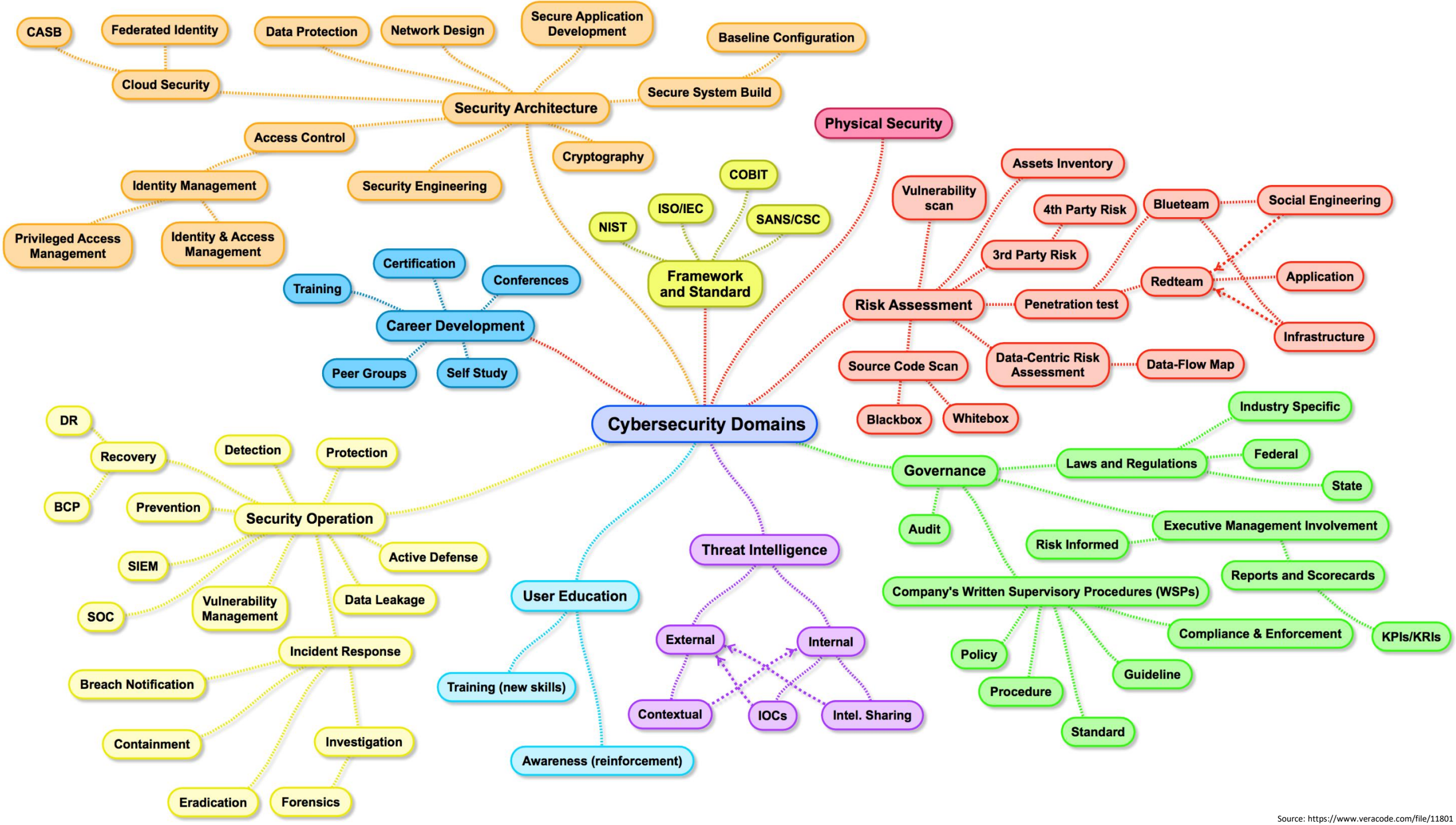
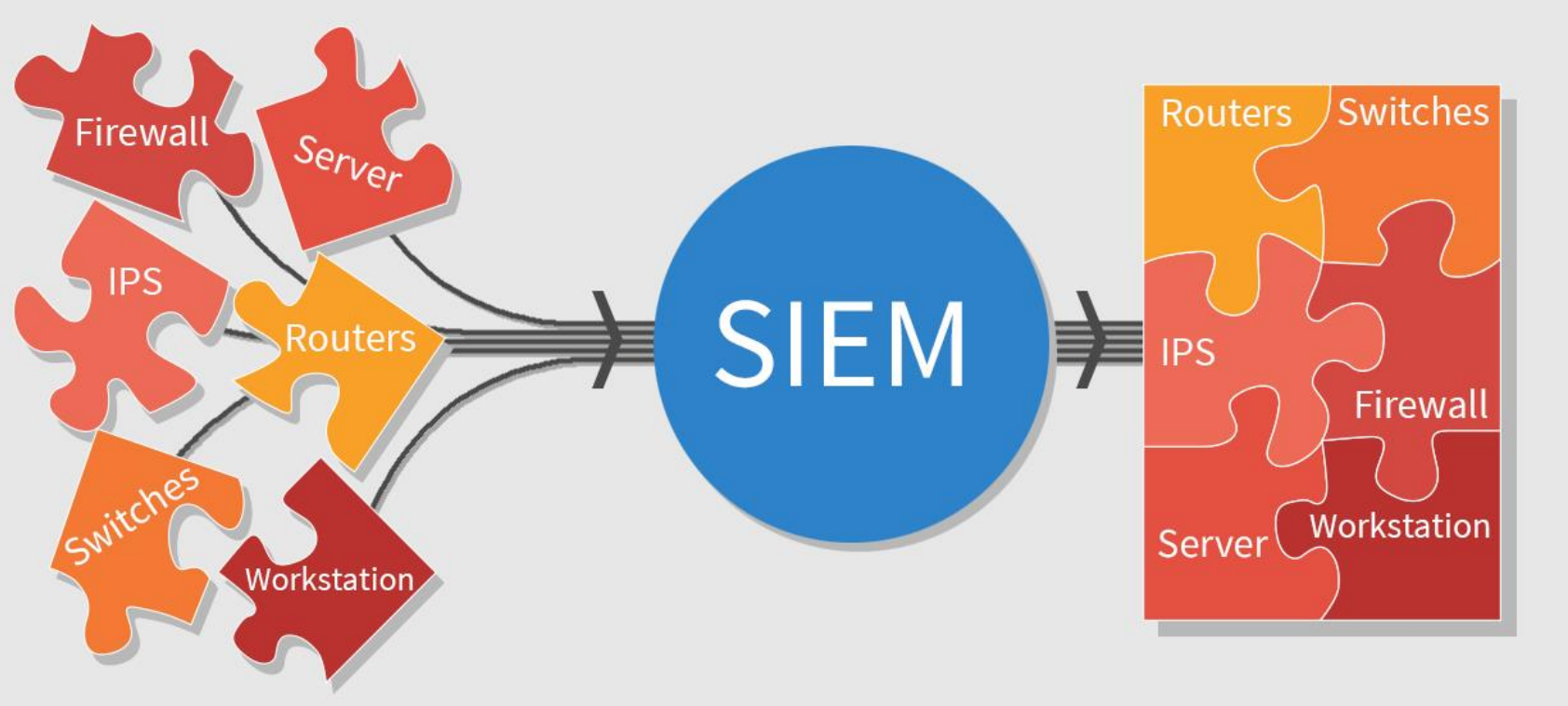
SIEM

