# Cloud Storage, Security and Design
# Unit 2

**VIRTUAL DATA:-** A virtual data center offers the capabilities of a traditional data center, but using cloud-based resources instead of physical resources. It provides an organization with the ability to deploy additional infrastructure resources at need without acquiring, deploying, configuring, and maintaining physical appliances. This enables organizations to take advantage of the flexibility, scalability, and cost savings of cloud computing.

## I. TRADITIONAL DATA CENTER VS. VIRTUAL DATA CENTER

The table below highlights the main differences between on-prem and virtual data centers.

| **Traditional data center** | **Point of comparison** | **Virtual data center** |
|---|---|---|
| A facility that houses computer hardware and provides computing capabilities. | **Definition** | A pool of cloud resources that uses virtualization to provide computing capabilities. |
| A high upfront cost as companies need to buy hardware and rent space. High electricity, cooling, and maintenance costs. | **Costs** | A cost-effective pay-as-you-use payment model. No initial investment necessary. |
| Capital expenditure (CapEx) as companies need to acquire and maintain physical assets. | **Main investment type** | Operating expenses (OpEx) as the company pays ongoing costs only. |
| Designing and building a data center can take months. Each new piece of hardware requires purchasing, configuring, and racking. | **Setup speed** | Building a new VDC is typically a matter of days. Adding new VMs and capabilities requires minutes. |
| The data center owner makes full use of CPU, memory, storage, and network resources. | **Hardware dedication** | A single machine can host multiple VMs, so clients can see performance issues if the vendor's device has too many tenants. |
| The team deploys physical servers with fixed CPUs, memory, and storage. Limited upgrade options and time-consuming server management. | **Servers** | The team deploys resizable virtual servers that keep up with current workload demands. |
| The team must plan for and set up switch ports, routers, and cabling. | **Networking gear** | Relies on software-defined networks (SDN) and virtual routers to scale network capacity up or down. |
| Data center security starts with entry restrictions and verifiable access to server racks. The in-house team is in | **Security** | The team focuses on IT-level security, while the provider takes care of physical protection. Most |

| | | |
|---|---|---|
| charge of IT-level security, too. | **considerations** | vendors offer services for IT-security as well. |
| Hard to implement and manage centralized security. | **Security centralization** | Has centralized security and management. |
| Companies need trained personnel to rack and stack equipment. Most companies have separate compute, storage, and network teams. | **Staff requirements** | As little as two or three people can manage a VDC, but staff members require strong expertise. |
| Migration is a slow and expensive project. | **Data center migration** | Migrating a VDC is quick, simple, and cheap. |
| Difficult to move the workload from one hardware to another. | **Workload migration** | Easy workload migration between hardware platforms. |
| Relatively static and predictable, and typically goes one way (adding more equipment). | **Scalability** | Dynamic provisioning enables teams to scale the number of VMs up and down with speed and ease. |
| A traditional data center is a large consumer of power. | **Power consumption** | Users do not cover power expenses. |
| Many repetitive tasks and coordination work, but not a lot of necessary expertise. | **Maintenance complexity** | Less repetitive tasks, but the team requires deep expertise. |
| Requires backup agents that the team must deploy, patch, and manage. | **Backups** | The hypervisor provides LAN-free and agentless backup services. |
| Each server needs a separate anti-virus program. | **Server anti-virus management** | Anti-virus operates at the hypervisor level. |
| Firewalls are centrally located and typically not part of the server. | **Firewalls** | A built-in property of the VM. |
| DR occurs on a per-application basis, and every app has a different solution. | **Disaster recovery** | DR is a service and enables center-wide strategies. |
| Requires accurate estimation of future needs to avoid unnecessary overhead. | **Future planning** | The company pays only for the needed capacity and can scale up and down to meet the current requirements. No overhead. |

# Security Information and Event Management (SIEM)

## II. 1. INTRODUCTION

### 1.1 *What is SIEM?*

Modern-day threats are continuously evolving in complexity and sophistication. A security team does not know what they will face next. With the increasing number of endpoint devices and growing reliance on cloud-based services,
potential attack surface area is expanding. Considering all these factors, it becomes difficult for security teams to keep track of events happening across an enterprise network.

It is a fact that organizations install multiple security devices and software to detect unusual behavior and identify a security incident. However, all such devices and software work in isolation and their efficiency falls short when it comes to detecting advanced threats. Without a doubt, attackers use an arsenal of tools to plan and execute an attack as
well as advanced techniques to evade detection by an organization's security system. As of 2020, attackers do not only focus on a single system or software; they launch distributed attacks on multiple systems, making it difficult for the existing security measures to detect unusual activity.

