# ENTERPRISE STRATEGY FOR BUILDING A NEXT-GEN SECURITY OPERATIONS CENTER (SOC)

Narayan Neelakantan

SANS GSEC, GCIH, GWEB
CISA, ISO 27001 LA
Former CISO – National Stock Exchange of India

March 21, 2017

## Introduction

The last few years have re-defined the way organizations approach cyber security. There has been a paradigm shift from a compliance based approach to a risk based approach and the realization that cyber security is no longer an option but a necessity. However, most enterprise security teams are unable to decide on the best strategy to build a robust cyber security capability primarily due to:

1. The fast-paced evolution of threats and mushrooming of products/solutions to mitigate them.
2. Identifying focus areas and building a value proposition for investment in cyber security.

Security Operations Center (SOC) is one such area which is often the most debated due to the complexity and the cost involved in setting up and managing it. This paper attempts to provide a practitioner's perspective to developing a sound strategy on building SOC capabilities.

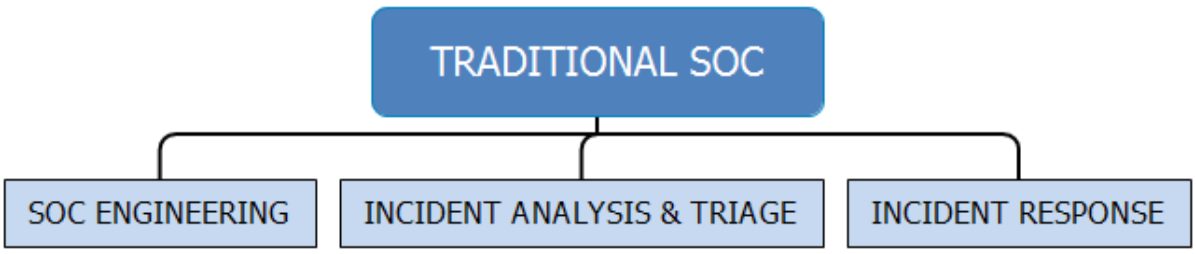
## Security Operations Center (SOC)

Industry experts including Gartner have published numerous articles and papers on the need for enterprises to adopt a holistic approach to cyber security by building detection, response & recovery capabilities rather than relying only on prevention mechanisms. A SOC enables the organization to build and mature detection and response capabilities in a structured and phased manner. It is the first line of defense for an organization and the SOC team is responsible for monitoring, triaging, escalating and responding to cyber incidents and attacks. The key ingredients for setting up a successful SOC is to have the right mix of people, process and tooling.

The capabilities of a SOC along with their implementation methodology have evolved over the last few years, primarily to function more effectively and keep pace with the increased sophistication of cyber-attacks. The Security Operations Center has come a long way from a Network Operations Center (NOC) which also performs security monitoring to a Cyber Defense Center which provides real time monitoring and response capabilities against cyber-attacks. Depending on the maturity and capabilities provided by the SOC, they are generally categorized as traditional or Next-Gen SOC.

## Traditional SOC

A traditional SOC is implemented to maintain vigil on the information security posture of the organization. It involves dedicated analysts assessing real-time security data and manually responding to it. The analysts are deployed in a tiered manner generally called as L1, L2, L3 and so on depending on their skills, expertise & experience. The roles and responsibilities of these analysts are generally part of three main functions as depicted in the below figure.



**SOC Engineering**

One of the key ingredients of a successful SOC is deploying, updating & tuning tools appropriately. The SOC Engineering team is responsible for these activities. For e.g. An SIEM solution must be regularly tuned to ensure that false positives are at an acceptable level and alerts being triggered are in line with the requirements of the organization.

Engineering resources must be skilled in one or more SOC tools/solutions such as SIEM, DLP etc. and have good conceptual knowledge of security with experience of around 5 to 7 years.

**Incident Analysis & Triage**

The alerts generated by tools must be analyzed to identify if the event is worth investigating and can be classified as a potential incident. The triaging process is implemented using methods and processes commonly referred to as playbooks which enable an analyst to analyze alerts in the context of the organization.

This function consists of L1 & L2 analysts with experience in information security ranging from 0 to 2 years and 2 to 4 years respectively.