SECURITY INCIDENT and EVENT MONITORING



Source: https://www.veracode.com/file/11801



WHAT IS SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM)?

In the field of computer security, security information and event management (SIEM), software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

Source:
https://en.wikipedia.org/wiki/Security_information_and_event_management
https://www.pratum.com/blog/122-benefits-of-log-consolidation-in-a-siem-environment

Cybersecurity event

- A cybersecurity event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards.

Cybersecurity incident

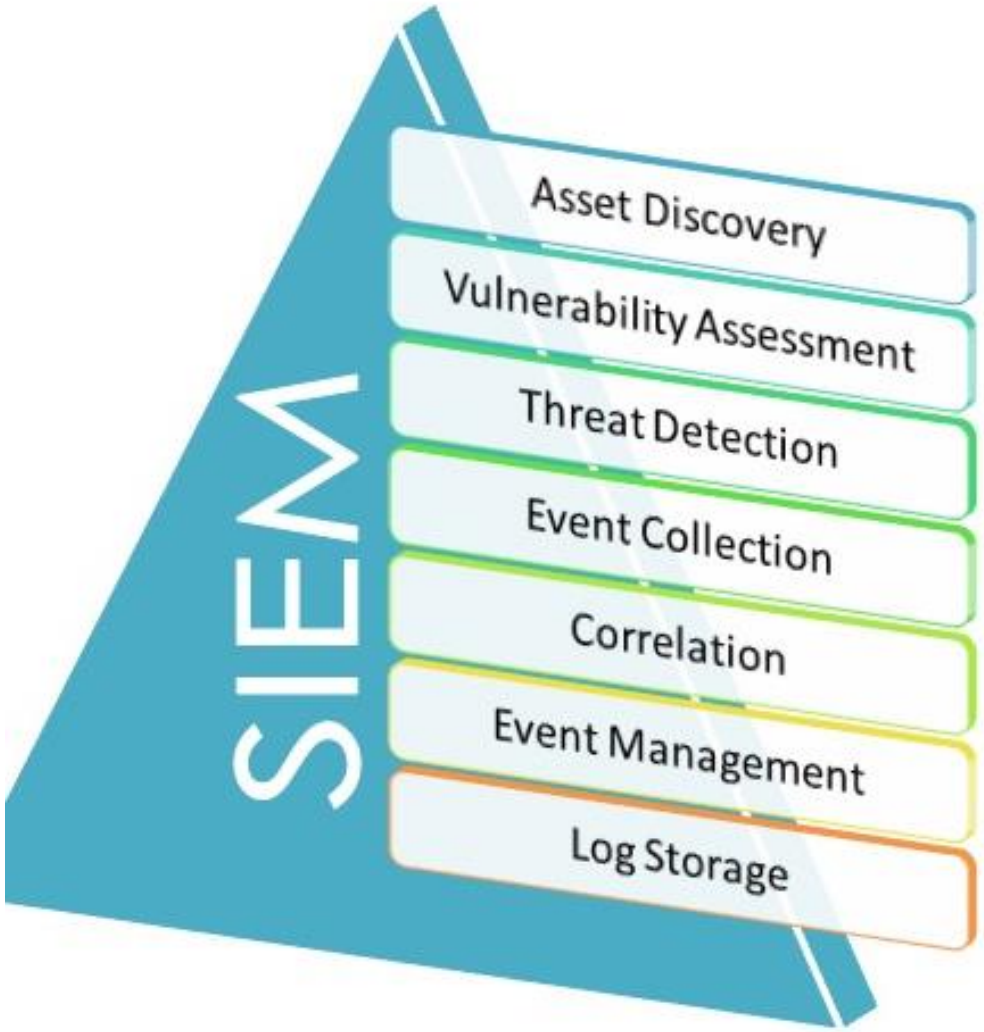
- A cybersecurity incident is an event or a series of events that have risen to a level requiring action to prevent them from negatively impacting the organization.