This is where a Security Information and Event Management (SIEM) comes in and helps a security team through real- time collection and analysis of log data. Gartner provides a widely accepted definition of SIEM as a "technology that supports threat detection, compliance, and security incident management through the collection and analysis (both near real-time and historical) of security events, as well as a wide variety of other event and contextual data sources.*

### 1.2 *How does a SIEM work?*

A SIEM solution collects logs and events data from various components of an enterprise network. After normalizing the data, it uses threat intelligence, inbuilt rules, and advanced analytical functions to detect security incidents real-time. In other words, SIEM offers a single-pane holistic view of an organization's information security.
Depending on its architecture, it arranges alerts into various categories such as malware, failed logins, successful logins, other potentially harmful activity, etc.

It combines two technologies: Security Information Management (SIM) and Security Event Management (SEM). In modern SIEM solutions, it is difficult to separate the two components. SIM primarily looks after data collection from log sources and generates the desired reports.
On the other hand, SEM performs real-time monitoring of enterprise systems for threat detection and event correlation.

When a SIEM solution identifies a potential threat, it generates alerts to notify the security team. Based on pre-defined rules, the priority of an alert can be low, medium, or high. For example, if the user account of user X generates ten login attempts in five minutes, that can
be considered as suspicious activity. Most likely, however, user X has forgotten their password and is unable to login. Suppose the same user account experiences 200 login attempts in the same duration. In that case, the SIEM solution will tag this activity as a high severity incident since it can be a brute-force attack.

## 1.3 *Why do you need SIEM?*

Modern SIEM solutions provide a robust method for threat detection, report generation, and long-term analytics of security logs. Scalable SIEM solutions ensure that they grow with an organization's business requirements and yield a maximum possible return on investment (ROI).

A SIEM solution supports a security team in responding to potential security incidents faster. It automates the tedious task of manually analyzing log data from different sources. As a result, a security team can focus on alerts with high risk and significant impact. For example, a single alert generated by an anti-virus solution may not garner sufficient attention. However, if an organization's firewall detects unusual traffic at the same time as the anti-virus alert, this could indicate that there is an ongoing security incident. This correlation is what SIEM makes possible.

Some of the benefits of SIEM solutions include:

- Increased efficiency of a security team and better utilization of man-hours
- Preventing potential security threats from becoming large-scale security incident
- Reducing overall security expenditures for an organization
- Providing a better system for reporting, log analysis, and data retention
- Minimizing the impact of security breaches

* https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

### 1.4 *Migrating a legacy SIEM to next-gen SIEM*

SIEM as a solution has been in the market for around two decades. Legacy SIEM solutions were complicated and hard to configure. This technology became redundant over time, and it was challenging to scale. These issues accelerated the development of SIEM solutions that are flexible, advanced, analytics-driven, and scalable. For any SIEM solution, collecting log data from a variety of sources is a simple operation. An organization has a dearth of options in terms of how they wish to store this data. The uphill battle is turning this data into actionable intelligence.

Organizations that rely on legacy SIEM solutions often find that their SIEM is static in nature. It lacks sufficient correlation features and is relatively complicated to support time-sensitive investigations. With the advent of cloud computing technology and SaaS delivery model, next-gen SIEM solutions have been able to cover the full scope of potential threats. Some of the commonly observed issues in legacy SIEMs are:

- Limited detection, investigation, and incident response capabilities due to limited data ingestion
- Ingestion of data is a tiresome process
- Fairly complex to operate and require skilled employees
- Generate a large number of false positive and false negative alerts
- Static and restrictive in nature with limited capabilities
- Incapable of detecting sophisticated threats and increase security risk
- Lack of scalability and adaptability to business needs
- Well-documented incidents of outages
- Lack of features to integrate with other security tools
- Often available in on-premises deployment model only

Organizations overcome this drawback by selecting a SIEM solution that allows their security team to manage the entire organization's security posture comprehensively. Next-gen SIEM solutions are analytics-driven and they enable organizations to monitor and respond to threats in real-time. Such SIEM solutions rely on threat intelligence (TI) to understand the risks an organization faces. Modern SIEMs do away with the limitation of deploying SIEM solutions on-premises. They can also be deployed on the cloud infrastructure or in a hybrid environment. Next-gen SIEM solutions go beyond applying simple data correlation rules and include specialized tools to deal with threats through the platform itself.