**Incident Response**

L1 & L2 analysts determine incidents which need to be further investigated and escalate them to the IR team. IR team focuses on these incidents, determines the impact of the incident and initiates appropriate countermeasures for containment and eradication. Contrary to popular belief, IR is not just limited to technical response. It must be looked at holistically from an organization perspective and involve key personnel across the organization such as Legal, PR etc. These personnel should be adequately trained to deal with cyber security incidents.

Drills are an excellent mechanism to test and further fine tune the incident management process. Drills should be conducted periodically as well an unannounced to make sure there is a well-oiled IR process working on the ground.

IR team consists of senior personnel with 8 to 10 years of experience with a solid understanding of information security and the organizations business in addition to knowledge of forensics, investigation methods, tools etc.

**Limitations**

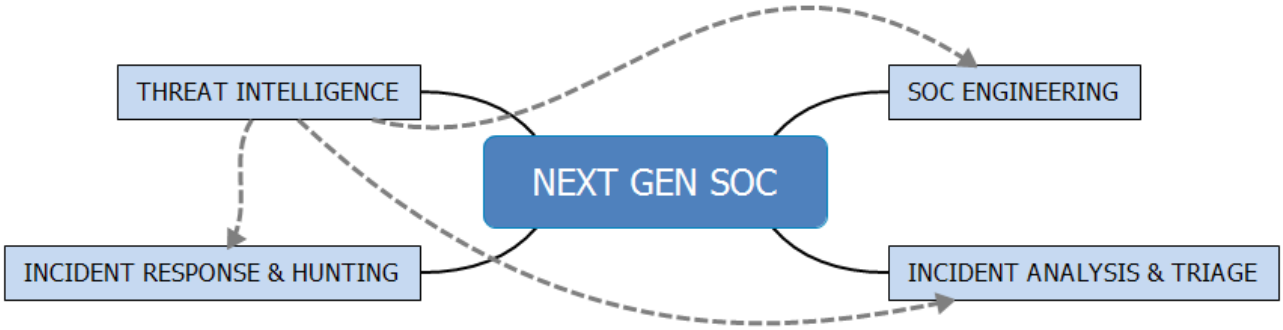
The traditional SOC model has several limitations as outlined below:

1. Traditional SOC's are not geared to detect sophisticated and advanced attacks as they are constrained by the limited visibility provided by tooling and techniques.
2. These models require the analysts and incident response teams to be dedicated and sitting out of the same room. It is a daunting task to recruit and retain skilled personnel for these roles.
3. The time to respond to sophisticated attacks is coming down drastically and the need of the

hour is to build continuous monitoring and continuous threat protection processes. The limited capabilities of the traditional SOC are inadequate to address this requirement.

## Next Gen SOC

The Next Gen SOC or SOC 2.0, attempts to overcome these limitations by building an ecosystem which significantly augments the cyber defense capabilities of an enterprise. In addition to implementing tools such as Network Traffic Analysis (NTA), Endpoint Detection & Response (EDR), Anomaly Detection etc. apart from SIEM, two key capabilities – Threat Intelligence & Hunting transform the traditional SOC into a next gen SOC, as depicted in below figure.




### Threat Intelligence (TI)

Threat Intelligence significantly enhances visibility and the ability to detect advanced attacks. TI is provided by open source communities, vendors etc. and can also be generated by the SOC. TI is generally divided into categories such as Strategic, Tactical & Operational. It enriches the other three functions of SOC and provides the foundation for building the capabilities of continuous monitoring and continuous threat protection. For example, Indicators of Compromise or IOC's are a type of threat intel which consists of C&C IP's, file hashes etc. that essentially are leading indicators of malicious activity and enhances the visibility of monitoring, response as well as hunting activities.

Further, TI integrates with existing tooling to improve detection while reducing false positives. There are standard formats such as STIX/TAXI which have been developed for publishing and consuming threat intel information.

### Hunting

The level of sophistication and targeted approach of current attacks requires a more proactive methodology for detection, if enterprises are to minimize the impact of these kind of cyber-attacks. Hunting leverages the capability of big data and analytics along with threat intelligence to search or hunt for potential malicious activity on historical data or logs.

