the malware code and translates it into something a human can read. In this way, it shows you what the malware designer might have been thinking while writing the malicious code.

- **Cuckoo sandbox:** Cuckoo Sandbox studies malware in a safe sandbox environment, recording its activity and then generating a report. This provides IT teams with data outlining how the malware attempts to impact your system.
- **CrowdStrike Falcon insight:** CrowdStrike Falcon automatically analyzes malware by combining CrowdStrike's threat intelligence with a sandbox environment. By comparing the malware's behavior in the sandbox to information from CrowdStrike's threat intelligence, Falcon Insight can determine whether the malware already exists or is new to the threat landscape.

Static Testing

Static Testing also known as Verification testing or Non-execution testing is a type of Software Testing method that is performed to check the defects in software without actually executing the code of the software application.

- Static testing is performed in the early stage of development to avoid errors as it is easier to find sources of failures and it can be fixed easily.
- Static testing is performed in the white box testing phase of the software development where the programmer checks every line of the code before handing it over to the Test Engineer.
- The errors that can't not be found using Dynamic Testing, can be easily found by Static Testing.
- It involves assessing the program code and documentation.
- It involves manual and automatic assessment of the software documents.

Documents that are assessed in Static Testing are:

- Test Cases
- Test Scripts.
- Requirement Specification.
- Test Plans.
- Design Document.
- Source Code.

Static Testing Techniques

Below are some of the static testing techniques:

- **Informal Reviews:** In informal review, all the documents are presented to every team member, they just review the document and give informal comments on the documents. No specific process is followed in this technique to find the errors in the document. It leads to detecting defects in the early stages.
- **Walkthroughs:** Skilled people or the author of the product explains the product to the team and the scribe makes note of the review of comments.
- **Technical Reviews:** Technical specifications of the software product are reviewed by the team of your peers to check whether the specifications are correct for the project. They try to find discrepancies in the specifications and standards. Technical specifications documents like Test Plan, Test Strategy, and requirements specification documents are considered in technical reviews.

- **Code Reviews:** Code reviews also known as Static code reviews are a systematic review of the source code of the project without executing the code. It checks the syntax of the code, coding standards, code optimization, etc.
- **Inspection:** Inspection is a formal review process that follows a strict procedure to find defects. Reviewers have a checklist to review the work products. They record the defects and inform the participants to rectify the errors.

Benefits of Static Testing

Below are some of the benefits of static testing:

- **Early detection of defects:** Static testing helps in the early detection of defects by reviewing the documents and artifacts before execution, issues can be detected and resolved at an early stage, thus saving time and effort later in the development process.
- **Cost-effective:** Static testing is more cost-effective than dynamic testing techniques. Defects found during static testing are much cheaper to find and fix for the organization than in dynamic testing. It reduces the development, testing, and overall organization cost.
- **Easy to find defects:** Static testing easily finds defects that dynamic testing does not detect easily.
- **Increase development productivity:** Static testing increases development productivity due to quality and understandable documentation, and improved design.
- **Identifies coding errors:** Static testing helps to identify coding errors and syntax issues resulting in cleaner and more maintainable code.

Limitations of Static Testing

Below are some of the limitations of static testing:

- **Detect some issues:** Static testing may not uncover all issues that could arise during runtime. Some defects may appear only during dynamic testing when the software runs.
- **Depends on the reviewer's skills:** The effectiveness of static testing depends on the reviewer's skills, experience, and knowledge.
- **Time-consuming:** Static testing can be time-consuming when working on large and complex projects.

Dynamic Testing

Dynamic Testing is a type of Software Testing that is performed to analyze the dynamic behaviour of the code. It includes the testing of the software for the input values and output values that are analyzed.

- The purpose of dynamic testing is to confirm that the software product works in conformance with the business requirements.
- It involves executing the software and validating the output with the expected outcome.
- It can be with black box testing or white box testing.

- It is slightly complex as it requires the tester to have a deep knowledge of the system.
- It provides more realistic results than static testing.