## III. 2. SIEM Use Cases

Security Information and Event Management (SIEM) solutions aggregate event and log data from the entire enterprise network. They help a security team in detecting and responding to security events, along with generating reports to demonstrate compliance. Once implemented, a SIEM solution becomes a vital component of an enterprise security strategy. As a result, there are a large number of use cases that it caters to. The following sub-sections discuss common SIEM use cases, from traditional to advanced capabilities. dern-day threats are continuously evolving in complexity and sophistication. A security team does not know what they will face next. With the increasing number of endpoint devices and growing reliance on cloud-based services, potential attack surface area is expanding. Considering all these factors, it becomes difficult for security teams to keep track of events happening across an enterprise network.

It is a fact that organizations install multiple security devices and software to detect unusual behavior and identify a security incident. However, all such devices and software work in isolation and their efficiency falls short when it comes to detecting advanced threats. Without a doubt, attackers use an arsenal of tools to plan and execute an attack as well as advanced techniques to evade detection by an organization's security system. As of 2020, attackers do not only focus on a single system or software; they launch distributed attacks on multiple systems, making it difficult for the existing security measures to detect unusual activity.

This is where a Security Information and Event Management (SIEM) comes in and helps a security team through real-time collection and analysis of log data. Gartner provides a widely accepted definition of SIEM as a "technology that supports threat detection, compliance, and security incident management through the collection and analysis (both near real-time and historical) of security events, as well as a wide variety of other event and contextual data sources.

## 2.1 *Data Exfiltration*

In 2020, enterprises depend on data for their business operations. This data can be customer information, supplier details, trade secrets, intellectual property, employee records, etc. The value of data for an organization cannot be straightforward put in terms of money. Data exfiltration refers to the unauthorized transfer of data from the enterprise network to a receiver. Mostly, this recipient is an attacker or a competitor. Other commonly used terms for data exfiltration include data extrusion and data theft. It is not just another external risk; it is also an internal risk as it can involve an insider.

Transfer of data is either manual or automatic. It is manual transfer when a user transfers organizational data to a physical device or over the Internet. In contrast, it is automatic when malware has infected a computer system. Irrespective of an organization's size, data exfiltration is a severe problem.

A SIEM solution detects data exfiltration events by closely monitoring network traffic to identify data transfer in large volumes. It may generate an alert when the recipient appears to be malicious or unknown. As SIEM solutions perform data correlation from multiple systems, they detect lateral movement and privilege escalation. In addition, they monitor email server logs to identify emails sent to untrusted receivers.

## 2.2 *Zero-day Attacks*

Attackers remain on the constant lookout to find vulnerabilities in an organization's IT infrastructure. In contrast, a security team continuously monitors their organization's IT infrastructure for detecting unusual activity and existing vulnerabilities. An IT infrastructure can consist of hundreds of devices and software from different vendors. While vendors regularly release patches and updates for their products and services, there are often vulnerabilities that are not publicly known. When attackers exploit this particular subset of vulnerabilities, it is called as a zero-day attack. Traditional security tools such as IDS/IPS device or anti-virus/anti-malware software fail to detect such attacks as their attack signatures do not exist. Using real-time monitoring of an organization's IT infrastructure, a SIEM solution alerts a security team as soon as it detects abnormal behavior. While a zero-day attack can virtually target any source in the network, SIEM solutions feature advanced investigation capabilities to allow a security team to search for specific data points or use data analysis results for identifying behavior patterns of a zero-day attack.

## 2.3 *Remote Access from Suspicious Location*

As we have adopted to the new-normal, remote access has become crucial for organizations in 2020. While remote access has its own set of benefits, it brings forth a new set of threats that must be addressed. Based on an organization's business units and employee locations, a security team has a fair idea of countries from where remote access is expected and may implement VPN-based logins for its employees.

SIEM solutions come with inbuilt correlation rules for detecting anomalies concerning remote access. By using a database of IP address associated with geographic locations, a SIEM solution provides contextual location information up to the city level. Further, by monitoring log in data for the enterprise network, it quickly generates an alert for the security team as it detects remote access from a suspicious location or concurrent VPN logins. Certain SIEM solutions may allow maintaining a white list or black list of countries for granting access to the enterprise network.

## 2.4 *Privilege Escalation*

It has become a necessity for organizations to implement an access level system to prevent unnecessary user access to their data. In the access level hierarchy, there will be users who sit at the top with high privileges. These users will have powerful permissions to access the network, exfiltrate data disrupt business, or install backdoors in a system.

When attackers break into an organization's network, they attempt to perform privilege escalation to increase the level of privileges associated with the compromised account. The ideal goal is to conduct vertical privilege escalation for gaining administrator-level system privileges. Horizontal privilege escalation only allows attackers to gain access to other user accounts on the same access level. SIEM solutions consisting of user and entity behavior analytics (UEBA) identify anomalous behavior. Modern SIEM solutions use UEBA to prepare a baseline of normal behavior so that the SIEM solution easily detects abnormal behavior.

