IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 16, 2022, accepted March 4, 2022, date of publication March 8, 2022, date of current version March 17, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3157738

Integrated Network and Security Operation Center: A Systematic Analysis

DEEPESH SHAHJEE AND NILESH WARE
Defence Institute of Advanced Technology, Pune, Maharashtra 411025, India
Corresponding author: Deepesh Shahjee (deepesh_shahjee@yahoo.com)

ABSTRACT Traditionally, network and security operation center teams have worked in silos despite commonalities. The network operating center (NOC) team is to provide operationality and availability of information technology (IT) assets, while the security operation center (SOC) team is to ensure IT assets security and protect them from cyber-security attacks. The convergence in IT assets and exponential growth in cyber-security threats in the present digital-online scenario have created many challenges in maintaining network and IT assets effectively and protecting them. It is vital to break these silos and bring them under one integrated unit to effectively counter cyber-security attacks, threats, and vandalism at a reduced operational cost. Despite its necessity, the relevant literature lacks an opinion. It focuses mainly on conceptual segments instead of a holistic view of an integrated NOC and SOC architecture, limiting further innovations in the field. A systematic literature review and analysis is conducted to collate and understand current research ideas in this paper. The mapped relevant literature and our expertise have been then used to propose the implementable state-of-the-art architecture of an integrated NOC and SOC, its definition, the main building blocks and its usefulness for the organizations. Only explicit knowledge of people is considered while neglecting the tacit knowledge in automating and integrating the processes of NOC and SOC, which is the major limitation of the relevant literature. Taping people tacit knowledge is necessary for utilizing the entire caliber of the NOC and SOC integration in the future.

INDEX TERMS Collaboration of network and security operation, integrated network and security operation, integrated NOC and SOC, netsecops, network security operation center.

I. INTRODUCTION

During network inception, network operation was the only requirement for network-based organizations and not even its management [1]. Subsequently, the network operation center (NOC) has become a nerve center to ensure ''power, ping and pipe'' to network computing resources and is measured on uptime service level agreements (SLA) [1], [2]. Meanwhile, organizations have conceptualized a separate security operation center (SOC) to counter rapidly evolving cyber security threats [2]. The SOC consists of people, processes, and technologies (PPT) framework to detect and identify threats and mitigate them before any breach occurs and have become an immune system with a purpose to ''detect, protect, react, and recover'' [2], [4], [34]–[42]. SOC performance is measured on defined response time SLA [2]. Information and cyber security have recently taken the front seat in the present online digital scenario due to the rise in information and cyber security threats. According to the cost of crime report analysis, reported security breaches by organizations have risen by 11% from 2017 to 2018 and a total increase of 67% in the last five years [3]. However, this cost of crime report only shows reported incidents, while incidents not detected may be much higher in numbers. Further, the average time to detect an incident was 196 days in 2018, and 69 days additional on average to mitigate them after its detection [3]. This detection time shows how inefficient organizations are at detecting and neutralizing these threats.

Therefore, integrating NOC and SOC is essential to fully utilize them as nerve and immune centers under one umbrella to overcome cyber threat detection and mitigation inefficiencies in real-time scenarios. However, the NOC and SOC teams are often get siloed and separated while serving different functionalities of the same campaign, which they really should not be [2], [5]–[7]. This siloed environment leads to poor incident response time or SLA in handling various incidents and thereby puts information technology (IT) infrastructure and assets of organizations at significant risk [7], [8].

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio.

Conversely, integrated NOCs and SOCs are more efficient and better coordinated to ensure IT infrastructure integrity, availability with enhanced SLA and real-time threat detection capabilities [7], [9], [10]. However, some routine and common factors such as staff reduction, skill deprecation, less knowledge sharing, privacy compromises, and some intellectual property leakages put the company or organization IT infrastructure at risk. Routinely, NOCs and SOCs are tasked to perform better and extraordinarily, with limited resources struggles to pace organizational growth. Leveraging common NOC and SOC characteristics to build an integrated team responsible for NOC and SOC functionalities is cost-effective and yield better operational efficiencies [11]–[15].

A few research gaps and challenges are revealed while performing systematic literature reviews and analysis of integrated NOC and SOC. The most prominent issues are the lack of an accurate definition of an integrated network and security operation center, its main components or building blocks, and state-of-the-art integrated architecture. Researchers have only covered the idea of integration at the conceptual level, which is at the evolving stage. For some researchers, integration may be carried out at initial tiers, keeping the status quo on others [2], [6], [8]–[10], [12]. For others, the integration team can have a shared pool where they can post all queries, which can be resolved by both team members keeping higher tiers intact [7], [11], [16]–[18]. A few challenges include non-availability of standards, integrated toolsets, insufficient automation, an unwillingness to share data thinking it might be mishandled or misinterpreted, and a lack of cross-team skills. These differences in views and challenges thwart organizations from integrating NOC and SOC and researchers from further innovation in this field [18]. Therefore, the main contribution of this analysis is to close this gap by establishing the veracity for a state-of-the-art architecture for integrated NOC and SOC. Hence, the authors conducted a systematic literature review and analysis to identify and include the current state of the art architecture. Subsequently, we introduce the state-of-the-art architecture of an integrated NOC and SOC resulting from the present scenario.

The structure of the rest of the paper is as follows. In Section I, this paper identifies relevant work. In Section II, the *Preferred Reporting Items for Systematic reviews and Meta-Analyses* (PRISMA) methodology proposed by Moher *et al.* [21] was adopted to carry out this systematic literature review and analysis. Section III is the first part of the main contribution of this analysis. We carried out a systematic analysis of relevant literature to understand the requirement and importance of integration in defining the definition of integrated NOC and SOC and its main components or building blocks. Section IV highlight the usefulness of integrated NOC and SOC vis-à-vis siloed NOC and SOC. Section V is the second part of the main contribution. This part focused on bringing the state-of-the-art of an integrated NOC and SOC from relevant literature. Section VI has proposed future development and research roadmap while identifying other open challenges. Finally, the author concludes with a complete systematic review of the analysis.

II. RELATED WORK

The availability of relevant literature related to state-of-the-art integrated NOC and SOC is rare because of its niche concept, especially its holistic view of integration. An essential issue within a significant part of this literature is that it is very segmented, lacks an agreed opinion, and focuses mainly on conceptual elements instead of a holistic view. Only a few researchers have attempted to define the architectural framework of integrated NOC and SOC in the discovered literature [6], [7], [11], [13], [16]. Though most researchers agree on its necessities, capabilities, efficiencies, and usefulness, there is no explicit agreement of what constitutes an integrated NOC and SOC. Similarly, much literature focuses on distinct attributes of an integrated network and security operation center without paying much attention to the holistic view [2], [10], [13], [51], [52], [55].

Authors have acknowledged a few publications somewhat relevant to our integrated NOC and SOC concepts, which is useful in understanding the integration concept. A few researchers use semi-structured interviews [19], surveys and on-site visits [20], [67], [68] and case studies [7], [9]. Further, interviews, surveys and case studies are used to verify and elaborate on the integration processes of NOC and SOC and their methodologies, and how SOC best practices can be integrated with the NOC for improving in time to detect the incident and its mitigation [7], [9], [19], [20]. The SANS log management survey [67] and cyber threat intelligence [68] survey reports emphasize the inability to differentiate normal from abnormal patterns. Moreover, it is advantageous to use platforms that can build benchmarks by integrating network elements, endpoint security activity and other IT systems compared to non-benchmarked systems [67]. Furthermore, the security monitoring system incorporates threat intelligence according to the observe, orient, decide, act (OODA) loop. This OODA loop helps detect patterns while analyzing network elements, security endpoints, and other log events [68]. Most researchers adopted a bottom-up technique while defining the definition of integrated NOC and SOC methodology [7], [9], which is difficult to understand the integrated concept definition and lacks a holistic view. However, surveys and interviews have provided some understanding into a small segment of particular building blocks of an integrated NOC and SOC but do not allow decisions upon a general state-of-the-art and highlighted its advantages and efficiencies.

Authors notice a paucity of holistic views and identify the status quo in integrating NOC and SOC. There is a need for standardization of terminologies and state-of-the-art architecture further to advance the field of NOC and SOC integration. Therefore, by this systematic analysis of integrated NOC and SOC, the authors initiate the *first step in this approach*.

Further, systematic literature analysis of this paper is different as authors put a heavier weight on quality than quantity

TABLE 1. Search protocol strategy.

Research questions (RQ)	RQ1. What is the state-of-the-art architecture of an integrated NOC & SOC for an organization? RQ2. Which challenges are needs to be resolved in future for holistic development of integrated NOC and SOC?
Search criteria	English Language; Search Keywords are preferred in Title, Abstract and Index Keywords
Search keywords	"Integration" ''Security OR Network'' AND ''Operations'' AND ''Center"
Search methods	Keyword search, backward search, forward search
Inclusion method	Literature having basic concepts of NOC, SOC and detailed architecture of integrated NOC & SOC approaches
Electronic database	Scopus, IEEE Xplore Digital Library, Science Direct, Google Scholar and World Wide Web
Date	January 2000 to September 2021

of the included literature. There is a lack of established norms to date to assess the integrated NOC and SOC literature quality. Therefore, the authors considered the venue of the paper, the proposed solution, and the methodology the researchers adopted for quality assessment. During the analysis phase, we leveraged the integration of NOC and SOC knowledge of the researchers in this analysis and identified the limitations of the proposed solution and its evaluation. The authors further suggested addressing these limitations or improving the integration design.

III. METHODOLOGY

This section introduces the methodology used to conduct this analysis and its adopted search strategy, including the research questions, eligibility criteria, electronic databases, search keywords/methods, and data extraction. The search strategy adopted and research questions addressed by this systematic analysis is shown in Table 1. Despite the practical importance of information security in the present digital era, limited literature is available on integrated NOC and SOC, especially regarding a commonly agreed definition and its holistic view. This limitation makes it difficult for researchers to have rational and creative thinking, which hampers future research, innovation, and development. Therefore, the authors aim to synthesize the relevant literature to establish a state-of-the-art architecture and address the challenges for future research.

This systematic analysis was conducted according to the PRISMA statement, as proposed by Moher *et al.* [21] and incorporated with the other standard guidelines [22]–[25] to tailor this systematic literature analysis for the engineering and computer science domain. This PRISMA flow is primarily adapted for this analysis since it is evidence-based with a minimum set of items for reporting in systematic reviews and meta-analyses. It establishes the quality of the reviews, allows readers to assess strengths and weaknesses, permits replication of review methods, and structures. It formats the review using PRISMA headings, identification and screening, and eligibility and include phases. The PRISMA flow process adopted for relevant literature collection is illustrated in Fig. 1.

A. IDENTIFICATION AND SCREENING PHASE

The records were identified through the following electronic databases: Scopus, IEEE Xplore, Science Direct and Google Scholar. The authors adopted these databases because of their renowned names in engineering, information systems, computer science, and cybersecurity. The search is focused mainly on mapping existing literature on the integration of NOC and SOC and in the fields of engineering and computer science. The search then further curtailed for cyber and information security, network management and operation, network security intelligence center, network topology and security, security information and event management (SIEM), information security incidents, computer emergency response team (CERT), security intelligence centers, and data triage fields.

