FINAL YEAR PROJECT - 2

Final Solution Paper

Muhammad Muneeb Qureshi
BSCS/1-18/M01021

Understand and apply Security concepts

Security management concepts and principles are inherent elements of a security policy and solution deployment. They define the basic parameters required for a secure environment.

They also define the goals that policy designers and system implementers must meet to create a secure solution.

Confidentiality, Integrity, and Availability (CIA) (i.e., the CIA triad) are often viewed as the primary goals and objectives of a security infrastructure.

Security controls are typically judged on how well they conform to these three core information security principles. Vulnerabilities and risks are also rated according to the threat they pose to one or more of the CIA's triad principles.

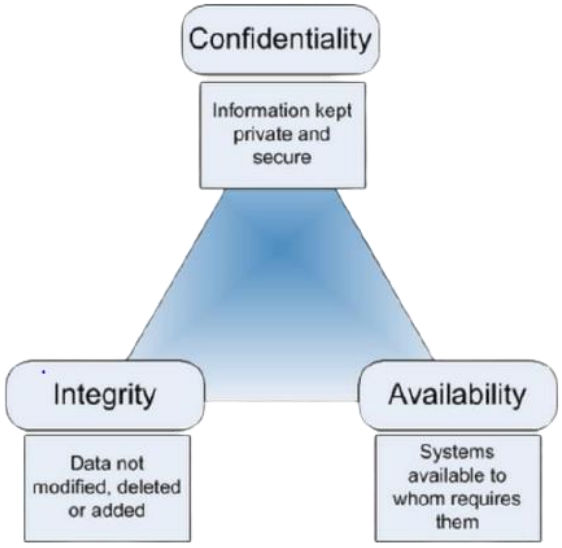


Figure: 1.1

Capstone of Information Security – People, Process & Technology

As an IT or information security professional, one cannot read a blog, book or article without coming across these three words. people, processes, technology.

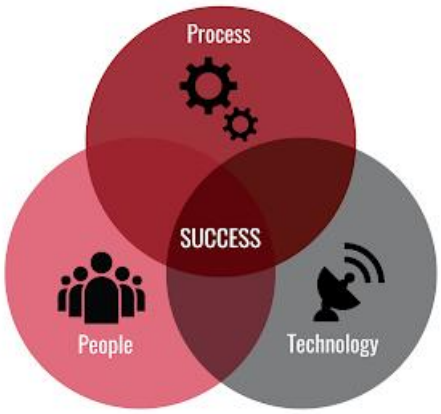
Popularized in the InfoSec world around the turn of the century by Bruce Schreier, these three names have been central to all ITIL practices since their inception in the 1980s, and emerged in conjunction with Harold Leavitt's theoretical diamond model. 1965 (with organizational tasks as the fourth component).

It is also known as the "Golden Triangle", the 3 keys to successfully implementing project and organizational change and a fundamental approach to solving complex business problems.

The reason for this triangle approach lies in a very important fact:

- ✓ Doing this effectively in any organization requires an approach that optimizes the relationships between people, process and technology.
- ✓ Focusing on one or two areas creates an imbalance. You (Employers) are wasting a lot of money and time, and your best employees are looking for work elsewhere.
- ✓ Take new technologies for example, many companies believe that by implementing a shiny new tool, all their problems will go away.

What they don't see, however, is that technology is only as good as the processes around it, and the processes only as good as the people running them.



Service Models

Just as delivery models play an important role in cloud computing, service models are also an important consideration. The service model that a cloud conforms to determines an organization's reach and control over the computing environment and characterizes a level of abstraction for its use. A service model can be updated as a public cloud or as one of them

other deployment models. Three well-known and commonly used service models are:

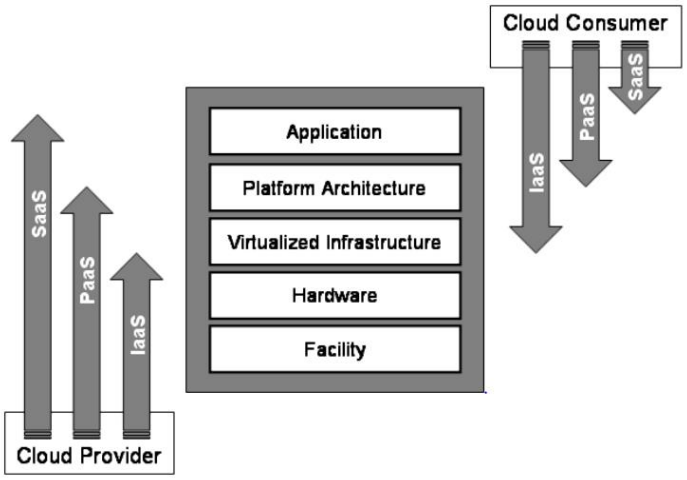
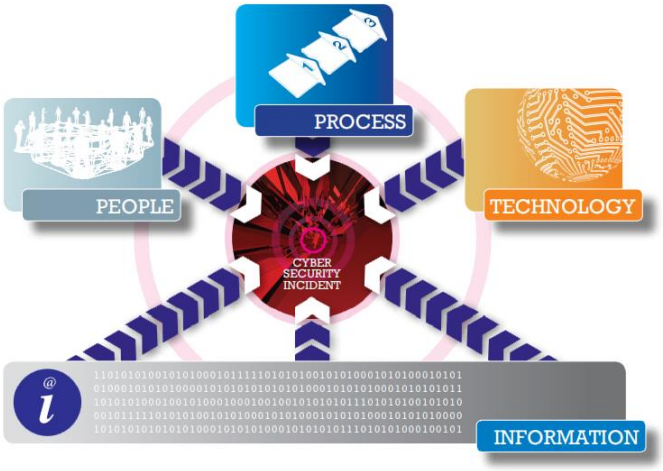


Figure 1: Differences in Scope and Control among Cloud Service Models

It illustrates the differences in scope and control between the cloud customer and cloud provider for each of the service models discussed above. Five conceptual levels of a general approach
Cloud environments are identified in the base diagram and apply to public clouds and all other deployment models. Arrows to the left and right of the chart indicate the approximate reach of cloud providers and cloud customers and control over the cloud environment for each service model. In general, the higher a cloud provider's support level, the more limited the cloud customer's reach and control over the cloud system.
Likewise, the platform architecture layer includes compilers, libraries, utilities, middleware and other software tools and development components required to deploy and deploy applications.
The application layer represents deployed software applications intended for end-user software clients or other programs and made available through the cloud.

People, Processes, Technology and Information

Each SOC must be supported by the right combination of people, processes, technology and information, as shown below.



Main considerations for each phase of the cyber security monitoring and logging process

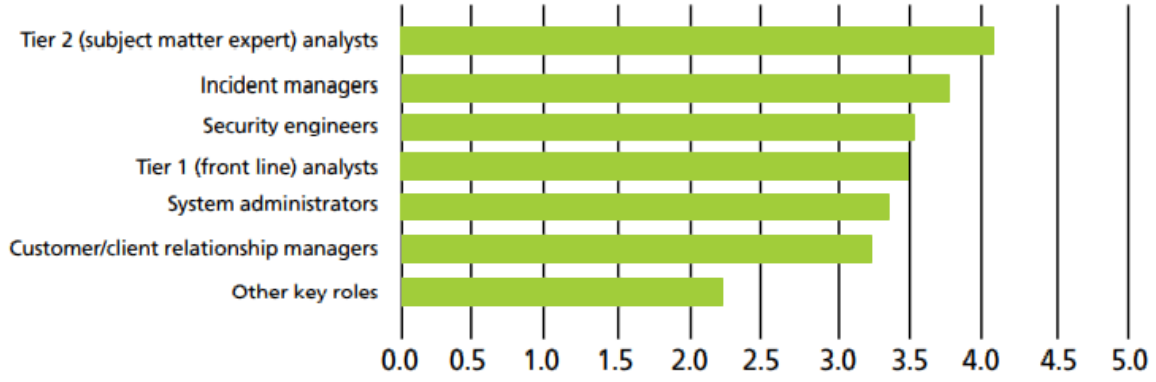
In a realistic scenario, participants identified how four different types of people in the SOC (there may be more roles) typically use processes, technology and information to help them fulfill their roles effectively. The results of this analysis are presented in the table below, which illustrates how processes, technology, and information support different roles (shown in the People column).

People	Process	Technology	Information
Technical delivery Manager (SOC Manager)	• Reporting • Customer relationships • To gather information • Observance	• Reports • Analyze • Compliance	
Frontline Analysts (L1)	• Event filtering • To gather information • Monitor warnings/alerts • Escalation of warnings/alerts • Ticket management	• File management tools • SIEM tools • Ticketing • Database • Customer relationship management (CRM)	• Customer • Active • Warnings • Alerts • Events

	• First contact with the customer	• Configuration Management Database (CMDB)	
Second Line Analysts (L2)	• Incident Assessment • Trend analysis • Root cause analysis • Thorough investigations • Escalation to third-line analysts • Incident lifecycle management • Alarm Settings • Creation of statistics • Contact with important assets	• Threat Intelligence	• Customer • Active • Warnings • Alerts • Events • Customer Profile • Front line evidence
Third Line Analyst (Very technical, incident response; L3)	• Host intrusion analysis • Malware Scan • Network intrusion analysis	• Specialist tools	
SOC Administrator	• SOC Process • Team management • Creation of SOC statistics • Career Development • SOC PPTI Validation • Climbing point • Capacity Management • Observance	• Ticketing • Reports • Troubleshooting • HR systems • Tools for metrics	

People

Most respondents place a high value on the different types of people employed by SOCs, as can be seen from the table below.



Types of people employed in Security Operations Centers (SOC)

"A good analyst can detect weak and slow abnormal events"

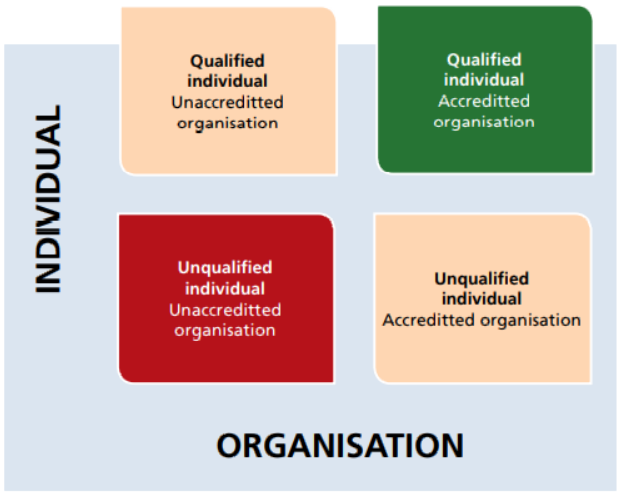
SOC professional qualifications

For a variety of technical security services, such. There are many different professional qualifications available, such as penetration testing and responding to cybersecurity incidents. However, few, if any, are available for deployment by security operations centers or the analysts they employ.

Analysis of the responses to the project surveys showed that the SOC (and NOC) service providers received strong support for professional qualifications, accreditation and a code of conduct, as shown by the high average responses in the table below (scores are given as a rating of 1 until 5).

Requirements	related to SOC	related to the NOC
Have professional certification (similar to those used by CREST for penetration testing and cybersecurity incident service providers)	3.73	3.41
Employment of people with professional qualifications	3.67	3.26
Are supported by a professional code of conduct (e.g., to obtain guarantees about the quality and integrity of the services provided and to carry out an independent problem-solving process).	3.52	3.24

The optimal combination is shown in the green box in Figure 10 below. It's the only combination you specify with a noticeable level of protection in case something should go wrong and also reduces the chances of something going wrong first place.



Combinations of accreditation for organizations and the individuals they employ

Project research has shown that specific qualifications and learning options are available (e.g., SANS) that should be examined and contextualized.

Work is currently underway (with support from the UK Government) in higher education to develop learning and development pathways that result in people being better qualified and sufficiently qualified to work in NOCs and SOCs.