## 2.5 *Brute Force Attacks*

The threat of brute force attacks is one of the oldest challenges faced by organizations across the globe. While brute force attacks have been around for more than two decades, they use a simple trial and error method to crack passwords. An attacker uses a combination of alphabets, numbers, and special characters to successfully guess the password. They can also utilize dictionary words and commonly used words to increase the success rate.

It becomes imperative for organizations to implement sufficient measures to prevent a successful DDoS attack.
A successful brute force attack results in an attacker getting access to user credentials. Using these credentials, they can steal sensitive information such as intellectual property, trade secrets, and personally identifiable information. Many SIEM solutions come with in-built rules that create alerts for suspicious source IP addresses that exceed the threshold of rejected/invalid login attempts in the given time. Advanced SIEM rules may include the identification of failed login attempts over a longer duration of time and blocking compromised accounts involving failed login attempts before one successful login.

## 2.6 *PowerShell Attacks*

Traditional malware attacks involve the execution of malicious code on a target system. On the contrary, file-less malware attacks utilize inbuilt Windows tools such as PowerShell to perform malicious attacks. Since the attack involves legitimate programs, it is challenging to detect PowerShell attacks. Given the importance of PowerShell for security operations, disabling it is not a solution. For organizations, the situation has further worsened due to the large-scale distribution of exploit kits.

A SIEM solution analyzes incoming event logs for detecting malicious activity. For detecting PowerShell attacks, the platform looks for specific event IDs and their characteristics in event logs coming from Windows systems. For example, while detecting lateral movement, the SIEM solution will look for Windows Remote Management (WinRM) along with PowerShell command Enter-PSSession.

## 2.7 *Lateral Movement*

After an attacker can gain the initial access into an enterprise network, they seek to move deeper into the network for finding sensitive data and critical assets. The initial access may be the result of a malware infection or phishing attack. Then, an attacker may impersonate a genuine user to avoid being detected. Lateral movement is generally observed in advanced cyber attacks wherein the attackers aim to inflict the maximum possible damage. Stealing credentials, privilege escalation, and gaining access to sensitive information form critical components of an attack involving lateral movement.

Unlike traditional security systems that perform in isolation, SIEM solutions have a comprehensive view of events happening across an enterprise network. With logs coming in from multiple systems and devices, it becomes easy to detect techniques used in lateral movement. With real-time monitoring combined with behavioral analysis, SIEM solutions streamline investigation of lateral movement with contextual evidence.

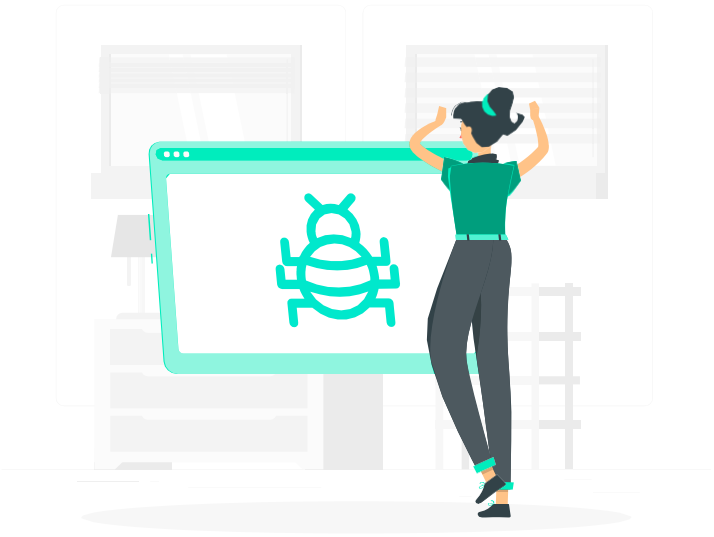

## 2.8 *Insider Threats*

Many studies have concluded over the years that insider threat is one of the prominent reasons behind security breaches. In contrast to most of the security risks an organization faces, this originates from within the organization. Insider threats can go unnoticed as a legitimate user is performing malicious actions. Insider threat is not limited to an employee stealing data from enterprise network; it can also occur due to unintentional acts such as losing a laptop or storage drive and sending an email at an incorrect mail address.

SIEM solutions have multiple mechanisms to detect insider threats. A SIEM solution detects abnormal user behavior by analyzing login time, frequency of login, and commonly used resources. Further, they utilize threat intelligence (TI) feeds in correlation with network traffic to identify a command and control center and user participation in the communication. Other signs that trigger alerts include encryption of data, movement of large amounts of data from one resource to another, and lateral movement.