The search was conducted from January 2000 to September 2021. All articles published before January 2000 were dropped. Only English language papers were included in the systematic literature analysis as an exclusion criterion. The following *search keywords* are used, viz., "Integration" "Security OR Network" AND "Operations" AND "Center," which resulted in a large number of results, though only a few portions are relevant to our analysis. Full-term "Network Operation Center" and "Security Operation Center" are applied to identify relevant literature and filtered with "integration" OR "combined" terms. The abbreviations

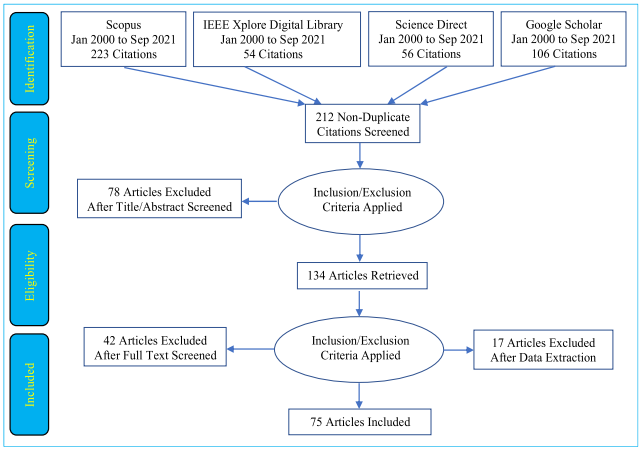

FIGURE 1. PRISMA flow diagram.

"NOC" and "SOC" are not considered for literature search because it also abbreviates "network on a chip" (NoC) and "system on a chip" (SoC), which produces an immense number of other results.

During this Screening process, a total of 439 articles/ literature are filtered from selected electronic databases for further processing. After that, records screening was carried out thoroughly on 439 records to remove the duplicities. A total of 212 records are taken for further systematic analysis by dropping 227 records based on duplicity filter criteria.

B. ELIGIBILITY AND INCLUDE PHASE

During this eligibility and include phase, the quality assessment process is administered to genuine and peer-reviewed research articles, reviews, conference papers, books, and website pages. For example, articles were included in the review process only if the abstracts were on NOC, SOC, and integration of NOC and SOC further to maintain the quality and relevance of the research literature.

A total of 134 articles were retrieved after applying first stage inclusion/exclusion criteria based on abstract/title screening. Finally, 75 articles were selected for systematic literature review and analysis after applying second stage inclusion/exclusion criteria and data extraction on the full-text screening. The data extracted features were: article to be genuine, peer-reviewed and original paper, review paper, conference paper, books, and web pages. Table 2 lists the electronic database wise literature results.

TABLE 2. Electronic database wise search result.

Electronic Database	Search Criterion	Sum
Scopus	Title, Abstract & Keywords	223
IEEE Xplore Digital Library	Document title, Abstract	54
Science Direct	Title, Abstract & Keywords	56
Google Scholar	Title of the Article	106
Total		**439**
Articles left after duplicate removal		**212**
Articles left after selection criteria		**134**
Articles selected for review and analysis		**75**

IV. FINDINGS AND INTERPRETATION

The previous section showed how the research methodology was adopted to obtain relevant NOC and SOC integration literature. This section introduces the first part of our main contribution. We analyze the literature and present the findings and interpretations of data collection sets. Fig. 2 illustrates the year-wise publications of the extracted research papers. The graph shows the trends of security and network operations and their integration concept, which is exponentially high in 2021. The authors expect the same trends in the future since the online and digital scenarios have taken the front seat during this pandemic. Therefore, to improve the information security posture of an organization against the increased cyber threats in the present online and digital era, the authors see the necessity to establish the state-of-the-art architecture of integrated NOCs and SOCs.

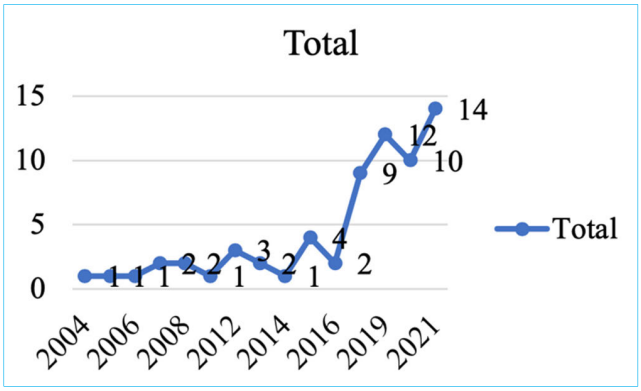

FIGURE 2. Year wise research literature trend.

The authors divided this part of the research analysis into the definition, integrated NOC and SOC architecture, and building blocks of an integrated NOC and SOC. The relevant research literature on these topics is presented in Table 3.

TABLE 3. Literature of definition, architecture & building blocks.

Topic	No of Articles
Definition	20
Integrated NOC & SOC architecture	8
Building Blocks of Integrated NOC & SOC	6

A. DEFINITIONS

This section briefly introduces some of the definitions that are related and ambiguous to an integrated NOC and SOC scenario. Integrated NOC and SOC are complex unit structures encompassing network and security operations and management [7], [11], [16], [26], [27]. Integration is a system of systems concept that handles network and security campaigns using network devices, software, and other infrastructure to manage its overall operation and maintenance, and to enhance the organization overall security posture round the clock, i.e., 24 / 7, 365 days per year [28]. Integrated NOC and SOC can improve the overall organization security posture [5]–[7], [9]–[11], [13], [16]–[18], [30], [31]. However, there is no clear terminology or proof of concept describing the integrated NOC and SOC. The succeeding paragraphs delimits integrated NOC and SOC from other related terms:

1) NETWORK OPERATION CENTER

A network operations center is also known as a "network management center". It is single or multiple locations from where network operation and management are exercised over the organization infrastructure. Network management tasks, such as faults, performance, configuration, administration, and security (FCAPS), are managed by the NOC team adopting the FCAPS model [26]. For example, in a telecommunication scenario, NOCs are responsible for monitoring equipment failures, access networks, connectivity, alerts, events, and performance issues that may affect the telecom

network and services [26], [27], [32]. Thus, one can say that NOC is the basis of an organization nervous system [2].

2) SECURITY OPERATION CENTER

The SOC consists of analysts, operators, and subject matter experts who monitor security endpoints, sensors, IT infrastructure, applications, and services. They use various technologies and processes as per invoked organization policies to deter IT infrastructure misuse and policy violation from preventing and detecting cyber threats and attacks, security breaches, and online abuse and respond to cyber incidents [34]. Holistically, it represents overall organizational security vision and strategy. It uses either PPT or People, processes, technologies, governance and compliance (PPTGC) frameworks to manage the entire security campaign of an organization [4], [34]–[42], [48]. This operational methodology is accomplished by a system of systems architecture rather than a single system. It also creates security awareness in mitigating the exposed risks and helps to fulfill the organization security posture.

3) SECURITY INTELLIGENCE CENTER

The security intelligence center (SIC) term was first used in 2017 as the successor of SOCs''. The SIC aims to provide a more holistic, integrated view than a SOC, which can fully visualize and manage security intelligence in one place. [43]. Therefore, numerous technologies such as knowledge management, big data analytics, and information security have been combined [44] from various other terms and terminologies of NOC and SOC.

4) INTEGRATED NOC AND SOC

While mapping the literature, the authors saw the lack of commonly agreed-upon terminology and definition for an integrated NOC and SOC due to existing tools and agencies between siloed NOC and SOC. Definitions vary widely, making it difficult to understand the integrated NOC and SOC and how it is efficient and advantageous from silos operation methodologies. To have a clear definition of an integrated NOC and SOC, the authors define its know-how and know-why of an integrated NOC and SOC and put it in a nutshell as driven by the relevant literature below:

''The merging of NOC and SOC is a continuous integration and continuous development campaign at strategic, operational, and tactical working culture vis-à-vis its technologies, processes, and people for the better security posture of an organization. Integrating NOC and SOC cannot be completed by a single system but rather by using a system of systems. It is a management of the FCAPS, use of OODA loop, and plan, check, do, act (PCDA) cycle, intelligence cycle, triaging, collaborating, cross-correlating, SLA, standard operating procedures, and identifying common patterns from the integrated tools and dashboards. It is a team of integrated NOC and SOC analysts and subject matter experts of defenders by cross-training them to expand their range of skills, adjust their mindsets, tap each other skillsets, and experience to identify, manage, and resolve incidents or faults effectively and to counter the rough attackers. It creates situational awareness, mitigates the exposed risks, and helps fulfil regulatory requirements. When an incident occurs regarding a NOC and SOC specific issue, there is shared accountability and authority among the integrated team of defenders on triaging, remediating, handling, and making recommendations to stakeholders and system-owners of the respective impacted system.''

B. ARCHITECTURE OF INTEGRATED NOC & SOC

While the previous section defines the integrated NOC and SOC, in this section, the authors analyze the available literature on the architecture of NOC, SOC, and integrated NOC and SOC. From the relevant literature, the architecture of an integrated NOC and SOC primarily consists of three elements: personnel, processes, and technology. Networks and cybersecurity technologies are constantly evolving; it is essential to understand their infrastructures, current processes, procedures, policies, and other controls in the organizations/industries and how these elements are controlled and monitored. The comparative research aims to develop a state-of-the-art holistic architecture of an integrated NOC and SOC. The comparative research aims to develop a state-of-the-art architecture that can be implementable in organizations. Towards this, validation of state-of-the-art architecture has been carried out using the ''*Delphi Technique*'' at the elemental level by seeking a consensus from the experts in the field of network and security operation centers of an organization through a series of questionnaires [71]. Though, it is highlighted that the integration of network and security operation centers is a continuous process due to fast-evolving technologies in the present digital and cyber- security era. Therefore, architecture or framework are rarely mature; it is just a version, as one will see new things over time that may not be reflected in it. Part one covers three different general architectural approaches applied to NOC, SOC, and integrated NOC and SOC designs throughout the literature. At the same time, part two of this section aims to develop a state-of-the-art architecture of an integrated NOC and SOC from the relevant literature. The distribution of related literature on NOC, SOC, and integrated NOC and SOC is listed in Table 4.

TABLE 4. Literature on NOC, SOC, integrated NOC & SOC and reports.

Architecture	No of Articles
NOC	09
SOC	15
Integrated NOC and SOC	35
Threat Reports	04

1) GENERAL NETWORK ARCHITECTURE

Network architectures are classified as centralized, distributed, and decentralized based on the network architecture depicted in Fig. 3 [46]. Centralized architecture describes

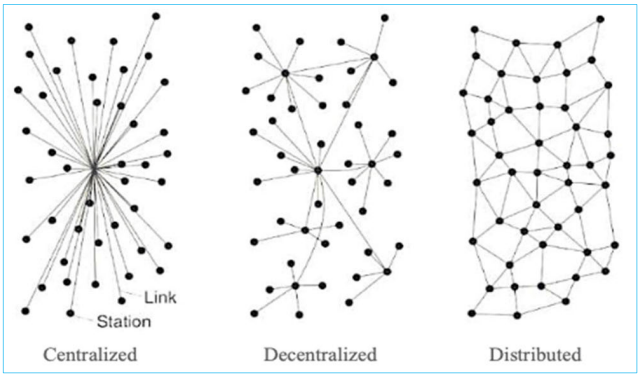

FIGURE 3. Different types of networks.

wherein different network/data resources are placed at various locations and managed from one central location.

A distributed architecture resembles one single system operating across several subsidiaries. It appears for users as if they are dealing with one entity. The distributed system enables all entities to retrieve, process, combine, and provide information and services to other entities [46]. It allows for evenly sharing workload and data among all distributed networks.

In a decentralized architecture, the concept of centralized and distributed architecture collaboration takes place [44]. A decentralized network comprises a few networks with possibly limited capabilities reporting to one or more centralized networks. While mapping the previous literature with current, a remarkable shift is observed from centralized to decentralized networks. The main reason for this shift in design architecture is probably to build more redundancy and to avoid a single point of failure [4], [26], [46], [47].