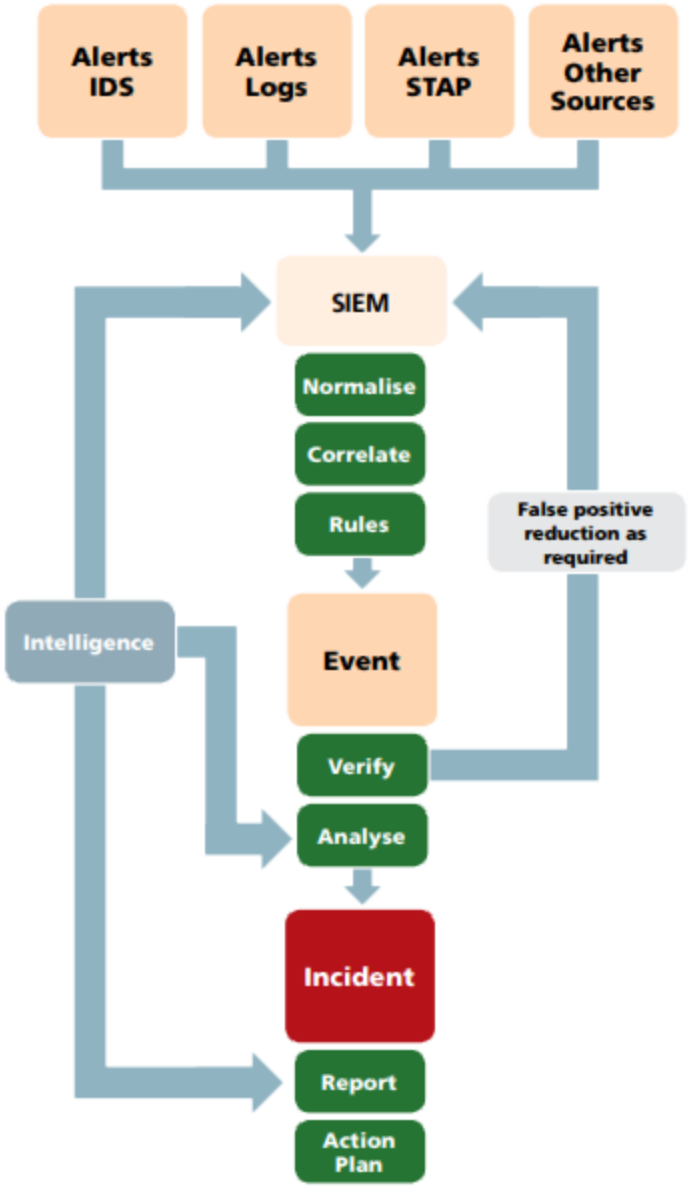
Process

SOCs are typically supported by different types of processes for different purposes, such as: e.g.:

- Operational (including call center, case management, event management, supervision, personnel management, triage)
- Analytics (e.g., event analysis, incident response, reporting, investigation, threat intelligence)
- Business and Technology (including access management, architecture, compliance, BCP, process improvement, usage situation).

The process of event analysis.

Many SOCs use a workflow approach to manage relevant events from multiple sources. Events are categorized, prioritized and reviewed by a designated analyst according to a defined process as shown in Figure below.



The event analysis process

"Sometimes you have to let analysts be hunters to look for anomalies"

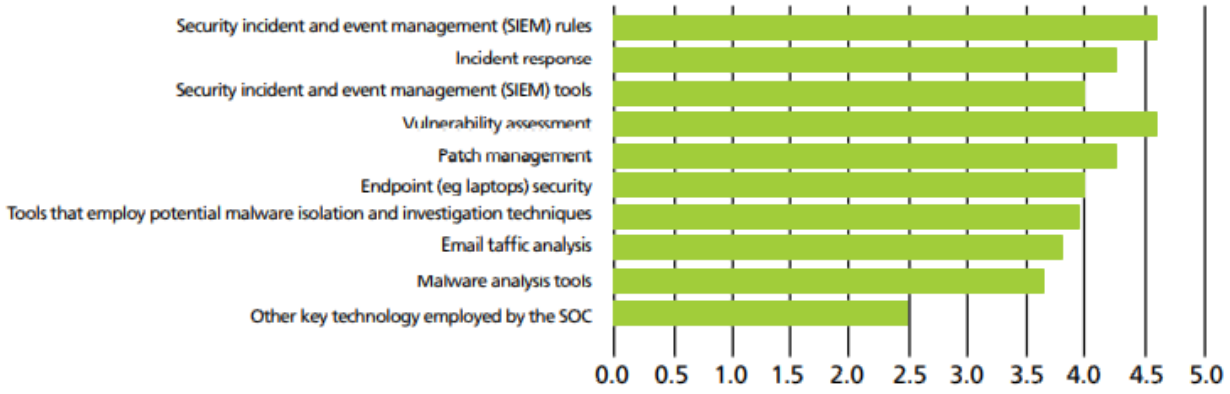
Technology

Each SOC is supported by a suite of tools and other technologies, typically focused on a good (commercial)SIEM engine.

The majority of project survey respondents value all aspects of SOC technology as shown

table below.

How much value would you place on each of the following types of technologies used in Security Operations Centers (SOCs)?



SIEMs received the highest rating of any SOC technology from project survey respondents, which is not surprising given that they are at the core of nearly all SOCs.

"You can do a lot more with free tools if you invest more in people than in commercial products"

Cybersecurity and logging approaches

Project research evaluated many different ways to conduct cybersecurity registration and monitoring. that

The advantages and disadvantages of each approach are listed in the table below.

Approach	Advantages	Disadvantages
cloud and device based/software as service provider	• Costs • Observance • Good for small businesses • Elementary • Easy to deploy	• One size doesn't fit all • Inflexible • Compliance is not about security • Not integrated into internal processes • No knowledge/context of their surroundings • Technically oriented: Reports, but fewer analyze deeply
Shared/MSSP – (Obtained from a network service IT provider/service subcontract)	• All-in-one service in addition to the existing contract • Costs are often built into the existing budget • Cost-benefit compared to internal • Delivery capability around the clock or "follow the sun" Services	• Less emphasis on security, second Priority for availability/SLA etc. • Conflict of Interest • Issues with multi-tenancy sharing • Security is not a core competency of MSSP • Loss of business context
Shared/MSSP – (Obtained from a managed security Service provider)	• Security Experts • 24/7 support and continuity • Integrated solutions and scenarios (e.g. incident response)	• Costs may increase due to the need for specialists • Vendor/Solution Ban • Additional OPEX costs • Loss of context and commercial orientation • Lack of internal flexibility evacuated prisoner
Captive Outsourced (Hybrid model)	• Keep solution option • Custom SLAs • Separate choice of service and solution provider	• More expensive than mini MSSP
Inhouse/ in-sourced a service	• More control • Integration into operations • Better knowledge of the company • Choice of software/hardware solutions • Custom SLAs • Less privacy issues	• Possible loss of efficiency • Responsibility for routine updates and Software/Hardware Maintenance • Ongoing maintenance obligation capacity and investments • Higher cost (usually) • Employees/Skills/Retention • Lack of global "visibility" • Supervise personnel for other duties

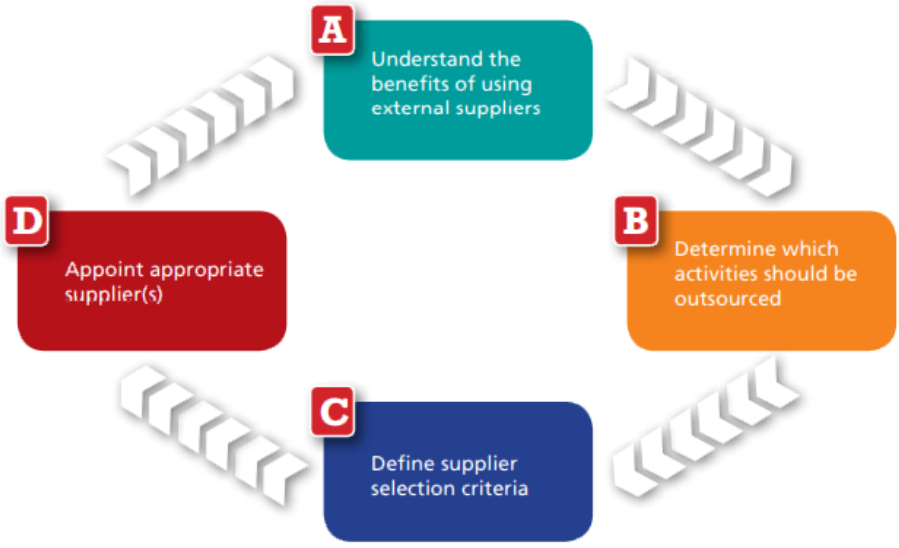
The supplier selection process.

If your organization decides to hire a third-party cybersecurity monitoring and logging service provider, regardless of:

This raises many questions that you need to answer, such as:

- What kind of service do I need?
- How many services do I have to buy?
- Who did I buy it from?
- How much is it?
- What should I look for in a potential supplier?

Therefore, a systematic and structured process has been developed to support you in selecting a suitable supplier, as shown in Figure below.

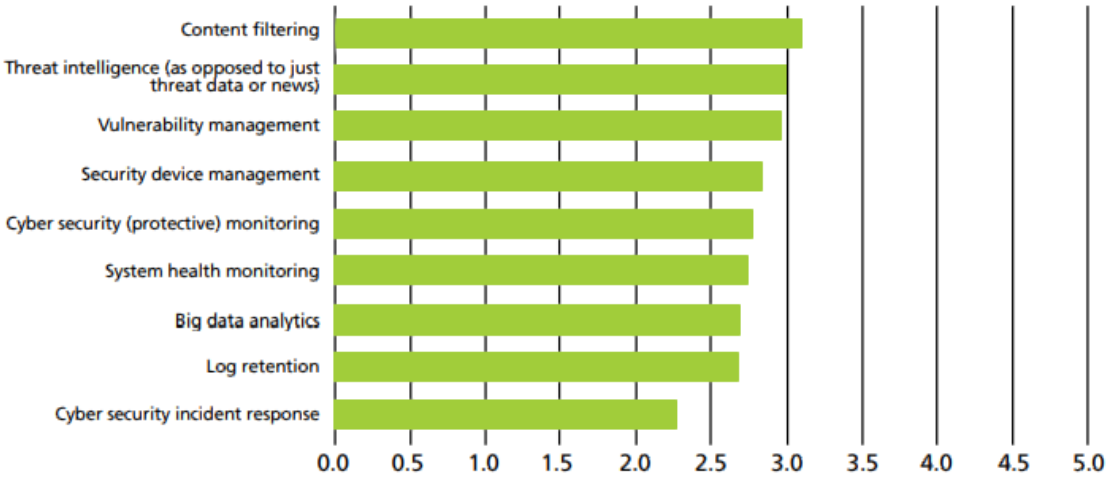


The supplier selection process

Determine which activities should be outsourced

Follow-up activities as indicated in the table below:

To what extent would you consider outsourcing the following to cybersecurity monitoring and logging providers?



Most businesses need professional help with cybersecurity logging and monitoring proactively. However, it is very difficult for them to identify reputable organizations that have access to qualified and competent professionals and experts who can respond appropriately while protecting sensitive business information and attacks.

Summary of the main results

This has brought together all aspects of cybersecurity monitoring and logging in one place and highlighted what it is

General best practices for each major component. Explain how your organization:

- Capture the most relevant cybersecurity events and correlate them with appropriate logs covering a wide spectrum.
- Document management challenges.
- Establish an appropriate cybersecurity monitoring process to help identify and analyze indicators of compromise (which may be caused by actual or potential cybersecurity incidents); and respond to cybersecurity anomalies events quickly and efficiently.

- Establish appropriate logging and monitoring capabilities for cybersecurity, considering the benefits of using a Security Operations Center (SOC).
- Find the right cybersecurity monitoring and reporting tools, processes, and people to help you easily, effectively, and efficiently at the right price.