Dynamic Testing Techniques

Dynamic testing is broadly classified into two types:

- **White box Testing:** White box testing also known as clear box testing looks at the internal workings of the code. The developers will perform the white box testing where they will test every line of the program's code. In this type of testing the test cases are derived from the source code and the inputs and outputs are known in advance.
- **Black box Testing:** Black box testing looks only at the functionality of the Application Under Test (AUT). In this testing, the testers are unaware of the system's underlying code. They check whether the system is generating the expected output according to the requirements. The Black box testing is further classified as, Functional Testing and Non-functional Testing.

Benefits of Dynamic Testing

Below are some of the benefits of dynamic testing:

- **Reveals runtime errors:** Dynamic testing helps to reveal runtime errors, performance bottlenecks, memory leaks, and other issues that become visible only during the execution.
- **Verifies integration of modules:** Dynamic testing helps to verify the integration of modules, databases, and APIs, ensuring that the system is working seamlessly.
- **Accurate reliability assessment:** Dynamic testing helps to provide accurate quality and reliability assessment of the software thus verifying that the software meets the specified requirements and functions as intended. This helps to make sure that the software functions correctly in different usage scenarios.

Limitations of Dynamic Testing

Below are some of the limitations of dynamic testing:

- **Time-consuming:** Dynamic testing can be time-consuming in the case of complex systems and large test suites.
- **Requires effort:** It requires significant effort in complex systems to debug and pinpoint the exact cause.
- **Challenging:** In case of testing exceptional or rare conditions it can be challenging to conduct.
- **May not cover all scenarios:** Dynamic testing may not cover all possible scenarios due to a large number of potential inputs and execution paths.

Static Testing vs Dynamic Testing

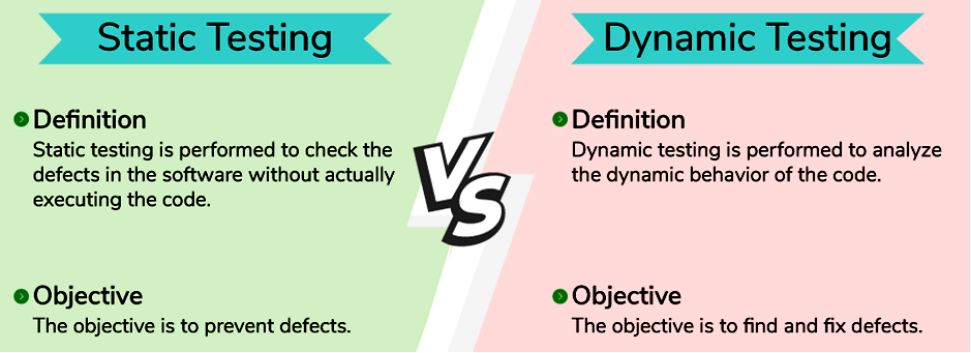
Below are the differences between static testing and dynamic testing:

Parameters	Static Testing	Dynamic Testing
Definition	Static testing is performed to check the defects in the software without actually executing the code.	Dynamic testing is performed to analyze the dynamic behavior of the code.
Objective	The objective is to prevent defects.	The objective is to find and fix defects.
Stage of execution	It is performed at the early stage of software development.	It is performed at the later stage of the software development.
Code Execution	In static testing, the whole code is not executed.	In dynamic testing, the whole code is executed.
Before/ After Code Deployment	Static testing is performed before code deployment.	Dynamic testing is performed after code deployment.
Cost	Static testing is less costly.	Dynamic testing is highly costly.
Documents Required	Static Testing involves a checklist for the testing process.	Dynamic Testing involves test cases for the testing process.
Time Required	It generally takes a shorter time.	It usually takes a longer time as it involves running several test cases.
Bugs	It can discover a variety of bugs.	It exposes the bugs that are explorable through execution hence discovering only a limited type of bugs.
Statement Coverage	Static testing may complete 100% statement coverage incomparably in less time.	Dynamic testing only achieves less than 50% coverage.
Techniques	It includes Informal reviews, walkthroughs, technical reviews, code reviews, and inspections.	It involves functional and non-functional testing.
Example	It is a verification process.	It is a validation process.

Difference between Static and Dynamic Testing

Testing is the most important stage in the Software Development Lifecycle (SDLC). It helps to deliver high-quality products to the end-user and also provides an opportunity for the developer to improve the product. Testing is of many types and is chosen based on the

product that is being developed. Static Testing and Dynamic Testing are the two testing techniques that will be discussed in this article.