## 2.9 *Malware Detection*

Malware is an umbrella term that includes virus, trojan horses, worm, spyware, ransomware, and adware. As per the general understanding, it refers to any malicious program that intends to cause damage to a system or gain unauthorized access. Over the years, many prominent malware families and their variants have caused substantial damages to enterprises across the globe. Stuxnet and WannaCry are a few examples.



Malware is generally delivered through drive-by downloads, email attachments, and freeware websites. Modern-day SIEM solutions perform continuous monitoring of enterprise systems to detect malicious files with known hashes. They rely on historical data, and threat intelligence feeds to detect malicious programs in enterprise systems. While next-gen SIEM solutions use signature-based techniques and attack patterns, they also form hypotheses for further examination by security teams based on behavior analysis.

## 2.10 *Unauthorized Access to the Shared Folders*

File system plays a crucial role in an organization's business operations. In a traditional setup, a shared file system creates a storage area network for allowing multiple computer systems to gain access to the storage space. An organization's access level system may guide the extent of access granted to individuals. Like this, cloud-based services are being increasingly used to share storage space among employees.

SIEM solutions track logins across the enterprise systems for revealing malicious actions from insiders as well as outsiders. To start with, SIEM solutions aggregate authentication records from multiple systems and services to determine account takeover incidents. Traditional security systems considered every successful login as authorized access. However, next-gen SIEM solutions go beyond this assumption to use correlation rules and behavior analytics to identify anomalous activities and detect unauthorized access to shared folders.

## 2.11 *Excessive Web Activities*

An enterprise network sends and receives a plethora of requests and responses every day. These requests can be anything: database connection requests, website access, file downloads, video conferencing data, etc. Manually, it is not feasible for security teams to check the requests one-by-one. As the size of an enterprise network increases, the number of requests and responses increase invariably.

A SIEM solution reduces the burden on a security team by filtering through unnecessary network events. By utilizing inbuilt correlation rules and threat intelligence, a next-gen SIEM generates alerts for excessive database connections, firewall connections from a single source, excessive outbound connections, among other malicious behaviors. Such alerts are accompanied by contextual information, allowing a security team to swiftly decide and take action.

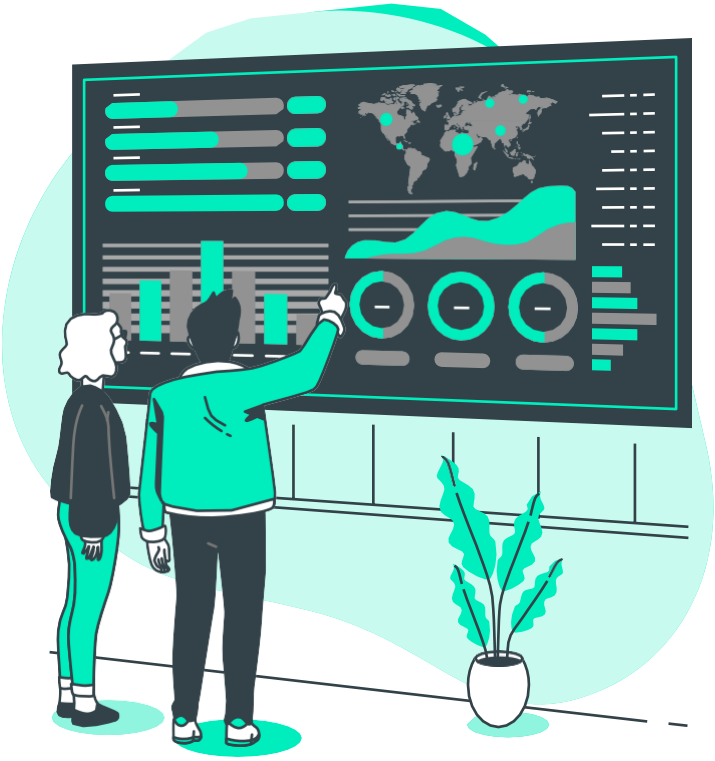
## IV. 3. Evaluation Criterias

### 3.1 *Scalability and Big Data Infrastructure*

An enterprise network and its components continue log generation without any breaks unless there is a downtime. As an organization grows in leaps and bounds, so does its log data. While many organizations plan for infrastructure expansion well ahead of their requirements, they cannot predict the amount of log data their enterprise network would generate in future. A modern SIEM solution should rely on big data infrastructure to be able to scale with an organization in every possible parameter: devices, log sources, size of data, processing power, and efficiency.