The general process is described below;

a. Develop a cybersecurity logging and monitoring plan

The workshop participants identified what a perfect cybersecurity monitoring and logging scenario would look like, which can be broken down into four main categories as shown in the table below:

Approach	Advantages
Clear goal	• Set yourself clear goals: Be aware of what you want to achieve yourself • Identify the benefits of cybersecurity monitoring and logging

	• Know your own organization/environment.
Risk-based and process-based approach	• Adopt a risk-based approach to cybersecurity monitoring and reporting • Information on cybersecurity risks and recent incidents related to risk assessments • Business process-based assessments • Use a simple process approach • Strong fundamentals of cybersecurity monitoring and logging.
More targeted threat analysis	• Tools to handle logs correctly • Understand normal system/network behavior • Quick access to threat source data • Integrated and actionable threat intelligence/news/intelligence • Good KPIs that can provide meaningful ROI data. • Best Resources • Investing in people's skills • Integral part of the SLA (both internal and external) • Longer term time/resources to build partnerships with cybersecurity monitoring and logging providers.
Better Resources	• Investing in people's skills • Integral part of the SLA (both internal and external) • Longer term time/resources to build partnerships with service providers for cybersecurity monitoring and logging services.

b. Meet cybersecurity monitoring and logging requirements

c. Identify sources of potential indicators of compromise

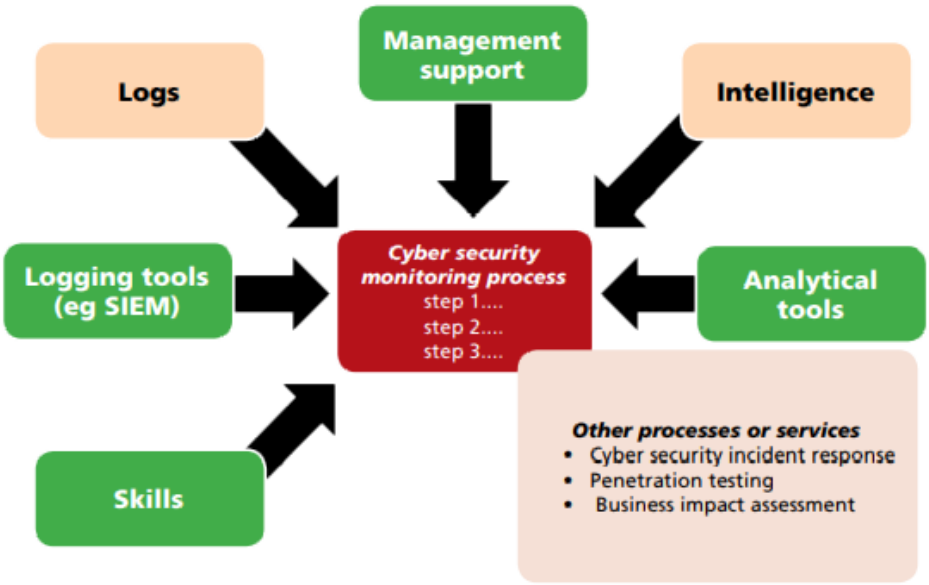
Cyber security monitoring – key components

d. Build or buy cybersecurity monitoring and logging services

The process is designed to help you select suitable providers as shown in below:

The supplier selection process

e. Build capacity in your cybersecurity framework



Cyber security framework

f. Maintaining cybersecurity logging and monitoring capabilities

Focus area	Activities
Log Management	• Ensure organizations register cyber incidents and that records are kept correct and of good quality • Look beyond existing compliance rules (not just logging, logging the good things) • Log Analysis • Integration of new techniques/tools.
Incident Response	• Bring the attacker's mindset into the realm of defense against an attack • Use of new technologies in engagement activities • Promote best practices for incident response • Response times and methods.
Cybersecurity intelligence and situational awareness	• Use of Information Collected • Management of security assessments outside of SIEM • SOC developments intended to be used primarily as a refined SIEM tool • Integration of cyber threat intelligence into surveillance • True situational awareness.

The customer Experience	• Custom solutions for customer analysis: training/what is the best way to implement the solutions? • Valuation • Risk-based reporting and metrics; • Simplified interpretation for clients (i.e., reports easy to understand/less technical) • Maturity of managed security services and customer value, including: about reports.

Chapter# 01 - Introduction

Cloud computing provides for highly scalable consumer and enterprise applications with minimal or no capital investment. Security as a Service (SECaaS) allows organizations to employ a third party/ Managed Service Providers (MSPs) to manage operations and manage cybersecurity. Outsourced security solutions include services such as data loss prevention, antivirus management, security operations and intrusion detection. SECaaS is inspired by Software as a Service (SaaS). SECaaS allows a company's end users to use services such as authentication and helpdesk provided by this third party. By using a SECaaS provider, organizations benefit from the experience and innovation of a dedicated cybersecurity team that specializes in the complexities of preventing security breaches in a cloud computing environment.

Purpose

The purpose of this document is to present a detailed description of the Security as a Service [SECaaS]. It will explain the purpose, features, challenges, opportunities, and recommendations on national level to enhance a better appetite as per international practices.

Document Conventions

When writing this document, it was inherited that all requirements have the same priority. Document addresses foundation of information security amidst the almost overall functionalities of “Security as a Service” best practices and later on the detailed features have been discussed.

Intended Audience and Reading Suggestions

This document contains general and statistical information geographically about the” Security as a Service”, detailed functionalities and features, usage for organizations, and the rights assigned to these users. This document is intended for:

Business and IT professionals: Potentially, the C-level Executives Business (CEOs, COOs, CFOs) and IT professionals (CTOs, CIOs, CISOs) involved in cybersecurity decisions and product purchases.

Security Practitioners: Monitors, evaluates, validates and ensures the proper implementation of protective, corrective and detective controls within the organization.

Think Tanks: Think tanks (also called policy institutes or research institutes).

Security Engineers: In order to assure that the developers are developing the application exactly in manner to fulfill the requirement of the project.

Risk Managers IS Auditors/ IS Consultants: Cyber risk is a rapidly evolving and growing part of the general field of risk management.

Cybersecurity product vendors: Consultants who advise buyers of computer security products. Analysts serving investors and stakeholders in IT security companies.

Security Researchers: Explores and shares the emerging concerns.

Investors and financiers of IT security companies: Angeles, VCs, Private Equity, Investment Bankers, Private Offices and Corporate Venture Capital.

Chapter# 02 - Literature Review

SECaaS is a comprehensive solution that helps an organization to address any security problem without having its own security personnel. By outsourcing security needs, the organization can focus on generating more business instead of locking up its digital assets.

Today many of us work with computers, play with computers at home, go to school online, buy products from merchants around the world internet, we take our laptops to the cafe to read emails, we use our smartphones to check our bank balances and we track our exercises with sensors on our wrists. In other words, computers are ubiquitous.

While technology is changing at an ever-faster pace, much of the theory about how we can protect ourselves remains behind. Understanding the basics of information security will give a solid foundation for dealing with changes as they occur.

In this chapter, I discuss some basics of information security, including security models, attacks, threats, vulnerabilities, and risks. I'll also delve deeper into some slightly more complex concepts as I delve deeper into risk management, incident response, related managed services example security operation center (SOC) and defense etc.

The unexpected and unprecedented global pandemic of COVID-19 has brought about dramatic changes around the world. Due to the social distancing that has been put in place to contain the pandemic, remote working has become the new norm in many organizations. The prevalence of remote working has not only brought benefits to organizations, but also security risks. While telecommuting has been around for decades and many security-related issues have been explored by previous research, the researcher found no studies assessing workers' security awareness and concerns about telecommuting.

Given the critical importance of people's security awareness in protecting information security, it is necessary to know the state of security awareness in telecommuting. In addition, employees with low security awareness should receive training to improve the level of awareness. Therefore, this study aims to explore current awareness and concerns about telecommuting safety in organizations by conducting an employee survey. Through the responses to the survey, the researcher found that security awareness varies between groups of telecommuters of different ages, different sectors and organizations of different sizes.

Meanwhile, the researcher also found that the COVID-19 pandemic did not have much of an impact on people's safety concerns in telecommuting and managed security services environments.

Definition - Foundation of Information Security

In general, security means protecting your assets, whether from attackers entering your networks, natural disasters, vandalism, loss or misuse. Ultimately, it will try to protect itself from the most likely forms of attack as reasonably possible given its environment.

There may have a wide variety of potential assets that you want to protect. These can be physical assets with intrinsic value, such as gold, or items of value to your business, such as computer hardware. There may also have valuables of a more ethereal nature, such as software, source code, or data.

In today's computing environment, you will probably find that your logical assets (assets that exist as data or intellectual property) are at least as valuable as your physical assets (which are tangible objects or materials), if not more valuable. This is where information security comes in.

While technology allows us to access a large amount of information with a single mouse click also poses significant security risks. If information about the systems used by our employers or our banks is exposed to an attacker, the consequences can be truly disastrous. Suddenly, in the middle of the night, we were able to find the contents of our bank account that had been transferred to a bank in another country. Our employer could lose millions of dollars, face lawsuits and reputational damage as a result of a system configuration error that allowed an attacker to access a database of Personally Identifiable Information (PII) or proprietary information. These topics appear in the media with alarming regularity.

Thirty years ago, these gaps were almost non-existent, mainly because the technology was at a relatively low level and few people were taking advantage of it.

Information Security is defined as “the protection of information and information systems from access, use, disclosure, disruption, alteration, or destruction,” under United States law.

In other words, you want to protect your data and systems from those who want to misuse it, intentionally or unintentionally, or from those who shouldn't have access to it at all.

Safety must be worthwhile. Organizations don't have infinite budgets, so they need to spend their money wisely. Additionally, an organization's budget includes a percentage of money spent on security, just like most other business tasks and processes require capital, not to mention employee payments, insurance, retirement, etc.

It is recommended to choose the security measures that provide the best protection at the lowest resource cost.

Security must be legally justifiable. The laws of your jurisdiction are the backbone of organizational security. If someone invades your territory and breaches security, especially if such activity is illegal, their only recourse may be legal action response available to delete or close.

In addition, many decisions made by an organization have legal liability issues. When it is necessary to defend a security measure in court, legally backed security will significantly protect your business from large fines, penalties or allegations of negligence.

Security is a journey, not a destination. It's not a process that will ever end. It's not possible to fully secure anything because vulnerabilities are constantly changing. Our implemented technology evolves over time through users and adversaries discover bugs and develop exploits. What was sufficient yesterday may no longer be sufficient tomorrow. When new vulnerabilities are discovered as new attack vectors are discovered and new exploits are created, we must respond by re-evaluating our security infrastructure and responding appropriately.

Understand and apply Security concepts

Security management concepts and principles are inherent elements of a security policy and solution deployment. They define the basic parameters required for a secure environment.

They also define the goals that policy designers and system implementers must meet to create a secure solution.

Confidentiality, Integrity, and Availability (CIA) (i.e., the CIA triad) are often viewed as the primary goals and objectives of a security infrastructure.

Security controls are typically judged on how well they conform to these three core information security principles. Vulnerabilities and risks are also rated according to the threat they pose to one or more of the CIA's triad principles.

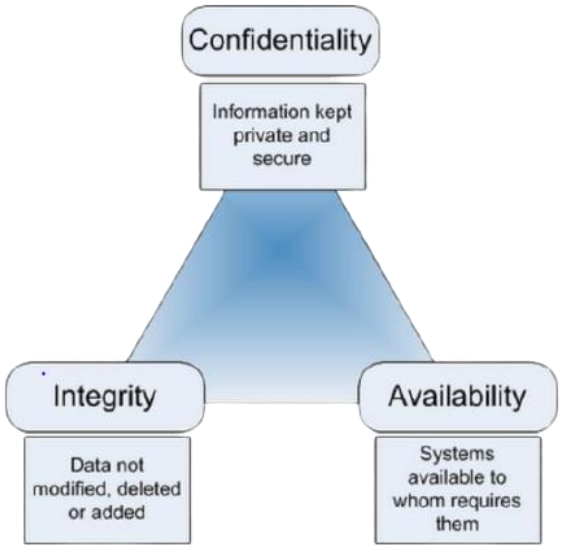


Figure: 1.1

Confidentiality - Disclose information to specific people. Data must be protected in all states (at rest, in progress, in motion):

E.g.: As an example, let's imagine that a person withdraws money from an ATM.