2) NOC ARCHITECTURE

NOC is the nerve center of an organization with different roles and responsibilities that ensure the availability of a network with the required speed and performance for its stakeholders [2], [14]. As per Chavan [26], the earliest NOCs began in the 1960s. A network control center opened in 1962 by American Telephone and Telegraph Company (AT&T) in New York uses status boards to display switch and routing information in real-time from AT&T most important toll switches. Later, AT&T enhanced the network control center with a modernized network operation center in 1977. A NOC model with an end-to-end communication service provider (CSP) architecture is shown in Fig. 4. This model defines a NOC, which consists of five layers: the display of alerts and messages layer, business support system (BSS) layer, operation support system (OSS) layer, network management system (NMS), FCAPS layer, and an element management system (EMS) layer [26], [32].

3) SOC ARCHITECTURE

SOC is the immune center of an organization with different roles and responsibilities. It follows either PPT or PPTGC

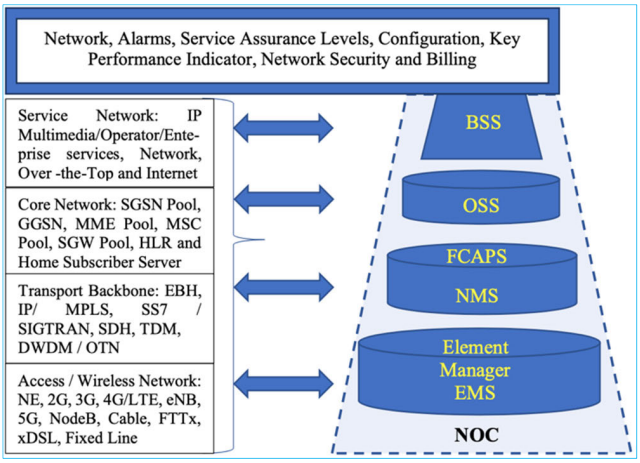

FIGURE 4. NOC architecture: end-to-end CSP network.

framework for the real-time security operations and management [4], [34]–[42], [48]. To analyze cyber and security incidents, it follows a tiered approach of triage, analyses, and neutralizing it, or else escalating the issue to higher tiers for subject matter experts for detailed analysis. Fig. 5 depicts the architecture model of SOC, which shows four components: data collection, data processing, correlation analysis, and visualization [37]. One of the SOC models proposed by Bidou *et al.* [48] defines SOC, which consists of five parts: event generators, event collectors, message databases, analysis engines, and reaction management software. The SOC box architecture has certain limitations in the present scenario, as it is almost a decade old. The SOC box architecture is a centralized system with numerous single points of failure. With the complexity of current information technologies, landscapes, and technological developments, distribution-based architectures are more appropriate. Subsequently, the SOC box architecture has undergone many changes to compete with the present evolving technologies. Its immediate successor is the distributed security operation center (DSOC), as proposed by the same authors Bidou *et al.* The DSOC architecture lays the foundation for the distributed

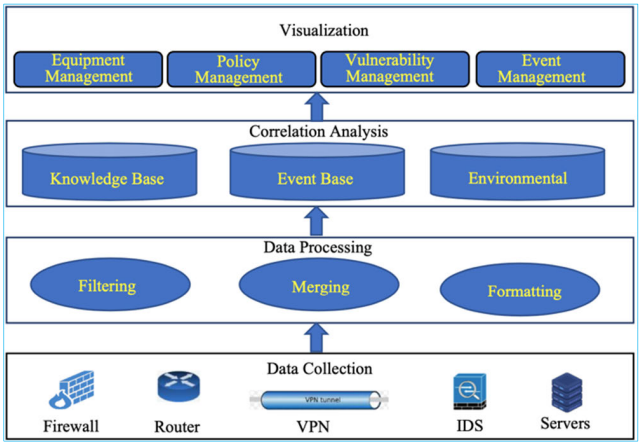

FIGURE 5. The architecture of SOC.

TABLE 5. Classification of literature of NOC & SOC commonalities.

Relevant Literature	Classification of literature: NOC & SOC Commonalities			
	Infrastructure	personnel	process	Technology
Hernandez, 2018 [7]	✓	✓		
Goodchild, 2009 [9]	✓	✓		✓
Hae *et al.*, 2016 [16]	✓	✓	✓	✓
Miloslavskaya, 2018 [11]	✓	✓	✓	✓
Extrahop, 2018 [49]	✓	✓	✓	✓
McGillicuddy, 2019 [6]	✓	✓	✓	
McGillicuddy, 2020 [50]	✓	✓	✓	
Amy and Karnam, 2012 [51]	✓	✓	✓	✓
Bea, 2020 [30]	✓	✓	✓	✓
Bocetta, 2021 [12]	✓	✓	✓	✓
Chon and Jaeger, 2007 [2]	✓	✓		✓
David, 2008 [8]	✓	✓	✓	✓
Fortinet, 2018 [52]	✓	✓	✓	✓
Lackey, 2021 [13]	✓	✓	✓	✓
McGillicuddy, 2019 [53]	✓	✓	✓	
Miloslavskaya, 2021 [54]	✓	✓	✓	
Morrison, 2018 [55]	✓	✓	✓	✓
Rebasoft, 2021 [15]	✓	✓	✓	✓
Roberson, 2019 [19]	✓	✓	✓	✓
Udeshi, 2018 [56]	✓	✓	✓	✓
Weinberg, 2020 [18]	✓	✓	✓	✓
Total	21	21	19	16

grid SOC (GSOC) architecture for critical infrastructures. These architectures show a shift from a centralized to a distributed SOC architecture over time to avoid single-point failure.

4) INTEGRATED NOC & SOC ARCHITECTURE

The general architecture of integrated NOC and SOC is either centralized, decentralized, or distributed [47] according to the strategic choice of the organization. As the architecture of NOC and SOC has adopted the framework of people, processes and technology or people, process technology, governance, and compliance [20], [26], [27], [34], [35], [37], [39], [41], it is advantageous to integrate NOC and SOC under one umbrella for enhanced efficiencies, cost-effectiveness, and improved SLA [7], [11], [13]–[15], [18], [19]. The relevant literature reveals that integrating NOC and SOC is advantageous in improving the SLA of network and security by integrating either at all tiers or a few tiers [7]. Regarding the integration of NOC and SOC, the identified literature mainly suggests the integration concept because it has commonalities in NOC and SOC infrastructures and operations, personnel knowledge, processes, and detection technologies. The classification of relevant literature to show the state-of-the-art methodologies is shown in Table 5. Therefore, a well-accepted literature classification scheme of N. Hernandez [7] and Hae *et al.* [16] is used.

For some researchers, integration at all tiers is beneficial for streamlining incident management processes [11], [16]. However, for other researchers, complete integration only at tier one and a few shared workflows with shared ticketing at higher tiers are recommended [5], [7], [13], [14]. It further defines that the integration introduces powerful synergies between SOCs and NOCs via people, collaboration, toolkits, and techniques. Full integration is the complete solution at all tiers, although work is in progress and needs continuous refinement as per the latest emergent technologies and cyber threats [11]. Researchers agree to integrate NOC and SOC as per the relevant literature because it is operationally viable, efficient, effective, and cost-attractive. Conversely, they differ in the extent to which integration is required between NOC and SOC [6]–[8], [11], [12], [15], [16], [30].

Furthermore, the integration of NOC and SOC is viable because the operational methodologies are mostly identical at their initial tiers, as both use similar tiered structures of monitoring and response teams. In addition, they share the same toolkits, analyst workstations, dashboards, SLA, ticketing systems, helpdesks, investigation teams, and triage of reported and detected incidents. However, some differences exist at higher tiers, primarily in subject matter experts (SME). Their union would be better sensemaking with situational awareness from a long-term perspective, as the NOC primary concern is providing infrastructure availability with

TABLE 6. Duties and responsibilities of an integrated NOC & SOC.

Duties and Responsibilities of an Integrated NOC and SOC Team	
Tier one	**Alert-Triage Analyst**: Proactive alarm or alert monitoring 24 / 7, 365 days per year. Continuously monitors the alert queues. Triages network and security alerts, issue tickets and manage as defined SLA. Fault and incident management through health & alerts status monitoring of network elements and security endpoints sensors. If required, collect data, perform analysis, and escalate the case to higher tiers.
Tier Two	**Fault-Incident Responder**: Network and security management support. The root cause analysis and change execution support and performs deep-dive incident analysis by correlating data from various sources. Determines if a critical IT infrastructure or data set has been impacted. Advises on remediation and supports new analytic methods for detecting threats, co-ordination with security, network and IT infrastructure vendors. Escalation of the case, if required.
Tier Three	**Network-Threat Hunter SME**: Change validation and fault management, coordination with network and IT infrastructure and network management through FCAPS model. They process in-depth knowledge of network elements, security endpoints and sensors, threat intelligence, forensic and malware reverse engineering. Also, have know-how functioning of the specific application or underlying IT infrastructure. Acts as an incident hunter, not waiting for escalated incidents only. Deeply involved in threat detection analysis, its development, tuning and implementation. Reporting and analysis and improvement suggestions.
Tier Four	**Integrated NOC and SOC Manager**: Management of resources such as people, shift scheduling budget and technology. Strategy to meet defined SLA. Communicate with management. Serve as organization point person for business-critical infrastructure incidents and extend directions for the integrated NOC and SOC and input to the organization network and security strategy.

the required performance. In contrast, the SOC ensures overall organization security and integrity [7], [16]. For example, when a performance bottleneck is detected, the NOC team members may attribute the problem to the network element failure and fix it by replacing the complete network unit or reconfiguring the network parameters. Conversely, for the same issue, the SOC team members may attribute the problem to unwarranted hacking activities, thus prompting a detailed investigation [18].

Therefore, an integrated approach can quickly resolve such issues in a real-time scenario. In addition, it paves the way for powerful synergies between NOC and SOC through the PPT framework in tiered monitoring, incident response, service recovery of infrastructure growth, and complexities [16].

C. BUILDING BLOCKS OF AN INTEGRATED NOC & SOC

In the previous section, we examined the architecture of the NOC, SOC, and integrated NOC and SOC. In this section, our main contribution is to highlight the building blocks of an integrated NOC and SOC. The architecture of NOC and SOC were analyzed previously, paving the way for defining processes to refine functions and operations, selecting the right technology to make efficient operations, and cross- training the right people with the right skills to handle integrated technology of both NOC and SOC scenarios simultaneously [16], [27], [34], [35], [37]. People, processes, and technology are the core building blocks of integrated NOC and SOC, as depicted in Fig. 6. Therefore, the people, process, and technology framework allow the authors to define an integrated NOC and SOC and its building block components cohesively [35], [58] and explained in the following paragraphs.

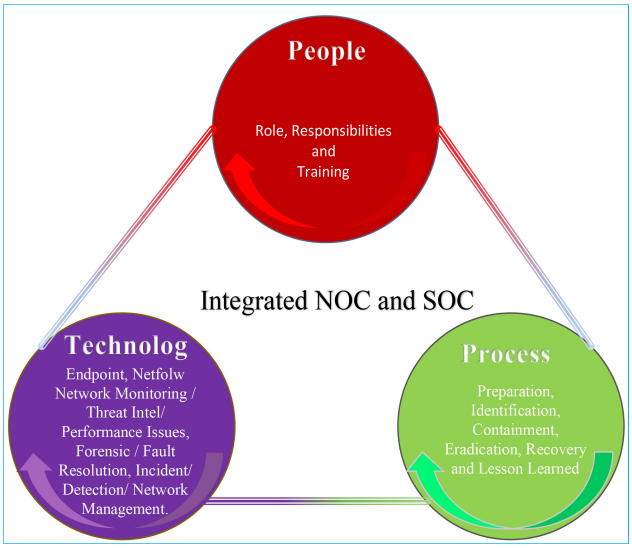

FIGURE 6. Building blocks of integrated NOC and SOC.