### 3.2 *Data Aggregation*

It is reasonable for a prospective customer to expect that their SIEM solution would process log data from all enterprise systems. Most common systems include security devices, firewalls, VPNs, IPS/IDS, email server, FTP server, gateways, and anti-virus/anti-malware products. If a SIEM tool is not compatible with your existing infrastructure setup, it should not be a part of your security strategy.
The native support should cover operating system logs, database connection log, system logs, and cloud-based service logs as a minimum. Some next-gen SIEM solutions may allow security teams to develop manual code for processing log data from a particular source that it does not provide native support for.



### 3.3 *Correlation and Alerts*

Legacy SIEM solutions identify most of the security events from different devices, but they have minimal or negligible power to establish a correlation between them. Modern SIEMs use correlation to provide a broader context of security events and help a security team in focusing on high risk alerts that can have a significant impact on the enterprise network. Most SIEM solutions come with inbuilt correlation rules to identify a threat, vulnerability, or an ongoing security incident. Each correlation rule specifies a sequence of events that indicate an anomaly or deviation from the usual behavior inside an enterprise network. A prospective SIEM buyer must look for a SIEM vendor whose team consists of security experts with extensive domain knowledge and experience.

### 3.4 *Security Analytics*

Security analytics help security teams in performing advanced investigation, instead of limiting themselves to the traditional practice of waiting for correlation rules to trigger. Manually defined correlation rules require a dedicated team for continuous modification and upgrades. Threat environment evolves at a rapid pace and correlation rules alone decrease the efficiency of a SIEM solution over time. Security analytics utilize machine learning algorithms to help a SIEM solution in identifying attack patterns and threats with no prior signatures, rules, or patterns. For machine learning techniques to perform efficiency, they need a vast amount of test data for analysis in a time-bound manner. Big data architecture is required in the backend to extract new insights and suggest actionable results to the security team.

### 3.5 *User and Network Behavior Analytics*

Instead of looking at event logs for each user, a SIEM solution provides a security team with a comprehensive view of user activity along with contextual data. With the continuous influx of log data into a SIEM solution, it creates alerts for known threats and behavioral changes. Next-gen SIEM solutions come with this capability to provide insights into user and network-based threats that would often go unnoticed. Behavioral analytics is supported by artificial intelligence (AI) and machine learning (ML) technologies to minimize detection time and response time for threats faced by an organization.

### *3.7 Threat Intelligence*

There exist many threat intelligent services that provide information about tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), and other contextual information about threats and security incidents. Using this information, a SIEM solution substantially improvises its detection capabilities. For example, if a computer system is communicating with an external IP address, the next-gen SIEM solution would quickly identify whether the destination IP address is a previously known command and control (C&C) server for malicious activities. On the other hand, a modern SIEM solution should gather relevant incident data from various sources to help a security team in analyzing the impact of a security incident. An ideal SIEM solution combines incoming log data from enterprise network components with threat intelligence data for increasing the chances of early detection.

### 3.8 *Search and Forensic Investigation*

Traditional SIEM solutions only collect log data from different sources in the enterprise network. Further, they come with limited flexibility in search capabilities that directly constraint the visibility of a security team. Modern SIEM solutions have adapted to flexible search queries to allow organizations to create their own search queries to meet their organization-specific security requirements. Such solutions enable a security team to explore log data to discover additional details of a security incident. Certain SIEM solutions may help a security team by presenting an incident-specific visual timeline of how the situation unfolded.