The person in question will likely try to keep secret the personal identification number (PIN) that allows you to withdraw money from the ATM if you have your ATM card. In addition, the ATM owner will keep the account number, balance and any other information necessary for communication with the bank from which the money is withdrawn confidential. The bank will also keep the ATM transactions and account balance changes confidential after the funds have been withdrawn.

Examples of confidentiality requirements

- PII/PHI must be protected from disclosure using approved algorithms.
- The password and confidential field must be masked.
- The dormant password should not be stored in clear text.
- TLS must be used to transmit sensitive information.
- The use of insecure transmissions (e.g., FTP etc.) should not be allowed.
- Log files should not contain any confidential information.

Integrity - Integrity is the ability to prevent people from changing your data in one

unauthorized or unwanted way. To maintain integrity, not only:

Need the tools to prevent unauthorized changes to your data, but want the ability to undo unwanted authorized changes?

A good example of mechanisms you can use to check integrity are:

in the file systems of many modern operating systems such as Windows and Linux. To prevent unauthorized changes, these systems often implement permissions that restrict the actions that an unauthorized user can perform on a given file. For example, the owner of a file may have read and write permissions, while others may only have read permissions or no open permissions. In addition, some of these systems

Aspects of integrity include:

- Accuracy: Be correct and precise
- Veracity: Being an accurate reflection of reality.
- Validity: factually or logically correct
- Accountability: Taking responsibility or being bound by actions and results
- Responsibility: being responsible for or in control of something or someone
- Integrity: Having all required components or parts completeness: have a complete scope; complete inclusion of all necessary elements

Availability - The final tier of the CIA triad is availability. Availability refers to the ability to access our data when we need it. For example, you may lose availability due to a power outage, operating system or application problems, network attacks, or system compromises. When an external party, such as an attacker, causes such problems, it is commonly referred to as a Denial of Service (DoS) attack.

Availability: Data should always be available when it is needed.

- Statistics used:
- MTD/RTO/RPO
- IF
- MTBF/MTTR
- Examples of availability requirements:
- The software must meet the availability requirements of 99.999% specified in the SLA.
- The software must support access for up to 200 users at the same time.
- The software must support replication and provide load balancing.
- The mission-critical software function should be back to normal within 30 minutes.

Identification: The user must be clearly identified.

Authentication: Validation of an entity's identity request.

Authorization: Confirms that an authenticated entity has the required rights and permissions.

Audit: All activities in the app/system should be audited (identify technical problems/violations)

Accountability: Follow-up of an action with a subject.

Capstone of Information Security – People, Process & Technology

As an IT or information security professional, one cannot read a blog, book or article without coming across these three words. people, processes, technology.

Popularized in the InfoSec world around the turn of the century by Bruce Schreier, these three names have been central to all ITIL practices since their inception in the 1980s, and emerged in conjunction with Harold Leavitt's theoretical diamond model. 1965 (with organizational tasks as the fourth component).

It is also known as the "Golden Triangle", the 3 keys to successfully implementing project and organizational change and a fundamental approach to solving complex business problems.

The reason for this triangle approach lies in a very important fact:

Doing this effectively in any organization requires an approach that optimizes the relationships between people, process and technology.

Focusing on one or two areas creates an imbalance. You (Employers) are wasting a lot of money and time, and your best employees are looking for work elsewhere.

Take new technologies for example, many companies believe that by implementing a shiny new tool, all their problems will go away.

What they don't see, however, is that technology is only as good as the processes around it, and the processes only as good as the people running them.

But how to ensure the right balance? - Always start with your employees

- Identify your key players and understand what each of them wants and what they bring to the table.
- Confirm that you have senior management support (from the start) because without them you will fail.
- Make sure your team consists of the right people with the right skills, experience and attitude to help you solve your problem. Practical experience is priceless, too many organizations only have theoreticians and consultants.
- Once your employees are engaged, think about the process
- A process is defined as a series of actions or steps taken to achieve a specific goal. Ask yourself: What processes do we need to solve this business problem?
- A good starting point is to identify important milestones. Once these are in place, you can focus on a more granular level by looking at process variations, exceptions, interdependencies, and supporting processes.
- Now discuss these processes with your stakeholders. Make sure they know what's expected of them and get advice from them on potential gaps and issues.
- And finally, you choose the technology
- Now that your people and processes are in order, you can now turn to technology to support them.
- It is never a good idea to force a technology and then adapt to the people and processes around it. At the same time, you need to understand and accept that SaaS stands for "Software as a Service" and is not the same as custom software development.
- Technology should always be the last consideration once the problem is clearly understood and the solution requirements are clearly defined.

All this is not new, but seems to be forgotten time and again.

In short, to do this effectively in any organization, the relationships between people, processes and technology must be optimized. Exactly in that order!

Background

Performance Models

Public Cloud

Public cloud computing is one of many deployment models that have been defined [Mel11].

Delivery models generally characterize the management and provisioning of computing resources for the delivery of services to consumers and the distinction between classes of service.

Consumers A public cloud is a cloud in which the infrastructure and computing resources that make it up are made available to the general public over the Internet. It is owned and operated by a cloud provider that provides cloud services to consumers and is by definition outside of consumer organizations.

Private Cloud

At the other end of the spectrum are private clouds. a private cloud is an environment in which the computing environment is managed solely by a single organization. It can be managed by the organization or a third party and hosted inside or outside the organization's data center. A private cloud has the potential to give businesses have better control over cloud infrastructure, computing resources, and consumers than a public cloud.

There are two other deployment models for community and hybrid clouds.

Community Cloud

A community cloud falls somewhere between public and private clouds in terms of consumer audience. It's a bit like a private cloud, but the computing infrastructure and resources are exclusive to two or more organizations that share privacy, security, and regulatory considerations, rather than a single organization.

Hybrid Cloud

Hybrid clouds are more complex than other deployment models because they involve the composition of two or more clouds (private, community or public). Each member remains a unique entity, but is linked to the others by proprietary or standardized technology that allows portability of applications and data between them.

While the choice of deployment model affects the security and privacy of a system, the deployment model itself does not determine the level of security and privacy for a given cloud.

This level mainly depends on the certainties such as B. the strength of security and privacy policies, the strength of security and privacy controls, and the level of visibility into the performance and management details of the deployed cloud environment. obtained independently from the organization (e.g., through independent vulnerability testing or operational audits).

Service Models

Just as delivery models play an important role in cloud computing, service models are also an important consideration. The service model that a cloud conforms to determines an organization's reach and control over the computing environment and characterizes a level of abstraction for its use. A service model can be updated as a public cloud or as one of them

other deployment models. Three well-known and commonly used service models are:

- **Software as a Service**
  Software as a Service (SaaS) is a service delivery model in which one or more applications and the computing resources to run them are provided for on-demand use as a turnkey service. The main goal is to reduce the total costs for development, maintenance and operation of hardware and software. Security precautions are primarily provided by the cloud provider. The cloud consumer does not manage or control the underlying cloud infrastructure or individual applications, except for the selection of settings and the limited configuration of management applications.

- **Platform as a Service**

  Platform as a Service (PaaS) is a service delivery model where the computing platform is offered as an on-demand service on which applications can be developed and deployed. The primary goal is to reduce the cost and complexity of purchasing, hosting and managing the platform's underlying hardware and software components, including databases and software development tools. The development environment usually has a specific purpose, determined by the cloud provider and tailored to their platform design and architecture. The
  The cloud consumer manages the settings of the application environment and platform applications. Security agreements are shared between the cloud provider and the cloud consumer.

- **Infrastructure as a Service.**
  Infrastructure as a Service (IaaS) is a service delivery model where the basic computing infrastructure of servers, software, and network devices is delivered as an on-demand service on which a platform for developing and running applications can be built. The main goal is to avoid buying, hosting and managing the basic hardware and software components of the infrastructure, and instead getting those resources in the form of virtualized objects controllable through a service interface.

The cloud user generally has a lot of freedom in choosing the operating system and development environment they wish to host. Security safeguards outside of the core infrastructure are primarily provided by the cloud consumer.

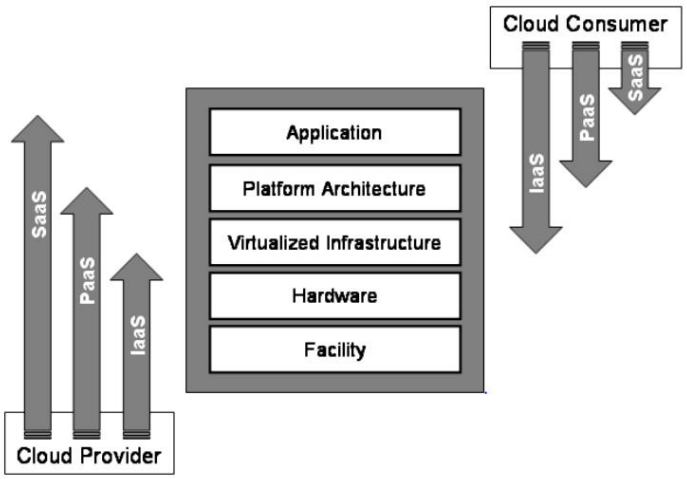


Figure 1: Differences in Scope and Control among Cloud Service Models

It illustrates the differences in scope and control between the cloud customer and cloud provider for each of the service models discussed above. Five conceptual levels of a general approach

Cloud environments are identified in the base diagram and apply to public clouds and all other deployment models. Arrows to the left and right of the chart indicate the approximate reach of cloud providers and cloud customers and control over the cloud environment for each service model. In general, the higher a cloud provider's support level, the more limited the cloud customer's reach and control over the cloud system.

The two lowest levels shown represent the physical elements of a cloud environment, which are under the complete control of the cloud provider, regardless of the service model. Heating, ventilation, air conditioning (HVAC), electricity, communications and other aspects of the physical environment. The factory floor forms the lowest layer, the equipment layer, while the computers, network, storage components and other physical elements of the IT infrastructure form the hardware layer immediately above.

The other layers are the logical elements of a cloud environment. The virtualized infrastructure layer includes software elements such as hypervisors, virtual machines, virtual data

Storage and virtual network components used to realize the infrastructure on which a computing platform can be built. While virtual machine technology is often used at this level, other ways of providing the necessary software abstractions are not excluded.
Likewise, the platform architecture layer includes compilers, libraries, utilities, middleware and other software tools and development components required to deploy and deploy applications.
The application layer represents deployed software applications intended for end-user software clients or other programs and made available through the cloud.

- **Security as a Service (SECaaS)**

Security as a Service (SECaaS) is an agreement where a third party, such as B. a security provider or managed service provider (MSP), provides a company with a robust security infrastructure, functions and maintenance and is reliable.

SECaaS is inspired by Software as a Service (SaaS). SECaaS allows a company's end users to use services such as authentication and helpdesk provided by this third party.

Depending on the usage, SECaaS can be a suitable model for the desired company as it effectively offloads the resources required for on-premises security infrastructure. It also redistributes the manpower and attention that local infrastructure would require. Some SECaaS offerings make this model easy to design, such as B. Antivirus and antispyware protection, but full authentication capabilities using mobile device biometrics and Public Key Infrastructure (PKI) are the strengths of the SECaaS spectrum. When offered as a service, this comprehensive offering provides a different answer to the business decision to build or buy a well-designed solution than when one is offered for purchase as a subscription.

SECaaS implies the product's high degree of pre-integration, interoperability and proven operational readiness. If a SECaaS cannot be easily implemented or deployed, this already indicates a level of customer access that is no longer desired due to the desire to host or build it off-premises.

Chapter# 03 - Evolution of monitoring and logging

To support cybersecurity logging and monitoring, organizations often implement industry-leading security systems technology, including the provision of firewalls; protection and analysis against malware; network intruder detection; host-based protection and SIEM.