Source: ISO/IEC 27001

SIEM FUNCTIONS

SIEM, when successfully implemented, helps organizations with its following functions:

- Reveals potential known and unknown threats
- Monitors the activities of authorized users and their privileged access to various resources
- Compiles a regular report
- Backs up incident response (IR)

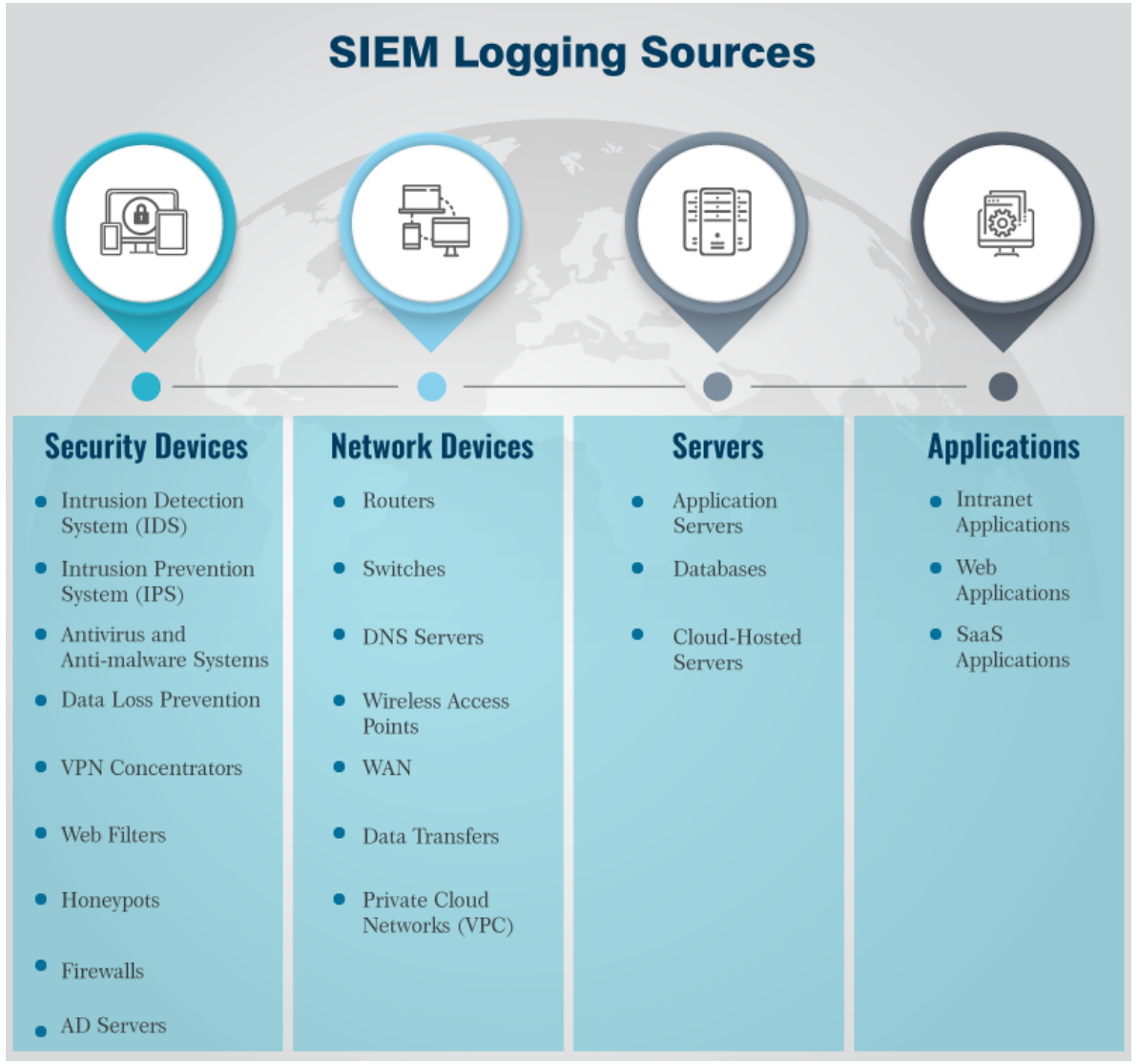


Source: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

Generic Architecture of SIEM

SIEM gathers logs from various devices, the sources of these logs are usually divided into four categories:

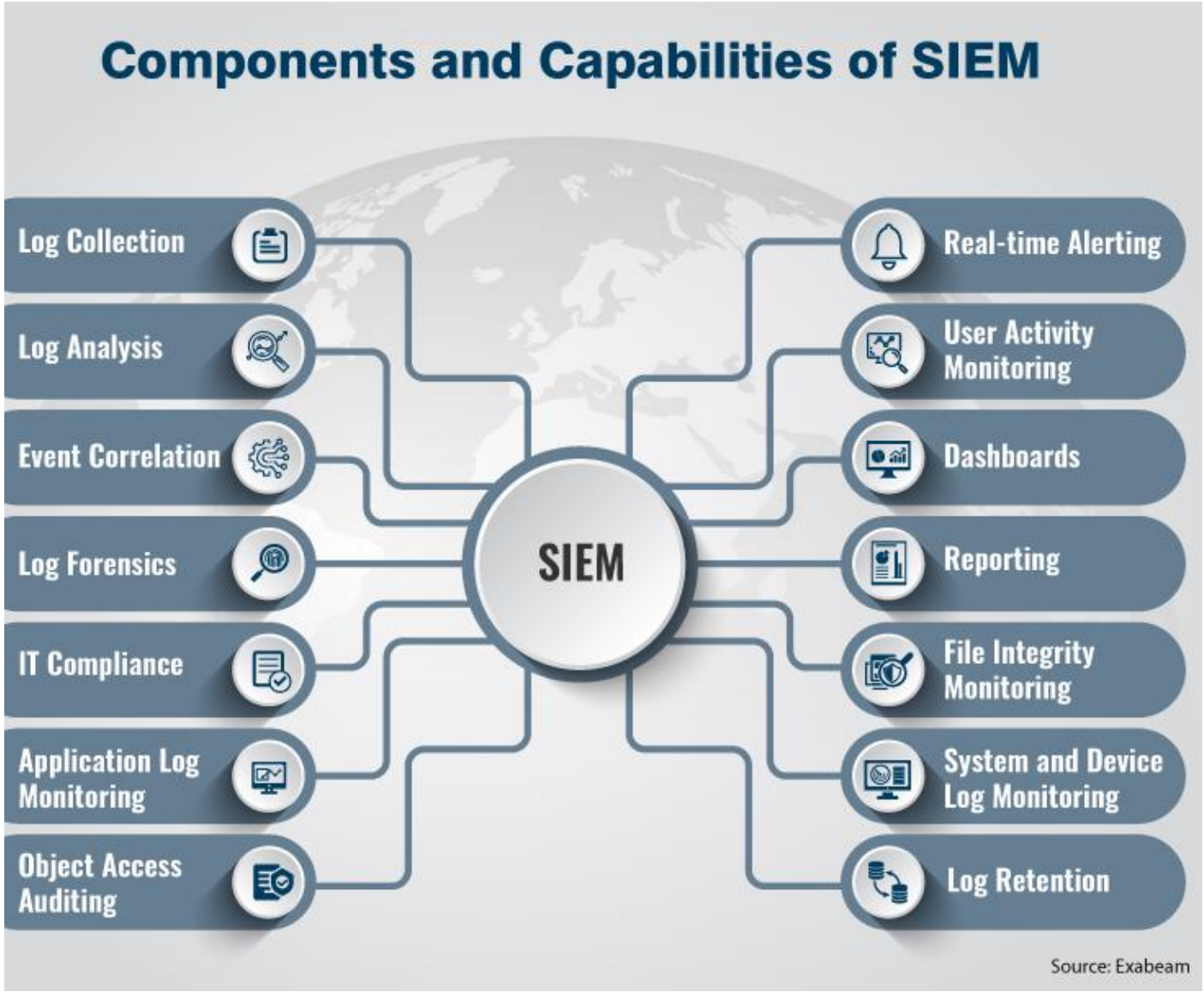
- Security devices
- Network devices
- Servers
- Applications



Source: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

Components and Capabilities of SIEM

- **Data Aggregation**
- **Threat Intelligence Feeds**
- **Correlation between Events and Monitoring**
- **Analytics**
- **Alerting**
- **Dashboards**
- **Compliance**
- **Log Retention**
- **Forensic Analysis**
- **Threat Hunting**
- **Incident Response**
- **SOC Automation**