Security intelligence

Security intelligence refers to the practice of collecting, standardizing and analyzing data that is generated by networks, applications, and other IT infrastructure in real-time, and the use of that information to assess and improve an organization's security posture. The discipline of security intelligence includes the deployment of software assets and personnel with the objective of discovering actionable and useful insights that drive threat mitigation and risk reduction for the organization.

Benefits of security intelligence

Security intelligence has significant benefits for IT organizations that face strict regulatory compliance requirements for the sensitive data they collect through web applications. The gathering of security intelligence feeds into other downstream SecOps processes that help secure the IT infrastructure against cyber attacks.

IT organizations adopt security information and event management (SIEM) tools to bolster security intelligence-gathering efforts. Here are three ways that IT organizations can benefit from gathering security intelligence more quickly and efficiently.

Improved regulatory and standards compliance

Regulatory compliance is a key driver of IT security initiatives for organizations covered by HIPAA, PCI DDS, or those seeking compliance with the ISO 27001 standard. Tools that collect, standardize and analyze log data can help IT organizations demonstrate compliance with a specified security standard.

Enhanced threat detection and remediation

Detecting security threats is a core function of SIEM tools. Today's best tools use machine learning and big data to correlate events buried in millions of log files across the network. That translates into faster threat detection and better response times when detecting IoCs.

Simplified security operations

Today, IT organizations can automate many types of security intelligence-gathering tasks through cutting-edge SIEM tools, simplifying their operations and reducing the cost of gathering actionable and useful security intelligence.

Security breach

A security breach is any incident that results in unauthorized access to computer data, applications, networks or devices. It results in information being accessed without authorization. Typically, it occurs when an intruder is able to bypass security mechanisms.

Technically, there's a distinction between a security breach and a data breach. A security breach is effectively a break-in, whereas a data breach is defined as the cybercriminal getting away with information. Imagine a burglar; the security breach is when he climbs through the window, and the data breach is when he grabs your pocketbook or laptop and takes it away.

Confidential information has immense value. It's often sold on the dark web; for example, names and credit card numbers can be bought, and then used for the purposes of identity theft or fraud. It's not surprising that security breaches can cost companies huge amounts of money. On average, the bill is nearly $4m for major corporations.

Types of security breaches

There are a number of types of security breaches depending on how access has been gained to the system:

- An exploit attacks a system vulnerability, such as an out of date operating system. Legacy systems which haven't been updated, for instance, in businesses where outdated and versions of Microsoft Windows that are no longer supported are being used, are particularly vulnerable to exploits.
- **Weak passwords** can be cracked or guessed. Even now, some people are still using the password 'password', and 'pa$$word' is not much more secure.
- **Malware attacks,** such as phishing emails can be used to gain entry. It only takes one employee to click on a link in a phishing email to allow malicious software to start spreading throughout the network.
- **Drive-by downloads** use viruses or malware delivered through a compromised or spoofed website.
- **Social engineering** can also be used to gain access. For instance, an intruder phones an employee claiming to be from the company's IT helpdesk and asks for the password in order to 'fix' the computer.

Understanding Big Data Security Analytics

Understanding Big Data Security Analytics is crucial in today's digital landscape, where cybersecurity threats are constantly evolving. You must grasp the concept of Big Data Security Analytics, which involves the application of advanced analytical methods to detect and prevent potential breaches.

By utilising tools like LogRhythm and IBM QRadar, organisations can delve into massive amounts of data to identify patterns, anomalies, and threats that may otherwise go unnoticed. Big Data Security Analytics plays a pivotal role in safeguarding sensitive information and networks by providing real-time monitoring and proactive threat detection.

Through continuous analysis of logs, network traffic, and user behaviour, companies can strengthen their overall cybersecurity posture and respond swiftly to any suspicious activities. It is imperative to invest in robust security analytics solutions to stay ahead of cyber threats and protect valuable assets.

Big Data Security Analytics

You can enhance cyber security through the practice of Big Data Security Analytics, which involves using advanced analytical methods to identify and mitigate threats like insider threats and network activity anomalies.

This process entails utilising state-of-the-art technologies such as machine learning and artificial intelligence to analyse large volumes of data in real time. This allows organisations to detect potential security incidents proactively.