This heterogeneous approach to selecting security solutions offers organizations the best technologies and improved security because they are not limited to a single security vendor or platform.

Information technology is so intertwined with modern business that cyber risk has become a business risk. SOC teams are under more pressure than ever to manage this risk by identifying and responding to threats across a variety of infrastructures, business processes and users. Additionally, SOC Administrators are in a unique position to bridge the gap between business processes and the highly technical work that takes place in the SOC. Managers must demonstrate their alignment with the business and their real value, a challenge when threats are ever-changing and sometimes go undetected. How do we know if our security teams are aligned to the unique threats our organization faces? How do we get consistent results and show we can detect and respond to threats in a timely manner to minimize business impact? And how can we create a stimulating learning environment where analysts can be creative and problem solve while staying focused on the mission?

A security operations center (SOC), also known as an information security operations center, is becoming a necessity for organizations of all sizes and across all industries. As the COVID-19 pandemic has fueled a massive increase in mobility through social distancing and home office measures, organizations have had to adapt to cloud and remote platforms. To counteract the new and increased risks, Managed Security Operations Centers offer companies maximum protection.

Anatomy of a Managed Security Operations Center

Given its importance to all organizations, you need to understand the anatomy of the managed SOC inside and out. But to understand how your SOC management might work, it's important to understand what a SOC looks like and how SOCs interact with other segments of your business. In this guide, we will break the anatomy of the Cybersecurity Operations Center into two main sections:

A comprehensive overview of what SOCs are, what they contain and what they do

How SOCs relate to the rest of your cybersecurity infrastructure and anatomy

By the end of this blog, you will be well equipped to bolster your defenses, with or without the help of outside service providers. But first, let's see why SOC management is so important.

Why managing security activities is so important

According to a 2019 McKinsey report on the future of risk-based cybersecurity, maturity-based approaches that measure success using control thresholds are doomed to fail. They will overwhelm the company's internal IT teams as the number and complexity of the programs being monitored increases exponentially.

This is even more true now in a world impacted by COVID-19 and why Managed SOC is so important: An in-house SOC solution is rarely serviceable.

While the report identifies SOC development as part of a maturity-centric approach, it does not address how the managed SOC works to anticipate and mitigate these challenges when guided by a managed security service provider (MSSP). With cyber defense becoming a prohibitive internal management challenge, organizations need to hire MSSPs.

Security Operations Center (SOC) 101

Whether managed internally or externally, a strong SOC is an essential part of your overall cybersecurity architecture. Although SOCs differ in nature, they must conform to the definition of the security (or risk-based) paradigm. Almost all SOCs work closely with or as part of an organization's incident response team. The focus is on identifying risks that could culminate in events and responding (often more critically) to events that could culminate in cyberattacks.

The following sections discuss the infrastructure and personnel that make up a SOC. Next, we look at the features and a case study of a SOC in action.

Selected example: Interactive computer training

As mentioned above, your SOC can contain as many (or as few) of your organization's cybersecurity functions as you need, managed both internally and externally. One unexpected area where you can shine is in employee training programs.

For example, consider the innovative tabletop incident response exercise offered by RSI Security as part of our SOC and MSSP suites. Once your organization has developed an Incident Response Plan (IRP), we create different scenarios to test it by simulating attacks or threats. These limitations of the IRP help to identify the vulnerabilities, the spots that need to be fixed or optimized the most.

Typical scenarios include simple and complex malware deployments, wireless network attacks, and cloud computing-based stress tests, which are becoming increasingly valuable in our highly mobile age.

Managed SOC architecture integration

As the previous sections illustrate, your SOC configuration can be flexible and scalable to meet your specific business needs and capabilities. The same goes for fitting into your organization's overall cybersecurity framework, whether the SOC itself is managed internally or externally. For example, a SOC can cover full incident management, as described above, or it can focus on more limited versions, such as B. Managed Detection and Response.

The following sections identify areas of ideal synergy between your SOC anatomy and your broader organizational approach to cybersecurity. This includes basic and advanced risk mitigation practices, as well as training and awareness raising for regulatory compliance.

Monitor and remediate threats and risks

A SOC is primarily used to respond to attacks and events. However, to respond effectively, the SOC must also incorporate monitoring practices into the SOC function itself or in conjunction with elements of your organization dedicated to that function.

Components of a threat and vulnerability management program include, but are not limited to:

- Continuous vulnerability scanning; Analysis of identified risk or threat factors.
- Collect and mobilize intelligence on threats, across organizations and industries.
- Risk analysis for cloud platforms, applications, websites and all other assets.
- Internet of Things (IoT) assessments for smartphones and connected devices.
- Threat Lifecycle Management and Asset or Infrastructure Lifecycle Management.

These measures are not limited to your budget. Threat management within or related to your SOC must also consider third-party risks. Each vendor and vendor you work with brings its own set of threats, including its MSSPs. Your SOC helps reduce them.

Typical scenarios include simple and complex malware deployments, wireless network attacks, and cloud computing-based stress tests, which are becoming increasingly valuable in our highly mobile age.

Integration of the overall architecture of the SOC

As outlined in the previous sections, your SOC configuration can be flexible and scalable according to the specific characteristics and resources of your organization. The same goes for fitting into your organization's overall cybersecurity framework, whether the SOC itself is managed internally or externally. For example, an SOC can cover all incident management, as described in this case, or it can focus on the latest releases and only specify detection and overall response.

The following subsections identify areas of ideal synergy between your SOC anatomy and your broader organizational approach to cybersecurity. This includes basic and advanced risk mitigation practices, as well as training and awareness raising for regulatory compliance.

Deep and complex analytical methods

For organizations faced with what some security experts call "advanced persistent threats," a simple vulnerability management program may not be enough to protect your urgent business. They must use advanced analysis techniques that match the threats.

Start with penetration testing or penetration testing. It is a form of "ethical" hacking by a cybersecurity expert or team of experts to simulate an attack on your system so that you can investigate the genuine malicious attacks that resemble it. Whether internal or external, your SOC is an ideal partner for penetration test team members or penetration testers.

The two main types of penetration testing are the most expensive: external and internal. The first, also known as "black hat", requires little or no knowledge of security architecture: the hack fails from scratch. The latter, also known as "white hat," simulates an insider attack by a current employee, former content contributor, or other initiative intended to be introduced into your organization's network.

Track and facilitate regulatory compliance

One obvious area where your SOC integrates seamlessly with other systems is in analyzing and enforcing regulatory compliance. While the SOC focuses on violations, you can also use it to conduct or facilitate specific audits and compliance assessments.

For example, consider the following compliance-based implementations and integrations:

A NIST Security Operations Center is optimized to look for compliance violations specific to NIST Special Publication 800-171, Cybersecurity Model Maturity Certification, and other requirements for contractors working with the Department of Defense (DoD).

A joint task force composed of your SOC, Human Resources and other designated departments to oversee the reporting of violations as defined in the Health Insurance Portability and Accountability Act, which applies to companies involved in health and environmental businesses.

A simplified assessment of Payment Card Industry (PCI) Data Security Standard (DSS) compliance (required for all businesses that process credit card payments) is performed by delegating all PCI-specific monitoring, analysis and reporting responsibilities to your SOC.

A SOC can facilitate all compliance issues, from creating necessary controls and analyzing gaps to reporting patches and remediation work required for long-term maintenance.

Continuous and expanded awareness

Above we describe a specific use case for managed SOC: innovative hands-on interactive training. With close collaboration between your SOC, internal IT and other MSSPs on your team, you can streamline all of your ongoing security awareness training.

Managed Security can create a series of regular workshops and documentation to train your staff, either as your SOC or in close collaboration with your existing SOC. We offer basic courses on topics such as phishing (and vishing/smishing), as well as quizzes and activities to test your employees' knowledge. We can complement these introductory lessons with advanced training on anything from cryptography to automation.

Essentially, your SOC can be described as your organization's cybersecurity operations center. Through a combination of cutting-edge software and highly skilled security experts, an SOC works in real-time to mitigate existing threats and defend against potential threats on the horizon. The two main types of SOC. While they offer many of the same basic features, they work in different ways.

Internal SOC

Some larger companies have a SOC with all employees in the company. These centers, referred to as the internal SOC, contain all of the people, software, infrastructure, and tools needed to manage, detect, and validate today's threats while extending them well into the future. The benefits of an internal (on-site) SOC include full organizational control and on-site professionals ready to respond immediately to emergencies. These benefits come with additional costs beyond the capabilities of many small businesses.

Outsourced SOC

For many small and medium-sized businesses, the cost of hiring a full in-house cybersecurity team and acquiring the necessary equipment to run a good on-premises SOC is simply prohibitive. However, every business needs a skilled and professional cybersecurity team. This often means that companies use third-party cybersecurity services. SOC as a Service (SOCaaS) is a way for companies to get the same benefits as an in-house SOC without the high cost and limited flexibility. One of the most outstanding features of SOCaaS is the 24/7 monitoring of your network. Because of this, some organizations use a third-party SOCaaS to work with their internal cybersecurity team.

The responsibilities of a SOC team

Your SOC acts as your organization's first line of defense against immediate and ongoing cyber threats from multiple sources. In today's business environment, having access to real-time information with seamless processes that keep your business on track is essential. The downside of these abilities is their potential vulnerability to outside attacks. While virtually all devices come with firewalls and security features to protect data, these tools are not suitable for trained and determined criminals attempting to break into professional networks. Whether you have a fully staffed on-site SOC team or outsource services to a supplier, the roles and responsibilities of your SOC team are essentially the same. Your SOC team is the human element of your security system and is responsible for executing these tasks.

Installation and management of security equipment

Each SOC team works with multiple teams to protect data within a corporate network. To provide your organization with custom security, your SOC team needs the hardware and software to understand your security environment. Tools used by your team include firewalls, data analytics, intrusion detection, threat and vulnerability management tools, data loss prevention, and reporting technology. While these tools are useful tools, using them successfully requires a SOC team that can select and leverage the tools needed for a particular organization.

Investigation and analysis of suspicious activity

Each network continuously receives information about the actions performed in each part of the system. SIEM tools continuously monitor data for suspicious activity that could indicate a threat. When alerts for suspicious activity are received, the SOC team analyzes them to understand the danger of the threat and generate an appropriate response.

The ability to detect threats allows a SOC team to prevent the threat from spreading and causing significant damage within the network. The ability to contain a threat locally can prevent your business from losing productivity and cash flow due to system failures.

Reduce downtime and keep your business running

Software without the guidance of a trained cybersecurity team can result in a flood of alerts. However, many of these alerts are false positives that need to be addressed by your IT team. When it comes to constant notifications, your business has two choices. Suppose the warnings are false or they shut down the systems repeatedly. First, the company runs the risk of criminal activity penetrating deeper into the system. The second leads to several stops to study possible threats.

When an SOC team examines real-time information, appropriate personnel and stakeholders can be notified of serious threats, and countermeasures can be implemented before the threat reaches critical business infrastructure. In the event of false positives or real security threats, your SOC team works continuously to resolve the issue without costly downtime.

Assistance with regulatory compliance

Many types of businesses are required to meet specific government standards. Meeting changing standards and preparing for audits can be time-consuming and complex. Your SOC team uses tools to keep your cybersecurity practices updated to meet standards such as NIST, CMMC, PCI, GLBA, FISMA, GDPR, NERC-CIP and GDPR.

Job titles and roles within the SOC team

While an effective SOC team uses advanced tools and software to provide any organization with effective security measures, the roles within the team go well beyond selecting and deploying software. Cybersecurity professionals work in a multi-layered system to eliminate threats through best practices, threat detection and response. In general, you can assume that each SOC team consists of the following cybersecurity professionals.

Security Analyst

As first responders to incidents, security analysts are responsible for analyzing threats at three levels, including detection, investigation, and rapid response.