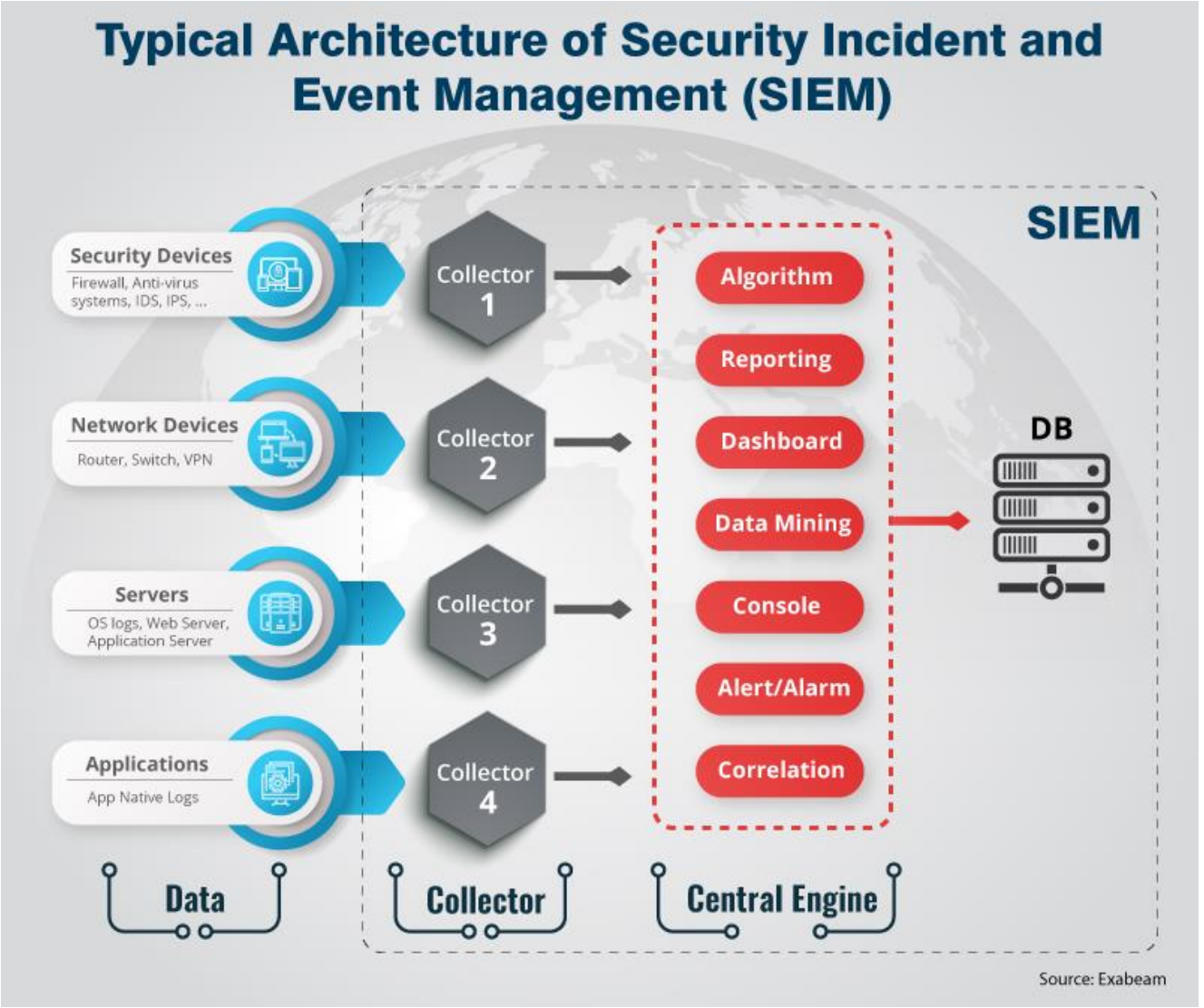


Source: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

Data Aggregation

In the context of SIEM, data aggregation is the process of gathering data from numerous organizational systems (security systems and network devices).

Each device compiles a log file containing all the activities of the device; these activities are referred to as events.



Source: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

Data Aggregation Examples

- Collects / receives logs (from any source):
- UDP, TCP, FTP, SFTP, SNMP, syslog, r-syslog, syslog-ng

- Windows logs (security, application & system) :
- Binary & captive – logs must be liberated & converted to text
- Options include agent push, server pull.

- Linux, Unix, AIX, & network equipment:
- Syslog – Messaging structure, payload agnostic
- Emergency, alert, critical, error, warning, notice, info, or debug
- Most applications write logs to EVT [X] / syslog

- Other applications write logs to:
- Database table
- Text or XML in folder or directory

Threat Intelligence Feeds

Under this, your SIEM system will have a combined data of internal logs and third-party artifacts, which is primarily focused on learning from your firm's access on how to improve your existing threat awareness and response system.

This component is usually focusing on only one area of interest and delivers the report online.