By leveraging these technologies, Big Data Security Analytics can reveal patterns and trends that may suggest malicious activity, enabling organisations to respond promptly to potential threats before they escalate into significant security breaches.

The integration of machine learning algorithms enables the system to continuously learn and adapt to emerging threats, making Big Data Security Analytics a critical component in the contemporary cyber security landscape.

Importance of Big Data Security Analytics

The importance of Big Data Security Analytics for you lies in its ability to proactively detect and respond to security incidents, safeguarding against data breaches and cyber threats. By analysing vast amounts of data in real time, you can identify unusual patterns or behaviours that may indicate potential threats, providing you with the ability to mitigate risks promptly.

Leveraging cloud security measures enhances the efficiency of Big Data Security Analytics for you by ensuring the protection of data both at rest and in transit. With the continuous evolution of cyber threats, the integration of advanced threat detection mechanisms within these analytics solutions becomes crucial for you in maintaining data privacy and enhancing cyber resilience.

Types of Big Data Analytics in security

Various types of Big Data Analytics are employed in security, including diagnostic analytics, predictive analysis, and prescriptive analytics, catering to both structured and unstructured data sources.

Diagnostic analytics focuses on analysing historical data to recognize patterns and trends, while predictive analysis employs machine learning algorithms to foresee potential threats.

Prescriptive analytics goes beyond this by proposing actions to reduce risks and enhance overall security posture. These analytics techniques are vital in detecting anomalies and suspicious activities within a distributed security infrastructure, allowing organizations to protect against cyber threats preemptively.

Use cases for Big Data Security Analytics

Big Data Security Analytics offers a wide range of use cases, including network traffic analysis, user behaviour profiling, and monitoring cloud security, all designed to improve threat detection capabilities.

For example, in the context of threat hunting, Big Data Security Analytics can employ supervised learning algorithms to analyse extensive data sets and detect unusual patterns that

may signal security breaches. By utilising machine learning methods, organizations can detect anomalies proactively and promptly react to threats before they become more serious.
These analytical tools are essential in enhancing **incident response** timelines, allowing security teams to promptly investigate and address cyber threats, ultimately reducing potential damages.

Big Data Security tools for analysis

In the realm of Big Data Security Analytics, tools such as LogRhythm and IBM QRadar stand out for their robust capabilities in threat evaluation, anomaly detection, and security alerts.

These Security Information and Event Management (SIEM) platforms are essential for integrating data security training and threat intelligence into security operations. By aggregating and analysing security logs from various sources, SIEM tools allow organisations to proactively monitor their IT environments for suspicious activities and potential security breaches.

SIEM platforms help centralise security event information, enabling swift incident response and improving overall security posture. The advanced features of SIEM solutions aid in correlating security events, establishing baselines, and identifying emerging threats for prompt mitigation.

Stages of Big Data Security Analytics

The stages of Big Data Security Analytics typically involve data collection, processing, analysis, and action, with technologies like UEBA enhancing user behaviour analytics for improved threat identification.
Data collection is key in the initial phase. A diverse range of data is sourced from various endpoints and network traffic. This data is then processed to transform it into a usable format for analysis.

Moving on to the analysis stage, advanced technologies such as deep learning and data mining step in to identify patterns and anomalies that might signal potential security threats. UEBA tools leverage these technologies for real-time monitoring of user behaviour, enabling organisations to rapidly detect and respond to any suspicious activities.

The benefits of Big Data Security Analytics

The benefits of Big Data Security Analytics for you include proactive threat detection, **rapid incident response**, and enhanced visibility into network activity, all of which contribute to fostering cyber resilience and data protection.

By leveraging advanced algorithms and machine learning capabilities, Big Data Security Analytics can help your organisation identify and prioritise potential security breaches before they escalate. Real-time monitoring and threat evaluation allow your company to detect anomalies and take immediate action to mitigate risks quickly. This proactive approach not only safeguards sensitive data but also minimises the impact of security incidents.

The comprehensive insights provided by Big Data Security Analytics empower your organisation to continuously improve its security posture, ensuring you stay ahead of evolving cyber threats.