- ✓ Tier 1 – Receives and analyzes alerts on a daily basis, determines the relevance and urgency of these threats, and performs triage to determine if a genuine security incident has occurred.
- ✓ Tier 2 - Remediates real-world security incidents using threat intelligence to identify the location and severity of the attack and implement a containment and remediation strategy.
- ✓ Tier 3 - Manage critical security incidents with vulnerability assessments and penetration tests, isolate vulnerabilities, investigate alerts and identify threats that have penetrated the network.
- ✓ To do this, security analysts use sophisticated software to monitor and detect threats. They may also be involved in creating a cyber security plan, training staff and creating documentation. Security analysts are often the first to respond to threats.

Safety Engineer

Engineers, also known as security architects, create security architectures and work with developers to integrate security into the development of business systems and processes. Security engineers are responsible for building security architectures and systems. This includes maintaining existing software and tools, providing updates, and recommending new tools for more effective security. Engineers also document requirements, procedures, and protocols to ensure all employees and network users have access to resources that help keep the organization secure.

SOC manager

The security manager oversees the actions of the entire SOC team and reports directly to the CISO. From overseeing staff to creating policies and logs, the SOC administrator must perform multiple tasks to ensure the SOC is running smoothly at all times. A SOC Administrator's responsibilities include:

Manage SOC team members

- Coordination with safety engineers.
- Creation of a recruitment policy
- management of financial activities
- Evaluation of incident reports
- Preparation and implementation of crisis communication plans.

- Compliance Reports
- Inform business leaders

CISO

The Chief Information Security Officer (CISO) is responsible for defining and describing an organization's security activities. They approve security policies, strategies and procedures. As the leading SOC expert, the CISO is responsible for managing compliance and reporting security concerns directly to the CEO and senior management of the organization.

Budget considerations when creating your SOC

For any business or organization, security is more than a cost. It's a return on investment that saves you money versus the cost of a security breach. However, all businesses must operate within their current budgets to survive. When trying to balance an effective SOC while staying within your budget, it's helpful to review key budget considerations before making final decisions about your SOC.

Staff

The size of your SOC depends on the size of your organization, the type of data you need to protect, and the risks in your industry. But the personnel costs of a small internal SOC can also be expensive. Information security analysts made an average salary of $99,730 in 2019. Any effective SOC team requires multiple security analysts at different levels, as well as advanced security personnel.

In addition to the cost of paying staff salaries, it can be costly to hire qualified security professionals to fill your available roles. The cybersecurity industry faces a skills shortage. There just aren't enough qualified people entering the industry to fill the demand. For companies seeking security professionals using traditional recruitment methods, the process can quickly become costly.

Solid and professional security solutions

In short, your SOC is an essential part of your cyber defense framework. Whether managed internally or externally, it's the best way to keep up with the evolving threats and attacks in our mobile business environment. Finally, it integrates and strengthens all internal systems.

Some organizations respond to these issues by using existing IT staff as security experts. This can backfire in more ways than one. IT professionals without proper training cannot provide the same level of service as trained security professionals. Worse, when employees have to focus on

multiple roles, the organization can be at greater risk. For a SOC to be effective against today's modern cyber threats, it needs a highly skilled and trained team of security specialists.

Over time

Cybersecurity requires 24/7 coverage and the ability to respond to threats as they arise. For companies building an internal SOC, this means hiring more staff. It also means thinking about additional or part-time staff to cover sick days and holidays. Threat actors, from extortionists to nation-state actors, target weekends and holidays for successful cyberattacks. As IT staff and cybersecurity professionals spend more time on vacation, response times slow down and cybercriminals are more likely to achieve their goals.

Security Tools

Whether you have an on-premises SOC team or a vendor-provided SOCaaS, the security tools and software used to protect your network must be efficient enough to handle a significant amount of data. While it's possible to find lower costs by researching security vendors, it's important to ensure costs aren't being reduced by using outdated or ineffective tools. An organization may struggle to provide the tools needed to deploy state-of-the-art security solutions, but many third-party SOC providers already have the resources.

Compliance Audits

Failing an audit can be expensive. The preparation of your audits and the audit process is also a considerable effort. A 2019 study found that two-thirds of organizations budget for security. Compliance mandates were a major factor behind the need to increase spending, with 69% of respondents citing this as a priority.

Any organization trying to achieve government-mandated compliance can expect to add this cost to their cybersecurity budget.

- Gap analysis to identify and fix gaps before the audit
- Updated documentation of policies, procedures, and technologies.
- The audit, which is usually performed by a third party
- Time that employees of the company spend preparing for the audit
- Implementation and training of compliance processes and procedures
- Ongoing maintenance to keep up with changing regulations and rising risks

The costs of non-compliance, which may include fines, additional audits, damage to reputation, restriction of the provision of certain services, and loss of customers.

Software maintenance costs

Technology is constantly growing and evolving. For threat actors, the vulnerabilities exposed by such changes present opportunities to access and exploit multiple networks. For businesses, the potential risks combined with the required upgrades represent the need to spend more money on advanced software or upgrade existing software. Security software must be updated regularly to meet new compliance standards or to eliminate newly discovered vulnerabilities.

Key functions of a SOC team

Your SOC team implements a unique cybersecurity strategy for your organization to assess and eliminate incoming threats before they disrupt your business. As the center of any security system, the SOC team works with the efforts of all IT staff and members to complete a fully effective security system. These are the main functions of a SOC team.

- Monitor – Using advanced software and data security analysts, the SOC monitors events within a network to look for unusual or suspicious behavior.
- Prevention – Automated monitoring and alerting allows the SOC to isolate pending threats to prevent threat actors from moving across the network. Prevention can also eliminate vulnerabilities before a malicious actor enters the network.
- Detect – Through monitoring and UEBA, the SOC team can identify normal behavior and unusual patterns from threat actors that are masking criminal activity within the system.
- Investigate - When threats are detected, SOC analysts and engineers investigate the source of the attack and the vulnerabilities that helped the attacker gain access to the network.
- Respond - When an attack occurs, the SOC team must respond immediately to neutralize the threat, remediate vulnerabilities, protect unaffected systems, and repair affected areas of the network.

SOC, NOC and IT: the differences and how they work together

Advanced technology enables businesses and organizations to quickly perform tasks that they could not perform in the past. Thanks to these advances, companies across all industries are more productive and sophisticated than many people ever thought possible. However, with these advances come complex networks that need to work well for everything to work as it should (or often works). Today's technology is forcing even small and medium-sized businesses to use correlated networks and devices to keep business running and properly maintaining customer satisfaction. These networks require experienced professionals to maintain them and protect them from potential threats.

While it would be great if a single technology solution could provide comprehensive network security and support, this simply isn't possible. The professionals who oversee the systems are trained to specialize in certain techniques to make them work. Depletion of this specialized

concentration results in an overall decrease in capacity. When companies search for the technical support they need, they often mistakenly think that common terms are slightly different versions of the same thing. That's not the case. Your organization does not need a SOC or NOC. You need a version of both. And even if you outsource most of your IT support, you'll likely need onsite IT experts as well. Learning about NOC, SOC, and IT responsibilities can help you better understand how they work and identify the best solutions for your business.

NOC: Network Operations Center

A Network Operations Center (NOC) is a fully managed team of remote specialists that provides 24/7 network performance protection. These teams have experience with the technology used to keep your business running smoothly at all times. The goal of every NOC is to maintain uninterrupted service from on-premises and cloud-based devices.

Although specific services vary by provider, an NOC typically provides these services.

- ✓ 24/7 network optimization for a healthy network
- ✓ Proactively monitor for issues that could cause downtime
- ✓ Manage updates and patches
- ✓ Reduce downtime and manage alerts
- ✓ Ensure a consistent flow of data
- ✓ backup management
- ✓ network communication
- ✓ Trend detection and analysis reports
- ✓ Refurbishment instructions and step-by-step plan

SOC: Security Operations Center

Just like your NOC, a SOC works to maintain the usefulness of an organization's network. However, all tasks performed by the SOC team are related to network security and threat protection. Whether your SOC is local or remote, it must provide these services.

- ✓ 24/7 security risk monitoring
- ✓ Proactive monitoring to detect potential threats on a network
- ✓ Security updates and patches when vulnerabilities become known
- ✓ Prevent network outages by isolating or preventing threats
- ✓ Risk identification and analysis reports
- ✓ Follow government safety regulations
- ✓ Responding to and remediating security threats

IT: IT department, helpdesk or services

The information technology (IT) team of any organization has a wide range of responsibilities. Most people in an organization see the IT team as the group that steps in to install new software, reboot the system, or fix technical problems as they arise. While IT professionals perform these tasks, they also have many day-to-day tasks to keep the technical systems up and running. Unlike centers that are designed to provide 24/7 network support, a typical IT team is there to maintain and support day-to-day operations. An external IT helpdesk can be used to resolve issues outside of office hours and to support a small in-house IT team.

Services provided by an IT team include:

- ✓ Management of an existing technology system to maintain order of work
- ✓ Building and maintaining infrastructure and hardware within a company's technology system.
- ✓ Maintain operational functions.
- ✓ installation and maintenance of computer network systems.
- ✓ Create a contingency plan for system emergencies
- ✓ Creation and maintenance of a company website.
- ✓ Monitoring and maintenance of a company's communication network.

While IT, NOC and SOC provide a range of functions related to the operation and security of a network, they specialize in different areas. When these specialized services are clearly defined, NOC, SOC and IT activities correlate and coordinate for a highly functional and secure network. Today's advanced technology offers organizations of all types new opportunities to get the cybersecurity technology and support they need. All of these services can typically be outsourced to provide companies with full, partial or emergency services in addition to on-site staff.

Conclusion

Organizations rarely have adequate cybersecurity and surveillance capabilities. They often suffer from a lack of budget,

resources, technology or recognizing the nature and extent of the problem.

While you probably won't achieve a cybersecurity and logging utopia, you can create a more efficient cybernetwork.

Monitoring and security functions. To achieve this, you need:

- Identify and investigate anomalies in cybersecurity events
- Realize that details matter
- Prioritize your cybersecurity and logging activities
- Correlate suspicious events with cybersecurity intelligence
- Consider building or buying a Security Operations Center as this seems to be one of the main avenues.
- Effectively support cybersecurity monitoring and logging.

- Find the right help from knowledgeable third-party providers for carefully selected activities
- Keep an eye on future requirements.

What organizations often need is the ability to access proven qualified, knowledgeable and competent people working for organizations who have been independently assessed against best practices and have policies, processes and procedures in place to oversee all relevant events confidential information.

Answer# 03 Methodologies

An Information Security Operations Center (ISOC or SOC) is a facility where security personnel monitor corporate systems, protect against security breaches, and proactively identify and mitigate security risks.

Historically, SOC was considered heavy infrastructure available only to very large or security-conscious organizations. Today, with new collaboration tools and security technologies, many small organizations are setting up virtual SOCs that do not require special installation and can employ part-time employees from security groups, operations and development. Many organizations implement managed SOCs or hybrid SOCs that combine in-house staff with the tools and expertise of managed security service providers (MSSPs).

Motivation for a SOC. to build

A SOC is an advanced step in an organization's security maturity. These are the factors that usually make companies take this step:

Requirements of standards such as the Payment Card Industry Data Security Standard (PCI DSS), official regulations or customer requirements

Businesses need to protect highly sensitive data

History of security breaches and/or public investigations

Organization Type – For example, a government agency or Fortune 500 company will almost always have the size and threat profile to warrant an SOC or even multiple SOCs.

SOC focus area SOC US level of interest

control and digital forensics

Apply compliance, penetration testing, and vulnerability testing. 62%

monitoring and risk management

Capture events from logs and security systems, identify and respond to incidents. 58%

Network and system administration

Management of security systems and processes such as identity and access management, key management, endpoint management, firewall management, etc. 48%

Areas of intervention of an SOC

A SOC can have different functions in an organization that can be combined. Below are the SOC focus areas with the importance assigned to them in the SOC Survey Exabeam Status.

SOC Facilities The classic security operations center is a physical facility that is well secured in terms of cybersecurity and physical security. It's a large room with security guards at desks overlooking a wall of screens displaying security statistics, alerts, and details of upcoming incidents. Many SOCs look very different these days. For example, a virtual SOC (VSOC) is not a physical entity, but rather a group of security professionals working in a coordinated manner to perform the functions of a SOC.