### 3.6 *Advanced Threat Detection*

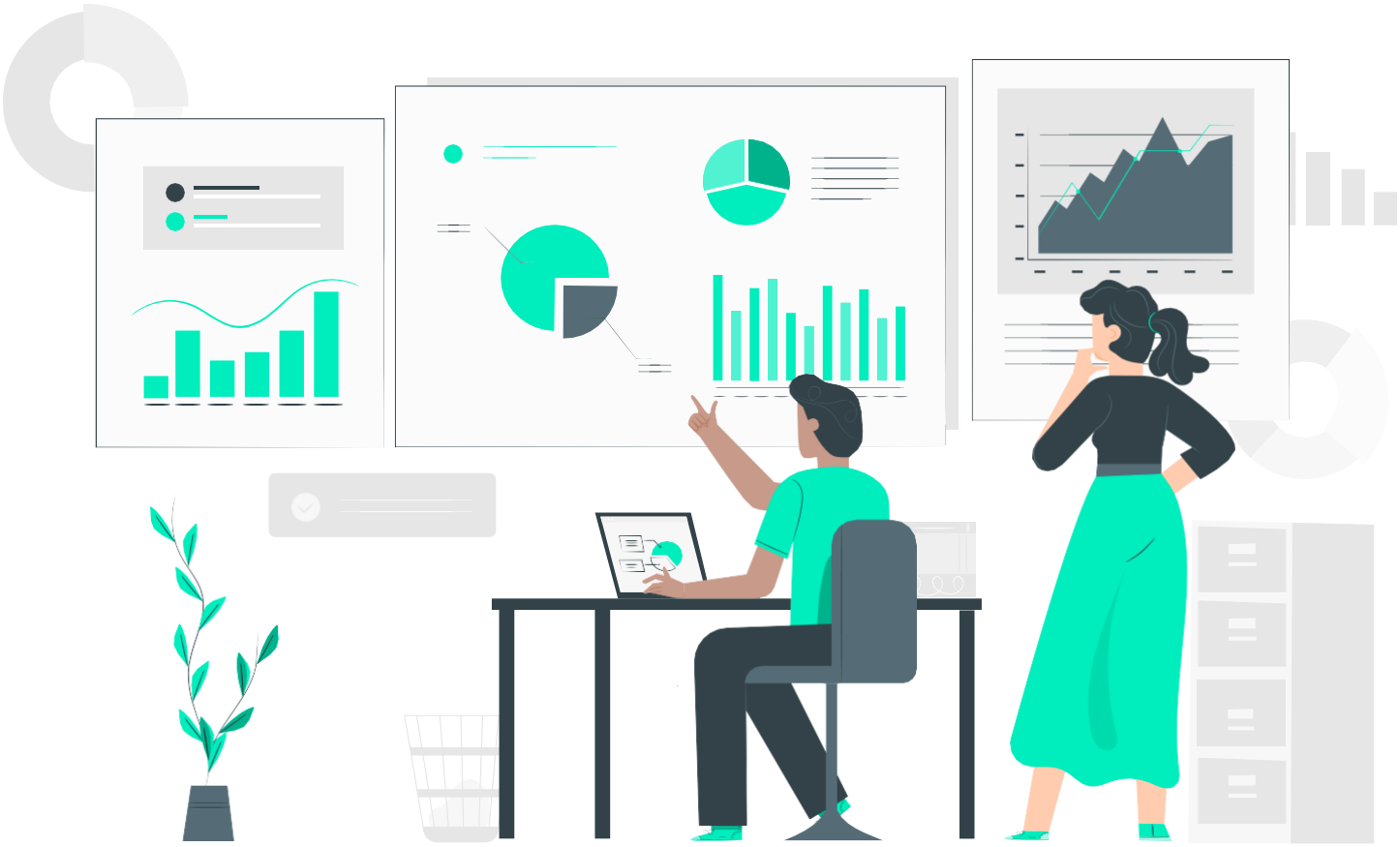
A modern SIEM solution should be capable of adapting to the continuously evolving threat environment. This capability is achieved through the combination of behavior analysis, network monitoring, endpoint detection, and threat intelligence feeds. Advanced threat detection is not only limited to detecting a threat; a SIEM solution should provide information such as the scope of a threat, movement across the network, and possible solutions to the threat. Legacy SIEMs come with in-built static search queries that result in high false positives. As a result, security teams often fail to detect threats. Next-gen SIEM solutions allow a security team to create their search queries for detecting threats and indicators of compromise (IOCs). With this freehand, a security team can customize alerts specific to an organization's business requirements for maximum utilization.

### 3.9 *Compliance*

Fulfilment of compliance obligations is one of the prominent reasons behind the success of SIEM solutions. Next-gen SIEM solutions offer highly customizable reports for their users. These solutions further classify different reports across various categories specific to applicable regulations and standards. Before selecting a suitable SIEM solution, an organization must check whether the prospective SIEM solution provides reporting capabilities for their organization-specific compliance reports. Suppose a SIEM solution does not come with inbuilt reports for a regulation or standard. In that case, it must provide customizable reporting options to help a security team in fulfilling their compliance obligations.

### 3.10 *SOC Automation*

A SIEM solution becomes the foundation for an organization's Security Operation Centre (SOC). Next-gen SIEM solutions must automate SOC processes for enabling a security team to focus on critical and high-risk alerts. Generating alerts and creating tickets, gathering contextual data for an alert, providing information for mitigation, and creating reports on mitigation actions are some of the processes that a modern SIEM solution should automate. Moreover, for low-risk alerts, a security team should be equipped with features to define rules for mitigation so that containment actions are performed automatically.