Source: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

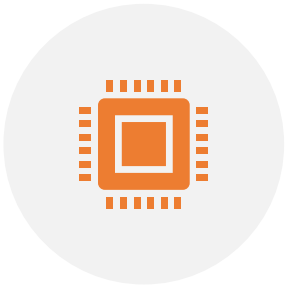
Correlation between Events and Monitoring

The event correlation is an essential part of SIEM. It makes it possible to detect threats and abnormal pattern of activities that can go unnoticed and eventually lead to compromised data.

It first collects data related to security from various network devices, security devices, servers, and applications. Then it would go ahead with the research of your firm’s security environment. On the basis of the gained information, it will then draft correlation rules to identify malicious threats.

Source: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

Analytics



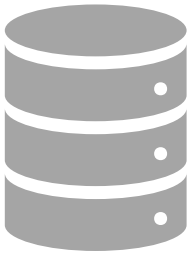
As deploying the SIEM solutions are quite challenging, that is why most organizations are looking for machine learning as one of the features in the security analytics of SIEM solutions.

Technologies, such as machine learning and statistical models, are used under security analytics to build a deeper connection between various data elements.

Source: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

Alerting

This capability of the SIEM solutions is responsible for the automated analysis of events, which sends alerts to the concerned security team for notifying them about the immediate issues.



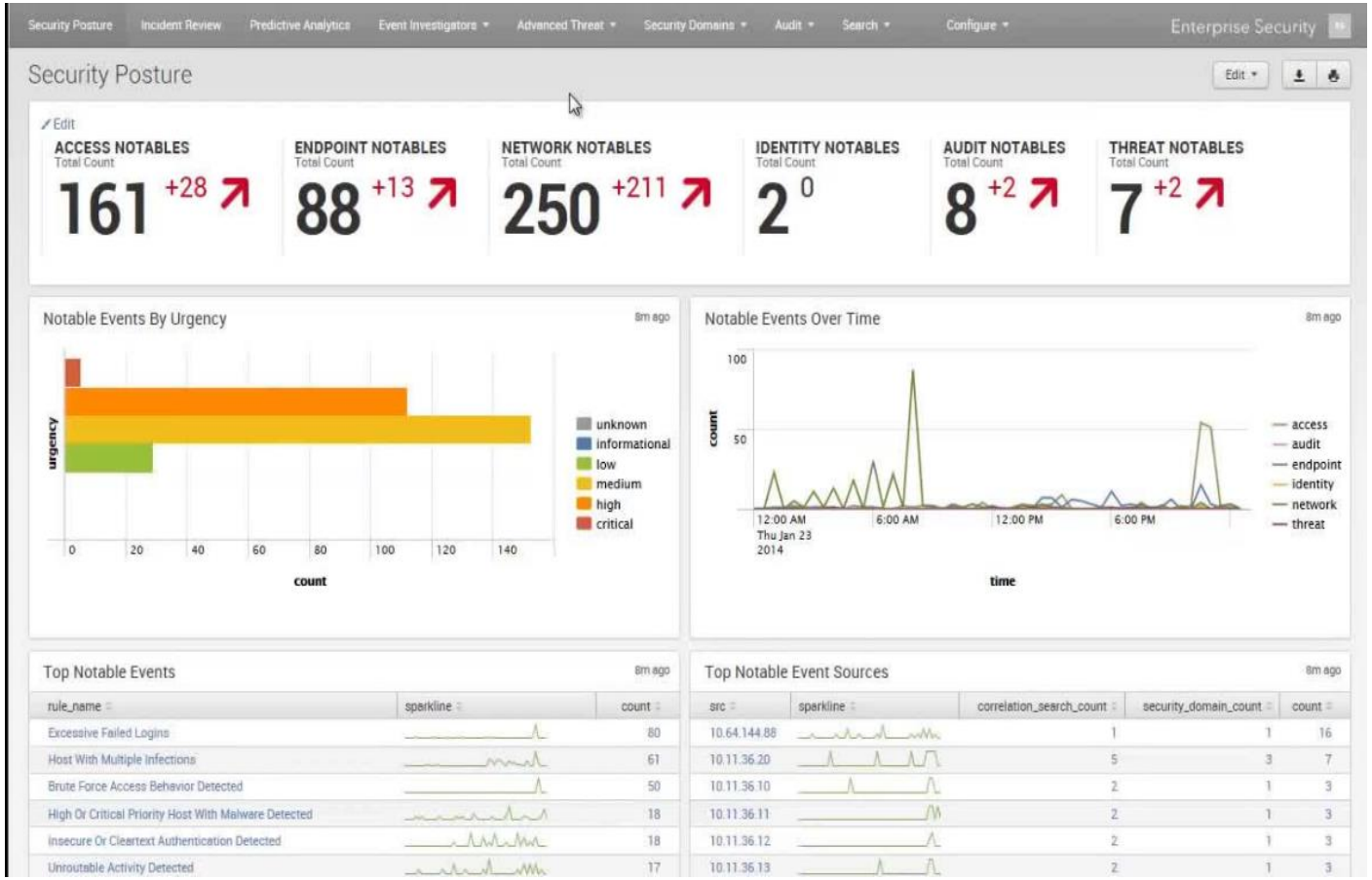
These events can be set up on various data points, such as during data aggregation phase or the event correlation phase. The real-time working of this capability can eliminate the threat as quickly as possible.