1) PEOPLE

As seen from the relevant literature, NOC and SOC teams share the same working methodology at their initial tiers, such as monitoring events, escalating issues, providing triage on incidents, and up-channeling communications [26], [27], [32], [34], [35], [57], [58]. However, at higher tiers, some differences are apparent in the roles and responsibilities of subject matter experts [7], [10], [15], [19]. Both teams monitor and analyze events on respective dashboards coming from various network and security endpoint sensors throughout the infrastructure, utilizing similar tools to maintain vigilance of the enterprise network [11], [12], [18], [16].

TABLE 7. Training courses for an integrated NOC & SOC team.

Task Title	Required Training Syllabi for Integrated NOC and SOC Team Personnel
Tier one (Operator)	Alert and events triage methodologies, intrusion protection & detection, network & security-based tools such as SIEM, host- based investigative training, and other tool-specific training. Training could include SANS and Koeing certification such as Security Essentials Bootcamp (SEC401) CompTIA Network+ (N10-008) and Network Essential (Koing).
Tier two (Analyst)	Network, security and host-based forensics, basic threat intelligence and normal malware assessment, incident response and log reviews methodologies. Training could include SANS and Koing certification such as Intrusion Detection In-Depth (SEC503), System and Network Security Introduction (Koing) and Cisco Network Security Audit (Koing), Advanced Security Essentials & Enterprise Defender (SEC501), Troubleshooting Networks with Wireshark Certification (Koing), Hacker tools, techniques, exploits and incident handling (SEC504).
Tier three (SME)	Training on network configuration, tool-specific training for data aggregation and analysis, threat intelligence, network and security with VPN configuration and anomaly-detection. Training could include SANS and Koeing certification such as intrusion detection in-depth (SEC503), Hacker Tools, Techniques, Exploits and Incident Handling (SEC504), Intense Hands-on Pen Testing Skill Development (SEC561), Reverse-Engineering Malware (FOR610), Malware Analysis Tools and Techniques. Cisco Network Configuration and Security with VPN Certification (CCNA and CCNP security courses) Koeing.
Tier four (Manager)	Project management course, general people management skills, network management and incident response management training. Training could include CISSP, CISA, CISM or CGEIT. "Cisco Certified Network Associate (200-301 CCNA)". PRTG Network Monitor (Koing), RSA NetWitness Platform Foundations 11.3 (Koing), RSA NetWitness Logs & Packets Administration & Operations (Koing).

Integrating NOC and SOC teams at various tiers will result in better synergy in utilizing both team expertise and improving operational efficiency by multitasking, cross-training, and knowledge sharing between team members [7], [16]. For example, the NOC team has expertise in network support and in-depth knowledge of network protocols such as transmission control protocol (TCP), internet protocol (IP), and open systems interconnection (OSI) layers [26]. At the same time, the SOC team prerequisite is to have in-depth knowledge of organization network configurations and protocols, security/cyber threats know-how, and network protection methodologies [34], [58]. Therefore, having two siloed teams for identical tasks at various tiers can lead to many issues such as loss of productivity, communication ambiguity, delay in trouble resolution, and data breaches. Roles and responsibilities, training, and collaboration are sub-stepping blocks of people elaborated in the following paragraphs.

- **Role and responsibilities**: The role and responsibilities of an integrated team can be formalized by tweaking the existing roles and responsibilities of the NOC and SOC teams. As per work, size, scope, and 24 / 7, 365 days per year continuous operation, different analysts, subject matter experts, and a manager are required per tier hierarchy. Having numerous parallels between NOC and SOC, the authors derived three roles and responsibilities for an integrated NOC and SOC, viz., analysts, subject matter experts, and a manager from relevant literature, which are listed in Table 6.

Various roles and responsibilities, for example, at tier one or two, the operator or analyst tasks of both NOC and SOC are fairly easy and similar [7], [26], [41]. At tier three, subject matter experts handle escalated matters requiring specialized triage methods as it contains both network and security incidences [7], [35]. However, as per some researchers, with cross-training, on-the-job training (OJT), this limitation of different skillsets can be overcome, which paves the way for the integration of NOC and SOC at all tiers [6], [14], [16], [18], [55]. Further, with the convergence of IT infrastructure and security, the thin demarcation line between them becomes more complicated and ambiguous as more advanced cyber-attacks tend to cover their footprints by multiple hops between numerous IT infrastructures. For example, the famous ''*stuxnet pen-drive-based advance persistence attack*'' was successful because of silos working between NOC and SOC. Having integrated NOC and SOC teams could have detected the potentially common patterns of attack by the correlation between alerts and events on their respective integrated tools by subject experts instead of the siloed operation of monitoring network faults and security events alone [16].''

- **Training**: Cross-training is the key for multitasking in an integrated NOC and SOC scenario along with readjusting the first line of defenders for better sensemaking and situational awareness to encompass both network and security spectrum [14], [16], [50], 55], [56]. Highly trained and multitasked employees are more beneficial and productive, as they appreciate their roles and responsibilities. Further, training strengthens their core working methodology and resolves knowledge gaps, and work quality and consistency are enhanced many fold [16]. In due course, training personnel always benefit the organization since trained personnel tend to resolve problems quickly with minimum human errors. A study conducted by Accenture and Ponemon Institute revealed that the overall cost of hiring experts to a company is decreased drastically by imparting higher training to employees [3]. Multitasking by OJT or shadowing more experienced team members is another form of imparting the necessary skills [60].

With the above discussion and relevant literature, we can frame training syllabi for personnel placed in an integrated NOC and SOC scenario. Both teams require cross-training and multitasking with each other subject matter to make the integrated team self-reliant [16]. The tasks of analysts, SME, and managers are highly technology-driven, evolving, and demanding. Therefore, the integrated NOC and SOC team requires continuous training to handle such tasks. [7], [14], [16], [26], [55]. The required training syllabi as proposed for personnel working at an integrated NOC and SOC are listed in Table 7. In addition to operators, analysts and SME, integrated NOC and SOC also require an overall manager for its complete management [7], [26], [35].

The responsibilities of an integrated manager are to look after entire work processes and organizational IT infrastructure resource handling to provide, protect, and connect. The organization of the integrated NOC and SOC is shown in Fig. 7.

- **Collaboration**: Collaboration is a unique methodology of an integrated scenario that requires team members to manage as per the FCAPS model while ensuring the availability of the overall organization IT infrastructure as per defined SLA [7], [26]. Shamus McGillicuddy emphasizes the need for integrated tools, logs, and data that are crucial for the collaboration of NOC and SOC [5], [54]. According to Karnam *et al.* [51], the collaboration of a shared knowledge talent pool is essential for an integrated NOC and SOC. The integrated team success must have constant hand-holding, interaction, and unambiguous communication for smooth operation [29], [30], [49], 53], [56].

2) PROCESS

The previous section showed how the relevant literature on people applies to an integrated building block. This section focuses on the processes related to the second building block of an integrated NOC and SOC. Different processes are part

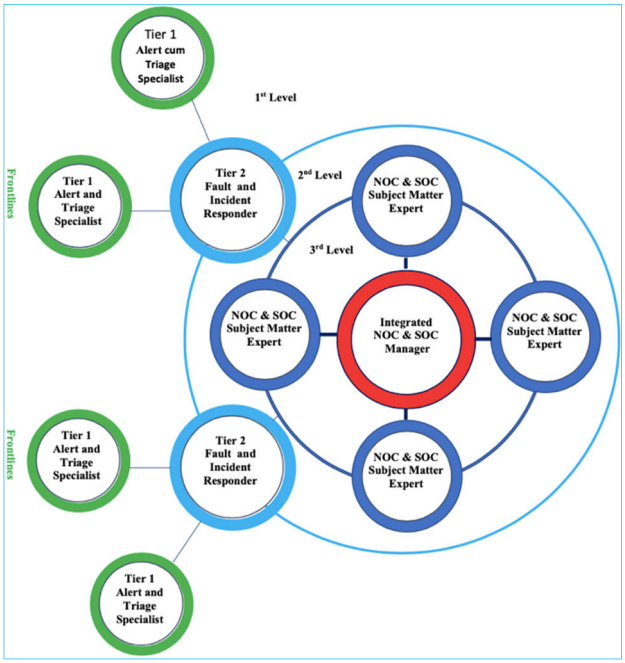

FIGURE 7. Organization of integrated NOC and SOC.

of the network and security operations, which are similar in their functionalities. For example, almost two identical help desk processes exist, viz., one at the NOC and another at the SOC. An integrated helpdesk is created by merging the existing helpdesks [16]. Case management is another process that is merged, because it also follows the tier-escalation methodology. For example, the responsibilities of case creation and alerts at an initial tier for its evaluation and further escalation to higher tiers are defined in this process. Furthermore, resources are effectively allocated based on the workflow and criticalness [7], [12].

An integrated NOC and SOC aim to manage the network as per the FCAPS management model [26] and to define security endpoints and sensors, protect the overall network, recover and respond to or prepare for incidents, and ensure the availability of IT infrastructure [41], [58]. One way to structure the underlying processes is through the incident response lifecycle and FCAPS model management.

In addition, the OODA loop and PCDA cycle concept process are seen in the evaluation of threats to defend, recover, and manage networks or similar frameworks, as presented in ISO/IEC 27035:2016 [26], [42], [58], [59], [61]–[64]. The commonly used incident response process is based on the Computer Incident Advisory Capability (CIAC) model of the United States, department of energy (DOE). This model consists of six stages: preparation, identification, containment, eradication, recovery, and lessons learned. Cichonski *et al.* [65] proposed an incident response lifecycle consisting of four steps: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity. The integrated NOC and SOC approach facilitate information sharing, availability, and close collaboration