### 3.11 *Dashboards & Reports*

Dashboards on SIEM solutions visualize the security posture of an organization. A SIEM solution may come with a variety of dashboards for different purposes. However, a prospective SIEM solution must allow the security team to customize and create new dashboards as per their needs. Similarly, having a set of inbuilt report configurations help organizations in the initial setup and running of their SIEM solution. However, as business operations expand and security requirements change, an organization should be capable of customizing existing reports and generating new reports. Before selecting a SIEM solution, an organization must see the customizations it offers for their security teams for streamlining their day-to-day operations.

### 3.12 *Automated Response*

Manually responding to low risk alerts and performing straightforward tasks take a reasonable amount of time. As a result, the overall efficiency of a security team decreases, and they miss out on high risk alerts. Repeating the same task again and again also increases the chances of fatigue and frustration. In such a state, even the best of security professionals may miss a critical alert that needed immediate attention. Next-gen SIEM solutions allow security teams to define automated responses for commonly detected alerts. For example, suppose a user has not been able to sign in after 10 attempts in 10 minutes. In that case, this user account can be blocked and an alert can be generated for the security team to decide whether the block should continue.

### 3.13 *Retention*

Next-gen SIEM solutions require vast resources in terms of data. This need for data is driven due to the underlying machine learning algorithm. Besides, there is no limit to the amount of log data that can be generated in a day by an enterprise network. A SIEM solution should be capable of storing historical data over time without affecting its integrity. Historical data helps SIEM platforms in making the correct predictions and minimizing the number of false positive alerts. Moreover, with the availability of historical data, security teams can trace the source of breaches with minimum hassle. Certain jurisdictions may require an organization to store their security-related information for a specified duration.

### 3.14 *Fault Tolerant*

Fault tolerance refers to the ability of a system to continue its operations even when one or more of its substituent components fail. In the context of SIEM solutions, the backend architecture must be fault tolerant because if the architecture gets disrupted, all the clients of a SIEM vendor will be affected. Modern SIEMs must be fault tolerant to ensure that there does not exist a single point of failure (SPOF) in the entire backend architecture. Business-critical systems such as SIEM solutions must be fault tolerant to ensure business continuity and high availability. Before selecting a SIEM solution for their organization, a security team must understand the specifics of underlying architecture from the concerned SIEM vendor.

## A. *Logsign Security Information and Event Management*

| **Big data infrastructure with infinite scalability** | **Limitless log collection and storage** | **Detection of any complex threats** | **Fast and effective data protection** |
|---|---|---|---|
| Rapid deployment & easy configuration in every environment | Collects every log from every environment with multiple, flexible pricing options | Comprehensive correlation of all your data | Mitigation & eradication of threats |
| Unlimited log collection & storage | Advanced parsing and indexing techniques | Accelerated, detailed incident investigation | Automated incident notification, response, and remediation |
| Massively parallelized, fault tolerant system | Easy-to-work with normalized, classified, and enriched data | Early detection of cybersecurity threats | Minimized response times excluding alert fatigue |
| Long-term data retention | | Uncovered anomalies and IOCs | Early prevention of phishing and suspicious network traffic |

*B. Why Logsign SIEM?*

**360-Degree Visualization**

Visualization with hundreds of built-in security analytics-driven dashboards and reports

**Smartly Designed UI**

Easy-to-use platform and built-in modules, along with the flexibility to create new ones

**Affordable Data Security**

Calculating cost is simple with Logsign's multiple, flexible pricing options

*C. Features of Logsign SIEM*

**Smartly Designed Big Data Environment**

- Big data infrastructure based on Hadoop & NoSQL
- Unlimited scalability for petabyte-level experience
- Fast and easy deployment
- Massively parallelized system with flexibility to add any number of users, notes, or sources
- Continuously active with zero performance loss
- Unlimited log storage
- Long-term data retention

**Find the Hiddens**

- Search functionality with Logsign's drill-down, full-text search
- Accelerated incident investigation
- Uncovering threats, anomalies, and IOCs using the MITRE ATT&CK framework

**Heighten the Visualization**

- 200+ built-in alerts, dashboards, and reports with easy customization
- Easy-to-use wizards
- User delegation with increased focus on visibility and responsibility

**Create Your Own Data Lake**

- 400+ built-in integrations and vendor-free integration capabilities
- Unstructured data parsing with free plugin service
- Limitless data collection from any source from any environment
- Real-time data enrichment with real-time threat intelligence
- Flexible data policy manager

**Detect Complicated Threats**

- Comprehensive correlation of data
- Risk-score based incident triage
- Advanced detection with minimum noise

**Safeguard Your Data**

- Automated incident response
- On-time incident notification
- Automated remediation actions for threats and vulnerabilities