Source: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

Dashboards

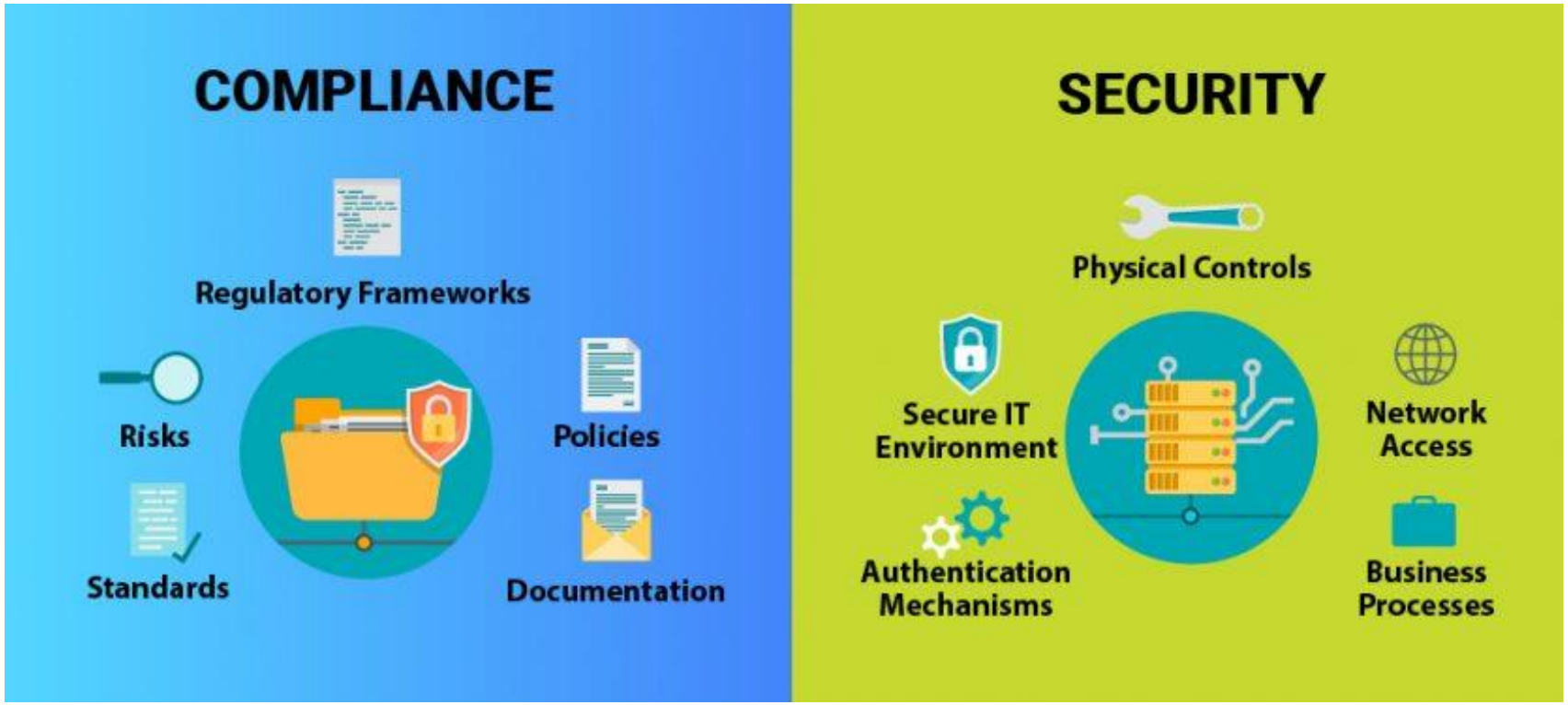
Dashboards offer tools to convert event data into charts based on the data that are not by the regular patterns.

This helps the security team to identify trends and anomalies with the help of an informational visualization of the processed data.



Source:

https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/



Compliance

SIEM can generate reports that comply with standards, such as HIPAA, PCI/DSS, HITECH, SOX, and GDPR.

It merely states that the gathering of the compliance data can be automated with the help of applications. This data can then be used to generate reports that will be adaptable by the existing security system, governance, and auditing processes.

Source:
https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/
https://phoenixnap.com/blog/security-vs-compliance

Log Retention

Large-scale organizations generate a high volume of logs every day. In such a case, industry standards, such as PCI DSS, HIPAA, and SOX, demand these logs to be retained within a period of 1–7 years. Though storing historical logs for long-term is generally used in compliance and forensic purposes. SIEM ensures that which logs can be retained for further use. To reduce the high-volume storage of these logs, SIEM uses the following strategies:

Syslog servers—normalizes logs to retain only required data in a standardized format

Deletion schedules—Old logs get eliminated, which are no longer needed for the compliance purpose

Log filtering—Required logs are filtered based on their source system or any other rules as defined by the SIEM administrator

Summarization—Summarization of logged data to manage only the data that are essential for compliance and forensics (eg: distinct IPs, event counts, etc.)

