SOC:

Challenges :

Integration part. Difficult to achieve

Is the skills of the Engineers working on that ?

SOC Brain of security. It requires it requires people of equal calibre. Gud amount of people require to run a SOC.

**REQUIREMENTS FOR AN EFFECTIVE SOC**

factors affecting an SOC have different aspects: human resources, processes and technologies.

## Human resources:

Perhaps the most important resource for the success of an SOC is its staff. Unfortunately, there is often a lack of qualified specialists – a deficiency generally countered with continuing education and training, but also with technical resources (automation and orchestration, machine learning, artificial intelligence). Although the resources currently available are very effective and constantly becoming more powerful, they cannot (yet) replace human abilities altogether. Therefore an adequate number of qualified specialists are required, usually two to three at minimum.

ISOC staff requires expertise and continuous training in the following areas:

• Operating systems

• Multiple hardware platforms

• Networking systems (routers, switches, firewalls) and protocols

• Directory systems

• Database technologies

• Applications for corporate and OT domains

• Power system protocols

• Malware analysis

• Intrusion detection and prevention systems

• Programming or scripting

• Investigative/forensics processes

• Chain of custody issues

• Ethics

• Corporate policy.

Processes:

the SOC is a service center that works in close contact with its customers. The processes are extremely important, must be clearly defined and most importantly they must run smoothly in a crisis situation.

The key processes relate to the following areas:

* Processes for escalation to management as well as to the legal, compliance and HR divisions
* Bringing in support, be it internal departments outside of the SOC or third-party experts, e.g. in special areas like forensics or malware analysis or for incident management in general
* An enterprise risk management interface.
* In-house and external communication processes and the corresponding maintenance of a comprehensive communications matrix with all of the necessary contact information
* Threat modeling, i.e. preparing threat models specific to the organization and situations
* Monitoring, triage and alerts based on this modelling.
* Procedures for the analysis of incidents and their classification according to impact and urgency.
* Incident handling, i.e. how the SOC responds during an actual security incident
* Restoring normal operations.
* Ensuring seamless traceability of SOC processes.

The threat models make it possible to answer the following questions:

* What threats are relevant to the organization?
* What kinds of precautions are required?
* How do these threats manifest from a technical standpoint?
* How, and with what tools, can the SOC detect these threats?
* How can such attacks be prevented or neutralized?
* What precautions can be taken?

5.2 Key Process Areas for an ISOC

ISOC operations are heavily process dependent. ISOC processes identify roles and

responsibilities, required resources, action steps, escalation criteria, and reporting requirements.

5.2.1 Key ISOC Processes

ISOC performance is process oriented. Developing and maintaining appropriate processes will

allow measuring and improving the ISOC performance. Key ISOC processes include:

• Event log monitoring

• Notification

• Escalation processes

• Daily ISOC watch and watch turnover

• Shift logging

• Incident logging

• Compliance monitoring

• Reporting

• Incident investigation.

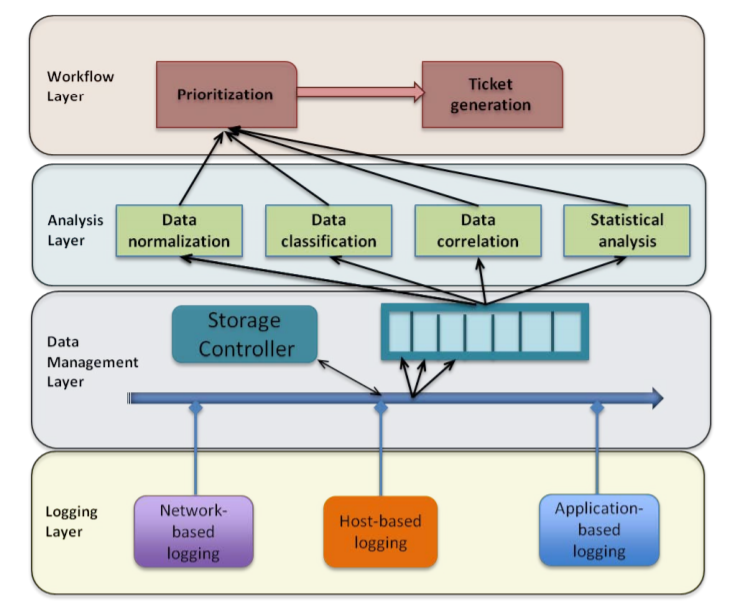
## Technologies:

The most important technical realms of an SOC are:

* A **platform with security information** (security intelligence)
* Tools for the **investigation and analysis** of incidents
* A complete, current list of all IT components (asset database), including the relevant responsibilities and contact information. Systems can only be protected if their existence is known in the first place.
* A system for **recording, managing and documenting** security incidents and the corresponding processes (incident management system)

The information platform is usually a classic SIEM or at least offers some of its features, but it might also be a well-configured log management system with the right monitoring rules. What is important here is to integrate as many relevant information sources as possible from across the entire organization, but most certainly the following:

* Security-related activities at all endpoints, i.e. not only the users’ workstations
* Security-related activities on the network (network traffic, firewall logs, proxy logs, vulnerability scans, etc.)
* Authentication and authorization processes (LDAP, Active Directory, VPN, etc.)



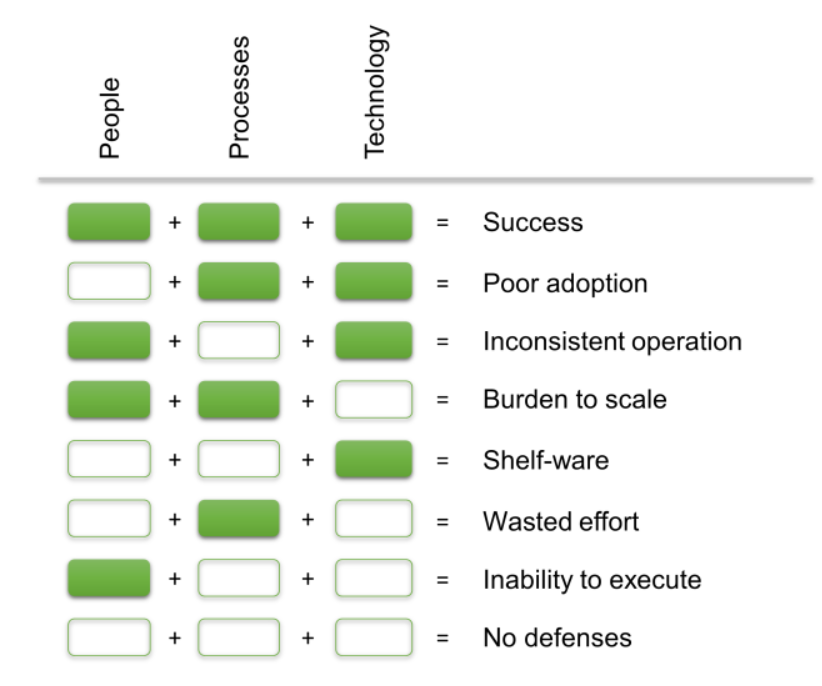
A single **SIEM** server receives log data from many sources and can generate one report that addresses all of the relevant logged security events among these sources.

(forcible entry )Intrusion detection and prevention systems (IDS/IPS) alone won't be able to detect or prevent malware like this, which is why a **SIEM** is so **essential**. Additionally, **SIEM** solutions are able to aggregate data from across your entire network, and analyze this data together to limit false-positives

## What is a SIEM solution?

**A SIEM solution consists of a number of components involved in Security Information Management (SIM) and Security Event Management (SEM) including the following:**

* **Data Aggregation**
* **Threat Intelligence**
* **Security Event Correlation**
* **Advanced Analytics**
* **SOC Automation**
* **Dashboards**
* **Threat Hunting**
* **Forensics**
* The graphic below highlights the impact of any shortfalls:



### 1. Define project and requirements

The first step to launching a SIEM implementation process is planning the project’s timeline. This involves outlining the scope of the project along with its necessary informational, budgetary, and physical resources. Here, companies should define their goals and identify all necessary resources.