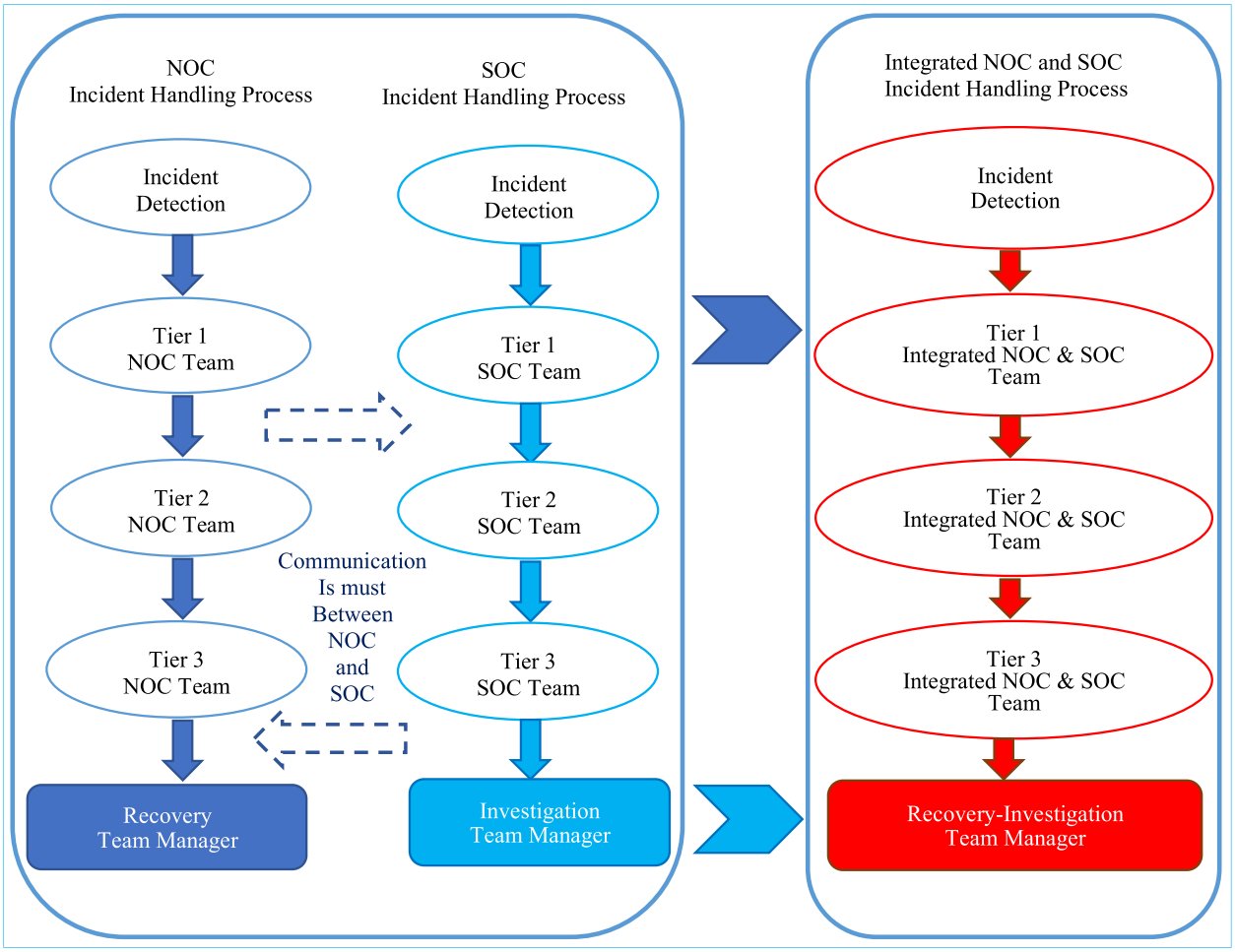

FIGURE 8. Integrated NOC & SOC process management.

among the integrated team members compared to siloed team operations. [2], [7], [8], [11], [14]–[16], [19], [30], [50]. The integration of siloed NOC and SOC processes for ease of information sharing and collaboration, as seen in the relevant literature, is as follows:

- **NOC and SOC process integration:**Two different NOC and SOC processes can be integrated, reconfigured, and automated based on commonalities under the integration approach [16], [52]. For example, instead of manning two separate incident response helpdesks for NOC and SOC (handling basic calls and ticket generation), a single integrated helpdesk manages NOC and SOC calls, incidents, and ticket generations can be formed, as shown in Fig. 8. The integrated helpdesk team can perform tier-one analysis using the integrated tools and techniques to identify a performance bottleneck or cyber incident and route the incident accordingly to tier-one response teams. If the incident is critical or severe, it can be escalated to either the second or third tier for in-depth investigation and timely resolution. Subsequently, an automated fault or incident identification and switching process can be created to route the task to the respective recovery teams without involving any operator.
- **Integrated Case Handler**: All incidents are tracked and handled via an integrated case handler and stored at a data center or warehouse for knowledge management. Case monitoring is performed automatically via its status and escalated if the case is critical or unrecoverable as per predefined fixed SLA. Further, after each case resolution, the subject case resolution methodology is stored at the knowledge management data center for operator reference for similar case resolution, if any, in the future. This methodology further improves triage accuracy and reduces service recovery lead time, and improves SLA [14], [18], [42].
- **Integrated Process and Case Handler as Design Enabler**: The integration of NOC and SOC processes and case handler as enabled by the collaboration of NOC and SOC makes it more modular for operators to perform their tasks smoothly. This integration enables the operator to work efficiently and focuses on core strategically defined incident management and service recovery tasks. In addition, this will require less OJT with minimum maintenance to perform better tasks.

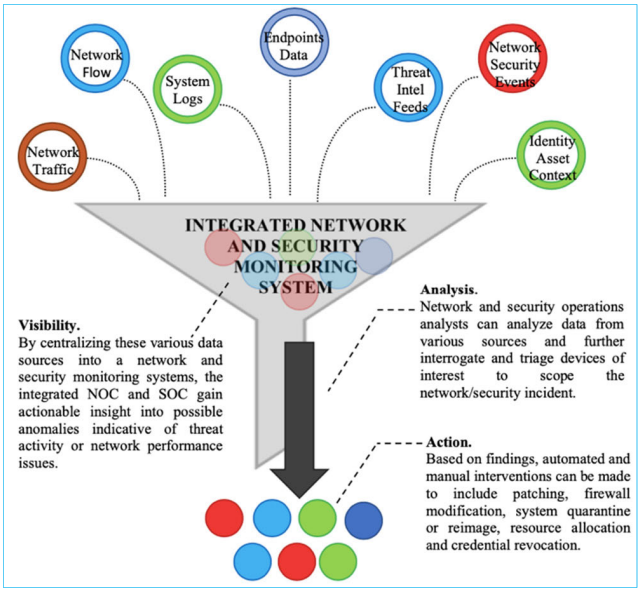

FIGURE 9. Compatible technology aid detection.

3) TECHNOLOGY

Having seen people and process building blocks in the previous sub-section, the technology and its know-how are elaborated in this section, as seen in the relevant literature. The data aggregator collects data from the integrated network elements and security endpoints from the fault, configuration, performance, and recovery management processes. These information aggregator/integrators, incident detection, analytic, and overall management solutions are the technology enablers for the successful integration of NOC and SOC [7], [16], [19], [30], [56].

Integrating network and security dashboards is feasible in the present era of technology enablers. The integrated dashboards incorporate real-time data as received from interconnected network elements, security endpoints (PCs, laptops, mobile devices, switches, and servers), and data from various other log aggregators and event generators [9], [49]. This integrated dashboard acts as a force multiplier for analysts because it displays real-time data logs and events with correlated data analytics, which helps analysts pinpoint the actual cause of any incidents or faults that could have been difficult in siloed operations [52], [54], [66]. As mapped from relevant literature, compatibility of technologies is crucial, and data separation in siloed operations is harmful in the present era of information and cyber security. Therefore, the integration of data from all network elements and security endpoints is imperative when reporting into the incident management solution, as depicted in Fig. 9, for compatible technology aid detection [8], [26], [43], [51], [54]. Further, the integration of NOC and SOC architecture is now achievable with the present network and security technologies by adopting the following methodologies:

- **Corelating to Security Incidents**: For some researchers, integration of threat intelligence, asset, identity, and other situational information is also an effective security monitoring solution that can assist the analysts in investigation process management [7], [11], [16], [17], [42]. For example, an alert is raised based on network activity, which may contain only the suspicious endpoints IP address. To investigate suspicious endpoints, analysts require other information at the incident alert for its correct correlation. The required information is a hostname, owner of the suspicious endpoint (laptop or computer), dynamic host configuration protocol (DHCP), and sourced records for tracing and mapping of IP. Therefore, it is better to incorporate all the network and security assets and identification information in an integrated NOC and SOC monitoring dashboard because it improves the organization SLA.
- **Benchmarking:** As mapped from relevant literature, it is better to build a benchmark for the activities of users, applications, network elements, and other security endpoints. This establishes and verifies normal from abnormal behavior and acts as a force multiplier when data are collected and integrated from complete network elements and security endpoints. The know-how and why of normal patterns aid analysts in detecting suspicious patterns quickly. Hence, a correctly benchmarked, well-configured, and integrated network and security data analysis system generates accurate alerts and events that are more reliable and can be trusted. These alerts are prioritized according to the severity of the analyst monitoring and fast response [7].

According to the SysAdmin, Audit, Network, and Security (SANS) institute log management survey [67], one of the limitations, as cited by respondents, is the inability to differentiate normal from abnormal patterns. Therefore, it is advantageous to use platforms that can build benchmarks by integrating network elements, endpoint security activity, and other IT systems compared to non-benchmarked systems.

- **Threat Intelligence**: According to SANS cyber threat intelligence (CTI) surveys [68], it is advantageous in security monitoring system capabilities to incorporate threat intelligence as per the OODA loop. It helps detect patterns while analyzing network elements, security endpoints, and other log events. These patterns are analyzed and correlated with old incidents, attacks, and anomalies data from the existing in-house knowledge management data center to enhance the detection capability of a compromised system or user before it exhibits the characteristics of a breach.
- **Fusion of hardware and software data**: With the advancement in technologies, the integrated dashboard can be presented to operators and analysts with an integrated global picture to monitor several interdependencies between interconnected network elements and security endpoints in real-time campaigns. This integrated dashboard is presently achievable in an integrated scenario wherein complete data from entire network

elements, and security endpoints are correlated, corrected, fused, and then presented to analysts on their dashboard for real-time monitoring and responses.

V. STATE-OF-THE-ART ARCHITECTURE OF AN INTEGRATED NOC AND SOC

The authors examined the definition, architecture, and building blocks of an integrated NOC and SOC in the previous section. This section introduces the second part of our main contribution, and the authors answer the first research question as shown in the research. This section mapped all the relevant academic literature and formulated a state-of-the-art architecture for an integrated NOC and SOC. However, some researchers have suggested a layered approach for the integrated NOC and SOC approach [16], while a few suggested a zone infrastructure concept [31].

The integration of NOC and SOC is not a one-time measure, rather a continuous development and integration process. New and more advanced threats continue to emerge [3], which necessitates new tools and better collaboration between NOC and SOC teams to handle them. Therefore, the authors have proposed a layered and scalable state-of-the-art architecture in which twin processes, technologies, and operators of NOC and SOC are combined under an integrated concept to remove duplicities. However, different processes, technologies, and operators are not merged and are brought directly under the integrated concept [16]. The state-of-the-art architecture of an integrated NOC and SOC consists of three layers, viz., physical data source, FCAPS/system management, and overall situational/service management layers.

A. PHYSICAL DATA SOURCE LAYER

This layer comprises all the integrated network elements and security endpoints that work similarly to the nervous system. Further, measurable data such as built-in tests, hardware, software serviceability maps, performance parameters, and various other logs are collaborated and used by the respective NMS in the higher system management layer for monitoring and management purposes. These critical integrated data are plugged in and connected to the service management layer via the logs and events integrator/aggregator for detailed analysis and processing. Fig. 10 shows the layered methodology of NOC, SOC and achieved integrated NOC and SOC.

B. FCAPS MANAGEMENT LAYER

In this layer, NMS performs real-time monitoring of the integrated network elements and security endpoints based on fault, configuration, administration, performance, and security management based on the FCAPS model [26] and works similar to an immune system. Network and security-related alerts, events, and performance statistics are generated from this layer and fed into the overall situational/service management layer through the logs and events integrator and consolidator for further real-time processing.

C. OVERALL SITUATIONAL MANAGEMENT LAYER

It is a top layer that works similarly to a human brain as it receives inputs from logs, events, and the nervous and immune systems, which are physical data and FCAPS/system layers. It generates a holistic overall situational picture and provides decision-making capabilities for the manager and operators to judge the operational impact of the incidents and assist in the recovery process. Furthermore, the logs and events from both lower layers are collected, correlated, mapped, and indexed under a centralized data center and used by integrated tools for performing various data-related tasks [16], [26]. Tasks such as incident management, auditing, detection, forecasting, and impact analysis are performed by this layer. The layer methodology of integrated NOC and SOC is shown in Fig. 11.