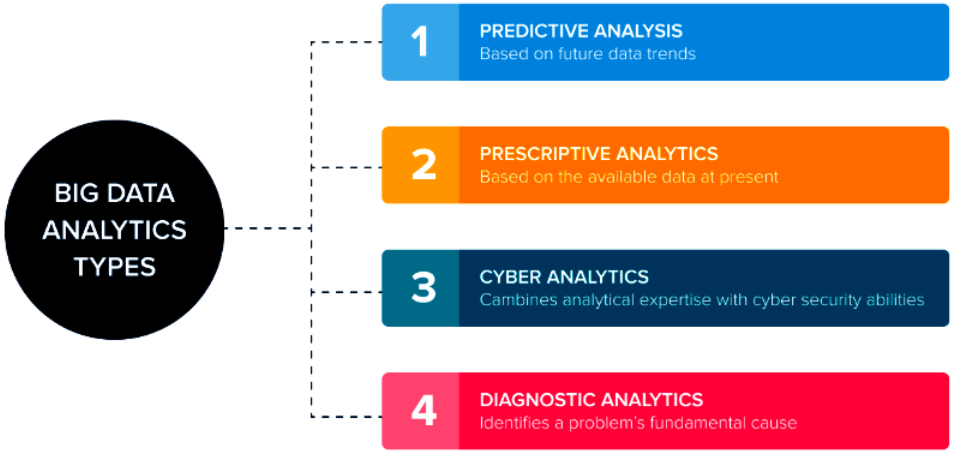
The challenges of implementing Big Data Security Analytics

When implementing Big Data Security Analytics, you may encounter challenges such as data privacy concerns, skill gaps, and the complexity of analysing vast amounts of security data. Navigating the realm of security analytics can be daunting, especially given the evolving landscape of data privacy regulations that govern how organisations handle sensitive information.

The increasing sophistication of security incidents requires specialised cybersecurity expertise to detect and respond to threats promptly. Best practices suggest that continuous training and upskilling of cybersecurity professionals are essential to staying abreast of cyber threats. Therefore, it is crucial for businesses to invest in enhancing the knowledge and skills of their security teams.

Identifying Big data analytics types

Now that you know Big data analytics, let's look at the five types one may understand and us



- **Predictive analysis:** Data trends can be predicted with statistics, modeling, data mining, artificial intelligence, and machine learning. It is the most common and user-friendly approach to analytics. This model aims to forecast the outcomes of various company reaction scenarios to a given circumstance.
    - There are several kinds and sizes of predictive analytics models, but they all utilize a scoring method to determine the chance that a certain result will occur. Transactional profiling, decision analysis & optimization, and predictive modeling are the three pillars of predictive analytics. Predictive analytics explores transactional and historical data for trends to detect risks and opportunities.
    - Prescriptive analytics is one of the three primary forms of data analysis used by organizations. Using prescriptive analytics, the analyst may provide the optimal recommendations for a specific circumstance based on the available data. Prescriptive analytics place more emphasis on the present condition than descriptive and predictive analytics, which are more concerned with the past and future.

- **Cyber analytics:** Cyber analytics, which combines analytical expertise with cybersecurity abilities, is a new and rapidly increasing skill set in the BI and data analytics industry. The amount and sophistication of cyber threats have increased with the number of internet-connected devices.
- **Diagnostic analytics:** Diagnostic Analytics does precisely what its name implies: it identifies a problem's fundamental cause. It gives a full understanding of a problem's core cause.

  Big data engineers use analytics to find the cause of an occurrence. Diagnostic analytics techniques include drill-down, data mining, data recovery, churn cause analysis, and customer health score analysis. Examining the underlying causes of the most significant churn indicators and identifying patterns among your most loyal

DDoS attack

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

Identify a DDoS attack

The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable. But since a number of causes - such a legitimate spike in traffic - can create similar performance issues, further investigation is usually required. Traffic analytics tools can help you spot some of these telltale signs of a DDoS attack:

- Suspicious amounts of traffic originating from a single IP address or IP range
- A flood of traffic from users who share a single behavioral profile, such as device type, geolocation, or web browser version
- An unexplained surge in requests to a single page or endpoint
- Odd traffic patterns such as spikes at odd hours of the day or patterns that appear to be unnatural (e.g. a spike every 10 minutes)

There are other, more specific signs of DDoS attack that can vary depending on the type of attack.