Challenges in building a security operations center

Security teams building an SOC face several common challenges:

Limited Visibility: A centralized SOC does not always have access to all organizational systems. This can be end devices, encrypted data or systems managed by third parties that have an impact on security.

White Noise: A SOC receives massive amounts of data, and most of it is irrelevant to security. Enhance Security Information and Event Management (SIEM) and other tools used in the SOC to filter noise, leverage machine learning, and advanced analytics.

False Positives and Alert Fatigue: SOC systems generate a large number of alerts, many of which do not turn out to be genuine security incidents. False alerts can waste a lot of time for security analysts and make it harder to spot genuine alerts.

These three challenges are addressed by a Security Information and Event Management (SIEM) system that drives day-to-day operations in modern SOCs. Read more about SIEM below under Technologies used in the SOC.

What is SecOps?

Security Operations (SecOps) is a collaboration between IT operations and security teams, where security and operations personnel share ownership and accountability for security vulnerabilities. It is a set of SOC processes, practices, and tools that can help organizations more effectively meet their security goals.

Before security operations

In the past, operations and security teams had conflicting goals. Operations was responsible for configuring the systems to meet performance and availability goals. Security was responsible for reviewing a checklist of compliance or regulatory requirements, patching security gaps, and building defenses.

In this environment, security was a burden seen as slowing down operations and overloading. But in reality, security is one of the requirements of any computer system, just like availability, performance or basic functionality.

After security operations

SecOps brings operations and security teams together in one organization. Security “shifts to the left”: It is not at the end of the process, but at the beginning when requirements are defined and systems are designed. Instead of operators setting up a system and security guards stepping in to protect it, systems are designed from the ground up with security in mind.

To DevSecOps

SecOps has additional implications for companies adopting DevOps: the unification of development and operations teams into one group with shared responsibility for IT systems. In this environment, SecOps brings with it even broader collaboration between security, operations, and software development teams. This is known as DevSecOps. This shifts security even further to the left, building security into systems from the earliest stages of development.

SecOps in the SOC

SecOps in the SOC

The classic security operations center does not support SecOps: security analysts sit in their own room and respond to incidents, while operations take place in another room or building, with computer systems, with little or no communication between them. However, modern SOC can encourage a SecOps mentality:

Analysts can keep operations personnel continuously informed of threats to the company's systems and current incidents.

Analysts can proactively identify security gaps and work with operations to close them.

The Facility may contact the SOC for advice on the security implications of any system, component, supplier, or customization.

The Security Maturity Spectrum: Are you ready for a SOC?

Different organizations are at different stages of developing their security presence. We define five stages of security maturity: In stages 4 and 5, an investment in a security operations center becomes relevant and valuable.

Step 1 - Initial

minimalist

“Security is not our primary concern. We have AV and FW. We're fine!"

Without SIEM

no registration

Basic FW on the edge

AV in use

Step 2 - Development

reagent

"We have not investigated any solutions and do not believe we are at risk. We will process a breach if it occurs.

Without SIEM

a disk

Added patch management

Dedicated FW and DMZ

Added basic identity and access management

Step 3 - Define

To worry

“We are in danger, but the budget is an issue. We are overwhelmed by the warnings we face. We need help prioritizing and dealing with threats.

You are considering a SIEM or have a simple SIEM implementation

Added network segmentation and multi-FW

Added data classification

Overwhelmed by warnings and logs

You have to prioritize them

Concerned about budget optimization due to limited resources

Step 4 - Managed

Progressive

“We have a budget to invest in security. We have a limited workforce and need to maximize it.

SIEM is integrated in most domains

Think of analytics as a way to reduce attention

Consider tools to streamline incident investigation

You want to increase operational efficiency and maximize employee performance

Intrigued by the idea of threat hunting

Step 5 - Optimization

mature security

“We definitely know each other. We are constantly renewing and improving our program.

Very mature SIEM implementation

Integrated into almost every system

Conduct threat detection with experienced analysts.

Has custom security features built into your workflows

Able to create your own DS algorithms

Interested in the cost-effectiveness and risk mitigation of third-party solutions.

SOC Implementation Pattern

Here are common patterns for implementing a SOC in your organization:

- Dedicated SOC
  Classic SOC with dedicated facilities, dedicated full-time staff, fully in-house operated, 24/7 operational.
- Distributed SOC
  Some full-time and some part-time, mostly 8x5 in each region.
- Multifunctional SOC/NOC
  A dedicated facility with a dedicated team that performs the functions of a Network Operations

- Fusion SOC
  A traditional SOC combined with new features such as Threat Intelligence, Operational Technology (OT).

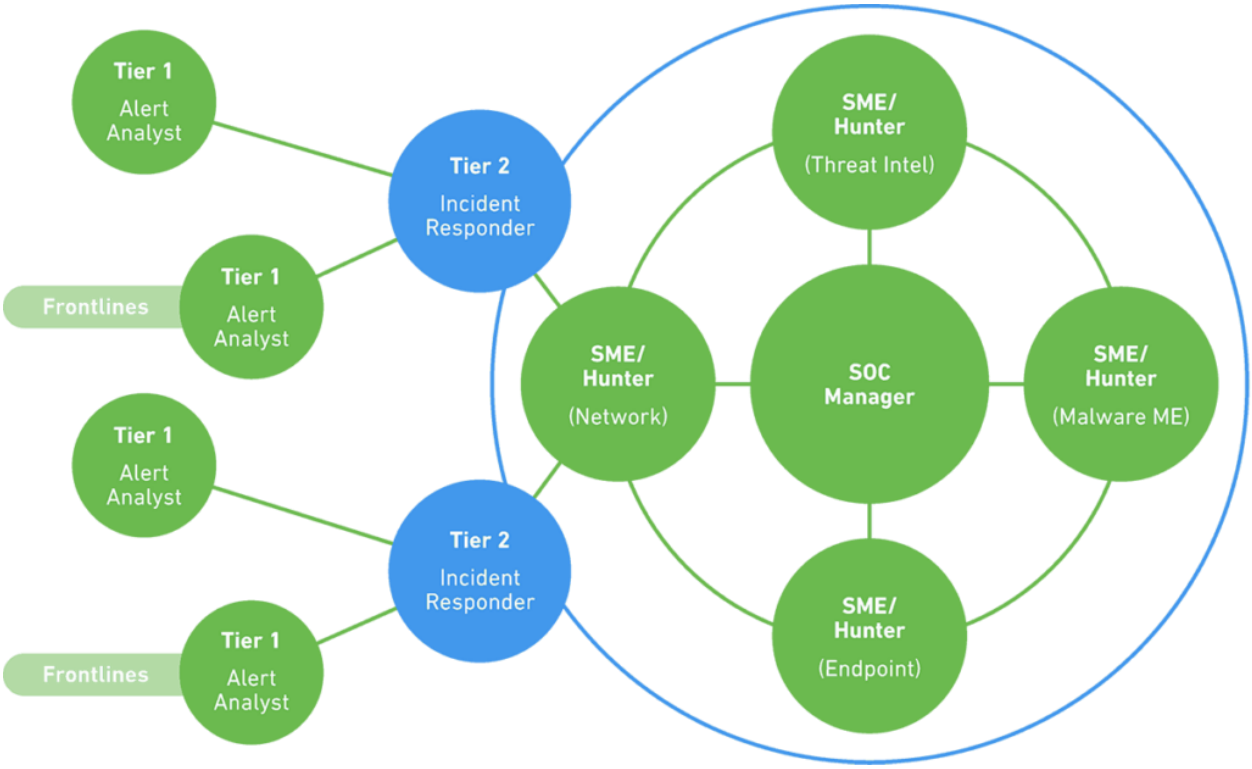
- Command SOC/Global SOC
  Coordinates other SOCs in a global organization and provides threat intelligence, situational awareness and advice.

- Virtual SOC
  No dedicated facilities, part-time team members, mostly responsive and triggered by a high-profile security alert or incident. The term virtual SOC is also sometimes used for an MSSP or managed SOC (see below).

- Managed SOC / MSSP / MDR
  Many companies rely on Managed Security Service Providers (MSSP) to outsource SOC services. Modern offerings are called Managed Detection and Response (MDR). Managed SOCs can be fully outsourced or co-managed with in-house security personnel.

Who works in a SOC?

A Security Operations Center has a hierarchy of roles with a clear escalation path. Daily alerts are received and reviewed by Level 1 analysts; an actual security incident is elevated to Level 2 Analyst; and Business Critical Incidents recruit the Level 3 Analyst and, if required, the SOC Manager.



Role Qualification Features

Level 1 Analyst

Alert Investigator

Skills in system administration, web programming languages like Python, Ruby, PHP, scripting languages, security certifications like CISSP or SANS SEC401 Monitors SIEM alerts. Manage and configure security monitoring tools. Prioritize and sort alerts or issues to confirm they are genuine security incidents.

Level 2 Analyst

Incident Responder Similar to Level 1 Analyst but with more experience including Incident Response. Advanced forensics, malware assessment, threat intelligence. Having a hacker certification or training course from White Hat is a huge plus. It receives incidents and performs in-depth analysis related to threat intelligence to identify the threat actor, the type of attack, and the systems or data affected. Sets containment, remediation and recovery strategy and acts accordingly.

Level 3 Analyst

Subject Matter Expert/Threat Hunter Similar to Level 2 Analyst, but with even more experience, including high-level incidents. Experience with data visualization and cross-organizational penetration testing tools. Malware reverse engineering, experience in identifying and developing responses to new threats and attack patterns. He conducts daily vulnerability assessments and penetration tests, and reviews alerts, industry news, threat intelligence, and security data. It actively searches for threats that have penetrated the network, as well as unknown vulnerabilities and security holes. When a major incident occurs, he joins the Tier 2 Analyst to respond and manage it.

Level 4 SOC manager

Commander Similar to Level 3 Analyst including project management skills, incident response management training and strong communication skills. As a military unit commander, responsible for hiring and training SOC personnel, responsible for defense and offensive strategy, managing resources, priorities and projects, and leading the team in responding to mission-critical security incidents. Acts as the company's point of contact for security, compliance and other security incidents.

Security Engineer

Support and Infrastructure A degree in computer science, computer engineering, or information assurance, usually combined with certifications such as CISSP. A software or hardware specialist who focuses on the security aspects of information systems design. He creates solutions and tools that help organizations resiliently deal with business disruption or malicious attacks. He sometimes works within the SOC and sometimes supports it.

SOC tools

A SOC cannot function without technology. The following table lists the traditional and next-generation tools used in the current Security Center. Below we present some of the most important ones in more detail.

Traditional tools

- Security Information and Event Management (SIEM)
- Governance, Risk and Compliance (GRC) systems.
- Vulnerability scanners and penetration testing tools
- Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Wireless Intrusion Prevention
- Firewall, Next Generation Firewall (NGFW) which can act as IPS and Web Application Firewall (WAF).
- Log management systems (mostly as part of SIEM)
- Cyber Threat Intelligence Resources and Databases

Next generation tools

- Next-generation SIEMs built on a big data platform and incorporating machine learning and advanced behavioral analytics, threat detection, integrated incident response, and SOC automation
- Network traffic analysis (NTA) and application performance monitoring (APM) tools.
- Endpoint Detection and Response (EDR), which helps detect and mitigate suspicious activity on hosts and user devices
- User and Entity Behavior Analytics (UEBA), which uses machine learning to identify suspicious behavior

Security Information and Event Management (SIEM)

The core technology of a SOC is a SIEM system that collects system logs and events from security tools from across the organization. SIEM uses statistical and correlation models to identify events that could constitute a security incident, alert SOC personnel, and provide contextual information to support investigations. A SIEM acts as the "single pane of glass" that allows the SOC to monitor operating systems.