Most companies have similar goals, all of which relate to building a network security management system centralized at the point of a new SIEM. Businesses need to set basic rules, identify necessary compliance and policy requirements, and structure their post-implementation SIEM management plan.

SIEM products require connections to virtually all of your network infrastructure and software assets for optimal performance, so defining log sources is a good place to start. Logs come from different locations throughout your company's network.

These are some basic components that most companies include while scoping their SIEM requirements and log sources:

**Security control logs**

* [**Intrusion detection and prevention systems (IDPS)**](https://www.g2.com/categories/intrusion-detection-and-prevention-systems-idps)
* Intrusion detection and prevention systems (IDPS) are used to inform IT administrators and security staff of anomalies and attacks on IT infrastructure and applications. These tools detect malware, socially engineered attacks, and other web-based threats. IDPS also provide preemptive intrusion prevention capabilities for internal threats and potentially compromised systems.
* Intrusion detection and prevention systems monitor systems for abnormal behavior and potential vulnerabilities that can leave a business susceptible to cyberattacks. Companies choose to adopt these to protect their sensitive business information and ensure their computing infrastructure performs as needed.
* [**Endpoint protection software**](https://www.g2.com/categories/endpoint-protection):
* Endpoint protection software provides security solutions to oversee and manage devices that have access to a company’s or person’s private network. These software tools protect against a number of security threats and attempt to normalize security measures across multiple devices.
* [**Data loss prevention (DLP) software**](https://www.g2.com/categories/data-loss-prevention-dlp)
* Data loss prevention (DLP) software, also known as data leak prevention software, is used to secure control and ensure compliance of sensitive business information. A key component of DLP solutions is distribution control, which ensures users do not send private information outside of corporate business networks. Security staff and network administrators set business rules that determine who can view, change, and share confidential data. DLP tools often control data on both the network and endpoint level to ensure policies remain consistent across the company. These tools are used to ensure the protection of data and prevent leaks by internal sources.
* [**Threat intelligence software**](https://www.g2.com/categories/threat-intelligence):

# Best Threat Intelligence Software

Threat intelligence software provides organizations with information related to the newest forms of cyber threats like zero-day attacks, new forms of malware, and exploits. Companies utilize the tools to keep their security standards up to date and fit to combat new threats as they emerge. These tools can improve security performance by providing information on threats to their specific networks, infrastructure, and endpoint devices

* [**Firewalls**](https://www.g2.com/categories/firewall)
* A **firewall** is a system designed to prevent unauthorized access to or from a private network. You can implement a **firewall** in either hardware or software form, or a combination of both. **Firewalls** prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets
* Honeypots
* A **honeypot** is a **security** mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities so you can study them to improve your **security** policies
* Web filters
* A **Web filter**, which is commonly referred to as "content control software", is a piece of software designed to restrict what websites a user can visit on his or her computer. ... However, they can also be installed on the network side, either by an ISP or a business, to restrict the **Web** access of multiple users at once.

**Network infrastructure logs**

* Routers
* It connects different networks together and sends data packets from one network to another.

a router connects multiple switches, and their respective networks, to form an even larger **network**.

* [Routers](https://www.cisco.com/c/en/us/solutions/small-business/networking/routers.html) guide and direct network data, using packets that contain various kinds of data—such as files, communications, and simple transmissions like web interactions.
* Switches:

switch connects multiple devices to create a **network**Controllers

* Servers
* Databases
* Internal applications

**Other data points**

* Network architecture
* Network policy configurations
* IT assets :

s/w or h/w