The objective of Hunting is to identify suspicious patterns which may be a potential indicator of malicious activity. Hunting is either hypothesis or IOC driven, wherein an analyst creates possible threat scenarios and maps out corresponding threat actors and vectors. A data scientist along with the analyst creates an algorithm to identify traces of potential attacks using these vectors. The next step is to run this algorithm on historical data & logs.

Hunting is very effective in identifying patterns of low and slow attacks which are not picked up by real-time monitoring rules of an SIEM.

**Implementation**

Next Gen SoC's may be the enterprise's answer to effectively mitigating cyber-attacks. However, their implementation can be challenging. Organizations need to deploy the right tooling supported by processes and a team with diverse skill sets. This essentially means that SIEM's are not enough, and must include tools such as anomaly detection, UBA, EDR, response automation etc. to improve visibility, threat detection & IR capabilities. Skilled personnel in the security domain continue to be scarce, more so experts in incident response which requires greater understanding of information security in general coupled with the ability and experience to investigate and respond to threats in near real-time. These challenges have led to enterprises increasingly taking the hybrid approach to implement Next Gen SOC.

## Hybrid SOC

Hybrid SOC is an approach for implementing Next gen SOC, and is fast gaining popularity among enterprises. The hybrid approach is the middle path between completely in-sourced & completely out-sourced SOC. It allows the enterprise to selectively outsource services while retaining the ownership and orchestration responsibility with the in-house SOC team. This is particularly beneficial as the in-house team has a much better understanding of the business context leading to a more efficient and effective system for continuous threat monitoring and management. For example, services, such as hunting, forensics and a part of Incident response requiring in depth technical knowledge and experience can be outsourced and orchestration, initial analysis & response can be insourced. The major advantages of hybrid SOC are:

1. Reduced cost of setup and management compared to an in-sourced SOC.
2. Shared threat intel provides greater visibility of emerging threats.
3. The diverse skill requirement of Next Gen SOC ranging from Incident response to Hunting is fulfilled with high quality experienced resources provided by service provider.
4. Significantly reduces enterprise effort in attracting, training and retaining talent.
5. In house security team, which understands the business context complemented by outsourced security experts contributes in enhancing the efficiency and effectiveness of SOC.

## Conclusion

The challenges posed by the fast-changing threat landscape are forcing enterprises to adopt new methods and techniques to effectively protect their organizations from cyber-attacks. The traditional SOC model is not capable of thwarting today's sophisticated cyber-attacks.

Enterprises must evolve and mature their SOC's to Next Gen SOC's. However, the complexity of Next Gen SoC's introduces several implementation and operational challenges. The hybrid approach to building a Next Gen SOC helps overcome these challenges and aids in creating an effective and

efficient SOC for continuous monitoring and management of cyber threats. It is important to note that implementing an orchestration tool & automating SOC processes enable an enterprise to derive maximum value from a hybrid SOC.

## About the author

**Narayan Neelakantan** is a seasoned professional with more than 16 years of experience in Cyber Security, IT Governance, Risk & Compliance and IT Infrastructure.

He is the co-founder & CEO of Block Armour – a blockchain based cyber security product startup. Prior to taking the entrepreneurial plunge, he worked with National Stock Exchange (NSE) as Head – IT Risk & Compliance & CISO.

He has been a visionary and driving force in building NSE's IT Risk Management strategic plan, roadmap, methodology, policies, organizational model, staffing, governance, and reporting from the ground up.

During his role at NSE, he built robust & successful organization wide security programs, including "Governance, Risk and Compliance" and Security Operations Center (SOC) by leveraging his strong Risk acumen and deep technical background in IT infrastructure.

He conceptualized a strategic program to build a state of the art system to strengthen the organization's Situational Awareness & Response capabilities against advanced threats.

As an entrepreneur, he currently consults & offers services to organizations on strategy, implementation & maturing their Cyber Security practice.

Narayan is a well-known speaker at various national and international conferences where he shares his passion, views & concerns on Cyber Security. He also publishes thought leadership articles on Cyber Security. He has been featured on national newspapers.

He is on the advisory board of the Cyber Security Research Institute (UK) and member of several security forums.

You can reach him at narayann@blockarmour.com