1) INCIDENT MODULE

A case management system is incorporated in this overall situational management layer, as defined in the previous section. It aids integrated management and operators in informed decision making and reduces human errors. It identifies regular reoccurring incidents and alarms analysts for their necessary actions. However, unresolved or critical incidents are escalated at higher tiers for detailed analysis by SME for quick resolution within defined SLA.

2) AUDITING MODULE

This module assists the integrated network and security team in auditing IT infrastructure as per policies invoked and detecting information security issues and bugs by scanning the entire network elements. This IT infrastructure assessment further exposes known vulnerabilities, if any, and alerts operators to quick responses.

3) DETECTING AND FORECASTING MODULE

This module assists in detecting and forecasting threats by using statistical analytics on previous performance trends based on the data warehouse, as discussed in an earlier section. The overall situational management layer flags out abnormal behavior based on benchmarking for necessary investigation. This information is statistically extrapolated, analyzed, and armed with the integrated manager for necessary actions to avoid organizational data breaches.

4) IMPACT ANALYSIS MODULE

This module correlates previous and current events from all IT infrastructure equipment and data centers to identify and assist the integrated teams on the probable root causes of an incident, the IT infrastructure involved, and the chain of events of the incident. It also analyzes the impact on the organization network and data breaches, if any. It provides recommendations and other corrections for service recovery.

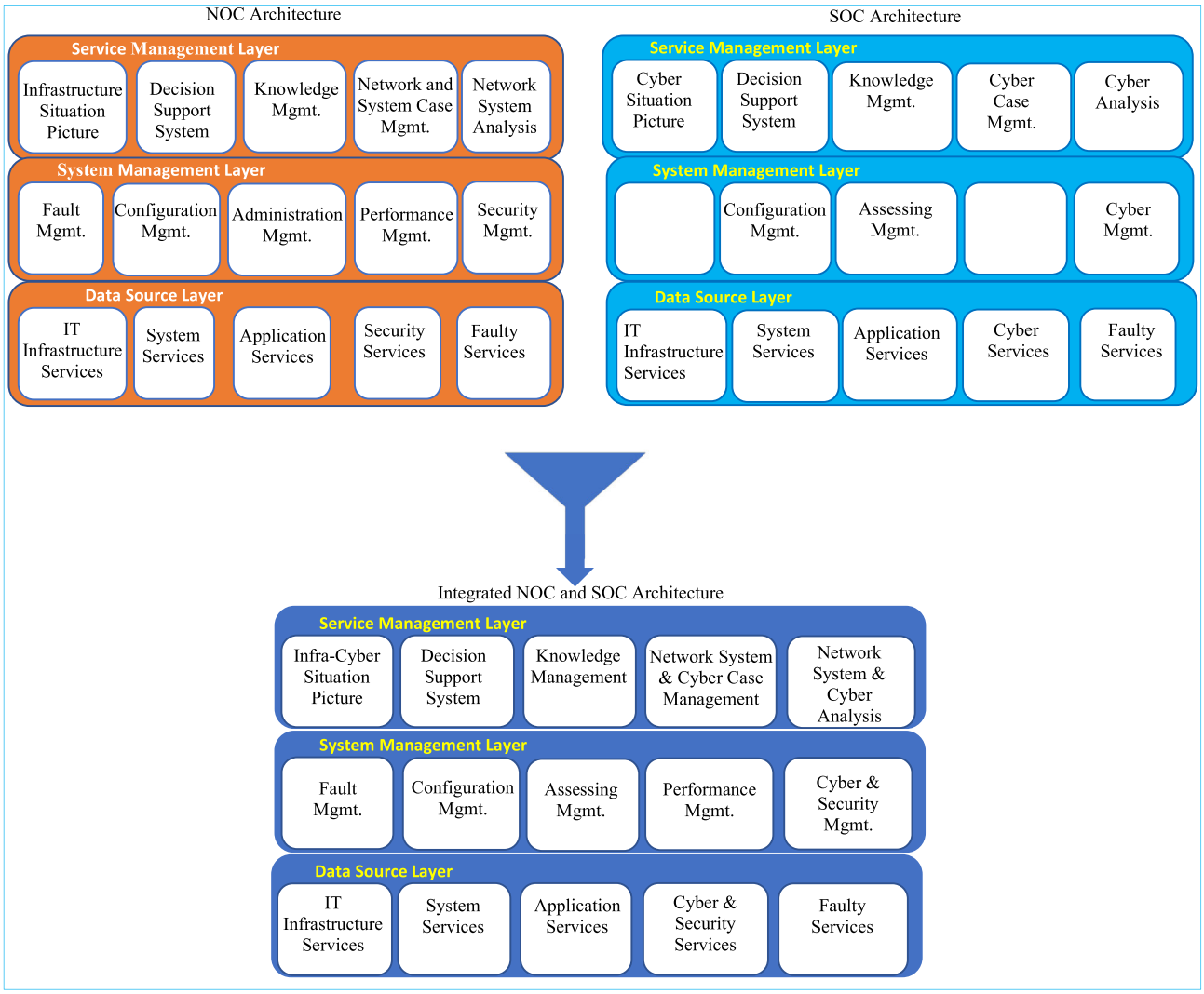

FIGURE 10. Layer architecture of integrated NOC & SOC.

VI. USEFULNESS OF INTEGRATED NOC AND SOC

In the previous sections, the authors show how the relevant literature has assisted in exploring the state-of-the-art architecture. This section discusses the usefulness of integrated NOC and SOC campaigns for organizations and businesses.

A. IMPROVED NETWORK AND SECURITY POSTURE

NOC teams usually receive various alerts related to performance issues on their dashboard, but most turn out to be security-related problems on detailed investigation [7], [18]. For example, denial of service attacks (DoS). Conversely, security issues may be the root cause of company or organizational network performance-related problems. For example, a recently configured firewall rule by the SOC personnel may inadvertently block the company or organization legitimate network traffic. Therefore, working together in an integrated approach can quickly resolve such issues of DoS and network performance with the collaboration of both teams in real-time. However, it would have taken extra time in the siloed approach and led to more security damage.

B. IMPROVED SERVICE LEVEL ASSURANCE AND RESPONSE TIME

As seen above, in an integrated network and security posture, the collaboration between NOC and SOC team members resolves the problem quickly in real-time. Furthermore, this quick response in resolving the issues has reduced the impact of the attack on the company or organization reputation [7], [18]. Therefore, the faster response time of an integrated approach indirectly leads to a better service-level agreement.

C. BETTER COST AND IMPROVED OPERATIONAL EFFICIENCY

Common toolkit duplicities are not available in the integrated NOC and SOC campaigns as they exist in siloed NOC and SOC operation, which cuts the overall cost to an organization [7], [10], [14], [18], [19], [30], [55], [56]. Furthermore, saving person-hours while resolving the issues in less time can lead to operational efficiency in an integrated scenario.

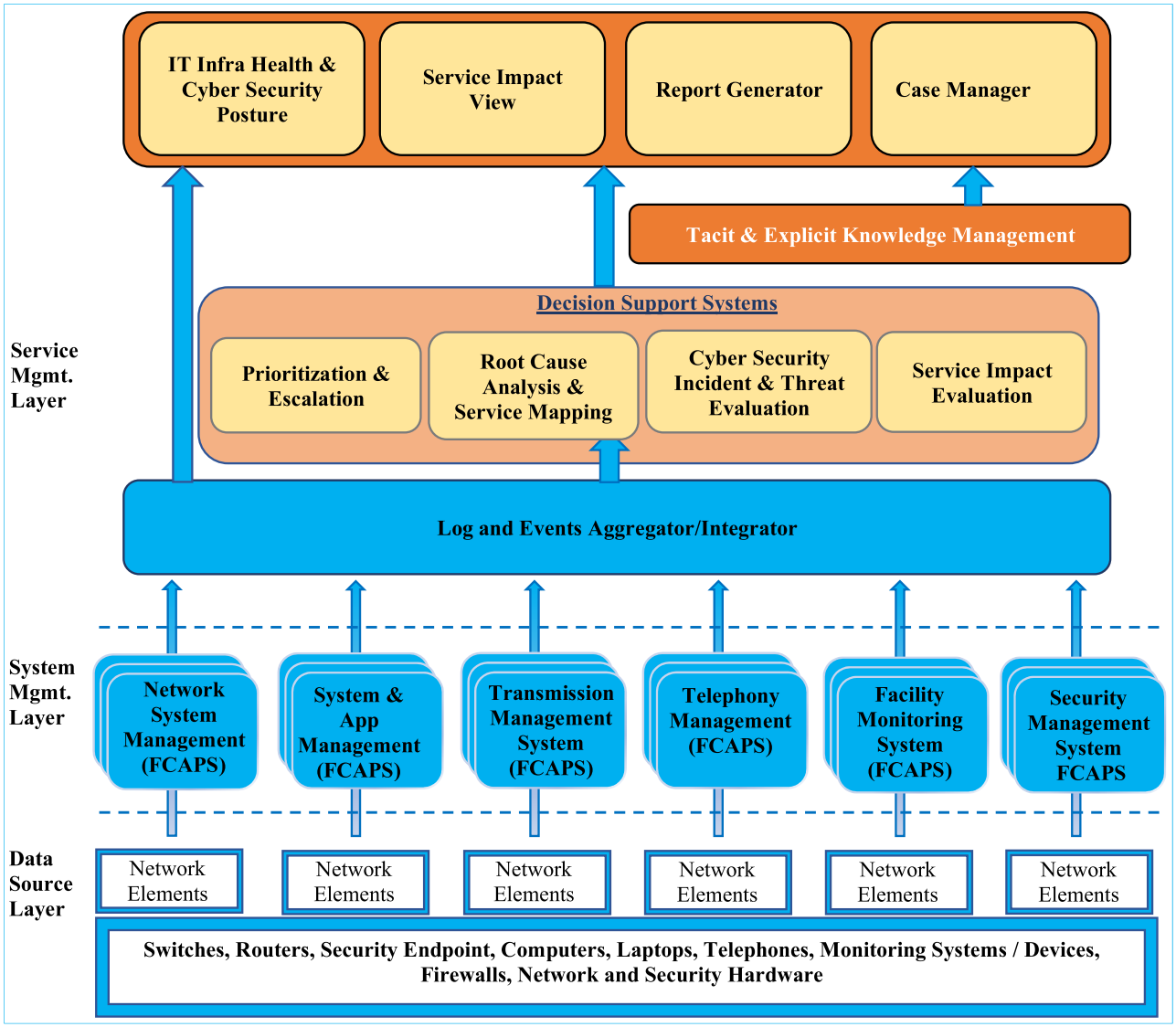

FIGURE 11. State-of-the-art architecture of an integrated NOC & SOC.

Hence, this reduces the NOC and SOC analysts time on common processes and functions and frees them up for network and security strategic planning and other activities of an organization.

VII. CHALLENGES

In the previous section, the authors discussed the usefulness of the integrated NOC and SOC. In this section, the authors answer the second research question as shown in the research. As seen in the relevant literature, each system faces different challenges depending on its working models, levels of integration, architecture, and organization size [7]. The integrated NOC and SOC also have a few challenges presented in the succeeding paragraphs according to the PPT framework adopted in this systematic analysis paper.