Firewalls, next-generation firewalls (NFGWs), and web application firewalls (WAFs)

Firewalls are an essential part of any cybersecurity arsenal. Two new technologies fill or replace the traditional firewall:

i. NGFW - Extends the firewall by providing intrusion detection and prevention with deep packet inspection capabilities. NGFWs can block threats at the network perimeter using techniques such as URL filtering, behavioral analysis, and geolocation filtering. They use a reverse proxy to terminate connections and inspect content before it reaches a web server.

ii. WAF - A WAF is deployed to web applications, examines traffic and identifies traffic patterns that may represent malicious activity. A WAF can detect attacks while minimizing false positives by learning acceptable URLs, parameters, and user input, and using that data to identify traffic or input that deviate from the norm.

These technologies are used in the modern SOC to reduce the attack profile of websites and web applications and collect higher-quality data about legitimate and malicious traffic impacting critical web properties.

Endpoint Detection and Response (EDR)

EDR is a new category of tools that help SOC teams respond to attacks on endpoints such as user workstations, mobile phones, servers or IoT devices. These tools are based on the assumption that attacks will happen and that the SOC team generally has very limited visibility and control over what's happening on a remote endpoint. EDR solutions are deployed on endpoints, providing instant and accurate data on malicious activity and enabling SOC teams to remotely manage endpoints for immediate mitigation.

For example, the SOC team can use EDR to identify 50 ransomware-infected endpoints, isolate them from the network, wipe the machines, and recreate them. All of this can be done in seconds to instantly detect attacks, prevent spread and aid in eradication.

SOC monitoring tools

Monitoring is an important function of the tools used in the SOC. The SOC is responsible for overseeing computer systems and user accounts throughout the organization, as well as overseeing the security tools themselves. B. Ensuring that antivirus software is installed and up to date on all systems in the organization. The primary tool that orchestrates monitoring is SIEM. Organizations use many dedicated monitoring tools, such as B. Network Monitoring and Application Performance Monitoring (APM). For security reasons, however, only SIEM, with its cross-functional view of IT and security data, can provide a complete monitoring solution.

Motivation to use state-of-the-art SOC tools

Next-gen SIEM: Helps reduce alert fatigue so analysts can focus on the alerts that matter. New analytics capabilities combined with a wealth of security data enable next-generation SIEMs to uncover incidents that no security tool alone can detect.

NTA: Easy to implement, ideal for detecting abnormal network behavior. Useful when the SOC has access to the traffic to be examined and wants to examine the lateral movement of attackers already inside the perimeter.

UEBA: Uses machine learning and data science techniques to detect malicious insiders or bypass security controls. This makes it much easier to identify an account compromise, whether by external or internal attackers.

EDR: Provides strong protection against workstation or server compromise and helps manage mobile workers. Provides the data needed to conduct historical research and uncover root causes.

Which tools should I start with?

These steps for using tools were suggested by Gartner's Anthony Chuvakin.

Greenfield SOCs → SIEM only

Established SOC → Add automated threat intelligence, NTA and EDR sandboxing.

Forward Learning → Add UEBA and a comprehensive internal threat intelligence platform deployed as part of the next generation SIEM

SOC processes facilitated by a SIEM: key examples

- Malware Research: SIEM can help security personnel combine data about detected malware across the enterprise, correlate it with threat intelligence, and understand affected systems and data. Next-generation SIEMs provide security orchestration capabilities, incident schedule visualization, and can even automatically “push” malware into a threat intelligence sandbox.
- Phishing Prevention and Detection: SIEM may use behavioral analysis and correlation to determine whether a user clicked on a phishing link distributed via email or other means. When an alert is triggered, analysts can look for similar patterns across the organization and over time to determine the full extent of the attack.
- Human Resources Investigation - When an employee is suspected of being directly involved in a security incident, a SIEM can help by collecting all the data about the employee's interaction with IT systems over a long period of time. A SIEM can uncover anomalies, e.g. B. Connections to company systems at unusual times, elevation of privileges or the movement of large amounts of data.
- Mitigating the risk of employees leaving: According to research by Intermedia, 89% of departing employees retain access to at least some company systems and use those credentials to log in. A SIEM can map the problem across a large organization and determine which systems have unused credentials, which former employees have access to the systems, and which sensitive data is affected.

SOC process

How SecOps and DevSecOps are transforming the SOC

Previously, the Security Operations Center processes were completely isolated from other parts of the organization. Developers would build systems, IT operations would run them, and security would be responsible for protecting them. It is now clear that consolidating these three functions into one organization with shared security responsibilities can improve security and result in significant operational efficiencies.

Here are some ways a SOC can integrate its processes with development and IT:

a) Build a distributed SOC with DevOps members – DevOps teams can help respond to incidents because of their deep knowledge of IT systems and learn from security staff about threats and critical vulnerabilities.
b) Couple threat hunters with DevOps team leaders – Instead of discovering a threat and reporting it up, threat hunters can work directly with development or operations teams to close the vulnerability at its source.
c) Open the SOC for Guidance and Consultation - Anyone performing work that impacts security should have an easy way to reach the SOC and consult with the top security professionals in the organization.
d) Build Security Centers of Excellence – The SOC can work with select development and operations groups to implement security best practices and then showcase those achievements across the organization to drive SecOps practices.

A basic incident response model

As SOCs undergo transformation and assume additional roles, their core activity remains incident response. The SOC is the organizational unit that is expected to detect, contain, and mitigate cyberattacks on the organization. The individuals responsible for incident response are Tier 1, Tier 2, and Tier 3 analysts, and the software they primarily rely on is the SOC's Security Information and Event Management (SIEM) system.

a) TIER 1 - Event classification

Tier 1 analysts monitor user activity, network events, and security tool signals to identify events that deserve attention. (Notification generation and ticketing

Traditional SIEM

A SIEM collects security data from organizational systems and security tools, correlates it with other events or threat data, and generates alerts for suspicious or anomalous events.

Next generation SIEM

Next-generation SIEMs use machine learning and behavioral analytics to reduce false alarms and alarm fatigue, and discover hard-to-detect complex events like lateral movement, insider threats, and data exfiltration.

TIER 2 – Prioritization and investigation

Tier 1 analysts prioritize, select the most important alerts and investigate them further. Real security incidents are escalated to Tier 2 analysts.

Finding and exploring data

Traditional SIEM

A SIEM can help Tier 1 and Tier 2 analysts search, filter, decompose, and visualize years of security data. Analysts can easily retrieve and compare relevant data to better understand an incident

Next generation SIEM

Next-generation SIEMs are based on data lake technology that enables organizations to cost-effectively store unlimited amounts of data. They also leverage machine learning and user event behavioral analytics (UEBA) to easily identify high-risk events and display them to analysts.

TIER 3 - Containment and Recovery

Once a security incident has been identified, it's a matter of gathering more data, identifying the source of the attack, containing it, recovering data, and restoring system operation.

Context on incidents and security orchestration

Traditional SIEM

When a real security incident is identified, a SIEM provides context around the incident—for example, what other systems were accessed with the same IPs or user credentials.

Next generation SIEM

Next-generation SIEMs provide SOAR (Security Orchestration and Automation) capabilities. They can be integrated with other security systems and can automatically carry out containment

measures. For example, quarantine a malware-infected email, download the malware, and test it in a threat intelligence sandbox.

TIER 4 – Remediation and Mitigation

SOC staff are working to identify broad vulnerabilities related to the attack and plan mitigation measures to prevent further attacks.

Reporting and Dashboarding

Traditional SIEM

Remediation and mitigation is an ongoing activity, and they require visibility into the status and activity of critical security and IT systems. SIEMs have a cross-organizational view that can provide this visibility.

Next generation SIEM

Next-generation SIEMs leverage machine learning and data science capabilities that create intelligent baselines for groups of users and devices. This allows faster and more accurate detection us.

LEVEL 5 – Evaluation and testing

SOC staff review attack and mitigation steps, collect additional forensic data, make final conclusions and recommendations, and complete audit and documentation.

Compliance Reports

One of the primary functions of a SIEM is to generate reports and audits for regulatory requirements and standards such as PCI DSS, HIPAA and SOX, both on an ongoing basis and following an incident or breach. Get that visibility.

COS measurement

Here are some key metrics that can help understand the volume of activity in the SOC and how effectively analysts are managing the workload.

Important points to remember:

Modern SOCs require collaboration and collaboration between development, operations, and security teams. Increasingly complex infrastructures and the speed of agile processes require skills that security teams cannot achieve alone.

Effective security tools must support all phases of the incident response process. Centralizing information, providing quick analysis, and supporting in-depth research are essential in this regard.

Metrics can help you measure the effectiveness of your SOC processes if used with care. Be sure to include the measurement results in the evaluation and refinement processes.

Metric definition What it measures

Mean Time to Detection (MTTD) The average time it takes for the SOC to detect an incident. The effectiveness of the SOC in handling important alerts and identifying actual incidents

Mean Time to Resolution (MTTR) Mean time until the SOC occurs and neutralizes the threat. How effective is the SOC in gathering relevant data, coordinating a response, and taking action

Total number of incidents per month Number of security incidents detected and handled by the SOC Security environment activity level and scope of controls managed by the SOC

Types of Incidents Number of incidents by type: web attack, attrition (brute force and destruction), email, device loss or theft, etc. The main types of activities managed by the SOC and which preventative security measures should target

Analyst Productivity Number of units processed per analyst: Level 1 Alerts, Level 2 Incidents, Level 3 Threats Detected How well are analysts covering as many alerts and threats as possible?

Case escalation breakdown Number of events coming into SIEM, alerts reported, suspected incidents, confirmed incidents, escalated incidents The effective capacity of the SOC at each level and the expected workload for the different analyst groups.

The future of SOC

The Security Operations Center is undergoing an exciting transformation. It integrates with operations and development departments and leverages powerful new technologies while maintaining traditional command structures and functions to identify and respond to critical security incidents.

We show how SIEM is a foundational SOC technology and how next-generation SIEMs, including new capabilities like behavioral analysis, machine learning, and SOC automation, open up new possibilities for security analysts.

The impact of a next-generation SIEM on the SOC can be significant:

Reduce alert fatigue with User Entity Behavioral Analysis (UEBA) that goes beyond correlation rules to reduce false positives and uncover hidden threats.

Improve MTTD by helping analysts discover incidents faster and collect all relevant data.

Improve MTTR by integrating with security systems and leveraging SOAR (Security Orchestration, Automation and Response) technology.

Enable threat detection by giving analysts quick and easy access to powerful investigation of unlimited amounts of security data.

Answer# 04 **Project Thesis References**

Following are the references used in formulation of my project thesis named;

[**Security as a Service - Challenges and Opportunities for Pakistan**]

- Global Cybersecurity Outlook 2022 by World Economic Forum (In collaboration with Accenture)
- Navigating the 2021 Cyberthreat Landscape by ISACA
- Towards a Digital Single Market for NIS Products and Services - FINDINGS Simon Forge| SCF Associates Ltd – Colin Blackman| CEPS Athanasios Drougkas, Dimitra Liveri | ENISA Validation Workshop| Brussels| 12 October 2016 by (European Union Agency for Network and Information Security - ENISA)
- CLOUD SECURITY REPORT 2021 – Cybersecurity Insiders by ISC2
-
- ASSESSING AND IMPROVING SECURITY AWARENESS AND CONCERNS IN TELEWORKING by Biliangyu Wu
- EUROPEAN CYBERSECURITY MONTH (ECSM) 2020 Deployment Report APRIL 2021 by (European Union Agency for Network and Information Security - ENISA)
- State of Cybersecurity 2021 - Despite Disruptive Pandemic Year, Cybersecurity Workforce Challenges and Opportunities Remain Consistent by ISACA
- A Resilient Cybersecurity Profession Charts the Path Forward (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2021 by ISC2
- Guidelines on Security and Privacy in Public Cloud Computing - Special Publication 800-144 by NIST
- Securonix Next-Generation SIEM Harness the Power of Big Data Using Machine Learning
- https://www.verifiedmarketresearch.com/product/global-security-as-a-service-market-size-and-forecast-2025/
- https://www.okta.com/identity-101/security-as-a-service-secaas/
- https://www.crowdstrike.com/cybersecurity-101/security-as-a-service-secaas/
- https://www.gartner.com/reviews/market/managed-security-services