Source: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

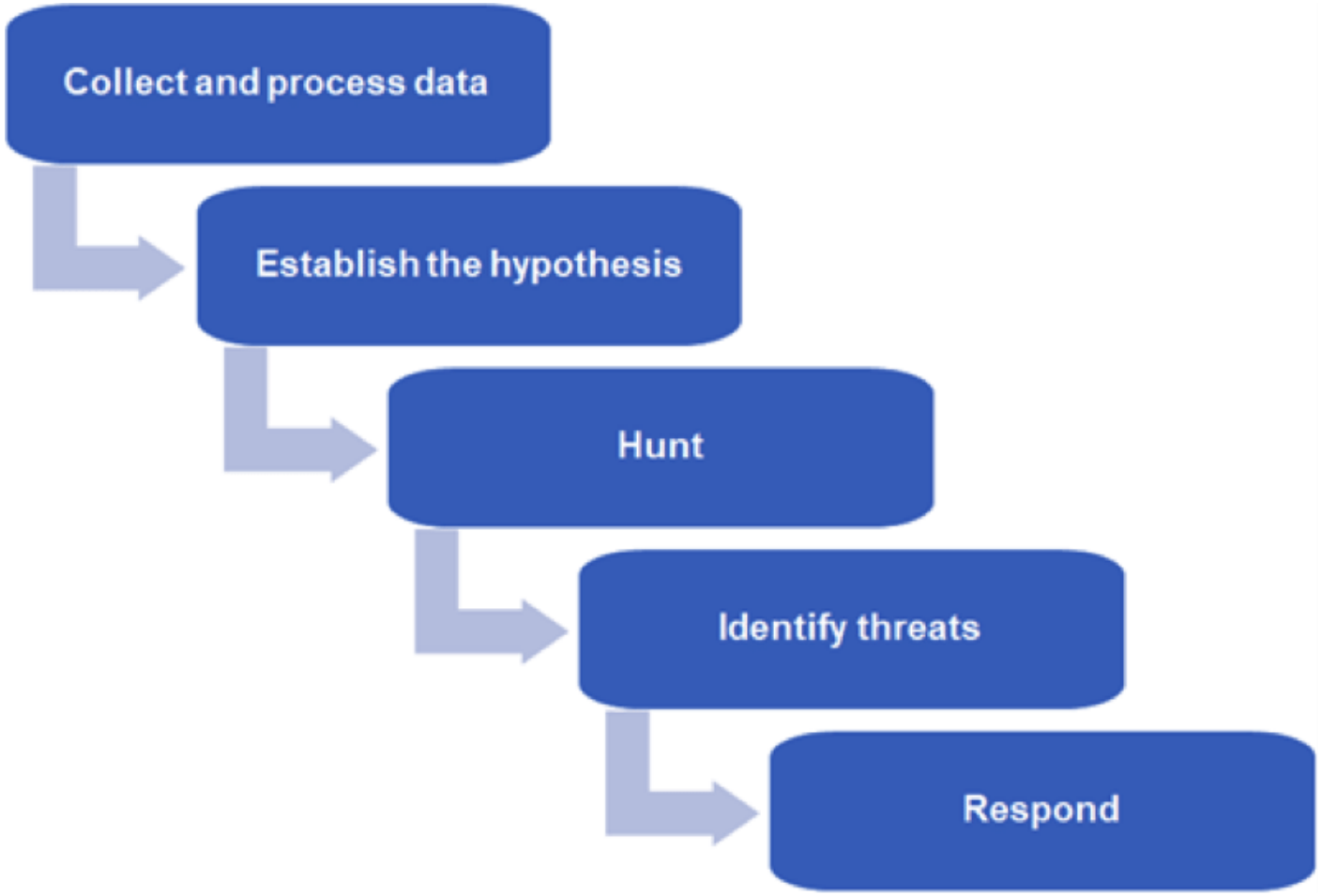
Forensic Analysis

The forensic analysis uses logs and event data to investigate a security incident.

It is the process of in-depth analysis of the stored data to discover the details to reconstruct the entire incident. This complete process helps in finding the source of the incident, its scope, and a lot more.

Source: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

Threat Hunting



For uncovering threats, the concerned team members have the authorization to run queries on the logs and event data.

Automated security workflows can accelerate this process to reveal malicious threats and to make them stop from damaging the network or systems.

Source:
https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/
https://resources.infosecinstitute.com/category/enterprise/threat-hunting/#gref

Incident Response

The data collected through SIEM helps Incident Response team to identify the attack and respond to them as quickly as possible.

Without the logs and event data, the IR team will need extra time to evaluate the data that are efficiently done by SIEM.

Source: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

SOC Automation

With the help of advanced SIEMs, it is now possible to automate the IR.

But for this, it is required that the security systems are orchestrated, which is, in general, termed as *Security Orchestration, Automation and Response*.

Source:
https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/
https://www.slideshare.net/cisoplatform7/a-fully-automated-soc-fact-or-fiction