A. LIMITED INTEGRATED TOOLS FOR INTEGRATED NOC AND SOC

As seen in the NOC and SOC scenarios, the problem is further aggregated by configuring and using individual NOC and SOC tools, such as Syslog/SNMP-based, HP Open View, NetXMS, Zabbix, Monolith, Netcool SIEM based, Snort IDS, RSA Splunk, and others. Deploying separate NOC and SOC tools does not solve the overall integration approach vis-à-vis its advantages and efficiency [7], [16]. The configuration and maintenance process of tools is laborious and time consuming [34], [42], [45], [63], [64]. Wrongly configured tools aggregate the number of false positives, which further increases analyst tasks. Integrated and correctly configured tools are imperative in resolving a specific problem for the integrated scenario, which enhances the capabilities of integrated analysts. The integration of tools eases the analyst operation but poses a greater challenge [5], [15], [54].

For example, toolkits are available as per IT technologies and standards instead of integrated operational technologies, which leads to unreliability issues [69]. This scenario further aggregates complexities in performing routine tasks by analysts rather than inculcating a negative effect on the fault, threat identification, performance, and SLA for detection, protection, and resolution. Therefore, IT and operationally suited, correctly configured, and tested toolkits require time for an integrated campaign [7], [9], [11], [16] [17].

B. INSUFFICIENT LEVEL OF AUTOMATION

There is hardly any automation of the integrated NOC and SOC processes and their functionalities [52], [56], [70]. However, most work is performed manually in the current scenario, where trained personnel are hardly available. For example, network monitoring, threat scanning, events/alert monitoring, and incident tasks were monitored and performed manually. Automation has a solution to overcome the non-availability of trained workforce issues and is free from human errors while performing monotonous jobs such as alerts and event monitoring [5]. According to the relevant literature, the operational implementation of machine learning, artificial intelligence, and data science techniques to formulate and automate fault tracing, performance monitoring and alerting, and detection of attacks and other monotonous processes is possible. However, there are a few difficulties in the automation process of capturing tacit knowledge of analysts and SME. However, these techniques have been proven for siloed NOC and SOC operations but not for the integrated operation scenario.

Automation techniques in an integrated scenario and their effectiveness based on FCAPS monitoring, alerts and event generation and monitoring, incident management, and detecting attack processes need to be formulated, developed, compared, and tested. In addition, the automation process may yield more false positives vis-à-vis manual processing. Filtering such false-positive alters requires specific knowledge and experience based on expert tacit knowledge. Hence, capturing tacit knowledge in automation processes is a topic of future research. Therefore, in-depth research studies and development are to be carried out by academia and industry to evaluate their usability in an integrated scenario.

C. NON-DEFINED STANDARDS

Standards and industry best practices are yet to be formulated, developed, and implemented for an integrated NOC and SOC owing to its evolving technology compared to siloed NOC and SOC operations. Therefore, the practical viability of an integrated NOC and SOC is lacking because of the non-availability of defined standards. The lack of best practices also means no actual strategies or decision support for an organization. Therefore, decision-makers find it difficult to choose the best network and security operation model with the correct scope and capabilities to support an organization vision, network, and security strategies.

The non-availability of standards is also a concern in security operation centers [58]. Integrated NOC and SOC best practices and standards are imperative for the in-depth implementation of an integrated campaign with full benefits. However, a few such best practices on integrated NOC and SOC concepts have been suggested by the SANS institute and others [7], [11], [16]. However, they are not implemented due to the non-availability of recognized standards from industries as they are biased to a certain extent. Therefore, impartial and genuine industry policies need immediate attention and international standardization to overcome such biases.

VIII. CONCLUSION

This systematic analysis aims to map the relevant literature in identifying, analyzing, and defining the state-of-the-art architecture of an integrated NOC and SOC from a purely academic perspective. The objective is to analyze the relevant literature and collaborate with a holistic, workable, state-of-the-art architecture. The authors planned the analysis review by collecting and mapping numerous studies from electronic databases and the world wide web. Electronic databases were searched rigorously by including various keywords and terms relevant to NOC, SOC, and integrated NOC and SOC. The integrated NOC and SOC architecture components follow the people, process, and technology framework. The authors elaborated these integrated NOC and SOC architecture components as defined in the relevant academia. As revealed in the relevant literature, the researchers have not clarified the clear-cut definition, state-of-the-art architecture, and building blocks of an integrated NOC and SOC. However, only concept definition and a few integration methods are considered at the organization or industry level. The authors defined the state-of-the-art architecture of an integrated network and security operation center and identified the challenges that may hinder its future development and innovation. These challenges can serve as a yardstick for future research and development, as the proposed integration concept is the basis of continuous integration and continuous development campaigns.

One of the well-known challenges is the non-availability of integrated toolkits for integrated team members, which significantly impacts defined SLA. Cross-training and OJT with technical awareness enhance the resolution of the knowledge gap for better network and security posture. While looking at various processes in an integrated scenario, it is imperative to integrate and automate them to achieve better operational efficiencies. Further, the authors can see that the relevant literature lacks a concise definition of the specific processes incorporated and their correlation and interaction in an integrated scenario. Therefore, the non-availability of integrated process definitions may be difficult in developing state-of-the-art architectures.

To utilize the full potential of an integrated approach, the PPT framework needs to be synchronized with and collaborated amongst them and other IT infrastructures. In addition, there are limited and immature automation techniques

in the PPT framework of integrated network and security operation methodologies. Compared to the PPT components of an integrated NOC and SOC, international standards and standard operating procedures are lacking. This immaturity puts roadblocks to security audits and overall integrated NOC and SOC assessments. Further, the non-availability of standards prevents organizations from accepting and implementing integrated architecture concepts and future developments.

In summary, the integrated NOC and SOC campaign paves the way for organizations to prepare themselves in a more efficient and resilient way to counter any network or security threats or cyber-attacks in real-time. However, it needs to be planned thoroughly, integrated, and implemented after a successful proof of concept, assessed and validated regularly, and improved incrementally to unveil the full potential of integrated NOC and SOC. If followed correctly, they improve the organization ability to manage network, performance, threat detection, and security aspects seamlessly and prevent any performance bottlenecks, security compromises, data breaches, and overall organizational reputation.

REFERENCES

[1] (2020). *The History of NoC Monitoring Network*. Accessed: Sep. 2021. [Online]. Available: https://www.chrsolutions.com/assets/files/NoC-HistoryTimeline.pdf

[2] Y. G. Chon and B. Jaeger. (Dec. 13, 2007). *Efficiency Through NoC/SOC Convergence Under*. Accessed: Sep. 2021. [Online]. Available: https://www.csoonline.com/article/2121964/efficiency-through-NoC-soc-convergence.html

[3] K. Bissell and L. Ponemon. (Apr. 28, 2019). *The Cost of Cybercrime*. Ponemon. Accessed: Sep. 2021. [Online]. Available: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

[4] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," *IEEE Access*, vol. 8, pp. 1–25, 2020.

[5] S. McGillicuddy. (May 22, 2018). *NetOps & SecOps Collaboration: Shared Tools are Essential*. Accessed: Sep. 2021. [Online]. Available: https://www.kentik.com/blog/netops-secops-collaboration-shared-tools-are-essential/

[6] S. McGillicuddy, "Bridging the gap between NetOps and SecOps: NetSecOps," Enterprise Manage. Associates, Boulder, CO, USA, Tech. Rep., Jul. 2019, pp. 1–4. [Online]. Available: http://assets.extrahop.com/whitepapers/EMA-NetSecOps-White-Paper.pdf

[7] N. Hernandez, "NoC and SOC integration opportunities increased efficiency incident response cyber security," SANS Inst., Bethesda, MD, USA, Tech. Rep., 2018, pp. 1–26. [Online]. Available: https://sansorg.egnyte.com/dl/cNkVP4S4Ux

[8] J. David. (Dec. 10, 2008). *Secure Your Operations Through NoC and SOC Integration*. [Online]. Available: https://docplayer.net/2408670-Secure-your-operations-through-NoC-soc-integration.html

[9] J. Goodchild. (Nov. 15, 2009). *Network and Security Operations Convergence: A Mini-Case Study*. Accessed: Sep. 2021. [Online]. Available: http://www.networkworld.com/article/2237963/compliance/network-and-security-operations-convergence.html

[10] ExtraHop. (Jun. 10, 2019). *Five Quantifiable Reasons to Integrate Security and IT*. Accessed: Sep. 2021. [Online]. Available: https://www.forbes.com/sites/extrahop/2019/06/10/five-quantifiable-reasons-to-integrate-security-and-it/?sh=3563ec295d39

[11] N. Miloslavskaya, "Network security intelligence center as a combination of SIC and NoC," *Proc. Comput. Sci.*, vol. 145, pp. 354–358, Jan. 2018.

[12] S. Bocetta. (Jul. 27, 2021). *How to Bridge the Gap between Netops and Secops for Ultimate Network Management and Security*. Accessed: Sep. 2021. [Online]. Available: https://www.infoq.com/articles/netops-secops-closing-gap/?utm_campaign=infoq_content&utm_source=infoq&utm_medium=feed&utm_term=DevOps

[13] J. Lackey. (May 1, 2021). *NetOps and SecOps: Breaking Down the Silos*. Accessed: Sep. 2021. [Online]. Available: https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2020/05/01/netops_and_secopsb-pSxA.html

[14] M. Mann. (Apr. 15, 2021). *Whats Driving SOC-NoC Convergence*. Accessed: Sep. 2021. [Online]. Available: https://www.open-systems.com/blog/whats-driving-soc-NoC-convergence/

[15] Rebasoft. (Mar. 24, 2021). *Integrating NetOps/SecOps*. Accessed: Sep. 2021. [Online]. Available: https://www.rebasoft.net/netops-secops.php

[16] T. S. Hae, L. K. Thong, S. N. Matthew, and T. C. How, *Smart Network and Security Operations Centre*. Pretoria, South Africa: DSTA Horizons, pp. 24–31, 2016.

[17] N. Miloslavskaya, "Developing a network security intelligence center," *Proc. Comput. Sci.*, vol. 145, pp. 359–364, Jan. 2018.

[18] N. Weinberg. (May 14, 2020). *4 Key Benefits of NoC and SOC Integration and Tips for Making it Work*. Accessed: Sep. 2021. [Online]. Available: https://www.csoonline.com/article/3541582/4-key-benefits-of-nocsoc-integration-and-tips-for-making-it-work.html

[19] M. Roberson, "WhatWorks in SOC/NoC integration: Improving time to detect, respond and contain with ExtraHop reveal(x)," SANS Inst., North Bethesda, MD, USA, Tech. Rep., Jun. 2019. [Online]. Available: https://www.netdescribe.com/wp-content/uploads/2020/05/SANS-WhatWorks-Revealx-case-study.pdf

[20] C. Crowley and J. Pescatore, "Common and best practices for security operations centers: Results of the 2019 SOC survey," SANS Inst., North Bethesda, MD, USA, Tech. Rep., 2019. [Online]. Available: https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf

[21] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "PRISMA statement," *PLOS Med.*, vol. 6, no. 7, 2009, Art. no. e1000097.

[22] S. Kraus, M. Breier, and S. Dasí-Rodríguez, "The art of crafting a systematic literature review in entrepreneurship research," *Int. Entrepreneurship Manage. J.*, vol. 16, no. 3, pp. 1023–1042, Sep. 2020.

[23] K. S. Khan, R. Kunz, J. Kleijnen, and G. Antes, "Five steps to conducting a systematic review," *J. Roy. Soc. Med.*, vol. 96, no. 3, pp. 118–121, Mar. 2003.

[24] C. Okoli, "A guide to conducting a standalone systematic literature review," *Commun. Assoc. Inf. Syst.*, vol. 37, no. 1, pp. 880–910, 2015.

[25] D. Tranfield, D. Denyer, and P. Smart, "Towards a methodology for developing evidence-informed management knowledge by means of systematic review," *Brit. J. Manage.*, vol. 14, no. 3, pp. 207–222, Sep. 2003.

[26] S. Chavan. (Dec. 24, 2016). *Best Practices for Building Network Operations Center*. Accessed: Sep. 2021. [Online]. Available: https://www.slideshare.net/SatishChavan4/best-practices-for-building-network-operations-center

[27] J. Mathenge. (Feb. 23, 2021). *The Network Operations Center (NoC): How NOCs Work?* Accessed: Sep. 2021. [Online]. Available: https://www.bmc.com/blogs/NoC-network-operations-center/#

[28] A. Gorod, R. Gove, B. Sauser, and J. Boardman, "System of systems management: A network management approach," in *Proc. IEEE Int. Conf. Syst. Syst. Eng.*, Apr. 2007, pp. 1–5.

[29] S. Mcgillicuddy, "A guide to NetOps and SecOps collaboration," Enterprise Manage. Associates, Boulder, CO, USA, Tech. Rep., 2019, pp. 1–5. [Online]. Available: https://www.netscout.com/sites/default/files/2019-04/EMA-NETSCOUT-0219-WP2.pdf

[30] S. Bea. (Dec. 7, 2020). *7 reasons why its time for NetSecOps*. Accessed: Sep. 2021. [Online]. Available: https://accedian.com/blog/7-reasons-why-its-time-for-netsecops/

[31] N. Miloslavskaya, "Security zone infrastructure for network security intelligence centers," *Proc. Comput. Sci.*, vol. 169, no. 2019, pp. 51–56, 2020.

[32] G. Nizri. (Apr. 28, 2012). *Network Operations Center Best Practices & Challenges*. Accessed: Sep. 2021. [Online]. Available: https://www.thousandeyes.com/learning/techtorials/network-operations

[33] Ingram. (Jan. 13, 2021). *Managed NoC & Help Desk Services*. Accessed: Sep. 2021. [Online]. Available: https://s3.amazonaws.com/Professional_Services/ds/IMPreferred-managedNOC-helpdesk-DS.pdf

[34] C. Onwubiko, "Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, Jun. 2015, pp. 1–10.

[35] A. Torres, "Building a world-class security operations center: A roadmap," SANS Inst., Bethesda, MD, USA, Tech. Rep., 2015, pp. 1–10. [Online]. Available: https://www.academia.edu/38868050/Building_a_World-Class_Security_Operations_Center_A_Roadmap

[36] P. Jacobs, A. Arnab, and B. Irwin, "Classification of security operation centers," in *Proc. Inf. Secur. South Afr.*, Aug. 2013, pp. 1–7.

[37] Y. T. Duna, M. F. A. Razaka, M. F. Zolkiplib, T. F. Beea, and A. Firdaus, "Grasp on next generation security operation centre (NGSOC): Comparative study," *Int. J. Nonlinear Anal. Appl.*, vol. 12, no. 2, pp. 869–895, Apr. 2021.
[38] M. A. Majid and K. A. Z. Ariffi, "Success factors for cyber security operation center (SOC) establishment," in *Proc. INCITEST*, Jul. 2019, pp. 1–11.
[39] I. P. E. D. Nugraha, "A review on the role of modern SOC in cybersecurity operations," *Int. J. Current Sci. Res. Rev.*, vol. 4, no. 5, pp. 408–414, May 2021.
[40] S. Schinagl, K. Schoon, and R. Paans, "A framework for designing a security operations centre (SOC)," in *Proc. 48th Hawaii Int. Conf. Syst. Sci.*, Jan. 2015, vol. 3, no. 1, pp. 2253–2262.
[41] D. Nathans, *Designing and Building Security Operations Center*. Waltham, MA, USA: Elsevier, 2015.
[42] P. Danquah, "Security operations center: A framework for automated triage, containment and escalation," *J. Inf. Secur.*, vol. 11, no. 4, pp. 225–240, 2020.
[43] N. Miloslavskaya, "Analysis of SIEM systems and their usage in security operations and security intelligence centers," *1st Int. Early Res. Career Enhancement School Biologically Inspired Cogn. Archit.*, vol. 636, pp. 282–288, Aug. 2017.
[44] N. Miloslavskaya, "Security intelligence centers for big data processing," in *Proc. 5th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, Aug. 2017, pp. 7–13.
[45] M. Vielberth and G. Pernul, "A security information and event management pattern," in *Proc. 12th Latin Amer. Conf. Pattern Lang. Programs*, Valparaiso, Chile, 2018, pp. 1–12.
[46] N. B. Truong, U. Jayasinghe, T. W. Um, and G. M. Lee, "A survey on trust computation in the Internet of Things," *Trust Inf. Infrastructure (TII)*, vol. 33, pp. 1–20, Jan. 2016.
[47] A. K. Ganame, J. Bourgeois, R. Bidou, and F. Spies, *A Global Security Architecture for Intrusion Detection on Computer Networks*. Amsterdam, The Netherlands: Elsevier, pp. 30–47, 10, Mar. 2008.
[48] R. Bidou, J. Bourgeois, and F. Spies, "Towards a global security architecture for intrusion detection and reaction management," in *Information Security Applications*. Berlin, Germany: Springer, 2003.
[49] Extrahop. (Aug. 28, 2018). *An Executive Guide to Integrating SecOps and NetOps*. Accessed: Sep. 2021. [Online]. Available: https://assets.extrahop.com/whitepapers/Integrating NetOps and SecOps ebook.pdf
[50] S. McGillicuddy. (May 26, 2020). *NetOps-SecOps Collaboration has its Benefits and Challenges*. Accessed: Sep. 2021. [Online]. Available: https://www.techtarget.com/searchnetworking/feature/NetOps-SecOps-collaboration-has-its-benefits-and-challenges
[51] F. Amy and S. Karnam. (2012). *Top 10 Tips for Achieving Effective Security + Operations Collaboration*. Accessed: Sep. 2021. [Online]. Available: https://www.slideshare.net/sri747/top-10-tips-for-effective-socnoc-collaboration-or-integration
[52] Fortinet. (Aug. 23, 2018). *NoC-SOC Divide Bridging the Architectural Requirements Understanding the Key for Integration*. Accessed: Sep. 2021. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/ebook/bridging-the-NoC-soc-divide.pdf
[53] S. McGillicuddy. (May 21, 2019). *A Guide to NetOps and SecOps Collaboration*. Accessed: Sep. 2021. [Online]. Available: https://www.netscout.com/sites/default/files/2019-04/EMA-NETSCOUT-0219-WP2.pdf
[54] N. Miloslavskaya, "Network protection tools for network security intelligence centers," *Proc. Comput. Sci.*, vol. 190, pp. 597–603, Jan. 2021.
[55] J. Morrison. (Sep. 19, 2018). *NetOps and SecOps Collaboration Solves the Data Silo Problem*. Accessed: Sep. 2021. [Online]. Available: https://www.plixer.com/blog/netops-and-secops-collaboration-solves-the-data-silo-problem/
[56] C. Udeshi. (Nov. 20, 2018). *Why SOC and NoC Teams Can Benefit by Working Closely Together*. Accessed: Sep. 2021. [Online]. Available: https://blogs.infoblox.com/community/why-soc-and-NoC-teams-can-benefit-by-working-closely-together/
[57] D. McClelland. (Feb. 2, 2021). *NoC VS. SOC: What is the Difference?* Accessed: Sep. 2021. [Online]. Available: https://www.soscanhelp.com/blog/NoC-vs.-soc-whats-the-difference
[58] C. Zimmerman, *Ten Strategies of a World-Class Cybersecurity Operations Center*. Bedford, U.K.: MITRE Corp., 2014, pp. 1–346.
[59] ISO/IEC 10040. (1992). *ISO/IEC 10040:1998(EN) Information Technology—Open Systems Interconnection—Systems Management Overview*. Accessed: Sep. 2021. [Online]. Available: https://www.iso.org/obp/ui/#iso: std: iso-iec:10040: ed-2: v1: en
[60] S. C. Sundaramurthy, J. Case, T. Truong, L. Zomlot, and M. Hoffmann, "A tale of three security operation centers," in *Proc. ACM Workshop Secur. Inf. Workers*, New York, NY, USA, 2014, pp. 43–50.
[61] (Nov. 28, 2016). *ISO/IEC 27035-1:2016 Information Technology—Security Techniques—Information Security Incident Management—Part 1: Principles of Incident Management*. [Online]. Available: https://www.iso.org/standard/60803.html
[62] A. Business. (Oct. 24, 2020). *The AT&T Cybersecurity Incident Response Toolkit*. Accessed: Sep. 2021. [Online]. Available: https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response
[63] J. Oksanen, "Organizing a network operation centre on campus best practice document," CSC/Funet Led Working Group on AccessFunet, Helsinki, Finland, Tech. Rep. GN3-NA3-T4-NOC-BPD, Jan. 2013.
[64] Ashton and Metzler. (Jun. 20, 2008). *The Next Generation Network Operations Center How the Focus on Application Delivery is Redefining the NoC*. [Online]. Available: http://www.ashtonmetzler.com/Metzler_NOC_paper1.pdf
[65] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," NIST, Gaithersburg, MD, USA, Aug. 2012.
[66] S. McGillicuddy and J. Kies. (Sep. 22, 2018). *NetSecOps: Everything Network Managers Must Know About Collaborating With Security*. Accessed: Sep. 2021. [Online]. Available: https://assets.extrahop.com/whitepapers/EMA_Micro_Focus_NetSecOpsWebina_Sept2018.pdf
[67] SANS Institute. (Oct. 24, 2014). *SANS: 2014 Log Management Survey Report*. Accessed: Sep. 2021. [Online]. Available: https://titanwolf.org/Network/Articles/Article?AID=5ae1ec26-7542-4680-b506-a31486f20815#gsc.tab=0
[68] R. M. Lee. (Jan. 19, 2021). *2021 SANS Cyber Threat Intelligence (CTI) Survey Results*. Accessed: Sep. 2021. [Online]. Available: https://www.sans.org/webcasts/2021-cyber-threat-intelligence-cti-survey-results-116475/
[69] F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G.-J. Ahn, "Matched and mismatched SOCs: A qualitative study on security operations center issues," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, London, U.K., Nov. 2019, pp. 1955–1970.
[70] N. Smith. (Apr. 16, 2018). *An Overview of Fortinet Integrated NoC-SOC Solution*. Accessed: Sep. 2021. [Online]. Available: https://www.fortinet.com/blog/business-and-technology/fortinet-delivers-the-industry-s-first-integrated-NoC-soc-soluti
[71] B. Gallotta, J. A. Garza-Reyes, and A. Anosike, "Using the Delphi method to verify a framework to implement sustainability initiatives," in *Proc. Int. Conf. Ind. Eng. Oper. Manage.*, Bandung, Indonesia, 2018, pp. 1–12.

DEEPESH SHAHJEE is currently pursuing the M.Tech. degree in technology management with the Defence Institute of Advanced Technology (Deemed to be University), Pune, under the Ministry of Defence, India. His current research interests include cybersecurity, defence network, security operating centers, and artificial intelligence on the role of automation and cybersecurity within a defence organization.

NILESH WARE received the Ph.D. degree from the Indian Institute of Technology Delhi in the area of operations and supply chain management. He is currently an Assistant Professor with the Defence Institute of Advanced Technology (Deemed to be University), Pune, under the Ministry of Defence, India. His area of research mainly pertains to quality management, operations management, supply chain management, project management, and defence oriented problems. His research articles have been published in *Management Science Letters*, *Global Journal of Flexible Systems Management*, *Expert Systems with Applications*, *Industrial Engineering Journal*, and journals of national and international repute. He has guided around 30 M.Tech. students and four Ph.D. Scholars in various research areas.